User Guide

for

OmniVista 2500 NMS
Version 4.8R2

January 2024

Revision A

Part Number 060911-00

ALE USA Inc.
2000 Corporate Center Drive
Thousand Oaks, CA 91320
+1 (818) 880-3500

Table of Contents

1.0 Getting Started with OmniVista 2500 NMS....1-1
OmniVista 2500 NMS User Interface....1-1
Banner Links....1-2
Unacknowledged Alarm Display....1-3
Applications....1-3
Customizing the Dashboard....1-6
Configuration/Display Icons/Buttons....1-9
Working with Tables....1-11
Setting Up OmniVista 2500 NMS for Network Management....1-12
Discovering Devices....1-12
Editing Discovered Devices....1-13
Configuring Traps....1-15
Saving Changes....1-15
PolicyView QoS....1-16
2.0 The Dashboard....2-1
Banner Links....2-1
Applications....2-2
Unacknowledged Alarm Display....2-6
Widgets....2-6
Viewing Additional Information....2-7
Configuring the Widget Display....2-8
Linking to the Application....2-8
Customizing the Dashboard....2-8
Global Dashboard....2-8
WLAN Advanced Dashboard....2-10
IoT Dashboard....2-11
Performance Monitoring Dashboard....2-12
Application Widgets....2-12
Global Application Widgets....2-13
WLAN Advanced Widgets....2-18
IoT Widgets....2-18
3.0 Analytics....3-1
Using Analytics....3-2
Configuring Analytics....3-3

Reports 3-3
Report Options 3-4
Top N Applications 3-11
Top N Applications - Advanced 3-19
Top N Clients 3-28
Network Health 3-34
Configuring the Information Displayed 3-37
Top N Ports Utilization 3-38
Top N PoE Ports Utilization 3-43
Top N PoE Switches Utilization 3-47
Network Availability 3-49
Alarms 3-50
AP Uptime/Downtime 3-53
AP Uptime/Downtime Table 3-53
Average AP/Link Uptime Table 3-54
Statistics Overview 3-54
Basic Statistics Workflow 3-54
Automatic Statistics Workflow 3-55
Statistics 3-56
Profiles 3-66
Creating a Profile 3-67
Editing a Profile 3-68
Deleting a Profile 3-68
Viewing a Profile 3-69
Summary View 3-69
Switch Information 3-69
Applications Management 3-69
Creating Application Mapping 3-69
Editing Application Mapping 3-70
Deleting Application Mapping 3-70
Anomalies 3-70
Settings 3-71
Collection Profile 3-71
Analytics Configuration 3-71
Application Visibility Statistics Configuration 3-72
PoE Configuration 3-72

4.0 AP Registration 4-1
Stellar AP Bootup Sequence 4-2
Stellar AP Series Device Management Workflow 4-3
AP Device as an 802.1X Client 4-3
802.1X Authentication Use Cases 4-4
AP Security Recommendations 4-5
Access Points 4-5
Reviewing an AP 4-6
Adding an AP 4-7
Editing an AP 4-9
Zigbee Configuration 4-11
Deleting an AP 4-14
Resetting an AP 4-15
Zigbee Device Discovery 4-15
Rebooting an AP 4-15
Setting the AP LED Mode 4-15
Performing Actions on an AP 4-16
Access Point List 4-16
Managed/Unmanaged APs 4-16
Bridge APs 4-21
Remote Access Points 4-23
AP Group 4-28
Creating an AP Group 4-28
Editing an AP Group 4-35
Deleting an AP Group 4-35
Zigbee Device Discovery 4-35
AP Group List 4-35
Detailed Information 4-37
Certificate 4-41
Creating a Certificate 4-42
Editing a Certificate 4-42
Deleting a Certificate 4-42
Downloading a Certificate 4-42
Uploading an LDAP Certificate 4-42
Uploading an 802.1X Client Certificate 4-43
Uploading a Local RadSec Certificate 4-43

Uploading a Stellar BLE Certificate 4-45
Syslog Over TLS Certificate 4-45
Uploading....4-48
Stellar WIFI RTLS Certificate....4-48
Certificate List....4-48
Stellar BLE Data Format....4-50
Stellar WiFi RTLS Data Format 4-52
External Captive Portal Config File....4-53
Creating an External Captive Portal Config File 4-53
Editing an External Captive Portal Config File....4-54
Deleting an External Captive Portal Config File....4-54
Downloading an External Captive Portal Config File 4-54
External Captive Portal Config File List 4-54
IoT/Location/Advanced Analytics Server....4-54
Creating a Service 4-55
Editing a Service....4-57
Deleting a Service....4-57
IoT/Location/Advanced Analytics Server Information 4-57
Data VPN Servers 4-58
Creating a Data VPN Server....4-58
Editing a Data VPN Server 4-59
Deleting a Data VPN Server 4-59
Exporting VPN Settings 4-59
Data VPN Server List....4-59
5.0 App Launch....5-1
Edit Mode....5-1
Adding a Launch Icon....5-1
Editing a Launch Icon 5-2
Deleting a Launch Icon 5-2
Arranging Launch Icons....5-2
6.0 Application Visibility 6-1
Application Visibility Application....6-1
Application Visibility Configuration....6-2
Devices Management....6-3
List of Devices/AP Groups....6-3
Signature Files....6-5

Viewing Signature Files 6-5
Importing a Signature File....6-5
Upgrading a Signature File 6-6
Deleting a Signature File 6-6
Signature Profiles 6-6
Viewing Signature Profiles....6-6
Creating a Signature Profile....6-7
Editing a Signature Profile 6-8
Cloning a Signature Profile 6-8
Applying a Signature Profile 6-9
Removing a Signature Profile 6-9
Deleting a Signature Profile 6-9
Summary View....6-10
Settings....6-10
Audit Configuration 6-10
Update Configuration....6-11
7.0 Audit 7-1
Log Files by Type 7-1
Viewing Log Files....7-3
Searching Through Log Files....7-4
Filtering Log File Entries 7-5
Downloading Log Files 7-5
All Current Logs 7-5
Collect Support Information 7-5
Collecting Log Files 7-5
User Activity Report 7-6
Settings....7-6
8.0 Authentication Servers 8-1
LDAP Servers 8-2
RADIUS Servers....8-2
ACE Servers 8-2
TACACS+ Servers....8-2
LDAP Server Management....8-3
Adding an LDAP Server....8-3
Modifying an LDAP Server 8-4
Deleting an LDAP Server....8-5

Configuring an LDAP Server 8-5
LDAP Server Management Table....8-6
RADIUS Server Management....8-7
Adding a RADIUS Server 8-8
Editing a RADIUS Server....8-8
Deleting a RADIUS Server 8-8
Configuring a RADIUS Server 8-9
RADIUS Server Management Table....8-9
ACE Server Management....8-10
Adding an ACE Server....8-10
Deleting an ACE Server....8-10
Configuring an ACE Server 8-10
TACACS+ Server Management 8-11
Adding a TACACS+ Server 8-11
Editing a TACACS+ Server 8-12
Deleting a TACACS+ Server 8-12
TACACS+ Server Management Table 8-12
9.0 Captive Portal 9-1
Configuration 9-1
Creating a Captive Portal Configuration 9-2
Editing a Captive Portal Configuration....9-2
Assigning a Captive Portal Configuration 9-2
Deleting a Captive Portal Configuration....9-2
Profile 9-2
Creating a Captive Portal Profile 9-3
Editing a Captive Portal Profile....9-3
Assigning a Captive Portal Profile 9-3
Deleting a Captive Portal Profile....9-3
Profile Domain Policy List....9-4
Creating a Profile Domain Policy....9-4
Editing a Profile Domain Policy....9-4
Assigning a Profile Domain Policy....9-4
Deleting a Profile Domain Policy 9-4
Domain Policy List....9-5
Creating a Captive Portal Domain Policy List....9-5
Editing a Captive Portal Domain Policy List....9-5

Assigning a Captive Portal Domain Policy List 9-5
Deleting a Captive Portal Domain Policy List 9-5
Customization 9-5
Creating a Captive Portal Customization 9-6
Editing a Captive Portal Custom File 9-7
Applying a Captive Portal File 9-7
Deleting a Captive Portal Customization 9-7
View 9-7
10.0 CLI Scripting 10-1
CLI Script 10-2
Pre-Configured Scripts 10-2
Creating a Script File 10-2
Importing a Script File 10-7
Editing a Script File 10-8
Sending a Script File 10-8
Deleting a Script File 10-9
CLI Script Details 10-9
Logs 10-9
Displaying a Log File 10-9
Exporting a Log File 10-10
Deleting a Log File 10-10
Terminal 10-10
Connecting to a Device 10-10
Session Preferences 10-10
Settings 10-11
11.0 Control Panel 11-1
Watchdog 11-1
Scheduler Jobs 11-2
Starting/Stopping Scheduled Jobs 11-2
Viewing Scheduler Jobs 11-2
Editing a Scheduled Job 11-3
Deleting a Scheduled Job 11-4
Scheduler History 11-5
Session Management 11-5
Session Information 11-5
12.0 Discovery Overview 12-1

Managed Devices 12-2
Discovering/Re-Discovering Devices 12-2
Discovering Stellar AP Series Devices 12-4
Enabling/Disabling IoT 12-4
Enabling/Disabling Statistics 12-4
Enabling/Disabling Network Advisor Monitoring 12-4
Adding a Device 12-4
Cloning a Device 12-8
Editing a Device 12-8
Deleting a Device 12-8
Searching for a Device 12-9
Perform Device Operations 12-9
OmniVista Network Advisor 12-11
Installing/Configuring SecureCRT 12-15
Discovery Displays 12-17
Graphical Views 12-25
Discovery Profiles 12-26
Creating a Discovery Profile 12-26
Editing a Discovery Profile 12-28
Deleting a Discovery Profile 12-28
Profile Information 12-28
NaaS Device Licenses 12-30
Licensed Device List 12-30
Device License Details 12-31
Device License Status 12-32
Third-Party Devices Support 12-32
Adding Third-Party Device Support 12-32
Editing Third-Party Device Support 12-33
Deleting Third-Party Device Support 12-34
Mibset List 12-34
Import MIBs 12-34
Importing MIBs 12-35
Hardware Inventory 12-35
Asset Information 12-35
Ports 12-36
Port Information 12-36

Link 12-37
Creating a Link 12-37
Cloning a Link 12-38
Editing a Link 12-38
Deleting a Link 12-38
Existing Links Table 12-38
Scheduled Upgrades 12-39
Creating a Scheduled Upgrade 12-39
Editing a Scheduled Upgrade 12-41
Deleting a Scheduled Upgrade 12-41
Scheduled Upgrade List 12-41
FAQs/Troubleshooting 12-42
SPB Service Port 12-43
Service Port Information 12-43
Settings 12-43
Setting Frequencies 12-43
IP Failover 12-45
Switch Monitoring 12-45
Other Settings 12-45
13.0 External Apps 13-47
14.0 Groups 14-48
MAC Groups 14-48
Creating a MAC Group 14-48
Editing a MAC Group 14-49
Deleting a MAC Group 14-49
VLAN Groups 14-49
Editing a VLAN Group 14-49
Deleting a VLAN Group 14-50
Network Groups 14-50
Creating a Network Group 14-50
Editing a Network Group 14-50
Deleting a Network Group 14-50
Multicast Groups 14-50
Creating a Multicast Group 14-51
Editing a Multicast Group 14-51
Deleting a Multicast Group 14-51

Service Groups 14-51
Creating a Service Group 14-51
Editing a Service Group 14-51
Deleting a Service Group 14-51
Services 14-52
Creating a Service 14-52
Editing a Service 14-52
Deleting a Service 14-52
Service Port 14-52
Creating a Service Port 14-53
Editing a Service Port 14-53
Deleting a Service Port 14-53
15.0 IoT 15-1
IoT Overview 15-2
IoT Prerequisites 15-2
Enabling IoT 15-2
NTP Requirements 15-3
Internet Requirements 15-3
Troubleshooting 15-3
IoT Logs 15-3
Alcatel IP Phones 15-3
Inventory 15-3
Inventory List 15-4
Configuring Google Workspace 15-9
Configuring OmniVista for Zigbee Support 15-10
Assigning a Custom Category to a Device 15-10
Category 15-11
Creating a Custom Category 15-11
Editing a Custom Category 15-12
Deleting a Custom Category 15-12
Category List 15-12
Enforcement 15-12
Configuring IoT Enforcement 15-12
Configuring IoT Enforcement Exceptions 15-14
Settings 15-15
IoT Configuration 15-15

16.0 IP Multicast (PIM) 16-1
PIM Global Configuration 16-1
Creating a PIM Global Profile 16-2
Editing a PIM Global Profile 16-2
Assigning a PIM Global Profile 16-2
Removing a PIM Global Profile 16-2
Deleting a PIM Global Profile 16-2
PIM Interface 16-3
Displaying PIM Interfaces 16-3
Creating a PIM Interface 16-3
Deleting a PIM Interface 16-3
PIM Candidate 16-3
Creating a PIM Candidate Profile 16-4
Editing a PIM Candidate Profile 16-4
Deleting a PIM Candidate Profile 16-4
PIM Device View 16-5
17.0 License Management 17-1
License Home Screen 17-1
Licenses 17-2
Device Licenses 17-3
Service Licenses 17-3
Add/Import a New License 17-4
OmniVista Licensing Options 17-4
Device License Options 17-5
Service License Options 17-5
Important Notes for Updating Licenses 17-5
Add or Import License 17-7
18.0 Locator 18-1
Locator Screen 18-2
Search Type 18-2
Search Results 18-3
Browse Screen 18-3
Settings Screen 18-3
Locate 18-3
Locating a Switch 18-3
ARP Results Table 18-5

Netforward Results Table 18-5
Locate on Map 18-9
Browse 18-9
Browse Results 18-9
Settings 18-13
General 18-13
Data Retention Policy 18-14
Locator Data Statistics 18-14
19.0 Multimedia Services 19-1
mDNS Flow 19-2
Gateway mDNS 19-2
Responder mDNS 19-2
Legacy mDNS 19-3
Gateway Devices 19-3
Creating an mDNS Gateway 19-3
Editing an mDNS Gateway 19-4
Deleting an mDNS Gateway 19-4
Gateway Devices Table 19-4
Responder 19-4
Responder Devices 19-5
Edge Devices 19-9
Service Rules 19-10
Server Policies 19-11
Client Policies 19-12
Server Cache 19-14
Legacy mDNS 19-14
Configuring mDNS for a Device 19-14
Editing an mDNS Configuration 19-15
Deleting an mDNS Configuration 19-15
Viewing mDNS Configurations 19-15
Poll 19-16
mDNS Sharing 19-16
Creating a Sharing Rule 19-16
Editing a Sharing Rule 19-16
Deleting a Sharing Rule 19-16
mDNS Sharing List 19-16

20.0 Notifications 20-1
Notifications Home 20-2
Viewing Traps 20-2
Acknowledging/Deleting Specific Traps 20-4
Acknowledging/Deleting All Traps 20-4
Polling Devices for Traps 20-4
Trap Definition 20-5
Viewing Trap Definitions 20-5
Editing a Trap 20-5
Trap Responder 20-6
Creating a Trap Responder 20-6
Editing a Trap Responder 20-11
Deleting a Trap Responder 20-11
Viewing Trap Responders 20-11
Trap Configuration 20-11
Device Selection 20-12
Configure Traps 20-12
Summary 20-13
Settings 20-14
Notification Configuration 20-14
Trap E-Mail Configuration 20-14
21.0 OV System Health 21-1
VA Health Information 21-1
Viewing Options 21-2
Detailed Views 21-2
Settings 21-3
Threshold Settings 21-3
Trap Setting 21-3
Data Collection 21-3
Refresh Setting 21-3
22.0 PolicyView 22-1
Creating Policies for Users and Groups 22-2
Creating Policies for Resources 22-2
Creating One Touch Policies 22-2
View/Modify Policies and Policy Lists 22-2
Expert Mode 22-3

Creating Policies for Applications 22-3
QoS-Qualified Devices 22-3
Saving Changes to the Switch 22-3
Required Traps 22-4
Policy Precedence and Conflicts 22-4
Users and Groups Policies 22-4
Unified Policies 22-4
Unified Policy List 22-14
Resource Policies 22-17
Add to Policy List 22-17
Resource 22-18
Resource Group 22-18
One Touch Policies 22-19
One Touch Data Policies 22-19
One Touch ACL Policies 22-22
One Touch Voice Policies 22-23
One Touch Voice MAC Policies 22-25
Policies and Policy Lists 22-26
Policies 22-26
Policy Lists 22-27
Policies by Switch 22-28
Expert Mode 22-30
Creating a Custom Policy 22-30
Applying a Custom Policy to the Network 22-30
Editing a Custom Policy 22-31
Deleting a Custom Policy 22-31
Policy Information 22-31
23.0 Preferences 23-1
User Settings 23-2
Locale 23-2
Theme 23-3
Inactivity Timeout 23-3
Table/List View Mode 23-4
Temperature Unit 23-4
Device Naming Pattern 23-4
Colors 23-4

Sounds....23-5
System Settings....23-6
Branding....23-6
Proxy....23-6
ProActive Lifecycle Management....23-6
Videos....23-10
Email....23-10
SMS....23-10
CA Certificate Import....23-11
Install Zulu CEK....23-12
Collect Support Info....23-12
Enforce Strong Password....23-12
Google Map API....23-12
24.0 Provisioning....24-1
Provisioning Overview....24-2
Provisioning Prerequisites....24-2
DCHP/DNS Configuration....24-2
Configure the Cloud Agent (Currently-Deployed Switches Only)....24-3
Basic Deployment Workflow....24-3
New Switches....24-3
Currently-Deployed Switches....24-5
Matching a Rule....24-6
Thin Switch Deployment Overview....24-7
Thin Switch Deployment Workflow....24-7
Troubleshooting....24-9
Provisioning Fails....24-9
Provisioning Logs....24-9
Rules....24-9
Creating a Provisioning Rule....24-10
Editing a Provisioning Rule....24-17
Deleting a Provisioning Rule....24-17
Rules List....24-17
Results....24-18
Golden Configuration....24-19
Force Provisioning....24-23
Results Table....24-24

Settings....24-25
Enable/Disable Auditing....24-26
Thin-Client Mode....24-26
Action When No Matching Rule Is Configured....24-26
Frequency of Audit....24-27
25.0 Quarantine Manager....25-1
Quarantine Manager Requirements....25-2
Hardware/Software Requirements....25-2
OmniVista Hardware/Software....25-2
Configuration Requirements....25-3
Candidates....25-4
Candidates Quarantine List....25-4
Fortinet Web Site....25-5
Banned....25-5
Adding a Device to the Banned List....25-6
Editing a Device on the Banned List....25-6
Releasing a Device from the Banned List....25-6
Retry....25-6
Re-Polling for Banned Devices....25-6
Banned Quarantine List....25-6
Never Banned....25-7
Adding a Device to the Never Banned List....25-7
Editing a Device on the Never Banned List....25-7
Deleting a Device from the Never Banned List....25-7
Never Banned Quarantine List....25-7
Disabled Ports....25-8
Release a Device from the Disabled Port List....25-8
Edit a Device in the Disabled Port List....25-8
Retry a Port Operation....25-8
Disabled Port List....25-8
Rules....25-9
Quarantine Manager Rule Overview....25-9
Rule Types....25-9
Built In Rules....25-9
Custom Rules....25-10
Regular Expressions Overview....25-11

Creating a Quarantine Manager Rule 25-13
Editing a Quarantine Manager Rule 25-14
Deleting a Quarantine Manager Rule 25-14
Enabling/Disabling a Quarantine Manager Rule 25-14
Importing a Quarantine Manager Rule 25-14
Quarantine Manager Rule List 25-15
Configuration 25-16
Quarantined Manager Remediation (QMR) 25-16
Configuring Quarantine Manager 25-16
Configuring Quarantine Manager 25-17
Assigning Quarantine Manager to Network Devices 25-18
Creating Quarantine Subnets (Optional) 25-18
Configuring Quarantine Manager on OmniAccess WLAN Devices 25-18
Responders 25-19
Creating a Quarantine Manager Responder 25-19
Editing a Quarantine Manager Responder 25-20
Deleting a Quarantine Manager Responder 25-20
Automatic Event Responders List 25-20
TAD Profile 25-21
Creating a TAD Profile 25-21
Assigning a TAD Profile 25-22
Editing a TAD Profile 25-23
Deleting a TAD Profile 25-23
Monitoring Group List 25-23
TAD View 25-24
Monitoring Groups 25-24
Port Ranges 25-24
Statistics Port 25-24
Statistics Anomaly Traffic 25-25
Statistics Anomaly Summary 25-25
Settings 25-25
SysLog Listener 25-25
SysLog Generator Target 25-26
26.0 Report 26-1
Report Configuration 26-1
Creating a Report 26-2

Editing a Report 26-3
Deleting a Report 26-3
Report List 26-3
27.0 Resource Manager 27-1
Backup/Restore 27-2
Performing a Backup 27-2
Editing a Configuration Backup File 27-5
Deleting a Backup 27-5
Exporting/Viewing Backup Files 27-5
Backup Information 27-6
Important Facts About Back Ups 27-7
Performing a Restore 27-8
File Selection 27-8
Configuration 27-8
Compare 27-9
Selecting Files 27-9
Comparing Files 27-9
Summary View 27-9
Summary View Table 27-10
Upgrade Image 27-10
Importing the Upgrade Files 27-11
Installing the Upgrade Files 27-11
ISSU Upgrade 27-13
AOS Release 7 27-14
AOS Release 8 27-14
Important Information About Upgrades 27-14
File Sets Information 27-15
Inventory 27-15
Creating an Inventory Report 27-15
Auto Configuration 27-16
Auto Configuration Overview 27-16
Auto Configuration on a New Switch 27-17
Automatic Configuration Updates 27-17
Creating an Instruction File 27-19
Editing an Instruction File 27-20
Deleting an Instruction File 27-20

The Instruction Files List 27-21
Switch File Set 27-22
Overview 27-22
Creating a Switch File Set 27-23
Assigning a Switch File Set 27-23
Editing a Switch File Set 27-24
Deleting a Switch File Set 27-24
Settings 27-24
Backup Retention Policy 27-24
BMF Upgrade Settings 27-24
28.0 SAA 28-1
SAA Prerequisites 28-2
Enable SAA Traps 28-2
Configure SAA Metrics 28-2
Configuring SAAs 28-2
Ethernet OAM 28-2
Creating an SAA 28-3
Editing an SAA 28-4
Deleting an SAA 28-4
SAA Ethernet List 28-4
Viewing SAA Statistics 28-5
Table Display 28-6
Profile Association 28-6
Creating an SAA VM Profile 28-6
SAA VM Profiles and VM Movement 28-7
Deleting an SAA VM Profile 28-7
SAA Profiles List 28-8
Viewing SAA VM Profile Statistics 28-8
Table Display 28-9
Settings 28-10
Ethernet Config 28-10
MAC Config 28-10
29.0 Services 29-1
SPB Overview 29-2
Service 29-2
Creating a Service 29-2

Editing a Service....29-4
Deleting a Service....29-5
Service Table....29-5
Polling Switches for SPB Information....29-7
L2 Profiles....29-7
Creating a Profile....29-7
Editing a Profile....29-7
Deleting a Profile....29-8
L2 Profiles Table....29-8
Polling Switches for SPB Information....29-8
Global Settings....29-8
Selecting Switches for SPB Configuration....29-8
Polling Switches for SPB Information....29-8
30.0 SIP....30-1
SIP Overview....30-2
Active Calls....30-3
Viewing Active Call Records....30-3
Ended Calls....30-5
Viewing Ended Call Records....30-5
One Touch Profile....30-8
SIP One Touch Profile Parameters....30-8
Creating a SIP One Touch Profile....30-9
Editing a SIP One Touch Profile....30-9
Deleting a SIP One Touch Profile....30-9
Removing a SIP One Touch Profile....30-10
Applying a SIP One Touch Profile....30-10
Viewing SIP One Touch Profiles....30-10
SIP Profile....30-10
Creating a SIP Profile....30-10
Editing a SIP Profile....30-11
Deleting a SIP Profile....30-11
Applying a SIP Profile....30-11
Viewing SIP Profiles....30-12
Global Params Profile....30-13
Trusted Servers Profile....30-14
Threshold Profile....30-16

SOS Profile 30-17
TCP Port Profile 30-18
UDP Port Profile 30-19
Device View 30-20
SIP Profile 30-21
TCP Port Profile 30-21
UDP Port Profile 30-21
Global Param Profile 30-22
Trusted Server Profile 30-22
Threshold Profile 30-22
SOS Profile 30-22
SIP Statistics 30-22
31.0 Topology 31-1
Topology Maps 31-2
Working with Topology Maps 31-3
Working with Geo Maps 31-22
Creating/Cloning/Editing/Deleting Maps 31-27
Working with Network Devices 31-28
Installing/Configuring SecureCRT 31-34
32.0 Unified Access 32-1
Unified Profile 32-1
Authentication and Classification 32-2
Configuring Unified Profile 32-3
Workflow 32-3
Unified Profile Templates 32-4
Client Isolation: Allowed Contacts List 32-21
Device Config 32-54
Configuration Information 32-57
Access Role Profile Information 32-65
Profile Polling 32-85
33.0 UPAM 33-1
Summary 33-1
Authentication 33-2
Summary 33-3
Workflow 33-4
NAS Clients 33-5

Access Policy....33-7
Authentication Strategy....33-10
Attribute for LDAP....33-13
Role Mapping for LDAP/AD....33-13
Employee Account....33-15
Company Property....33-16
Company Property....33-19
Switch User Account....33-22
Authentication Record....33-25
Captive Portal Access Record....33-30
Switch Access Record....33-30
Guest Access....33-32
Summary....33-32
Guest Access Strategy....33-33
Guest Account....33-62
Guest Device....33-70
Self-Registration Request....33-74
Guest Operator....33-75
Global Configuration....33-76
BYOD Access....33-78
Summary....33-79
BYOD Access Strategy....33-79
BYOD Device....33-81
Settings....33-86
Email Server....33-87
External Log Server....33-87
LDAP/AD Configuration....33-88
LDAPS Certificates....33-90
External RADIUS....33-90
Captive Portal Page....33-92
RADIUS Server Certificates....33-94
Additional Trust CA....33-95
Captive Portal Certificates....33-96
RADIUS Attribute Dictionary....33-99
RADIUS Attribute Dictionary List....33-100
Web Content Filtering....33-100

Web Content Filtering Workflow 33-101
Creating a WCF Profile 33-101
Editing a WCF Profile 33-102
Deleting a WCF Profile 33-102
WCF Profile List 33-102
34.0 Users and User Groups 34-1
Security Levels 34-2
Default Groups, Users, Roles 34-2
Working with User Groups, Users, and User Roles 34-3
Two-Factor Authentication 34-3
Role Management 34-3
Creating a User Role 34-4
Editing a User Role 34-5
Deleting a User Role 34-5
Existing Roles Table 34-5
User Role Feature 34-5
Group Management 34-6
Creating a User Group 34-7
Editing a User Group 34-7
Deleting a User Group 34-7
Existing Groups Table 34-7
User Management 34-7
Creating a User 34-8
Editing a User 34-8
Deleting a User 34-8
Existing Users Table 34-8
Authentication Server 34-8
Configuring External RADIUS Server Authentication 34-9
Configuring CPPM RADIUS Authentication 34-14
Two-Factor Authentication 34-16
Two-Factor Authentication User Set Up and Login 34-17
Two-Factor Authentication Table 34-20
35.0 VLAN Manager 35-1
VLAN Overview 35-1
VLANs Table 35-2
Creating a VLAN 35-3

Creating VLANs by Device 35-4
Creating VLANs by Maps 35-6
Editing a VLAN 35-7
Copying a VLAN 35-7
Deleting a VLAN 35-7
VLAN Actions....35-7
Enabling/Disabling VLANs....35-7
Viewing/Modifying Spanning Tree 35-8
Viewing/Configuring IP Routers....35-13
VLAN Details 35-15
Basic Information 35-15
Detailed View....35-16
MVRP 35-18
Summary View....35-18
Configuring MVRP 35-20
IP Interface 35-22
Creating an IP Interface....35-22
Editing an IP Interface 35-23
Deleting an IP Interface 35-23
Viewing IP Interfaces....35-23
Poll....35-25
VLAN Template 35-26
Creating a VLAN Template....35-26
Editing a VLAN Template 35-26
Deleting a VLAN Template 35-26
VLAN Template List....35-26
36.0 VM Manager 36-1
Virtualization/VM Manager Overview....36-2
Virtualization 36-2
Configuring VM Manager....36-5
Hypervisor Systems....36-6
Creating a VM Server 36-6
Editing a VM Server....36-7
Deleting a VM Server....36-7
Hypervisor Systems Table....36-7
VM Locator - Host Networks....36-7

Searching for Host Machines....36-7
Host Network Table....36-7
VM Locator - VM Networks....36-9
Searching for Virtual Machines....36-9
VM Networks Table....36-10
Exclude VLAN....36-11
Creating an Exclude VLAN....36-11
Editing and Exclude VLAN....36-12
Deleting an Exclude VLAN....36-12
Exclude VLAN List....36-12
VM VLAN Configuration....36-12
VM VLAN Configuration - Apply UNP VLAN....36-12
VM VLAN Configuration - Enable MVRP Ports....36-13
VM VLAN Configuration - Enable One-Touch SPB....36-13
VLAN Notification....36-13
Resolving a VM Configuration Problem....36-14
Notification List....36-15
VMM Devices List....36-15
VMM Devices List....36-15
Settings - VM Polling....36-17
Settings - SBP....36-17
37.0 VXLANs....37-1
VXLAN Service....37-2
Creating a VXLAN Service....37-2
Creating an Service Distribution Point (SDP) Tunnel....37-3
Re-Applying a VXLAN Service....37-3
Editing a VXLAN Service....37-4
Deleting a VXLAN Service....37-4
SAP Profile....37-4
Creating a SAP Profile....37-4
Assigning a SAP Profile....37-4
Editing a SAP Profile....37-5
Deleting a SAP Profile....37-5
Access Port Profile....37-5
Creating an Access Port Profile....37-6
Editing an Access Port Profile....37-6

Deleting an Access Port Profile 37-6
VXLAN Device View 37-6
VXLAN Information 37-6
VM Snooping Overview 37-8
VM Snooping Profile 37-9
VM Snooping Statistics 37-11
Device View 37-12
38.0 WLAN 38-1
SSIDs 38-1
Creating an SSID 38-2
Editing an SSID 38-20
Deleting an SSID 38-20
Applying an SSID 38-21
Editing an SSID AP Group/Schedule 38-22
Enabling/Disabling an SSID 38-22
SSIDs Table 38-22
WLAN Service (Expert) 38-24
Creating a WLAN Service Profile 38-24
WIPS 38-34
Network Overview 38-35
WIPS Views and Policies 38-36
Intrusive AP 38-40
Wireless Attacks 38-42
RF Management 38-42
RF Profile 38-43
RF Scan View 38-52
Heat Map 38-53
Creating a Heat Map 38-54
Editing a Heat Map for a Floor 38-58
Deleting a Heat Map 38-59
Viewing Heat Maps 38-59
Floor Plan 38-59
Creating a Floor Plan 38-60
Viewing Wi-Fi Coverage 38-63
Editing a Floor Plan 38-63
Deleting a Floor Plan 38-63

Exporting a Floor Plan as a PDF 38-64
Floor Plan List....38-64
Client 38-64
Client Summary 38-64
Wireless Client List 38-65
Wired Client List....38-67
Wireless Client Session 38-68
Wired Client Session 38-69
Client Blacklist 38-69

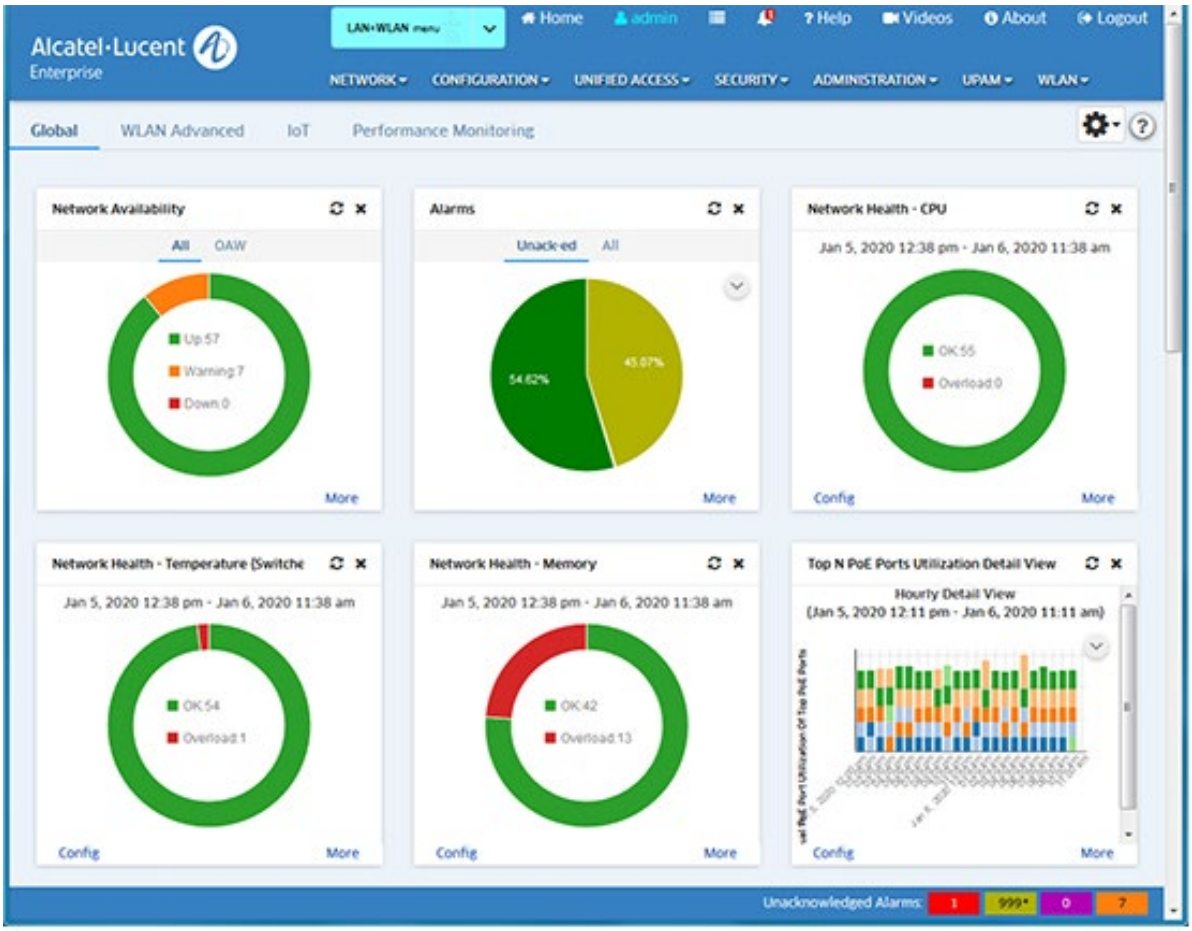
1.0 Getting Started with OmniVista 2500 NMS

Alcatel-Lucent Enterprise's OmniVista 2500 NMS uses a web-based user interface. The Web GUI is supported on the following browsers: Chrome 79+ (on Windows and Redhat/SuSE Linux client PCs), Firefox 62+ (on Windows and Redhat/SuSE Linux client PCs), and Microsoft Edge 80+ (on Windows client PCs), This Quick Start guide will get you up and running with OmniVista 2500 NMS. The sections below provide an overview of the OmniVista 2500 NMS.

- OmniVista 2500 NMS User Interface
- Applications
- Customizing the Dashboard
- Configuration/Display Buttons
- Working with Tables
- Setting Up OmniVista 2500 NMS for Network Management
- Discovering Devices
- Editing Discovered Devices
- Configuring Traps
- Saving Changes

OmniVista 2500 NMS User Interface

The OmniVista 2500 NMS Home Page displays a dashboard with application widgets that provide an overview of key applications. The widgets also link directly to their application, so you can access the application for more detailed information/configuration. The dashboard is customizable. You can add/remove widgets, and drag and drop them into any order, as well as close widgets and refresh widget content. The Global Tab displays all selected widgets for all applications. The WLAN tab displays all selected Stellar Wireless Application Widgets.



Banner Links

The following links are available in the Banner on the Home Page and on all screens in OmniVista:

- **LAN/WLAN Menu Option -** By default, all application drop-down menus (for both LAN and WLAN Devices) are displayed ("LAN+WLAN Menu"). You can click on the LAN/WLAN Menu drop-down and select "WLAN Menu" to display application drop-down menus specific to WLAN devices (e.g., SSIDs, APs). The Banner will turn gray, indicating you are in WLAN Menu Mode.
- **Home -** Returns the user to the Home Page.
- **Admin -** Displays the current user (e.g., fat2). Click to bring up the User Management Screen.
- **Application Results -** Displays a list of user actions taken in the Device Catalog and SSIDs applications (e.g., Remove/License/Unlicense a device, create/edit/delete SSID). Click on the **Copy** button to save the list of actions to the clipboard. At this time, this feature is only supported in the Device Catalog and SSIDs applications.
- **Unsaved Device Notifications -** If any managed devices have unsaved changes in the Working Directory, a number will appear on the Unsaved Device Notifications icon (Bell). Click on the icon to view the number of devices with unsaved changes. Click on the **Save** icon, then click **OK** at the Confirmation Prompt to save the changes to the devices. There is also an option to ignore unsaved changes for

Stellar APs. Unsaved changes on Stellar APs are generally not a problem since Stellar APs receive the latest configuration at reboot. To prevent notifications for unsaved changes on Stellar APs, click on **Settings**, uncheck the "Unsaved Changes Notification for Stellar Access Points" checkbox, and click **OK**.

- **Videos -** Launches the Alcatel-Lucent Enterprise YouTube Demo Playlist.
- **About -** Displays basic OmniVista information (e.g., build number and date).
- **Logout -** Logs you out of OmniVista.

Unacknowledged Alarm Display

A real-time display of unacknowledged alarms is displayed at the bottom of the Home Page and on all screens in OmniVista. The number of alarms in each category (e.g., Critical, Major, Minor) is displayed. Click on a category to go to the Notifications application and view all alarms in the selected category.

Applications

Applications in OmniVista are organized as shown below. By default, all application drop-down menus (for both LAN and WLAN Devices) are displayed in the LAN+WLAN Menu. If the WLAN Menu is selected, application drop-down menus specific to WLAN devices are displayed (e.g., SSIDs, APs) to make it easier for the user to locate WLAN-specific applications. Note that there is no change to the content within the applications (i.e., the applications have not been modified to be "WLAN-specific"). The content of the applications accessed through the WLAN Menu and the LAN+WLAN Menu are the same. The menus are organized as described below.

LAN+WLAN Menu

Network

- Discovery
- Topology
- AP Registration
- SAA
- Locator
- Notifications
- VM Manager
- Analytics
- Application Visibility
- Provisioning
- IoT

Configuration

- VLANs
- Services
- VXLANs
- IP Multicast
- CLI Scripting

- PolicyView
- SIP
- Captive Portal
- Groups
- App Launch
- Report
- Resource Manager

Unified Access

- Unified Profile
- Unified Policy
- Multimedia Services
- Paid Account Services

Security

- Users and User Groups
- Authentication Servers
- External Apps
- Quarantine Manager

Administration

- Control Panel
- Preferences
- Audit
- License
- OV System Health

UPAM

- Summary
- Authentication
- Guest Access
- BYOD Access
- Settings
- Web Content Filtering

WLAN

- SSIDs
- Wireless Intrusion Protection System (WIPS)
- RF Management
- Heat Map
- Floor Plan
- Client

WLAN Menu

SSIDs

- SSIDs
- WLAN Service (Expert)

APs

- Inventory
- Topology
- VLANs
- Configuration Manager
- SSH/Telnet
- Heat Map
- Floor Plan
- IoT/Location Server
- Data VPN Server

Analytics

- Analytics Reports
- AV-Devices Management
- AV-Signature Files
- AV-Signature Profiles
- AV-Summary View

Clients

- Summary
- Client List
- Client Session
- Client Blocklist
- IoT
- Locator
- Access Records

Guest/BYOD

- Guest Access
- BYOD Access
- Captive Portal

Authentication

- Policy
- NAS Clients
- Certificates
- Accounts
- Authentication Servers

- External Servers

Policies

- ACL/QoS
- Unified Profile
- Resource Groups
- Device Config

RF

- RF Home
- RF Profile
- RF Scan View

Security

- OV Users and User Groups
- Wireless Intrusion Protection System (WIPS)
- External Apps
- Web Content Filtering

Alarms/Logs

- Notifications
- Audit Logs

Administration

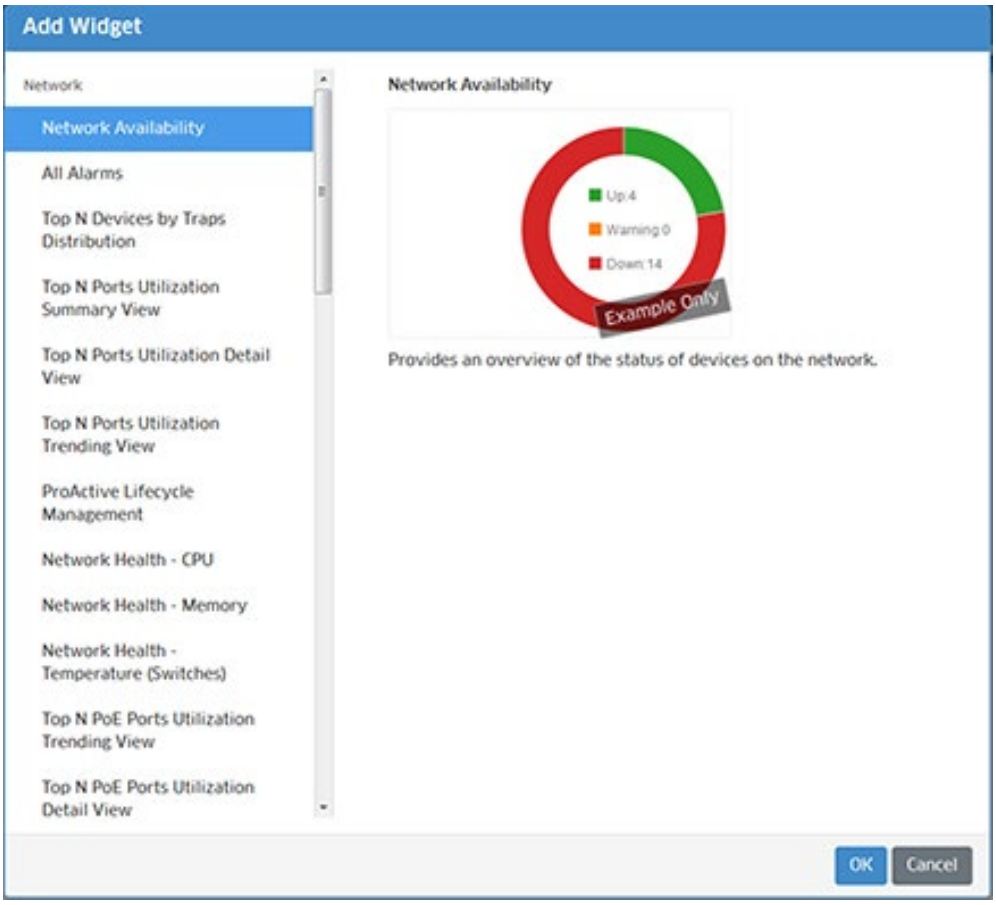
- Report
- Control Panel
- Preferences
- Licenses
- OV System Health

Customizing the Dashboard

You arrange widgets on the Dashboard by clicking on a widget and dragging it to a new location. You can also add or remove widgets from the Dashboard, customize the Dashboard layout using the Dashboard Settings option, and set the Dashboard refresh rate. This section provides an overview of application widgets and the Dashboard. For detailed information see the Dashboard Help.

Adding Widgets

To add a widget to the Dashboard, click on the Settings icon and select **Add Widget**. The Add Widget Screen, shown below, is displayed. All available widgets are displayed. (Widgets that are already displayed on the Dashboard are not displayed.) You can select a widget to display a sample of the widget and a brief summary of the information provided by the widget.



Select an available widget from the list and click **OK**. The widget will be added to the upper-left of the dashboard. You can then drag and drop the widget to any position in the Dashboard. Note that you can only add one widget at a time. Repeat the procedure to add additional widgets

Removing Widgets

To remove a widget from the dashboard, click on the Delete icon (**x**) at the top-right corner of the widget. You can add the widget back or add a new widget by clicking on the Settings icon and selecting **Add Widget**.

Additional Options Provided Within Widgets

You can configure Dashboard display settings for certain widgets (e.g., Analytics Statistics) by clicking on the **Config** link at the bottom of the widget. You can then modify certain display options, such as the number of items displayed in the widget, the time period displayed in the widget, etc. This modifies the display on the Dashboard only. It does not modify the display within the application.

You can also hover over certain displays (e.g., Analytics to view more detailed information, and click on data within certain widgets to display additional information (e.g., clicking on bar and donut graphs displays additional information such as numeric values, clicking on Quarantine Manager topics at the bottom of the graph displays additional information for each topic).

Click on the **More** link at the bottom of a widget to open the full application for the widget. To return to the Dashboard, click on the Alcatel-Lucent Enterprise logo at the top left corner of the screen.

The Favorites Widget and Adding Items to the Favorites Tab

The Favorites widget allows users to create a list of “quick links” for easy access to any OmniVista 2500 NMS application. To add an application to the Favorites list, start typing the name of the application in the text box. As text is entered, auto-complete displays a list of matching applications. Click an application to select it, then click the add icon (**+**).

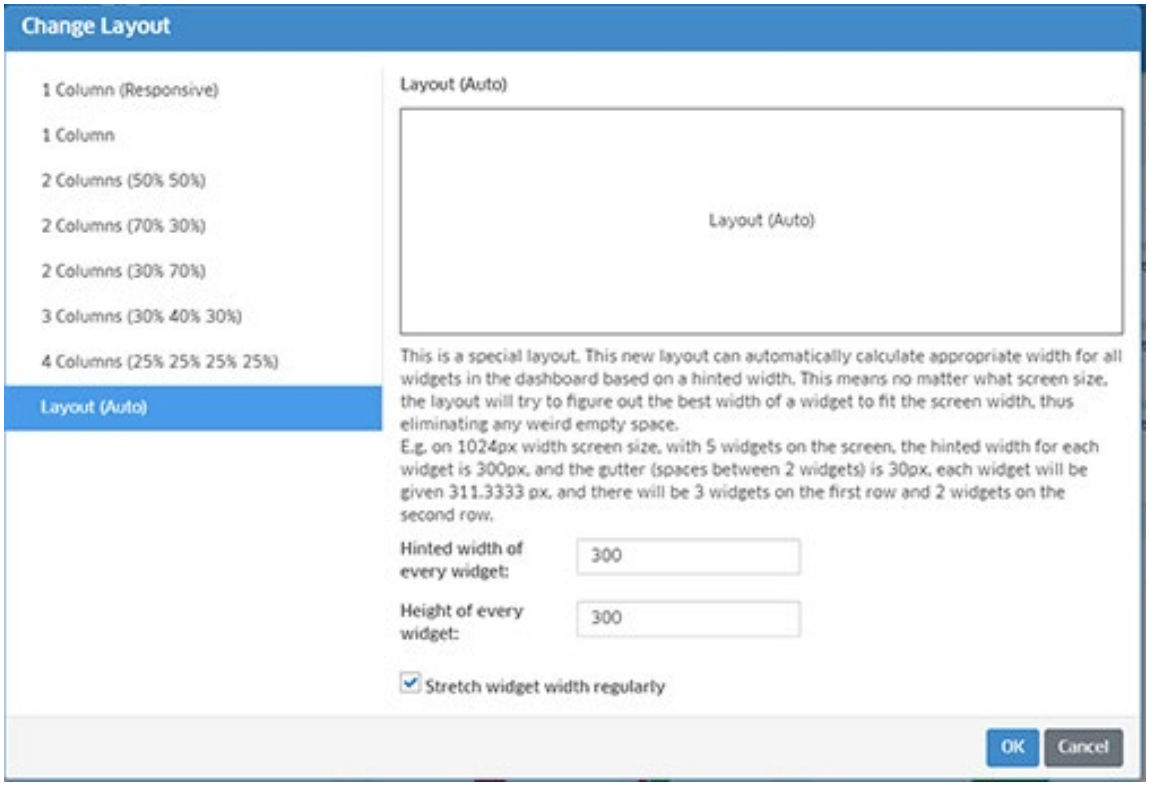
To replace an application in the list of Favorites, click the Edit icon. Begin typing the new application name. Select the application and click the Save icon.

Note: Once an application has been added to the Favorites widget, a link to the application will also display under the Favorites tab in the OmniVista 2500 NMS Main Navigation Menu.

To remove an application from the Favorites widget, click the Delete icon (**x**) next to the application link.

Customizing the Dashboard Layout

The Settings option also enables you to customize the Dashboard layout. To customize the layout, click on Settings icon and select **Change Layout**. The Change Layout Screen appears. By default, widgets are displayed in the "Auto" layout. To change the layout, select an option on the left. When you select a layout on the left, the layout is displayed in the Layout area. To choose that layout, click **OK**. The change takes effect immediately. If necessary, you can re-arrange the widgets in the new layout, by clicking and dragging them to new locations on the Dashboard.



Setting the Dashboard Refresh Rate

The data in the Dashboard Widgets is refreshed at regular intervals. To set the refresh rate, click on Settings icon and select Settings. Enter a refresh rate, in minutes. (Minimum refresh rate = 5, Default = 5).

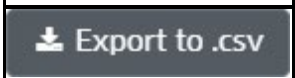
Configuration/Display Icons/Buttons

OmniVista 2500 NMS provides standard tools for interacting with configuration/display screens. These icons/buttons include:

Configuration Icons/Buttons	
	Add Click the Add icon to create a new entry within the configuration screen.
	Edit To edit an existing entry, select the entry in the configuration screen and click the Edit icon.
	Copy/Duplicate Used to duplicate an existing entry in a list or table. Select an entry in a table, and click on the Copy/Duplicate icon to bring up a configuration screen with the selected configuration. You can then modify certain fields to quickly create a new entry. This can save time when creating multiple entries with similar configurations.
	Delete To delete an entry, select the entry and click the Delete icon.
Table Icons/Buttons	
	Table View Table view organizes configuration screens in a table-based layout that is viewed and sorted similar to a spreadsheet. Table data may be exported to CSV files.
	List View List View organizes information and configuration tasks in a list view. Note that information displayed in List View cannot be Printed via the OmniVista 2500 NMS Print button. To print information from a particular screen, switch to Table View (if available).
	Settings Used to configure the column headings to display in a table. Click on the Settings button and select the column headings you want to display.
	Refresh The Refresh button loads the latest data for an application table, chart or list.
	Help Click on the Help button to load for a context-sensitive walk-through of an application, table or configuration screen.

	Sort Information displayed in List View may be sorted in alphabetical order, either ascending or descending, by clicking on the Sort button. You can also click on the Up/Down arrows at the top of any table column in Table View to sort the data in ascending or descending order based on the selected column.
	Search Click the Search button and enter search criteria in the "Search..." field to display specific entries in the table. Click on the "x" to the right to return to the original display.

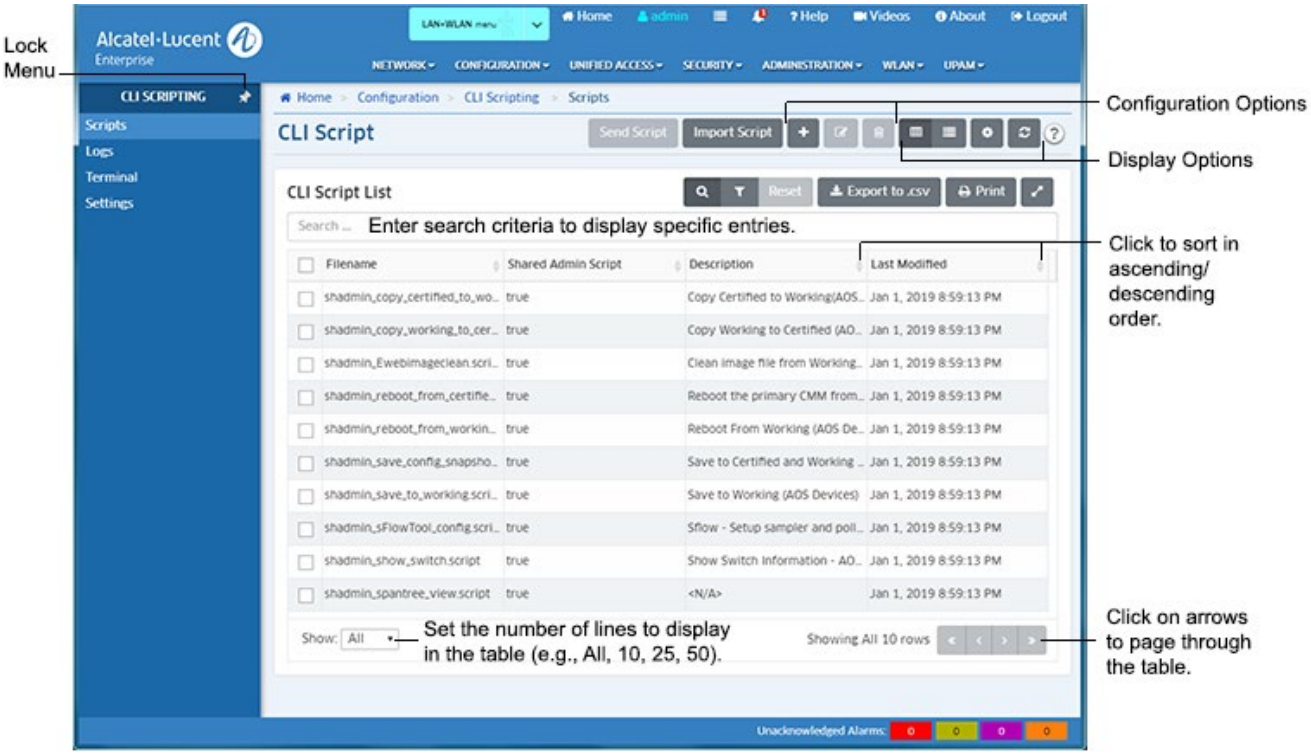
	Filter
	Users can create custom filters for OmniVista 2500 NMS tables to display specific data. To create a custom filter:
	• Click the filter button.
	• In the Filter screen, click **Add**.
	• Enter a **Filter Name** for the custom filter.
	• Enter a **Filter Description** for the filter.
	• In the **Conditions** area, for “Filter elements where ... of the following apply”, specify the strictness of the conditions (e.g., display results if ANY condition is encountered, or only display results if ALL of the conditions are encountered).
	• Select an option from the application-specific conditions list. This automatically enables the conditions.
	• Next, fine-tune conditions by selecting options under the following pull down menus:
	  ○ have/not have
	  ○ Name - select a column heading to use in the filter.
	  ○ contains
	  ▪ begins with
	  ▪ ends with
	  ▪ equal
	  ▪ not equal
	  ○ [enter value] - enter a specific text string
	  ○ non-case sensitive/case sensitive
	• Additional application-specific conditions may be added to the conditions outlined in the previous step by clicking the “Add new Condition” link.
	• You can also add a completely new group of conditions by clicking the Add icon and repeating the steps outlined above.

	Reset Click the Reset button after filtering a table to return to the original display.
	**Export to CSV** Click the CSV button to download information displayed in Table View to a CSV (spreadsheet) file.

Add to Report	**Add To Report** Click to create a report for the page. These reports are PDF versions of tables and reports generated in certain OmniVista applications (e.g., Discovery, Locator, Analytics). Basically, in addition to viewing information in real-time in OmniVista (e.g., Discovery Inventory List, Analytics Utilization Reports), you can generate PDFs of the screens. When a report is generated, it takes a current snapshot of the application information. These reports can be generated immediately or you can schedule them to be generated at regular times/intervals (e.g., Daily, Weekly). You can also configure a report to be e-mailed when it is generated. Reports are configured in the Report application.
Print	**Print** Print Table View information by clicking the Print button. Note that information displayed in List View cannot be Printed via the OmniVista 2500 NMS Print button (button is not available). To print information from a screen, switch to Table View (if available).
	Full Screen Click to display the current screen in full-screen view (without top and side menus). Click on the button again or click on the **X** in the upper-right corner of the screen to return to the default view.

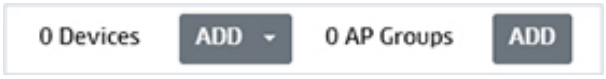
Working with Tables

Information in OmniVista is primarily presented in table format. There are common functions/behaviors for tables in OmniVista. the general functionality of each area is described below. Details for each button are provided in the Configuration/Display Buttons section.

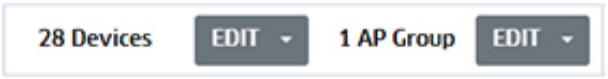


- **Configuration Options -** Used to create, edit, delete entries (e.g., create, edit, delete a CLI Script). Details for each button are provided in the Configuration/Display Buttons section.
- **Display Options -** Used to change the table display from Table View to List view, to set the columns you want to display, and to refresh the data in the table. Details for each button are provided in the Configuration/Display Buttons section.
- **Filter, Export, Print -** You can filter the data that is displayed by clicking on the Filter icon and selecting/creating a filter. You can also export the table into a .csv file, or print the table. Details for each button are provided in the Configuration/Display Buttons section.
- **Search -** Enter search criteria in the **Search...** field to display specific entries in a table. As you enter criteria, only those entries matching the criteria will appear in the table. Click on the **Reset** button to return to the original table display.
- **Sort -** Click on one of the arrows at the top of a column to sort the table in ascending or descending order based on the column.
- **Set Lines to Display/Page Through Table -** Set the number of lines to display in the table using the **Show** drop-down menu at the bottom left corner of the table. You can also page through a large table using the arrows at the bottom right corner of the table.

On most screens, all configured items are displayed in a table. As show above, you can search or sort to display specific items. Applications with larger tables (e.g., VLANs) do not display data by default. You must select the devices/AP Groups you want to display in the table. These applications feature a Device Selection Bar at the top of the table (shown below). Click on the Devices **ADD** button and/or the AP Groups **ADD** button to select the devices you want to display.



To change the display, click on the Devices **EDIT** button and/or the AP Groups **EDIT** button to add/remove devices/AP Groups.

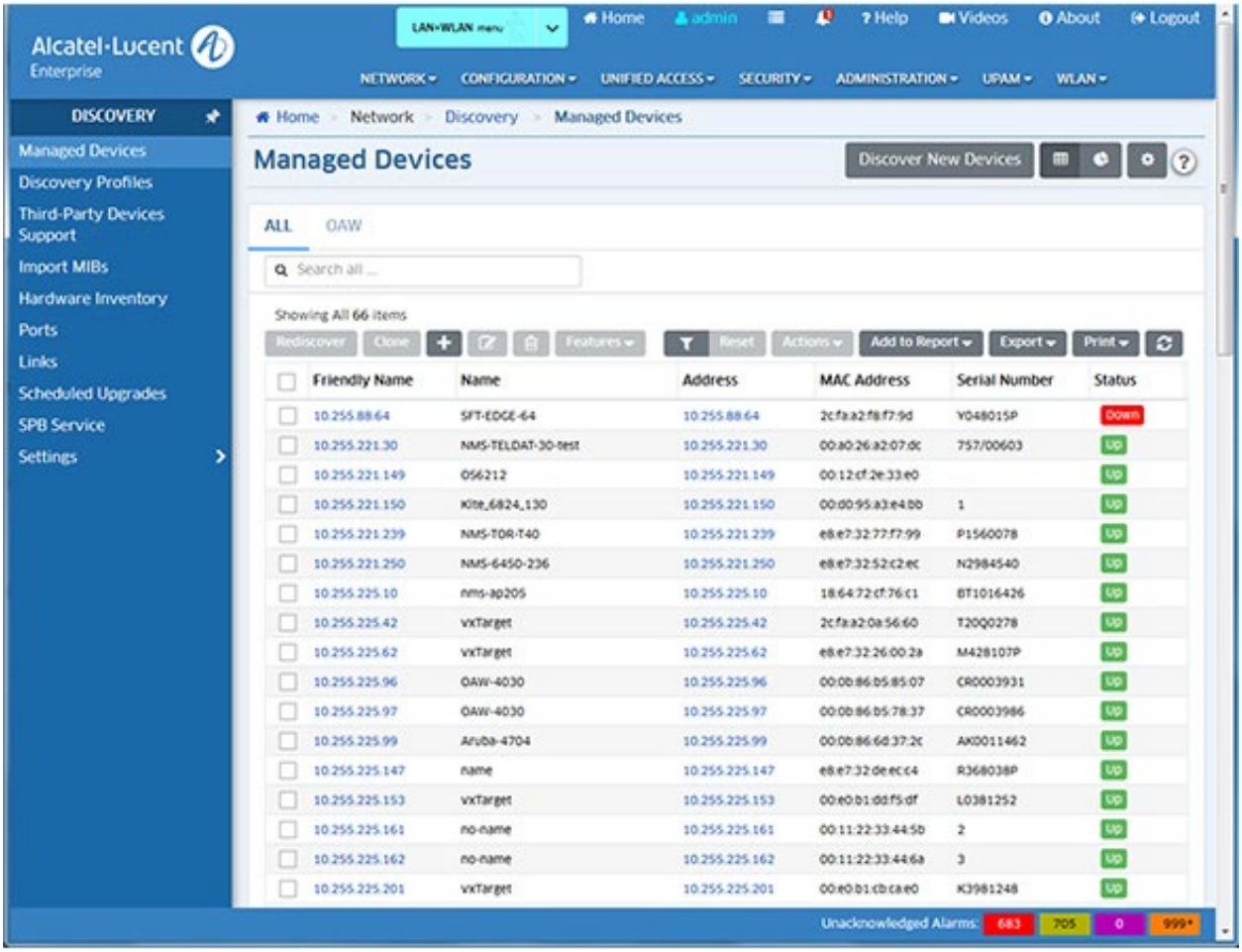


Your device selection will remain persistent until you change it or log out of OmniVista. If you log out, the default setting (no display) returns.

Setting Up OmniVista 2500 NMS for Network Management

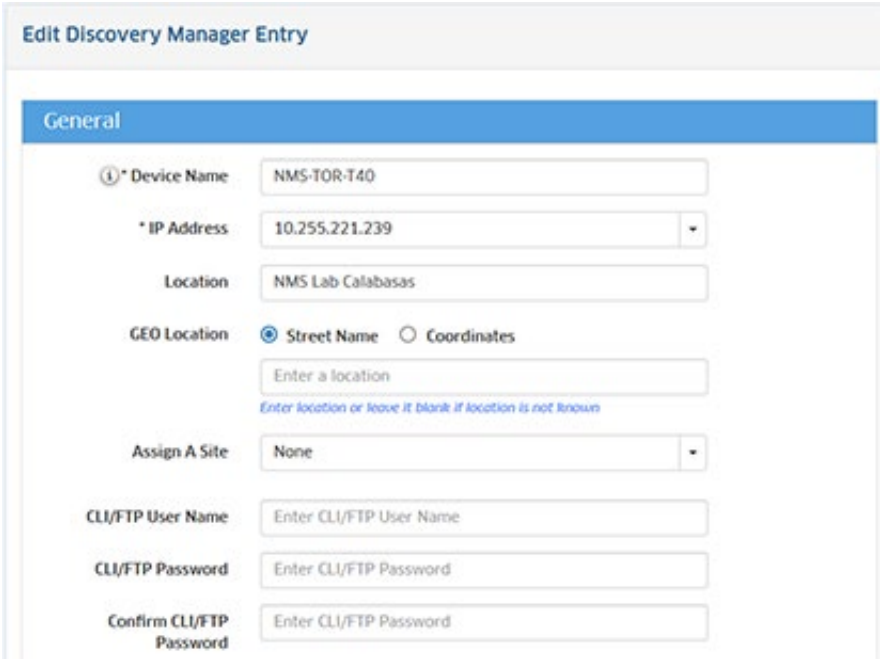
Discovering Devices

After you log into OmniVista, open the Discovery application to discover devices on your network. Click on the **Discover New Devices** button and enter a range of devices to discover. You can use the Default Discovery Profile for your initial discovery. (A Discovery Profile contains the parameters that are used by OmniVista when performing a discovery (e.g., SNMP version used to discover devices, FTP/Telnet passwords needed to connect to a device). When the discovery is complete, all devices discovered are displayed on the Managed Devices Screen.



Editing Discovered Devices

Once switches are discovered, you may want or need to edit entries in the Managed Devices List. To edit a discovered device, select the device in the list and click on the Edit icon to display the Edit Discovery Manager Entry window, shown below.



Why Edit a Discovered Device?

To Redefine the Primary IP Address

When switches are auto-discovered via a Ping Sweep or ARP discovery, each IP address in a range or subnet is pinged. OmniVista uses the first IP address that responds to a ping as that device's primary IP address. However, if multiple VLANs exist in the device, additional IP addresses in the device will also respond to pings. The Edit Discovery Manager Entry window's **IP Address** field combo box lists these additional IP addresses and enables you to select any address listed as the device's primary IP address.

To Specify the Correct Write Community Name

All devices that are discovered are initially specified to have the default write community name, **public**. If any discovered devices in your network have a non-default write community name, use the Edit Discovery Manager Entry window's SNMP Settings tab to specify the correct community name to OmniVista. If the correct write community name is not specified to OmniVista, you will not be able to write configuration changes to the switch.

Please Note: Switches' SNMP write (set) community names are not configurable from OmniVista. SNMP read (get) and write (set) community names can only be configured by logging onto the switch.

To Specify the CLI or FTP User Name and Password

Firmware configuration files for AOS devices can be saved to the OmniVista server and restored when desired. When files are saved, they are FTPed from the switch to the OmniVista server. When files are restored, they are FTPed from the server to the switch. New configuration files can also be installed via FTP. To FTP files, OmniVista must know the FTP login name and password that is defined on the switch. The **CLI/FTP User Name** and **CLI/FTP Password** fields on the Edit Discovery Manager Entry window enable you to specify this information to OmniVista.

Please Note:

- If you do not define the FTP login names and passwords and you attempt to save, restore, or update configuration files for these devices, you will be individually queried for the FTP login name and password of each individual switch for which configuration files are being saved, restored, or updated.
- The user names and passwords entered in these fields are used for FTP ONLY. They are not used for Telnet. When you Telnet to a device, you will be queried for a user name and password.

To Redefine the SNMP Version or SNMP Parameters

The Edit Discovery Manager Entry window enables you to redefine the SNMP version that OmniVista uses to communicate with AOS devices. You can also redefine SNMP parameters. The SNMP version or parameter settings that OmniVista uses cannot be changed until OmniVista has connected to the switch. AOS devices support SNMP version 1, SNMP version 2 or SNMP version 3.

Configuring Traps

It is necessary to configure the switches in the network to send OmniVista the traps that are needed by different applications. Traps are configured in the Notifications application. The traps OmniVista needs for each application are listed below.

Traps Needed for Topology
coldStart, warmStart, linkUp, linkDown

Note: For proper link display in Topology, linkUp and linkDown traps must be enabled for each individual port.

Traps Needed for PolicyView QoS
policyEventNotification

Saving Changes

The directory structure that stores AOS image and configuration files in flash memory is divided into two parts:

- The certified directory contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory. (Note that you can specifically command a switch to load from either directory.)
- The working directory contains files that may -- or may not -- have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes to the working directory. You cannot save configuration changes directly to the certified directory.

Note that the files in the certified directory and in the working directory may be different from the running configuration of the switch, which is contained in RAM memory. The running configuration is the current operating parameters of the switch, which are originally loaded from the certified or working directory. Modifications made to the running configuration of the switch must be saved to the working directory (or lost). The working directory can then be copied to the certified directory if and when desired.

When changes are made to the configuration of an AOS device -- such as configuring the traps the switch should transmit -- the change is written to the running configuration of the switch. However, if the switch is powered off, the running configuration will be lost. To make changes to the running configuration persistent, you must save the running configuration to the working directory of the switch. You should also then copy the working directory to the certified directory, so the changes will be persistent when the switch is booted from the certified directory.

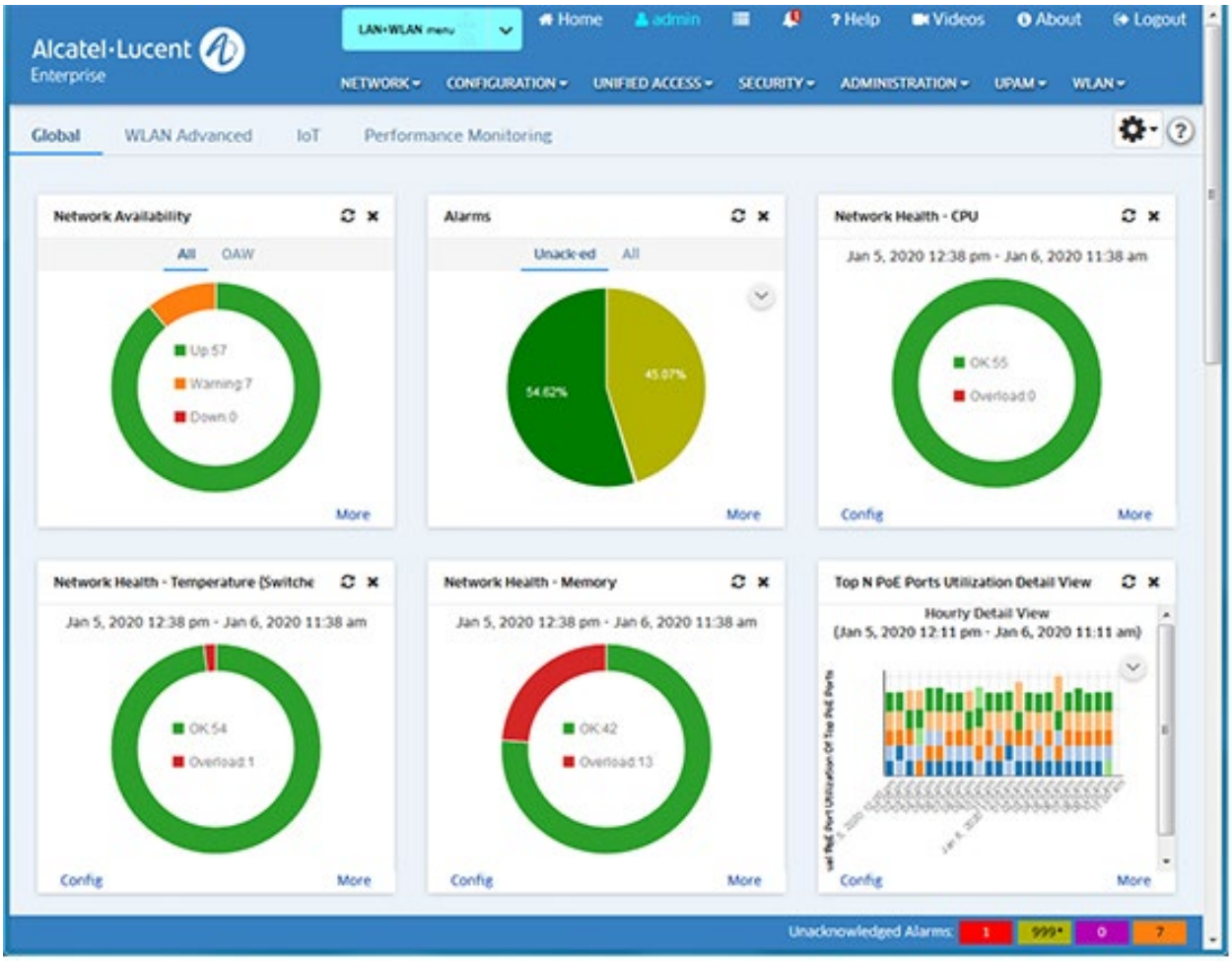
You can perform these operations in the Topology application by selecting a device(s) and clicking on the application operation (Copy Working/Running to Certified).

PolicyView QoS

When PolicyView QoS is executed, it writes the address of the LDAP server to each QoS-enabled switch in the Discovery Inventory List. (All AOS devices are QoS-enabled.) In the case of AOS devices, the LDAP address is written to the running configuration of the switch. For this reason, once PolicyView QoS has executed, all AOS devices will be left with their running configuration in the **Unsaved** state (indicating that the running configuration has changes that have not been saved to the working directory). It is important to save the running configuration to the working directory and then the certified directory after PolicyView QoS has executed. To do this, follow the steps in Saving Changes, above.

2.0 The Dashboard

The OmniVista 2500 NMS Home Page displays a dashboard with application widgets that provide a quick overview of key applications. The widgets also link directly to their application, so you can access the application for more detailed information/configuration. The Dashboard is customizable; you can add/remove widgets, and drag and drop them into any order on the Dashboard. The Global tab displays all selected widgets for all applications (Default); the WLAN Advanced tab displays all selected Stellar Wireless Application Widgets; the IoT tab displays all selected IoT Application Widgets, and the Performance Monitoring tab displays all selected Analytics Statistics Charts.



See the OmniVista Getting Started Help for an overview of the OmniVista User Interface, as well as procedures for setting up OmniVista for network management.

Banner Links

The following links are available in the Banner on the Home Page and on all screens in OmniVista:

- **LAN/WLAN Menu Option -** By default, all application drop-down menus (for both LAN and WLAN Devices) are displayed ("LAN+WLAN Menu"). You can click on the LAN/WLAN Menu drop-down and select "WLAN Menu" to display application drop-

down menus specific to WLAN devices (e.g., SSIDs, APs). The Banner will turn gray, indicating you are in WLAN Menu Mode.

- **Home -** Returns the user to the Home Page.
- **Admin -** Displays the current user (e.g., fat2). Click to bring up the User Management Screen.
- **Application Results -** Displays a list of user actions taken in the Device Catalog and SSIDs applications (e.g., Remove/License/Unlicense a device, create/edit/delete SSID). Click on the **Copy** button to save the list of actions to the clipboard. At this time, this feature is only supported in the Device Catalog and SSIDs applications.
- **Unsaved Device Notifications -** If any managed devices have unsaved changes in the Working Directory, a number will appear on the Unsaved Device Notifications icon (Bell). Click on the icon to view the number of devices with unsaved changes. Click on the **Save** icon, then click **OK** at the Confirmation Prompt to save the changes to the devices. There is also an option to ignore unsaved changes for Stellar APs. Unsaved changes on Stellar APs are generally not a problem since Stellar APs receive the latest configuration at reboot. To prevent notifications for unsaved changes on Stellar APs, click on **Settings**, uncheck the "Unsaved Changes Notification for Stellar Access Points" checkbox, and click **OK**.
- **Videos -** Launches the Alcatel-Lucent Enterprise YouTube Demo Playlist.
- **About -** Displays basic OmniVista information (e.g., build number and date).
- **Logout -** Logs you out of OmniVista.

Applications

Applications in OmniVista are organized as shown below. By default, all application drop-down menus (for both LAN and WLAN Devices) are displayed in the LAN+WLAN Menu. If the WLAN Menu is selected, application drop-down menus specific to WLAN devices are displayed (e.g., SSIDs, APs) to make it easier for the user to locate WLAN-specific applications. Note that there is no change to the content within the applications (i.e., the applications have not been modified to be "WLAN-specific"). The content of the applications accessed through the WLAN Menu and the LAN+WLAN Menu are the same. The menus are organized as described below.

LAN+WLAN Menu

Network

- Discovery
- Topology
- AP Registration
- SAA
- Locator
- Notifications
- VM Manager
- Analytics
- Application Visibility
- Provisioning
- IoT

Configuration

- VLANs
- Services
- VXLANs
- IP Multicast
- CLI Scripting
- PolicyView
- SIP
- Captive Portal
- Groups
- App Launch
- Report
- Resource Manager

Unified Access

- Unified Profile
- Unified Policy
- Multimedia Services
- Paid Account Services

Security

- Users and User Groups
- Authentication Servers
- External Apps
- Quarantine Manager

Administration

- Control Panel
- Preferences
- Audit
- License
- OV System Health

UPAM

- Summary
- Authentication
- Guest Access
- BYOD Access
- Settings
- Web Content Filtering

WLAN

- SSIDs
- Wireless Intrusion Protection System (WIPS)
- RF Management
- Heat Map
- Floor Plan
- Client

WLAN Menu

SSIDs

- SSIDs
- WLAN Service (Expert)

APs

- Inventory
- Topology
- VLANs
- Configuration Manager
- SSH/Telnet
- Heat Map
- Floor Plan
- IoT/Location Server
- Data VPN Server

Analytics

- Analytics Reports
- AV-Devices Management
- AV-Signature Files
- AV-Signature Profiles
- AV-Summary View

Clients

- Summary
- Client List
- Client Session
- Client Blocklist
- IoT
- Locator
- Access Records

Guest/BYOD

- Guest Access
- BYOD Access
- Captive Portal

Authentication

- Policy
- NAS Clients
- Certificates
- Accounts
- Authentication Servers
- External Servers

Policies

- ACL/QoS
- Unified Profile
- Resource Groups
- Device Config

RF

- RF Home
- RF Profile
- RF Scan View

Security

- OV Users and User Groups
- Wireless Intrusion Protection System (WIPS)
- External Apps
- Web Content Filtering

Alarms/Logs

- Notifications
- Audit Logs

Administration

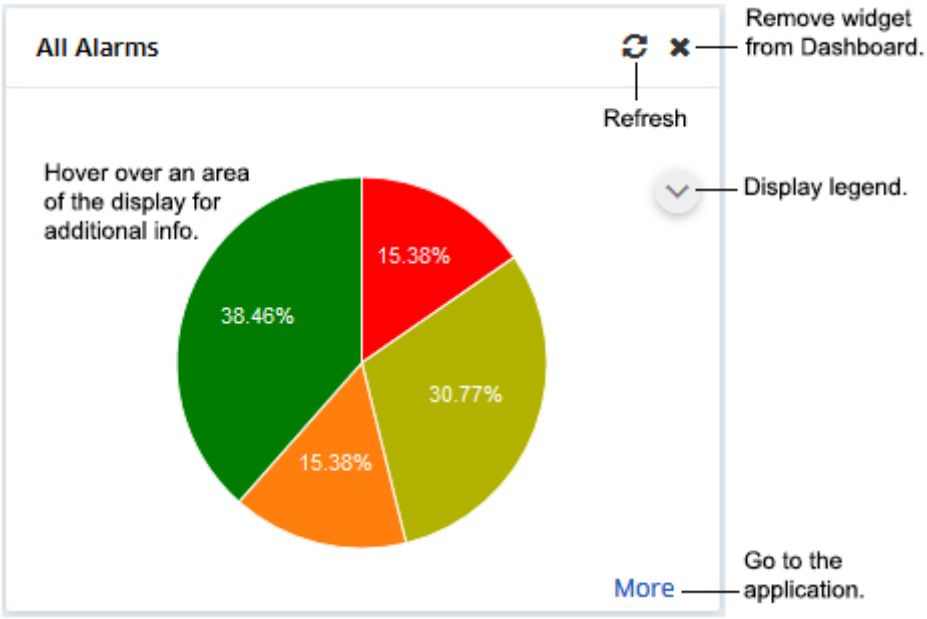
- Report
- Control Panel
- Preferences
- Licenses
- OV System Health

Unacknowledged Alarm Display

A real-time display of unacknowledged alarms is displayed at the bottom of the Home Page and on all screens in OmniVista. The number of alarms in each category (e.g., Critical, Major, Minor) is displayed. Click on a category to go to the Notifications application and view all alarms in the selected category.

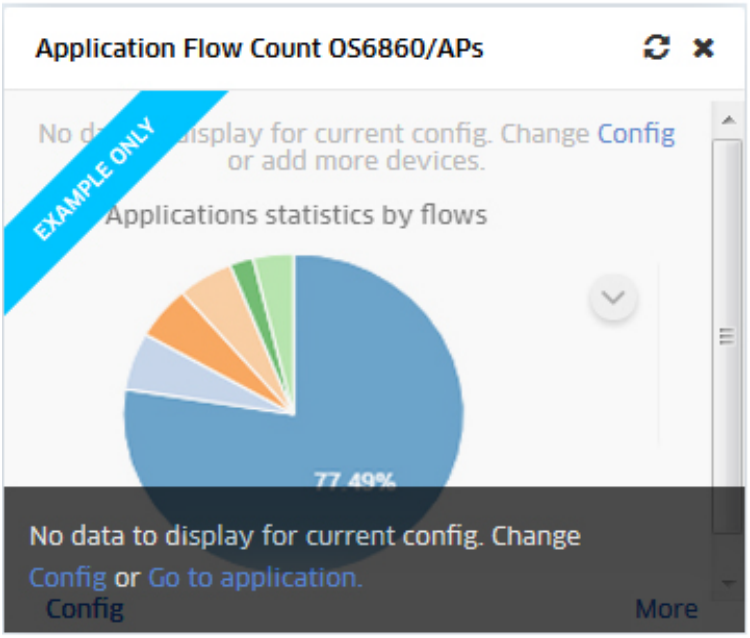
Widgets

Application widgets provide a quick overview of key applications. You can hover the mouse over a widget or click on an area of the widget to display additional information, display a legend for the information in the widget, immediately refresh widget information, remove a widget from the Dashboard, configure the widget display, and directly access an application through a widget for detailed information or application configuration. Note that the options available (e.g., display additional information, configure the widget display) vary depending on the widget.



You can also customize the Dashboard by arranging widgets on the Dashboard, adding/removing widgets to/from the Dashboard, and changing the Dashboard layout.

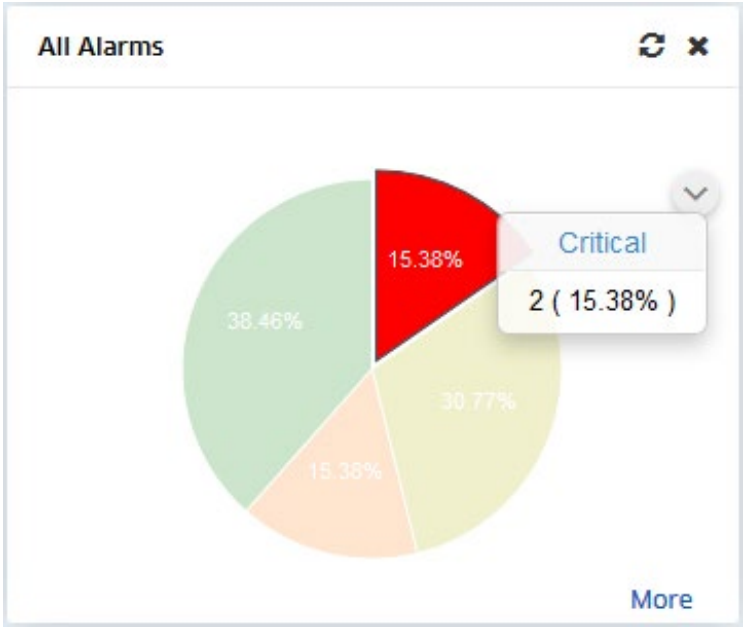
If no data has been generated for a Dashboard widget, or the widget is not properly configured to display data, a sample widget is displayed, as shown below. This may be because the application has not yet been configured (e.g., you have not created Analytics Profiles to generate Analytics Reports), or the widget may need to be configured to display data (e.g., there is no data available for the time period configured for the widget). Hover over the bottom of the widget, then click on the "Config" link to configure the widget display (if applicable), or click on the "Go to application" link to go to the application and configure the application to generate data. Note that some widgets (e.g., Inventory, Network Availability) are not configurable, so the "Config" link is not available.



Hover over the bottom of the widget, then click on the applicable link to configure the widget display (**Config**) or the application (**Go to application**).

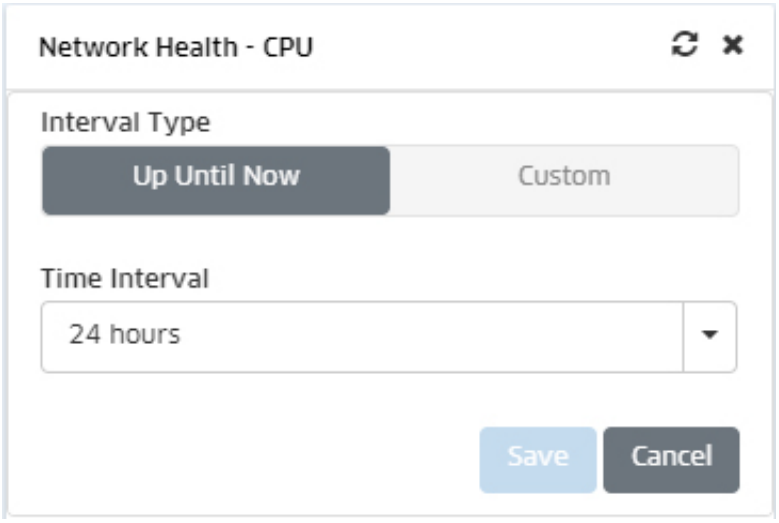
Viewing Additional Information

You can hover over certain widgets to display additional information, or click on an area for more detailed information. For example, the Alarms Widget displays information in a pie chart format for about Notifications for all managed devices. Hover the mouse over an area of the chart to view the number of alarms in that category and the percentage of alarms in that category. You can also click on an area of the chart to view more detailed information. The Alarms Widget will open the Notifications application to display a list of alarms in the selected category. Other widgets will display detailed information about specific devices.



Configuring the Widget Display

You can configure Dashboard display settings for certain widgets (e.g., Network Health) by clicking on the **Config** link at the bottom left corner of the widget. You can then modify certain display options, such as the Interval Type and Time Interval displayed in the widget. Make any modifications and click on the **Save** button. The widget will be displayed with the new configuration.



Note: This modifies the display on the Dashboard only. It does not modify the display within the application.

Linking to the Application

Click on the **More** link at the bottom of a widget to go to the page in the full application. For example, if you clicked on the **More** link in the Alarms Widget, you would go to the Notifications application. To return to the Dashboard, click on the Alcatel-Lucent Enterprise logo at the top left corner of the screen.

Customizing the Dashboard

You arrange widgets on the Dashboard by clicking on a widget and dragging it to a new location. You can also add/remove widgets to/from the Dashboard, and customize the Dashboard layout. The sections below detail the procedures for the Global Dashboard, the WLAN Dashboard, the IoT Dashboard, and the Performance Monitoring Dashboard.

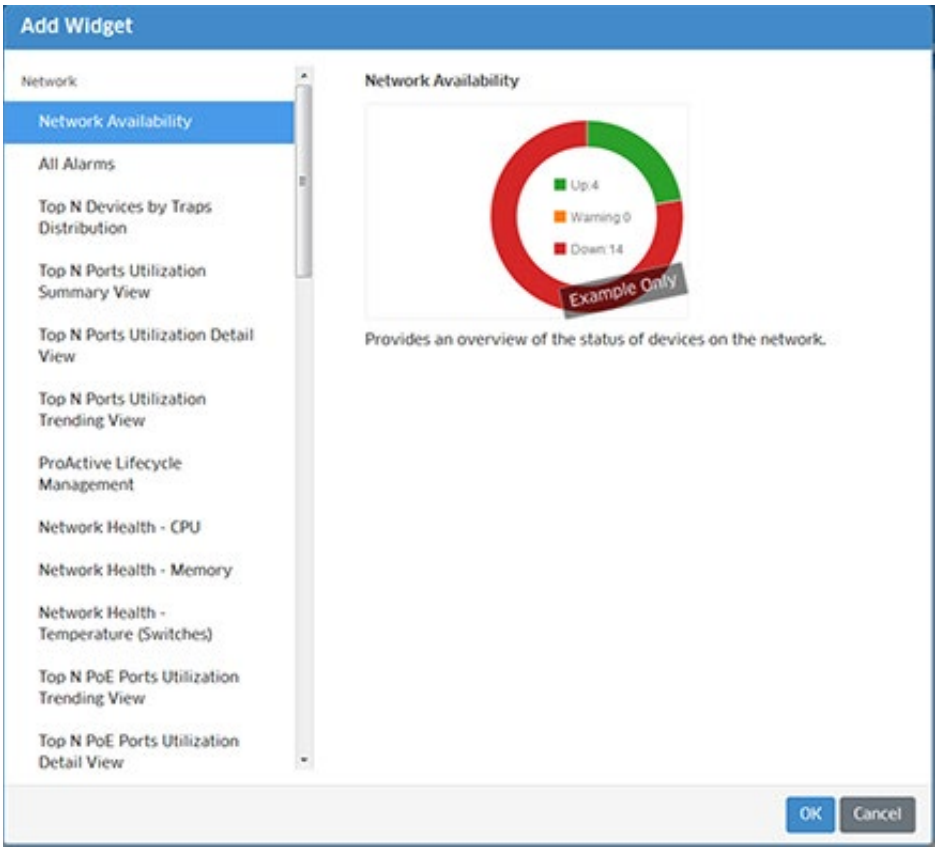
Global Dashboard

The Global tab displays all selected widgets for all applications. The following sections detail customizing the Dashboard for the Global Tab.

Adding Widgets

To add a widget to the Global Dashboard, click on the Settings icon and select **Add Widget**. The Add Widget Screen, shown below is displayed. Available widgets are displayed on the left side of the screen. (Widgets already on the Dashboard are not displayed.) You can select a widget to display a sample of the widget and a brief summary of the information provided by the widget.

Select an available widget from the list and click **OK**. The widget will be added to the upper-left of the Dashboard. You can then drag and drop the widget to any position in the Dashboard. Note that you can only add one widget at a time. Repeat the procedure to add additional widgets.

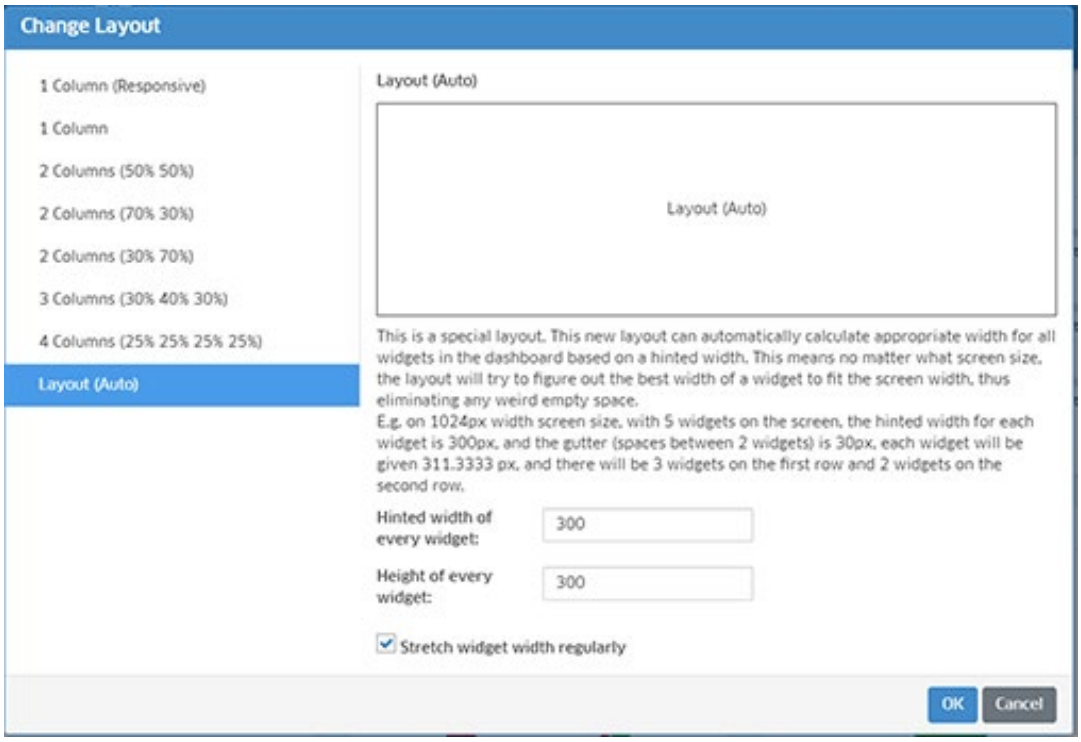


Removing Widgets

To remove a widget from the dashboard, click on the Delete icon at the top-right corner of the widget. You can add the widget back or add a new widget by clicking on the Settings icon and selecting **Add Widget**.

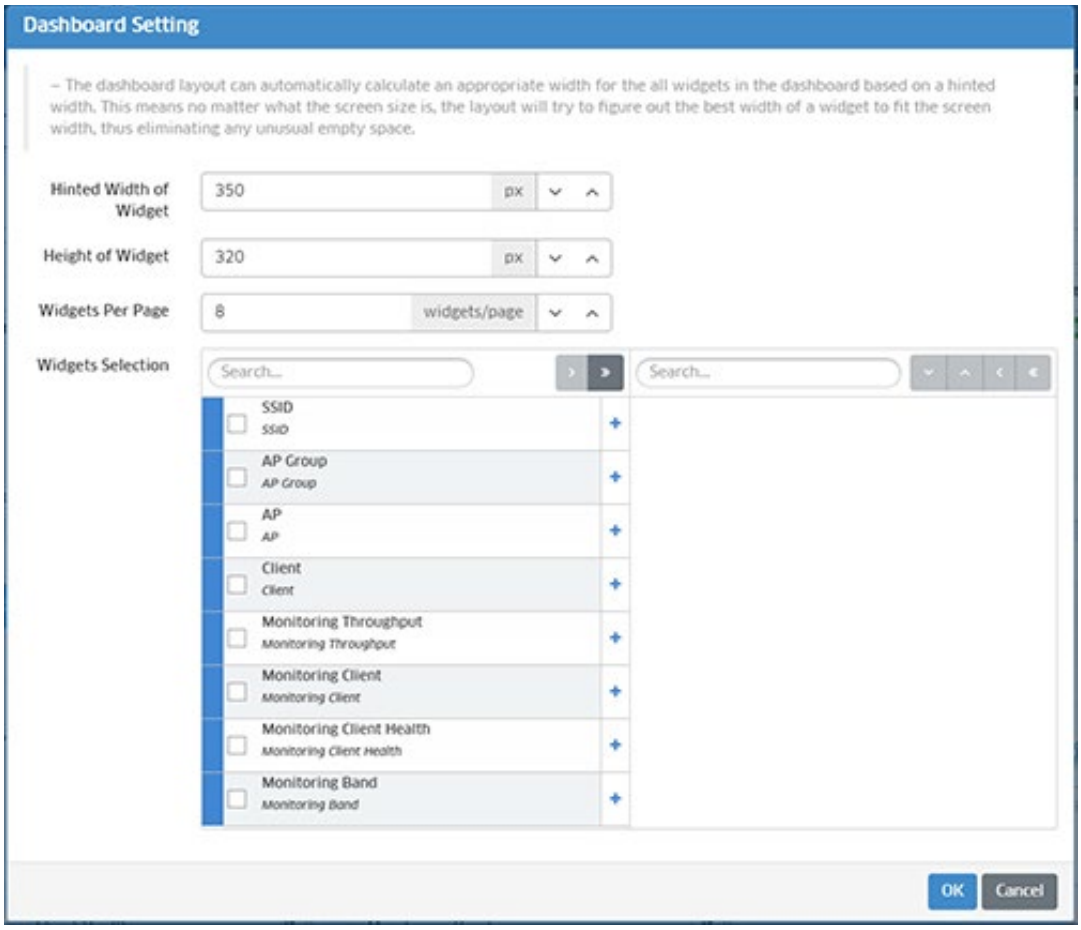
Changing the Dashboard Layout

The Settings option also enables you to customize the Dashboard layout. To customize the layout, click on Settings icon and select **Change Layout**. The Change Layout Screen appears. By default, widgets are displayed in the "Auto" layout. To change the layout, select an option on the left. When you select a layout on the left, the layout is displayed in the Layout area. To choose that layout, click **OK**. The change takes effect immediately. If necessary, you can re-arrange the widgets in the new layout by clicking and dragging them to new locations on the Dashboard.



WLAN Advanced Dashboard

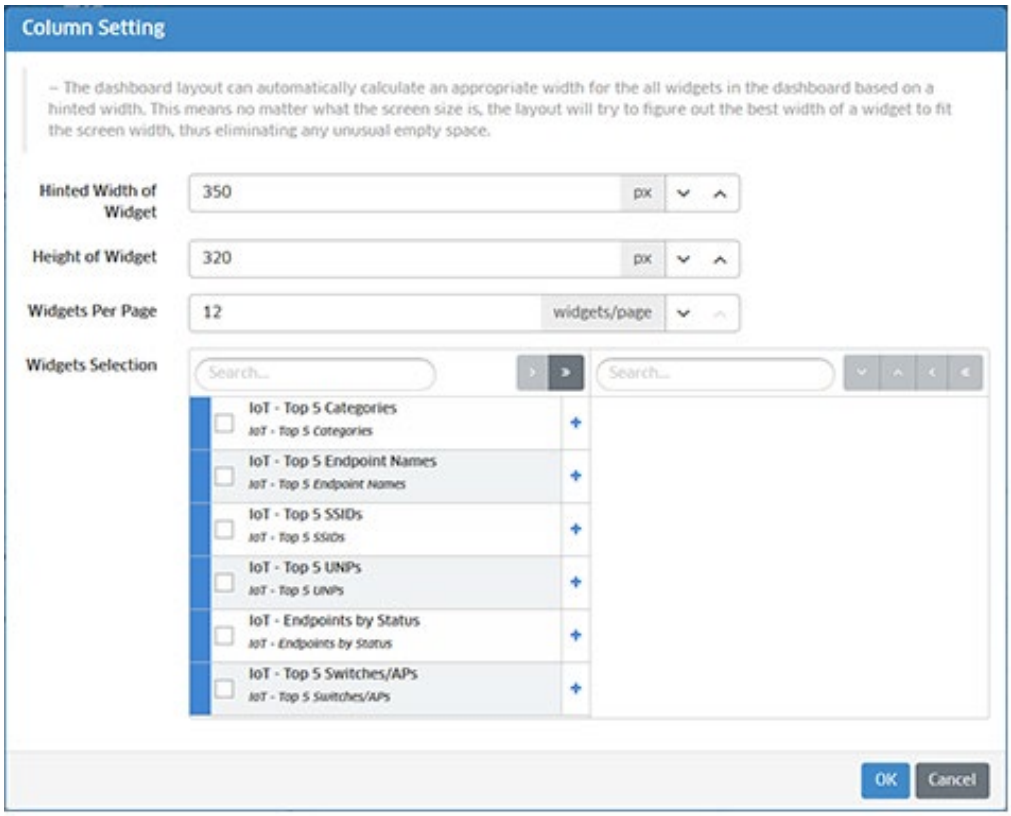
The WLAN Advanced tab displays all selected Stellar Wireless Application Widgets. Click on the Settings icon to bring up the Dashboard Setting Window (shown below) to customize the dashboard. Select layout options, then select the application widgets you want to display on the Dashboard. (Available widgets are displayed in the left column; selected widgets are displayed in the right column.) Click **OK** to apply the settings. If necessary, you can re-arrange the widgets in the new layout by clicking and dragging them to new locations on the WLAN Dashboard.



Note: By default, information for all managed APs is displayed in the widgets on the WLAN Dashboard. However, you can filter the information displayed by clicking on the **View By** link in the top left corner of the Dashboard and filtering the information displayed by SSID, AP Group, AP, and Client. The display filter will persist until it is changed or you log out of the session. If you log out, the display will return to the default setting (All).

IoT Dashboard

The IoT tab displays all selected IoT Application Widgets. Click on the Settings icon to bring up the Column Setting Window (shown below) to customize the dashboard. Select layout options, then select the application widgets you want to display on the Dashboard. (Available widgets are displayed in the left column; selected widgets are displayed in the right column.) Click **OK** to apply the settings. If necessary, you can re-arrange the widgets in the new layout by clicking and dragging them to new locations on the IoT Dashboard.



Performance Monitoring Dashboard

The Performance Dashboard displays Analytics Statistics Chart View Profile widgets. Statistics Chart View Profiles are graphical displays of collected statistics data. The profiles are configured in the Analytics application on the Analytics Statistics Chart View Screen (Network - Analytics - Statistics - Chart Views). To add a Statistics Chart View Profile widget to the dashboard, click on the Add icon at the top-right corner of the screen to bring up the Add Statistics Widget Window. Enter a **Name** for the widget, select a Statistics Chart View Profile from the **Chart View Profile** drop-down, and click on the **Create** button. The Statistics Chart View Profile will appear as a widget on the Performance Monitoring Dashboard. Repeat to add additional profile widgets. You can add up to 20 widgets to the dashboard. Note that you can click on the "Add New" link in the Chart View Profile drop-down to go to the Create View Profile Screen and create additional profiles, then return to the Dashboard to create a new widget. Also note that if you delete a profile from the Analytics Chart Views Screen, the widget for that profile will be removed from the Performance Monitoring Dashboard.

By default, a graphical view of the profile is displayed. Click on the Table icon at the top of the widget to display the data in table format. Click on the Graph icon at the top of the widget to return to graphical view. You can also click on the "Config" link at the bottom of the widget to modify the display time range.

Application Widgets

The following Global, WLAN Advanced, and IoT application widgets are available. Some widgets (e.g., Network Availability, Licenses) collect and display information automatically. Others (e.g., All Alarms, Top N Clients) require configuration in an application (e.g., Notifications, Application Visibility/Analytics) to display information. The descriptions below

provide an overview of the information provided by each widget and a link to the applicable help file for application configuration, if required. For detailed configuration procedures, see the applicable online help.

Global Application Widgets

The following Global application widgets are available.

Network

- **Network Availability -** Displays the current operational state (Up/Warning/Down) of all managed LAN Devices (All), and for APs (OAW). Each warning state is displayed as a percentage of all monitored switches. Click on a warning state to view a list of devices in that state. You can then click on a link to the Notifications application to view traps.
- **Alarms -** Displays an overview of Notification alarms (Acknowledged and Unacknowledged) for all managed devices by severity level (Normal, Warning, Minor, Major, Critical). Click on "Unack-ed" to view Unacknowledged Alarm information. Click on "All" to view information on all alarms (Acknowledged and Unacknowledged). Click on a severity level in the pie chart to go to the Notifications Home Screen and view traps with the selected severity level. You must configure traps in the Notifications application to generate and display information for this widget.
- **Top N Devices by Trap Distribution -** Displays a summary of traps by device and severity level. You must configure traps in the Notifications application to generate and display information for this widget.
- **Top N Ports Utilization Summary View -** Displays a summary view of the top network ports based on utilization. Switches/ports are displayed in a list view from highest to lowest utilization for the configured time period (e.g., day, week). You must create an Analytics Profile in the Analytics application and assign the profile to switches/ports to generate and display information for this widget.
- **Top N Ports Utilization Detail View -** Displays a detailed bar chart view of the top network ports based on utilization. While the Summary View displays the information for the configured time period (e.g., last 24 hours), this view provides a detailed view of the specified time interval. For example, if a report is configured to display information for the last 24 hours, the Detail View displays information for each hour within those 24 hours. Hover over an area in a bar chart to view information about devices/ports. You must create an Analytics Profile in the Analytics application and assign the profile to switches/ports to generate and display information for this widget.
- **Top N Ports Utilization Trending View -** Displays predicted future port utilization in a line chart based on past utilization. Port utilization predictions can provide valuable insight for capacity management. Click on a data point to view information about devices/ports. You must create an Analytics Profile in the Analytics application and assign the profile to switches/ports to generate and display information for this widget.
- **ProActive Lifecycle Management -** Provides an overview of ProActive Lifecycle Management information for network devices, such as the percentage/number of network devices under warranty or out of warranty. Information includes: OS Release Support, Hardware Support, Warranty Support, and Service Support. Page through

the widget to view each category. Click on the widget to go to the ProActive Lifecycle Management website.

- **Network Health - CPU -** Displays CPU usage information for all discovered devices. You can also set CPU Health Thresholds. These thresholds will be used to generate Notifications Traps in the Notifications applications if CPU Health Traps are configured.
- **Network Health - Memory -** Displays Memory usage information for all discovered devices. You can also set Memory Health Thresholds. These thresholds will be used to generate Notifications Traps in the Notifications applications if Memory Health Traps are configured.
- **Network Health - Temperature (Switches) -** Displays Temperature information for all discovered switches. You can also set Temperature Health Thresholds. These thresholds will be used to generate Notifications Traps in the Notifications applications if Temperature Health Traps are configured.
- **Top N PoE Ports Utilization Trending View -** Displays PoE Port power utilization in line chart format for PoE-enabled ports on the network. Click on a data point for more detailed information. You must create an Analytics Profile in the Analytics application and assign the profile to switches/ports to generate and display information for this widget.
- **Top N PoE Ports Utilization Detail View -** Displays PoE Port power utilization in bar chart format for PoE-enabled ports on the network. Hover the mouse over a bar chart for more detailed information. You must create an Analytics Profile in the Analytics application and assign the profile to switches/ports to generate and display information for this widget.
- **Top N PoE Switches Utilization Summary View** - Displays PoE Port power utilization by switch in pie chart format. Hover the mouse over a section for more detailed information. You must create an Analytics Profile in the Analytics application and assign the profile to switches/ports to generate and display information for this widget.
- **OmniVista Network Advisor** - Displays a list of OmniVista Network Advisor instances that are available to assign to one or more managed devices. Click on **Launch** to open the website for the Network Advisor instance. Click on the "More" link to open a list of Network Advisor instances from which you can add or remove instances.

IoT

- **IoT - Top 5 Categories -** Displays a list of the top 5 IoT categories based on the number of endpoints in each category. Click on each tab to view by endpoint status (Active/Error/Offline). Click on the "More" link for a table view of all endpoints by category.
- **IoT - Top 5 Endpoint Names -** Displays a list of the top 5 IoT endpoint names based on the number of endpoints by name. Click on each tab to view by endpoint status (Active/Error/Offline). Click on the "More" link for a table view of all endpoints by name.
- **IoT Top 5 SSIDs -** Displays a list of the top SSID endpoint names based on the number of endpoints on each SSID. Click on each tab to view by endpoint status (Active/Error/Offline). Click on the "More" link for a table view of all endpoint SSIDs.

- **IoT - Top 5 Switches/APs -** Displays a list of the top switches/APs based on the number of endpoints connected to the switch/AP. Click on each tab to view by endpoint status (Active/Error/Offline). Click on the "More" link for a table view of all switches/APs.
- **IoT Top 5 UNPs -** Displays a list of the top UNPs based on the number of endpoints assigned to each UNP. Click on each tab to view by endpoint status (Active/Error/Offline). Click on the "More" link for a table view of all UNPs.
- **IoT - Endpoints by Status -** Displays an overview of all endpoints by status (Error/Active/Offline). Hover over a status to view the number and percentage of endpoints in each status. Click on the "More" link for a detailed table view of all endpoints.

WLAN

- **UPAM Status -** Displays the administrative status of the AP Service in OmniVista.
- **AP Groups -** Displays information for all configured AP Groups. Click on a group to display information on APs in the group.
- **AP Management -** Displays information for all Managed and Unmanaged APs. Click on a category (Managed, Unmanaged) to display an overview of the administrative status for APs in that category (the number of APs Up/Down). Click again on that status information for information on the individual APs in that category.
- **Intrusive APs -** Displays the number of Intrusive APs detected on the network by category (e.g., Rouge AP, Interfering AP). Click on a category to display information for information on the individual APs in that category. This widget displays information based on policies configured in the WIPS application.
- **Wireless Attacks in the Last 24 Hours -** Displays information about attacks on the wireless network. This widget displays information based on policies configured in the WIPS application.
- **Client Health -** Displays information about all clients currently connected to APs, including Blocklisted Clients. The graph gives an overview of signal strength for clients, including the number of clients in each category.
- Best - Signal strength is more than -65
- Good - Signal strength is between -80 and -65
- Fair - Signal strength is less than -80.

Application Analytics - Layer 4

- **Top N Clients Detail View -** Displays detailed bar chart view of the top network clients. For example, if a report is configured to display data for the last 24 hours, the Detail View displays data for each hour within those 24 hours. Hover over an area in a bar chart to view information about a client. You must create an Analytics Profile in the Analytics application and assign the profile to switches/ports to generate and display information for this widget.
- **Top N Clients Summary View -** Displays summary information for the top network clients based on the number of traffic flows for each client in a pie chart view. Hover over a section to view client information. Click on a section to view application information for that client. You must create an Analytics Profile in

the Analytics application and assign the profile to switches/ports to generate and display information for this widget.

- **Top N Apps Detail View -** Displays a detailed bar chart view of the top applications being accessed on the network for the configured time period. For example, if a report is configured to show data for the last 24 hours, the Detail View displays data for each hour within those 24 hours. Hover over an area in a bar chart to view information about an application. You must create an Analytics Profile in the Analytics application and assign the profile to switches/ports to generate and display information for this widget.
- **Top N Apps Summary View -** Displays summary information about the top applications being accessed on the network in a pie chart view with each application displayed as a percentage of the total traffic for all monitored switches. The top applications are determined using sFlow. Hover over a section to view application information. Click on a section to view client or switch information. You must create an Analytics Profile in the Analytics application and assign the profile to switches/ports to generate and display information for this widget.

Application Analytics - Layer 7

- **Application Flow Count OS6860/APs -** Displays traffic flow information for applications/application groups discovered on the network, and the percentage of network resources being used by each application for the selected devices and configured time period. OS6860/OS6860E Switches and APs provide flow information (number of flows) in the App Discovery view and packet/byte information in the App Count view.
- **Application Bandwidth Usage Summary View -** Displays packet/byte count information for applications/application groups discovered on the network, and the percentage of network resources being used by each application for the selected devices and configured time period. The information is displayed in pie chart view.
- **Application Bandwidth Usage -UNPs Summary View -** Displays packet/byte count information for applications/application groups discovered on the network over the configured period of time, and the percentage of network resources being used by each application by UNP. The information is displayed in pie chart view.
- **Application Bandwidth Usage Detail View -** Displays packet/byte count information for applications/application groups discovered on the network, and the percentage of network resources being used by each application for the selected devices and configured time period. The information is displayed in line chart view.
- **Application Bandwidth Usage-UNPs Detail View -** Displays packet/byte count information for applications/application groups discovered on the network over the configured period of time, and the percentage of network resources being used by each application by UNP. The information is displayed in line chart view.

General

- **Locator -** Used to locate the switch and slot/port that is directly connected to a user-specified end station. Enter the end station's IP Address, Host Name, MAC address, or Authenticated User ID to locate the switch and slot/port to which the end station is connected. Enter the search criteria and click on **Locate**. OmniVista will display the results in the Locator application.

- **Favorites -** The Favorites widget allows users to create a list of “quick links” for easy access to any OmniVista 2500 NMS application. To add an application to the Favorites list, start typing the name of the application in the text box. As text is entered, auto-complete displays a list of matching applications. Click an application to select it, then click the add icon (**+**). To replace an application in the list of Favorites, click the **Edit** icon. Begin typing the new application name. Select the application and click the **Save** icon. Once an application has been added to the Favorites widget, a link to the application will also display under the Favorites tab in the OmniVista 2500 NMS Main Navigation Menu. To remove an application from the Favorites widget, click the Delete icon next to the application link.
- **Quarantine Manager -** Displays an overview of the number of devices in each Quarantine Manager category (Candidates, Banned, Never Banned, Disabled Ports). You must configure Quarantine Manager to display information for this widget.
- **Device Licenses -** Displays an overview of device license usage. Information is displayed for all enabled licenses (ALE Devices, Third Party Devices, OmniAccess Stellar APs) including the number of devices being managed, maximum number of devices that can be managed, and expiration (if applicable). This widget automatically displays information for all discovered network devices.
- **Service Licenses -** Displays an overview of service license usage. Information is displayed for all enabled licenses (VMs, Stellar AP Guest Devices, Stellar AP On-Boarding Devices, and UPAM Redundancy) including the number of devices being managed, maximum number of devices that can be managed, and expiration (if applicable). This widget automatically displays information for all discovered network devices.
- **OV System Health -** Provides an overview of health information for the OmniVista Virtual Appliance (VA). For more detailed information, click on the "More" link to go the the OV System Health Screen. Click on the "Config" link to go the OV System Health Settings Screen and configure OV Stem Health settings (e.g., trap settings, widget refresh interval). If there is a mis-configuration of the VA, an error message will appear at the top of the widget. Click on the message to go to the OV Misconfiguration Screen for more details.
- **Network Health Unacknowledged Traps -** Displays the number of unacknowledged Switch Module, Switch Port, AP CPU, and AP Memory Traps. Click on a row to go to the Notifications applications to view the traps. If necessary, click on the "Config" link at the bottom of the widget to go to the Notifications application and quickly configure the necessary traps. After selecting devices on the Devices Selection Screen of the Trap Configuration Wizard, the applicable traps (healthMonModuleTrap, healthMonPortTrap, apCPUOverrun, apMemoryOverrun) will be pre-selected on the Configure Traps Screen.

SAA Ethernet

- **Top N RTT Paths -** Displays the top number of paths with the highest round-trip time.
- **Top N Jitter Paths -** Displays the top number of paths with the highest jitter.
- **Top N Packets Lost Paths** - Displays the top number of paths with the highest packets lost.

WLAN Advanced Widgets

The following WLAN Advanced application widgets are available.

- **SSIDs -** Displays all configured WLAN Services.
- **AP Groups -** Displays information for all configured Stellar AP Groups. Click on the "AP(s)" link in the AP Count column to display information on APs in the group. This widget automatically displays information for all configured groups.
- **APs -** Displays information for all registered Stellar APs. This widget automatically displays information for all registered APs
- **Most Recent 1000 Client Records -** Displays information about all active clients on the network. Click on the "More" link at the bottom of the widget to display the most recent 1,000 client sessions on all Stellar APs on the network. You can then click on the "Go to App" link to go to the UPAM Wireless Client List Screen. Click on a client in the widget to bring up the "Details of Client" window, which displays detailed information about the selected client and its sessions.
- **Client Throughput -** Displays information about data throughput for all clients currently connected to Stellar APs. This widget automatically displays information for all registered APs.
- **Client Health -** Displays health information for all clients currently connected to Stellar APs. This widget automatically displays information for all registered APs.
- **Band Usage -** Displays radio band information for all clients currently connected to Stellar APs. This widget automatically displays information for all registered APs.
- **Client Density -** Displays information about the number of clients and system throughput on your network.
- **Upload Throughput -** Displays information about client upload throughput.
- **Download Throughput -** Displays information about client upload throughput.
- **Distribution of Clients per AP-** Displays information about the number of clients associated with each AP.

Note: By default, the WLAN Tab displays information on all registered Stellar APs. You can also filter the view to display information by specific SSID, AP Group, AP, or Client. Click on the “View by” link at the top of the Dashboard to filter the display.

IoT Widgets

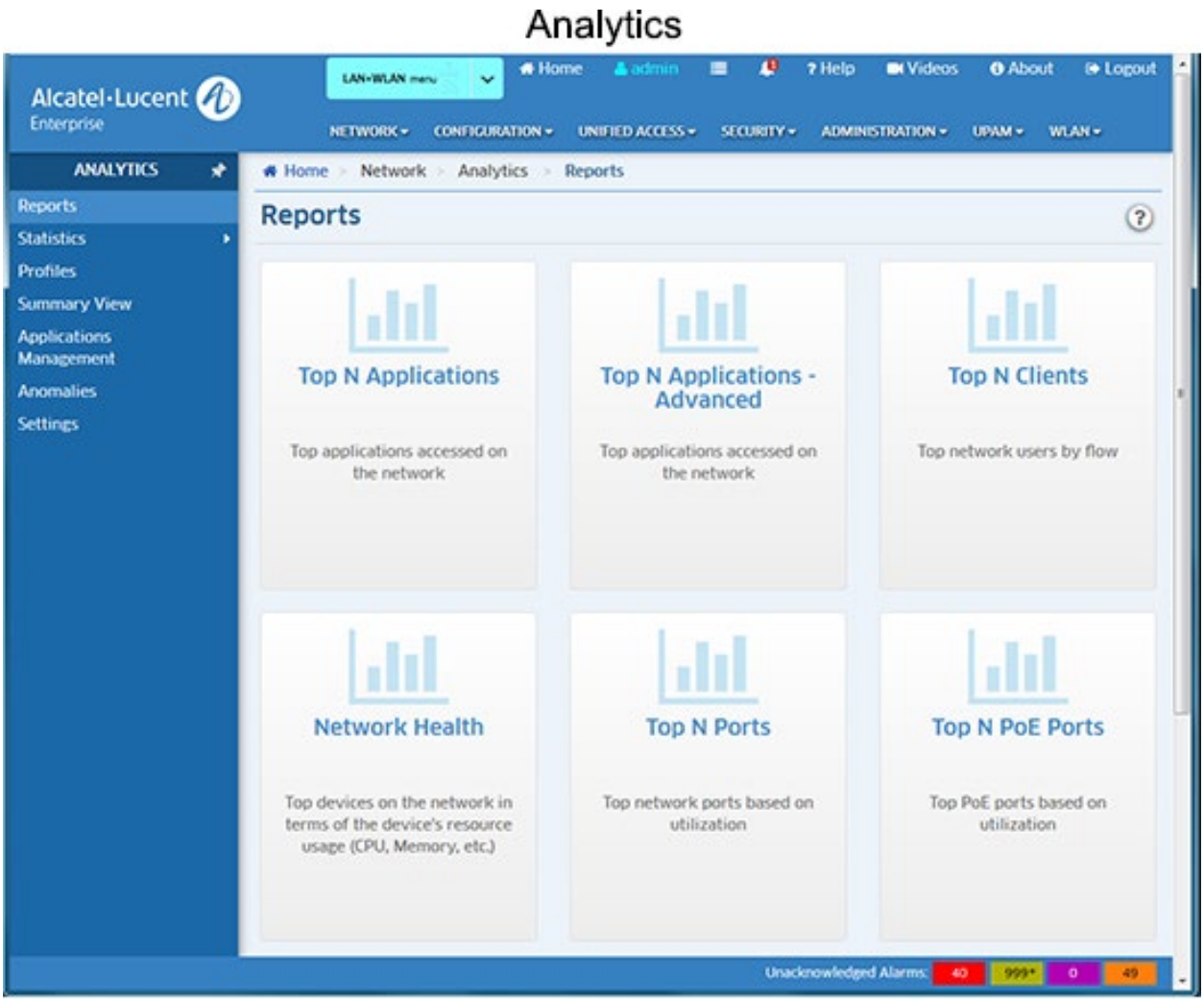
The following IoT application widgets are available.

- **IoT - Top 5 Categories -** Displays a list of the top 5 IoT categories based on the number of endpoints in each category. Click on each tab to view by endpoint status (Active/Error/Offline). Click on the "More" link for a table view of all endpoints by category.
- **IoT - Top 5 Endpoint Names -** Displays a list of the top 5 IoT endpoint names based on the number of endpoints by name. Click on each tab to view by endpoint status (Active/Error/Offline). Click on the "More" link for a table view of all endpoints by name.
- **IoT Top 5 SSIDs -** Displays a list of the top SSID endpoint names based on the number of endpoints on each SSID. Click on each tab to view by endpoint status (Active/Error/Offline). Click on the "More" link for a table view of all endpoint SSIDs.

- **IoT - Top 5 Switches/APs -** Displays a list of the top switches/APs based on the number of endpoints connected to the switch/AP. Click on each tab to view by endpoint status (Active/Error/Offline). Click on the "More" link for a table view of all switches/APs.
- **IoT Top 5 UNPs -** Displays a list of the top UNPs based on the number of endpoints assigned to each UNP. Click on each tab to view by endpoint status (Active/Error/Offline). Click on the "More" link for a table view of all UNPs.
- **IoT - Endpoints by Status -** Displays an overview of all endpoints by status (Error/Active/Offline). Hover over a status to view the number and percentage of endpoints in each status. Click on the "More" link for a detailed table view of all endpoints.

3.0 Analytics

The Analytics Application provides users with a comprehensive view of network resource utilization, including views of users, devices, and applications. The application also provides information on usage trends, including predictive analysis of future network resource utilization. The Reports Screen (shown below) is used to view Analytics Reports and configure how the information is displayed.



Note: The Analytics Application provides real-time viewing of Analytics Reports. You can also schedule Analytics Reports to be generated and stored as PDF documents using the Report Application. This way, in addition to real-time viewing in the Analytics Application, you can automatically generate and store Analytics Reports that you can view at any time. Note that users authenticated through an external RADUIS Server can only generate live reports, not scheduled reports. Users authenticated through the Local OmniVista Authentication Server can generate both live and scheduled reports.

Using Analytics

The Analytics application enables users to create different reports (e.g., Top N Applications, Top N Ports Utilization) that provide a comprehensive view of network and device utilization. The following screens are used to view/analyze the network using the Analytics application:

- **Reports -** Used to configure reports that provide a comprehensive view of network resource utilization and device status. Top N Applications, Top N Applications - Advanced, Top N Clients, Network Health, and Top N Ports Utilization Reports can be configured to show network utilization over different time periods (e.g., daily, hourly, monthly), and show trends in network utilization over those time periods. The Top N Ports Utilization Report can also provide predictive analytics to show expected future usage. Other reports can provide a "real-time" view of all discovered network switches (Network Availability, Alarms). The following reports can be created:
- **Top N Applications -** Displays information about the top applications being accessed on the network, including which users are using an application, and which switches have the most traffic for an application. The Top N Applications are determined using sFlow. To generate a Top N Applications Report, you must first create an Analytics Profile.
- **Top N Applications - Advanced -** Displays information about the top applications being accessed on the network based on Signature Profiles configured in the Application Visibility Application.
- **Top N Clients -** Displays information for the Top Network clients including the number of traffic flows for each client. To generate a Top N Clients Report, you must first create an Analytics Profile.
- **Network Health -** Displays the health of all discovered network devices in terms of CPU, Memory, Temperature.
- **Top N Ports -** Displays network ports by utilization over time; and also provides predictive analytics to show future port utilization trends. To generate a Top N Ports Utilization Report, you must first create an Analytics Profile.
- **Top N PoE Ports -** Displays network PoE port power utilization by port. To generate a Top N PoE Ports Report, you must first create an Analytics Profile.
- **Top N PoE Switches -** Displays network PoE port power utilization by switch. To generate a Top N PoE Switches Report, you must first create an Analytics Profile.
- **Network Availability -** Displays the current operational state of all discovered network devices (Up/Warning/Down).
- **Alarms -** Displays network alarms by severity level for all discovered network devices.
- **AP Uptime/Downtime -** Displays detailed information about Stellar AP Uptime/Downtime and AP/OmniVista Link status.
- Statistics - Used to collect, monitor, and view statistical information for devices throughout the network.

  Collection - Used to create custom Collection Profiles to collect statistics from specific switches containing specific statistics variables

  Chart Views - Used to create View Profiles to view statistics data.
- **Profiles -** Used to create Analytics Profiles. To generate an Analytics Top N Applications, Top N Applications - Advanced, Top N Clients, and Top N Ports

Utilization Report you must first create an Analytics Profile that defines the switches/ports that you want to view and the type of information that you want to view on those switches/ports.

- **Summary View -** Displays basic information on all supported network devices, including any Analytics Profiles defined for a device.
- **Applications Management -** When generating a Top N Applications Report, the Analytics application uses port numbers to identify application traffic. This screen is used to create port/application mappings to identify applications traffic.
- **Anomalies -** Displays any port utilization anomalies. An anomaly is a utilization data point that fall outside of expected norms based on past usage.
- **Settings -** Used to configure preferences for port utilization trending and anomaly detection in the Analytics application.

Note: Remember, to generate Top N Applications, Top N Clients, and Top N Ports Utilization Reports, you must first create an Analytics Profile that defines the switches/ports that you want to view and the type of information that you want to view on those switches/ports. To generate a Top N Applications - Advanced Report, you must first create a Signature Profile in the Application Visibility Application that defines the switches/ports that you want to view and the type of information that you want to view on those switches/ports. Data will only be gathered and displayed for those switches/ports included in the profile. You do not need to create a profile for Network Availability, Alarms, Network Health, or SIP Reports.

Configuring Analytics

The first step in generating analytics information for Top N Applications, Top N Clients, and Top N Ports Utilization Reports is to go to the Profiles Screen and create an Analytics Profile. Analytics information is gathered by creating an Analytics Profile that specifies the information to be viewed (e.g., Top N Applications, Top N Ports Utilization) and the network switches/ports that will be monitored. The Profile Type will determine the type of Analytics Report that you can generate (e.g., Top N Applications, Top N Users). Reports will generate data only for those switches/ports included in a profile.

Network Availability, Alarms, Network Health, provide a "real time view" of the network. You do not need to create a profile for these reports. However, to view network alarms (Alarm Report) you must go to the Notifications application and configure traps on the switches you want to monitor. Network alarms will then be displayed on the Alarms Report Screen. (These alarms are also displayed, along with all network alarms, in the Notifications application.)

You can view all Analytics Reports on the applicable report screen. The information in the reports is presented in graphical and linear format, depending on the report type.

Reports

Analytics Reports provide users with a comprehensive view of network resource utilization, including information on users, devices, and applications. Reports can also provide information on usage trends, including predictive analysis of future network resource utilization. Top N Applications, Top N Applications - Advanced, Top N Clients, Network Health, and Top N Ports Utilization Reports can be configured to show network utilization over different time periods (e.g., daily, hourly, monthly), and show trends in network utilization over those time periods. The Top N Ports Utilization Report can also provide predictive analytics to show expected future usage. Other reports can provide a "real-time" view of all discovered network switches (Network

Availability, Alarms). You can view the reports in different formats and customize how the data is displayed. The following reports can be created:

- **Top N Applications -** Displays information about the top applications being accessed on the network, including which users are using an application, and which switches have the most traffic for an application.
- **Top N Applications - Advanced -** Displays information about the top applications being accessed on the network based on Signature Profiles configured in the Application Visibility Application.
- **Top N Clients -** Displays information for the Top Network clients including the number of traffic flows for each client.
- **Network Health -** Displays the health of all discovered network devices in terms of CPU, Memory, Temperature.
- **Top N Ports -** Displays network ports by utilization over time; and also provides predictive analytics to show future port utilization trends.
- **Top N PoE Ports -** Displays network PoE port power utilization by port.
- **Top N PoE Switches -** Displays network PoE port power utilization by switch.
- **Network Availability -** Displays the current operational state of all discovered network devices (Up/Warning/Down).
- **Alarms -** Displays network alarms by severity level for all discovered network devices.

Note: To generate a Top N Applications, Top N Applications - Advanced, Top N Clients, and Top N Ports Report, you must **first create an Analytics Profile** using the Profile Screen that defines the switches/ports that you want to view and the type of information that you want to view on those switches/ports. Date will only be gathered and displayed for those switches/ports included in the profile. You do not need to create a profile for Network Availability, Alarms, Network Health, or SIP Reports. These reports simply show real-time information for all discovered switches.

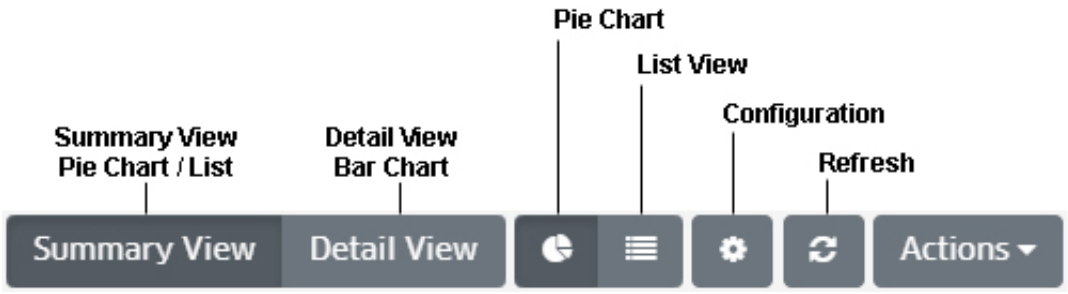
Note: Top N Apps & Clients Profiles use sFlow to gather information. When these profiles are created, the OmniVista Server is automatically configured as the sFlow Receiver. However, sFlow can be configured on a device outside of OmniVista (e.g., using the CLI). If sFlow is configured on a device outside of OmniVista and the OmniVista Server is designated as the sFlow Receiver, the information for that device is sent to OmniVista and included in Top N Applications and Top N Clients Reports. (Information will be displayed in these reports even if no profile was created and assigned in OmniVista.) If the device is not known to OmniVista (or if the Analytics Application is not supported on the device), sFlow information is sent to OmniVista, but the information is not included in those reports.

The sections below describe the different report options and basic behavior for all reports. The report options vary depending on the report type (e.g., Top N Applications, Network Health). Specific views/options are detailed in the help pages for each report type. Click on a link above to view specific instructions for each report type.

Report Options

Analytics Reports can be viewed in different formats (e.g., pie chart, bar chart). You can also configure a custom view to change the amount of information displayed (e.g., the number of Applications/Clients displayed), as well as the timeframe that you want to view (e.g., last 24

hours, last 7 days). You can also view data trends by "drilling down" in a Detailed Report. You can also print a report or download a report in PDF or PNG format, and even include the data as part of a scheduled report that is automatically generated in the Report Application. These options can be configured using the Options Bar (shown below) displayed at the top of every report.



View Options

By default, the Summary View is initially displayed for all reports. This may be displayed graphically as a pie chart (e.g., Top N Applications, Top N Ports Utilization) or in a list (e.g., Network Health). The Detail View displays a detailed subset of the information in a bar chart format. While in the Detail View, you can also display an even more detailed subset of the data to view data trends. For example, if a Summary View is displaying data for the last week, the Detail view will display data for each day of the last week; and clicking on a day in the Detail view chart will display data for each hour of that day, enabling you to view hourly data trends.

For "Top N" Reports (e.g., Top N Applications, Top N Clients), you can configure the amount of data displayed and the time period you want to view. You can set the number of "top" (in terms of utilization) applications, clients, or switches you want in the display. For example, you might want to see the top 10 applications displayed in a Top N Applications Report; or the top 20 ports displayed in a Top N Ports Utilization Report. You can also configure the time period to display (last 24 hours, last 7 days, last 4 weeks).

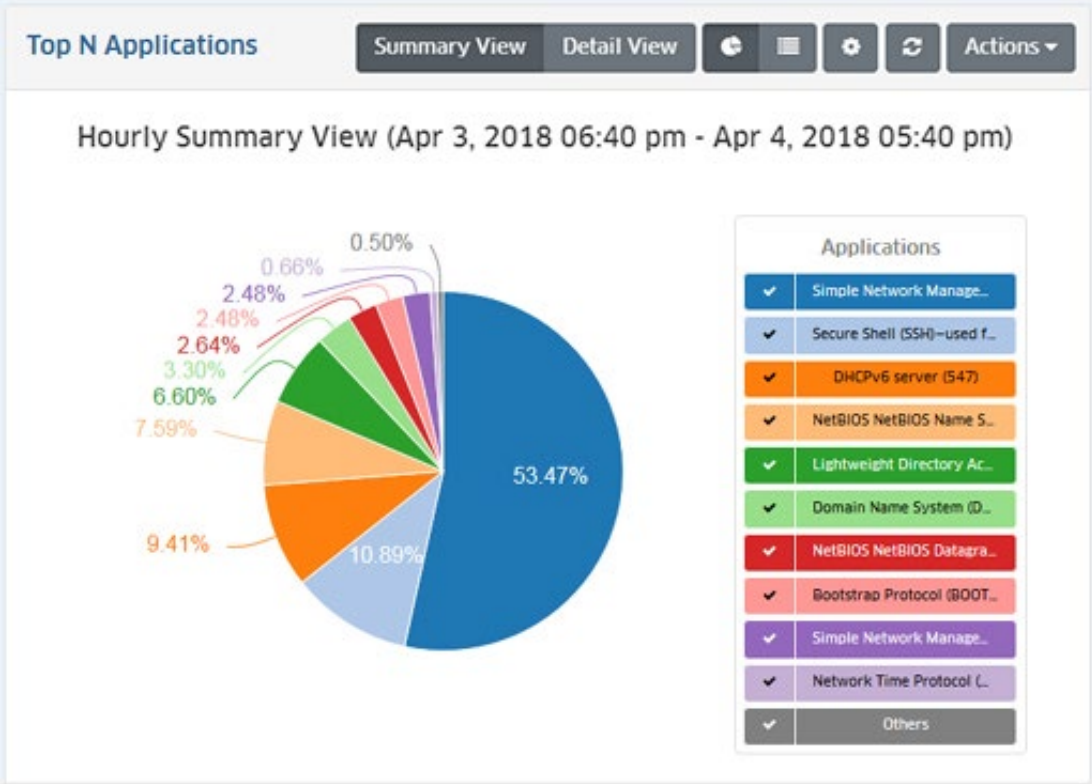
The chart legend to the right of each display labels each item in the chart by color and text. By default, information from all switches/ports included in a profile is displayed. The number of entities displayed in the legend and the chart depends of the number you configure for the profile (e.g., top 10, top 20). However, you can click on the **Select Devices** button at the top of the screen to display only information from specific switches/ports.

> **Note:** You may notice a category labeled "Others" in "Top N" Reports. Remember, only the "top" applications, clients, or switches as determined by the profile (top 10, top 20) are displayed. There may be many others in the profile that are not in the "top" 10 or 20. The "Others" category gives you an idea of all of the other applications, clients, or switches in the profile with low utilization rates that do not qualify as a "top" application, client, or switch.

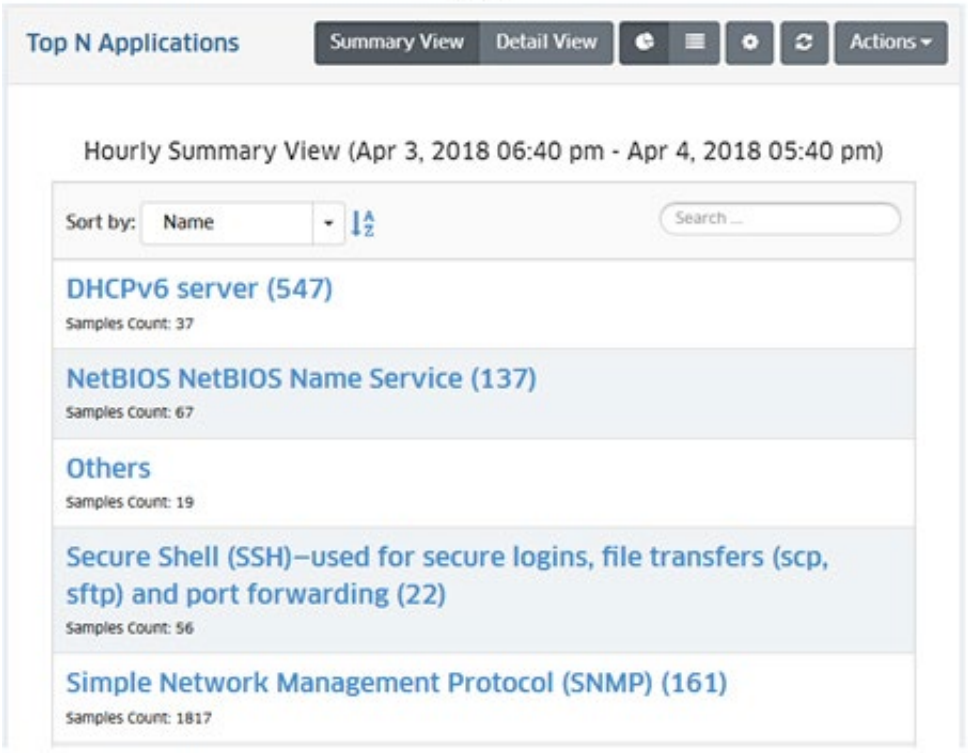
Summary View

The Summary View displays information either in pie chart format, with each entity (e.g., application, client) displayed at a percentage of the total for the configured time period (e.g., 24 hours); or in list format, with each entity listed from highest to lowest. By default, data for the past 24 hours is shown. However, you can change the timeframe, as well as the number of entities displayed (top applications, top ports). The examples below show an Hourly Summary View for the Top N Applications Report.

Summary View
Pie Chart

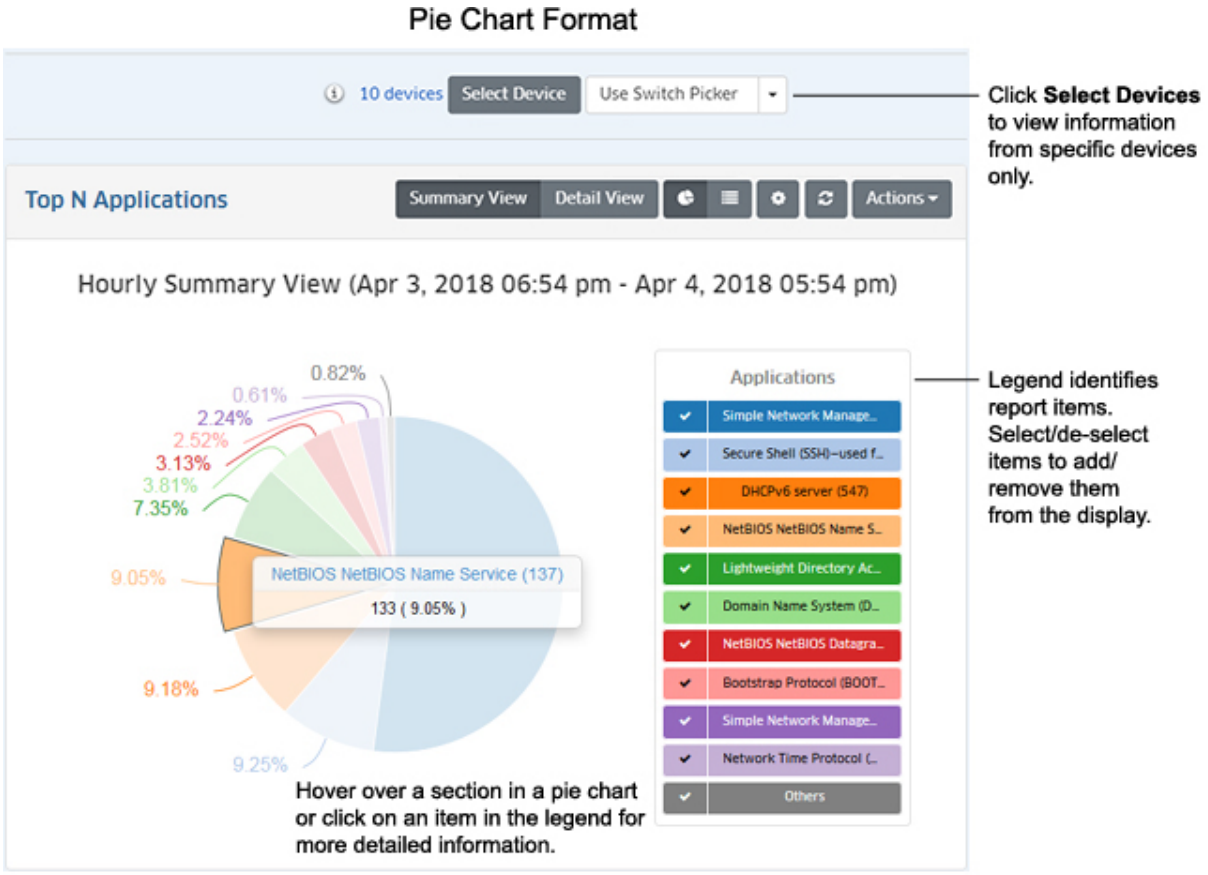


Summary View
List



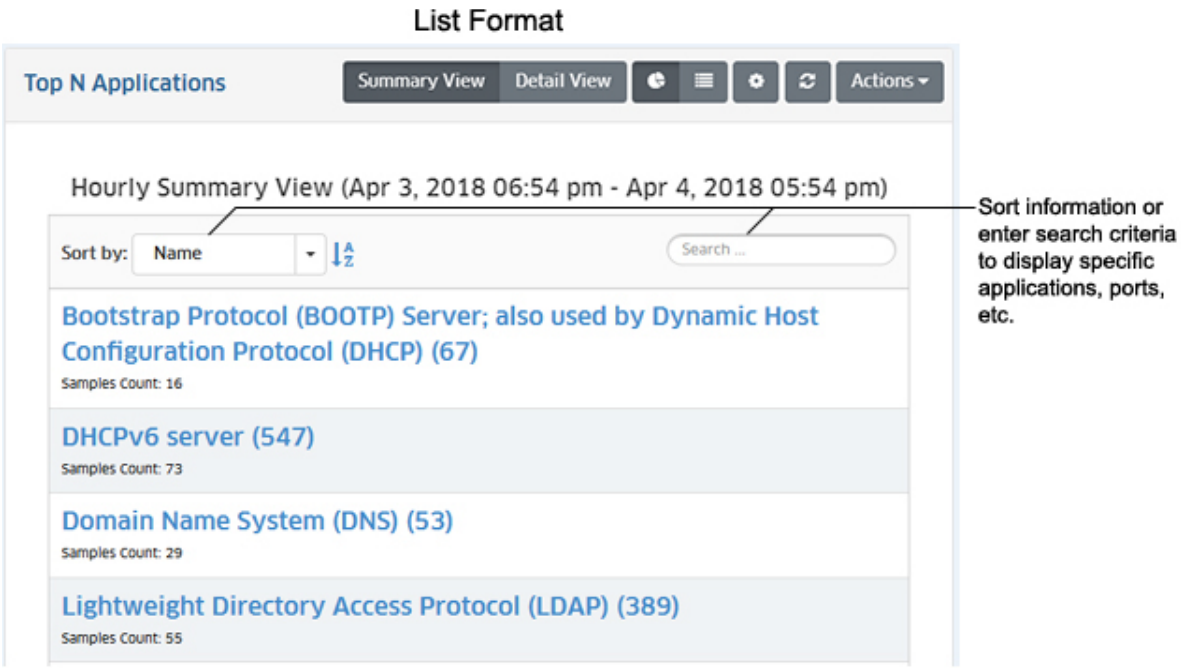
Pie Chart Format

The Pie Chart Format displays information in a pie chart with each entity displayed as a percentage of the total. The legend identifies each item in the chart by color and text. For example, the legend in a Top N Applications Report (shown below) identifies the applications displayed in the pie chart. (The legend in a Top N Ports Utilization Report would identify the switches/ports displayed.) You can hover over a section of the chart (or click on an item in the legend) to view detailed information for that section. For example, in the Top N Applications pie chart below, you could hover over an application in the chart to view the number of flows from that application. You can also click select/deselect an item in the legend to add/remove the item from the display.



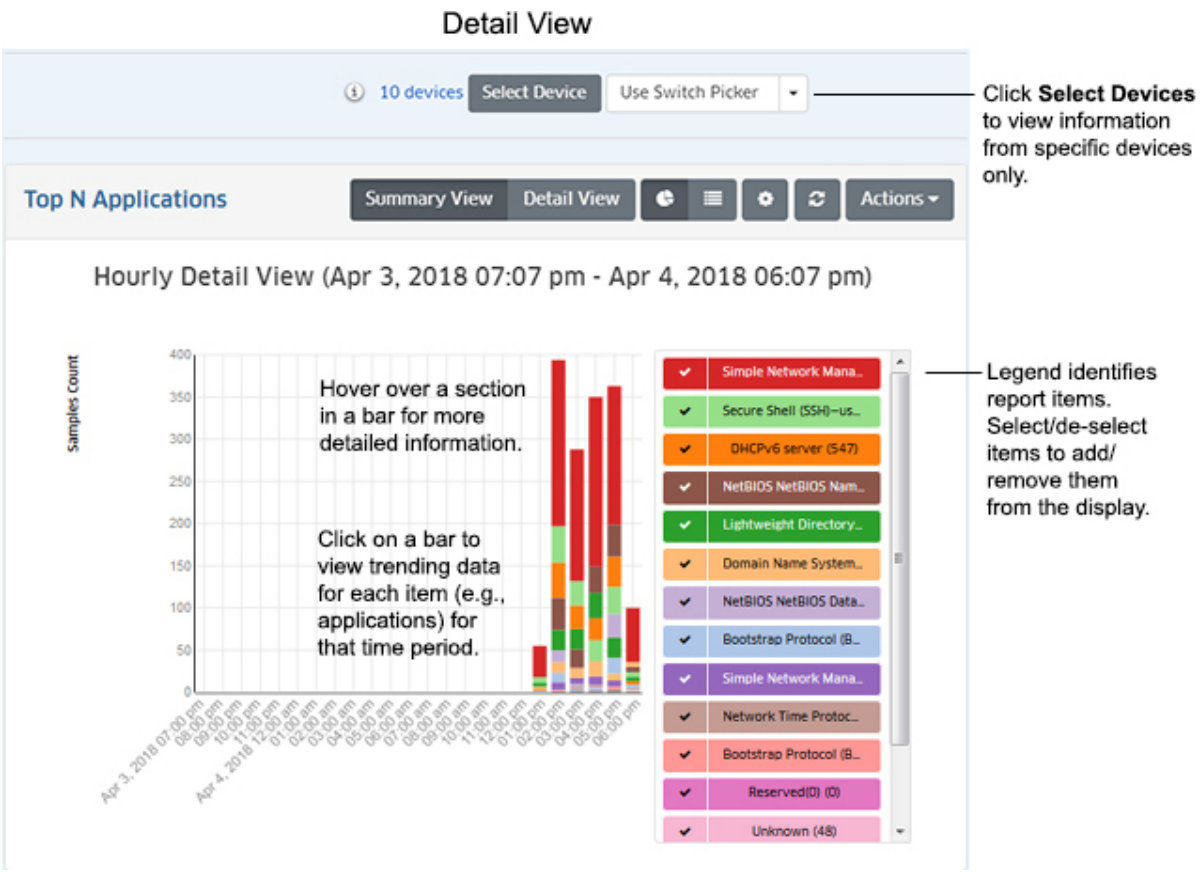
List Format

The List Format displays information in list form (e.g., a list of Switches, Applications, or Users displayed from highest to lowest). You can sort the display by specific criteria (e.g., name), sort in ascending/descending order by, or search for and display specific information (e.g., display only a specific application or port number). The example below shows a Top N Applications Report.



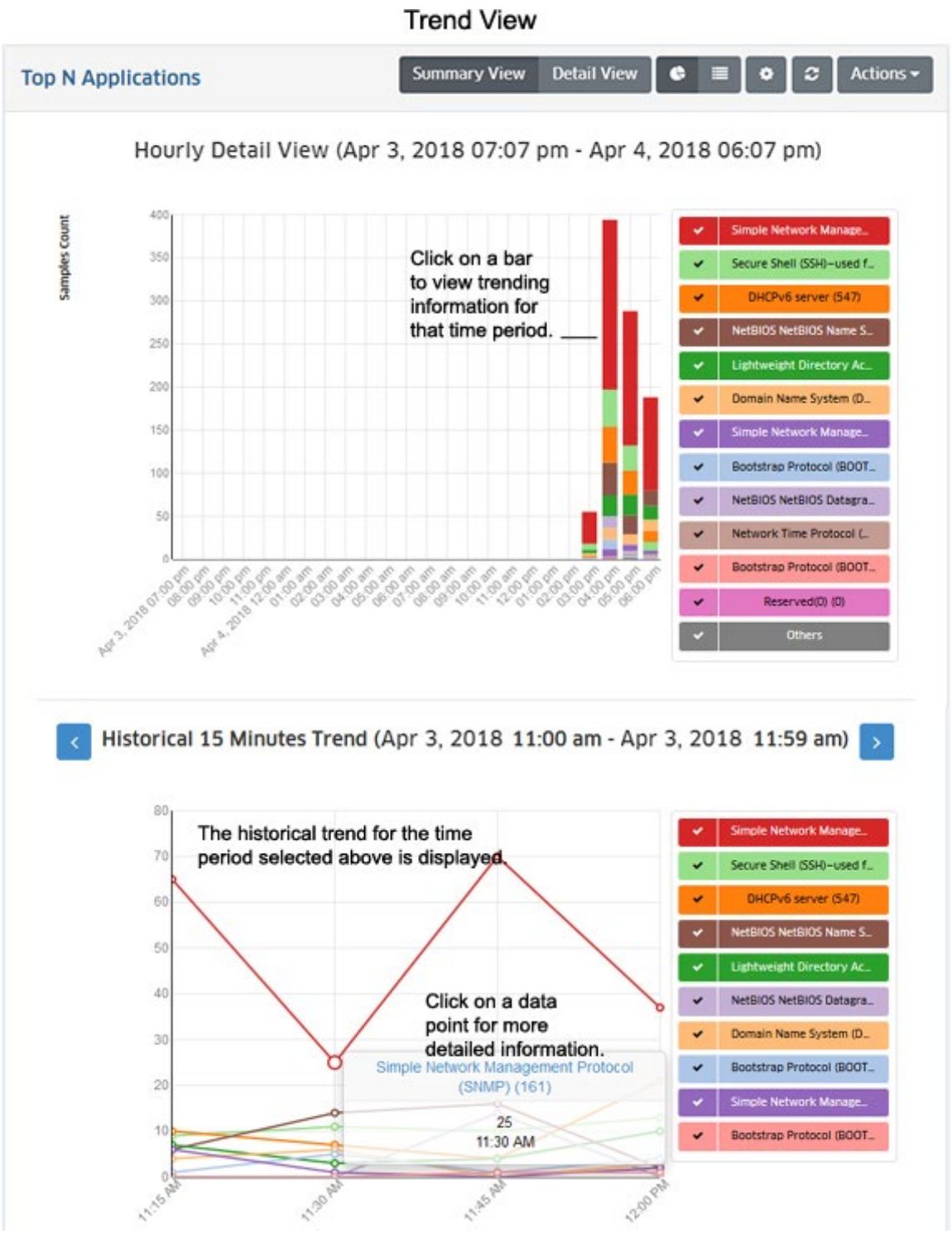
Detail View

The Detail View displays a detailed subset of the information in bar chart format for the configured time period. For example, if a report is configured to show data for the last 24 hours, the bar chart view would display data for each hour over those 24 hours. The legend identifies each item in the chart by color and text. For example, the legend in a Top N Applications Report (shown below) identifies the applications displayed in the bar chart. (The legend in a Top N Ports Utilization Report would identify the switches/ports displayed.) You can hover over an area in a bar to view detailed information for that item. For example, in the Top N Applications bar chart below, you could hover over an area in a bar to view the number of flows from that application. Or you can click on an item in the legend to isolate the item in the display and show the same detailed information. You can also click select/deselect an item in the legend to add/remove the items from the display. You can also view data trends by "drilling down" on a data set to see a subset of that data.



Data Trends

You can view data trends by "drilling down" on a data set to see a subset of that data. Click on a bar in the chart to view the data trend for that selection. For example, if you selected one of the bars in an Hourly Detail View, the trend for that hour would be displayed in 15-minute increments (as shown below). (If you selected one of the bars in a Daily Detail View, the trend for that hour would be displayed in one-hour increments.) You can scroll forward or back through the trending date using the arrows at the top of the chart.



Depending on the timeframe in the chart (e.g., Monthly, Weekly), data trend subsets are displayed as follows:

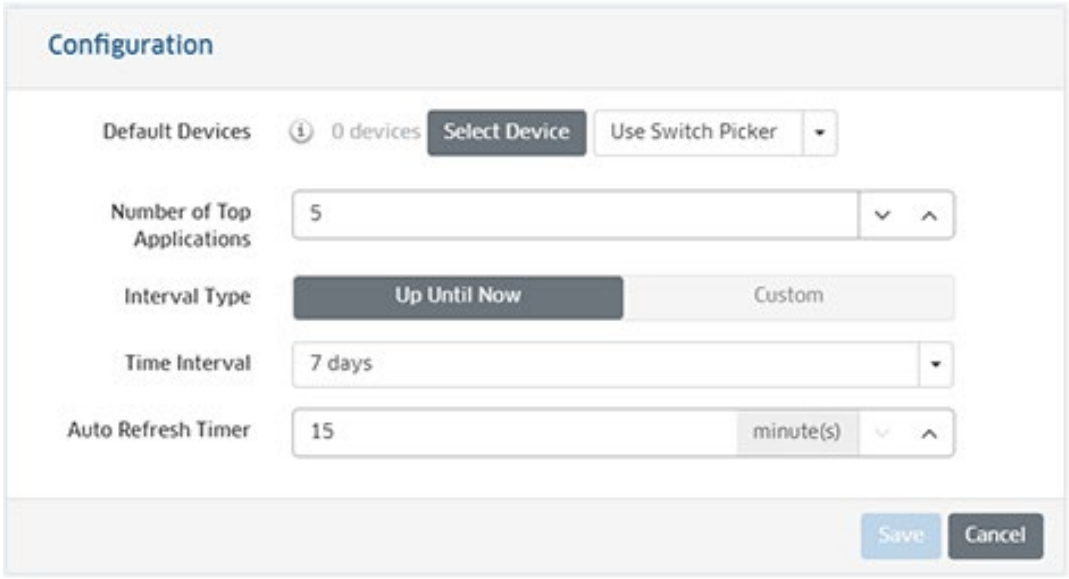
- Monthly Details View - A Weekly Trending View
- Weekly Details View - Daily Trending View
- Daily Details View - Hourly Trending View

- Hourly Details View - 15-minutes Trending View.

Configure a Custom Report

You can configure the report view by clicking on the Configuration icon and customizing the display. The Configuration Screen for the Top N Applications Report is shown below. The configuration options vary depending on the report type. Specific field descriptions are defined in the help pages for each report type. Once you update any options and click on the **Save** button, reports will be displayed in the new format.

Configuration Screen



Download/Print a Report

You can download a report in PDF or PNG format or send the report to a printer by clicking on the **Actions** button in the Options Bar and making a selection from the drop-down menu (**Download PNG Image**/**Download PDF Document**/**Print Image**).

Schedule a Report

You can add the current report view to a Report that you create in the Report Application by clicking on the **Actions** button in the Options Bar and selecting **Add to Report**. The Report Application enables you to create and schedule Analytics Reports that can be viewed and stored as PDF documents. This way, in addition to real-time viewing of Analytics Reports in the Analytics Application, you can automatically generate and store Analytics Reports that you can view at any time. See the Report Configuration Help for more information.

Top N Applications

The Analytics Top N Application Report Screen displays information about the top applications being accessed on the network. The Top N Applications are determined using sFlow. OmniVista identifies the applications using the TCP/UDP port obtained from sFlow packets. In other words, traffic on a specific port is identified as coming from a specific application. Well known ports (e.g., 161 for SNMP, 80 for HTTP) are automatically identified and labeled in the Top N

Applications Report. Other applications can be mapped to a port using the Applications Management Screen.

To generate a Top N Applications Report, you must first create and assign an Analytics Profile using the Profile Screen that defines the switches/ports that you want to view and the type of information that you want to view on those switches/ports.

> **Note:** sFlow is enabled on a port when you create an Analytics Profile. However, sFlow can also be enabled on a port using the CLI. If sFlow is enabled on a port using the CLI and the OmniVista Server is configured as the receiver, Top N Applications data will be displayed in OmniVista.
>
> **Note:** sFlow packets cannot be sent through the EMP Port. If you want to gather Top N App data from a switch you cannot use the EMP IP when discovering the switch.

By default, the Summary View is displayed (pie chart) with each application displayed as a percentage of the total number of flows for the configured time interval (e.g., last 24 hours). Information from all switches in the profile is displayed. However, there are view options that you can use to view information for specific switches/ports:

- **Filter by Device -** Click on the **Select Devices** button at the top of the screen to display only information for specific switches/ports.
- **Filter by Analytics Profile -** Click on the **Filter by Profile** drop-down and select a profile to display information for specific profiles. With this option, you can configure profiles for different groups of switches/ports and then view information only for those specific switches/ports.

The information can be displayed in different formats, and you can also configure the amount of information displayed.

Report Views

The Top N Applications Report can be displayed in a Summary View or a Detail View. The Summary View provides a summary of application traffic for the configured time interval (e.g., last 24 hours (default), last 7 days). The Detail View displays a subset of the data in a bar chart format. For example, if a report is configured to display data for the last 24 hours, the Summary View will display a summary of the data for the last 24 hours; and the Detail View will then display data for each hour within those 24 hours.

> **Note:** Report Views and configuration options are configured using the Options Bar located at the top of the report. This help page contains view and configuration information specific to Top N Applications Reports. For specific information on all of the options available, see the "Report Options" section of the Analytics Reports Help.

Summary View

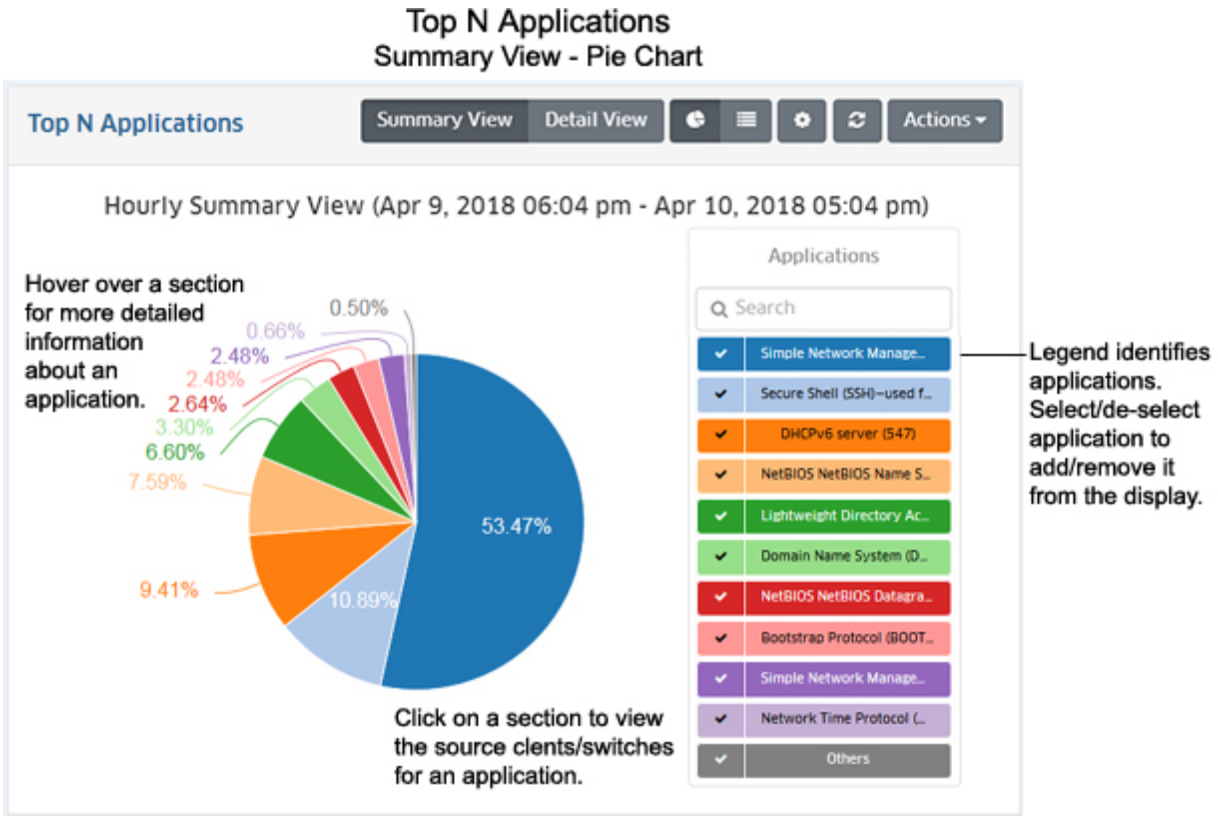
By default, the Summary View is displayed. This view provides a summary of application traffic for the configured time interval (e.g., last 24 hours). By default, the pie chart format is displayed; however, a list format is also available.

Pie Chart Format

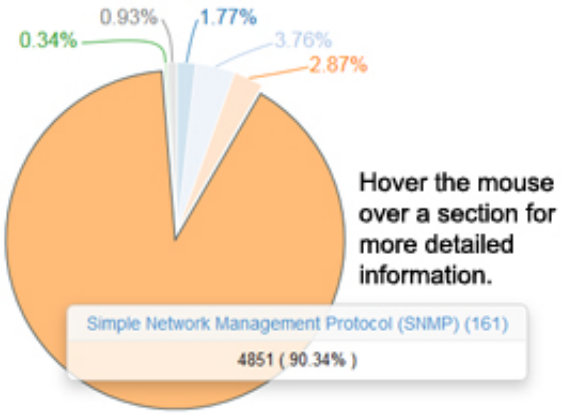
By default, the Summary View is displayed as a pie chart, with each application displayed as a percentage of the total traffic for all monitored switches for the configured time interval. By default, an Hourly Summary Report is displayed, showing a summary of the data over the last

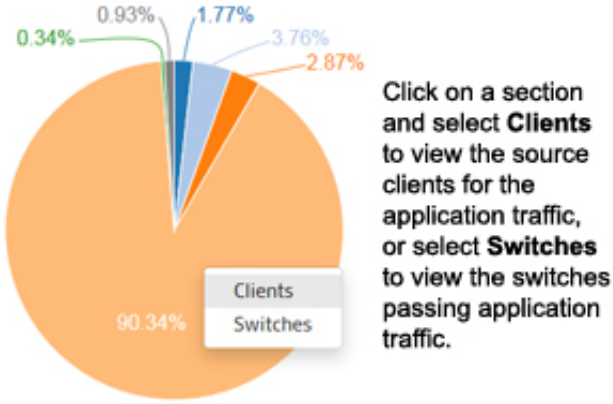
24 hours. (The Detail View will then display detailed information for each hour.) However, you can configure the report to display different time interval s (e.g., last 24 hours, last 7 days).

The legend on the right of the screen identifies each application in the chart by color and text. You can hover over a section of the chart to view detailed information for that section. Or you can click on an application in the legend to isolate the item in the display and show the same detailed information. You can also click select/deselect an application(s) in the legend to add/remove the application(s) from the display. The example below shows an Hourly Summary View.



Hover the mouse over a section of the chart (or click on an application in the legend) to view the number of flows for that application over the time interval displayed (e.g., last 24 hours). In the example below, hovering over the SNMP section of the pie chart shows the total number of SNMP flows as 4851, or 90.34% of the totals number of application flows. You can also view information on which clients are accessing an application, and which switches are passing traffic for that application.

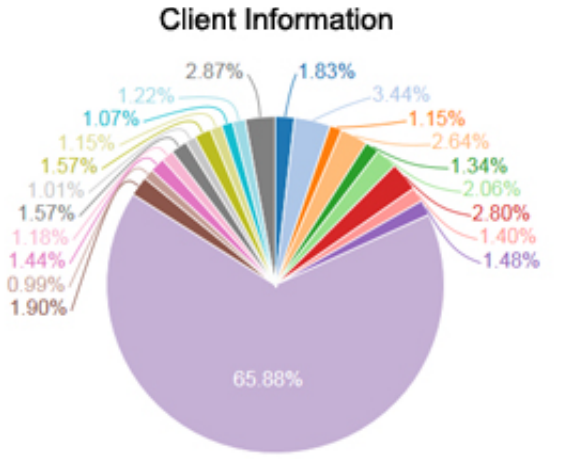




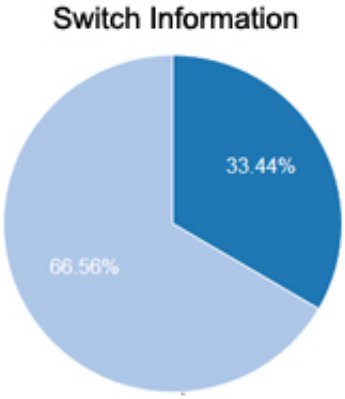
Client and Switch Information

When in the Pie Chart View of the Top N Applications Report you can view information about clients accessing an application (by source IP address) or the switches passing the application traffic. Click on a section and select **Clients** to view client information, or **Switches** to view switch information. The pie chart will be broken down by client or switch for that application (as shown below). The legend identifies the client or switch by color and text, or you can hover over a section to view the client/switch IP address (along with detailed flow information). You can also select/de-select switches/clients in the legend to add/remove them from the display.

The example below shows client and switch information for the SNMP application. In this example, many clients are using the SNMP application with the traffic passing between two switches. Click on the Back Arrow (**<**) above the legend to return the default view.

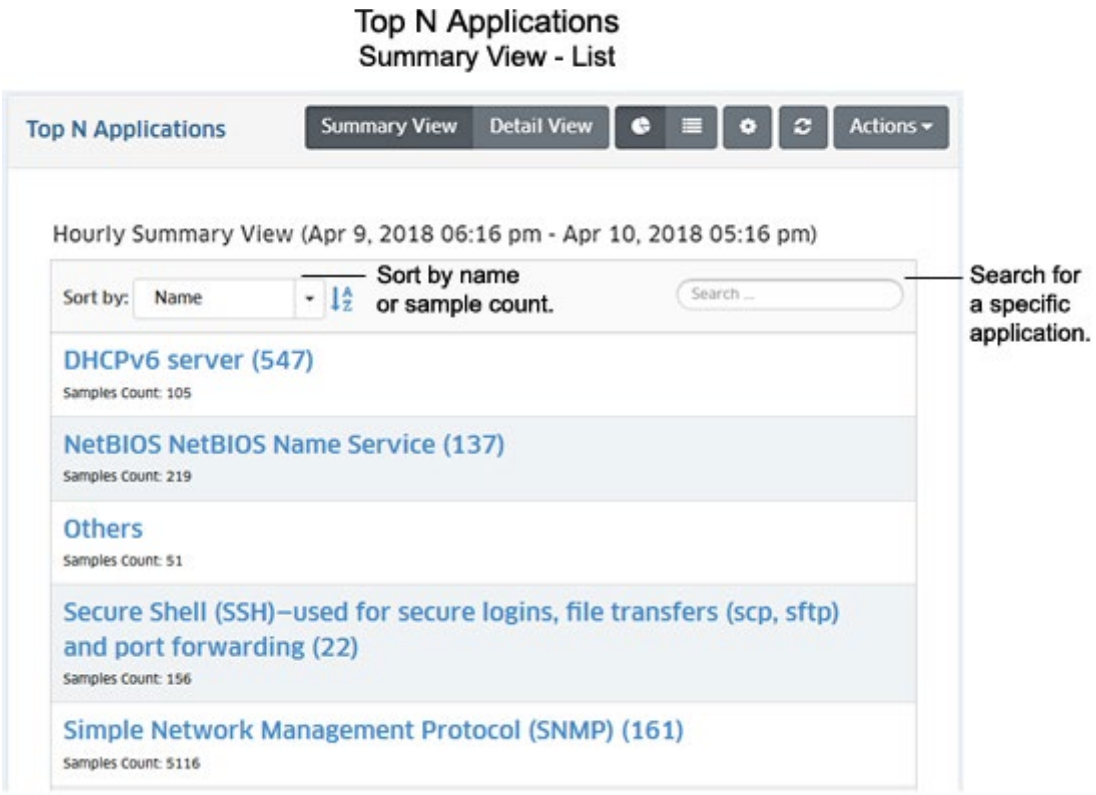


Information for each client/switch is displayed.
Hover over a section for more detailed information.



List Format

The list format displays a list of applications with packet count information for each one. By default, the list is displayed by application name in alphabetical order; however, you can select "Samples Count" in the **Sort by** drop-down menu to display the applications by sample count. You can also search for and display a specific application by entering the application name in the **Search** field.



Detail View

The Detail View displays a detailed subset of the information in bar chart format for the configured time period. For example, if a report is configured to show data for the last 24 hours, the Summary View will display a summary of the data for the last 24 hours; and the Detail View will then display data for each hour within those 24 hours.

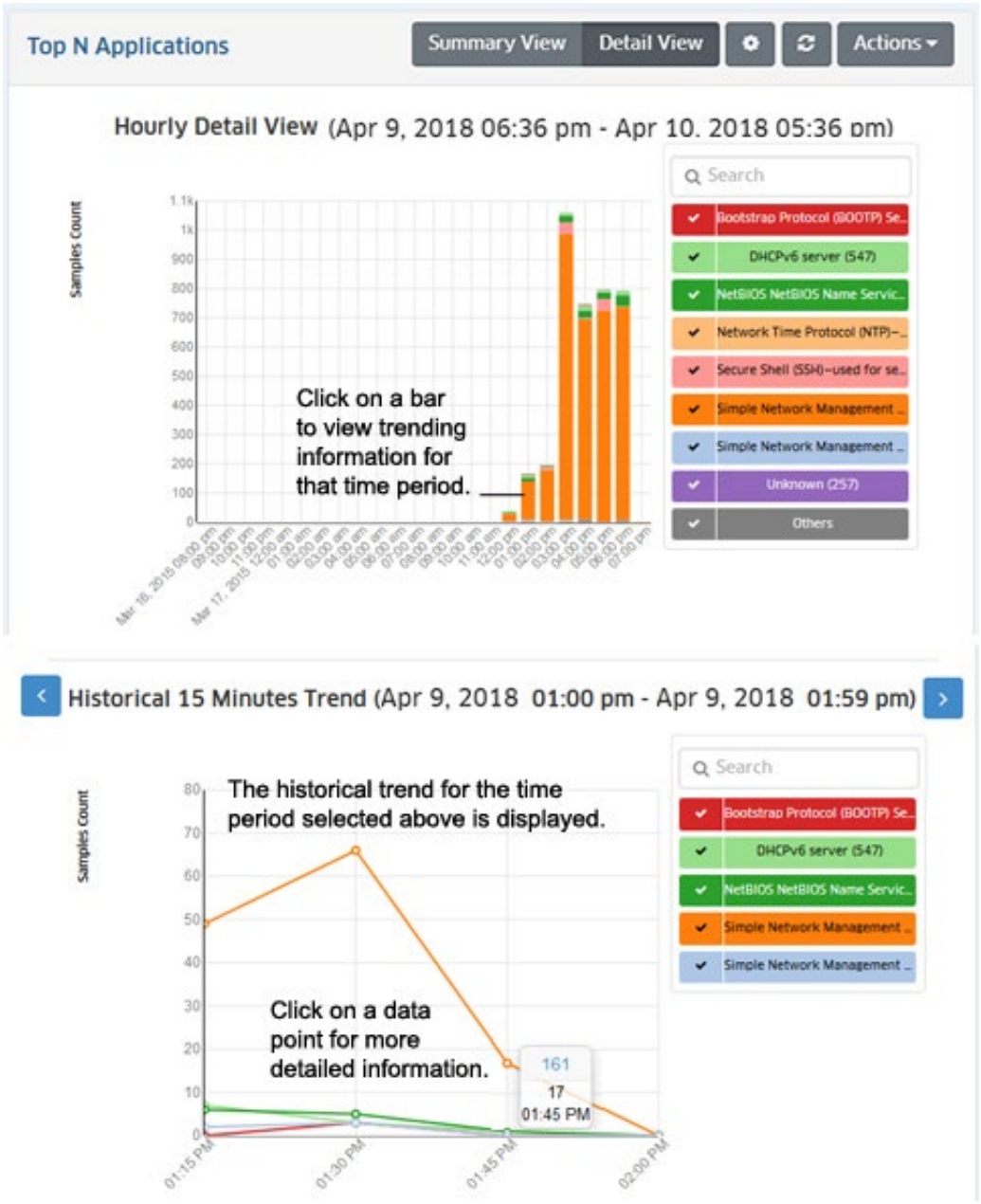
> **Note:** You can also click on a bar to view usage trends for that time interval. For example, if you clicked on a day in the chart below, you can view hourly usage trends for each application for that day.

As in the Summary Pie Chart view, you can hover the mouse over a section of the chart to view the number of flows for that application over the configured time interval (e.g., hour). In the example below, hovering over the SNMP section of a bar shows the total number of SNMP flows as 27 out of a total of 38 flows for that hour, or 71.05% of the total number of application flows for that hour.

Trending Information

When in Detail View, you can click on a bar in the chart to view usage trends for each application for the selected time interval by "drilling down" on a data set to see a subset of that data. For example, if you selected one of the bars in an Hourly Detail View, the trend for that hour would be displayed in 15-minute increments (as shown below). Click on a data point in the

trending view for more detailed information. You can scroll forward or back through the trending date using the arrows at the top of the chart.



Configuring the Information Displayed

You can configure the amount of information displayed (e.g., the number of applications you want to view) as well as the time interval that you want to view. To configure the report display, click on the Configuration icon to bring up the Configuration Screen, then complete the fields as described below to configure how information displayed in the report.

- **Default Devices -** By default, all top switches/ports are displayed. However, you can click on the **Select Devices** button to display only information from specific switches.
- **Number of Top Applications -** The number of applications you want to display (Range = 1 - 20, Default = 5).
- **Interval Type -** The time interval for the information:
- **Up Until Now -** Displays all information in the selected time interval (e.g., last 24 Hours).
- **Custom -** Set the start and end time for the information you want to display. You can display up to 3 months of data.
- **Time Interval -** The time interval you want to display in the report (the past 24 Hours, 7 Days, or 4 Weeks).
- **Auto Refresh Timer -** How often you want to refresh the data display, in minutes (Range = 15 - 60, Default = 15). The configuration option is only available when "Up Until Now" is selected for Interval Type.

When you are done, click the **Save** button. The report display will immediately change to the new view. This will remain the view until it is changed again.

Top N Applications - Advanced

The Analytics Top N Applications - Advanced Report Screen displays information about the top applications being accessed on the network based on Signature Profiles configured in the Application Visibility Application. Signature Profiles include the specific application groups/applications being monitored as well as the specific switches being monitored, so the information displayed is determined by the applications and switches included in the profile. Only information for those applications and switches is displayed. By default, the Summary View is displayed (pie chart) with each application displayed as a percentage of the total for the configured time interval (e.g., last 24 hours). The information can be displayed in different formats, and you can also configure the type and amount of information displayed.

> **Note:** Report Views and configuration options are configured using the Options Bar located at the top of the report. This help page contains view and configuration information specific to Top N Applications - Advanced Reports. For specific information on all of the options available, see the "Report Options" section of the Analytics Reports Help.

Report Views

Signature Profiles are created in the Application Visibility Application. When you click on the Top N Applications - Advanced link, you have the option to select the type of information you want to display (App Flow Count or App Bandwidth Usage). You can also select to view information for all switches in a type, or select specific switches.

- App Flow Count - Displays traffic flow information for applications/application groups discovered on the network, and the percentage of network resources being used by each application for the selected devices and configured time period. OS6860/OS6860E Switches and Stellar APs provide flow information (number of flows) in the App Flow Count view and packet/byte information in the App Bandwidth Usage view. All device types sample data.
- ***For all 6860s/APs -*** Displays flow information for all OS6860/6860E Switches and Stellar APs.

- ***Tabular Views -*** Displays flow information for all OS6860/6860E Switches and Stellar APs in list format.
- ***Manually Select Devices -*** Click on the link, then click on the **Select Device** button to bring up the Device Selection Window. Select the device(s) you want to include in the report, and click **OK**.
- App Bandwidth Usage - Displays packet/byte count information for applications/application groups discovered on the network over the configured period of time, and the percentage of network resources being used by each application for the selected devices and configured time period. You can also view application information by UNP Access Role Profile, Top Users per Application, or Top Applications per User by clicking on the applicable button. (Displaying data by "user" displays data by device IP.)
- ***For All Devices -*** Displays packet/byte count information for all devices.
- ***Tabular Views -*** Displays packet/byte count information for all devices in list format.
- ***Manually Select Devices -*** Click on the link, then click on the **Select Device** button to bring up the Device Selection Window. Select the device(s) you want to include in the report and click **OK**.

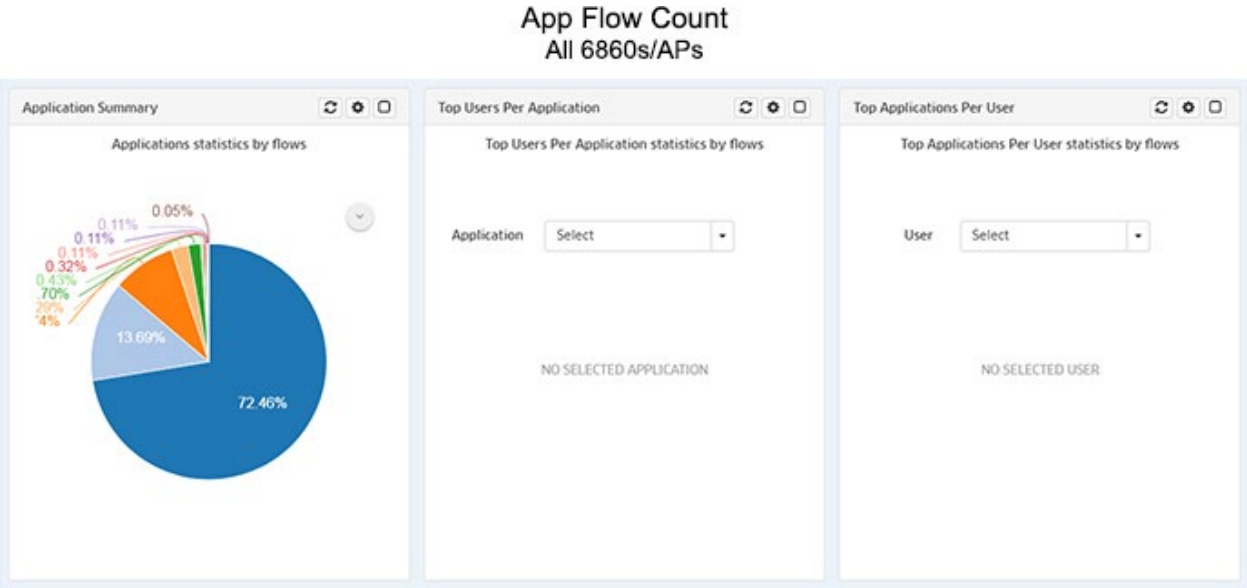
App Flow Count

The App Flow Count view displays traffic flow information for applications/application groups discovered on the network, and the percentage of network resources being used by each application for the selected switches and configured time period. Select a display option to display data as described below: All 6860s/APs, Tabular View, Manually Select Devices.

All 6860s/APs

Select "For All 6860s/APs" to display the information for all devices in the profile in Pie Chart Format. Three reports (shown below) are available. The first report chart automatically displays the Application Summary, with each application displayed as a percentage of the total traffic for the devices. The second report is used to display the Top Users Per Application. And the third report is used to display the Top Applications Per User. Note that if there is not enough room on the screen, the reports are displayed vertically. Scroll down to view each report.

> **Note:** "Top Users Per Application" and "Top Applications Per User Reports" are supported on AOS devices and Stellar APs (AWOS 3.0.6x and higher).



At the top of each display, you can click on the Refresh button to refresh the data, the Configuration button to configure the report, or the Maximize button to for a full screen display. Click on the Down Arrow to display a legend for the chart.

> **Note:** When you are in full screen display for any of the above pie charts, you can click on the List View or Tabular View buttons to change the display.

Application Summary

The Application Summary Report automatically displays application flow statistics for selected devices as a pie chart, with each application displayed as a percentage of the total traffic for the selected devices. Click on the Down Arrow to display a legend for the chart. By default, an Hourly Summary Report is displayed, showing a summary of the data over the last 24 hours. However, you can configure the report to display different time intervals (e.g., last 24 hours, last 7 days). The legend on the right of the screen identifies each application in the chart by color and text. You can hover over a section of the chart to view detailed information for that section. Or you can click on an application in the legend to isolate the item in the display and show the same detailed information. You can also click select/deselect an application(s) in the legend to add/remove the application(s) from the display.

Top Users Per Application

The Top Users per Application Report displays the top users (IP address) for the selected application. As shown above, no data is initially displayed. Select an application from the **Application** drop-down menu to display the top users for the selected application. Click on the Down Arrow to display a legend for the chart.

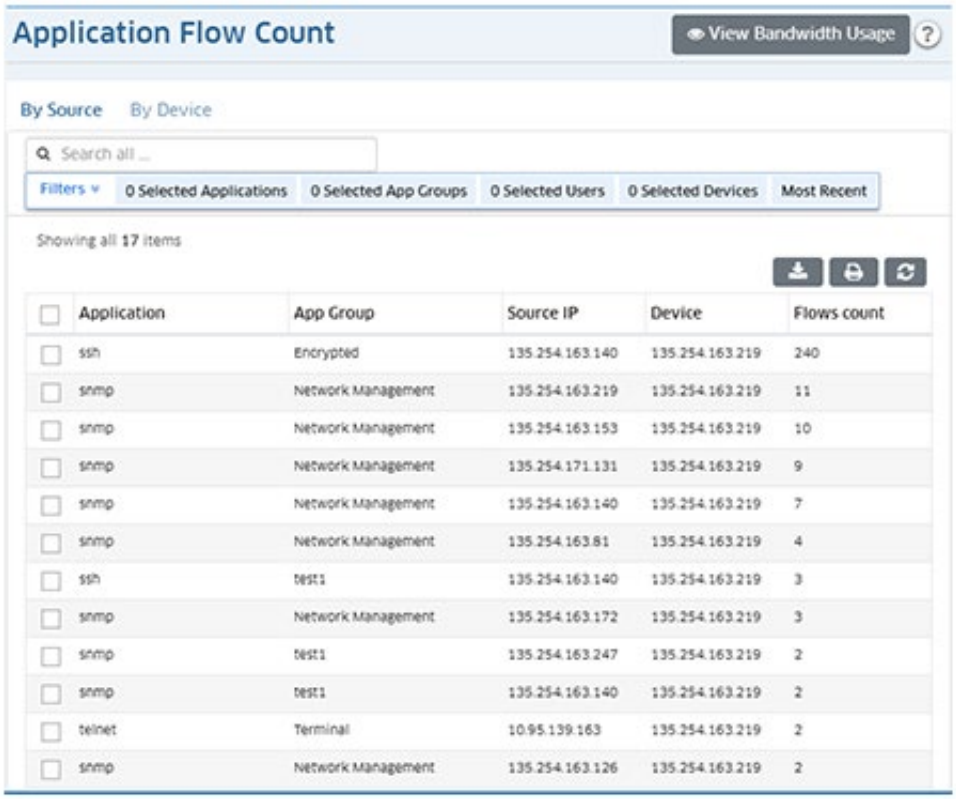
Top Applications Per User

The Top Applications per User Report displays the top applications for the selected user (IP address). As shown above, no data is initially displayed. Select a user (IP address) from the **User** drop-down menu to display the top application for the selected user. Click on the Down Arrow to display a legend for the chart.

Tabular Format

Select "Tabular Views" to view data in a table format. The "By Source" tab displays flow data by the source (client) generating the flows. The "By Device" tab displays flow data with the switch to which the source (client) generating the flows was connected. By default, all flow data in the database is displayed for all devices. You can enter search criteria in the Search Bar to search for specific information or you can click on the Filter Bar to filter the table to display specific information. You can also click on the **View Bandwidth Usage** button to view application bandwidth usage in tabular format.

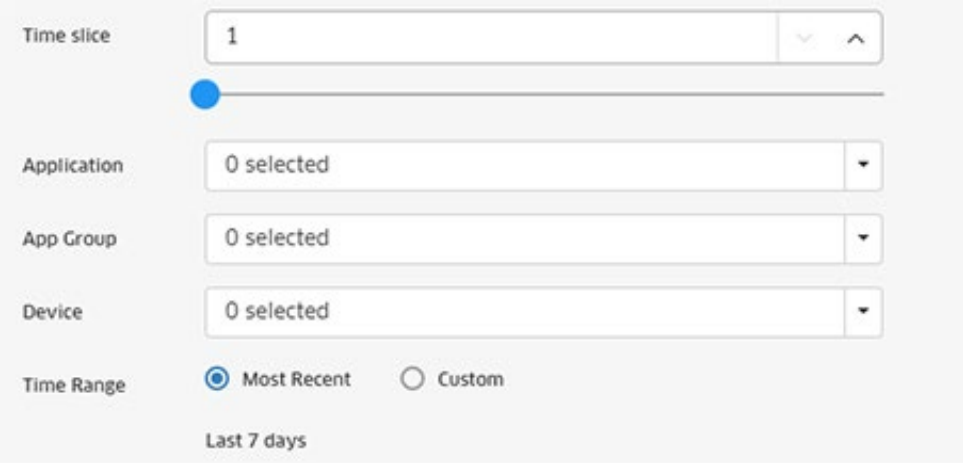
App Flow Count
Tabular View



Note: OmniVista begins collecting flow records as soon as a profile is assigned to a device. OmniVista can store up 20,000 records, at which point the data is overwritten with new records.

Filtering the Table View

Click on the Filter Bar at the top of the table to bring up the Filter Options Screen. Complete the fields to filter the table view and click on the **X** in the upper-right corner of the screen to close the screen and view the filtered table. The available filters vary depending on whether you are viewing the table in "By Device" or "By Source" view. The screen below shows the filters available for "Device" view.



- **Time Slice (Device View Only) -** The number of hours you want to display for each day. for the display. For example, if you enter "1", the table will display flow data for each hour of each day for each application. If you enter "2", the table will display flow data for every other hour of each day for each application.
- **Application -** Select the application(s) you want to display. Press **CTRL** and click to select multiple applications.
- **App Group -** Select the application(s) you want to display. Press **CTRL** and click to select multiple groups.
- **Source IP (Source View Only) -** Select the clients you want to display. Press **CTRL** and click to select multiple clients
- **Device -** Select the devices you want to display. Press **CTRL** and click to select multiple devices.
- **Time Range -** Select the applicable radio button:
- **Most Recent -** Displays data for the last 7 days.
- **Custom -** Configure the time range you want to display.

Manually Select Devices

Select "Manually Select Devices" and click on the Select Devices button to view data for specific devices. The data displays and viewing options are the same as those available in the All 6860s/APs option.

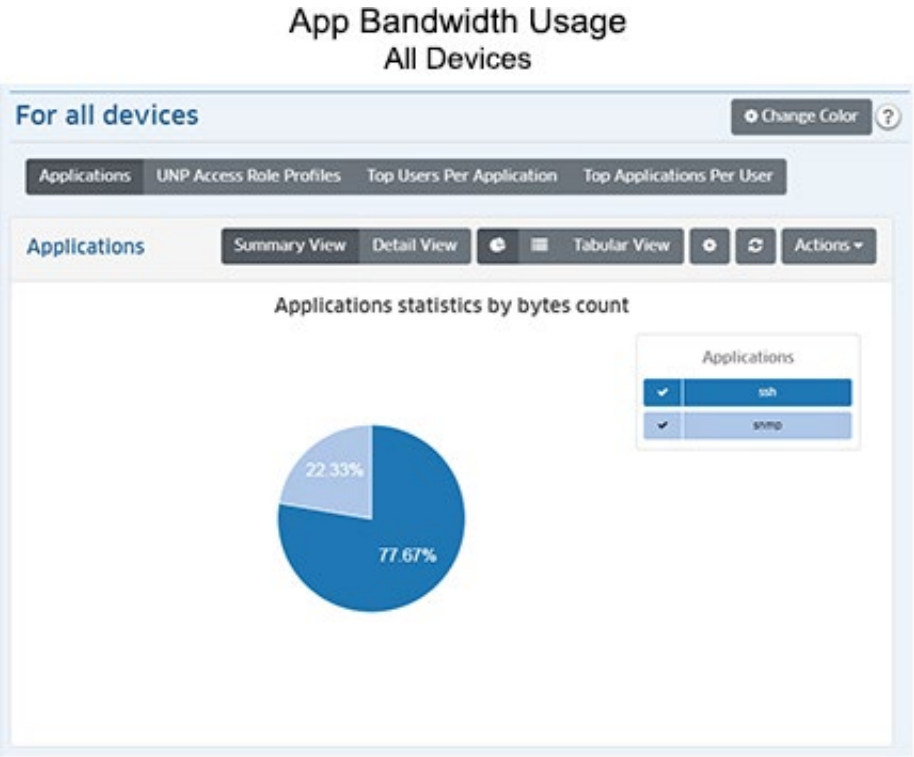
App Bandwidth Usage

The App Bandwidth Usage view displays packet/byte count information for applications/application groups discovered on the network, and the percentage of network resources being used by each application for the selected switches and configured time period. Select a display option to display data as described below: All Devices, Tabular View, Manually Select Devices.

All Devices

Select "For All Devices" to display the information for all devices in the profile in Pie Chart Format. By default, App Bandwidth Usage Reports are displayed in Summary View as a pie chart (packet count), with each application displayed as a percentage of the total traffic for the selected switches. By default, an Hourly Summary Report is displayed, showing a summary of

the data over the last 24 hours. However, you can configure the report to display different time intervals (e.g., last 24 hours, last 7 days). The legend on the right of the screen identifies each application in the chart by color and text. You can hover over a section of the chart to view detailed information for that section. Or you can click on an application in the legend to isolate the item in the display and show the same detailed information. You can also click select/deselect an application(s) in the legend to add/remove the application(s) from the display. You can also display information in a detailed line graph by clicking on the **Detail View** button at the top of the screen. view.



Four reports (shown below) are available. The first report chart (Applications) automatically displays data, with each application displayed as a percentage of the total traffic for all devices. The second report (UNP Access Role Profiles) displays application information by UNP Access Role Profile. The third report displays the Top Users Per Application. And the fourth report displays the Top Applications Per User.

Applications

The Application Summary Report automatically displays application flow statistics for selected devices as a pie chart, with each application displayed as a percentage of the total traffic for the selected devices. Click on the Down Arrow to display a legend for the chart. By default, an Hourly Summary Report is displayed, showing a summary of the data over the last 24 hours. However, you can configure the report to display different time intervals (e.g., last 24 hours, last 7 days). The legend on the right of the screen identifies each application in the chart by color and text. You can hover over a section of the chart to view detailed information for that section. Or you can click on an application in the legend to isolate the item in the display and show the same detailed information. You can also click select/deselect an application(s) in the legend to add/remove the application(s) from the display.

UNP Access Role Profiles

The UNP Access Role Profile Report displays application information by UNP Access Role Profile. Configured UNPs are displayed in the legend to the right.

Top Users Per Application

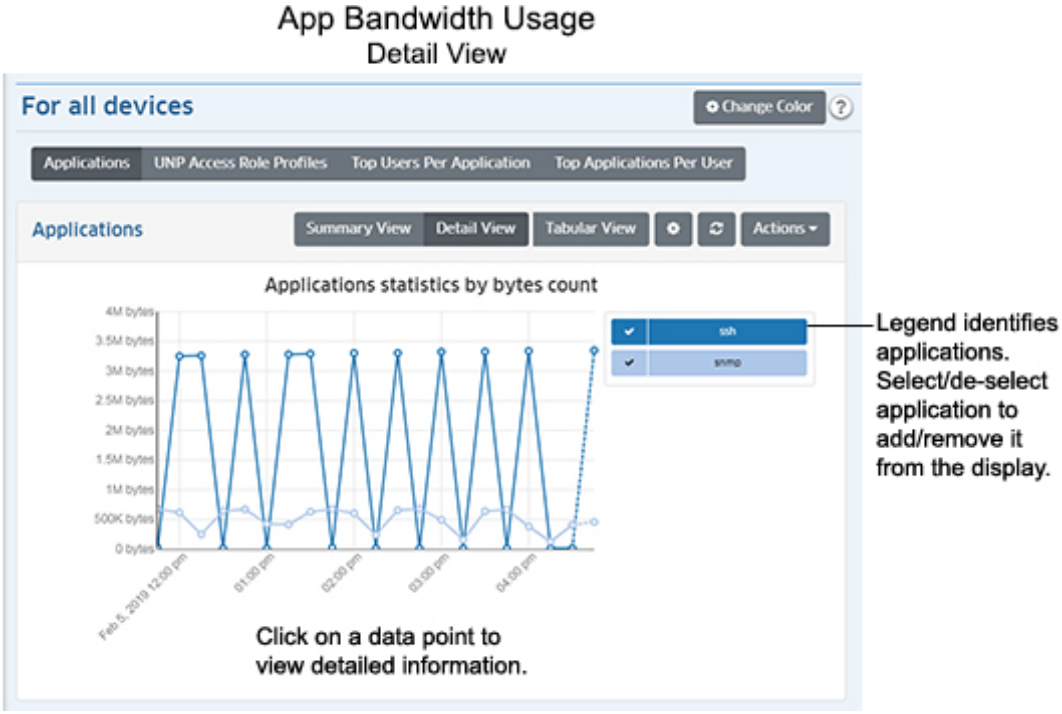
The Top Users per Application Report displays the top users (IP address) for the selected application. Select an application from the **Application** drop-down menu to display the top users for the selected application. Click on the Down Arrow to display a legend for the chart.

Top Applications Per User

The Top Applications per User Report displays the top applications for the selected user (IP address). Select a user (IP address) from the **User** drop-down menu to display the top application for the selected user. Click on the Down Arrow to display a legend for the chart.

Detail View

The Detail View displays detailed data in a line chart for the configured time period. Click on a data point for detailed information. As in the Pie Chart view, the legend on the right of the screen identifies each application in the chart by color and text. And you can also click select/deselect an application(s) in the legend to add/remove the application(s) from the display.

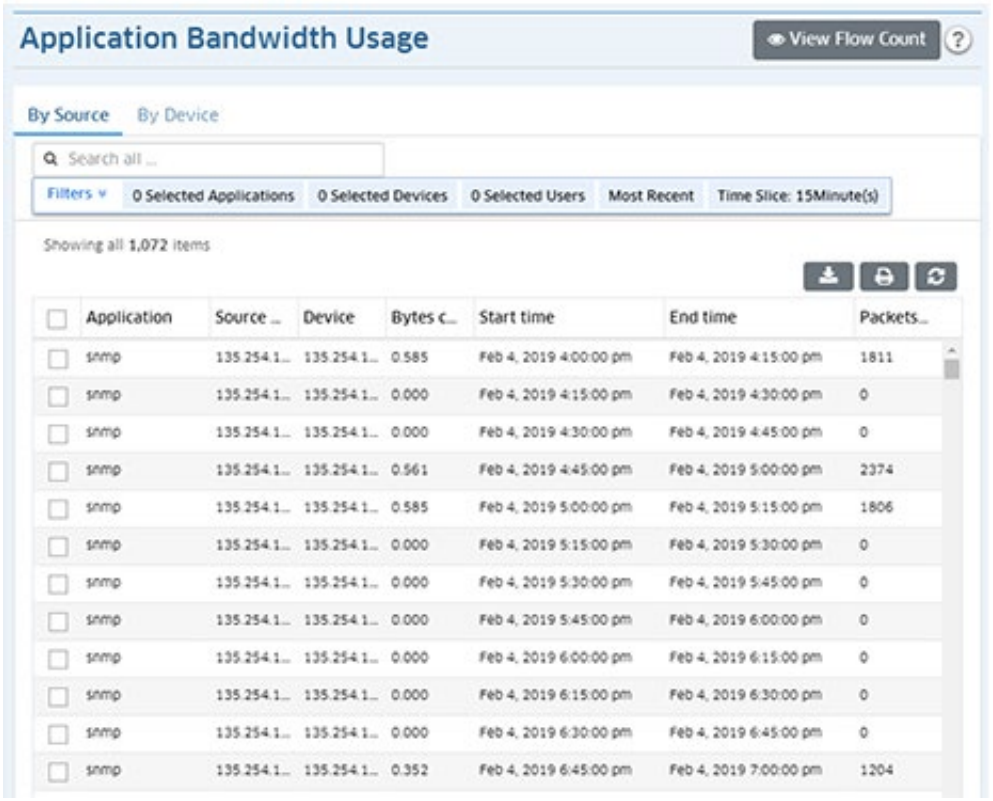


Tabular Format

Select "Tabular Views" to view data in a table format. The "By Source" tab displays flow data by the source (client) generating the flows. The "By Device" tab displays flow data with the switch to which the source (client) generating the flows was connected. By default, all flow data in the database is displayed for all devices. You can enter search criteria in the Search Bar to search for specific information; or you can click on the Filter Bar to filter the table to display specific

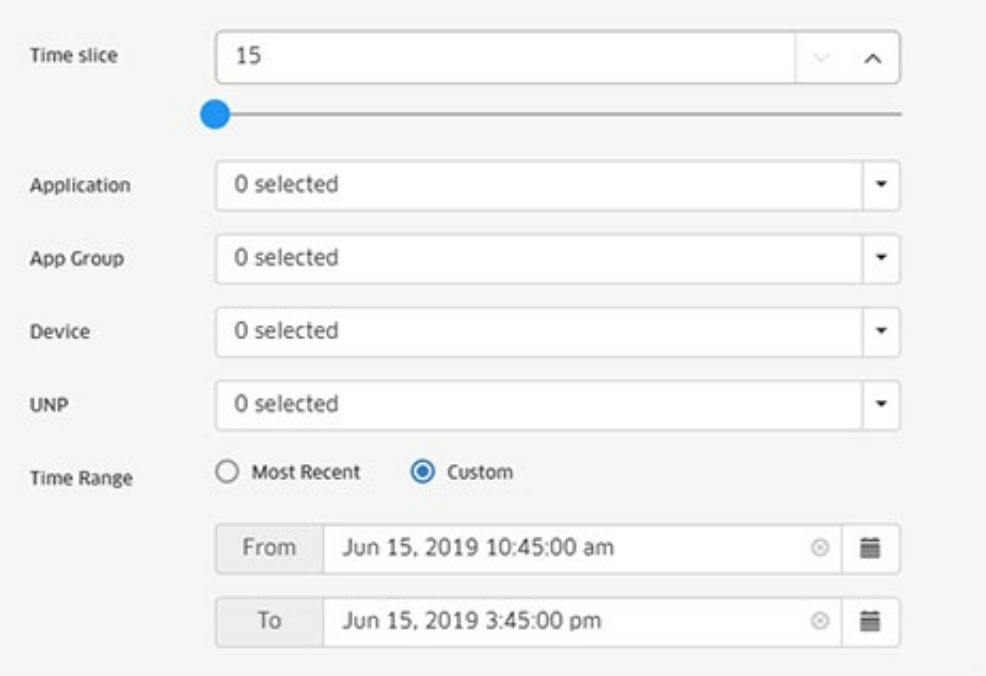
information. You can also click on the **View Flow Count** button to view application flow data in tabular format.

App Bandwidth Usage
Tabular View



Filtering the Table View

Click on the Filter Bar at the top of the table to bring up the Filter Options Screen. Complete the fields to filter the table view and click on the **X** in the upper-right corner of the screen to close the screen and view the filtered table. The available filters vary depending on whether you are viewing the table in "By Device" or "By Source" view. The screen below shows the filters available for "Device" view.



- **Time Slice (Device View Only) -** The number of hours you want to display for each day. for the display. For example, if you enter "1", the table will display flow data for each hour of each day for each application. If you enter "2", the table will display flow data for every other hour of each day for each application.
- **Application -** Select the application(s) you want to display. Press **CTRL** and click to select multiple applications.
- **App Group -** Select the application(s) you want to display. Press **CTRL** and click to select multiple groups.
- **Source IP (Source View Only) -** Select the clients you want to display. Press **CTRL** and click to select multiple clients
- **Device -** Select the devices you want to display. Press **CTRL** and click to select multiple devices.
- **UNP -** Select the UNP(s) you want to display. Press CTRL and click to select multiple UNPs.
- **Time Range -** Select the applicable radio button:
- **Most Recent -** Displays data for the last 7 days.
- **Custom -** Configure the time range you want to display.

Manually Select Devices

Select "Manually Select Devices" and click on the Select Devices button to view data for specific devices. The data displays and viewing options are the same as those available in the All Devices option.

Configuring the Information Displayed

You can configure the amount and type of information displayed (e.g., the number of applications displayed, byte or packet information) as well as the time interval that you want to view. To configure the report display, click on the Configuration icon in the upper-right corner of

the report to bring up the Configuration Screen, then complete the fields as described in the following sections. The available options vary depending on the view (e.g., App Flow Count, App Bandwidth Usage, Packet Count, Byte Count).

- **Choose Chart -** Select the information you want to display:
- **App Groups -** Displays flow information for all application groups included in the Signature Profile(s) of the selected switch(es) (Default).
- **Applications -** Displays flow information for all applications included in the Signature Profile(s) of the selected switch(es).
- **Data Interval -** The amount of time, in minutes, between each data point in the Detail View (Range = 15 - 120, Default = 15).
- **Counter Type -** Select whether you want to display data packet or byte count.
- **Data Unit -** Select the date unit for the byte count (Default = MB).
- **Top (apps) -** The number of application groups/applications you want to display (Range = 1 - 50, Default = 5).
- **Time Period Type -** The time interval for the information:
- **Hourly (Last 24 Hours) -** Displays all information for the last 24 Hours. Use the Time Period field to configure the number of hours of data to display (1 - 24).
- **Hourly (Any 24 Hours) -** Allows you to display information for a specific 24-hour period over the last week. Use the sliders on the Time Period field to configure the 24-hour period you want to display. You can also set the time period to fewer than 24-hours.
- **Daily (Any 7 Days) -** Allows you to display information for a specific 7-day period over the last 30 days. Use the sliders on the Time Period field to configure the 7-day period you want to display. You can also set the time period to fewer than 7 days.
- **Updating Interval -** How often you want to refresh the data display, in minutes (Range = 1 - 20, Default = 5).

Note: For App Flow Count - Top Users per Application or Top Applications per User Reports, if any of the reporting device OS's are lower than AOS 8.5R4/AWOS 3.0.6.x, the "Time Period Type" field will not be displayed.

When you are done, click the **Apply** button. The report display will immediately change to the new view. This will remain the view until it is changed again.

Note: You can change the display colors in a report by clicking on the **Change Color** button at the top of the report. The currently-displayed colors are shown. Click on a color to change it. When you are finished, click OK. Wherever that color is displayed in the report (and legend), it will be displayed in the new color. Click on the Restore Default Colors button to return all colors to the default settings.

Top N Clients

The Analytics Top N Clients Report Screen displays information for the top network clients including the number of traffic flows for each client. OmniVista uses the sFlow packet to determine the IP address of the client. By default, the Summary View is displayed (pie chart) with each client displayed as a percentage of the total for the configured time interval (e.g., last 24 hours). Information from all network switches in the profile is displayed. However, you can click on the **Select Devices** button to display only information from specific switches. The

information can also be displayed in different formats, and you can also configure the amount of information displayed.

To generate a Top N Clients Report, you must first create and assign an Analytics Profile using the Profile Screen that defines the switches/ports that you want to view and the type of information that you want to view on those switches/ports.

> **Note:** sFlow is enabled on a port when you create an Analytics Profile. However, sFlow can also be enabled on a port using the CLI. If sFlow is enabled on a port using the CLI and the OmniVista Server is configured as the receiver, Top N Clients data will be displayed in OmniVista.
>
> **Note:** sFlow packets cannot be sent through the EMP Port. If you want to gather Top N App data from a switch you cannot use the EMP IP when discovering the switch.

Report Views

The Top N Clients Report can be displayed in a Summary View or a Detail View. The Summary View provides a summary of application traffic for the configured time interval (e.g., last 24 hours (default), last 7 days). The Detail View displays a subset of the data in a bar chart format. For example, if a report is configured to display data for the last 24 hours, the Summary View will display a summary of the data for the last 24 hours; and the Detail View will then display data for each hour within those 24 hours.

By default, the Summary View is displayed (pie chart) with each application displayed as a percentage of the total number of flows for the configured time interval (e.g., last 24 hours). Information from all switches in the profile is displayed. However, there are view options that you can use to view information for specific switches:

- **Filter by Device -** Click on the **Select Devices** button at the top of the screen to display only information for specific switches.
- **Filter by Analytics Profile -** Click on the **Filter by Profile** drop-down and select a profile to display information for specific profiles. With this option, you can configure profiles for different groups of switches and then view information only for those specific switches.

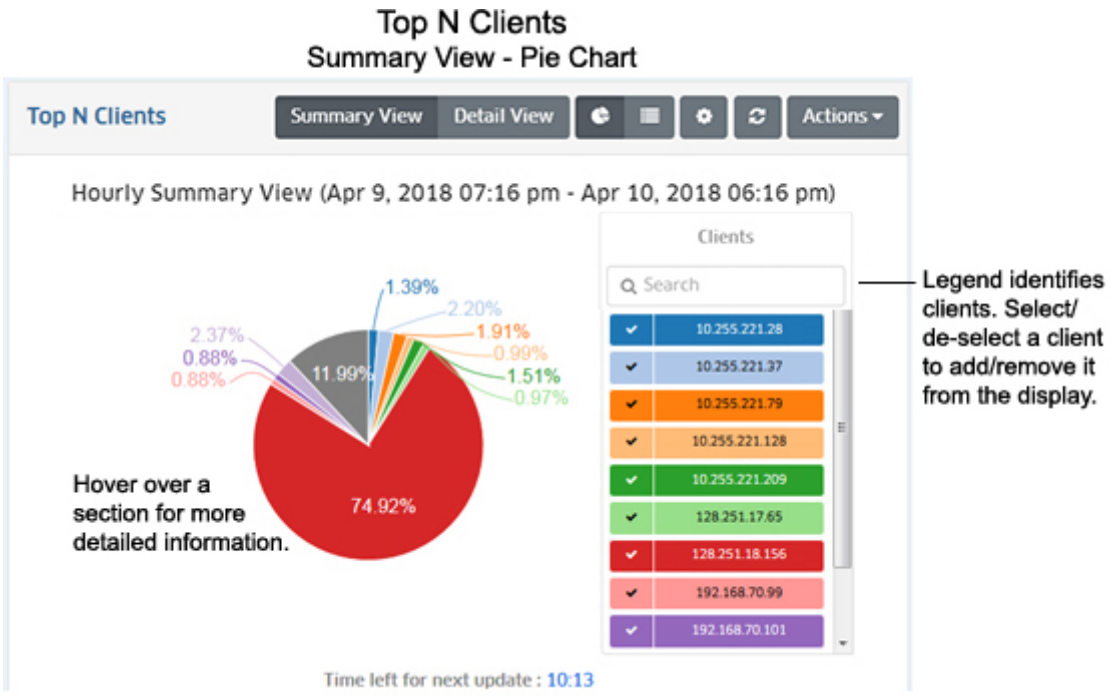
Summary View

By default, the Summary View is displayed. This view provides a summary of client traffic for the configured time interval (e.g., last 24 hours). By default, the pie chart format is displayed; however, a list format is also available.

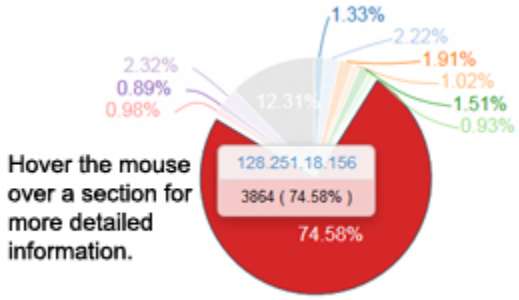
Pie Chart Format

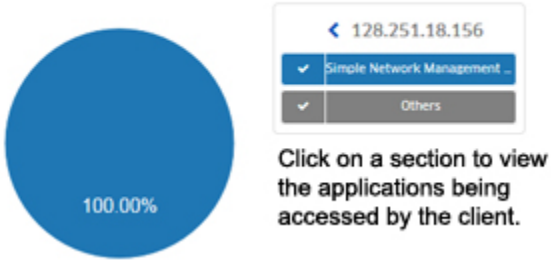
By default, the Summary View is displayed as a pie chart, with each client displayed as a percentage of the total traffic for all monitored switches for the configured time interval. By default, an Hourly Summary Report is displayed, showing a summary of the data over the last 24 hours. (The Detail View will then display detailed information for each hour.) However, you can configure the report to display different time interval s (e.g., last 24 hours, last 7 days).

The legend on the right of the screen identifies each client in the chart by color and text. You can hover over a section of the chart to view detailed information for that section. Or you can click on a client in the legend to isolate the item in the display and show the same detailed information. You can also click select/deselect a client(s) in the legend to add/remove a client(s) from the display. The example below shows an Hourly Summary View.



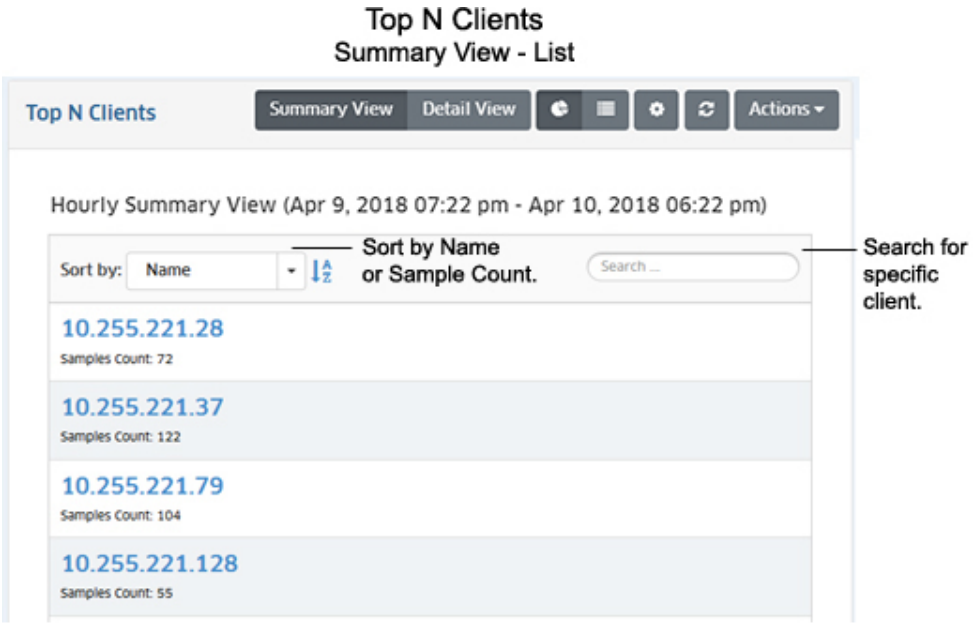
Hover the mouse over a section of the chart (or click on a client in the legend) to view the number of flows for that client over the time interval displayed (e.g., last 24 hours). In the example below, hovering over the section of the pie for client 128.251.18.156, displays the number of flows from that client as 3864, or 74.58% of the total number of traffic flows from that client. You can also view information on applications a client is accessing by clicking on a client section of the pie. The pie chart will change to display all of the applications that the client is accessing. You can also hover over a section of the pie to more detailed information about the application. The legend to the right will identify the applications by color and text. Click on the Back (<) arrow above the legend to return to the previous view.





List Format

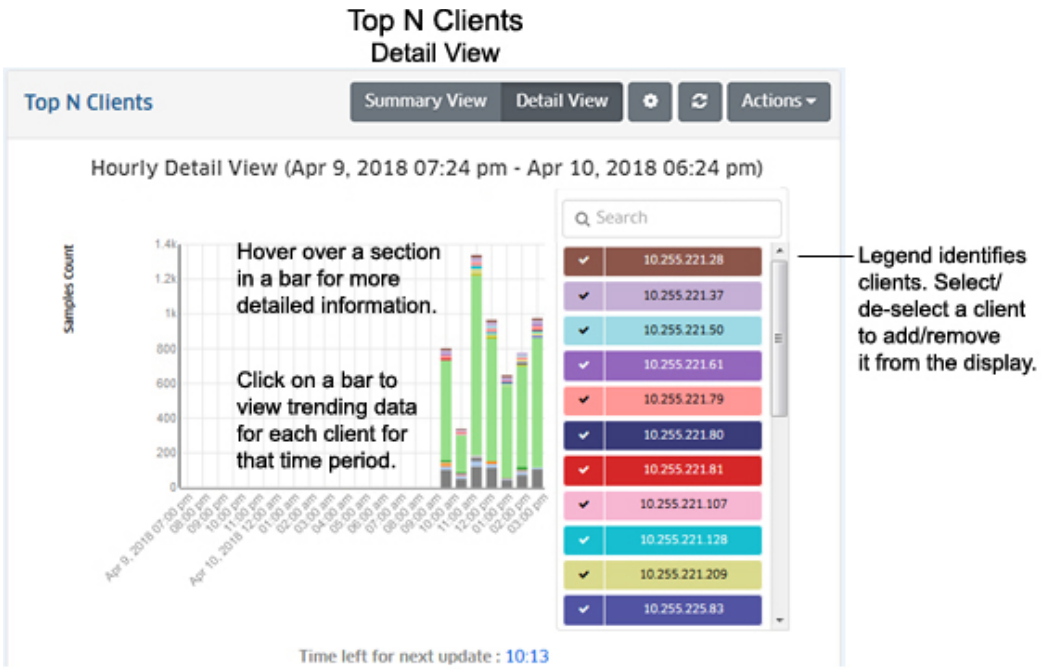
The list format displays a list of clients with packet count information for each one. By default, the list is displayed by client IP address in order; however, you can select "Samples Count" in the **Sort by** drop-down menu to display the clients by Sample Count. You can also search for and display a specific client by entering the client IP address in the in the **Search** field.



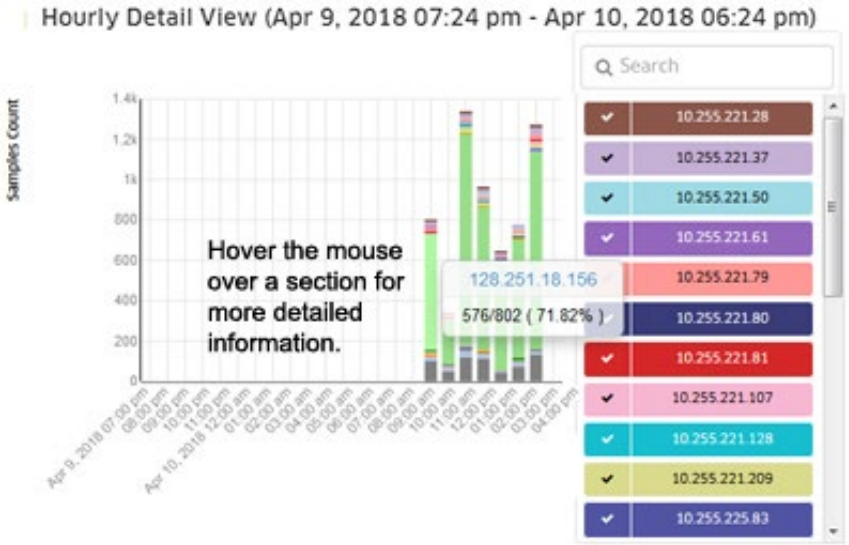
Detail View

The Detail View displays information in a bar chart view. While the Summary View displays the information for the configured time interval (e.g., last 24 hours), this view provides a detailed view of the specified time interval. For example, if a report is configured to display data for the last 24 hours, the Summary View will display a summary of the data for the last 24 hours; and the Detail View will then display data for each hour within those 24 hours.

> **Note:** You can also click on a bar to view usage trends for that time interval. For example, if you clicked on a day in the chart below, you can view hourly usage trends for each application for that day.

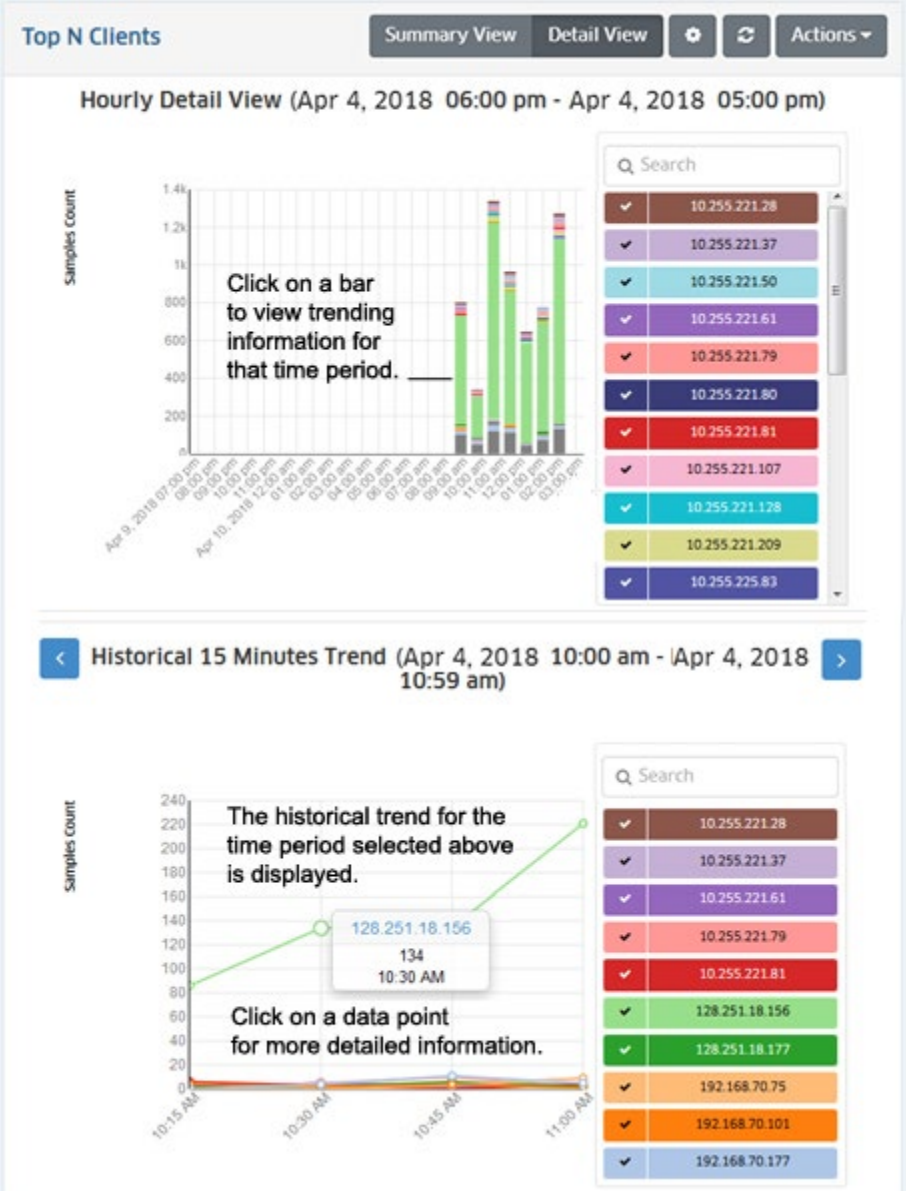


As in the Summary (Pie Chart) view, you can hover the mouse over a section of the chart to view the number of traffic flows for a client over the time interval displayed (e.g., hour). In the example below, hovering over the 128.251.18.156 client of a bar chart shows the total number of traffic flows as 576 out of a total of 802 flows for that hour, or 71.82% of the total number of traffic flows for that hour.



Trending Information

When in Detail View, you can click on a bar in the chart to view usage trends for each client for the selected time interval by "drilling down" on a data set to see a subset of that data. For example, if you selected one of the bars in an Hourly Detail View, the trend for that hour would be displayed in 15-minute increments (as shown below). Click on a data point in the trending view for more detailed information. You can scroll forward or back through the trending date using the arrows at the top of the chart.



Configuring the Information Displayed

You can configure the amount of information displayed (e.g., the number of users you want to view) as well as the time interval that you want to view. To configure the report display, click on the Configuration icon to bring up the Configuration Screen, then complete the fields as described below to configure how information displayed in the report.

- **Default Devices -** By default, all top switches/ports are displayed. However, you can click on the **Select Devices** button to display only information from specific switches.
- **Number of Top Clients -** The number of clients you want to display (Range = 1 - 20, Default = 5).
- **Interval Type -** The time interval for the information:
- **Up Until Now -** Displays all information in the selected time interval (e.g., last 24 hours).

- **Custom -** Set the start and end time for the information you want to display. You can display up to 3 months of data.
- **Time Interval -** The time interval you want to display in the report (the past 24 Hours, 7 Days, or 4 Weeks).
- **Auto Refresh Timer -** How often you want to refresh the data display, in minutes (Range = 15 - 60, Default = 15). The configuration option is only available when "Up Until Now" is selected for Interval Type.

When you are done, click the **Save** button. The report display will immediately change to the new view. This will remain the view until it is changed again.

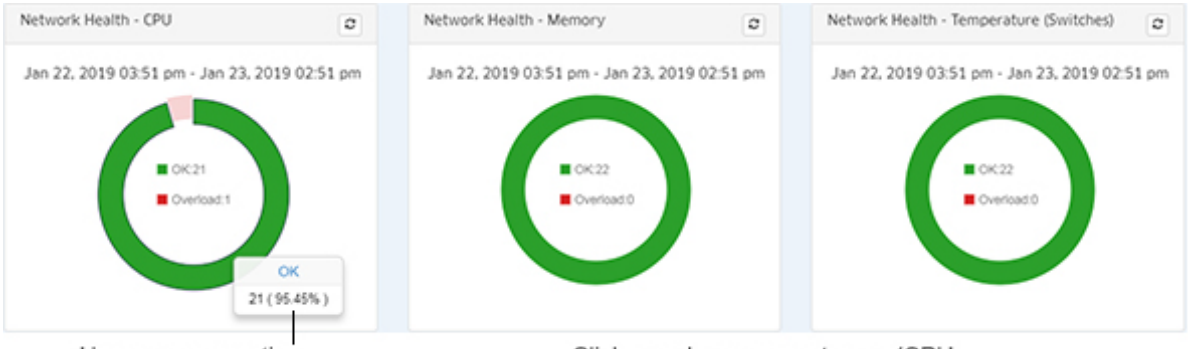
Network Health

The Analytics Network Health Report Screen displays the health of all discovered network devices in terms of CPU, Memory, Temperature. The widgets on the page provide a status overview for all network devices for each health category. Hover over an area in the widget for more information. Click on a widget to bring up an overview screen for a specific health category (CPU, Memory, Temperature), where you can view detailed information on each network device and set health thresholds for devices.

In addition, the information can be displayed in different views, and you can also configure the amount of information displayed. Report Views and configuration options are configured using the Options Bar located at the top of the report. This help page contains view and configuration information specific to Network Health Reports. For specific information on all of the options available, see the "Report Options" section of the Analytics Reports Help.

Report Views

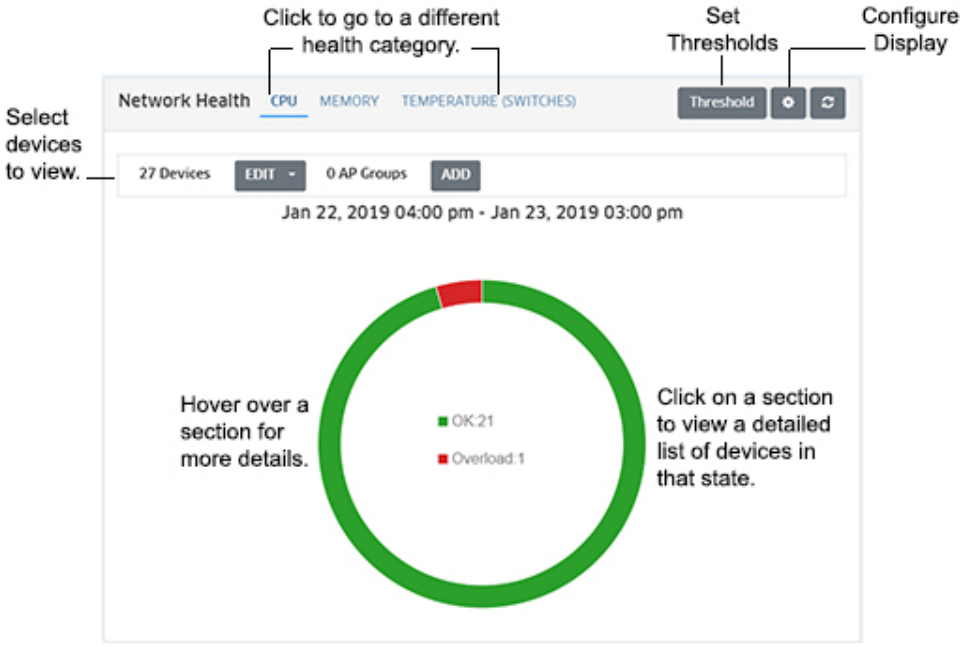
The main Network Health Screen provides a status overview for all network devices for each health category (CPU, Memory, Temperature). Each category displays an overview of the number of devices over threshold (Overload) and within threshold (OK). Hover over a section in the widget for more information. Click on a widget to go an overview page for a health category (e.g., CPU, Memory, Temperature). From there, you can view a detailed list of devices in each health state (Overload/OK), and set thresholds for each Health Category.



Health Category Overview

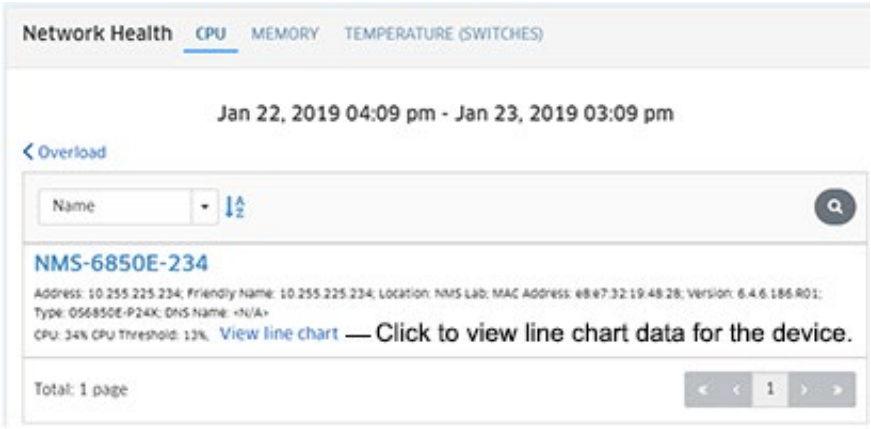
Click on a Health Category on the overview page to view more detailed information for that category (e.g., CPU). Click on the Devices or AP Groups **ADD** button and select the devices you want to view. Click on the **EDIT** button to select different devices. Hover over a section for

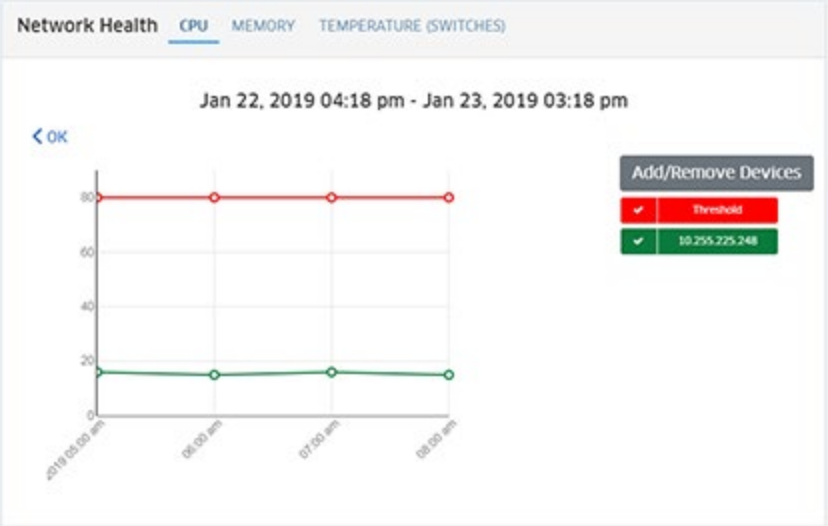
more information on that state (Overload, OK). Click on a section to view a detailed list of devices in that state. You can also click on the **Threshold** button to set device thresholds for the Health Category, or the **Settings** icon to configure the display.



Health Category Detailed View

Click on a section of the graphic (e.g., Overload, OK) to display detailed information for all selected devices in that state (e.g., Overload). The screen displays detailed device information. You can also click on the "View line chart link" to display a line chart view of the data for the configured time period.





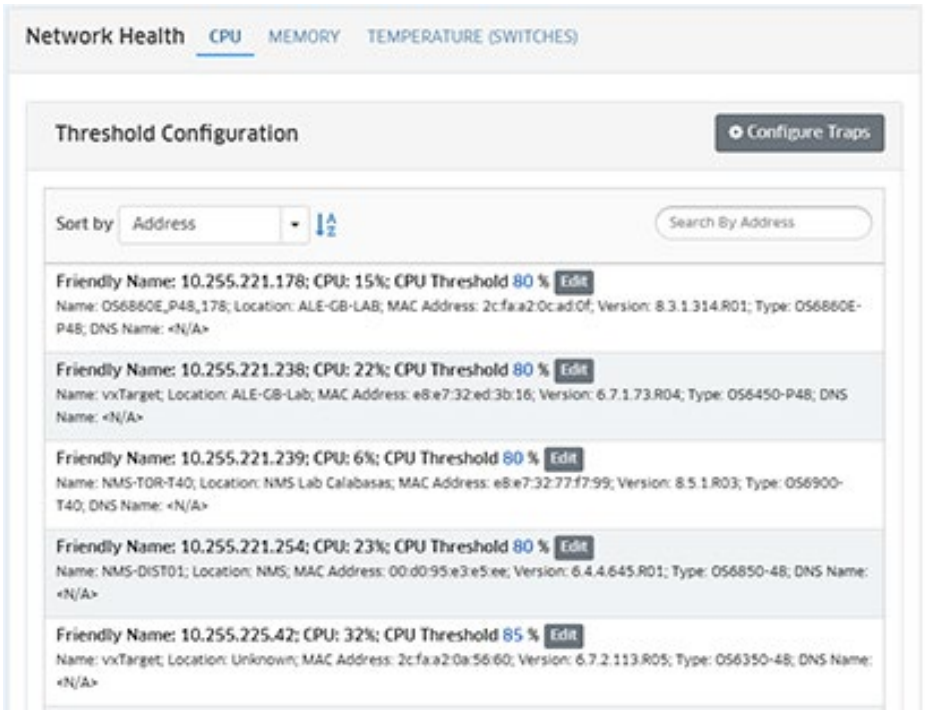
Click on the **Add/Remove Devices** button above the legend to add/remove devices to/from the display. You can view information for up to 20 devices.

Setting Health Thresholds

You can configure health thresholds for any discovered device. Health Thresholds are used to set limits for health traps. If a device has been configured to send health traps, a trap will be sent whenever a monitored item's current threshold exceeds the configured health threshold.

From the overview screen, click on the **Configure Health Threshold**s button to view and set thresholds for the Health Category for selected devices. If necessary, click on the Devices or AP Groups **ADD** or **EDIT** buttons to add/remove selected devices. Threshold information for all selected devices is displayed. To edit a threshold for a specific device, click on the **Edit** button next to the device and change the threshold. Repeat to change the threshold for any additional devices. When you are finished, click on the **Save** button.

> **Note:** You can only configure health thresholds for up to 20 devices at a time (including AOS Devices and Stellar APs.) If you select more than 20 devices, the **Configure Health Thresholds** button will not activate. You can configure health thresholds for more than 20 devices, but you must configure them in groups of 20 (select and configure 20 devices, select and configure an additional 20 devices, etc.).



You can also click on the **Configure Traps** button to quickly configure Health Threshold Traps for the selected devices. The first screen of the Notifications Trap Wizard (Devices Selection) will appear with the selected device(s) pre-selected. Click on the **Next** button to go to the Configure Traps Screen. Depending on the devices selected, the "Configure AOS 6.x Traps" and/or the "Configure AOS 7.x/8.x Traps" options will appear. The Health Threshold Traps are already pre-selected. (If you want to configure additional traps, expand the traps options to add additional traps.) Otherwise, click on the **Next** button to go to the Summary Screen to review the configuration. Click on the **Finish** button to configure the traps for the selected device(s).

> **Note:** Stellar APs do not support or display Temperature information. Also note that you can only configure the Temperature Threshold on AOS 6.x devices. The Temperature Threshold is hard-coded on AOS 8.x devices and cannot be configured. Also note that changes made to health thresholds will not appear until the next polling cycle (up to an hour).

Configuring the Information Displayed

You can configure the amount of information displayed. To configure the report display, click on the Configuration icon at the top of one of the Health Threshold Category overview screens to bring up the Configuration Screen, then complete the fields as described below to configure the information displayed in the report.

- **Interval Type -** The time interval for the information:
- **Up Until Now -** Displays all information in the selected time interval (e.g., last 24 hours).
- **Custom -** Set the start and end time for the information you want to display. You can display up to 3 months of data.
- **Time Interval -** The time interval you want to display in the report (the past 24 Hours, 7 Days, or 4 Weeks).

- **Auto Refresh Timer -** How often you want to refresh the data display, in minutes (Range = 15 - 60, Default = 15). The configuration option is only available when "Up Until Now" is selected for Interval Type.

When you are done, click the **Save** button. The report display will immediately change to the new view. This will remain the view until it is changed again.

Top N Ports Utilization

The Analytics Top N Ports Utilization Report Screen displays the top network ports based on utilization. By default, the Summary View is displayed (list view). In this view, switches/ports are displayed in a list view from highest to lowest utilization for the configured time period (e.g., day, week). By default, all top switches/ports are displayed. However, there are view options that you can use to view information for specific switches/ports:

- **Filter by Device -** Click on the **Select Devices** button at the top of the screen to display only information for specific switches/ports.
- **Filter by Analytics Profile -** Click on the **Filter by Profile** drop-down and select a profile to display information for specific profiles. With this option, you can configure profiles for different groups of switches/ports and then view information only for those specific switches/ports.

The information can be displayed in different formats, and you can also configure the amount of information displayed.

To generate a Top N Ports Utilization Report, you must first create and assign an Analytics Profile using the Profile Screen that defines the switches/ports that you want to view and the type of information that you want to view on those switches/ports. Note that port utilization must be greater than 1% (e.g., a one Gig port should have at least a 10 Mbps data rate) before data is displayed for the port.

Report Views

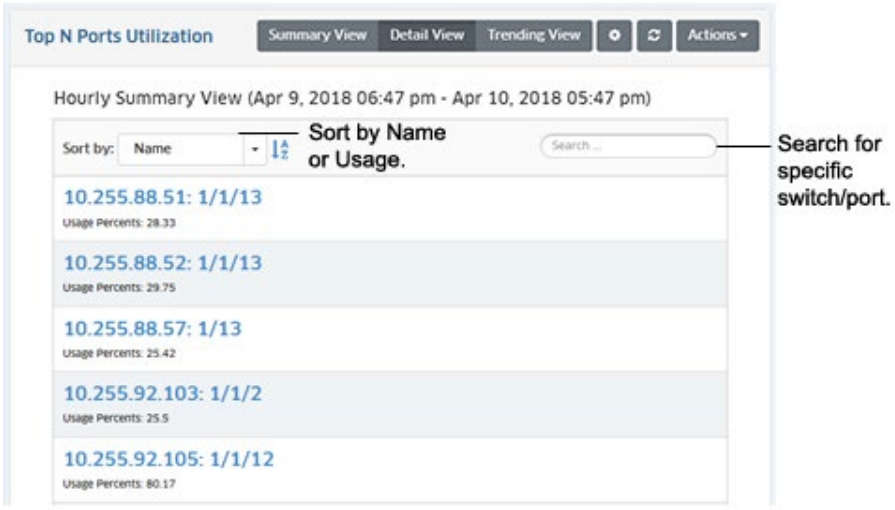
The Top N Ports Utilization can be displayed in a Summary View or a Detail View. The Summary View provides a summary of port traffic for the configured time interval (e.g., last 24 hours). The Detail View displays a subset of the data in a bar chart format. For example, if a report is configured to display data for the last 24 hours, the Summary View will display a summary of the data for the last 24 hours; and the Detail View will then display data for each hour within those 24 hours. The Trending View is used to view predicted future port utilization based on past utilization. Port utilization predictions can be used to predict future usage from past trending patterns and provide valuable insight for capacity management.

> **Note:** Report Views and configuration options are configured using the Options Bar located at the top of the report. This help page contains view and configuration information specific to Top N Ports Utilization Reports. For specific information on all of the options available, see the "Report Options" section of the Analytics Reports Help.

Summary View

By default, the Summary View is displayed. In this view, switches/ports are displayed in a list view from highest to lowest utilization for the configured time period (e.g., last 24 hours). Utilization for each port is displayed as a percentage of the total utilization for all monitored ports for the configured time period.

Top N Ports Utilization
Summary View

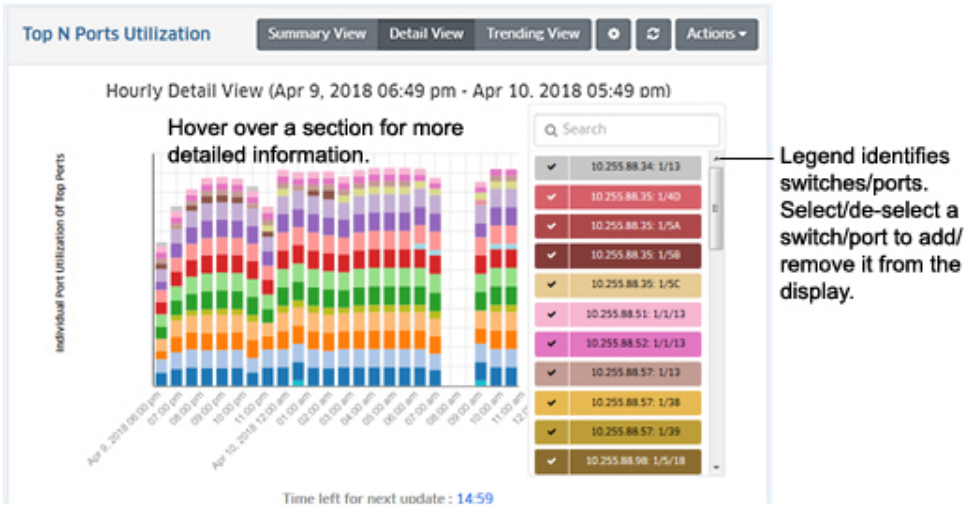


Detail View

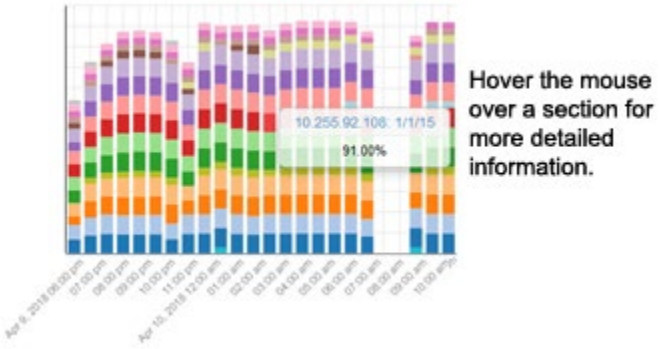
The Detail View displays information in a bar chart view. While the Summary View displays the information for the configured time period (e.g., last 24 hours), this view provides a detailed view of the specified time interval. For example, if the Summary View displays information for the last 24 hours, the Detail View will display information for each hour within those 24 hours.

Depending on the number of ports you configured for display (e.g., top 10 ports, top 15 ports), any monitored ports that qualify during the configure time interval (e.g., last 24 hours) are displayed. Ports are simply stacked numerically in each bar by IP address and port number (the order is not based on utilization). The legend on the right of the screen identifies each switch/port in the chart by color and text. You can hover over a section of the chart to view detailed information for that section. Or you can click on a switch/port in the legend to isolate the switch/port in the display and show the same detailed information. You can also click on the checkmark to select/deselect switches/ports in the legend to add/remove them from the display. The example below shows an hourly Detail View for a one-day period.

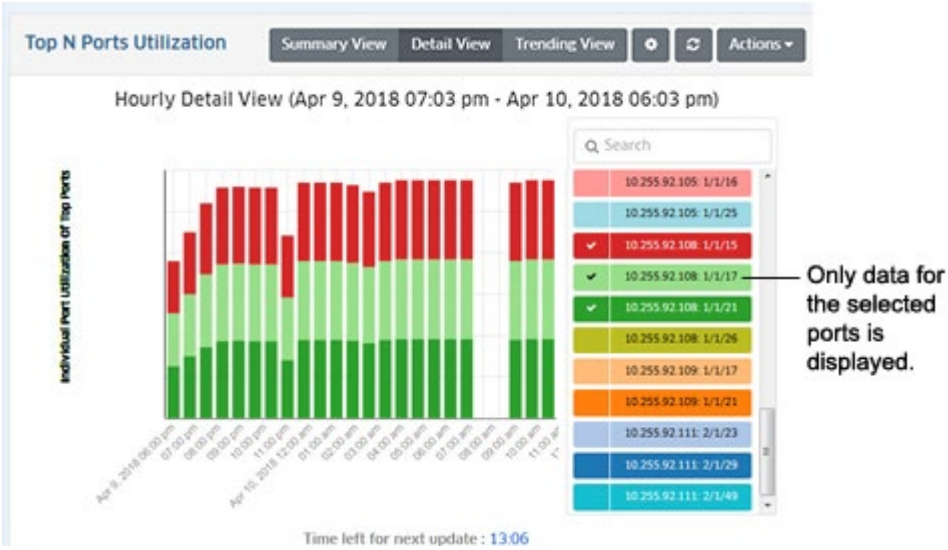
Top N Ports Utilization
Detail View



You can hover the mouse over a section of the chart to view the number of flows for that application over the time period displayed (e.g., hour). In the example below, which shows hourly usage, hovering over a section of a bar chart shows switch 10.255.92.106, port 1/1/5 with a utilization of 91% for that hour.



If you want to isolate a port or ports, you can select/deselect the port(s) in the legend.



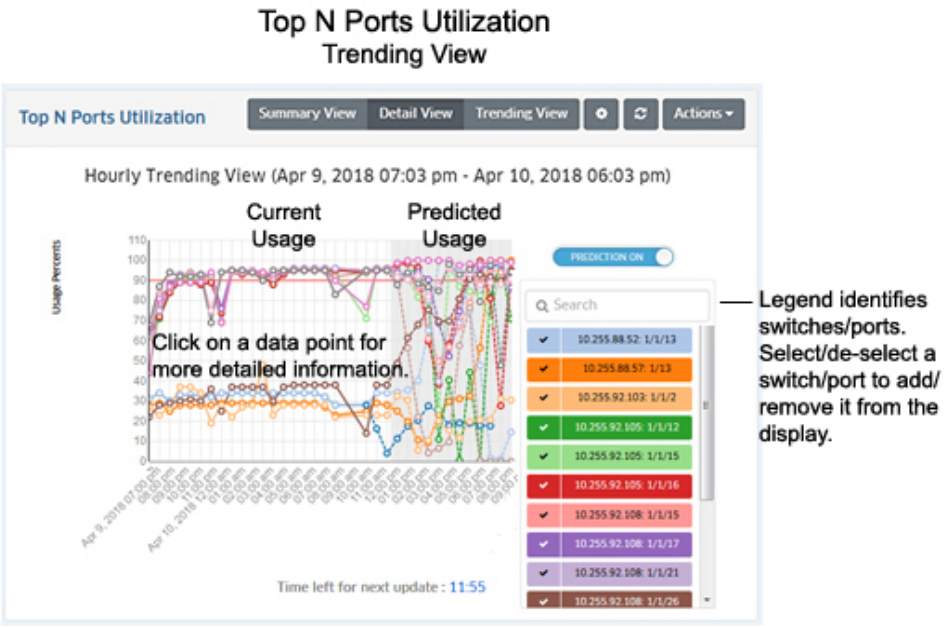
Trending View

The Trending View is used to view predicted future port utilization based on past utilization. Port utilization predictions can provide valuable insight for capacity management. To make port utilization predictions, OmniVista samples past port utilization for a period of time (Prediction: Training Timeout), and predicts future utilization within a configurable error rate (Prediction: Training Error) using a machine learning algorithm.

To view future trending information, click on the **Trending View** button and enable the **Prediction On** slider. When you initially enable the slider, the slider will display "Prediction in progress" while OmniVista samples and learns port utilization rates. The predicted utilization will then appear in the display to the right of the current utilization. The predicted usage area of the display will be slightly shaded to differentiate it from current usage. The amount of predicted data displayed depends on the interval time configured for the report (e.g., last 24 hours, last 7 days). For predicted data, OmniVista will display approximately one-half of the configured interval time, as shown in the table below.

Configured Time Interval	Amount of Predicted Data
Last 24 Hours	12 Hours
Last 7 Days	3 Days
Last 4 Weeks	2 Weeks

If OmniVista is unable to determine future utilization, a message will appear at the top of the display with a link to the reason(s) (e.g., *10.255.225.234: 1/10. Message: Prediction Analytics for port could not be performed due to insufficient data for Training*).



The information is displayed in the chart based on the trending configuration settings set in the Trending View Configuration Screen. The screen is also used to set training parameters that OmniVista will use to learn about past/current usage to predict future usage.

Configuring Trending Information

As with other reports, the Trending View Configuration Screen is used to configure how information displayed in the report. It is also used to set training parameters that OmniVista will use to learn about past/current usage to predict future usage. Detailed trending parameters are set in the Preferences Application on the Settings Screen. By default, OmniVista will use these parameters to predict future utilization. Any parameters that you configure on this screen will override the parameters configured in the Preferences Application. Click on the Configuration icon on the Trending Screen to bring up the Trending Configuration Screen, then complete the fields as described below.

- **Prediction -** Enables/Disables trending prediction.
- **Number of Top Ports** - The number of top ports (in terms of utilization) that you want to display (Range = 1 - 20, Default = 10).
- **Interval Type -** The time interval for the information:
- **Up Until Now -** Displays all information in the selected time interval (e.g., last 24 Hours).

- **Custom -** Set the start and end time for the information you want to display. You can display up to 3 months of data. When data reaches the 3-month maximum, it is overwritten with new data.
- **Time Interval -** The time interval you want to display in the report (the past 24 Hours, 7 Days, or 4 Weeks).
- **Auto Refresh Timer -** How often you want to refresh the data display, in minutes (Range = 15 - 60). The configuration option is only available when "Up Until Now" is selected for Interval Type.
- **Threshold** - The threshold level you want to set for the display. A red horizontal line will display on the chart at this threshold level to enable you to quickly see any data that has crossed the level. For example, a threshold of 90, will show a horizontal line at 90% utilization parallel to x-axis of graph.
- **Prediction: Training Timeout -** Specifies how long OmniVista will train, in seconds, by sampling past port utilization. In other words, this specifies how long OmniVista will sample port utilization data before beginning to predict future trends (Range = 15 - 600, Default = 60).
- **Prediction: Training Error -** The target error percentage to which OmniVista will be trained (Default = 0.1 - 1.0, Default = 0.5).

When you are done, click the **Save** button. The report display will immediately change to the new view. This will remain the view until it is changed again.

Configuring the Information Displayed

You can configure the amount of information displayed (e.g., the number of ports you want to view) as well as the time period that you want to view. To configure the report display, click on the Configuration icon to bring up the Configuration Screen, then complete the fields as described below to configure the information displayed in the report.

- **Default Devices -** By default, all top switches/ports are displayed. However, you can click on the **Select Devices** button to display only information from specific switches.
- **Number of Top Ports -** The number of top ports you want to display (Range = 1 - 20, Default = 5).
- **Interval Type -** The time period for the information:
- **Up Until Now -** Displays all information in the selected time interval (e.g., last 24 hours).
- **Custom -** Set the start and end time for the information you want to display. You can display up to 3 months of data.
- **Time Interval -** The time interval you want to display in the report (the past 24 Hours, 7 Days, or 4 Weeks).
- **Auto Refresh Timer -** How often you want to refresh the data display, in minutes (Range = 15 - 60, Default = 15). The configuration option is only available when "Up Until Now" is selected for Interval Type.

When you are done, click the **Save** button. The report display will immediately change to the new view. This will remain the view until it is changed again.

Top N PoE Ports Utilization

The Analytics Top N PoE Ports Utilization Report Screen displays the top network PoE ports based on the percentage of allocated power being utilized by each PoE Port. You can use the report to determine ports that may be drawing more power than anticipated. For example, if you configure a port's maximum power assuming that a low-power device would be connected to the port but an endpoint device that draws more power is connected, the port's PoE utilization will be 100%. Once you determine which PoE Ports are drawing more power than anticipated based on a Top N PoE Ports Utilization Report, you can use the Locator application to determine what devices are connected to those ports and make any necessary configuration adjustments.

By default, the Detail View is displayed (Bar Chart). In this view, switches/ports are displayed in a bar chart from highest to lowest utilization for the configured time period (e.g., day, week). By default, data from all switches are selected for display. However, there are view options that you can use to view information for specific switches/ports:

- **Filter by Device -** Click on the **Select Devices** button at the top of the screen to display only information for specific switches/ports.
- **Filter by Analytics Profile -** Click on the **Filter by Profile** drop-down and select a profile to display information for specific profiles. With this option, you can configure profiles for different groups of switches/ports and then view information only for those specific switches/ports.

The information can be displayed in different formats, and you can also configure the amount of information displayed.

To generate a Top N PoE Ports Utilization Report, you must first create a Top N PoE Ports Utilization Profile using the Profile Screen. The profile defines the switches that you want to view (all ports on the selected switches are included in the report). Note that utilization must be greater than 0% before data is displayed for the port.

> **Important Note:** A Top PoE Ports Utilization Report can be generated for any PoE-enabled switch. PoE must be enabled on switches/ports to generate PoE Port Utilization data. PoE is enabled and configured on switches/ports using the CLI. See the applicable *OmniSwitch CLI Reference Guide* for more information.

Report Views

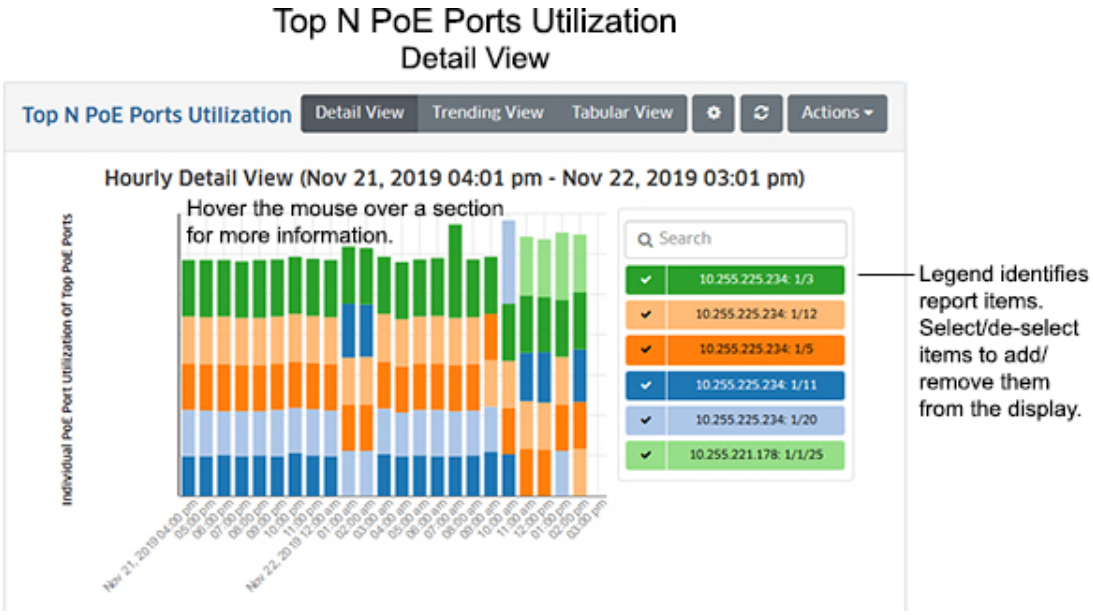
The Top N Ports Utilization can be displayed in a Detail View, Trending, or Tabular View. The Detail View provides PoE port utilization for the configured time interval (e.g., last 24 hours) in a bar chart format. The Trending View displays PoE port utilization for each port in a line chart for the configured time interval. The Tabular View brings up the Discovery Ports Screen, and provides detailed port information (including PoE information) for all ports included in the Profile.

> **Note:** Report Views and configuration options are configured using the Options Bar located at the top of the report. This help page contains view and configuration information specific to Top N PoE Ports Utilization Reports. For specific information on all of the options available, see the "Report Options" section of the Analytics Reports Help.

Detail View

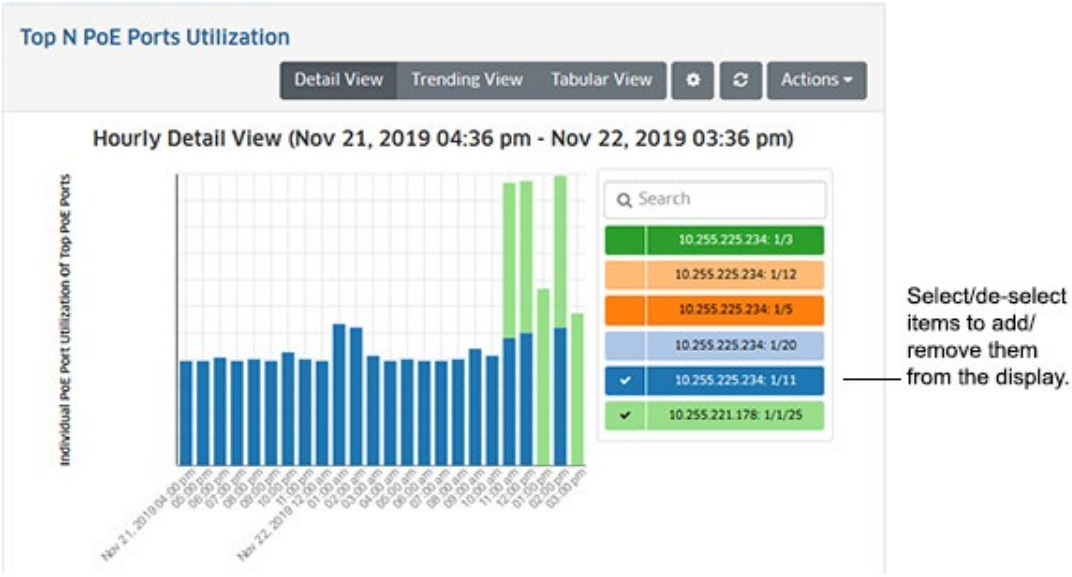
The Detail View provides a bar chart view of the specified time interval (e.g., last 24 hours). Depending on the number of switches/ports you configured for display (e.g., top 5 ports, top 10 ports), any monitored ports that qualify during the specified time interval are displayed. Ports are stacked from highest to lowest utilization. The legend on the right of the screen identifies each switch/port in the chart by color and text.

You can hover over a section of the chart to view detailed information for that section. You can also click the checkmark to select/deselect a switches/ports in the legend to add/remove them from the display. Or you can click on a switch/port in the legend to isolate the switch/port in the display and show the same detailed information. The example below shows an hourly Detail View for a one-day period.



Hover the mouse over a section of the chart to view the detailed utilization information about a port. In the example below, which shows hourly usage, hovering over a section of a bar chart shows port 1/3 on switch 10.255.225.234 with a PoE utilization of 28.33% (8,500 mW) of the total power available for that port for that hour.

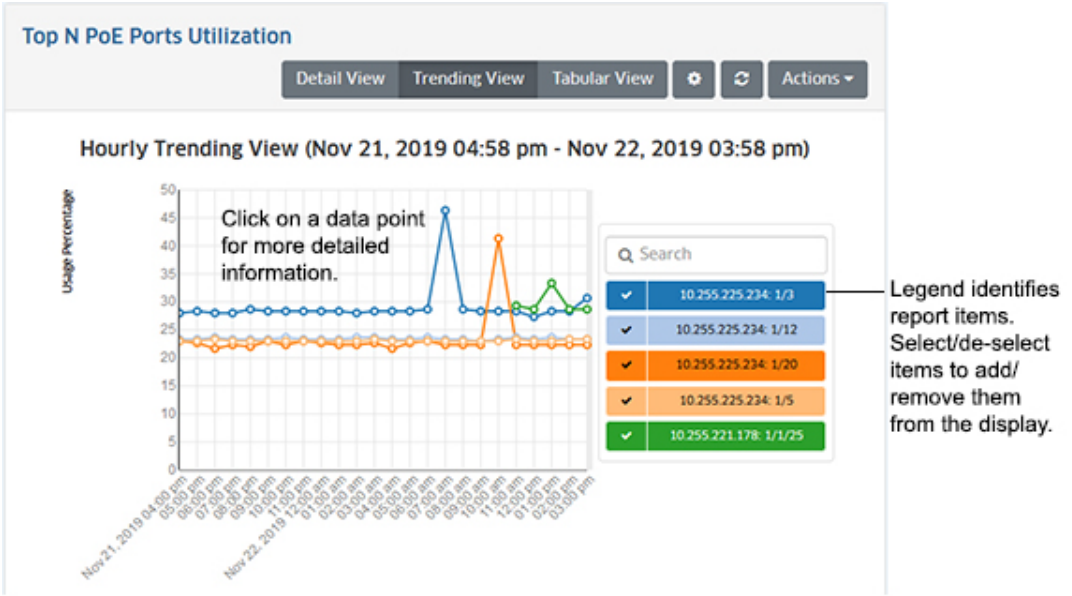
If you want to view specific ports, you can select/deselect the port(s) in the legend.



Trending View

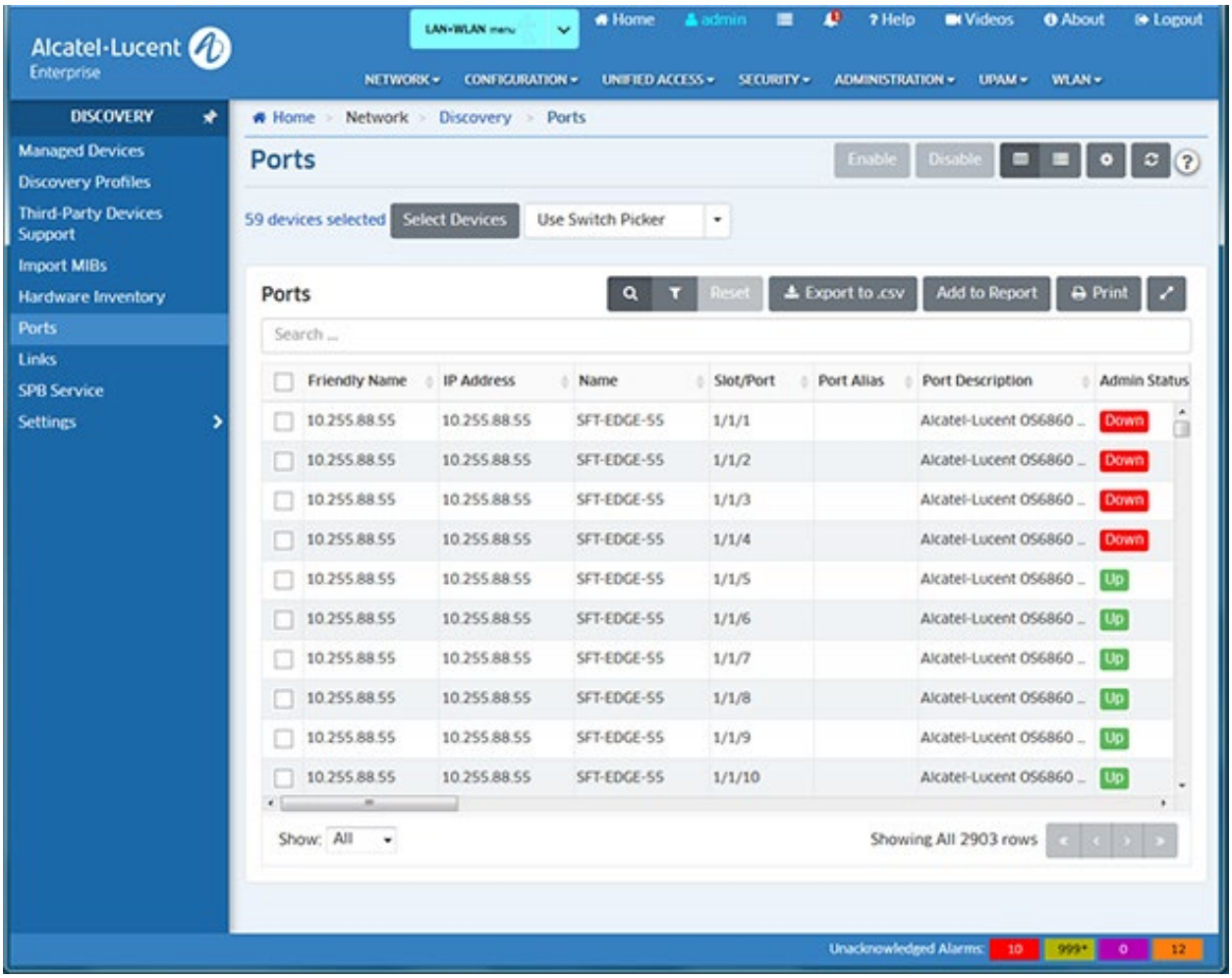
The Trending View provides a bar chart view of the specified time interval (e.g., last 24 hours). Depending on the number of switches/ports you configured for display (e.g., top 5 ports, top 10 ports), any monitored ports that qualify during the specified time interval are displayed.

You can hover over a section of the chart to view detailed information for that section. You can also click the checkmark to select/deselect a switches/ports in the legend to add/remove them from the display. Or you can click on a switch/port in the legend to isolate the switch/port in the display and show the same detailed information. The example below shows an hourly Detail View for a one-day period.



Tabular View

Clicking on the Tabular View button takes you to the Ports Screen (Network - Discovery - Ports), where you can view detailed port information for all network switches.



Configuring the Information Displayed

You can configure the amount of information displayed (e.g., the number of ports you want to view) as well as the time period that you want to view. To configure the report display, click on the Configuration icon to bring up the Configuration Screen, then complete the fields as described below to configure the information displayed in the report.

- **Default Devices -** By default, all top switches/ports are displayed. However, you can click on the **Select Devices** button to display only information from specific switches.
- **Number of Top Ports -** The number of top ports you want to display (Range = 1 - 20, Default = 5).
- **Interval Type -** The time period for the information:
- **Up Until Now -** Displays all information in the selected time interval (e.g., last 24 hours).
- **Custom -** Set the start and end time for the information you want to display. You can display up to 3 months of data.

- **Time Interval -** The time interval you want to display in the report (the past 24 Hours, 7 Days, or 4 Weeks).
- **Auto Refresh Timer -** How often you want to refresh the data display, in minutes (Range = 15 - 60, Default = 15). The configuration option is only available when "Up Until Now" is selected for Interval Type.

When you are done, click the **Save** button. The report display will immediately change to the new view. This will remain the view until it is changed again.

Top N PoE Switches Utilization

The Analytics Top N PoE Switches Utilization Report Screen displays PoE utilization by switch. By default, the Pie Chart View is displayed. In this view, switches are displayed in a pie chart with the total amount of PoE power each switch is using based on the total number of switches being displayed (e.g., Top 5, Top 10). By default, data from all switches are selected for display. However, there are view options that you can use to view information for specific switches:

- **Filter by Device -** Click on the **Select Devices** button at the top of the screen to display only information for specific switches.
- **Filter by Analytics Profile -** Click on the **Filter by Profile** drop-down and select a profile to display information for specific profiles. With this option, you can configure profiles for different groups of switches and then view information only for those specific switches.

The information can be displayed in different formats, and you can also configure the amount of information displayed.

To generate a Top N PoE Switches Utilization Report, you must first create a Top N PoE Ports Utilization Profile using the Profile Screen. The profile is used to define the switches that you want to view (all ports on the selected switches are included in the report). Note that utilization must be greater than 0% before data is displayed for the switch.

> **Important Note:** A Top PoE Switches Utilization Report can be generated for any PoE-enabled switch. PoE must be enabled on switches/ports to generate PoE Port Utilization data. PoE is enabled and configured on switches/ports using the CLI. See the applicable *OmniSwitch CLI Reference Guide* for more information.

Report Views

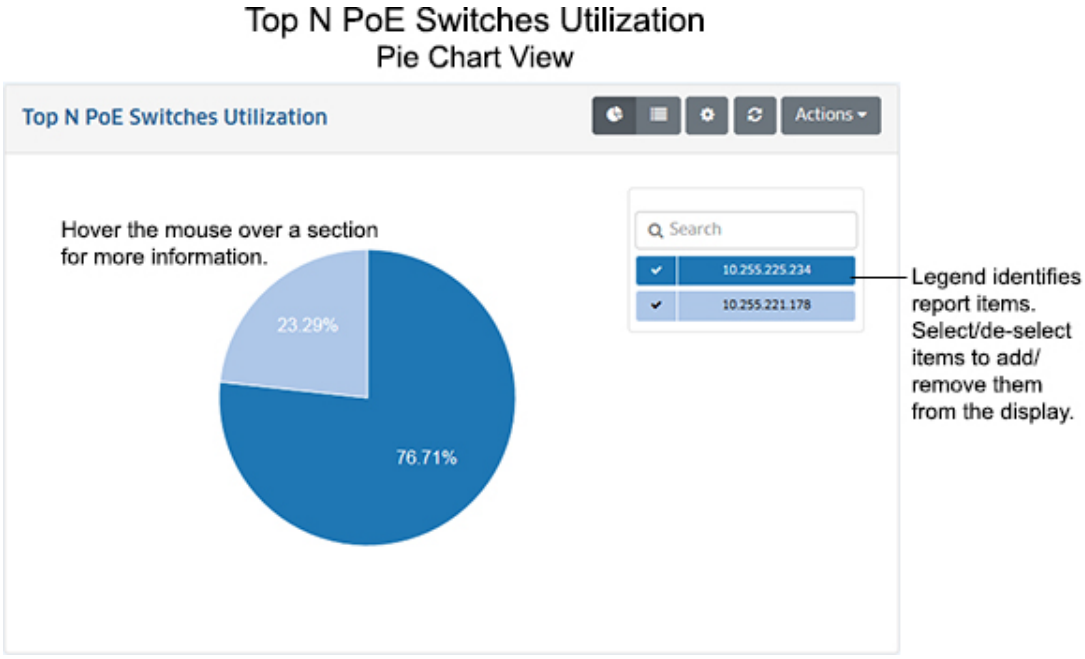
The Top N PoE Switches Utilization Report can be displayed in a Pie Chart View or a List View. In the Pie Chart View, switches are displayed in a pie chart with the total amount of PoE power each switch is using based on the total number of switches being displayed (e.g., Top 5, Top 10).

> **Note:** Report Views and configuration options are configured using the Options Bar located at the top of the report. This help page contains view and configuration information specific to Top N Ports Utilization Reports. For specific information on all of the options available, see the "Report Options" section of the Analytics Reports Help.

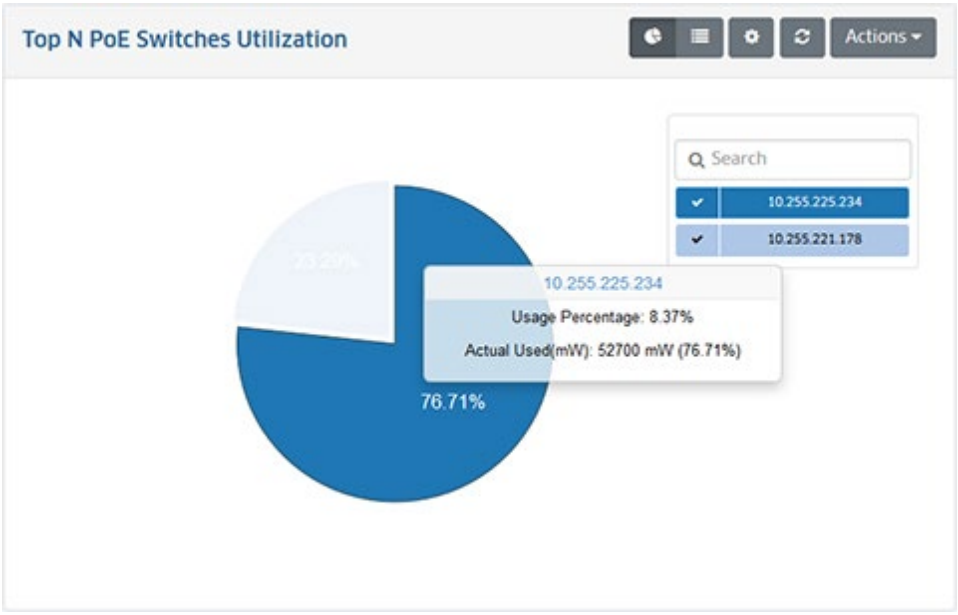
Pie Chart View

The Pie Chart View is displayed by default. In this view, switches are displayed in a pie chart with the total amount of PoE power each switch is using based on the total number of switches being displayed (e.g., Top 5, Top 10). In the example below, two switches are displayed,

10.255.225.234 and 10.255.221.178. Switch 10.255.225.234 is using 76.71% of the total power available for both switches. Switch 10.255.221.178 is using 23.29%.



Hover over a section of the chart to display more detailed information. The "Usage Percentage" is the percentage of total PoE power available on the switch that is currently being used. In the example below, Switch 10.255.225.234 is using 8.3% of the total PoE power available on the switch. The "Actual Used" shows the total mW (52,700) being used by the switch, and the percentage of the total power available for both switches.



List View

Click on the List icon at the top of the chart to display switches in List View. By default, switches are displayed in a list view from lowest to highest PoE utilization d as a percentage of the total PoE utilization for all displayed switches (e.g., Top 5, Top 10) for the configured time period (e.g., last 24 hours). You can click on the Sort arrow to sort the switches from highest to lowest.

Configuring the Information Displayed

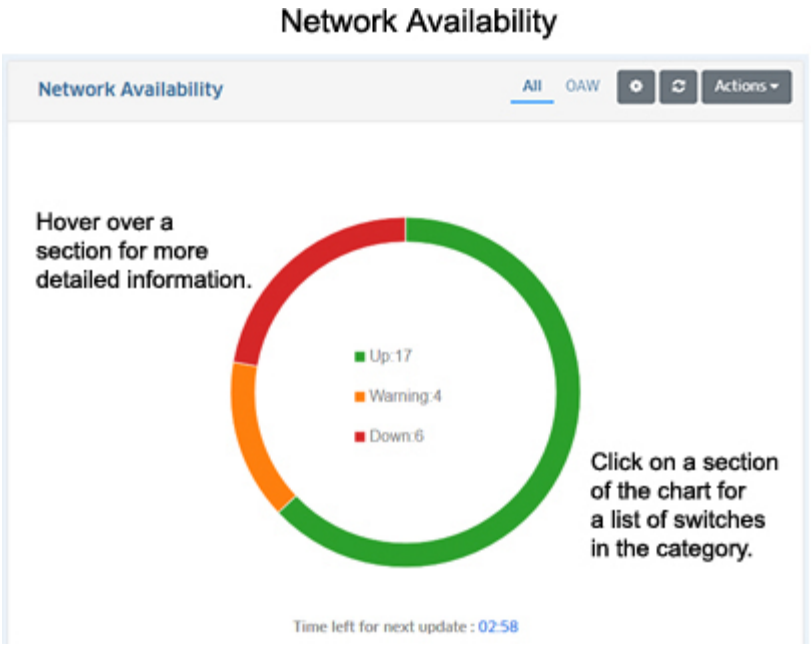
You can configure the amount of information displayed (e.g., the number of ports you want to view) as well as the time period that you want to view. To configure the report display, click on the Configuration icon to bring up the Configuration Screen, then complete the fields as described below to configure the information displayed in the report.

- **Default Devices -** By default, all top switches/ports are displayed. However, you can click on the **Select Devices** button to display only information from specific switches.
- **Number of Top Switches -** The number of top switches you want to display (Range = 1 - 20, Default = 5).
- **Auto Refresh Timer -** How often you want to refresh the data display, in minutes (Range = 15 - 60, Default = 15).

When you are done, click the **Save** button. The report display will immediately change to the new view. This will remain the view until it is changed again.

Network Availability

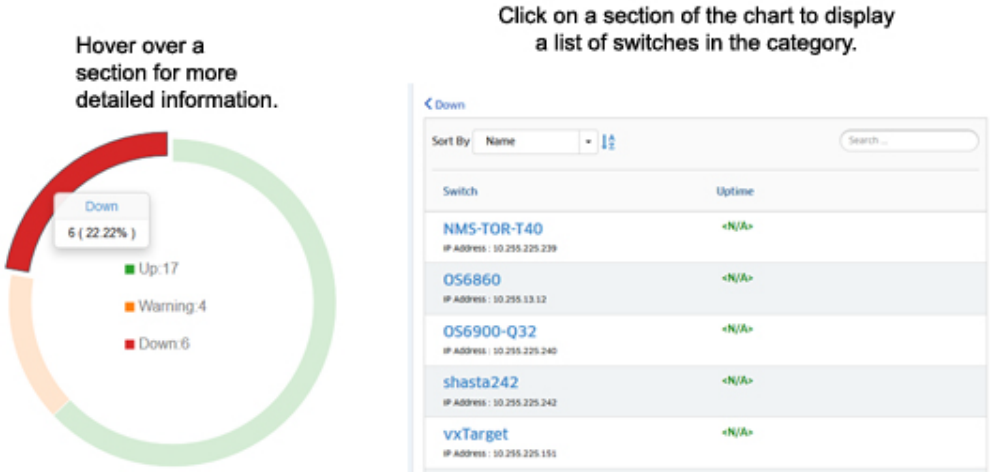
The Analytics Network Availability Screen displays the current operational state of all discovered network devices (Up/Warning/Down). Each category is displayed as a percentage of all monitored switches. The information can be displayed in different formats, and you can configure the information displayed.



Note: Report Views and configuration options are configured using the Options Bar located at the top of the report. This help page contains view and configuration information specific to Network Availability Reports. For specific information on all of the options available, see the "Report Options" section of the Analytics Reports Help.

Report Views

You can view the Network Availability Report in a couple of different ways. Hover the mouse over a category to display a brief summary of the category (the number of switches in the category, along with the percentage of all monitored switches in that category). You can also click on a category to display a list of switches in the category, with specific information about each switch. If you click on a category to display the list view, you can click on the "Back" link (<) to return to the default view.



Configuring the Information Displayed

You can configure the refresh rate for the data displayed by clicking on the Configuration icon in the Options Bar to bring up the Configuration Screen. Set the Auto Refresh Timer and click on the **Save** button. (Range = 1 - 10 minutes).

Alarms

The Analytics Alarms Screen displays network status/traps for all discovered switches. By default, a graphical pie chart view is displayed. The reported alarms in each severity level are displayed as a percentage of the total alarms reported. You can click on a severity level in the pie chart to view the switch(es) from which the alarms originated, and the number of those alarms received, along with the percentage of the total number of alarms received from that switch. In addition, the information can be displayed in different formats, and you can also configure the amount of information displayed.

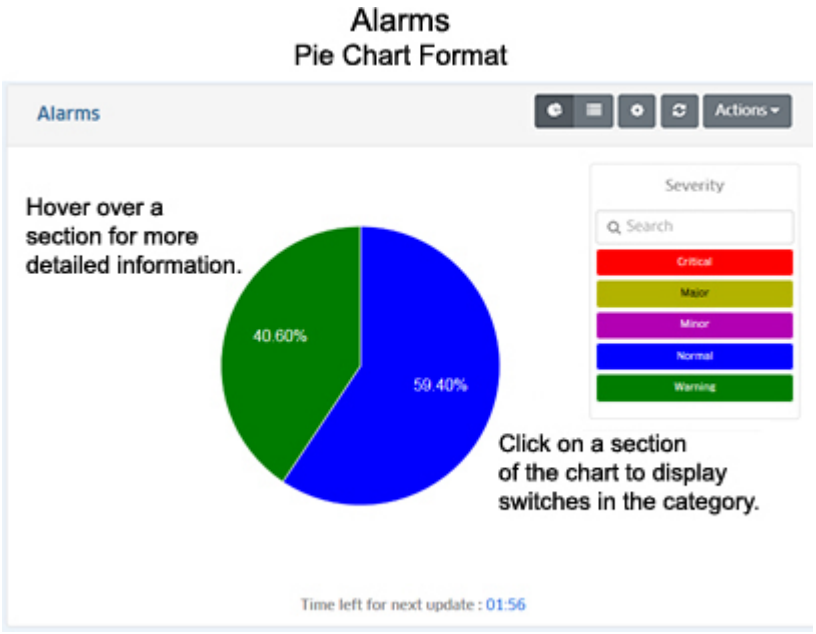
Note: Report Views and configuration options are configured using the Options Bar located at the top of the report. This help page contains view and configuration information specific to Alarm Reports. For specific information on all of the options available, see the "Report Options" section of the Analytics Reports Help.

Report Views

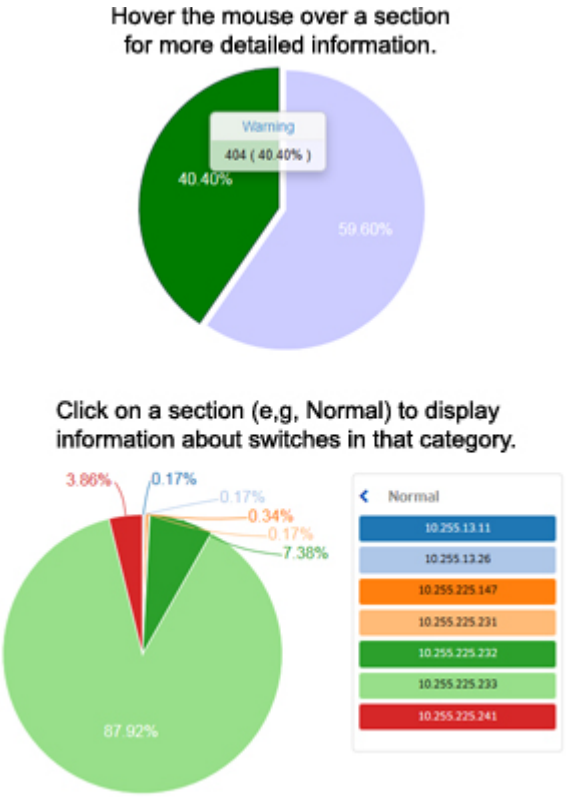
You can view the Alarms Report in a number of ways. By default, the pie chart format is displayed. You can also view a list of all alarms.

Pie Chart Format

By default, the pie chart view is displayed. The reported alarms in each severity level are displayed as a percentage of the total alarms reported. You can hover over a section of the chart for more details about the alarm category or click on a section in the pie chart to view the switch(es) from which the alarms for that category originated.

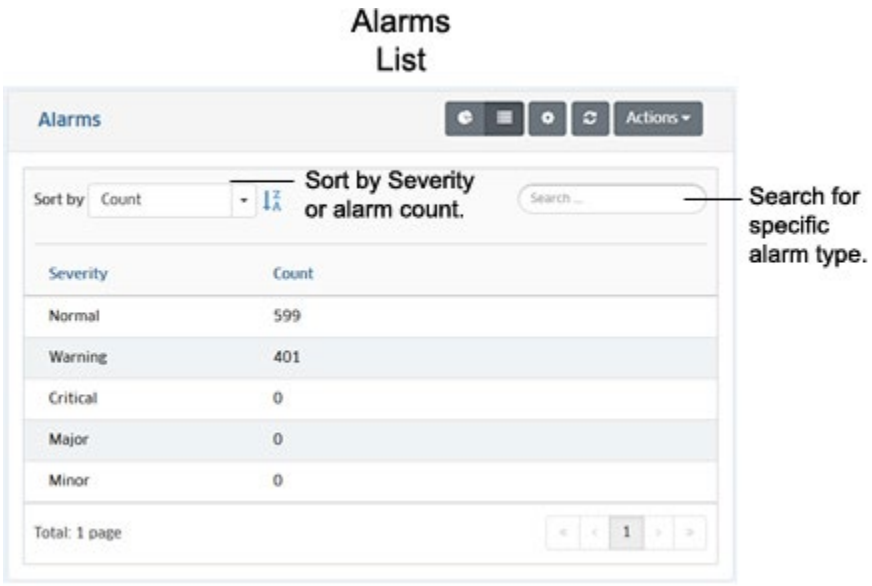


Hover over a section of the pie chart to display the number of alarms generated for that category. Click on a section of the chart to view information about the switches generating the alarms for that category (the legend will change from Severity Level categories to identify the switches. You can then hover over a section to display detailed information for a specific switch. Click on the Back Arrow (<) above the legend to return to the default view.



List Format

The list format displays the exact alarm count for each severity level. By default, the list is displayed by alarm count; however, you can select "Severity" in the **Sort by** drop-down menu to display the applications by sample count. You can also search for and display a specific severity level by entering the name in the **Search** field.



Configuring the Information Displayed

You can configure the amount of information displayed (e.g., refresh timer). To configure the display, click on the Configuration icon to bring up the Configuration Screen, then complete the fields as described below to configure the information displayed in the report.

- **Number of Switches -** The number of switches you want to display (Range = 1 - 10).
- **Auto Refresh Timer -** How often you want to refresh the data display, in minutes (Range = 15 - 60).

When you are done, click the **Save** button. The report display will immediately change to the new view. This will remain the view until it is changed again.

AP Uptime/Downtime

The Analytics AP Uptime/Downtime Screen displays detailed information about the Uptime/Downtime of Stellar APs, and the Uptime/Downtime of the link between APs and OmniVista. By default, Average AP/Link Uptime information is displayed. Click on the **AP Uptime/Downtime** button to view Stellar AP Uptime/Downtime information. Click on the **Average AP/Link Uptime** button to return to the default view.

The AP Uptime/Downtime information is based on either on Last Registration Time for the AP (Network - AP Registration - Access Points - Last Registration Time) or the "Last Up Time" received from alaOVSwitchUp/alaOVSwitchDown traps (Network - Notifications - Notifications Home). The Average AP/Link Uptime Report is based on the total AP down time value in the AP Uptime/Downtime Report for AP Power Down and AP Link Down.

> **Note:** By default, information for all APs for the last 30 days is displayed (up to 5,000 records). If there are more than 5,000 records on the OmniVista Server, you will be prompted to download the records from the server as a .csv file.

AP Uptime/Downtime Table

- **Date -** The date and time the AP was last "Up" prior to the most recent time the AP went "Down".
- **AP Name -** The user-configured name for the AP.
- **Time When AP Went Down -** The date and time the AP went down.
- **Total AP Uptime Until This Event -** The total amount of time the AP was "Up" before going "Down".
- **Time When AP Was Restored -** The date and time the AP was restored to "Up" status.
- **Link Down -** The current link status for the link between the AP and OmniVista. This field indicates whether or not the AP link to OmniVista is currently "Up" (Yes) or "Down" (No). If the link is "Down", OmniVista cannot communicate with the AP, but the AP can communicate with clients.
- **AP Power Down -** The current AP power status. This field indicates whether or not the AP is currently "Up" (Yes) or "Down" (No). If an AP is "Down" (e.g., powered down, rebooting), the AP cannot communicate with OmniVista or clients.

Average AP/Link Uptime Table

- **AP Name -** The user-configured name for the AP.
- **Average AP Uptime -** The percentage of time when the AP was "Up".
- **Average Link Uptime -** The percentage of time when the link between the AP and OmniVista link was "Up".

Statistics Overview

The Analytics Statistics feature enables you to collect and view statistics for network devices. To use the Statistics Feature, you set up your collection preferences (the information you want to collect), and enable statistics collection on the switch(es) you want to monitor. All managed switches are automatically included in a Default Statistics Collection Profile. This profile is used to set the statistics attributes (e.g., CPU Utilization, RxTx Utilization) that will be collected by OmniVista. Once you enable statistics collection on a switch(es), OmniVista automatically collects these statistics from all ports on those switch(es). You can then view statistics by creating View Profiles containing the switches and statistics attributes you want to view. You can also automatically configure and enable statistics collection any new switches added to the network. The Statistics application is configured using the following screens:

- **Statistics -** Used to quickly view current statistics on a device(s), create a Collection Profile, and view statistics from an existing Chart View.
- **Collection -** Used to create custom Collection Profiles to collect statistics from specific switches containing specific statistics variables
- **Chart Views -** Used to create View Profiles to view statistics data.
- **Settings -** Used to enable and configure automatic statistics collection from new switches added to the network.

Basic Statistics Workflow

To generate statistics data, you must first enable statistics collection on a switch(es) in the Managed Devices Table. By default, OmniVista collects data from all ports on a switch. Statistics data is then collected based on the statistics attributes configured in the Default Collection Profile. All managed switches are automatically included in the Default Collection Profile. The statistics attributes collected in the Default Profile can be configured as well as the polling interval and data retention period. You can also configure custom Collection Profiles to collect specific statistics attributes from specific switches. The basic steps for collecting and viewing statistics are:

1. View/Modify the Default Collection Profile

In the Analytics Menu, click on "Statistics", then click on "Collection" to bring up the Collection Screen. In the List of Collection Profiles, select the "Default Profile" and click on the Edit icon to view the attributes being collected. By default, all attributes are collected. You can change these defaults by selecting/unselecting attributes and clicking the **Apply** button. See the Collection online help for more information.

2. Enable Statistics on Network Switches

Go to the Managed Devices Screen (Network - Discovery - Managed Devices). Select the switch(es) on which you want to enable Statistics, click on the **Features** drop-down, and select

Enable Statistics. OmniVista will begin collecting statistics from those switches based on the attributes set in the Default Collection Profile.

3. Create View Profiles

Return to the Analytics application. In the Analytics Menu, click on "Statistics", then click on "Chart Views" to bring up the Chart Views Screen. Click on the Add icon to create a View Profile containing the switches and attributes you want to display and click the **Create** button. See the Chart Views online help for more information.

4. View Statistics Data

After creating the View Profile, you will be returned to the Chart Views Screen. Click on the name of the View Profile you just created to bring up the statistics display. By default, statistics data is displayed in graphical format. You can customize the way the data is displayed (e.g., line color/width, display timeframe); and you can also display the data in tabular format. See the Chart Views online help for more information.

Note: Once you create View Profiles, you can add them to the Performance Monitoring Dashboard for a quick view of network statistics. See the Dashboard online help for more information.

Automatic Statistics Workflow

Statistics are automatically enabled and configured automatically on any **new** switch you add to the network. To configure automatic statistics collection:

1. Set the Number of Switches

Go to the Settings Screen (Analytics - Settings). In the Collection Profile section at the top of the screen, you can set the number of new switches on which you want to automatically enable statistics collection in the **Enable Statistics Automatically On** field. If you select "All" (Default) all new devices will begin collecting the selected Statistics Attributes when they are added to the network. If you select "10" the first 10 devices added to the network will collect the selected attributes; if you select 20, the first 20 devices added to the network will collect the selected attributes, etc. That this will not affect any devices on your network that have already been configured statistics. Statistics configurations on those devices will not change.

When a new switch is added to the network, OmniVista will add the switch to the Default Collection Profile and begin collecting the attributes defined in the Default Profile. You can add these switches to a Collection Profile or just create View Profiles to view statistics data.

2. Create View Profiles

In the Analytics Menu, click on "Statistics", then click on "Chart Views" to bring up the Chart Views Screen. Click on the Add icon to create a View Profile containing the switches and attributes you want to display and click the **Create** button. See the Chart Views online help for more information.

3. View Statistics Data

After creating the View Profile, you will be returned to the Collection Screen. Click on the name of the View Profile you just created to bring up the statistics display. By default, statistics data is displayed in graphical format. You can customize the way the data is displayed (e.g., line color/width, display timeframe); and you can also display the data in tabular format. See the Chart Views online help for more information.

Statistics

The Analytics Statistics Screen is used to quickly view statistics on a device(s), create a View Profile, and view statistics from an existing View Profile.

Statistics Quick View

You can select statistics attributes and devices for a quick view of statistics for a specific device(s). Click on the **Selectors** drop-down and select the **Choose Attributes & Devices** radio button (selected by default). In the Attributes field, click on the **Add** or **Edit** button to bring up the Attribute List Window. Select the attributes you want to view and click **OK**. In the Devices field, click on the **Add** or **Edit** button and select the device(s) you want to view. to bring up the Attribute List Window. Select the attributes you want to view and click **OK**. Click on the **View** button to view the statistics for the selected attributes and devices. Click on the **Switch to Table** button to view the statistics in table format.

Create a View Profile

You can also save the attributes and devices you selected as a new View Profile. Click on the **Save As** drop-down and select **Save As New**. The Create View Profile Screen will appear. Enter a **Profile Name** and click on the **Create** button. You can also modify the attributes before selecting the **Create** button, if necessary. Click on the **Switch to Table** button to view the statistics in table format.

View Statistics From an Existing View Profile

You can also quickly view an existing View Profile. Click on the **Selectors** drop-down and select the **Choose a View Profile** radio button. Select a profile from the **View Profile** drop-down and click on the **View** button. Click on the **Switch to Table** button to view the statistics in table format.

Collection

The Analytics Statistics Collection Screen is used to create Custom Collection Profiles that specify specific devices and variables (e.g., CPU usage, port utilization) that you want to monitor. The List of Collection Profiles displays all configured Custom Collection Profiles (as well as the Default Profile) and is used to create, edit, and delete profiles. It is also used to schedule profiles and start and stop profiles.

> **Important Note:** The IP source address of the SNMP Service on a device must be the same as the IP address discovered for the device by OmniVista. Statistics cannot collect data if the IP source of the SNMP Service on the device is different than the discovered IP address for the device.

Statistics can be generated for the following statistics attributes:

- Switch Health (e.g., Rx Utilization, Tx Utilization, CPU Utilization)
- Module Health (e.g., Rx Utilization, RxTx Utilization, CPU Utilization)
- Port Health (e.g., Rx Utilization, RxTx Utilization)
- Ethernet Ports (e.g., Rx Bytes, Rx Unicast Frames, Tx Lost Frames, Tx Error Frames)

Note: Not all attributes are supported on all device types. When you generate statistics for a device, OmniVista automatically detects which attributes are supported for a device.

Using the Statistics Feature

OmniVista generates statistics data for all switches on which Statistics is enabled. Statistics can be enabled on individual switches on the Managed Devices Screen; and statistics can be enabled on a specific switch(es) by creating a Custom Collection Profile. A Collection Profile specifies the switches and attributes (e.g., CPU usage, port utilization) that you want to monitor, as well as the polling intervals and statistics data retention requirements. Profiles are created on the Collection Screen and data is displayed (for any switch on which Statistics is enabled) on the Chart Views Screen.

Creating a Collection Profile

To start collecting data, create a Collection Profile containing the devices and variables that you want to monitor. Click on the Add icon at the top of the screen to open the Create Collection Profile Screen, complete the screens fields described below.

- **Name -** The profile name. It is advisable to use meaningful names and/or descriptions for profiles, so that when glancing at the List of Collection Profiles list you will be able to distinguish one from another. For example, you may want to add a device name or IP address, and the type of variable you are monitoring, such as CPU or port utilization.
- **Description -** An optional profile description.
- **Poll Devices Periodically-** Enables (On)/Disables (Off) automatic polling for the profile. OmniVista will continuously poll the devices in the profile based on the Poll Interval and Data Retention Period. Disabling automatic polling performs the same function as stopping a profile on the Collection Profile List Screen. There may be times when you want to temporarily disable automatic polling. For example, if you wish to spend more time viewing and analyzing a certain group of statistics, automatic polling will interfere by updating these statistics when the next polling cycle is performed. To prevent this, you can edit the profile to disable automatic polling (Default = On).
- **Poll Interval -** When automatic polling is enabled, specify the desired polling rate, in minutes (Range = 1 - 60, Default = 5).
- **Data Retention Period -** The amount of time Statistics Data is saved on the OmniVista Server. You can specify the retention period in Days or Hours. When the specified data retention period is reached, new incoming data will overwrite the oldest data. For example, if you specify a data collection size of 30 days, new incoming data will begin to overwrite the oldest data after 30 days of data have been saved to the server. (Range = 1 - 180 Days, Default = 30 Days).
- **List of Selected Devices -** Click on the **Add** button and use the Switch Picker or Topology Map option to select the switch(es) you want to monitor.
- **Attributes -** Select the attributes you want to monitor with the profile. All of the available attributes are displayed. By default, all of the attributes are selected. You can change the default attribute settings by clicking on the "Go To Settings" link to go to the Analytics Settings Screen.

After completing the fields above, click on the **Create** button. The profile will then appear in the List of Collection Profiles. You can go to the Chart Views Screen to view statistics in graphical or table format.

Editing a Statistics Profile

Click on a profile in the List of Collection Profiles and click on the Edit icon. The Edit Collection Profile Screen will appear. Edit any parameters as described above and click on the **Apply** button. You cannot edit the profile name.

Deleting a Statistics Profile

Click on a profile(s) in the List of Collection Profiles and click on the Delete icon. Click on **OK** at the Confirmation Prompt. Note that deleting a profile also **deletes all statistical data** associated with the profile.

Scheduling a Profile

You can schedule a profile to start at a specific time in the future, run for a specific period of time, or run at regular intervals. If you schedule a profile to start at a specific time (set the Start Time only), the profile will start at that time and continue running. If you set a profile to run for a specific time period (set Start Time and End Time), the profile will only run during the specified time period and then stop.

If you schedule a profile to run at regular intervals, the profile will run and collect data for the profile's configured Data Retention Period, stop, and then restart at the scheduled interval. For example, if you schedule a profile with a 30-day Data Retention Period to begin running on the current date and set the Interval for 60 days, the profile will run for 30 days, and then stop. The profile will then automatically re-start after 60 days and run again for 30 days.

To schedule a profile, you must first stop the profile by selecting the profile in the List of Collection Profiles and clicking on the **Stop** icon, then click on **OK** on the Results screen. Once the profile has stopped, select it and click on the **Schedule** button. The Schedule window will appear. Configure the fields as described below to configure the profile schedule and click on **OK**. After creating the schedule, you **must** restart the profile.

- **Start Time -** Enter/select the date and time you want the scheduled profile to start running. If you set only a Start Time, the profile will start at the specified time and continue running. If you do not set a Start Time, the scheduled profile will begin running immediately.
- **End Time -** Enter/select the date and time you want the scheduled profile to stop running. The profile will run only for the configured time period and then stop. If you do not set an End Time, the schedule profile will continue running.
- **Interval -** Use the fields to enter a regular interval for the job to repeat (e.g., 45 days, 60 days). The profile will stop running when the Data Retention Period is reached. The profile will then automatically re-start at the specified interval. The Interval cannot be less than the Data Retention Period configured for the profile.
- **Repeat -** If you want to repeat the configured interval, enter the number of times you want it to repeat (Range = 0 - 999).

Note: You can view details of any scheduled Statistics Profile job in the User Defined Jobs tab of the Scheduler Jobs Table (Administrator - Control Panel - Scheduler Jobs).

Starting/Stopping a Profile

A profile starts collecting data as soon as it is created. You can stop a profile by selecting the profile(s) in the Profile Statistics List and clicking on the **Stop** icon at the top of the list. Click **OK** on the Results Screen. The profile will stop collecting data. You will not lose previously-collected data. The data will be stored on the OmniVista Server based on its Data Retention Period.

To restart a profile that has been stopped, select the profile(s) and click on the **Start** icon at the top of the list. Click **OK** on the Results Screen. The profile will begin collecting data and the data will be stored on the OmniVista Server. However, there will be a gap for the period during which the profile was stopped.

List of Collection Profiles

- **Name -** The user-configured name of the profile.
- **Status -** The running status of the profile (Running, Stopped). If a profile is "Running", it is collecting data. If a profile is "Stopped" it is not currently collecting data.
- **Running Mode -** Indicates whether the profile is "Manual" or "Scheduled". A Manual Profile runs continuously. A Scheduled Profile runs at specified intervals.
- **Start Time -** The most recent time the profile was started and began collecting data. A profile begins collecting data when it is created.
- **End Time -** The most recent time the profile was stopped. If a profile has been continuously running since the last time it was started, the field will be blank.
- **Interval -** The profile polling rate, in seconds (Range = 20 - 60, Default = 60).
- **Data Retention -** The amount of time Statistics Data is saved on the OmniVista Server. (Range = 1 - 180 Days, Default = 30 Days).
- **Owner -** The user who created the profile.
- **Created Time -** The date and time the profile was created.
- **Description -** The user-configured description for the profile.

Chart Views

The Analytics Statistics Chart Views Screen displays a list of configured View Profiles, which provide graphical and tabular views of collected Statistics data. The screen is used to create, edit, delete, and view collected Statistics data.

Creating a View Profile

You can create a View Profile from any switch(es) from which you are collecting Statistics data. The View Profile is independent of any specific Collection Profile. As long as OmniVista is collecting statistics from a switch (either through a Collection Profile or enabling statistics on a switch on the Managed Devices Screen), that switch can be included in a View Profile. To create a View Profile, click on the Add icon at the top of the List of View Profiles, complete the fields as described below, then click on the **Create** button.

- **Profile Name -** The View Profile name. It is advisable to use meaningful names and/or descriptions, so that when glancing at the List of View Profiles you will be able to distinguish one from another. For example, you may want to add a device name or IP address, and the type of attribute you are monitoring, such as CPU or port utilization.

- **Description -** An optional View Profile description.
- **Choose Attributes -** Select the statistics attributes that you want to include in the View Profile (e.g., Rx Utilization, CPU Utilization). All available attributes are displayed. You can select a category (e.g., Switch Health, Module Health) to select all attributes in that category; or select individual attributes from categories. Note that up to 50 Counters can be displayed in a View Profile. If you select attributes that generate more than 50 Counters (e.g., Port Health attributes on switches with more than 50 operational ports), when you try to create the profile, you will receive a message to remove some of the Counters from the profile. See note below for more information.
- **Selected Devices** - Click on the **Add** button and use the Switch Picker or Topology Map option to select the switch(es) you want to include in the View Profile.
- **List of Available Counters -** Counters are the lines used to display the statistics data collected for each selected attribute. OmniVista automatically creates line options for each Counter, and assigns each Counter a default line color and width. Up to 50 Counters can be displayed in a View Profile. If the attributes selected create 50 or fewer Counters, the Counters will be displayed "Selected Counters" tab. If more than 50 Counters are required for the selected attributes (e.g., Port Health attributes on switches with more than 50 operational ports), all of the Counters will appear in the "Available Counters" tab. In this case, select the Counters you want to display (up to 50), click on the **Add Counters** button, and click **OK** at the Confirmation Prompt to move the Counters to the "Selected Counters" tab. Click on the "Selected Counters" tab to view the selected Counters. All of the Counters for each attribute are displayed in the List of Selected Counters as described below.
- **Line Options -** The line color and thickness used to display the attribute in the line chart. You can change the line color or width of a Counter's line by clicking on the line in the Line Options Column and selecting a different color and/or width. You can change these defaults now or any time you are viewing a Profile.
- **Scale -** The scale used on the line chart for the attribute. By default, all attributes are set to a Scale of 1. When two or more attributes are being graphed simultaneously, the graph line for one attribute may be disproportionately large (or small), making it difficult to view. If this situation occurs, you may wish to select a different scale for that attribute. In this context, scale is really a multiplier. The range of scale values is 0.001 - 1000. You can change the scale used to plot a Counter by clicking on the Scale Column and selecting a different scale. You can change the scale now or any time you are viewing a Profile.
- **User Variable -** The specific attribute being monitored (e.g., Switch Rx Utilization, Port Rx Utilization).
- **Category -** The Category and Sub-Category of the attribute (e.g., Switch-Health).
- **Device Name -** The name of the device being monitored.
- **IP Address -** The IP address of the device being monitored.
- **Chassis -** The number of the chassis being monitored, if applicable.
- **Slot -** The slot being monitored, if applicable.
- **Port -** The port being monitored, if applicable.

  Note: You can have a maximum of 50 Counters in a View Profile. If you want to remove a Counter(s) from the Chart, select the Counter(s), click on the **Remove Counters** button, and click **OK** at the Confirmation Prompt. The Counter(s) will be

moved to the "Available Counters" tab. To add any variables, click on the "Available Counters" tab, select the Counter(s), click on the **Add Counters** button, and click **OK** at the Confirmation Prompt.

Viewing Statistics Data

To view statistics data, select a View Profile in the View Profile List and click on the **View Statistics** button at the top of the list (or just click on the Profile Name). You can only view data for one profile at a time. Data is displayed as a percentage of the maximum capacity for each attribute (0 - 100 %). By default, data is displayed for the last hour. However, you can change the display time range or display more detail within a time range. You can also change the line color/width or scale of a Counter to make it easier to view in the chart.

Note: You can click on the **Switch to Table** button at the top of the screen to display detailed data in table view. From Table View, you can click on the **View Chart** button to return to chart view.

Note: Statistics are collected based on a one-hour average for each attribute.

As shown in the example above, the data for the profile (e.g., Switch 2 Statistics) is displayed in a line chart at the top of the screen and the attributes included in the profile are displayed below in the Counters table. (You can click on the button at to bottom of the graph to move the Counters to the right of the graph.) You can use the Counters Table as a legend to view different attributes in the line chart. You can also select an attribute(s) and click on the **Show** or **Hide** buttons to add or remove them from the chart. When you hide an attribute, the it will be "grayed out" in the Counters Table. Data will still be collected for the attribute(s), the data will just not be displayed in the chart. Select the hidden attribute(s) and click on the **Show** button to display the attribute in the chart. You can also select an attribute and click on the Delete icon to remove the it from the View Profile.

> **Note:** OmniVista automatically polls devices in a profile based on the Automatic Polling Interval configured for the profile. However, you can click on the **Refresh** button above

the chart to perform an immediate poll and re-display of the data. You can also click on the **Save to PNG** button to save/view the chart as a .png file.

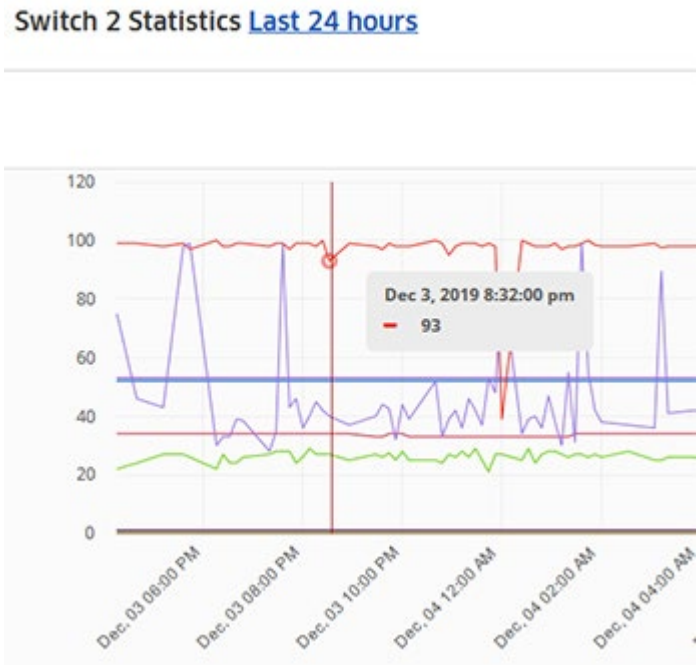
Changing the Display Time Range

By default, data is displayed for the last hour. Click on the time range link (e.g., "last 1 hour") to bring up the Time Range Window. Change the time range as described below and click on the **Get Data** button.

- **Until Now -** Displays data from the last time the profile was started until the present time. If you select this option, you can set a duration:
- **All Data -** Displays all data during the time configured for the profile (e.g., 30 days).
- **Last 7 Days -** Displays data for the last 7 days.
- **Last 24 Hours -** Displays data for the last 24 hours.
- **Last Hour -** Displays data for the last hour.
- **Custom -** Set a Start Time and End Time for the data display. Only data collected during this time period is displayed.

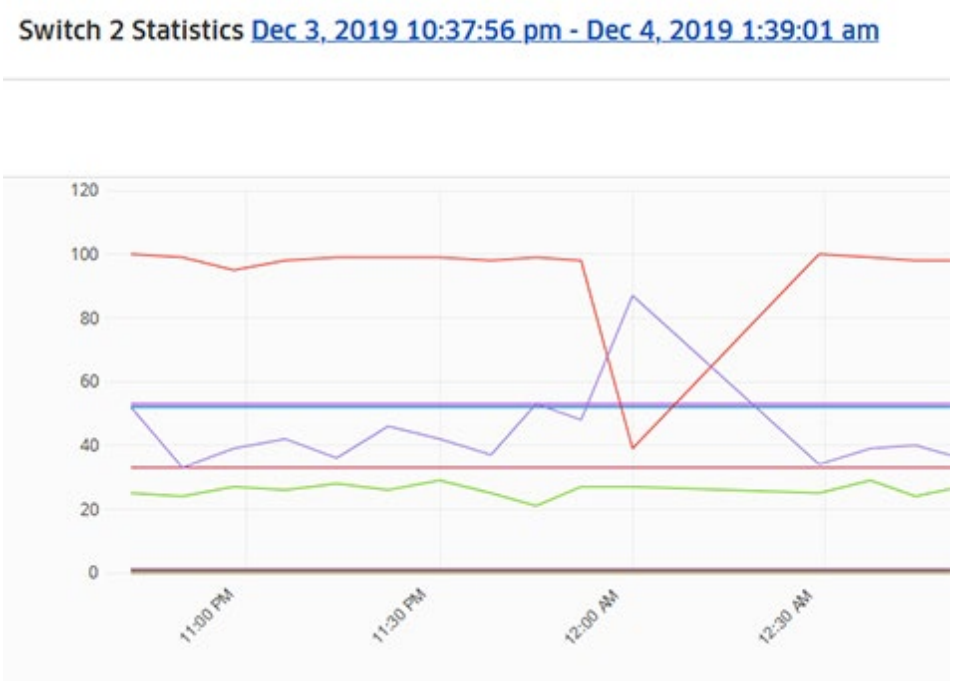
Displaying More Detail in a Time Range

You can place the cursor on an attribute line anywhere along the timeline to view exact data for that attribute at a specific time, as shown below. The data displayed is based on the polling interval configured for the profile. For example, if the polling interval is 60 seconds, data is displayed at one-minute intervals as you move the cursor along the timeline. The line color for the attribute is displayed along with the data. Specific data for each poll is also available in Table View.



You can also zoom in on a specific period on a time range to view more detail. Click and drag the mouse along the section of the graph that you want to view. The section is highlighted in gray, as shown below.

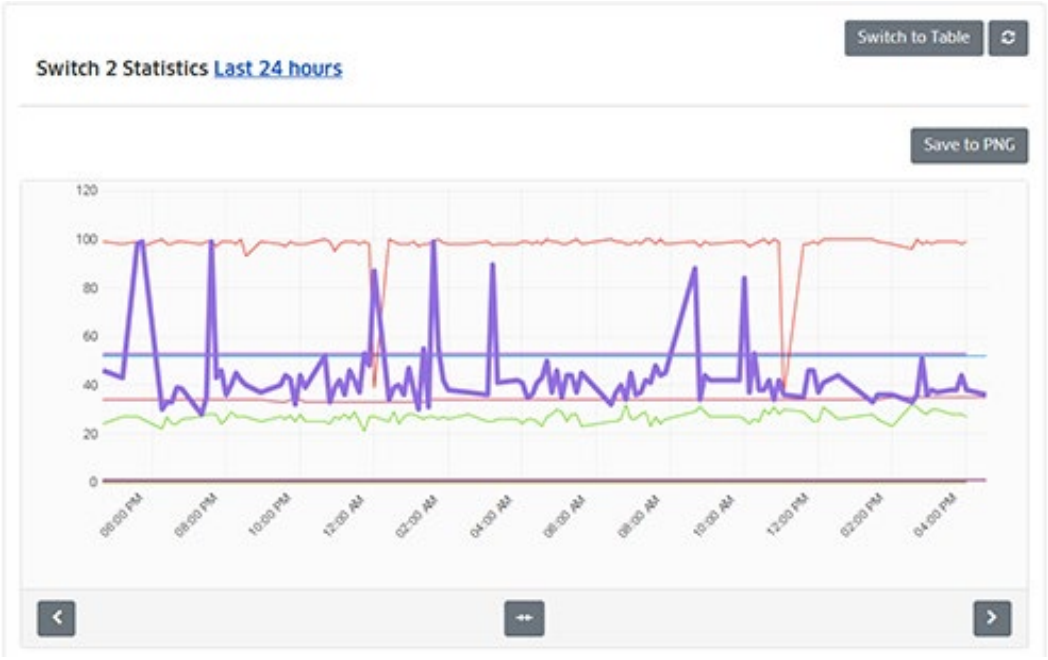
Release the mouse clicker and the time range you selected will be displayed in detail. As you can see, rather than displaying the last hour of data, the graph now displays a detailed view of the selected time range (December 3, 2019 10:37:56 p.m. - December 4, 2019 1:39:01 p.m.)



Changing a Counter's Line or Scale

You can change the color or width of a Counter's line to help you track the Counter more easily. To change a line color or width, click on the line in the Line Options Column of the Counters Table. To change a line width, click on the Line Width drop-down and select a different width. To change the line color, click on Line Color drop-down, choose a different line color, then click on

the **Choose** button. When you are done, click anywhere in the display to close the window. The Counter will be displayed in the chart with the new color and/or width, as shown below.

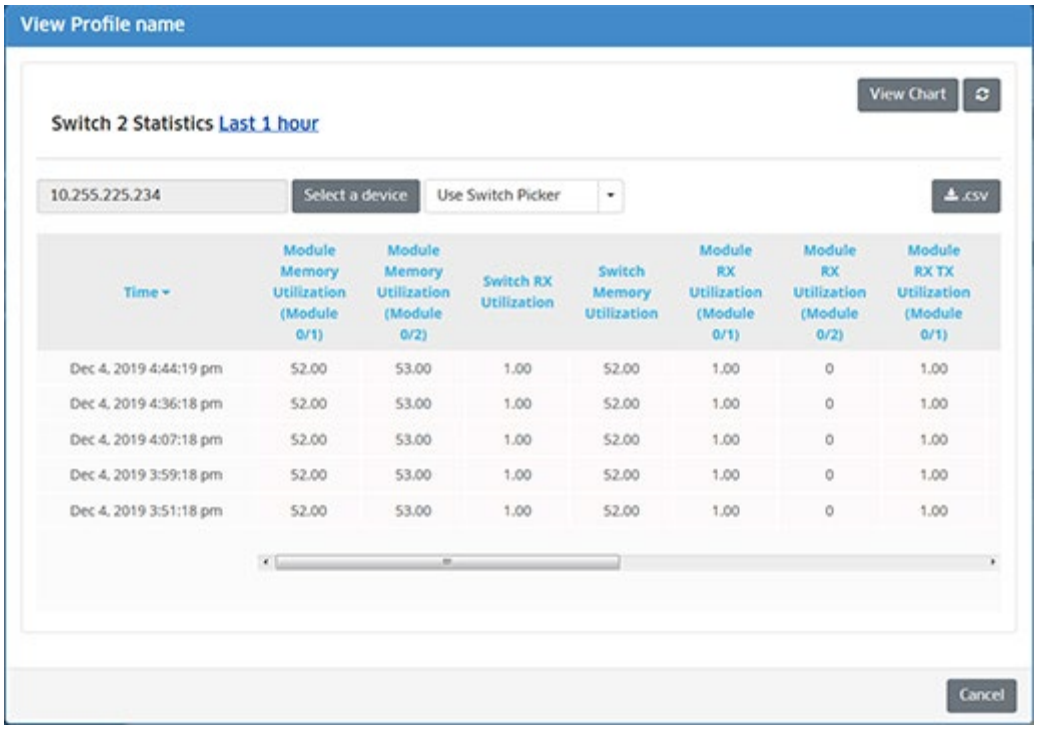


You can also change the scale used to plot a Counter by clicking on Scale Column and selecting a different scale. By default, all Counters are set to a Scale of 1. When two or more Counters are being graphed simultaneously, the graph line for one Counter may be disproportionately large (or small), making it difficult to view. If this situation occurs, you can select a different scale for that Counter. In this context, scale is really a multiplier. The range of scale values is 0.001 - 1000.

Table View

To display data in a detailed table view, click on the **Switch to Table** button at the top of a profile chart screen. You can only view statistics for one device at a time. Click on the **Select a Device** button, select a device, then click on **OK** to display the data. Table View provides detailed information at each data poll. The information is displayed as a percentage of the maximum value for each attribute.

You can only view statistics for one switch at a time. Click on the **Select a Device** button to view data for a different switch in the profile. Click on the **View Chart** button to return to chart view.



Note: You can click on the .CSV button at the top of the table to view/save the table as a .csv file. The timestamp on the .csv file is the OmniVista Server time.

Editing a View Profile

Click on a profile in the View Profile List and click on the Edit icon. The Edit View Profile Screen will open. Edit any parameters as described above and click on the **Apply** button. You cannot edit the profile name.

Deleting a View Profile

Click on a profile(s) in the View Profile List and click on the Delete icon. Click on **OK** at the Confirmation Prompt. Note that deleting a profile also **deletes all statistical data** associated with the profile.

View Profile List

The View Profile List displays information for all View Profiles. Click on a Profile Name to view statistics data for the profile. Click on a switch in the Devices Column for detailed information on devices in the profile.

- **Profile Name -** The user-configured name of the profile.
- **Description -** The user-configured description for the profile.
- **Devices -** The devices included in the Chart. Click on a device for more detailed information.

Profiles

The Analytics Profiles Screen displays currently-configured Analytics Profiles, and is used to create, edit, and delete profiles. The first step in generating analytics information for Top N

Applications, Top N Clients, Top N Ports Utilization, and Top N PoE Ports Utilization Reports is to create an Analytics Profile. A profile consists of the type of information you want to view (Profile Type) and the switches/ports that you want to analyze. Note that a switch can only be in **one** profile of a particular Profile Type at a time.

Creating a Profile

Click on the Add icon. Complete the fields in the Create Profile Wizard as described below:

Configuration Screen

- **Profile Name -** The user-configured name for the profile.
- **Profile Type -** Select a Profile Type from the drop-down menu:
- **Top N Apps & Clients -** This profile gathers information about the top applications being accessed on the network, including which clients are accessing an application, and which switches have the most traffic for an application. Data from this profile type is displayed in both the Top N Applications Report (displays application information) and in the Top N Clients Report (displays client information).
- **Top N Ports Utilization -** This profile gathers information about port utilization.
- **Top N PoE Ports Utilization -** This profile gathers information about PoE port utilization. Note that a Top N PoE Ports Utilization Profile will generate data for both Top N PoE Port Reports and Top N PoE Switch Reports.
- **Sampling Rate (Top N Apps & Clients Only) -** The ratio of packets observed at the data source to the samples generated. For example, a sampling rate of 100 specifies that, on average, 1 sample will be generated for every 100 packets observed.
- **Usage Threshold - (Top N PoE Ports Utilization Only) -** Sets a Notification threshold for total PoE power usage for switches in the profile, in percent. When the usage threshold is reached or exceeded, a notification is sent to the user via the Notifications application. This setting overrides the Default Usage Threshold setting configured on the Settings Screen for all switches in the configured profile (Range = 1 - 99, Default = 99). Note that this setting is only supported on AOS 8.x Devices.

Device/Port Selection Screen

- **Default Ports Template (Top N Apps & Clients, Top N Ports Utilization Profiles only) -** You can use this option to assign the profile to the same ports on selected switches. Rather than selecting switches and then selecting ports for each switch, you can assign the profile to the same ports on multiple switches. For example, to assign the profile to ports 1/1 through 1/10, enter 1/1-1/10, then click on the Add icon. When you select switches in the next step, the profile will be assigned to ports 1 through 10 on all selected switches and the "Apply Ports Template" message will appear.

You can also create multiple templates to be applied to different switch types. For example, you can create a template for 6850 Switches (e.g., 1/1-1/10) and create a template for 6860 Switches (e.g., 1/1/1-1/1/10). When you select switches in the next step, the profile will be assigned to ports 1 through 10 on all selected 6850 Switches, and ports 1/1/1 through 1/1/10 on all selected 6860 Switches.

When selecting ports for a Top N Apps & Clients or Top N Ports Utilization Profile, is recommended that you only select required ports, not all ports, to conserve disk space on the OmniVista Server.

- **Add/Remove Switches -** Click on the **Add/Remove Switches** button. From the list of switches, select the switch(es) you want to analyze, then click **OK**. The selected switch(es) will be displayed. Click on the **Add/Remove Ports** button to specify ports. Note that if you created a Default Ports Template, you do not need to configure ports, ports will automatically be assigned based on the template.
- **Add/Remove Ports (Top N Apps & Clients, Top N Ports Utilization Profiles only) -** Select a switch and click on the **Add/Remove Ports** button. From the list of ports, select the port(s) that you want to analyze, then click **OK**. If you selected multiple switches, select the next switch and repeat until ports have been selected for all switches. Click on the **Create** button. After clicking on the **Create** button, the status of the operation will be displayed in the Results Table. Click **OK** to return to the Profiles Screen.

Note: When selecting ports for a Top N Apps & Clients or Top N Ports Utilization Profile, it is recommended that you only select required ports, not all ports, to conserve disk space on the OmniVista Server.

Note: It is not necessary to configure ports in a Top N PoE Ports Utilization Profile. When you select a switch(es) for the profile, all PoE-enabled ports on the switch are included in the profile. Note that it is recommended that you select only a few required switches, not all of the switches, to maintain performance on the OmniVista Server.

Note: If you change the IP address of a switch after assigning a "Top N App & Clients Profile" to the switch, you must re-assign the profile to the switch.

Editing a Profile

Select the profile in the Profiles Screen and click on the Edit icon to bring up the Edit Profile Wizard. Note that you cannot edit the Profile Name or Profile Type. Depending on the Profile Type, you can add/remove switches and/or ports to/from a profile on the Device/Port Selection Screen.

To add/remove switches to/from a profile, click on the **Add/Remove Switches** button and select the switches you want to add/remove to/from the profile. When you are done editing, click on the **Apply** button. The status of the operation will be displayed in the Results Table. Click **OK** to return to the Profiles Screen. Note that removing a switch from a profile automatically removes any ports associated with that switch and removes the sFlow configuration from the ports.

To add/remove ports from a profile, select a switch, click on the **Add/Remove Ports** button and select the ports you want to add/remove to/from the profile. When you are done editing, click on the **Apply** button. The status of the operation will be displayed in the Results Table. Click **OK** to return to the Profiles Screen. Note that removing a port from a profile removes the sFlow configuration from the port.

Deleting a Profile

Select the profile(s) in the Profiles Screen, click on the Delete icon, then click **OK** at the confirmation prompt. The status of the operation will be displayed in the Results Table. Click **OK** to return to the Profiles Screen. If the profile has been assigned to devices, a warning prompt will appear. You can click on the "Device" link to see which switches the profile has been

assigned to. Click **OK** to remove the profile from the listed switches. Note that you can remove a profile from a specific switch(es) by editing the profile.

Viewing a Profile

Click on a profile in the Profiles to view details of the profile. The Profile Name and Profile Type will be displayed. You can expand the Switches area to view information about switches associated with the profile.

Summary View

The Analytics Summary View Screen displays basic information for all discovered network switches, including any Analytics Profiles to which a switch might belong. Click on a switch to view detailed switch information. If the switch is included in an Analytics Profile(s), the Profile Name(s) is displayed in the Profiles field. Click on the **View** button to go to the Profiles Screen and view profile details. From the Profiles Screen, you can view, edit, or delete the profile.

Switch Information

- **Address -** The switch IP address.
- **Name -** The user-configured switch name.
- **Location -** The user-configured switch location (if no location was configured by the user, the field will display "Unknown").
- **MAC Address -** The switch MAC address.
- **Version -** The switch AOS version.
- **Type -** The switch type (e.g., OS10K, OS6900).

Applications Management

When generating a Top N Applications Report, the Analytics application uses port numbers to identify application traffic. In other words, traffic on a specific port is identified as coming from a specific application. The Analytics Application Management Screen is used to create, edit, and delete application/port mapping. Well known ports (e.g., 161 for SNMP, 80 for HTTP) do not need to be mapped. By default, these ports are automatically mapped and are displayed on the screen.

Creating Application Mapping

Well known ports (e.g., 161 for SNMP, 80 for HTTP) do not need to be mapped. By default, these ports are automatically mapped and are displayed on the screen. To map other ports to an application, follow the steps below.

> **Note:** If you have an existing application ports mapping file (.json file), you can import the file rather than creating individual mappings as described in the steps below.

1. Click on the displayed mode button (Range Based/Enumerated) to select the **Mode** to use for monitoring/mapping. When you click on the button, select the **Mode** on the Select Mode Window and follow the instructions below:

- **Range-Based -** This mode is used to set a range of ports that are monitored by the Analytics application. Traffic on these ports is monitored and can be displayed in the Top N Applications Report. Information for all of these ports is available to be

displayed (depending on how you configure the report), however, only those ports that you have mapped will be labeled with the application. Other ports will be labeled "Unknown". If you select Range Based Mode, enter a range of ports to be monitored, then click **OK**.

- **Enumerated -** This mode requires that you define specific ports to be monitored. Only those ports you define when you create a mapping will be monitored. If you select Enumerated Mode, click **OK**.

2. Click on the Add icon. On the Create Application Mapping Screen, complete the fields as described below:

- **Application Name -** Enter the name of the application (e.g., SNMP).
- **Ports -** Enter the port or port range to be associated with the application. If you are entering a range of ports, separate the port numbers with a "-" (e.g., 20-21).

Importing/Exporting an Application Ports Mapping File

If you have an existing application ports mapping file (.json file), you can import the file into OmniVista 2500 NMS. Click on the **Import** button to bring up the Import an Applications Ports Mapping File window and click on the **Browse** button. Locate the file and click **OK**. The port mappings in the file will appear in the list on the Applications Management Screen. Note that this new mapping **will override** your existing mapping.

You can also create an application ports mapping .json file by exporting your existing mapping list. To create/export the file, click on the **Export** button. At the prompt screen, select **Save File** and click **OK**. The file will be downloaded to your default download area.

Editing Application Mapping

Click in the checkbox next to a mapping entry and click on the Edit icon to bring up the Edit Application Mapping Screen. Edit the Application Name and click on the **Update** button. The updated entry will appear in the list on the Application Management Screen. You cannot edit the ports. To map a different Application to a port, you must delete the mapping entry and create a new one.

Deleting Application Mapping

Click in the checkbox next to a mapping entry, click on the Delete icon, then click **OK** at the confirmation prompt.

Anomalies

The Analytics Anomalies Screen displays any anomalies that are discovered in established port utilization trends. The information is displayed in a list that describes the anomaly and its origins (e.g., IP address, Port). Anomaly detection uses Z-Score to check for anomalies in the latest port utilization data gathered from hourly polling over the past 30 days. Z-Score is a statistical measurement of a score's relationship to the mean in a group of scores. In other words, it measures utilization for a port for a specific hour to determine its relationship with utilization for the same hour over the sampling period (30 days). A data point that deviates considerably from an established pattern is flagged as an anomaly and displayed on the Anomalies Screen. Z-Score parameters are configured on the Preferences - Analytics Screen.

You can configure the information displayed by clicking on the Configuration icon to bring up the Configuration Screen and set any or all of the displayed columns. Click on the **Add To Report**

button to create a report in the Report Application (see the Report Configuration Help for more information).

> **Note:** A minimum of 11 days of data is required for anomaly calculation. Also, seasonal variation for periods of more than 30 days cannot be adequately learned using this method. For example, an annual usage pattern would be affected by lower usage due to holidays/vacations.

Settings

The Analytics Settings Screen is used to configure preferences for port utilization trending and anomaly detection in the Analytics application, as well as preferences for Analytics Statistics. When you have configured the value(s), click the **Apply** button. The change takes effect immediately.

Collection Profile

The following settings are used to set automatic statistics collection on new switches and configure the default Statistics Profile collection settings. By default, these settings are pre-selected when you configure a Collection Profile. These default settings can be modified when you configure a Collection Profile.

- **Enable Statistics Automatically On -** Automatically enables statistics collection on new devices when they are added to the network. Select the number of new devices on which you want to automatically enable Analytics Statistics collection. This will be applied to new devices added to your network. (By default, statistics collection is enabled on 2000 devices for a new OmniVista installation and 0 devices for an OmniVista upgrade.) If you select "All" all new devices will begin collecting the selected Statistics Attributes when they are added to the network. If you select "10" the first 10 devices added to the network will collect the selected attributes; if you select 20, the first 20 devices added to the network will collect the selected attributes, etc. This does not apply to any devices on your network that were configured for Statistics, as configurations on those devices will not change. Note that if you choose "All" and you add a large number of network devices, there is a risk of performance impact.
- **Statistics Attributes to Collect By Default -** Select the default Statistics Attributes you want to collect from any new Custom Performance Monitoring Profiles. Note that these are the default settings; you can change these settings when creating a profile. This will be applied to new profiles. It does not affect attributes included in any existing profile.

Analytics Configuration

- **sFlow Port -** The sFlow port used to gather analytics data (Default = 6343).
- **Max Top N Apps/Clients Data Size/Day -** OmniVista receives Top N Apps and Top N Clients data from devices via sFlow packets. This sets the maximum amount of Top N Apps and Top N Clients data for **all** devices retained in the OmniVista Database each day, in MB. When the data reaches this limit, the oldest data for that day will be overwritten by newer data. (Range = 32 - 256, Default = 64).
- **Outlier Detection: Lower Threshold -** Used for anomaly detection. The threshold value used to determine if new port utilization is lower than mean utilization for that port:

  - BEYOND2Z-SCORE - Any value that falls outside 2 times Standard Deviation from mean on a normal distribution curve.
  - BEYOND2.5Z-SCORE - Any value that falls outside 2.5 times Standard Deviation from mean on a normal distribution curve.
  - BEYOND3Z-SCORE - Any value that falls outside 3 times Standard Deviation from mean on a normal distribution curve. (Default)
- **Outlier Detection: Higher Threshold -** Used for anomaly detection. The threshold value used to determine if new port utilization is higher than mean utilization for that port:
  - BEYOND2Z-SCORE - Any value that falls outside 2 times Standard Deviation from mean on a normal distribution curve.
  - BEYOND2.5Z-SCORE - Any value that falls outside 2.5 times Standard Deviation from mean on a normal distribution curve.
  - BEYOND3Z-SCORE - Any value that falls outside 3 times Standard Deviation from mean on a normal distribution curve. (Default)
- **Prediction: Training Timeout -** Used for port utilization trending. Specifies how long OmniVista will train, in seconds, by sampling past port utilization. In other words, this specifies how long OmniVista will sample port utilization data before beginning to predict future trends (Range = 30 - 600, Default = 60).
- **Prediction: Training Error -** Used for port utilization trending. The target error percentage to which OmniVista will be trained (Default = 0.1 - 1.0, Default = 0.5).
- **Top N Ports Purge -** The amount of time, in months to retain analytics port utilization data before it is purged from the OmniVista Database (Range = 1 - 8, Default = 3).
- **Top N Switches Purge -** The amount of time, in months to retain analytics switch resource data before it is purged from the OmniVista Database (Range = 1 - 8, Default = 3).
- **Top N Apps Purge -** The amount of time, in months to retain analytics application data before it is purged from the OmniVista Database. It is recommended to keep the retention time to a minimum to avoid disk storage problems that may be experienced due to the high inflow of sFlow packets (Range = 1 - 24, Default = 3).
- **Top N Clients Purge -** The amount of time, in months to retain analytics client data before it is purged from the OmniVista Database. It is recommended to keep the retention time to a minimum to avoid disk storage problems that may be experienced due to the high inflow of sFlow packets (Range = 1 - 24, Default = 3).

Application Visibility Statistics Configuration

- **AppMon/AppFP Schedule Interval -** The amount of time OmniVista will wait to poll devices for Application Monitoring Statistics.
- **DPI Schedule Interval -** The amount of time OmniVista will wait to poll devices for Application Enforcement Statistics.

PoE Configuration

- **PoE Polling Interval -** The interval, in hours, for OmniVista to poll switches for PoE Port utilization data (range 1 - 24. Default = 1).

- **Top N PoE Purge -** The amount of time, in months to retain analytics PoE Port utilization data before it is purged from the OmniVista Database (Range = 1 - 8, Default = 8).
- **Default PoE Threshold Usage -** Sets the default PoE power threshold for switches in a PoE Profile, in percent. When the usage threshold is reached or exceeded, a notification is sent to the user via the Notifications application (Range = 1 - 100, Default = 99).

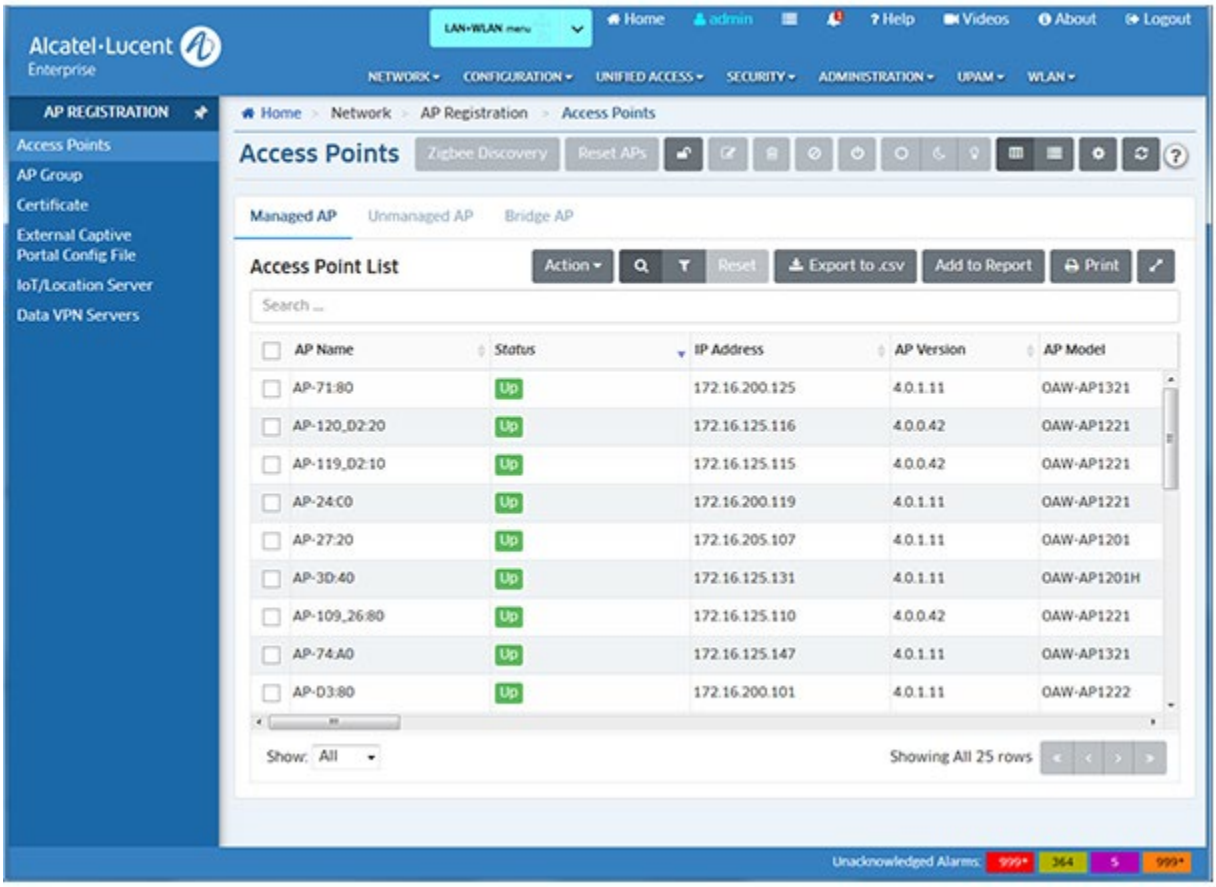
4.0 AP Registration

The AP (Access Point) Registration application is used to register Stellar AP Series Devices with OmniVista and configure the APs into AP Groups that can be managed by OmniVista. When Stellar AP Series Devices are connected to the network, the AP automatically contacts, and registers with, the OmniVista Server. OmniVista initially classifies the AP as "unmanaged", and displays it in the Unmanaged Access Point List. At this point, the APs are in an "unmanageable" state; OmniVista is aware of the APs but cannot yet manage them. The Network Admin can review these APs and place them into a "trusted" state where they can be managed by OmniVista.

Stellar AP Series Devices are managed by AP Group. OmniVista does not manage individual APs. The attributes configured for the AP Group (e.g., Management VLAN, RF Profile) are applied to all APs in the group. All APs are initially assigned to the Default AP Group. You can configure additional AP Groups and assign specific APs to them. You configure Stellar AP Series Devices in OmniVista (e.g., Notification traps, Resource Manager backups) by applying the configuration to an AP Group. In OmniVista applications (e.g., Notifications, Resource Manager), rather than presenting the user with individual APs when applying a configuration (as is done with AOS Devices), OmniVista presents the user with the option of applying a configuration to AOS Devices and/or AP Groups. Any configuration applied to an AP Group is applied to all APs in the group.

The bootup sequence for APs and the basic workflow for configuring APs for OmniVista management is provided below.

AP Registration

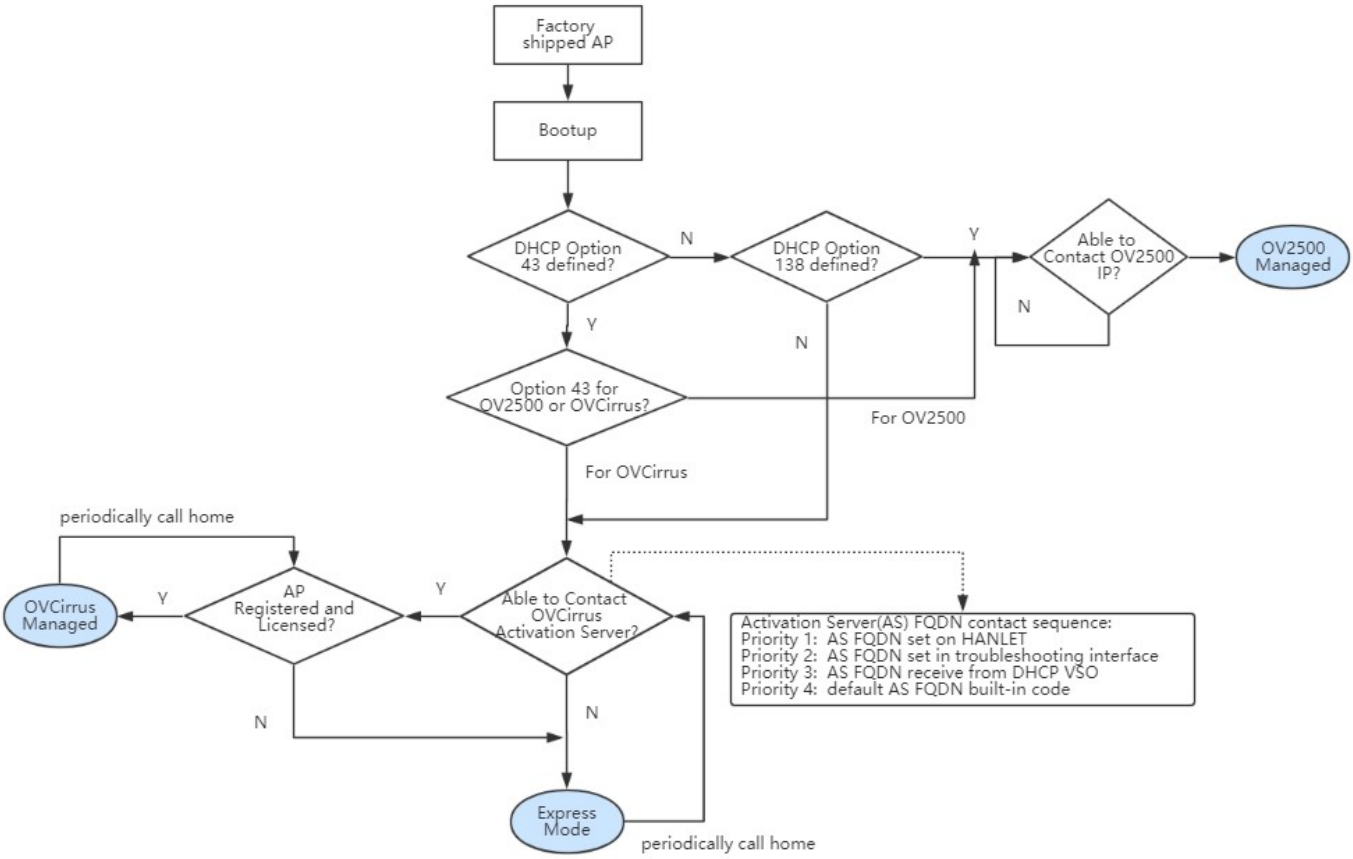


The following screens are used to register and configure Stellar AP Series Devices for OmniVista management.

- **Access Points -** Used to view and manage all discovered Stellar APs.
- **AP Group -** Used to view and manage Stellar AP Groups.
- **Certificate -** Used to view and configure AP Certificate Files. The Certificate File is used to establish a secure connection between OmniVista and APs when using the Web UI Device Management Tool.
- **External Captive Portal Config File -** Used to view and configure External Captive Portal Config Files. This file is used to establish a secure connection between OmniVista and an external captive portal server.
- **Location Service -** Displays configured WiFi Location Based Service (LBS) Profiles and is used to create, edit, and delete profiles.
- **Data VPN Servers** - Used to view and configure VPN Servers for Remote Access APs.

Stellar AP Bootup Sequence

The bootup sequence for Stellar AP Series Device is shown below. The diagram displays the bootup sequence for APs managed in Express Mode as well as APs Managed by OmniVista. The workflow for configuring APs for OmniVista management is shown in AP Device Management Workflow.



Stellar AP Series Device Management Workflow

The basic workflow for configuring Stellar AP Series Devices for OmniVista management is shown below.

1. Connect the AP to the network. The AP will contact, and register with, OmniVista and the APs will be displayed in the Unmanaged Access Points List.

2. Go to the Access Points Screen (Network - AP Registration - Access Points) and review the APs in the Unmanaged Access Points List.

3. Place the APs into "Trusted" status. Select the APs, then click on the checkmark icon at the top of the screen to place the APs into "Trusted" status. The APs will appear in the Managed Access Points List, as well as the Discovery Hardware Inventory Table. They will also be displayed in the Topology Physical Network Map and Default AP Group Map.

4. All APs are initially placed into the Default AP Group. You can manage the APs using the Default AP Group or you can go to the AP Group Screen to create a new AP Group and move specific APs in the new group. An AP can only belong to one AP Group.

5. To move APs into a new group, go back to the Access Points Screen. Select AP(s) that you want to move and edit the Group Name field to assign them to the new group.

Once an AP(s) is assigned to a group (including the Default AP Group), you can configure the APs in OmniVista (e.g., Notification Traps, Resource Manager Backups) by applying the configuration to the AP Group. In these applications (e.g., Notifications, Resource Manager), rather than presenting the user with individual APs when applying a configuration (as is done with AOS Devices), OmniVista presents the user with the option of applying a configuration to AOS Devices and/or AP Groups. Any configuration applied to an AP Group is applied to all APs in the group.

> **Note:** Stellar APs are connected to a PoE switch and the PoE switch physically connects to a router that provides DHCP service for both AP and WiFi users. If the AP receives Option 43, Sub-Option 1 from the DHCP server specifying ALE as the vendor, the AP will boot up and connect to OmniVista for management. When configuring your DHCP Server, specify the ALE Vendor ID "alenterprise" for Option 43, Sub-Option 1 (1:c:61:6c:65:6e:74:65:72:70:72:69:73:65:). For more information, see the *Alcatel-Enterprise OmniAccess Stellar User Guide*.

AP Device as an 802.1X Client

When an 802.1X (supplicant) device is connected to a UNP port on which 802.1X authentication is enabled, the switch will attempt to authenticate the device using 802.1X EAP frames. If after a configurable amount of time the device does not respond to the EAP frames sent by the switch, the device is identified as a non-802.1X (non-supplicant) device and undergoes MAC address authentication.

When a Stellar AP is connected to an OmniSwitch UNP port on which the AP Mode and 802.1X authentication is enabled, the switch starts to send EAP frames to the AP device. If the AP device does not respond to the EAP frames, the switch will identify the AP as a non-supplicant and will attempt to authenticate the AP with other methods. To ensure that the switch will identify the AP device as a supplicant (802.1X client), enable 802.1X functionality for the AP Group to which the AP belongs and specify an 802.1X client certificate to install on the APs in the group. A built-in 802.1X client certificate is provided by default or you can generate and upload a custom client certificate.

Note: OAW-AP1101 does not support the AP 802.1X client feature due to low flash size. All other APs, including other low-end APs (OAW-AP1201H, OAW-AP1201L, OAW-AP1201HL), support this feature.

Note: When an AP is operating as an 802.1X client, the AP does not support untagged WLAN/SSID/client and cannot participate in a Mesh deployment.

802.1X Authentication Use Cases

The following use case examples document the steps for configuring 802.1X authentication for the AP.

OmniVista UPAM 802.1X Server with Built-In Certificate on the APA

1. Enable 802.1X Supplicant functionality for the AP Group.
2. Select the Built-In Certificate from the drop-down menu.

OmniVista UPAM 802.1X Server with a Custom Client Certificate on the AP

1. Generate the client certificate (Cert, Private Key, CA cert) externally.
2. Import the client certificate into the UPAM database in OmniVista.
    a. Import the client certificate from AP Registration - Certificate menu and assign the certificate a name.
    b. Import the client CA certificate into UPAM - Settings - AP 802.1X Trust CA
3. Push the custom client certificate to the APs.
    a. Enable 802.1X Supplicant functionality for the AP Group.
    b. Select the custom certificate name that was imported in Step 2(a).

Use an External Radius 802.1x Server with Built-In Certificate on the AP

1. Download the UPAM Server CA certificate from UPAM - Settings - AP 802.1X Trust CA. This is the CA used to validate the AP as an 802.1x client. Import this CA into the external Radius server.
2. Push the built-in certificate to the APs.
    a. Enable 802.1X Supplicant functionality for the AP Group.
    b. Select the Built-in Certificate.

Use an External RADIUS 802.1X Server with a Custom Client Certificate on the AP

1. Generate the client certificate (Cert, Private Key, CA cert) externally.
2. Import the client CA certificate into the external RADIUS server database so the RADIUS server will trust the AP.
3. Push the custom client certificate to the APs.
    a. Import the client certificate from AP Registration - Certificate menu and assign the certificate a name.
    b. Enable 802.1X Supplicant functionality for the AP Group.
    c. Select the custom certificate name that was imported in Step 3(a).

802.1X Authentication with Username (AP MAC Address)

An 802.1X (supplicant) AP device can undergo certificate-based (see use cases above) or username-based 802.1X authentication. For username-based authentication, the user/pass = AP MAC address is configured in the UPAM database. When the AP MAC address attempting to authenticate matches the configured user/pass MAC address, UPAM returns a UNP profile/VLAN ID to the switch. This is often done when the user wants to assign a different VLAN based on the authentication result.

Note that when configuring username-based 802.1X authentication, the 802.1X Supplicant option for the AP Group should be set to "Off" and Secure Mode is enabled on the switch port. This will ensure that the switch will learn the AP MAC address and perform the 802.1X authentication according to the configuration (Access Auth Profile) on the switch.

AP Security Recommendations

- Do not rely on the Default Client Certificate on APs and the Default Server Certificate on UPAM. It is recommended that you install Custom Client Certificates on APs/AP Groups and a Custom Server Certificate on UPAM for improved security.
- It is recommended that you set up an 802.1x Failure Policy on the switch port depending on whether you want the AP (and its clients) to have connectivity to the network even if the AP fails 802.1x authentication; or if you want the AP (and its clients) to be completely blocked from network access if the AP fails 802.1x authentication.

Note: To learn about 802.1x authentication failures where AP is the client, check your RADIUS Server's Authentication Records.

Access Points

The AP Registration Access Points Screen displays information about all Stellar AP Series Devices known to OmniVista. The Access Points Screen is also used to review unmanaged APs and place them into "trusted" status, as well as edit, and delete APs. You can also configure APs to communicate with Zigbee devices (e.g., Assa Abloy door locks), perform an immediate discovery of Zigbee devices, and set the Zigbee device discovery Interval, reset an AP, reboot an AP, set an APs LED Mode, and perform certain actions on APs (e.g., open the Web UI Device Management Tool to manage an individual AP, view an AP in a Heat Map, view port information for an AP). You can also add Remote Access Points (RAP) - offsite, remote APs that can be managed from your local OmniVista Server through a VPN.

Important Note: OmniVista supports up to 4,000 APs. However, when applying a configuration to a large number of APs, (e.g., performing a backup in the Resource Manager application, applying Signature Profiles in the Application Visibility application), it is recommended that you apply the configuration to 500 APs at a time, and repeat if necessary.

Note: Stellar APs are connected to a PoE switch and the PoE switch physically connects to a router that provides DHCP service for both AP and Wi-Fi users. If the AP receives Option 138 from the DHCP server specifying the OmniVista Server IP, the AP will boot up and connect to the OmniVista Server for management. When configuring your DHCP Server, specify the OmniVista Server IP address for Option 138. For more information, see the *Alcatel-Enterprise OmniAccess Stellar User Guide.*

> **Note:** Remote APs require a VPN Server and an OmniVista Freemium Account. Click here for details on adding/configuring Remote APs. The Remote AP feature is supported on Stellar APs running AWOS 4.0.0.xx and higher.

An AP can be in one of two states - Managed and Unmanaged. Managed APs are licensed APs that have been "trusted" and are being managed by OmniVista. Unmanaged APs are APs that are not yet manageable, either because they are unlicensed, untrusted, or there is some configuration problem. These APs can be reviewed by a Network Administrator, who can resolve any problems and place them into a "managed" state, if desired.

Reviewing an AP

When APs are connected to the network, the AP automatically contacts, and registers with, the OmniVista Server. OmniVista initially classifies the AP as "unmanaged", adds it to the Default AP Group, and displays it in the Unmanaged Access Point List. The list may also contain APs that have been manually added but have not yet registered with OmniVista, unlicensed APs, and APs with a Country Code conflicts.

The Network Admin reviews the APs in the Unmanaged List and can place them into a "trusted" state. If the AP is registered, licensed, and there are no Country Code conflicts, the Network Administrator can place the AP into a "trusted" state. The AP will move to the Manageable Access Point List and can be managed by OmniVista. If there are license or country code conflicts, the AP is not eligible to be placed into a "trusted" state and these conflicts must be resolved before the AP can be placed into a "trusted" state.

> **Note:** The first time you open OmniVista, the "Init Registration App" window will appear. This is used to set certain basic pre-provisioning AP parameters (e.g., Country Code, Trust Status). Complete the fields in the window. This pre-provisioning procedure will only have to be done the first time you open the AP Registration application. The configuration will automatically be applied to any subsequent APs you add.

APs must be “trusted” to be managed by OmniVista. The “Trust All” field in the Init Registration App" window is enabled by default. This can be convenient when initially adding a large number of APs. If you would like to exercise administrative intervention before accepting new APs, you might want to click on the Trust All" icon (lock in unlocked position) at the top of the Access Points screen to toggle the setting back to “Untrust All” (lock in locked position).

Trusted/Untrusted APs

APs must be licensed and in a "trusted" state to be managed by OmniVista. To place an "untrusted" AP into a "trusted" state, select the AP(s) in the Unmanaged AP List and click on the "Change to Trust Status" icon (circle with checkmark) at the top of the screen and click **OK** at the Confirmation prompt. The AP will be moved to the Managed AP List.

To place a "trusted" AP into "untrusted" status, select the AP(s) in the Managed AP List and click on the "Change to Untrusted Status" icon (circle with line) at the top of the screen and click **OK** at the Confirmation prompt. The AP will be moved to the Unmanaged AP List.

You can also set the default "trust" behavior for any APs that are added and licensed using the "Trust All/Untrust All" icon at the top of the screen (lock icon). If set to "Trust All" icon (lock in unlocked position), any APs that are added and licensed are automatically "trusted". If set to "Untrust All" (lock in locked position), any APs that are added and licensed are automatically "untrusted" and will have to be manually set to "trusted" for management. Click on the icon to toggle to "Trust All" or "Untrust All".

License Conflict

If there are no licenses available for a registered AP, you must free up licenses by deleting an AP or purchase additional license before you can manage the AP. Once this is resolved, you can move the AP to the "trusted" state and manage the AP with OmniVista.

Country Code Conflict

Wireless regulations vary by country, so APs are configured and shipped based on the country's regulations. The Country Code configured for the AP Group used to manage these APs must match the country code for the APs it is managing. If they do not match, the APs will remain in the Unmanageable Access Point List until the problem is resolved.

For the most part, this should not be a problem. When you install OmniVista, you select the Country Code as part of the installation process. So if you are managing APs in the U.S., you will configure the OmniVista Country Code as "US" during installation. The Default AP Group is then configured with a "US" RF Profile and by default, APs are initially assigned to this profile.

A problem will occur if you selected the wrong Country Code during installation. If this is the case, you must modify the RF Profile for the Default AP Group to match the Country Code Configured in OmniVista. Go the RF Profile Screen (WLAN - RF - RF Profile), select the default RF Profile and modify the Country Code to match the Country Code configured during OmniVista installation.

A second scenario that will cause a Country Code conflict is if you are using OmniVista to manage AP in two countries (e.g., U.S. and Canada). In this case, you would have to configure two different AP Groups with different RF Profiles - a U.S AP Group with a U.S. RF Profile and a Canadian AP Group with a Canadian RF Profile. You would then assign the U.S. APs to the U.S. AP Group and the Canadian APs to the Canadian AP Group. Click here for more information on configuring AP Groups.

Adding an AP

When Stellar AP Series Devices are connected to a switch, the AP automatically contacts, and registers with, the OmniVista Server. It is then displayed on the Unmanaged Access Point List, where a Network Admin can review it before moving it to the Managed Access Point List. However, you can manually add an AP and configure its AP Group and RF Profile in OmniVista before the AP is connected to the network. When that AP is later connected to the network, OmniVista will automatically recognize and configure it, and move it to the Managed Access Point List. You can manually add a single AP, or perform a batch import of multiple APs by importing an Excel or .csv file.

Adding a Single AP

APs are manually created using the Unmanaged Access List screen. From the Unmanaged Access List Screen, click on the Add icon and complete the fields as described below.

- **AP MAC -** The MAC address of the AP.
- **AP Name -** A user-configured name for the AP.
- **AP Location -** The location of the AP. If you check the **Get location for LLDP** the AP will automatically get its location from LLDP. (1 - 255 characters, no special symbols except “,”and “/”)
- **Group Name -** The group to which the AP will belong. Select an AP Group from the drop-down menu containing existing groups, or click on the Add icon in the drop-

down to go to the AP Group Screen and create a new group. You can the return to the Access Points Screen and create the AP. If you do not select an AP Group, the AP will be assigned to the Default AP Group. You can edit the AP at any time to move it to another group.

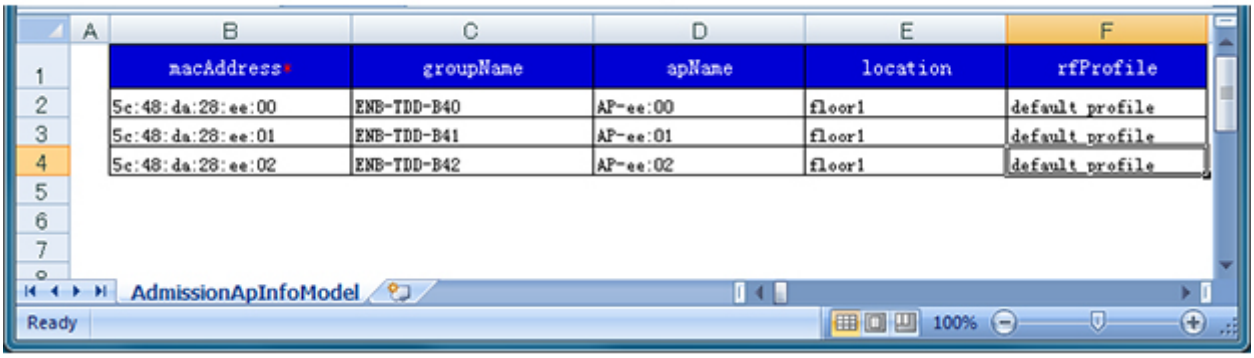
- **RF Profile -** The RF Profile assigned to the AP. Select an RF Profile from the drop-down menu containing profiles, or click on the Add icon in the drop-down to go to the RF Profile Screen and create a new profile. You can the return to the Access Points Screen and create the AP. If you do not select an RF Profile, the AP will be assigned to the Default RF Profile. Note that APs in the same AP Group can have different RF Profiles, However, the Country Code parameter in the RF Profile must be the same for all APs in an AP Group.

Adding Multiple APs

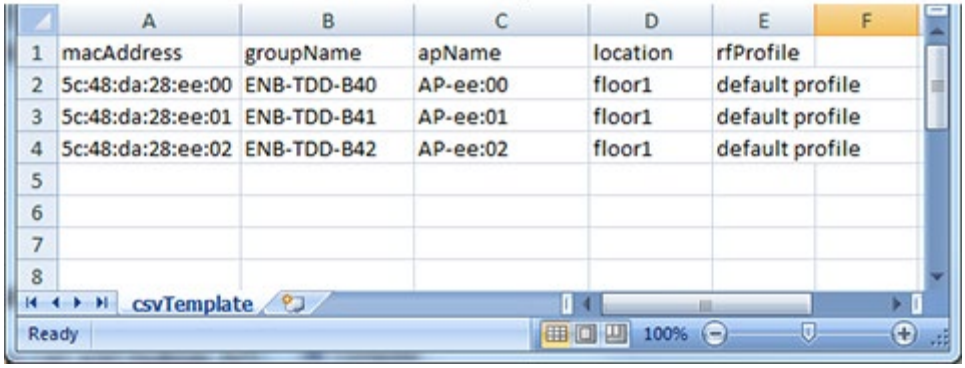
You can add multiple APs at once by importing an Excel or CSV file containing AP information. Click on the **Upload .csv/.xsl** button at the top of the Unmanaged Access Point List. The Import File Screen will appear. Click on the **Upload File** button and locate the Excel or CSV File. Click on the **Import** button to Import the file to OmniVista. The files must follow a specific format and template.

If necessary, click on the **Template** button to import an Excel and a CSV Template (both templates are contained in a Zip File). Each template has formatted sample information that you can use to create your import file. Both templates can be opened using Excel. The format required for each file type is shown below.

Excel Template



CSV Template



Imported APs are "trusted" and are displayed in the Managed Access Point List. If there is a problem with an AP (e.g., wrong Country Code, a license is not available), the AP will appear in

the Unmanaged Access Points List until the problem is resolved. See Reviewing an AP for more information.

Editing an AP

You can edit an AP to change an AP's IP mode and address, edit and APs Scanning Mode, migrate an AP to another OmniVista Server, and configure other AP options. Select an AP in the Access Points List, click on the Edit icon, then select Edit Basic Info, Edit IP Mode, Edit Dedicated Scanning Mode, Edit IoT Radio Configuration, Edit Radio Configuration, Migrate to Other OV, Edit Mesh Configuration, Web Content Filtering, AP Configuration Update, or Location/Advanced Analytics Server.

Edit Basic Information

Select an AP and select **Edit Basic Info**. The AP Information Edit Screen appears. Edit the fields as described below, then click on the **Apply** button.

- **AP MAC -** The MAC address of the AP. Display only. Cannot be edited.
- **AP Name -** A user-configured name for the AP.
- **AP Location -** The location of the AP. If you select the “Get location for LLDP” checkbox, OmniVista will use LLDP to automatically add the location.
- **Group Name -** The group to which the AP will belong. Select an AP Group from the drop-down menu containing existing groups, or click on the Add icon in the drop-down to go to the AP Group Screen and create a new group. You can the return to the AP Information Edit Screen and edit the AP Group Name field with the new AP Group. Note that if you edit an AP's Group, the AP will automatically reboot for the change to take effect.
- **Group Description -** User-configured AP Group description. Display only. Cannot be edited.
- **RF Profile -** The RF Profile assigned to the AP. Select an RF Profile from the drop-down menu containing profiles or click on the Add icon in the drop-down to go to the RF Profile Screen and create a new profile. You can the return to the AP Information Edit Screen and edit the RF Profile field with the new profile. Note that APs in the same AP Group can have different RF Profiles, However, the Country Code parameter in the RF Profile must be the same for all APs in an AP Group.

Edit IP Mode

When you select **Edit IP Mode**, the Edit IP Mode Screen appears. Edit the fields as described below then click on the **Apply** button.

Note: OmniVista obtains and saves the IP address information reported by the Access Point. When you make any changes to the IP mode, the changes are pushed directly to the Access Point; however, the Edit IP Mode screen may still display the previous IP address information until OmniVista receives the updated information from the Access Point.

- **IP Mode**
  - **DHCP -** Obtain the IP address from a DHCP Server.
  - **Static -** Configure a Static IP address by completing the fields below.
- **IP -** The IP address for the AP.
- **Netmask -** The IP address network mask for the AP.

- **Default Gateway -** The default gateway used for AP forwarding.
- **Preferred DNS -** The IP address of the DNS Server used by the AP.
- **Alternate DNS -** The IP address of the alternate DNS Server used by the AP.

Edit Dedicated Scanning Mode

Wireless networks operate in environments with electrical and radio frequency devices that can interfere with network communications. You can set APs to examine the radio frequency environment in which the Wi-Fi network is operating, identify interference, and classify its sources. An analysis of the results can then be used to quickly isolate issues with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel.

Generally, APs perform background scanning as well as serving wireless clients connecting to the network (AP Mode). With the help of background scanning, we can detect the interference and attacking from foreign devices and provide corresponding containment to protect the network by sending De-authentication packets.

When you set an AP to "Scanning Mode", the AP is dedicated to working in Wi-Fi scanning among channels. No clients can associate with the AP. In "Scanning Mode", foreign devices around the network are continuously detected and strongly contained. At the same time, the condition of the Wi-Fi channels is monitored, and you can learn about the Wi-Fi environment quality on the RF Scan View Screen (WLAN - RF Management - RF Scan View). You can also select an AP in the Access Point List, click on the **Actions** button and select **RF Scan View** to go to the RF Scan View Screen and view information about a specific AP.

Select an AP(s) in the Access Point List, click on the Edit icon and select **Edit Dedicated Scanning Mode**. The Edit Dedicated Scanning Mode window appears with the MAC Addresses of the selected AP(s) in the MAC Address field. Select the applicable radio button, then click **Apply**.

- **Once** - Select this radio button and click on **Yes** at the Confirmation prompt. The AP(s) will temporarily be set to "Scanning Mode" and will perform a scan one time before returning to the default AP Mode. The scan may take up to five (5) minutes and no clients will be able to associate with the AP during the scan. The results of the scan can be viewed on the RF Scan View Screen (WLAN - RF Management - RF Scan View).
- **Always -** Select this button to set the AP(s) to "Scanning Mode" for an extended period of time. The APs will remain in "Scanning Mode" until you turn it off. You can deploy a new AP or change an existing AP in your network to work in Scanning Mode for monitoring and analysis of the Wi-Fi environment. The results of the scan can be viewed on the RF Scan View Screen (WLAN - RF Management - RF Scan View).
- **Off -** Select this button to turn off "Scanning Mode" and return the AP to the default AP Mode.

Edit IoT Radio Configuration

If an AP supports the IoT Radio function, the **Edit IoT Radio Configuration** option will be activated. The IoT Radio Configuration is used to configure Zigbee Devices and BLE. Set the **Use Private Config** button to **On** to configure Zigbee or BLE.

Note: This configuration will take precedence over the IoT Radio configuration for the AP set in the AP Group configuration.

Zigbee Configuration

OmniVista can be used to monitor and enable/disable supported Zigbee devices (e.g., Assa Abloy door locks). However, supported APs must be configured to discover and connect to Zigbee devices. The IoT application is used to monitor and manage Zigbee devices (Network - IoT - Inventory). See the IoT Inventory help for more information for more information, including setting up OmniVista to support Zigbee devices.

By default, the "Use Private Config" option is off and the Zigbee configuration is derived from the AP Group to which the AP belongs. If you want to configure private Zigbee parameters for a **single** AP, enable " Use Private Config" and specify the private settings. If the "Use Private Config" option is turned off at a later time, the private Zigbee configuration is removed from the AP the AP Group settings are pushed to the AP or BLE Gateway.

To configure Zigbee parameters for a single AP, set the **Use Private Config** button to **On**, set the **IoT Radio Mode** to **Zigbee**, complete the fields as described below, then click the **Apply** button.

- **Channel Setting -** The wireless channel used to communicate with the Zigbee device. It is recommended that you use a different channel than the channel used for the WLAN.
- **PAN ID -** The Personal Area Network (PAN) that the Zigbee device is connected to. A PAN is wireless network that communicates on the 2.4GHz Band. The PAN-ID for the AP (BLE Gateway) is automatically generated using last two bytes of the AP MAC address by default. To avoid conflict, it is not recommended that you set the PAN-ID manually. If it is necessary, make sure the configured value is unique. (Range = 1 - 65534)
- **Device Discovery -** Enables/Disables automatic discovery of Zigbee devices (Default = On).
- **Discovery Duration -** The frequency of automatic discovery of Zigbee devices, in seconds (Range - 60 - 900, Default = 120).
- **Use Vendor ID -** Enables/Disables the specified Zigbee Vendor OUI (below). When enabled, OmniVista can communicate with the Zigbee device specified by the MAC OUI. To communicate with supported door locks, you **must** enable this field. The Vendor OUI is pre-filled with the MAC OUI for supported door locks (00:17:7A).
- **Vendor OUI -** The Zigbee Vendor OUI. This field is pre-filled with the MAC OUI for supported door (00:17:7A).
- **Auto-Accept MAC OUI -** You can click on the Add icon and add MAC OUIs here to "Auto-Accept" and enable Zigbee end devices. Do **not** enter the MAC OUI for supported door locks. These devices must be "Manually Accepted" and enabled in the Zigbee Devices Table on the IoT Inventory Screen.

BLE Configuration

By default, the "Use Private Config" option is off and the BLE configuration is derived from the AP Group to which the AP belongs. If you want to configure private BLE parameters for a single AP, enable " Use Private Config" and specify the private settings. If the "Use Private Config"

option is turned off at a later time, the private BLE configuration is removed from the AP the AP Group settings are pushed to the AP or BLE Gateway.

To configure BLE for a single AP, set the **Use Private Config** button to **On**, set the **IoT Radio Mode** to **BLE**, complete the fields as described below, then click the **Apply** button.

- **Advertising**
  - **Advertising -** Enables/Disables the BLE advertising function for the AP. If enabled, the AP will broadcast BLE packets. If Advertising is enabled, the AP will broadcast BLE packets. BLE Advertising is optional for Asset Tracking. If disabled, the AP will detect surrounding BLE Tags/Beacons and will report information to the server for analysis.
  - **Emission Frequency -** The time circle during which the BLE packets will be broadcast, in milliseconds. (Range = 20 - 9,000,000, Default = 200)
  - **Tx Power -** The transmit power used to broadcast BLE packets, in dBm. (Range = -20 - 10, Default = 4)
  - **Tx Channel -** The transmit channel used to broadcast BLE packets. It is recommended that you use a different channel than the channel used for the WLAN.
  - **Advertising Protocol -** Specify the BLE protocol used to define the broadcasting BLE beacon format.
    - **iBeacon -** Apple iBeacon format.
    - **Eddystone-URL -** Google Eddystone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.
    - **Eddystone-UID -** Google Eddystone format. A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
      - **Namespace -** 20 characters containing 0-9a-f.
      - **Instance ID -** 12 characters containing 0-9a-f.
- **Scanning**
  - **Scanning -** Enables/Disables the Bluetooth beacon scanning function for the AP.
  - **Scanning Interval -** The Bluetooth scanning interval for the AP, in milliseconds. (Range = 4 -10240, Default = 100)
  - **OUI Allowlist -** Specify the MAC OUI Allowlist to filter devices for BLE beacon broadcasting. Only those beacons broadcasting from the devices within the OUI Allowlist are valid and will be reported.

Edit Radio Configuration

Select an AP(s) and click on the **Edit Radio Configuration** option to edit an AP's radio frequency.

- **APs MAC List -** Lists the MAC address(es) of the selected AP(s).
- **Use Private Config -** Enable the **Use Private Config button** to configure the selected AP's radio to a different setting than the one configured in the AP Group to which the AP belongs. This will take precedence over the radio band configured for the AP in the AP Group configuration.

Migrate to Other OV

When you select **Migrate to Other OV**, the Migrate to Other OV Screen appears with the selected AP's MAC address in the APs MAC List field. Enter the IP address the OmniVista Server to which you want to migrate the AP and click on the **Apply** button. The AP will be released from your OmniVista Server and migrate to the other server, where it will be displayed in the Unmanaged AP Tab. The Administrator of the other OmniVista Server can then license and configure the AP.

Edit Mesh Configuration

The Edit Mesh Configuration Screen is used to configure the Mesh configuration for an AP. Select an AP in the Access Points List and select **Edit Mesh Configuration**. Complete the fields as described below, then click on the **Apply** button.

- **Enable** - Select the "Yes" radio button to enable the AP to operate as a wireless Mesh node.
- **Is Root** - Select the "Yes" radio button if the AP will serve as the root of the Mesh network.
- **SSID** - Edit the name of the SSID for the Mesh network.
- **Band** - The radio band for the Mesh network (2.4G, 5G, or 6G).
- **Encryption Type** - Select the type of encryption to use for the connections between Mesh/Bridge APs from the drop-down list. The list will present only the encryption types that are supported by the AP model. For example, if the AP supports only two of the following encryption types, then only those two types will appear in the drop-down list.
    - **Both(WPA & WPA2)**
    - **WPA-2-Personal**
    - **Both(WPA2 & WPA3)**
    - **WPA-3-Personal**
- **Mcast Rate** - The Multicast rate that is applied to "Multicast Video Stream" to help reduce jitters in a Mesh environment. Select the rate to apply to Multicast traffic from the drop-down menu (6, 12, 24, 36, 48, or 54, Default = 24).
- **Passphrase** - Enter the passphrase for the Mesh network.
- **Confirm passphrase** - Re-enter the Mesh network passphrase.
- **Mode** - The AP is operating (Mesh or Bridge).

Configuring the Mesh configuration for an AP is particularly useful for an out-of-the-box Mesh configuration. Out-of-the- box Mesh is a feature that helps you quickly set up a Mesh network without configuring the out-of-box APs. The out-of-box APs will establish a Mesh network with hardcoded settings. You only need to specify the Mesh root, then other APs will establish a Mesh configuration automatically.

Web Content Filtering

Web Content Filtering (WCF) enables you to allow/deny Stellar AP access to web sites based on specific security or content filters (e.g., Malware Sites, Gambling). WCF Profiles, configured on the WCF Profile Screen (UPAM - Web Content Filtering - WCF Profile), contain the

condition(s) and actions to allow/deny access to these sites. A WCF Profile is included as part of an Access Role Profile or SSID and pushed to an AP Group(s). However, Web Content Filtering must first be enabled on an AP(s).

- **APs MAC List -** Lists the MAC address(es) of the selected AP(s).
- **Use Private Config -** Web Content Filtering is disabled by default. Enable the **Use Private Config** button to enable/disable Web Content Filtering on the selected APs. This will take precedence over the Web Content Filtering administrative state configured for the AP(s) in the AP Group configuration.
- **Web Content Filtering -** Enables/Disables Web Content Filtering on the selected AP(s).

Web Content Filtering can be enabled at the individual AP or AP Group Level. If enabled at the AP Group level, all APs in the group that support Web Content Filtering are enabled. However, you can override that configuration on individual APs in a group by editing an AP here.

AP Configuration Update

The AP Configuration Update option is an expert tool that can be used to update AP wireless parameters. Complete the fields as described below, then click on the **Apply** button**.**

- **APs MAC List** - Enter the MAC address of the AP to which you want to push the configuration.
- **Operation** - Select one of the following:
  - **Add New Configuration** - Push the WLAN or RF configuration to the AP. The new configuration is applied after the next AP reboot or reload.
  - **Clear Configuration** - Clear the WLAN or RF configuration from the AP. The configuration is cleared after the next AP reboot or reload.
- **Configuration Detail** - Enter the WLAN or RF configuration in JSON format.

Using the AP Configuration Update option to update AP WLAN and RF parameters is particularly useful for troubleshooting purposes. Contact ALE Support for this function, if necessary.

Location/Advanced Analytics Server

This option is used to enable location and advanced analytics for a specific AP(s). When you select this option, you are taken to the Location/Advanced Analytics Server Screen. The MAC address(es) of the selected AP(s) are displayed in the APs MAC List. Enable **Use Private Config** to enable the following options:

- **OmniVista Cirrus WiFi RTLS -** If enabled, AP(s) sends real-time location data to OmniVista Cirrus 10.1 and above to provide Wi-Fi RTLS services.
- **OmniVista Cirrus Advanced Analytics -** If enabled, AP(s) sends itself and client data to OmniVista Cirrus 10.1 and above to provide Wi-Fi advanced analytics services.

Deleting an AP

You can delete an AP from OmniVista, for example, to free up AP Licenses. Select the AP(s) in the Access Point List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Resetting an AP

You can reset an AP by selecting the AP(s) in the Access Points List and clicking on the **Reset APs** button. The AP will reset to the factory default configuration and reboot. When an AP is rebooted as part of a reset, the latest configuration available on OmniVista is downloaded to the AP. If the AP is unable to connect to OmniVista, the AP will come up with the factory default configuration.

Zigbee Device Discovery

When Zigbee Mode is enabled on a supported Stellar AP, the AP automatically discovers and connects to Zigbee devices based on the configured Discovery Interval. However, you can select an AP(s) in the Access Points List and click on the **Zigbee Discovery** button at any time to have the selected AP(s) immediately scan for Zigbee devices. You can also change the Discovery Interval setting for an AP(s). Select an AP(s) and click on the **Zigbee Discovery** button. Set the new **Discovery Interval**, and click on the **Apply** button. The selected AP(s) will immediately scan for Zigbee devices and the new Discovery Interval will take effect. (Range - 60 - 900, Default = 120).

Rebooting an AP

You can manually reboot an AP by selecting the AP(s) and clicking on the **Reboot** button at the top of the screen. When an AP is rebooted, the latest configuration available on OmniVista is downloaded to the AP. If the AP is unable to connect to OmniVista, the AP will reboot with the latest saved local configuration.

Setting the AP LED Mode

You can set the LED mode on an AP by selecting the AP(s) in the Access Point List and clicking on one of the LED Mode buttons at the top of the screen.

- **Normal Mode** (Default) **-** The LED displays in normal mode (Red/Green/Blue).
- **Night Mode -** The LED indicator is shut off.
- **Blink Mode -** LED alternately blinks Red/Green/Blue so that you can visually locate the AP(s).

LED Indicators

The LED light on the AP indicates the following conditions:

- RED (Flashing) - System abnormal, link down
- RED (Solid) - System startup
- RED and BLUE (Rotate Flashing) - OS upgrading
- BLUE (Solid) - System running, dual bands working
- GREEN (Flashing) - No SSID created
- GREEN (Solid) - System running, single band working
- RED, BLUE, and GREEN (Rotate Flashing) - System running (used to visually locate an AP).

Performing Actions on an AP

You can perform certain actions/configurations on an AP(s). Select an AP(s), click on the **Actions** drop-down, and select an action. Note that some action may not be available depending on the AP model or whether you select a single AP or multiple AP. The following actions are available: AP Web, Heat Map, Port Management, and RF Scan View.

Using the Web UI Device Management Tool

You can connect to individual Stellar APs using the Web UI Device Management Tool. The tool can be used to view and configure certain management parameters on an individual AP. Select an AP in the Access Point List. Click on the **Actions** drop-down and select **AP Web**. The Login page for the Web UI Management Tool will appear. The password is set on the AP Group Screen (AP Web configuration).

Viewing an AP in a Heat Map

You can view a Stellar AP in an existing Heat Map. Select the AP in the Access Point List. Click on the **Actions** drop-down and select **Heat Map**. The Heat Map application will open to the Heat Map containing the selected AP.

Viewing AP Downlink Ports

You can view port information and enable/disable downlink ports on OAW-1201H APs. Select an AP(s) in the Access Point List. Click on the **Actions** drop-down and select **Port Management**. The Inventory Ports Screen will appear with the ports from the selected AP(s) displayed.

Viewing Radio Frequency Scan Mode Information

You can view scanning mode data for an AP. Select and AP in the Access Points List. Click on the **Actions** drop-down and select **RF Scan View**. The RF Management RF Scan View Screen will appear, displaying data for the selected AP.

Access Point List

The Access Point List displays basic information about Managed and Unmanaged APs, as well as information on Bridge APs. You can also configure and apply a default configuration to Bridge APs. Click on the applicable tab to display basic information. Click on a device to display detailed information for the device. You can also filter the Unmanaged AP List by category.

Managed/Unmanaged APs

Basic Information

- **Up Time -** The amount of time the AP has been "Up" since the last time it was "Down" or rebooted.
- **AP Name -** Name of the AP.
- **Status -** The AP status:
    - **Up -** AP is reachable.
    - **Down -** AP is not reachable.

  - **Unknown -** The AP has not been seen yet (AP was manually created/imported).
- **IP Address -** The IP address of the AP.
- **AP Version -** The AP OS version.
- **AP Model -** The model type of the AP (e.g., OAW-AP1221, OAW-AP1251).
- **Group Name -** The AP Group to which the AP belongs.
- **AP MAC -** The MAC address of the AP.
- **BLE MAC -** The MAC address for the AP beacon, if applicable.
- **IP Mode -** The mode used to obtain the AP IP address (DHCP or Static).
- **Default Gateway -** The default gateway used for AP forwarding.
- **Subnet Address -** The IP subnet address of the AP.
- **AP Location -** The AP location currently assigned in the AP. There are two location modes:
  - **LLDP Mode (Default) -** The location is retrieved from the LLDP ALE TLV.
  - **Fixed/User String Mode -** The location is hard coded with a user sting.
- **Country Code -** The AP Country Code.
- **Management VLAN ID -** The VLAN used to manage the AP.
- **RF Profile -** The RF Profile applied to the AP.
- **Static Neighbor AP -** The neighbor AP to which the connected wireless client might roam. In the detailed view, you can click on the number of neighbors for detailed information on the AP's neighbors.
- **Saved/Unsaved -** Indicates whether or not the current AP configuration has been saved to OmniVista (Saved/Unsaved).
- **LED Model -** The LED Mode configured for the AP.
- **DNS -** The IP address of the DNS Server used by the AP.
- **Channel -** The radio frequency working channel for the AP.
- **Noise Floor -** The measure of the signal created from the sum of all noise sources and unwanted signals within a measurement system, where noise is defined as any signal other than the one being monitored.
- **Channel Utilization -** The utilization of the working channel on the AP, which indicates the wireless resource.
- **EIRP -** The Effective Isotropically Radiated Power radio frequency for the AP.
- **LACP Status -** Indicates whether or not the AP supports link aggregation (Supported/Unsupported).
- **Link Status -** The LACP link status (Up/Down).
- **Work Mode -** The AP Work Mode:
  - **AP Mode -** AP serving wireless clients
  - **Mesh Mode -** AP is working as a wireless mesh node.
  - **Bridge Mode -** AP is working as a wireless bridge node.
- **Channel Width -** The channel width of the AP.
- **Client Count -** The number of clients connected to the AP.

- **Web Content Filtering -** The administrative status of Web Content Filtering on the AP.
- **Group Description -** An optional user description for the AP Group.

Detailed Information

General

- **AP Name -** Name of the AP.
- **Group Name -** The AP Group to which the AP belongs.
- **Group Description -** An optional user description for the AP Group.
- **AP MAC -** The MAC address of the AP.
- **BLE MAC -** The MAC address of the BLE AP, if applicable.
- **Status -** The IP reachability of the AP (Up/Down).
- **IP Mode -** The mode used to obtain the AP IP address (DHCP or Static).
- **IPv4**
  - **IP Address -** The IPv4 address of the AP.
  - **Subnet Address -** The IPv4 subnet address of the AP.
  - **Default Gateway -** The Ipv4 default gateway used for AP forwarding.
  - **DNS -** The IPv4 address of the DNS Server used by the AP.
- **IPv6**
  - **IP Address -** The IPv6 address of the AP.
  - **Default Gateway -** The IPv6 default gateway used for AP forwarding.
  - **DNS -** The IPv6 address of the DNS Server used by the AP.
- **Work Mode -** The AP Work Mode:
  - **AP -** AP serving wireless clients.
  - **Mesh -** AP is working as a wireless mesh node.
  - **Bridge -** AP is working as a wireless bridge node.
- **AP Model -** The AP model type (e.g., OAW-AP-1101).
- **AP Version -** The AP OS version (e.g., 3.0.3.22).
- **AP Location -** The location where the AP is installed.
- **AP Geo Location -** The AP Geo Location, if applicable.
- **Client Count -** The number of clients connected to the AP.
- **Neighbor AP -** Click on the "View" link to display a list of neighbors APs to which the connected wireless client might roam. The list includes static and automatically-discovered neighbors.
- **Source of LLDP -** The source of the AP location information (LLDP protocol or manually configured).
- **Last Registration Time -** The date and time that OmniVista received the AP's last registration request packet.
- **Discovered Time -** The date and time the AP was discovered in the Discovery application.

- **Uptime -** The amount of time the AP has been "Up" since the last time it was "Down" or rebooted.
- **Management VLAN ID -** The VLAN used to manage the AP. This is the VLAN ID retrieved from the 802.1ab “Port Vlan Id” TLV.
- **LED Model -** The LED Mode configured for the AP.
- **Country Code -** The AP Country Code.

Status

- **Channel -** The radio frequency working channel for the AP.
- **Noise Floor -** The measure of the signal created from the sum of all noise sources and unwanted signals within a measurement system, where noise is defined as any signal other than the one being monitored.
- **Channel Width -** The channel width of the AP.
- **Channel Utilization -** The utilization of the working channel on the AP, which indicates the wireless resource.
- **EIRP -** The Effective Isotropically Radiated Power radio frequency for the AP.
- **LACP Status -** Indicates whether or not the AP supports link aggregation (Supported/Unsupported).
- **Link Status -** The LACP link status (Up/Down).
- **Saved/Unsaved -** Indicates whether or not the current AP configuration has been saved to OmniVista (Saved/Unsaved).

Radio Configuration

- **RF Profile -** The RF Profile applied to the AP.
- **Use Private Config -** Administrative State of Private Config option (Enabled/Disabled).

IoT Radio Configuration

- **Use Private Config -** Administrative State of Private Config option for BLE or IoT (Enabled/Disabled). If enabled, the IoT Radio can be configured for BLE or Zigbee.
- **IoT Radio Mode -** The IoT Radio Mode (BLE or Zigbee).

Zigbee Configuration

- **Channel Setting -** The wireless channel used to communicate with the Zigbee device.
- **PAN ID -** The Personal Area Network (PAN) that the Zigbee device is connected to. A PAN is wireless network that communicates on the 2.4GHz Band. By default, the PAN-ID for the AP (BLE Gateway) is automatically generated using last two bytes of the AP MAC address by default. (Range = 1 - 65534)
- **Device Discovery -** The administrative status of automatic discovery of Zigbee devices (On/Off, Default = On).
- **Discovery Duration -** The frequency of automatic discovery of Zigbee devices, in seconds (Range - 60 - 900, Default = 120).

- **Use Vendor ID -** The administrative status of using the Zigbee Vendor MAC OUI to communicate with Zigbee devices (On/Off, Default = Off).
- **Vendor OUI -** The Vendor MAC OUI (supported door lock OUI is 00:17:7A).
- **Auto-Accept MAC OUI -** A list of MAC OUIs on the AP Allowlist. If a Zigbee device is on this Allowlist, it will be "Auto-Accepted" and enabled.

BLE Configuration

- **Advertising**
  - **Advertising -** The administrative state of the BLE advertising function for the AP. If enabled, the AP will broadcast BLE packets. (Enabled/Disabled)
  - **Emission Frequency** - The time circle during which the BLE packets will be broadcast, in milliseconds. (Range = 20 - 9,000,000, Default = 200)
  - **Tx Power -** The transmit power used to broadcast BLE packets, in dBm. (Range = -20 - 10, Default = 4)
  - **Tx Channel -** The transmit channel used to broadcast BLE packets.
  - **Advertising Protocol -** Specify the BLE protocol used to define the broadcasting BLE beacon format.
    - **iBeacon -** Apple iBeacon format.
    - **Eddystone-URL -** Google Eddystone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.
    - **Eddystone-UID -** Google Eddystone format. A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
      - **Namespace -** 20 characters containing 0-9a-f.
      - **Instance ID -** 12 characters containing 0-9a-f.
- **Scanning**
  - **Scanning -** The administrative state of the Bluetooth beacon scanning function for the AP. (Enabled/Disabled)
  - **Scanning Interval -** The Bluetooth scanning interval for the AP, in milliseconds. (Range = 4 -10240, Default = 100)
  - **OUI Allowlist -** Specify the MAC OUI Alowlist to filter devices for BLE beacon broadcasting. Only those beacons broadcasting from the devices within the OUI Allowlist are valid and will be reported.

VPN Settings

- **Management VPN -** The VPN tunnel between the AP and OmniVista. Through the management VPN, an AP can be managed by remote OmniVista Server instance which could be across the public Internet.
  - **Server's Public IP -** The management VPN server’s public IP address.
  - **Server's Port -** The management VPN server’s port.
  - **Server's VPN IP -** The management VPN server’s VPN IP address.
  - **AP's VPN IP -** The AP’s VPN IP address which will be used to establish the management VPN connection.

- **Data VPN -** The VPN tunnel between the AP and the VPN Server. The VPN Server could be deployed in different place than the OmniVista Server. The Data VPN is used to carried user traffic rather than AP management packets.
    - **Data VPN Name -** The name of the Data VPN
    - **AP's VPN IP -** The AP's VPN IP address, which is used to establish the Data VPN connection.
    - **AP's Public Key -** The AP's public key used to encrypt the data in the VPN tunnel.
    - **AP's Private Key -** The AP's private key used to encrypt the data in the VPN tunnel.

Web Content Filtering

- **Use Private Config -** The administrative status of "private config" on the AP. If Private Config is enabled, you can set the Web Content Filtering administrative state for the AP. This will take precedence over the Web Content Filtering setting in the AP Group configuration.
- **Web Content Filtering -** The administrative status of Web Content Filtering on the AP.

Certificate Information used in 802.1X Supplicant on AP Management Port

This section is shown only when the AP belongs to an AP Group on which 802.1X Supplicant authentication is turned on. See AP Device as an 802.1X Client for more information.

- **Certificate File Name -** The name of the certificate file.
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -**Validity ending time of the certificate file.
- **Expiry Status -** The expiration status of the certificate.
- **Issued by -** The certification authority (CA) that issued the certificate.
- **Issued to -** The entity to which the certificate is assigned.

Bridge APs

The Bridge AP tab displays information on APs working in wireless bridge mode. You can set and apply certain global default configurations to Bridge APs

- **Bridge Name -** Name of the bridge AP.
- **Bridge MAC -** MAC address of the bridge AP.
- **Status -** Link status of the wireless bridge connection.
- **IP Address -** IP address of the bridge AP.
- **SSH Login -** SSH Login administrative status (Enabled/Disabled).
- **AP Web -** AP Web Management administrative status (Enabled/Disabled).
- **Web Server Certificate -** The certificate used for communication between the Web Server of the Bridge AP and browser.
- **Use Default Certificate -** Indicates whether the bridge AP's SSH/AP Web/Web Server Certificate setting is same as the Default Configuration (Yes/No).
- **Far End AP IP -** The IP address of the upper node of the bridge link (not displayed if AP is the root AP in the bridge).

- **Far End AP MAC -** The MAC address of the upper node of the bridge link (not displayed if AP is the root AP in the bridge).

Bridge AP Default Configuration

You can set and apply certain global default configurations to Bridge APs. To set these default configurations click on the **Default Configuration** button at the top of the Bridge Access Point List, complete the fields below, then click on the **Apply** button. Once a Bridge AP comes online, these default configurations are applied to the AP. You can also apply the default configuration to APs in the Bridge Access Point List by select the AP(s) and clicking on the **Apply Default Configuration** button.

SSH

- **SSH Login -** Enables/Disables SSH login for APs in the group. If enabled:
  - **Password -** Enter a password that will be required to access an AP through SSH.
  - **Confirm -** Confirm the password.

AP Web

- **AP Web -** Enables/Disables web management of APs in the group. If enabled:
  - **Password -** Enter a password that will be required to access an AP through the Web Management UI.
  - **Confirm -** Confirm the password.

Certificate

Web Server - The Certificate used for communication between the AP Web Server and browser.

Filtering the Unmanaged Access Point List

By default, the Unmanaged AP List displays all unmanaged APs. However, you can filter the list to display specific APs by clicking on one of the filter buttons at the top of the list.

- **All (Default) -** Displays all unmanaged APs.
- **Unlicensed -** Displays unlicensed APs. If the number of registered APs exceeds the number of available AP licenses, you will be unable to set the AP to a "trusted" state and move it to the Manageable APs List. The AP will be displayed in the Unmanaged AP List until you purchase or free up a license.
- **Untrusted -** Displays untrusted APs. These are APs that have been registered with OmniVista but are still in an "untrusted" state.
- **Conflict Country Code -** Displays APs with a country code violation. On these APs, the Country Code for the AP is different than the Country Code configured on the AP Group to which the AP is assigned.
- **Unregistered -** Displays unregistered APs. These are APs that have been manually added to OmniVista but have not yet registered with OmniVista. Once an AP is connected to the network, it automatically contacts the OmniVista Server and is registered with OmniVista.

Remote Access Points

You can configure an offsite, remote AP as a Remote Access Point (RAP) that can be managed by your local OmniVista Enterprise installation through a VPN Tunnel. You must first install a VPN VM (see the *OmniVista Enterprise 4.7R1 Installation and Upgrade Guide* for installation instructions). You then add AP(s) using OmniVista Cirrus, the cloud-based version of OmniVista.

When the AP(s) is connected to the network, it automatically contacts the OmniVista Cirrus Activation Server, which downloads the necessary IP and VPN configurations so the AP can be added to your List of Managed Devices and managed by your local OmniVista Enterprise installation. Adding/configuring remote APs for management consists of the following steps:

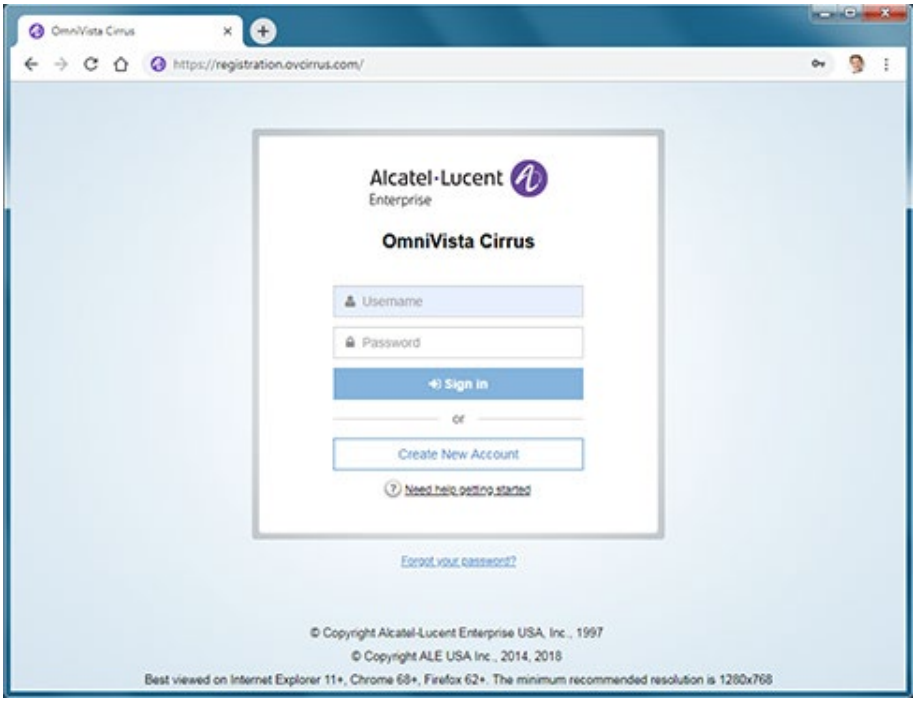
1. Create an OmniVista Cirrus Account
2. Add/Configure APs

Note: The Remote AP feature is only supported on Stellar APs running AWOS 4.0.0.xx and higher.

Creating an OmniVista Cirrus Account

OmniVista Cirrus offers a “Freemium” account which you can use to add Remote APs. Follow the steps below to create an OmniVista Cirrus “Freemium” Account.

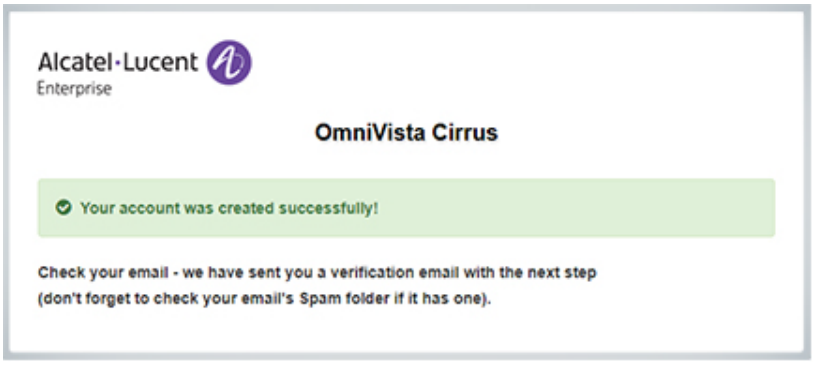
1. Go to the OV Registration Portal.



2. Click on the **Create a New Account** button. The Create New Account Screen will appear.

3. Complete the fields. Fields marked with an asterisk (*) are required. At the bottom of each screen, click **Continue** to move to the next screen. Note that the username you enter will be used to log into OmniVista Cirrus once your account is created. Also note that the e-mail address you enter will be used to verify your account and complete the process. When you have

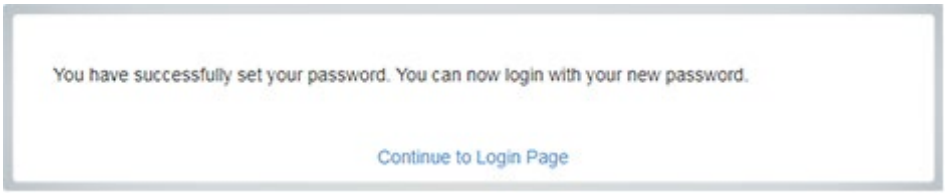
completed and reviewed all of the fields, accept the terms and conditions and click on the **Create Account** button. A Confirmation Screen will appear.



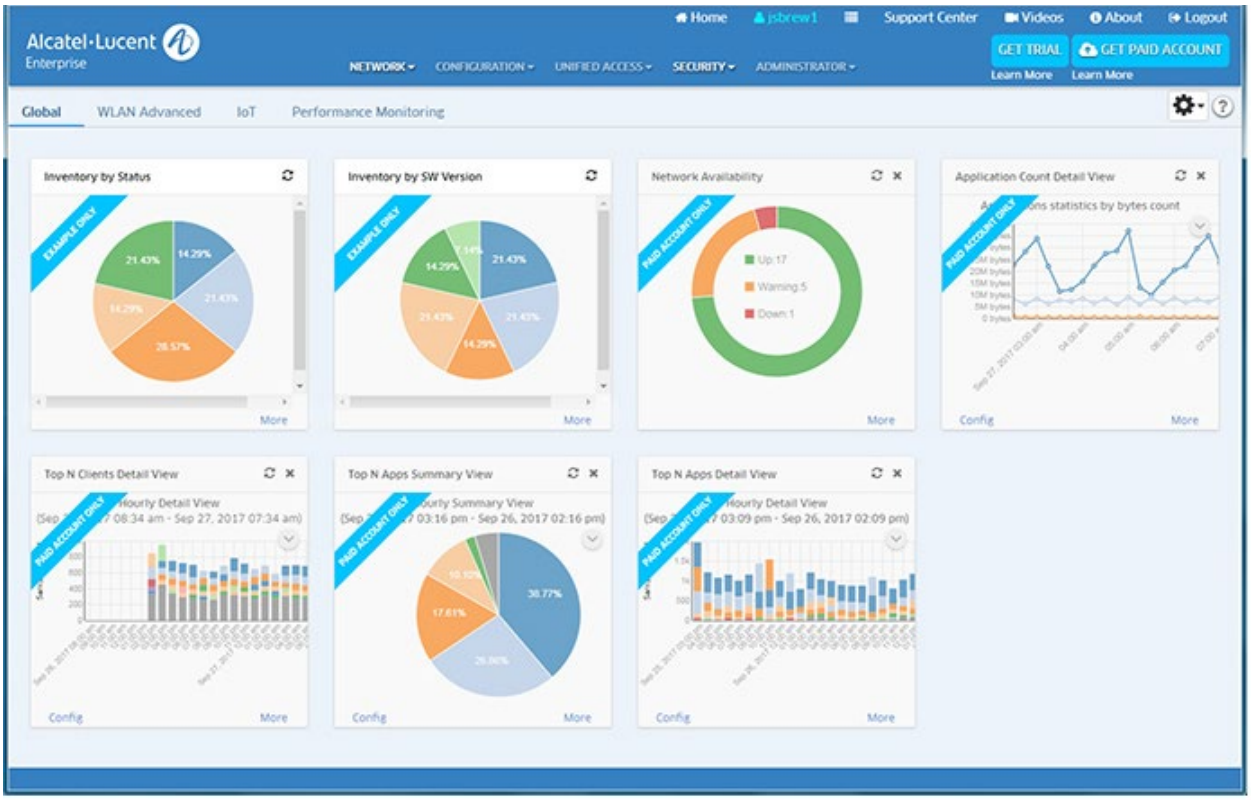
4. Go to the e-mail account you entered in Step 3 above. You will receive an e-mail from ALE USA Inc (noreply@ovcirrus.com) containing instructions and a verification link. Click on the **Go to Verify Account** link. The Set Password Screen will appear.

Important Note: There is a link in the body of the email to download the required device OS software for OmniVista Cirrus. APs must be running a minimum software version of AWOS 4.0.0.xx. Click on the link to download the software. If necessary, you can use this software to upgrade your devices.

5. Create and confirm your password, then click on the **Save** button. The Confirmation Screen below will appear.



6. Click on the **Continue to Login Page** link and log into OmniVista Cirrus using the username and password you created. After successful login, the OmniVista Cirrus Freemium Dashboard will appear.

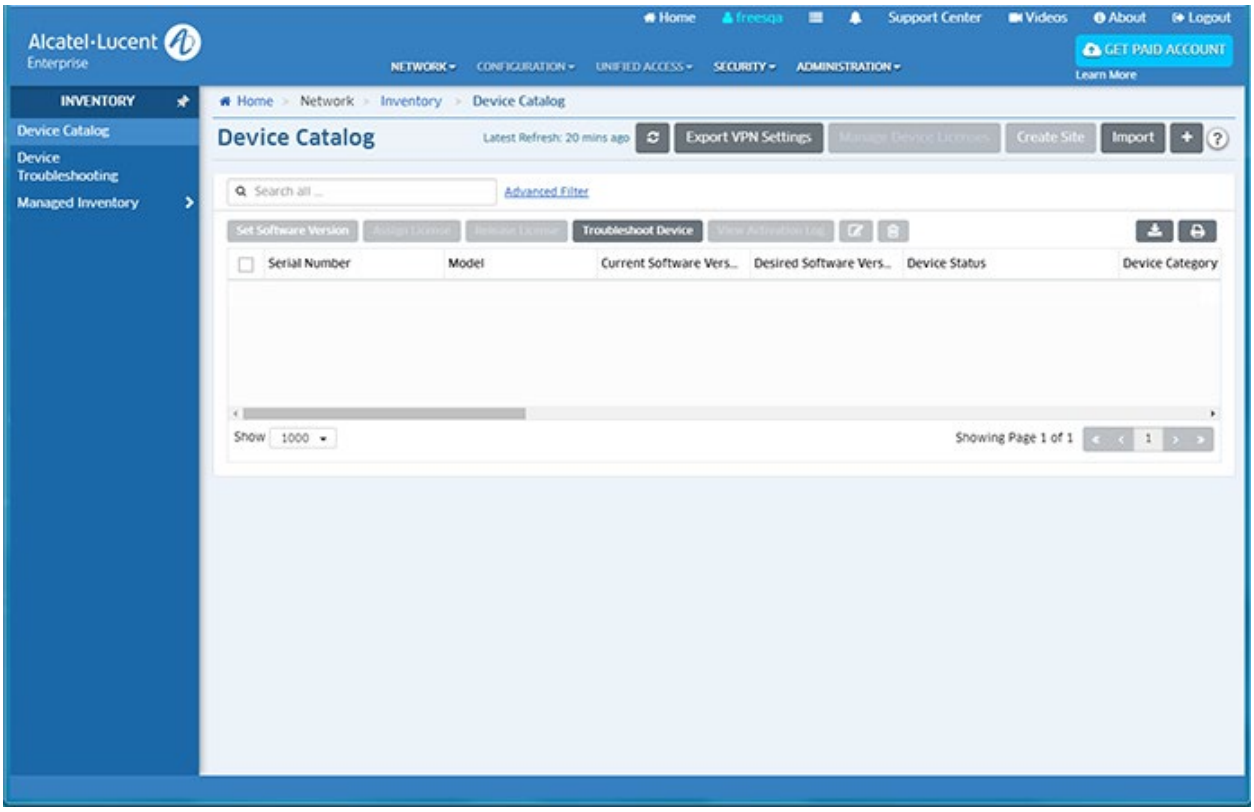


Note: You will continue to log into https://registration.ovcirrus.com using the username and password you created to access your OmniVista Cirrus Freemium Account.

Add/Configure APs

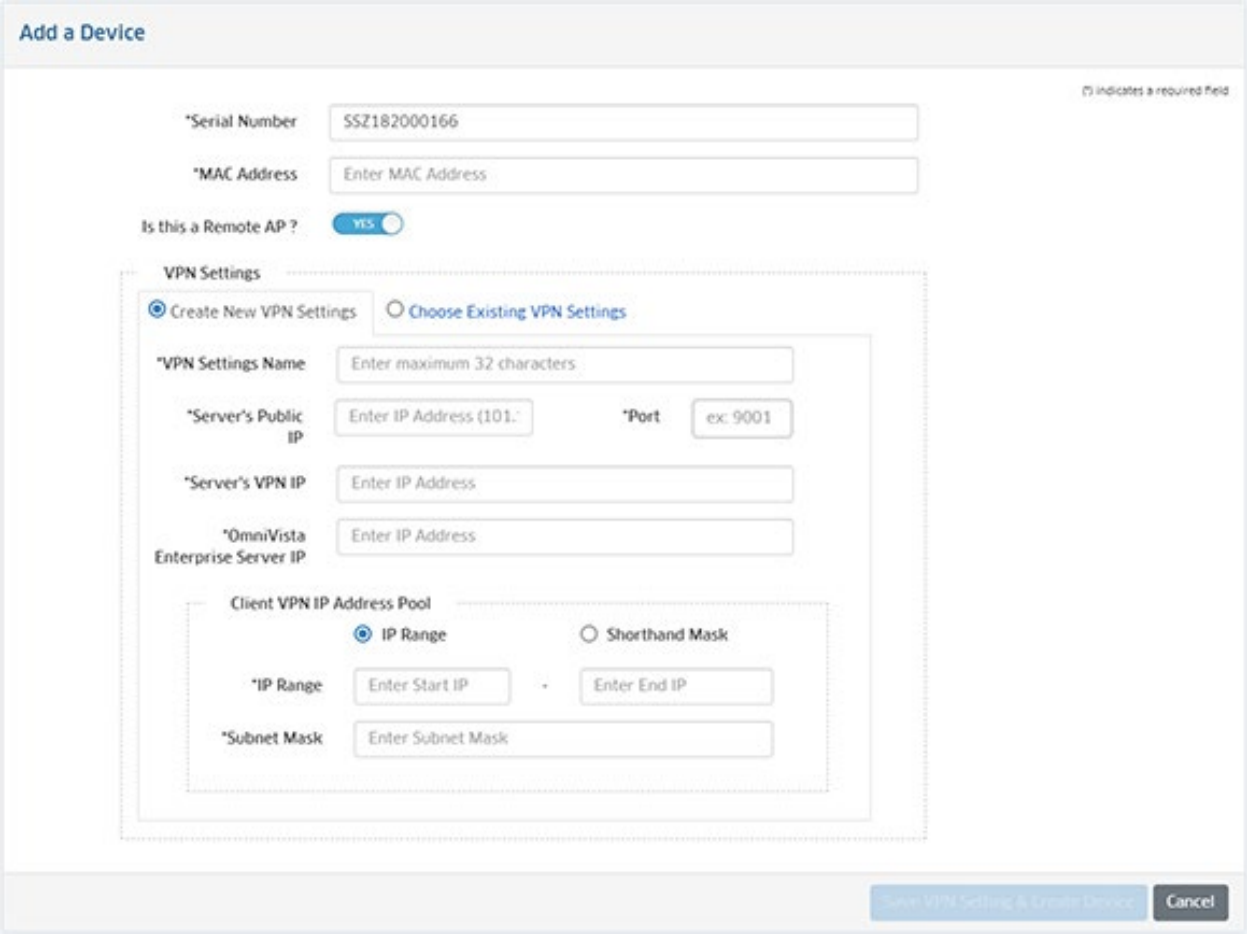
Devices are added using the Device Catalog application.

1. Select **Network - Inventory - Device Catalog** to bring up the Device Catalog application.



3. Click on the Add icon (**+**) in the upper-right corner of the screen to bring up the Add a Device Screen.

3. Enter the AP **Serial Number**, then enable the **Is this a Remote AP Field** to open the Remote AP configuration fields.



4. Complete the fields as described below, then click on the **Save VPN Settings and Create Device** button to add the AP to the Device Catalog.

- **MAC Address -** The MAC address of the AP.
- **Is This a Remote AP -** Click the slider to "Yes".
- **VPN Settings -** The VPN Tunnel configuration between the VPN Server and the OmniVista Enterprise Server. Select the **Create New VPN Settings** radio button to initially configure a Tunnel. Once you configure and save Tunnel Settings, they are saved under the VPN Settings Name and you can simply select **Choose Existing VPN Settings** to select an existing VPN configuration when adding Remote APs.
  - **VPN Settings Name -** User-configured name for the VPN configuration.
  - **Server's Public IP -** The VPN Server's Public IP address (configured when you installed the VPN VM).
  - **Port -** The VPN Server Port.
  - **Server's VPN IP -** The VPN Server's Private IP address (configured when you installed the VPN VM).
- **OmniVista Enterprise Server IP -** The IP address of your OmniVista Enterprise Server.
  - **Client VPN IP Address Pool -** The
    - **IP Range -** Enter a starting and ending IP address range.

- **Shorthand Mask -** Enter a shorthand mask for the IP Range
- **Subnet Mask -** Enter the subnet mask for the Client VPN IP Address Pool.

AP Group

The AP Registration AP Group Screen displays information about configured AP Groups. The screen is also used to create, edit, and delete AP Groups. You can also configure APs to communicate with Zigbee devices (e.g., Assa Abloy door locks), perform an immediate discovery of Zigbee devices and set the Zigbee device discovery Interval. Stellar AP Series Devices are managed by AP Group. OmniVista does not manage individual APs. You must first add APs to AP Groups. The attributes configured for the AP Group (e.g., Management VLAN, RF Profile) are applied to all APs in the group.

Once an AP(s) are assigned to a group, you configure the APs in OmniVista (e.g., Notification traps, Resource Manager backups) by applying the configuration to the AP Group. In OmniVista applications (e.g., Notifications, Resource Manager), rather than presenting the user with individual APs when applying a configuration (as is done with AOS Devices), OmniVista presents the user with the option of applying a configuration to AOS Devices and/or AP Groups. Any configuration applied to an AP Group is applied to all APs in the group.

Note: Only "admin" and "netadmin" users can add, edit, delete AP Groups.

Creating an AP Group

When an AP initially registers with OmniVista, the AP is placed into a pre-configured Default AP Group ("default group"). You can create new AP Groups containing specific APs. Create the AP Group as described below, then go to the Access Points Screen (Network - AP Registration - Access Points) and edit the Group Name to move the AP(s) into the new AP Group. An AP can belong to only one AP Group at a time. An AP Group can contain up to 512 APs.

Note: When OAW-AP1201BG APs initially register, they are placed into a pre-configured Default Beaconing Group ("default BLEGW group"). Both the "default group" and the "default BLEGW group" can be edited; however, they cannot be deleted.

Note: Do not add APs with different RF parameters to the same AP Group. For example, if some APs support 160 MHz Channel Width and others do not, then create two AP Groups and two RF Profiles. Group APs supporting 160MHz channel width into their own AP group and assign a 160 MHz RF profile to that AP group.

Click on the Add icon and complete the fields as described below to configure an AP Group. When you are finished. click on the **Create** button.

General

- **Group Name -** Enter a unique name for the group (up to 64 characters).
- **Group Description -** Enter an optional description for the group.
- **Auto Group VLANs -** A list of VLAN IDs to allow auto grouping of APs during initial registration. Based on the management VLAN ID received by LLDP, the AP can automatically be assigned to the corresponding AP Group.
- **RF Profile -** Select an RF Profile for the group. The RF profile contains the wireless attributes that are applied to all APs in the group. The RF Profile is configured using the RF Profile Screen (WLAN - RF - RP Profile).

Extended SSID Scale

- Extended SSID Scale - Enables/Disables extending the number of SSIDs that can be assigned to the AP Group to 14. When enabled (On), only AP models that support up to 14 SSIDs can join the AP Group. When disabled (Off), any AP model can join the group. (Default = Disabled)
    - Stellar AP models that support up to 14 SSIDs: AP1201, AP1321, AP 1322, AP1261, AP1361D, AP1362, AP1301H, AP1331, AP1351, AP1451, AP1411, AP1431, AP1201BG.
    - Note that the Extended SSID Scale status does not apply to 6GHz networks, which have a limit of 4 SSIDs per AP Group.

Time

- **Timezone -** The timezone in which the APs are located.
- **Daylight Saving Time -** Enable if Daylight Saving Time is in effect in the timezone.
- **NTP Server List -** Enter the NTP Server List for this AP Group. This sets the server list or all APs in the group
- **NTP Server -** The NTP Server configured for the network to which the APs are connected.

802.1X Supplicant on AP Management Port

This option configures APs in the group to operate as 802.1X clients. See AP Device as an 802.1X Client for more information.

- **802.1x Supplicant -** Enable/Disable 802.1x for APs in the group. If enabled:
    - **Certificate for 802.1x -** Select the "Built-in Certificate" or a custom 802.1x client certificate used for secure communication between the AP and an OmniSwitch. Note that out-of-the-box APs have a "Built-in Certificate" that is common to all APs. It is recommended that you use a custom 802.1x client certificate to improve network security. See AP Security Recommendations for more information.

Note: OAW-AP1101 does not support the AP 802.1X client feature due to low flash size. All other APs, including other low-end APs (OAW-AP1201H, OAW-AP1201L, OAW-AP1201HL), support this feature.

Syslog

- **Log Remote -** Enable/Disable remote logging AP events.
- **Syslog Server**
    - **IP** - The IP address of the remote Syslog Server.
    - **Port** - The port used to connect to the remote Syslog Server.
    - **TLS** - Enable/Disable the use of the Transport Layer Security encryption method for remote logging of AP events.
- **Certificate** - If TLS is enabled (On), select a Syslog Over TLS Certificate.

- **Log Level** - Select a log level (e.g., Error, Warning, Notice) for each area. This sets the log levels for all APs in the group. Note that the System, Security, Wireless, Network, and User log levels must be equal to or higher than the AP Debug log level.

Post Mortem Dump

- **PMD -** Enables/Disables Post Mortem Dump (PMD) of information for APs in the group.
- **TFTP Server -** The IP address of the TFTP Server used for PMD.

SSH

- **SSH Login - Enables/Disables SSH login for APs in the group. If enabled:**
  - **For Support Account -** The SSH password used for an SSH connection to the AP.
    - **Password -** Enter a password that will be required to access an AP through SSH.
    - **Confirm -** Confirm the password.
  - **For Root Account -** Configuring a Root Account Password Seed adds a second layer of security for AP access. When you configure a Password Seed, the Root Password is derived from a character string composed of two parts: the Password Seed and the Fixed Root Password. The Password Seed can be changed on demand. This feature is only supported on APs running AWOS 4.0.0 and higher. A Root Account Password Seed will not be configured for any APs in the group running a lower AWOS.
    - **Password Seed -** Enter a Root Account Password Seed for the APs in the group.
    - **Confirm -** Confirm the Password Seed.

AP Web

- **AP Web -** Enables/Disables web management of APs in the group. If enabled:
  - **Password -** Enter a password that will be required to access an AP through the Web Management UI.
  - **Confirm -** Confirm the password.

Client Behavior Tracking

- **Upload To SFTP/TFTP Server -** Enables/Disables uploading of a Client Behavior Log File to an FTP Server. If enabled, enter:
  - **Server Type -** FTP Server type (SFTP/TFTP).
  - **Sever IP/Host Name** - IP address or Host name of the FTP Server.
  - **Port** - FTP port number.
  - **Remote Path** - File path on the FTP Server storing the Client Behavior Log.
  - **User Name (SFTP Server only)** - User name used to access the SFTP Server.
  - **Password (SFTP Server only)** - Password used to access the SFTP Server.

  - **Confirm (SFTP Server only)** - Re-enter the password used to access the SFTP Server.
  - **Log Upload Period** - Frequency for uploading the Client Behavior Log to the FTP Server, in hours (Range = 1 - 24, Default = 1).
- **Upload to Syslog Server -** Enables/Disables uploading of Client Behavior Syslog messages to a remote Syslog Server. If enabled, enter:
  - **Syslog Server IP -** IP address of the Syslog Server.
  - **Syslog Port -** Syslog Port number.

Certificate

- **Web Server -** The Certificate used for communication between the AP Web Server and browser.
- **Third Party External Portal Server -** The Certificate used to communicate with a third-party portal server.
- **Local LDAP -** The certificate used for secure communication between the AP and an LDAP Server if the user authentication source is the local LDAP Server.
- **Local RadSec** - The Certificate used for secure communication between the AP and a local, third-party RADIUS Server that uses RadSec (RADIUS-over-TLS).

SNMP Setting

This option allows third-party SNMP-based platforms to monitor APs in a group using SNMP. OmniVista does not use SNMP to manage Stellar APs. With defined SNMP MIBs, an Administrator can monitor APs, configured services, and wireless clients and their traffic utilization.

- **SNMP Agent**
  - **SNMP Service -** Enables/Disables (On/Off) the SNMP Service on APs in the AP Group.
  - **Version -** The SNMP version. Select v3 or v2c. (Default = v3)
    - **v3 -** When SNMP v3 is selected, complete the following:
      - **User Name -** The user account name.
      - **Password -** The password for the user account.
      - **Confirm -** Confirm the specified password.
    - **v2c** - When SNMP v2c is selected, complete the following field:
      - **Read Community -** The credential used for communication between the network management system and APs.
- **Trap**
  - **Trap Service -** Enables/Disables (On/Off) SNMP Trap Service on APs in the AP Group.
  - **Version -** The SNMP version. Select v3 or v2c. (Default = v3)
    - **v3 -** When SNMP v3 is selected, complete the following fields:
      - **User Name -** The user account name.
      - **Password -** The password for the user account.
      - **Confirm -** Confirm the specified password.
      - **Server IP -** The server to which AP trap messages are sent. This is the IP address of the network management server you are

using. It is not recommended that you use the OmniVista Cirrus Server IP address to avoid the posting of duplicate traps in OmniVista

- **v2c** - When SNMP v2c is selected, complete the following fields:
  - **Community -** The credential used for communication between the network management system and APs.
  - **Server IP -** The server to which AP trap messages are sent. This is the IP address of the network management server you are using. It is not recommended that you use the OmniVista Server IP address to avoid the posting of duplicate traps in OmniVista.

Note: The Privacy and Authentication Protocol used by APs is SHA+AES, and the APs use the same Auth and Priv passwords.

IoT Radio Configuration

- **IoT Radio Mode -** Select **BLE** or **Zigbee** to configure the IoT Radio Mode. If an AP in the group supports BLE Beaconing or Zigbee devices the BLE or Zigbee configurations (below) will be applied to the AP(s).

BLE Configuration

This option is used to enable/disable BLE Beaconing for APs in the group. BLE Beaconing is used by the Location Service to deliver location services like way-finding, geo-location, geo-notification, and geo-fencing.

- **Advertising**
  - **Advertising -** Enables/Disables the BLE advertising function for the AP. If Advertising is enabled, the AP will broadcast BLE packets. If disabled, the AP will detect surrounding BLE Tags/Beacons and will report information to the server for analysis. Note that BLE Advertising **must** be enabled for Stellar Asset Tracking.
  - **Emission Frequency** - The time circle during which the BLE packets will be broadcast, in milliseconds. (Range = 20 - 9,000,000, Default = 200)
  - **Tx Power -** The transmit power used to broadcast BLE packets, in dBm. (Range = -20 - 10, Default = 4)
  - **Tx Channel -** The transmit channel used to broadcast BLE packets. It is recommended that you use a different channel than the channel used for the WLAN.
  - **Advertising Protocol -** Specify the BLE protocol used to define the broadcasting BLE beacon format.
    - **iBeacon -** Apple iBeacon format. Note that you must select iBeacon for Stellar Asset Tracking.
    - **Eddystone-URL -** Google Eddystone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.
    - **Eddystone-UID -** Google Eddystone format. A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
      - **Namespace -** 20 characters containing 0-9a-f.
      - **Instance ID -** 12 characters containing 0-9a-f.

- **Scanning**
  - **Scanning -** Enables/Disables the Bluetooth beacon scanning function for the AP. Note that BLE Scanning **must** be enabled for Stellar Asset Tracking.
  - **Scanning Interval -** The Bluetooth scanning interval for the AP, in milliseconds. (Range = 4 -10240, Default = 100)
  - **OUI Allowlist -** Specify the MAC OUI Allowlist to filter devices for BLE beacon broadcasting. Only those beacons broadcasting from the devices within the OUI Allowlist are valid and will be reported.

Zigbee Configuration

OmniVista can be used to monitor and enable/disable Zigbee devices (e.g., Assa Abloy door locks). However, supported APs must be configured to discover and connect to Zigbee devices. Zigbee devices are supported on the following APs - OAW-AP1201, OAW-AP1201BG, OAW-AP1320, and OAW-AP1360. The IoT application is used to monitor and manage Zigbee devices (Network - IoT - Inventory). See the IoT Inventory help for more information on Zigbee device support, including setting up OmniVista to support Zigbee devices.

Note: The AP Group configuration is applied to any APs in the group that support Zigbee devices. You can set different Zigbee configurations for individual APs in a group by editing the AP in the Access Points Screen. The configuration for individual APs configured on the Access Points Screen will take precedence over the Zigbee device configuration configured for the AP Group.

- **Device Discovery -** Enables/Disables automatic discovery of Zigbee devices (Default = On).
- **Discovery Duration -** The frequency of automatic discovery of Zigbee devices, in seconds (Range - 60 - 900, Default = 120).
- **Use Vendor ID -** Enables/Disables the specified Zigbee Vendor OUI (below). When enabled, OmniVista can communicate with the Zigbee device specified by the MAC OUI. To communicate with supported door locks, you **must** enable this field. The Vendor OUI is pre-filled with the MAC OUI for supported door locks (00:17:7A).
- **Vendor OUI -** The Zigbee Vendor OUI. This field is pre-filled with the MAC OUI for supported door (00:17:7A).
- **Auto-Accept MAC OUI -** You can click on the Add icon and add MAC OUIs here to "Auto-Accept" and enable Zigbee end devices. Do **not** enter the MAC OUI for supported door locks. These devices must be "Manually Accepted" and enabled in the Zigbee Devices Table on the IoT Inventory Screen.

IoT/Location/Advanced Analytics Server

This option is used to set an IoT/Location/Advanced Analytics Server Profile for APs in the group. If the location service is enabled, APs in the group will report IoT/wireless scanning data/advanced analytics data to the selected server(s). IoT/Location/Advanced Analytics Servers are configured on the AP Registration IoT/Location/Advanced Analytics Server Screen. Select a server from the drop-down list.

- **WiFi RTLS Server Profile -** Select a Wi-Fi RTLS Server Profile for APs. You can select a sub profile based on the engine type (Aeroscout or OmniVista Cirrus WiFi RTLS) and configure the necessary server parameters.

- **Advanced Analytics Server Profile -** Select a Wi-Fi Analytics Server profile for APs. The system default profile (Simple-Event-Collection) is **only** for AP event collection for the purpose of troubleshooting, For advanced analytics, must create and select an OmniVista Cirrus Advanced Analytics Profile for APs to send advanced analytics data to OmniVista Cirrus 10.1 and above.
- **OmniVista Cirrus Advanced Analytics -** If you select an OmniVista Cirrus Advanced Analytics Profile, select **On** to enable advanced analytics collection for OmniVista Cirrus 10.1 and above.
- **BLE LBS Profile -** BLE Location. Stellar Location Engine (OmniAccess Stellar Asset Tracking)
- **Zigbee Server Profile -** The Zigbee Server. If you have created a profile for Assa Abloy locks, the profile name will be displayed.

Data VPN Setting

- **Data VPN Server(s) -** Select the VPN Server used for the Data VPN Tunnel. The user traffic will be carried in the data VPN tunnel between the APs and selected VPN Server.

Web Content Filtering

Web Content Filtering (WCF) enables you to allow/deny Stellar AP access to web sites based on specific security or content filters (e.g., Malware Sites, Gambling). WCF Profiles, configured on the WCF Profile Screen (UPAM - Web Content Filtering - WCF Profile), contain the condition(s) and actions to allow/deny access to these sites. A WCF Profile is included as part of an Access Role Profile or SSID and pushed to an AP Group(s). However, Web Content Filtering must first be enabled on an AP(s).

- **Web Content Filtering -** Enables/Disables Web Content Filtering for all APs in the AP Group.

Web Content Filtering can be enabled at the AP Group Level or individual AP level. If enabled at the AP Group level, all APs in the group that support Web Content Filtering are enabled. However, you can override that configuration on an individual AP(s) in a group by editing the Web Content Filtering configuration for the AP(s) on the Access Points Screen.

Miscellaneous

- **Virtual IP Address -** The virtual IP address used for Captive Portal redirection in the AP. You can customize the IP address according to your network deployment to avoid exposing the AP management interface.
- **Called Station ID -** RADIUS attribute. You can define a message in the Called-Station-Id attribute and utilize it for communication between a NAS client and RADIUS Server. For example, in a multiple-branch scenario, you can define the AP location in the Called-Station-Id sent to RADIUS server, so when a client sends an authentication request to the RADIUS Sever, the server will the AP forwarding the client traffic.
- **IPv6 L3 Forwarding -** Enables/Disables the IPv6 L3 Forwarding on APs. Once enabled, IPv6 packets received by APs will be handled at the application level and forwarded on Layer 3. By default, the IPv6 service is disabled.

- **IGMP Snooping -** Enables/Disables Internet Group Management Protocol (IGMP) snooping of network traffic to control delivery of IP multicasts.

Editing an AP Group

Select an AP Group in the AP Group List and click on the Edit icon to bring up the Edit Group Wizard. On the Edit Group screen, edit the fields as described above, then click on the **Next** button. The Review screen will appear. Review any changes, then click the **Commit** button. If necessary, click the **Back** button to make any additional changes before clicking on the **Commit** button. You cannot edit the Group Name field. Also note that the RF Profile must be from the same country. You cannot edit an AP Group with an RF Profile from a different country.

> **Note:** You cannot edit the Group Name, Group Description, or Auto Group VLANs fields on the Default AP Group or Default BLEGW Group.

Deleting an AP Group

Select an AP Group(s) in the AP Group List and click on the Delete icon. Click **OK** at the Confirmation Prompt. APs in the deleted group(s) will be moved to the Default AP Group. You cannot delete the Default AP Group or Default BLEGW Group.

Zigbee Device Discovery

When Zigbee Mode is enabled on a supported Stellar AP, the AP automatically discovers and connects to Zigbee devices based on the configured Discovery Interval. However, you can select an AP(s) in the Access Points List and click on the **Zigbee Discovery** button at any time to have the selected AP(s) immediately scan for Zigbee devices. You can also change the Discovery Interval setting for an AP(s). Select an AP(s) and click on the **Zigbee Discovery** button. Set the new **Discovery Interval**, and click on the **Apply** button. The selected AP(s) will immediately scan for Zigbee devices and the new Discovery Interval will take effect. (Range - 60 - 900, Default = 120).

AP Group List

The AP Group List displays basic information about AP Groups. Click on a group in the list to display detailed information broken down by category.

Basic Information

- **Group Name -** User-configured name for the AP Group.
- **Auto Group VLANs -** A list of VLAN IDs used to allow auto grouping of APs during initial registration.
- **Group Description -** User-configured description for the group.
- **Managed AP Count -** The number of Managed APs in the group.
- **Unmanaged AP Count -** The number of Unmanaged APs in the group.
- **Client Count -** The number of clients connected to the AP.
- **RF Profile -** The RF Profile associated with the group. The RF profile contains the wireless attributes that are applied to all APs in the group.
- **Extendid SSID Scale** - Whether the number of SSIDs that can be assigned to the AP Group is extended (On/Off).

- **Timezone -** The timezone in which the APs are located.
- **NTP Server List -** The NTP Server List for this AP Group.
- **Log Level -** The log level for configured for AP events for APs in the group, if applicable.
- **Log Remote -** The IP address of the remote Syslog Server, if applicable.
- **Syslog Server IP -** The port used to connect to the remote Syslog Server, if applicable.
- **PMD -** Post-Morten Dump status (On/Off).
- **TFTP Server -** The IP address of the TFTP Server used for PMD, if applicable.
- **SSH Login -** SSH Login status (On/Off).
- **AP Web -** AP web management status (On/Off).
- **Upload to SFTP/TFTP Server -** Client Behavior Tracking File Upload to FTP Server administrative status (On/Off).
- **Server Type -** The FTP Server type used for client behavior tracking (SFTP/TFTP).
- **Server IP/Host Name -** The IP address or Host name of the FTP Server used for client behavior tracking.
- **Port -** The FTP port used for client behavior tracking.
- **Remote Path -** File path on the FTP Server storing the client behavior log.
- **User Name -** User name used to access the FTP Server for client behavior tracking.
- **Log Upload Period -** Frequency for uploading the Client Behavior Log to the FTP Server, in hours (Range = 1 - 24, Default = 1).
- **SNMP Service -** Administrative status of the SNMP Service on APs in the group (On/Off).
- **Read Community -** The credential used for communication between the network management system and APs.
- **Trap Service -** Administrative status of the Trap Service on APs in the group (On/Off).
- **Trap Community -** The credential used for communication between the network management system and APs.
- **Trap Server IP -** The server to which AP trap messages are sent. This is the IP address of the network management server being used.
- **IoT Location Server -** The LBS Profile configured for the AP Group.
- **Virtual IP Address -**The virtual IP address used for Captive Portal redirection in the AP.
- **Upload to Syslog Server -** Client Behavior Tracking File Upload to Syslog Server administrative status (On/Off).
- **Syslog Server IP -** The remote Syslog Server IP address, if applicable.
- **Syslog Port -** The Syslog Server Port.
- **Called Station ID** - A message in the Called-Station-Id attribute used for communication between a NAS client and RADIUS Server.
- **Data VPN Server(s) -** The data VPN server(s) configured for Remote APs.

- **IPv6 L3 Forwarding -** The administrative status of the IPv6 service for APs in the group (On/Off).
- **IoT Radio Mode -** The IoT Radio Mode (BLE, Zigbee, Disabled).
- **Web Content Filtering -** The administrative status of Web Content Filtering on the AP.
- **802.1X Supplicant -** The status of 802.1x for APs in the group (On/Off).
- **Certificate for 802.1X -** The 802.1x certificate used to secure communication between the AP and an OmniSwitch (Built-in Certificate or the name of a custom certificate). If 802.1x is disabled (Off) for the AP, this field is blank.
- **Local RadSec** - The Certificate used for secure communication between the AP and a local, third-party RADIUS Server that uses RadSec (RADIUS-over-TLS).
- **IGMP Snooping -** The administrative status of the IGMP Snooping function on the AP.

Detailed Information

General

- **Group Name -** User-configured name for the AP Group.
- **Group Description -** User-configured description for the group.
- **Auto Group VLANs -** A list of VLAN IDs used to allow auto grouping of APs during initial registration.
- **Managed AP Count -** The number of Managed APs in the group. Click on the number to view detailed information about each AP.
- **Unmanaged AP Count -** The number of Unmanaged APs in the group. Click on the number to view detailed information about each AP.
- **Number of APs Registered Through VPN Tunnel -** The
- **Client Count -** The number of clients currently connected to the AP. Click on the number to view detailed information about each client.
- **RF Profile -** The RF Profile associated with the group. The RF profile contains the wireless attributes that are applied to all APs in the group.

Extended SSID Scale

- **Extended SSID Scale** - Whether the number of SSIDs that can be assigned to the AP Group is extended (On/Off).

802.1X Supplicant on AP Management Port

- **802.1x Supplicant -** The status of 802.1x for APs in the group (On/Off).
- **Certificate for 802.1x -** The "Built-in Certificate" or the name of a custom 802.1x client certificate.

Time

- **Timezone -** The timezone in which the APs are located.
- **NTP Server List -** The NTP Server List for this AP Group.

Syslog

- **Log Remote** - The remote logging status of AP events (On/Off).
- **Syslog Server**
  - **IP** - The IP address of the remote Syslog Server.
  - **Port** - The port used to connect to the remote Syslog Server.
  - **TLS** - Whether the Transport Layer Security encryption method is used for remote logging of AP events (On/Off).
    - **Certificate** - If TLS is enabled (On), the Syslog Over TLS Certificate that is used.
- **Log Level** – The log level configured for AP events for APs in the group, if applicable.

Post Mortem Dump

- **PMD -** Post-Morten Dump status (On/Off).
- **TFTP Server -** The IP address of the TFTP Server used for PMD, if applicable.

SSH

- **SSH Login -** SSH Login status (On/Off).

AP Web

- **AP Web -** AP web management status (On/Off).

Client Behavior Tracking

- **Upload to SFTP/TFTP Server -** Client Behavior Tracking File Upload to FTP Server administrative status (On/Off).
- **Upload to Syslog Server -** Client Behavior Tracking File Upload to Syslog Server administrative status (On/Off).

Certificate

- **Web Server -** The Certificate used for communication between the AP Web Server and web browser when using the AP UI through https.
- **Third Party External Portal Server -** The Certificate used to communicate with the third-party portal server by the AP when integrated with a third-party portal authentication server.
- **Local LDAP -** The Certificate used to communicate with the local LDAP server by the AP when authenticating with a local LDAP server.
- **Local RadSec** - The Certificate used for secure communication between the AP and a local, third-party RADIUS Server that uses RadSec (RADIUS-over-TLS).

SNMP Setting

- **SNMP Agent**
  - **SNMP Service** - Administrative status of the SNMP Service on APs in the group (On/Off).

- **Version** - The SNMP version (v3 or v2c).
  - **v3** - If SNMP v3 was selected:
    - **User Name** - The user account name.
  - **v2c** - If SNMP v2c was selected:
    - **Read Community** - The credential used for communication between the network management system and APs.

- **Trap**
  - **Trap Service** - Administrative status of the Trap Service on APs in the group (On/Off).
  - **Version** - The SNMP version (v3 or v2c).
    - **v3** - If SNMP v3 was selected:
      - **User Name** - The user account name.
      - **Server IP** - The server to which AP trap messages are sent. This is the IP address of the network management server you are using.
    - **v2c** - If SNMP v2c was selected:
      - **Community** - The credential used for communication between the network management system and APs.
      - **Server IP** - The server to which AP trap messages are sent. This is the IP address of the network management server you are using.

IoT Radio Configuration

- **Use Private Config -** Administrative State of Private Config option for BLE or IoT (Enabled/Disabled). If enabled, the IoT Radio can be configured for BLE or Zigbee.
- **IoT Radio Mode -** The IoT Radio Mode (BLE or Zigbee).

Zigbee Configuration (OAW-AP1201, OAW-AP1201BG, OAW-AP1320, and OAW-AP1360 only)

- **Channel Setting -** The wireless channel used to communicate with the Zigbee device.
- **PAN ID -** The Personal Area Network (PAN) that the Zigbee device is connected to. A PAN is wireless network that communicates on the 2.4GHz Band. By default, the PAN-ID for the AP (BLE Gateway) is automatically generated using last two bytes of the AP MAC address by default. (Range = 1 - 65534)
- **Device Discovery -** The administrative status of automatic discovery of Zigbee devices (On/Off, Default = On).
- **Discovery Duration -** The frequency of automatic discovery of Zigbee devices, in seconds (Range - 60 - 900, Default = 120).
- **Use Vendor ID -** The administrative status of using the Zigbee Vendor MAC OUI to communicate with Zigbee devices (On/Off, Default = Off).
- **Vendor OUI -** The Vendor MAC OUI (supported door lock OUI is 00:17:7A).
- **Auto-Accept MAC OUI -** A list of MAC OUIs on the AP Allowlist. If a Zigbee device is on this Allowlist, it will be "Auto-Accepted" and enabled.

BLE Configuration (OAW-AP1201, OAW-AP1231, OAW-AP1320, OAW-AP1360 and OAW-AP1201BG only)

- **Advertising**
  - **Advertising -** The administrative state of the BLE advertising function for the AP. If enabled, the AP will broadcast BLE packets. (Enabled/Disabled)
  - **Emission Frequency** - The time circle during which the BLE packets will be broadcast, in milliseconds. (Range = 20 - 9,000,000, Default = 200)
  - **Tx Power -** The transmit power used to broadcast BLE packets, in dBm. (Range = -20 - 10, Default = 4)
  - **Tx Channel -** The transmit channel used to broadcast BLE packets.
  - **Advertising Protocol -** Specify the BLE protocol used to define the broadcasting BLE beacon format.
    - **iBeacon -** Apple iBeacon format.
    - **Eddystone-URL -** Google Eddystone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.
    - **Eddystone-UID -** Google Eddystone format. A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
      - **Namespace -** 20 characters containing 0-9a-f.
      - **Instance ID -** 12 characters containing 0-9a-f.

- **Scanning**
  - **Scanning -** The administrative state of the Bluetooth beacon scanning function for the AP. (Enabled/Disabled).
  - **Scanning Interval -** The Bluetooth scanning interval for the AP, in milliseconds. (Range = 4 -10240, Default = 100)
  - **OUI Allowlist -** Specify the MAC OUI Allowlist to filter devices for BLE beacon broadcasting. Only those beacons broadcasting from the devices within the OUI Allowlist are valid and will be reported.

IoT Location Server

- **WiFi RTLS Server Profile -** The WiFi RTLS Server Profile associated with the AP Group.
- **Advanced Analytics Server Profile -** The Advanced Analytics Server Profile Profile associated with the AP Group.
- **OmniVista Cirrus Advanced Analytics -** The administrative status of OmniVista Cirrus Advanced Analytics for the AP Group.
- **BLE LBS Profile -** The LBS Profile associated with the AP Group.
- **Zigbee Server Profile -** The Assa Abloy Profile associated with the AP Group.

Data VPN Settings

- **Data VPN -** The VPN tunnel between the AP and the VPN Server. The VPN Server could be deployed in different place than the OmniVista Server. The Data VPN is used to carried user traffic rather than AP management packets.
    - **Data VPN Name -** The name of the Data VPN
    - **AP's VPN IP -** The AP's VPN IP address, which is used to establish the Data VPN connection.
    - **AP's Public Key -** The AP's public key used to encrypt the data in the VPN tunnel.
    - **AP's Private Key -** The AP's private key used to encrypt the data in the VPN tunnel.

Miscellaneous

- **Virtual IP Address -** The virtual IP address used for Captive Portal redirection in the AP.
- **Called Station ID** - A message in the Called-Station-Id attribute used for communication between a NAS client and RADIUS Server.
- **IPv6 Service -** Enables/Disables the IPv6 service for APs in the group. Once enabled, IPv6 packets received by an AP are be handled at the application level and forwarded at Layer 3 forwarded. By default, the IPv6 service is disabled.
- **IGMP Snooping -** Enables/Disables the IGMP Snooping function on the AP.

Certificate

The AP Registration Certificate Screen displays information and is used to create, edit, delete, and download a Web Server/External Portal Server Certificate File. This Certificate File are used to establish a secure connection between OmniVista and APs when using the Web UI Device Management Tool as well as a secure connection to an External Portal Server. The page is also used to upload a Local LDAP Certificate to OmniVista:

- Local LDAP Certificate, which is used to establish a secure connection between an AP and a Local LDAP Server.
- 802.1X Client Certificate, which is used to establish a secure connection between an AP and an OmniSwitch.
- Local RadSec Certificate, which is used to establish a secure connection between an AP and a local, third-party RADIUS Server that uses RadSec (RADIUS-over-TLS).
- Stellar BLE Certificate, which is used to establish a secure connection between an AP and a BLE destination server for Asset Tracking.
- Syslog Over TLS Certificate, which is used to establish a secure connection between an AP and a remote Syslog Server.
- Stellar WiFi RTLS Certificate, which is used to establish a secure connection between an AP and an external server to provide real-time location data.

Once the certificates are created/uploaded, you **must** go to the AP Group Screen and edit an AP Group to apply the certificate(s) to the AP Group. The fields are located in the "Certificate" section of the AP Group configuration screen.

Creating a Certificate

Click on the Add icon, select **Web Server/External Portal Server**, and complete the fields as described below. When you are finished, click on the **Create** button.

- **Name -** The name of the certificate file.
- **File -** Click on the **Select** button to locate the file.
- **Password -** The Private Key Password to use when generating the key file.
- **Confirm-** Re-enter the password.
- **Description -** Enter a description for the certificate file.

Important Note: APs only support certificates based on FQDN, not IP Address. When generating the CSR file, you must match the "CN" field to the URL "mywifi.al-enterprise.com."

To generate a Web Server/External Portal Server Certificate file, follow the example below:

1. Generate a private Key: *openssl genrsa -des3 -out ap_server.key 2048*.

2. Generate a CSR (Certificate Signing Request): *openssl req -new -key ap_server.key -out ap_server.csr -sha256*. Note that you must enter the URL "mywifi.al-enterprise.com" for the Common Name (CN).

3. Sign and generate the AP certificate using a root CA: *openssl x509 -req -in ap_server.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out ap_server.crt -days 3560 -sha256*.

4. Merge ap_server.crt and ap_server.key to a single file: *type ap_server.crt ap_server.key > ap_server.pem*.

Editing a Certificate

You can edit the description of a Web Server/External Portal Server Certificate. Select the certificate in the Certificate List and click on the Edit icon. When you are finished, click on the **Apply** button.

Deleting a Certificate

Select the certificate in the Certificate List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Downloading a Certificate

Select a file in the Certificate List and click on the **Download** icon at the top of the screen to download the file to your PC.

Uploading an LDAP Certificate

Click on the Add icon and select **Local LDAP** to bring up the Create Local LDAP Certificate Screen. Complete the fields as described below, then click on the **Create** button.

- **Upload CA File -** Click on the **Upload** button and locate the LDAP Server's CA Certificate. Click on the **Import** button.

- **Upload Server File -** Click on the **Upload** button and locate the AP Certificate File. Click on the **Import** button.
- **Upload Server Key File -** Click on the **Upload** button and locate the AP Certificate Private Key File. Click on the **Import** button.
- **Name -** Enter a Name for the Certificate.
- **Private Key Password -** Enter a Private Key Password to encrypt the key file when generating the CA File.

Uploading an 802.1X Client Certificate

A built-in 802.1X client certificate is provided by default. If you want to upload a custom 802.1X client certificate, click on the Add icon and select **802.1X Client** to bring up the Create 802.1X Client Certificate Screen. Complete the fields as described below, then click on the **Create** button.

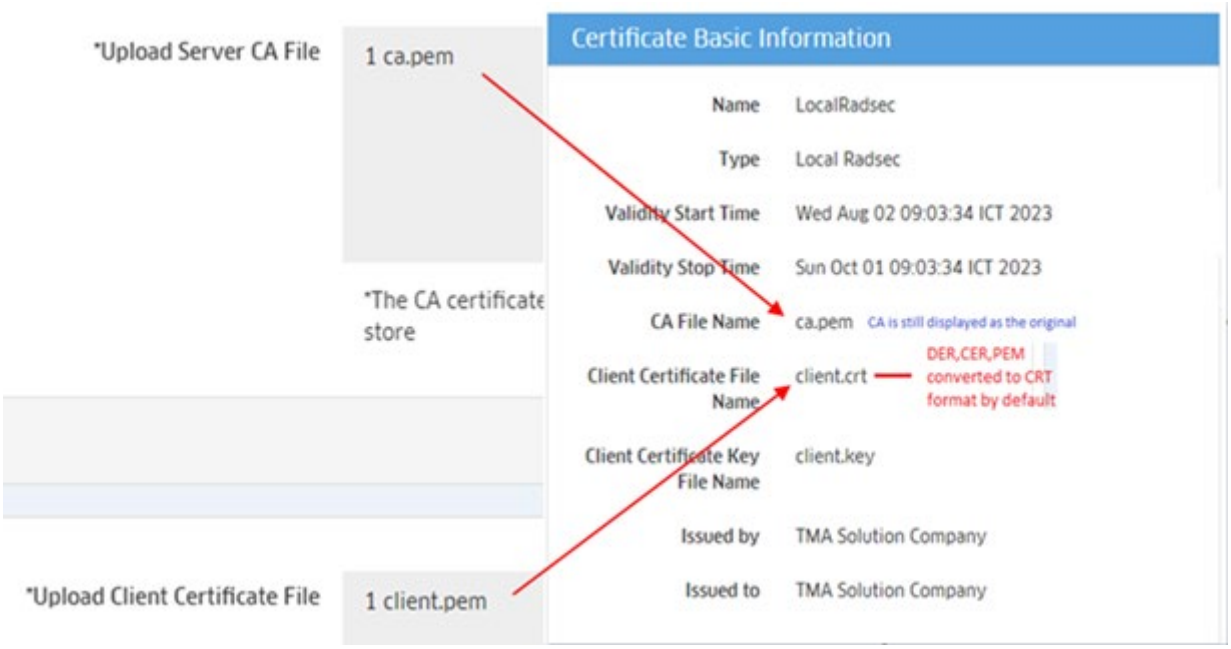
- **Upload AP Certificate -** Click on the **Upload** button and locate the 802.1X Client CA Certificate. Click on the **Import** button.
- **Upload Server Key File -** Click on the **Upload** button and locate the AP Certificate Private Key File. Click on the **Import** button.
- **Name -** Enter a Name for the Certificate.
- **Private Key Password -** Enter a Private Key Password to encrypt the key file when generating the CA File.

Uploading a Local RadSec Certificate

Consider the following information when uploading a Local RadSec Certificate in OmniVista:

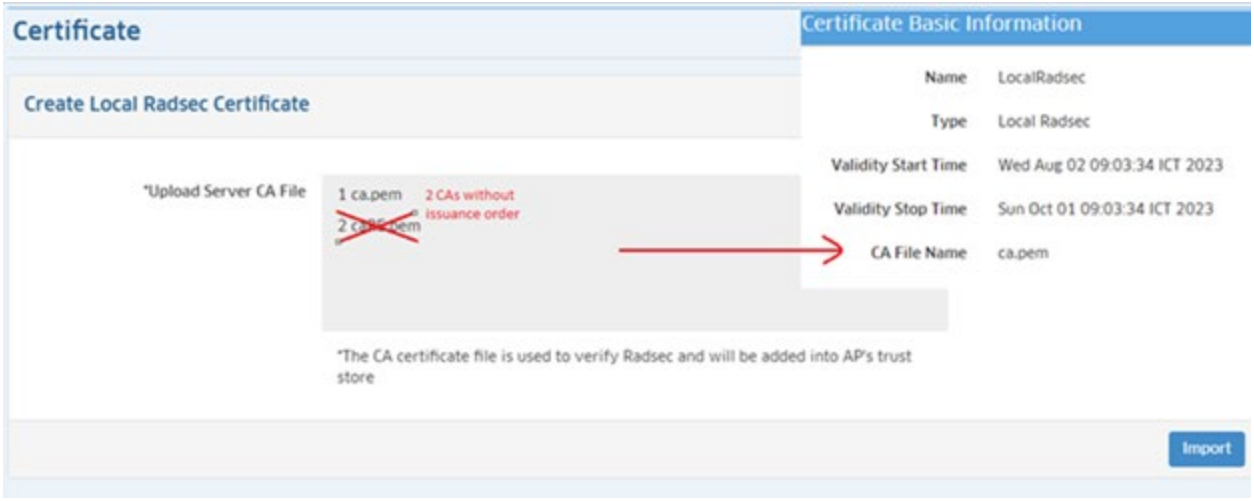
- A Local RadSec Certificate in OmniVista is supported to provide a TLS-enabled connection between RadSec Client (Stellar AP) and RadSec Server (TLS-enabled RADIUS server). Creating a certificate consists of four ingredients: CA, Client Certificate, Client Key and Password for the Key. From OmniVista, an Admin user can push these certificates to the AP by selecting the Local RadSec option in the AP Group.
  To create a Local RadSec Certificate in OmniVista, you must upload and import three ingredient files:
  - **CA Certificate file:** Supports only PEM or DER encoded certificates (e.g. .pem .cer. der .crt) and multiple CAs with issuance order.
  - **Client Certificate file:** Supports only PEM or DER encoded certificates. However, OV will translate all acceptable formats to **.crt** format due to AP's requirement.
  - **Client Key file:** Supports only **.key** file.

And, Password for Client Key.



Notes:

1. Do not import multiple CAs without an issuance order. If you import multiple CAs without an issuance order, OmniVista only parses and applies the first one to the AP.



2. Make Client Certificate and Client Key in two files separately. Client Certificate file should not include Client Key because when OmniVista converts certificate to CRT format, only the certificate part is converted, and the private key part is ignored.

3. CA Certificate file will be converted to CRT format and applied to AP, but content of the Certificate part is not changed.

To upload a Local RadSec Certificate, click on the Add icon and select Local Radsec to bring up the Create Local Radsec Certificate Screen. Complete the fields as described below, then click on the Create button.

- **Upload Server CA File** - Click on the Upload button and locate the RadSec CA Certificate. Click on the Import button.
- **Upload Client Certificate File** - Click on the Upload button and locate the AP Certificate File. Click on the Import button.
- **Upload Client Key File** - Click on the Upload button and locate the AP Certificate Private Key File. Click on the Import button.
- **Name** - Enter a Name for the Certificate.
- **Private Key Password** - Enter a Private Key Password to encrypt the key file when generating the CA File.

Uploading a Stellar BLE Certificate

The Stellar BLE data reporting channel to any Asset Tracking application uses Kafka. However, the built-in common device certificate on the AP allows communication only with Stellar AP Asset Tracking solutions. You can upload a custom device certificate to the AP that will support sending BLE data to third-party Asset Tracking applications.

> **Note:** Refer to Stellar BLE Data Format for information about the data format used to send BLE messages to third-party Asset Tracking applications.

To upload a BLE Certificate, click on the Add icon and select **Stellar BLE** to bring up the Create Stellar BLE Certificate Screen. Complete the fields as described below, then click on the **Create** button.

- **Upload Server CA File** - Click on the **Upload** button and locate the Stellar BLE CA Certificate. Click on the **Import** button.
- **Upload Server File** - Click on the **Upload** button and locate the AP Certificate File. Click on the **Import** button.
- **Upload Client Key File** - Click on the **Upload** button and locate the AP Certificate Private Key File. Click on the **Import** button.
- **Name** - Enter a Name for the Certificate.
- **Private Key Password** - Enter a Private Key Password to encrypt the key file when generating the CA File.

Syslog Over TLS Certificate

The Syslog Over TLS Certificate is used when configuring remote logging of AP events over TLS

- A CA is generated and uploaded to OmniVista and pushed to the AP by selecting the Syslog Over TLS option in the AP Group.
- A Server Certificate is also created to add to the remote Syslog Server.

Creating and Uploading the CA Certificate

To create a CA Certificate for Syslog Over TLS, complete the following steps:

1. Create an empty directory and navigate into that directory:

mkdir CA
cd CA

2. Create a few directories and give starting values to some support files:

mkdir certs crl newcerts private
echo "01" > serial
cp /dev/null index.txt

3. Copy **openssl.conf** to the current directory. Depending on your distributions, the source directory might be different, so check the list of files in the OpenSSL package before copying:

cp /etc/ssl/openssl.cnf openssl.cnf

4. Edit **openssl.conf** in the current directory:

vi openssl.cnf

5. Search for the following part and replace ./DemoCA with a single dot:

[CA_default]
dir = ./demoCA # Where everything is kept
certs = $dir/certs # Where the issued certs are kept

Change to:
[CA_default]
dir = . # Where everything is kept
certs = $dir/certs # Where the issued certs are kept

6. As a last step, generate the certificate for the CA:

openssl req -nodes -new -x509 -keyout private/cakey.pem -out cacert.pem -days 365 -config openssl.cnf

The following will be displayed. Answer the questions as shown in the following example:

Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'private/cakey.pem'

You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value.
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:CN

State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) [ ]:BJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:HAN
Organizational Unit Name (eg, section) [ ]:.
Common Name (e.g. server FQDN or YOUR name) [ ]:chong
Email Address [ ]:chong@163.com

After the certificate is generated, you can view the **cacert.pem** certificate file:

```
.
├── cacert.pem
├── certs
├── crl
├── index.txt
├── newcerts
├── openssl.cnf
├── private
│   └── cakey.pem
└── serial
```

To upload the generated CA certificate, click on the Add icon and select **Syslog Over TLS** to bring up the Create Syslog Over TLS Certificate Screen. Complete the fields as described below, then click on the **Create** button.

- **Upload CA File** - Click on the **Upload** button and locate the Syslog Over TLS CA Certificate. Click on the **Import** button.
- **Name** - Enter a Name for the Certificate.

Creating a Server Certificate

The next step is to create and sign a certificate for your syslog-ng OSE server. The common name should contain the FQDN or IP address of your server and the E-mail address should be left blank.

openssl req -nodes -new -x509 -keyout serverkey.pem -out serverreq.pem -days 365 -config openssl.cnf

openssl x509 -x509toreq -in serverreq.pem -signkey serverkey.pem -out tmp.pem

openssl ca -config openssl.cnf -policy policy_anything -out servercert.pem - infiles tmp.pem

rm tmp.pem

The differences between the certificate and the generated CA certificate are as follows:

Common Name (e.g. server FQDN or YOUR name) [ ]:*
Email Address [ ]:

The generated **servercert.pem** and **serverkey.pem** files are required by the Syslog Server.

```
.
├── cacert.pem
```

```
├── certs
├── crl
├── index.txt
├── index.txt.attr
├── index.txt.old
├── newcerts
│   └── 01.pem
├── openssl.cnf
├── private
│   └── cakey.pem
├── serial
├── serial.old
├── servercert.pem
├── serverkey.pem
└── serverreq.pe
```

Uploading Stellar WIFI RTLS Certificate

The Stellar WiFi RTLS data reporting channel uses Kafka. However, the built-in common device certificate on the AP allows communication only with the OmniVista Cirrus 10 Stellar WiFi engine. You can upload a custom device certificate to the AP that will support sending WiFi RTLS data to third-party RTLS applications.

Note: Refer to Stellar WiFi RTLS Data Format for information about the data format used to send RTLS messages to third-party RTLS applications.

To upload a Stellar WiFi RTLS Certificate, click on the Add icon and select **Stellar WIFI RTLS** to bring up the Create Stellar WIFI RTLA Certificate Screen. Complete the fields as described below, then click on the **Create** button.

- **Upload Server CA File** - Click on the **Upload** button and locate the Stellar WIFI RTLS CA Certificate. Click on the **Import** button.
- **Upload Server File** - Click on the **Upload** button and locate the AP Certificate File. Click on the **Import** button.
- **Upload Client Key File** - Click on the **Upload** button and locate the AP Certificate Private Key File. Click on the **Import** button.
- **Name** - Enter a Name for the Certificate.
- **Private Key Password** - Enter a Private Key Password to encrypt the key file when generating the CA File.

Certificate List

Web Server/External Portal Server File

- **Name -** The name of the certificate file.
- **Type -** The type of certificate (Web Server/External Portal Server).
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **Format -** The format of the certificate file (e.g., .pem).

- **Description -** User-configured description for the certificate file.
- **Issuer -** The entity that issued the certificate.
- **Serial Number -** Serial number of the certificate.

Local LDAP File

- **Name -** The name of the certificate file.
- **Type -** The type of certificate (Local LDAP).
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **CA File Name -** The name of the CA file.
- **Server File Name -** The name of the certificate file.
- **Key File Name -** The name of the key file.
- **Issued By-** The entity that issued the certificate.
- **Issued To -** The entity to which the certificate was issued.

802.1X Client File

- **Name -** The name of the certificate file.
- **Type -** The type of certificate (802.1X Client).
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -**Validity ending time of the certificate file.
- **AP Certificate File Name -** The name of the CA file.
- **Key File Name -** The name of the key file.

Local RadSec

- **Name -** The name of the certificate file.
- **Type -** The type of certificate (Local RadSec).
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **CA File Name -** The name of the CA file.
- **Client Certificate File Name -** The name of the client certificate file.
- **Client Certificate Key File Name -** The name of the client key file.
- **Issued By-** The entity that issued the certificate.
- **Issued To -** The entity to which the certificate was issued.

Stellar BLE

- **Name -** The name of the certificate file.
- **Type -** The type of certificate (Stellar BLE).
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **Client CA File Name -** The name of the CA file.
- **Client Certificate File Name -** The name of the client certificate file.
- **Client Certificate Key File Name -** The name of the client key file.

- **Issued By-** The entity that issued the certificate.
- **Issued To -** The entity to which the certificate was issued.

Syslog Over TLS

- **Name -** The name of the certificate file.
- **Type -** The type of certificate (Syslog Over TLS).
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **CA File Name -** The name of the CA file.
- **Issued By-** The entity that issued the certificate.
- **Issued To -** The entity to which the certificate was issued.

Stellar WiFi RTLS

- **Name -** The name of the certificate file.
- **Type -** The type of certificate (Stellar WiFi RTLS).
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **Client CA File Name -** The name of the CA file.
- **Client Certificate File Name -** The name of the client certificate file.
- **Client Certificate Key File Name -** The name of the client key file.
- **Issued By-** The entity that issued the certificate.
- **Issued To -** The entity to which the certificate was issued.

Stellar BLE Data Format

Consider the following information and data format that is used to send BLE messages to third-party Asset Tracking applications:

- The payload data format of the Bluetooth gateway report is an array of JSON, which contains one or more Bluetooth device information scanned in a reporting cycle.
- The reported information includes information about the scanned Bluetooth device and the Bluetooth gateway. Consider the following data format used to report the scanned information.

	Field	Description	Format	Type
data	timestamp	When the device was scanned	**ISO 8601 time format** *2019-04-28T23:54:32-0800*	String
	advType	Broadcast frameworks	*iBeacon / Edyuid / Edyurl / KonLoc / KonTLM / iBeaconPB /KonSP/S1 /UnKnow*	String
	deviceMac	Mac of the scanned device	*dc08560034ef*	String
	txPower	The strength of the signal measured at 1 meter from the device	*If not ibeacon frame, default value 0*	Int
	rssi	Detected device RSSI value	*Average: {"50":268}* *Complete: {"-44":20,"-45":25,"-47":26}*	Object
	rawData	Complete Broadcast message *(If AdvType is **KonTLM** or **iBeaconPB** or **KonSP**, report the field, otherwise not)*	*0201061AFF4C00021 5FACEC0DEFEEDCAFE FACEC0DEFEEDCAFE0 0140012C5*	String
dataType		Type of device being scanned	*ble / wifi / ble_wifi*	String
bleMac		Bluetooth mac for gateway device	*dc08561325df*	String
wlanMac		Wlan mac for gateway device	*dc08561325c0*	String
apModel		Model of AP device	*OAW-AP1201*	String
timestamp		When gateway report data	**Unix time format** *1556524473*	Long Int

Notes:

1. To get smoothing BLE data, if the RssiFormat is “average” and the number of scans in a reporting cycle is greater than three, the highest and lowest values are removed and the average value is taken.
2. To include the channel of the BLE channel of collected RSSI:
    a. BLE has only three fixed broadcast channels, and in a broadcast event, a broadcast packet is transmitted on each channel. As a result, it is not possible for the scanning device to specify that the scanning should take place on a specific channel.
    b. In a scanning event, the device will scan three channels in turn, and the scanned response data does not contain the channel.
    c. If it is the scanning channel of the WiFi, that is supported.

The reporting JSON data format is similar to the following:

For normal scene, that is to say the “filter_mode” is set to “NoFilter” and “RssiFormat” is set to “average”, The AdvType does not contain KonTLM & iBeaconPB.


```
{
    "data":[
        {
            "timestamp":"2019-04-28T23:54:32-0800",
            "advType":"iBeacon",
            "deviceMac":"dc08562afd7f",
            "txPower":-69,
            "rssi":{"-50":268}
        },
        {
            "timestamp":"2019-04-28T23:54:35-0800",
            "advType":"iBeacon",
            "deviceMac":"dc08562ad85f",
            "txPower":-69,
            "rssi":{"-52":236}
        }
    ],
    "dataType":"ble",
    "bleMac":"dc08561325df",
    "wlanMac":"dc08561325c0",
    "apModel":"OAW-AP1201",
    "timestamp":1556524473
}
```


Stellar WiFi RTLS Data Format

Consider the following information and data format that is used to send WiFi RTLS data to third-party RTLS applications:

- The payload data format of the gateway report is an array of JSON, which contains one or more WiFi device information scanned in a reporting cycle.
- The reported information includes information about the scanned WiFi device and the gateway. Consider the following data format used to report the scanned information.

Field		Description	Format	Type
data	timestamp	When the device was scanned	**ISO 8601 time format** *2019-04-28T23:54:32-0800*	String
	channel	The channel on which the ap operates	*11*	int
	scannedChannel	The channel to which the device is scanned	*6*	int
	deviceMac	Mac of the scanned device	*dc08560034ef*	Int
	isAssociated	Is associated or not	*True / False*	int
	rssi	Detected device RSSI value	*-69*	int
wlanMac		Wlan mac for gateway device	*dc08561325c0*	String
apModel		Model of AP device	*OAW-AP1201*	String
timestamp		When gateway report data	**Unix time format** *1556524473*	Long Int

The reporting JSON data format is similar to the following:

For normal scene, "RssiFormat" is set to "average", the report data format as follows:

```
{
    "data":[
        {
            "timestamp":"2029-10-28T23:54:32-0800",
            "channel":1,
            "sannedScannel":11,
            "deviceMac":"dc08562ad8c0",
            "isAssociated ":0,
            "rssi": {"-33": 6}
        },
        {
            "timestamp":"2029-10-28T23:56:32-0800",
            "channel":1,
            "sannedScannel":11,
            "deviceMac":"dc08562ad840",
            "isAssociated ":0,
            "rssi": {"-32": 4}
```

External Captive Portal Config File

The AP Registration External Captive Portal Config File Screen displays information and is used to create, edit, delete, and download a custom External Captive Portal Configuration File. The file is used to establish a secure connection between OmniVista and an external captive portal server.

Creating an External Captive Portal Config File

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

- **Name -** The name of the configuration file.
- **File -** Click on the **Select** button to locate the file.
- **Description -** Enter a description for the configuration file.

Select a file in the External Captive Portal Config File List and click on the **Sync to All APs** button to push the file to all Stellar APs. You can specify the file for APs (by AP Group) on the AP Group Screen by editing an AP Group to use the custom file (Certificate configuration).

Editing an External Captive Portal Config File

Select a configuration file in the External Captive Portal Config File List and click on the Edit icon. You can only edit the password. When you are finished, click on the **Apply** button.

Deleting an External Captive Portal Config File

Select a configuration file in the External Captive Portal Config File List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Downloading an External Captive Portal Config File

Select a file in the External Captive Portal Config File and click on the **Download** icon at the top of the screen to download the file to your PC.

External Captive Portal Config File List

- **Name -** The name of the configuration file.
- **Description -** User-configured description for the configuration file
- **Create Time -** Time when the configuration file was uploaded to OmniVista.

IoT/Location/Advanced Analytics Server

The AP Registration IoT/Location/Advanced Analytics Server Screen displays configured Aeroscout/Stellar Asset Tracking//OmniVista Cirrus WiFi RTLS/OmniVista Cirrus Advanced Analytics, and Assa Abloy Profiles and is used to create, edit, and delete profiles. OmniVista can integrate with an Aeroscout, OmniVista Cirrus WiFi RTLS, and OmniAccess Stellar Asset Tracking Server to provide Location Based Services (LBS); OmniVista Advanced Analytics to provide advanced analytics data to OmniVista Cirrus 10.1 and above installations, and an Assa Abloy Server to provide Zigbee service. BLE Location Service is a pre-configured service dedicated to OmniAccess Stellar Asset Tracking. LBS/IoT is configured for APs at the AP Group level using the AP Group Screen. Advanced Analytics is configured at the AP or AP Group level on the Access Points or AP Group Screen.

The table below lists the features and engines that are supported on each AP model.

Feature	Engine	Supported AP Model
BLE LBS	Stellar Asset Tracking	AP1201, AP1201BG, AP1230, AP1320, AP1360, AP1311
Wi-Fi RTLS	Aeroscout	All

Wi-Fi RTLS	OmniVista Cirrus WiFi RTLS	AP1201, AP1220, AP1230, AP1250, AP1320, AP1360, AP1311, AP1351, AP1301
Wi-Fi Analytics	OmniVista Cirrus Advance Analytics	AP1201, AP1220, AP1230, AP1250, AP1320, AP1360, AP1311, AP1351, AP1301
Zigbee	Assa Abloy	AP1201, AP1201BG, AP1320, AP1360, AP1311

Creating a Service

Click on the Add icon, complete the fields below, then click on the **Create** button to create a profile. The fields vary depending on the Engine Type (e.g., Aeroscout, Stellar, Assa Abloy).

- General
- **Name -** The name of the Location Service Profile or IoT Profile.
- **Description -** An optional description for the Location Service Profile or IoT Profile.
- **Engine Type -** Select the application Location Engine from the drop-down:

  Aeroscout - APs integrate with the Aeroscount location engine.

  Stellar Asset Tracking - APs integrate with Asset Tracking to provide BLE Location Based Services.

  OmniVista Cirrus WiFi RTLS - APs integrate with OmniVista Cirrus 10.1 and above to provide Wi-Fi RTLS Services.

  OmniVista Cirrus Advanced Analytics - APs integrate with Advanced Analytics for OmniVista Cirrus 10.1 and above.

  Assa Abloy - APs integrate with an Assa Abloy Server to provide Zigbee Services.

  Server IP/Host - The IP address or Host Name of the Location Engine, or IoT Zigbee Assa Abloy Server (Assa Abloy Visionline Zigbee Server). Default FQDN for Stellar Engine is *kafka.omniaccess-stellar-asset-tracking.com*. For OmniVista Cirrus Advanced Analytics, select your region from the drop-down (Americas, Europe, Middle East and Africa).

  AP Listen Port Number (Aeroscout) - The AP Listen Port (Range = 0 - 65535, Default = 1144).

  Server Port Number - The server port number (Range = 0 - 65535, Default = 9093 for Stellar/OmniVista Cirrus WiFi RTLS/OmniVista Cirrus 10.1 and above, 443 for Assa Abloy).

  User Name (Assa Abloy) - The user name used to log into the Assa Abloy Server.

  Password (Assa Abloy) - The password used to log into the Assa Abloy Server.

- **WiFi Location** (Aeroscout)
  - **Minimal Reporting Interval -** The interval (in seconds) for APs to report wireless scanning data to the Location Engine for location calculation (Default 30).
  - **Un-Associated Clients -** If enabled (checked), when a client report is started, unassociated client information will be sent to the Location Engine. If disabled (unchecked), only associated client information will be sent.
  - **BLE Location** (Stellar Asset Tracking)

- **Upload Interval -** The interval (in seconds) for APs to report BLE scanning data to the Location Engine for location calculation (Range = 1 - 30, Default = 5). Note that the Upload Interval **must** be set to 2 seconds for Stellar Asset Tracking.
- **Scanning Type Allowlist -** Select the BLE tag beacon format(s) that will be reported to the BLE Location Server (iBeacon, Eddystone-URL, Eddystone-UID, KonLoc, KonTLM, iBeaconPB, KonSP, Unknown rssi, Unknown rssi & rawData). Note that you **must** select at least the following types for Stellar Asset Tracking: iBeacon, KonLoc, and KonSP. You can select multiple types from the drop-down.
- **RSSI Format -** Specify the BLE tag RSSI format reported to the Location Server.

Average - Report the average BLE tag RSSI calculated by all values scanned in an upload interval.

- **List -** Report all the BLE tag RSSI values scanned in an upload interval.
- **OmniVista Cirrus WiFi RTLS**
  - **Upload Interval -** The interval (in seconds) for APs to report scanning data to the Location Engine for location calculation (Range = 15 - 255, Default = 30). Note that the Upload Interval **must** be set to 2 seconds for Stellar Asset Tracking.
  - **Un-Associated Clients -** If enabled (checked), when a client report is started, unassociated client information will be sent to the Location Engine. If disabled (unchecked), only associated client information will be sent.
- **OmniVista Advanced Analytics**
- **QoE Events -** Select the QoE Events data that you want to send to OmniVista Cirrus 10.1 and above. By default, all events are selected.
  - **User Info** - Information about users accessing the wireless network (e.g., association, authentication, roaming, DHCP). (Range = 1-15, Default = 5)
  - **User Tracking Info** - Information about users accessing the Internet (e.g., website URL). (Range = 1 - 15, Default = 5)
  - **Short AP Info** - AP information (e.g., AP uptime, AP downtime). (Range = 1 - 15, Default = 3)
  - **AP Info** - Major AP information (e.g., AP CPU status, Memory status). (Range = 1 - 15, Default = 5)
  - **AP Radio Info** - AP wireless radio information (e.g., band, channel, power). (Range = 1 - 15, Default = 5)
  - **AP WLAN Info** - AP WLAN information (e.g., SSID info). (Range = 1 - 15, Default = 5)
  - **AP Channel Info** - AP Channel information (e.g., channel number, bandwidth). (Range = 15 - 60, Default = 60)
  - **AP Channel Change** - AP Channel change event update (Instant). Instant means that the AP will send the report every 30 seconds.
  - **AP Rogue Info** - AP rogue information (e.g., interfering APs, rogue APs). (Range = 15 - 60, Default = 60)

  - **AP Neighbor Info** - Detected AP neighbor information. (Range = 15 - 60, Default = 60)
  - **Rogue Client Info** - Rogue client information (Range = 15 - 60, Default = 60)
  - **Wired User Info** - Information about wired users accessing the Internet (e.g., website URL) (Range = 1 - 15, Default = 5)
- **Upload Interval -** Set the interval, in minutes, for uploading each type of QoE Event Data to OmniVista Cirrus 10.1 and above. Range and default values are shown above.

Editing a Service

Select a profile and click on the Edit icon. Edit the fields as described above, then click on the **Apply** button. Note that you cannot edit the profile name.

Deleting a Service

Select a profile, click on the Delete icon, then click **OK** at the Confirmation Prompt.

IoT/Location/Advanced Analytics Server Information

Basic Information

The IoT/Location Advanced Analytics Server List displays basic information about configured profiles

- **Name -** The name of the Location Service Profile or IoT Profile.
- **Description -** An optional description for profile.
- **Engine Type -** The Location Engine Service or IoT Server Name used for the profile.
- **Engine Server IP -** The IP address or Host Name of the Location Engine.
- **AP Listen Port Number -** The AP Listen Port (Range = 0 - 65535, Default = Aeroscout - 1144, Stellar - 9093, Assa Abloy - 443).

Detailed Information

Click on a profile in the IoT/Location Server List for detailed profile information. The information displayed varies depending on the Engine Type (e.g., Aeroscout, Stellar, Assa Abloy).

Basic Information

- **Name -** The name of the Location Service Profile or IoT Profile.
- **Description -** An optional description for profile.
- **Engine Type -** The Location Engine Service or IoT Server Name used for the profile.
- **Server IP/Host -** The IP address or Host Name of the Location Engine.
- **AP Listen Port Number -** The AP Listen Port (Range = 0 - 65535, Default = Default = Aeroscout - 1144, Stellar - 9093, Assa Abloy - 443).
- **Server Port Number -** The server port number (Range = 0 - 65535, Default = 9093 for Stellar/OmniVista Cirrus WiFi RTLS/OmniVista Cirrus 10.1 and above, 443 for Assa Abloy).

- **User Name (Assa Abloy) -** The user name used to log into the Assa Abloy Visionline Zigbee Server.

WiFi Location (Aeroscout)

- **Minimal Reporting Interval -** If WiFi Location is enabled, the interval (in seconds) for APs to report wireless scanning data to the Location Engine for location calculation (Default 30).
- **Un-Associated Clients -** The administrative status of the reporting of unassociated client information (Yes/No). If enabled, when a client report is started, unassociated client information will be sent to the Location Engine. If disabled (unchecked), only associated client information will be sent.

BLE Location (Stellar Asset Tracking)

- **Upload Interval -** The interval (in seconds) for APs to report BLE scanning data to the Location Engine for location calculation.
- **Scanning Type Allowlist -** The BLE tag beacon format(s) that will be reported to the BLE Location Server. The selection can include formats (iBeacon, Eddystone-URL, Eddystone-UID, KonLoc, KonTLM).
- **RSSI Format -** The BLE tag RSSI format reported to the Location Server.
    - **Average -** Report the average BLE tag RSSI calculated by all values scanned in an upload interval.
    - **List -** Report all the BLE tag RSSI values scanned in an upload interval.

OmniVista Cirrus WiFi RTLS

- **Upload Interval -** The interval (in seconds) for APs to report scanning data to the Location Engine for location calculation (Range = 15 - 255, Default = 30). Note that the Upload Interval **must** be set to 2 seconds for Stellar Asset Tracking.
- **Un-Associated Clients -** If enabled (checked), when a client report is started, unassociated client information will be sent to the Location Engine. If disabled (unchecked), only associated client information will be sent.

OmniVista Advanced Analytics

- **QoE Events -** The QoE Events data configured for the profile.
- **Upload Interval –** The QoE Event Data upload interval for each configured event.

Data VPN Servers

The AP Registration Data VPN Servers Screen displays all configured Data VPN Servers and is used to create, edit, and delete Data VPN Servers. You can also export Data VPN Settings to use when deploying Data VPN Server VMs. Data VPN Servers are required to pass data to/from remote locations. Currently, a single VPN Server is used for Remote AP Management and data.

Creating a Data VPN Server

Click on the Add icon, complete the fields as described below, then click on the **Create** button to create a Data VPN Server Profile.

General

- **Name -** User-configured name for the Data VPN Server. It must be unique. (1 - 64 characters)
- **Description -** A description of the Data VPN Server. (1 - 255 characters)
- **Server's Public IP -** The public IP address of the Data VPN Server.
- **Server's Port -** The network port of the Data VPN Server. (Range = 1 - 65535)
- **Server's VPN IP -** The VPN IP address of the Data VPN Server.

Client VPN IP Address Pool

Select the **IP Range** or **Shorthand Mask** radio button and complete the fields as described below to create the IP pool which will be used to assign IP address to the clients connecting to the VPN tunnel.

- **IP Range**
- Enter the Starting and Ending IP Address in the range and Subnet Mask (e.g., Starting IP Address = 192.168.1.1, Ending IP Address = 192.168.1.254 with subnet mask = 255.255.255.0).
- **Shorthand Mask**
- Enter the IP pool shorthand mask format e.g., 192.168.1.0/24).

Encryption Keys

- **Server's Public Key -** The Data VPN Server’s public key used for secure communication between the Data VPN Server and client.
- **Server's Private Key -** The Data VPN Server’s private key used for secure communication between Data VPN Server and client.

Editing a Data VPN Server

Edit the fields as described above and click on the Apply button. You cannot edit the Server Name.

Deleting a Data VPN Server

Select a server(s) in the Data VPN Server List and click on the Delete icon. Click **OK** at the Confirmation Prompt. If a Data VPN Server had been applied to an AP Group, it cannot be deleted.

Exporting VPN Settings

Select a Data VPN Server Profile in the Data VPN Servers List and click on the Export VPN Settings icon (next to Delete icon) at the top of the list. The settings will be downloaded in a .conf File to you Download Directory. You can then import the settings into a Remote Data VPN Server.

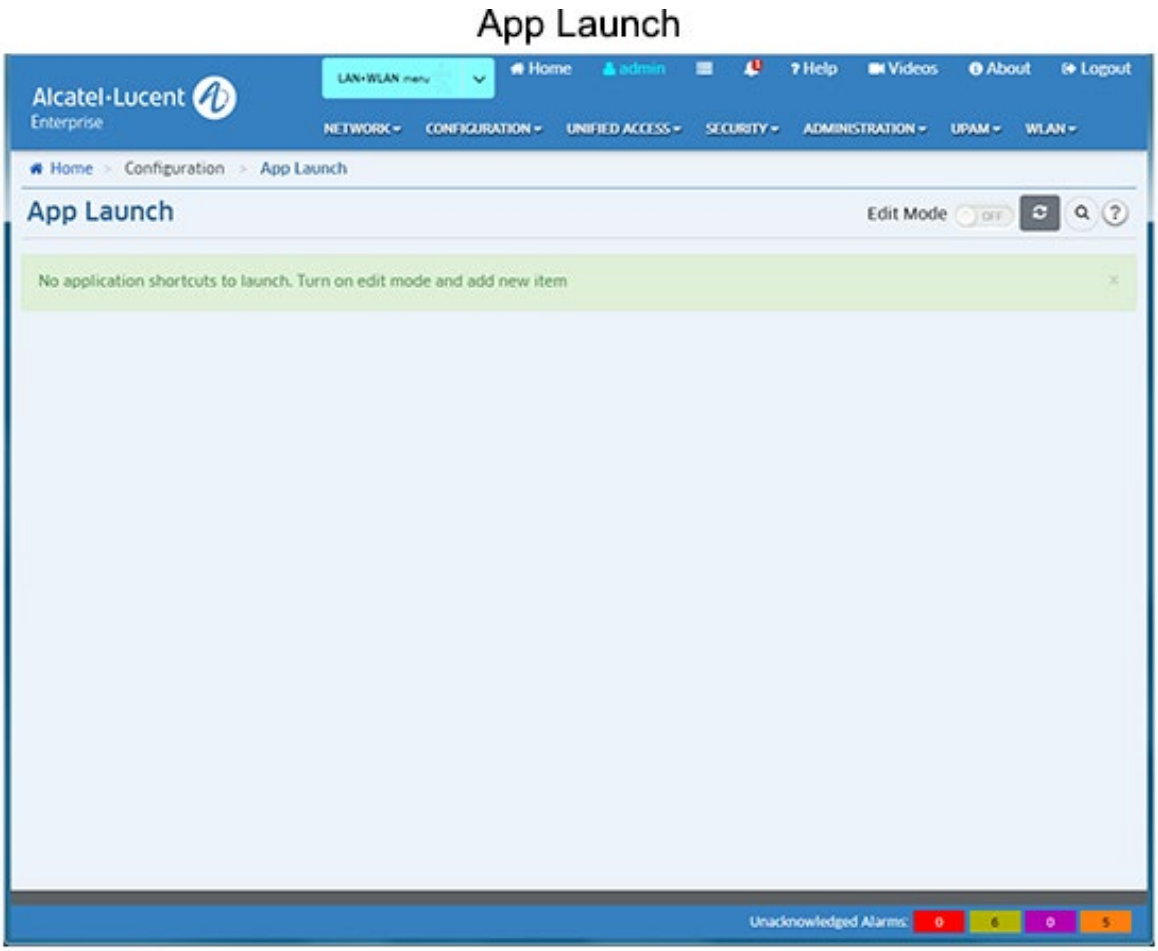
Data VPN Server List

- **Name -** User-configured name for the Data VPN Server. It must be unique.
- **Description -** A description of the Data VPN Server.

- **Server's Public IP -** The public IP address of the Data VPN Server.
- **Server's Port -** The network port of the Data VPN Server.
- **Server's VPN IP -** The VPN IP address of the Data VPN Server.

5.0 App Launch

The App Launch Screen enables you to launch web-based (e.g., OpenStack) applications using OmniVista. You can add/edit/delete application links and arrange the links on the page. Once a link is added to the page, you can click on it to open the application in a new browser tab.



Edit Mode

To add/edit/delete an application link or arrange links on the page, click on the **Edit Mode** slider to change the mode to **On**. The Add icon will appear next to the slider, and any existing links on the page will display in Edit Mode.

Adding a Launch Icon

To add a launch icon, click on the Add icon to bring up the "Add New Application" Window. Enter an **Application Name** and the **URL** needed to access the application. If you have an image for the icon, click on the **Browse** button to locate the image file. (If you do not have an image, a generic image will be used along with the Application Name you entered.) When you are done, click on the **Add** button. The icon will appear on the App Launch page. When you are finished, change the **Edit Mode** slider back to **Off**.

> **Note:** Images can be .jpg, .gif, or .png files, with a maximum size of 60 x 60 pixels. Note that if you add a large number of links you can use the search feature to

search for a specific application link on the screen. Enter the name of the application in the **Search** field. The other links are temporarily removed and the link you are searching for is isolated on the screen.

Editing a Launch Icon

To edit a launch icon, change the **Edit Mode** to **On** and click on the edit symbol in the corner of the icon to bring up the "Edit Application" Window. Edit the necessary fields and click on the **OK** button. The updated icon will appear on the App Launch page. When you are finished, change the **Edit Mode** to **Off**.

Deleting a Launch Icon

To delete a launch icon, change the **Edit Mode** to **On** and click on the delete symbol ✖ in the corner of the icon. Click **Yes** at the confirmation prompt. When you are finished, change the **Edit Mode** to **Off**.

Arranging Launch Icons

Change the **Edit Mode** to **On**, you can also arrange the icons on the page. Click on the **Setting** icon to bring up the "Settings" Screen. Configure the display options as described below.

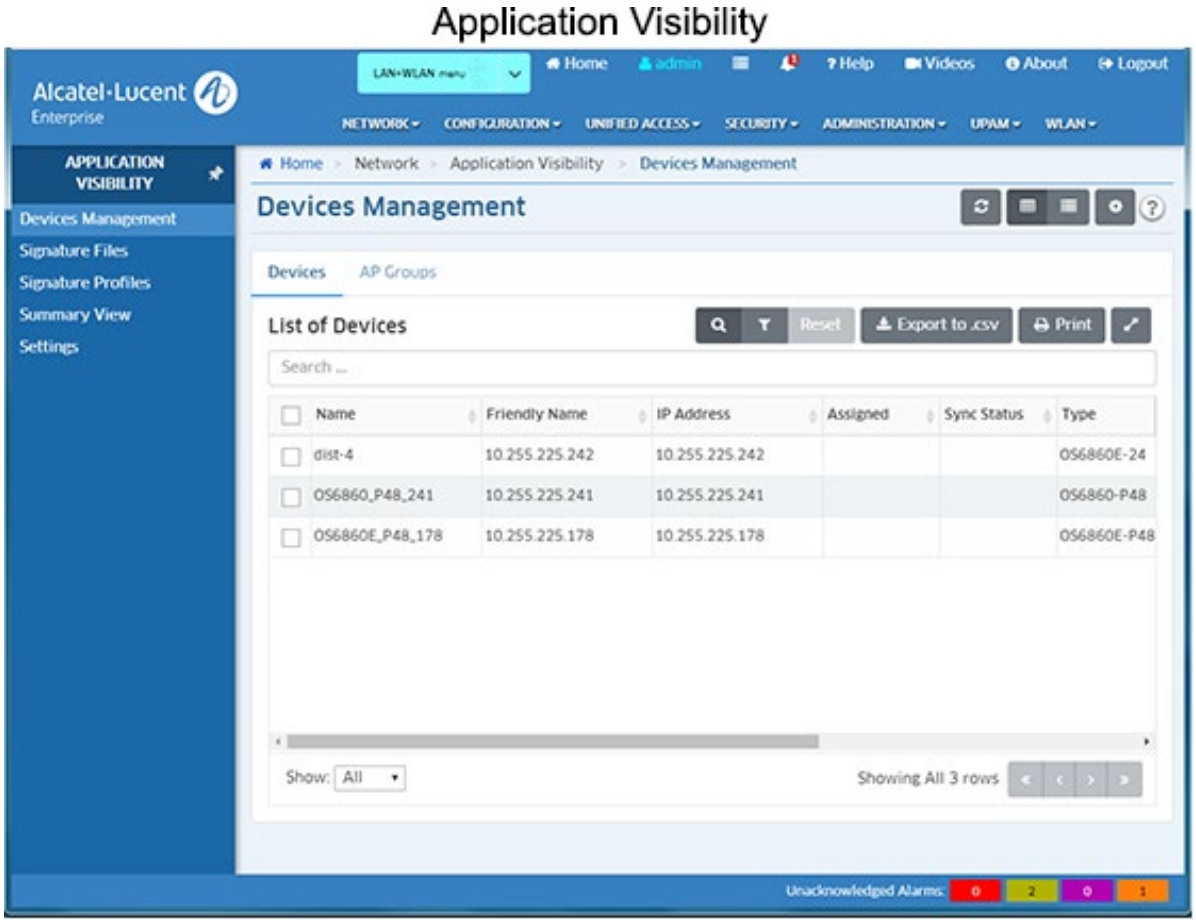
- **Items per Page -** Select the maximum number of icons you want displayed on the page (15, 30, 45).
- **Sort By** - Select **Name** to display the icons alphabetically by name. Select **Creation Date** to display the icons chronologically by when they were added to the page. Select **Custom** to sort the icons manually by dragging them to new positions.

After making your selections, click **OK**. If you selected **Name** or **Creation Date**, the icons will be automatically displayed in the order selected. If you selected **Custom**, you can then drag the icons to their new positions. When you are finished, change the **Edit Mode** to **Off**.

6.0 Application Visibility

The Application Visibility Application supports monitoring and QoS configuration of Application traffic flows, and performs statistics profiling on the collected data. OmniVista simplifies Application Visibility configuration for the network by enabling you to quickly configure Application Visibility on switches throughout the network. Application Visibility is supported on OS6860E Switches, including a virtual chassis of OS6860/OS6860E Switches where at least one OS6860E is present, and APs.

> **Note:** OmniVista must be able to FTP to a switch to gather information for the Application Visibility Application. When you initially discover network switches using the Discovery Application, make sure to specify the CLI/FTP User Name and Password for the switches in the Discovery Profile. If you do not specify the CLI/FTP User Name and Password during discovery, you can specify them anytime using the Topology application. Go to the Topology application (Network - Topology), select the switch in the Topology Map that you want to monitor, click on the **Discovery - Edit Device** option in the Operations panel to bring up the Edit Discovery Manager Device Screen and edit the fields.



Application Visibility Application

The Application Visibility Application identifies application/protocol flows based on Application Signatures that identify an associated application or protocol. To enable Application Visibility, you create a Signature Profile that includes all of the signatures for applications/protocols that you want to monitor/control and apply that profile to network switches/ports. Once Application

Visibility is enabled on switch ports, the switch can identify traffic flows included in the profile. You can then use the Top N Applications - Advanced Report in the Analytics Application to monitor network usage for each application/protocol; and use the Application Enforcement feature in Application Visibility to assign QoS/UNP Policies to the traffic. The page links on the left side of the screen (shown above) are used to view and configure Application Visibility:

- **Devices Management -** Displays all network switches supporting Application Visibility. In addition to the name, IP address, and operational status of each switch, the screen indicates whether or not an Application Visibility Profile has been assigned to the switch. You can also select a switch to display more detailed information and enable/disable automatic Signature Profile updates. (Automatic Signature Profile updates are only supported on OS6860/6860E Switches and Stellar AP Series Devices only).
- **Signature Files -** Displays all Signature Files downloaded/imported into OmniVista. It is also used to download/import Signature Files.
- **Signature Profiles -** Used to create Signature Profiles. Signature Profiles are created from a Signature File, which contains Application Signature information in pre-configured Application Groups (groups of related applications protocols). You create a Signature Profile by selecting one or more applications/application groups (or creating a custom group) that contain the applications/protocols you want to monitor/control. You then assign the Signature Profile to network switches/ports.
- **Summary View -** Used to view information on switches configured for Application Visibility.
- **Settings -** Used to configure Signature File update settings. Signature Files are regularly updated to either provide new signatures, or to update existing signatures which have changed. The Settings Screen is used to configure how often OmniVista will check the ALE Signature File Repository for updates. If an update is available, OmniVista will automatically download the file. You can also configure how often OmniVista will check any switches configured for Application Visibility to make sure they have the most recently downloaded Signature File. Note that the Signature File Auto-Update Feature is supported on OS6860/6860E Switches and Stellar AP Series Devices.

Application Visibility Configuration

The Application Visibility Application supports monitoring and QoS/UNP configuration of Application traffic flows, and performs statistics profiling on the collected data. OmniVista Cirrus simplifies Application Visibility configuration for the network by enabling you to quickly configure Application Visibility on switches throughout the network. Configuring Application Visibility for Application Monitoring and Application Enforcement consists of the following steps:

1. Download and import Signature Files from the Alcatel-Lucent Enterprise (ALE) Signature File website. Signature Files for OS6860/6860E Switches/APs are provided by ALE and are automatically downloaded/updated. (Signature Files Management Screen).
2. Create Signature Profiles from the Signature File. (Signature Profiles Screen).

   Configure Monitoring - Using the "Create Signature Profile" Wizard. Wizard guides the user through configuration of application monitoring groups.

   Configure Enforcement - Using the "Create Signature Profile" Wizard. Wizard guides the user through configuration of application enforcement groups. User

must then configure an Access Role Profile in the Unified Access Application based on the configured enforcement groups.

3. Apply Signature Profiles to network switches/ports. (Signature Profiles Screen).

Devices Management

The Application Visibility Devices Management Screen displays information about all network switches and Stellar AP Series Devices (AP Groups) that support Application Visibility. In addition to the name, IP address, and operational status of each device, the screen indicates whether or not an Application Visibility Profile has been assigned to the device. Click on a device to display more detailed information and/or enable/disable automatic Signature File updates. Note that the Signature File Auto-Update Feature is supported on OS6860/6860E Switches and Stellar AP Series Devices only.

List of Devices/AP Groups

Basic information about AOS Switches and Stellar AP Series Devices is displayed in the List of Devices/AP Groups. Click on "Devices" or "AP Groups" at the top of the list to view information about switches or Stellar AP Series Devices. Click on a switch or AP Group to display more detailed information.

AOS Switch Information

The List of Devices displays basic information about AOS Switches. Click on a switch to display more detailed information.

Basic Information

- **Name -** The user-configured switch name, if applicable.
- **Friendly Name -** The device label as configured in the Preferences application (e.g., device IP address, System name, DNS name).
- **IP Address -** The device IP address ("Master" switch/chassis IP address for a stack or virtual chassis configuration).
- **Assigned -** The name of the Signature Profile assigned to the switch, if applicable.
- **Sync Status -** Whether or not the Signature Profile assigned to the switch is in sync with the profile stored in OmniVista. If the Signature Profile in OmniVista is different than the one on the switch, Sync Status will indicate "out of sync".
- **Type -** The switch model type (e.g., OS6900-X20).
- **Version -** The switch AOS build number.
- **Status -** The switch operational status.
- **MAC Address -** The switch MAC address ("Master" switch/chassis MAC address for a stack or virtual chassis configuration).

Detailed Information

- **Name -** The user-configured device name, if applicable.
- **Version -** The switch AOS build number.
- **Serial Number -** The switch serial number.
- **Type -** The switch model type (e.g., OS6900-X20).

- **IP Address -** The device IP address ("Master" switch/chassis IP address for a stack or virtual chassis configuration).
- **MAC Address -** The switch MAC address ("Master" switch/chassis MAC address for a stack or virtual chassis configuration).
- **Signature Profile -** The name of the Signature Profile assigned to the switch, if applicable.
- **Signature File -** The name of the Signature File assigned to the switch, if applicable.
- **Signature Version -** The version of the Signature File assigned to the switch, if applicable.
- **Status -** The switch operational status.
- **Auto Update (OS6860/6860E Only) -** Enables/Disables (On/Off) Signature File auto update. If the "Signature Auto Update" option is enabled on the Application Visibility Settings Screen, OmniVista automatically downloads newer 8.x Signature File versions from the ALE Signature File Repository when they become available. If Signature File "Auto Update" is enabled on a switch, after downloading a new Signature File version, OmniVista first updates any Signature Profiles created with the older Signature File version. If that updated Signature Profile is being used by the switch, OmniVista then automatically assigns the updated profile to switch.

Note that auto update only occurs on Signature Files within the same "Major" version (the first number in the file version). For example, if version 1.1.1 is stored in OmniVista and version 1.2.1 is available in the repository and downloaded, OmniVista will automatically update the Signature Profile(s) that are using Signature File version 1.1.1 with version 1.2.1 and apply them to any switches with that profile. If version 2.1.1 is available and downloaded, OmniVista will download the file, but will not update any profiles using 1.x.x Signature Files switches using those profiles.

Signature File automatic update check frequency is configured on the Application Visibility Settings Screen.

Stellar AP Series Device Information

The List of AP Groups displays basic information about AP Groups. Click on a switch to display more detailed information.

Basic Information

- **Name -** The AP Group Name
- **Assigned -**The name of the Signature Profile assigned to the AP Group, if applicable.
- **Sync Status -** Whether or not the Signature Profile assigned to the AP Group is in sync with the profile stored in OmniVista. If the Signature Profile in OmniVista is different than the one on the switch, Sync Status will indicate "out of sync".

Detailed Information

- **Name -** The AP Group name.
- **Signature Profile -** The name of the Signature Profile assigned to the switch, if applicable. **Signature File -** The name of the Signature File assigned to the switch, if applicable.

- **Signature Version -** The version of the Signature File assigned to the switch, if applicable.
- **Sync Status -** Whether or not the Signature Profile assigned to the AP Group is in sync with the profile stored in OmniVista. If the Signature Profile in OmniVista is different than the one on the switch, Sync Status will indicate "out of sync".
- **Auto Update (OS6860/6860E Only) -** Enables/Disables (On/Off) Signature File auto update. If the "Signature Auto Update" option is enabled on the Application Visibility Settings Screen, OmniVista automatically downloads newer 8.x Signature File versions from the ALE Signature File Repository when they become available. If Signature File "Auto Update" is enabled on a switch, after downloading a new Signature File version, OmniVista first updates any Signature Profiles created with the older Signature File version. If that updated Signature Profile is being used by the switch, OmniVista then automatically assigns the updated profile to switch.

Note that auto update only occurs on Signature Files within the same "Major" version (the first number in the file version). For example, if version 1.1.1 is stored in OmniVista and version 1.2.1 is available in the repository and downloaded, OmniVista will automatically update the Signature Profile(s) that are using Signature File version 1.1.1 with version 1.2.1 and apply them to any switches with that profile. If version 2.1.1 is available and downloaded, OmniVista will download the file, but will not update any profiles using 1.x.x Signature Files switches using those profiles.

Signature File automatic update check frequency is configured on the Application Visibility Settings Screen.

Signature Files

The Application Visibility Signature Files Screen displays all imported Signature Files, and is used to upgrade/import Signature Files. A Signature File contains application signature information that is used to create Signature Profiles. Once you create a Signature Profile, you assign that profile to switches to monitor/control application traffic on the network.

Viewing Signature Files

The Signature File Management Screen displays all Signature Files in OmniVista Cirrus. Signature Files are binary files (e.g., AppSig.upgrade_kit_1) that are provided by Alcatel-Lucent Enterprise (ALE) and are automatically downloaded/updated.

> **Note:** Signature Auto Update is enabled on the Application Visibility Screen, which is available for a System User. If you are logged in as a System user, go to the Network - Application Visibility Settings Screen to enable Signature Auto Update. If Signature Auto Update is enabled, OmniVista Cirrus automatically downloads newer Signature File versions when they become available.

Importing a Signature File

OmniVista Cirrus automatically checks the ALE Signature File Repository and updates and downloads Signature Files (see Upgrading a Signature File below). There should be no need to import these Signature Files into OmniVista Cirrus. If necessary, you can download a Signature File and click on the **Import** button to import the file into the Application Visibility application.

Upgrading a Signature File

OmniVista Cirrus regularly checks the ALE Signature File Repository for newer Signature File versions. The update check frequency is configured on the Application Visibility Settings Screen (System User.) If OmniVista Cirrus detects that a new Signature File version is available (e.g., version 1.1.1 is stored in OmniVista Cirrus and version 1.2.1 is available in the repository), OmniVista Cirrus automatically downloads the file. However, you can manually upgrade a Signature File at any time by selecting the file and clicking on the **Upgrade** button.

> **Note:** If Signature File "Auto Update" is enabled on a switch (configured on the Devices Management Screen), after downloading the new Signature File version, OmniVista Cirrus first updates any Signature Profiles created with the older Signature File. If a switch has "Auto Update" enabled and that Signature Profile is being used by the switch, OmniVista Cirrus then automatically assigns the updated profile to the switch or AP Group. Note that profiles and switches are only automatically updated if they are using the same "Major" version of the new Signature File (e.g., profile and switch are using version 1.1.1 and version 1.2.1 is available and downloaded by OmniVista Cirrus).

Deleting a Signature File

To delete an imported Signature File from the repository, select the file in the table and click on the Delete icon. Click **OK** at the confirmation prompt. Note that you cannot delete a Signature File that has been assigned to switches on the network.

Signature Profiles

The Application Visibility Signature Profiles Screen displays all configured Signature Profiles and is used to create, apply, edit, clone, and delete profiles. Signature Profiles are created from a Signature File, which contains Application Signature information for individual applications/protocols as well application groups (pre-configured groups of related applications/protocols). You create a Signature Profile by selecting one or more applications/application groups (or creating a custom group) that contain the applications/protocols you want to monitor/control. You then assign the Signature Profile to network switches. Multiple Signature Profiles can be created from a single Signature File, each containing a different combination applications/application groups. And a Signature Profile can be assigned to one or more switches. However, a switch can be assigned only one Signature Profile.

> **Note:** Application/protocol traffic is monitored using the Analytics application. To view statistics on applications/protocols you have configured in a profile, go to the "Top N Applications - Advanced" Screen (Network - Analytics - Top N Applications - Advanced). Once you configure a profile and assign it to switches statistics for the applications/protocols in the profile are displayed in graphical and table format.

Viewing Signature Profiles

The Signature Profiles Screen displays all configured Signature Profiles. Click on a profile to display detailed profile information.

- **Profile Name -** The user-configured name for the profile.
- **Description -** A user-configured description for the profile.
- **File Name -** The name of the Signature File used in the profile.

- **File Version -** The file version of the Signature file used in the profile.
- **Applications -** Lists the applications included in the profile.
- **Application Groups -** Lists the application groups included in the profile.
- **Devices -** Lists the switches to which the profile has been assigned.
- **AP Groups -** Lists the AP Groups to which the profile has been assigned.

Creating a Signature Profile

Signature Profiles are created from a Signature File, which contains application signature information for individual applications/protocols and application groups. You create a Signature Profile by selecting one or more applications/application groups (or creating a custom group) that contain the applications/protocols you want to monitor/control. The Signature Profile Wizard guides you through the steps to create a profile.

There must be at least one application/application group in a profile. In addition to monitoring groups, you can also create enforcement groups using the "Create Signature Profile" Wizard. Click the Add icon to create a new profile. The "Create Signature Profile" Wizard appears. Complete the screens as described below. After creating a profile, you must apply it to switches/ports in the network.

Create Signature Profile Wizard

Click on the Add icon to bring up the Create Signature Profile Wizard. The wizard guides you through creating a Signature Profile containing both monitoring groups and enforcement groups. You can create monitoring groups only, without creating enforcement groups. However, to configure enforcement, you must configure an enforcement group in the wizard. For enforcement, you then create an Application Visibility Policy List that you use to configure an Access Role Profile. Complete the screens in the wizard as described below, then click on the **Create Profile** button.

Name and Description

Enter a **Profile Name**. Enter a name describing the profile you are creating (e.g., 6860 Profile). You can also enter a profile **Description**. Click **Next**.

Select File

Select a Signature File. LAN Devices (e.g., AppSig.upgrade_kit_1), APs use the AppSig.upgrade_kit Files. You can only select one Signature File at a time. If your network contains both LAN Device and APs, repeat to apply Signature Files to each device type. After selecting a Signature File, click **Next**.

Select Groups/Apps - Monitor Flow Count

To select Monitoring Groups, click on **Groups**, then click on the **Choose App Groups** button. Select the groups you want to include in the profile and click **OK**. You can also create a custom Application Group to include only those applications that you want to monitor by clicking on the **Create App Group** button. Enter an **Application Group Name** and **Description**, select the applications you want to include in the group, and click **OK**.

To select Monitoring Applications, click on **Applications**, then click on the **Choose Apps** button. Select the applications you want to include in the profile and click **OK**. Note that if an application is included in a group, you cannot configure it individually.

At this point, you can click on the **Create Profile** button to just create a Monitoring Profile or click the **Next** button to configure an Enforcement Profile.

Select Enforcement Groups - Bandwidth Usage and Enforcement

To select Bandwidth/Enforcement Groups, click on **Groups**, then click on the **Choose App Groups** button.

Select the groups you want to include in the profile and click **OK**. You can also create a custom Application Group to include only those applications that you want to monitor by clicking on the **Create App Group** button. Enter an **Application Group Name** and **Description**, select the applications you want to include in the group, and click **OK**.

To create bandwidth enforcement policies, click on the link next to **ACL/QoS** and configure a policy. To configure an Access Role Policy, click on the link next to **Access Role Profile** and select a profile from the drop-down list.

To select Bandwidth/Enforcement Applications, click on **Applications**, then click on the **Choose Apps** button. select the applications you want to include in the profile and click **OK**. Note that if an application is included in a group, you cannot configure it individually.

> **Note:** When you configure an Access Role Profile this workflow will not assign the selected Access Role Profile to the devices. You must first assign the Access Role Profile to the devices from Unified Profile Application. All users having the Access Role Profile will be affected.

When you are finished, click on the **Create Profile** button.

The profile creation is complete and can be used to create reports for monitoring the applications in the profile using the Analytics Application. To configure application enforcement, and create Application Count Reports in the Analytics application, you must create an Application Visibility Policy List using Signature File Groups; and create an Access Role Profile using the Policy List.

Editing a Signature Profile

From the Signature Files Management Screen, click on an Upgrade Kit to display the Signature Files. Select a Signature File and click on the Edit icon. You can edit the Profile Name, Description, and Application Groups as described above. When you are done editing, click on the **OK** button. After editing the profile, you must apply it to switches/ports in the network. Note that you cannot edit a Default Profile.

Cloning a Signature Profile

You can clone an existing profile and edit it to create a new profile. Note that when you import a Signature File, a Default Profile is created and appears in the Signature Profiles Table. These profiles contain all of the applications/application groups for each file type. You can create a new profile from scratch as described below, or you can clone one of the default profiles and modify it to create a new profile. To clone and modify a Default Profile, select the profile and click on the Clone icon. The "Create Signature Profile Wizard" appears. Use the wizard to modify the default profile to create a new one.

1. Select a Signature File and click the Clone icon.
2. Edit the profile as described above and click the **OK** button.
3. Apply the profile to switches/ports in the network.

Applying a Signature Profile

After creating/editing/cloning a profile, you must apply it to devices/ports in the network. Select the Signature Profile and click on the **Apply to Devices** button at the top of the screen. The Apply to Devices Screen will appear.

1. Select the AOS Devices/AP Groups to which you want to assign the profile. Only devices/AP Groups without an applied Signature Profile that support the profile type you are applying are displayed (e.g., OS6860/APs are displayed for a profile created with an OS6860/AP Signature File).
2. For AOS Devices, click on the "Add Port" Link under each device to select device ports. (Only OS6860N switches running 8.7R2, or higher, support Application Visibility configuration on link aggregate member ports; OS6860/6860E switches do not.).
3. Click on the **Apply** button. The progress is displayed on the Action Results Screen. Click **OK** to return to the Signature Profiles Screen.

   Note: You can only assign one (1) Signature Profile to a device/AP Group. Also, when you apply a Signature Profile, any pre-existing Application Visibility configuration on a device is erased and the new profile configuration is used, including any Application Visibility configuration done from the CLI.

   Note: If a Signature Profile is applied to an AP Group that contains APs that do not support Application Visibility, (AP1201, AP1201H, AP1101), the profile will not be applied to those APs. If none of the APs in the group support Application Visibility, the profile apply operation will still succeed. If a new AP that supports Application Visibility is added to the group at a later date, the profile will automatically be applied to that AP.

   Note: To apply a new profile to a switch with an existing profile, you must first remove the old profile from the switch before assigning the new one.

Removing a Signature Profile

As mentioned above, when applying a profile, only supported Devices/AP Groups **without** an assigned Signature Profile are displayed. If you want to apply a different profile to a Device/AP Group, you must first remove the old profile before applying a new one. The process is similar to applying a profile. Select the Signature Profile you want to remove from a Device/AP Group and click on the **Apply to Devices** button. The Devices/AP Groups to which the profile has been applied are displayed in the List of Selected Devices Table. Select a Device/AP Group and click on **REMOVE**. Click on the **Apply** button.

Deleting a Signature Profile

To delete a profile, select it and click on the Delete icon. Click **OK** at the confirmation prompt. Note that you cannot delete a Signature Profile that has been applied to devices on the network. You must first remove the profile from any devices before deleting it.

Summary View

The Application Visibility Summary View Screen is used to view information on switches configured for Application Visibility. Click on a switch to view which ports are enabled for monitoring/enforcement.

- **Friendly Name -** The device IP address.
- **Name -** The user-configured switch name.
- **MAC Address -** The switch MAC address.
- **Version -** The AOS software version installed on the switch (e.g. 8.2.1.309.R01).
- **Location -** The physical location of the switch (e.g., Lab).
- **Status -** The administrative status of the switch (Up/Down).
- **Type -** The switch model type (e.g., OS6860E-U28).
- **DNS Name -** The switch DNS name.
- **File Name -** The name of the Signature File contained in the Signature Profile (e.g.,
- UAppSig.upgrade_kit)
- **File Version -** The Signature File version (e.g., 1.1.2).
- **Profile Name -** The name of the Signature Profile assigned to the switch.

Settings

The Application Visibility Settings Screen is used to configure automatic Signature File update settings. Signature Files are regularly updated to either provide new signatures, or to update existing signatures which have changed. OmniVista can be configured to periodically check the ALE Signature File Repository to determine if a new Signature File is available. If "Signature Auto Update" is enabled, OmniVista will check the ALE Signature File Repository as configured below. If a new file version is available, OmniVista will automatically download the file and update any Signature Profiles using the older Signature File version. If "Auto Update" is enabled on a switch (configured on the Devices Management Screen), OmniVista will automatically update the switch if it is using the updated Signature Profile.

You can also check for a recent Signature File update any time by clicking on the **Update Now** button. And you can click on the **Test Connection** button to check if you have properly configured the URL Signature File Repository connection.

Configure the fields as described below. When you are finished, click on the **Save** button to save the new preferences to the OmniVista Server. Click on **Revert** to return a field to its previous value. Click on **Default** to return all values to the default settings.

> **Note:** Automatic Signature File updates are only supported on 8.x Signature Files (OS6860/6860E Switches).

Audit Configuration

- **Audit Switch Every -** How often OmniVista will check the Signature File version on Application Visibility-configured switches, in Hours. The audit is used to verify that Signature Files contained in a Signature Profile on a switch are in sync with the Signature Files stored in OmniVista. If the profile on a switch is out of sync with the Signature File in OmniVista, the status for the switch will be changed to "Out of Sync". (Range = 1 - 24, Default = 1)

Update Configuration

- **Check for Every -** How often OmniVista will check the Signature File Repository for updates (1 day, 7 days, 15 days, 30 days, None). If an update is available, OmniVista will automatically download the Signature Files. The first time you log into OmniVista, OmniVista will download the latest Signature Files from the Repository once an update time is configured and signature auto-update is enabled. ● **Update Time -** The number of hours after a new Signature File is downloaded that OmniVista will wait before updating the file on applicable Signature Profiles/switches. Note that an auto update job will only run in the same day if the auto update time is at least 1 hour later than the current time. **Signature Repository -** The location of the Signature File Repository (pre-filled *https://ep1.fluentnetworking.com/omnivista/signature/pull*).
- **User Name -** The username for the Signature File Repository (pre-filled - *omnivista*).
- **Password -** The password for the Signature File Repository (pre-filled).
- **Signature Auto Update -** Enables/Disables (On/Off) automatic Signature File check/download.

Notes:

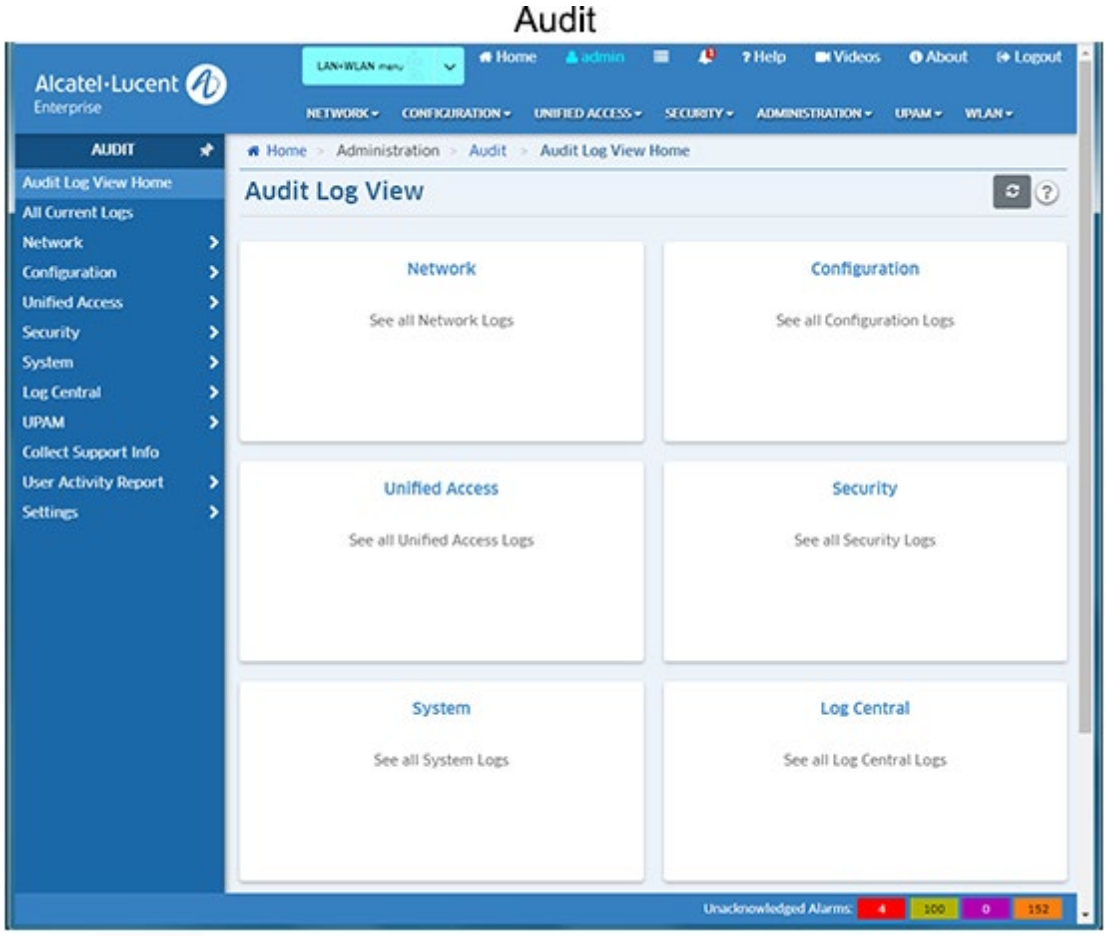
- If OmniVista fails to download signature files, it will retry 5 times. The interval between the retries is 5 minutes.
- The Signature Auto Update will only run in the same day if the auto update time is at least 1 hour later than the current time.
- OmniVista will log all actions (e.g., check update, download file, update to switches) in the "afn_autoupdate.log" file.

7.0 Audit

The Audit application is used to monitor client and server activity, such as the date and time when a user logged into OmniVista, when an item was added to the discovery database, when a configuration file was saved, or when a particular application was launched. The information is contained in log files, which are organized by type (e.g., Network, Configuration), as shown on the Audit Home Page.

The application enables you to view log files, search through log files, and download files. You can view current log files or historical log files that have been archived by OmniVista. Log Files are archived based on preferences configured on the Audit Settings Screen.

> **Note:** You can also click on the Collect Support Info link in the tree to collect log files from a network device that can be sent to Technical Support to troubleshoot problems.



Log Files by Type

You can click on one of the tiles on the home page to view the log files in a category (e.g., Network, Configuration), or you can click on a category on the left side of the screen to display a list of log files in the category. Click on a log file to display the contents of the file. The log files in each category are listed below.

> **Note:** Click on the "All Current Logs" link on the left side of the home page to display a list of all current logs. You can then click on a log to display the contents.

Network	Configuration	Unified Access
Analytics Predictive Service Analytics Service Analytics Service Worker AV Audit Service AV Auto Update AV Service Call Home Service Discovery Discovery Lite NG Discovery Polling Statistics Trap Config Traps VM Locator VM Manager Error VM Manager Service WMA	CLI Scripting Policy Resource Manager Resource Manager Backup Info Resource Manager Client Service Resource Manager Config SIP Service VLAN Creation Result VLAN Deletion Result VLAN Service VLAN Service Worker VXLAN Service	Access Guardian 2.0 BYOD mDNS Wireless Service
Security	**System**	**Log Central**
Quarantine	Active MQ Backup Restore DAL Service Data Migration FTP Service HSQL DB Poller Service Mongo DB Open LDAP OV 2500 Server OV Client Redis Scheduled Backup Scheduler Service Syslog Telegraf Tomcat Catalina Tomcat Host Manager Tomcat Local Host Tomcat Local Host Access Log Tomcat Manager Tomcat OV Report Tomcat OV Web VA Config VA Upgrade Watchdog CLI Watchdog Service Worker Poller Service	Log Central
UPAM	**User Activity Report**	
Jetty Radius UPAM	User Activity Report	

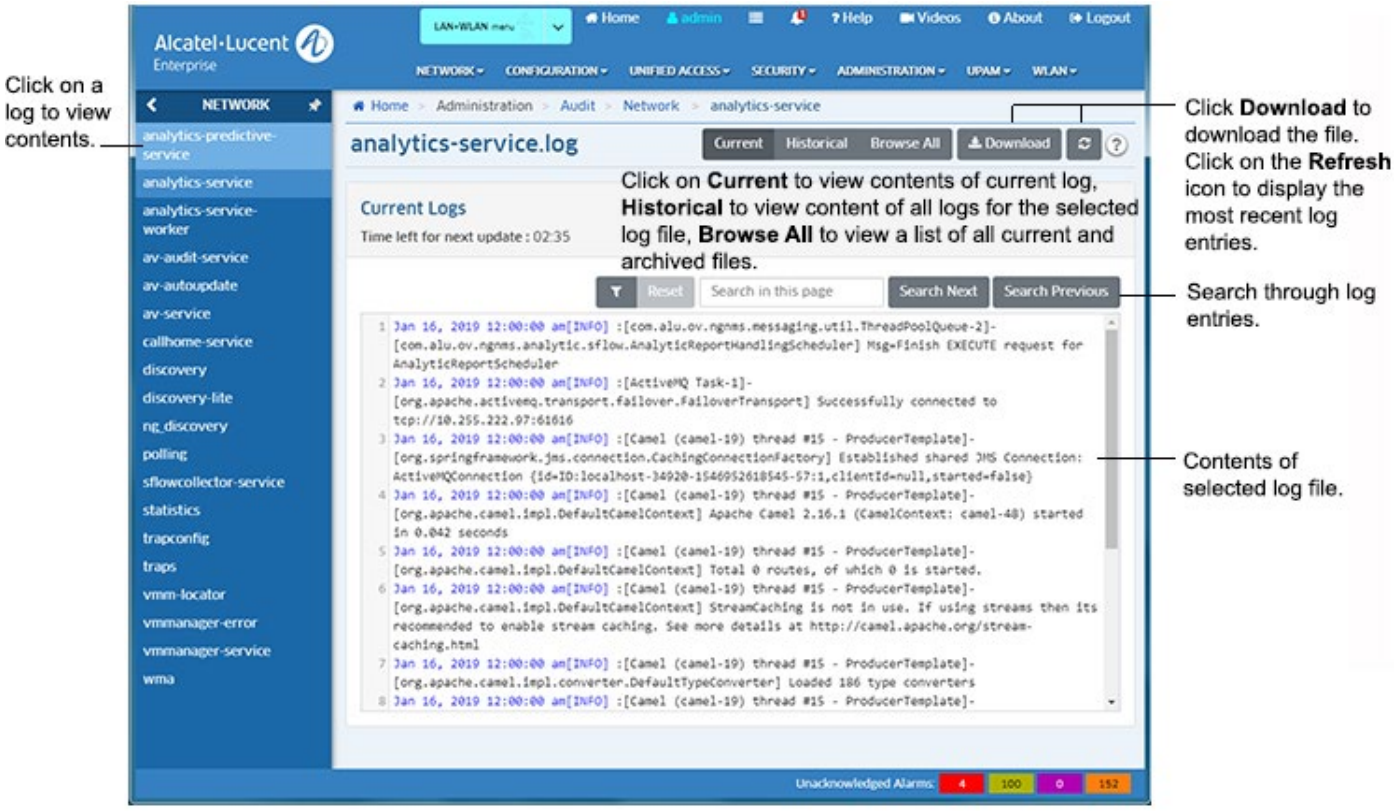
Note: The Log Central link displays the ngnms.log file. This file includes log entries from all log files in real time, with the most recent entries at the top of the file. You can scroll through the file using the scroll bar and arrows on the right side of the screen, or you can also search by keyword. Enter the search criteria in the "Search in this page" field at the top of the log file and click on the **Search Nex**t button. The word or phrase is highlighted in yellow throughout the file. You can scroll through the file or click on the **Search Next** or **Search Previous** buttons to search through the file. Click on the Cancel Search icon **x** at the top of the table to cancel the search.

You can also create and apply a filter to display specific log entries only. Click on the Filter icon to bring up the Filter Selection window. Select an existing filter and click on the **Apply** button to apply the filter to the current display. You can also click on the Add icon to create a new filter. Enter a Filter Name and Filter Description, set the conditions for the filter and click on the **Add** button. Then select the filter to apply it to the current display. Click on the **Reset** button to cancel the filter and return to the unfiltered view of the file.

Click on the **Current** button (default) to display the contents of the current file. Click on the **Historical** button to display all ngnms.log file information, including archived files. Click on the **Browse All** button to view a list of all archived ngnms.log Files. Click on a file in the list to display the contents of the file. Click on the **Download** button at the top of the screen to save the file to your computer. Click on the Refresh icon to refresh the display with the most recent log entries.

Viewing Log Files

By default, when you click on a log file (e.g., discovery.log, polling.log) the most current log entries are displayed. This "current" view is determined by the settings you configure on the Settings Screen. Once the number of entries reaches the configured number, the log file is archived with the current date and stored in OmniVista. When viewing a log file, the Audit application enables you to view the contents of the current selected log file, view the contents of all log files (current and archived) for the selected log file, or a view list of archived files, which you can then open and view.



To view a log file, click on a log file type the Home Page (e.g., Network, Configuration), or click on a log file type on the left side of the screen to display the list of log files for that type. Click on a log file (e.g., discovery.log, polling.log) to display the contents of the file. By default, the contents of the most current log file are displayed. This "current" view will display all of the contents that have not been archived. To view the contents of all log files for the selected log file (current and archived) click on the **Historical** button at the top of the screen.

To view a list of all log files (current and archived), click on the **Browse All** button at the top of the screen. A list of all log files for the selected log is displayed. The current log file is displayed at the top (e.g., polling.log) followed by all of the archived log files, identified by the date and time the file was archived (e.g., polling_04-29-2016_061727PM.rou). Click on a log file to display the contents of the file.

You can also download the contents of any log file you are viewing by clicking on the **Download** button at the top of the screen. The contents of the file can then be saved to your computer. Click on the Refresh icon to refresh the display with the most recent log entries.

Searching Through Log Files

You can scroll through the contents of a log file using the scroll bar and arrows on the right side of the screen. You can also search a log file by keyword. Enter the search criteria in the "Search in this page" field at the top of the log file and click on the **Search Nex**t button. The word or phrase is highlighted in yellow throughout the file. You can scroll through the file or click on the **Search Next** or **Search Previous** buttons to search through the file. Click on the Cancel Search icon **x** at the top of the table to cancel the search.

Filtering Log File Entries

You can create and apply a filter to display specific log entries only. Click on the Filter icon to bring up the Filter Selection window. Select an existing filter and click on the **Apply** button to apply the filter to the current display. You can also click on the Add icon to create a new filter. Enter a Filter Name and Filter Description, set the conditions for the filter and click on the **Add** button. Then select the filter to apply it to the current display. Click on the **Reset** button to cancel the filter and return to the unfiltered view of the file.

Downloading Log Files

You can download the contents of any log file you view by clicking on the **Download** button at the top of the screen. The contents of the log file will be downloaded as a text file that can be opened with any text editor.

All Current Logs

The Audit All Current Logs Screen displays a list of all current logs. Scroll or search through the list and click on a file to display the contents of the file. Select a file and click on the **Download** button to download the file to your computer. Click on the **Download All** button to download all of the log files to your computer. The files will be saved in a Zip file.

Collect Support Information

The Audit Collect Support Information Screen is used to collect log information from a network device that you can send to Alcatel-Lucent Enterprise (ALE) Technical Support to troubleshoot problems. The log files you specify are collected and downloaded to your OmniVista Client's "Download" Folder in a ZIP File that you can then send to Technical Support. This feature is **not** supported on wireless devices.

Collecting Log Files

Select a device, select the information to be collected as described below, then click on the **Collect** button to download the specified log files. You can only collect log files from one device at a time. Repeat to collect logs from additional devices.

- **Collect swlog files -** Enable (On) this field to collect all switch log files (On/Off, Default = On).
- **Collect cfg files -** Enable (On) this field to collect configuration files (e.g., boot.cfg, vcboot.cfg) from the Certified and Working Directories (On/Off, Default = On).
- **Select Tech Support -** Select the type(s) of Tech Support log files you want to download. By default, all file types are selected, however, you can select one or more specific types.
- **None (0 Selected) -** If you do not select any type of Tech Support log files, OmniVista will download all Configuration and Switch Log Files.
- **Show Tech Support -** Includes all Configuration and Switch Log Files plus tech support log file information (device hardware, firmware information).
- **Show Tech Support Layer 2 -** Includes all Configuration and Switch Log Files plus Layer 2 log file information (Layer 2 interface information).

- **Show Tech Support Layer 3 -** Includes all Configuration and Switch Log Files plus Layer 3 log file information (Layer 3 IP information)
- **Show Tech Support Engineering -** Includes all Configuration and Switch Log Files plus Engineering log file information (Virtual Chassis information). This file is only available for 7x/8x switches.

Files are downloaded in a ZIP file with the device IP Address and date and time in the file name. For example, 10.255.225.237_20180306145346 indicates that the files are from 10.255.225.237 and were collected on March 6, 2018 at 2:53:46 p.m. The date and times reflect the location of the OmniVista Server collecting the logs.

User Activity Report

The Audit User Activity Report Settings screen is used to set the number of days the User Activity Report is retained. Configure the number of days within the range described below, then click on the **Apply** button. To revert back to a previous value, click on the **Revert** button.

- **Maximum Days To Retain -** The number of days to retain the User Activity Report. (Range: 7 - 365 days, Default = 90 days)

Settings

The Audit Settings Screen is used to specify Audit Log File preferences. Configure a field as described below and click the **Apply** button. The changes take effect immediately. If you change a field configuration, you can click on the **Revert** button to revert a field to the previous setting. Click on the **Default** button to set all of the fields to the default settings.

- **Maximum Audit Entries -** The maximum number of entries that can exist in any one log file (Range = 50 - 10,000, Default = 2,000). Any entry in excess of the value in this field will cause the current log file to be archived. For example, if the field is set to 1,000 entries, and a log file contains 1,000 entries, when the next entry is received the following will occur:
- The current log file will be archived with 1,000 entries.
- A new version of the file will be created that contains the latest entry.
- **Maximum Audit File Copies -** The maximum number of audit files that can be created. When the audit file reaches the configured maximum number of audit entries, the file is saved and a new file is started (Range = 0 - 100, Default = 5).
- **Max Log File Size -** The maximum log file size, in KB (Range = 1 - 30,000, Default = 10,240). Any entry in the file that increases the file size beyond the value in this field will cause current files to be archived. For example, if the field is set to 5120 KB, and a file is at a file size of 5120 KB, when the next entry is received the following will occur:
- The current file will be archived with 5120 KB of information. The archive file will be located at *installation directory*/data/logs.
- A new version of the file will be created that contains the latest entry.

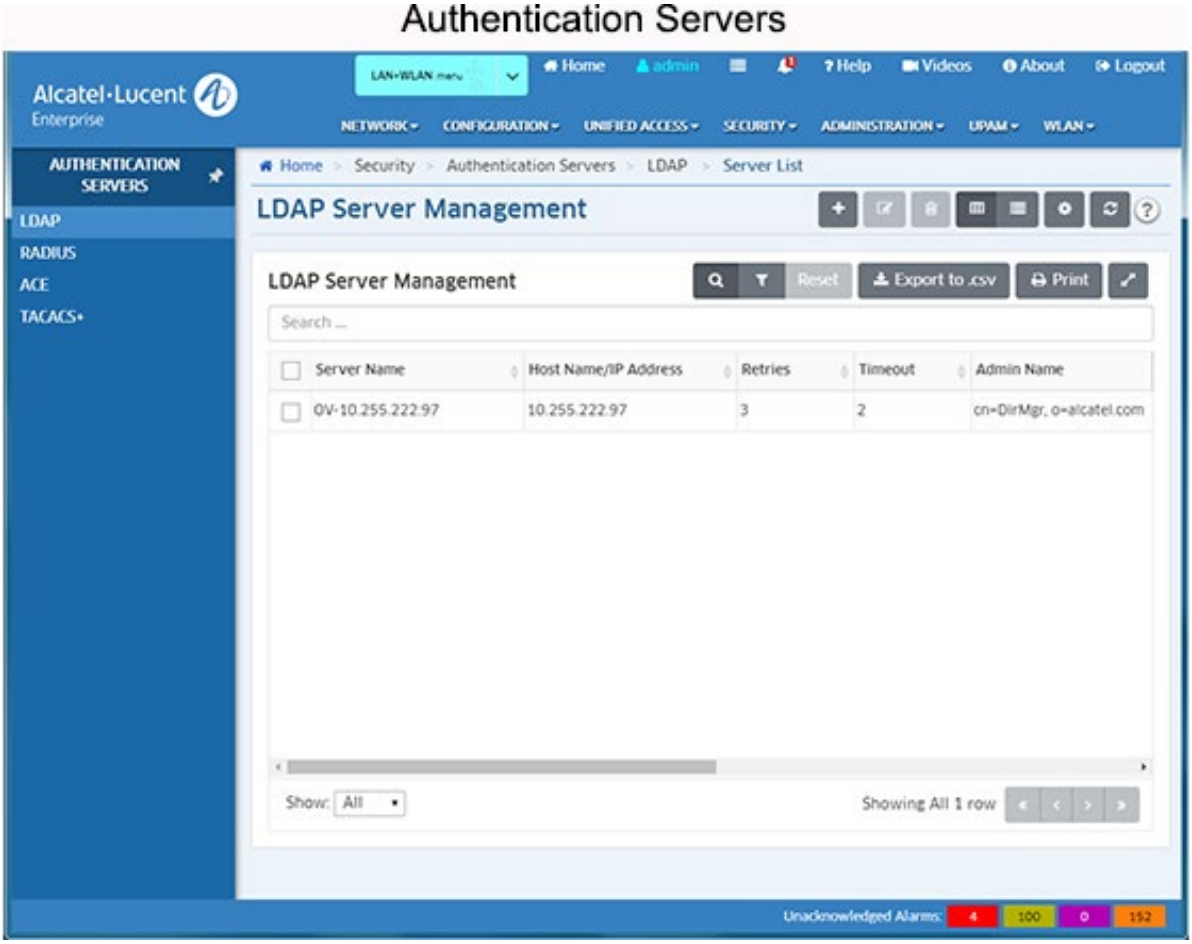
8.0 Authentication Servers

The Authentication Servers application enables you to create, modify, and delete authentication servers in OmniVista. An authentication server could be an LDAP, RADIUS, ACE, or TACACS+ Server. Any authentication server that you want to use, other than the default OmniVista LDAP Server, must be added to OmniVista. Adding a server to OmniVista basically informs OmniVista that the server exists. OmniVista does not search the network to locate available authentication servers, so any server that you add to OmniVista should actually exist (or should exist in the near future). When you add a server, you can also specify other information such as:

- Operating parameters for switches that will use the server for authentication, such as the number of retries the switch will attempt while communicating with the server.
- The user name and password used to login to the server (if applicable).
- The location of the server to be used as a "backup" server if the added server becomes unavailable.

Note: OmniVista cannot manage authentication server content.

When you open the Authentication Servers application, the LDAP Server Management Screen is displayed, and links to the LDAP, RADIUS, ACE, and TACACS+ screens are displayed on the left.



LDAP Servers

Lightweight Directory Access Protocol (LDAP) is a standard directory server protocol. The LDAP Server Management Screen lists all LDAP Authentication Servers known to OmniVista. It also enables you to add, modify, and delete LDAP Servers from the list of LDAP Servers known to OmniVista. By default, the OmniVista LDAP Server is automatically installed with OmniVista. However, any LDAP V3 server can be added to the list of known LDAP Servers.

RADIUS Servers

Remote Authentication Dial-in User Service (RADIUS) is a standard authentication and accounting protocol defined in RFC 2865 and RFC 2866. A built-in RADIUS Client is available in Alcatel-Lucent Enterprise AOS Switches. A RADIUS Server that supports Vendor Specific Attributes (VSAs) is required. VSAs carry specific authentication, authorization, and configuration details about RADIUS requests to and replies from the server. The RADIUS Server Management Screen lists all RADIUS Authentication Servers known to

OmniVista. It also enables you to add, modify, and delete Servers from the list of RADIUS Servers known to OmniVista.

ACE Servers

You can use a single external ACE Server for authentication of all switch access types. You are limited to a single ACE Server, because file **sdconf.rec** must be FTPed from the ACE Server to the switch's **/network** directory, to inform the switch of the ACE Server's IP address and other configuration information. This requirement means that the switch can communicate with only a single ACE Server at any one time. The ACE Server Management Screen enables you to add a single ACE Server to OmniVista. It also enables you to delete an ACE Server. An ACE Server cannot be configured or modified from OmniVista because all configuration information is contained in **sdconf.rec** file.

TACACS+ Servers

Terminal Access Controller Access Control System (TACACS+) is a standard authentication and accounting protocol defined in RFC 1321 that employs TCP for reliable transport. A built-in TACACS+ Client is available in the switch. A TACACS+ Server allows access control for routers, network access servers, and other networked devices through one or more centralized servers. The protocol also allows separate authentication, authorization, and accounting services. By allowing arbitrary length and content authentication exchanges, it allows clients to use any authentication mechanism. The TACACS+ Server Management Screen lists all TACACS+ Authentication Servers known to OmniVista. It also enables you to add and, modify, and delete Servers from the list of TACACS+ Servers known to OmniVista.

LDAP Server Management

The Authentication Servers LDAP Server Management Screen displays all LDAP Authentication Servers known to OmniVista. It also enables you to add, modify, and delete LDAP Servers from the list of LDAP Servers known to OmniVista. Lightweight Directory Access Protocol (LDAP) is a standard directory server protocol. The LDAP Client in the switch is based on several RFCs: 1798, 2247, 2251, 2252, 2253, 2254, 2255, and 2256. The protocol was developed as a way to use directory services over TCP/IP and to simplify the Directory Access Protocol (DAP) defined as part of the Open Systems Interconnection (OSI) effort. Originally, LDAP was a front-end for X.500 DAP.

The LDAP protocol synchronizes and governs the communications between the LDAP Client and the LDAP Server. The protocol also dictates how database information, which is normally stored in hierarchical form, is searched from the root directory down to distinct entries. In addition, LDAP has its own format that permits LDAP-enabled Web browsers to perform directory searches over TCP/IP.

The OmniVista LDAP Server is automatically installed in OmniVista. You cannot modify or delete it. However, if you want to use a different LDAP V3 server, you must add it to OmniVista. OmniVista only manages the built-in LDAP Server, other authentication servers must be managed outside of OmniVista. You can assign switches to such servers, but the Authentication Servers application does not allow you to add, modify, or delete users and user privileges in the LDAP database of such servers. This is because an LDAP Server's database must be configured for the specific schema used to manage users and there is no public API for configuring LDAP schemas.

> **Note:** LDAP Server Management supports both AOS and wireless devices; however certain attributes may not be supported on wireless devices. See the configuration fields below for more information.

Adding an LDAP Server

As mentioned earlier, the OmniVista LDAP Server is automatically installed in OmniVista and known to OmniVista. However, if you have configured a new LDAP Server, you must add it to the list of LDAP Servers known to OmniVista. To add a new LDAP Server, click on the Add icon and complete the fields as described below. When you are finished, click the **Create** button.

- **Server Name -** A unique name for the LDAP Authentication Server. This name will be used by OmniVista and the switch to identify the server.
- **Host Name/IP Address -** The name of the computer where the server is located OR the IP address of the computer where the server is located.
- **Backup Host Name/IP Address -** Each LDAP Server may optionally have a backup server. If you wish to define a backup server that will be used if this server is unavailable, enter the name of the computer where the backup server is located OR enter the IP address of the computer where the backup server is located.
- **Retries -** The number of retries that you want the switch to attempt when trying to contact the LDAP Server (Range = 1 - 3, Default = 3). (Not supported on wireless devices and ignored when applied to those devices.)
- **Timeout -** The number of seconds that you want the switch to wait before a request to the LDAP authentication server is timed out (Range = 1 - 30, Default = 2).
- **Password -** Password used to login to the LDAP Server (up to 128 characters).

- **Confirm Password -** Re-enter the LDAP Server password.
- **SSL -** Set this field to inform the switch whether SSL (Secure Socket Layer) is enabled or disabled on the LDAP authentication server. SSL can be set up on the server for additional security. (This usually involves adding digital certificates to the server.) When SSL is enabled, the server's identity will be authenticated. Refer to "Managing Authentication Servers" in your *Network Configuration Guide* and to the instructions provided by the LDAP Server's vendor for further information on setting up SSL on the LDAP Server. Select one of the following settings for this field (Default = NS):
  - **NS** - Non-secure encryption between UPAM and the LDAP Server.
  - **True** - SSL is enabled on the LDAP authentication server. When enabled:
    - LDAPS Certificates - Select an LDAP Certificate from the drop-down. You can also click on the "Add New" link to go to the LDAPS Certificate Screen and create a new certificate.
  - **False** - SSL is disabled on the LDAP authentication server.
- **Port -** The port number used as the LDAP port address. This is the port at which the LDAP Server "listens". By default, the port number is 389. However, note that the switch automatically sets the port number to 636 when SSL is enabled. (Port number 636 is typically used on LDAP Servers for SSL.) The port number on the switch must match the port number configured on the server.
- **Admin Name -** The name used to login to the LDAP Server.
- **Search Base -** The search base in the LDAP Server where authentication information can be found (e.g., o=alcatel.com).
- **VRF Name -** The VRF Instance associated with the LDAP Server, if applicable. Note that VRF is not supported when authenticating an OmniVista login via LDAP.
- **Use as On-Premises Server** - Select this option if you want to use a private LDAP/AD Server instead of one in cloud for AP authentication. In this scenario, user authentication requests are communicated directly between an AP and the LDAP/AD server and are not exposed in the public network. This option is only supported for BYOD access.

Note: SSL communication with the LDAP Server is not supported on OS6860 Switches (AOS 8.1.1 R01).

Modifying an LDAP Server

Select an LDAP Server in the list and click on the Edit icon. Edit any necessary fields as described above, then click on the **Save** button. It is important to note that you cannot modify values indiscriminately. The values must match those of the actual LDAP Server. For example, if you want to change the LDAP port address, you must first use the tools provided by your LDAP Server's vendor to change the port on the LDAP Server itself. You can then inform OmniVista that the port number has changed by modifying the **Port** field. Also note that you cannot edit an LDAP Server's name. You must delete it and create a new one.

Note: You cannot delete an LDAP Server that is currently being used by OmniVista.

Deleting an LDAP Server

Select an LDAP Server in the list and click on the Delete icon. Note that deleting an LDAP server will not cause switches that currently use that server to cease using it. Switches using the deleted LDAP Server will continue to use it until the switches are reassigned.

Configuring an LDAP Server

As mentioned earlier, the OmniVista LDAP Server is automatically installed along with the authentication server. However, if you want to use a different LDAP V3 server, you must add it to OmniVista. You can assign switches to such servers, but the Authenticated Servers application does not allow you to add, modify, or delete users and user privileges in the LDAP database of such servers. This is because an LDAP Server's database must be configured for the specific schema used to manage users and there is no public API for configuring LDAP schemas.

Before you add an LDAP Server to OmniVista's list of available authentication servers, you must first install the LDAP Server based on the instructions provided by the LDAP Server's vendor. You must then modify the LDAP Server's schema to add the LDAP objects required to manage Alcatel-Lucent Enterprise Switches, and configure user accounts on the server.

Required LDAP Schema Objects

The following objects must be added to an LDAP Server's schema so that it can manage Alcatel-Lucent Enterprise Switches. To modify the schema, follow the vendor's instructions. Each LDAP vendor provides a different way of modifying the schema.

- attribute accountfailtime oid-ataccountfailtime cis
- attribute accountstarttime oid-ataccountstarttime cis
- attribute accountstoptime oid-ataccountstoptime cis
- attribute numberofswitchgroups oid-atnumberofswitchgroups int single
- attribute switchgroups oid-atswitchgroups int
- attribute switchserialnumber oid-atswitchserialnumber cis
- attribute switchslotport oid-atswitchslotport cis
- attribute clientipaddress oid-atclientipaddress cis
- attribute clientmacaddress oid-atclientmacaddress cis
- attribute userPermissions oid-atuserPermissions int single
- attribute pm-access-priv-read-1 oid-atpm-access-priv-read-1 cis single
- attribute pm-access-priv-read-2 oid-atpm-access-priv-read-2 cis single
- attribute pm-access-priv-write-1 oid-atpm-access-priv-write-1 cis single
- attribute pm-access-priv-write-2 oid-atpm-access-priv-write-2 cis single
- attribute pm-access-priv-global-1 oid-atpm-access-priv-global-1 cis single
- attribute pm-access-priv-global-2 oid-atpm-access-priv-global-2 cis single
- attribute bop-asa-func-priv-read-1 oid-atbop-asa-func-priv-read-1 int single
- attribute bop-asa-func-priv-read-2 oid-atbop-asa-func-priv-read-2 int single
- attribute bop-asa-func-priv-write-1 oid-atbop-asa-func-priv-write-1 int single
- attribute bop-asa-func-priv-write-2 oid-atbop-asa-func-priv-write-2 int single

- attribute allowedTime oid-atallowedTime cis single
- attribute bop-asa-geo-priv-profile-number oid-atbop-asa-geo-priv-profile-number int single
- attribute bop-md5key oid-atbop-md5key cis single
- attribute bop-shakey oid-atbop-shakey cis single
- attribute bop-asa-snmp-level-security oid-atbop-asa-snmp-level-security int single

Configuring User Accounts on the Server

When you use an LDAP Server other than the OmniVista LDAP Server, you must set up all user accounts on the server based on the instructions provided by the LDAP Server's vendor. An OmniVista user is assigned a User Role based on information returned from the LDAP Server. The following use cases demonstrate how the User Role is assigned:

Scenario	OmniVista Group	OmniVista User Role	OmniVista Login
Username created on the LDAP/AD Server but not mapped to any groups on the server.	User successfully logs into OmniVista and is assigned to the "Default" Group	The "Default" Group is assigned to the "Read" User Role	User has read-only access
Username created and mapped to a group on the LDAP/AD Server	User successfully logs into OmniVista and is assigned to the matching Group in OmniVista	The User Role assigned to the matching OmniVista Group	User has access based on the User Role mapped to the assigned Group
Username created and mapped to a group on the LDAP/AD Server	No matching Group in OmniVista; user cannot log into OmniVista	N/A	N/A

See the Users and User Group online help for more information.

LDAP Server Management Table

The LDAP Server Management Table displays information about all LDAP Servers known to OmniVista.

- **Server Name -** A unique name for the LDAP Authentication Server. This name will be used by OmniVista and the switch to identify the server.
- **Host Name/IP Address -** The name of the computer where the server is located OR the IP address of the computer where the server is located.
- **Retries -** The number of retries that you want the switch to attempt when trying to contact the LDAP Server (Range = 1 - 3, Default = 3). (Not supported on wireless devices and ignored when applied to those devices.)
- **Timeout -** The number of seconds that you want the switch to wait before a request to the LDAP authentication server is timed out (Range = 1 - 30, Default = 2).
- **Admin Name -** The name used to login to the LDAP Server.

- **Search Base -** The search base in the LDAP Server where authentication information can be found (e.g., o=alcatel.com).
- **Port -** The port number used as the LDAP port address. This is the port at which the LDAP Server "listens". By default, the port number is 389. However, note that the switch automatically sets the port number to 636 when SSL is enabled. (Port number 636 is typically used on LDAP Servers for SSL.) The port number on the switch must match the port number configured on the server.
- **SSL -** Set to **NS**,**True** or **False** to inform the switch whether SSL (Secure Socket Layer) is enabled or disabled on the LDAP authentication server. SSL can be set up on the server for additional security. (This usually involves adding digital certificates to the server.) When SSL is enabled, the server's identity will be authenticated. Refer to "Managing Authentication Servers" in your *Network Configuration Guide* and to the instructions provided by the LDAP Server's vendor for further information on setting up SSL on the LDAP Server. (Not supported on wireless devices and ignored when applied to those devices.)
- **LDAPS Certificate** - The name of the LDAP Certificate selected when SSL is set to True.
- **Backup Host Name/IP Address -** Each LDAP Server may optionally have a backup server. If you wish to define a backup server that will be used if this server is unavailable, enter the name of the computer where the backup server is located OR enter the IP address of the computer where the backup server is located.
- **VRF Name -** The VRF Instance associated with the LDAP Server, if applicable. Note that VRF is not supported when authenticating an OmniVista login via LDAP.

RADIUS Server Management

The Authentication Servers RADIUS Server Management Screen displays all RADIUS Servers known to OmniVista. It also enables you to add, edit, and delete RADIUS Servers from the list of RADIUS Servers known to OmniVista. A built-in RADIUS Client is available in the switch. A RADIUS Server that supports Vendor Specific Attributes (VSAs) is required. VSAs carry specific authentication, authorization, and configuration details about RADIUS requests to and replies from the server. Refer to "Managing

Authentication Servers" in your *Network Configuration Guide* for specific information on the VSAs required. Before you add a RADIUS Server to OmniVista's list of RADIUS Servers known to OmniVista, you must first install and configure the RADIUS Server.

> **Note**: You cannot add, modify, or delete users and user privileges from RADIUS Servers in OmniVista.
>
> **Note:** RADIUS Server Management supports both AOS and wireless devices; however certain attributes may not be supported on wireless devices. See the configuration fields below for more information.
>
> **Note:** If you change the Shared Secret of the UPAM Radius Server, you also must update Shared Secret of NAS Client on the NAS Clients Screen (UPAM - Authentication - NAS Clients).
>
> **Note:** If OmniVista is running in a High-Availability (HA) configuration, you must set both the Active **and** Standby Node IP addresses as "Trusted" on the RADIUS Server.

Adding a RADIUS Server

After configuring a RADIUS Server, you must add it to the list of RADIUS Servers known to OmniVista. To add a new RADIUS Server, click on the Add icon and complete the fields as described below. When you are finished, click the **Create** button.

- **Server Name -** Unique name for the RADIUS Server. This name will be used by OmniVista and the switch to identify the Server.
- **Host Name/IP Address -** The name of the computer where the server is located OR the IP address of the computer where the Server is located.
- **Backup Host Name/IP Address -** Each RADIUS Server may optionally have a backup server. If you wish to define a backup server that will be used if this server is unavailable, enter the name of the computer where the backup server is located OR enter the IP address of the computer where the backup Server is located. (Not supported on wireless devices and ignored when applied to those devices.)
- **Retries -** The number of retries that you want the switch to attempt when trying to contact the RADIUS Server (Range = 1 - 3, Default = 3).
- **Timeout - Th**e number of seconds that you want the switch to wait before a request to the RADIUS Server is timed out (Range = 1 - 30, Default = 2).
- **Shared Secret -** The password to the RADIUS Server (maximum of 64 characters). The "Shared Secret" is essentially the server password. Note that the password you enter must be configured identically on the RADIUS Server. Also note that if you use a remote RADIUS Server with a Shared Secret greater than 16 characters, OmniVista only supports PAP and CHAP authentication.
- **Confirm Secret -** Re-enter the Shared Secret.
- **Authentication Port -** The port you to access the Server (Range = 1 - 65535, Default = 1812).
- **Accounting Port -** The port for accounting information (Range = 1 - 65535, Default = 1813).
- **VRF Name -** The VRF Instance associated with the RADIUS Server, if applicable. A RADIUS Server can be configured on any VRF instance including the default VRF instance. However, all of the servers (for example, all the RADIUS servers) must reside on the same VRF instance. Default value is "default". (Not supported on wireless devices and ignored when applied to those devices.)

Editing a RADIUS Server

Select a RADIUS Server in the list and click on the Edit icon. Edit any necessary fields as described above, then click on the **Save** button. It is important to note that you cannot modify values indiscriminately. The values must match those of the actual RADIUS Server. For example, if you want to change the RADIUS Authentication port, you must first use the tools provided by your RADIUS Server's vendor to change the port on the RADIUS Server itself. You can then inform OmniVista that the port number has changed by modifying the **Authentication Port** field.

Deleting a RADIUS Server

Select a RADIUS Server in the list and click on the Delete icon. Note that deleting an authentication server from the list of RADIUS Servers known to OmniVista will not cause

switches that currently use that RADIUS Server to cease using it. Switches using the deleted RADIUS Server will continue to use it until the switches are reassigned.

Configuring a RADIUS Server

Before you add a RADIUS Server to OmniVista's list of RADIUS Servers known to OmniVista, you must first install and configure the RADIUS Server, then configure user accounts on the Server.

Configuring the Server

Before you add a RADIUS Server to OmniVista's list of available authentication servers, you must first install the RADIUS Server based on the instructions provided by the RADIUS Server's vendor. Then, you must configure the RADIUS Server with the vendor specific attributes. These attributes carry specific authentication, authorization, and configuration details about RADIUS requests to and replies from the server. Refer to "Managing Authentication Servers" in your Network Configuration Guide for specific information on the VSAs required.

Configuring User Accounts on the Server

When you use a RADIUS Server for User Authentication, you must set up all user accounts on the server based on the instructions provided by the RADIUS Server's vendor. However, the authorization which includes the access level associated with each user will be controlled by the OmniVista server, based on the group a user is associated with. You cannot set up user accounts from OmniVista for any authentication server other than the OmniVista LDAP server, which is automatically installed with the Authentication Servers application.

Once you have installed, configured, and set up the user accounts on the RADIUS Server, you are ready to add the server to OmniVista.

RADIUS Server Management Table

The RADIUS Server Management Table displays information about all RADIUS Servers known to OmniVista.

- **Server Name -** Unique name for the RADIUS Server. This name will be used by OmniVista and the switch to identify the Server.
- **Host Name/IP Address -** The name of the computer where the server is located OR the IP address of the computer where the Server is located.
- **Retries -** The number of retries that you want the switch to attempt when trying to contact the RADIUS Server (Range = 1 - 3, Default = 3).
- **Timeout - The** number of seconds that you want the switch to wait before a request to the RADIUS Server is timed out (Range = 1 - 30, Default = 2).
- **Authentication Port -** The port you to access the Server (Range = 1 - 65535, Default = 1812).
- **Accounting Port -** The port for accounting information (Range = 1 - 65535, Default = 1813). **VRF Name -** The VRF Instance associated with the RADIUS Server, if applicable. A RADIUS Server can be configured on any VRF instance including the default VRF instance. However, all of the servers

- (for example, all the RADIUS servers) must reside on the same VRF instance. Default value is "default". (Not supported on wireless devices and ignored when applied to those devices.)
- **Backup Host Name/IP Address -** Each RADIUS Server may optionally have a backup server. If you wish to define a backup server that will be used if this server is unavailable, enter the name of the computer where the backup server is located OR enter the IP address of the computer where the backup Server is located. (Not supported on wireless devices and ignored when applied to those devices.)

ACE Server Management

The Authentication Servers ACE Server Management Screen can be used to add or delete an ACE Server. You can use a single external ACE Server for authentication of all switch access types. You are limited to a single ACE Server, because file **sdconf.rec** must be FTPed from the ACE Server to the switch's **/network** directory, to inform the switch of the ACE Server's IP address and other configuration information. This requirement means that the switch can communicate with only a single ACE Server at any one time. The ACE Server Management Screen enables you to add a single ACE Server to OmniVista. It also enables you to delete an ACE Server. An ACE Server cannot be configured or modified from OmniVista because all configuration information is contained in **sdconf.rec** file. Note that an ACE Server cannot be used for Layer 2 authentication or for policy.

Adding an ACE Server

Once you have installed and configured the ACE Server, you must add it to the list of ACE Servers known to OmniVista. To add a new ACE Server, click on the Add icon. When you assign the ACE Server to switches, the authentication server will automatically configure the switches to operate with the server.

Deleting an ACE Server

To delete an ACE Server from OmniVista, select the Server and click on the Delete icon. Deleting the ACE Servers known to OmniVista will not cause switches that currently use that ACE Server to cease using it. Switches using the deleted ACE Server will continue to use it until the switches are reassigned.

Configuring an ACE Server

Before you add the ACE Server to OmniVista, you must first install the ACE Server, based on the instructions provided by your ACE Server's vendor. You must also set up user accounts on the ACE Server. There are no server-specific parameters that must be configured for the switch to communicate with an attached ACE Server; however, you must FTP the **sdconf.rec** file from the server to the switch's **/network** directory. This file is required so that the switch will know the IP address of the ACE Server and other configuration information. For information about loading files into the switch, see the *OmniSwitch Switch Management Guide*.

> **Note:** An ACE Server stores and authenticates switch user accounts (i.e., user IDs and passwords), but does NOT store or send user privilege information to the switch. User privileges for logins are determined by the switch itself. When a user attempts to log into the switch, the user ID and password are sent to the ACE Server. The server determines whether the login is valid or not. If the login is valid, the user privileges must be determined. The switch checks its user database for the

user's privileges. If the user is not in the database, the switch uses the default privilege, which is determined by the default user account. For information about the default user account, see the "Switch Security" chapter of the *OmniSwitch Switch Management Guide*.

The ACE client in the switch is version 4.1; it does not support the replicating and locking feature of ACE 5.0, but it may be used with an ACE 5.0 server if a legacy configuration file is loaded on the server. The legacy configuration must specify authentication to two specific servers (master and slave). See the RSA Security ACE Server documentation for more information.

TACACS+ Server Management

The Authentication Servers TACACS+ Server Management Screen displays all TACACS+ Authentication

Servers known to OmniVista. It also enables you to add, edit, and delete TACACS+ Servers from the list of TACACS+ Servers known to OmniVista. Terminal Access Controller Access Control System (TACACS+) is a standard authentication and accounting protocol defined in RFC 1321 that employs TCP for reliable transport. A built-in TACACS+ Client is available in the switch. A TACACS+ Server allows access control for routers, network access servers, and other networked devices through one or more centralized servers. The protocol also allows separate authentication, authorization, and accounting services. By allowing arbitrary length and content authentication exchanges, it allows clients to use any authentication mechanism.

The TACACS+ Client offers the ability to configure multiple TACACS+ Servers. When the primary server fails, the client tries the subsequent servers. Multiple server configurations are applicable only for backup and not for server chaining.

Note: TACACS+ Server Management supports both AOS and wireless devices; however certain attributes may not be supported on wireless devices. See the configuration fields below for more information.

Adding a TACACS+ Server

Once you have installed, configured, and set up the user accounts on the TACACS+ Server, you are ready to add the server to OmniVista. To add a new TACACS+ Server, click on the Add icon and complete the fields as described below. When you are finished, click the **Create** button.

- **Server Name -** A unique name for the TACACS+ Authentication Server. This name will be used by OmniVista and the switch to identify the server.
- **Host Name/IP Address -** The name of the computer where the server is located OR the IP address of the computer where the server is located.
- **Backup Host Name/IP Address -** Each TACACS+ Server may optionally have a backup server. If you wish to define a backup server that will be used if this server is unavailable, enter the name of the computer where the backup server is located OR enter the IP address of the computer where the backup server is located.
- **Timeout -** The number of seconds that you want the switch to wait before a request to the TACACS+ authentication server is timed out. Default value is 2.

- **Shared Secret -** The password to the Server. (The "shared secret" is essentially the server password.) Note that the password you enter must be configured identically on the Server.
- **Confirm Shared Secret -** Re-enter the Shared Secret.
- **Port -** The port number used to access the TACACS+ Server (Default = 49).
- **VRF Name -** The VRF Instance associated with the TACACS+ Server, if applicable. A TACACS+ Server can be configured on any VRF instance including the default VRF instance. However, all of the servers (for example, all the TACACS+ servers) must reside on the same VRF instance. Default value is "default". (Not supported on wireless devices and ignored when applied to those devices.)

Editing a TACACS+ Server

Select a TACACS+ Server in the list and click on the Edit icon. Edit any necessary fields as described above, then click on the **Save** button. It is important to note that you cannot modify values indiscriminately. The values must match those of the actual TACACS+ Server. For example, if you want to change the TACACS+ authentication port, you must first use the tools provided by your TACACS+ Server's vendor to change the port on the TACACS+ Server itself. You can then inform OmniVista that the port number has changed by modifying the **Port** field.

Deleting a TACACS+ Server

Select a TACACS+ Server in the list and click on the Delete icon. Note that deleting a TACACS+ Server will not cause switches that currently use that TACACS+ Server to cease using it. Switches using the deleted TACACS+ Server will continue to use it until the switches are reassigned.

TACACS+ Server Management Table

The TACACS+ Server Management Table displays information about all TACACS+ Authentication Servers known to OmniVista.

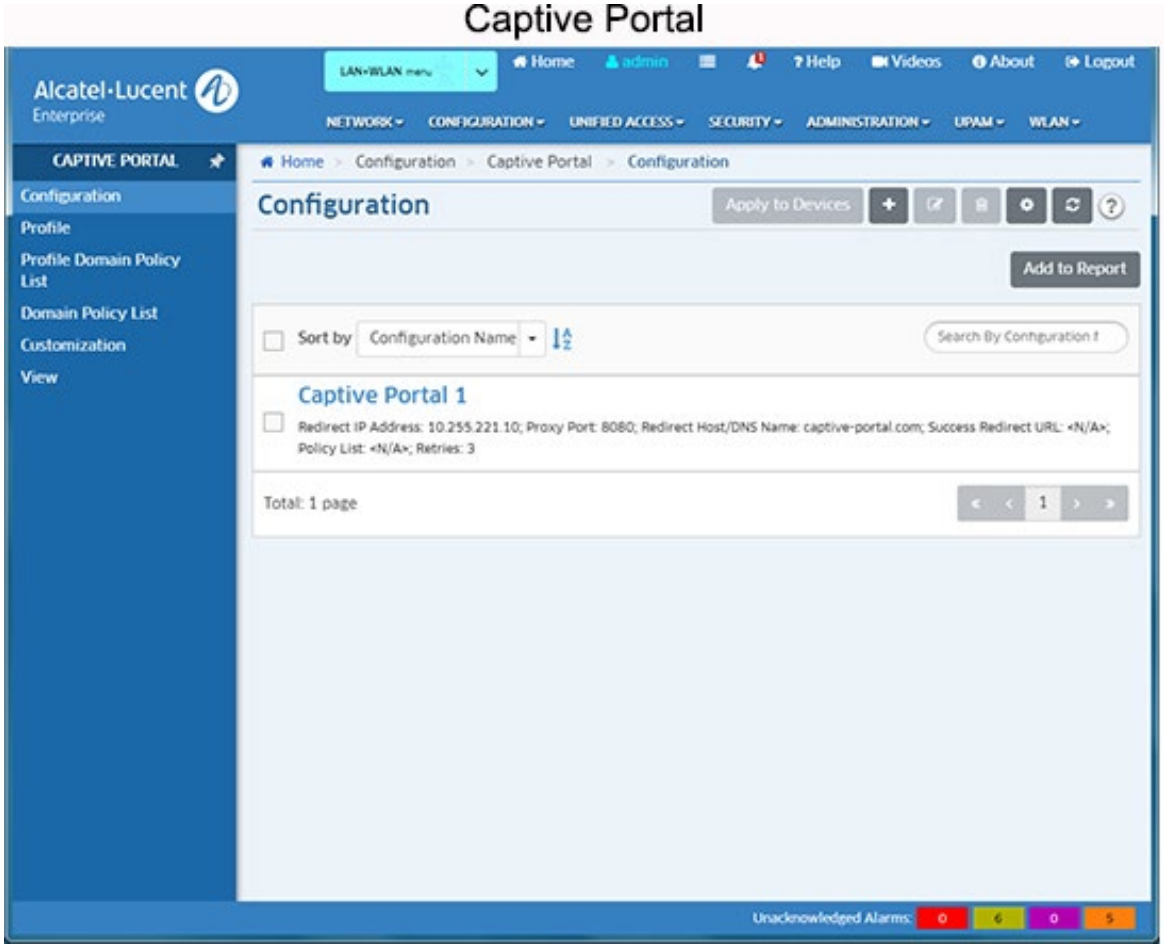
- **Server Name -** A unique name for the TACACS+ Authentication Server. This name will be used by OmniVista and the switch to identify the server.
- **Host Name/IP Address -** The name of the computer where the server is located OR the IP address of the computer where the server is located.
- **Timeout -** The number of seconds that you want the switch to wait before a request to the TACACS+ authentication server is timed out. Default value is 2.
- **Port -** The port number used to access the TACACS+ Server (Default = 49).
- **VRF Name -** The VRF Instance associated with the TACACS+ Server, if applicable. A TACACS+ Server can be configured on any VRF instance including the default VRF instance. However, all of the servers (for example, all the TACACS+ servers) must reside on the same VRF instance. Default value is "default". (Not supported on wireless devices and ignored when applied to those devices.)
- **Backup Host Name/IP Address -** Each TACACS+ Server may optionally have a backup server. If you wish to define a backup server that will be used if this server is unavailable, enter the name of the computer where the backup server is located OR enter the IP address of the computer where the backup server is located.

9.0 Captive Portal

Captive Portal authentication is mechanism by which user credentials are obtained through Web pages and authenticated through a RADIUS server. If the authentication is successful, the RADIUS server may return a role (policy list) that is applied to traffic from the user device. The OmniSwitch implementation supports an internal Captive Portal mechanism. An internal Web server on the local switch presents Captive Portal Web pages to obtain user credentials.

Internal Captive Portal authentication is a configurable option for a UNP Access Role Profile that is applied after a user is assigned to the profile (after the initial 802.1X or MAC authentication or classification process). This type of authentication does not change the Access Role Profile assignment for the user device. Instead, Captive Portal provides a secondary level of authentication that is used to apply a new role (QoS policy list) to the user. An external, guest Captive Portal authentication mechanism is provided through the Bring Your Own Device (BYOD) feature, which integrates Access Guardian with ClearPass Policy Manager (CPPM).

For more information, see the "Using Captive Portal Authentication" section of the Access Guardian chapter in the *OmniSwitch Network Configuration Guide*.



Configuration

The Captive Portal Configuration Screen displays all configured Captive Portal global configurations and is used to create, edit, and delete Captive Portal Global Configurations.

Creating a Captive Portal Configuration

Click on the Add icon. Enter a **Configuration Name**, configure the fields as described below, then click on the **Create** button. When you are finished, select the checkbox next to the profile and click on the **Apply to Devices** button to assign the configuration to switches on the network.

Configuration

- **Configuration Name -** The unique name for the Configuration. This name will be used by OmniVista and not to be assigned to the switch.
- **Redirect IP Address -** The IP address of the Redirect Server.
- **Redirect Host/DNS Name -** The Host Name/DNS Name of the Redirect Server.
- **Proxy Port -** The TCP port on the proxy server.
- **Success Redirect URL -** The Captive Portal's Redirect URL upon successful authentication. **Retries -** The number of times a device can try to login before Captive Portal determines that authentication for that device has failed (Range = 1 - 99, Default = 3).
- **Policy List -** The Unified Policy List to apply to the authenticated user device. (You can also click on the Add icon to go to the Unified Policy List Screen and create a Policy List.)

Editing a Captive Portal Configuration

Select a Configuration in the list and click on the Edit icon to bring up the Edit Captive Portal Configuration Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server. Note that you cannot edit the Configuration Name.

Assigning a Captive Portal Configuration

When you click the **Apply to Devices** button, the Apply to Devices Screen appears. Select the switch(es) to which you want to assign the configuration and click on the **Apply** button. Click **OK** to return to the Configuration Screen.

> **Note:** To "unassign" a configuration from a switch(es), select the configuration and click on the **Apply to Devices** button. The Apply to Devices Screen appears. The switches to which the configuration is assigned will appear on the right. Move the switches from which you want to "unassign" the configuration to the left side of the screen and click the **Apply** button.

Deleting a Captive Portal Configuration

Select a Configuration in the list and click on the Delete icon, then click **OK**, at the confirmation prompt. If the configuration has been assigned to a switch, a second prompt will appear. Click **OK** on the second prompt to delete the configuration.

Profile

The Captive Portal Profile Screen displays all configured Captive Portal Profiles and is used to create, edit, and delete Captive Portal Profiles. A Captive Portal profile is a configuration entity that provides flexible assignment of Captive Portal configuration parameters to devices

classified into specific UNP Access Role Profiles. However, this type of profile is only valid when assigned to Access Role Profiles on which Captive Portal authentication is enabled. When a Captive Portal profile is applied to a UNP Access Role Profile, the parameter values defined in the Captive Portal profile override the global Captive Portal parameter values configured for the switch. If there is no Captive Portal profile associated with an Access Role Profile, the global Captive Portal configuration is applied.

Creating a Captive Portal Profile

Click on the Add icon. Enter a **Profile Name**, configure the fields as described below, then click on the **Create** button. When you are finished, select the checkbox next to the profile and click on the **Apply to Devices** button to assign the profile to switches on the network.

Captive Portal Profile Configuration

- **Profile Name -** The unique name for the Captive Portal profile.
- **Policy List -** The QoS policy list to apply when Captive Portal authentication is successful but the RADIUS server did not return a policy list. (You can also click on the Add icon to go to the Unified Policy List Screen and create a Policy List.)
- **AAA Server Profile -** The AAA profile used to define specific device authentication configuration options, such as which servers to use for Captive Portal authentication and parameter values for session timers and RADIUS attributes. If there is no AAA profile assigned, the global AAA configuration for the switch is used. (You can also click on the Add icon to go to the Unified Policy List Screen and create a AAA Server Profile.)
- **Success Redirect URL Name -** The Captive Portal's Redirect URL upon successful authentication. **Retries -** Number of Captive Portal retries before failure is declared.

Editing a Captive Portal Profile

Select a Captive Portal Profile in the list and click on the Edit icon to bring up the Edit Captive Portal Profile Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server. Note that you cannot edit the Profile Name.

Assigning a Captive Portal Profile

When you click the **Apply to Devices** button, the Apply to Devices Screen appears. Select the switch(es) to which you want to assign the Captive Portal Profile and click on the **Apply** button. Click **OK** to return to the Configuration Screen.

> **Note:** To "unassign" a profile from a switch(es), select the profile and click on the **Apply to Devices** button. The Apply to Devices Screen appears. The switches to which the profile is assigned will appear on the right. Move the switches from which you want to "unassign" the profile to the left side of the screen and click the **Apply** button.

Deleting a Captive Portal Profile

Select a Captive Portal Profile in the list and click on the Delete icon, then click **OK**, at the confirmation prompt. If the profile has been assigned to a switch, a second prompt will appear. Click **OK** on the second prompt to delete the profile.

Profile Domain Policy List

The Captive Portal Profile Domain Policy List Screen displays all configured Captive Portal Domain Profiles and is used to create, edit, and delete Captive Portal Domain Profiles. A Captive Portal Domain Profile is used to assign a Captive Portal Profile and QoS Policy List to users logging in from a specific domain (e.g. NA02/tut).

Creating a Profile Domain Policy

Click on the Add icon. Select a Captive Portal **Profile Name** from the drop-down list. (You can also click on the Add icon to go to the Captive Portal Profile Screen to create a profile.) Configure the fields as described below, then click on the **Create** button. When you are finished, select the checkbox next to the profile and click on the **Apply to Devices** button to assign the configuration to switches on the network.

Profile Domain Pass Policy Configuration

- **Profile Name -** Select a Captive Portal Profile from the drop-down menu. (You can also click on the Add icon to go to the Captive Portal Profile Screen to create a profile.)
- **Domain -** A unique name for the Captive Portal Domain Policy.
- **Policy List -** Select a Unified Policy List from the drop-down menu. This Policy List will replace the one in the Access Role Profile upon successful Captive Portal authentication only if the domain is known. (You can also click on the Add icon to go to the Unified Policy List Screen and create a Policy List.)
- **Realm -** Select Suffix/Prefix. For example: Suffix: NA02/tut; Prefix: tu@alu.com.

Editing a Profile Domain Policy

Select a policy and click on the Edit icon to bring up the Edit Profile Domain Policy List Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server. Note that you cannot edit the Profile Name.

Assigning a Profile Domain Policy

When you click the **Apply to Devices** button, the Apply to Devices Screen appears. Select the switch(es) to which you want to assign the policy and click on the **Apply** button. Click **OK** to return to the Configuration Screen.

> **Note:** To "unassign" a profile from a switch(es), select the policy and click on the **Apply to Devices** button. The Apply to Devices Screen appears. The switches to which the profile is assigned will appear on the right. Move the switches from which you want to "unassign" the profile to the left side of the screen and click the **Apply** button.

Deleting a Profile Domain Policy

Select a policy and click on the Delete icon, then click **OK**, at the confirmation prompt. If the profile has been assigned to a switch, a second prompt will appear. Click **OK** on the second prompt to delete the profile.

Domain Policy List

The Captive Portal Domain Policy List Screen displays all configured Captive Portal Domain Policy Lists to create, edit, and delete Captive Portal Policy Lists. This screen enables you to define Policy Lists for different realms in which the endpoints are successfully authenticated. This is similar to creating a Profile Domain Policy List without the profile coming into play.

Creating a Captive Portal Domain Policy List

Click on the Add icon. Enter a **Profile Name**, configure the fields as described below, then click on the **Create** button. When you are finished, select the checkbox next to the profile and click on the **Apply to Devices** button to assign the profile to switches on the network.

Captive Portal Domain Policy List Configuration

- **Domain -** The Captive Portal Profile Authenticated Domain Name.
- **Policy List -** The Unified Policy List to apply when Captive Portal authentication is successful but the RADIUS server did not return a policy list. (You can also click on the Add icon to go to the Unified Policy List Screen and create a Policy List.)
- **Realm -** The Captive Portal Profile Authenticated Pass Realm.

Editing a Captive Portal Domain Policy List

Select a Policy List and click on the Edit icon to bring up the Edit Domain Policy List Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server. Note that you cannot edit the Domain.

Assigning a Captive Portal Domain Policy List

When you click the **Apply to Devices** button, the Apply to Devices Screen appears. Select the switch(es) to which you want to assign the Policy List and click on the **Apply** button. Click **OK** to return to the Configuration Screen.

> **Note:** To "unassign" a Policy List from a switch(es), select the profile and click on the **Apply to Devices** button. The Apply to Devices Screen appears. The switches to which the profile is assigned will appear on the right. Move the switches from which you want to "unassign" the profile to the left side of the screen and click the **Apply** button.

Deleting a Captive Portal Domain Policy List

Select a Policy List and click on the Delete icon, then click **OK**, at the confirmation prompt. If the profile has been assigned to a switch, a second prompt will appear. Click **OK** on the second prompt to delete the Policy List.

Customization

The Captive Portal Customization Screen displays all Customized Captive Portal web page files and is used to create, edit, and delete custom Captive Portal web page files. These files (e.g., html files, jpeg files) are used to create the web pages that are presented to the user during Captive Portal Login. OmniSwitches contain a default set of Captive Portal web page files. However, OmniVista enables you to import and then customized these files. You can then upload these custom files to switches. When you import the files from a switch using OmniVista,

all of the necessary Captive Portal web page files are zipped together in an "archive" file. You can then customize the Captive Portal web pages by editing individual files within this archive and then uploading the edited archive to a switch(es). When a customized archive is uploaded to a switch, Captive Portal presents these web pages to the user, rather than the default pages stored on the switch.

Creating a Captive Portal Customization

Click on the Add icon to bring up the Customization Workflow Wizard. Creating a Custom Captive Portal Customization consists of the following steps. After completing the steps as described below, click the **Create** button.

1. Import the Archive File
2. Download the Archive File for Editing
3. Upload the Edited Archive File
4. Apply the Archive File to Switches

Import the Archive

Enter a **File Set Name** for your customized set of files and an optional **Description**, then import the files. As mentioned earlier, OmniVista zips all of the Captive Portal web page files into a single archive file). You can actually import the file from a switch or import an existing archive from a local machine.

- **Import from a Switch -** Click on the **Select Switch** button and select a switch from which to download the files. Select **Release Folder** to import the default set of Captive Portal web page files or **Custom Folder** to select a previous set of customized files, then click on the **Import** button. Click on the **Next** button to download the file.
- **Import from Local Machine -** If you already have an edited archive that you want to upload from a local machine, click on the **Browse** button to locate the file. Click **Upload** to upload the file to OmniVista, then click **Next** to apply the file to switches. Note that if you import the file from a local machine, Steps 2 and 3 will be skipped and you only need to apply the edited file to switches.

Download the Archive File for Editing

If you import the Archive File from a switch, click on **Download** button then click on the download prompt to download the file. The file will be downloaded to your default download directory. Edit the necessary file(s) in the archive using the editor of your choice. When you are done, click on the **Next** button to upload the file.

Upload the Edited File

Click on the **Browse** button to locate the edited Archive File, then click on the **Upload** button to upload the file to OmniVista, then click the **Upload** button.

Apply the File to Switches

Select the switch(es) to which you want to assign the file and click on the **Finish** button. Note that you can also apply existing Archives to switches by selecting the Archive in the list and clicking on the **Push to Switches** button. The new Custom Archive that you apply will replace any existing Custom Archive on the switch(es).

Editing a Captive Portal Custom File

Select an Archive from the list and click on the Edit icon to bring up the Customization Workflow Wizard. You cannot edit the File Name; however, you can edit the Archive File and apply this edited Archive File to the same switch(es) or a different switch(es). Follow the steps a described above to apply an edited Archive File.

Applying a Captive Portal File

You can also apply existing Archives to switches. Select an Archive File in the list, click on **Push to Switches** button, select the switches to which you want to apply the file, then click on the **Push File** button. Click **OK** to return to the Configuration Screen. The new Custom Archive that you apply will replace any existing Custom Archive on the switch(es).

> **Note:** To "unassign" an Archive File from a switch, select it and click on the **Push to Switches** button. The Apply to Devices Screen appears. The switches to which the field is assigned will appear on the right. Move the switches from which you want to "unassign" the file to the left side of the screen and click the **Push File** button. Note that when a file is applied to a switch, it will override existing files. The switch will then present the default Captive Portal web pages to the user.

Deleting a Captive Portal Customization

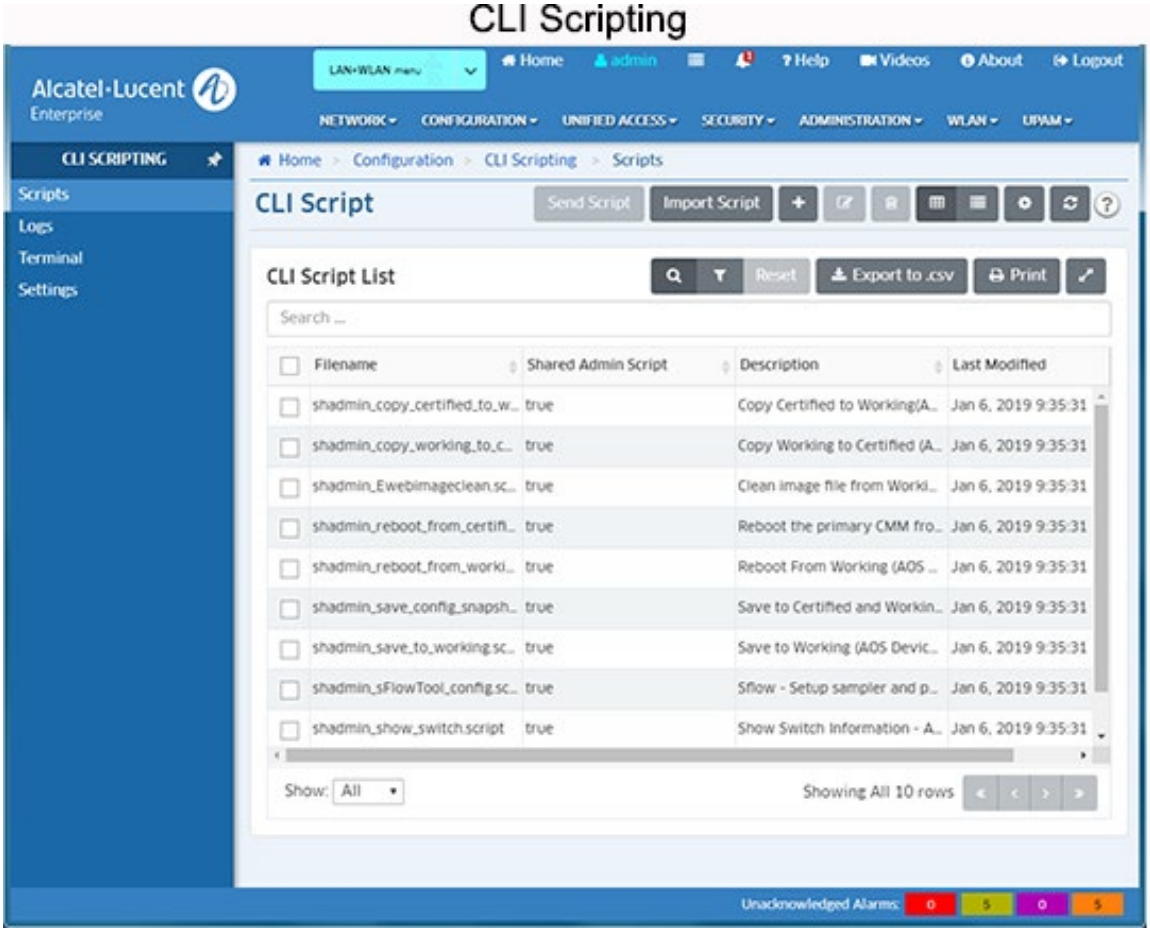
Select a file and click on the Delete icon, then click **OK**, at the confirmation prompt. If the file has been assigned to a switch, a second prompt will appear. Click **OK** on the second prompt to delete the file.

View

The Captive Portal View Screen is used to display Captive Portal configurations on specific switches. Click on the **Browse** button and select a switch. The Captive Portal configuration for the selected switch is displayed - Configuration, Profile, Profile Domain Policy List, and Domain Policy List. Click on each to view configuration details.

10.0 CLI Scripting

The CLI Scripting application is used to connect to and configure network devices via the CLI; and to configure multiple devices by creating CLI Script Files and applying the files to devices on the network.



The following screens are used for CLI Scripting:

- **Scripts -** Used to create CLI Scripting Files. You can then use these text-based files to configure one or more devices by applying the file via a Telnet or SSH session. You can also import existing text-based script files. Scripts can be created and stored on the local client, or can saved to the OmniVista Server so they can be available to other clients ("shared").
- **Logs -** Displays log files of all CLI Scripts that have been applied to network devices. You can click on a log file to view CLI Scripting results on a command-by-command basis to see if the contents of the file were successfully applied to a device(s).
- **Terminal -** Used to establish CLI Scripting sessions by logging in to one or more devices and configuring the devices via supported CLI commands. Note that OmniVista CLI Scripting also supports SSHv2 enhanced encryption.
- **Settings -** Used to set the retention period for CLI Scripting Logs.

CLI Script

The CLI Scripting CLI Script Screen displays a list of all configured CLI Script Files. It is also used to create, import, edit, and delete, script files, and send script files to network devices. A CLI Script File is a text-based file used to configure one or more devices through OmniVista's CLI Scripting feature. CLI Scripting is especially useful in applying batch updates or common configurations across multiple devices. When a script file is applied, each command in the file is sent to the device. A user can create a CLI Script that is only available to that user, or can create a "shared" script that is available to any network administrator.

> **Note:** Before attempting to send a script, OmniVista must know the CLI/FTP user name and password for each device being configured. If necessary, go to the Discovery application to specify CLI/FTP user name and password. You can also specify the CLI/FTP user name and password using the "Discovery - Edit Device" operation in the Topology application.
>
> **Note:** You cannot send scripts to Stellar Wireless Devices.

Pre-Configured Scripts

OmniVista includes pre-configured CLI Script Files, which are displayed in the CLI Script List (along with any user-configured scripts). These pre-configured scripts are "shared" scripts and are available to any network administrator. A brief description of each script, as well as the contents of the script file, are provided in the Details Panel for the script. Click on a script in the CLI Script List to view script details.

> **Important Note:** Use caution when using the **shadmin_Ewebimageclean** script. Use the Resource Manager application to perform a full backup on the switch prior to an upgrade.

Creating a Script File

Click on the Add icon. Enter a **Filename** for the script (e.g., show_switch). The file extension ".script" will be added automatically when the script file is saved. Select the **Shared Admin Script** checkbox to create a "shared" script that can be used by network administrators. If you do not select the checkbox, the script will only be available to you. When a "shared" script is created, the prefix "shadmin" is automatically assigned to the filename. To add a description of the script that will appear in the Details Panel, enter the description as follows at the top of the script. For example:

<js>
/ @@**Enter a description here**@@*/*

Enter the commands to be applied to the switch via this script in the **Commands** field. Enter one command per line. The script can be a combination of both CLI commands and JavaScript. You can also define variables or use OmniVista built-in variables to be used in the script. Note that if a script with the same name currently exists, an error message will appear. Re-name the script and continue as described above. Verify that the syntax of all the commands is correct, then click the **Add** button. The filename will be listed in the CLI Script List in alphabetical order. Select the script in the CLI Script List and click on the **Send Script** button to send the script to a network switch(es).

CLI and Java Scripts

Scripts can be a combination of both CLI commands and JavaScript. The following is an example of a CLI script containing JavaScript:

```
--------- script start ----------
<js>
var devtype =
cli.deviceType();
if
(devtype.indexOf(
"OS68") > -1)
cli.sendCmd("ls");
else if
(devtype.indexOf(
"OS62") > -1)
cli.sendCmd("dir")
; else
cli.sendCmd
("files"); if
(devtype.ind
exOf("OS68
") > -1)
{
cli.setTimeout(3, 30);
cli.sendCmd("show log swlog");
}
else if (devtype.indexOf("OS66") > -1)
{
cli.setTimeout(5, 0);
cli.sendCmd("show log swlog");
}
cli.trace("I got: " + cli.lastResponse() );
cli.sendCmd("ls " + "$USERVAR" ); /* user defined variable! */

</js>
--------- script end ----------
```

Notice in the above example, the usage of the variable **'cli'** . This is a built-in variable that can be used within the scripting blocks. CLI offers the following functions:

- **sendCmd(String cmd)** allows the user to send a CLI command to the switch.
- **lastResponse()** returns a string that represents the switch output from the last command the user sent to the switch (whether the command was sent via JavaScript or just entered as CLI in the cli script itself). Device Type () returns the same string as can be seen via the Topology applications "Type" column.
- **setTimeout(minutes, seconds)** allows a caller to specify a hint to the CLI Scripting application about how long it could take for the next command to return a response. In the example above, the JavaScript specifies a timeout of 3 minutes and 30

seconds to apply to the next command (show log swlog) if the device is something like an OS6800-48. It specifies 5 minutes if the device is something like an OS6624. Some commands can be slow in returning output to the CLI Scripting/SSH session, so this can help prevent the scripting session from timing out before a response is received. Once the session is receiving a response from the command (e.g., show log swlog), the default timeout will be automatically reset. The user specified timeout does not take affect for the entire session, just the CLI command used after the call to setTimeout (minutes, seconds). You may specify "0" for minutes or seconds according to what is needed. Negative numbers are converted to '0' internally, thus ignored.

If both minutes and seconds contain either "0" and/or negative numbers, the timeout request will be ignored. Therefore, the minimum timeout will be 1 second (ex: cli.setTimeout(0, 1);).

- **trace(String message)** logs any arbitrary string passed as its 'message' argument to the CLI Scripting Audit Log. Can be contained in a variable for instance. **expectPrompt(String prompt)** sets-up the particular script (running on whatever devices) to expect a prompt that is not in the default collection of expected prompts. In other words, it allows the user to temporarily add to the set of prompts that CLI Scripting is hard-coded to recognize. **deviceType()** returns a string that contains the device's type as seen in the Topology application.
- **cliSleep(milliseconds)** allows the user to set a time, in milliseconds, before the next CLI command is executed.
- **errorLog(String message)** logs any 'error' argument to the CLI Scripting Audit Log. Can be contained in a variable for instance.
- **cli.sendCmd(more)** by default, the switch will stop running a command at a confirmation prompt and wait for the user to confirm the action. The 'more' command tells OmniVista to expect a specific prompts(s) and continue running the script. For example, the 'more' variable should be used when sending a script to reload the working directory (**reload working no rollback-timeout**). In the example below, the 'more' command tells OmniVista to expect the "Confirm Activate" and "Confirm New Activate" prompts, and to reload the switch from the Working Directory in 10 minutes.

--------- script start ----------

<js> cli.sendCmd("more");

cli.expectPrompt("Confirm Activate

(Y/N) :"); cli.expectPrompt("Confirm New

Activate (Y/N) :"); cli.sendCmd("reload

working no rollback-timeout in 10:10");

cli.sendCmd("y");

</js>

--------- script end ----------

Enter only one command per line. Operational commands that automatically issue a confirmation prompt and require the user to type a response (such as, Y or N) are not supported in CLI script files. Examples include **takeover**, **reload**, **fsck**, etc. Do not attempt to include these command types in the script file. Instead, manually issue them via the standard CLI command line prompt. These operations can also be issued on a device-by-device basis via WebView or OmniVista.

> **Important Note:** If a command that takes a long time to complete (e.g., "write memory flashsynchro") , is issued as the last command in a CLI script, the session can end right after the command is issued, ending the session before the command is executed. To avoid this problem, either add another command at the end of the script ("show chassis"), **or** add a tapps timeout. For example, the following command sets a timeout of 0 minutes and 15 seconds: *<tapps> set timeout 0 15 </tapps>*

Built-In Variables

OmniVista built-in variables are listed below.

- **$BASE_MAC** - Replaced automatically with target base MAC address.
- **$BOOT_DIR** - Replaced automatically with target boot directory (ex: working).
- **$CHASSIS_TYPE** - Replaced automatically with target chassis type.
- **$IP_ADDRESS** - Replaced automatically with target switch IP address.
- **$LOGIN_ID** - Replaced automatically with target CLI/FTP User Name.
- **$LOGIN_PWD** - Replaced automatically with target CLI/FTP Password.
- **$READ_PWD** - Replaced automatically with target community string for SNMP reading.
- **$SECOND_PWD** - Replaced automatically with the value of secondary password in the Discovery list item, if applicable. The secondary password for a device is set in the Edit Discovery Manager Entry window in the Discovery application.
- **$SYS_LOCATION** - Replaced automatically with the location of the device as defined in sysLoction MIB-II variable.
- **$SYS_NAME** - Replaced automatically with the name of the device as defined in sysName MIB-II variable.
- **$SYSTEM_OID** - Replaced automatically with target unique object ID.
- **$SYS_VERSION** - Replaced automatically with the MPM Version of the device as displayed in OmniVista.
- **$WRITE_PWD** - Replaced automatically with target community string for SNMP writing.
- **cli.forgetPrompt()** - This CLI script directive is used to reverse the **cli.expectPrompt()** directive, providing a way to ignore prompts that interfere with script execution.

> **Important Note:** If you are using Built-In variables **within a Java Script**, the variable must be contained within quotes (e.g. " **$BASE_MAC"**). If you are using Built-In variables outside of a Java Script, the quotes are not required.

Script Directives

A tag, called <tapps> allows certain directives to the CLI Scripting application. <tapps> does not use a scripting engine. It is a set of supported commands that tell the CLI Scripting application how to handle certain actions. For example, a user may write the following CLI script that uses all of the supported <tapps> commands:

<tapps> set
timeout 5
</tapps> qos
apply
<tapps> import
another.script </tapps>
<tapps> second password
</tapps>

set timeout: The above script specifies a timeout for the *qos apply* command. It performs the same function as the previous Java Script example, but the user does not need to specify seconds. However, the user must always specify minutes (the minutes can be "0" if the user wants to specify the timeout only in seconds).

Examples:
As shown above, to set a timeout of 5 minutes, only the *minutes* parameter is required:

<tapps> set
timeout 5
</tapps> qos
apply

To set a timeout of 15 seconds, you must first specify 0 minutes , then 15 seconds:
<tapps> set
timeout 0 15
</tapps> qos
apply

To set timeout of 5 minutes and 15 seconds, you would enter:
<tapps> set
timeout 5 15
</tapps> qos
apply

> **Note:** The *set timeout* command only applies to the next command in the script (e.g., *qos apply*). Thereafter, the timeout reverts back to its default.

import script: The import script directive tells the CLI Scripting application to insert the commands from the specified script at that spot in the current script. This allows re-use of scripts by other scripts. In the example above, if the CLI Scripting application script named "another.script" contained only the command 'ls' , then 'ls' would be inserted at runtime at that point in the current script. The log output for a running of the current script would show the command 'qos apply' sent, followed by the command 'ls' being sent. Detection of loops takes place at strategic points in the CLI Scripting application on both the client and server sides.

second password: The second password directive tells the CLI Scripting application to prepare to send the password again. Some devices have a second login capability that requires the use of a second password. This second password for a given device is set by the user via Topology when a device is selected for Editing. The value in the Topology 'Secondary Password:' field will be used by this new <tapps> feature as the password to set when or if the device prompts for a password.

last command: On some devices (e.g., OA5510-TE), commands such as 'reload' will 'hang' the OmniVista CLI Scripting session because the switch session will end without closing the session with OmniVista. The 'last command' directive, <tapps> lastcmd </tapps>, alerts OmniVista that the next command is the last command and a response may not be received after this command. OmniVista will gather whatever response is given before reload and close the session. For example:

<js>
cli.sendCmd("enable");
cli.sendCmd("$SECOND_PWD");
cli.expectPrompt("Do you want to save config before rebooting (y/[n])");
cli.expectPrompt("Do you really want to reboot the Chassis (y/[n])");
</js> reload n

<tapps> lastcmd </tapps> y

The expectPrompt() calls in the java scripts train the CLI Script to send the next value upon receiving the specific prompt from the switch. Note that 'lastcmd' is used before “Y” and not reload command.

Importing a Script File

Although OmniVista allows users to manually create script files within the CLI Scripting application, existing script files can also be imported. In other words, a file containing a set of CLI commands can be accessed from a server or local drive and then applied to one or more devices. This allows users to maintain a library of network configurations and then apply them to devices in their network as needed. Before importing a file to one or more devices, consider the following important guidelines:

- Any script file being imported must be text-based (ASCII).
- Although file extensions such as **.txt** and **.ascii** are supported, the file extension **.script** is recommended.
- All CLI commands contained in the file must be supported on the device. Also, operational commands that automatically issue a confirmation prompt and require the user to type a response (such as, Y or N) are not supported in CLI script files. Examples include **takeover** , **reload** , **fsck** , etc.
- CLI commands must also be entered into the text file *one command per line* . Only one script file can be imported at a time.

To import a script file, click the **Import Script** button at the top of the screen. On the **Import Script** window, click on the **Browse** button to locate the file. Select the file and click on the **Import** button, then click **Finish**. The script will be imported as a "shared" script with the current date appended to the script name (e.g., new_script20161026.script).

Note: If you are browsing for a file with an extension other than **.script** , be sure to select **Files of Type -> All Files** in the dialog box.

Editing a Script File

Select the script in the CLI Script List and click on the Edit icon. Edit the script commands and click on the **Apply** button. Note that you cannot edit the script name or "shared" status. If you want to change the "shared" status of script, delete the script and re-create it.

Important Note: When the changes are saved, the previous contents of the script file are overwritten. To preserve the original contents of the file, be sure to make a backup copy before editing.

Sending a Script File

You can send a script file to a single device or multiple devices in the network. Select a script in the CLI Script List and click on the **Send Script** button to bring up the Send Script Wizard. Complete the screens as described below.

Script Info

The name and contents of the selected script file are displayed. Click **Next**. (Note that you have the option of selecting a different script. Click on the **Browse** button to bring up all of the scripts in the CLI Script List, select a script and click **OK**, then click **Next**.)

Device Selection

Select an option from the drop-down menu (User Switch Picker/Use Topology) and click on the **Add/Remove Devices** button to select devices.

- **Use Switch Picker -** Select the devices and click **OK**. Click **Next**.
- **Use Topology -** The Topology application will launch in the Physical Map view. Select the device(s), then click on the **OK** button at the bottom of the Detail Panel to return to the Send Script Wizard. The devices will appear in the list of devices. Click **Next**.

Scheduler

You can send a script immediately to the selected device(s), or schedule the script to be run at a specific time or at regular intervals. After selecting/configuring an option, click **Next**.

- **Now -** The script will be sent immediately to the selected device(s)
- **Periodically -** Schedule the script as described below.

  Start Time - Set a time to start the repeating script.

  End Time - Set a time to stop the repeating script.

  Simple - Select this option to configure a repeating script. Set an **Interval** using the Days/Hours/Minutes/Seconds fields, and enable the **Repeat** field to the number of times to repeat the script until the configured "End Time" is reached.

  Cron - Select this option and use the drop-down menus in each tab (e.g., Minute, Hour, Day) to configure a repeating cron job. The cron job will continue until the configured "End Time" is reached.

Define User Variables

If there are variables within the script, the **Define User Variables** Screen is displayed. Click in field next to the variable and enter value to be used. After completing all of the variable fields, click the **Send Script** button at the bottom of the screen.

Deleting a Script File

Select the Script File in the CLI Script List and click on the Delete icon. Click **OK** at the confirmation prompt. Note that when a file is deleted, it is permanently removed from the scripting_files directory, and cannot be recovered.

CLI Script Details

The CLI Script List displays basic information about all configured CLI Scripts stored on the OmniVista Server. Click on a script to view the commands contained in the script.

- **File Name -** The Script Filename.
- **Shared Admin Script -** Whether or not the script is a shared script (True) or not (False).
- **Description -** A brief description of the script.
- **Commands -** The commands contained in the script.

Logs

The CLI Scripting Logs Screen displays a list log files of all CLI Scripts that have been applied to network devices. You can click on a log file to view CLI Scripting results on a command-by-command basis. In other words, it displays whether the contents of a file were successfully applied to the device. A log file also provides a record of a particular configuration, as well as effective troubleshooting information, when applicable. The screen can be used to view, export, or delete CLI Scripting Logs.

> **Note:** As with the scripting files, log files are automatically stored on the OmniVista Server or local system. File locations may vary, depending on the OmniVista installation, but can generally be found at a path similar to the following: Alcatel OmniVista 2500\data\cli_scripting_logs. By default, log files are placed in a directory indicating the IP address of the corresponding device.

Displaying a Log File

Click on a log file to display the contents. You can look through the file to view the application of the Log File on a command-by-command basis. Unless an error has occurred, the log file will closely resemble the script file (i.e., it will list only the CLI commands that were applied to the device). If an error occurs, an error notification is displayed in the log, following the CLI command that triggered the error. You can search for a command or specific text string in the log file by entering the text in the Search field and clicking on the **Search Next** or **Search Previous** buttons. You can also configure a filter to view specific information by clicking on the Filter icon and creating/selecting a filter.

Exporting a Log File

You can export a log file to another location (directory). Select the file and click on the **Export** button. Browse to the location to which you want to export the file and click **OK**.

Deleting a Log File

Select the log file(s) and click on the Delete icon. Click **OK** at the confirmation prompt.

Terminal

The CLI Scripting Terminal Screen is used to establish a basic CLI Scripting session with a device. You can locate and connect to a device using a Switch Picker or the Topology Map. Once you are connected to a device, log into the device to issue CLI Scripting commands. Note that OmniVista must know the CLI/FTP user name and password for a device to log into the device. If necessary, go to the Discovery application to specify CLI/FTP user name and password. You can also specify the CLI/FTP user name and password using the "Discovery - Edit Device" operation in the Topology application.

Connecting to a Device

You can locate and connect to a device using a Switch Picker or the Topology Map.

Switch Picker

To connect to a device using the Switch Picker, select **Use Switch Picker** from the drop-down menu and click on the **Browse** button. Select the switch you want to connect to and click **OK**. The shell preference (Telnet/SSH) configured for the selected device in the Discovery application will be enabled. Click on the **Telnet** button or the **SSH** button at the top of the screen to connect to the device. The shell preference configured for the selected device will be enabled. Log into the device to begin the session. To disconnect from a device, click on the **Disconnect** button at the top of the screen, or enter *exit* at the command prompt.

> **Note:** You can also enter search criteria (e.g., IP address, OS Version, Location) in the Device field to search for and select a device to connect to.

Topology Map

To connect to a device using the Topology Map, select **Use Topology** from the drop-down menu and click on the **Browse** button. The Topology application will open. Select the device you want to connect to. The Detail Panel for the device will open. Click on the **OK** button at the bottom of the Detail Panel and log into the device to begin the session. The session will be established using the shell preference (Telnet/SSH) configured in the Discovery application for the selected device. To disconnect from a device, click on the **Disconnect** button at the top of the screen, or enter *exit* at the command prompt.

Session Preferences

SSH (Secure Shell) provides CLI Scripting sessions with enhanced encryption and security. SSH may be mandatory for some device types. OmniVista uses SSH by default for those devices requiring SSH. However, for AOS and other devices where SSH is optional, standard Telnet is the default setting. To use SSH, you must specify SSH either on a device-by-device basis, or on multiple devices using the Discovery Profile feature in the Discovery application.

Note: You can configure the size of the type used in the session by clicking on the Settings icon at the top of the screen.

Settings

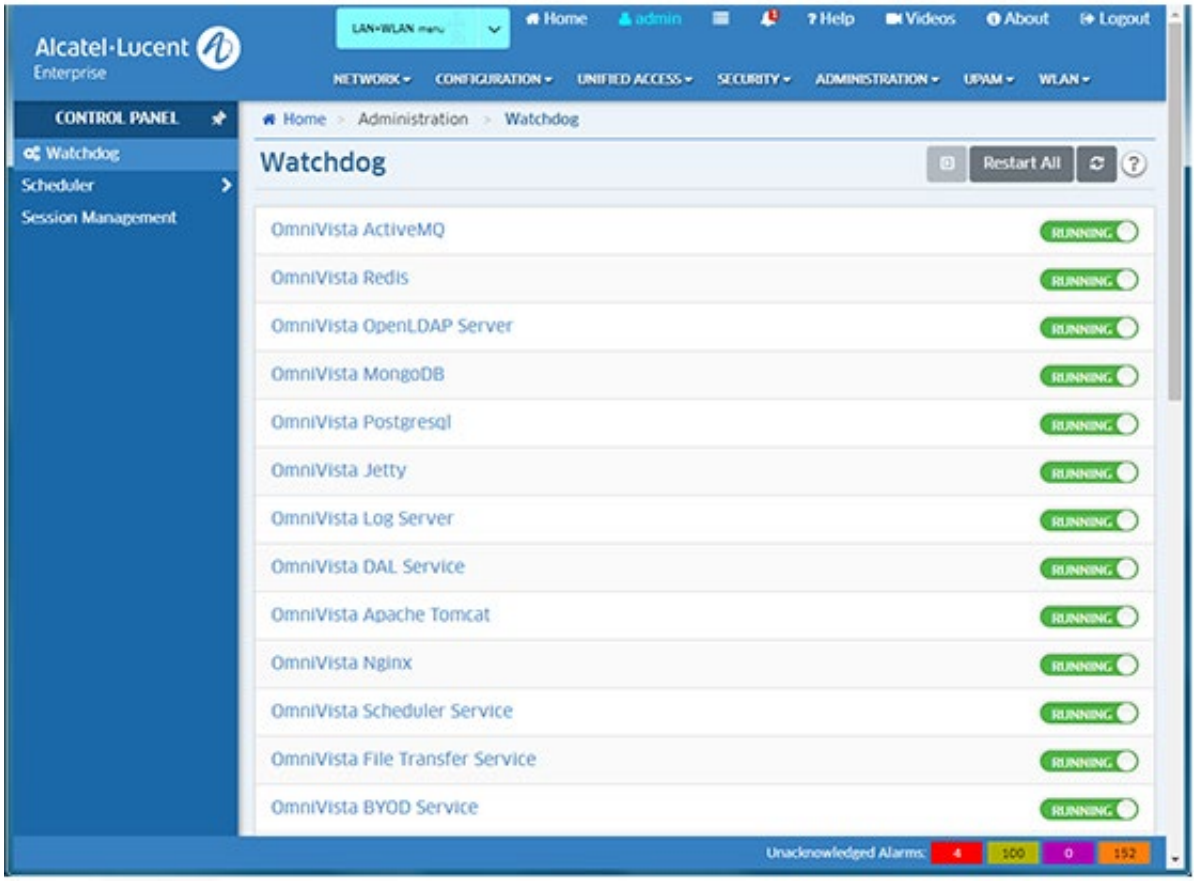
The CLI Scripting Settings Screen is used to set the retention period for CLI Scripting Logs. Once the configured retention period is reached, the oldest log files will be overwritten with newer files.

- **Days to Retain -** The number of days to retain CLI Scripting Log Files on the OmniVista Server (Range = 1 - 365, Default = 180).

11.0 Control Panel

The Control Panel application is used to access the Watchdog, Scheduler, and Session Management features. The Watchdog feature displays the status of all services used by OmniVista; and is used to start/stop services. The Scheduler feature provides an overview of all currently Scheduled jobs (System Jobs and User-Defined Jobs), and is used to start/stop, edit, or delete a User-Defined Job. The Scheduler feature also provides a history of all completed Scheduler jobs. The Session Management feature displays a list of all OmniVista Client login sessions, and can be used to log out a session.

Control Panel



Watchdog

The Control Panel Watchdog Screen displays the status of all of the services used by OmniVista (Running/Stopped). Click on any service to view an information panel for the service (e.g., description, status, dependencies, statistics). To start/stop a service, click on the slider control next to the service (**Running**/**Stopped**). If you are stopping a service, click **Yes** at the confirmation prompt. Click on the Start All icon to start all stopped services. To stop and restart all services, Click on the **Restart All** button.

You can also stop/start a service in the information panel. To stop a service, click on the **Stop** button, then click **Yes** at the confirmation prompt. This will stop the service and all of its dependent services. To start a Service, click the **Start** button to start the service and all of its dependent services.

Warning: If you stop certain services (e.g., ActiveMQ, Apache Tomcat) or a service that these services depend on, the web server will shut down, and you will have to restart the service manually. You will receive a warning prompt whenever you try to shut down one of these services.

Scheduler Jobs

The Control Panel Scheduler Jobs Screen provides an overview of all currently Scheduled jobs (System Jobs and User-Defined Jobs). System Jobs are automatically scheduled by OmniVista. System Jobs cannot be edited or deleted. User-Defined Jobs are scheduled by users within OmniVista applications (e.g., using the Resource Manager application to scheduled backup job). To view specific details about a job, click on the job in the table to display job details (e.g., Start Time, End Time, Cron Description). You can also start/stop, edit, or delete a User-Defined Job. Note that you can only view System Jobs. You cannot start/stop, edit, or delete these jobs.

Starting/Stopping Scheduled Jobs

You can start/stop/pause a job by selecting the job and clicking on the applicable icon:

- **Start-** Register the job in the schedule and start executing immediately if its start time is in the past.
- **Stop -** Stop the current job. Stopped job will execute normally in the next cycle.
- **Pause -** Stop the current execution and save its progress state. The job also is removed from the schedule and will not be executed at next trigger. You can restart the job by selecting it and clicking on the Start icon. The job will be started job from the last state and resume the job schedule.

Viewing Scheduler Jobs

The Scheduler Jobs Table lists all schedule System and User-Defined Jobs. Click on the applicable tab at the top of the table to view a list of each type. The table provides the basic information. Click on a job to view detailed information.

Basic Information

- **Name -** The system-generated job name.
- **Group -** The system-generated job group. A job group is a logical grouping of related jobs grouped by application, framework, etc. (e.g., Analytic, Poller, VM Snooping). You can sort or search on a job group in the Scheduler Jobs Table to view related jobs.
- **Status -** The status of the job (e.g., Scheduled, Waiting).

Detailed Information

- **Name -** The system-generated job name.
- **Group -** The system-generated job group. A job group is a logical grouping of related jobs grouped by application, framework, etc. (e.g., Analytic, Poller, VM Snooping). You can sort or search on a job group in the Scheduler Jobs Table to view related jobs.
- **Priority -** The job priority. If jobs are initialized at the same time, the job with the higher priority will begin first (Range = 1 - 10).

- **Actor -** The system-generated behavior description for the job.
- **Overlap Policy -** The Overlap Policy determines the action OmniVista will take if there is a job overlap:

  Ignore When Overlap - The next run (cycle) of the job will be skipped if it is still being executed at the scheduled time.

  Replace When Overlap - The job will start fresh (restart) in the next run (cycle) if it is still being executed at the scheduled time.
- **Action From Crash Policy -** The Crash Policy determines the action to take if the job crashes before completion:

  Start Afresh From Crash - The job will start fresh in the next run (cycle) if it is in a failed state at the scheduled time.

  Resume From Crash - The job will resume from the failure point in the next run (cycle) if it is in a failed state at the scheduled time.
- **Start Time -** The configured start time for the job.
- **End Time -** The configured end time for the job.
- **Schedule -** The schedule type for the job:

  Simple - The job repeats at specific intervals.

  Interval - The repeat interval for the job (e.g., 1 Day, 1 Hour).

  Repeat - The number of times the job will repeat.

  Retry Count - The number of times the job will retry after a failure.

  Retry Interval - The duration from failure to next retry, in seconds.

  Timeout - The maximum amount of time the job will run before timing out, in seconds.

  Owner - The user who created the job (e.g., admin). User-Defined Jobs only.

  Cron - The job is a recurring Cron job.

  Cron Description - A brief description of the Cron Job.

  Retry Count - The number of times the job will retry after a failure.

  Retry Interval - The duration from failure to next retry, in seconds.

  Timeout - The maximum amount of time the job will run before timing out, in seconds.

  Owner - The user who created the job (e.g., admin). User-Defined Jobs only.

Editing a Scheduled Job

You must be an admin user to edit a scheduled job. To edit a job, select the job in the Scheduler Jobs table and click on the Edit icon. Edit the fields as described below and click on the **Save** button. Note that you can only edit a "Paused" or "Waiting" Scheduler job. If necessary, select the job you want to edit and click on the Pause icon. When you are done editing the job, click on the Start icon to activate the job.

- **Name -** The system-generated job name. This field cannot be modified.
- **Group -** The system-generated job group. A job group is a logical grouping of related jobs grouped by application, framework, etc. (e.g., Analytic, Poller, VM Snooping). You can sort or search on a job group in the Scheduler Jobs Table to view related jobs. This field cannot be modified.

- **Priority -** The job priority. If jobs are initialized at the same time, the job with the higher priority will begin first (Range = 1 - 10).
- **Actor -** The system-generated behavior description for the job. This field cannot be modified.
- **Device Type -** The type of device (All Devices, Specific Devices, Device Families). The default is "All Devices". If you select "Specific Devices", a switch picker will appear to enable you to select specific devices. If you select "Device Families", select one or more device families from the "Device Family" drop-down menu. This field is only available for jobs requiring a device (e.g., Up/Down Poller Job, DAL Poller Job).
- **Overlap Policy -** Sets the Overlap Policy that determines the action to take if there is a job overlap:

  Ignore When Overlap - The next run (cycle) of the job will be skipped if it is still being executed at the scheduled time.

  Replace When Overlap - The job will start fresh (restart) in the next run (cycle) if it is still being executed at the scheduled time.
- **Action From Crash Policy -** Sets the Crash Policy that determines the action to take if the job crashes before completion:

  Start Afresh From Crash - The job will start fresh in the next run (cycle) if it is in a failed state at the scheduled time.

  Resume From Crash - The job will resume from the failure point in the next run (cycle) if it is in a failed state at the scheduled time.
- **Start Time -** Enable this option and schedule a specific start day and time for the job. You can enter the date and time in the field or use the drop-down calendar to select the day, and then edit the time in the field. Note that if the start time is before the current time, the job will start immediately.
- **End Time -** Enable option field and schedule a specific end day and time for the job. You can enter the date and time in the field or use the drop-down calendar to select the day, and then edit the time in the field.
- **Schedule**

  Simple - Select this radio button and schedule the job to repeat at specific intervals (e.g., Days, Hours, Minutes, Seconds). Enable the **Repeat** option to limit the number of times the interval will be repeated.

  Cron - Select this radio button to schedule the job as a recurring Cron job.

  Retry - Enable this option and configure the job retry option: Count = how many times the job will retry after a failure. Interval = the duration from failure to next retry, in seconds. (Count Range = 0 - 99, Interval Range = 0 - 99)

  Timeout - Enable this option and configure the maximum amount of time a job will run before timing out, in seconds (Range = 20 - 9999). If it is disabled, a job execution could run forever.

Deleting a Scheduled Job

To delete a job, select the job in the Scheduler Jobs table and click on the Delete icon. Click **OK** at the confirmation prompt. The job will be deleted and will no longer run.

Scheduler History

The Control Panel Scheduler History Screen displays a historical overview of all completed Scheduler jobs (e.g., device audit, license audit). Click on a job to view specific details about the job. You can manually remove an event(s) by selecting the event(s) and clicking on the Delete icon. Note that you must be an "admin" user to view the Scheduler History Screen.

Session Management

The Control Panel Session Management Screen displays a list of all OmniVista Client login sessions and can be used to log out a session. A single user can have multiple sessions, logging into the server from different clients. Logging out one session will not affect other sessions of same user. To log out of a session(s), select the session(s), click on the **Logout Selected Sessions** button, and click **Yes** at the confirmation prompt.

Session Information

The Session Management Table displays the following information about each user who logged into the server:

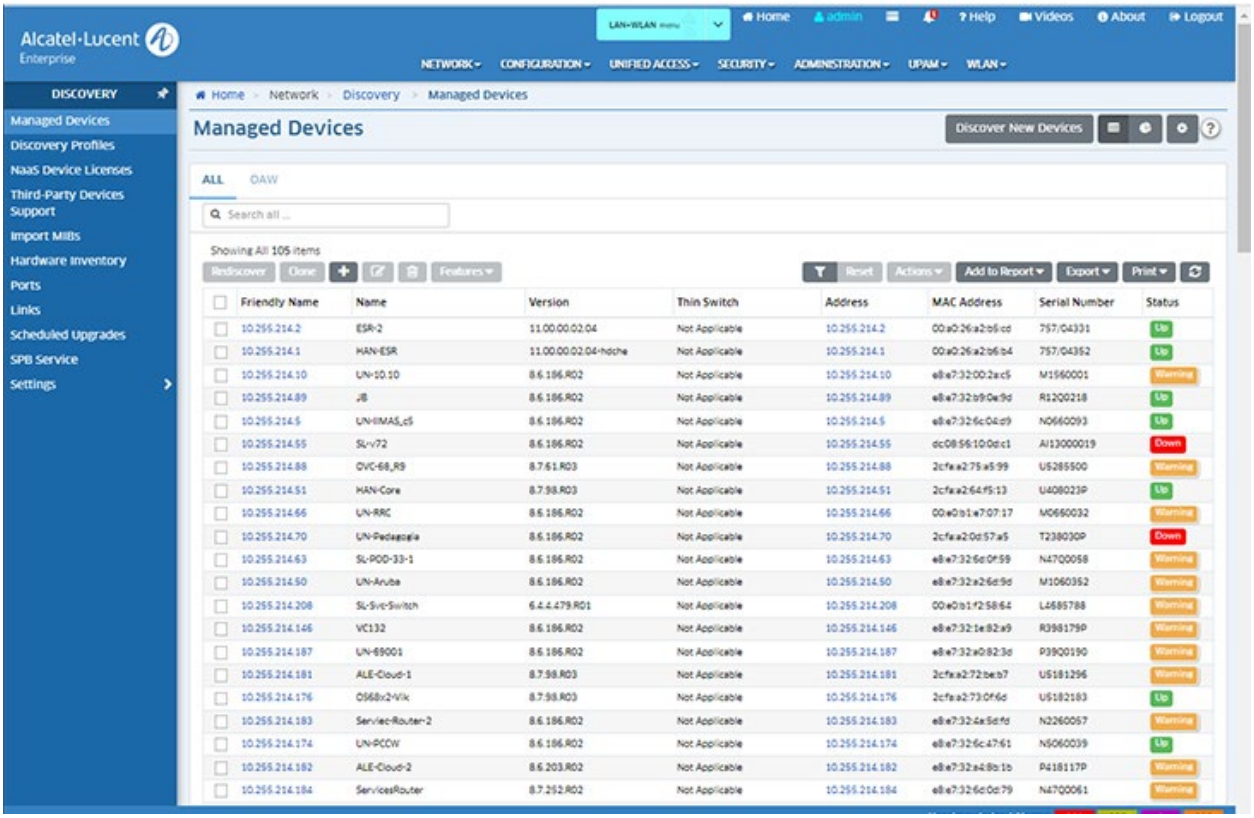
- **User Name -** The user name.
- **Host Name -** The host name of the client where this session originated. If the address cannot be resolved to a host name, the IP address is displayed.
- **IP Address -** The IP address of the client where this session originated.
- **First Name -** The first name of the user.
- **Last Name -** The last name of the user.
- **Description -** The user description.
- **Login Server -** The name of the Authentication Server used to authenticate the session.
- **Logged in Since -** A timestamp of when was the session was created. **User Groups -** The user group(s) to which the user belongs.

12.0 Discovery Overview

The Discovery application is used to discover network devices. The information gathered is used by OmniVista applications to view and configure the network. The information includes:

- Alcatel-Lucent Enterprise devices in the network.
- The links between devices in the network. This information is used to display network links in graphical maps of network regions.
- Additional link information required by OmniVista's Locator application.
- Third-party devices built by Cisco and Extreme.
- Any additional third-party devices for which support has been added.

Discovery



Discovery is configured and performed using the screens below:

- **Managed Devices -** Displays a list of all discovered network devices. It is also used to discover/rediscover devices.
- **Discovery Profiles -** Used to create a profile containing the parameters used for discovery (e.g., SNMP version, permissions).
- **NaaS Device Licenses -** Displays the Network as a Service (NaaS) licensing information for discovered switches running AOS Release 8.8R1 or higher.
- **Third-Party Devices Support -** Used configure discovery parameters for third-party devices (e.g., OID, Display Name).

- **Import MIBs -** Used to import new or updated MIB files into OmniVista.
- **Hardware Inventory -** Used to view inventory information (e.g., CMM, Chassis, Power Supplies) for any discovered device.
- **Ports -** Used to display information about ports on network devices, and is also used to enable/disable device ports.
- **Link -** Displays all links that were learned during the discovery process or created manually in OmniVista. It is also used to manually create, edit, and delete manual links.
- **Scheduled Upgrades -** Used to schedule automatic upgrades for your network devices.
- **SPB Service -** Displays information about SPB Services in the network.
- **Settings -** Used to configure automatic discovery frequency parameters, enable/disable IP Failover, and configure switch monitoring.

Managed Devices

The Discovery application Managed Devices Screen displays a list of all discovered network devices (default). It is also used to discover/re-discover devices, Enable/Disable IoT, Enable/Disable Statistics Collection, and add/clone/edit/delete/search for devices. You can also perform certain operations on devices such as ping/poll devices, configure traps, locate end stations, and reboot devices.

> **Note:** Admin and Netadmin users will see all discovered network devices. For other users the devices displayed depend on the User Role and User Group as defined in the Users and User Groups application). Only the devices in the maps associated with a User's Role will be displayed.
>
> **Note:** If any managed devices have unsaved configuration changes in their Working Directory, a number will appear in the Notification icon (Bell icon) at the top of the screen. When you click on the Notification icon, the number of devices in this condition is displayed. Click on the **Save Now** button to save changes to the Working Directories of the devices.

Discovering/Re-Discovering Devices

You can discover new network devices or re-discover devices to update information for those devices. Note that the procedures below apply to all devices **except** Stellar AP Series Devices. Click here for information on discovering Stellar AP Series Devices.

Discovering Devices

OmniVista performs a discovery based on a specified IP address range and Discovery Profile. The Range specifies the IP address range in which you want to discover devices. The Range is associated with a Discovery Profile. The Discovery Profile contains the parameters that are used by OmniVista when performing the discovery (e.g., SNMP version used to discover devices, FTP/Telnet passwords needed to connect to a device).

> **Important Note:** An IP range must not include a broadcast IP. If your network is divided into subnets, create multiple IP ranges with one IP range per subnet.

Discovering Devices Using an Existing Range

To discover devices using an existing range, click on the **Discover New Devices** button at the top of the screen. Any configured ranges appear in the Ranges List. Select a range and click on the **Discover Now** button. When you click on the **Discover Now** button, the discovery will begin and a progress screen will appear. When the discovery is complete the discovered devices will appear on the Managed Devices Screen.

Creating a New Range for Discovering Devices

If you want to create a new Range, click on the **Discover New Devices** button to bring up the Ranges List. Click on the Add icon and complete the fields as described below. When you are finished, select the new Range in the Ranges List and click on the **Discover Now** button. When you click on the **Discover Now** button, the discovery will begin and a progress screen will appear. When the discovery is complete the discovered devices will appear on the Managed Devices Screen.

- **Start IP -** The starting IP address of the discovery range (e.g., 10.255.10.1)
- **End IP -** The ending IP address of the discovery range (e.g., 10.255.10.254)
- **Subnet Mask -** The subnet mask used for the discovery range (e.g., 255.255.255.0)
- **Description -** A description for the discovery range.
- **Choose Discovery Profiles -** Select the Discovery Profile(s) to use for the discovery. If necessary, click on the Add icon to go to the Discovery Profiles Screen and create a new profile. After the profile is created, return to this screen and create a new range using the new profile(s). You **must** associate a discovery range with at least one Discovery Profile to perform the discovery.

  If you want to use more than one Discovery Profile for new range, drag and drop the profiles in the list to prioritize the order in which they are used for discovery. OmniVista will first attempt to discover each device using the first profile listed. If OmniVista cannot communicate with a device using the first profile, it will try the next profile, and so on. If OmniVista cannot communicate with a device using any of the profiles, it will attempt to communicate with the switch using the default profile. Once OmniVista successfully communicates with and discovers a device, it will use that Discovery Profile for all future communications with that device (unless you edit the device in the list).

Re-Discovering Devices

You can "re-discover" previously discovered devices to update information about a device(s). For example, you might wish to re-discover a device to learn VLAN information that was not gathered during the first discovery; or re-discover a device if that device was re-configured outside of OmniVista. To re-discover a device(s), select the device(s) in the list and click on the **Rediscover** button. The discovery will begin and a progress screen will appear. When the discovery is complete the discovered devices will appear on the Managed Devices Screen.

Note: If a switch was discovered previously, and a new discovery is performed using a Discovery Profile that specifies different parameters (e.g., CLI/FTP user name and password, Shell Preference), the profile values will not overwrite the values already specified to OmniVista for that device. The values specified in the profile will apply to newly-discovered devices only.

Discovering Stellar AP Series Devices

The discovery process is different for Stellar Aps. These devices automatically contact OmniVista when they are connected to the network. The AP Registration application in OmniVista places these devices in an "Unmanageable" state. At this point, they do not appear in the Discovery or Topology applications. You then go to the AP Registration application and place the devices into "Manageable" state. Once you designate the devices as "Manageable", the devices will appear in the Discovery and Topology applications and can be configured in OmniVista.

> **Note:** When a Stellar AP reboots, it reboots from the last saved configuration. It is recommended that users regularly perform a “Save to Running” operation on Stellar APs to save the most recent configuration in the event an AP reboots but is unable to connect to OmniVista to retrieve the latest configuration.

Enabling/Disabling IoT

The IoT application provides a detailed, "real-time" view of all endpoint devices connected to AOS Switches and Stellar APs (e.g., PCs, Tablets, Smartphones). IoT is disabled on AOS Switches and Stellar APs by default. To enable IoT on a switch/Stellar AP, select the switch(es)/AP(s) in the Managed Devices List, click on the **Features** drop-down, and select **Enable IoT**. The switches/APs will appear in the "Enable IoT - Confirm" switch picker window. (Note that switches/APs that do not support IoT will not appear in the window.) Click **OK** to enable IoT.

OmniVista will begin collecting IoT information for endpoints connected to the switches/APs. Go to the IoT application to view information (Network - IoT).

To disable IoT on a switch/AP, select a switch/AP in the Managed Devices List, click on the **Features** drop-down, and select **Disable IoT** button.

Enabling/Disabling Statistics

The Analytics Statistics feature enables you to collect and view performance statistics for network switches. To enable statistics collection on a switch(es), select the switch(es) on which you want to enable statistics, click on the **Features** drop-down, and select **Enable Statistics**.

Enabling/Disabling Network Advisor Monitoring

By default, OmniVista Network Advisor monitoring is disabled. To enable Network Advisor monitoring on a device(s), select the device(s) in the Managed Devices List, click on the **Features** drop-down, and select **Enable OmniVista Network Advisor**. The "Select OmniVista Network Advisor Instance" dialog opens. Select the Network Advisor instance that you want to monitor your devices from the drop-down list and click **OK**. You can also click on **Add New** to add a new Network Advisor instance to the list.

Adding a Device

You can manually add a device to the list. Click on the Add icon bring up the Add New Device Screen and complete the fields as described below. After completing the fields, click on the Add icon to add the device. Note that you can "clone an existing device” to quickly add a new device.

> **Note:** Do **not** manually add a Stellar AP using the Managed Devices List. To manually add a Stellar AP, go to the Unmanaged Devices Tab of the Access Points Screen

(Network - AP Registration - Access Points - Unmanaged Devices Tab). Once a Stellar AP is added to the Unmanaged Devices List, the AP automatically contacts the OmniVista Server and is added to the Managed Devices List once it is connected to the network.

This includes manually adding a "Down" Stellar AP to the Managed Devices List. If you manually add a "Down" Stellar AP to the Managed Devices List, it will consume a Third-Party License. Once the AP comes "Up" and registers with OmniVista, you will not be able to delete the previous entry or release the license.

General

- **IP Address -** The device's primary IP address.
- **Assign a Site -** If you have configured sites in the Geo Maps feature, you can select a site from the drop-down to initially assign the device to the site. Geo Map Sites are configured in the Topology application. See the Topology Help for more information on Geo Maps.
- **Location -** A user-configured location description for the device.
- **CLI/FTP User Name -** The user name that OmniVista will use to establish CLI/FTP sessions with the discovered devices. The user name specified will be used to auto-login to devices when CLI sessions are established. It will also be used to perform FTP with the device when configuration files are saved and restored (see note below).
- **CLI/FTP Password -** The password that OmniVista will use to establish CLI/FTP sessions with the discovered devices. The user name specified will be used to auto-login to devices when CLI sessions are established. It will also be used to perform FTP with the device when configuration files are saved and restored (see note below).
- **Confirm CLI/FTP Password -** Confirm the CLI/FTP Password.
- **Secondary Password -** The secondary CLI/FTP Password, if applicable.
- **Confirm Secondary Password -** Confirm the secondary CLI/FTP Password, if applicable.

Note: The CLI/FTP User Name and Password fields enable you to inform OmniVista of the device's CLI/FTP User Name and Password. A device's CLI/FTP User Name and Password cannot be configured from OmniVista, they must be configured directly on the device. If you do not define the CLI/FTP User Name and Password and you attempt to save, restore, or upgrade configuration files for a device, you will be individually prompted for the CLI/FTP User Name and Password of each individual device for which configuration files are being saved, restored, or upgraded. Also, OmniVista will be unable to auto-login to the device when establishing CLI Scripting sessions.

SNMP

- **SNMP Version -** The SNMP version that OmniVista will use to communicate with the device. The default version for AOS devices is v2, but v1 and v3 are also supported.
- **Timeout (msec) -** The time period, in milliseconds, that OmniVista will wait for a switch to respond to a connection request before assuming that the request has timed-out (Default = 5,000).

- **Read Community** - The device's "get" community name. The "get" community name enables OmniVista to read information from the device (see note below).
- **Write Community -** The device's "set" community name. The "set" community name enables OmniVista to write information to the device (see note below).
- **Retry Count -** The number of times that OmniVista will attempt to connect to a switch (Default = 3).
- **User Name (SNMP v3 Only)** - The SNMP version 3 user name.
- **Auth & Priv Protocol (SNMP v3 Only)** - The authentication protocol OmniVista will use for SNMP communication with the device. Authentication uses a secret key to produce a "fingerprint" of the message. The fingerprint is included within the message. The device that receives the message uses the same secret key to validate that the fingerprint is correct. If it is, and if the message was received in a timely manner, then the message is considered authenticated. Otherwise, the message is discarded. The fingerprint is called a Message Authentication Code, or MAC. Note that if you are using SHA256+AES 192 or 256 authentication protocols you must download and install the Zulu Cryptography Extension Kit (CEK) using the Preferences application (Preferences - System Settings Install Zulu CEK). If a protocol is selected, complete the fields below:
    - **Auth Password -** The password that OmniVista will use for the authentication protocol. This must be the same password that is defined on the switch. If no authentication password is entered, neither authentication nor privacy encryption will be used.
    - **Confirm Auth Password -** Re-enter the Auth password.
    - **Private Password -** The password that will be used as the secret key. This must be the same password that is defined on the switch for the CBC-DES Symmetric Encryption Protocol. If an authentication password is entered, but no privacy password is entered, authentication will be used without privacy encryption.
    - **Confirm Private Password** - Re-enter private password.
- **Context Name (SNMP v3 Only)** - A unique context name for this context. An SNMP context is a collection of management information accessible by an SNMP entity, in this case OmniVista. A context identifies a subset of management information, in this case the management information OmniVista has about the individual device. OmniVista, as an SNMP entity, has access to many SNMP contexts: one for each device it manages. Each context must be identified by a unique context name and a unique context ID. Note that an item of management information may exist in more than one context. Technically, the Context Name and Context ID provide a means of distinguishing specific instances of information in the MIB modules from the set of all instances of that information within the management domain.
- **Context ID (SNMP v3 Only)** - A unique context ID for this context. As explained above, each context must be identified by a unique context name and a unique context ID. Note that neither the **Context Name** nor the **Context ID** are required for AOS or default third-party devices supported by OmniVista. Leave these fields blank unless you are using a non-default third-party device that requires definition of a Context Name and Context ID.

  Note: If a device's "get" and "set" community names are "public" (the default) you can leave these fields blank (OmniVista uses the default name (public) when the field is blank. The community names are not configurable from

OmniVista, they must be configured directly on the device. Also note that when you use SNMP Version 3, community names are ignored.

Advanced Settings

- **Trap Station User Name -** The user name that will be used when an AOS device is configured to send traps to OmniVista. AOS devices require that a valid device user name be specified with the trap station configuration entry. If this field is left blank, the following switch user names will be used by default for trap station configuration entries:
    - If OmniVista is configured to use SNMP version 3 with this device, the SNMP version 3 user name entered for the device will be used as the switch user name in the trap station configuration entry.
    - If OmniVista is configured to use SNMP version 1 or SNMP version 2 with this device, the read community string for the device will be used as the switch user name in the trap station configuration entry.

  When using SNMP version 1 or 2, switch user names are interchangeable with community strings as long as community string mapping is not in use on the switch. If community string mapping is not in use, and an AOS switch is discovered using SNMP version 1 or 2 with a default read community string of "public", or even with a non-default read community string such as "thomas", these community strings are valid switch user names for trap station configuration entries. In this case, no further configuration is required and this field can be left blank. However, if community string mapping is enabled on the device, the community string with which the switch is discovered is not guaranteed to be a valid device user name, and thus is not guaranteed to be a valid device user name for a trap station configuration entry. In this case, you should enter a valid device user name in the Trap Station User Name field.
- **Discover Link -** Specifies how OmniVista will discover the device's links to other devices.
- **Shell Preference -** OmniVista's CLI Scripting application supports both the Telnet and SSH command line interfaces. SSH (Secure Shell) is a Telnet-like utility that provides encryption and is far more secure than Telnet. If you select **SSH**, SSH will be used as the default command line interface for the device. In addition, Secure Shell FTP will be used as the default FTP method in Resource Manager. If you select **Telnet**, Telnet will be used as the default command line interface for the device and regular FTP will be used as the default FTP method in Resource Manager. Ensure that devices are capable of SSH before you enable the **Prefer SSH** checkbox. OmniVista does not verify devices' SSH capabilities. All AOS devices are SSH-capable. (Default = SSH)
- **Use Get Bulk -** Enables/Disables Get Bulk Operations. The SNMP version 2 Get Bulk operation is used for retrieving large amounts of data, particularly from large tables. The Get Bulk operation performs continuous Get Next operations, each time requesting the number of table rows specified by the value in the **Max Repetitions** field (below). For example, if the value in the Max Repetitions field is 10, each Get Next operation will request 10 rows of table data. Note that the number of rows of data returned by the device will be determined by the amount of memory the device has available at that time. Note that "Use Get Bulk" is only applicable to device discovery or polling. Other applications in OmniVista (e.g., Statistics) may internally use getBulk operations to retrieve data from devices regardless of the option chosen here. (Default = Enabled)

- **Max Repetitions -** The number of rows of table data that the Get Bulk operation will request in each Get Next operation, if enabled.
- **Allow Port Disabling -** Enables/disables port disabling for the Quarantine Manager application. If port disabling is enabled, and the Quarantine Manager application is configured for port disabling, ports on the device will automatically be disabled if a Quarantine Rule is matched.

Cloning a Device

Select a device in the list and click on the **Clone** button at the top of the screen. The Add New Device Screen will appear with the SNMP and Advanced Settings reflecting the configuration of the selected device. Enter the IP address and passwords for the new device and, if necessary, edit any SNMP or Advanced Settings fields. After completing the fields, click on the Add icon to add the device.

Editing a Device

You can edit a single device or edit multiple devices at the same time. To edit a single device, select a device in the list and click on the Edit icon. The Edit Discovery Manager Entry Screen will appear. Edit any fields as described above and click on the **Apply** button. Note that you cannot edit the Device Name.

To edit multiple devices, select the devices in the list and click on the Edit icon. The Edit Discovery Manager Entry Screen will appear and the selected devices will be listed in the IP Address Field. You can click on the device list to bring up the Selected Devices Window to display device information. Click again anywhere on the screen to close the window. Edit any fields as described above and click on the **Apply** button.

Note that if a field has different values among the selected devices (e.g., different location, different password), the field will be blank (drop-down menu) or grayed out ("yes/no" slider field), and a "Click to Overwrite" link will appear beneath the field. If you want to configure a common value for the field on all selected devices, click on the "Click to Overwrite" link and enter a value. If you want the values on each device to remain as they are, leave the field as it is. If you change your mind and want the fields to retain their original values, click on the "Retain Original Values" link **before** clicking on the **Apply** button.

> **Note:** Stellar AP Series Devices are edited on the Access Points Screen in the AP Registration application (Network - AP- Registration - Access Points). When you select one of these devices and click on the Edit icon, you will be redirected to the AP Information Edit Screen in the AP Registration application. When you apply the edit, the changes will be reflected in the Hardware Inventory List after the next poll. Also note that the Discovery Multi-Edit feature is not supported on Stellar APs. To edit multiple Stellar APs, go to the Access Points Screen in the AP Registration application.
>
> **Note:** When you edit a device, it is important to understand that you are editing OmniVista's knowledge of the device, not the device itself.

Deleting a Device

Select a device(s) and click on the Delete icon, then click **OK** at the confirmation prompt. Note that when you delete a Stellar AP Series Device, the device is removed from the Hardware

Inventory List in the Discovery application and placed into "Unmanageable" status on the Access Points Screen.

Searching for a Device

You can search for a device by keyword by entering the search criteria in the Search fields at the top of the list. Enter any search criteria based on the contents found in the table and the list will change to display only those devices containing the search criteria.

Perform Device Operations

You can also perform certain operations on devices in the list such as ping/poll devices, configure traps, locate end stations, and reboot devices. Select a device(s) in the list. Click on the **Actions** button at the top of the list and select an option from the drop-down list. Note that not all operations are supported on all devices; and some operations can only be performed on a single device, not multiple devices. If an operation is not supported for the selected device(s), it will be grayed out in the list.

- **Ping -** Immediately pings the selected device(s). Progress is shown on the Progress Screen. Click the **Finish** button to return to the Managed Devices Screen. Execution of the Ping operation is different depending on the device type:
  - **AOS Devices -** OmniVista performs an SNMP ping first. If the SNMP ping succeeds, OmniVista reports the operation as successful. If it fails, OmniVista generates an "alaSNMPDown" trap and continues to perform an SSH/Telnet ping. OmniVista uses Telnet or SSH based on Shell Preference (default = SSH). If the SSH/Telnet ping succeeds, OmniVista reports the device ping operation as successful. If it fails, OmniVista reports the operation as failed and generates an "alaOvSwitchDown" trap. Note that for an SSH/Telnet ping, OmniVista does not use require any user credentials for authentication. It is just ping test.
  - **OmniAccess WLAN Controller, OmniAccess WLAN IAP, OS 2220, and Third-Party Devices -** OmniVista performs an SNMP ping. If the SNMP ping succeeds, OmniVista reports the operation as successful. If it fails, OmniVista reports the operation as failed and generates an "alaOvSwitchDown" trap.
  - **Stellar APs -** OmniVista checks device reachability and manageability via WMA. If it succeeds, OmniVista reports the operation as successful. If it fails, OmniVista reports the operation as failed and generates an "alaOvSwitchDown" trap.
- **Poll For Traps -** Immediately polls the selected device(s) for traps. A message is displayed at the top of the Managed Devices Screen when polling is complete. Traps can be viewed in the Notifications application.
- **Poll Links -** Immediately polls links on the selected device(s). Progress is shown on the Progress Screen. Click the **Finish** button to return to the Managed Devices Screen.
- **Configure Health Thresholds -** Brings up the Configuring Devices Health Thresholds Screen. Health Thresholds are used to set limits for health traps. If a device has been configured to send health traps, a trap will be sent whenever a monitored item's current utilization exceeds the configured health threshold. Configure the CPU, Memory, or Temperature Threshold for the selected device(s) and click on the **Apply** button. Note that you cannot configure the Temperature

Threshold for OS10K, OS6900, or OS6860 devices. The Temperature Threshold is hard coded on devices. Also note that changes made to health thresholds will not appear until the next polling cycle (up to an hour).

Note: You can also quickly configure Health Threshold Traps from the Configuring Devices Health Thresholds Screen by clicking on the **Configure Traps** button at the top of the screen. The first screen of the Notifications Trap Wizard (Devices Selection) will appear with the selected device(s) pre-selected. Click on the **Next** button to go to the Configure Traps Screen. Depending on the devices selected, the "Configure AOS 6.x Traps" and/or the "Configure AOS 7.x/8.x Traps" options will appear. The Health Threshold Traps are already pre-selected. (If you want to configure additional traps, expand the traps options to add additional traps.) Otherwise, click on the **Next** button to go to the Summary Screen to review the configuration. Click on the **Finish** button to configure the traps for the selected device(s).

- **Locate End Stations -** Launches the Locator application and searches for all end stations that are attached to the selected switch. All end stations found are displayed in the Locator application's Browse Screen.
- **Webpage -** Opens up a Web session with the selected device. The web session application varies depending on the device. For example, AOS devices will open a WebView session.
- **Device Inventory -** Launches the Inventory Screen in the Resource Manager Application for the selected switches, which enables you to create and Inventory Report for the selected devices.
- **Backup Device -** Launches the Backup Wizard in the Resource Manager Application, which enables you to perform a configuration backup of the selected devices.
- **SSH -** Opens up a Telnet session with the selected device in the CLI Scripting application.
- **SSH Custom -** Opens an SSH session with the selected device using a custom SSH client installed on your computer. Select a device and click on **SSH Custom**. At the prompt, click on **Open SecureCRT Application**. The SecureCRT® Client window will open. Enter the device Username and Password at the prompts. SecureCRT will connect to the device. OmniVista supports the SecureCRT SSH Client. Note that you must install SecureCRT on your OmniVista Client and configure SecureCRT settings so that it is the default SSH Client on your computer. If it is not installed and configured correctly, a blank page will appear when you attempt to connect using the "SSH Custom" option.
- **Configure Traps -** Launches the Trap Configuration Wizard in the Notifications application to enable you to configure traps for the selected devices.
- **View Traps -** Opens the Notifications Home page to display traps for the selected device.
- **Reboot -** Reboots the selected device(s) You have the option of rebooting from the Working, Certified, or Other Directory and setting a time for the reboot. Click on the Reboot operation link and use the **Reboot From** drop-down to select the directory you want to reboot from. In the **Reboot Delay** dropdown select when you want to reboot to occur (now, a specific number of minutes from now, or at a specific date

and time). Note that when you reboot multiple devices, there is a minimum delay of 30 seconds before the devices reboot (even if you select the Reboot now option). If you select a large number of devices, the delay is equal to roundoff of (30 + (deviceCount/4), in seconds (e.g., if you select 1,000 devices, the delay is 280 seconds, or 4 minutes). The delay allows time to push the "Reboot" command to all devices.

- **Copy Running/Working to Certified -** Copies the contents of the working/running directory in the primary CMM to the certified directory in the primary CMM. Note that the Copy Working to Certified command also automatically synchronizes the switch's CMMs after the copy operation is completed.
- **Copy Certified to Working/Running -** Copies the contents of the certified directory in the primary CMM to the working/running directory in the primary CMM. For AOS 6 devices, this means that if the device is running from the Certified Directory, this will copy the configuration from Certified to Working directory, then change the Running directory to the Working directory. For AOS 5 and AOS 8 devices, if the device is running from the Certified Directory, this will copy the configuration to the Certified Directory.
- **Save to Running -** Saves the primary CMM's current running configuration to the current running directory of the switch. OmniVista supports the Multiple Working Directories Feature on certain devices (e.g., OS10K, OS6900). This feature allows the user to create multiple "working" directories on the switch that can be used to save specific switch configurations. When the Save to Running Command is executed, the device(s) save the CMM's current running directory to the current user-defined "working" directory (Running Directory). Note that if you select a group of devices and some do not support multiple working directories, the devices will save the CMM's current running directory to the device's current "working" directory, whether it is a user-defined directory or the Working Directory.
- **Scheduled Upgrades -** Takes you to the Scheduled Upgrades Screen's Upgrade Wizard where you can schedule immediate or periodic software upgrades on a device(s).

  Note: For Virtual Chassis stacks (running AOS 8.5R2 or higher or 6.7.3.R04 higher), if you attempt to save a configuration to the Running Directory and there has been a change in the Virtual Chassis stack topology since the last save, a warning prompt will appear listing the problem devices. You can proceed to save the configuration(s) on all devices, or make any necessary configuration updates to devices before saving. If you proceed with the save without addressing the changes, a trap will be generated (virtualchassisstatuschange) in the Notifications application.

OmniVista Network Advisor

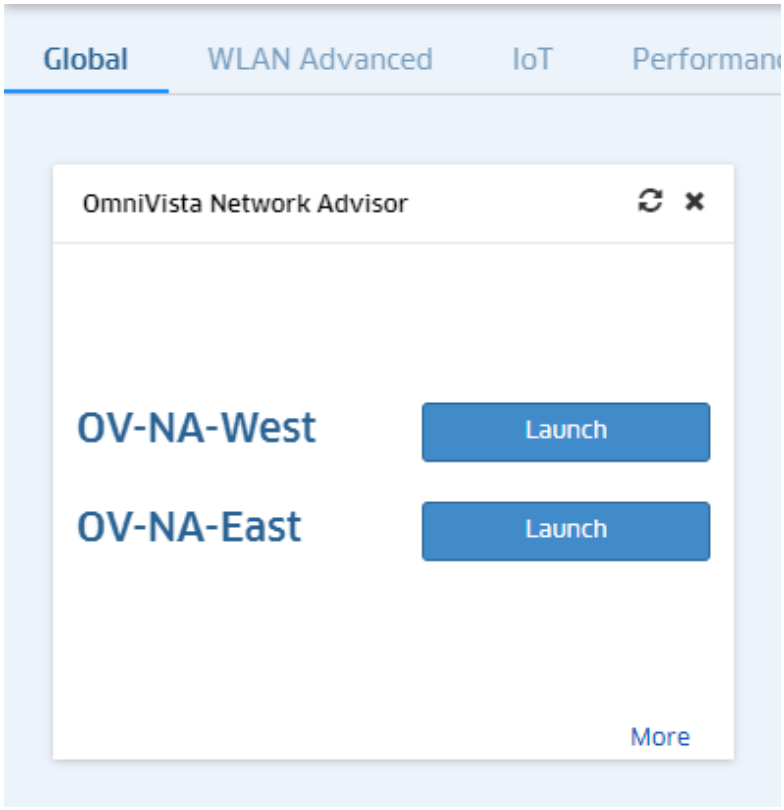
OmniVista Network Advisor is an important troubleshooting tool that you can use to monitor the network and take action to correct any detected network problems. When Network Advisor monitoring is enabled for a device(s), the device begins to send Syslog messages to the specified OmniVista Network Advisor instance. Network Advisor analyzes Syslog messages received from monitored devices to identify anomalies in the network. When an anomaly is detected, Network Advisor notifies system administrators and other authroized persons through Rainbow. Anomaly notifications can alert those receiving notifications that something, potentially serious, has taken place and even suggest steps to immediately remediate the problem.

Using Network Advisor to Monitor Managed Devices

OmniVista Cirrus integration with OmniVista Network Advisor allows you to configure Network Advisor monitoring for one or more managed devices. This process involves declaring Network Advisor instances that you can select and assign to managed devices.

To declare Network Advisor instances to access in OmniVista Cirrus, a Network Advisor application widget is available to add to the Global Dashboard of the OmniVista Cirrus Home page. This widget displays a list of Network Advisor instances that are available to assign to managed devices. You can also open the website for a specific instance by clicking on **Launch** next to the list entry. To add or remove a Network Advisor instance, click the "More" link on the widget.

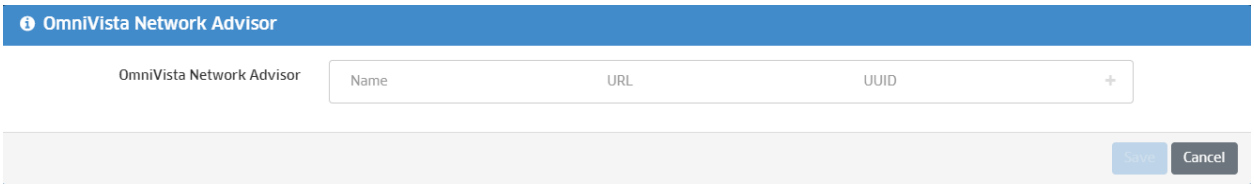
An OmniVista Network Advisor application widget is available to add to the Global Dashboard of the OmniVista Cirrus Home page. This widget displays a list of Network Advisor instances that are available to assign to managed devices. You can also open the website for a specific instance by clicking on **Launch** next to the list entry. To add or remove a Network Advisor instance, click the "More" link on the widget.



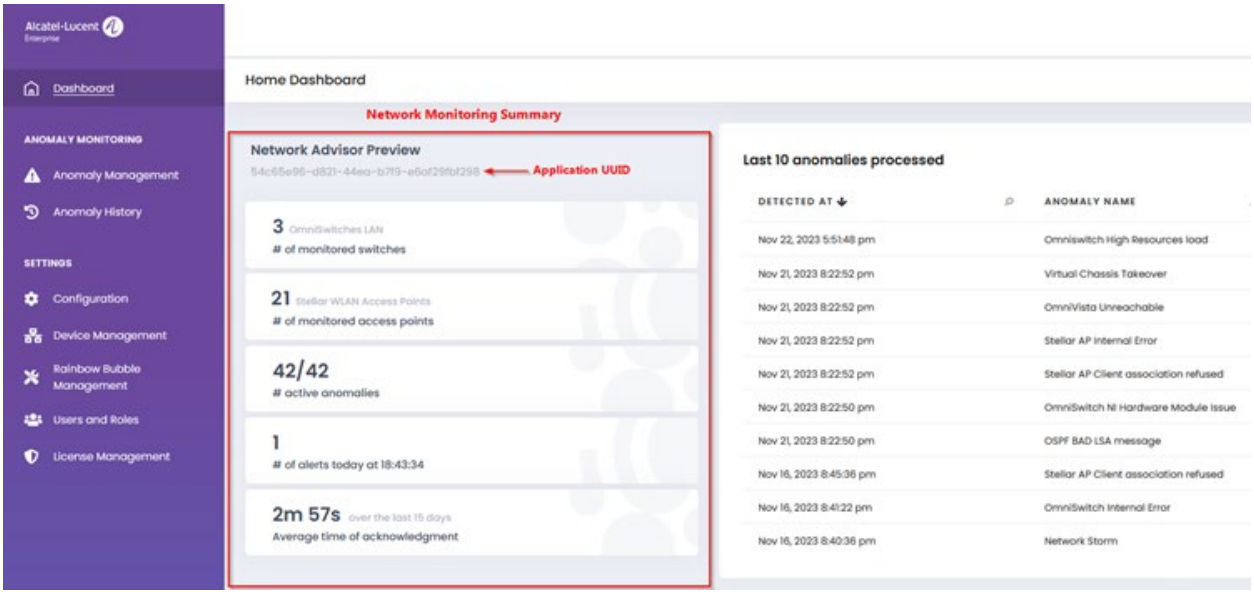
After you have added the OmniVista Network Advisor widget to the Global Dashboard and declared Network Advisor instances, you can assign one or more managed devices to an instance. Once assigned to an instance, Network Advisor will begin monitoring that device to detect any anomalies defined in the Network Advisor application.

Declaring a Network Advisor Instance

Network Advisor instances are declared in OmniVista Cirrus by clicking the "More" link on the OmniVista Network Advisor widget to open the OmniVista Network Advisor dialogue window. Complete the fields as described below for each Network Advisor instance that you want to declare, then click **+** to add the instance to the list:



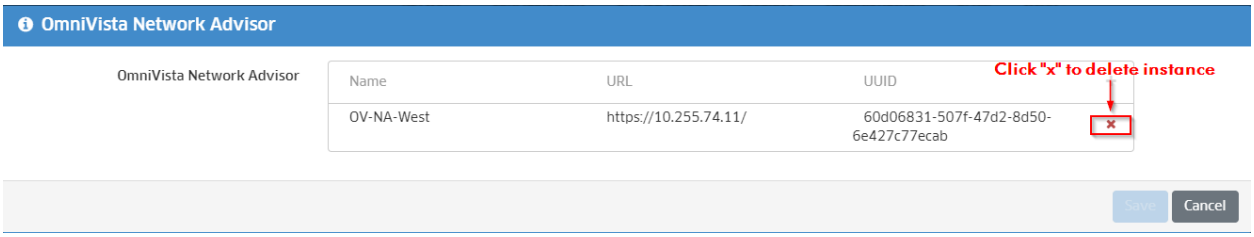
- **Name** - Enter a unique name to identify the instance in OmniVista.
- **URL** - Enter the IP address or FQDN of the website for the Network Advisor instance that you want to associate with the specified name.
- **Application UUID** - Enter the Application UUID for the Network Advisor instance that will monitor this device. A unique Application UUID is automatically generated (even if OmniVista synchronization is disabled) for every installation of OmniVista Network Advisor. This Application UUID is provided during the OmniVista Network Advisor installation process. This UUID is located on the Home Dashboard of the Network Advisor instance. For example:



When you are done adding the Network Advisor instances that you want to declare, click on **Save**. The OmniVista Network Advisor widget will display the declared instances with a **Launch** button next to each instance, as shown above.

Removing a Network Advisor Instance

To remove a Network Advisor Instance, make sure the instance is not assigned to any devices, then click the "More" link on the OmniVista Network Advisor widget to open the OmniVista Network Advisor dialogue window. Click on the **x** next to each instance that you want to remove.



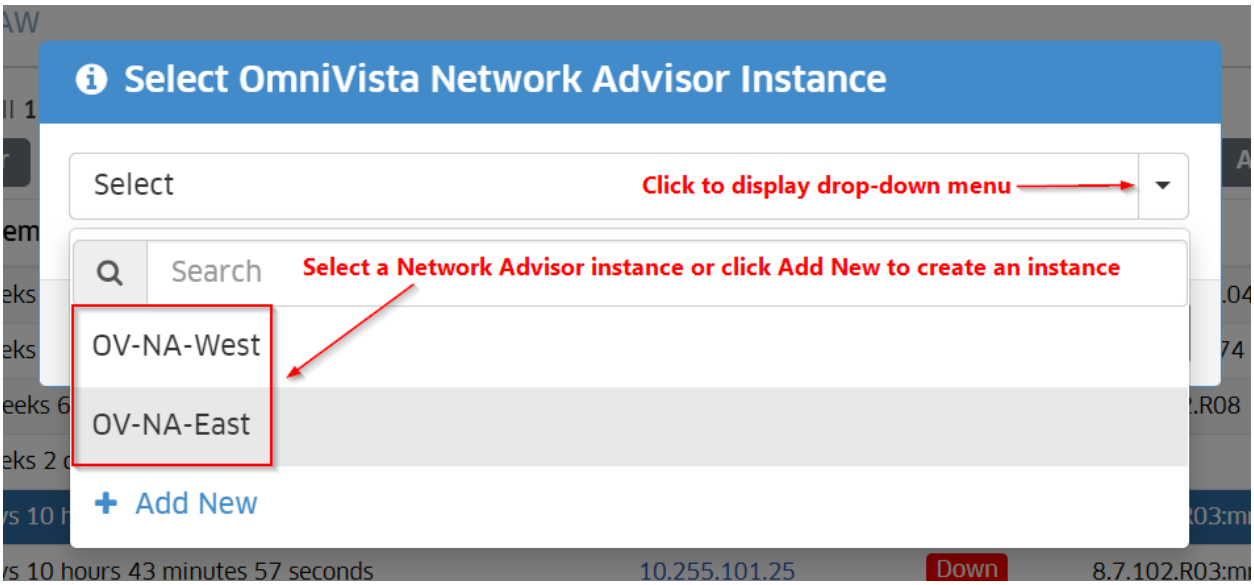
When you are done deleting one or more instances, click **Save**.

Note: If the Network Advisor instance you are attempting to remove is assigned to one or more devices, an error message is displayed on the widget and the instance is not removed.

Enabling/Disabling Network Advisor Device Monitoring

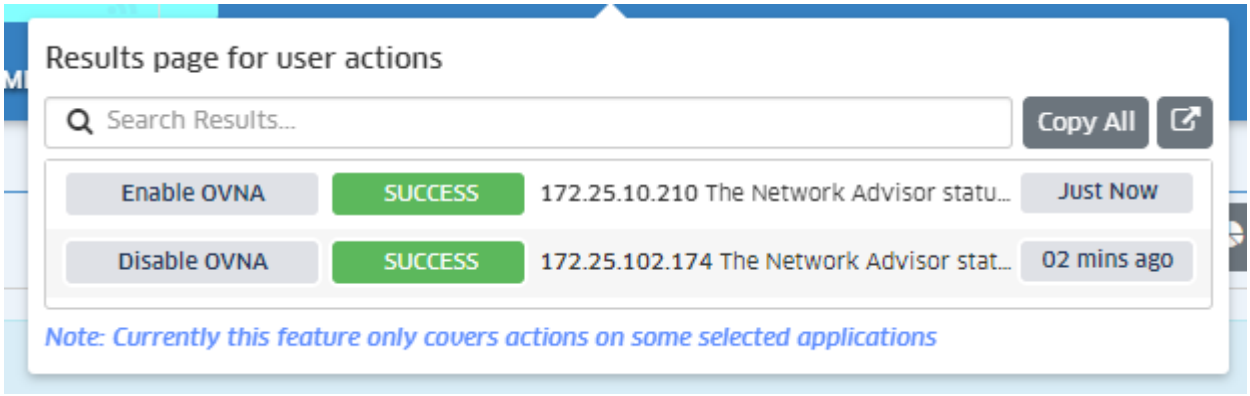
Note: OmniVista supports Network Advisor monitoring only for Managed devices. If a device is not yet in the Managed state, you cannot activate Network Advisor monitoring for that device.

Network Advisor monitoring is enabled on one or more devices by selecting device(s) in the Managed Devices List. then clicking on **Features** and selecting **Enable OmniVista Network Advisor** from the drop-down list. The "Select OmniVista Network Advisor Instance" dialog opens. Select the Network Advisor instance that you want to monitor your devices from the drop-down list and click **OK**. You can also click **Add New** to create a new instance to add to the list.



To disable Network Advisor monitoring, select one or more monitored devices in the Managed Devices List, click on the **Features** drop-down, and select **Disable OmniVista Network Advisor**. Click **OK** at the confirmation prompt.

When you enable or disable Network Advisor monitoring for a device, the Results page displays the status of the requested action.



Synchronizing OmniVista With Network Advisor

Synchronizing data between OmniVista Cirus and declared Network Advisor instances notifies Network Advisor instances of the following information:

- When monitoring is enabled for a device in OmniVista, the Network Advisor instance is notified and the device is added to the Monitored Devices list for that instance.
- When monitoring is disabled for a device in OmniVista, the Network Advisor instance assigned to that device is notified and the device is removed from the Monitored Devices list for that instance.

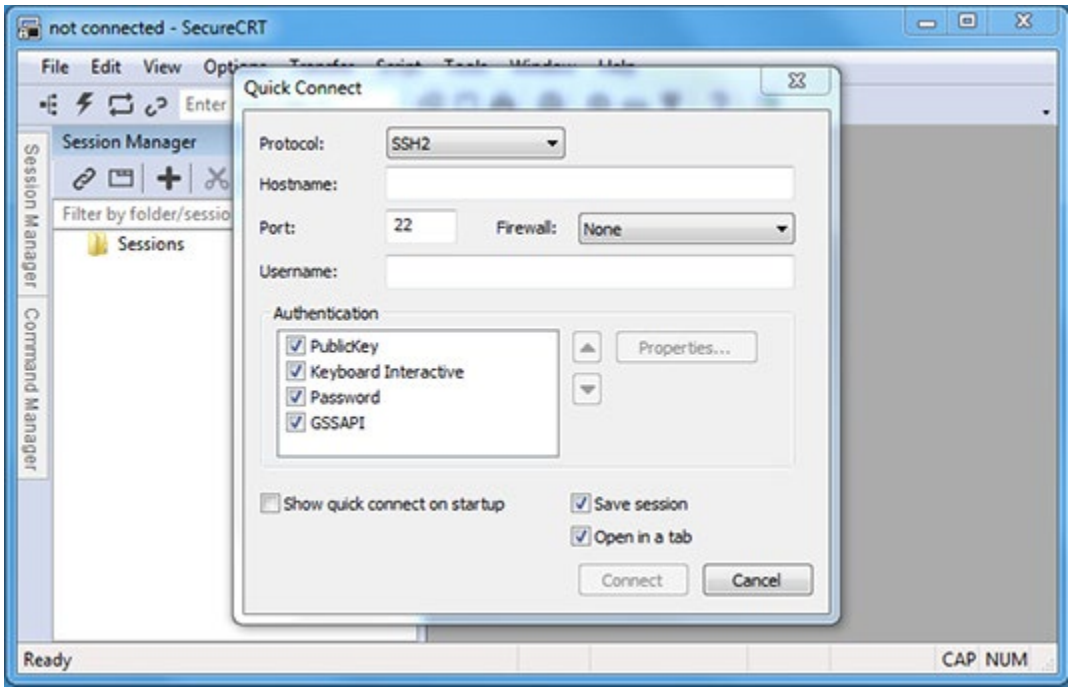
The synchronizing of data allows declared Network Advisor instances to maintain an up-to-date list of managed OmniVista Cirrus devices that the instance will monitor for detected anomalies. Network Advisor will periodically poll the associated OmniVista Cirrus installation to obtain monitored device information. Enabling or disabling data synchronization is done through the Network Advisor instance. Refer to the "OmniVista Synchronization" section in the *OmniVista Network Advisor User Guide* for more information.

Note: For each Network Advisor instance, there is only one association configured with an OmniVista installation. A single OmniVista installation can support declaring multiple Network Advisor instances, but a single Network Advisor instance only supports synchronization with one OmniVista installation. As a result, there is no duplication of monitored devices across multiple Network Advisor instances; each instance monitors specific devices not monitored by other instances.

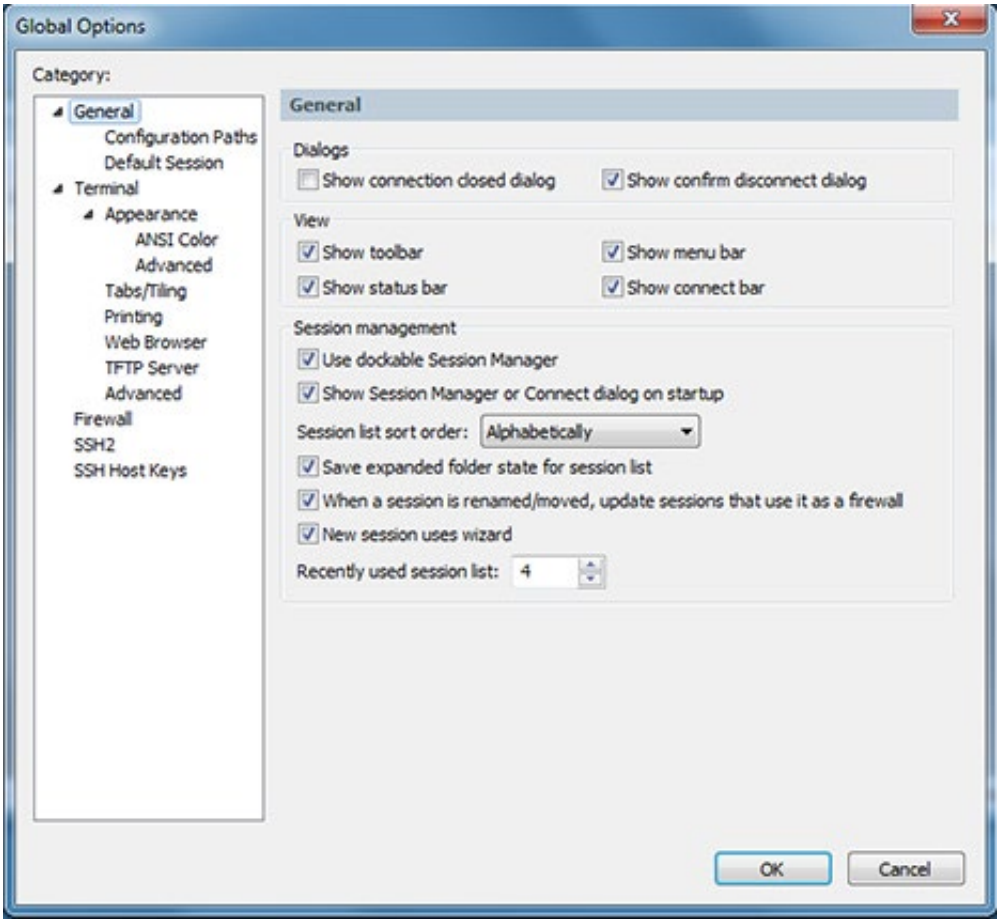
Installing/Configuring SecureCRT

1. Download and install SecureCRT on your OmniVista Client

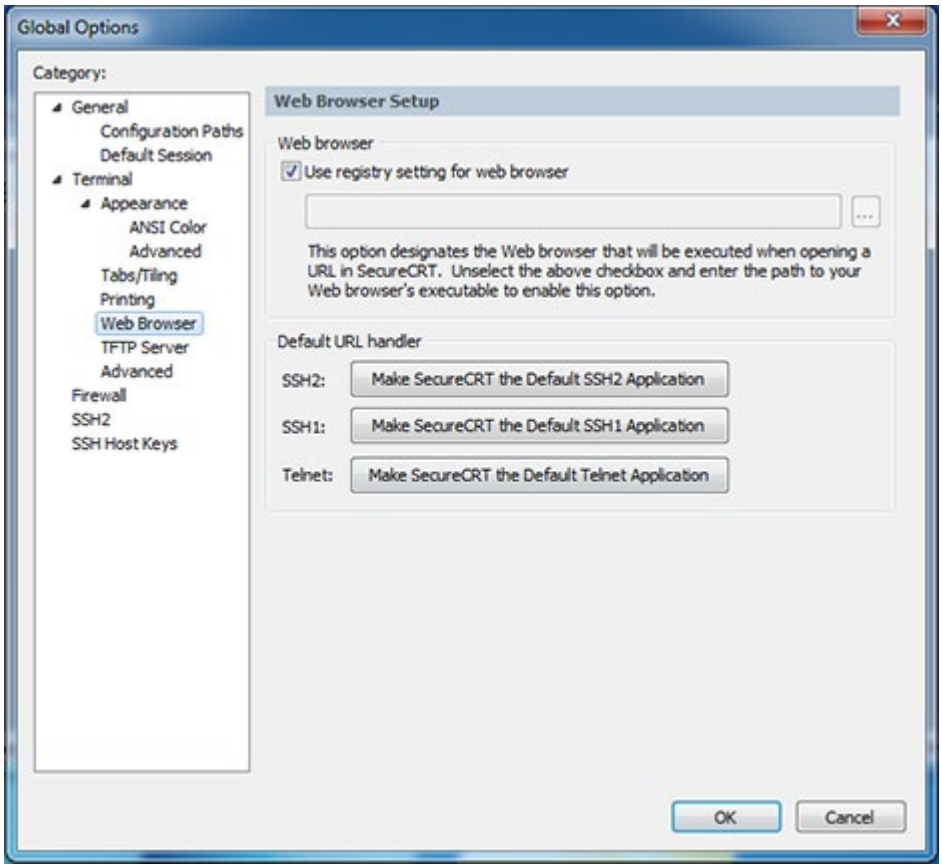
2. Open SecureCRT.



3. Close the Quick Connect Window. Click on the Options menu and select Global Options.



4. Click on Web Browser. Make sure “Use registry setting for web browser” is checked, and click **OK**. You can now open a Custom SSH session to a device from the Managed Devices Screen or in the Topology application.



Note: Your browser must be able to make SSH2 connections and SecureCRT must be set as your default SSH2 application to use the Custom SSH feature.

Discovery Displays

By default, a table containing all discovered device is displayed. You can also click on the Chart View icon to view graphical charts breaking down discovered device by device type, AOS version, and physical location.

Note: The information displayed in the list is updated based on the frequency settings configured on the Discovery Setting Frequencies Screen. You can perform an immediate poll on a device(s) to update information by selecting the device(s) in the list and clicking on the **Rediscover** button at the top of the screen.

Managed Devices List

The Managed Devices Screen displays basic information on all discovered network devices. There are two tabs in the table. "All" displays all discovered network devices. "OAW" displays only wireless devices. Click on a device to display detailed information for the device, including device modules (e.g., chassis, CMM, NI).

Note that if any devices in the Managed Devices List have unsaved configuration changes in their Working Directory, a number will appear in the Notification icon (Bell icon) at the top of the

screen. Click on the Notification Icon. The number of devices in this condition is displayed. Click on the Save Icon button to save changes to the Working Directories of the devices.

Basic Information

- **Friendly Name -** The Friendly name is derived from the Device Naming convention set in the Preferences application - Preferences - Device Naming (e.g., IP address, DNS Name).
- **Name -** The name of the device.
- **Version -** The version number of the device software (e.g., 8.5.255.R02). OmniVista may not be able to determine the software version on some third-party devices. In these cases, the field will be blank.
- **Thin Switch -** Indicates if the managed switch is running in Thin Switch Client mode. See Thin Switch Deployment for more information. Note that the switch reports its Thin Switch mode status in a periodic Call-Home to OmniVista every 30 minutes by default, so OmniVista will wait until the next Call-Home to update this field. If the switch doesn't Call-Home for any reason, this field may never get updated. The amount of time before the next periodic Call-Home from the switch to OmniVista is configurable through the Settings Screen. See the Settings Screen Online Help for more information.
  - **Yes -** Switch was provisioned to run in the Thin Switch Client mode. However, it does not necessarily mean that the switch is currently running in the Thin Switch Client mode. For example, if the Cloud Agent was disabled on the switch, OmniVista will still indicate "Yes" for Thin Switch Client mode but the switch will not be running in Thin Switch Client mode until the next switch reboot.
  - **No -** Switch is not running in the Thin Switch Client mode.
  - **No Applicable -** Switch is not eligible to be provisioned as a Thin Switch Client. *Note that only switches running AOS Release 8.8R1 (or higher) can be provisioned as Thin Switch Clients.*
- **Address -** The IP address of the device.
- **MAC Address -** The MAC address of the device.
- **Serial Number -** The serial number of the device.
- **Status -** The operational status of the device.
  - **AOS Devices**
    - **Up** - Device responds to SNMP requests or SSH/Telnet (as per Shell preference) ping request from OmniVista. "Up" Status does not necessarily mean that device is manageable from OmniVista. Refer to the "SNMP Status" column for management status.
    - **Warning** - There is one or more unacknowledged trap on the device.
    - **Down** - Device does not respond to SNMP Requests as well as Telnet/SSH ping requests from OmniVista.
  - **Stellar APs, OmniAccess WLAN Controller, OmniAccess WLAN IAP, OS 2220, and Third-Party Devices**
    - **Up** - AP is manageable from OmniVista.
    - **Warning** - There is one or more unacknowledged trap on the device.

    - **Down** - Device is not manageable from OmniVista. However, it may still be "Up" and functional on the network.
- **DNS Name -** The DNS name of the device.
- **Type -** The type of device chassis (e.g., OS6860E-24).
- **IoT Status -** Indicates if IoT is enabled or disabled (the default) for the device. When enabled, OmniVista collects IoT information for endpoints connected to the device. See Enabling/Disabling IoT.
- **Statistics Status -** Indicates if statistics collection is enabled or disabled for the device.
- **System Up Time -** The amount of time the device has been "Up" since the last reboot.
- **AP Group Name -** The name of the AP Group to which the Stellar AP Series Device belongs.
- **Data VLANs -** VLAN(s) used for traffic of client connected to the AP (q-tagged VLAN).
- **Management VLAN -** The VLAN used to connect to the AOS Switch (untagged VLAN).
- **SSIDs -** The SSIDs of the AP.
- **Reason Down -** The reason the device is down, if applicable. If the device is "Up", the field is blank. Note that if an AP goes down, the "Reason Down" field may not update to "Blank" when the AP returns to an "Up" state. For APs, ignore this field if the AP Status is "Up".
- **Location -** The physical location of the device (e.g., Test Lab).
- **System Contact -** Contact information for the person responsible for the device.
- **Activated Licenses -** The number of licenses used by the device.
- **FTP User Name -** The CLI/FTP user name for the device.
- **SNMP Status (AOS only) -** Displays "Up" if the device is manageable by OmniVista, "Down" if the device is not manageable by OmniVista. This attribute is supported on AOS devices only. Column will be blank or display "Non Applicable" for other device types.
- **SNMP Version -**The SNMP version used to discover the device (v1, v2, v3).
- **v1/2 Read Community -** The device's SNMP v1/2 "get" community name, if applicable.
- **v1/2 Write Community -** The device's SNMP v1/2 "set" community name, if applicable.
- **Last Known Up At -** The date and time when the last poll was initiated on the device.
- **v3 User Name -** The device's SNMP v3 user name, if applicable.
- **Last Upgrade Status -** The status of the last firmware upgrade on the device.
    - "Successful" - Successful BMF and Image upgrade performed.
    - "Successful (BMF)" - Successful BMF upgrade performed.
    - "Successful (Image)" - Successful Image upgrade is performed.
    - "Failed (BMF, Image)" - BMF and Image upgrade failed.

  - "Failed (BMF)" - BMF upgrade failed.
  - "Failed (Image)" - Image upgrade failed.
- **Backup Date -** The date that the device's configuration and/or image files were last backed-up to the OmniVista Server.
- **Backup Version -** The firmware version of the configuration and/or image files that were last backed-up to the OmniVista Server.
- **Description** - A description of the device, usually the vendor name and model.
- **Traps -** The status of trap configuration for the device. "On" means that traps are enabled. "Off" means that traps are disabled. "Not Configurable" means that traps for this device are not configurable from OmniVista. (Note that traps may have been configured for such devices outside of OmniVista.) "Unknown" means that OmniVista does not know the status of trap configuration on this device.
- **Running From -** For AOS devices, this field indicates whether the switch is running from the Certified directory or from the Working directory. This field is blank for all other devices. For AOS devices, the directory structure that stores the switch's image and configuration files in flash memory is divided into two parts:
  - The Certified directory contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory.
  - The Working directory contains files that may or may not have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes to the working directory. You cannot save configuration changes directly to the certified directory.

  Note that the files in the certified directory and in the working directory may be different from the running configuration of the switch, which is contained in RAM. The running configuration is the current operating parameters of the switch, which are originally loaded from the certified or working directory but may have been modified through CLI commands, WebView commands, or OmniVista. Modifications made to the running configuration must be saved to the working directory (or lost). The working directory can then be copied to the certified directory if and when desired.

  Note: OmniVista supports the Multiple Working Directories Feature available on OS10K and OS6900 Switches (AOS Release 7.2.1.R01 and later). This feature allows the user to create multiple Working Directories on the switch that can be used to save specific switch configurations. The user can create any name for these "Working" Directories (e.g., "Marketing Switch 05-23-15"). If the switch is running from one of these user-created directories, the directory name is displayed in this field.
- **Changes -** This field indicates the state of changes made to the switch's configuration. This field is blank for all other devices. This field can display the following values:
  - **Certified -** Changes have been saved to the working directory, and but the working directory has been copied to the certified directory. The working directory and the certified directory are thus identical.

  - **Uncertified -** Changes have been saved to the working directory, but the working directory has not been copied to the certified directory. The working directory and the certified directory are thus different.
  - **Unsaved -** Changes have been made to the running configuration of the device that have not been saved to the working directory. For Stellar APs, an unsaved configuration may not be an issue because when APs reboot, they always receive and build their configuration from OmniVista. Saving the configuration on Stellar APs is helpful if an AP reboots and OmniVista is not reachable. In this case, APs use the previously saved configuration.
  - **Blank -** When this field is blank, the implication is that OmniVista knows of no unsaved configuration changes and assumes that the working and certified directories in flash memory are identical.
- **Discovered -** The date and time when OmniVista successfully pings or polls the switch for the first time. This value remains unchanged until the switch entry is deleted. This field will remain blank if OmniVista does not ping or poll the switch at all.
- **No. of Licenses Used -** The total number of Core (AOS), Stellar AP Series Devices, or Third-Party licenses being used. For example, a single AOS device requires one license. A stack of 4 switches requires 4 licenses, a VC of 6 requires 6 licenses. If a stack splits, the number of licenses reserved for the device before the split is maintained even though modules have been reduced to less than 5. This way, the license counts are reserved for the stack to recover.
- **License Type -** The type of license used by the device (e.g., ALE, Third-Party, ALE Access Point).
- **Synchronized Status -** Whether the Primary CMM's working directory is identical to the working directory on the other CMM module (if present).
  - **Synchronized -** The primary CMM's working directory is identical to the working directory on the secondary CMM. Note that if a switch is in Virtual Chassis (VC) mode, and it is VC of 1, the Synchronized Status is always "Synchronized".
  - **Not Synchronized -** The primary CMM's working directory is not identical to the working directory on the secondary CMM.
  - **Not Applicable -** Only one CMM module is installed.
  - **Unknown -** The synchronization state is unknown.
- **Upgrade Schedule -**The name of the Scheduled Upgrade to which the device is assigned, if applicable. "Not Scheduled" means the device has not been assigned to a Scheduled Upgrade.
- **NaaS/CAPEX Device -** The Device License mode of operation for the switch (NaaS, CAPEX, CAPEX Undecided). See NaaS Device Licenses for more information. Note that NaaS device licensing is supported only on switches running AOS Release 8.8R1 or higher.
- **IoT VRF** - The VRF ID of the IoT-enabled device.
- **OmniVista Network Advisor** - Indicates whether or not OmniVista Network Advisor is monitoring the device (Enable/Disable).
- **OmniVista Network Advisor Instance** - Tthe URL of the OmniVista Network Advisor instance that is monitoring the device. This field is blank if OmniVista Network Advisor monitoring is disabled.
-

Detailed Information

Basic Information

- **Name -** The Friendly name of the device. The Friendly name is derived from the Device Naming convention set in the Preferences application - Preferences - Device Naming (e.g., IP address, DNS Name).
- **Address -** The IP address of the device.
- **MAC Address -** The MAC address of the device.
- **Serial Number -** The serial number of the device.
- **Status-** The operational status of the device.
    - **AOS Devices**
        - **Up -** Device responds to SNMP requests or SSH/Telnet (as per Shell preference) ping request from OmniVista. "Up" Status does not necessarily mean that device is manageable from OmniVista. Refer to the "SNMP Status" column for management status.
        - **Warning -** There is one or more unacknowledged trap on the device.
        - **Down -** Device does not respond to SNMP Requests as well as Telnet/SSH ping requests from OmniVista.
    - **Stellar APs**, **OmniAccess WLAN Controller, OmniAccess WLAN IAP, OS 2220, and Third-Party Devices**
        - **Up -** AP is manageable from OmniVista.
        - **Warning -** There is one or more unacknowledged trap on the device.
        - **Down -** Device is not manageable from OmniVista. However, it may still be "Up" and functional on the network.
- **DNS Name -** The DNS name of the device.
- **Type -** The type of device chassis (e.g., OS6860E-24).
- **Version -** The version number of the device software (e.g., 8.5.255.R02). OmniVista may not be able to determine the software version on some third-party devices. In these cases, the field will be blank.
- **Location -** The physical location of the device (e.g. Test Lab).
- **Description** - A description of the device, usually the vendor name and model.
- **System Contact -** Contact information for the person responsible for the device.

License Information

- **No. of Licenses Used -** The total number of Core (ALE) or Third-Party licenses being used. For example, a stack of 4 switches would require 4 licenses, a VC of 6 would require 6 licenses. If a stack splits, the number of licenses reserved for the device before the split is maintained even though modules have been reduced to less than 5. This way, the license counts are reserved for the stack to recover.
- **License Type -** The type of license used by the device (e.g., ALE, Third-Party, ALE Access Point). **Activated Licenses -** The number of licenses used by the device.
- **Activated Licenses -** The number of licenses used by the device.
- **NaaS/CAPEX Device -** The Device License mode of operation for the switch (NaaS, CAPEX, CAPEX Undecided). See NaaS Device Licenses for more information. Note that NaaS device licensing is supported only on switches running AOS Release 8.8R1 or higher.

Status Information

- **Traps -** The status of trap configuration for the device. "On" means that traps are enabled. "Off" means that traps are disabled. "Not Configurable" means that traps for this device are not configurable from OmniVista. (Note that traps may have been configured for such devices outside of OmniVista.) "Unknown" means that OmniVista does not know the status of trap configuration on this device.
- **Running From -** For AOS devices, this field indicates whether the switch is running from the Certified directory or from the Working directory. This field is blank for all other devices.
- **Changes -** This field indicates the state of changes made to the switch's configuration. This field is blank for all other devices. This field can display the following values:
  - **Certified -** Changes have been saved to the working directory, and but the working directory has been copied to the certified directory. The working directory and the certified directory are thus identical.
  - **Uncertified -** Changes have been saved to the working directory, but the working directory has not been copied to the certified directory. The working directory and the certified directory are thus different.
  - **Unsaved -** Changes have been made to the running configuration of the device that have not been saved to the working directory. For Stellar APs, an unsaved configuration may not be an issue because when APs reboot, they always receive and build their configuration from OmniVista. Saving the configuration on Stellar APs is helpful if an AP reboots and OmniVista is not reachable. In this case, APs use the previously saved configuration.
  - **Blank -** When this field is blank, the implication is that OmniVista knows of no unsaved configuration changes and assumes that the working and certified directories in flash memory are identical.
- **Last Upgrade Status -** The status of the last firmware upgrade on the device.
  - "Successful" - Successful BMF and Image upgrade performed.
  - "Successful (BMF)" - Successful BMF upgrade performed.
  - "Successful (Image)" - Successful Image upgrade is performed.
  - "Failed (BMF, Image)" - BMF and Image upgrade failed.
  - "Failed (BMF)" - BMF upgrade failed.
  - "Failed (Image)" - Image upgrade failed.
- **Synchronized Status -** Whether the Primary CMM's working directory is identical to the working directory on the other CMM module (if present).
  - **Synchronized -** The primary CMM's working directory is identical to the working directory on the secondary CMM. Note that if a switch is in Virtual Chassis (VC) mode, and it is VC of 1, the Synchronized Status is always "Synchronized".
  - **Not Synchronized -** The primary CMM's working directory is not identical to the working directory on the secondary CMM.
  - **Not Applicable -** Only one CMM module is installed.
  - **Unknown -** The synchronization state is unknown.

Note: If a switch is in Virtual Chassis (VC) mode, and it is VC of 1, the Synchronized Status is always "Synchronized".

- **SNMP Status -** Displays "Up" if the device is manageable by OmniVista.
- **IoT Status** - Indicates if IoT is enabled or disabled (the default) for the device. When enabled, OmniVista collects IoT information for endpoints connected to the device.
- **Statistics Status** - The status of statistics collection for the device (Enable/Disable).
- **OmniVista Network Advisor** - The status of OmniVista Network Advisor monitoring for the device (Enable/Disable).
- **OmniVista Network Advisor Instance** - The URL of the OmniVista Network Advisor instance that is monitoring the device. This field is blank if OmniVista Network Advisor monitoring is disabled.

Security Information

- **FTP User Name -** The user name that OmniVista will use to establish CLI/FTP sessions with the discovered devices. The user name specified will be used to auto-login to devices when CLI sessions are established. It will also be used to perform FTP with the device when configuration files are saved and restored.
- **SNMP Version -** The SNMP version that OmniVista will use to communicate with the device. The default version for AOS devices is v2, but v1 and v3 are also supported.
- **Read Community** - The device's "get" community name. The "get" community name enables OmniVista to read information from the device.
- **Write Community -** The device's "set" community name. The "set" community name enables OmniVista to write information to the device.

Other Information

- **Backup Date -** The date that the device's configuration and/or image files were last backed-up to the OmniVista Server.
- **Backup Version -** The firmware version of the configuration and/or image files that were last backed up to the OmniVista Server.
- **Last Known Up At -** The date and time when the last poll was initiated on the device.
- **Discovered -** The date and time when OmniVista successfully pings or polls the switch for the first time. This value remains unchanged until the switch entry is deleted. This field will remain blank if OmniVista does not ping or poll the switch at all.
- **System Up Time -** The amount of time the device has been "Up" since the last reboot.
- **Reason Down -** The reason the device is down, if applicable. If the device is "Up", the field is blank. Note that if an AP goes down, the "Reason Down" field may not update to "Blank" when the AP returns to an "Up" state. For APs, ignore this field if the AP Status is "Up".
- **Thin Switch -** Indicates if the managed switch is a running in Thin Switch Client mode. See Thin Switch Deployment for more information. Note that the switch reports its Thin Switch mode status in a periodic Call-Home to OmniVista every 30 minutes by default, so OmniVista will wait until the next Call-Home to update this

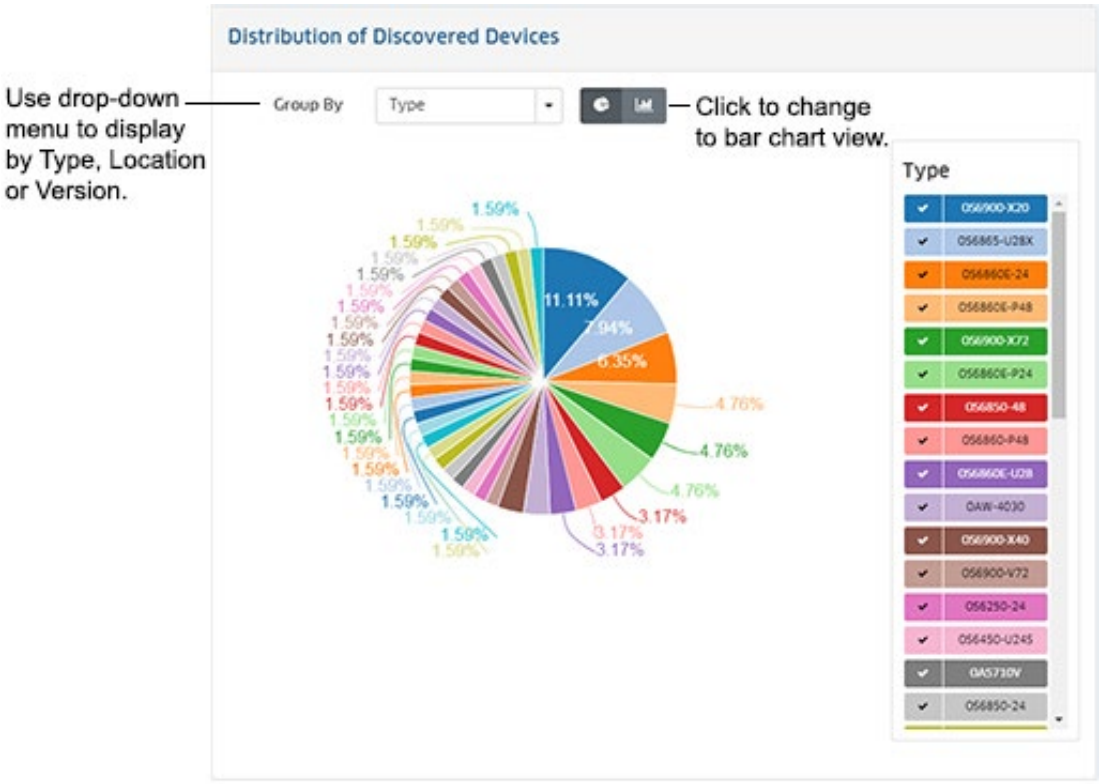
field. If the switch doesn't Call-Home for any reason, this field may never get updated. The amount of time before the next periodic Call-Home from the switch to OmniVista is configurable through the Settings Screen. See the Settings Screen Online Help for more information.

- **Yes -** Switch is running in the Thin Switch Client mode. However, it does not necessarily mean that the switch is currently running in the Thin Switch Client mode. For example, if the Cloud Agent was disabled on the switch, OmniVista will still indicate "Yes" for Thin Switch Client mode but the switch will not be running in Thin Switch Client mode until the next switch reboot.
- **No -** Switch is not running in the Thin Switch Client mode.
- **No Applicable -** Switch is not eligible to be provisioned as a Thin Switch Client. *Note that only switches running AOS Release 8.8R1 (and higher) can be provisioned as Thin Switch Clients.*

Graphical Views

For a graphical view of discovered devices grouped by category, click on the Chart View icon at the top of the screen. By default, the pie chart view is shown, with the inventory information displayed by type. Click on the bar chart option to view the information in bar chart format. Hover the mouse over a section for the number of devices in the category. Change the view using the **Group by** drop-down menu:

- **Type -** Group discovered devices by device type (e.g., OS6860-48, Aruba AP).
- **Location -** Group discovered devices by physical location listed for the device (e.g., NMS Lab, SQA Lab).
- **Version -** Group discovered devices by software version running on the device (e.g., 6.4.3.575.R01, 1.7.1.10).



Discovery Profiles

The Discovery Profiles Screen displays all configured Discovery Profiles and is used to create, edit, and delete profiles. A Discovery Profile is used when discovering network devices. A Discovery Profile contains the parameters that are used by OmniVista when performing a discovery (e.g., SNMP version used to discover devices, CLI/FTP passwords needed to connect to a device).

Creating a Discovery Profile

Click on the Add icon to bring up the Create Discovery Profile Screen. Complete the fields in each section as described below, then click on the **Create** button.

General

- **Name -** The profile name.
- **CLI/FTP User Name -** The CLI Scripting (Telnet)/FTP user name that OmniVista will use to establish CLI Scripting and FTP sessions with the discovered devices.
- **CLI/FTP Password -** The CLI scripting (Telnet)/FTP user name that OmniVista will use to establish CLI Scripting and FTP sessions with the discovered devices. Note that the user name and password specified will be used to auto-login to devices when CLI Scripting sessions are established. They will also be used to perform FTP with the device when configuration files are saved and restored.
- **Confirm CLI/FTP Password -** Re-enter the CLI/FTP Password.
- **Secondary Password -** Optional Secondary Password used to connect to devices. **Confirm Secondary Password -** Re-enter the Secondary Password.

Note: If you do **not** define the CLI/FTP username and password, and you attempt to save, restore, or upgrade configuration files for AOS devices, you will be individually queried for the FTP login name and password of each individual switch for which configuration files are being saved, restored, or upgraded. In addition, OmniVista will be unable to auto-login to the device when establishing CLI Scripting sessions.

SNMP

- **SNMP Version -** The SNMP version used to discover devices (v1, v2, v3). (Default = v2) **Timeout -** The time period, in milliseconds, that OmniVista will wait for a switch to respond to a connection request before assuming that the request has timed-out.
- **Read Community (v1 and v2 only) -** The Read Community Name, which is used to read information from a device.
- **Write Community (v1 and v2 only) -** The Write Community Name, which is used to write information to a device.
- **Retry Count -** The number of times OmniVista will attempt to attempt to connect to a switch.
- **User Name (v3 only) -** The SNMP version 3 user name.
- **Auth & Priv Protocol (v3 only) -** Select the authentication protocol OmniVista will use for SNMP communications with the discovered switches (None, MD5, or SHA).

- **Auth Password (v3 only) -** The password that OmniVista will use for the MD5 or SHA authentication protocol (if applicable).
- **Confirm Auth Password (v3 only) -** Confirm the authentication password entered above.
- **Priv Password (v3 only) -** The password that will be used as the secret key (if applicable).
- **Confirm Priv Password (v3 only) -** Confirm the privilege password entered above.
- **Context Name (v3 only) -** The unique context name for this context. (An SNMP context is a collection of management information accessible by an SNMP entity, in this case OmniVista.)
- **Context ID (v3 only) -** The unique context ID for this context. Each context must be identified by a unique context name and a unique context ID.

Note: If a device's Read and Write Community Names are "public" (Default), you can leave these fields blank (OmniVista uses the default name, "public" when the field is blank.) Read and Write Community Names are not configurable from OmniVista; they can only be configured by logging onto a device. Also note that when you use SNMP v3, Read and Write Community Names are ignored.

Advanced Settings

- **Trap Station User Name -** The device username that will be used when an AOS device is configured to send traps to OmniVista. AOS devices require that a valid device username be specified with the trap station configuration entry. If this field is left blank, the following switch usernames will be used by default for trap station configuration entries:
- If OmniVista is configured to use SNMP version 3 with this device, the SNMP version 3 user name entered for the device will be used as the switch user name in the trap station configuration entry.
- If OmniVista is configured to use SNMP version 1 or SNMP version 2 with this device, the read community string for the device will be used as the switch user name in the trap station configuration entry.
- **Discover Link -** Specifies how OmniVista will discover the physical links associated with the discovered devices. Links to other switches are displayed graphically on OmniVista's Topology maps.

  Normally - This setting is used for devices that support adjacency protocols, such as AOS devices. Adjacency protocols (such as XMAP and AMAP) enable OmniVista to discover the physical links associated with specific devices.

  ~~**As OEM Device** - This setting enables you to use the new "end station search" functionality from the Locator application to automatically discover links for devices that do not support adjacency protocols. If this setting is used and the device does not support an adjacency protocol that enables OmniVista to discover physical links, the end station search algorithms used by the Locator application are invoked at each polling cycle to discover the device's links. All links discovered are displayed on Topology maps automatically.~~
- **Shell Preference -** Specifies the default command line interface to be used for discovered devices. OmniVista's CLI Scripting application supports both the Telnet and SSH command line interfaces. SSH (Secure Shell) is a Telnet-like utility that

provides encryption and is far more secure than Telnet. When the SSH setting is used, SSH will be used as the default command line interface for the device. If the Telnet setting is used, Telnet will be used as the default command line interface for the device (Default = SSH). Ensure that devices are capable of SSH before you use the SSH setting. OmniVista does not verify the SSH capabilities of a device. All AOS devices are SSH-capable. (Default = SSH)

- **Use Get Bulk -** Enables (Yes)/Disables (No) the "Get Bulk' operation. When enabled, the "Get Bulk" operation is used for retrieving large amounts of data, particularly from large tables. The Get Bulk operation performs continuous "Get Next" operations, each time requesting the number of table rows specified by the value in the **Max Repetitions** field (described below). For example, if the value in the **Max Repetitions** field is ten, each Get Next operation will request 10 rows of table data. Note that the number of rows of data actually returned by the switch will be determined by the amount of memory the switch has available at that time.
- **Max Repetitions -** The number of rows of table data that the "Get Bulk" operation will request in each "Get Next" operation.

Editing a Discovery Profile

Select a profile from the Existing Profiles Table and click on the Edit icon. Update any fields as described above and click on the **Update** button. Note that you cannot edit a profile name.

Deleting a Discovery Profile

Select a profile(s) from the Existing Profiles Table, click on the Delete icon, then click **OK** at the confirmation prompt.

Profile Information

Basic Discovery Profile information is displayed in the Existing Profiles Table. Click on a profile to display detailed information.

Basic Information

- **Name -** The profile name.
- **SNMP Version -** The SNMP version used to discover devices (v1, v2, v3). (Default = v2)
- **v1/2 Read Community -** The SNMP v1/v2 Read Community Name, which is used to read information from a device, if applicable.
- **v1/2 Write Community -** The SNMP v1/v2 Write Community Name, which is used to write information to a device, if applicable.
- **v3 User Name -** The SNMP v3 user name, if applicable.

Detailed Information

- **Name -** The profile name.
- **CLI/FTP User Name -** The CLI Scripting (Telnet)/FTP user name that OmniVista will use to establish CLI Scripting and FTP sessions with the discovered devices.
- **SNMP Version -** The SNMP version used to discover devices (v1, v2, v3). (Default = v2)

- **Timeout -** The time period, in milliseconds, that OmniVista will wait for a switch to respond to a connection request before assuming that the request has timed-out.
- **Read Community (v1 and v2 only) -** The Read Community Name, which is used to read information from a device.
- **Write Community (v1 and v2 only) -** The Write Community Name, which is used to write information to a device.
- **Retry Count -** The number of times OmniVista will attempt to attempt to connect to a switch.
- **User Name (v3 only) -** The SNMP version 3 user name.
- **Auth & Priv Protocol (v3 only) -** The authentication protocol OmniVista will use for SNMP communications with the discovered switches (None, MD5, or SHA).
- **Auth Password (v3 only) -** The password that OmniVista will use for the MD5 or SHA authentication protocol (if applicable).
- **Confirm Auth Password (v3 only) -** Confirm the authentication password entered above.
- **Context Name (v3 only) -** The unique context name for this context. (An SNMP context is a collection of management information accessible by an SNMP entity, in this case OmniVista.)
- **Context ID (v3 only) -** The unique context ID for this context. Each context must be identified by a unique context name and a unique context ID.
- **Trap Station User Name -** The device user name that will be used when an AOS device is configured to send traps to OmniVista. AOS devices require that a valid device user name be specified with the trap station configuration entry. If this field is left blank, the following switch user names will be used by default for trap station configuration entries:
    - If OmniVista is configured to use SNMP version 3 with this device, the SNMP version 3 user name entered for the device will be used as the switch user name in the trap station configuration entry.
    - If OmniVista is configured to use SNMP version 1 or SNMP version 2 with this device, the read community string for the device will be used as the switch user name in the trap station configuration entry.
- **Discover Link -** Specifies how OmniVista will discover the physical links associated with the discovered devices. Links to other switches are displayed graphically on OmniVista's Topology maps:
    - **Normally -** This setting is used for devices that support adjacency protocols, such as AOS devices. Adjacency protocols (such as XMAP and AMAP) enable OmniVista to discover the physical links associated with specific devices.
    - ~~**As OEM Device** - This setting enables you to use the new "end station search" functionality from the Locator application to automatically discover links for devices that do not support adjacency protocols. If this setting is used and the device does not support an adjacency protocol that enables OmniVista to discover physical links, the end station search algorithms used by the Locator application are invoked at each polling cycle to discover the device's links. All links discovered are displayed on Topology maps automatically.~~

- **Shell Preference -** Specifies the default command line interface used for discovered devices. OmniVista's CLI Scripting application supports both the Telnet and SSH command line interfaces. SSH (Secure Shell) is a Telnet-like utility that provides encryption and is far more secure than Telnet. When the SSH setting is used, SSH will be used as the default command line interface for the device. If the Telnet setting is used, Telnet will be used as the default command line interface for the device. (Default = SSH)
- **Use Get Bulk -** Enables (Yes)/Disables (No) the "Get Bulk' operation. When enabled, the "Get Bulk" operation is used for retrieving large amounts of data, particularly from large tables. The Get Bulk operation performs continuous "Get Next" operations, each time requesting the number of table rows specified by the value in the **Max Repetitions** field (described below). For example, if the value in the **Max Repetitions** field is ten, each Get Next operation will request 10 rows of table data. Note that the number of rows of data actually returned by the switch will be determined by the amount of memory the switch has available at that time.
- **Max Repetitions -** The number of rows of table data that the "Get Bulk" operation will request in each "Get Next" operation.

NaaS Device Licenses

The Discovery NaaS Device Licenses Screen displays the Device Licensing information for discovered switches running AOS Release 8.8R1 or higher. Use this screen to determine and monitor the status of the Device License for each device.

Licensed Device List

A device interacts with a designated License Activation Server to obtain a Device License (NaaS, CAPEX, or CAPEX Undecided). OmniVista obtains the Device License information by polling devices via SNMP at regular intervals or when a device is rediscovered. The following Device License information is then displayed for each discovered licensed device on the NaaS Device Licenses screen:

- **Name -** The name of the device.
- **IP Address -** The IP address of the device.
- **MAC Address -** The MAC address of the device.
- **Version -** The version number of the device software (e.g., 8.8.128.R01). If OmniVista is not be able to determine the software version, the field will be blank.
- **AP Group -** The name of the AP Group to which the Stellar AP Series Device belongs. Note that NaaS Device Licensing is currently not supported by Stellar APs.
- **Role -** In a Virtual Chassis (VC) configuration, the switch is running as a master or slave of the VC.
- **NaaS/CAPEX Device -** The Device License mode of operation for the switch.
  - **NaaS -** The switch is a licensed device that participates in the NaaS subscription-based model.
  - **CAPEX -** The switch does not participate in the NaaS subscription-based model.
  - **CAPEX Undecided** - The switch has not yet obtained a license.
- **Serial Number -** The serial number of the device.
- **VC Name -** The serial number of the master switch in a VC configuration.
- **Management Feature on Device -** The status of the Management Feature License (Licensed, Not Licensed, Grace Period, or Expired). This feature license allows

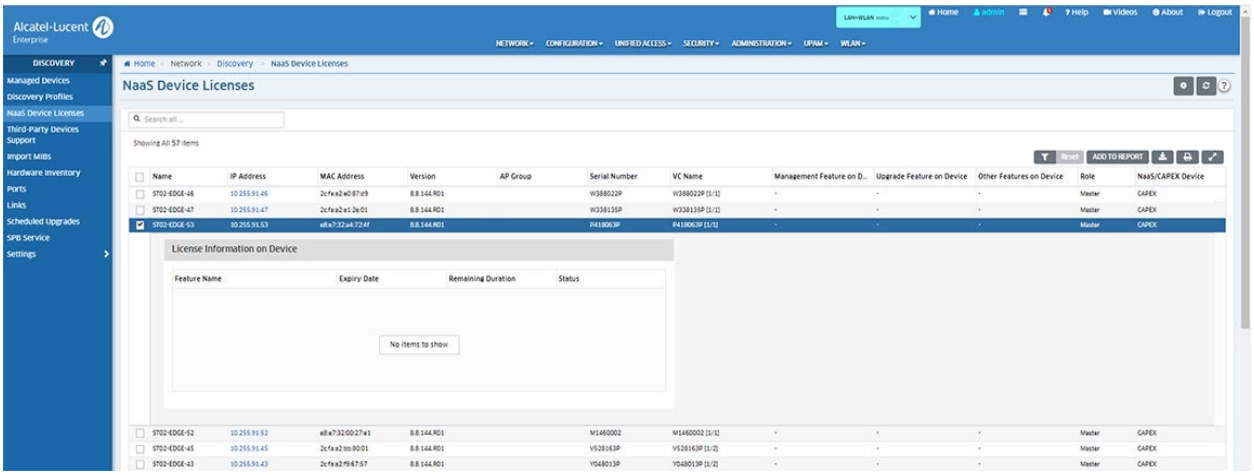
management capabilities on the switch. Note that when this license expires and the device enters a Grace Period, a configuration change can be applied to the switch. However, after the Grace Period ends, the device goes into a degraded mode during which a configuration change is not allowed.

- **Upgrade Feature on Device -** The status of the Upgrade Feature License (Licensed, Not Licensed, or Expired). This feature allows software upgrades on the switch. If this license is "Expired", OmniVista will not include this device as an available device to select for an upgrade. There is no Grace Period triggered when this feature license expires.
- **Other Features on Device -** The status of all other licensed features (Licensed, Not Licensed, Grace Period, or Expired), except the Management and Upgrade licensed features. Click on a device entry to display the licensing details for the additional features.

Note: If the device is reported as a CAPEX or CAPEX UNDECIDED device, the "Management Feature on Device", "Upgrade Feature on Device", and "Other Features on Device" fields will be blank.

Device License Details

If a device is licensed for features other than the Management or Upgrade features, the following information is displayed for each additional licensed feature when you click on a device entry in the NaaS Device Licenses list:



- **Feature Name -** The name of the feature licensed for the device.
  - **Essentials -** The default license for the switch that licenses the use of basic features.
  - **Advanced -** The basic features license plus the Data Center and 10G feature licenses.
- **Expiry date -** The date on which the feature license expires.
- **Remaining duration -** The remaining amount of time for the Grace Period.
- **Status -** The status of the feature license (Licensed, Not Licensed, Grace Period, or Expired).

Note: The "Other Features on Device" field value may represent the status of multiple feature licenses on the device. This field will display the status of the feature with the least amount of time. For example, if there is more than one feature on the device and one of the features has an expired license, then "Expired" is displayed for this field value, even if the other feature licenses have not expired. If none of the feature licenses are expired and more than one of the features is in the Grace Period, then the status with the lowest amount of time remaining in the Grace Period is displayed.

Device License Status

- **Licensed -** The feature is licensed for the device and the license expires on the given date. For example, "Licensed (until Jan 20, 2022)".
- **Not Licnsed –** The feature is not licensed for the device.
- **In Grace Period -** The NaaS license expired and is in a 30-day grace period that ends on the given date (e.g., "In Grace Period (until Feb 20, 2022"). When the grace period ends, the license goes into a "degraded" mode. Note that the end of the grace period is calculated based on the number of days the device is active. If the NaaS license expires and the device is not active, the grace period will not start until the device is active again. For example, if a device is inactive after the license expires and then goes active after 15 days, the 30-day grace period starts after the 15 days and ends 45 calendar days after the license expires.
- **Expired -** The NaaS device license has expired. Note that when the Management License expires, the management of all features goes into a grace period followed by a degraded mode. During the grace period, the switch can be managed but not upgraded. At the end of grace period, the switch goes into a degraded mode where the switch cannot be managed for the features and the system cannot be upgraded. When the Upgrade License expires, the switch will go into the degraded mode immediately (no grace period).

Note: To check the Device License status on a supported AOS switch, use the **show naas license** CLI command.

Third-Party Devices Support

The Discovery Third-Party Devices Support Screen is used to enable discovery and support of third-party devices. The Third-Party Devices Support Screen enables you to add support for third-party devices, edit third-party device support, delete support for unwanted third-party devices. The Mibset List displays all configured third-party device support information.

> **Note:** Support for Cisco and Extreme devices must be added manually as described below.

Adding Third-Party Device Support

To add support for a third-party device, click on the Add icon and complete the fields as described below. When you have completed the fields, click on the **Create** button. The entry will appear in the Mibset List.

- **IOD -** The device's Object ID. Enter only the portion of the OID relative to the ".1.3.6.1.4.1." (".iso.org.dod.internet.private.enterprises") branch. For example, enter only '9' for Cisco devices rather than '.1.3.6.1.4.1.9', or '1916' for Extreme devices,

rather than '.1.3.6.1.4.1.1916". Using this vendor value (e.g., 9, 1916) will enable OmniVista to recognize all devices from the vendor. Note that you can also enter specific vendor device values (e.g., '1916.800.1.1.2.1.5.1') for each vendor device if you want each device to have a different name while using the same mibset.

- **Display Name -** The name to be used for the device.
- **MIB Directory Name -** The directory name of the device's MIB. If you want to use MIB-2 level support for third-party devices, enter **mib-2**. This generic MIB-2 directory already exists in OmniVista. If you are not using standard MIB-2, enter a new directory name for the MIB. Note that the directory does not have to actually exist; it will be created automatically when you import the MIB.
- **Enabled -** Select **On** or **Off** to enable (On) or disable (Off) discovery for the device.
- **Icon -** The generic third-party icon appears in the Icon field. If you have an icon you would like to display for the device, click on the **Choose Image** button and locate the image. The image will appear in the Icon field.

Traps for Third-Party Devices

By default, OmniVista supports generic MIB-2 traps for third-party devices. If you import a new, custom MIB for a third-party device, OmniVista will automatically scan the MIB for new traps and integrate any traps it finds. Note that MIBs do not include synopses for traps. OmniVista will create a synopsis "on the fly" for any new trap it integrates. You can go to the Trap Definition Screen in the Notifications application and edit the synopses or severity levels that OmniVista assigns to new traps.

Third-Party Device Support After Discovery

Once third-party devices have been discovered, OmniVista supports the following functionality for the devices:

- **Web Browser -** OmniVista enables you to launch web-based element managers for third-party devices using the "Webpage" operation in the Topology application.
- **Telnet or SSH (as applicable) -** OmniVista enables you to initiate Telnet or SSH sessions to third-party devices using the Terminal Screen in the CLI Scripting application.
- **Custom MIBs -** OmniVista allows you to import custom MIBs for third-party devices (as described above).
- **Custom Icons -** OmniVista enables you to import a custom icon that will be used to represent a specific third-party device.
- **Traps -** By default, OmniVista supports generic MIB-2 traps for third-party devices. In addition, whenever you import a new, custom MIB for a third-party device, OmniVista will scan the MIB for new traps and automatically integrate any traps it finds.
- **Locator -** OmniVista's Locator application supports third-party devices.

Editing Third-Party Device Support

Select an entry in the Mibset List and click on the Edit icon. Edit the fields as described above, then click on the **Update** button. Note that you cannot edit the OID or Display Name.

Deleting Third-Party Device Support

Select an entry in the Mibset List and click on the Delete icon. Click **OK** at the confirmation prompt.

Mibset List

The Mibset List displays information about configured third-party device support.

- **OID -** The device's Object ID.
- **Display Name -** The name that is used for the device.
- **MIB Directory Name -** The directory that contains the device's MIB.
- **Enabled -** "True" (enabled) indicates that the device is included in the discovery process. "False" (disabled) indicates that the device is not included in the discovery process.

Import MIBs

The Discovery Import MIBs Screen is used to import new or updated MIB files into OmniVista. All MIB files are imported to the OmniVista Server. Before you import MIBs, it is important to understand that the purpose of this function is to import MIB files that reside somewhere on your local file system into OmniVista. A mibs.txt ASCII file lists the order in which the MIBs will be compiled. Also:

- All MIB files that you import must have a file extension of **.mib**.
- If you create a new MIB directory for a new device, note that you must import a complete set of MIBs into that directory. This means that if any proprietary MIBs you are using have imports of standard MIBs, the standard MIBs must be included and imported into that directory as well.
- For the MIBs to compile correctly, you are strongly advised to order them so that all the referenced MIB files are compiled before the files that reference them. MIB compilers follow import references from one MIB to another on the fly, and do not strictly require that the MIBs be compiled in any particular order. For this to work successfully, however, the MIB filenames must match the import statements exactly, and unfortunately this is almost never the case. To avoid these problems, as stated above, order the MIB files so that all the referenced MIB files are compiled before the files that reference them. You can specify the order in which the MIB files will be compiled by selecting files and using the **Up** and **Down** arrows in the Import Files to Mibset Screen, as described in the procedure below. MIB files will be compiled in the order that the files are listed in the Import Files to Mibset Screen.
- It is not advisable to add new MIB files to a MIB directory supplied by default with OmniVista. It is preferable to create a separate new directory for each new third-party device you want to support.
- Once you have completed the MIB importation process, OmniVista does not immediately parse the MIBs. When you discover a device with an OID that is specified for the MIB directory into which you imported the new MIBs, OmniVista will poll the device for standard MIB-II objects. If the standard MIB-II MIBs are not included in the directory, error messages will be written to file server.txt (which can be viewed from the Audit application). Any proprietary MIBs that you imported into the directory will not be parsed until you load the MIB Browser for a device with an

OID that is specified for that directory. However, if you close the OmniVista client and completely stop the OmniVista server after completing the MIB importation process, then start the server, the MIBs will be parsed when the server starts.

Importing MIBs

Follow the steps below to import MIB files into OmniVista.

1. Select the **Mibset to be updated** from the drop-down box at the top of the screen (e.g., Cisco). If you entered a new directory name in the Third-Party Device Support Screen, the name will be displayed in the drop-down menu.
2. Click on the **Import** button, then click on the **Upload Files** button.
3. Browse to the folder containing the MIBs you want to import, select all of the files and click **Open**. The files will appear in the imported into the Import Files to Mibset Screen.

   Note: If you are using Chrome, you will have the option of selecting an **Upload Folder** button in Step 2. Select the folder containing the MIB Files to import all of the files in the folder. This option is not supported in Firefox or Internet Explorer.
4. The MIB files will be loaded into OmniVista in the correct order. However, you can adjust this order by selecting individual files and clicking the **Up** and **Down** arrows in the upper-right corner of the screen.
5. Click the **Apply** button. The MIB files are imported to the OmniVista Server.

Hardware Inventory

The Discovery Hardware Inventory Screen is used to view inventory information (e.g., CMM, Chassis, Power Supplies) for any discovered device. To view information for a device(s), select an option from the drop-down menu (Use Switch Picker/Use Topology App), click on the **Select Device** button and select a device(s). You can select up to 512 devices at a time. Click on a device in the table for more detailed information.

Asset Information

- **Friendly Name -** A user-definable name for the device. If no name was configured, the IP address of the device is displayed.
- **Module Type -** The physical type of module or submodule in this physical location (e.g., Chassis, NI). Note that the value for this field displays as "Unknown" for a brief period while a newly-installed module or submodule is identified.
- **Module Name -** The manufacturer's name for the module (e.g. OS6850--C48, OS6850-BPS-PS).
- **Description -** The user-definable description of this particular module or submodule. The module description can be defined through SNMP.
- **Serial Number -** The serial number of the module or sub-module.
- **Number of Clients -** The number of clients currently connected to the Stellar AP Series Device.
- **Part Number -** The part number of the module or sub-module.
- **MAC Address -** The base MAC address for the module or submodule. If not applicable, the field will be blank.
- **OS Version -** The OS version number running on the module. If not applicable, the field will be blank.

- **Uboot Version -** The U-Boot version running on the module. If not applicable, the field will be blank.
- **HW Revision -** The hardware revision number for the module. If not applicable, the field will be blank.
- **Firmware Version -** The version/revision level of the module or submodule firmware. If not applicable (e.g., Power Supply), the field will be blank or displays “0.0”.
- **Manufacturer Name -** The manufacturer of the module.
- **License -** Additional licenses (other than the Core License) active on the module (e.g., Advanced), if applicable.
- **Slot -** The slot in the chassis where the module resides. If not applicable, the field will be blank.

Ports

The Discovery Ports Screen is used to display information about ports on network devices, and is also used to enable/disable device ports. Click on the **Select Devices** button and use the Switch Picker or Topology option to select the devices you want to view. You can select up to 50 devices at a time. You can also enable/disable ports by selecting the port(s) and click on the **Enable** or Disable **button** at the top of the screen.

Port Information

- **Friendly Name -** Displays the device label as configured in the Preferences application (e.g., device IP address, System name, DNS name).
- **IP Address -** The IP address of the device on which the port resides.
- **Name -**The user-defined name for the device.
- **Slot/Port -** The slot/port number on the device.
- **Port Alias -** The user-defined alias for the port.
- **Port Description -** A detailed description of the interface (e.g., Alcatel-Lucent OS6900 QNI 1/1A)
- **Admin Status -** The administrative status of the port (Up/Down). When the admin status of a port is "Up", the port can receive and transmit data as long as a cable is connected and no physical or operational problems exist. When the admin status of a port is "Down", the port will not transmit or receive data even if a cable is connected and the physical connection is operational. Note that physical or operational problems may cause a port to be nonfunctional even when its admin status is enabled.
- **Operational Status -** The operational status of the port (Up/Down/Unknown). If the operational status of a port is "Up", the admin status of the port is "Up" and a cable is connected to the port and transmitting data.

Note: If an interface's Admin Status is "Down", its Operational Status will also be "Down". When the Admin Status is changed to up, the interface's Operational Status will change to "Up" if the interface is ready to transmit and receive packets; or the Operational Status will change to "Dormant" if the interface is waiting for external actions; or the Operational Status will remain "Down" if there is a fault that prevents it from going "Up".

- **Operational State Changed At -** The date and time the operational status of the port last changed (from "Up" to "Down" or "Down" to "Up").

- **Configured Speed -** The configured interface line speed, in Mbps. If the port is set to "Auto", the switch automatically sets the line speed to match the attached device.
- **Negotiated Speed -** The actual speed of the port.
- **Auto Negotiation -** Auto Negotiation status on the port (On = Enabled, Blank = Disabled).
- **Default VLAN -** The default VLAN to which the port is assigned.
- **Last Time Link Changed -** The last time the configuration for the interface was changed. Note that this field is not supported on switches running AOS 6.x.
- **Number of Status Changes -** The total number of times the configuration of the interface has changed. Note that this field is not supported on switches running AOS 6.x.
- **Port Type -** The port type (e.g., Ethernet-CSMA/CD).
- **Specific Type -** Detailed information about the port type (e.g., LAG, Stack).
- **Port Properties -** The port configuration properties (e.g., UNP, Mobile, LLDP).
- **LAG Port Member -** The Link Aggregation Port(s) on the device, if applicable.
- **UNP Status -** Indicates whether or not UNP is Enabled/Disabled on the port.
- **Port Split Status -** The split port status of the switch (Auto, 40GB, or 4 x 10GB). The Split Port Feature is only supported on OS6900-Q32/X72 Switches running AOS 7.3.4.R01 and later. If the port is on a non-supported device, the field will display "False".
- **VFL Port -** Indicates whether or not the port is a VFL port (True/False)
- **PoE Status -** The administrative status of PoE on the port (True=enabled, False=disabled). If the device/port does not support PoE, the field will display "False".
- **PoE Wattage -** The amount of PoE power being used by the device (if applicable), in milliwatts.

Note: The Discovery Ports feature is supported on the following devices: OS6250, OS6350, OS6400, OS6450, OS6560, OS6850/OS6850E, OS6855, OS9000, OS6860/OS6860E, OS6865, OS6900, OS9700/OS9700E, OS9800/OS9800E, OS9900, OS10K, OAW-AP1201H, and OAW-AP1201HL

Link

The Discovery Link Screen displays all links that were learned during the discovery process, or created manually in OmniVista. It is also used to manually create, clone, edit, and delete manual links. Unlike automatically-discovered Links, which disappear from the Topology map view when they become unreachable, manual links will be persistent and display in RED when the link goes down. This enables users to manually configure critical links, such as the network core links (which are seldom changed), providing better monitoring capability for critical links.

Creating a Link

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

- **IP Address 1 -** The IP address of one device in the link. Select an option from the drop-down menu (Use Switch Picker/Use Topology), click on the **Select Device** button and select a device.
- **Slot/Port 1 -** Select a slot/port for IP address 1 from the drop-down menu.
- **LAG 1 -** If this is a link aggregation link, set the LAG 1 field to the Link Aggregation Number assigned by the device above when the link aggregation group was created.
- **IP Address 2 -** The IP address of the second device in the link. Select an option from the drop-down menu (Use Switch Picker/Use Topology), click on the **Select Device** button and select a device.
- **Slot/Port 2 -** Select a slot/port for IP address 2 from the drop-down menu.
- **LAG 2 -** If this is a link aggregation link, set the LAG 2 field to the Link Aggregation Number assigned by the device above when the link aggregation group was created.
- **Media Type -** Select the media type for the link from the drop-down menu.
- **Status -** Select the administrative status for the link from the drop-down menu (Up/Down). Note that you can edit the link later if you want to change the status.

Cloning a Link

You can clone an LLDP link to create a manual link. If an LLDP link goes down, a "Link Down" Trap is sent, but the link will disappear from the Topology map on the next poll because it no longer exists. However, if you clone an LLDP link to create a manual link, the manual link will continue to display (in Red) on the Topology map.

Click on the **Clone LLDP To Manual** button to bring up the Clone LLDP To Manual Screen. Click on the Links **ADD** button and select the link(s) you want to clone. (You can click on the **EDIT** button to add/remove links from the selection.) When you are finished, click on the **Create** button. The new manual link(s) will appear in the Existing Links Table.

You can also clone and edit an LLDP link to quickly create a new manual link on different ports on a device. Clone and create a manual link as described above. Select the new manual link in the Existing Links Table, click on the Edit icon, and edit the link.

Editing a Link

You can edit manual links, select a manual link in the Existing Links Table and click on the Edit icon. Edit the available fields as described above and click on the **Apply** button.

Deleting a Link

Select a link in the Existing Links Table and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Existing Links Table

- **Origin** - The origin of the link (e.g., AMAP, LLDP, Manual).
- **IP Address 1** - The IP address of one switch in the link.
- **Slot/Port 1** - The slot and port that connect the link on IP address 1.
- **LAG 1** - If this is a link aggregation link, this field displays the Link Aggregation reference number assigned by the first switch when the link aggregation group was created.

- **IP Address 2** - The slot and port that connect the link on IP address 1.
- **Slot/Port 2** - The slot and port that connect the link on the second switch, specified above. **LAG 2** - If this is a link aggregation link, this field displays the Link Aggregation reference number assigned by the second switch when the link aggregation group was created.
- **Ring ID -** The Ethernet Ring Protection (ERP) ID, if applicable.
- **Media Type** - The media type of the link (e.g., Ethernet).
- **Status** - The status of the link (e.g., Up/Down/Unknown).

Scheduled Upgrades

The Discovery Scheduled Upgrade Screen is used to schedule automatic software image upgrades for your network devices. The Scheduled Upgrade Feature enables you to schedule automatic upgrades to specific network devices during specific time windows (e.g., non-business hours) to ensure minimal network disruption. You can create, edit, and delete scheduled upgrades. Configured scheduled upgrades are displayed in the Scheduled Upgrades List and you can enable/disabled at any time.

Upgrade images must be downloaded to your computer from the Business Portal and imported into OmniVista. You can import the images in the Resource Manager Upgrade Image Screen (Configuration - Resource Manager - Upgrade Image) prior to creating a scheduled upgrade; or you can import the necessary images(s) when you create the scheduled upgrade. A device must be managed and the Running Configuration must be saved for an upgrade to occur.

Note that scheduled upgrades can also be configured in the Topology application by selecting a device(s) in a Topology Map and selecting "Scheduled Upgrades" in the Device Actions menu to bring up the Schedule Software Upgrade Wizard. Upgrades can also be scheduled on the Discovery - Managed Devices Screen by selecting a device(s) in the List of Managed Devices and selecting "Scheduled Upgrades" from the Actions drop-down menu to bring up the wizard.

> **Important Note:** It is recommended that you schedule upgrades on devices so that they do not adversely affect network performance. For example, stagger upgrades of different devices in different time windows during non-busy hours.

Creating a Scheduled Upgrade

Click on the Add icon, complete the fields as described below, then click on the **Create** button. When creating a scheduled upgrade, you define the schedule, the devices, and the software version to be used for the upgrade.

- **Schedule Name -** User-configured name for the scheduled upgrade.
- **Scheduler Setting -** Select **Now** to schedule an immediate upgrade. All devices included in the scheduled upgrade will be upgraded. Select **Later or Periodically** to schedule an upgrade at a later time or schedule a recurring upgrade as described below. Creating a periodic, recurring upgrade ensures that all devices included in the scheduled upgrade will be upgraded. If all devices included in the upgrade schedule are not upgraded during the configured time window, the remaining devices will be automatically upgraded during the next recurrence. Those devices that have already been upgraded will be skipped.
- **Start At -** Select the time when you want to begin the upgrade (e.g., 12:00 AM).

- **Time Window -** The time window for upgrading the devices in the schedule. If a device in the schedule has not been updated when the time window expires, it will not be upgraded for during that scheduled upgrade, but will be upgraded during the next recurrence. Those devices that have already been upgraded will be skipped.
- **Recurrence Pattern -** Select the interval for a recurring upgrade.

  No Recurrence - Upgrade will occur once at schedule date and time.

  Daily - Upgrade will occur on the schedule day at the configured "Start At" time. By default, the upgrade will occur every day ("Every 1 Day"). You can customize it by clicking on the "Every 1 Day" field and entering a number (Range = 1 - 30 days). For example, you could configure a Daily Upgrade to occur every 2 days if you want it to occur every other day.

  Weekly - Upgrade will occur once a week on the selected day at the configured "Start At" time. Select the day of the week on which you want the upgrade to occur. The upgrade will occur every week on that day at the configured "Start At" time. You can select more than one day to perform weekly upgrades on multiple days of the week.

  Monthly - Upgrade will occur monthly on the configured day at the configured "Start At" time. Select the first radio button to schedule the upgrade for a specific day of the month (1 - 31), for a specific number of months. By default, the upgrade will occur on the first day of every month ("Day 1 of every 1 Month"). However, you can customize it. For example, you could schedule the upgrade for the 15th day every other month ("Day 15 of every 2 Months"). Select the second radio button to schedule the upgrade on a specific day of the week (e.g., Second Tuesday), for a specific number of months.

  Every Weekday - Upgrade will occur every weekday at the configured "Start At" time.
- **Range of Recurrence -** Select the start and end date, if applicable, for the scheduled upgrade.

  Start Date - Enter the start date for the scheduled upgrade. The scheduled upgrade will begin on that date at the configured "Start At" time.

  End Date - Select the "No End Date" radio button to continue the scheduled upgrade indefinitely. Select the "End by" radio button to enter an end date for the upgrade. The "End Date" option is not available for a "one-time" (No Recurrence) upgrade.
- **Devices Selection -** Click on the **Change Selection** button to bring up the Devices List to select specific devices for upgrade. A device (switch or AP) can only be in one schedule. If a switch in a Virtual Chassis is added to a schedule, all of the switches in that VC are included.
- **Set Software Version -** Select an available upgrade software version from the drop-down menu, as described below. If the desired software version is not available, click on **Import New Image** to import the image into OmniVista.
- **Set Same Software Version for All Devices (same models only) -** Select an upgrade software version from the drop-down list to upgrade all selected devices to that software version. If you select multiple devices, the devices must use the same base software. If you select devices that use different software (e.g., OAW-AP1221 and OS6450), "Do Not Upgrade" will be your only option. Select the "Set Different Software Version for Each Device" option.

- **Set Different Software Version for Each Device -** When you select this option, all selected devices will appear. Under the "Desired Software Version" column, select the upgrade software version for each device. Under the "Install Action" column, select "Upgrade Image" if you are upgrading Image Files, or "BMF" if you are upgrading U-Boot/Miniboot Files. In the "Install Directory" column enter the directory where you want to install the files (Default = /flash/working). Note that if you are performing an Image File upgrade **and** a U-Boot/Miniboot upgrade, refer to the applicable *OmniSwitch AOS Switch Management Guide* **before upgrading**.
- **Review -** Review the devices and schedule that you have configured.

Editing a Scheduled Upgrade

Select a schedule upgrade in the Scheduled Upgrade List, click on the Edit icon, edit the fields as described above, then click on the **Apply** button.

Deleting a Scheduled Upgrade

Select a schedule upgrade in the Scheduled Upgrade List, click on the Delete icon, then click **OK** at the Confirmation Prompt.

Scheduled Upgrade List

The Scheduled Upgrade List provides information on all scheduled upgrades. You can also select an upgrade in the list and click on the **Enable** or **Disable** buttons to enable/disable a scheduled upgrade.

- **Schedule Name -** User-configured name for the scheduled upgrade.
- **Start Time -** The time the upgrade is schedule to start.
- **Duration -** The time window for upgrading the devices in the schedule.
- **Status -** The status of the schedule upgrade.
- **Scheduled -** The upgrade is scheduled to occur in the future. Note that if some of the devices in a scheduled upgrade were not upgraded during the configured time window, the status will change from "Upgrading" back to "Scheduled" until the next recurrence of the upgrade.
- **Upgrading -** The upgrade is taking place within the configure time window.
- **Disabled -** The scheduled upgrade has been disabled.
- **Devices List -** The devices being upgraded. Click on the devices in the column to view a full list of devices, and additional information on each device, including the upgrade status of each device.
- **Create Date -** The date the upgrade schedule was created.
- **Last Updated Date -** The date and time the scheduled upgrade took place.
- **Results -** The result of the upgrade. You can also click on the View icon to the right of the result to view logs for the schedule upgrade.
- **Scheduled Was Scheduled -** The scheduled upgrade has been created and devices will update at the scheduled time.
- **"X" Number of Upgrades So Far -** The number of devices ("X") that have been upgraded so far during the scheduled upgrade. Once all devices are upgraded successfully, the status will change to "Schedule Was Disabled".

- **Schedule Has No Device -** The schedule upgrade has been created, but contains no devices.
- **Schedule Was Disabled -** The scheduled upgrade is currently disabled.

FAQs/Troubleshooting

Problem	Resolution
The image I want to use is not displayed in the "Desired Software" drop-down menu.	• The image has not been imported into OmniVista. Upgrade images must be downloaded to your computer from the Business Portal and imported into OmniVista. You can import the images in the Resource Manager Upgrade Image Screen (Configuration - Resource Manager - Upgrade Image) prior to creating a scheduled upgrade; or you can import the necessary images(s) when you create the scheduled upgrade.
Some devices in the scheduled upgrade were not upgraded.	• The configured time window ran out before all of the devices were upgraded. The devices will be upgraded on the recurrence. • If a device is already running the desired software version. it will not be upgraded. Assume that the device was manually upgraded from the CLI after the schedule was created. • If a device is "unsaved" the device will not be upgraded. It will be skipped. • OmniVista was not able to connect to the device because it did not have the correct credentials.
How can I monitor the progress of the upgrade? Are there logs available?	• You can view a log for a scheduled upgrade by clicking on the upgrade in the Scheduled Upgrade List to bring up upgrade details. Click on the "View" icon next to the "Results" field to display the log. • Logs can be viewed in the Scheduler Application (Administration Control Panel - Scheduler - Scheduler History). Locate the upgrade job in the Scheduler History List and click on it to view the log.
Will devices automatically reboot as part of the upgrade process?	• Yes.
If a device is running a higher version than the version set in the schedule, will it be	• The device will be downgraded. A message will inform the user that the device will be downgraded.

Problem	Resolution
skipped or downgraded when the scheduled upgrade occurs?	

SPB Service Port

The Discovery SPB Service Screen is used to display information about SPB Services Ports on network devices. SPB Services are configured on edge devices, so only edge devices are displayed. Click on the **ADD** or **EDIT** button at the top of the screen to select the devices you want to view (you can select up to 50 devices at a time), then select the service(s) you want to view on those devices from the **SPB Service ID** drop-down.

> **Note:** If you navigate to this page directly from an SPB Map in Topology, the devices in the map you were viewing are automatically displayed in the table, and all SPB Services are pre-selected.

Service Port Information

- **Service ID -** The Service Port ID.
- **System Name -** The system name assigned to the SPB bridge.
- **IP Address -** The IP address of the device on which the port resides.
- **Service Identifier -** The SPB Instance Service Identifier (ISID).
- **Type -** Service Access Point (SAP) or Service Distribution Point (SDP).
- **Admin Status -** The administrative status of the SBP interface (Up/Down).
- **Operational Status -** The operational status of the SPB interface (Up/Down).
- **Statistics -** Indicates if ingress and egress statistics collection for packets flowing through the service is Enabled or Disabled.
- **Trusted -** The trust mode for the SAP (Trusted/Untrusted). (Default = Trusted).
- **Priority -** The priority value to set for tagged and untagged packets received on an untrusted SAP.
- Values range from 0 (lowest priority) to 7 (highest priority).
- **System ID -** The system ID of the SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.
- **BVLAN -** The SPB base VLAN assigned to exchange ISIS-SPB control traffic with other SPB bridges.
- **Port -** The slot/port or link aggregate ID of the SPB interface.
- **SAP Description -** An optional description configured for the SAP. By default, the description is blank.

Settings

Setting Frequencies

Once the first discovery is complete, OmniVista performs automatic periodic discoveries to keep its information about the network updated. The Discovery Setting Frequencies Screen is used to configure the frequency of automatic periodic discoveries.

Configuring Automatic Polling

You can configure the frequency of automatic polling. Enter a value (Days, Hours, Minutes) in the applicable Automatic Discovery Type and click on the **Apply** button.

Automatic Discovery Types

OmniVista performs the following automatic discoveries:

- Full Discovery
- Occasional Updates
- Regular Updates
- Frequent Updates

Note: The default automatic discovery settings vary depending on the size of the network.

Full Discovery

Full Discoveries include:

- Down Switch Polling
- Frequent Update Polling
- Regular Update Polling
- Auto-discovery of network devices as specified in the Discovery application.

Occasional Updates

Occasional Updates include:

- Down Switch Polling
- Frequent Update Polling
- Regular Update Polling

Regular Updates

Regular Updates include:

- Down Switch Polling
- Frequent Update polling as described above.
- Additional polling for:
  Detailed chassis, module, and port information
  VLAN information
  Link Aggregation
  Ethernet link discovery (i.e., polling AMAP tables)
- Locator
- MAC address column from the ARP Table
- Bridge Forwarding Table

Frequent Updates

Frequent Updates include:

- Down Switch Polling
- Polling the standard MIB-II scalar variables sysName and sysDescr
- For AOS devices, polling for:

  The running directory (certified or working), the certification status, and the administrative status of all CMMs.

  The configuration change status; i.e., has the configuration changed since the last save of memory.

Automatic Discovery Defaults

The default automatic discovery settings vary depending on the size of the network. Each automatic discovery type will be pre-filled with a default polling interval based on the size of the network you are managing, as shown in the table below.

Default Discovery Polling Intervals				
Number of Managed Devices	**Full Discovery**	**Occasional Updates**	**Regular Updates**	**Frequent Updates**
Low (up to 500)	8 Hours	4 Hours	1 Hours	5 Minutes
Medium (500 - 2000)	10 Hours	6 Hours	2 Hours	15 Minutes
High (2000 - 5000)	12 Hours	8 Hours	4 Hours	30 Minutes
Very High (5000 - 10000	18 Hours	12 Hours	8 Hours	2 Hours

IP Failover

The Discovery IP Failover Screen is used to specify whether or not OmniVista will use a device's alternate IP address for SNMP traffic if the primary IP address fails. If IP Failover is enabled and a device fails to respond to SNMP requests, the OmniVista Server tries to reach the switch using the alternate IP address. If the attempt is successful, all subsequent management traffic is diverted to this new address. Use the **IP Failover** slider to enable (On) or disable (Off) the feature and click on the **Apply** button.

Switch Monitoring

The Discovery Switch Monitoring Screen is used to configure discovery polling of "down" devices. OmniVista polls down switches once per minute to check if the switches have come back up. Select the **Always** radio button if you want this monitoring to occur all the time. Select the **Only if Polling Enabled** radio button if you want this monitoring to occur only when normal OmniVista polling is enabled. After making a selection, click the **Apply** button. The change takes effect immediately.

Other Settings

The Discovery Other Settings Screen is used to enable/disable OmniVista polling using the REST API interface. REST API Polling is supported for Locator, Topology LLDP Links, and Shortest Path Bridging (SPB) and improves performance for these features. REST API Polling is supported on switches running AOS 8.7R3 and higher. By default, the **Poll Using REST API**

field is enabled. If disabled, or if a device does not support this feature, OmniVista will use the SNMP interface for polling.

After making a selection, click the **Apply** button. The change takes effect immediately.

Pre-requisites for REST API Polling:

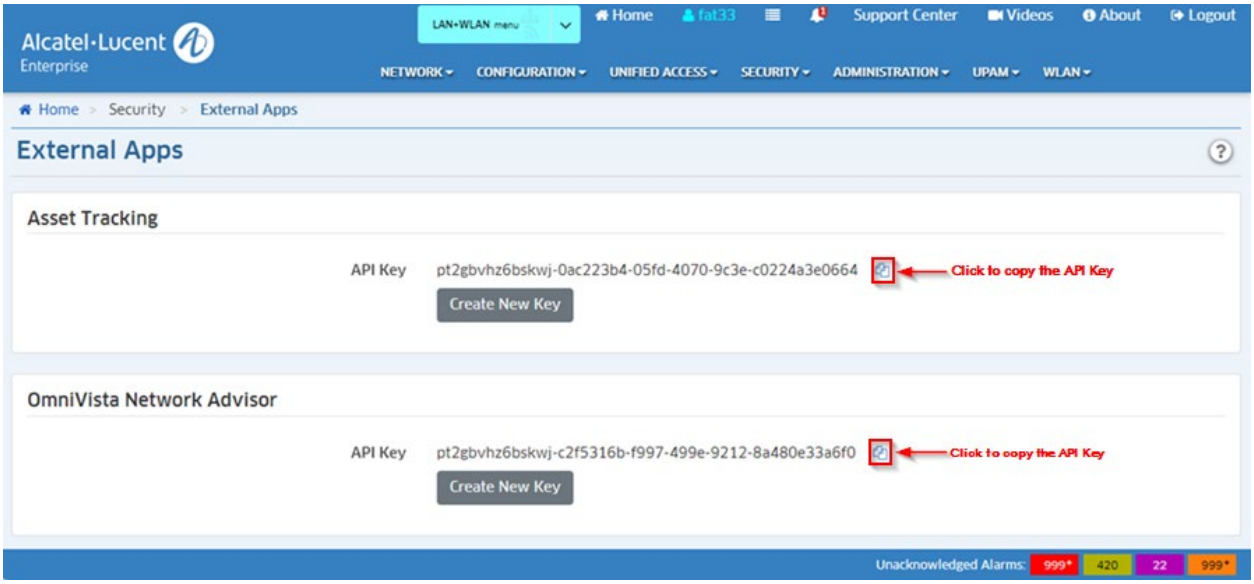
- HTTP AAA authentication must be configured on the switch using the following CLI command:
  - **aaa authentication http <*server*>**
- AOS 8.7R3 or 8.8R1 - HTTP and WebView services must be enabled on the switch using the following CLI commands:
  - **webview server enable**
  - **webview access enable**
  - **ip service http admin-state enable**
- AOS 8.9R1 and higher - HTTP and WebView services must be enabled on the switch using the following CLI commands:
  - **webview server enable**
  - **ip service http admin-state enable**
- CLI user must be specified in device properties and that user must have read permissions to access the configuration and statistical data of the features. To update device properties, navigate to Managed Devices (Network - Discovery), select one or more switch(es) and Edit.

Troubleshooting

1. If the REST API poll fails for any reason, OmniVista will fall back to using the SNMP interface for polling. To determine if OmniVista is using SNMP or REST API for polling:
   a. View the "ov2500-server" and "worker-poller-service" Audit log files in OmniVista (Administration - Audit - System).
   b. Search for the "Fallback" keyword to determine if OmniVista is using REST API for polling. If the search for this keyword fails, then OmniVista is using REST API polling.
2. Incorrect credentials may result in switches periodically generating many authentication failure traps. To prevent or arrest a trap storm caused by this, specify correct credentials for managed switches or disable REST API polling.

13.0 External Apps

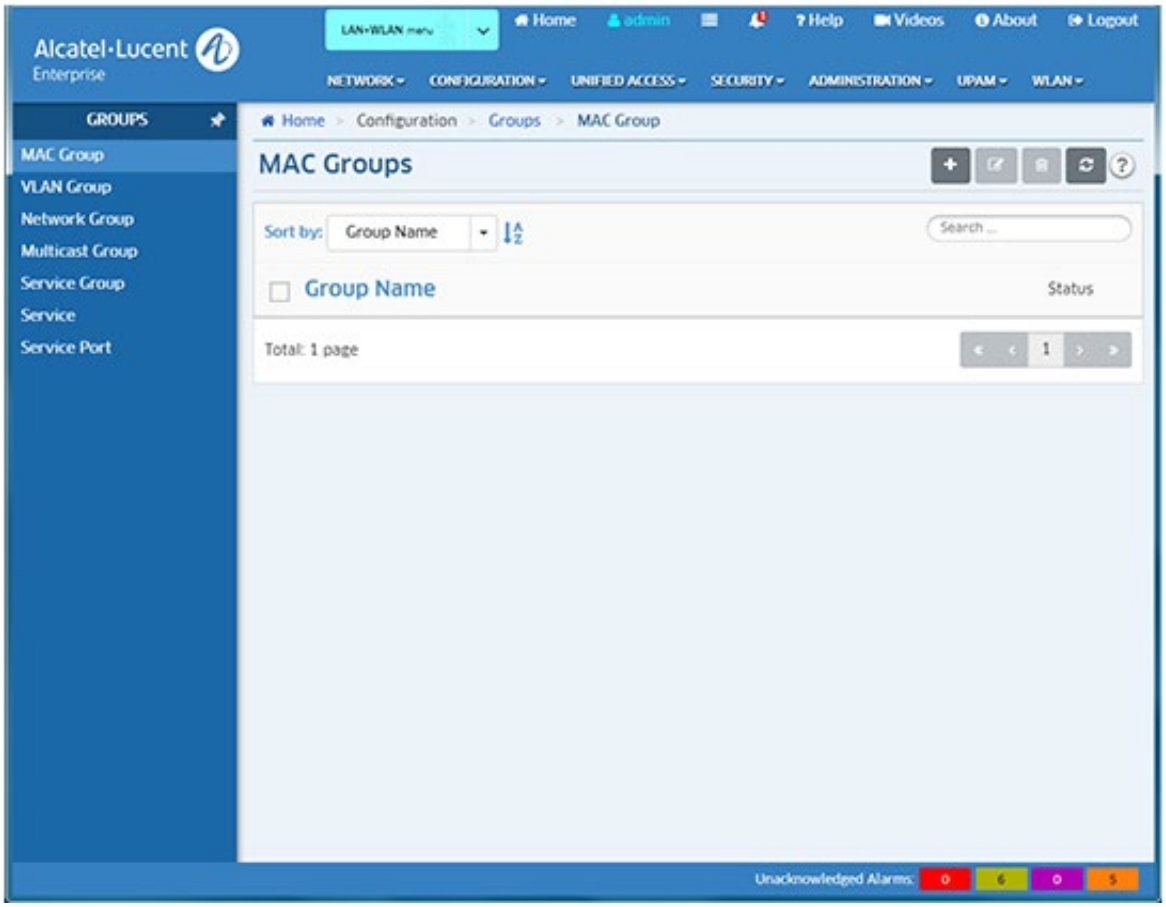
The External Apps Screen is used to create an API security key that is used by external devices/applications to access the OmniVista Server. For example, the Asset Tracking Engine or a Network Advisor instance will use this key to access OmniVista. Click on the "Copy" icon next to the key to copy the key to configure the external device/application for access to OmniVista. You can click on the Create New Key button at any time to create a new key that can then be copied and used to provide external access to OmniVista.



14.0 Groups

The Groups Application enables you to create groups, which can be used in various PolicyView conditions. Groups are stored on an LDAP (Lightweight Directory Access Protocol) repository that is automatically installed with OmniVista and resides on the same device as the OmniVista server. When the switches in the network are notified to re-cache their policy information, the firmware loads the groups referred by these policies. The Groups application enables you to create five types of groups: MAC Groups, VLAN Groups, Network Groups, Multicast Groups, and Service Groups. You can also configure Services and Service Ports to be used in Service Groups.

Groups



MAC Groups

The Groups MAC Groups Screen displays all configured MAC Groups. The screen is used to create, edit, and delete MAC Groups, which can be used in creating various policy conditions, such as source MAC group condition and destination MAC group condition.

Creating a MAC Group

Click on the Add icon. Enter a **Name** for the MAC Group. Enter a **MAC Address** and click on the Add icon. Repeat to add additional addresses. When you are done, click on the **Create**

button. The MAC Group will appear in MAC Groups List. Note that you must enter at least one MAC Address.

Editing a MAC Group

Click on the MAC Group that you want to edit to view the MAC Addresses in the MAC Group. Note that you cannot edit a MAC Group name. To edit a MAC Group name, you must delete the MAC Group and create a new one.

- To **add** a MAC Address to the Group, enter the **MAC Address**, then click on the Add icon. Repeat to add additional addresses. When you are done, click on **Update** button.
- To **edit** a MAC Address, click on the Edit icon, edit the address, then click on the Save icon. Repeat to edit additional addresses. When you are done, click on the **Update** button.
- To **delete** a MAC Address, click on the Delete icon next to the MAC Address you want to delete. Repeat to delete additional addresses. When you are done, click on the **Update** button.

Deleting a MAC Group

To delete a MAC Group(s), select the checkbox next to the group(s) in the list, click on the Delete icon, then click **OK** at the confirmation prompt.

> **Note:** MAC Groups that are in use by policy conditions cannot be deleted. To delete these MAC groups, remove them from the policy conditions.

VLAN Groups

The Groups VLAN Groups Screen displays all configured VLAN Groups. The screen is used to create, edit, and delete VLAN Groups.

Creating a VLAN Group

Click on the Add icon. Enter a **Name** for the VLAN Group. Enter a **VLAN Range** and click on the Add icon. Repeat to add additional VLAN Ranges. When you are finished, click on the **Create** button. The VLAN Group will appear in VLAN Groups List. Note that you must enter at least one (1) VLAN range.

Editing a VLAN Group

Click on the VLAN Group that you want to edit to view the VLAN ranges in the VLAN Group. Note that you cannot edit a VLAN Group name. To edit a VLAN Group name you must delete the VLAN Group and create a new one.

- To **add** a VLAN Range to the Group, enter a **VLAN Range** and click on the Add icon. Repeat to add additional ranges. When you are done, click on the **Update** button.
- To **edit** a VLAN Range, click on the Edit icon, edit the range, then click on the Save icon. Repeat to edit additional ranges. When you are done, click on the **Update** button.

- To **delete** a VLAN Range, click on the Delete icon next to the VLAN Range you want to delete. Repeat to delete additional ranges. When you are done, click on the **Update** button.

Deleting a VLAN Group

To delete a VLAN Group(s), select the checkbox next to the group(s) in the list, click on the Delete icon, then click **OK** at the confirmation prompt.

> **Note:** VLAN Groups that are in use by policy conditions cannot be deleted. To delete these VLAN groups, remove them from the policy conditions.

Network Groups

The Groups Network Groups Screen displays all configured Network Groups. The screen is used to create, edit, and delete Network Groups.

Creating a Network Group

Click on the Add icon. Enter a **Name** for the Network Group. Enter a **Subnet IP/Subnet Mask** and click on the Add icon. Repeat to add additional subnets. When you are finished, click on the **Create** button. The Network Group will appear in Network Groups List. Note that you must enter at least one Subnet IP/Subnet Mask.

Editing a Network Group

Click on the Network Group that you want to edit to view the Subnets in the Network Group. Note that you cannot edit a Network Group name. To edit a Network Group name, you must delete the Network Group and create a new one.

- To **add** a Subnet Address to the Group, enter a **Subnet IP/Subnet Mask** and click on the Add icon.
- Repeat to add additional subnets. When you are finished, click on the **Update** button.
- To **edit** a Subnet, click on the Edit icon, edit the address, then click on the Save icon. Repeat to edit additional Subnets. When you are done, click on the **Update** button.
- To **delete** a Subnet, click on the Delete icon next to the Subnet you want to delete. Repeat to delete Subnets. When you are done, click on the **Update** button.

Deleting a Network Group

To delete a Network Group(s), select the checkbox next to the group(s) in the list, click on the Delete icon, then click **OK** at the confirmation prompt.

> **Note:** Network Groups that are in use by policy conditions cannot be deleted. To delete these Network groups, remove them from the policy conditions.

Multicast Groups

The Groups Multicast Groups Screen displays all configured Multicast Groups. The screen is used to create, edit, and delete Multicast Groups.

Creating a Multicast Group

Click on the Add icon. Enter a **Name** for the Multicast Group. Enter a **Subnet IP/Subnet Mask** and click on the Add icon. To add additional subnets, click on the Add icon and enter the subnets. When you are finished, click on the **Create** button. The Multicast Group will appear in Multicast Groups List. Note that you must enter at least one Subnet IP/Subnet Mask.

Editing a Multicast Group

Click on the Multicast Group that you want to edit to view the Subnets in the Multicast Group.

- To **add** a Subnet Address to the Group, enter the **Subnet IP/Subnet Mask**, then click on the Add icon. Repeat to add additional subnets. When you are done, click on the **Update** button.
- To **edit** a Subnet, click on the Edit icon, edit the address, then click on the Save icon. Repeat to edit additional Subnets. When you are done, click on the **Update** button.
- To **delete** a Subnet, click on the Delete icon next to the Subnet you want to delete. Repeat to delete Subnets. When you are done, click on the **Update** button.

Deleting a Multicast Group

To delete a Multicast Group(s), select the checkbox next to the group(s) in the list, click on the Delete icon, then click **OK** at the confirmation prompt.

> **Note:** Multicast Groups that are in use by policy conditions cannot be deleted. To delete these Multicast groups, remove them from the policy conditions.

Service Groups

The Groups Service Groups Screen displays all configured Service Groups. The screen is used to create, edit, and delete Service Groups.

Creating a Service Group

Click on the Add icon. Enter a **Group Name** for the Service Group. Select a Service(s) and click on the **Create** button. If you want to create a new Service, click on the Add Icon to go to the Services Screen and create the Service. When you click on the **Create** button on the Services Screen you will be returned to the Create Service Group Screen to finish creating the Service Group. Note that you must enter at least one service. Also, you cannot use Source and Destination Services in group.

Editing a Service Group

Click on the Service Group that you want to edit, then click on the Edit Icon. Add or remove Services from the group as described above then click on the **Update** button. You cannot edit a Service Group name. To edit a Service Group name, you must delete the Service Group and create a new one.

Deleting a Service Group

To delete a Service Group(s), select the checkbox next to the group(s) in the list, click on the Delete icon, then click **OK** at the confirmation prompt.

Note: Service Groups that are in use by policy conditions cannot be deleted. To delete these Service Groups, remove them from the policy conditions.

Services

The Groups Services Screen displays all configured Services, which are used to create Service Groups. The screen is used to create, edit, and delete Services.

Creating a Service

Click on the Add icon. Complete the fields as described below, then click on the **Create** button.

- **Service Name -** User-configured name for the Service.
- **Protocol -** Select a protocol for the Service. By default, the TCP radio button is selected and TCP ports are displayed. Click on the UDP radio button to display UDP ports.
- **Source Port -** Select a source port from the Source Port drop-down list. The drop-down box includes a list of well-known TCP or UDP ports. Select a port(s) from the drop-down menu (you can also select "Check All" to select all ports. Click "Uncheck All" to deselect the ports and start over). If you want to create a new port, click on the Add Icon to go to the Service Port Screen and create a new port. When you click on the **Create** button on the Service Port Screen you will be returned to the Create Service Screen to finish creating the Service. Note that you can specify a Source Port, a Destination Port, or both.
- **Destination Port -** Select a destination port from the Destination Port drop-down list. The drop-down box includes a list of well-known TCP or UDP ports. Select a port(s) from the drop-down menu (you can also select "Check All" to select all ports. Click "Uncheck All" to deselect the ports and start over). If you want to create a new port, click on the Add Icon to go to the Service Port Screen and create a new port. When you click on the **Create** button on the Service Port Screen you will be returned to the Create Service Screen to finish creating the Service. Note that you can specify a Source Port, a Destination Port, or both.

Editing a Service

Click on the Service that you want to edit, then click on the Edit Icon. Edit the field(s) as described above then click on the **Update** button. You cannot edit a Service Name. To edit a Service Name, you must delete the Service and create a new one.

Deleting a Service

To delete a Service(s), select the checkbox next to the Service(s) in the list, click on the Delete icon, then click **OK** at the confirmation prompt.

Note: Services that are in use by policy conditions cannot be deleted. To delete these Services, remove them from the policy conditions.

Service Port

The Groups Service Port Screen displays all configured Service Ports, which are used to create Services. By default, the TCP radio button is selected and TCP Services are displayed. Click on

the UDP radio button to display UDP Services. The screen is used to create, edit, and delete Service Ports.

Creating a Service Port

Click on the Add icon. Complete the fields as described below, then click on the **Create** button.

- **Name -** User-configured name for the Service Port.
- **Port Number -** Enter a Service Port number.

Editing a Service Port

Click on the Service Port that you want to edit, then click on the Edit Icon. Edit the field(s) as described above then click on the **Update** button. You cannot edit a Service Port name. To edit a Service Port name, you must delete the Service Port and create a new one.

Deleting a Service Port

To delete a Service Port(s), select the checkbox next to the port(s) in the list, click on the Delete icon, then click **OK** at the confirmation prompt.

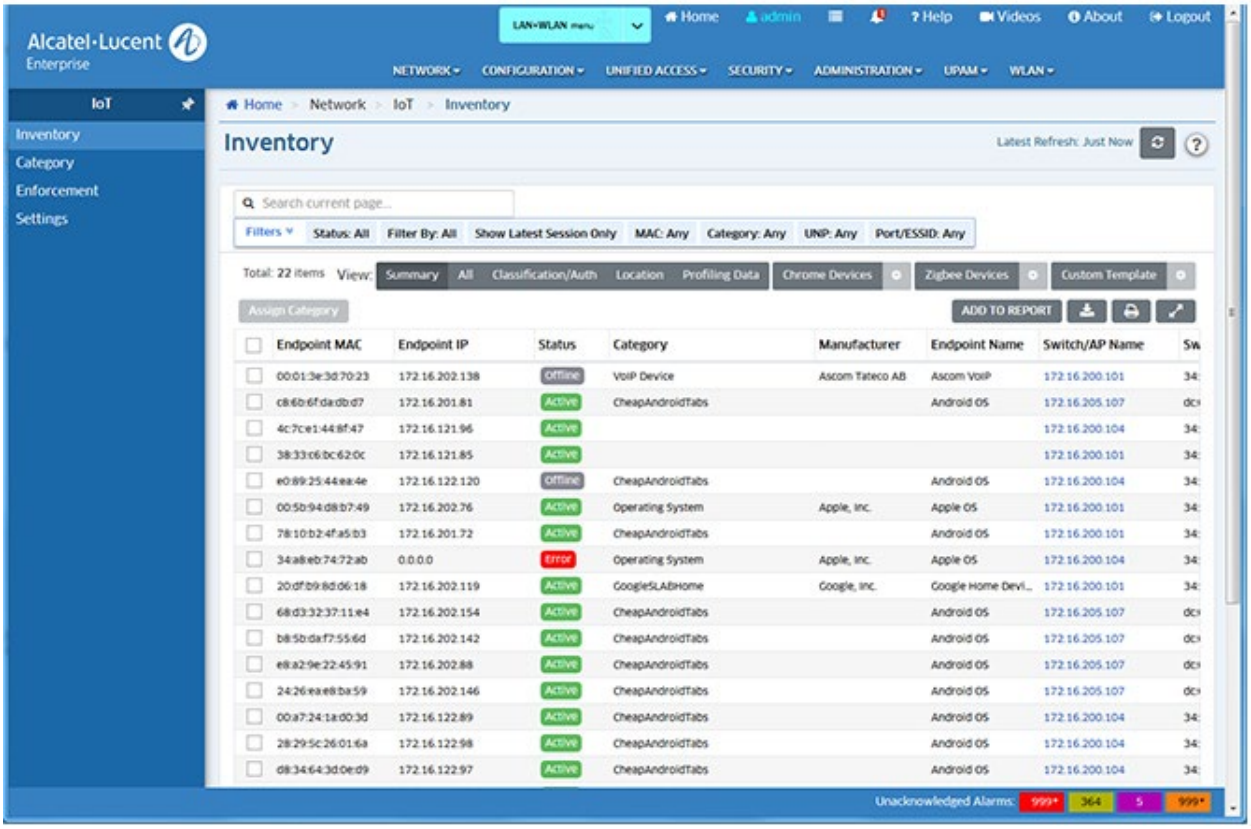
> **Note:** Service Ports that are in use by Services cannot be deleted. To delete these Service Ports, remove them from the Service.

15.0 IoT

The IoT application provides a detailed view of all endpoint devices connected to AOS Switches and Stellar APs (e.g., PCs, Tablets, Smartphones). OmniVista uses information received from AOS Switches and Stellar APs to track and categorize these devices and presents detailed information for the devices on the Inventory Screen. The application can also be configured to integrate with Google Workspace to collect device information and provide network security for Chrome devices; and can discover, enable/disable, and provide information on Zigbee devices. An overview of IoT functionality, as well as troubleshooting tips are provided below.

Important Note: Certain prerequisites (detailed below) **must** be met to use the IoT application. Verify that all prerequisites have been met before using IoT.

IoT



Note: IoT is supported on AOS 8.x Switches (AOS 8.6R1 and higher) and Stellar APs (3.0.7.xx and higher), and provides information on IPv4 endpoint devices.

The IoT application is configured using the following screens:

- **Inventory -** Provides detailed information on all endpoint devices that connect to the network.
- **Category -** Displays information about device categories, and is used to create custom categories.
- **Enforcement -** Used to configure category-based enforcement on devices.
- **Settings -** Used to configure IoT data retention preferences.

IoT Overview

When a client/endpoint is connected to an AOS Switch/Stellar AP, the switch/AP sends MQTT messages to OmniVista in real-time. This information includes the device MAC address, DHCP fingerprint, User-Agent, TCP signatures, network behavior, and more. Once the device is learned, OmniVista connects to a cloud-based Device Fingerprinting Service to categorize the device.

Device category information is populated based on Device Fingerprinting Service query results. The initial category is usually more broad or generic. As data transfer occurs between device endpoints and switches/APs, OmniVista monitors network packets and uses the additional information to query the Device Fingerprinting Service Database and arrive at a more specific category. Over time, the category for each endpoint device can change as more fingerprints are received. For example, a device may initially be categorized as "Phone, Tablet or Wearable". As more fingerprints are received, the device may next be categorized as an "Apple Mobile Device", and then an "Apple iPhone".

Note that OmniVista automatically connects to a cloud-based Device Fingerprinting Service to categorize devices. No configuration is required on OmniVista to make this connection. However, you must have an Internet connection that allows OmniVista to connect to the service. See Internet Requirements below for more information.

IoT Prerequisites

IoT must be enabled on individual AOS Switches and Stellar APs. The IoT application also requires an NTP Server to sync the time for OmniVista and switches/Stellar APs, as well as an Internet connection to connect to the Device Fingerprinting Service and the Zigbee Device Server at the Customer Site (e.g., Hotel).

Enabling IoT

IoT is disabled on AOS Switches and Stellar APs by default. To enabled IoT on a switch/Stellar AP, go to the Managed Devices Screen (Network - Discovery - Managed Devices), select the switch(es)/AP(s) in the Managed Devices List, click on the **Features** drop-down, and select **Enable IoT**. The switches/APs will appear in the "Enable IoT - Confirm" switch picker window. (Note that switches/APs that do not support IoT will not appear in the window.) Click **OK** to enable IoT. OmniVista will begin collecting IoT information for endpoints connected to the switches/APs.

> **Note:** When IoT is enabled on a switch, it is enabled globally on all UNP Ports. However, it is not enabled on fixed ports. For these ports you must SSH to the switch and issue the following CLI command: **device-profile port *x/x/x* admin-state enable**.

To disable IoT on a switch/Stellar AP, select the switch(es)/AP(s) in the Managed Devices List, click on the **Features** drop-down, and select **Disable IoT** button. See the Managed Devices online help for more information.

> **Note:** If IoT is disabled on a device or a device is removed from the Managed Devices List, the device remains in the Inventory List with device information "grayed out" and the last know information displayed.

NTP Requirements

An NTP Server(s) is required for a consistent Inventory view of IoT devices. Switches/Stellar APs must be synced to the same time, for OmniVista to correctly display session start time/end time, and sort and filter of IoT Inventory data. Switches/Stellar APs must have access to at least one NTP Server, whether local or external.

Internet Requirements

You must have an Internet connection to use the IoT application. If you have a firewall, it must be configured to allow access to the Device Fingerprinting Service (**api.fingerbank.org**), or the Zigbee Server at the Customer Site (e.g., Hotel).

Troubleshooting

IoT Logs

The IoT Inventory and IoT Profiler Logs in the Audit application (Administration - Audit) can be used to troubleshoot problems in the IoT application. Go to the Audit application, click on "Network" on the left side of the screen, then select "iot-inventory" or "iot-profiler" for IoT-specific problems, or "zcs" for Zigbee-specific problems and view the logs.

Alcatel IP Phones

When IoT is enabled on a switch and you connect an Alcatel IP Phone (IPTouch) on a UNP Port, the switch will not send fingerprinting information to OmniVista. You must SSH to the switch and disable automatic prioritization of IP phone traffic by entering the following CLI command: **qos no phones**.

Inventory

The IoT Inventory Screen provides detailed information on all endpoint devices that connect to the network (e.g., PCs, Tablets, Smartphones). New endpoint association or disassociation (Endpoint Status) is updated in "real-time" (click on the Refresh button to display the latest information). Once an endpoint is Active, any changes to the endpoint (e.g., profile change, IP address change) are updated every 5 minutes for devices connected to Stellar APs, and every 15 minutes for devices connected to AOS Switches.

Information can be retained for up to 60 days, at which time is it overwritten. By default, only the latest session is displayed in the Inventory List for each device; however, you can display all available information by unchecking the “Show Latest Session Only” checkbox on the filter window. By default, the maximum number of sessions displayed per endpoint device is three (3) per switch/AP (current record and 2 historical records). Data Retention and display settings are configured on the IoT Settings Screen. By default, information for all devices is displayed. The information can be filtered by clicking on the Filters Bar at the top of the screen. Any filters that are applied are displayed in the bar.

The IoT application can be configured to integrate with Google Workspace to collect device information and provide network security for Chrome devices. Click on the **Google Workspace Settings** button at the top of the Inventory List to configure Google Workspace for IoT. Note that Google Workspace Integration is only supported on devices connected to AOS Switches running AOS 8.6R2 and later, or devices connected to APs connected to AOS Switches running AOS 8.6R2 and later.

The IoT application can also be used to enable/disable and monitor Zigbee devices (e.g., Assa Abloy Door Locks). OmniVista interfaces with a Zigbee Server and Stellar APs to provide Zigbee device support. Once OmniVista and APs are configured for Zigbee support, Zigbee devices are discovered and displayed in the IoT Zigbee Devices Table. Click on the **Zigbee Devices** button to view and enable/disable Zigbee devices.

> **Important Note:** There are network prerequisites and configuration steps that **must** be completed to enable IoT. See the IoT Overview online help for an overview of the application including prerequisites.

Inventory List

By default, the "Summary" view of the Inventory List is displayed, which gives an overview of device inventory. The column headings differ depending on the view you choose (e.g., Summary, All, Classification/Auth). You can also create a custom view. There is also a Chrome Device View, which displays any Chrome Devices learned through Google Workspace, and a Zigbee Device View, which displays Zigbee Device information. You can also manually assign a Custom Category to a device.

> **Note:** Endpoints with IPv6 addresses attached to AOS devices may take up to 15 minutes to display. Endpoints with IPv6 addresses attached to Stellar APs will not be displayed in the Inventory list since Stellar APs do not support IPv6.

- **Endpoint MAC -** The MAC Address of the device.
- **Endpoint IP -** The IP Address of the device.
- **Status -** The operational status of the device on the network.
    - **Active -** The device was active on the network when it was last known by OmniVista. Note that if a switch/AP is deleted from OmniVista or IoT is disabled on a switch/AP, OmniVista will display all devices connected to that switch/AP as "Offline" regardless of the device's actual status. This is because OmniVista receives no updates regarding these devices in these scenarios. If a switch/AP goes down, OmniVista will not automatically change the status of the devices connected to it.
        - **Offline -** The device is not currently active on the network. Note that if IoT is disabled on a device or a device is removed from the Managed Devices List, the device remains in the Inventory List with device information "grayed out" and the last know information displayed.
        - **Error -** The device was unable to connect to the network (e.g., MAC Authentication fails).
- **Category -** The device category (e.g., Datacenter Appliance, Phone/Table/Wearable). Note that that initial Category value is not likely to be very specific. As more activity happens on the endpoint device, switches/APs send additional details about the endpoint, and the category description will be more specific. Also note that for some devices, this field may be empty. This generally happens when insufficient fingerprint information about the device is available. (e.g., switch/AP receives only the MAC address of the endpoint and the MAC is unknown or unpopular).
- **Manufacturer -** The device manufacturer.
- **Endpoint Name -** The name of the endpoint device as determined by the Device Fingerprinting Service.

- **Endpoint Version -** The endpoint device OS version.
- **Category Hierarchy -** The Category, Manufacturer, and Endpoint name used to categorize the device.
- **Switch/AP Name -** The IP address of the switch/AP through which the device is connected to the network.
- **Switch/AP MAC -** The MAC address of the switch/AP through which the device is connected to the network.
- **Port/ESSID -** The switch port or ESSID through which the device is connected to the network.
- **Port Type -** The port type through which the device is connected to the network (Wireless/Wired/UNP).
- **Port Description -** A description of the port through which the device is connected to the network, as received from the device.
- **VLAN -** The VLAN through which the device is connected to the network.
    - **AOS Devices -** The untagged VLAN, or the tagged VLAN if traffic is tagged.
    - **Stellar APs -** The VLAN mapped to the Access Role Profile.
- **Tunnel Type -** If the endpoint is set up on tunnel, the tunnel type is displayed:
    - SPB
    - VXLAN
    - L2GRE
    - Guest Tunnel.
- **Far End IP -** The IP address of the far end tunnel termination (displayed for wireless clients only).
- **VPN ID -** The Tunnel ID that identifies a GRE Tunnel VPN (displayed for wireless clients only).
- **UNP -** The Access Role Profile assigned to the device, if applicable.
- **UNP Type -** The UNP type, if enforcement is applied:
    - Default UNP
    - Pass-Alternate UNP
    - Auth-Server Down UNP
    - UNP from Classification
    - UNP from RADIUS
    - UNP from OmniVista Enforcement.
- **Policy List -** The Policy List applied to the device, if applicable.
- **Authentication Type -** The type of authentication used for the device (e.g., MAC, 802.1X)
- **Authentication Status -** The status of device authentication, if applicable (e.g., Passed, Failed).
- **Connection Error -** The connection error if the device was unable to connect to the network, if applicable.
- **Enforcement Status -** The status of profile enforcement, if applicable:
    - Initial - Initial status.

  - Excluded - Matching by Exclusion Rules, no mapping.
  - Enforced - Successfully mapped to category.
  - Failed - SNMP enforcement failed.
  - Pending - Enforcement request was send to switch/AP. One reason may be that ARP is not configured on the device.
  - Disabled - OmniVista is working in manual mode.
- **Start Time -** The time the device first accessed the network.
- **End Time -** The time the device disconnected from the network.
- **Last Updated -** The last time OmniVista received message from the device and the message was successfully processed.

Note: Stellar APs connected to AOS devices are displayed in the Inventory List. To prevent a Stellar AP from being displayed in the Inventory List, you must disable IoT profiling on the switch port connected to the AP using the following CLI command: **device-profile port *slot/port* admin-state disable**.

Customizing the Display

By default, the "Summary" view of the Inventory List is displayed. The display can be changed by clicking on a display option button at the top of the list (e.g., **All**, **Classification/Auth**, **Location**). You can also create a custom display buy clicking on the **Custom Template** button, then clicking on the Configuration icon and selecting the columns you want to display.

Exporting IoT Inventory Records

To export IoT Inventory records to a single CSV file, click on the **Export** button and select one of the following options:

- **Current Page** – Exports all records on the current page to a single CSV file.
- **All Records** – Exports all records to a single CSV file.

After you select one of the above options, browse to the location where you want to export the records to a single CSV file and click **Save**.

Google Workspace Inventory List

Click on the **Chrome Devices** button at the top of the Inventory List to bring up the Chrome Device Inventory List. Only devices learned from Google Workspace will be displayed in this view.

- **Endpoint MAC -** The MAC Address of the device.
- **Endpoint IP -** The IP Address of the device.
- **Status -** The operational status of the device on the network.
  - **Active -** The device was active on the network when it was last known by OmniVista. Note that if a switch/AP is deleted from OmniVista or IoT is disabled on a switch/AP, OmniVista will display all devices connected to that switch/AP as "Offline" regardless of the device's actual status. This is because OmniVista receives no updates regarding these devices in these scenarios. If a switch/AP goes down, OmniVista will not automatically change the status of the devices connected to it.

  - **Offline -** The device is not currently active on the network, the switch/AP to which the device is connected was deleted from OmniVista, or IoT was disabled on the switch/AP to which the device is connected.
  - **Error -** The device was unable to connect to the network (e.g., MAC Authentication fails).
- **Status from Google Workspace -** The status of the device from Google Workspace.
  - **Active -** The device is enrolled into the domain.
  - **Delinquent -** The annual license for the domain has expired and the device no longer receives policies and settings. When a new license is purchased, the device will return to "Active" state.
  - **Deprovisioned -** The device is no longer eligible to be enrolled into the domain. The order has been canceled, and the device's settings have been cached on the device. If the device is activated again, the latest system settings are applied to this newly activated device.
  - **Disabled -** The device has been disabled by the administrator and cannot be used.
  - **Inactive -** The device is not enrolled into the domain.
  - **Return Arrived -** The request to replace this device has arrived. This is applicable only for those devices purchased directly from Google.
  - **Return Requested -** A request has been made to replace this device. This is applicable only for those devices purchased directly from Google.
  - **Shipped -** The device has shipped. This is applicable only for those devices purchased directly from Google.
  - **Unknown -** The status of the device cannot be determined.
- **Recent Users -** A list of recent device users, in descending order, by last login time.
- **Annotated User -** The user of the device as noted by the Google Workspace administrator. Maximum length is 100 characters. Empty values are allowed.
- **OS Version -** The operating system version of the device.
- **Model -** The device model.
- **Switch/AP Name -** The IP address of the switch/AP through which the device is connected to the network.
- **Port/ESSID -** The switch port or ESSID through which the device is connected to the network.
- **Category -** The Chrome device category (e.g., Active Chrome Device, Inactive Chrome Device). You must enable the following option in Google Workspace Settings - "Enable Google Workspace based auto categorization" for categorization to work.
- **UNP -** The Access Role Profile assigned to the device, if applicable.
- **Start Time -** The time the device first accessed the network.
- **End Time -** The time the device disconnected from the network.
- **Last Updated -** The last time OmniVista received message from the device and the message was successfully processed.
- **Device ID -** The unique ID of the Chrome device. It's generated by Google Workspace.

- **MAC -** The device MAC address.
- **Serial Number -** The device serial number.
- **Org Unit Path -** The full parent path, including the organizational unit name associated with the device. Path names are case insensitive. If the parent organizational unit is the top-level organization, it is represented as a forward slash, /.
- **Annotated Asset ID -** The asset identifier as noted by the Google Workspace administrator, or specified during enrollment.
- **Annotated Location -** The address or location of the device as noted by the Google Workspace administrator. Maximum length is 200 characters. Empty values are allowed.
- **Firmware Version -** The Chrome device's firmware version.
- **Kind -** The type of Chrome device resource.
- **Last Enrollment Time -** The date and time the device was last enrolled.
- **Last Sync -**The date and time the device was last synchronized with the policy settings in the Google Workspace Admin console.
- **Notes -** Notes about this device added by the Google Workspace administrator. This property can be searched with the list method's query parameter. Maximum length is 500 characters. Empty values are allowed.
- **Order Number -** The device's order number. Only devices directly purchased from Google have an order number.
- **Platform Version -** The Chrome device's platform version.
- **Support End Date -** The final date the device will be supported. This is applicable only for those devices purchased directly from Google.
- **Will Auto Renew -** Determines if the device will auto renew its support after the support end date. This is applicable only for those devices purchased directly from Google. This is a read-only property. Possible values are:
    - **True -** The support will be automatically renewed (Default).
    - **False -** The support will not be automatically renewed.
- **ETag -** ETag of the resource.

Zigbee Devices Inventory List

Click on the **Zigbee Devices** button at the top of the Inventory List to view Zigbee Device Information. There are three tabs at the top of the table. The "New Devices" Tab displays information for all discovered Zigbee devices. Once a device is "Accepted" it is enabled and moved to the "Accepted Devices" Tab. If an "Accepted" device is manually "Rejected", it is moved to the "Rejected Devices" Tab and is disabled..

- **Device IEEE MAC -** The IEEE MAC Address of the Zigbee device.
- **AP MAC -** The MAC Address of the AP connected to the Zigbee device.
- **Name -** The name of the Zigbee device. A name is automatically assigned by the Zigbee Server. You can click on the Edit icon in the field to update the name (e.g., Room 101).
- **PAN-ID -** The Personal Area Network (PAN) that the Zigbee device is connected to. A PAN is wireless network that communicates on the 2.4GHz Band.

- **Channel -** The wireless channel used to communicate with the Zigbee device.
- **Network Address -** The network address assigned to the Zigbee device when it connects to the PAN.
- **RSSI Value -** The Received Signal Strength Indicator (RSSI) value between the AP and the Zigbee device.
- **LQI Value -** The Link Quality Index. This percentage value should be above 30% to communicate seamlessly with the Zigbee device. If the value falls below 10%, the communication is not possible.
- **Status -** The status of the device (Up/Down).
- **Admin Status -** The administrative status of the device (New/Accepted/Rejected).
- **Auto Accept Status -** The status assigned to the Zigbee device when it was discovered.
    - **Auto Accepted -** The device is included in the Whitelist OUI of the AP that connects to it.
    - **Auto Rejected -** The device is not in the Whitelist OUI of the AP that connects to it, the device is "Auto rejected.
    - **Manually Accepted -** The device was previously "Auto Rejected" or manually rejected, and was then manually accepted by the user.
    - **Manually Rejected -** The device was previously "Auto Accepted" or manually accepted, and was then manually rejected by the user.

  Note: OmniVista does not require a Fingerprint Service to obtain Zigbee Device (e.g., Assa Abloy locks). APs read device-specific information from Zigbee devices (e.g., locks), and the Zigbee Server (e.g., Assa Abloy Server).

Accepting/Rejecting Zigbee Devices

When a Zigbee device (e.g., Assa Abloy door lock) is discovered, it initially appears in the "New Devices" tab of the Zigbee Device List with an Auto Accept Status of "Auto Rejected". To accept and enable the device, click on the Edit icon in the Name field and change the device name (e.g., Room 101, Room 102). Then select the device and click on the **Accept** button. Click **OK** at the Confirmation Prompt. The device will be enabled and moved to the "Accepted Devices" Tab.

To "Reject" and disable an "Accepted" device, select the device in the "Accepted Devices" Tab and click on the **Reject** button. Click **OK** at the Confirmation Prompt. The device will be disabled and moved to the "Rejected Devices" Tab.

Configuring Google Workspace

The IoT application integrates with Google Workspace to collect device information and provide network security for Chrome devices. Click on the **Chrome Devices** button, then click on the **Google Workspace Settings** button at the top of the Inventory List to bring up the Google Workspace Settings window and configure the connection to the Google Workspace Service. Complete the fields as described below, then click on the **OK** button.

- **Google Workspace User -** The Google Workspace username (e.g., <user key name>@<project Id>.gserviceaccount.com).
- **Service Account E-Mail -** The E-Mail of the user account with permission to access scope https://www.googleapis.com/auth/admin.directory.device.chromeos.readonly.

- **Access Key -** Download the Google Workspace Access Key to your computer. Click on the **Browse** button to locate the key. The Access Key is a generated P12 format key (IAM & Admin > Service Account in https://console.cloud.google.com/home/dashboard).
- **Auto Sync Interval -** The interval for OmniVista to perform a data sync with Google Workspace, in hours. You can also click on the **Sync With Google Workspace Now** button at the top of the Inventory List at any time to perform an immediate sync. (Range = 1 - 24, Default = 3).
- **Enable Google Workspace Based Categorization -** Check this box if you want Chrome devices to be categorized based on data from Google Workspace, otherwise, devices will be categorized based on the OmniVista IoT application.

Configuring OmniVista for Zigbee Support

OmniVista can be used to monitor and enable/disable Zigbee devices (e.g., Assa Abloy door locks). OmniVista interfaces with a Zigbee Server and Zigbee-enabled Stellar APs to support these devices. Configuring OmniVista for Zigbee support consists of the following steps:

1. Configure the connection between OmniVista and the Zigbee Server.

- Go to the IoT/Location Server Screen (Network - AP Registration - Access Points IoT/Location Server) and add the Assa Abloy Zigbee Server. See the IoT/Location Server Help for more information. Note that OmniVista must be able to connect to the Zigbee Server, which in installed onsite at the customer location (e.g., Hotel).

2. Enable/configure Zigbee Mode on Stellar APs.

- Zigbee Mode must be enabled and configured on an AP(s) (at the AP Group Level) for the AP(s) to discover and connect to Zigbee devices. Zigbee is enabled on an AP Group by setting the IoT Radio Mode to "Zigbee" and the IoT/Location Server Profile to the Assa Abloy Server you added on the IoT/Location Server Screen. Go to the AP Group Screen (Network - AP Registration - AP Group) to configure an AP Group for Zigbee. You can then add the APs that you want to use for Zigbee devices to the AP Group. See the he AP Group Help for more information.

It is recommended that you configure APs for Zigbee support at the AP Group level. However, you can configure it on an individual AP by selecting the AP in the Access Points List and editing the "IoT Radio Configuration. See the Access Points Help for more information.

3. Enable Zigbee on the Zigbee device.

- Once Zigbee Mode is enabled/configured on APs, Zigbee devices are automatically discovered and appear in the IoT Zigbee Device Table. However, you must enable Zigbee on the Zigbee device. Select the device and click on the **Accept** button at the top of the table.

Assigning a Custom Category to a Device

You can override the Default Category assigned to a device through Fingerprinting and manually assign a Custom Category to a device. Select the device(s) in the Inventory List and click on the **Assign Category** button. The Assign Category - Confirmation window appears. Select a Custom Category from the **Choose Category** drop-down, then click on the **Assign** button. The selected device(s) will appear in the Inventory List with the new Custom Category name. Note that if Enforcement was configured for the assigned Category, endpoints might

change their UNP mapping to the UNP that mapped with new category, or to no enforcement if the new category has no UNP mapping.

To remove an assigned Custom Category from a device and return it to its Default Fingerprinting Category, edit the Custom Category to remove the device. Go to the Category Screen, select the Custom Category, and click on the Edit icon. Any devices to which you have manually assigned the Custom Category will be listed by MAC Address in the MAC Based Field. Click on the "X" next to the device(s) that you want to remove, and click on the **Apply** button. The device(s) will again be categorized by its Default Fingerprinting Category and the device(s) will be displayed in the Inventory List with its Default Fingerprinting Category.

> **Note:** Deleting a Custom Category will return all devices in that Category to their Default Fingerprinting Category.

Category

The IoT Category Screen displays information about device categories, and is used to create, edit, and delete custom categories. OmniVista monitors network packets to determine the types of devices connected to the network and interfaces with a Device Fingerprinting Service to categorize them. Categories are hierarchical. Default Categories are the top-level categories and are provided and listed by default. When a device is initially categorized, it will be assigned one of these top-level categories (e.g., Phone, Tablet or Wearable). As OmniVista monitors packets and learns more about a device, the category assigned to the device will become more specific. For example, a device may initially be categorized as "Phone, Tablet or Wearable". As OmniVista learns more about the device, the device may be categorized as an "Apple Mobile Device", and then an "Apple iPhone". As OmniVista learns these new categories, they are added to the List of Categories. You cannot edit or delete the Default Categories, but you can configure Custom Categories based on the category hierarchies that have been detected.

> **Important Note:** There are network prerequisites and configuration steps that **must** be completed to enable IoT. See the IoT Overview Online Help for an overview of the application including prerequisites.

Creating a Custom Category

Click on the Add icon at the top of the Category List to bring up the Create Custom Category window. Complete the fields as described below, then click on the **Create** button.

- **Category Name -** A name for the Custom Category.
- **Description -** An optional description for the category.
- **Mapping Conditions** - You can create a Custom Category based on an existing category (Hierarchy Based) or create a Custom Category based on MAC Address (MAC Based).
- **Hierarchy Based -** Click on the **Add/Remove** button to bring up a list of categories. Only those category hierarchies that have been detected and displayed on the Inventory Screen are displayed for selection. Add/Remove categories to create the Custom Category.
- **MAC Based -** Enter a MAC Address and click on the Add icon (+). Repeat to add additional MAC Addresses. Click on the Delete icon (x) to remove a MAC Address from the Custom Category.

The new Custom Category will appear at the bottom of the Category List. The Custom Category will be displayed for any online devices in the Inventory List matching the new category.

Editing a Custom Category

Select a category and click on the Edit icon at the top of the Category List. Edit the fields as described above, then click on the **Apply** button. Note that you cannot edit a Default Category.

Deleting a Custom Category

Select a category(ies) and click on the Delete icon at the top of the Category List. Click **OK** at the Confirmation Prompt. Any devices matching the deleted Custom Category in the Inventory List will revert to the applicable default category.

Category List

- **Category Name -** The name of the Default or Custom Category.
- **Type -** The type of category (Default/Custom).
- **Description -** A description for the Custom Category.
- **Mapping Conditions** - The category hierarchy substring used for categorizing the Custom Category.

Enforcement

The IoT Enforcement Screen is used to configure category-based device authentication. OmniVista monitors network packets to determine the types of devices connected to the network and interfaces with a Device Fingerprinting Service to categorize them. The IoT Enforcement feature enables you to authenticate devices by associating a Category with an Access Role Profile. Once a device accesses the network and is categorized, the assigned Access Role Profile is applied to the device. You can associate different Access Role Profiles with different categories; and you can enable automatic or manual enforcement Categories.

You can also specify exceptions for specific devices by SSID, MAC address, AP Group, or IP address. When a device matching one of these exceptions is categorized, it will not be subject to IoT enforcement configured for its category.

Important Note: There are network prerequisites and configuration steps that **must** be completed to enable IoT. See the IoT Overview online help for an overview of the application including prerequisites.

Configuring IoT Enforcement

The Enforcement Screen lists all Default and Custom IoT Categories. IoT Enforcement is automatically enabled for all Categories by default (the **Automatic Enforcement** button at the top of the screen is set to "On"). However, you can manually enable/disable IoT Enforcement on specific Categories.

Automatic IoT Enforcement

If necessary, set the **Automatic Enforcement** button at the top of the screen to "On". Assign an Access Role Profile to a Category(ies) as described below. Configured Access Role Profiles for a Category will automatically be applied to any device that matches the Category. If a Category is not assigned an Access Role Profile, there will be no IoT Enforcement for that Category.

> **Note:** If you change Automatic Enforcement from "On" to "Off", enforcement will continue for any device on which enforcement was previously enabled, unless you

manually disable enforcement for the Category used for the device, or if the device re-initializes or roams to another switch/AP. If you change Automatic Enforcement from "Off" to "On", Automatic Enforcement will only be applied to devices that connect to the network and match a configured Enforcement Category after you enable Automatic Enforcement. If you delete a Category/ARP mapping, the new mapping configuration will be applied the next time an endpoint reconnects to a switch/AP.

Manual IoT Enforcement

If Automatic Enforcement is disabled (Off), Access Role Profiles assigned to Categories are not applied to devices. However, you can manually enable IoT Enforcement for specific Categories. With the **Automatic Enforcement** button at the top of the screen set to "Off", select a Category(ies) and click on the **Enable Enforcement** button at the top of the Category List. The Enable Enforcement window will appear. Review the Categories in the Enable Enforcement column and click on **OK**.

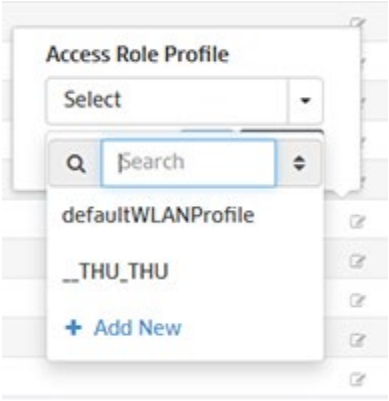
Assign an Access Role Profile to a Category(ies) as described below. The Access Role Profile will be applied to any device that matches the Category.

Note: Manual Enforcement is applied to currently-connected clients only. If Automatic Enforcement is "Off", you must apply enforcement manually whenever IoT-based enforcement is desired.

Note: After enabling manual enforcement for a Category(ies), if an endpoint roams to another switch/AP or re-initializes, there will be no IoT Enforcement for that Category. You must disable Enforcement of the Category and enable it again to apply IoT enforcement manually to currently-connected endpoints.

Assigning an Access Role Profile to a Category

Click on the Edit icon to the right of the Access Role Profile column to bring up the Access Role Profile drop-down menu. Click on the drop-down to bring up a list of all configured Access Role Profiles, select a profile and click **OK**. The assigned Access Role Profile will be displayed in the Access Role Profile column next to the Category.



You can also click on "Add New" to go to the Access Role Profile Scree and create a new profile. Once the profile is created, return to the IoT Enforcement Screen and select the new profile.

Important Note: The Access Role Profile must exist on the switches/APs connected to the endpoint devices. If you are creating a new Access Role Profile, you must first assign the profile to any applicable switch(es)AP Group(s) before assigning it to a

Category in the IoT application. See the Access Role Profile online help for more information on creating and assigning Access Role Profiles.

Editing an Access Role Profile Assignment

You can change the Access Role Profile assigned to a Category at any time. Click on the Edit icon to the right of the Access Role Profile column and follow the procedure above to assign a new Access Role Profile.

Deleting an Access Role Profile Assignment

You can delete an Access Role Profile assignment at any time. Click on the Delete icon to the right of the Access Role Profile column, then click OK at the Confirmation Prompt. The Category will move to the bottom of the list and will no longer have an assigned Access Role Profile. You can later assign an Access Role Profile at any time.

Configuring IoT Enforcement Exceptions

You can specify exceptions for specific devices by SSID, MAC address, AP Group, or IP address. When a device matching one of these exceptions is categorized, it will not be subject to IoT enforcement configured for its category. To create IoT Enforcement exceptions, click on the **Exception List** button at the top of the screen to bring up the Exception List Screen. Add SSID(s), MAC address(es), AP Group(s), or IP address(es) to the exception list as described below and click on the **Apply** button.

The Summary at the top of the Exception List displays the number of SSID(s), Endpoint MAC(s), AP Group(s), and Switch(es)/APs that have been added to the Exception List. Click on one of the items or scroll down to add/remove devices from the Exception List.

Note: If an endpoint is initially configured for Enforcement and later added to the Exception List, the endpoint can remain assigned to the Enforcement UNP because the switch/AP will cache the Enforcement UNP and reapply it to the endpoint if it reconnects. To add a device that was assigned to an Enforcement UNP to the Exception List, first remove Enforcement from the endpoint, then add it to the Exception List.

SSID(s)

To add devices associated with an SSID to the Exception List, click on the **Change Selection** button to bring up the SSID Selection window. Select an SSID(s) and click on the **Add** button, then click on **OK** to add the SSID(s) to the Exception List. To remove an SSID(s) click on the **Change Selection** button to bring up the SSID Selection window. Select an SSID(s) and click on the **Remove** button, then click on **OK** to remove the SSID(s) from the Exception List.

Endpoint MAC(s)

To add devices by MAC address to the Exception List, input a device MAC Address and press **Enter** to add it to the Exception List. To remove a device, click on the "Selected Endpoint MAC(s) link to bring up the Endpoint Selection window. Select a device MAC address(es) and click on the **Remove** button, then click on **OK** to remove the devices(s) from the Exception List.

AP Group(s)

To add devices associated with APs in an AP Group to the Exception List, click on the **Change Selection** button to bring up the SSID Selection window. Select an SSID(s) and click on the **Add** button, then click on **OK** to add the AP Group(s) to the Exception List. To remove an AP

Group(s) click on the **Change Selection** button to bring up the AP Group Selection window. Select an AP Group(s) and click on the **Remove** button, then click on **OK** to remove the AP Group(s) from the Exception List.

Switch/AP(s)

To add devices by IP address to the Exception List, click on the **Change Selection** button to bring up the Device Selection window. Select a device(s) and click on the **Add** button, then click on **OK** to add the device(s) to the Exception List. To remove a device(s) click on the **Change Selection** button to bring up the Device Selection window. Select a device(s) and click on the **Remove** button, then click on **OK** to remove the device(s) from the Exception List.

Settings

The IoT Settings Screen is used to configure IoT data retention preferences. Set the fields as described below, then click on the **Apply** button.

IoT Configuration

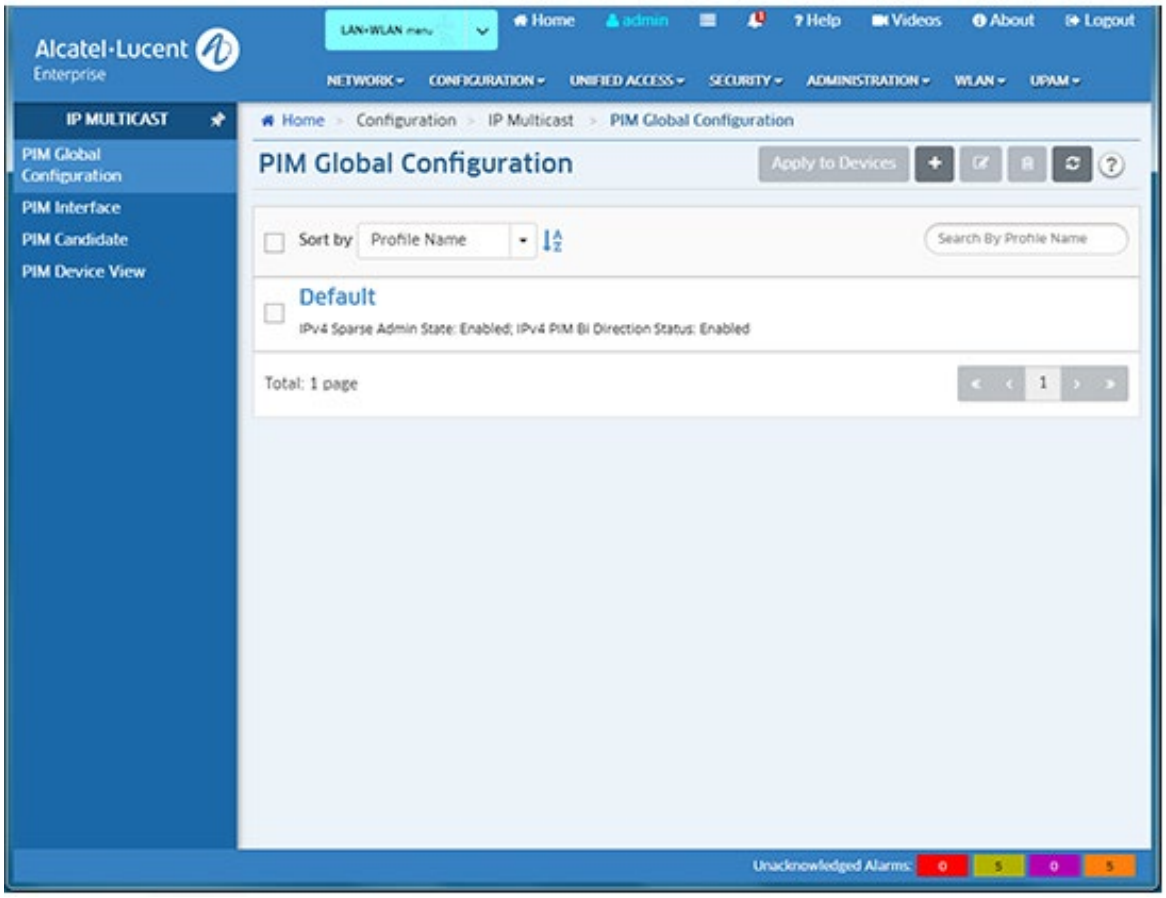
- **Days Before Purge -** The number of days an endpoint device record will be kept if there are no updates for the device (Range = 1 - 60, Default = 30).
- **Historical Records Count -** The number of historical records retained for an endpoint switch/AP combination (Range = 0 - 25, Default = 2).
- **Total Records -** The total number of IoT records OmniVista will store in the database. Records above the threshold are purged. Historical records are purged first, followed by offline records (Range = 1 - 500,000, Default = 100,000).

16.0 IP Multicast (PIM)

Protocol-Independent Multicast (PIM) is an IP multicast routing protocol that uses routing information provided by unicast routing protocols. Creation of Multicast VXLAN Services requires PIM configuration on devices in the VXLAN. The following screens are used to configure and view PIM configuration on the network:

- **PIM Global Configuration -** Used to configure PIM configuration profiles, which can be applied to switches on the network.
- **PIM Interface -** Used to configure a PIM interface(s) on a switch(es).
- **PIM Candidate -** Used to configure Candidate Bootstrap Routers (C-BSRs) and Bootstrap Routers (BSRs).
- **PIM Device View -** Used to view PIM configurations on network switches.

PIM



PIM Global Configuration

The PIM Global Configuration Screen displays all configured PIM Global Profiles and is used to create, edit, assign, and delete PIM Global Profiles. The Global Profile enables PIM on the switch, and configures basic PIM parameters.

Creating a PIM Global Profile

Click on the Add icon. Configure the profile as described below, then click on the **Create** button.

- **Profile Name -** User-configured profile name.
- **IPv4 Sparse Admin State -** Enables/Disables PIM-Sparse Mode (SM) protocol on the switch.
- **IPv4 PIM Bi Direction Status -** Enables/Disables Bi-Directional PIM on the switch.

Note: You can configure up to four (4) PIM Profiles; however, two profiles cannot have the same values. For example, two profiles cannot be configured with both Sparse Mode and Bi-Directional status enabled, or with both disabled.

Editing a PIM Global Profile

Select the profile and click on the Edit icon to bring up the Update PIM Global Configuration Screen. Edit the fields as described above then click on the **Update** button to save the changes to the server. The configuration will be applied and the status displayed on the Action Results Screen. Click the **Finish** button to return to the PIM Global Configuration Screen. Note that you cannot edit the Profile Name.

Note: Two profiles cannot have the same values. For example, two profiles cannot be configured with both Sparse Mode and Bi-Directional status enabled, or with both disabled.

Assigning a PIM Global Profile

Select a profile and click on the **Apply To Devices** button. Select an option (Use Switch Picker/Use Topology) and select the switch(es) to which you want to apply the profile and click the **Apply** button. The configuration will be applied and the status displayed on the Action Results Screen. Click the **Finish** button to return to the PIM Global Configuration Screen.

Removing a PIM Global Profile

To remove a profile from a switch(es), select the profile and click on the **Apply To Devices** button. Select the switches from which you want to remove the profile and click on the **Apply** button. The removal resets the values of Spare Admin State and Bi-Direction Status to "Disable".

Deleting a PIM Global Profile

To delete a Profile(s), select the Profile(s) in the table and click on the Delete icon, then click **OK** at the confirmation prompt. The configuration will be applied and the status displayed on the Action Results Screen. Click the **Finish** button to return to the PIM Global Configuration Screen.

Note: You can delete non-default profiles even the profile was assigned to switch. The deletion resets the values of Spare Admin State and Bi-Direction Status to "Disable". Also note that you cannot delete Default PIM profile, you can only remove the profile from the switches.

PIM Interface

The PIM Interface Screen is used to display information about configured PIM interfaces and to create or delete PIM interfaces. After enabling PIM on a switch by applying a PIM Global Profile, you must configure an IP interface as a PIM interface to enable multicast routing for VXLANs. An interface can be any IP router interface that has been assigned to an existing VLAN.

Displaying PIM Interfaces

You can view configured PIM interfaces by searching for PIM interfaces on a device(s) or by searching for specific PIM interface by name. Select a search option from the Search by drop-down menu (**Device** or **Interface**), then click on the **Select Devices** or **Select Interface** button to select the device(s)/interface(s) you want to view and click **OK**. If you select multiple devices, PIM interfaces common to those devices are displayed.

> **Note:** The status of the PIM interface may not reflect the actual status of the interface on the switch. For example, PIM Enabled may show "false" instead of "true". The PIM interface status is not synchronized with the switch.

Creating a PIM Interface

Click on the Add icon. The Configure PIM Interface Screen appears. Select an option from the drop-down menu (Use Switch Picker/Use Topology) and click on the **Add/Remove Devices** button and select a device(s). If you select a single device, all IP interfaces configured on the device are displayed. If you select multiple devices, only those interfaces common to all selected devices are displayed. Select an interface and click the **Create** button. The configuration will be applied and the status displayed on the Action Results Screen. Click **Finish** to return to the PIM Interface Screen.

> **Note:** If there are no IP interfaces configured on a device, or no common interfaces among multiple devices, click on the Add icon to bring up the VLANs application and configure the interface(s).

Deleting a PIM Interface

To delete an interface(s), select the interface(s) and click on the Delete icon, then click **OK** at the confirmation prompt.

PIM Candidate

The PIM Candidate Screen displays all configured PIM Candidate Profiles and is used to create, edit, and delete PIM Candidate Profiles. A PIM Candidate Profile is the Candidate Rendezvous Point (RP) Router and Candidate Bootstrap Router (BSR) configured on the switch. In PIM-SM, shared distribution trees are rooted at a common forwarding router, referred to as a Rendezvous Point (RP). The RP unencapsulates Register messages and forwards multicast packets natively down established distribution trees to receivers. The resulting topology is referred to as the RP Tree (RPT).

A Candidate RP Router is a PIM-enabled router that sends periodic Candidate RP advertisements to the Bootstrap Router (BSR). When a BSR receives a Candidate RP advertisement, the BSR may include the CRP in its RP-set.

The role of a Candidate BSR is to keep routers in the network up to date on reachable Candidate RPs. The BSR's list of reachable Candidate RPs is also referred to as an RP set. There is only one BSR per PIM domain. This allows all PIM routers in the PIM domain to view the same RP set. A Candidate RP periodically sends out messages, known as C-RP advertisements. When a BSR receives one of these advertisements, the associated Candidate RP is considered reachable (if it has a valid route). The BSR then periodically sends its RP set to neighboring routers in the form of a Bootstrap message.

A Candidate BSR is a PIM-enabled router that is eligible for BSR status. To become a BSR, a Candidate BSR must become elected. A Candidate BSR sends Bootstrap messages to all neighboring routers. The messages include its IP address, which is used as an identifier, and its priority level. The Candidate BSR with the highest priority level is elected as the BSR by its neighboring routers. If two or more Candidate BSRs have the same priority value, the C-BSR with the highest IP address is elected as the BSR.

Creating a PIM Candidate Profile

Click on the Add icon. Select an option from the drop-down menu (Use Switch Picker/User Topology) and click on the **Browse** button to select the device on which you want to configure the PIM Candidate Profile. Configure the Candidate RP and Candidate BSR as described below.

> **Note:** Devices will only be available/displayed if a PIM Interface has been configured on the device. If no PIM Interfaces have been configured, no devices will be available to create a PIM Candidate Profile.

- **Candidate RP**
- **Candidate RP Address -** The IP address that will be advertised as a Candidate-RP. The IP address must belong to a PIM enabled interface. Only one RP address is supported per switch. Select a PIM Interface from the drop-down list. You can also click on the Add icon to go to the PIM Interface Screen and configure a PIM Interface.
- **Candidate RP Group Address/Prefix Length -** The group address for which the local router will advertise itself as a Candidate-RP and prefix length of the multicast group.
- **Candidate RP Bidir -** Enables/Disables Bi-Directional mode.
- **Candidate BSR**
- **Candidate BSR Address -** The IP address of the Candidate BSR. Select a PIM Interface from the drop-down list. You can also click on the Add icon to go to the PIM Interface Screen and configure a PIM Interface.

Editing a PIM Candidate Profile

Select the profile and click on the Edit icon to bring up the Update PIM Candidate Screen. Edit the fields as described above then click on the **Update** button to save the changes to the server, and update the profile on the device(s).

Deleting a PIM Candidate Profile

To delete a profile(s), select the Profile(s) in the table and click on the Delete icon, then click **OK** at the confirmation prompt to remove the profile from the server and the device(s).

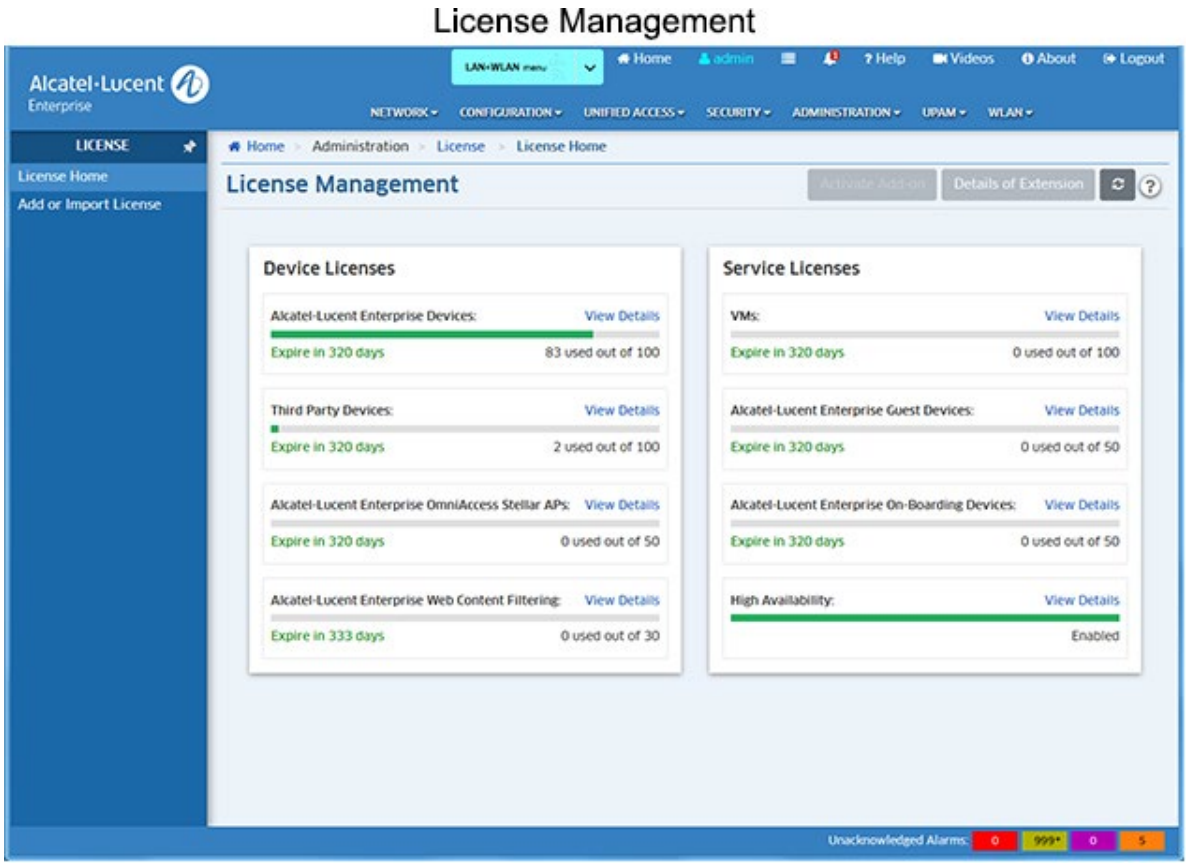
PIM Device View

The PIM Device View Screen is used to view PIM configurations on network switches. To view a configuration, select an option from the drop-down menu (Use Switch Picker/Use Topology), click on the **Browse** button, select a switch, and click **OK**. Click on a configuration setting (e.g., PIM Global, PIM Interface) to expand the view and see configuration details.

17.0 License Management

OmniVista 2500 NMS licensing is based on the license purchased. A user is allowed to manage up to the maximum number of devices allowed for that license. The License Home Screen (shown below) provides an overview of all current licenses. The Add or Import License Screen is used to import and activate a new license.

> **Note:** A free Demo License and a free Evaluation License are also available. See OmniVista Licensing Options for more information.



License Home Screen

The License Home Screen provides an overview of all licenses purchased and activated by the user. The information includes the number of devices currently being managed and the total number of devices that can be managed using the license. The number of days remaining before each license expires is also displayed. If the number of devices currently being managed is more than 90% of the total number of devices that can be managed with the current license, the bar graph is displayed in Red, otherwise, it is displayed in Green. If the license is within 30 days of expiring, the license information at the bottom of the bar graph is displayed in Red; otherwise, it is displayed in Black.

Click on the "View Details" link for any license to view additional license information:

- **Unit -** The type of device managed by the Node Management License (e.g., ALE Devices, Third Party Devices, ALE Guest Devices).
- **Max Count -** The maximum number of the devices that can be managed with the current license.
- **Available -** The number of devices still available on the current license.
- **Usage -** The percentage of the maximum number of devices currently being managed. If the number of devices currently being managed exceeds 90 percent of the maximum number allowed on the license, the bar graph is displayed in Red; otherwise, it is displayed in Green.

The number of devices that can be managed with each license is determined by the License Key that the user is given and enters at installation. A new license can be imported and activated using the Add/Import Screen. There are also licensing options that can be used to demo an application before purchasing a full Production License.

> **Note:** If no Node Management License available in OmniVista, only the Add/Import Screen is displayed.

Licenses

There are two types of licenses that can be purchased - Device Licenses and Service Licenses.

- **Device Licenses -** Licenses a user to manage a specific number of devices.
- **Alcatel-Lucent Enterprise Devices -** Licenses ALE devices (e.g., OS10K, 6900, 6860).
- **Third Party Devices -** Licenses third-party devices (e.g., Cisco).
- **Alcatel Lucent Enterprise OmniAccess Stellar APs -** Licenses OmniAccess Stellar Wireless Devices (e.g., OAW-AP1101, OAW-AP1201).
- **Alcatel Lucent Enterprise Web Content Filtering - Licenses** a user to enable Web Content Filtering on Stellar APs
- **Service Licenses -** Licenses a user to manage a specific number of devices for the following services:
- **VMs -** Licenses Virtual Machines (VMs).
- **Alcatel Lucent Enterprise Guest Devices -** Licenses Stellar AP guest devices.
- **Alcatel-Lucent Enterprise On-Boarding Devices -** Licenses Stellar AP on-boarding devices. High Availability - Licenses the OmniVista High Availability Feature.
- **High Availability -** Licenses the OmniVista High Availability Feature.

  Note: If you purchase additional licenses or license extensions through your Business Partner, the **Activate Add-On** button at the top of the screen will be activated. Click on the button to activate the licenses. If you do not click on the button, the new licenses/extensions will automatically be activated when older licenses expire. If you purchase a license extension, the **Detail of Extension** button will be activated. Click on the button to see when the extension will be applied.

Device Licenses

Alcatel-Lucent Enterprise (ALE) Devices

Licenses a specific number of ALE devices (e.g., OS10K, 6900, 6860) that can be managed. OmniVista has been certified to manage up to 10,000 devices (includes AOS and Third-Party Devices).

Third Party Devices

Licenses a specific number of third-party devices (e.g., Cisco) that can be managed.

Alcatel Lucent Enterprise (ALE) OmniAccess Stellar APs

Licenses a specific number of OmniAccess Stellar Wireless Devices (e.g., OAW-AP1101, OAW-AP1201) that can be managed. The license enables a user to manage a specific number of Stellar Access Points (APs). The following licenses are available:

- 10 APs
- 20 APs
- 50 APs
- 100 APs
- 500 APs.

Web Content Filtering

Licenses a specific number of Stellar APs for the Web Content Filtering feature. The following licenses are available:

- 10 APs
- 20 APs
- 50 APs
- 100 APs
- 500 APs.

Service Licenses

VMs

Licenses the number of Virtual Machines (VMs) that can be managed. VMs can be deployed on vCenters and Hyper-V Servers; and OmniVista supports a mixture of Hypervisor types. The OmniVista VM Manager application supports up to 5,000 VMs. More than 5,000 Virtual Machines are allowed; however, a warning message will be displayed and an entry will be written to the VMM Log File.

Alcatel Lucent Enterprise (ALE) Guest Devices

Licenses the number of Stellar AP guest devices that can be managed simultaneously. The following licenses are available:

- 10 Guest Devices

- 20 Guest Devices
- 50 Guest Devices
- 100 Guest Devices
- 500 Guest Devices
- 1000 Guest Devices.

Alcatel-Lucent Enterprise (ALE) On-Boarding Devices

Licenses the number of Stellar AP on-boarding devices that can be managed. The following licenses are available:

- 10 Devices
- 20 Devices
- 50 Devices
- 100 Devices
- 500 Devices
- 1000 Devices.

High Availability

Licenses the OmniVista High Availability Feature, which enables OmniVista to operate in High-Availability Mode. The High Availability License enables you to create a primary and secondary OmniVista Server on separate Virtual Machines. If the primary server fails, the secondary server takes over with minimal downtime.

Add/Import a New License

New Licenses are imported and activated using the Add/Import Screen. Note that you cannot downgrade a Node Management License or a VMM License. Also, make sure that the new license you are using will be adequate to manage the number of devices you were managing with the older version of OmniVista. If you are managing more devices than are allowed on your new license, you many lose some discovered devices.

OmniVista Licensing Options

There are three (3) types of OmniVista Licenses:

- **Starter Pack -** Is free and enables you to use OmniVista (Node Management, VMM) on a limited basis. This license comes with OmniVista and is available "out of the box".
- **Evaluation -** Is free and gives you full use of OmniVista (Node Management, VMM), but for a limited time. This license must be downloaded from Alcatel-Lucent Customer Support.
- **Production -** Gives you full use of OmniVista without expiration.

Device License Options

	Starter Pack	Evaluation	Production
Device Count	30 (10 AOS, 10 Third Party, 20 Stellar AP)	Chosen at license generation (full OV functionality)	Chosen at license generation (full OV functionality)
Expires	No	60 Days	No

Service License Options

	Starter Pack	Evaluation	Production
VMs	10	100	Chosen at license generation (full VMM functionality)
ALE Guest Devices	10	20	Chosen at license generation (full VMM functionality)
ALE On-Boarding Devices	10	20	Chosen at license generation (full VMM functionality)
Expires	No	60 Days	No

Note: The High-Availability License is only available as a Production License. It does not expire.

Important Notes for Updating Licenses

The following rules apply when updating Alcatel-Lucent Enterprise Node Management Licenses and VMM Licenses:

Production License to Production License

- If the device count of the existing Production License is less than or equal to that of the new Production License, the update is allowed without any warning prompt.
- If the device count in the existing Production License is greater than that of the new Production License:
  - If the current number of discovered devices is less than or equal to the device count of the new Production License, the user can update to the new Production License after a confirmation prompt.
  - If the current number of discovered devices is greater than the device count of the new Production License, the user is prompted to reduce the number of devices to be less than or equal to the count of the new Production License. The user can then update to the new Production License after user confirmation.

Non-Expired Evaluation License to Production License

- If the device count of the non-expired Evaluation License is less than or equal to that of the Production License, the update is allowed without any warning prompt.

- If the device count of the non-expired Evaluation License is greater than that of the Production License:
  - If the current number of discovered devices is less than or equal to the device count of the Production License, the user can update to the Production License after a confirmation prompt.
  - If the current number of discovered devices is greater than the device count of the Production license, the user is prompted to reduce the number of devices to be less than or equal to the count of the Production License. The user can then update to the Production License after user confirmation.

Expired Evaluation License to Production License

- If the device count of the expired Evaluation License is less than or equal to that of the Production License, the update is allowed without any warning prompt.
- If the device count of the expired Evaluation License is greater than that of the Production License:
  - If the current number of discovered devices is less than or equal to the device count of the Production License, the user can update to the Production License after a confirmation prompt.
  - If the current number of discovered devices is greater than the device count of the Production license, contact Customer Support.

Non-Expired Evaluation License to Starter Kit License

- If the device count of the non-expired Evaluation License is equal to 10, the update is allowed.
- If the device count of the non-expired Evaluation License is greater than 10, contact Customer Support.

Expired Evaluation License to Starter Kit License

- If the device count of the expired Evaluation License is equal to 10, the update is allowed.
- If the device count of the expired Evaluation License is greater than 10, contact Customer Support.

Expired Evaluation License to Non-Expired Evaluation License

- If the device count of the expired Evaluation License is equal to or less than the device count of non-expired Evaluation License, the update is allowed.
- If the device count of the expired Evaluation License is greater than the device count of non-expired Evaluation License, contact Customer Support.

Production License to Evaluation License

- This is considered a downgrade and is not allowed.

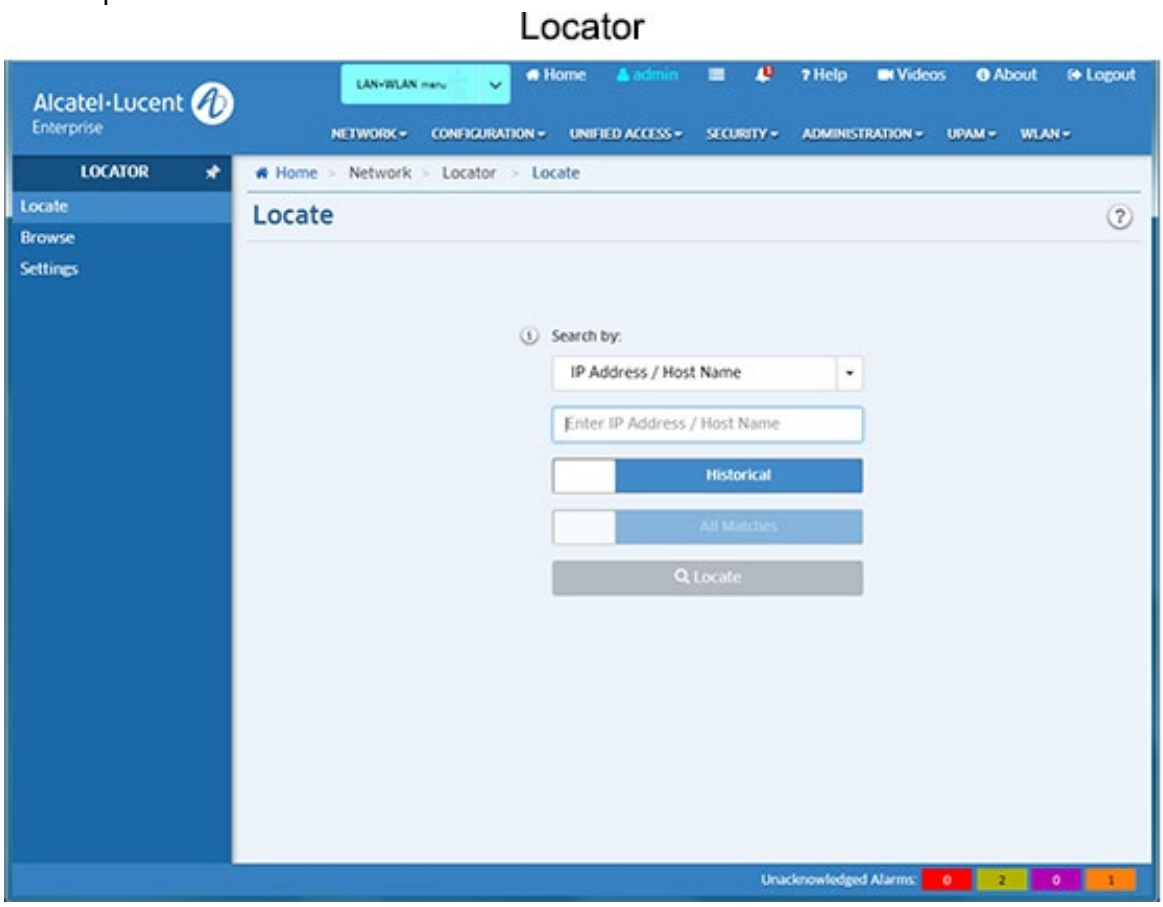
Add or Import License

The License Add or Import License Screen is used to activate a license, either by importing a license file, or entering a license key(s). To import a License File (.dat), download the file, then click on the **Download** icon, locate the file, import the file, then click on the **Submit** button. To activate a file using the license key, enter the license key in the License Key field. Note that you can enter multiple license keys. Each key must be entered on a new line (after entering a key, hit **Enter** to enter another license key). When you are done entering license keys, click on the **Submit** button.

18.0 Locator

The Locator application is a search tool within OmniVista. There are four (4) screens in the Locator application (accessed by clicking on the link on the left side of the screen) that are used to perform different functions:

- The **Locate** screen enables you to locate the switch and slot/port that is directly connected to a user-specified end station. You can enter the end station's IP address or Host Name, MAC address, or Authenticated User ID to locate the switch and slot/port to which the end station is connected. Locator can perform a "Historical" search or a "Live" search. A "Historical" search is performed by searching a database of information that was previously established by polling network switches. A "Live" search, as its name implies, is performed by searching network switches in real time.
- The **Browse** screen enables you to search in the "opposite direction" of the **Locator** screen. Instead of entering an end station's address to locate the switch and slot/port to which the end station is connected, the **Browse** screen enables you to search for and list all end stations connected to user-specified switch ports. The end stations are located by searching the Historical database. Locator cannot perform live searches from the **Browse** screen.
- The **Settings** screen is used to set Locator timeout values and data retention policies.



Note: The Locator application supports IPv4 addresses only. IPv6 is not supported.

Locator Screen

To locate a switch, select a category from the Search by drop-down list, and enter the corresponding search criteria below (IP Address/Host Name, MAC Address, or Authenticated User ID). Choose to perform a Historical or Live search by clicking on the slider, then click **Locate**.

Although you can enter an end station's IP address, host name, MAC address, or Authenticated User ID to locate the switch and slot/port that is directly connected to the end station, Locator actually searches for the end station's MAC address. If you enter an IP address, host name, or Authenticated User ID, the first thing Locator does is find the corresponding MAC address. This MAC address is displayed in the search results, with a time stamp. The time stamp informs you how current the information is, which is especially important when performing historical searches. Locator then uses the MAC address to search for the switches, slots, and ports associated with the MAC. These are the final search results.

Whether performing a live search or a historical search, success in locating an end station depends on accurate topology information about switch-to-switch links. This information can be gathered using the Discovery application to discover new devices or re-discover existing devices; or by manually creating links using the Discovery - Link Screen.

Search Type

You can perform a Historical search or a Live search. As stated earlier, A "Historical" search is performed by searching a database of information that was previously established by polling network switches. A "Live" search, as its name implies, is performed by searching network switches in real time. The search process for each type is described below.

Historical Search

If a Historical search is performed, Locator first checks the list of Discovery Inventory List determine if the IP address, host name, or MAC address entered matches that of a known switch. If it does, a message is displayed informing the user and no further search is performed. If the IP address, host name, or MAC address entered does not to match a known switch, Locator assumes that the address is that of an end station and continues the search.

Live Search

If a Live search is performed, Locator will find all switches/slots/ports that meet the following criteria: the address entered was seen at the switch/slot/port, and the switch/slot/port is NOT connected to another switch device. If you select **1st Match Only**, only the first such switch/slot/port will be found. In most cases - as long as the network administrator has confidence in the consistency of the network's configuration - this result will be sufficient to locate the end station. If it is suspected that the first match may not be completely accurate, selecting **All Matches** will cause all switches/slots/ports that meet the criteria to be found and displayed. Locator performs the search based on the search criteria entered, as described below.

For a Live Search, the Discovery Inventory List must contain switches that are supported by OmniVista (Alcatel-Lucent Enterprise and Third-Party). Every effort has also been made to support third-party devices, but that support is not guaranteed.

To successfully perform a live search for an IP address, the network's gateway device must be supported by OmniVista. Otherwise, Locator may not be able to resolve the IP address entered to a MAC address.

Locator searches for link information in the Topology database. This database must contain information about the links that exist between network switches. There are two methods of populating the Topology database with information about network links:

- Discover or re-discover devices using the Discovery application.
- Provide link information manually using the Discovery - Link Screen.

Search Results

When the search is complete, the search results are displayed in both an ARP Results Table and a Netforward Results Table. The ARP Results Table displays results matching the search criteria found in the ARP Table. The Netforward Table displays results matching the search criteria found in the Bridge Forwarding Tables.

Browse Screen

As stated earlier, the Browse screen enables you to search for and list all end stations connected to user-specified switch ports. The end stations are located by searching the Historical database. Locator cannot perform live searches from the Browse screen.

To browse for an AOS Device(s), click on **Select Devices** at the top of the table, select a device(s) and click on **ADD**. To browse for Stellar AP Series Devices, click on **Select AP Groups**, select a group(s) and click on **ADD**. When you click **ADD**, the results will appear in the Netforward Results Table at the bottom of the screen. Click on ADD MORE to select and browse for additional devices.

Settings Screen

The Settings screen is used to set Locator timeout values and data retention policies.

Locate

The Locator Locate Screen enables you to locate the switch and slot/port that is directly connected to a user-specified end station. You can enter the end station's IP Address, Host Name, MAC Address, or Authenticated User ID to locate the switch and slot/port to which the end station is connected. Locator can perform a "Historical" search or a "Live" search. A "Historical" search is performed by searching a database of information that was previously established by polling network switches. A "Live" search, as its name implies, is performed by searching network switches in real time.

Locating a Switch

Select the type of search you want to perform from the Search by drop-down menu (IP Address/Host Name, Auth. User, MAC Address/Host Name) and the search criteria as described below. The search results are described below.

- **Search by -** Select IP Address/Host Name, MAC Address, or Authenticated User ID from the drop-down list, then enter the search criteria.

- **Historical/Live Search -** Click on the slider to select a **Historical** Search or a **Live** Search. If you are performing a Live search, select **1st Match Only** to display only the first match found. (Note that OmniVista will stop searching after at least one match is found; however more than one match may be displayed.) As long as the network administrator has confidence in the consistency of the network's configuration, this result will be sufficient to locate the end station. If it is suspected that the first match may not be completely accurate, select **All Matches** to display all switches/slots/ports that meet the selected criteria.

Note: To locate a device in a Live Search, the device must be "Live" (active on the network within the last 5 minutes). "Live" is defined by the timeout defined by the switch (5 minutes). Also note that Live Search does not search for wired or wireless clients connected to Stellar APs. Stellar APs are not polled during a Live Search.

Search Results

When the search is complete, the search results are displayed in both the ARP Results Table and the Netforward Results Table. The ARP Results Table displays results matching the search criteria found in the ARP Table. The Netforward Table displays results matching the search criteria found in the Bridge Forwarding Tables.

When searching by IP address, the Netforward Results Table includes results for all client MAC addresses associated with an IP address in the ARP history. This is an effective method for finding duplicate IP addresses. The Timestamp in the Netforward Results table is the time the MAC address was reported in the Device (switch or AP) MAC address table. Since the Netforward Results Table displays MAC addresses associated at any time with the IP address, the current IP address for each MAC address may be different than the search IP address.

Note: You can use the "Freeze the first __ columns" feature to lock columns when you scroll right to view information. Enter the number of columns you want to freeze, and those columns will remain visible as you scroll right.

You can also perform certain actions on specific devices/ports in the Netforward Results Table. Select a row in the table and click on the **Action** button at the top of the table and select one of the following options:

- **Locate On Map -** Launch the Topology application and display the selected device in Topology map view.
- **Quarantine Manager -** Launch the Quarantine Manager application for the selected MAC address.
- **Port -** Update the port status in the table, or enable/disable the selected port.
- **Show ClearPass Authentication -** Launch the Authentication Records Screen in the Premium Services (BYOD) application for the selected MAC address. This option is only available if a ClearPass Server is configured and connectivity can be established.
- **Show Access Guardian Diagnostics -** Launch the Diagnostics Screen in the Unified Profile application for the selected MAC address.

Note: If the device you are searching for is a switch and not an end station, a notification will appear and you can click on the Locate on Map button to launch the Topology application and display the selected device in Topology map view.

ARP Results Table

In the ARP Results Table, Locator reports information for the end station you are searching on. Note that if you make changes to a switch's VLAN configuration, or if you make hardware changes (such as replacing a board), the results in the Initial Lookup area may not be correct. Before using Locator, re-poll such switches using the **Poll** Screen. This will ensure that the ARP tables are populated with current information. The ARP Results Table fields are defined below.

When searching by IP address, the ARP Results Table provides information on only the IP address in the search query. When searching by MAC address, the ARP Results Table provides information on all IP addresses associated over time with the MAC address entered in the search query. This is helpful for tracking changes in the client device IP address over time, and in conjunction with the Netforward Results, can assist in the device location over time.

- **Client IP Address -** The IP address of the end station. This field is only applicable for the ARP Results Table. The Netforward Results Table only supports Historical Locate with IP Address.
- **Device IP Address -** The IP address of the device directly connected to the end station.
- **Device Name -** The name of the device directly connected to the end station.
- **MAC Address -** The MAC address of the end station connected to the device.
- **Timestamp -** The date and time the device was located.
- **End Station Name -** The DNS name of the end station device.
- **VPRN ID -** The VPRN ID of the device directly connected to the end station, if applicable. If multiple VRFs are configured on the device, the VRF ID is displayed. If none are configured (and if the feature is not available on the device), the column will display "Default", indicating that the switch is operating as a single routing instance.

Netforward Results Table

In the Netforward Results Table, Locator reports all switches/slots/ports that meet **both** of the following criteria: the MAC address entered when searching by MAC address, or all MAC addresses associated with an IP address when searching by IP address was/were seen at the switch/slot/port, **and** the switch/slot/port is **not** connected to another switch device.

The Netforward Results Table fields are defined below. The table display will vary depending on the view option you choose - Location (default), Classification, Data Center, or Template, which is used to create custom views. If a ClearPass Server is configured and connected, a BYOD button will appear to enable you to view information on the ClearPass Server.

Location

- **MAC Address -** The MAC address of the end station connected to the selected device.
- **Device IP Address -** The IP address of the device connected to the end station.
- **Device DNS -** The DNS Name of the device.
- **Device Name -** The user-configured device name.
- **Slot/Port -** The slot/port number on which the device was learned.
- **Port Alias -** The user-configured alias for the slot/port (configured on the device through the CLI).

- **Port Speed -** The port speed.
- **Port Admin Status -** The port administrative status (Up/Down).
- **Port Operational Status -** The administrative status of the port (Up/Down). A port is considered operational if the Admin Status is “Up” and the port is transmitting traffic.
- **Port Duplex Mode -** The port duplex mode (half duplex, full duplex, or auto duplex).
- **SSID -** The SSID of the device connected to the end station.
- **WLAN Service -** The WLAN Service used by the device, if applicable.
- **Physical Location -** The physical location of the device connected to the end station.
- **Timestamp -** The time the information was gathered.

Classification

- **MAC Address -** The MAC address of the end station connected to the selected device.
- **Auth User -** The 802.1x Authenticated User associated with the device connected to the end station, if applicable.
- **UNP -** The User Network Profile (UNP) that the device is associated with, if applicable.
- **ISID -** The ISID associated with the device.
- **Classification Source -** The Classification Policy by which the device was learned.

Data Center

- **MAC Address -** The MAC address of the end station connected to the selected device.
- **Service ID-** The Service ID associated with the device.
- **ISID -** The ISID associated with the device.

Template

You can create an additional two (2) custom views by clicking on the **Custom Template** button, entering a **Template Name**, selecting the fields you want to display and clicking **OK**. You can also change the order of the fields when you are creating the template by dragging fields up or down in the list before clicking **OK**. The name of the new view will then be displayed in a button at the top of the Netforward Results Table, and can be used to view the selected fields. You can configure up to 2 new views. Creating an additional view will replace one of the previous views. Custom templates are associated with the current logged in user, so every user can have different custom templates. The available fields are defined below.

- **Client IP Address -** The IP address of the end station. This field is only applicable for the ARP Results Table. The Netforward Results Table only supports Historical Locate with IP Address.
- **MAC Address -** The MAC address of the end station connected to the device.
- **Device IP Address -** The IP address of the device directly connected to the end station.
- **Time Stamp -** The time the information was gathered.
- **Domain -** The Layer 2 domain: VLAN, VPLS, SPB, EVB within the switches where the MAC is found.

- **Disposition -** The port disposition (e.g., Bridging/Filtering).
- **VLAN ID-** The VLAN associated with the port.
- **Slot/Port -** The slot/port number on which the device connected to the end station was learned.
- **Port Alias -** The user-configured alias for the slot/port (configured on the device through the CLI).
- **Port Admin Status -** The administrative status of the port (Up/Down).
- **Port Speed -** The port speed of the device connected to the end station.
- **Port Duplex Mode -** The port duplex mode (half duplex, full duplex, or auto duplex).
- **End Station Name -** The DNS name of the end station device.
- **Device DNS Name-** The DNS Name of the device.
- **Device Name -** The user-configured switch system name of the device connected to the end station.
- **Last Updated -** The last time the information in the table was updated.
- **Auth User -** The 802.1x Authenticated User associated with the device connected to the end station, if applicable.
- **VRF ID-** The VRF ID of the device directly connected to the end station, if applicable. If multiple VRFs are configured on the device, the VRF ID is displayed. If none are configured (and if the feature is not available on the device), the column will display "Default", indicating that the switch is operating as a single routing instance.
- **UNP -** The User Network Profile (UNP) that the device is associated with, if applicable.
- **Classification Source -** The Classification Policy by which the device was learned.
- **Service ID -** The Service ID associated with the device.
- **ISID -** The ISID associated with the device.
- **Chassis -** The chassis number for devices supporting the Virtual Chassis feature.

The fields below are only populated by devices authenticated through UPAM. Otherwise, the fields will be blank.

- **User Name -** The authentication information on the user who has logged in.
- **MAC Vendor -** The manufacturer of the network equipment based on the Organization Unique Identifier (OUI).
- **Category -** The category of the device (e.g., Computer, Mobile, Tablet).
- **Family -** The production vendor of the device (e.g., Alcatel-Lucent Enterprise, Apple, Microsoft)
- **CP End Station Name -** The ClearPass End Station name.
- **Host Name -** The port operational state (Up/Down).
- **Sponsor Name** - The Guest User sponsor.
- **Visitor Name -** The name of the Guest User.
- **Visitor Company -** The company of the Guest User.

- **Expires At -** The date and time when the Guest Account expires.
- **Certificate Valid From -**The date and time when the Guest Account was created.
- **Certificate Valid Up To -** The onboarding information of the date the certificate will expire.
- **User Type -** The User Type authenticated through the device (e.g., Employee, Guest).
- **BYOD Server -** The BYOD Server name.
- **BYOD Server Timestamp -** The time of the last recorded authentication activity.
- **SSID -** The SSID if the device.
- **WLAN Service -** The WLAN Service used by the device.
- **Authentication Type -** The authentication method used to authenticate the device (e.g., 802.1x, MAC)
- **Authentication Status -** The authentication status of the device. Note that for wireless users connected to Stellar APs, the results show online devices only - that is those devices that pass authentication and are connected to the network. Therefore, the authentication status will always be "success" for wireless clients connected to Stellar APs. If a client passes MAC authentication but does not perform Captive Portal authentication, the client is still considered online with a limited role. Therefore, the authentication status for the client will still be success.
- **Physical Location -** The physical location of the device.

BYOD

Available only if ClearPass Policy Manager (CPPM) is defined in the BYOD application and connectivity can be established.

- **User Type -** The BYOD/ClearPass User Type authenticated through the device (e.g., Employee, Guest). You can also place the mouse over the user to view detailed ClearPass user information. BYOD is only supported on Alcatel-Lucent Enterprise Switches running AOS 6.4.6.R01 and later, AOS 6.6.5.R01 and later, AOS 7.3.4.R02 and later, and AOS 8.1.1.R01 and later. Note that the connection to the CPPM Server and Database must be configured properly in the Unified Access application to gather the necessary information for this field.
- **ClearPass Server -** The ClearPass Server name.
- **IP Address -** The IP address of the ClearPass Server.
- **User Name -** CPPM endpoint authentication information on the user who has logged in.
- **Category -** CPPM endpoint profiling information on the class of device (e.g., Computer, Smart Device, Access Points, VoIP Phone).
- **Family -** CPPM endpoint profiling information on the device family (e.g., Windows, Apple, Alcatel, Unix).
- **CP End Station Name -** CPPM endpoint profiling information on the device name (e.g., Windows Vista/7/2008, Apple iOS Device, Alcatel IP Phone, Wireless AP).
- **Host Name -** CPPM endpoint profiling information on the Host Name.
- **Sponsor Name -** CPPM guest information on the sponsor.

- **Visitor Name -** CPPM guest information on the visitor's name.
- **Visitor Company -** CPPM Guest information on the visitor's company.
- **Expires At -** CPPM guest information on the date when authorization will end.
- **Cert Valid From -** CPPM onboarding information of the date the certificate was issued.
- **Cert Valid To -** CPPM onboarding information of the date the certificate will expire.
- **MAC Vendor -** The manufacturer of the network equipment based on the Organization Unique Identifier (OUI).
- **ClearPass Time Stamp -** The time of the last authentication activity recorded in ClearPass

Locate on Map

If the device you are searching for is a switch and not an end station, a notification will appear and you can click on the **Locate on Map** button to launch the Topology application and display a regional map in the Physical Network that contains the selected device. The device is automatically selected and centered in the map display.

Browse

The Locator Browse Screen enables you to search in the "opposite direction" of the **Locator** screen. Instead of entering an end station's address to locate the switch and slot/port to which the end station is connected, the Browse screen enables you to search for and list all end stations connected to devices. The end stations are located by searching the Historical database. Locator cannot perform live searches from the Browse screen.

To browse for an AOS Device(s), click on Devices **ADD** button and select a device(s). You can select up to 512 AOS Devices at a time. To browse for Stellar AP Series Devices, click on the AP Groups **ADD** button. When you click **ADD**, the results will appear in the Netforward Results Table at the bottom of the screen. To browse for different devices/AP Groups, click on the applicable **EDIT** button.

Note: Locator does not periodically poll clients connected to Stellar APs. When browsing for clients connected to APs, you must perform a manual poll by clicking on the link following the prompt at the top of the Netforward Results Table: "Not finding what you were looking for in the results? Click here". OmniVista will poll APs and display the most recent results in the table.

Browse Results

The browse results are displayed in the Netforward Results Table. The Netforward Results Table fields are defined below. The table display will vary depending on the view option you choose - Location (default), Classification, Data Center, Layer 3, or Template, which is used to create custom views. If a ClearPass Server is configured and connected, a BYOD button will appear to enable you to view information on the ClearPass Server.

Note: You can use the "Freeze the first __ columns" feature to lock columns when you scroll right to view information. Enter the number of colums you want to freeze, and those columns will remain visible as you scroll right.

You can also perform certain actions on specific devices/ports in the Netforward Results Table. Select a row in the table and click on the **Action** button at the top of the table and select one of the following options:

- **Locate On Map -** Launch the Topology application and display the selected device in Topology map view.
- **Quarantine Manager -** Launch the Quarantine Manager application for the selected device.
- **Port -** Update the port status in the table, or enable/disable the selected port.

Location

- **MAC Address -** The MAC address of the end station connected to the device.
- **Device IP Address -** The IP address of the switch to which the end station is connected.
- **Device DNS Name-** The DNS Name of the device.
- **Device Name -** The user-configured switch system name of the device connected to the end station.
- **Slot/Port -** The slot/port number on which the device connected to the end station was learned.
- **Port Alias -** The user-configured alias for the slot/port (configured on the device through the CLI).
- **Port Speed -** The port speed of the device connected to the end station.
- **Port Admin Status -** The port administrative status (Up/Down).
- **Port Operational Status -** The administrative status of the port (Up/Down). A port is considered operational if the Admin Status is “Up” and the port is transmitting traffic.
- **Port Duplex Mode -** The port duplex mode (half duplex, full duplex, or auto duplex).
- **VLAN ID-** The VLAN associated with the port.
- **Disposition -** The port disposition (e.g., Bridging/Filtering).
- **Time Stamp -** The time the information was gathered.

Classification

- **MAC Address -** The MAC address of the end station connected to the device.
- **Auth User -** The 802.1x Authenticated User associated with the device connected to the end station, if applicable.
- **UNP -** The User Network Profile (UNP) that the device is associated with, if applicable.
- **VLAN ID -** The VLAN that is associated with the device.
- **Classification Source -** The Classification Policy by which the device was learned.

Data Center

- **MAC Address -** The MAC address of the end station connected to the device.
- **VLAN ID -** The VLAN associated with the device.
- **Service ID-** The Service ID associated with the device.
- **ISID -** The ISID associated with the device.

Layer 3

- **MAC Address -** The MAC address of the end station.
- **IP Address -** The IP address of the device connected to the end station.
- **VRF ID-** The VRF ID of the device directly connected to the end station, if applicable. If multiple VRFs are configured on the device, the VRF ID is displayed. If none are configured (and if the feature is not available on the device), the column will display "Default", indicating that the switch is operating as a single routing instance.

Template

You can create an additional two (2) custom views by clicking on the **Custom Template** button, entering a **Template Name**, selecting the fields you want to display and clicking **OK**. (You can change the order of the fields when you are creating the template by dragging a field up or down in the list before clicking **OK**.) The name of the new view will then be displayed in a button at the top of the Netforward Results Table, and can be used to view the selected fields. You can configure up to 2 new views. Creating an additional view will replace one of the previous views. Custom templates are associated with the current logged in user, so every user can have different custom templates. The available fields are defined below.

- **Client IP Address -** The IP address of the end station.
- **MAC Address -** The MAC address of the end station connected to the device.
- **Device IP Address -** The IP address of the device directly connected to the end station.
- **Time Stamp -** The time the information was gathered.
- **Domain -** The Layer 2 domain: VLAN, VPLS, SPB, EVB within the switches where the MAC is found.
- **Disposition -** The port disposition (e.g., Bridging/Filtering).
- **VLAN ID-** The VLAN associated with the port.
- **Slot/Port -** The slot/port number on which the device connected to the end station was learned.
- **Port Alias -** The user-configured alias for the slot/port (configured on the device through the CLI).
- **Port Admin Status -** The administrative status of the port (Up/Down).
- **Port Speed -** The port speed of the device connected to the end station.
- **Port Duplex Mode -** The port duplex mode (half duplex, full duplex, or auto duplex).
- **End Station Name -** The DNS name of the end station device.
- **Device DNS Name-** The DNS Name of the device.
- **Device Name -** The user-configured switch system name of the device connected to the end station.
- **Last Updated -** The last time the information in the table was updated.
- **Auth User -** The 802.1x Authenticated User associated with the device connected to the end station, if applicable.

- **VRF ID-** The VRF ID of the device directly connected to the end station, if applicable. If multiple VRFs are configured on the device, the VRF ID is displayed. If none are configured (and if the feature is not available on the device), the column will display "Default", indicating that the switch is operating as a single routing instance.
- **UNP -** The User Network Profile (UNP) that the device is associated with, if applicable.
- **Classification Source -** The Classification Policy by which the device was learned.
- **Service ID -** The Service ID associated with the device.
- **ISID -** The ISID associated with the device.
- **Chassis -** The chassis number for devices supporting the Virtual Chassis feature.

The fields below are only populated by devices authenticated through UPAM. Otherwise, the fields will be blank.

- **User Name -** The authentication information on the user who has logged in.
- **MAC Vendor -** The manufacturer of the network equipment based on the Organization Unique Identifier (OUI).
- **Category -** The category of the device (e.g., Computer, Mobile, Tablet).
- **Family -** The production vendor of the device (e.g., Alcatel-Lucent Enterprise, Apple, Microsoft)
- **CP End Station Name -** The ClearPass End Station name.
- **Host Name -** The port operational state (Up/Down).
- **Sponsor Name** - The Guest User sponsor.
- **Visitor Name -** The name of the Guest User.
- **Visitor Company -** The company of the Guest User.
- **Expires At -** The date and time when the Guest Account expires.
- **Certificate Valid From -**The date and time when the Guest Account was created.
- **Certificate Valid Up To -** The onboarding information of the date the certificate will expire.
- **User Type -** The User Type authenticated through the device (e.g., Employee, Guest).
- **BYOD Server -** The BYOD Server name.
- **BYOD Server Timestamp -** The time of the last recorded authentication activity.
- **SSID -** The SSID if the device.
- **WLAN Service -** The WLAN Service used by the device.
- **Authentication Type -** The authentication method used to authenticate the device (e.g., 802.1x, MAC)
- **Authentication Status -** The authentication status of the device. Note that for wireless users connected to Stellar APs, the results show online devices only - that is those devices that pass authentication and are connected to the network. Therefore, the authentication status will always be "success" for wireless clients connected to Stellar APs. If a client passes MAC authentication but does not perform Captive Portal

authentication, the client is still considered online with a limited role. Therefore, the authentication status for the client will still be success.

- **Physical Location -** The physical location of the device.

BYOD

Available only if ClearPass Policy Manager (CPPM) is defined in the BYOD application and connectivity can be established

- **User Type -** The BYOD/ClearPass User Type authenticated through the device (e.g., Employee, Guest). You can also place the mouse over the user to view detailed ClearPass user information. BYOD is only supported on Alcatel-Lucent Enterprise Switches running AOS 6.4.6.R01 and later, AOS 6.6.5.R01 and later, AOS 7.3.4.R02 and later, and AOS 8.1.1.R01 and later. Note that the connection to the CPPM Server and Database must be configured properly in the Unified Access application to gather the necessary information for this field.
- **ClearPass Server -** The ClearPass Server name.
- **IP Address -** The IP address of the ClearPass Server.
- **User Name -** CPPM endpoint authentication information on the user who has logged in.
- **Category -** CPPM endpoint profiling information on the class of device (e.g., Computer, Smart Device, Access Points, VoIP Phone)
- **Family -** CPPM endpoint profiling information on the device family (e.g., Windows, Apple, Alcatel, Unix).
- **CP End Station Name -** CPPM endpoint profiling information on the device name (e.g., Windows Vista/7/2008, Apple iOS Device, Alcatel IP Phone, Wireless AP)
- **Host Name -** CPPM endpoint profiling information on the Host Name.
- **Sponsor Name -** CPPM guest information on the sponsor.
- **Visitor Name -** CPPM guest information on the visitor's name.
- **Visitor Company -**CPPM Guest information on the visitor's company.
- **Expires At -** CPPM guest information on the date when authorization will end.
- **Cert Valid From -** CPPM onboarding information of the date the certificate was issued.
- **Cert Valid To -** CPPM onboarding information of the date the certificate will expire.

Settings

The Locator Settings Screen is used to set Locator timeout values and data retention policies. When you have configured the value(s), click the **Apply** button. The change takes effect immediately.

General

- **Historical Requests Response Timeout -** The amount of time, in seconds, that Locator will request historical data before timing out.
- **Live Requests Response Timeout -** The amount of time, in seconds, that Locator will request live data before timing out.

- **Locator Poll Requests Response Timeout -** The amount of time, in seconds, that Locator will poll a device before timing out.
- **802.1q Port Filtering -** This feature allows you to exclude 802.1q tagged ports from polling results and live searches when AMAP / XMAP is not operating or a link is not present on the tagged port. Filtering modes are described below.
- **Standard Mode:** 802.1q Ports are included in polling and searches.
- **Exclude Q-Tagged Ports:** 802.1q Ports are excluded from polling and searches.

Note: Virtual Machines communicate using tagged packets. If you are using VM Manager, 802.1q Port Filtering **must** be set to **Standard Mode** so that OmniVista can detect Virtual Machines with tagged frames.

Data Retention Policy

If Data Retention Policy is disabled, Locator will not remove data during polling and will accumulate unbounded data. To enable Data Retention Policy, move the slider to "Enabled" and set the retention period as described below.

- **Data Retention Period -** The number of days that Locator data will be retained (Default = 30).

Locator Data Statistics

When Data Retention is enabled, information that is older than the number of days specified in the Data Retention Period field is automatically deleted from the database. In addition, the number of days the data has been retained as well as the number of end station records being retained is listed. To refresh this information, click the Refresh icon. To purge all Locator data, click the **Purge All Locator Data** button, then click **Yes** at the confirmation prompt.

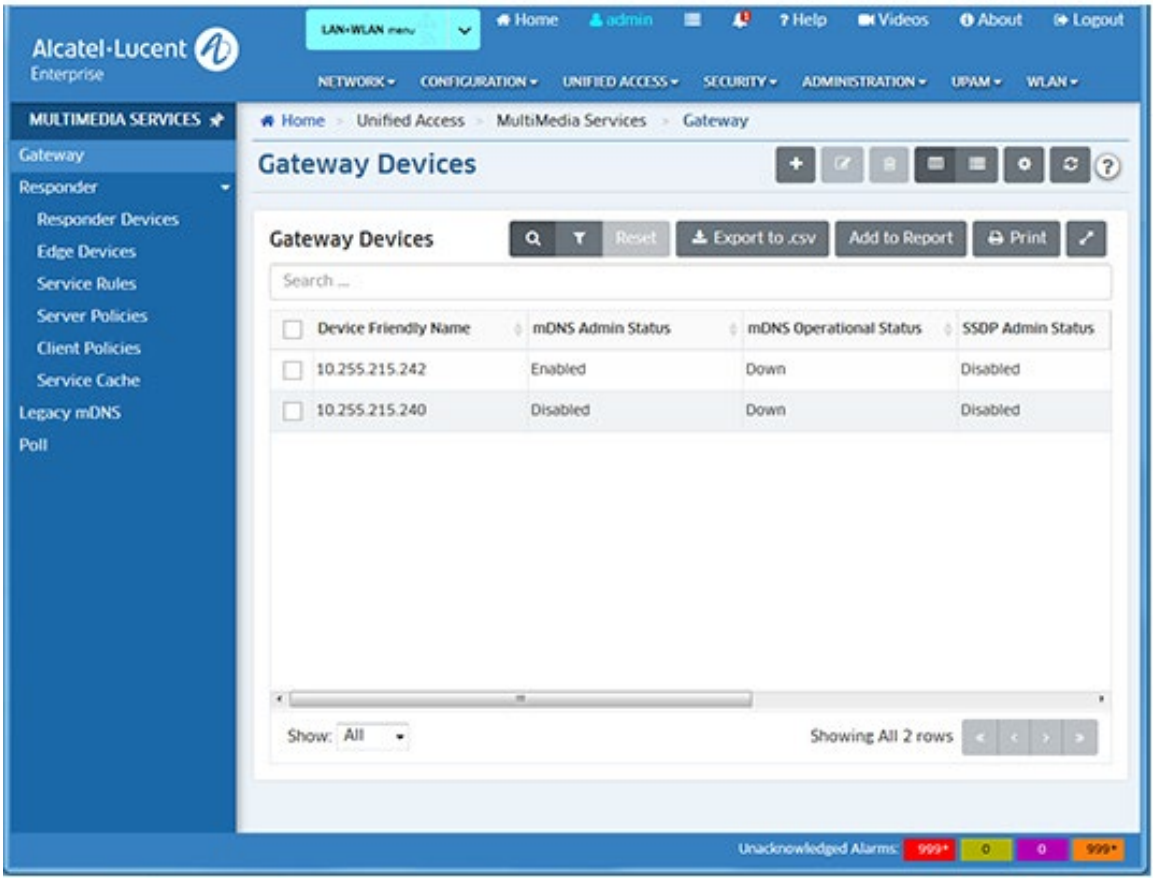
- **Retained Locator Data in Days -** The number of days Locator data has been retained.
- **Number of End Station Records Retained -** The number of end station records retained.

19.0 Multimedia Services

The Unified Access Multimedia Services application is used to configure the Multicast Domain Name System (mDNS) protocol. mDNS is used by "Zero Configuration Networking" solutions such as Apple's Bonjour, Avahi LGPL, and Linux NSS-mDNS. mDNS is a resolution service that is used to discover services on a LAN. mDNS allows the resolution of host names to IP addresses within small networks without the need of a conventional DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets and is implemented by Apple Bonjour, Avahi (LGPL), and Linux NSS-mDNS. In a BYOD network, mDNS is leveraged by providing wireless guests and visitors access to network devices, such as printers. There are three types of mDNS that can be configured using OmniVista.

- **Gateway mDNS -** Uses an OmniSwitch as a gateway to relay mDNS messages and enables the discovery of services across VLANs.
- **Responder mDNS -** Uses Responder Switches to relay mDNS messages and enables the discovery of services; and also enables you to configure and apply rules and policies to the service requests.
- **Legacy mDNS -** Uses a GRE Tunnel between an OmniSwitch and a WLAN Controller which acts as a gateway to relay mDNS messages. Legacy mDNS is limited to L2, which means clients can only discover services within the same L2 domain (VLAN). The clients cannot discover services across VLANs.

Multimedia Services



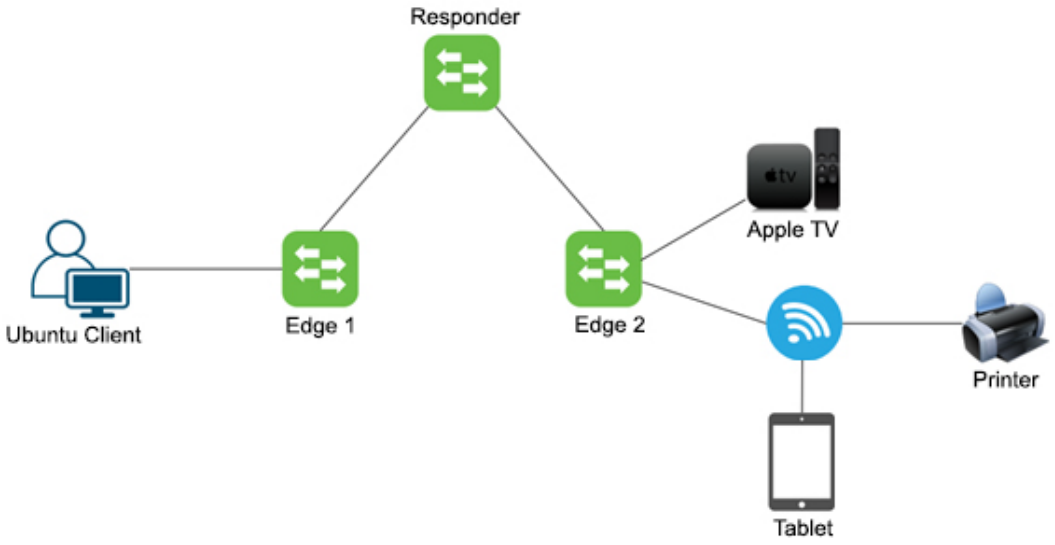
mDNS Flow

Gateway mDNS

Gateway mDNS is used if the network has no WLAN controller. In this mode, the traffic from the edge switch is forwarded to the configured gateway switch. The OmniSwitch acts as a gateway to flood mDNS messages over designated switch VLANs. A Gateway mDNS Switch replaces the Wireless Controller used in Legacy mDNS, and can be used if there are Stellar APs in the network. Wireless clients connected to APs request the mDNS service offered. The mDNS message from the Bonjour capable wired service device is encapsulated and relayed to the Gateway OmniSwitch. The Gateway OmniSwitch then relays the mDNS messages received to the APs over the designated Gateway VLANs. All of the devices with which you want to communicate must be connected to the VLANs specified when the Gateway Switch is configured.

Responder mDNS

Responder mDNS is configured on Responder Switches which communicate with Edge Switches/Stellar APs to which clients connect. In this mode, the Responder Device acts as a core switch. Server Rules are created on the Responder Device that contain Sever Policies and Client Policies. The Service Rules define the criteria by which the Responder Device decides which services can be shared with which client requests.



Notes:

- It is the Network Administrator's responsibility to make sure that IP connectivity exists between Edge Devices and mDNS Responder Switches. This is considered infrastructure configuration and is required in general for various features, including mDNS. A user may need to manually configure static routes on Responder Switches and other intermediate devices in the network to ensure connectivity. OmniVista CLI scripting can be used to push this infrastructure configuration to switches.
- If there is no rule/policy configured on a switch, the default behavior AOS behavior is “restrict all”. So, after configuring mDNS Responder Switches, a user should also create Service Rules and Policies from OmniVista and push them to Responder Switches.

- Configure Responder and Edge Devices first. Then, let users join the network and share mDNS Services. If this is sequence is not followed, users must share services again after the Responder and Edge Devices are configured for mDNS Services.
- OmniVista performs mDNS configuration functions only. Control Plane functions (e.g., which mDNS packets are dropped and which policies are matched in the network), are not displayed in OmniVista.

Legacy mDNS

Legacy mDNS is configured on an OmniSwitch by creating a GRE Tunnel between the OmniSwitch and a Wireless LAN Controller. The following figure below provides a sample mDNS workflow setup. The wireless clients connected to Access Point 1 (AP1) or Access Point 2 (AP2) request the mDNS service offered.

The mDNS feature is enabled on the OmniSwitch to support the mDNS service. A Layer 2 GRE tunnel interface is configured from the WLAN controller to the OmniSwitch to relay the mDNS messages. The mDNS message from the Bonjour capable wired service device is encapsulated and relayed from the OmniSwitch to the configured WLAN controller over the GRE tunnel. The WLAN controller then relays the mDNS messages received via the OmniSwitch GRE tunnel to the APs over the AP GRE tunnels.

Note that the WLAN controller uses a multicast optimization algorithm and forwards Bonjour response messages to targeted user devices, instead of all devices on all APs. This limits the unnecessary flooding of the Bonjour/mDNS traffic to improve the Wi-Fi performance.

Gateway Devices

The mDNS Gateway Devices Screen displays all configured mDNS Gateway Switches and is used to create, edit, and delete, mDNS Gateway Switches. An mDNS Gateway Switch replaces the Wireless Controller used in Legacy mDNS, and can be used if there are Stellar Access Points (APs) in the network. A Gateway mDNS Switch floods mDNS messages over designated VLANs. Wireless clients connected to APs request the mDNS service offered. The mDNS message from the Bonjour capable wired service device is tagged with a VLAN and relayed to the Gateway Switch. The Gateway Switch then relays the mDNS messages received to the APs over the designated Gateway VLANs.

The mDNS Gateway Model is a simpler configuration that the Responder Model. When you use the Gateway Model, you configure a switch as an mDNS Gateway and specify a list of VLANs that will be flooded with mDNS messages. The Responder Model uses Responder Switches to relay mDNS messages and enables the discovery of services across VLANs; and also enable you to configure and apply rules and policies to the data traffic.

> **Note:** mDNS Gateway is supported on OS6450 Switches running AOS 6.7.2.R02 or higher; and OS6860E, OS6865, and OS6900 Switches running 8.4.1.R02 or higher. A switch can be configured as **either** a Gateway Device or a Responder Device. It cannot be configured for both.

Creating an mDNS Gateway

Click the Add icon to go to the Add Gateway Device Configuration Screen and complete the fields as described below. When you are done, click on the **Create** button.

- **Device Friendly Name -** Click on the **ADD** button and use the switch picker or Topology application to select the switch you want to configure as a gateway.

- **mDNS Admin Status -** The mDNS administrative status (Enabled/Disabled). mDNS relay enables the OmniSwitch to allow Apple devices to discover services with minimal configuration by the administrator.
- **SSDP Admin Status -** The SSDP administrative status (Enabled/Disabled). SSDP relay enables the OmniSwitch to allow non-Apple devices to discover services with minimal configuration by the administrator.
- **VLANs List -** Select VLAN(s) from the drop-down list. This is the list of VLANs on the Gateway Switch where the mDNS server/client traffic from the edge devices is expected to arrive. mDNS packets are forwarded to all VLANs specified in this list. Specify the mDNS VLAN(s) that are used in the network. However, if the specified VLAN(s) do not exist on the Gateway Switch, you must create them in the VLAN application later for the configuration to work in the network.

Editing an mDNS Gateway

Select the switch in the Gateway Devices Table and click on the Edit icon to bring up the Add Gateway Device Configuration Screen. Edit the allowable fields as described above and click on the **Apply** button.

Deleting an mDNS Gateway

Select the switch in the Gateway Devices Table, click on the Delete icon, then click **OK** at the confirmation prompt.

Gateway Devices Table

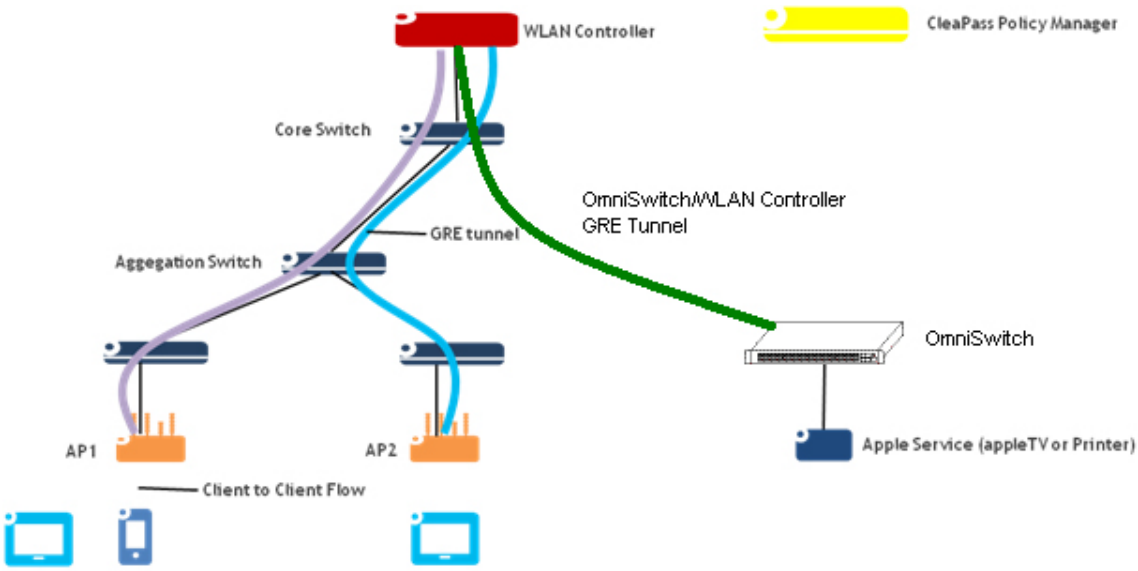
The Gateway Devices Table displays The fields are defined below.

- **Device Friendly Name -** The switch IP address.
- **mDNS Admin Status -** The mDNS administrative status (Enabled/Disabled).
- **mDNS Operational Status -** The mDNS operational status. (Up/Down).
- **SSDP Admin Status -** The SSDP administrative status (Enabled/Disabled).
- **SSDP Operational Status -** The SSDP operational status (Up/Down).
- **VLANs List -** The list of device VLANs configured for mDNS. mDNS packets are flooded on all specified VLANs.

Responder

The mDNS Responder Screen displays the number of configured Responder Switches, Edge Switches, Service Rules, Server Policies, Client Policies, and Service Cache. Click on a widget to go the applicable screen for a detailed view of the configuration.

Responder mDNS is configured on Responder Switches which communicate with Edge Switches/Stellar APs to which clients connect. In this mode, the Responder Device acts as a core switch. Server Rules are created on the Responder Device that contain Sever Policies and Client Policies. The Service Rules define the criteria by which the Responder Device decides which services can be shared with which client requests.



Responder Devices

The mDNS Responder Devices Screen displays information about mDNS Responder Devices. The screen is also used to create, edit, and delete Responder Devices, and re-apply the configuration to a Responder Device. Responder Devices relay mDNS messages and enable the discovery of services across VLANs; and also enables you to configure and apply rules and policies to the data traffic. Service Rules, containing Server Policies and Client Policies define the criteria by which the Responder Device determines which services can be shared with which client requests. The mDNS Responder Screen is the main screen to configure the full workflow for mDNS, including creating Responder Devices, configuring linked Edge Devices, and configuring Service Rules, Server Policies, and Client Policies.

> **Note:** The following devices can be configured as Responder Devices: OS6860, OS6865, OS6900, OS9900, running AOS 8.7R1 and higher. A switch can be configured as **either** a Responder Device or a Gateway Device. It cannot be configured for both. A switch cannot be configured as a Responder Device if it has already been configured as an mDNS Gateway, or as an Edge Device for another Responder.

If you want to configure a switch that has already been configured as a Gateway Device, go to the Gateway Device Screen and delete the switch. If the switch does not appear in the Gateway Device List, go to the Poll Screen and poll the switch. Then return to the Gateway Devices Screen and delete the switch.

Responder mDNS Workflow

1. Create a Responder Device.

2. Create Edge Devices for the Responder Devices.

3. Create Service Rules.

- Create Server Policies.
- Create Client Policies.

Important Note: Configure Responder and Edge Devices first. Then, let users join the network and share mDNS Services. If this is sequence is not followed, users must share services again after the Responder and Edge Devices are configured for mDNS Services.

Create a Responder Device

Click on the Add icon to bring up the Setup an mDNS Responder Screen. Complete the fields as described below, then click on the **Enabled as Responder and Configure** button.

- **Configure Responder For -** Select "Use Switch Picker" or "Use Topology App" and click on the **Select Device** button to select a device. Only supported AOS devices are available for selection. See note above.
- **Looback0 IP address -** The existing Loopback0 IP address is pre-filled in the field if it is already configured on the switch. If it does not exist on the switch, it will be created on the switch based on your input. You can edit the Loopback0 IP Address when the IP Address of the Responder Device is **not** the loopback0 IP address.

The Responder Device will appear on the Responder Devices Screen. Select the device in the list and click on the Edit icon to complete the configuration.

Completing the Responder Configuration

After creating a Responder Device as described above, select the device in the Responder Devices List and click on the Edit icon, and complete the fields on the "Setup a mDNS Responder" Screen as described below to complete the setup. When you are finished click on the **Apply** button.

General

- **Responder Device -** Pre-filled with the IP address of the selected device.
- **mDNS Admin Status -** Enables/Disabled mDNS on the switch (Default - Enabled).
- **Looback0 IP address -** The existing Loopback0 IP address is pre-filled in the field if it is already configured on the switch. If it does not exist on the switch, it will be created on the switch based on your input. You can edit the Loopback0 IP Address when the IP Address of the Responder Device is **not** the loopback0 IP address.

Edge Devices Common Configuration

Check the "Use These Common Configs For All Edge Devices Associated To This Responder" checkbox and configure the fields as described below to quickly apply these basic configurations to all selected Edge Devices.

- **Use These Common Configs For All Edge Devices Associated To This Responder -** Select this checkbox to quickly apply the Edge device configurations you create to all Edge Devices associated with this Responder.
- **Default Preselect VLANs -** Select a VLAN from the drop-down. Click on the Add icon to select additional VLANs. For every query packet generated by the Responder Device, the mDNS packet has a VLAN tag of 4095. These mDNS packets are flooded to AOS Edge Devices over these configured access VLANs.
- **Default WLAN (SSID) List -** Select a WLAN (SSID) from the drop-down. Click on the Add icon to select additional WLANs (SSIDs). For every query packet generated by the Responder Device, the mDNS packet has a VLAN tag of 4095. These mDNS

packets are flooded to AP Edge Devices over these configured access WLAN(s)/SSID(s).

- **Default mDNS Admin Status -** Enables/Disabled mDNS for the Edge Devices.

Edge Device Selection

Click on the **Add** button to select Edge Devices (either AOS Switches **or** AP Groups). The switches/AP Groups will appear in the List of Selected Devices. If you have **not** created an Edge Device Common Configuration (as described above), configure Edge Device VLANs/ WLANs (SSIDs), mDNS Admin Status, and Loopback 0 IP address on individual switches/AP Groups.

> **Note:** The following devices can be configured as Edge Devices: OS6465, OS6560, OS6860, OS6865, OS6900, and OS9900, running AOS 8.5R1 and higher; and Stellar APs running 4.0.1 and higher (except for OAW-AP1101). Only supported devices or AP Groups containing supported devices are available for selection.

Service Sharing Configuration

Service Rules specify the services that will be shared with clients. You can configure Service Sharing Rules for the Responder Device at this time or configure them later on the applicable OmniVista Screens (e.g., Service Rules, Server Policies, Client Policies). A Service Rule must contain a Server Policy and a Client Policy. Note that you must configure Service Rules to share services on the network. If there are no Service Rules configured, the Responder Device will learn all the services, but will not process any query received from an mDNS client.

To configure Service Rules now, click on the **Add** icon and configure Service Sharing Rules for the Responder as described below. When you are done, click on the **Create** button. To configure additional rules, click on the "Create Another" checkbox. A Service Rule must include a Server Policy and/or a Client Policy.

- **Rule Name -** Enter a name for the rule.
- **Service IDs -** Select a Service ID(s) from the drop-down menu. These are the services that will be shared on the network.
- **Server Policies -** Server Policies are applied to traffic originating from a server (sharing source). Select an existing Server Policy from the drop-down menu. A Service Rule can have **one** Server Policy. If necessary, click on the "Add New" link to go to the Server Policies Screen and create a new policy.
- **Client Policies -** Client Policies are applied to traffic from a client (the device requesting the service). Select an existing Client Policy from the drop-down menu. A Service Rule can have **one** Client Policy. If necessary, click on the "Add New" link to go to the Client Policies Screen and create a new policy.

The configured rules will be displayed on the applicable screen (e.g., Service Rules, Server Policies, Client Policies), where they can be edited, deleted and any time.

Editing a Responder Device

Select a Responder Device in the list and click on the Edit icon. Complete the fields as described below and click on the **Apply** button.

General

- **Responder Device -** Pre-filled with the IP address of the selected device.
- **mDNS Admin Status -** Enables/Disabled mDNS on the switch (Default - Enabled).
- **Looback0 IP Address -** Pre-filled with the Loopback IP address assigned when creating the Responder Device. This field can be edited. If you change it, the Loopback0 IP address will be changed on the switch.

Edge Devices Common Configuration

Check the "Use These Common Configs For All Edge Devices Associated To This Responder" checkbox and configure the fields as described below to quickly apply these basic configurations to all selected Edge Devices.

- **Use These Common Configs For All Edge Devices Associated To This Responder -** Select this checkbox to quickly apply the Edge device configurations you create to all Edge Devices associated with this Responder.
- **Default Preselect VLANs -** Select a VLAN from the drop-down. Click on the Add icon to select additional VLANs. For every query packet generated by the Responder Device, the mDNS packet has a VLAN tag of 4095. These mDNS packets are flooded to AOS Edge Devices over these configured access VLANs.
- **Default WLAN (SSID) List -** Select a WLAN (SSID) from the drop-down. Click on the Add icon to select additional WLANs (SSIDs). For every query packet generated by the Responder Device, the mDNS packet has a VLAN tag of 4095. These mDNS packets are flooded to AP Edge Devices over these configured access WLA(s)/SSID(s).
- **Default mDNS Admin Status -** Enables/Disabled mDNS for the Edge Devices.

Edge Device Selection

Click on the **Add** or **Edit** buttons to select/deselect Edge Devices (switches **or** AP Groups). The switches/AP Groups will appear in the List of Selected Devices. If necessary, you can edit the VLAN's/Default WLAN (SSID) List, mDNS Admin Status, and Loopback 0 IP address on individual switches/AP Groups.

Service Sharing Configuration

If Service Rules are configured for the Edge Device, they will appear in the list. To edit a Service Rule or Server Policy, click on the Rule or Policy Name hyperlink, edit the rule or policy and click on the **Apply** button.

To add a Service Rule, click on the Add icon and complete the fields as described above. To delete a Service Rule, select the rule(s) and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Deleting a Responder Device

Select a Responder Device in the Responder Device List and click on the Delete icon. Click **OK** at the Confirmation Prompt. Note that the following objects will be also deleted in that responder: Service Rule, Server Policy Client Policy, and related Edge Devices. When you delete a Responder Device, all mDNS configurations on the Responder Device and associated Edge Devices are set to default.

Re-Applying the Configuration to a Responder Device

To re-apply an existing configuration to a Responder Device, select the device in the Responder Devices List and click on the **Re-Apply** button at the top of the list. This will re-apply the existing OmniVista Responder configuration, overriding the current configuration. This can be used to resolve a mismatched configuration between the OmniVista and AOS.

Responder Devices List

- **Responder Device -** The IP address of the Responder Device.
- **Admin Status -** The mDNS administrative status (Enabled/Disabled).
- **Operational Status -** The mDNS operational status. If a device does not have a Loopback0 IP address or it is unreachable, the operational status will be down (Up/Down).
- **Config Status -** The mDNS configuration status (Success/Failed).
- **Loopback0 IP -** The Responder Device's Loopback0 IP address.
- **Service Sharing Rules -** The Service Sharing Rules configured for the Edge Device. The number of rules are displayed. You can hover over the number to display the rule names.

Click on a Responder Device in the list for more detailed information, including Edge Devices and Service Rules. Click on a link in the Rules List to add, edit, or delete a Rule, Server Policy, or Client Policy.

Edge Devices

The mDNS Edge Devices Screen displays information about mDNS Edge Devices. The screen is also used to edit or delete Edge Devices. Switches/Stellar APs are created when configuring a Responder Device.

> **Note:** The following devices can be configured as Edge Devices: OS6465, OS6560, OS6860, OS6865, OS6900, and OS9900, running AOS 8.5R1 and higher; and Stellar APs running 4.0.1 and higher (except for OAW-AP1101). Only supported devices or AP Groups containing supported devices are available for selection.

Editing an Edge Device

Select an Edge Device in the Edge Devices List, click on the Edit icon, complete the fields as described below, then Click on the **Apply** button.

- **Edge Device IP Address -** Pre-filled with the device IP address.
- **mDNS Admin Status -** Enables/Disabled mDNS on the device (Default - Enabled).
- **VLANs -** The VLANs associated with the Edge Device.
- **Loopback0 IP Address -** The device Loopback IP address.

Note: To delete an Edge Device, remove it from the associated Responder Device on the Responder Devices Screen. Go to the Responders Devices Screen, select the Responder Device associated with the Edge Device and click on the Edit icon. Go to the "Edge Devices Selection" area and remove the Edge Device(s).

Edge Devices List

- **Device Friendly Name -** The device IP address (or user-configured device name).
- **AP Group Name -** The AP Group name, if applicable.
- **mDNS Admin Status -** The mDNS administrative status on the device.
- **Operational Status -** The mDNS operational status. If a device does not have a Loopback0 IP address or it is unreachable, the operational status will be down (Up/Down).
- **VLANs/SSIDs -** The VLANs/SSIDs associated with the device. The number of VLANs/SSIDs is displayed. Hover over or click on the link to display a list of VLANs/SSIDs.
- **Loopback0 IP -** The device Loopback0 IP address.
- **Responder IP Address -** The IP address of the Responder Device associated with the Edge Device.

Service Rules

The mDNS Responder Service Rules Screen displays information about Responder Service Rules. The screen is also used to create, edit, and delete Responder Service Rules. Service Rules specify the services that will be shared between servers and clients. If there are no service rules configured, the Responder Device will learn all the services, but will not process any query received from the mDNS client. After creating a Service Rule, configure Server Policies and Client Policies for the Service Rule. A Service Rule must contain a Server Policy and/or a Client Policy.

Creating a Service Rule

Select the Responder Device on which you want to configure the Service Rule from the "Service Rules Of Responder" drop-down at the top of the screen. Click on the Add icon, complete the fields as described below, then click on the **Create** button.

- **Device -** Pre-filled with the IP address of the device on which you are configuring the Service Rule.
- **Name -** The user-configured name for the rule (e.g., Scanner Rule, Apple TV Rule).
- **Service IDs -** Select the service(s) that will be included in the rule. These services will be shared on the network. You can click on the Poll button to refresh the Service IDs known by the Responder Device.
- **Server Policy -** Select a Server Policy from the drop-down to associate with the rule. You can click on the "Add New" link to create a new policy and associate the policy with the rule.
- **Client Policy -** Select a Client Policy from the drop-down to associate with the rule. You can click on the "Add New" link to create a new policy and associate the policy with the rule.

Editing a Service Rule

Select Service Rule in the Service Rules List and click on the Edit icon. Edit any fields as described above, then click on the **Apply** button.

Deleting a Service Rule

Select a Service Rule(s) in the Service Rules List, click on the Delete icon, then click on **OK** at the Confirmation Prompt.

Service Rules List

- **Name -** The user configured name for the rule.
- **Origin -** Where the rule originated (e.g., OmniVista Operator).
- **Service IDs -** The Service ID(s) included in the rule. The number of Service IDs is displayed. Hover over, or click on the link to display a list of services.
- **Server Policy -** The Server Policy associated with the rule.
- **Client Policy -** The Client Policy associated with the rule.

Server Policies

The mDNS Responder Server Policies Screen displays information about Responder Server Policies. The screen is also used to create, edit, and delete Responder Server Policies. Server Policies are part of a Service Rule and are applied to traffic originating from a server (sharing source). A Server Policy is required if you want to share a service. The Server Policy is configured for the “sharing side”. For example, if you are going to share a printer, the source who is sharing the printer is called “Printer Server”. The Server Policy is used to restrict which servers are allowed to share the printer (e.g., only servers located in specified VLANS, locations, MAC addresses).

Creating a Server Policy

Select the Responder Device on which you want to configure the Server Policy from the "Server Policies Of Responder" drop-down at the top of the screen. Click on the Add icon, complete the fields as described below, then click on the **Create** button. A Server Policy must contain **at least one** of the mapping criteria (e.g., VLAN, Location, Access Role Profile, User Name, MAC address).

- **Policy Name -** The user-configured name for the policy (e.g., Printer Server, Scanner Server). The Policy Name can be a maximum of 31 characters in length.
- **VLANs -** Select the VLAN(s) to include in the policy. Only servers on this VLAN(s) can share the service.
- **Access Role Profiles -** Select the Access Role Profile(s) to include in the policy. This condition is only supported on devices running AOS 8.7R2 and AWOS 4.0.1 and higher.
- **Locations -** Enter a location(s) to include in the policy. This field provide location(s) to be mapped to the server policy. Only servers with this location(s) can share the service (see notes below).
- **User Names -** Enter a user name(s) to include in the policy. Only servers with this user name(s) can share the service.
- **MACs -** Enter a MAC address(es) to include in the policy. Only servers with this MAC address(es) can share the service.

Notes:

- If the Port Alias is set, the Location = Port Alias.
- If the Port Alias is not set AND the System Location is set (not default, by default, System Location is empty), the Location = System Location + Port ID (e.g., System Location = "x" and the Port ID = 1/1/1, the Location will be "x 1/1/1").
- If the Port Alias is not set AND the System Name is set (not default, by default, System Name is "no-name"), the Location = System Name + Port ID (e.g., System Name = "sx" and the Port ID = 1/1/1, the Location will be "sx 1/1/1").
- If none of above are valid, the Location = Chassis ID + Port ID.
- For APs, the Location will be the Location of the AOS Port that the AP is linking to.

Editing a Server Policy

Select Server Policy in the Server Policies List and click on the Edit icon. Edit any fields as described above, then click on the **Apply** button.

Deleting a Server Policy

Select a Server Policy in the Server Policies List, click on the Delete icon then click on **OK** at the Confirmation Prompt.

Server Policies List

- **Policy Name -** The user configured name for the policy.
- **Origin -** Where the policy originated (e.g., OmniVista Operator, UPAM BYOD Portal).
- **VLANs -** The VLAN(s) associated with the policy.
- **Access Role Profiles -** The Access Role Profile(s) associated with the policy.
- **Locations -** The location(s) associated with the policy.
- **User Names -** The user name(s) associated with the policy.
- **MACs -** The MAC address(es) associated with the policy.

Client Policies

The mDNS Responder Client Policies Screen displays information about Responder Client Policies. The screen is also used to create, edit, and delete Responder Client Policies. Client Policies are part of a Service Rule and are applied to traffic from a client (the device requesting the service). A Client Policy specifies which clients can see/discover the service. Only clients matching the conditions in the policy will see the sharing services.

Creating a Client Policy

Select the Responder Device on which you want to configure the Server Policy from the "Server Policies Of Responder" drop-down at the top of the screen. Click on the Add icon, complete the fields as described below, then click on the **Create** button. A Client Policy must contain **at least one** of the mapping criteria (e.g., VLAN, Location, Access Role Profile, User Name, MAC address).

- **Policy Name -** The user-configured name for the policy (e.g., Printer Server, Scanner Server). The Policy Name can be a maximum of 31 characters in length.
- **VLANs -** Select the VLAN(s) to include in the policy. Only clients on this VLAN(s) can see/discover the service.
- **Access Role Profiles -** Select the Access Role Profile(s) to include in the policy. This condition is only supported on devices running AOS 8.7R2 and AWOS 4.0.1 and higher.
- **Locations -** Enter a location(s) to include in the policy. This field provide location(s) to be mapped to the server policy. Only clients with this location(s) can see/discover the service (see notes below).
- **User Names -** Enter a user name(s) to include in the policy. Only clients with this user name(s) can see/discover the service.
- **MACs -** Enter a MAC address(es) to include in the policy. Only clients with this MAC address(es) can see/discover the service.

Notes:

- If the Port Alias is set, the Location = Port Alias.
- If the Port Alias is not set AND the System Location is set (not default, by default, System Location is empty), the Location = System Location + Port ID (e.g., System Location = "x" and the Port ID = 1/1/1, the Location will be "x 1/1/1").
- If the Port Alias is not set AND the System Name is set (not default, by default, System Name is "no-name"), the Location = System Name + Port ID (e.g., System Name = "sx" and the Port ID = 1/1/1, the Location will be "sx 1/1/1").
- If none of above are valid, the Location = Chassis ID + Port ID.
- For APs, the Location will be the Location of the AOS Port that the AP is linking to.

Editing a Client Policy

Select Server Policy in the Server Policies List and click on the Edit icon. Edit any fields as described above, then click on the **Apply** button.

Deleting a Client Policy

Select a Client Policy in the Client Policies List, click on the Delete icon, then click **OK** at the Confirmation Prompt.

Client Policies List

- **Policy Name -** The user configured name for the policy.
- **Origin -** Where the policy originated (e.g., OmniVista Operator).
- **VLANs -** The VLANs associated with the policy. The number of VLANs is displayed. Hover over, or click on the link to display a list of VLANs.
- **Access Role Profiles -** The Access Role Profile(s) associated with the policy
- **Locations -** The location(s) associated with the policy.
- **User Names -** The user name(s) associated with the policy.
- **MACs -** The MAC address(es) associated with the policy.

Server Cache

The mDNS Responder Service Cache Screen displays a list of services learned by mDNS for Responder Devices. Select a Responder Device from the **mDNS Cache Of Responder** drop-down to display the information. The cache contains information about the traffic passed by clients on the network.

Note: Service Cache is polled every one hour. If you do not see an entry, please wait for next polling.

Server Cache Table

- **Service Instance -** The device name of the service instance.
- **Service ID -** The type of service.
- **IP Address -** The IP address of the device on which the service was discovered.
- **Port -** The UDP port number of the discovered service instance.
- **Policy List -** The policy(ies) associated with the service instance.
- **Location -** The location derived from the edge switch.
- **VLAN -** The VLAN ID assigned for the service.
- **MAC Address -** The MAC address assigned for the service.
- **User Name -** The user name assigned for the service.

Legacy mDNS

The mDNS Legacy mDNS Screen is used to create, edit, delete, and view mDNS configuration on your network. Only **one** mDNS configuration per device is supported.

Configuring mDNS for a Device

Before you begin, configure the GRE tunnel interface before attempting to associate the interface with the mDNS tunnel relay. The GRE tunnel must also be configured on the OmniAccess WLAN controller. An IP address is required to bring the interface up; if necessary, specify a dummy IP address when configuring the interface. Follow the steps below to configure a switch for mDNS.

1. Click the Add icon button to go to the "Add mDNS Configuration" Screen.

2. Click on the **Select Devices** button to bring up a list of switches that are available for mDNS configuration.

3. Select a switch and click **OK**. You will be returned to the Add mDNS Configuration Screen and the switch you selected will appear in the **Switch** field.

4. Complete the fields as described below:

- **Switch -** The IP address of the selected switch is pre-filled in this field.
- **Select OAW Controller -** Select an OmniAccess WLAN Controller to which you want to connect.
- **mDNS GRE Tunnel -** Select a GRE Tunnel to be used to forward packets to the selected OmniAccess WLAN Controller. This is the GRE Tunnel from the OmniSwitch to the OmniAccess Controller. (Only Layer 2 GRE tunnels are supported.)

- **mDNS Admin Status -** The mDNS administrative status (Enabled/Disabled).
- **Router IP Address -** The router IP address.
- **Router IP Mask -** The router IP mask.
- **Tunnel Source IP Address -** The source IP address of the GRE Tunnel from the switch to the controller. This field is pre-filled with the IP address of the selected switch.
- **Tunnel Dest IP Address -** The destination IP address of the GRE Tunnel from the switch to the controller. This field is pre-filled with the IP address of the selected OAW Controller.
- **VRF ID -** The VRF of the GRE Tunnel. *This field will only be visible if the device supports the Multiple VRF feature **and** SNMPv3 was used for discovery.*

5. Click **OK**. The switch will appear in the list of switches on the mDNS Configuration Screen.

Editing an mDNS Configuration

Select the switch in the mDNS Configuration Table and click on the Edit icon to bring up the "Edit mDNS Configuration" Screen. Edit the allowable fields as described above and click on the **Apply** button.

Deleting an mDNS Configuration

Select the switch in the mDNS Configuration Table, click on the Delete icon, then click **OK** at the confirmation prompt.

Viewing mDNS Configurations

The mDNS Configuration Table displays all switches currently configured for mDNS. The fields are defined below.

- **Name -** The user configured name for the device.
- **Device -** The IP address of the device.
- **mDNS GRE Tunnel -** The name of the GRE Tunnel to be used to forward packets to the OmniAccess WLAN Controller.
- **mDNS Admin Status -** The mDNS administrative status (Enabled/Disabled).
- **mDNS Oper Status -** The mDNS operational status (Up/Down).
- **Router IP Address -** The router IP address.
- **Router IP Mask -** The router IP mask.
- **Admin Status -** The router administrative status (Enabled/Disabled).
- **Tunnel Source IP Address Type -** Currently, only IPv4 is supported.
- **Tunnel Source IP Address -** The source IP address of the GRE Tunnel from the switch to the controller. This field is pre-filled with the IP address of the selected switch.
- **Tunnel Dest IP Address Type -** Currently, only IPv4 is supported.
- **Tunnel Dest IP Address -** The destination IP address of the GRE Tunnel from the switch to the controller. This field is pre-filled with the IP address of the selected OAW Controller.

Poll

The mDNS Poll Screen is used to poll Gateway and Responder Switches for updates the mDNS configuration in the OmniVista Database. Click on the **ADD** button, select "Use Picker" or "Use Topology", and select the switch you want to poll. Click **OK**. The switch appears in the List of Selected Devices Table. Click on **Poll Now** to poll the devices.

mDNS Sharing

The mDNS Sharing Screen displays information about mDNS Sharing Rules, and is used to create, edit, and delete mDNS Sharing Rules. mDNS Sharing Rules enable you to configure a policy for device sharing using the mDNS protocol. Only devices matching the mDNS Sharing rule will be allowed to access the shared device.

Creating a Sharing Rule

Click on the Add icon to bring up the mDNS Sharing Screen. Complete the fields as described below, then click on the **Create** button.

- **Device Name -** The name of the device to be shared with other users (no spaces).
- **Device Type -** The type of the device to be shared with other users.
- **MAC Address -** The MAC address of the device to be shared with other users.
- **Shared With -** The user account that can access the shared device.

Editing a Sharing Rule

Select Sharing Rule in the mDNS Sharing List and click on the Edit icon. Edit any fields as described above, then click on the **Apply** button.

Deleting a Sharing Rule

Select a Sharing Rule(s) in the mDNS Sharing List, click on the Delete icon, then click on **OK** at the Confirmation Prompt.

mDNS Sharing List

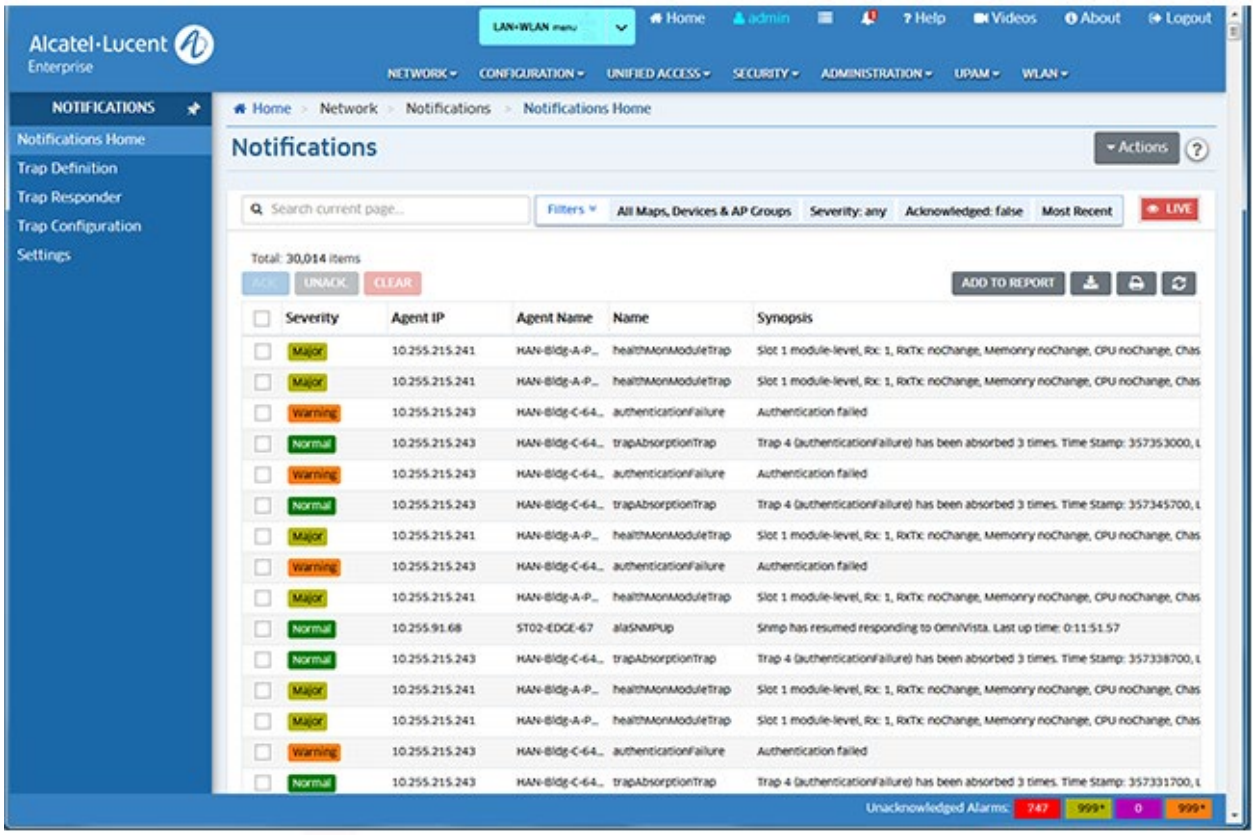
- **Device Name -** The name of the device to be shared with other users.
- **Device Type -** The type of the device to be shared with other users.
- **MAC Address -** The MAC address of the device to be shared with other users.
- **Shared With -** The user account that can access the shared device.

20.0 Notifications

The Notifications application is used to monitor traps and configure trap management tasks using the following screens:

- **Notifications Home -** Displays all traps received from network devices and provides basic trap information (e.g., severity level, date/time received). You can also use this screen to acknowledge, renounce, and clear traps, as well as poll devices for traps.
- **Trap Definition -** Displays a list of all supported traps, as defined in the MIBs, and provides a brief description of each trap. You can also edit a trap's severity level and trap synopsis.
- **Trap Responder -** Used to configure the response (if any) that you want OmniVista to take when a specified trap is received on the OmniVista server. The trap can be specified by severity level or through the use of filters. The response can take the form of an e-mail sent to a user-specified address and/or the execution of an external program or script on the OmniVista Server.
- **Trap Configuration -** Used to configure traps for network devices.
- **Settings -** Used to set trap preferences (e.g., trap port, number of traps displayed).

Notifications



Notifications Home

The Notifications Home Screen displays configured traps received from network devices and provides basic trap information (e.g., severity level, date/time received). Click on a trap to display detailed trap information. You can also use this screen to acknowledge/delete specific traps, quickly acknowledge/delete all traps in the Notifications Table, or poll devices for traps.

Viewing Traps

By default, all traps from all devices are displayed in the Notifications Table. However, you can use the filter function to customize the display. Select one or more options from the "Filters" drop-down menus and select search criteria.

- **Filter By -** Select which devices you want to view.
- **All -** Select "All" to display configured traps from all network devices.
- **Map -** Select "Map" and select a map(s) to display traps from only the devices contained in the selected map(s).
- **Device -** Select "Device", select Switch Picker or Topology in the "Select Using" drop-down, then click **EDIT** in the "Devices Selected" field to view traps from specific devices. You can also select "Quick Select" and select a device(s) from the drop-down menu.
- **AP Group -** Select "AP Group" and select a group(s) from the drop-down to display traps from a specific AP Group(s).
- **NMS Level -** Select "NMS Level" to display traps received from the Wireless Intrusion Protection System (WIPS) application.
- **Trap Names -** Enter a trap name to search for a specific trap. To search for multiple traps, enter each trap name separated by a comma, with no space after the comma. (e.g., alasnmptrapup,alasnmptrapdown).
- **Severity -** Select the Severity Level(s) of the traps you want to display: Critical, Major, Minor, Warning, Normal. You can select multiple Severity Levels by clicking on each level and then clicking anywhere outside the field box. De-select a previously-selected level by clicking on it. You can also select all levels by clicking on "Select All at the top of the drop-down menu). If you select "Remove All" levels, all traps are displayed, regardless of Severity Level ("0 Selected" - Default).
- **Acknowledged -** Select whether you want to view all traps (Any), Acknowledged Traps (True), or traps that have not been acknowledged (False).
- **Time Range -** By default, the most recent traps are displayed (Most Recent). To display traps from a specific time range, select the "Custom" radio button and enter the time range.

After setting the view criteria as described above, the table will be filtered based on selected criteria. Click on the **X** in the right corner of the Filter Configuration window to close the window.

You can also use the "search" function to further filter the current Notifications Table display. Enter any search criteria in the Search Field at the top of the table. The display will update to display only those entries that contain the search criteria. Delete the search criteria or click on the "x" at the far right of the Search Field to reset the display. Note that you do not have to click on the Search icon after entering the search criteria. The display will update as you enter the criteria. If you enter search criteria and click on the Search icon, click on the Search icon again to display the Search Field.

Note: By default, all traps from all devices are displayed and updated in real-time (indicated by the red "Live" icon at the top-right corner of the table. If you apply a filter, live update is disabled. When you return to the default settings, live update is again enabled. Also note that if you scroll through the table and new traps are received, a "New Traps" message will appear. Click on the message to return to the top of the table and view the new traps.

Basic Trap Information

The Notifications Table provides an overview of each trap. Click on a trap to display detailed information.

- **Agent IP -** The IP address of the device that generated the trap.
- **Agent Name -** The name of the device that generated the trap.
- **Name -** The name of the trap as defined in the MIB.
- **Synopsis -** A brief description of the trap.
- **Date/Time -** The date and time the trap was received by OmniVista Server using the OmniVista system clock. However, for traps received that are "replays" of previously-generated traps, the date/time will be adjusted to the time that the original trap was sent. This is calculated by adjusting the time received by the difference between the current upTime of the source device and the upTime contained within the trap itself. Therefore, it is possible for new traps to be added to the display with old timestamps. So, if the network was down for hours, you may suddenly see traps appear from hours ago.

Detailed Trap Information

The Detailed Information pane provides detailed information for the selected trap. Click on a trap to display detailed information.

- **Name -** The name of the trap as defined in the MIB.
- **Severity -** The severity level assigned to the trap in the Notifications Application's Trap Definitions Window (Normal/Warning/Minor/Major/Critical). Note that you can edit the severity level of a trap using the Trap Definition Screen.
- **Group Name -** The AP Group of the Stellar AP Series Device (Stellar AP Series Devices only). **Acknowledged -** Indicates whether or not the trap has been acknowledged (True) or not acknowledged (False). See Acknowledging/Deleting Traps for more information.
- **Trap OID -** The trap object identifier number.
- **Description -** A detailed description of the trap as it appears in the MIB.
- **Synopsis -** A brief description of the trap. When a trap has variables associated with it, the values of some or all of the variables may appear in the synopsis. For example, in the trap synopsis "Link down on slot 6 port 2," the numbers "6" and "2" are trap variable values for the link down trap.
- **Source IP -** The IP address of the device that forwarded the trap to OmniVista.
- **Agent IP -** The IP address of the device that generated the trap.
- **Agent Name -** The name of the device that generated the trap, if configured.

- **Uptime -** The length of time the device that sent the trap has been up (or the amount of time since the last reset), specified in days, hours, minutes, and seconds.
- **Date/Time -** The date and time the trap was received by OmniVista Server using the OmniVista system clock. However, for traps received that are "replays" of previously-generated traps, the date/time will be adjusted to the time that the original trap was sent. This is calculated by adjusting the time received by the difference between the current upTime of the source device and the upTime contained within the trap itself. Therefore, it is possible for new traps to be added to the display with old timestamps. So, if the network was down for hours, you may suddenly see traps appear from hours ago.

Note: You can click on the "Show More" link at bottom of the pane to display specific MIB variable information contained in the trap.

Acknowledging/Deleting Specific Traps

You may want to temporarily remove traps from the display by "acknowledging" the traps, or permanently delete traps from the OmniVista Server. Select a trap(s) and click on the **ACK** button at the top of the table to remove the trap(s) from the display. (You can also hover the mouse over a trap status and click on **ACK** to acknowledge single trap.) The traps will still be stored on the OmniVista Server, but will now only by displayed when you set the "Acknowledged" filter to "True". To return an "Acknowledged" Trap to the display, select a trap(s) and click on the **UNACK** button at the top of the table. To permanently a delete trap(s) from the OmniVista Server, selecting the trap(s) and click on the **CLEAR** button at the top of the table.

You can quickly acknowledge or delete specific Severity types at once using the filter to specify a Severity level, selecting all of the traps in the table and clicking on the **ACK** or **CLEAR** button at the top of the table.

Note: Once traps are cleared, the traps are permanently removed from OmniVista.

Acknowledging/Deleting All Traps

To acknowledge all traps in the Notifications Table, click on the **Actions** button at the top of the screen, select **Ack All**, and click **OK** at the Confirmation Prompt. The traps will be removed from the display. The traps will still be stored on the OmniVista Server, but will now only by displayed when you set the "Acknowledged" filter to "True". To permanently delete all displayed traps from the OmniVista Server, click on the **Actions** button at the top of the screen, select **Clear All**, and click **OK** at the Confirmation Prompt.

Note: The **Ack All** and **Clear All** buttons are grayed out if any traps are selected in the Notifications Table. To enable the buttons, de-select the traps.

Polling Devices for Traps

To poll a device(s) for new traps click on the **Poll for Traps** button at the top of the screen to bring up the Poll for Traps window. Select the device(s) you want to poll and click on the **Poll Now** button. The device(s) will immediately be polled for traps.

Trap Definition

The Notifications Trap Definition Screen displays a list of all the supported traps as defined in the MIBs, and provides basic trap information (e.g., severity level, date/time received). Click on a trap to display detailed trap information. You can also edit a trap or reset a trap to the installation defaults.

Viewing Trap Definitions

The Trap Definitions List displays basic trap information (e.g., name, severity level). Click on a trap to display detailed trap information. You can also search for traps by entering search criteria (e.g., Name, Severity) in the "Search" field. Only those traps matching the search criteria are displayed. You can also filter the traps displayed, export the table to a .csv file, or print a copy of the table.

Basic Trap Information

- **Name -** The name of the trap as defined in the MIB.
- **Severity -** The severity level assigned to the trap in the Notifications Application's Trap Definitions Window (Normal/Warning/Minor/Major/Critical).
- **Synopsis -** A brief description of the trap.
- **Definition -** Indicates whether the trap is a "Default" trap or "Custom" trap.

Detailed Trap Information

The Detailed Information pane provides detailed information for the selected trap. If a field contains ellipsis (...), click on the field to display all of the information.

- **Name -** The name of the trap as defined in the MIB.
- **OID -** The trap object identifier number.
- **Generic ID -** The Generic Trap ID number. Only SNMPv1 traps make use of a generic ID. For SNMPv2 and SNMPv3 traps, this field will show a value of zero.
- **Specific ID -** Trap specific ID number. Only SNMPv1 traps make use of a specific ID. For SNMPv2 and SNMPv3 traps, this field will show a value of zero.
- **Severity -** The severity level assigned to the trap (Normal/Warning/Minor/Major/Critical).
- **Synopsis -** A brief description of the trap. When a trap has variables associated with it, the values of some or all of the variables may appear in the synopsis. For example, in the trap synopsis "Link down on slot 6 port 2," the numbers "6" and "2" are trap variable values for the link down trap.
- **Definition -** The trap definition.
- **Description -** A detailed description of the trap as it appears in the MIB. Click on the "Show More" link to display s detailed MIB description.

Editing a Trap

You can edit a trap Severity Level or Synopsis. To edit a trap, select the trap in the Trap Definition List and click on the Edit icon. Edit the Severity Level and/or Synopsis and click on the **Apply** button. To return the field(s) to the default settings, select the trap in the Trap Definition List, click on the **Reset** button, then click **OK** at the confirmation prompt.

Trap Responder

The Notifications Trap Responder Screen displays all configured trap responders, and is used to create, edit, or delete Trap Responders. A Trap Responder enables you to specify a response (if any) that you want

OmniVista to take when specified traps are received by OmniVista. You can specify the traps to which OmniVista will respond by IP address range, trap type, and severity level. OmniVista can make the following responses to receipt of a specified trap:

- OmniVista can send an e-mail to any address you specify. You can specify the information you want included in the e-mail through the use of variables. Variables exist for information such as the trap name, synopsis, description, etc.
- Execute an external program or script on the OmniVista Server Forward traps to a specific IP address.

Creating a Trap Responder

Click on the Add icon to open the Trap Responder Wizard. Complete the configuration as described below to configure the Agent, Trap Type, and Response. Only traps originating from the specified Agent and Trap Type will trigger the configured response. After completing all of the screens in the Wizard, click on the **Create** button.

Agent

The Agent is the IP address range or AP Group of the Responder. The Responder will only respond to traps received from this IP address range or AP Group(s).

- Agent Type
- Device - Enter an Agent Start IP and Agent End IP to specify the range.
- AP Group - Select AP Group(s).

  Note: You **must** use the "AP Group" option to configure a Trap Responder for Stellar APs. Trap Responders cannot be configured for Stellar APs using the "Device" IP Range option.

When you are finished, click the **Next** button to go the Trap Type window.

Trap Type

The Trap Type fields enable you to specify the traps to which OmniVista will respond by severity level; or, you can specify the traps to which OmniVista will respond using filters. Note that you can specify traps by severity level **or** filters, but you cannot specify traps using both severity levels and filters. (In other words, you cannot "AND" specified severity levels and specified filters to create an expression.) If you create a trap responder that specifies both severity level and filters, the trap responder will respond to all traps with the specified severity (even if they do not match the filter), and all traps that match the specified filters (even if they do not have the specified severity).

Severity Level

To select a severity level(s), move the corresponding slider to "Respond". OmniVista will send a response for any trap matching the selected severity level(s).

Filter

To use a filter, select "Any selected filter" (default) from the **Must Match** drop-down menu, then click on the **Filter** button to bring up the Filter Selection window and select a filter(s). OmniVista will send a response for any trap that matches **any** selected filter. If you select "All selected filters" from the **Must Match** drop-down menu, OmniVista will send a response for any trap that matches **all** of the selected filters.

To create a new filter, click on the Filter button to bring up the Filter Selection window, then click on the Add icon. Enter a Filter Name and optional Filter Description, then click on the "Add new condition" link to add a filter condition. Click on the "Add new condition" link to add additional conditions, if necessary. When you are finished, click on the **Add** button to add the new filter. The following conditions can be configured for filters:

- Name
- Synopsis
- Agent
- Agent Name
- Date/Time
- Severity
- SNMP Variables

When you are finished configuring the Trap Type, click the **Next** button to go the Response window.

Response

Complete the fields as described below to configure the Response action to any traps matching the configured criteria.

- **Enable Responder -** Enable (On)/Disable (Off) the Responder.
- **Description -** Enter a description for the Responder.
- **Action -** Select the action that the Responder will take if the configured criteria is met, then configure the applicable fields as described below.
- **Send an E-Mail -** Responder will send an e-mail as configured below. Be sure to configure the configure the E-Mail settings in the Preferences application (Preferences - System Settings - Email). OmniVista will not send an E-Mail Responder unless these settings have been configured.

  E-Mail To - Enter an e-mail address(es). Multiple e-mail addresses must be separated by a semi-colon (e.g., john.smith@al-enterprise.com; jane.sullivan@al-enterprise.com).

  E-Mail Subject - By default, the following is included in the E-Mail Subject Line: "OmniVista: Trap(s) Received $TrapSeverityCount$" (explained in the Trap Variables section below). You can also enter any additional information you want to include in the subject line.

  E-Mail Body - By default the variable $Details$ (explained in the Trap Variables section below) is included in the body of the e-mail. The variable automatically includes trap details in the body of the e-mail. You can also enter any additional information you want to include in the e-mail.

- **Run an Application on the Server-** Responder will run an application on the OmniVista Server as configured below.
- **Command -** The command to be executed.
- **Arguments -** The arguments to the command specified the Command field, or accept the default argument - the variable $Synopsis$ (explained in the Trap Variables section below).
- **Start Directory -** The directory in which the command will be executed.
- **Standard Input -** The standard input for the command in the **Standard Input** field, or accept the default standard input, the variable $Details$ (explained in the Trap Variables section below).
- **Forward Traps -** Responder will forward traps to the specified IP address .
- **Destination IP -** The destination IP address. Only one IP address can be entered per Responder. However, you can create multiple Responders to forward the trap to multiple recipients.
- **Destination Port -** The destination UDP port number (Default = 162).
- **Acknowledge Traps -** Responder will automatically acknowledge the trap(s). This will prevent the traps from being displayed in the Notifications Table. Acknowledged traps are only displayed in the table when the "Acknowledged" filter is set to "True".

When you are finished, click the **Next** button to go the Summary window.

Trap Variables

You can use the following variables when you configure an automatic trap responder. There are two types of variables: generic variables (which currently apply only to traps) and trap-specific variables.

Generic Variables

$Details$

For traps, this variable is equivalent to the following combination of text and trap-specific variables (trapspecific variables are described in the following section):

Trap Received: $TrapName$

Severity: $TrapSeverity$

Synopsis: $TrapSynopsis$

Agent: $TrapAgent$ Variables: $TrapVariables$

Output Example:

Trap Received: portPartitioned

Severity: Minor

Synopsis: Port jabber on slot 7 frtrunking port 1 instance 156 (port state alternated between enabled and disabled more than 50 times in 200 ms) Agent: 128.251.30.27

$Synopsis$

For traps, this variable is equivalent to the trap-specific variable $TrapSynopsis$, which is a brief description of the trap.

Output Example: Port jabber on slot 7 frtrunking port 1 instance 156 (port state alternated between enabled and disabled more than 50 times in 200 ms)

Trap Specific Variables

$TrapName$

The name of the trap (as defined in the MIB)

Output Example: portPartitioned

$TrapSynopsis$

A brief description of the trap.

Output Example: Port jabber on slot 7 frtrunking port 1 instance 156 (port state alternated between enabled and disabled more than 50 times in 200 ms)

$TrapDescription$

A detailed description of the trap (as it appears in the MIB)

Output Example: A portPartitioned trap occurs when the physical port has transitioned through enable/disable states faster than 10 times in the past second...indicative of a flaky cable.

$TrapSeverity$

The severity level assigned to the trap in the Notifications application's Trap Definitions pane. The severity level can be Normal, Warning, Minor, Major, or Critical.

Output Example: **Minor**

$TrapSeverityCount$

A summary of the trap severity counts.

Output Example: (2 Critical)

$TrapSeverityInt$

The severity level assigned to the trap in the Notifications application's Trap Definitions pane, expressed as an integer. The severity level integer can be 1 (Normal), 2 (Warning), 3 (Minor), 4 (Major), or 5 (Critical). ***Output Example:*** **3**

$TrapSnmpVersion$

The version of the trap request, either 1 (version 1) or 2 (version 2).

All traps sent with SNMP version 1 protocol are "version 1" trap requests. All traps sent with SNMP versions 2, 2c, or 3 protocol are "version 2" trap requests. There are actually two different types of trap requests (not three). The message packet in which trap requests are sent can be one of four different versions: 1, 2, 2c, or 3. When you use the AOS CLI to create a version 1 trap station, version 1 traps in version 1 protocol are sent to that station. When you use the AOS CLI to create a version 2 trap station, version 2 traps in version 2c protocol are sent to that station. When you use the AOS CLI to create a version 3 trap station, version 2 traps in version 3 protocol are sent to that station. The version 2 trap request itself is identical whether wrapped in a version 2 or version 3 packet.

Output Example: **1**

$TrapSource$

The IP address of the switch that generated the trap.

Output Example: **127.0.0.1**

$TrapUpTime$

The length of time the switch that sent the trap has been up (or the amount of time since the last reset).

Output Example: **21 hours, 35 minutes, 49 seconds**

$TrapAgent$

The IP address of the SNMP agent.

Output Example: **128.251.30.27**

$TrapAgentName$

The name of the switch that generated the trap.

Output Example: **NMS-6450**

$TrapV1Enterprise$
The enterprise name. This only applies to SNMP Version 1 traps.

Output Example: **.1.3.6.1.4.1.800.3.1.1**

$TrapV1GenericID$

The generic trap number. This only applies to SNMP Version 1 traps.

Output Example: **6**

$TrapV1SpecificID$

The enterprise trap number. This only applies to SNMP Version 1 traps.

Output Example: **10**

$TrapVariables$

Describes all of the variables in the trap.

$TrapVariable[1]$, $TrapVariable[2]$...

Accesses the first (second, etc.) variable in the trap.

$TrapVariable[someVariableName]$

Accesses the trap variable by its name.

Summary

The Summary window displays the Responder configuration. Click on the **Create** button to create the Responder. If necessary, click on the **Back** button to make any changes before creating the Responder.

Editing a Trap Responder

Select the Responder in the Trap Responder List and click on the Edit icon. Edit the Agent and Trap Type as described above, then click on the **Apply** button.

Deleting a Trap Responder

Select the Responder(s) in the Trap Responder List, click on the Delete icon, then click **OK** at the confirmation prompt.

Viewing Trap Responders

The Trap Responder List displays basic trap responder information (e.g., trap type, response description). Click on a trap responder to display more detailed formation.

- **Agent -** The network region or IP address range configured for the Responder. The Responder will only respond to traps received from this region or IP address range.
- **Trap Type -** The severity level(s) or filter(s) configured for the Responder. The Responder will only respond to traps with this (these) severity level(s) or filter(s). You can also create filters for any or all of the Responder
- **Response Description -** The user-configured Response Description.
- **Enable Responder -** Indicates whether or not the Responder is enabled (True) or disabled (False).

Trap Configuration

The Notifications Trap Configuration Screen brings up the Trap Configuration Wizard, which is used to configure network devices to send traps to the OmniVista Server. Until you configure traps, you will not be able to receive or view any trap notifications on the Notifications Home Screen. Configuring traps is a two-part process: first you select the devices for which you want to configure traps, then you specify the traps you want to be sent to the OmniVista Server. At the end of the process, OmniVista displays a summary of all the switches and traps you selected, and indicates whether the configuration was successful or not.

Note: You cannot configure traps for AOS Wireless Devices from OmniVista (only AOS Switches and Stellar AP Series Devices). However, you can configure traps on wireless devices and forward them to OmniVista for display.

Device Selection

The Device Selection window is used to select the devices/AP Groups for which you want to configure traps.

Server Information

- **IP Address (Read Only) -** The IP address of the OmniVista Server. This is automatically filled based on the OmniVista Server address you entered during installation.
- **Trap Port (Read Only) -** The destination trap port number on the OmniVista Server that receives alarms and traps. This field is automatically filled based on the Trap Port you configure on the Settings Screen.

Device Selection

- **Configure For -** Select the type of device(s) for which you will be configuring traps:
- **Device -** AOS Devices.
- **AP Group -** Stellar AP Series Devices. Traps will be configured for all APs in the group.
- **Device Type (AOS Devices only) -** If you selected "Device" above, select the device type for which you want to configure traps. This will limit the available devices displayed for selection to the selected device type. Note that, no matter which type you choose, only devices that are "available" (Up) are displayed.
- All - All available network devices are displayed.
- AOS - Only AOS devices (pre-7x) are displayed.
- AOS 7x/8x - Only AOS 7x/8x devices are displayed.
- 6200 - Only OS6200 devices are displayed.
- **Select Devices/AP Group Selection -** If you selected "Device" above, use the Switch Picker (Default) or the Topology application to select the specific devices for which you want to configure traps. If you selected "AP Group" above, select the AP Group(s) for which you want to configure traps.

Note: You cannot configure traps for wireless devices from OmniVista, However, you can configure traps on wireless devices and forward them to OmniVista for display.

When you are finished, click the **Next** button to go the Configure Traps window. Click on the **Reset Trap Configuration** button to delete the configuration and start over.

Configure Traps

The Configure Traps window is used to select the traps you want to configure for the selected devices. The traps available for each device type are different. Depending on the device(s) selected, you will have the option to configure traps for each device type.

1. If you are configuring traps for "Devices" and selected more than one device type, click on a trap type to open the Trap Configuration pane for that device type (AOS, AOS 7x/8x, 6200).
2. Configure the trap information fields at the top of the pane:
   - Trap Subscription State
     On - The OmniVista Server will be notified about traps (Default).
     Off - The OmniVista Server will not be notified about traps.
     Delete - Deletes the trap configuration information previously saved to the switch. Use the Delete option when the OmniVista Server has been moved to a different computer and now has a different IP address.
   - Save (Non-Stellar AP Series Devices only)
     All - Saves all trap configuration information specified, including port number, server IP address, selected switches, selected traps, state, and protocol.
     Port Only - Saves only the port number and no other trap configuration information. Use this save option after configuring the OmniVista Server to receive traps on a different port. Note that the port number can be changed using the Settings Screen.
     State Only - Saves only the state information (On, Off, or Delete) and no other trap configuration information. If Delete is selected, the entry for the OmniVista server is removed from the trap configuration table for the selected switches.
     Traps Only - Saves only the trap information specified. Does not save Port or State information. Protocol Only - Saves only the protocol used to send traps to the NMS server (SNMPv1, SNMPv2, or SNMPv3). Applies only to AOS Switches.
     Note: If you select one of the "Only" Save options (Port Only, State Only, Traps Only, or Protocol Only), and no trap information had previously been configured for the specified device, when you click Finish, the entire configuration will be saved. This is comparable to doing a Save "All."
     Protocol (Non-Stellar AP Series Devices only) - Select the protocol used to send traps to the NMS server (SNMPv1, SNMPv2, or SNMPv3). (Default = SNMPv3) Applies only to AOS/6200 Switches).
3. Select the traps you want to enable in the **Select Traps to Enable** area.
4. If you are configuring traps for "Devices" and selected more than one device type, click on additional trap types and repeat the above steps to configure traps for additional device types (non- Stellar AP Series Devices). When you are finished, click on the **Next** button to go to the Summary window. Click on the **Reset Trap Configuration** button to delete the configuration and return to the Devices Selection window and start over.

Summary

The Summary window displays the traps you configured. If you are configuring traps for "Devices" and selected more than one device type, click on a device type (AOS, AOS 7x/8x, 6200) to review the configuration. If necessary, click on the **Back** button to return to the Configure Traps window and make any updates. When you are finished, click on the **Finish** button. Click on the **Reset Trap Configuration** button to delete the configuration and return to the Devices Selection window and start over.

Settings

The Notifications Settings Definition Screen is used to configure Notifications and Trap E-Mail settings. After making a change to one or more of the settings as described below, click on the **Apply** button.

Notification Configuration

- **Max No. of Notifications to Store at Server -** The maximum number of received traps that can be stored on the OmniVista Server. When a trap is received that exceeds the value in this field, the newly-received trap overwrites the oldest trap stored on the server. (Range = 1,000 - 300,000).
- **Trap Port Number -** The destination trap port number on the OmniVista Server that receives alarms and traps. The number entered in the Trap Port Number field must match the port number that the switch is configured to send traps to (Default = 162).
- **Use Trap Replay Polling -** If enabled (On), OmniVista will poll all discovered devices for missing traps at startup, and will continue to periodically poll devices for missing traps (Default = On).
- **Generate OmniVista Switch Up/Down Traps -** If enabled (On), OmniVista will send Switch Up/Down traps (Default = On).

Use OmniVista Trap Absorption - If enabled (On), similar traps received from non-AOS devices during the trap absorption period are "absorbed," and a 'trapAbsorbtionTrap' trap is generated similar to existing AOS traps. This trap contains details, such as the total number of 'sufficiently-similar' traps received since the original trap. For example, if OmniVista receives a 'ChassisTrapsAlert' trap from a switch, OmniVista will 'absorb' all of the traps it receives from the same switch that are 'sufficiently similar' to 'ChassisTrapsAlert', until the trap absorption period expires. Note that **t**wo traps are considered to be "sufficiently similar" when their names, agent IP address, trap OID, severity, and enterprise OID (if defined) are same, and all their trap variables (if any) are also same. (Default = Off) • **Absorption Period -** The amount of time, in seconds, OmniVista will "absorb" similar traps. OmniVista extends the trap absorption period when a 'trapAbsorbtionTrap' trap is generated. For example, if a trap absorption period is set to 15 seconds and a 'sufficiently-similar' trap is received on the 8th second, the period for that trap is extended for another 15 seconds. If no 'sufficiently-similar' traps for a trap are received during the trap absorption period, the trap absorption period expires for that trap. (Range = 0 600, Default = 15)

- **Receive WIPS Traps –** Enables (On)/Disables (Off) receiving traps from the Wireless Intrusion Protection System (WIPS) application. (Default = On)

Trap E-Mail Configuration

The Trap E-Mail configuration fields are used to define the default values for OmniVista "trap responder" emails. Trap responder e-mails are e-mails that OmniVista generates automatically when specified traps are received from network devices. The Trap Responder Screen is used to configure OmniVista to send an email when a specified trap is received. (Traps can be specified by severity level, or by use of a filter.)

However, to prevent e-mail storms that would result from receipt of multiple traps, OmniVista does NOT send one e-mail per trap received. Rather, OmniVista "combines" responder e-mails to prevent storms. By default, OmniVista will send a "combined" responder e-mail when: one

minute has passed since the first trap was received for which an e-mail was not generated, OR 100 traps have been received.

- **Maximum Trap Limit -** The number of received traps that will trigger a trap responder e-mail. Enter the number of received traps that will trigger a trap responder e-mail.
- **Maximum Time Limit -** The maximum time period, in seconds, that can elapse before a trap responder e-mail is triggered. The time period begins when a trap is received for which an e-mail was not generated.

21.0 OV System Health

The OV System Health Screen provides an overview of the OmniVista Virtual Appliance (VA), including CPU usage, memory usage, and network traffic. It also provides information if there is a problem with the VA configuration. By default, data for the last 1 hour is displayed and refreshed every 5 minutes. However, you can modify the display and refresh rate. In addition, you can use the Settings Screen to set thresholds for trap generation as well as data retention.

VA System Health

VA Health Information

Click on one of the tabs to display Virtual Appliance information as described below.

- **CPU -** Displays the percentage of total Hypervisor CPU being used by the VA.
- **Memory -** Displays the amount of memory, in GB, being used by the VA. This includes physical memory and swap space. Click on the **View Other Charts** drop-down to display:
- **Paging -** Displays memory paging data for the VA, in Kbps. This includes pagein and pageout.
- **Memory Commit -** Percentage of committed memory being used by the VA.
- **Data Partition -** Displays the amount of Data Partition memory being used by the VA.
- **OS Partition -** Displays the amount of OS Partition memory being used by the VA.

- **Network -** Displays the amount of network traffic, in Kbps, to/from the VA. This includes Tx/Rx of all NICs on the VA (not including the Loopback interface).
- **OV Misconfiguration -** Displays details on any VA mis-configurations if applicable. Click on the **Check VM Configuration** button to re-check the configuration. OmniVista checks the following VA configuration areas:
- CPU Core
- RAM
- HDD
- CPU Reservation (only applicable for VMware ESXi with VMware Tools installed)
- Memory Reservation (only applicable for VMware ESXi with VMware Tools installed).

Viewing Options

By default, data for the last 1 hour is displayed and refreshed every 5 minutes. To change the defaults, click on the Configuration icon in the top-right corner of the screen to bring up the Configuration window. Set the field(s) as described below and click on the **Save** button.

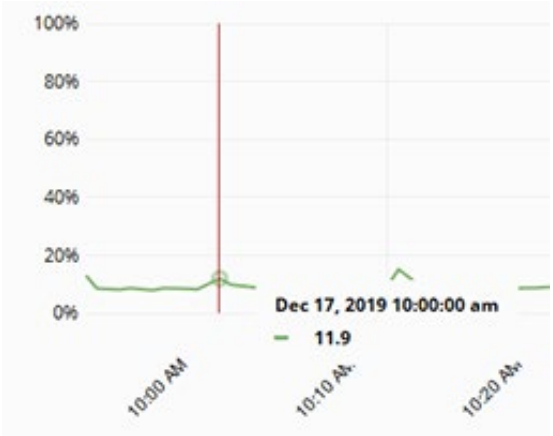
- **Interval Type**
- **Up Until Now -** Displays continuous data up to the present time (Default).

  Time Interval - The time interval displayed on the chart (Last Hour, Last 24 Hours, Last 7 Days, Last 4 Weeks).

  Auto Refresh Timer - The refresh frequency for the data display, in minutes (Range = 1 - 15, Default = 5).
- **Custom -** Click on the **Custom** button and set a start time and end time to view data for a specific time period. Click in the **Select Start Time** field, set the date on the Calendar, then click on the Clock icon to set the time. Repeat to set the End Time.

Detailed Views

Hover the mouse over a line for detailed information about that data point (as shown below). You can also view more detail for a time period on a chart by left-clicking and dragging the mouse across the time period you want to view. Click the Refresh icon at the top of the chart to return to the original view.



Settings

The OV System Health Settings Screen is used to set OmniVista Virtual Appliance (VA) Health trap thresholds, as well as data collection and retention intervals. Configure a field(s) as described below, then click on the **Save** button.

Threshold Settings

Set the trap thresholds as described below. When a configured threshold is exceeded, OmniVista will generate a trap that will be displayed in the Notifications Table.

- **CPU Utilization** - The maximum percentage of Hypervisor CPU used by the VA before a trap is sent (Range = 1 - 100, Default = 90).
- **Memory -** The maximum percentage of Hypervisor Memory used by the VA before a trap is sent (Range = 1 - 100, Default = 95).
- **Paging -** The maximum amount of memory paging, in Kbps, used by the VA before a trap is sent (Range = 1,000 - 20,000, Default = 10,000).
- **Memory Commit -** The maximum percentage of committed Hypervisor Memory used by the VA before a trap is sent (Range = 50 - 200, Default = 150).
- **Data Partition -** The maximum percentage of Data Partition used by the VA before a trap is sent (Range = 1 - 100, Default = 80).
- **OS Partition -** The maximum percentage of OS Partition used by the VA before a trap is sent (Range = 1 - 100, Default = 80).

Trap Setting

- **Waiting Time For Next Same Trap -** The amount of time, in minutes, OmniVista will wait before sending a second trap of the same type. For example, if the Waiting Time is set to 60, OmniVista will send a trap when a threshold is crossed, and if the problem persists, send another trap 60 minutes later. This will continue until the problem is resolved. (Range = 30 - 120, Default = 60).

Data Collection

- **Data Collecting Interval -** The data collection interval, in seconds. OmniVista will poll the VA according to this setting (Range = 60 - 3,600, Default = 60).
- **Data Retention -** The number of days OmniVista will retain VA Health Data. When this setting is exceeded, older data is overwritten ((Range = 1 - 90, Default = 30).

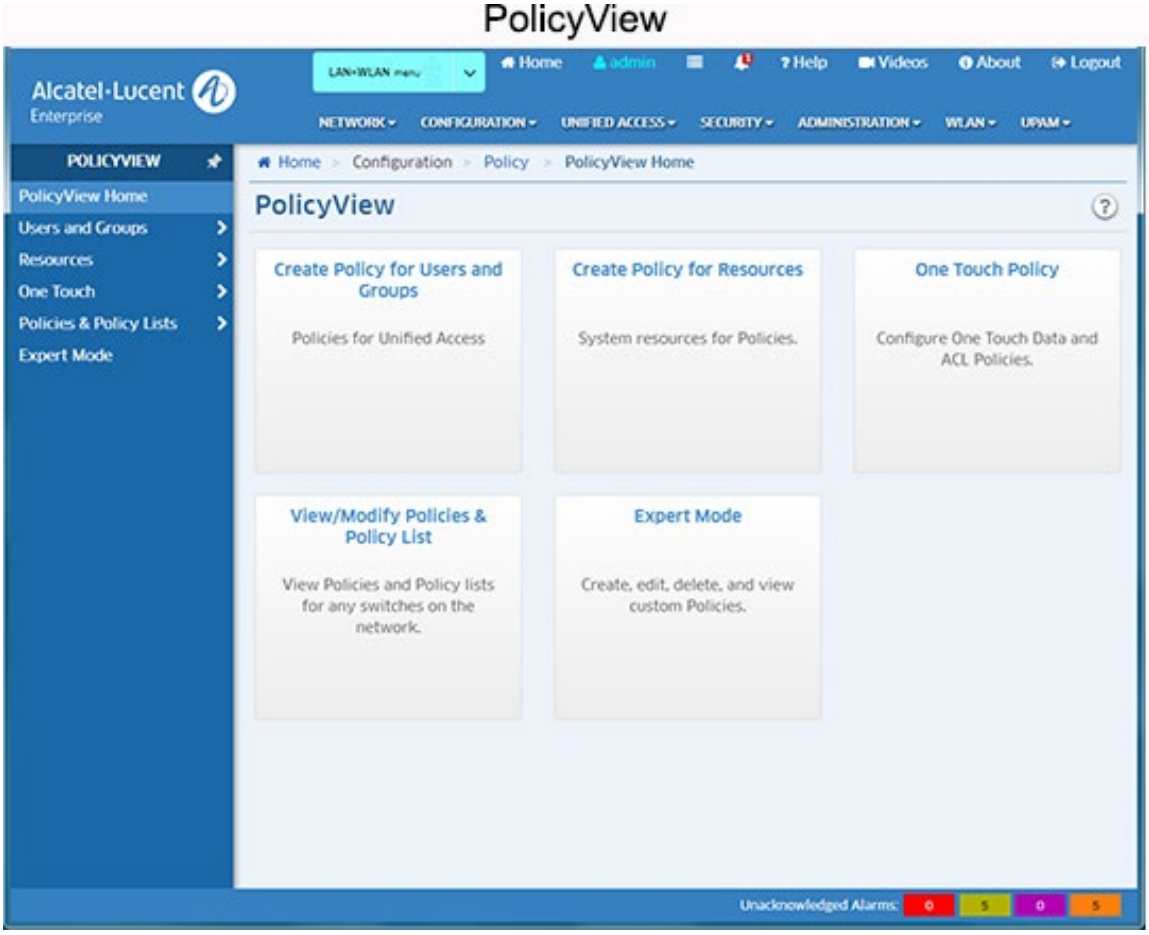
Refresh Setting

- **Widget Refresh Interval -** The refresh interval for the data displayed on the OV System Health Dashboard Widget, in minutes ((Range = 1 - 15, Default = 1).

22.0 PolicyView

The PolicyView application enables you to create Quality of Service (QoS) policies that specify QoS for network traffic. Policy rules are stored in a Lightweight Directory Access Protocol (LDAP) repository that is automatically installed with OmniVista and resides on the same device as the OmniVista Server. QoS-qualified devices in the network are notified when new or modified Policy rules are available on the LDAP repository via an SNMP interface. Software resident in the switch is responsible for retrieving the Policy rules from the LDAP repository, interpreting the Policy rules, and enforcing them on the switch.

When you first open the PolicyView application, links to the following options are displayed: Create Policies for Users and Groups, Create Policies for Resources, Create One Touch Policies, View/Modify Policies and Policy Lists, and Expert Mode.



The PolicyView application provides wizards to enable you to create specific QoS policy types (e.g., Application, Resource); and an "Expert" option that enables you to create more complex QoS Policies. These policies can be applied to all QoS-enabled devices in the list of All Discovered Devices or to selected QoS-enabled devices. These policies are created by associating a "Condition" with an "Action." A condition specifies criteria that, when true, will cause traffic to flow as specified by the associated action. A condition can specify criteria such as the following (a limited example):

- A source MAC address or a source IP address or a source VLAN ID, so that the condition applies to traffic originating from that source only

- A destination MAC address or a destination IP address or a destination VLAN ID, so that the condition applies to traffic flowing to that destination only.

An action specifies the treatment traffic is to receive when the criteria specified by the condition are true. This treatment may include the priority and bandwidth to be allocated to the traffic, its minimum and maximum output rates, and the manner in which packets are tagged upon egress from the switch (if at all).

The PolicyView application also provides a simplified "One Touch" mode that enables you to create QoS policies for data traffic and Access Control Lists (ACLs) with minimal effort and maximum simplicity. If you use the One Touch option to create QoS policies for your network, there is no need to understand the underlying QoS definitions and constructs. The One Touch modes enable you to create QoS policies without bothering with the normal complexity associated with QoS. All QoS policies created using One Touch Policies are automatically applied to all QoS-enabled devices in the list of All Discovered Devices (Topology application).

The PolicyView application supports Provisioned QoS actions. By default, Provisioned QoS provides best effort QoS in the switch. A Provisioned QoS action enables you to provide traffic with QoS other than best effort and to define the network resources, such as bandwidth and priority, to be made available to the traffic. When the criteria defined by the associated condition are true, traffic will be assigned to a queue that delivers the QoS specified by the action.

> **Important Note:** Enabling Open Flow will consume all available TCAM resources. If Open Flow is enabled, you will be unable to configure QoS Policies. Any policies created before Open Flow is enabled will still function. However, you will be unable to create new policies.

Creating Policies for Users and Groups

The Users and Groups Policy is used to create/edit Unified Access Policies. Unified Policies are QoS Policies that can be applied to both wireline and wireless devices.

Creating Policies for Resources

The Resource Policy option is used to create/edit system resources for QoS Policies. Although you can use Policy View Expert Mode to create Policies for User Network Profiles (UNP), this can be time consuming. The Resource Policy option can be used to quickly create resources and resource groups that can be turned into Policies and added to Policy Lists.

Creating One Touch Policies

PolicyView provides a One Touch option that enables you to create One Touch Data and One Touch ACL Policies for traffic with minimal effort and maximum simplicity. One Touch Data policies enable you to assign a desired quality of service - Platinum, Gold, Silver, or Bronze - to all traffic flowing to, and originating from, specific data servers. One Touch ACL Policies enable you to create ACL Policies to all traffic flowing to, and originating from, specific Network Groups.

View/Modify Policies and Policy Lists

This option enables you to view and modify all Policies and Policy Lists stored in the LDAP Server. To view the policies, click on the **Select Devices** button to open the Device Selection Wizard and select the switches you want to view. The devices will appear in the Selected

Devices Table. Select a device in the table to display the Policies and Policy Rules for the selected device.

Expert Mode

In the **Expert** mode, conditions and actions are not created automatically; and the user defines the devices to which the policies are assigned. The Expert mode enables you to create conditions and actions manually, by specifying each individual parameter. In the Expert mode, you can create conditions that specify MAC addresses, IP address, protocols, VLAN IDs, specific DSCP or TOS values, or specific 802.1 priority values.

Creating Policies for Applications

This option enables you to create Application Visibility Policies and Policy Lists for Application traffic flows.

QoS-Qualified Devices

A QoS-qualified device is a device that can support the PolicyView application and provisioned QoS. AOS devices are qualified devices. QoS-qualified devices are identified during the discovery process. The list of QoS-qualified is available and can be displayed on Expert Mode Screen.

Saving Changes to the Switch

When PolicyView is executed, it writes the address of the LDAP repository to each QoS-qualified switch in the Inventory List in the Discovery application. The LDAP address is written to the running configuration of the switch. For this reason, once PolicyView has executed, all switches are left with their running configuration in the "Unsaved" state (indicating that the running configuration has changes that have not been saved to the working directory). When a switch reboots, its running configuration is lost, so it is important to save the running configuration, and then to save the running configuration to the certified directory after PolicyView has executed. To do this, follow the steps below.

> **Note**: All changes made to the switch configuration will be saved, including any changes made via the CLI, WebView, or other OmniVista applications, in addition to the changes made by the PolicyView application.

1. Go to the Discovery application to view all discovered devices in the Managed Devices List.
2. Scroll right to the "Changes" column and sort the list according to the switch configuration state.
3. Select all switches with "Unsaved" changes. Click on the Actions drop-down and select **Save to Running**. The "Changes" field will display "Uncertified" when the changes are saved to the Running directory.
4. Select all switches with "Uncertified" changes. Click on the Actions drop-down and select **Copy Working/Running to Certified**. The "Changes" column will go blank when the Working/Running Directory is saved to the Certified Directory (this may take a few minutes).

> **Note:** You could also perform the operation above using the operations in the Topology application.

Required Traps

You must configure the switches in the network to send OmniVista the traps that are needed by the PolicyView application. To configure traps for one or more devices, go to the Topology application, select the device(s) and select **Notifications - Configure Traps** from the Operations panel. The Trap Configuration Wizard appears with the selected switches. PolicyView requires the following traps:

- 8 - policyEventNotification

Note: See the Notifications application help for step-by-step instructions for configuring traps.

Policy Precedence and Conflicts

PolicyView enables you to define the precedence of policies created in PolicyView. A policy rule's precedence determines which policy will take effect in the rare case of a conflict. QoS policies can be created through the CLI, through WebView, and through SNMP MIB browsers as well as through PolicyView. Policies created through the CLI, WebView, or MIB browsers are not written to the LDAP repository and are not manageable through the PolicyView application.

Important Note: If you are using OmniVista to create policies, do **not** use any outside management tools (including the CLI) to create/edit policies, conditions, or actions.

Policies created in PolicyView are assigned a precedence value between 30001-65535. However, precedence values 30001-65535 are not reserved for PolicyView policies. Policies can also be created using the CLI, WebView, or a MIB browser, and these policies can be assigned any precedence value between 065535. Therefore, it is possible to assign these policies the same precedence that is assigned to policies created through the PolicyView application. For this reason, if you are creating policies using PolicyView as well as outside management tools (which is NOT recommended), do not assign precedence values between 30001-65535 to any policies created outside of the PolicyView application.

- One Touch Voice policies have precedence values between 45000 and 65535.
- One Touch Data policies have precedence values between 40000 and 44999. Expert Mode policies have precedence values between 30000 and 39999.

Users and Groups Policies

The PolicyView Create Policies for Users and Groups option enables you to configure Unified Policies and Unified Policy Lists.

Unified Policies

The Unified Access Unified Policies Screen application displays configured Unified Policies and is used to create, edit, delete, and view Unified Policies. Unified Policies are QoS Policies that can be applied to both wireline and wireless devices. Unified Policies are created using a wizard that guides you through each of the steps needed to create the Policy and apply the Policy to devices in the network.

Note: Unified Policies are only displayed in the Unified Policies Table. They are **not** displayed with other configured QoS Policies in the Expert Mode Existing Policies Table.

Note: You cannot apply a policy to an IAP from the Unified Policies application. To apply a policy to an IAP, configure the policy(ies) as part of a Policy List, configure an Access Role Profile with the Policy List, and apply the profile to the device(s). Access Role Profiles are configured in the Unified Access application (Unified Access - Device Config - Access Role Profile).

Creating Unified Policy

Unified Policies are created using a wizard that guides you through each of the steps needed to create the policy and apply the policy to devices in the network. To create a Unified Policy, click on the Add icon. The wizard will then guide you through the following screens:

- **Configuration -** Basic policy configuration (e.g., Policy Name, Precedence)
- **Device Selection -** Specify the devices to which you will apply the policy
- **Set Condition -** Specify the conditions that must be true before traffic will be allowed to flow.
- **Set Action -** Specify parameters for the traffic that will flow.
- **Validity Period -** Specify the time period for the policy to be effective.
- **Review -** Review the policy details before creating the policy.

Note: As you configure a policy, conditions and actions are verified against the devices selected for the policy. If a condition or action is not supported by one of the selected devices, and error message will appear indicating the error and corrective action to be taken.

Note: If you edit a Group (e.g., MAC Group, Network Group, IP Multicast Group) that is used in a Policy Condition you cannot just re-notify devices to push the updated policy. You must create a new Group with the new configuration. Then you must edit the policy by selecting the new (modified) Group and notifying the devices.

Important Note: If you are using OmniVista to create policies, do **not** use any outside management tools (including the CLI) to create/edit policies, conditions, or actions.

Config for Policy

The Unified Policies Config for Policy Screen is used to configure basic Policy parameters. When you have completed all of the parameters, click the **Next** button at the bottom of the screen or click on Device Selection on the left side of the screen to move to the next step.

- **Name -** The Policy name.
- **Precedence -** The Policy precedence. By default, the precedence field is pre-filled with the lowest unused precedence value (Range = 0 - 65535).

Click on **Show Advanced Options** to display and configure the options below:

- **Default List -** Adds the rule to the QoS Default Policy List. (Default = No. Not supported on AOS Wireless Devices and is ignored when applied to these devices.)
- **Enabled** - Enables the policy. (Default = Yes)
- **Save -** Marks the policy rule so that it may be captured as part of the switch configuration. (Default = Yes. Not supported on Stellar AP Series Devices and is ignored when applied to these devices.) **Log Matches -** Configures the switch to log messages about specific flows coming into the switch that match this policy rule.

(Default = Yes. Not supported on Stellar AP Series Devices and is ignored when applied to these devices.)

- **Send Trap -** Enables traps for the Policy. (Default = No. Not supported on AOS Wireless Devices and Stellar AP Series Devices and is ignored when applied to these devices.))
- **Reflexive** - Enables support for the Reflexive for the policy. Reflexive policies allow specific return connections that would normally be denied. (Default = Ignore. Only supported on AOS Wireless Devices. Only "No Reflexive" is supported.)

Note: The Config for Policy Screen for Unified Policies is similar to Config for Policy Screen in Expert mode. However, Unified Policies created for Wireless Controllers will accept the "No Reflexive" option.

Device Selection

The Unified Policies Device Selection Screen is used to select the devices/AP Groups to which you want to apply the Policy. Click on the Devices **ADD** button to select devices; click on the AP Groups **ADD** button to select AP Groups. Click on an **EDIT** button to add/remove devices/AP Groups.

Click on the **Next** button at the bottom of the screen or click on Set Condition on the left side of the screen to move to the next step. If necessary, you can also click the **Back** button to return to the screen and add/delete devices.

Note: In Expert Mode, you can only select AOS Devices for Policy creation. However, you can select wireline and wireless devices when creating Unified Policies. Also note that you cannot select IAP Devices when creating Unified Policies.

Set Condition

The Unified Policies Set Condition Screen contains a list of Conditions that you can configure for the Policy (e.g., MAC Condition, IP Condition). When you create a Condition, the Condition(s) you configure must be true before traffic is allowed to flow. Click on a Condition to display the configuration options for the

Condition. (Click again on the Condition to close the configuration options.) When you have completed all of the parameters for the Condition(s), click the **Next** button at the bottom of the screen or click on Set Action on the left side of the screen to move to the next step. If necessary, you can also click the **Back** button to return to the screen.

Conditions

A brief description of each Condition is provided below. Click the hyperlink for each Condition for detailed configuration instructions.

- **L2 MACs -** Create a Condition that applies the policy to traffic originating from a MAC
- address/group/range or to traffic flowing to a MAC address/group. (Note that for Wireless Controllers, MAC Addresses cannot contain wildcard characters).
- **L3 IPs -** Create a Condition that applies the policy to traffic originating from an IP address/network group or to traffic flowing to an IP address/network group. (Note that any IP address can be masked). L3 DSCP/TOS - Create a Condition that applies the policy to traffic with a specified value in either the DSCP (Differentiated Services Code Point) byte or in the IP TOS (IP Type of Service) byte. Both DSCP

and IP TOS are mechanisms used to convey QoS information in the IP header of frames.

- **L4 Services -** Create a Condition that applies the policy to traffic flowing between two TCP or UDP ports, or to all traffic originating from a TCP or UDP port, or to all traffic flowing to a TCP or UDP port. You can also create a Condition using an existing service/service group.
- **L7 Application Visibility -** Create a Conditions that applies the policy to traffic flowing to/from an Application Group or Application.

Note: Some conditions are not supported on certain devices. Please refer to detailed notes of each condition below for supported conditions.

L2 MACs

A MAC Condition applies the Policy to traffic flowing from/to a MAC Address/Group. Note that Layer 2 Conditions (conditions that specify MAC Addresses) are "lost" when traffic passes through a router. For this reason, it may be advisable to specify other types of Conditions (such as a Layer 3 Condition, which specifies IP Addresses) when traffic is expected to travel more than one router hop.

Select the parameter(s) you want to configure by selecting the applicable checkbox. Click on **Single** to configure a single MAC Address or **Group** to configure a MAC Group, then enter a MAC address or select a MAC Group from the drop-down menu. (You can also click the Add icon to go to the **Groups** application and create a new MAC Group.)

- **Source MAC Address/MAC Group -** Configuring a Source MAC Address/Group Condition restricts the policy to traffic that flows from this MAC Address/Group only. If you do not select this option, you are effectively stating that the Source MAC Address/Group traffic is not a criterion for the policy.
- **Destination MAC Address/MAC Group -** Configuring a Destination MAC Address/Group Condition restricts the policy to traffic that flows to this MAC Address/Group only. If you do not select this option, you are effectively stating that the Destination MAC Address/Group traffic is not a criterion for the policy.
- **Source MAC Range -** Configuring a Source MAC Range Condition restricts the policy to traffic that flows from this MAC Range only. If you do not select this option, you are effectively stating that the Source MAC Range traffic is not a criterion for the policy.

Notes:

- Conditions that specify both a source and a destination MAC address may be rejected by some switch platforms as invalid. However, if you wish to create policies for both source and destination traffic, you can create one policy for the source traffic and a second policy for the destination traffic.
- MAC addresses may contain the wildcard character *. However, one * character must be entered for each individual hex digit in the MAC address: for example, **00435C:******, not **00435C:***.
- The following MAC address ranges are assigned to Alcatel-Lucent Enterprise voice devices and Alcatel-Lucent Enterprise IP phones. You can create Conditions specifying these address ranges using the MAC Address tab.
- Voice Devices

00809F3A0000 - 00809F3AFFFF
00809F3B0000 - 00809F3BFFFF
00809F3C0000 - 00809F3CFFFF

- IP Phones
  00809F3D0000 - 00809F3DFFFF
- Multi-Media Devices
  00809F3E0000 - 00809F3EFFFF
  00809F3F0000 - 00809F3FFFFF
- Source MAC Range is only supported on AOS Wireless Devices.
- Source MAC Group and Destination MAC Address/MAC Group are not supported on Wireless Controllers, and are ignored when applied to those devices.
- MAC Conditions are not supported on IAP Devices, and are ignored when applied to those devices.
- MAC Range is not supported on Stellar AP Series Devices and is ignored when applied to those devices.

L3 IPs

An IP Condition applies the Policy to traffic originating from, or flowing to, an IP Address/Network group. Any IP Address can be masked. Note that a Condition that specifies both a Source and Destination IP Address/Network Group will be rejected by the switch as invalid. However, if you wish to create policies for both Source and Destination traffic, you can create one policy for the Source traffic and a second policy for the Destination traffic.

Select the parameter(s) you want to configure by selecting the applicable checkbox. For Source/Destination IP Address, click on **Single** to configure a single IP Address (and **Shorthand** or **Subnet Mask**, if applicable), or click on **Group** to configure a Network Group, then enter an IP Address or select a Network Group from the drop-down menu. (You can also click the Add icon to go to the **Groups** application and create a new Network Group.)

- **Fragment (only available for AOS Switches) -** Select this checkbox to restrict the policy to TCP packet fragments.
- **Source IP Address/Network Group -** Configuring a Source IP Address/Network Group Condition restricts the policy to traffic that flows from this IP Address or Subnet Mask/Network Group only. If you do not select this option, you are effectively stating that the Source IP Address or Subnet Mask/Network Group traffic is not a criterion for the policy.
- **Destination IP Address/Network Group -** Configuring a Destination IP Address/Network Group Condition restricts the policy to traffic that flows to this IP Address/Network Group only. If you do not select this option, you are effectively stating that the Destination IP Address or Subnet Mask/Network Group traffic is not a criterion for the policy.
- **Multicast IP Address Range (not available for Wireless Controllers) -** Configuring a Multicast IP Address/Group Condition restricts the policy to traffic that flows to this IP Multicast Address Group only. If you do not select this option, you are effectively stating that the Destination IP Multicast Address or Subnet Mask/Group traffic is not a criterion for the policy.

Notes:

- When configuring an IP Address Condition, you can also click either the **Shorthand Mask** or **Subnet Mask** button to configure a Subnet Mask. If you are using a Shorthand Mask, select a value from the Shorthand Mask drop-down list. If you are using a full Subnet Mask, enter the mask in the IP Subnet Mask field. Note that the * wildcard character is not allowed in IP addresses.
- Short Hand Mask and Group are ignored when applying Unified Policies to Wireless
- Controllers or IAPs, and is ignored when applied to those devices. Source IP Address Range is not supported on IAP devices and is ignored when applied to those devices.
- Stellar AP Series Devices only support IPv4 conditions.

Important Note: When creating an IP Condition for a **NAT** Action you must specify a Network Group in the Condition. NAT will only work when both the Condition and Action specify network groups. To create a "One-to-Many" Condition and action, create a Network Group with a single entry for the Condition.

L3 DSCP/TOS

A DSCP/TOS Condition applies the Policy to incoming traffic that has a specified value in either the DSCP (Differentiated Services Code Point) byte or in the TOS (Type of Service) byte. Both DSCP and TOS are mechanisms used to convey QoS information in the IP header of frames. DSCP and TOS are mutually exclusive - you can use either DSCP or TOS but not both. Click on the applicable button (DSCP or TOS) and enter a value.

- **DSCP -** Defines the QoS treatment a frame is to receive from each network device. This is referred to as per-hop behavior. If you are using DSCP, you can define any value in the range 0 - 63 as the DSCP value in the IP header of the frame. Traffic that contains this value will match this condition.
- **TOS -** A TOS value creates a condition that applies the policy to traffic that has the specified TOS value in the IP header of frames. Enter any value from 0 - 7 to specify the value of the precedence field in the TOS byte that will match this condition. A value of 7 has the highest precedence and a value of 0 has the lowest.

Notes:

- Please refer to the Switch Release Notes for information on the specific QoS functions available on various current platforms and combinations of hardware/firmware.
- You cannot create a policy condition based on DSCP or TOS values for Wireless Controllers/IAPs. DSCP/TOS conditions are ignored when applying Unified Policies to Wireless Controllers/IAPs.

L4 Services

A Service Condition applies the policy to Service Protocol traffic (TCP or UDP) flowing from/to two TCP or UDP ports, or to traffic flowing from/to a TCP or UDP Service or Service Group. Select a type of Service Condition you want to configure, then configure the parameter(s) as described below.

- **Protocol Only -** Select **TCP** or **UDP** to create a condition for a Service Protocol only.

- **Port(s) -** To configure the Condition for a specific Service Port, select a **Source** and **Destination** Port from the drop-down menu to specify a specific port for the service you selected. You can also click on the Add icon to go to the Groups application and create new Service Ports.
- **Service -** Select a Service from the drop-down menu. You can also click on the Add icon to go to the Groups application and create a new Service.
- **Service Group -** Select a Service Group from the drop-down menu. You can also click on the Add icon to go to the Groups application and create a new Service Group.

Notes:

- Wireless Controllers do not have source and destination ports. They only contain a unique service port. Therefore, you cannot specify both Source and Destination port for Wireless Controllers.

L7 Application Visibility

An Application Visibility Condition applies the policy to traffic flowing to/from an Application Group or Application. Note that the drop-down menus are populated with the Application Groups/Applications contained in the Signature Profile for the selected switch. If you select multiple switches, only those Application Groups/Applications common to all switches will be displayed. Also note that the **App Name** button will not be displayed if you select any OS6900 Switches, as this option is not offered for these devices. If all of the selected switches are OS6860 devices, both the **App Group** and **App Name** buttons are displayed.

- **App Group -** Select an Application Group from the drop-down menu.
- **App Name -** Select an Application from the drop-down menu.

Note: The Application Visibility Condition is not supported on AOS Wireless Devices and will not be displayed if only these devices are selected.

Set Action

The Unified Policies Set Action Screen contains a list of Actions that you can configure for the Unified Policy (e.g., QoS, NAT). A Policy Action enables you to specify the treatment traffic is to receive when it flows. This includes the priority the traffic will receive, its minimum and maximum output rates, and the values to which specified bits in the frame headers will be set upon egress from the switch. When the Conditions specified by the Policy Condition are true, traffic will flow as specified by the Policy Action.

Click on an Action to display the configuration options for the Action. (Click again on the Action to close the Action.) When you have completed all of the parameters for the Action(s), click the **Next** button at the bottom of the screen or click on Validity Period on the left side of the screen to move to the next step. If necessary, you can also click the **Back** button to return to the screen.

Actions

A brief description of each Action is provided below. Click the hyperlink for each Action for detailed configuration instructions.

- **QoS -** Create an Action to specify QoS actions to impose on traffic that meets the configured policy condition(s). When the conditions specified by the policy are true,

traffic will flow as specified by the policy action. Quality of Service applies to Session Type for wireless devices. Quality of Service is not supported on IAP devices and is ignored when applied to those devices.

- **TCM -** Create an Action to specify Tri-Color Marking (TCM) actions to impose on traffic that meets the configured policy condition(s). TCM provides a mechanism for policing network traffic by limiting the rate at which traffic is sent or received on a switch interface. TCM meters traffic based on user-configured packet rates and burst sizes and "marks" the metered packets as green, yellow, or red based on whether the traffic meets the configured rates. This "color marking" determines the packet's precedence when congestion occurs. TCM is not supported on wireless devices and is ignored when applied to those devices.

QoS

The QoS Policy Action option enables you to specify QoS actions to impose on traffic that meets the configured policy condition(s). When the conditions specified by the policy are true, traffic will flow as specified by the policy action.

- **Disposition -** Set the Action to **Accept** or **Drop** traffic that meets the configured condition(s).
- **Quality of Service (QoS) Parameters -** Specify the QoS priority the traffic will receive if it meets the configured condition(s).
- **Platinum** priority provides the highest quality of service (and maps to a firmware priority of 7).
- **Gold** provides the next-highest quality of service (and maps to a firmware priority of 5).
- **Silver** provides the next-highest quality of service (and maps to a firmware priority of 3).
- **Bronze** provides the same quality of service as best effort (and maps to a firmware priority of 1). A separate egress queue is maintained in the hardware for traffic of each different priority.
- **Output Flow Setting** (not supported on IAP Devices and is ignored when applied to those devices)
- **Max Output Rate (kbits/sec) -** Specify the maximum amount of traffic, in kilobits-per-second, which is guaranteed to be transmitted from the port. Even if no other traffic exists, the output will be limited to the rate specified here.
- **Set Color of Packet -** Enables/Disables Three Color Marking (TCM) for output traffic flows. This parameter is not supported on AOS Wireless Devices or Stellar AP Series Devices and is ignored when applied to those devices.
- **Output Mapping** (not supported on IAP Devices and is ignored when applied to those devices)
- **802.1p Priority Level -** If you want outgoing packets tagged with an 802.1p priority level, set the **802.1p Priority Level** field to any value between 0 to 7 to specify the desired outgoing 802.1p priority for the traffic. A value of **7** indicates the highest priority and a value of 0 indicates the lowest priority. Note that for ports that are configured for 802.1q, this value is used in the 802.1q header and indicates the outgoing priority of the frame. When a frame is de-queued for transmission, it is assigned the priority of the queue and mapped to the outgoing 802.1p priority. This

priority is combined with the VLAN group ID to create the 802.1p/q header for transmission. Note that if traffic matches the criteria specified by the policy condition, but the outgoing port does not support 802.1p tagging, the policy action will fail. This parameter is not supported on AOS Wireless Devices and is ignored when applied to those devices.

- **DSCP/TOS -** Enable/Disable DSCP/TOS Precedence. The TOS byte is defined in RFC 791. This byte contains two fields. The precedence field is the three high-order bits (0-2) and is used to indicate the priority for the frame. The type of service field (bits 3-6) defines the throughput, delay, reliability, or cost for the frame; however, in practice these bits are not used. If you enable the **TOS Precedence** radio button, set the associated field to any value from 0-7 to specify the value that will be inserted into the precedence field of the TOS byte upon egress from the switch. A value of 7 has the highest precedence and a value of 0 has the lowest precedence. Note that you can enable **either** the DSCP or the TOS Precedence radio button to specify the mechanism you want to use (if any) to convey QoS information in the IP header of frames. DSCP and TOS are mutually exclusive. You can use either DSCP or TOS, but not both. This parameter is not supported on AOS Wireless Devices and is ignored when applied to those devices.

TCM

The TCM Policy Action option enables you to specify Three-Color Marking (TCM) actions action to impose on traffic that meets the configured policy condition(s). TCM provides a mechanism for policing network traffic by limiting the rate at which traffic is sent or received on a switch interface. TCM meters traffic based on user-configured packet rates and burst sizes and "marks" the metered packets as green, yellow, or red based on whether the traffic meets the configured rates. This "color marking" determines the packet's precedence when congestion occurs. TCM is not supported on AOS Wireless Devices and is ignored when applied to those devices.

- Committed Traffic Policing
- **Committed Information Rate -** The guaranteed bandwidth, in bits-per-second, for all traffic that ingresses on the port.
- **Peak Information Rate -** The peak bandwidth, in bits-per-second, for all traffic that ingresses on the port.

Validity Period

The Unified Policies Validity Period Screen enables you to add a validity period to a condition by specifying the time periods when the policy is active and enforced. Select a validity period from the **Validity Periods** drop-down list:

- **AllTheTime -** The policy will be enforced all days of the week, all months of the year, and all hours of the day.
- **Weekdays** - The policy will be enforced on weekdays (Monday - Friday), all months of the year. Each weekday is 24 hours (midnight to midnight).
- **Weekends -** The policy will be enforced on Saturday and Sunday, all months of the year. Each Saturday and Sunday is 24 hours (midnight to midnight).
- **WorkingDay -** The policy will be enforced on weekdays (Monday - Friday), from 9:00 a.m. to 5:00 p.m., all months of the year.

- **Custom -** Select to create a custom validity period by specifying specific days, months, and times.

When you have completed all of the parameters, click the **Next** button at the bottom of the screen or click on Review on the left side of the screen to move to the next step. If necessary, you can also click the **Back** button to return to the screen.

> **Note**: The pre-configured validity period **AllTheTime** is the default and is automatically assigned to the condition when the **Ignore Validity Period in defining Policy Condition** checkbox is checked. You can configure a validity period when configuring an IP Condition or Service
>
> Condition. If you do not specify an IP or Service Condition, the configured period is not applied for Wireless Controllers.

Advanced Wireless Settings

For Wireless Controllers, you can specify an absolute period or a periodic period.

- **Absolute**- Specifies an absolute time range, with a specific start and/or end time and date.
- **Periodic** - Specifies a recurring time range. Specify the start and end time and all days or selected days of the week.

Review

The Unified Policies Review Screen is used to review the Policy configuration before saving the Policy. After reviewing the Policy, click the **Create** button to save the policy to the LDAP Server. You can also click the **Back** button to return to a previous screen.

Applying a Unified Policy to the Network

After configuring and saving a policy(ies), you must apply the policy(ies) by notifying devices/AP Groups in the network. If you click **Notify All**, all of the policies listed in the Existing Policies Table are applied to all of the devices/AP Groups configured for each policy. To apply the policy(ies) only to certain devices/AP Groups, click on the Devices **ADD** button to select devices, click on the AP Groups **ADD** button to select AP Groups, then click on **Notify Selected**.

After notifying the devices, you can view the status of the re-cache operation, by clicking on the **Status** button to view the Devices Pending Notification Table. In addition, you can view the success or failure of the re-cache operation for each switch in the policy.log file of the Audit application, including an indication of any error that may have occurred. Note that the re-cache operation for each switch occurs in a separate thread and may take some time. Any errors that occur will also be reported in the server.txt file, in the Audit application.

> **Note:** When you notify network switches, all QoS-enabled switches flush their policy tables and reload policies from the LDAP repository, which is very expensive in terms of switch resources and time. It is recommended that you review all policies that you have created and apply them at the same time to minimize switch downtime.

Editing a Unified Policy

To edit a policy, select the policy in the Existing Unified Policies Table and click on the Edit icon. Use the wizard to make any edits. When you are done, apply the edited policy to the network.

Note that if you modify a policy and select different device types at the Device Selection Step (AOS/Wireless), a warning dialog will be displayed if the condition in the policy is not supported on one of the selected device types. For example: *"Condition mis-match: condition (L2 MACs and L4 Service) is not valid for selected device. Do you want to remove the mis-match conditions?"* If you select **Yes**, the mis-matched conditions will be removed from edited policy. Otherwise, the newly selected devices will be removed from Device Selection list.

Deleting Unified Policy

To delete a policy(ies), select the policy(ies) in the Existing Unified Policies Table, click on the Delete icon, then click **OK** at the confirmation prompt.

> **Note:** Deleting a policy(ies) in the Existing Unified Policies Table will not automatically update policy(ies) on any switch that contain this policy(ies). To delete a policy(ies) on switch, select an option from the drop-down menu (Use Switch Picker/Use Topology), click on the **Select Device** button and select the device(s), then click the **Notify Selected** button.

Policy Information

The Existing Unified Policies Table displays information for all configured policies. You can also click on a policy to view detailed information about the Policy (e.g., Condition, Action).

- **Policy Name -** The name of the Policy.
- **Scope -** The scope of the Policy (e.g., IP Filtering, Provisioned).
- **Precedence -** The Precedence value of the Policy (0 - 65535).
- **Enable -** Indicates whether or not the Policy is enabled.
- **Save -** Indicates whether or not the rule will be recorded during a snapshot command.
- **Log Matches -** Indicates whether or not matches to this rule are logged in the QoS Log.
- **Reflexive -** Indicates whether or not the Policy is reflexive. Reflexive Policy Rules allow specific return connections that would normally be denied (Yes/No).
- **Default List-** Indicates whether or not the Policy is saved to the Default Policy List. By default, a Policy Rule is added to this list when it is created. A Policy Rule remains a member of the Default List even when it is subsequently assigned to additional Policy Lists.
- **SLA Policy Trap -** Indicates whether or not an SLA Policy Trap is configured for the policy.

Unified Policy List

The PolicyView Unified Policy List Screen displays all configured Unified Policy Lists, including the Unified Policies included in each list, and is used to create, edit, delete, view and apply Unified Policy Lists. A Unified Policy List is a set of Unified Policies that are grouped together

and assigned to devices as a group. A Unified Policy List can be applied to AOS Switches, Stellar APs, or ClearPass Servers. For IAPs, a Policy List must be applied as part of an Access Role Profile. Access Role Profiles are configured in the Unified Access application (Unified Access - Device Config - Access Role Profile).

Unified Policy List Information

The following information is displayed for each Unified Policy contained in the Unified Policy List. (Click on a Unified Policy List to display the Unified Policies contained in the list.)

- **Name -** The name of the Unified Policy.
- **Condition -** The Unified Policy Condition information (e.g., IP Policy Condition would display the Source/Destination/Multicast IP address of the condition).
- **Action -** The Unified Policy Action to take if the traffic matches the Policy condition (e.g., QoS Accept/Drop)
- **Precedence -** The Precedence value of the Unified Policy (0 - 65535).
- **Validity Period -** The configured validity period for the Unified Policy.

Creating a Unified Policy List

Click on the Add icon. The Create Unified Policy List Wizard appears. Complete the screens as described below, then click on the **Create** button.

Config for Policy List

Enter a **Name** for the Unified Policy List and select the Unified Policies you want to include in the list from the **Add Unified Policies** drop-down menu. (All of the currently-configured Unified Policies appear in the list. You can also click the Add icon to go to Unified Policies Screen and create a new Unified Policy(ies) to add to the list.) When you select a Unified Policy from the drop-down menu, the Unified Policy will appear in a table below, so you can review the Unified Policy and modify the Precedence value, if needed.

If you are assigning a Policy List to AOS Switches, AOS Wireless Devices, and Stellar AP Series Devices, select an option from the drop-down menu at the bottom of the table to override the default behavior of the devices. The default behavior for traffic that does not match a policy is different for AOS Switches, AOS Wireless Devices, and Stellar AP Series Devices. For AOS Switches and Stellar AP Series Devices, the default behavior is to "accept" the traffic. For AOS Wireless Devices, the default behavior is to "deny" the traffic. For example, if you create a Source IP Policy for a single IP address, by default AOS Switches and Stellar AP Series Devices would accept traffic that does not come from that IP address while AOS Wireless Devices would drop the traffic.

- **OV-L3-AcceptAllPolicy -** Traffic that does not match any of the policies will be accepted on all devices.
- **OV-L3-DenyAllPolicy -** Traffic that does not match any of the policies will be denied on all devices.
- **Device-Default -** Traffic that does not match any of the policies will be accepted/denied according to the device's default behavior. If you do not make a selection from the drop-down menu, this option is automatically used.

Review the Policy List configuration(s) in the table, then click the **Create** button. The new Unified Policy List will appear on the Unified Policy Lists Screen.

Note: The Wireless User Role contains a QoS rule and an Access List, which is a set of ACLs. For User Role, Wireless Controllers support two (2) QoS attributes - Bandwidth Contract - Upstream and Downstream. However, OmniVista only supports configuring Downstream Bandwidth. Additionally, the User Role can contain only a single Bandwidth Contract. So if the Unified Policy List contains more than one QoS Rule, OmniVista will display an error message: "Unified Policy List can't contain more than one QOS Action."

Device Selection

The Device Selection Screen is used to select the devices/AP Groups to which you want to apply the Policy List. Click on the Devices **ADD** button to select devices; click on the AP Groups **ADD** button to select AP Groups. Click on an **EDIT** button to add/remove devices/AP Groups.

Applying a Unified Policy List to the Network

After configuring and saving a policy list, you must apply policy list by notifying devices/AP Groups in the network. If you click **Notify All**, all of the policy lists are applied to all of the devices/AP Groups configured for each policy. To apply the policy list only to certain devices/AP Groups, click on the Devices **ADD** button to select devices, click on the AP Groups **ADD** button to select AP Groups, then click on **Notify Selected**.

Note: A Unified Policy List can be applied to wireless devices as part of an Access Role Profile.

After notifying the devices, you can view the status of the re-cache operation, by clicking on the **Status** button to view the Devices Pending Notification Table. In addition, you can view the success or failure of the re-cache operation for each switch in the policy.log file of the **Audit** application, including an indication of any error that may have occurred. Note that the re-cache operation for each switch occurs in a separate thread and may take some time. Any errors that occur will also be reported in the server.txt file, in the **Audit** application.

Note: When you notify network switches, all QoS-enabled switches flush their policy tables and reload policies from the LDAP repository, which is very expensive in terms of switch resources and time. It is recommended that you review all policies that you have created and apply them at the same time to minimize switch downtime.

Editing a Unified Policy List

You can edit the Unified Policies included in a Unified Policy List or edit the Precedence value of any Unified Policy in the list. Select a Unified Policy List and click on the Edit icon. The Edit Unified Policy List Screen appears. Click on the **Add Unified Policies** drop-down menu. (All of the currently-configured Unified Policies appear in the list. You can also click the Add icon to go to Unified Policies Screen and create a new Unified policy(ies) to add to the list.) Select/ unselect Unified Policies to add/remove them from the Unified Policy List. When you are finished editing the Unified Policy, click the **Update** button. The updated Unified Policy List will appear on the Unified Policy Lists Screen.

Deleting a Unified Policy List

To delete a Unified Policy List(s), select the list(s), click on the Delete icon, then click **OK** at the confirmation prompt. Note that you cannot delete a Unified Policy List that is associated with an Access Role Profile. To delete the list, you must first remove it from associated Access Role Profile.

Note: Deleting a Unified Policy List(s) will not automatically update policy list(s) on any switch that contain this policy list(s). To delete a policy list(s) on switch, select an option from the drop-down menu (Use Switch Picker/Use Topology), click on the **Select Device** button and select the device(s), then click the **Notify Selected** button.

Unified Policy List Information

Click on a Unified Policy List to display the information about the Policies contained in the list. The following information is displayed for each Unified Policy contained in the Unified Policy List.

- **Policy Name -** The name of the Policy.
- **Action -** The Policy Action to take if the traffic matches the Policy condition (e.g., QoS Accept/Drop)

Resource Policies

The PolicyView Create Policy for Resources option enables you to configure Resource/Resource Group QoS Policies. Although you can use the QoS Expert Mode option to create Policies for User Network Profiles (UNP), this can be time consuming. Resources and Resource Groups can be used to quickly create Resources that can be turned into Policies and added to Policy Lists.

When you select "Create Policy From Resources" from the main PolicyView screen, the Add To Policy List Screen appears. You can use this screen to create a policy using an existing Resource/Resource Group and add it to a Policy List. If necessary, you can click on the Resource or Resource Group link on the left side of the screen to create a new Resource or Resource Group.

Add to Policy List

The PolicyView Add to Policy List Screen is used to create a policy from Resource or Resource Group and assign the policy to a Policy List.

Creating a Resource Policy

Click the checkbox next to the **Resource** or **Resource Group** Field and select an existing Resource or Resource Group from the drop-down menu (You can also click the Add icon to go to the Resource or Resource Group screen and create a new Resource/Resource Group, before returning to this screen to select it.) Configure the remaining fields as described below, then click the **Create** button.

- **Precedence -** Set the Precedence for the Policy.
- **Action -** Set the action to be taken for the traffic if the conditions match the policy:
- **Accept -** Accept the traffic.
- **Drop -** Drop the traffic
- **Platinum -** Apply Platinum Precedence to the traffic.
- **Gold -** Apply Gold Precedence to the traffic.

- **Silver -** Apply Silver Precedence to the traffic.
- **Bronze -** Apply Bronze Precedence to the traffic.
- **Policy List -** Select an existing Policy List from the drop-down menu to associate with the Policy. You can also click the Add icon to go to the Policy List screen and create a new Policy List, before returning to this screen to select it.

After creating the Resource Policy, click on the **Notify All** button to add the Resource/Resource Group to the Policy List and notify the switches in the network. To view the status of the re-cache operation, click on the **Status** button to view the Devices Pending Notification Table. In addition, you can view the success or failure of the re-cache operation for each switch in the policy.log file of the Audit application, including an indication of any error that may have occurred. Any errors that occur will also be reported in the server.txt file, in the Audit application. Note that the re-cache operation for each switch occurs in a separate thread and may take some time.

> **Important Note:** Clicking the **Notify All** button causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP Server, which is very expensive in terms of switch resources and time. Any switch to which the Policy List has already been assigned will also recache its policy tables.

Resource

The PolicyView Resource Screen displays information for all configured Resources, and is used to create, edit, or delete a Resource. A Resource is created by specifying a name, Destination IP/Subnet, and/or a Service Group for the Resource.

Creating a Resource

Click on the Add icon. Enter a **Name** for the Resource then. Select the **Destination IP Address** checkbox and enter a **Destination IP** and **Destination Subnet**, and/or select the **Destination Service Group** checkbox and select an existing **Service Group** from the drop-down menu. (You can also click the Add icon to go to the **Groups** application and create a new Service Group for the Resource). Click **OK** to save the Resource configuration.

Once the Resource is defined and saved, the corresponding LDAP Policy Rules, with a default initial precedence value of “50000” (which can be modified), an action of “Accept” and validity period of “AllTheTime”, is created and saved to the LDAP Server.

Editing a Resource

To edit parameters for an existing Resource, select the Resource in the Resource List and click on the Edit icon. Edit the Destination IP Address and/or Destination Service Group parameter(s), then click **OK**. You cannot edit the Resource Name, you can only delete the Resource and create a new one.

Deleting a Resource

To delete a Resource, select the Resource(s) in the Resource List and click on the Delete icon, then click **OK** at the confirmation prompt.

Resource Group

The PolicyView Resource Group Screen displays information for all configured Resource Groups, and is used to create, edit, or delete a Resource Group from existing Resources.

Creating a Resource Group

Click on the Add icon. Enter a **Name** for the Resource Group and select a Resource(s) from the list of Resources. (You can also click the Add icon to go to the Resource Screen and create a new Resource, before returning to this screen to select it.) Click **OK** to save the Resource Group configuration.

Once the Resource Group is defined and saved, the corresponding LDAP Policy Rules, with a default initial precedence value of “50000” (which can be modified), an action of “Accept” and validity period of “AllTheTime”, is created and saved to the LDAP Server.

Editing a Resource Group

To edit parameters for an existing Resource Group, select the Resource Group in the Resource Group List and click the Edit icon. Add/delete Resources to/from the Resource group, then click **OK**. You cannot edit the Resource Group Name, you can only delete the Resource Group and create a new one.

Deleting a Resource Group

To delete a Resource Group, select the Resource Group(s) in the Resource Group List and click on the Delete icon, then click **OK** at the confirmation prompt.

One Touch Policies

The PolicyView QoS One Touch option enables you to quickly create One Touch Data, ACL, and Voice Policies for network traffic. One Touch Data Policies enable you to assign a desired quality of service Platinum, Gold, Silver, or Bronze - to all traffic flowing to, and originating from, specific Data Servers. One Touch ACL Policies enable you to create ACL Policies for all traffic flowing to, and originating from, specific

Network Groups. All policies created are applied to all QoS-enabled devices in the List of All Discovered Devices. (You can use the Expert mode if you need to assign a different priority to any server.)

When you select "One Touch Policy" from the main PolicyView screen, the One Touch Data Screen appears. Click on the One Touch ACLs link on the left side of the screen to configure One Touch ACL Policies. Click the One Touch Voice link on the left side of the screen to configure One Touch Voice Policies.

One Touch Data Policies

The PolicyView One Touch Data Screen displays all of the Data Servers that have been configured with a One Touch Data Policy and the status of the policy on the LDAP Server:

- **Saved -** The policy has been successfully written to the LDAP Server.
- **Unsaved -** The new policy, or modified policy has not been saved to the LDAP Server
- **Error -** An error condition has made it impossible to write the policy to the LDAP Server.

The screen is used to create, edit, or delete one of the following One Touch Data Policies:

- **Platinum** - provides the highest quality of service (and maps to a firmware priority of 7)
- **Gold** - provides the next-highest quality of service (and maps to a firmware priority of 5)
- **Silver** - provides the next-highest quality of service (and maps to a firmware priority of 3)
- **Bronze** - provides the same quality of service as best effort (and maps to a firmware priority of 1)

Creating a One Touch Data Policy

Select a Priority from the drop-down menu, then click on the Add icon. Enter the IP address of the Data Server in the **Server IP Address** field, and click **Create**. The Data Server will appear in the table with the Status "Unsaved". Click on the Save icon ✔, to save the Policy to the LDAP Server. The Priority selected will be applied to all Data Servers in the table. When you are finished, click on **Notify All** to apply the policy to all of the switches in the network.

> **Important Note:** Clicking the **Notify All** button causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP Server, which is very expensive in terms of switch resources and time. If any One Touch Data policy has already been defined, the switch(es) to which the policy is assigned will also re-cache its policy tables. **It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime**.

Applying a One Touch Data Policy

When you click the **Notify All** button, the policy(ies) is applied to all switches in the network. To view the status of the re-cache operation, click on the **Status** button to view the Devices Pending Notification Table. In addition, you can view the success or failure of the re-cache operation for each switch in the policy.log file of the **Audit** application, including an indication of any error that may have occurred. Any errors that occur will also be reported in the server.txt file, in the **Audit** application. Note that the re-cache operation for each switch occurs in a separate thread and may take some time.

Editing a One Touch Data Policy

Select a Priority from the drop-down menu. The status of all of the Data Servers in the table will change to "Unsaved". Click on the Save icon ✔, to save the Policy to the LDAP Server. The Priority selected will be applied to all Data Servers in the table. When you are finished, click on **Notify All** to apply the policy to all of the switches in the network.

> **Important Note:** Clicking the **Notify All** button causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP Server, which is very expensive in terms of switch resources and time. If any One Touch Data policy has already been defined, the switch(es) to which the policy is assigned will also re-cache its policy tables. **It is recommended that you verify all policies that you have edited and apply them at the same time to minimize switch downtime**.

Deleting One Touch Data Policy

To delete a One Touch Data Policy(ies), select the server(s) in the table and click on the Delete icon, then click **OK** at the confirmation prompt. When you click the **OK** button:

- All One Touch Data policies for the servers you selected are removed from the LDAP Server. All One Touch Data policies for the servers you selected are removed from switch attributes in the LDAP "role" objects.
- The server(s) are removed from the table.
- A confirmation message is displayed when the LDAP Server has been successfully updated. The success of the operation is also reported in the policy.log file in the **Audit** application.
- An SNMP message is sent to each QoS-qualified device in the List of All Discovered Devices, informing that the information in the LDAP repository has changed and commanding the devices to update their cached policies with the current information from the LDAP repository. Note that the re-cache operation for each switch occurs in a separate thread and may take some time. Be sure to check the policy.log file in the **Audit** application for the re-cache status of each switch.

Example of a New One Touch Policy (or Edit Policy) Operation

Let's say **Platinum** was selected as the priority for the following two Server IP addresses:

164.178.32.107

164.178.33.51

When saved, the following policies are created and written to the LDAP Server:

OneTouchDR$S164.178.32.107

Condition specifies traffic originating from source IP address 164.178.32.107.

Action specifies Platinum QoS for this traffic.

OneTouchDR$D164.178.32.107

Condition specifies traffic transmitted to destination IP address 164.178.32.107.

Action specifies Platinum QoS for this traffic.

OneTouchDR$S164.178.33.51

Condition specifies traffic originating from source IP address 164.178.33.51.

Action specifies Platinum QoS for this traffic.

OneTouchDR$D164.178.33.51

Condition specifies traffic transmitted to destination IP address 164.178.33.51.

Action specifies Platinum QoS for this traffic.

Please note that the names beginning with "OneTouchDR" are the names used for the policies in the LDAP Server. Within the PolicyView QoS application, all One Touch Data policies are referred to by the generic composite name **OneTouchDR**, no matter how many individual One Touch Data policies have been written to the LDAP Server. One Touch Data rules that have been created automatically by PolicyView can be viewed in the Expert mode window.

One Touch ACL Policies

The PolicyView One Touch ACLs Screen displays all of the Network Groups that have been configured with a One Touch ACL Policy, as well as the Accessibility configured for the policy (Accept/Drop), and status of the policy on the LDAP Server.

- **Saved -** The policy has been successfully written to the LDAP Server.
- **Unsaved -** The new policy, or modified policy has not been saved to the LDAP Server
- **Error -** An error condition has made it impossible to write the policy to the LDAP Server.

The screen is used to create, edit, or delete a One Touch ACL Policy for a Network Group.

Creating a One Touch ACL Policy

Click on the Add icon. Select an existing Network Group from the **ACL IP Server Group** drop-down menu, and an **Accessibility** option for the group (Accept/Drop), and click **Create**. The One Touch ACL Policy will appear in the table with the Status "Unsaved". Click on the Save icon ✔ to save the Policy to the LDAP Server. The Priority selected will be applied to all Data Servers in the list. When you are finished, click on the **Notify All** button to apply the policy to all of the switches in the network.

> **Important Note:** Clicking the **Notify All** button causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP Server, which is very expensive in terms of switch resources and time. If any One Touch ACL Policy has already been defined, the switch(es) to which the policy is assigned will also re-cache its policy tables. **It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime**.
>
> **Note:** You can also click the Add icon to go to the **Groups** application and create a new Network Group, before returning to this screen to select it.

Applying a One Touch ACL Policy

When you click the **Notify All** button, the policy(ies) is applied to all switches in the network. To view the status of the re-cache operation, click on the **Status** button to view the Devices Pending Notification Table. In addition, you can view the success or failure of the re-cache operation for each switch in the policy.log file of the **Audit** application, including an indication of any error that may have occurred. Any errors that occur will also be reported in the server.txt file, in the **Audit** application. Note that the re-cache operation for each switch occurs in a separate thread and may take some time.

Editing a One Touch ACL Policy

Select the policy and click the Edit icon. Edit the **Accessibility** Field (Accept/Drop), click **Update**. The policy will appear in the table with the Status "Unsaved". If necessary, repeat to edit additional entries in the list. You cannot edit the ACL IP Server Group. When you are finished, click on the Save icon ✔, to save the update(s) to the LDAP Server, then click on the **Notify All** button to apply the policy to all of the switches in the network.

> **Important Note:** Clicking **Notify All** causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP Server, which is very expensive in terms of switch resources and time. If any One Touch ACL policy has already been

defined, the switch(es) to which the policy is assigned will also re-cache its policy tables. **It is recommended that you verify all policies that you have edited and apply them at the same time to minimize switch downtime.**

Deleting a One Touch ACL Policy

To delete a policy(ies), select the policy(ies) in the table, click on the Delete icon, then click **OK** at the confirmation prompt. When you click the **OK** button:

- All One Touch ACL policies for the ACL IP Network Group(s) you selected are removed from the LDAP Server.
- All One Touch ACL policies for the ACL IP Network Group(s) you selected are removed from switch attributes in the LDAP "role" objects.
- The Network Groups are removed from the table.
- A confirmation message is displayed when the LDAP Server has been successfully updated. The success of the operation is also reported in the policy.log file in the **Audit** application.
- An SNMP message is sent to each QoS-qualified device in the List of All Discovered Devices, informing them that the information in the LDAP Server has changed and commanding the devices to update their cached policies with the current information from the LDAP Server. Note that the re-cache operation for each switch occurs in a separate thread and may take some time. Be sure to check the policy.log file in the **Audit** application for the re-cache status of each switch.

Example of a One Touch ACL Policy Creation

Let's say we have selected **Data Center Switches** as the Network Group and **Accept** as the accessibility option. When saved, the following policies are created and written to the LDAP Server:

OneTouchAR$SData Center Switches

Condition specifies traffic originating from source IP Network group 'data center switches' Action specifies accept as the disposition for this traffic

OneTouchAR$DData Center Switches

Condition specifies traffic transmitted to destination IP Network group 'data center switches' Action specifies accept as the disposition for this traffic

Note: Names beginning with "OneTouchAR" are the names used for the One Touch ACL policies in the LDAP repository.

One Touch Voice Policies

The PolicyView One Touch Voice Policies enable you to easily assign the highest quality of service to all voice traffic that is destined for Alcatel-Lucent Enterprise devices. There are four QoS priority queues supported by Alcatel-Lucent Enterprise devices: Platinum, Gold, Silver, and Bronze. Platinum provides the highest QoS and Bronze provides the lowest QoS. One Touch Voice Policies enable you to assign **Platinum** QoS to voice traffic. You can assign the policies by IP Subnet or MAC Address:

- One Touch Voice IP Policies - Create Platinum Layer 3 Policies for all voice traffic flowing to, and originating from, an IP subnet.

- One Touch Voice MAC Policies - Create Platinum Layer 2 Policies for all voice traffic flowing to, and originating from, devices for a specific vendor by entering a range of MAC Addresses for the vendor.

One Touch Voice IP Policies

The PolicyView One Touch Voice IP Policies Screen displays all of the One Touch Voice IP Policies that have been configured and the status of the policy on the LDAP Server:

- **Saved -** The policy has been successfully written to the LDAP Server.
- **Unsaved -** The new policy, or modified policy has not been saved to the LDAP Server
- **Error -** An error condition has made it impossible to write the policy to the LDAP Server.

The screen is used to create, edit, or delete One Touch Voice IP Policies for all voice traffic flowing to, and originating from, an IP subnet.

Creating a One Touch Voice IP Policy

Click on the Add icon. Enter a **Subnet IP** and **Subnet Mask** and click **Create**. The Network Subnet will appear in the table with the Status "Unsaved". If necessary, click on the Add icon to create additional policies. When you are finished, click on the Save icon ✔, to save the Policy(ies) to the LDAP Server. Next, click on the **Notify All** button to apply the policy to all of the switches in the network. Note that when you create a One Touch Voice IP Policy, two policies are created for each subnet entered - one for traffic originating from the subnet, and one for traffic flowing to the subnet.

> **Important Note:** Clicking **Notify All** causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP Server, which is very expensive in terms of switch resources and time. If any One Touch Voice IP Policy has already been defined, the switch(es) to which the policy is assigned will also re-cache its policy tables. **It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime**.

Applying a One Touch Voice IP Policy

When you click the **Notify All** button, the policy(ies) is applied to all switches in the network. To view the status of the re-cache operation, click on the **Status** button to view the Devices Pending Notification Table. In addition, you can view the success or failure of the re-cache operation for each switch in the policy.log file of the **Audit** application, including an indication of any error that may have occurred. Any errors that occur will also be reported in the server.txt file, in the **Audit** application. Note that the re-cache operation for each switch occurs in a separate thread and may take some time.

Editing a One Touch Voice IP Policy

Select a Subnet from the One Touch Voice IPs List and click the Edit icon. Edit the **Subnet Mask**, click **Update**, then click on the Save icon ✔, to save the update to the LDAP Server. If necessary, repeat to edit additional entries in the list. You cannot edit the IP Subnet you can only delete it and create a new one. When you are finished, click on the **Notify All** button to apply the policy to all of the switches in the network.

Important Note: Clicking **Notify All** causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP Server, which is very expensive in terms of switch resources and time. If any One Touch Voice IP Policy has already been defined, the switch(es) to which the policy is assigned will also re-cache its policy tables. **It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime**.

Deleting a One Touch Voice IP Policy

To delete a policy(ies), select the Subnet IP in the list, click on the Delete icon, then click **OK** at the confirmation prompt. When you click the **OK** button, all One Touch Voice IP Policies for the IP Subnet(s) you deleted are removed from the LDAP Server (both Layer 2 and Layer 3 Policies). When you are finished, click on the **Notify All** button to apply the deletion to all of the switches in the network.

Important Note: Clicking **Notify All** causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP Server, which is very expensive in terms of switch resources and time. If any One Touch Voice IP Policy has already been defined, the switch(es) to which the policy is assigned will also re-cache its policy tables. **It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime**.

One Touch Voice MAC Policies

The PolicyView One Touch Voice MAC Policies Screen displays all of the One Touch Voice MAC Policies that have been configured and the status of the policy on the LDAP Server:

- **Saved -** The policy has been successfully written to the LDAP Server.
- **Unsaved -** The new policy, or modified policy has not been saved to the LDAP Server
- **Error -** An error condition has made it impossible to write the policy to the LDAP Server.

The screen is used to create, edit, or delete One Touch Voice MAC Policies for all voice traffic flowing to, and originating from, a specific device by entering a range of MAC Addresses for the device.

Creating a One Touch Voice MAC Policy

Click on the Add icon. Enter a **Device** Name and **MAC Address** and click **Create**. The policy will appear in the One Touch Voice MACs List with the Status "Unsaved". If necessary, click on the Add icon to create additional policies. When you are finished, click on the Save icon ✔, to save the Policy(ies) to the LDAP Server. Next, click on the **Notify All** button to apply the policy to all of the switches in the network. Note that when you create a One Touch Voice MAC Policy, two policies are created for each MAC Address entered one for traffic originating from the MAC Address, and one for traffic flowing to the MAC Address.

Important Note: Clicking **Notify All** causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP Server, which is very expensive in terms of switch resources and time. If any One Touch Voice MAC Policy has already been defined, the switch(es) to which the policy is assigned will also re-cache its policy tables. **It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime**.

Applying a One Touch Voice MAC Policy

When you click the **Notify All** button, the policy(ies) is applied to all switches in the network. To view the status of the re-cache operation, click on the **Status** button to view the Devices Pending Notification Table. In addition, you can view the success or failure of the re-cache operation for each switch in the policy.log file of the **Audit** application, including an indication of any error that may have occurred. Any errors that occur will also be reported in the server.txt file, in the **Audit** application. Note that the re-cache operation for each switch occurs in a separate thread and may take some time.

Editing a One Touch Voice MAC Policy

Select a Policy from the One Touch Voice MACs List and click the Edit icon. Edit the **MAC Address**, click **Update**, then click on the Save icon ✔, to save the update to the LDAP Server. If necessary, repeat to edit additional entries in the list. You cannot edit the **Device** Name. You can only delete it and create a new one. When you are finished, click on the **Notify All** button to apply the policy to all of the switches in the network.

> **Important Note:** Clicking **Notify All** causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP Server, which is very expensive in terms of switch resources and time. If any One Touch Voice MAC Policy has already been defined, the switch(es) to which the policy is assigned will also re-cache its policy tables. **It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime**.

Deleting a One Touch Voice MAC Policy

To delete a policy(ies), select the Policy in the list, click on the Delete icon, then click **OK** at the confirmation prompt. When you click the **OK** button, all One Touch Voice MAC Policies you deleted are removed from the LDAP Server (both Layer 2 and Layer 3 Policies). When you are finished, click on the **Notify All** button to apply the deletion to all of the switches in the network.

> **Important Note:** Clicking **Notify All** causes all QoS-enabled switches to flush their policy tables and reload policies from the LDAP Server, which is very expensive in terms of switch resources and time. If any One Touch Voice MAC Policy has already been defined, the switch(es) to which the policy is assigned will also re-cache its policy tables. **It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime**.

Policies and Policy Lists

The PolicyView Policies and Policy Lists option enables you to view QoS Policies and create Policy Lists for network traffic.

Policies

The PolicyView Policies Screen displays basic information for all configured Policies. You can also click on a policy to view detailed information about the Policy (e.g., Condition, Action).

Policy Information

The list below defines all of the possible fields that can be displayed in the table. Not all of the fields below are displayed in the Default view. However, you can click on the **Select All** button to display all fields; or click on the **Custom** button to create a custom view to display only

specified fields. (Click on the **Custom** button, then click on the **Custom Template** button, select the fields you want to display, then click **OK**.) After creating a custom view, you can just click on the **Custom** button to display that custom view. You can change the custom view at any time for a different display.

- **Policy Name -** The name of the Policy.
- **Scope -** The scope of the Policy (e.g., IP Filtering, Provisioned).
- **Status -** Indicates whether or not the Policy has been saved to the LDAP Server (Saved/Unsaved).
- **Precedence -** The Precedence value of the Policy (0 - 65535).
- **Enabled -** Indicates whether or not the Policy is enabled (Yes/No).
- **Save -** Indicates whether or not the rule will be recorded during a snapshot command (Yes/No).
- **Log Matches -** Indicates whether or not matches to this rule are logged in the QoS Log (Yes/No). **Reflexive -** Indicates whether or not the Policy is reflexive. Reflexive Policy Rules allow specific return connections that would normally be denied (Yes/No).
- **Default List -** Indicates whether or not the Policy is saved to the Default List. A Default Policy List always exists in the switch configuration. By default, a Policy Rule is added to this list when the rule is created. A rule remains a member of the Default List even when it is subsequently assigned to additional lists (Yes/No).
- **SLA Policy Trap -** Indicates whether or not an SLA Policy Trap is configured for the policy.

Detailed Policy Information

- **Policy Rule -** The name of the Policy Rule and the Policy Rules configured for the Policy. **Policy Condition -** The Policy condition information (e.g., IP Policy condition would display the Source/Destination/Multicast IP address of the condition).
- **Policy Action -** The Policy action to take if the traffic matches the Policy condition (e.g., QoS Accept/Drop)
- **Policy Validity Period -** The configured validity period for the Policy.
- **Policy Roles -** The switches to which the Policy has been assigned.

Policy Lists

The PolicyView Policy Lists Screen displays all configured Policy Lists, including the Policies Rules included in each list, and is used to create, edit, and delete Policy Lists. You can click on a Policy List to display the Policies contained in the list. A Policy List is a set of Policies that are grouped together and can be assigned to switches as a group. The QoS/ACL Policies that you add to a Policy List can be defined using the PolicyView Application. You can also include Resources or Resource Groups in a Policy using the "Resources - Add to Policy" Screen.

Creating a Policy List

Click on the Add icon. The Create Policy List Screen appears. Enter a **Name** for the Policy List and select the Policies you want to include in the list from the **Add Policies** drop-down menu. (All of the currently-configured Policies appear in the list. You can also click the Add icon to go to Expert Mode and create a new policy(ies) to add to the list.) When you select a Policy from

the drop-down menu, the Policy will appear in a table below, so you can review the Policy and modify the Precedence value, if needed. When you are finished reviewing the Policy(ies), click the **Create** button. The new Policy List will appear on the Policy Lists Screen.

Editing a Policy List

You can edit the Policies included in a Policy List or edit the Precedence value of any Policy in the list. Select a Policy List and click on the Edit icon. The Edit Policy List Screen appears. Click on the **Add Policies** dropdown menu . (All of the currently-configured Policies appear in the list. You can also click the Add icon to go to Expert Mode and create a new policy(ies) to add to the list.) Select/unselect Policies to add/remove them from the Policy List. When you are finished editing the Policy, click the **Update** button. The updated Policy List will appear on the Policy Lists Screen.

> **Note:** Adding/deleting a policy to/from a policy list will automatically update any switch roles that contain this policy list with the updated policies.

Deleting a Policy List

To delete a Policy List(s), select the list(s), click on the Delete icon, then click **OK** at the confirmation prompt. Note that you cannot delete a Policy List that is associated with a User Network Profile (UNP). To delete the list, you must first remove it from the UNP.

Policy List Information

Click on a Policy List to display the Policies contained in the list. The following information is displayed for each Policy contained in the Policy List.

- **Name -** The name of the Policy.
- **Condition -** The Policy Condition information (e.g., IP Policy Condition would display the Source/Destination/Multicast IP address of the condition).
- **Action -** The Policy Action to take if the traffic matches the Policy condition (e.g., QoS Accept/Drop)
- **Precedence -** The Precedence value of the Policy (0 - 65535).
- **Validity Period -** The configured validity period for the Policy.

Policies by Switch

The PolicyView Policies by Switch Screen enables you to view Policies configured on specific devices. To view Policies for specific devices, click on the **Select Device** button to bring up the Selection Wizard. Select the device(s) you want to display, then click **OK**. Device information and Policy Status for each device is displayed. Select a device to display Policy and Policy List information for the device.

Device Information

The following information is displayed for each selected device:

- **Name -** The user-configured name for the device.
- **Address -** The IP Address of the device.
- **DNS Name -** The DNS name of the device, if applicable.
- **Device Type -** The device model (e.g., OS6850-48, OS6900-X20).

- **Version -** The AOS software version running on the device (e.g., 8.5.255.R02).
- **Policy Status** - Indicates whether or not the switch has re-cached its Policy information to contain the Policy. After a Policy is created and saved on the LDAP Server, the user assigns the Policy to the switch. This causes the switch to flush its Policy Tables and reload the latest Policies from the LDAP Server.

Policy Information

The following Policy information is displayed when you click on a device (click on a Policy to display detailed information about the Policy):

- **Name -** The name of the Policy.
- **Scope -** The scope of the Policy (e.g., IP Filtering, Provisioned).
- **Status -** Indicates whether or not the Policy has been saved to the LDAP Server (Saved/Unsaved).
- **Precedence -** The Precedence value of the Policy (0 - 65535).
- **Enabled -** Indicates whether or not the Policy is enabled (Yes/No).
- **Save -** Indicates whether or not the rule will be recorded during a snapshot command (Yes/No).
- **Log Matches -** Indicates whether or not matches to this rule are logged in the QoS Log (Yes/No). **Reflexive -** Indicates whether or not the Policy is reflexive. Reflexive Policy Rules allow specific return connections that would normally be denied (Yes/No).
- **Default List -** Indicates whether or not the Policy is saved to the Default List. A Default Policy List always exists in the switch configuration. By default, a Policy Rule is added to this list when the rule is created. A rule remains a member of the Default List even when it is subsequently assigned to additional lists (Yes/No).
- **SLA Policy Trap -** Indicates whether or not an SLA Policy Trap is configured for the policy.

Detailed Policy Information

The following information is displayed when you click on a Policy:

- **Policy Rule -** The name of the Policy Rule configured for the Policy.
- **Policy Condition -** The Policy condition information (e.g., IP Policy condition would display the Source/Destination/Multicast IP address of the condition).
- **Policy Action -** The Policy action to take if the traffic matches the Policy condition (e.g., QoS Accept/Drop)
- **Policy Validity Period -** The configured validity period for the Policy.
- **Policy Roles -** The switches to which the Policy has been assigned.

Policy List Information

The following Policy List information is displayed when you click on a device:

- **Name -** The Policy List name.
- **Policies -** The Policy Rules configured for the Policy.

Expert Mode

The PolicyView Expert Mode option is used to create, edit, delete, and view custom QoS Policies. Custom Policies are created using a wizard that guides you through each of the steps needed to create the Policy and apply the Policy to switches in the network. All currently configured Policies are listed in the Existing Policies Table. You can view basic information about a Policy in the table or click on a specific policy to view more detailed information.

> **Note:** You cannot create, delete, or edit a One Touch Policy in the Expert mode. You must use the applicable One Touch option (Data, ACL, Voice) to create, delete, or edit a One Touch policy.

Creating a Custom Policy

Custom Policies are created using a wizard that guides you through each of the steps needed to create the policy and apply the policy to switches in the network. To create a Custom Policy, click on the Add icon. The wizard will then guide you through the following screens:

- **Configuration** - Basic policy configuration (e.g., Policy Name, Precedence)
- **Device Selection** - Specify the devices to which you will apply the policy
- **Set Condition** - Specify the conditions that must be true before traffic will be allowed to flow.
- **Set Action** - Specify parameters for the traffic that will flow.
- **Validity Period** - Specify the time period for the policy to be in effect.
- **Review** - Review the policy details before creating the policy.

Note: As you configure a policy, conditions and actions are verified against the devices selected for the policy. If a condition or action is not supported by one of the selected devices, and error message will appear indicating the error and corrective action to be taken.

Applying a Custom Policy to the Network

After configuring and saving a policy(ies), you must apply the policy(ies) by notifying the switches in the network. When you click on the **Notify All** button, all of the policies listed in the Existing Policies Table are applied to all of the switches configured for each policy. To apply the policy(ies) only to certain devices, select an option from the drop-down menu (Use Switch Picker/Use Topology), click on the **Select Device** button and select the device(s), then click the **Notify Selected** button.

After notifying the switches, you can view the status of the re-cache operation, by clicking on the **Status** button to view the Devices Pending Notification Table. In addition, you can view the success or failure of the re-cache operation for each switch in the policy.log file of the Audit application, including an indication of any error that may have occurred. Note that the re-cache operation for each switch occurs in a separate thread and may take some time. Any errors that occur will also be reported in the server.txt file, in the Audit application.

> **Note:** When you notify network switches, all QoS-enabled switches flush their policy tables and reload policies from the LDAP repository, which is very expensive in terms of switch resources and time. It is recommended that you review all policies that you have created and apply them at the same time to minimize switch downtime.

Editing a Custom Policy

To edit a policy, select the policy in the Existing Policy Table and click on the Edit icon. Use the wizard to make any edits. When you are done, apply the edited policy to the network.

Deleting a Custom Policy

To delete a policy(ies), select the policy(ies) in the Existing Policies Table, click on the Delete icon, then click **OK** at the confirmation prompt.

> **Note:** Deleting a policy(ies) in the Existing Policies Table will not automatically update policy(ies) on any switch that contain this policy(ies). To delete a policy(ies) on switch, select an option from the drop-down menu (Use Switch Picker/Use Topology), click on the **Select Device** button and select the device(s), then click the **Notify Selected** button.

Policy Information

The Existing Policies Table displays basic information for all configured Policies. You can also click on a policy to view detailed information about the Policy (e.g., Condition, Action). Note that Unified Policies are not displayed in the Expert Mode Existing Policies Table. They are only displayed in the Existing Unified Policies Table.

Basic Information

- **Policy Name -** The name of the Policy.
- **Scope -** The scope of the Policy (e.g., IP Filtering, Provisioned).
- **Precedence -** The Precedence value of the Policy (0 - 65535).
- **Status -** Indicates whether or not the Policy has been saved to the LDAP Server.
- **Enable -** Indicates whether or not the Policy is enabled.
- **Save -** Indicates whether or not the rule will be recorded during a snapshot command.
- **Log Matches -** Indicates whether or not matches to this rule are logged in the QoS Log.
- **Reflexive -** Indicates whether or not the Policy is reflexive. Reflexive Policy Rules allow specific return connections that would normally be denied (Yes/No).
- **Default List-** Indicates whether or not the Policy is saved to the Default Policy List. By default, a Policy Rule is added to this list when it is created. A Policy Rule remains a member of the Default List even when it is subsequently assigned to additional Policy Lists.
- **SLA Policy Trap -** Indicates whether or not an SLA Policy Trap is configured for the policy.

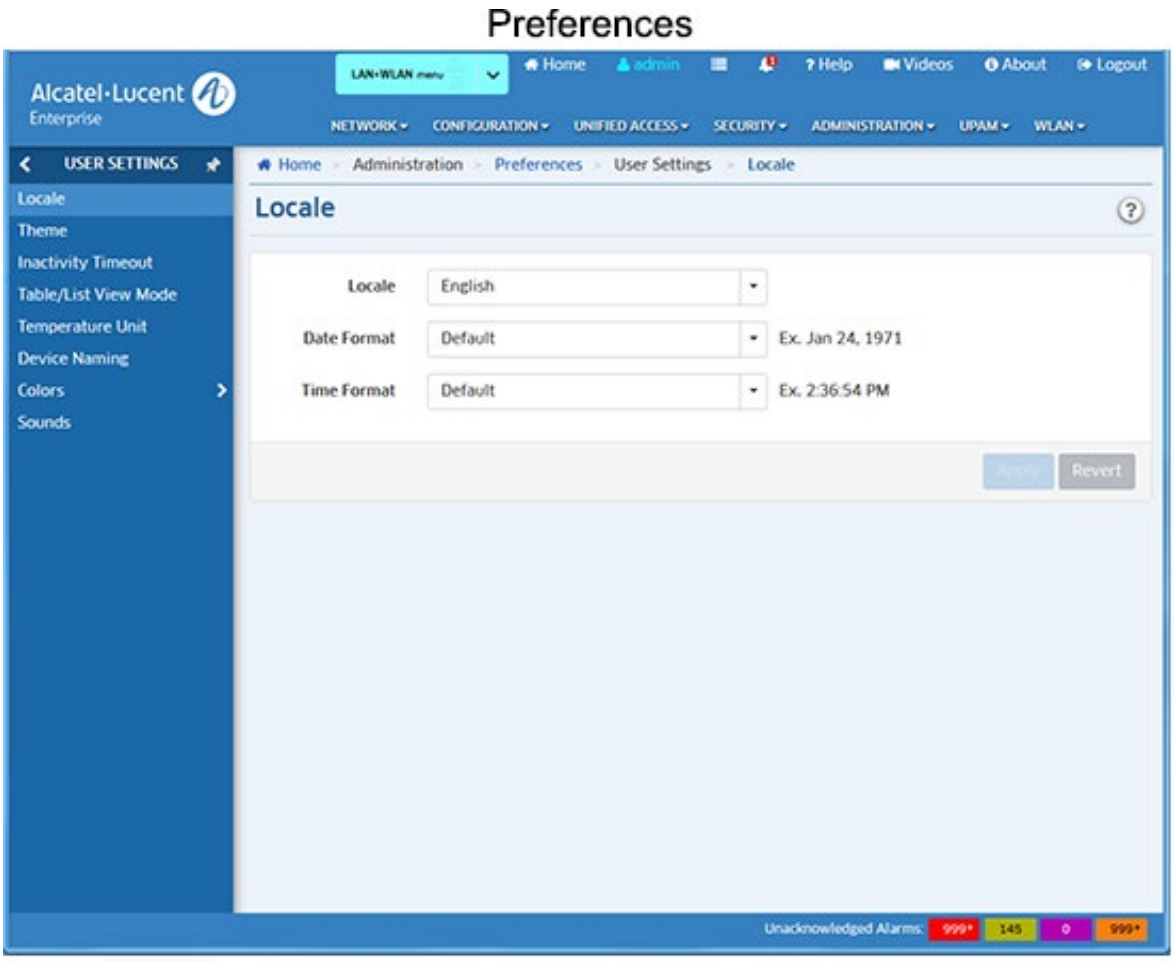
Detailed Information

- **Policy Rule -** The name of the Policy Rule and the Policy Rules configured for the Policy.
- **Policy Condition -** The Policy condition information (e.g., IP Policy condition would display the Source/Destination/Multicast IP address of the condition).
- **Policy Action -** The Policy action to take if the traffic matches the Policy condition (e.g., QoS Accept/Drop)

- **Policy Validity Period -** The configured validity period for the Policy.
- **Policy Roles -** The switches to which the Policy has been assigned.

23.0 Preferences

The Preferences Application is used to set OmniVista preferences for the web GUI. All Preferences have appropriate default values, so there is no need to change Preference settings unless you wish to. When a Preference is changed, the change takes effect immediately.



The following preferences can be configured. Any user can update their User settings; however, a user must be assigned to the Account Admin Role to configure System settings.

User Settings - These settings can be configured for each user.

- **Locale -** Used to set a system-wide language, and time/date format.
- **Theme -** Used to set the color scheme and look of OmniVista.
- **Inactivity Timeout -** Used to set the Inactivity Timer. If there is no user activity within this timeframe, the user is logged off.
- **Table/List View Mode -** Used to set the default display layout for all table/list screens in OmniVista.
- **Temperature Unit -** Used to set the temperature unit that will be displayed, when applicable, in OmniVista (e.g., Centigrade or Fahrenheit).
- **Device Naming -** Used to specify how devices are identified and displayed in OmniVista (e.g., IP address, Device Name, DNS Name).

- **Colors -** Used to configure the colors displayed in Dashboard Widgets for Network Status, Alarms, Quarantine Manager, and ProActive Lifecycle Management.

System Settings - These settings are system-wide settings that are configured for all users.

- **Branding -** Used to change the logo displayed on the OmniVista user interface and the logo displayed on reports created in the Report application.
- **Proxy -** Used to configure a Proxy for the OmniVista Client.
- **ProActive Lifecycle Management -** Used to enable/disable ProActive Lifecycle Management and manually upload information.
- **Videos -** Used to specify the Alcatel-Lucent Enterprise YouTube Demo Playlist that will play when the "Videos" link at the top of the OmniVista screen is clicked.
- **Email -** Used to specify the Simple Mail Transfer Protocol (SMTP) mail server that you want to use to send e-mails generated by OmniVista.
- **SMS -** Used to configure a connection to an SMS Provider and set SMS preferences.
- **CA Certificate Import -** Used to import a CPPM Client CA Certificate into OmniVista. Install Zulu CEK- Used to install the Zulu Cryptography Extension Kit (CEK).
- **Install Zulu CEK**- Used to install the Zulu Cryptography Extension Kit (CEK).
- **Collect Support Info** - Used to set the data retention period for Audit Support Information Logs on the OmniVista Server.
- **Enforce Strong Password** - Used to apply stronger password rules when creating OmniVista users (Security - Users & User Groups - User)
- **Google Map API** - Used to control whether or not the Google Map API is loaded.

User Settings

The following sections detail configuration of User Preferences.

Locale

The Preferences Locale Screen is used to set a system-wide language, and time/date format. When you have configured a parameter, click the **Apply** button. The changes take effect immediately.

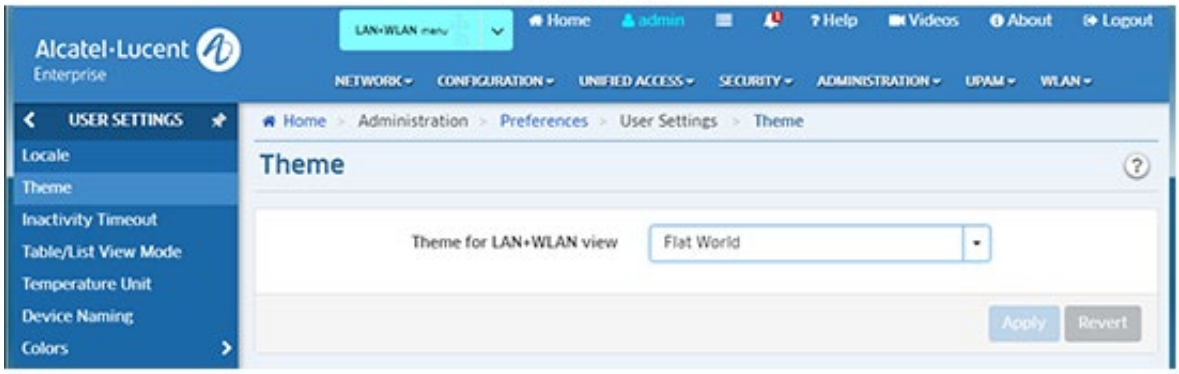
- **Language -** The language that will display (Default = English)
- **Date Format -** The date format that will display:
- **Medium -** Abbreviated Month, Day, Year (e.g., Nov 15, 2017)
- **Long -** Full Month, Day Year (e.g., November 15, 2017)
- **Full -** Day and Date (e.g., Wednesday, November 15, 2017)
- **Default -** Medium format (abbreviated Month, Day, Year (e.g., Nov 15, 2017)
- **Time Format -** The time format that will display:
- **Short -** Hours:Minutes - AM-PM (e.g., 3:15 PM)
- **Medium -** Hours:Minutes:Seconds - AM-PM (e,g, 3:15:50 PM)
- **Long -** Hours:Minutes:Seconds - AM-PM - Timezone (e.g., 3:15:50 PM PST)
- **Full -** Hours:Minutes:Seconds - AM-PM - Timezone (e.g., 3:15:50 PM PST)

- **Default -** Medium format (Hours:Minutes:Seconds - AM-PM (e.g., 3:15:50 PM)

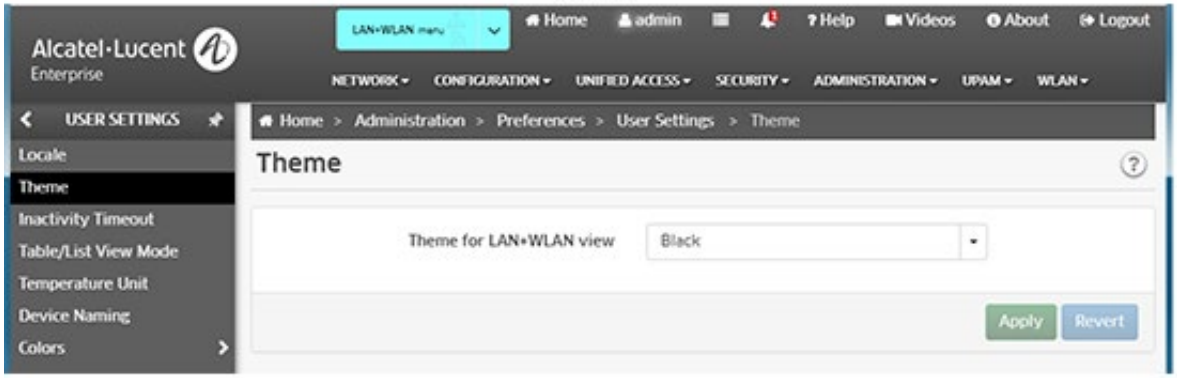
Theme

The Preferences Theme Screen is used to set the color scheme and look of OmniVista's default LAN+WLAN view. The default theme is "Flat World". To change the theme, select a theme and click the **Apply** button. The change takes effect immediately. The available themes are shown below.

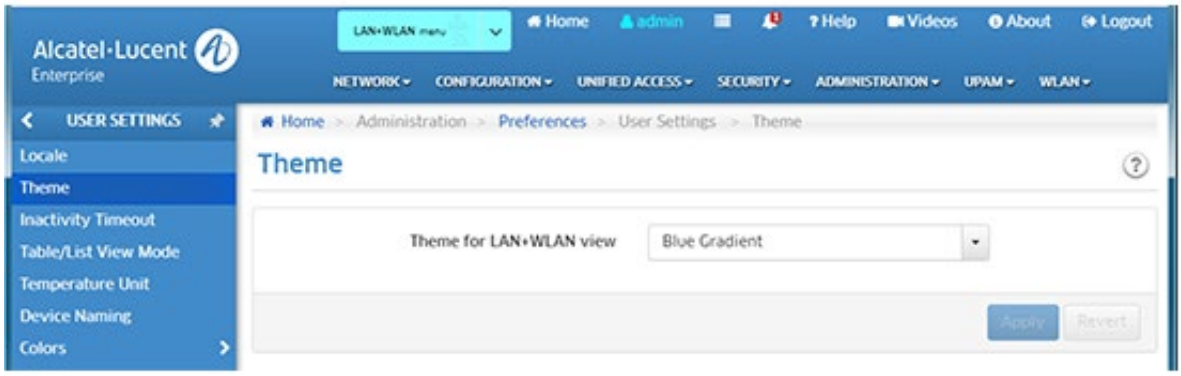
Flat World



Black



Blue Gradient



Inactivity Timeout

The Preferences Inactivity Timeout Screen is used to set the Inactivity Timer. If there is no user activity within this timeframe, the user is logged off. Enter a time, in minutes. You can also use the **+/-** symbols to increase/decrease the time by 5-minute increments, or use the slider for

larger increments. When you have configured the time, click the **Apply** button. The change takes effect immediately. (Range = 15 - 259,200 (25 weeks 5 days), Default = 15).

Table/List View Mode

The Preferences Table/List View Mode Screen is used to set the default display layout for all table/list screens in OmniVista. Note that you can always change the view on a table/list screen using the view option icons at the top of the screen. Select a display mode (Table or List) and click on the **Apply** button. The changes take effect immediately.

Temperature Unit

The Preferences Temperature Unit Screen is used to set the temperature unit that will be displayed, when applicable, in OmniVista. From the **Temperature Unit** drop-down menu, select "Celsius" or "Fahrenheit" and click on the **Apply** button. The change takes effect immediately.

Device Naming Pattern

The Preferences Device Naming Pattern Screen is used to specify how devices are identified and displayed in OmniVista (e.g., IP address, Device Name, DNS Name). This preference sets the device naming style for all applications within OmniVista. Select an option from the **Device Naming Pattern** drop-down menu and click on the **Apply** button. The change takes effect immediately.

Colors

The following sections detail configuring custom colors for OmniVista displays.

Network Status Color Preferences

The Preferences Network Status Color Preferences Screen is used to set the colors that display in the Topology application and Network Status widget on the Dashboard. You can change colors by clicking on a color and using the color picker; or you can enter a color using RGB Hexadecimal format (e.g., #2ca02c). When you have configured a setting, click the **Apply** button. The change takes effect immediately.

Alarms Color Preferences

The Preferences Alarms Color Preferences Screen is used to set the colors for alarm notifications that display in the Notifications application (and in the Topology application). You can change colors by clicking on a color and using the color picker; or you can enter a color using RGB Hexadecimal format (e.g., #2ca02c). When you have configured a setting, click the **Apply** button. The change takes effect immediately.

Quarantine Manager Color Preferences

The Preferences Quarantine Manager Color Preferences Screen is used to set the notification colors that display in the Quarantine Manager widget on the Dashboard. You can change colors by clicking on a color and using the color picker; or you can enter a color using RGB Hexadecimal format (e.g., #2ca02c). When you have configured a setting, click the **Apply** button. The change takes effect immediately.

ProActive Lifecycle Management Color Preferences

The Preferences ProActive Lifecycle Management Color Preferences Screen is used to set the colors that display for each status in the ProActive Lifecycle Management widget on the OmniVista Dashboard. Each status level (e.g., Supported, Not Supported) in the widget pie charts is also assigned a level number. For example, Level 0 corresponds to "Supported", Level 1 corresponds to "Support to End", and Level 2 corresponds to "Not Supported. (You can hover over a section of a pie chart to see the Level number that corresponds to a status level.) To change the color that will be displayed for a status level, change the corresponding Level number color on the Preferences Screen.

To configure a color, click on the color box next to a level, then use the color picker or enter a color using

RGB Hexadecimal format (e.g., #2ca02c) to change the color. When you have configured a color, click the **Apply** button. The change takes effect immediately. Click on the **Restore Default Colors** button to return all colors to their default settings.

Sounds

The Preferences Sounds Screen is used to set audible alarm sounds for certain OmniVista actions (e.g., UI Inactivity timeout is reached, Notifications Traps are received). Follow the steps below to configure alarm sounds.

Configuring Alarm Sounds

By default, alarm sounds are disabled. To set an alarm sound, slide the Enable button next to the action (UI Inactivity and/or Notifications) to **Yes**. Pre-configured alarm sounds are provided by OmniVista. You can listen to the sound by clicking on the Play icon next to the sound file name. By default, the volume on all sounds is enabled. However, you can set an alarm sound to silent by clicking on the Volume icon.

To change an alarm sound, click on the **Change** button and select a sound file on your computer. The new sound file name will appear. After configuring an alarm sound(s), click on the **Apply** button. The change takes effect immediately.

Note: .wav or .mp3 files are supported, with a maximum file size of 500KB.

UI Inactivity

The UI Inactivity Alarm will sound when the Inactivity Timeout Limit is reached. The Inactivity Timeout Limit is configured on the Preferences Inactivity Timeout Screen (Preferences - User Settings - Inactivity Timeout). The default sound file is displayed. You can change the sound as described above. when you are finished, click on the **Apply** button at the bottom of the screen.

Notifications

Notifications Alarms will sound when new traps are received. You can enable the same alarm sound for all Trap Severity Levels or enable alarms for specific Severity Levels (e.g., Critical, Major). You can also set different alarm sounds for different Severity Levels.

- To enable the same alarm sound for all Severity Levels, click on the **For All Severity Levels** checkbox. You can change the sound as described above.
- To enable an alarm sound for specific Trap Severity Levels, slide the Enable button to **Yes** for the Severity Level(s). You can change the sound as described above.

- To enable and set different alarm sounds for specific Trap Severity Levels, slide the Enable button to **Yes** for the Severity Level(s), click on the **Change** button and change the alarm sound as described above.

Note: Alarms will not sound for auto-acknowledged traps.

To restore all sounds to default. click on the **Restore Default Sounds** button.

System Settings

The following sections detail configuration of OmniVista System Preferences.

Branding

The Preferences Branding Screen is used to change the logo displayed on the OmniVista user interface and the logo displayed on reports created in the Report application. By default, the Alcatel-Lucent Enterprise logo is displayed. However, you can upload a custom logo to be displayed. To upload a custom logo, click on the "Upload Custom Logo" link to locate and upload the logo. The logo must conform to the size and dimensions shown. You can also select a dark or light background for the logo. Click on the applicable option to view how it will be displayed.

After uploading the file and selecting a background, click on the **Apply** button. The new logo will immediately appear in the upper left corner of the screen, replacing the Alcatel-Lucent Enterprise logo; and will appear on any reports you create. At any time, you can click on the "Use Default Logo" link and click the **Apply** button to return to the default Alcatel-Lucent Enterprise logo.

Proxy

The Preferences Proxy Screen is used to configure a web proxy for the Asset Management (Call Home) and Application Visibility Signature File Update Features. To configure a proxy, complete the fields and click on the **Apply** button. The change takes effect immediately.

Note: OV 2500 NMS-E 4.3R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for upgrade software, Application Visibility Signature Files, and ProActive Lifecycle Management. If the OV 2500 NMS-E 4.3R2 Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OV 2500 NMS-E 4.3R2 to connect to these external sites (Port 443):

- **ALE Central Repository –** ovrepo.fluentnetworking.com
- **AV Repository –** ep1.fluentnetworking.com
- **PALM –** palm.enterprise.alcatel-lucent.com
- **Call Home Backend -** us.fluentnetworking.com

ProActive Lifecycle Management

The Preferences ProActive Lifecycle Management (PALM) Screen is used to configure PALM preferences. The PALM Feature enables you to view support services status and lifecycle information for devices managed by your OmniVista 2500 NMS. PALM periodically gathers detailed inventory information for all discovered devices on your network (e.g., device name, MAC address, AOS version, NIs, power supplies) and uploads the information to the PALM web portal. The information can assist Alcatel-Lucent Enterprise in helping you manage

your inventory and your network; and is also available to you through a widget that can be displayed on the OmniVista 2500 NMS Dashboard for easy reference.

> **Note:** If you have not already registered, click on the **Register** button to register your OVID for Proactive Lifecycle Management. Registering PALM creates a subscription and allows you to directly access the PALM cloud-based application. If the OVID was already registered, you do not need to register again.

After updating any preferences, click on the **Apply** button. The change(s) take effect immediately.

- **OV ID** - The ID displayed is the PALM ID automatically assigned to your OmniVista Server at installation and is used to identify your system. It is not configurable.
- **Backend URL -** This is the URL for the PALM web portal. There is no need to change the URL unless directed to do so by Alcatel-Lucent Enterprise.
- **ProActive Lifecycle Management -** Enables/Disables the PALM Feature. When you install OmniVista 2500 NMS, the PALM option is selected by default on the License Agreement Screen. If you accept the default, PALM is automatically enabled following installation. If you opt out of the feature at installation and need to enable it later, click on the **ProActive Lifecycle Management** slider to select **Enabled**. Accept the License Agreement and click the **Accept** Button. To disable the feature, click on the **ProActive Lifecycle Management** slider to select **Disabled**. If enabled, you can click on the **Upload Now** button to perform an immediate upload of PALM data.
- **Inventory Status -** Displays the time and date of the last successful upload of PALM data, and the time and date of the next scheduled upload. Until the first successful upload, the field will display "Never". After an initial upload at installation, updated information is sent to the web portal every two (2) weeks.
- **PALM Widget Status -** Displays the time and date of the last successful sync with the ProActive Lifecycle Management widget displayed on the Dashboard, and the time and date of the next scheduled sync. Until the first successful sync, the field will display "Never".

> **Note:** You will be prompted to enable the PALM Feature whenever you add/relicense an OmniVista Core License in the License application. If necessary, you can always enable the feature on this screen.

> **Note:** If OmniVista is connecting to the Internet through a Proxy, you must enable it to connect to the PALM external site - **palm.enterprise.alcatel-lucent.com** (Port 443) and the Call Home Backend external site - **us.fluentnetworking.com** (Port 443). You can click on the "Verify Proxy Configuration" link to go the Preferences Proxy Screen and verify/modify your Proxy configuration.

ProActive Lifecycle Management Overview

The ProActive Lifecycle Management (PALM) Feature enables you to view support services status and lifecycle information for devices managed by your OmniVista 2500 NMS. OmniVista periodically gathers detailed information for all discovered devices on your network and uploads the information to the PALM web portal. Basic inventory information is also available through a widget that can be displayed on the OmniVista 2500 NMS Dashboard for easy reference. When you install OmniVista 2500 NMS, the PALM option is selected by default on the License Agreement Screen. If you accept this default, the feature is enabled and information is gathered

and sent to the web portal. After the initial upload, updated information is sent to the web portal every two (2) weeks.

> **Note:** You must have a PALM account set up before using the feature. The account can be set up by your Business Partner or you can click on the **Register** button on the Preferences ProActive Lifecycle Management page to register your OVID for PALM. Also note that if you choose not to enable the PALM Feature at installation, you can enable it at a later time in the Preferences application.

Setting Up ProActive Lifecycle Management

After installing OmniVista you must enable PALM (if necessary), and add the ProActive Lifecycle Management Widget on the OmniVista Dashboard.

Enabling PALM

During OmniVista 2500 NMS installation, users have the option to enable PALM on the License Agreement Screen. If you enabled PALM at installation, go to Adding the ProActive Lifecycle Management Widget. Otherwise, follow the steps below to enable the feature.

1. Go to the Preferences - System Settings - ProActive Lifecycle Management Screen.
2. Click on the **ProActive Lifecycle Management** slider to enable the feature. Accept the License Agreement and click the **Apply** Button.
3. After clicking **Apply**, a "Verify Proxy Configuration" link will appear to enable you to verify/update your proxy settings. If necessary, click on the link to go to the Preferences - System Settings - Proxy Screen to view/change proxy settings.

   Note: In addition to the PALM option presented during OmniVista 2500 NMS installation, you will be prompted to enable PALM whenever you add/relicense an OmniVista Core License in the License application.

Adding the ProActive Lifecycle Management Widget

The PALM Widget can be displayed on the OmniVista 2500 NMS Dashboard. The widget provides basic inventory information. Follow the steps below to add the widget to the Dashboard.

1. On the OmniVista 2500 NMS Dashboard, click on the Settings icon and select **Add Widget**.
2. Under "Network" scroll down the list of widgets, select ProActive Lifecycle Management and click **OK**. The widget will appear on the Dashboard.

   Note: The ProActive Lifecycle Management Widget is activated after the initial data upload, which occurs within two weeks of installation. Once the initial upload is complete, information is displayed in the widget.

Viewing Information

Information is displayed in the ProActive Lifecycle Management Widget. A series of pie charts provide an overview of devices on your network. For a more detailed view, you can click on the widget to go to the PALM web portal.

ProActive Lifecycle Management Widget

The ProActive Lifecycle Management Widget includes a series of pie charts that provide a quick overview of devices on your network. The example below shows the Operating System Release Screen. Hover over a section to view basic information (e.g., number of network devices supported/not supported). Click on the arrows (>>) to scroll through the different screens. Click on a pie chart to go to the PALM web portal for a more detailed view. The information in each pie chart is defined below.

- **Operating System Release –** Provides an overview of network devices running AOS software by displaying the percentage and number of network devices running supported and unsupported AOS software. "Not Supported" indicates that the software version running on a device is no longer supported by Alcatel-Lucent Enterprise.
- **Hardware Lifecycle -** Provides a "lifecycle" overview of network devices. "Not Supported" indicates a device has passed its End of Life date.
- **Warranty Status -** Provides an overview of the warranty status of network devices. "Not Supported" indicates that a device has past the warranty end date.
- **Support Service –** Provides an overview of the Support Agreement status of network devices. "Not Supported" indicates that a device no longer has a valid Support Service (maintenance) agreement.

PALM Web Portal

The ProActive Lifecycle Management web portal provides detailed information for your network devices. Click on any of the pie charts in the ProActive Lifecycle Management Widget to go to the web portal (login is required the first time you access the portal). The initial screen displays the same pie charts displayed on the OmniVista Dashboard. Click on any of the pie charts and scroll down to the bottom of the screen to view detailed information.

Manually Uploading Information

After the initial data upload, OmniVista 2500 NMS sends updated information to the PALM web portal every two weeks. However, you can manually initiate a data upload at any time on the ProActive Lifecycle Management Screen in the Preferences Application. Go to the Preferences - System Settings - ProActive Lifecycle Management Screen and click on the **Upload Now** button.

Videos

The Preferences Videos Screen is used to specify the Alcatel-Lucent Enterprise YouTube Demo Playlist that will play when the "Videos" link at the top of the screen is clicked. Enter the **YouTube Playlist ID**. (You can view the widow in the **Preview** window for confirmation.) Click on the **Apply** button to set the playlist.

Email

The Preferences Email Screen is used to specify the Simple Mail Transfer Protocol (SMTP) mail server that you want to use to send e-mails generated by OmniVista. You can also specify the "From" address that will be used for these e-mails. Complete the fields and click on the **Apply** button. The change takes effect immediately.

- **SMTP Server -** The Host Name or IP address of the SMPT Mail Server to be used for e-mails generated by OmniVista.
- **"From" Address** - The "From" address to be used in e-mails generated by OmniVista.
- **SMTP Authentication -** Enables (On) / Disables (Off) SMTP Authentication.
- **"To" Address To Test -** Enter an e-mail address to send a test e-mail and click on the **Send Test Email** button.

Note: All of the fields in the must be filled or the e-mails you define will not be sent. Mail servers usually require the "From" address to be a valid e-mail address. If it is not, the mail server is likely to discard the request.

Note: OmniVista can be configured to generate and send an e-mail upon receipt of user-specified traps. This can be configured from the Automatic Trap Responders window in the Notifications application. The "To" address for Trap Responder e-mails is specified in the Automatic Trap Responders window. The "From" address and the mail server to be used are specified as shown above.

Note: Email settings for UPAM **must** be configured on the UPAM Email Server Screen (UPAM Setting - Email Server).

SMS

The Preferences SMS Screen is used to configure a connection to an SMS Provider and set SMS preferences. The SMS Gateway feature enables OmniVista applications to send SMS messages (e.g., login credentials for Guest Users). OmniVista uses a third-party SMS provider (Plivo, Telefonica) to process SMS messages. Complete the fields and click on the **Apply** button.

- **SMS Provider -** Select an SMS Provider from the drop-down menu.
    - **Plivo** – Select Plivo to process SMS messages. If necessary, click on the "Register Plivo Account" link to go to the Plivo website and create an account.
    - **Telefonica** - Select Telefonica to process SMS messages. Setup an account with Telefonica before configuring your SMS preferences.
- **Provider Specific**
    - **Plivo SMS Provider**

        - **Auth ID -** Enter the Auth ID issued by the SMS Provider (displayed on the Plivo Dashboard tab).
        - **Auth Token -** Enter the Auth Token issued by the SMS Provider (displayed on the Plivo Dashboard tab).
    - **Telefonica SMS Provider**
        - **User Name** - Enter the user name for your Telefonica account.
        - **Password** - Enter the password for your Telefonica account.
- **Generic Attributes**
    - **Source Number(s) -** Enter source number(s) used for sending SMS messages. If you enter multiple number, Plivo will use a "round-robin" method to select the source number used (i.e., it will start with the first source number entered by the user, then used the next number in the list for the next SMS message). These numbers must match the Source numbers you configured in the Numbers tab in Plivo.
    - **Max No. of Messages per Day per Source Number -** The maximum number of messages per day that can be sent from a single source number.
    - **"To" Number to Test -** Enter a "Test" number and click on the **Send Test SMS** button to send a test SMS message to ensure that SMS is configured correctly.

Prerequisites

When a new customer signs up on Plivo platform, there are multiple checks that run in the background to assess the authenticity of the domain, company etc., with the information provided while registering. This is a standard that is followed across the industry to protect the platform from fraud attacks. If these checks fail to return a positive value, your domain/company will be unable to successfully create an account with Plivo. If this happens you will have to contact Plivo to confirm your identity, and Plivo will manually allowlist the domain and enable registering. To ease onboarding and avoid this problem, follow the steps below.

1. Send an e-mail to "sales@plivo.com" to ensure your domain is allowlisted prior to registering.
    - Email has to be sent from the same ID that will be used to register.
    - Email Subject: Alcatel-Lucent Enterprise Customer: Request SMS service authorization
    - The body must contain the company name, website and country of operation.

2. Upon receiving this email, Plivo will allowlist your domain and let you know that you are ready to sign up/register. This can take up to 48 hours.

3. After successful registration on Plivo, you can use the assigned Auth ID/Auth Token, on the Alcatel-Lucent Enterprise OmniVista platform.

CA Certificate Import

The Preferences CA Certificate Import Screen is used to import a CPPM Client CA Certificate into OmniVista. Enter an **Alias Name** for the certificate, then click on the **Browse** button to locate the certificate. Click on the **Apply** button to import the certificate. Supported file types include .crt, .der, and .pem.

Install Zulu CEK

The Preferences Install Zulu CEK Screen is used to install the Zulu Cryptography Extension Kit (CEK), which is required to support SNMPv3 with AES 192 and 256 authentication protocols. Click on the link to read through "Zulu Terms of Use". Click on the "Download the Zulu CEK" link and download the CEK Zip File. The Zip File contains a README.txt file, a License file, a Disclaimer file and two ".jar" files (local_policy.jar and US_export _policy.jar). Click on the **Browse** button to locate and select the two (2) ".jar" files. Click on the **Upload** button to upload and install the files.

Collect Support Info

The Preferences Collect Support Info Screen is used to set the data retention period for Audit Support Information Logs on the OmniVista Server. The logs can be sent to Alcatel-Lucent Enterprise (ALE) Technical Support to troubleshoot problems. Audit Support Log options are configured on Audit Collect Support Info Screen (Administration - Audit - Collect Support Info). Enter a retention period and click on the **Apply** button.

- **Max Retention Period -** Enter a retention period, in days (Range = 1 - 31, Default = 7). The logs will be retained on the OmniVista Server for the specified number of days. The log files can be downloaded to an OmniVista Client at any time during the retention period using the Audit Collect Support Info Screen (Administration - Audit - Collect Support Info).

Enforce Strong Password

The Preferences Enforce Strong Password Screen is used to apply stronger password rules when creating OmniVista users (Security - Users & User Groups - User). By default, strong password enforcement is "On" (enabled).

- **Enforce Strong Password** - Click the slider to "On" to enable strong password rules or "Off" to disabled strong password rules, then click on the **Apply** button.

When a user login profile is created, a visual indicator on the Create User Screen will let the user know if they are meeting the password restrictions as they enter the password they want to use. In addition, a password generator option is also available.

Note: Users created when Enforce Stong Password is turned "Off" can continue to use the same password even when Enforce Strong Password is turned "On". The strong password restrictions are not applied to existing users unless they attempt to edit their user profile after enforcement was turned "On".

Google Map API

The Preferences Google MAP API Screen is used to control whether or not the Google Map API is loaded. By default, calls are made to load this API. You can disable calls to load this API, which is useful if your firewall blocks this API.

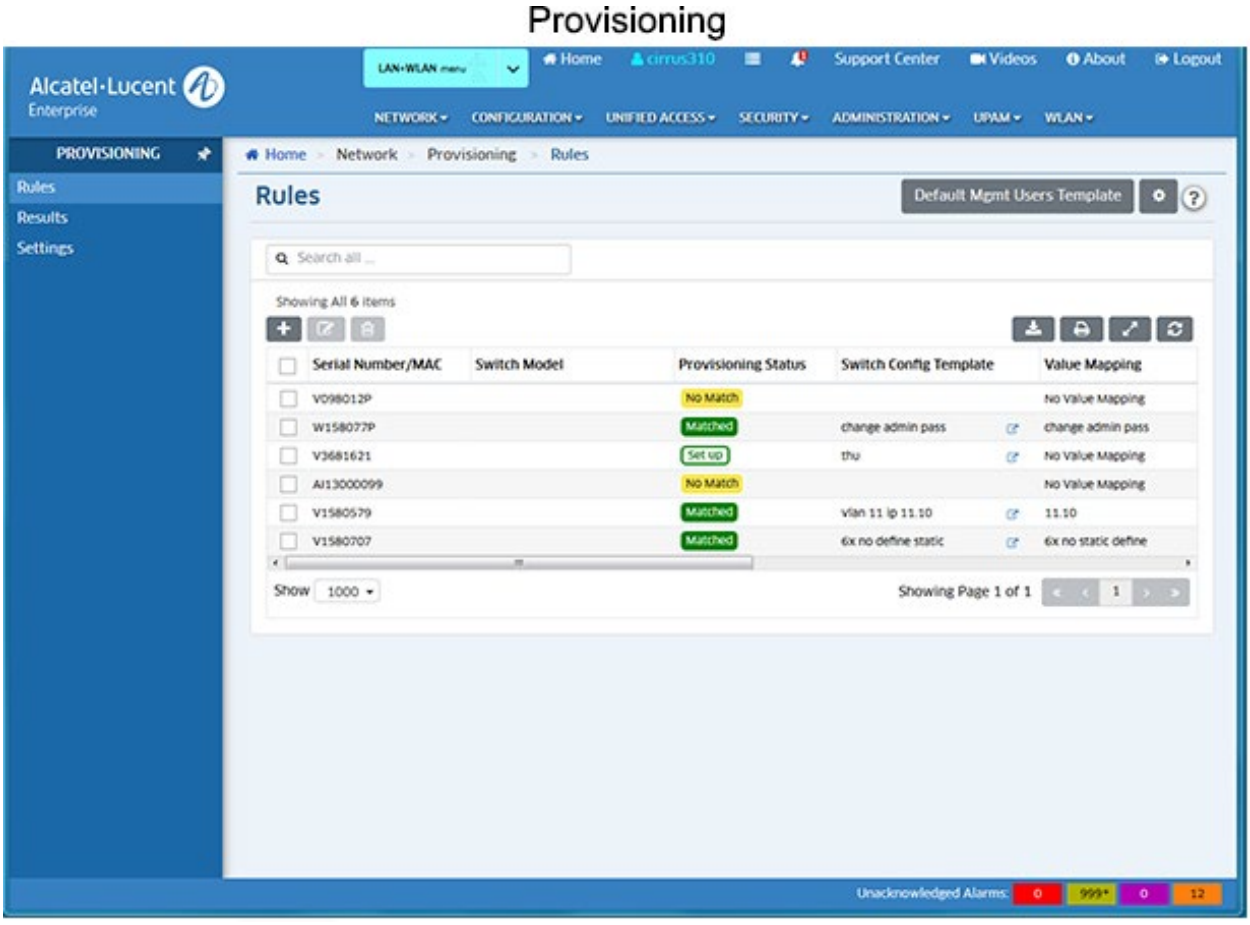
- **Disable Google Map API** - Click the slider to "On" to disable calls to the Google Map API or "Off" (the default) to enable calls to the API, then click on the **Apply** button.

24.0 Provisioning

The Provisioning application provides a simplified method for deployment of AOS Switches. The Provisioning application utilizes user-configured templates to automatically push Management User and Switch Configurations to AOS Switches. Using the application, you create Provisioning Rules containing Management User and Switch Configuration Templates for specific switches/switch models. When a switch contacts the OmniVista Server, the switch is then matched to a Provisioning Rule containing the Management User and Switch Configuration Templates for that switch/switch model. The Configuration Templates are then automatically pushed to the switch. Once the configuration is complete, the switch is added to the Managed Devices List and is manageable by OmniVista.

An overview of Provisioning functionality is provided below, as well as a basic workflow for configuring switches for provisioning, Thin Switch deployment, and a troubleshooting section.

> **Important Note:** There are network prerequisites and switch configuration steps that **must** be completed to enable Provisioning. See the Provisioning Prerequisites section below for required prerequisites.



> **Note:** The Provisioning application is supported on switches running AOS 6.7.2.R06 GA and higher or AOS 8.4.1.R03 GA and higher.

The following screens are used to provision switches:

- **Rules -** Used to create Provisioning Rules for switches/switch models containing Management User and Switch Configuration Templates that are pushed to switches. For example, you can configure a rule that will push a configuration to a specific switch (based on serial number or MAC Address) or to all OS6860-P48 Model Switches.
- **Results -** Displays information about all switches that have gone through the provisioning process (e.g., templates pushed to the switch, provisioning success/failure). The screen is also used to configure a "Golden Configuration" for a switch. A Golden Configuration is created from a switch backup and can be applied to a switch in the event there is an unwanted change to the switch's Running Configuration. The screen is also used to "Force Provision" a configuration to a provisioned switch. When you "Force Provision", the configuration is pushed to the switch the next time the switch contacts the OmniVista Server and matches a Rule.
- **Settings -** Used to configure Golden Configuration audit settings and onboarding rules for switches, and Thin Switch Client settings (periodic Call-Home time interval and retry attempts).

Provisioning Overview

Using the Provisioning application, you create Provisioning Rules containing Management User and Switch Configuration Templates for specific switches/switch models. When a switch boots up, it contacts the DHCP Server and gets the location of the OmniVista Activation Server. The Cloud Agent on the switch then makes an HTTPS call to the OmniVista Server and is matched to a Provisioning Rule containing the Management User and Switch Configuration Templates for that switch/switch model. OmniVista then uses SSH to log into the switch using the credentials specified in the Management User Template and configures/provisions the switch. Once provisioning is complete, the switch is added to the Managed Devices List and is manageable by OmniVista.

Once a switch is successfully provisioned, a Backup Job is also created on the switch to take automatic switch backups. The backups can be used to choose a configuration for marking it as the "Golden Configuration". See the Results Online Help for more information on the "Golden Configuration".

Provisioning Prerequisites

The prerequisite configurations below must be completed before using the Provisioning application. Once the prerequisites are met, switches can be deployed as described in the Basic Deployment Workflow section below.

DCHP/DNS Configuration

To enable switches to contact the OmniVista Server and receive the Provisioning configuration, you must first set up your DHCP Server to point to the local OmniVista Server as the Activation Server for provisioning. You must also setup DNS to resolve to point to your local OmniVista Server.

DHCP Configuration

- **Option 43**
  - **Sub-Option 1 -** Vendor ID. Validate the DHCP response (**must** be set with the value **alenterprise**). This sub-option is **only** required if you specify any of the sub-options listed below, **or** any devices on your network are running AOS 6.7.2 R03.
  - **Sub-Option 128 -** Activation Server FQDN. Set to **as-lite.myovcloud.net**.
  - **Sub-Option 134 -** Activation Server Port. The port number on the Activation Server to which the switches should communicate. By default, the switches communicate to Activation Server port 443. This sub-option is only supported on AOS 6.7.2R07 (and higher) and AOS 8.6R2 (and higher).

DNS Configuration

- Configure your DNS to resolve **as-lite.myovcloud.net** to point to your local OmniVista Server.

Configure the Cloud Agent (Currently-Deployed Switches Only)

Switches must contact the OmniVista Server to receive Provisioning Rules. New, "out of the box" switches automatically contact OmniVista when they are first connected to the network. However, to enable a currently-deployed switch to contact the OmniVista Server, you must telnet to the switch and modify the cloudagent.cfg file, and enable the Cloud Agent. See the Currently-Deployed Switches Workflow below for the steps to provision currently-deployed switches.

- **Modify the cloudagent.cfg File -** Configure the "Activation Server URL" field in the cloudagent.cfg file to enter an FDQN - **as-lite.myovcloud.net.**
- **Enable the Cloud Agent -** Telnet to the switch and issued the following CLI command: **cloud-agent admin-state enable**.

Note: If you do **not** want to use the Provisioning application to configure switches that are currently deployed on the network, do **not** perform any of the prerequisites on the switches. The switches will not contact the OmniVista Server for Provisioning and will continue to be managed by OmniVista as they have in the past.

Basic Deployment Workflow

The Rules Screen is used to create Provisioning Rules to automatically push Configuration Templates to switches. The basic deployment workflow is slightly different for new "out of the box" switches or currently-deployed switches.

New Switches

After configuring DHCP/DNS as described above (the Cloud Agent is already configured on new switches), set up Provisioning Rules and connect the switches to the network, as described below.

1. Go to the Rules Screen and click on the **Default Mgmt Users Template** button to view/configure a default Management Template. This Default Management Template is initially applied to any switch that is successfully provisioned and enables OmniVista management of the switch.

- When you open the Default Management Users Template, by default, "Create new credentials" under SNMP User Setup and "Use the same credential as SNMP User Setup" under "Other Access Methods" are selected. It is recommended that you use these default settings when deploying new switches. When these settings are used, OmniVista will log into the switch with the default "admin/switch" login credentials, and then create a new user based on the Username and Auth Password configured. OmniVista will then use this username and password to connect to, and manage the switch (addition to SSH, SNMP, SFTP). By default, the Username is "ov-enterprise". The Auth Password is automatically generated by OmniVista. You can use these defaults or change one or both of these fields. See the Rules online help for more information on configuring the Default Management Users Template.

Important Note: After successfully provisioning a switch(es), it is highly recommended that you change the default "admin" password on the switches. Use the CLI Scripting application to change the password. In the CLI Scripting application, you can SSH to an individual switch, or create a CLI Script to update the password on multiple switches. See the CLI Scripting online help for more information.

2. On the Rules Screen, click on the Add icon to create a Rule for a specific switch **or** switch model. The Rule contains identifying information for the switch/switch model, as well as Management User and Configuration Templates. For example, you can configure a rule that will push a configuration to a specific switch (by entering a serial number or MAC Address) **or** to all OS6860-P48 Model Switches (by entering the switch model). See the Rules online help for more information on creating Configuration Templates.

3. New switches initially boot up in the Certified Directory. However, switches should be running from the Working Directory for provisioning (unless the switch is provisioned as a Thin Switch, which can be running from the Certified, Working, or a user-defined directory). Before connecting a switch to the network, you must reboot the switch from the Working Directory.

- Power on the switch.
- Once the switch is powered up, connect to the Console Port on the switch and use one of the following CLI commands to reload the switch from the Working Directory.
  - 6.x Switches - **reload working no rollback-timeout**
  - 8.x Switches - **reload from working no rollback-timeout**

Note: A switch running from the Certified can be provisioned, however, the configuration is temporary and will not be persisted. The switch will lose its configuration if it reboots. If a switch is provisioned from the Certified Directory, reload the switch from the Working Directory and "Force Provision" the configuration to the switch from the Results Screen. When you "Force Provision" a switch, the configuration is pushed to the switch the next time the switch contacts the OmniVista Server and matches a Rule. See the Results Screen online help for more information on manually pushing ("Force Provisioning") a configuration to a provisioned switch.

4. New, "out of the box" switches running AOS 8.6R2 or higher automatically contact OmniVista. However, you must manually enable the Automatic Call Home Feature on new switches running 8.6R1 or lower as follows:

- Telnet to the device running AOS 8.6R1 or lower and disable the Cloud Agent using the following CLI command: **cloud-agent admin-state disable force** (enter **y** at the confirmation prompt)
- Enable the Cloud Agent using the following CLI command: **cloud-agent admin-state enable.**

5. Connect the switch(es) to the network. The switch(es) will contact the OmniVista Server, be matched to a corresponding Provisioning Rule, and the configuration in the templates will be pushed to the switch(es). Once configuration is complete, the switch(es) will be displayed in the Managed Devices List and manageable by OmniVista.

Note: See “Matching a Rule” below for more information on how Rules are pushed to switches.

Currently-Deployed Switches

After configuring DHCP/DNS, follow the steps below to provision currently deployed switches. Note that a switch should be running from the Working Directory for provisioning (unless the switch is provisioned as a Thin Switch, which can be running from the Certified, Working, or a user-defined directory). If a switch is running from the Certified Directory, reload the switch from the Working Directory before beginning the steps below.

- 6.x Switches - **reload working no rollback-timeout**
- 8.x Switches - **reload from working no rollback-timeout**

Note: A switch running from the Certified can be provisioned, however, the configuration is temporary and will not be persisted. The switch will lose its configuration if it reboots. If a switch is provisioned from the Certified Directory, reload the switch from the Working Directory and "Force Provision" the configuration to the switch from the Results Screen. When you "Force Provision" a switch, the configuration is pushed to the switch the next time the switch contacts the OmniVista Server and matches a Rule. See the Results Screen online help for more information on manually pushing ("Force Provisioning") a configuration to a provisioned switch.

1. If the switch is currently managed by OmniVista, go to the Managed Devices Screen (Network - Discovery - Managed devices) and delete the switch(s). Otherwise, go to Step 2.

2. Go to the Rules Screen and click on the **Default Mgmt Users Template** button to view/configure a default Management Template. This default Management Template is initially applied to any switch that is successfully provisioned and enables OmniVista management of the switch.

- Select "Use existing credentials" under SNMP User Setup. Enter the switch's/switches' current Username and Auth Password. OmniVista will use this username/password to connect to the switch. Select "Use existing credentials" under "Other Access Methods". Enter the switch's/switches' current CLI/FTP Username and Password. See the Rules online help for more information on configuring the Default Management Users Template.

3. Configure the Cloud Agent on the switch(es) to enable the switch(es) to begin calling the OmniVista Server for provisioning.

4. On the Rules Screen, click on the Add icon to create a Rule for a specific switch **or** switch model. The Rule contains identifying information for the switch/switch model. For example, you

can configure a rule that will push a configuration to a specific switch (by entering a serial number or MAC Address) **or** to all OS6860-P48 Model Switches (by entering the switch model). See the Rules online help for more information on creating Configuration Templates. When the switch(es) contacts the OmniVista Server, it will be matched to a corresponding Provisioning Rule, and the configuration in the templates will be pushed to the switch(es). Once configuration is complete, the switch(es) will be displayed in the Managed Devices List and manageable by OmniVista.

Note that you can retain a switch's current configuration. You do not need include a Configuration Template in the Rule. In this case, only the Management Template in the Rule will be pushed to the switch so that it can be managed by OmniVista. If you do include a Configuration Template in the Rule, it will append the existing Configuration File with the configuration in the Rule's Configuration Template.

If you do include a Configuration Template and it conflicts with the current switch configuration, provisioning will fail and the device will not be manageable by OmniVista. The switch will be displayed in the Results Table with a status of "Failed". You can then edit the Rule (or create a new one), and "Force Provision" the configuration to the switch from the Results Screen. When you "Force Provision" a switch, the configuration is pushed to the switch the next time the switch contacts the OmniVista Server and matches the Rule. See the Results Screen online help for more information on manually pushing ("Force Provisioning") a Rule to a switch.

> **Note:** See “Matching a Rule” below for more information on how Rules are pushed to switches.

Matching a Rule

When a new switch is connected to the network or the Cloud Agent is configured on an existing switch, the switch contacts the OmniVista Server every five (5) minutes until it is matched to a Rule. If the switch **is** matched to a Rule, it is configured, added to the Managed Devices List, and is manageable in OmniVista.

If a switch contacts the OmniVista Server and is **not** matched to a Rule, you can choose how OmniVista will handle the switch. You can:

- **Allow the Switch to Onboard (Default) -** The Default Management Users Template will be pushed to the switch. The switch will be displayed in the Managed Devices List and be manageable by OmniVista. The switch will also be displayed in the Results Screen with a status of "Succeeded". From there, you have the option of creating and manually pushing a configuration to the switch at any time. See the Results Screen online help for more information on manually pushing ("Force Provisioning") a configuration to a switch.
- **Do Not Allow the Switch to Onboard -** A Serial Number Rule will be automatically created for the switch. The Rule will be displayed on the Rules Screen with a Provisioning Status of "No Match". The switch will continue to contact the OmniVista Server until it matches a configured Provisioning Rule. You can configure a Rule for the switch at any time. Once the switch matches the Rule, it will be configured and be manageable by OmniVista.

Onboarding options are configured on the Settings Screen. See the Settings Screen online help for more information.

> **Note:** When a new switch is connected to the network or the Cloud Agent is configured on an existing switch, the switch contacts the OmniVista Server every five (5) minutes until it is matched to a Rule. Once a switch is successfully provisioned, if you want to

change the configuration on the switch, you can create a new Rule or edit the existing Rule and "Force Provision" the switch. See the Results Screen online help for more information on manually pushing ("Force Provisioning") a configuration to a switch.

Thin Switch Deployment Overview

OmniVista can provision an OmniSwitch running AOS release 8.8R1 or higher to run in Thin Switch mode. This mode helps to prevent sensitive information stored in the switch configuration from being tracked and enhances the switch security. The switch configuration is driven centrally from OmniVista; there is no local configuration on the switch allowed through the Command Line Interface (CLI) once the switch is running in the Thin Switch Client Mode. Consider the following when deploying switches to operate as Thin Switch Clients:

- Thin Switch Client mode is not configurable on the switch or saved in the switch configuration; a switch does not know it is a Thin Switch Client until OmniVista tells the switch to operate in that mode.
- Once a switch is configured as a Thin Switch, the "write memory" CLI command no longer works on the switch. Make sure that any minimal configuration required is done and saved before you provision the switch as a Thin Switch.
- A Thin Switch rule is not configurable for a switch that is currently managed by OmniVista. If the switch appears in the Managed Devices Screen (Network - Discovery - Managed Devices), delete the switch from the device list and then create the rule.
- There are two types of Call-Home requests that occur:
    - **Initial Call-Home -** The first Call-Home request after any reboot of the switch. After a reboot, the switch does not know that it is a Thin Switch; OmniVista tells the switch to run in Thin Switch Client mode.
    - **Periodic Call-Home -** Subsequent requests that occur after the intial Call-Home and before the next switch reboot.
- Changes to the running configuration on a Thin Switch can be made directly on the switch, but the changes cannot be saved to the switch configuration. However, you can send additional commands to a Thin Switch through an Incremental Template. This template is an optional attribute that you can configure for a Thin Switch provisioning rule that has already matched a switch (not configurable when creating a Thin Switch provisioning rule). Incremental Template commands are applied only once after the first periodic Call-Home from the switch. *Note that periodic Call-Home requests and the Incremental Template options are only supported when managing a Thin Switch.*
- The Thin-Client Mode section of the Provisional Settings screen allows you to change the amount of time between Call-Home requests and the number of times the switch attempts to connect with OmniVista.

Thin Switch Deployment Workflow

1. As described in the Prerequisites section above, configure the necessary DHCP/DNS configuration to enable the switch to contact the OmniVista server and receive the Thin Switch configuration. If DHCP is not configured in the network, then configure the minimun configuration requirements through the CLI on the switch to ensure reachability to the DNS server, NTP server, and OmniVista server.

- An "out-of-the-box" switch (no vcboot.cfg file) that is able to contact the OmniVista server can be provisioned as a Thin Switch without a minimal configuration. As a result, the switch will automatically Call-Home each time the switch reboots. Note that the

switch must be running AOS Release 8.6R2 or higher for the automatic Call-Home to work (see Step 4 in the New Switches section for more information).
- If a switch is not able to contact the OmniVista server, then minimal configuration is required on the switch. The vcboot.cfg file must contain the necessary configuration commands that will ensure network reachability to the OmniVista server *and* that the Cloud Agent is enabled on the switch (**cloud-agent admin-state enable**). Note that you must configure and save the required configuration to the vcboot.cfg file prior to provisioning the switch as a Thin Switch. The **write memory** CLI command is available to save the switch configuration until the switch is provisioned as a Thin Switch. See the Configure the Cloud Agent and Currently-Deployed Switches sections for more information.

2. Configure an OmniVista Thin Switch provisioning rule to match the serial number or MAC address of the switch. Note that matching a switch model number does not apply to Thin Switch rules. See the Rules online help for more information. There are two attributes that are specific to configuring a Thin Switch rule:

- Thin Switch **-** "Yes" or "No" (the default). Once a Thin Switch is provisioned and an entry for the switch appears in the Provisioning Results list, the Thin Switch attribute cannot be changed. To change the value of this attribute, the rule must be deleted and created again with a different value.
    - When the Thin Switch attribute value is set to "Yes", the "Save and Certify" field is set to "No" and cannot be changed.
    - When the Thin Switch Client mode is enabled on the switch, a "write memory" CLI command is not allowed.
- Desired Switch Config **-** A required attribute when Thin Switch is set to "Yes". A drop down menu offers three options for this attribute:

1. Switch Config Template and Incremental Template
2. Config snapshot from latest backup
3. Config snapshot from Golden Config (the default setting)

Note: If you attempt to create a provisioning rule on an already managed switch, an error message displays and the rule is not saved. Remove the switch from the Managed Devices Screen and create the rule again.

3. Reboot the switch or initiate a Call-Home from the switch using the **cloud-agent admin-state enable** CLI command. When the switch is discovered and matches the provisioning rule, OmniVista pushes the configuration specified in the rule to the switch.

- The configuration pushed by OmniVista is installed in the current running (Certified, Working, or user-defined) directory over the current running configuration.
- The vcboot.cfg of the Thin Switch is not modified in any way.
- OmniVista notifies the switch that it is now a Thin Switch Client.
- The onboarded Thin Switch is then managed by OmniVista and appears in the Provisioning Results list and in the Managed Devices list.

4. Once the switch is onboarded via a provisioning rule, OmniVista automatically performs a backup and scedules periodic backups. During each periodic backup, OmniVista backs up both the vcboot.cfg and the configuration snapshot (which is current OmniVista behavior).

5. Once onboarded and managed by OmniVista, a Thin Switch performs a periodic Call-Home request to notify OmniVista that it is a Thin Switch. When OmniVista receivs the periodic Call-Home request, OmniVista sends the Incremental Template if the Desired Switch Config attribute is set to "Switch Config Template and Incremental Template" and the Incremental Template Status is enabled. A configuration push does not occur for any of the other Desired Switch Config attribute values ("Config snapshot from latest backup" or "Config snapshot from Golden Config").

> **Note:** Periodic Call-Home requests by the switch and OmniVista pushing an Incremental Template configuration is supported only when managing Thin Switch. An Incremental Template is only pushed on Periodic Call-Home requests, not on an initial Call-Home when the switch reboots.

Troubleshooting

Provisioning Fails

If provisioning fails, first make sure that all prerequisites have been met. To view details for a specific switch, go to the Results Screen and check the "Last Provisioning Message" column for the reason. The most common cause of failure is that OmniVista does not know the correct credentials to SSH/SFTP the switch. The credentials that OmniVista uses to connect to the switch are specified in Default Management Template or in Custom Management Template on the Rules Screen. If the Configuration Template is the problem, make any necessary updates to the Configuration Template, and save it. The next time the switch contacts the OmniVista Server, provisioning should be successful.

Provisioning Logs

You can also view the Resource Manager Client Service Log in the Audit application (Administration - Audit) for more details. Click on the "Configuration" link on the left-hand side of the screen, then select "resource-manager-client-service". For troubleshooting problems with the Activation Server, view the OmniVista Web Log in the Audit application (Administration - Audit). Click on the "System" link on the left-hand side of the screen, then select "tomcat-ovweb".

Rules

The Provisioning Rules Screen displays information about currently-configured Provisioning Rules, and is used to create, edit, and delete Provisioning Rules. You can create Rules for specific switches (by serial number or MAC Address) or by switch model (e.g., OS6350-P10). If a switch matches a Rule (e.g., matching serial number, matching switch model), the Management and Configuration Templates in the Rule are pushed to the switch. When the configuration process is complete on the switch, the switch is displayed in the Managed Devices List and can be managed by OmniVista. The screen is also used to configure the view/configure the Default Management Users Template, and the Configuration and Management Templates.

> **Important Note:** There are network prerequisites and switch configuration steps that **must** be completed to enable Provisioning. See the Provisioning Overview Online Help for an overview of the application, including prerequisites, switch setup, and troubleshooting.

Creating a Provisioning Rule

Click on the Add icon at the top of the Rules List. Complete the fields as described below. Click on the Finish icon (checkmark) at the top of the Rules List when you are finished, then click **OK** at the Confirmation Prompt.

Note: You can create a Rule for a specific switch (Serial Number/MAC Address) **or** a switch model (e.g., OS6860-P48). A Rule can have Serial Number/MAC **or** Model Name but not both. Also note that if there is one Rule with a Serial Number and another Rule with MAC Address both pertaining to the same device, the Serial Number Rule will be used.

Note: When a Rule is created, OmniVista first checks to see if the Serial Number/MAC address exists in the Managed Devices List. If so, then an error message is displayed, and the rule is not created. If the device is not in the Managed Devices List, then the Rule is created.

- **Serial Number/MAC -** Enter either the switch serial number or MAC Address. This will match the Rule to a specific switch by serial number or MAC Address. See note below for more information on Serial Number Rules.
- **Switch Model -** Enter a **specific** switch model name (e.g., OS6350-P10, OS6860-P48, OS6900-Q32-F). This will match the Rule to any switch matching the specified switch model. You must enter the **specific** model name (e.g., OS6860-**P48**). If you do not include a specific model (e.g., OS6860), the rule will not match any switch model. Note that you can enter an "abbreviated" version of the switch model without hyphens or "OS" (e.g., 6860P48 or OS6860P48 or 6860-P48), but you must include the specific model (e.g., P48). Also note that you can only have one (1) Rule per switch model (e.g., one Rule for OS6860-P24, one Rule for OS6860-P48). Click here for a complete list of supported switch models.
- **Switch Config Template -** Select a Configuration Template from the drop-down menu; or click on **Add New** to create a new Configuration Template. This Configuration Template will be pushed to any switch matching the Rule. Note that you do not have to include a Configuration Template in the Rule. For example, you may want to onboard a switch with an existing configuration but do not want to modify that configuration. If you include a Configuration Template, the configuration in the Configuration Template will be appended to the existing configuration file on the switch.
- **Value Mapping -** If you create a dynamic Configuration Template, you must create Value Mappings for the variables in the template. Mapping Variables are explained below.
- **Mgmt Users Template -** Select a Management Template from the drop-down menu; or click on **Add New** to create new Management Template. By default, the Default Management Users Template pushed to the switch unless you select a different Management Template.
- **Thin Switch -** Select "Yes" or "No" from the drop-down menu to specify whether or not the matching switch will be provisioned to run in the Thin Switch Client mode. If the "Yes" option is selected, the Save and Certify field is automatically set to "No" and cannot be changed.
- **Desired Switch Config Template -** This field is required when the Thin Switch attribute is set to "Yes". Select one of the following options from the drop-down menu to specify which configuration is pushed to the switch:

  - **Switch Config Template and Incremental Template -** If an Incremental Template is specified, it will be pushed to the switch once during its periodic Call-Home. The Switch Configuration Template will be pushed to the switch every time the switch reboots.
  - **Config snapshot from latest backup -** The configuration snapshot taken from the latest OmniVista backup will be pushed to the switch every time the switch reboots. If the latest backup is not available, the Switch Configuration Template is used.
  - **Config snapshot from Golden Config** (the default setting) - The configuration snapshot taken from the Golden Configuration indicated in the Results page will be pushed to the switch every time the switch reboots. If the Golden Configuration is not available, the Switch Configuration Template is used.
- **Incremental Template -** Select an Incremental Template from the drop-down menu, or click on **Add New** to create a new Incremental Template. This type of configuration template is pushed to the switch only when a periodic Call-Home request is received from the switch, the Desired Switch Config Template attribute is set to "Switch Config Template and Incremental Template", and the Incremental Template Status is enabled. If the Incremental Template commands are applied successfully, then the template is not pushed again on the next periodic Call-Home received. Note that configuring related Incremental Template fields is not supported when creating a new Thin Switch rule.
- **Value Mapping Incremental Template -** If you create a dynamic Incremental Template, you must create Value Mappings for the variables in the template. Mapping Variables is explained below.
- **Incremental Template Status -** Select "Enabled" or "Disabled" from the drop-down menu. When set to "Enabled", the commands in an Incremental Template will be applied once to the switch when the next periodic Call-Home is received. This attribute is disabled if the switch sends a Call-Home after a reboot or after the template commands are successfully applied to the switch.
- **Save and Certify -** Save the configuration to the Certified Directory.

Note: Switch Model Rules can save time since they allow you to apply a configuration to a large number of switches at once. However, you may want to create a Switch Model Rule for a large number of switches but want to have a different Rule for some of those switches. In this case, after creating the Switch Model Rule, create a Serial Number Rule for those "different" switches. The Serial Number Rule will take precedence over the Switch Model Rule for those switches. Note that specifying a switch model number is not supported when creating Thin Switch rules; create a Serial Number Rule or MAC Address Rule instead.

Creating a Configuration Template

To create a Configuration Template for a Rule, go to the "Switch Config Template" column in the Rules Table, click on the drop-down arrow and select **Add New** to bring up the Edit Switch Config Template Screen. Click on the "Start From Scratch" tab to create a Configuration Template from scratch; or click on the "Select a Template" tab to select and edit an existing template and save it as a new one. When you are done, click on the **Save as New Template** button.

Note: Instructions for configuring a Static IP address for a specific switch (using a Serial Number Rule or MAC Address Rule) are displayed when you bring up the Configuration Template. Follow the instructions if you want to configure a Static IP Address in the template. The instructions are commented out. You can delete them or just configure the template below them. Note that configuring a Static IP address from a Configuration Template is not supported for Thin Switch Rules, so the instructions provided do not apply to Thin Switch Rules.

Note: You cannot configure a Static IP address that is assigned to a device in the Managed Devices List. You must first delete that device from the Managed Devices List before using that IP address.

The Configuration Template is created using CLI syntax. A Configuration Template is a set of commands that are read by the switch on reloading. A template can be static or dynamic. A Static Template (see sample below) is a template without variables. It is useful for deployments where all switches can work with exactly same configurations. The IP address is typically given by a DHCP server in such a deployment.

```
vlan 5 port default 1/1-48
ip interface vlan-5 address 192.168.5.3/24 vlan 5
ip multicast static-neighbor vlan5 port 1/49
ip multicast static-neighbor vlan5 port 1/50
ip multicast static-neighbor vlan5 port 1/51
ip multicast static-neighbor vlan5 port 1/52
lanpower start 1
system name Switch2
aaa authentication default local

```

Note: Certain commands that are handled by the Configuration Manager in AOS cannot be included in a Configuration Template (e.g., user admin password, write memory, configuration apply). If these commands are included in a Configuration Template, provisioning will fail. If provisioning fails for any reason, go to the Results Screen and check the "Last Provision Message" column for more information. You can also view the Resource Manager Client Service Log in the Audit application (Administration - Audit) for more details. Click on the "Configuration" link on the left-hand side of the screen, then select "resource-manager-client-service". If the Configuration Template is the problem, make any necessary updates to the Configuration Template, and save it. The next time the switch contacts the OmniVista Server, provisioning should be successful.

A Dynamic Template (see sample below) is a template with variables. It allows you to reuse the same Configuration Template even though different switches might need different values for some configurations. For example, different branches of an enterprise might use a different subnet range or VLAN.

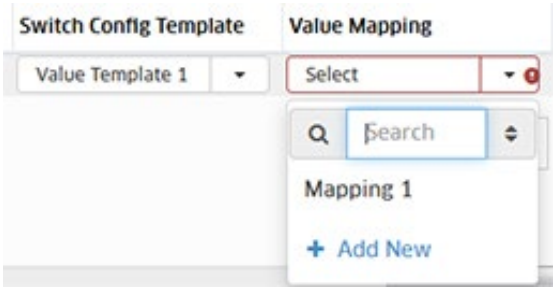
```
vlan 1 disable
vlan $VLAN members ports $PORTS tagged
no ip interface dhcp-client
ip interface $INTERFACE_NAME address $STATIC_IP/24 vlan $VLAN
```

Note: Special characters cannot be used when creating mapping variables (e.g., @ # +). OmniVista will ignore special characters. For example, "$test" is a correct mapping variable format. "$test@#+" will also be read as "$test" by OmniVista. Also note that

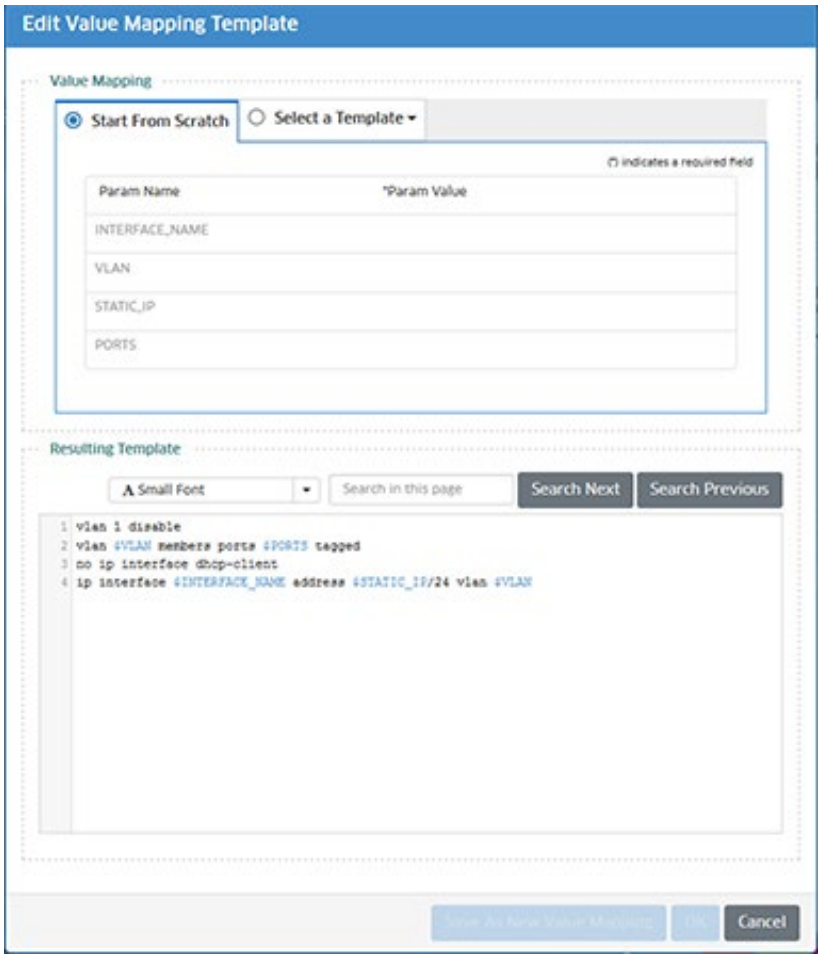
mapping variables cannot have spaces. If required, multi-word variables must be separated by an underscore (e.g., $test_1, not $test 1 or $test-1).

Configuring Value Mapping

A Dynamic Template requires value mapping for the variables in the template. Value Mapping is configured using the Value Mapping field in the Rules List. If the Configuration Template you selected contains variables, the Value Mapping field for the Rule will be activated. If you have already created a Value Mapping Template that you want to associate with the Dynamic Template, select it from the Value Mapping drop-down (e.g., Mapping 1).



To create a new Mapping Template, click on **Add New** to bring up the Edit Value Mapping Template window. The variables for the Dynamic Configuration Template are displayed at the top of the window (the Dynamic Template is shown at the bottom of the window). Enter values for each of the variables and click on the **Save As New Value Mapping** button. You can then select that Mapping Template from the Value Mapping drop-down.



Note: If you configure Management Users in the Configuration Template, OmniVista will use the Management User credentials defined in the Management Users Template to manage the switch.

Editing a Configuration Template

To edit an existing Configuration Template for a Rule, click on the Edit icon next to the template in the "Switch Config Template" column of the Rule. The Template Details Screen will appear displaying the current template configuration. Edit the configuration, then click on the **Save** button.

This change will not affect any switches that have previously matched the Rule and been successfully provisioned. The updated template will only be applied to subsequent switches connected to the network that match the Rule.

Configuring the Default Management Template

The Default Management Users Template is included in every Rule by default. You can edit the pre-configured default template and create and save custom Management Templates to include in a Rule. To edit the default template, click on the **Default Mgmt Users Template** button to bring up the Default Mgmt Users Template Screen. Complete the fields as described below and click on **OK**.

SNMP Settings

Configure the basic SNMP settings as described below.

- **SNMP Version -** The SNMP version that OmniVista will use to communicate with the switch. The default version for AOS devices is v2, but v3 is also supported.
- **Auth & Priv Protocol (SNMP v3 Only) -** The authentication protocol OmniVista will use for SNMP communication with the switch. Authentication uses a secret key to produce a "fingerprint" of the message. The fingerprint is included within the message. The device that receives the message uses the same secret key to validate that the fingerprint is correct. If it is, and if the message was received in a timely manner, then the message is considered authenticated. Otherwise, the message is discarded. The fingerprint is called a Message Authentication Code, or MAC.
- **Timeout -** The time period, in milliseconds, that OmniVista will wait for a switch to respond to a connection request before assuming that the request has timed-out (Default = 5,000)
- **Retry Count -** The number of times that OmniVista will attempt to connect to a switch (Default = 3).

SNMP User Setup

Configure the SNMP User Credentials for the switch as described below. These are the credentials that OmniVista will use to log into and manage the switch. You can create new SNMP User Credentials to access the switch, or used existing SNMP User Credential switch credentials to access the switch.

- **Create new credentials -** Select this radio button and complete the fields as described below to create new SNMP User credentials on the switch. OmniVista will then use these to connect to and manage the switch. This option is recommended for new, "out of the box" switches. If you also select "Use the same credential as SNMP User Setup" in the Other Access Methods section below, OmniVista will log into the switch with the default "admin/switch" login credentials, and then then create a new user based on the username and password you configure.
- **Use existing credentials -** Select this radio button and complete the fields as described below to retain the switch's existing SNMP User configuration. If you select this option, OmniVista will communicate with the switch using these credentials (OmniVista will expect that these credentials exist on the switch).
  - **Username -** The SNMP Username that OmniVista will use to connect to the switch. If you are creating new credentials, this is the new username that OmniVista will use to connect to the switch. If you are using existing credentials, this username must match the existing username on the switch.
  - **Auth Password -** The SNMP password that OmniVista will use to connect to the switch. If you are creating new credentials, this is the new password that OmniVista will use to connect to the switch. OmniVista auto-generates a password. You can change that password now, or later using OmniVista. If you are using existing credentials, this password must the existing password on the switch.
  - **Confirm Auth Password -** If you have changed the password (either for a new username/password or to match an existing switch password), re-enter the Auth Password.

- **SNMP Role -** Select the SNMP Role OmniVista Cirrus will have for device management - Read Only or Read/Write (Default).

Other Access Methods

Configure the CLI/FTP Credentials for the switch as described below.

- **Use the Same Credential as SNMP User Setup -** Use the CLI/FTP Username/Password and Role configured on the switch to access the switch. This option is recommended for new, "out of the box" switches. If this option is selected, OmniVista will log into the switch with the default "admin/switch" login credentials. If you also select "Create New Credentials" in the "SNMP User Setup" section, once OmniVista successfully logs into the switch, OmniVista will create a new username and password for the switch based on the username/password configured in the “SNMP User Setup” section above.
- **Create New Credentials -** Configure the CLI/FTP Username/Password and Role for CLI/FTP access to the switch.
  - **CLI/FTP User Name -** The user name that OmniVista will use to establish CLI/FTP sessions with the switch. The user name specified will be used to auto-login to devices when CLI sessions are established. It will also be used to perform FTP with the device when configuration files are saved and restored (see note below).
  - **CLI/FTP Password -** The password that OmniVista will use to establish CLI/FTP sessions with the switch. The user name specified will be used to auto-login to devices when CLI sessions are established. It will also be used to perform FTP with the switch when configuration files are saved and restored.
  - **Confirm CLI/FTP Password -** Confirm the CLI/FTP Password.
  - **CLI/FTP Role -** Select the SNMP Role OmniVista Cirrus will have for device management - Read Only or Read/Write (Default).
- **Use Existing Credentials -** Use the existing CLI/FTP Username/Password and Role currently configured on the switch for CLI/FTP access. Enter the CLI/FTP Username/Password. OmniVista will expect that these credentials exist on the switch. If they do not, the switch will fail during provisioning with an error message displayed on the Results page.

Note: If no Rule is defined for a switch, and the switch username/password is different than the one defined in the SNMP User Setup in the Default Management Users Template, OmniVista will be unable to connect to the switch and provisioning will fail. The switch will be displayed on the Results Screen with a Provisioning Status of "Failed". If this happens, configure a Rule for the switch using the "Use existing credentials" option under "Other Access Methods" on the Management Users Template, and "Force Provision" the switch. See the Results Screen online help for more information on "Force Provisioning".

Creating a Custom Management Template

You can create a Custom Management Template when creating a Rule. Click on the Add icon at the top of the Rules List to create the new Rule. Go to the "Mgmt Users Template" column in the Rules Table, click on the drop-down arrow and select **Add New** to bring up the Edit Management Users Template Screen. Complete the fields as described above, click on the **Save As New Template** button, enter a name for the Rule, and click **Save**. The new Management Template can then be selected from the drop-down.

Note: If a switch matches a Rule but the switch username/password are different than the credentials defined in the Management Users Template, OmniVista will be unable to connect to the switch and provisioning will fail. The switch will be displayed on the Results Screen with a Provisioning Status of "Failed". If this happens, configure a Rule for the switch using the "Use existing credentials" option under "Other Access Methods on the Management Users Template, and "Force Provision" the switch. See the Results Screen online help for more information on "Force Provisioning".

Editing a Provisioning Rule

Select a Rule in the Rules Table and click on the Edit icon at the top of the table. The Rule will move to the top of the table and all of the Rule fields will be activated above it. Edit any fields as necessary, then click on the small Edit icon to the left of the Rule.

This change will not affect any switches that have previously matched the Rule and been successfully provisioned. The updated Rule will only be applied to subsequent switches connected to the network that match the Rule. Note that if the previous Provisioning Status was "Matched", the status for this edited Rule will change to "Set Up" until a switch is connected to the network that matches the Rule.

Note: The Thin Switch attribute value for a Rule cannot be changed. To change this attribute value, delete the rule and create it again with a different value. See Thin Switch Deployment for more information.

Note: The related Incremental Template field values will be cleared and frozen when you edit a Thin Switch Rule to change the Desired Switch Config option from "Switch Config Template and Incremental Template" to one of the other remaining options.

Deleting a Provisioning Rule

Select a Rule(s) in the Rules list and click on the Delete icon. Click **OK** at the Confirmation Prompt. This will not affect any switches that were successfully provisioned after matching the Rule.

Rules List

- **Serial Number/MAC -** The switch serial number or MAC Address.
- **VC Serial Number/MAC -** The VC serial number or the VC MAC address if the matched rule specifies the VC serial number or the VC MAC address.
- **Switch Model -** The switch model number (e.g., OS6860-P48)
- **Provisioning Status -** The Provisioning status of the Rule.
  - **No Match -** Switch has contacted the OmniVista Server but there is not a matching Rule. A switch will contact OmniVista every five (5) minutes until it is matched to a Rule. At any time, you can configure a Rule for the device. The next time the switch contacts the OmniVista Server, it will be matched to the Rule and configured.
  - **Set Up -** A switch matching the Rule has not yet contacted the OmniVista Server. When the switch contacts the OmniVista Server and receives the configuration, the status will move to "Matched".
  - **Matched -** The Rule matched at least one switch that contacted the OmniVista Server.

- **Switch Config Template -** The Configuration Template used for the Rule.
- **Value Mapping -** If the Rule contains a Dynamic Configuration Template, the value mappings are displayed here.
- **Mgmt Users Template -** The Management Template used for the Rule.
- **Devices -** If one or two switch(es) match the Rule, the switch(es) will be displayed with a link to the switch in the Managed Devices List. If three or more switches match the Rule, two switches will be displayed with a "More" link. Click on the "More" link to display the remaining switches. Click on any specific switch to view the switch in the Managed Devices List.
- **Thin Switch -** Whether the switch will be provisioned as a Thin Switch Client ("Yes" or "No"). *Note that provisioning a switch as a Thin Switch Client is supported only on switches running AOS Release 8.8R1 (or higher).* See Thin Switch Deployment for more information.
- **Desired Switch Config Template -** If the Thin Switch attribute is set to "Yes", this field indicates which of the following configuration options will be pushed to switch:
  - **Switch Config Template and Incremental Template -** If an Incremental Template is specified, it will be pushed to the switch once during its periodic Call-Home. The Switch Configuration Template will be pushed to the switch every time the switch reboots.
  - **Config snapshot from latest backup -** The configuration snapshot taken from the latest OmniVista backup will be pushed to the switch every time the switch reboots. If the latest backup is not available, the Switch Configuration Template is used.
  - **Config snapshot from Golden Config** (the default setting) - The configuration snapshot taken from the Golden Configuration indicated in the Results page will be pushed to the switch every time the switch reboots. If the Golden Configuration is not available, the Switch Configuration Template is used.
- **Incremental Template -** The name of an Incremental Template that is used when provisioning a Thin Switch Client.
- **Value Mapping Incremental Template -** If the Thin Switch Client rule specifies a dynamic Incremental Template, the value mappings for the variables are displayed here.
- **Incremental Template Status -** Whether an Incremental Template will be pushed to a Thin Switch Client ("Enabled" or "Disabled").
- **Last Updated Time -** The last time the Rule was updated.
- **Save and Certify -** Whether the configuration has been saved to the Certified Directory.

Results

The Provisioning Results Screen displays information about all switches that have attempted provisioning through the Provisioning application. The screen is also used to configure a "Golden Configuration" for a switch and to "Force Provision a configuration to a device.

> **Important Note:** There are network prerequisites and switch configuration steps that **must** be completed to enable Provisioning. See the Provisioning Overview Online Help

for an overview of the application, including prerequisites, switch setup, and troubleshooting.

Golden Configuration

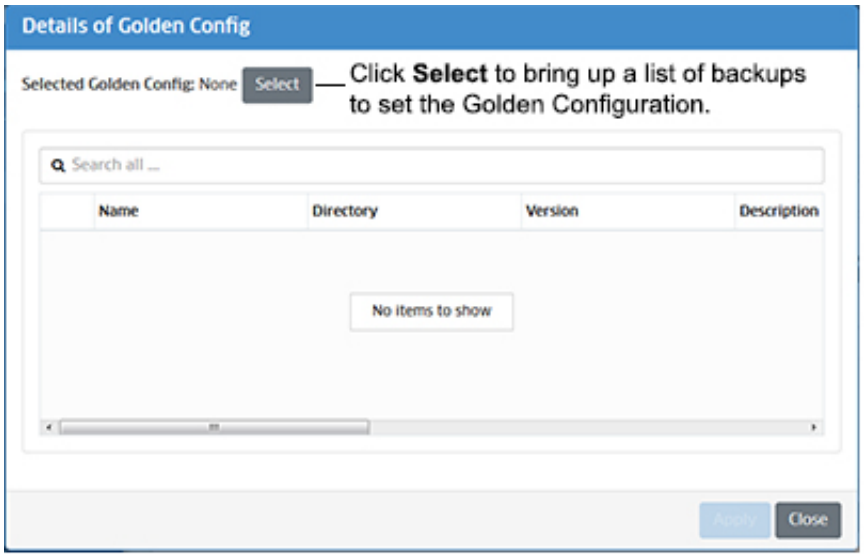
The "Golden Configuration" is a configuration selected from a list of the three (3) most recent switch backups that can be applied to a switch in the event there is an unwanted configuration change. The sections below detail how to set the initial Golden Configuration for a switch and how to change an existing Golden Configuration for a switch, and how to customize a Golden Configuration for a switch. You can also audit the Golden Configuration to see if it is different than the current Running Configuration.

Note: The Golden Configuration does not include switch users, as the user database on the switch is protected from a direct read/write by any external entity including OmniVista.

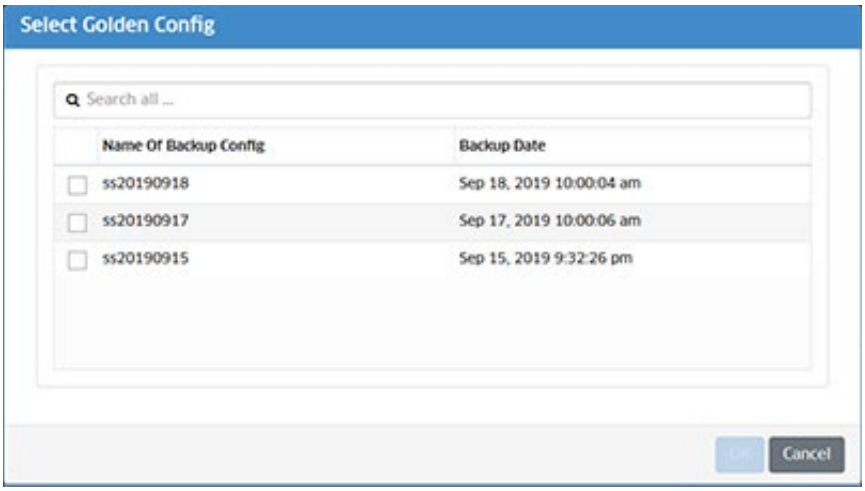
Note: Golden Configurations taken prior to release 4.5R2 will not contain configuration snapshot information. To compare configurations of devices taken prior to release 4.5R2, you must create a new Golden configuration for those devices.

Setting the Golden Configuration for a Switch

To set the initial Golden Configuration for a switch, go to the "Golden Config" column for the switch in the Results Table and click on the Edit icon in the field. The Details of Golden Config window will appear. Since a Golden Configuration has not yet been set for the switch, the fields will be empty.



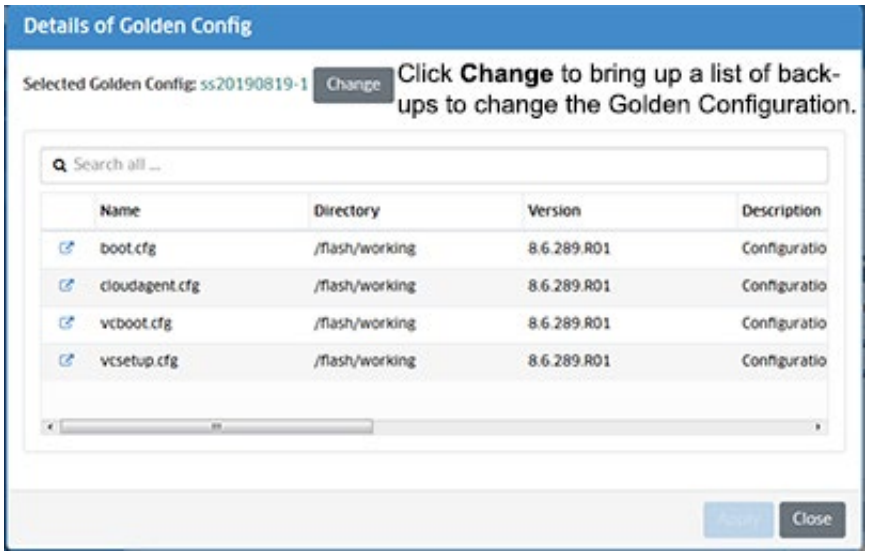
Click on the **Select** button. The Select Golden Configuration window will appear with a list of backups for the switch. When a switch is first provisioned, OmniVista begins daily configuration backups on the switch. The three (3) most recent backups are displayed. Select a backup from the list. (When you select a backup, a detailed view of the files contained in the backup is displayed.) Click **OK**, then click the **Apply** button to set the backup as the Golden Configuration.



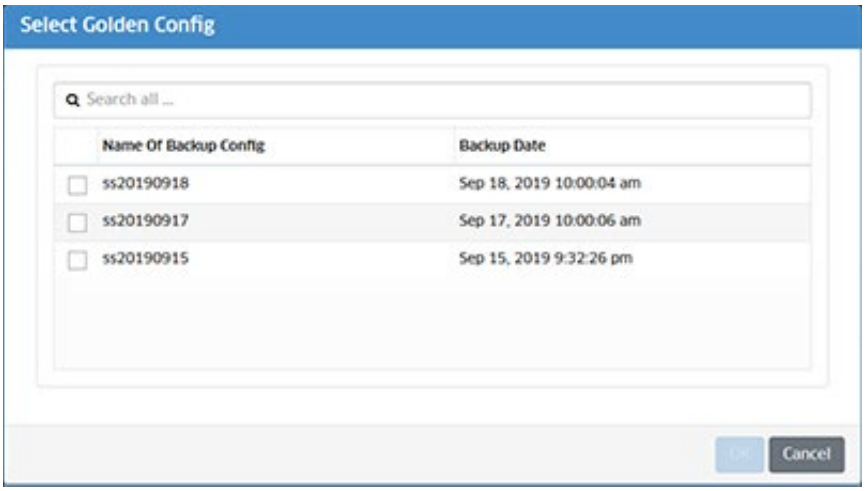
The backup you selected as the Golden Configuration will appear in the "Golden Config" Column of the switch in the Results Table.

Changing the Golden Configuration

If you have already set a Golden Configuration for a switch, you can change it at any time. Go to the "Golden Config" column for the switch in the Results Table and click on the Edit icon in the field. The Details of Golden Config window will appear, with the files contained in the Current Golden Configuration displayed.



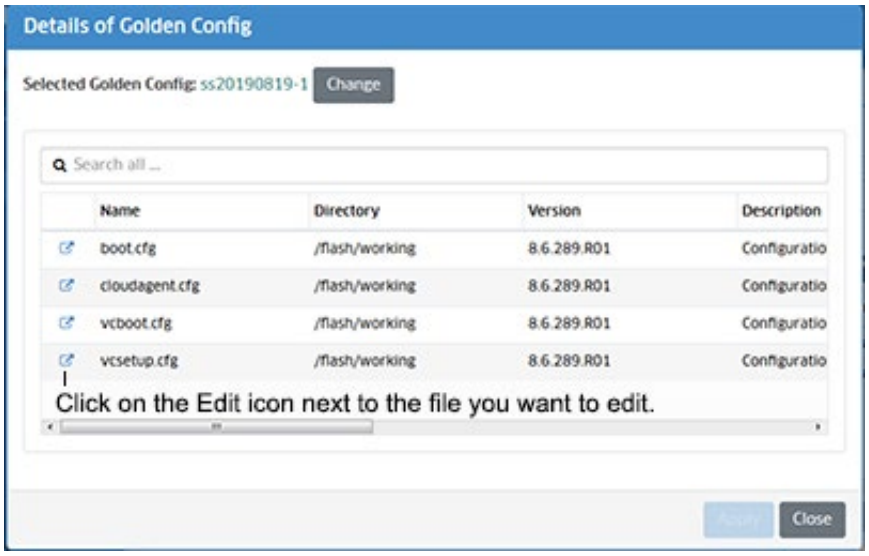
Click on the **Change** button. The Select Golden Configuration window will appear with the three (3) most recent backups for the switch. Select a backup from the list. (When you select a backup, a detailed view of the files contained in the backup is displayed.) Click **OK**, then click the **Apply** button to set the backup as the new Golden Configuration.



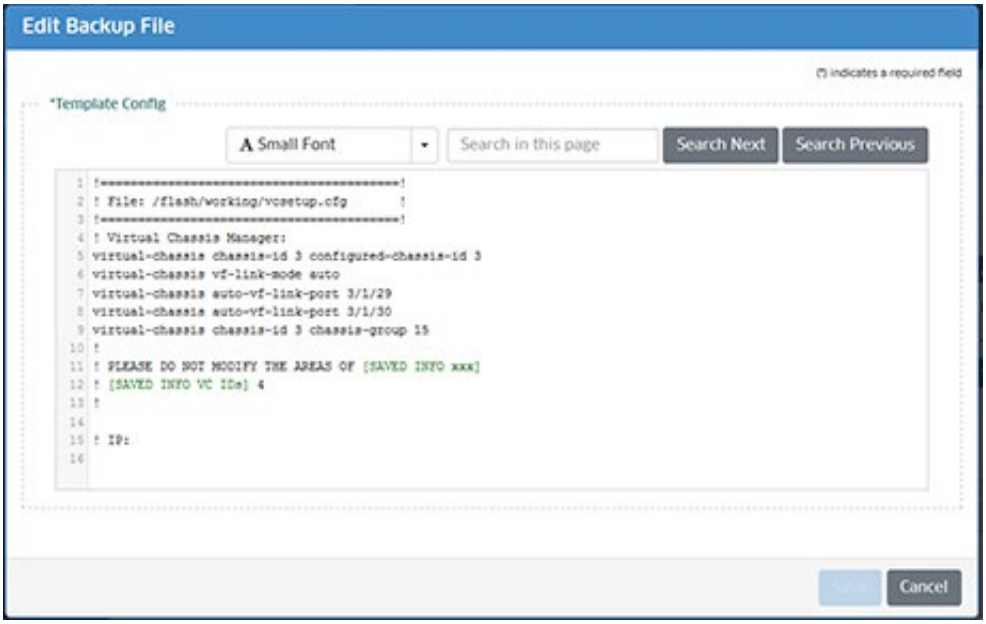
The backup you selected as the new Golden Configuration will appear in the "Golden Config" Column of the switch in the Results Table.

Customizing the Golden Configuration

You can customize the Golden Configuration by editing the configuration files within the Golden Configuration backup file. Go to the "Golden Config" column for the switch in the Results Table and click on the Edit icon in the field. The Details of Golden Config window will appear, with the files contained in the Current Golden Configuration displayed.



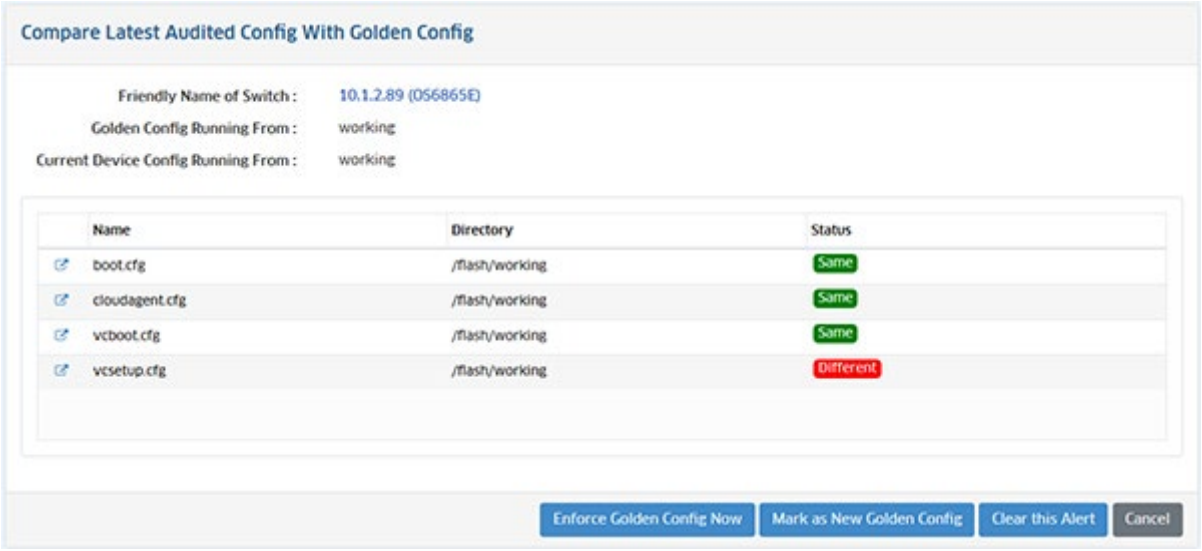
Click on the Edit icon next to the file you want to edit to bring up the Edit Backup File window. Edit the configuration file, click on the **Save** button, then click **Close** the close the window.



The Sync Status in the Results Table will now display Out of Sync. You can now force this new Golden Configuration to the switch or make it the new Golden Configuration as described below.

Auditing the Golden Configuration

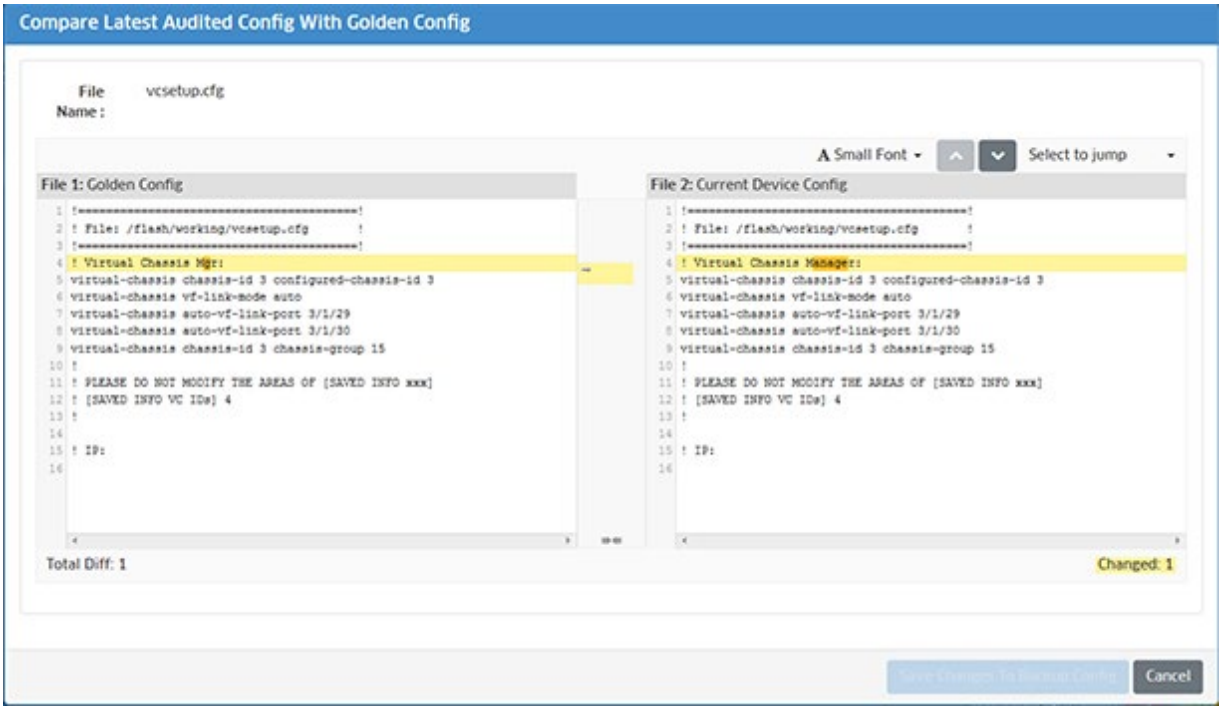
When the Golden Configuration and Running Configuration are different, an alert is displayed and the "Sync Status" column in the Results Table will display "Out of Sync". You can perform an audit to determine which configuration files are out of sync and compare the files for differences. Select the switch in the table and click on the **Audit** button. OmniVista will compare the Golden Configuration and the Running Configuration and highlight any files that have differences as "Out of Sync", as shown below.



You can click on one of the options at the bottom of the screen:

- **Enforce Golden Config Now -** Enforce the current Golden Configuration on the switch. This will copy the Golden Configuration to the switch as the new Running Configuration and reload the switch. Click on the button, then select the directory you want to write the Golden Configuration to. Note that you cannot enforce the Golden Configuration on a switch running from the Certified Directory. You must reload the switch from the Running Directory before enforcing the Golden Configuration on the switch.
- **Mark as New Golden Config -** Make the current Running Configuration the Golden Configuration. This marks the current Running Directory as the new Golden Configuration in OmniVista. To replace the current Running Directory with this Golden Configuration, you must next click on the **Enforce Golden Config Now** button. This will reload the switch with this Golden Configuration as the new Running Directory.
- **Clear This Alert/Cancel -** Do not change the configuration.

Or you could click on the Edit icon to the left of the "Different" file(s) to view a file comparison of the Golden Configuration version and the Running Directory Version of the file.



At this point you could edit the Running Configuration (Current Device Config) based on inputs from the Golden Configuration and click on the **Save Changes to Backup Config** button to save the changes to the Running Directory stored in OmniVista.

Force Provisioning

A switch may fail provisioning because of a problem with the configuration contained in a Configuration Template, or you may want to push a different configuration to a provisioned switch. Once a switch is provisioned through the Provisioning application, it contacts the OmniVista Server ("Calls Home"), at regular intervals. The **Force Provisioning Config** button is used to push a Provisioning Rule configuration to a matching switch the next time the switch

contacts the OmniVista Server. After creating/modifying a Rule, manually push the new configuration to the switch(es) as described below.

Select a switch(es), click on the **Force Provisioning Config** button, then click **OK** at the Confirmation Prompt. The configuration will be pushed to the selected switch(es) the next time the switch contacts the OmniVista Server.

If you decide you do not want to execute the command, click on the button, select **Stop Forcing Provisioning Config**, then click **OK** at the Confirmation Prompt to stop this process before the next "Call Home".

Results Table

- **Serial Number -** The switch serial number.
- **Device Name -** The switch name set in the Preferences application.
- **MAC -** The switch MAC Address.
- **Chassis List -** Displays a list of serial number for a stack or VC of 2 or more switches, or one serial number for standalone or a VC of 1.
- **Switch Model -** The switch model (e.g., OS6350-P10).
- **Switch Location/Geo Location -** The switch location, if set.
- **Operational Status -** The operational status of the switch.
    - **Up -** Device responds to SNMP requests or SSH/Telnet (as per Shell preference) ping request from OmniVista. "Up" Status does not necessarily mean that device is manageable from OmniVista. Refer to the "SNMP Status" column for management status.
    - **Warning -** There is one or more unacknowledged trap on the device.
    - **Down -** Device does not respond to SNMP Requests as well as Telnet/SSH ping requests from OmniVista.
- **Sync Status -** The sync status between the Running Directory and the Golden Configuration.
    - **In Sync -** The Running Directory and the Golden Configuration are the same.
    - **Out of Sync -** The Running Directory and the Golden Configuration are different.
    - **No Golden Config -** The Golden Configuration has not been set for the switch.
    - **No Audit Result -** There is no Audit Result yet.
- **Switch Config Template Used -** The name of the Switch Configuration Template applied to the switch, if applicable. You can click on the View icon in the field to view the Configuration Template.
- **Value Mapping Used -** The Value Mapping parameters used if the Switch Configuration Template is a Dynamic Template. You can click on the View icon in the field to view the Value Mapping parameters.
- **Mgmt Users Template Used -** The Management Users Template applied to the switch. You can click on the View icon in the field to view the Management Users Template.
- **Managed Device in OV -** The IP address of the switch.

- **Latest Config Sent -** The most recent time the latest configuration was sent to the switch. You can also click on the View icon to bring up the "Latest Config Detail" window to display additional information about the Configuration File, then click on the View icon in the window to view the Configuration File contents.
- **Golden Config -** The name of the backup file used as the Golden Configuration for the switch, if applicable. You can also click on the Edit icon to set a Golden Configuration for the switch.
- **Thin Switch -** Indicates if the switch was provisioned as a Thin Switch Client (Yes or No). Note that provisioning a switch as a Thin Switch Client is supported only on switches running AOS Release 8.8R1 (or higher). See Thin Switch Deployment for more information.
- **Incremental Template Apply Status -** Indicates whether an Incremental Template configuration was applied to the Thin Switch Client (Successful or Failed).
    - **Successful -** When an Incremental Template is successfully applied to the switch, the Incremental Template status is automatically disabled; the template is not sent again on the next periodic Call-Home.
    - **Failed -** The Incremental Template was not successfully applied and will be sent again on the next periodic Call-Home.
- **Periodic Audit -** Indicates if periodic auditing is enabled (Yes) or disabled (No) on the switch. You can also click on the Edit icon to enable/disable periodic auditing on the switch.
- **Status -** The result of the latest provisioning attempt for the device (Succeeded/Failed).
- **Last Provision Message -** Information regarding the last provisioning status. You can view the Resource Manager Client Service Log in the Audit application (Administration - Audit) for more details. Click on the "Configuration" link on the left-hand side of the screen, then select "resource-manager-client-service".
- **Force Prov -** Indicates whether the device was configured through "Force Provisioning" (Forced/No).
- **Last Updated -** The date/time when the provisioning information was last updated.

Note: After OmniVista issues the "Configuration Apply" command for the Configuration Template, OmniVista retrieves the status of the operation by checking the output of the "show configuration status" message. If for some reason, OmniVista is unable to receive this message (due to connectivity loss or the switch closing connection due to an SSH session timeout, for example), OmniVista will assume that the Configuration Template was successfully applied, report the provisioning process as "Successful" on the Results Screen, and add the device to the Managed Devices List.

- **Force Prov -** Indicates if "Force Provisioning Config" is enabled (Yes) or disabled (No) on the switch.
- **Last Updated -** The date and time the information was last updated.

Settings

The Provisioning Settings Screen is used to the configure onboarding process for switches that do not match a Provisioning Rule, and the Golden Template audit settings, and Thin Switch Client settings (periodic Call-Home time interval and retry attempts). Configure a setting, then click **Apply**. The changes take effect immediately.

Important Note: There are network prerequisites and switch configuration steps that **must** be completed to enable Provisioning. See the Provisioning Overview Online Help for an overview of the application, including prerequisites, switch setup, and troubleshooting.

Enable/Disable Auditing

If a Golden Configuration is configured for a Provisioning Rule, you can enable periodic auditing to check if a switch's Running Configuration matches the Golden Configuration for the switch. If the audit detects that the Running Configuration has changed from the Golden Configuration, an alert will appear. On the Results Screen, the Sync Status for affected switches will indicate "Out of Sync". You can click on the status for more details and to take corrective action. Audit frequency is configured as described below.

- **Should New Rules Have Audit Enabled by Default -** Enables(Yes)/Disables (No) auditing for the Rule. If enabled, (Default), the Golden Configuration of all switches matching the Rule will be audited at the configured frequency. Note that this is the default setting for newly-provisioned switches. It does not affect already-provisioned/managed switches.

Thin-Client Mode

The following configurable settings are pushed only to switches running AOS Release 8.8R1 (or higher) that match a Thin Switch Provisioning Rule (Thin Switch is enabled):

- **Time To Next Callhome -** The amount of time, in minutes, the switch waits before sending the next periodic Call-Home request. (Default = 30 minutes)
- **Max Retry Attempts -** The maximum number of times the Thin Switch attempts to reconnect with OmniVista. (Default = 30 attempts).

The Thin-Client Mode settings are not pushed to switches that are not provisioned to operate as a Thin Switch. See the Thin Switch Deployment Overview Online Help for more information.

Action When No Matching Rule Is Configured

When a switch matches a Provisioning Rule, it is configured and can be managed by OmniVista. However, a switch may not match any existing Provisioning Rules. You can choose to automatically onboard these switches (default), or not. Select a radio button to set the onboarding process. This setting applied to all switches that contact OmniVista for provisioning.

- **Onboard and manage devices even when they don’t have a matching Rule -** Allow switches to onboard even if they do not match a Provisioning Rule. The Default Management Users Template will be applied to the switch. The switch will be displayed in the Managed Devices List and will be manageable by OmniVista. The switch will also appear in the Results Table.
- **Do not onboard and manage devices with no matching Rule. Such devices will retry onboarding until a matching rule is defined for them -** Do not allow a switch to onboard if it does not match a Provisioning Rule. A Serial Number Rule with the Default Management Users Template will automatically be created on the Rules Screen with a Provisioning Status of "No Match". The switch will not be displayed in the Managed Devices List and will not manageable by OmniVista until it matches a

Provisioning Rule. The switch will continue to contact OmniVista until it is matched to a Rule.

Frequency of Audit

By default, if auditing is enabled, an audit is performed daily at 12:00 a.m. However, you can set the frequency as described below.

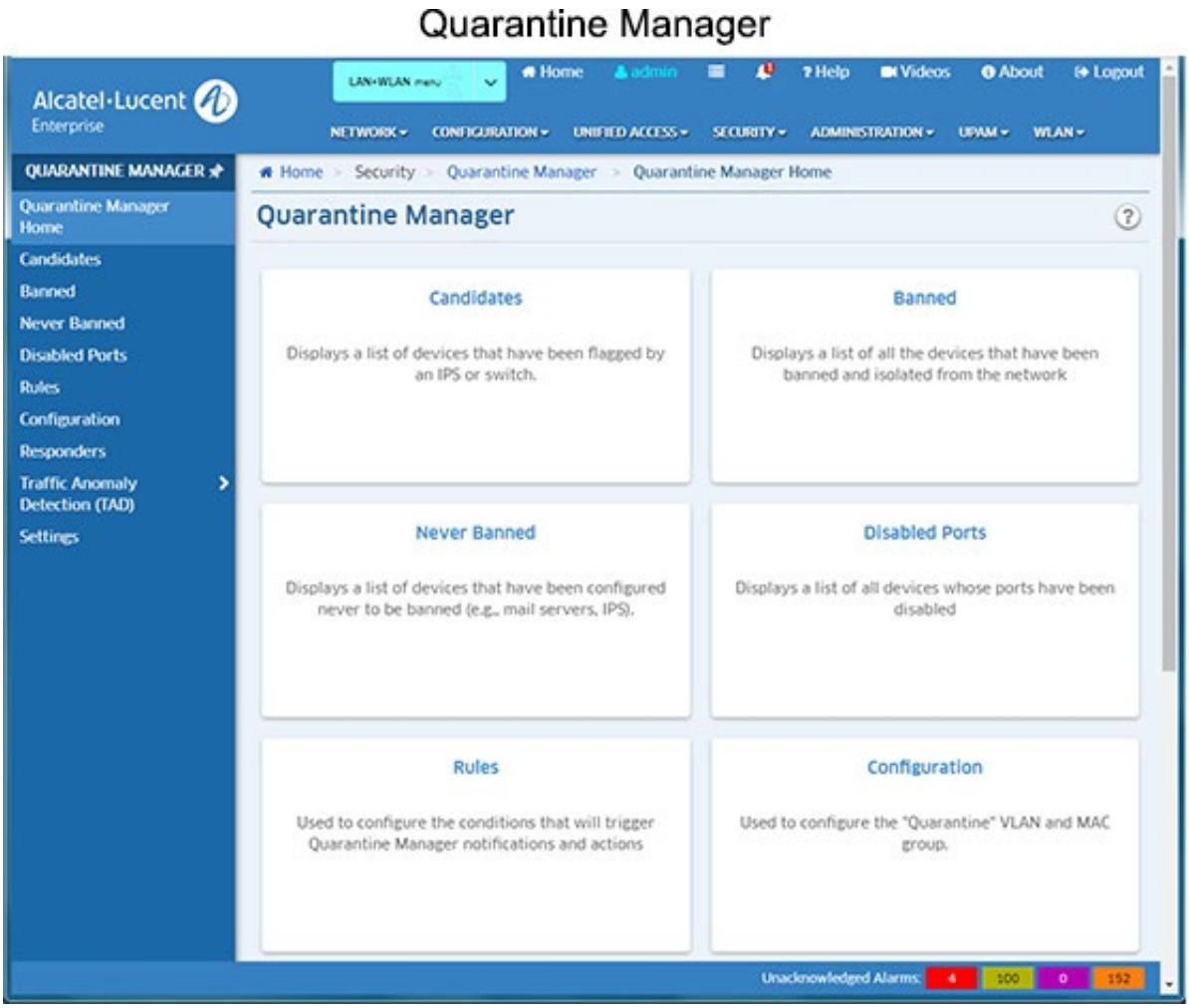
- **Start At -** The time of day to perform the audit.
- **Recurrence Pattern -** Configure the frequency of the audit.
    - **Hourly -** Select "Hourly", click in the "Every __ Hours" field and enter a number (Range = 1 - 24).
    - **Daily -** Select "Daily" to perform the audit 7 days a week at the configured "Start At" time. Select "Every Weekday" to perform the audit Monday through Friday at the configured "Start At" time.
    - **Weekly -** Select "Weekly" and select a day(s) of the week to perform the audit at the configured "Start At" time.
    - **Monthly -** Select "Monthly" and configure the days/number of months to perform the audit at the configured "Start At" time.

25.0 Quarantine Manager

The Quarantine Manager application enables the network administrator to quarantine devices to protect the network from attacks. The application works with an external Intrusion Prevention System (IPS), such as Fortinet, or a network device, such as an Alcatel-Lucent Enterprise AOS switch, which sends either a Syslog message or SNMP trap to Quarantine Manager containing the IP or MAC address of the offending device. (If an IP address is received, Quarantine Manager uses its Locator function to determine the device's MAC address.) These messages trigger Quarantine Manager Rules. Depending on the rule that is written for the event, the device can be immediately quarantined or placed in a Candidate List that can be reviewed by the Network Administrator for further action.

The application also includes the optional Quarantine Manager Remediation (QMR) feature. QMR is a switch-based application that interacts with Quarantine Manager to restrict network access of quarantined clients and provide a remediation path for these clients to regain their network access.

Note: Quarantine Manager cannot quarantine any devices on the EMP subnet because the EMP port has no mobility feature.



Quarantine Manager is configured using the following screens, which can be accessed from the Quarantine Manager Home Page or by clicking on the links on the left side of any Quarantine Manager screen.

- **Candidates -** Displays a list of devices that have been flagged by an IPS or switch. The Network Administrator can release a device from the list, ban a device, or configure a device to never be banned.
- **Banned -** Displays a list of all devices that have been banned and isolated from the network.
- **Never Banned -** Displays a list of devices that have been configured never to be banned (e.g., mail servers, IPS). Note that all switches discovered by OmniVista are implicitly on the Never Banned List even though they are not displayed.
- **Disabled Ports -** Displays a list of all devices whose ports have been disabled.
- **Rules -** Used to configure the conditions that will trigger Quarantine Manager notifications and actions. Configuration - Used to configure the "Quarantine" VLAN and MAC group, as well as the action that will be taken for the event. It is also used to configure the optional Remediation Server.
- **Responders -** Used to specify the responses, such as run an audio program or send an e-mail to the MIS director, based on the conditions given. Quarantine Manager Logs
- **Traffic Anomaly Detection (TAD) -** Used to configure the TAD feature. TAD is a network monitoring feature that detects anomalies in the network traffic by monitoring the difference in the rate of ingress and egress packets on a port, matching a specific traffic pattern.
- **Settings -** Used to specify SysLog settings for Quarantine Manager. The Audit application can be used to access the Quarantine log and Syslog. The logs contain detailed information about Quarantine Manager and Syslog events.

The following sections detail Quarantine Manager requirements and basic Quarantine Manager configuration.

Quarantine Manager Requirements

The following sections detail hardware/software and basic configuration requirements for Quarantine Manager.

Hardware/Software Requirements

OmniVista Hardware/Software

Quarantine Manager is sported on AOS6250, 6350, 6400, 6450, 6850, 6855, 6860, 9000, and 10K Switches, as well as Aruba. Fortinet software version 2.3 is supported.

External Notification Device

An external device must be set up to send notifications to the Quarantine Manager application. The application works with an external Intrusion Prevention System (IPS), such as Fortinet, or a network device, such as an Alcatel-Lucent Enterprise AOS switch, which sends either a Syslog

message or SNMP trap to Quarantine Manager containing the IP or MAC address of the offending device.

For example, a Fortinet IPS device must be set up to send Syslog messages to Quarantine Manager. This set up includes specifying the IP address of the OmniVista server and the port address for the OmniVista Syslog daemon (preset default is 514); and specifying what events received by the IPS will generate a Syslog Message. The message (either Syslog message or trap) must include the IP or MAC address of the offending device.

Remediation Server (Optional)

You can set up a Remediation Server that will work with Quarantine Manager to notify the user when a device is placed into the Banned List. The feature can also be configured to utilize programs/patches to debug the device and restore network access.

Quarantine Manager Remediation (QMR) is a switch-based application that interacts with Quarantine Manager to restrict network access of quarantined clients and provide a remediation path for these clients to regain their network access. A Network Administrator can set up a Remediation Server that will work with Quarantine Manager to notify the user when a device is placed into the Banned List. The feature can also be configured to utilize programs/patches to debug the device and restore network access.

When Quarantine Manager quarantines a client, the client MAC address is added to the MAC address group on the LDAP server. QMR pulls the MAC addresses from this group to populate the "Quarantined" MAC address group on the switch. At this point, network access for these clients is restricted to communication with the designated Remediation Server, and exception subnet if configured (and essential protocols such as ARP, DHCP, and DNS), until the client's quarantined status is corrected

When a client has corrected its quarantined state, Quarantine Manager updates the MAC address group on the LDAP server to remove the MAC address of the client. QMR will then restore network access to that client the next time QMR checks the LDAP MAC address group.

> **Note:** Configuring QMR and QoS inner VLAN or inner 802.1p policies is mutually exclusive. QMR overlays the inner VLAN tag, thus creating a conflict with related QoS policies. This is also true with QMR and VLAN Stacking services.

Configuration Requirements

Quarantine Manager is configured using the Configuration and Rules Screens as described below. Detailed instructions for each screen are provided in the on-line help for the screen.

Quarantine VLAN and MAC Group

A basic "Quarantine" VLAN is pre-configured on OmniVista. You customize this "basic" Quarantine VLAN using the Configuration Screen. You must also configure a "Quarantine MAC Group using the Groups application. After configuring the Quarantine VLAN and MAC Group, you apply the configuration to devices you want to monitor using Quarantine Manager.

Quarantine Manager Rules

Quarantine Manager Rules are configured for dealing with Syslog events and SNMP traps. The easiest way to use Quarantine Manager is to enable one of the Built-in Rules. The Rules determine which events from an external IPS or switch are propagated through the network. For example, when the IPS notices an attack, it generates a Syslog event. After receiving a Syslog

message, Quarantine Manager uses the rules to determine what device generated the event and whether or not the offending device is immediately quarantined (Banned) or placed on the Candidate List to be reviewed by the Network Administrator. The way in which a device is quarantined depends on the action that is configured for the rule.

If a device is placed in the Candidate list, all traffic to the suspect device continues. The Network

Administrator reviews each event in the Candidate List and decides what action to take. If a device is placed in the Banned list, it is quarantined until it is manually removed by the Network Administrator.

> **Note:** There are a number of important devices in a network that a Network Administrator will never want to be quarantined. Use the Never Ban List to ensure that important devices are never quarantined.

Creating Quarantine Subnets (Optional)

If a device is banned either by the Network Administrator if Quarantine Manager, the ban is applied to all devices in the network. However, you can segment your network by creating a logical "Quarantine" network. This will limit Quarantine Manager actions to only those switches in the "Quarantine" subnetwork(s). To create "Quarantine" subnet(s) create a map in the Topology application "Quarantine". You then create Quarantine subnets under the Quarantine network.

Candidates

The Quarantine Manager Candidates Screen displays all devices that have been placed in the Candidates Quarantine List. When an external Intrusion Prevention System (IPS), such as Fortinet, detects a possible attack on the network, it generates either a Syslog Event or an SNMP Trap. A Quarantine Manager rule can be configured (Configuration Screen) to trigger an action based on these events. The action will either immediately quarantine the offending device or place the device on the Candidates Quarantine List. If the device is placed on the Candidates List, traffic to and from that device will continue until the Network Administrator decides what action should take place. The Network Administrator can:

- **Release the Device from the Candidates List -** To remove a device from the Candidates list, select the device and click the **Release** button. The device is removed from the list. A device may return to the list if another event triggers a configured quarantine rule.
- **Ban the Device -** To ban a device from the network, select the device and click the **Ban** button. The device is removed from the network and placed in the Banned Quarantine List.
- Place the Device on the List of Devices to Never be Banned - To place a device in the Never Banned list, select the device and click the **Never Ban** button. The device is placed in the Never Banned list. An event will never trigger a quarantine rule for a device in the Never Banned Quarantine List.

Candidates Quarantine List

- **MAC Address -** The device's MAC address. Quarantine Manager Rules extract the IP address of the device. Quarantine Manager then uses the OmniVista Locator

Function to determine the MAC address. **IP Address -** The device's IP address. All Quarantine Manager Rules must extract the IP address from the Syslog Message or SNMP Trap. If the IPS sends a MAC address, the IP address will have a value of 0.0.0.0.

- **Timestamp -** The date and time the event occurred.
- **Reason -** The reason the event triggered a Quarantine Manager rule. For all Fortinet-generated events, select the event in the table and right-click to access a detailed description of the event.
- **Incident Count -** The number of times an anomaly has been seen for the candidate device.

Fortinet Web Site

You can access the Fortinet web site for a detailed description of any Fortinet event. To access the description:

1. Click on the event in the Candidates Quarantine List to highlight it; then right-click on the event. The Reason window will appear.
2. Click on the Fortinet web address button at the bottom of the Reason window. A Fortinet In-Depth Analysis page will appear describing the event in detail and providing any recommended actions.

Banned

The Quarantine Manager Banned Screen displays a list of all devices than have been quarantined, either by a Quarantine Manager rule, or by the Network Administrator. When a device is placed in the Banned

Quarantine List, it is quarantined from the rest of the network. Devices can automatically be added to the Banned List based on a Quarantine Manager rule or manually placed in the list by the Network Administrator. Once a device is placed in the Banned List, it remains quarantined until the Network Administrator manually releases it.

A Network Administrator can add a device to the list, edit a device on the list, release a device from the list, retry adding a device to the list, or re-poll the network for banned devices.

Note: DHCP requests from a banned device are sent to the Quarantine VLAN. The Network Administrator can direct banned traffic from the Quarantined VLAN to a Remediation Server that will provide the user with information explaining why their device was banned and what steps to take to connect to the network.

Note: Quarantine Manager can ban devices connected to an OmniAccess WLAN device using the device's "Blacklist" feature. However, the 'enable' password of the device must be entered in the Secondary Password field for the device using the "Discovery - Edit Device" Operation in the Topology application.

Note: Quarantine Manager uses a "Fast Re-Cache" mechanism. With this mechanism, the switch will look through LDAP only for the existence of quarantine MAC groups. The contents of the MAC group are added to the quarantine settings without flushing any other policies. This feature is only available on the 6400, 6850, 6855 and 9000 Series Switches running 6.3.1.R01 or later.

Adding a Device to the Banned List

In addition to automatically quarantining devices based on a Quarantine Rule, you can also manually quarantine a specific device by adding it to the Banned List. Click on the Add icon. Select the IP Address or MAC Address option, enter the IP address (or Host Name) or MAC address. Enter an optional explanation in the Reason field and click on the **Create** button. The device will appear in the list.

Editing a Device on the Banned List

Certain information about a banned device may not be picked up by a QM Rule. A Network Administrator is allowed to edit the IP Address and Reason for an entry in the Banned List to make it more closely match what the Network Administrator knows to be the best information about a banned device. Select the device in the list and click on the Edit icon. Edit the field(s) and click on the **Apply** button.

Releasing a Device from the Banned List

To release a device from the Banned List, select the device(s) in the list and click on the **Release** button. Click **OK** at the confirmation prompt.

Retry

To retry a failed operation (e.g., release device from the Banned List), select the device in the Banned List and click on the **Retry** button.

Re-Polling for Banned Devices

Click on the **Redo Ban** button to poll the network for banned switches. This is useful if you have banned switches without first creating a Quarantine VLAN or MAC Group.

Banned Quarantine List

- **MAC Address -** The device's MAC address. Quarantine Manager Rules extract the IP address of the device. Quarantine Manager then uses the OmniVista Locator function to determine the MAC Address.
- **IP Address -** The device's IP address or the host name. All Quarantine Manager rules must extract the IP address from the Syslog Message or SNMP Trap.
- **Timestamp -** The date and time the event occurred.
- **State -** The state of the banning action:
- Scheduled to be Banned (Ban is in process)
- Completed (Ban is complete)
- Partially Banned (Ban not completed for all devices)
- Scheduled to Be Released (Release is in process)
- Partially Released (Release not completed for all devices).
- **Reason -** The reason the event triggered a Quarantine Manager rule. For all Fortinet-generated events, select the event in the table and right-click to access a detailed description of the event.

- **Partial Results -** The devices where the ban has either succeeded, or for which the user has not configured/enabled Quarantine Manager. You can click on an entry to display a detailed view listing the switches that are included in the quarantine of the banned device.
- **VLAN Name -** The user-configured name for the Quarantine VLAN.
- **MAC Group Name -** The user-configured name for the Quarantine MAC Group.

Never Banned

The Quarantine Manager Never Banned Screen displays a list of devices that have been specified by the Network Administrator never to be banned (e.g., mail servers, IPS). The screen is used to add a device to the list, edit a device description on list, and delete a device from the list. A device placed on the Never Banned list can never be banned, either manually or automatically by Quarantine Manager. Important network servers should be placed in the Never Banned Quarantine List.

> **Note:** The OmniVista Server and all switches discovered by OmniVista are implicitly placed in the Never Banned list. Even though these devices do not appear in the list, they cannot be banned.

Adding a Device to the Never Banned List

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

- **Address -** Select the applicable tab and enter the device's IP Address (or host name) or MAC Address. Note that you can enter the host name only if the IP Address radio button is selected. If you ban a device by the MAC address, the IP address will display a value of 0.0.0.0. If you ban a device by its IP address, Quarantine Manager will use its Locator function to determine the MAC address.
- **Reason -** Enter a reason for placing the device on the Never Banned List.

Editing a Device on the Never Banned List

You can edit the Reason field for a device in the Never Banned List. Click on the Edit icon. Edit the field(s) as described above and click on the **Apply** button.

Deleting a Device from the Never Banned List

Select a device in the Never Banned List and click on the Delete icon. Click **OK** at the Confirmation prompt.

Never Banned Quarantine List

The Never Banned Quarantine List provides basic information for all devices on the list. Click on a device to display more detailed information.

- **MAC Address -** The device's MAC address.
- **IP Address -** The device's IP address or host name. If an Intrusion Prevention System (IPS) sends a MAC address, the IP address will have a value of 0.0.0.0.
- **Timestamp -** The date and time the device was placed on the Never Banned list.

- **Reason -** The reason the device is in the Never Banned list.

Disabled Ports

The Quarantine Manager Disable Ports Screen displays a list of all devices whose ports have been disabled, either by a Quarantine Manager Rule or by the Network Administrator. The screen is used to release a device from the list, edit a device description on list, and retry a failed port operation. When a port is disabled, an entry appears in the Disabled Ports List table. If you attempt to ban multiple MAC addresses for the same switch's slot/port, multiple entries will appear in the table.

> **Note:** If you disable a port that was already disabled, there will be two entries in the table. The first entry will contain the MAC address of the offending end station. The second entry will contain a null (possibly 000000:000000) MAC address. The reason for this second entry is that when you use the Banned Screen to release a MAC address, the port will not be re-enabled. The Network Administrator will have to manually re-enable the port by releasing the port from the Disabled Ports List.
>
> **Note:** When you release an entry from the Disabled Port List, the item will be removed. If it is the last item with the specified IP address and slot/port combination, then that port will be enabled. That is, the port will not be enabled until every device that caused it to be banned has been released.

Release a Device from the Disabled Port List

Select a device(s) in the list and click on the **Release** button. Click **OK** at the confirmation prompt.

Edit a Device in the Disabled Port List

You can edit the Reason and the Timestamp fields for a device in the Disabled Ports List. Select a device in the list and click on the Edit icon. Edit the field(s) and click on the **Apply** button.

Retry a Port Operation

To retry a failed operation during the enabling/disabling of a port, select the device in the Disabled Ports List and click on the **Retry** button.

Disabled Port List

- **Switch Address -** The device's IP address. Quarantine Manager Rules extract the IP address from Syslog Message or SNMP trap.
- **Port -** The disabled slot/port number.
- **Timestamp** - The date and time the event occurred.
- **MAC Address -** The device's MAC address. Quarantine Manager Rules extract the IP address of the device. Quarantine Manager then uses the OmniVista Locator function to determine the MAC address.
- **State -** The state of the disabling or enabling action:
- Completed (Disabling is complete)
- Failed (Disabling/enabling of a port failed)
- **Reason -** The reason a port was disabled.

Rules

The Quarantine Manager Rules Screen displays all configured Quarantine Manager Rules and is used to configure the conditions that will trigger Quarantine Manager notifications and actions. Quarantine Manager Rules determine which Syslog events or SNMP traps cause a device to be placed in the Candidates List or Banned List, or released. You can create, edit, delete, enable/disable, and import rules.

Quarantine Manager Rule Overview

Quarantine Manager Rules determine the conditions that will trigger Quarantine Manager notifications and actions. A rule contains:

- A trigger expression that specifies the event or trap that will trigger an action
- An extraction expression that is used to extract the source address from the event or trap
- An action to be taken when the event or trap is received (device is placed in the Candidates List or Banned List, or released).

Note: Banned rules have precedence over Candidate rules. If an event matches more than one rule, Quarantine Manager will match the first rule that places a device on the Banned list. If there is no rule that places the item on the Banned list, Quarantine Manager will match the first rule that places the device on the Candidate list.

Rule Types

There are two types of rules: Built-In Rules and Custom Rules. The Built-In Rules cannot be deleted (although they can be modified or disabled). Custom Rules are rules that the Network Administrator creates.

Built In Rules

There are thirteen (13) Built-In Rules that come with Quarantine Manager. Built-In Rules are initially configured in the Disabled state. You must edit these rules to change the "Enabled" status to "True" to enable these rules. The default action configured for all of the Built-In Rules is to send the device to the Candidates list for review by the Network Administrator. Although the rules are pre-configured, the Network Administrator can modify the them. The Built-In Rules are:

- **Alcatel DOS Trap Rule -** Triggers an action based on an AOS DOS trap (AlaDosTrap). The rule triggers an action in response to a Teardrop, Ping of Death, or Port Scan attack. You can use Regular Expressions to create rules for additional AOS DOS traps.
- **Brick -** Triggers an action on a Brick Anomaly Event.
- **Fortinet Anomaly -** Triggers an action on a Fortinet Attack Anomaly Event. Ignores Anomaly attacks configured to "Pass" on Fortigate.
- **Fortinet Signature -** Triggers an action on a Fortinet Syslog Signature event. Ignores Signature attacks configured to "Pass" on Fortigate.
- **Fortinet Virus -** Triggers an action on a Fortinet Virus Detection event. Only triggers on sub-type "infected".

- **HTTP Server DOS Attack Trap -** Triggers an action when a "Denial of Service" Trap is received from an HTTP Server.
- **OA SafeGuard Malware Cleared -** Triggers and action when SafeGuard clears malware.
- **OA SafeGuard Malware Detected -** Triggers and action when SafeGuard detects malware.
- **OA WLAN Containment on AP -** Containment has been enabled for a suspected rogue AP because
- the confidence level for that AP equals or exceeds the configured value for that setting.
- **OA WLAN Potential Rogue AP -** An AP has been detected with conditions that may cause it to be classified as a rogue or suspected rogue.
- **OA WLAN: Rogue AP Active -** Triggers an action when the switch classifies an Access Point as a "Rogue AP."
- **OA WLAN: Rogue AP Detected -** Triggers an action when the Access Point detects an active "Rogue AP."
- **OA WLAN: Station w/ Rogue AP -** Triggers an action when the Access Point detects traffic from a client through a "Rogue AP."

Fortinet Anomaly and Signature attack events include a "status=" attribute that can be "clear_session","pass_session", "dropped", "reset", or "detected". When Fortigate is configured to allow a particular attack (using the GUI to set its action to "Pass"), a Syslog event is still sent out for that attack, but its status is "detected"; meaning it is detected but not acted upon. Our built-in triggers are therefore designed to act on any value of "status=" EXCEPT for "detected". This means you can use the Fortigate control panel to selectively enable or disable attack actions and Quarantine Manager will behave consistently, without the need to change any of these triggers.

The Canned rules in Quarantine Manager for Fortigate have been modified as such, in both the anomaly and signature rules.

- log_id=0421073001.*status=[^p].[^t]
- log_id=0420070000.*status=[^p].[^t]

The [^p] was added to exclude any Syslog message starting with a "p" character, as well as a "t" character. This prevents quarantine for both "detected" and "pass_session" status.

The "pass_session" state was previously unknown.

> **Note:** Built In Rules cannot be deleted, however, they can be edited and enabled/disabled.
>
> **Note:** The Audit application can be used to access the Quarantine log and Syslog. The logs contain detailed information about Quarantine Manager and Syslog events.

Custom Rules

The Network Administrator can create Custom Rules using Regular Expressions to configure the trigger event and extraction expression. The rules can be based on an Intrusion Prevention System (IPS) event or an AOS SNMP trap notification. Custom Rules can be created, edited, deleted, enabled/disabled, and imported.

Note: You must be careful when creating a rule since a mis-configured rule could cause an important service to be inadvertently banned.

Regular Expressions Overview

Trigger Expressions

As stated earlier, a Trigger Expression is a regular Java expression that is used to determine if a Syslog message or SNMP Trap should trigger a quarantine action. If a Syslog Message or SNMP Trap matches this regular expression, the action is performed. For example, let's say that we are interested in a Fortinet Syslog Event that looks something like:

Fortinet Anomaly 03-08-200 14:09:34 device_id=FG36002805033253 log_id=0421073001 type=ips subtype=anomaly pri=critical attack_id=102039582 src=90.0.0.10 dst=10.10.10.100 src_port=2370 dst_port=139 src_int=internal dst_int=external status=dropped proto=6 service=139/tcp msg="netbios: *SMB.NTLMSSP.Attempt.B*

Many Syslog messages appear similar. However, each message may have a different date, device ID, source and destination address, etc. What is unique about each Syslog message is the log_id value. If you are interested in all Fortinet Syslog messages with a log_id of 0421073001, then the regular expression is easy - you can simply search for any message that contains the String log_id=0421073001. In the Trigger Expression Field you would type the value log_id=0421073001.

Extraction Expressions

As stated earlier, an Extraction Expression is a regular Java expression that specifies the source address of the offending device. Once a Syslog message matches a Trigger Expression, Quarantine Manager must extract the source address of the suspect end station from the message. In the Fortinet example above, the source address is preceded by the string "src=" and then an IP address. An IP address consists of 4 sets of numbers separated by the "." character. Each set is 1 to 3 characters in length and the numbers are decimal (0-9) digits. One way to express this is with the regular expression

src=([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})

Because we are only interested in the IP address and not the characters "src=", place ( ) around the IP address to indicate which part you want to capture. The [0-9] means any single character from 0-9, the {1,3} means that you are looking for a set of 1 to 3 numbers. The \. says that you are looking for a "." character. The backslash is an escape character that says take the "." literally (normally "." is a special character that means any character.

Often there are a number of regular expressions that you can use to achieve the same results. In the Fortinet example above, there is the string "src=" followed by the IP address, followed by either a space or a tab character. The regular expression for getting the IP address could be

src=([^]*)

The characters between the [ ] are ^, a space character and a tab character. This expression says: the string "src=" followed by a sequence of characters that are not spaces or tabs. This expression works well, but it can be difficult to read because the space and tab character are not "visible".

Another way to extract the IP address would be

src=([0-9.]*)

This says, the string "src=" followed by a sequence of characters that contain only numbers and the "." (a "." inside of [ ] does not need to be escaped).

> **Note:** If an extraction expression is not working, check the server.txt file to troubleshoot the problem.

Useful Operators for Quarantine Manager Rules

^ the "not" operator

[start of character list
] end of character list

(beginning of an expression
) end of an expression

[.] useful for escaping characters used as operators in regular expressions

Basic Regular Expressions

. Matches any single character

[...] Matches any one of the characters enclosed between the brackets. If the first character is a circumflex (^), then it matches any one character Not enclosed between the brackets. A hyphen (-) is used to indicate a range of characters.

**** Escape the special character that follows.

***** Matches any number (including none) of the single character that immediately precedes it.

+ Matches one or more occurrences of the preceding regular expression.

? Matches zero or one occurrences of the preceding regular expression.

For example:

[abc] Matches either an 'a', 'b' or 'c'

[a-z] Matches all lower case letters

[a-zA-Z] Matches all letters

[0-9a-fA-F] Matches all hex digits

[^0-9] Matches any character that is not a digit

AOS DOS Trap Configuration

In addition to the Built-In Rule for AOS DOS Traps (0, 2, 6), you can configure a Rule for other AOS DOS traps. For example, the built-in rule for AOS DOS Traps is:

TrapName=alaDoSTrap.*alaDoSType=[0|2|6]

This triggers a response on AOS DOS Trap type 0, 2, and 6.

To trigger on types 0, 2, 6, 9, 10, 11, 12 and 13, you would enter:
TrapName=alaDoSTrap.*alaDoSType=([0|2|6|9]|1[0123])

The ( ) form a group

Inside the group are basically two parts separated by a vertical bar | which means either or so we have

(A | B)

The first part (A) is

[0|2|6|9]

The square brackets [ ] mean match a single character from the list. The vertical bar | means or. So this expressions says either a 0 or 2 or 6 or 9.

The second part (B) is

1[0123]

which means a 1 followed by either a 0 or a 1 or a 2 or a 3

That expression could have been written as 1[0-3]

The dash - is a special character which is used to express a range.

Note that we could **not** have written the expression as alaDoSType=[0-13] to match all 13 types. This expression says a 0 through 1 or a 3. so it would match:

alaDoSType=0 alaDoSType=1 alaDoSType=3

Creating a Quarantine Manager Rule

Click on the Add icon and complete the fields as described below. When you are done, click on the **Create** button.

- **Name -** The user-defined name for the rule.
- **Description -** The user-defined description for the rule.
- **Trigger Expression -** A regular Java expression that is used to determine if a Syslog message or SNMP trap should trigger a quarantine action. If a Syslog message or SNMP Trap matches this regular expression, the action is performed. The regular expressions used by OmniVista are very similar to those used by programs such as PERL and AWK.
- **Extraction Expression -** A regular Java expression that specifies the source address of the suspect device. Use the ( ) expression to capture the source IP or MAC address. (Quarantine Manager also supports the hex form of IP addresses.) Once Quarantine Manager receives a Syslog message or SNMP trap that matches a Trigger Expression, it must extract from it the source address of the suspect end station.
- **Action -** The action to be taken when the rule is triggered:
- **Candidate List -** The device is added to the Candidates list. The device can still send and receive traffic. The Network Administrator reviews the list and determines what action to take (e.g., remove the device from the list, ban the device)
- **Quarantine -** The device is moved to the Quarantined VLAN and/or MAC Group, and added to the Banned list. While on the Banned list, the device cannot send or receive traffic. The device remains on the list until it is manually removed by the Network Administrator.
- **Release** - The device is released from the Quarantined VLAN and/or MAC Group. This can be used to allow an external system (e.g., Trouble Ticket System) to send a syslog message or trap to OmniVista to automatically release a quarantine without having to access OmniVista. Note that the Quarantine VLAN or MAC group must be properly set up for traffic to be quarantined. If you do not first configure a Quarantine

VLAN or MAC group, even a device on the Banned list could still pass traffic. The Quarantine VLAN or MAC group is configured in the Configuration Screen.

- **Event Type -** The type of triggering event (Syslog or Trap).
- **Enabled -** Administrative state of the rule:
- **On -** The rule is enabled.
- **Off -** The rule is disabled.

Editing a Quarantine Manager Rule

Select a rule in the list and click on the Edit icon. Edit the field(s) as described above and click on the **Apply** button. Note that you cannot edit a rule name.

Deleting a Quarantine Manager Rule

Select the rule(s) in the list that you want to delete and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Enabling/Disabling a Quarantine Manager Rule

To enable/disable a rule(s), select the rule(s) in the list and click on the **Enable/Disable Rules** button.

Importing a Quarantine Manager Rule

You can import a new rule from Alcatel-Lucent Enterprise without having to update the Quarantine Manager code. New rules are sent by Alcatel-Lucent Enterprise as .xml files.

1. Save the .xml file on your machine.
2. Click on the **Import** button.
3. Browse to the .xml file that you saved, select the rule and click **OK**. The Import window will close and the new rule will appear in the Rules table. A sample of an imported .xml file is shown below.

   Note: Imported rules are initially configured in the Disabled state. You must change the "Enabled" status to "True" to enable the rules.

.xml import file sample:

```
<?xml version="1.0"?>
<!DOCTYPE quarantineRules[
<!ELEMENT quarantineRules (quarantineRule)*>
<!ELEMENT quarantineRule (desc, trigger, extract)>
<!ELEMENT desc (#PCDATA)>
<!ELEMENT trigger (#PCDATA)>
<!ELEMENT extract (#PCDATA)>
<!ATTLIST quarantineRule name CDATA #REQUIRED
eventType (syslog | snmptrap) #REQUIRED
```

type (standard |custom) "standard" enabled (true | false) "false" action (ban | candidate | release) "candidate"

>

]>

<quarantineRules>

<!-- Forntinet Syslog IDS Signature Event -->

<quarantineRule name="test Signature" eventType="syslog">

<desc>test IDS Signature</desc>

<trigger>log_id=0420070000.*status=[^p].[^t]</trigger>

<extract>src=([0-9.]*)</extract> </quarantineRule>

</quarantineRules>

Quarantine Manager Rule List

The Rule List displays information about all Quarantine Manager Rules stored in OmniVista.

- **Name -** The user-defined name for the rule.
- **Description -** The user-defined description for the rule.
- **Trigger Expression -** A regular Java expression that is used to determine if a Syslog message or SNMP trap should trigger a quarantine action. If a Syslog message or SNMP Trap matches this regular expression, the action is performed. The regular expressions used by OmniVista are very similar to those used by programs such as PERL and AWK.
- **Extraction Expression -** A regular Java expression that specifies the source address of the suspect device. Use the ( ) expression to capture the source IP or MAC address. (Quarantine Manager also supports the hex form of IP addresses.) Once Quarantine Manager receives a Syslog message or SNMP trap that matches a Trigger Expression, it must extract from it the source address of the suspect end station.
- **Action -** The action to be taken when the rule is triggered:
- **Candidate List -** The device is added to the Candidates list. The device can still send and receive traffic. The Network Administrator reviews the list and determines what action to take (e.g., remove the device from the list, ban the device)
- **Quarantine -** The device is moved to the Quarantined VLAN and/or MAC Group, and added to the Banned list. While on the Banned list, the device cannot send or receive traffic. The device remains on the list until it is manually removed by the Network Administrator.
- **Release** - The device is released from the Quarantined VLAN and/or MAC Group. This can be used to allow an external system (e.g., Trouble Ticket System) to send a syslog message or trap to OmniVista to automatically release a quarantine without having to access OmniVista. Note that the Quarantine VLAN or MAC group must be properly set up for traffic to be quarantined. If you do not first configure a Quarantine VLAN or MAC group, even a device on the Banned list could still pass traffic. The Quarantine VLAN or MAC group is configured in the Configuration Screen.
- **Event Type -** The type of triggering event (Syslog or Trap).

- **Enabled -** Administrative state of the rule:
- **On -** The rule is enabled.
- **Off -** The rule is disabled.

Configuration

The Quarantine Manager Configuration Screen id used to configure Quarantine Manager, including the Quarantine VLAN, Quarantine MAC Group, and the optional Quarantine Manager Remediation (QMR) feature. By default, the name of the Quarantine VLAN is "Quarantined". A basic "Quarantine" VLAN is pre-configured on OmniVista ("Quarantined"). You customize this "basic" Quarantine VLAN using the Configuration Screen.

When a Quarantine Rule extracts an IP address from a device, OmniVista uses the Locator function to determine the MAC address of the device. The device is then automatically added to the Quarantined MAC group. When devices are banned, either through a Quarantine Manager rule or by the Network Administrator, they are added to the Quarantined VLAN and/or Quarantined MAC group. These devices no longer route traffic to any other devices in the network (although you can create a logical "Quarantine" subnet to limit Quarantine Manager actions to a specific set of switches on the network.). The devices remain in the Banned list until removed by the Network Administrator.

> **Note:** Quarantine Manager has the ability to ban devices connected to an OmniAccess WLAN device using the device's "Blacklist" feature.

Quarantined Manager Remediation (QMR)

Quarantine Manager Remediation (QMR) is a switch-based application that interacts with Quarantine Manager to restrict network access of quarantined clients and provide a remediation path for these clients to regain their network access. A Network Administrator can set up a Remediation Server that will work with Quarantine Manager to notify the user when a device is placed into the Banned List. The feature can also be configured to utilize programs/patches to debug the device and restore network access.

When Quarantine Manager quarantines a client, the client MAC address is added to the MAC address group on the LDAP server. QMR pulls the MAC addresses from this group to populate the "Quarantined" MAC address group on the switch. At this point, network access for these clients is restricted to communication with the designated Remediation Server, and exception subnet if configured (and essential protocols such as ARP, DHCP, and DNS), until the client's quarantined status is corrected

When a client has corrected its quarantined state, Quarantine Manager updates the MAC address group on the LDAP server to remove the MAC address of the client. QMR will then restore network access to that client the next time QMR checks the LDAP MAC address group.

> **Note:** Configuring QMR and QoS inner VLAN or inner 802.1p policies is mutually exclusive. QMR overlays the inner VLAN tag, thus creating a conflict with related QoS policies. This is also true with QMR and VLAN Stacking services.

Configuring Quarantine Manager

Configuring Quarantine Manager on network devices consists of the following steps:

- Setting Up Quarantine Manager

- Configuring Quarantine Manager
- Assigning Quarantine Manager to Devices.

Setting Up Quarantine Manager

As mentioned earlier, a basic "Quarantine" VLAN is pre-configured on OmniVista. You customize this "basic" Quarantine VLAN using the Configuration Screen. The initial Quarantine Manager setup consists of the following steps:

- Creating the Quarantine MAC Group
- Creating the Quarantine MAC Group Policy

Creating the Quarantine MAC Group

As shown in the Quarantine Configuration List, the pre-configured OmniVista Quarantine VLAN is associated with the "Quarantine" MAC Group. However, this MAC Group is not yet configured. You must go to the Groups application and create the Quarantine MAC Group using the MAC Groups Screen. The name must match the MAC Group name associated with the Quarantine VLAN. ("Quarantined").

> **Note:** If after creating the Quarantined MAC group you modify the name (either using the Groups application, CLI, or WebView), you must also modify the Quarantined MAC group name using the Configuration Screen and poll the switch for the change to take effect.

Creating the Quarantine MAC Group Policy

After creating the Quarantine MAC Group, you must create go to the PolicyView application and create a MAC Group Policy that will deny any traffic originating from the Quarantine MAC Group (PolicyView – Users & Groups - Unified Policies). On the Set Condition Screen of the Create Policy Wizard, create an L2 Source MAC Address Group condition for the "Quarantined" MAC Group; then on the Set Action Screen, set the disposition to "Drop".

Configuring Quarantine Manager

After creating and configuring the Quarantine MAC Group, select the Quarantine VLAN in the Quarantine VLAN List and click on Edit icon and complete the fields as described below to complete the configuration. When you are finished, click on the **Apply** button.

- **VLAN Name -** The Quarantine VLAN name (Default = Quarantined).
- **MAC Group Name -** The Quarantine MAC Group Name (Default - Quarantined).
- **Remediation URL (Optional) -** The URL of the Remediation Server (e.g., http://alaremediation.com). If the Remediation Server is running on a port other than the default port for the browser (e.g., 8080), the port needs to be included in the Remediation URL (e.g., (http://alaremediation.com:9090).
- **Remediation IP (Optional) -** The IP Address of the Remediation Server in the field. You must add the Remediation Server IP address to the Allowed Subnet List.
- **HTTP Proxy Port -** If there is a firewall/proxy configured for the network, enter the HTTP Proxy Port used by the network (e.g., 8080).
- **Default QMR Page -** Enables/Disables the default Quarantine Manager Remediation Web Page. If enabled, the page is automatically presented to the user if a Remediation Server is not configured. **Allow Port Disabling -** Enables/Disables the

Port Disabling feature. You can enable or disable a port rather than a device. By default, this checkbox is disabled. If the checkbox is checked, it means that you want to disable the port when a Quarantine rule is matched. Please note that you must turn on port disabling for each device in addition to turning on global port disabling. Go to the Discovery application, select the device in the Inventory List and click on the Edit icon to bring up the Edit Discovery Manager Entry Screen. In the Advanced Settings Section set "Allow Port Disabling" to "Yes". You can also edit a device by going to the Topology application, selecting the device, and clicking on the "Discovery - Edit Device" to bring up the Edit Discovery Manager Entry Screen. Note that port disabling looks for Locator Live Search information and does not look for historical information.

- **Subnets -** You can create an "Allowed Subnet List". This is a reserved QoS network group that includes the Remediation Server and any subnets to which a quarantined client is allowed access. Click on the Add icon and enter up to three (3) subnets. When you are finished, click on the **Create** button.

  Note: You must add the Remediation Server IP address/subnet mask to the "QMR Allowed Subnets" Group, so that a quarantined client can communicate with the Remediation Server. You can optionally add additional subnets to which quarantined devices will have access.

Assigning Quarantine Manager to Network Devices

After completing the Quarantine Manager configuration, you must assign the configuration to network devices. Select the Quarantined VLAN in the Quarantine Configuration List and click on the **Apply** to Devices button. Select an option from the drop-down menu (Use Switch Picker/Use Topology) to select network devices and click on the **Assign** button.

Creating Quarantine Subnets (Optional)

If a device is banned either by the Network Administrator if Quarantine Manager, the ban is applied to all devices in the network. However, you can segment your network by creating a logical "Quarantine" network. This will limit Quarantine Manager actions to only those switches in the "Quarantine" subnetwork(s). To create "Quarantine" subnet(s) you use the Maps feature in the Topology application to create a Logical network called "Quarantine". You then create Quarantine subnets by creating subnetworks under the Quarantine network.

Configuring Quarantine Manager on OmniAccess WLAN Devices

Quarantine Manager can ban wireless devices connected to an OmniAccess WLAN device by placing them in the OmniAccess "Blacklist". If wireless device(s) is found in a Quarantine Segment, the MAC address of the Quarantined device is placed in the blacklist. Due to limitations in the current OmniAccess device's SNMP implementation, the banned device is placed on the blacklist using SSH to send CLI commands to

OmniAccess. SSH must be able to login to the OmniAccess device. In addition, the OmniAcess device's 'enable' command must be executed and a secondary password is required to entry the privileges commands necessary to perform the blacklist. To enable automatic login, configure a valid user name and password for the OmniAccess device using the Discovery application.

Go to the Discovery application, select the device in the Inventory List and click on the Edit icon to bring up the Edit Discovery Manager Entry Screen. In the General Section enter a CLI/FTP User Name and Password (if necessary) and enter a Secondary CLI/FTP User Name and

Password. You can also edit a device by going to the Topology application, selecting the device, and clicking on the "Discovery - Edit Device" to bring up the Edit Discovery Manager Entry Screen.

Responders

The Quarantine Manager Responders Screen displays all configured Quarantine Manager automatic event responders, and is used to create, edit, and delete event responders. The screen is used to specify the response, such as external emails or scripts to be run (if any) that you want OmniVista to provide when quarantine actions are taken. This provides a method to integrate with trouble-ticket systems. OmniVista can make the following responses to the receipt of a specified event:

- Send an e-mail to any address you specify. You can use variables to specify the information you want to include in the e-mail. Variables exist for information, such as action, reason, Mac Address, etc.
- Execute an external program or script on the OmniVista server.

Creating a Quarantine Manager Responder

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

- **Banned -** Select whether or not you want OmniVista to respond when a device is banned (Respond/Ignore).
- **Released -** Select whether or not you want OmniVista to respond when a device is released from the Banned List (Respond/Ignore).
- **Response Description -** An optional description for the Responder.
- **Response Action -** The response you want OmniVista to take.
- **Send an E-Mail -** If you set the Respond Action to "Send an E-Mail", complete the fields as described below. It is important to note that all fields on the E-Mail Screen in the Preferences application must be complete, or the emails you define will not be sent.

  E-Mail To - The address to which the e-mail will be sent. (The "From" address in the responder emails is determined from the entry in the Use "From" Address field in the E-mail window of the Preferences application.)

  E-Mail Subject - The subject of the e-mail, which will appear in the e-mail Subject Line.

  E-Mail Body - Enter the body of the e-mail in the E-mail Body field by typing in the desired text and/or the desired variables. The variables you can use are explained in the Event Variables section below. You can also accept the default email body, which is the variable $Details$ (explained below).
- **Run an Application on the Server -** If you set the Respond Action to "Run an Application on the Server", complete the fields as described below.

  Command - Enter the command(s).

  Arguments - Enter the arguments to the command specified above, or accept the default argument, which is the variable $MacAddress$ (explained in the Event Variables section below).

  Start Directory - The directory in which the command should be executed.

Standard Input - Enter the standard input for the command, or accept the default standard input, which is the variable $Details$ (explained in the Event Variablessection below).

Event Variables

When sending an e-mail, you can specify the following variables in the E-Mail Body Filed to automatically include the specified information:

- **$Action$** - The action being taken, a ban or a release.
- **$Reason$** - The Reason field from the QM object.
- **$MacAddress$** - The MAC address of the device being banned or release.
- **$IpAddress$** - The IP address of the device being banned or release. If the IP address is unknown it will be displayed as 0.0.0.0
- **$VlanName$** - The name of the VLAN that the device was banned to or released from.
- **$MacGroupName$** - The MAC group that the device was banned to or released from.
- **$Details$** - Contains a message with the Action, Mac, IP address, Vlan, and MacGroupName.

Editing a Quarantine Manager Responder

Select a Responder in the Automatic Event Responders List and click on the Edit icon. Edit the field(s) as described above and click on the **Apply** button.

Deleting a Quarantine Manager Responder

Select a Responder in the Automatic Event Responders List and click on the Delete icon. Click **OK** at the Confirmation prompt.

Automatic Event Responders List

The Automatic Event Responders List provides information on all configured Quarantine Manager Responders.

- **Banned -** The Response OmniVista takes when a device is banned (Respond/Ignore).
- **Released -**The Response OmniVista takes when a device is released from the Banned List (Respond/Ignore).
- **Response Description -** An optional description for the Responder.
- **Response Action -** The response OmniVista takes if the Responder is set to "Respond (Send an EMail/Run an Application).
- **E-Mail To -** The address to which the e-mail is sent, if applicable.
- **E-Mail Subject** - The subject of the e-mail, which will appear in the e-mail Subject Line, if applicable.
- **E-Mail Body -** The body of the e-mail, if applicable.
- **Command -** Application command(s), if applicable.
- **Arguments -** Arguments to the command, if applicable.

- **Start Directory -** The directory in which the command should be executed, if applicable. **Standard Input -** The standard input for the command, if applicable.

TAD Profile

The Quarantine Manager Traffic Anomaly Detection (TAD) Profile Screen displayed all configured TAD Profiles, and is used to create, edit, delete, and assign TAD Profiles. TAD is a network monitoring feature that detects anomalies in the network traffic by monitoring the difference in the rate of ingress and egress packets on a port, matching a specific traffic pattern. TAD monitors these packets at configured intervals, counts the packets matching certain patterns, and applies anomaly detection rules configured by the user when an anomaly exceeds user-defined thresholds (e.g., log the event, send a trap, quarantine a port).

Note: TAD is supported on OS6850, OS6855, OS9700 Switches running AOS 6.4.6.R01.

Creating a TAD Profile

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button. You can create up to 32 monitoring-groups. After creating the group, you then configure the anomaly you want to detect, configure a rule to execute when the anomaly is detected, and assign a port or set of ports to the TAD Group.

- **Group Name -** The name of the TAD Monitoring Group (up to 32 characters)
- **Anomaly Type -** The type of the anomaly to be enabled or disabled.
- **All** (all) - All anomaly types are monitored.
- **ARP Address Scan** (arpaddrscan) - Occurs when a host sends a burst of ARP requests for multiple IP addresses.
- **ARP Flood** (arpflood) - Occurs when a host receives a burst of ARP request packets.
- **ARP Failure** (arpfailure) - Occurs when ARP queries do not elicit ARP responses.
- **ICMP Address Scan** (icmpaddrscan) - Occurs when multiple hosts receive ICMP echo request packets at the same time.
- **ICMP Flood** (icmpflood) - Occurs when a host receives a burst of ICMP echo request packets.
- **ICMP Unreachable** (icmpunreachable) - Occurs when a host receives a flood of ICMP Unreachable packets.
- **TCP Port Scan** (tcpportscan) - Occurs when a host receives a burst of TCP SYN packets for multiple TCP ports.
- **TCP Address Scan** (tcpaddrscan) - Occurs when multiple hosts receive TCP SYN packets at the same time.
- **SYN Flood** (synflood) - Occurs when a host receives a burst of TCP SYN packets on the same TCP port.
- **SYN Failure** (synfailure) - Occurs when a host receives fewer SYNACKs than SYNs it sent out.
- **SYN-ACK Scan** (synackscan) - Occurs when a host receives more SYNACKs than SYNs it sent out.
- **Fin Scan** (finscan) - Occurs when a host receives a burst of FIN packets.

- **Fin-Ack Diff** (finackdiff) - Occurs when a host sees more or fewer FINACK packets than it sent.
- **Rst Count** (rstcount) - Occurs when a host receives a flood of RST packets.
- **Count -** The number of packets that must be seen during the monitoring period to trigger anomaly detection. The valid range is 1 - 100,000. Supported anomalies and the default count for each are listed below:
- **all** - NA
- **arpaddrscan** - 50
- **arpflood** - 90
- **arpfailure** - 6
- **icmpaddrscan** -30
- **icmpflood** -90
- **icmpunreachable** - 20
- **tcpportscan** - 20
- **tcpaddrscan** - 30
- **synflood** - 90
- **synfailure** - 10
- **synackcan** - 2
- **finscan** - 6
- **finackdiff** - 5
- **rstcount** - 50
- **Sensitivity -** Sensitivity of anomaly detection to deviation from the expected traffic pattern. The valid range is 1 - 100. (Default = 50)
- **Period -** The time duration to observe traffic pattern, in seconds. The valid range is 5 to 3,600. (Default = 30)
- **Anomaly State -** Enables/Disabled anomaly detection.
- **Log -** Enables/Disables logging of detected anomalies. If enabled, the anomaly information will be written to a syslog if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)
- **Trap -** Enables/Disables the sending of a trap when an anomaly is detected. If enabled, a trap is sent if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)
- **Quarantine -** Enables/Disables quarantining of the port on which an anomaly is detected. If enabled, a port is quarantined if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)

Assigning a TAD Profile

After configuring the monitoring group, you must assign the ports that you want to monitor to that group. TAD applies the rules to match the specific packets when a port is in a monitoring-group. These rules exist as long as the port is a member of any monitoring-group. Select a TAD Monitoring Group in the Monitoring Group List and click on the **Apply to Devices** button. Configure the fields as described below, then select the device(s) to which you want to assign the profile.

- **Group Name -** Pre-filled with the selected monitoring group.
- **Action -** Select "Assign" (default) from the drop-down menu to assign the profile. You can also remove the selected profile, or assign the selected profile and remove any others assigned to the device(s).
- **Force Port Override** - Enables/Disables port override (On/Off). Select "On" to assign all selected ports to this TAD Group (and remove them from any previously assigned groups, if applicable).
- **Select Devices -** Select an option from the drop-down menu (Use Switch Picker/Use Topology) and click on the **Add/Remove Devices** button to select devices. After selecting devices, click on a device and click on the **Add/Remove Ports** button to select ports. Repeat for additional selected devices.

Click on the **Apply** button to assign the profile to devices/ports.

Editing a TAD Profile

Select a Monitoring Group in the Monitoring Group List and click on the Edit icon. Edit the field(s) as described above and click on the **Apply** button.

Deleting a TAD Profile

Select a Monitoring Group in the Monitoring Group List and click on the Delete icon. Click **OK** at the Confirmation prompt.

Monitoring Group List

The TAD Monitoring Group List provides information on all configured TAD Profiles.

- **Group Name -** The name of the TAD Monitoring Group (up to 32 characters) **Anomaly Type -** The type of the anomaly to be enabled or disabled.
- **Anomaly State -** Administrative state of Anomaly Detection (Enabled/Disabled).
- **Log -** Enables/Disables logging of detected anomalies. If enabled, the anomaly information will be written to a syslog if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)
- **Trap -** Enables/Disables the sending of a trap when an anomaly is detected. If enabled, a trap is sent if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)
- **Quarantine -** Enables/Disables quarantining of the port on which an anomaly is detected. If enabled, a port is quarantined if the anomaly is detected at configured levels (Count/Sensitivity/Period). (Default = Disabled)
- **Count - T**he number of packets that must be seen during the monitoring period to trigger anomaly detection. The valid range is 1 - 100,000.
- **Sensitivity -** Sensitivity of anomaly detection to deviation from the expected traffic pattern. The valid range is 1 - 100. (Default = 50)
- **Period -** The time duration to observe traffic pattern, in seconds. The valid range is 5 to 3,600. (Default = 30)

TAD View

The Quarantine Manager TAD View Screen is used to view TAD configurations and anomaly statistics for specific switches in the network. Select an option from the drop-down menu (Use Switch Picker/Use Topology) and click on the **Select a Device** button to select a device to view. The following information is available.

- Monitoring Groups
- Port Ranges
- Statistics Port
- Statistics Anomaly Traffic
- Statistics Anomaly Summary

Monitoring Groups

The Monitoring Groups Table displays information for TAD Monitoring Groups configured on the selected switch.

- **Group Name -** The name of the TAD Monitoring Group.
- **Anomaly Type -** The type of the anomaly to be enabled or disabled. Supported anomalies are described below.
- **Anomaly State -** Anomaly detection administrative status (Enabled/Disabled).
- **Log -** Anomaly detection logging state (Enabled/Disabled). (Default = Disabled)
- **Trap -** Anomaly detection trap state (Enabled/Disabled). (Default = Disabled)
- **Quarantine -** Anomaly detection quarantine state (Enabled/Disabled). (Default = Disabled) **Count -** Configured Count parameter. This is the number of packets that must be seen during the monitoring period to trigger anomaly detection. The valid range is 1 - 100,000.
- **Sensitivity -** Configured Sensitivity parameter. This is the anomaly detection to deviation from the expected traffic pattern. The valid range is 1 - 100. (Default = 50)
- **Period -** Configured monitoring time period. The time duration to observe traffic pattern, in seconds. The valid range is 5 to 3,600. (Default = 30)

Port Ranges

The Port Ranges Table displays information on ports being monitored by a TAD Monitoring Group.

- **Group Name -** The name of the TAD Monitoring Group.
- **Start Slot/Port -** The first slot/port number in the range of ports being monitored.
- **End Slot/Port -** The last slot/port number in the range of ports being monitored.

Statistics Port

The Statistics Port Table displays anomaly pattern counts on ports belonging to TAD Monitoring Groups.

- **Slot/Port -** The slot/port being monitored.
- **Packet Type -** The type of packet being monitored.

- **Last In -** The number of incoming anomaly packets observed during the last 5 seconds.
- **Last Out -** The number of outgoing anomaly packets observed during the last 5 seconds.
- **Total In -** The total number of incoming anomaly packets observed since monitoring was enabled.
- **Total Out -** The total number of outgoing anomaly packets observed since monitoring was enabled.

Statistics Anomaly Traffic

The Statistics Anomaly Traffic Table displays the anomaly counts on ports belonging to TAD Monitoring Groups.

- **Slot/Port -** The slot/port being monitored.
- **Anomaly -** The type of anomaly.
- **Packet Type -** The type of packet being monitored.
- **Current In -** The number of incoming anomaly packets observed.
- **Current Out -** The number of outgoing anomaly packets observed.
- **Last In -** The number of incoming anomaly packets observed during the last 5 seconds.
- **Last Out -** The number of outgoing anomaly packets observed during the last 5 seconds.

Statistics Anomaly Summary

The Statistics Anomaly Summary Table displays the anomaly check summary.

- **Slot/Port -** The slot/port being monitored.
- **Anomaly -** The type of anomaly.
- **Observed -** The number of times an anomaly was observed on this port since monitoring was enabled.
- **Detected -** The number of times an anomaly was detected on this port since monitoring was enabled (the number of times the anomaly exceeded monitoring limits.

Settings

The Quarantine Manager Settings Screen is used to specify the port number used for SysLog messages. SysLog messages are used by Quarantine Manager to configure network responses. Configure a field(s) as described below and click on the **Apply** button.

SysLog Listener

- **SysLog Port Number:** The port number of the SysLog Listener (Default = 514).

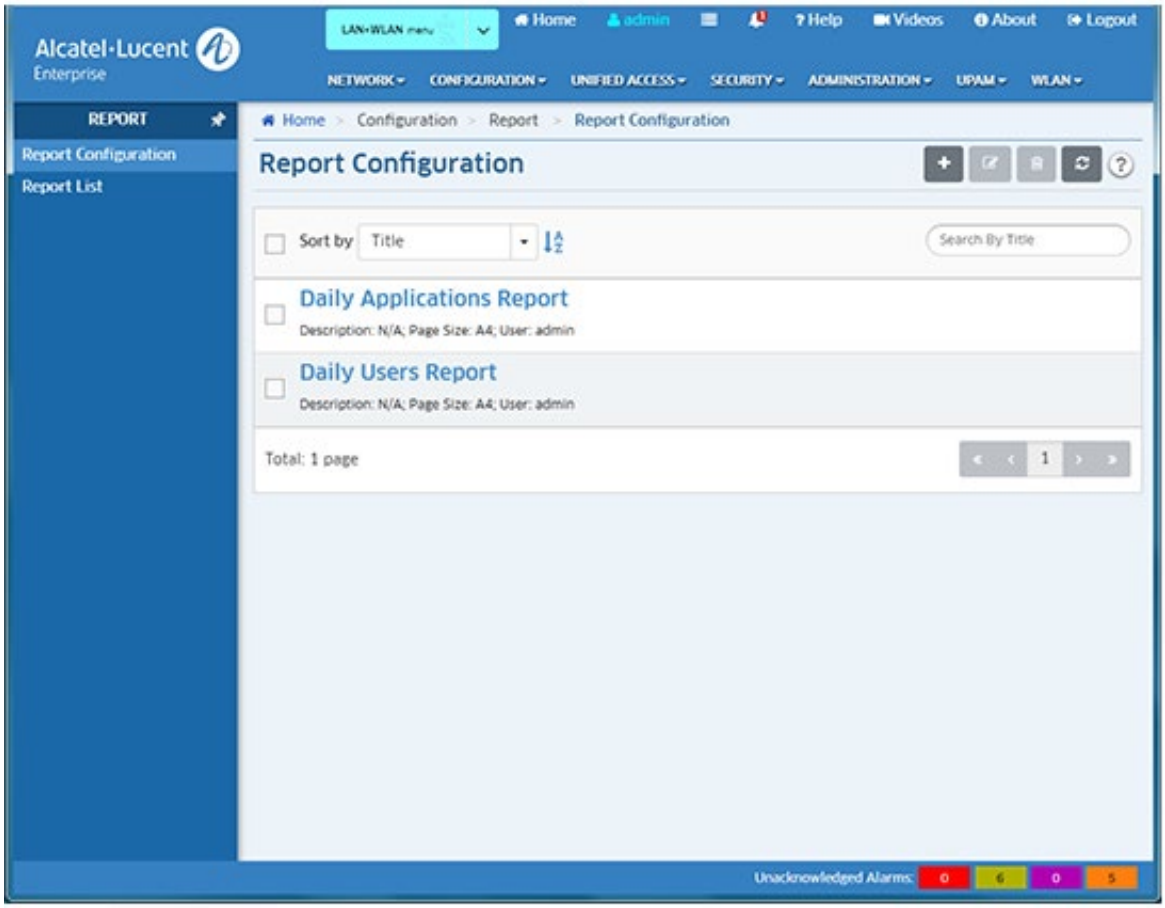
SysLog Generator Target

- **SysLog IP Address**: The IP address of the device that will receive the syslog messages.
- **SysLog Port Number:** The port number on the receiving device that will receive the syslog messages.

26.0 Report

The Report Application enables you to create and schedule reports in certain OmniVista applications (e.g., Discovery, Locator, Analytics). These reports are generated and stored as PDF documents. So, in addition to viewing information in real-time in OmniVista (e.g., Discovery Inventory List, Analytics Utilization Reports), you can generate PDFs of the screens. When a report is generated, it takes a current snapshot of the application information. These reports can be generated immediately, or you can schedule them to be generated at regular times/intervals (e.g., Daily, Weekly). You can also configure a report to be e-mailed when it is generated. The Report Configuration Screen is used to create/configure a report. These generated reports are then displayed on the Report List Screen, where they can be downloaded and viewed as PDFs.

Report



Note: Users authenticated through both local and external RADUIS Servers can generate reports. However, only users authenticated through the Local OmniVista Authentication Server can schedule reports. Users authenticated through an external RADUIS Server can only generate live reports.

Report Configuration

The Report Configuration Screen is used to create, edit, and delete Reports. These reports are PDF versions of tables and reports generated in certain OmniVista applications (e.g., Discovery, Locator, Analytics).

Basically, in addition to viewing information in real-time in OmniVista (e.g., Discovery Inventory List, Analytics Utilization Reports), you can generate PDFs of the screens. When a report is generated, it takes a current snapshot of the application information. These reports can be generated immediately, or you can schedule them to be generated at regular times/intervals (e.g., Daily, Weekly). You can also configure a report to be emailed when it is generated. These generated reports are then displayed on the Report List Screen, where they can be downloaded and viewed as PDFs.

Creating a Report

There are two steps to creating a report. First you must configure the report in the Report Application (report name, schedule, e-mail), then you must go to an application that supports the Report Feature (e.g.,

Discovery, Locator, Analytics), click on the **Add to Report** button at the top of a screen, and link that report to a Report Configuration.

1. Click on the Add icon and complete the fields as described below. After completing the fields, click on the **Create** button.
   - **Report Title -** Enter a title for the report.
   - **Schedule Settings**
   - **Purging Policy -** The report purging frequency. Select an option from the drop-down menu. The report will be removed from the server at the selected interval. Select "None" to never purge the report.
   - **Schedule -** The report creation schedule. Select the "Now" radio button to generate a single report immediately. Select the "Periodically" radio button to create the report at specific times/intervals (an initial report will also immediately be generated). The "Simple" option enables you to schedule the report generation every "x" number of days, hours, minutes, seconds (e.g., every 5 days, every 5 minutes). The "Cron" option enables you to schedule the report generation as a cron job (e.g., every minute, every hour, every year). Note that users authenticated through an external RADUIS Server cannot schedule reports. They can only generate live reports using the "Now" radio button.
   - **E-Mail -** Enter an address to e-mail an attached PDF of a report as configured in the Schedule field above. Each time a report is generated, an attached PDF of the report will be sent to the recipient. You can designate only one (1) e-mail recipient. Note that the E-Mail Preferences (Preferences - System Settings - E-Mail) must be configured for OmniVista to generate report e-mails.
   - **Other Settings -** Click on this button to set optional report print parameters (e.g., page size, orientation). You can also add a description to the report.
2. After creating the report, go a supported application (e.g., Discovery, Locator, Analytics) and click on the **Add to Report** button at the top of the screen. The Add to Report Window will appear with the report/report view displayed in the Widget Name field (e.g., Inventory, Top N Ports Utilization Report Widget). Select the Report you configured in Step 1 from the Report Configuration drop-down list and click **OK**. A report for that screen will now be generated according to that report configuration.

You can generate reports for other applications based on the same report configuration by going to those applications and clicking on the Add to Report button and selecting the report from the Report Configuration drop-down list.

> **Note:** The first time you configure a report (Step 1), a blank report is automatically generated and appears in the Report List. The report is blank because you have not yet associated the report with an application (Step 2). Once you complete Step 2, reports will be generated for that application based on the report configuration.
>
> **Note:** Sending a report email will fail if the email size exceeds the size limit of the email server. For example, Gmail does not allow sending emails larger than 25MB.
>
> **Note:** You can also manually generate a report at any time by selecting the report and clicking on the **Generate Report** button on the Report Details Screen. You can only manually generate a report configured with the Schedule set to "Now". You cannot manually generate a report configured with a "Periodic" schedule.

Editing a Report

Select the report and click on the Edit icon to bring up the Edit Report Configuration Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server. Note that you cannot edit the report title. You can edit the Report Settings, and/or click on the **Other Settings** button to edit the print parameters. You can also remove a report from this Report Configuration by clicking on the "X" next to the field.

Deleting a Report

Select a report and click on the Delete icon, then click **OK** at the confirmation prompt. At the prompt, you have the option of deleting all reports associated with the report configuration. To delete them, select the "Also delete all generated reports" checkbox.

Report List

The Report List Screen displays all generated reports. Reports are displayed with the report creator's user name, report title, the date the report was created, and the version number of the generated report if applicable. For example, if a report was created by the "admin" user titled Daily Users Report", on August 8, 2017, the report file name would be "admin_ Daily Users_Report_20170808.pdf". Subsequent scheduled or manually-generated reports would have a version number added to the end of the filename (e.g., admin_ Daily Users_Report_20170808_1.pdf, admin_ Daily Users_Report_20170808_2.pdf).

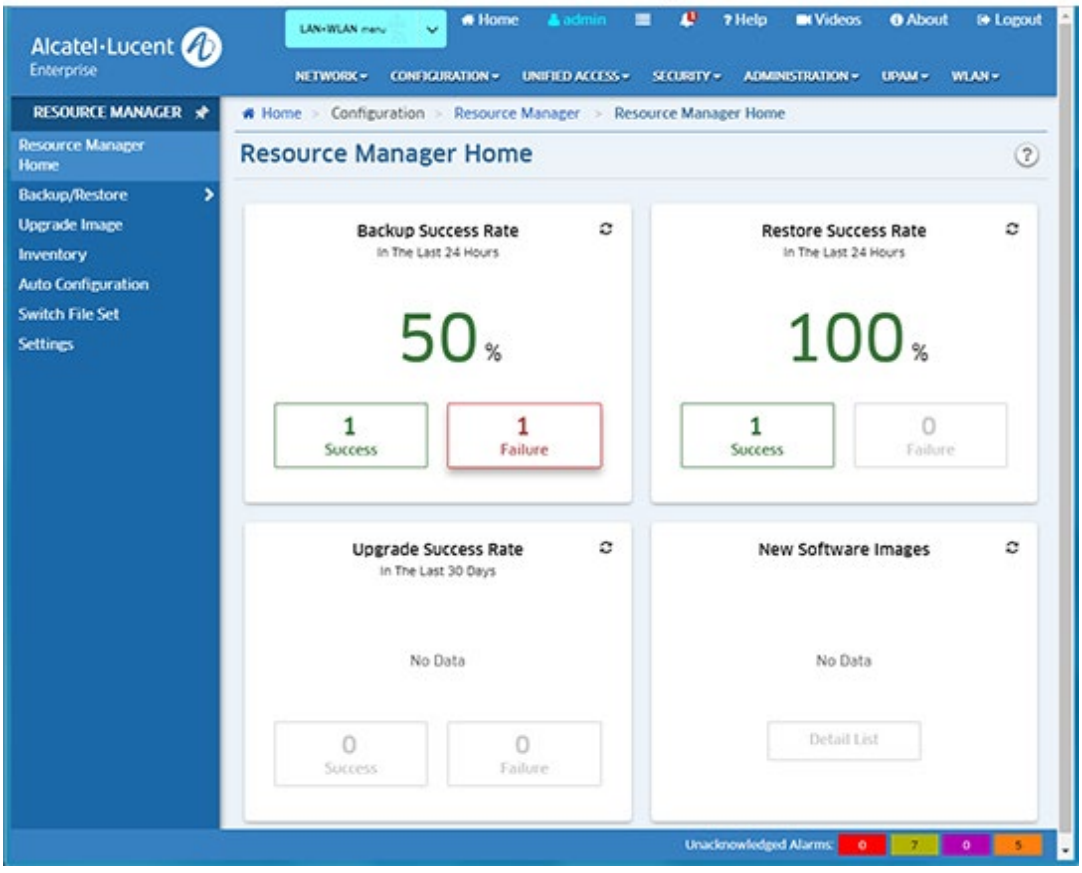
To download/view a report in PDF format, select the report and click on the **Download** button. You can open the report for viewing or save the report. To delete a report(s), select the report(s) and click on the Delete icon, then click **OK** at the confirmation prompt. Note that you can only delete finished reports. You cannot delete a report in the "Generating" state.

27.0 Resource Manager

The Resource Manager application enables you to manage the firmware configuration files on network devices. Click on the applicable link, as described below, to carry out specific operations.

- **Backup/Restore -** Backup the current firmware configuration files in network devices to the OmniVista Server, and restore the configuration files to the devices when desired. You can also compare Configuration Backup Files on the same device or different devices, edit an existing backup and save the changes as a new backup file (AOS Devices), and view a summary of all stored backups.
- **Upgrade Image - I**mport new or upgraded image and firmware files into OmniVista, and install the new files in network devices when desired. (Note that all new image files must be provided by Alcatel-Lucent Enterprise Customer Service.)
- **Inventory -** Run Inventory Reports on network devices that enable you to examine a device's configuration before performing the functions described above.
- **Auto Configuration -** Configure the Automatic Remote Configuration Feature. This feature provides automatic configuration or upgrade of an OmniSwitch without user intervention.
- **Switch File Set -** Assign customized Banner and Captive Portal Web Interface files to devices in the network.
- **Settings -** Used to set the amount of space that must be available on the CMM before an upgrade is allowed.

Resource Manager



Backup/Restore

The Resource Manager Backup/Restore Screen displays a list of all backups that currently exist on the server. The screen is used to backup configuration files for AOS Devices and Stellar APs. It is also used to schedule regular backups, edit a Configuration Backup File (boot.cfg), delete a backup from the OmniVista Server, and export/view backup files. Backups can be used to restore configuration files to the network devices from which they were originally taken. You can also compare Configuration Backup Files on the same device or different devices, and view a summary of all stored backups.

> **Note:** You can backup AOS Devices and Stellar AP Series Devices. OAW Devices cannot be backed up.
>
> **Note:** If you delete a device from OmniVista, any backups for the device are automatically deleted from the Backup/Restore Screen.
>
> **Note:** OmniVista supports the Multiple Working Directories Feature available on OS6900 Switches. When performing Configuration-Only or Full Backup on these devices, only the configuration or image files in the current running directory are backed up instead of the hardcoded “working” directory, in addition to the Certified Directory. The running directory can be any user-specified directory, including the Working Directory.

Performing a Backup

Click on the **Backup** button at the top of the screen to launch the Backup Wizard. Complete the screens as described below to backup one or more network devices. When you have completed all of the screens, click on the **Backup** button at the bottom of the screen to initiate the backup.

Backup Method

Select an option to choose a device selection method:

- **Backup by Devices -** To select specific AOS Devices from a list of discovered devices.
- **Backup by Maps -** To select a map(s) to backup all devices in the map(s). This option is used to backup **all** devices in the selected map(s). You cannot backup selected devices. To backup select devices, select the **Backup By Devices** option. Note that if some devices in a map are not on-line, a dialog box will pop up warning you of the condition. Click **Yes** to continue the backup. Click **Cancel** to cancel the backup. Also note that if a map contains AOS Devices **and** Stellar APs, the Stellar APs will not be backed up. Stellar APs can only be backed up by AP Group.
- **Backup by AP Groups -** To backup Stellar AP Series Devices. Stellar AP Series Devices are backed up by AP Group. All of the APs in the group will be backed up. When the backup is complete, the backup files for each AP will appear in the Backup Files List on the Backup Screen.

Note: If you are backing up more than 50 devices, it is recommended that you use the **Backup by Maps** option instead of creating one backup for each device.

Click on the **Next** button to go to the Device Selection Screen.

Device Selection

The options on this screen will depend on the Backup Method selected above.

- **Backup by Devices -** Select the AOS Device(s) you want to backup and click on the **Next** button to go to the Configuration Screen.
- **Backup by Maps -** Select the map(s) containing the devices you want to back up. Click on the **Next** button to go to the Configuration Screen.
- **Backup by AP Groups -** Select the AP Group(s) you want to backup and click on the **Next** button to go to the Configuration Screen.

Configuration

This screen is used to configure the type of backup performed (e.g., Full, Configuration Only, Images Only) and to schedule regular backups. Backup options (e.g., which directories to include, which files to include) vary according to the backup type. See the applicable section below for details on each backup type.

Full Backup

A Full Backup backs up both configuration files and image files. For AOS Devices, all files in the Certified and Working directories are backed up. This includes all configuration-related files (user credentials, banner, time zone, etc.), and image files. If you are performing a Full Backup, select the directory(ies) to be backed up (Certified or All).

> **Note:** Image files will not be FTPed from a device. OmniVista will only record file version(s). Therefore, before Restore is to proceed, the required image file set must be stored in the Upgrade Image Repository. If the required images are not in the Repository, they will need to be imported using the Upgrade Image Screen in Resource Manager. Also note that if the image file information retrieved from the device does not contain a file version, the file will be physically copied from the device.

Directory

If you are performing a Full Backup, select the directory(ies) to be backed up.

- **Certified -** Back up files in the Certified Directory.
- **All -** Back up files from the Working, Certified, Switch, and Network Directories.

Include Diagnostic and Dump Files (AOS Devices Only)

If you are performing a Full Backup on **all** files, you have the option to include/exclude Diagnostic and Dump Files. By default, Diagnostic and Dump files are not included in the backup. To include these files in the backup, set the **Include Diagnostic and Dump Files** slider to "On".

Description

Enter an optional description for the backup.

Configuration Only Backup

A Configuration Only Backup backs up all configuration-related files in all directories (including user credentials, banner, time zone, etc.). If are performing a Configuration Only backup, you will not have the option of selecting directories since all configuration-related files in all directories are backed up. However, on AOS Devices you will have the option to include/exclude Security Files from the backup for security reasons.

Include Security Files (AOS Devices Only)

If you are performing a Configuration Only backup, you will not have the option of selecting directories since all configuration-related files in all directories are backed up. However, on AOS devices you will have the option to exclude Security Files from the backup for security reasons. By default, Security Files are included in the backup. If you do not want to include Security Files in the backup, set the **Include Security Files** slider to "Off".

Description

Enter an optional description for the backup.

Images Only Backup

An Images Only Backup backs up image files only. Image files will not be FTPed from a device. OmniVista will only record file version(s). Therefore, before Restore is to proceed, the required image file set must be stored in the Upgrade Image Repository. If the required images are not in the Repository, they will need to be imported using the Upgrade Image Screen in Resource Manager. Note that if the image file information retrieved from the device does not contain a file version, the file will be physically copied from the device.

Description

Enter an optional description for the backup.

Schedule Setting

Enable the Schedule Setting option and complete the fields as described below to schedule a single or recurring backup. You can click on the **View Scheduler** button at the top of the Backup/Restore Screen to view a list of Scheduled Jobs, and to edit a user-configured job.

- **Start At -** Select the time when you want to begin the scheduled backup (e.g., 12:00 AM).
- **Recurrence Pattern -** Select the interval for a recurring backup.
- **Daily -** Backup will occur on the schedule day at the configured "Start At" time. By default, the backup will occur every day ("Every 1 Day"). You can customize it by clicking on the "Every 1 Day" field and entering a number (Range = 1 - 30 days). For example, you could configure a Daily Backup to occur every 2 days if you want it to occur every other day.
- **Weekly -** Backup will occur once a week on the selected day at the configured "Start At" time. Select the day of the week on which you want the backup to occur. The backup will occur every week on that day at the configured "Start At" time. You can select more than one day to perform weekly backups on multiple days of the week.

- **Monthly -** Backup will occur monthly on the configured day at the configured "Start At" time. Select the first radio button to schedule the backup for a specific day of the month, and for a specific number of months. By default, the backup will occur on the first day of every month ("Day 1 of every 1 Month"). However, you can customize it. For example, you could schedule the backup for the 15th day every other month ("Day 15 of every 2 Months").
- **Every Weekday** - Backup will occur every weekday at the configured "Start At" time.
- **Range of Recurrence -** Select the start and end date, if applicable, for the scheduled backup.
- **Start Date -** Enter the start date for the scheduled backup. The scheduled backup will begin on that date at the configured "Start At" time.
- **End Date -** Select "End by" to enter an end date for the backup. Select "No end date" to continue the backup indefinitely.

Review

The Review Screen enables you to review your backup configuration before initiating/scheduling the backup. If necessary, click on the **Back** button to make changes to the configuration. When you have verified the backup configuration, click on the **Backup** button to initiate/schedule the backup.

> **Note:** If the CLI/FTP username and password for a device was not previously defined to OmniVista, you will be prompted to enter them before the backup can proceed.

Editing a Configuration Backup File

You can edit the contents of a Configuration Only Backup File (boot.cfg file). This edited file is stored on the OmniVista Server and displayed in the Backup Table Description as "User-Modified Configuration File". Select a Configuration Only Backup file in the Backup Table and click on the Edit icon. In the Select boot.cfg in drop-down menu, select the directory of the file you want to edit (working or certified) and click on the **Get** button. The contents of the file will appear in the File Content area. Edit the file and click on the **Apply** button.

Deleting a Backup

Select the backup(s) you want to delete and click on the Delete icon. Click **OK** at the confirmation prompt.

Exporting/Viewing Backup Files

You can export and view the contents of the files in a backup. Click on a backup in the Backup Table to view the files contained in the backup. Select the file(s) you want to export. Click on the **Export** button at the top of the table, then click on **Save** to save the selected file(s) as a Zip File in your Download folder. To view the contents of a backup file, extract the file(s) and click a file to display the contents.

> **Note:** You cannot export .img files. These files should be downloaded from the ALE Business Portal. If you select a .img file when exporting files, the **Export** button will be de-activated.

Backup Information

The Backup Table displays basic information about backups stored on the OmniVista Server. Click on a backup to view detailed backup file information. By default, information about all backups store on the server is displayed. However, you can use the ""View Criteria" function to customize the display. Click on the "View Criteria" drop-down and select filters as described below. When you have selected all of your filters, click on the **X** in the upper-right corner of the window to close the window and view the filtered display.

- **Filter By**
- **All -** Displays information for all managed devices.
- **Map -** Displays information for devices in the selected map.
- **Device -** Displays information for selected devices.

  By Using Switch Picker - Click on the **EDIT** button to bring up a switch picker to select devices. Click **OK** to return to the Summary View Screen.

  By Using Topology - Click on the **EDIT** button to bring up the Topology application to select devices. Click **OK** to return to the Summary View Screen.

  By Using Quick Select - Click on the **EDIT** button and select a device(s) from the drop-down list.
- **Show Backups -** Select whether you want to view all backups for the selected device(s) or just the latest backup. By default, "Only the Latest One of Each Device" is selected.
- **Time Range -** By default, the "Last One Week" radio button is selected. To view backups from a specific time range, select the "Custom" radio button and configure the time range.

Basic Information

- **Device Name -** The user-configured name of the device.
- **Device Address -** The IP address of the device that was backed up.
- **Device Type -** The device/model type (e.g., OS6860E-24).
- **Date -** The date and time that the backup was initiated.
- **Backup Type -** The type of backup performed. The Backup type can be **Full Backup** (both configuration files and image files were backed up), **Configuration Only** (only configuration files were backed up), or **Image Only** (only image files were backed up).
- **Version -** The software version of the backup files (e.g., 8.4.1.193.R01).
- **Description -** The user-configured description for the backup, if applicable.

Detailed Information

- **Name -** The name of the individual file that was backed up and is currently stored on the OmniVista Server.
- **Directory -** The directory where the file was stored on the device (e.g., /flash/certified).
- **Version -** The firmware version of the file.
- **Description -** Alcatel-Lucent Enterprise provided description of the file.

- **Date -** The date the file was loaded into the device.
- **File Size -** The size of the file, in bytes.
- **File Check Sum -** The backup file checksum value.

Important Facts About Back Ups

The following sections provide important points to keep in mind when performing a backup on any device and Stellar AP Series Devices.

General

When performing a backup, firmware configuration files are FTPed from the device to the OmniVista Server. To gain access to the device, the FTP user name and password must to known to OmniVista. You can specify FTP user names and passwords via the Edit Discovery Manager Entry window. (See the Topology help for further information.) If you did not define FTP Logic names and passwords via the Edit Discovery Manager Entry window, and you attempt to save or restore configuration files, you will be queried for the FTP username and password for each individual device for which files are being saved or restored. If the FTP username and password are not supplied to OmniVista, the FTP process will return errors and the device will not be backed up. The process of backing up other devices will continue. Firmware is automatically copied and restored via FTP, and any errors that can occur when performing these tasks outside of OmniVista are also possible when using OmniVista.

If a backup operation fails in the middle of the backup operation (which could occur if a device goes down between the server and the target device), no files are saved on the server. If the full complement of files is not saved, any initial files that were saved are deleted from the server.

AOS Device backups include the contents of the certified directory and working directory. Only files in the flash memory of the primary MPM module are saved. No files are saved that end with .err , .dmp , /.. , or /. , as these files are either temporary or will cause problems during the FTP process due to conflict with system file names.

> **Important Notes:** The configuration files saved are those in flash memory and are not necessarily the configuration files that the device is currently running. The files are not zipped to save disk space on the OmniVista Server. The user may perform multiple backups on the same day, if so desired.

Users should not attempt to copy configuration files saved on the OmniVista Server to other machines. The saved files contain binary configuration information, including the IP address/MAC address of the source machine, and using these files on another machine could bring the network down.

> **Note:** SFTP will be used when a device is configured in OmniVista to use SSH. If a device is configured to use SSH in OmniVista, SSH must be enabled on the device itself.

Stellar AP Series Devices

Although you cannot perform a restore on a Stellar AP, backup files of Stellar APs can be used to analyze/troubleshoot problems with APs. Stellar AP are configured at the AP Group level, however, some APs in a group may have a different configuration, if for example, a configuration failed on one device in a group. Therefore, the backup file for Stellar APs contains information for each AP in the AP Group. The file can then be used to analyze/troubleshoot problems with APs in the group.

Note: You **can** perform an **image restore** on a Stellar AP. After backing up an AP Group (Image Only or Full Backup), Select a Backup(s) in the Backup List and click on the **Restore** button to bring up the Restore Wizard, then click on the **Restore** button at the bottom of the Wizard. Note that if you click on the Backup(s) to view the files being restored, you will notice that only the image file is selected.

Performing a Restore

You can restore a configuration to the device from a previous backup. Note that you can only restore the configuration to the original device from which the backup was taken. (Backups cannot be restored to other devices, because doing so would cause mismatched IP addresses and other network problems.) Select a Backup(s) in the Backup List and click on the **Restore** button to bring up the Restore Wizard. Complete the screens as described below.

File Selection

The selected Backup(s) are displayed. Click on a Backup to display a list of backup files available for the restore. Select the files you want to restore to the device. Repeat for additional devices. Click **Next**.

AOS 6x Device(s) Only

If the selected device(s) is an AOS 6.x Switch, and you selected files only in the Certified Directory, you have the option of restoring files to the Working Directory or restoring the files to both the Working and Certified Directories. Select the **Restore to Working Directory** or **Restore to Working & Certified Directory** radio button to specify the directory(ies) to which you want the backup restored. If you select files in only the Working Directory or in both the Certified and Working Directories, you will not have this option. The files will be restored to their respective directories. Also note that this option is not available for AOS 7.x or 8.x Switches.

Note: OmniVista supports the Multiple Working Directories Feature available on OS6900 Switches and OS6860 Switches. When performing Configuration-Only or Full Backup on these devices, only the configuration or image files in the current running directory are backed up instead of the hard-coded “working” directory, in addition to the Certified Directory. The running directory can be any user-specified directory, including the Working Directory.

Configuration

For AOS Devices, select the options to be taken if the following changes are detected on the device:

- **Continue to restore when chassis has changed** - Select this option if you want to continue the restore even if it is found that the chassis contents, or the chassis type, has changed since the backup. If you do not enable this checkbox, the restore will not take place if the chassis has changed.
- **Continue to restore when detecting new image files** - Select this option if you want to continue the restore even if it is found that a new image file resides on the

device (i.e., a file that was not previously backed up). If you do not enable this checkbox, the restore will not take place if a new image file is found on the device.

Click on the **Restore** button then click **Yes** at the Confirmation Prompt to initiate the restore. When the restore has successfully completed, click on the **Go to Topology to Reboot Device** link. The Topology application will open with the device(s) highlighted. Click on **Reboot** in the Device Actions area to reboot the device(s) to load the restored configuration into flash memory.

Note: You **must** reboot the device(s) to complete the restore operation.

Compare

The Resource Manager Compare Screen enables you to compare Configuration Backup Files on the same device or different devices using a "Diff" Utility to view any differences between the files on a line for line basis. You can compare files on different devices or compare files on the same device. You can also use the utility to compare text files on the local file system.

Note: The "boot.cfg" file is the target of this utility, however you can use it to compare any text-based files. You cannot use the utility to compare any binary files (e.g., .img, jpg, jar).

Selecting Files

The File Diff Screen is used to select the files you want to compare. To compare backup files from different devices or backups from the same device, select "Backup File" from the **Select From File** drop-down menu on the left side of the screen. Click on the **Browse** button to bring up a list of current backups. Select a backup to bring up a list of files contained in the backup. Select the file you want to compare, and click **OK**. Repeat the steps to select a backup file on the right side of the screen. When you have selected both files, click on the **Compare** button. The file comparison is displayed in the File Diff Window.

Note: To compare text files on the local file system, select "Local" from the from the **Select From File** drop-down menu. Click on the **Browse** button and browse to the files on the local system.

Comparing Files

The File Diff Window displays the files side-by-side with all of the differences highlighted (Changed, Inserted, Deleted). You can use the Arrow keys at the top of the screen on the right side of the window to jump to each change; or you can select a specific change from the **Select to Jump** drop-down menu. You can also use the scroll bars to scroll through the documents and view changes.

Summary View

The Resource Manager Summary View Screen displays a status summary of all backup/restore/upgrade operations saved on the OmniVista Cirrus Server. By default, all Backup/Restore/Upgrade operations are displayed. However, you can use the ""View Criteria" function to customize the display. Click on the "View Criteria" drop-down and select filters as described below. When you have selected all of your filters, click on the **X** in the upper-right corner of the window to close the window and view the filtered display.

- Select Devices
- **All Devices -** Displays information for all managed devices.

- **By Using Switch Picker -** Click on the **EDIT** button to bring up a switch picker to select devices. Click **OK** to return to the Summary View Screen.
- **By Using Topology -** Click on the **EDIT** button to bring up the Topology application to select devices. Click **OK** to return to the Summary View Screen.
- **By Using Quick Select -** Click on the **EDIT** button and select a device(s) from the drop down.
- **Type -** Select the type of operation(s) you want to view (Backup/Restore/Upgrade)
- **Status -** Select the status of the operation(s) you want to view (Success/Fail/All)

At any time, you can return to the default view by clicking on the **Reset** button next to the View Criteria to remove all filters.

Summary View Table

- **Summary Type -** The type of operation (Backup/Restore/Upgrade).
- **Device Address -** The IP address of the device.
- **Last Attempt Date -** The date and time that the operation was initiated.
- **Last Successful Date -** The date and time that the operation completed.
- **Attempt Type -** The type of operation performed (e.g., Full Backup).
- **Last Attempt Status -** The operation status (e.g., Success/Fail).
- **Description -** The user-configured description for the operation, if applicable.
- **Message -** Indicates whether or not the operation was successful (Back up Successfully/Finished Restore Configuration) or failed. If “failed” additional information is provided.

Upgrade Image

The Resource Manager Upgrade Image Screen displays all of the Software and Firmware Files stored in the Upgrade Image Repository on the OmniVista Server. These files are used to upgrade software, firmware, and FPGA files on network devices. Once you download the files from the Customer Support Web Site, you can import the files into the Upgrade Image Repository, and install the upgrade software and firmware on devices on the network. Note that FPGA upgrade is only supported on OS9000, OS6450, and OS6250 Switches running AOS 6.6.4.R01 and later.

> **Note:** OmniVista supports the Multiple Working Directories Feature available on OS10K (AOS Release 7.2.1.R02 and later), OS6900 Switches (AOS Release 7.2.1.R01 and later), and OS6860 Switches (AOS Release 8.1.1.R01 and later). On these devices, the Upgrade operation installs the files to the user-specified directory instead of the hard-coded Working Directory.
>
> **CAUTION:** Never attempt to import or install firmware files or upgrade packages acquired from any source other than Alcatel-Lucent Enterprise Customer Service. Image and Firmware files are specially packaged by Alcatel-Lucent Enterprise Customer Service for important into OmniVista, and contain an LSM file that describes the package contents to OmniVista. Resource Manager will prevent unsupported upgrades. When such an attempt is made, an error message is displayed informing the user that the upgrade has been rejected. This message also displays details of the versions of the switch software required to successfully perform the upgrade.

WARNING: If you are performing an image file upgrade **and** a U-Boot/Miniboot upgrade, you **must complete the image file upgrade before** upgrading the U-Boot and Miniboot files.

Importing the Upgrade Files

All upgrade files supplied by Alcatel-Lucent Enterprise Customer Service are packaged as WinZip executables and have a *.zip file extension. Do not attempt to unzip the firmware files manually. When you Import the WinZip executable, OmniVista automatically unzips the executable as part of the import process. Once the file is imported, the File Set (which contains all of the individual files) appears in the File Sets Table.

Upgrade files are available on the Alcatel-Lucent Enterprise Customer Service website. Download the file to your PC from the website. After downloading the file, click on the **Import** button to locate and import the file to OmniVista.

Note: You can delete a file from the File Sets Table by selecting the file(s), clicking on the Delete icon, then clicking **OK** at the Confirmation Prompt.

Installing the Upgrade Files

Remember, if you are performing an image file upgrade **and** a U-Boot/Miniboot upgrade, you **must complete the image file upgrade before** upgrading the U-Boot and Miniboot files. Select a File Set in the File Sets Table and click on the **Install** button. The Install Upgrade Image Software Wizard guides you through the upgrade process. Each screen in the wizard is detailed below.

Note: The switch FTP timeout default is 5 minutes, so the upgrade will fail if the time to transfer files from OmniVista to a switch is over 5 minutes. It is recommended that you increase the FTP timeout in switches you are upgrading to a higher value to make sure there is enough time to transfer files (CLI command: **session ftp timeout** <*time*>).

Firmware File Selection

All of the files in the File Set that you selected are displayed in the File Detail area. (The name of the imported Zip File is displayed in the File Name field.) Select the file(s) you want to install and click **Next** to go to the Devices Selection Screen.

Note: If you are upgrading Stellar AP Series Devices, Image Files for all AP Models in the AP

Group will be displayed in the File Detail Area. You cannot deselect any files. When you select an AP Group(s) in the next step, OmniVista will automatically apply the correct file to the corresponding AP Model(s) in the group.

Devices Selection

All devices/AP Groups that qualify for installation of the selected Upgrade files are displayed in the Select Devices area. Selection is slightly different depending on whether you are upgrading devices or Stellar AP Series Devices.

- **Device Upgrade -** Click on the Devices **ADD** button and select **Use Picker** or **Use Topology App** to select the devices you want to upgrade. The selected devices will

appear in the List of Selected Devices. If you decide to change devices, click on the **EDIT** button to add/remove devices. When you are done selecting devices, click on the **Next** button to go to the Software Installation Screen.

- **Stellar AP Series Device Upgrade -** To upgrade individual APs, click on the Devices **ADD** button, select **Use Picker** or **Use Topology App** and select the devices you want to upgrade. To upgrade all APs in a Group, click on the AP Groups **ADD** button and select the group(s) you want to upgrade. If you decide to change devices/groups, click on the **EDIT** button to add/remove devices. When you are done selecting groups, click on the **Next** button to go to the Software Installation Screen.

Note: The lowest supported AOS version for OS6855P-14 devices is AOS 6.4.4.9.R01. The lowest supported AOS version for OS6450 devices is AOS 6.6.3.360.R01. The highest supported AOS version for OS6400 devices is AOS 6.4.5.487.R02.

Software Installation

If you are upgrading devices, select the installation options as described below. Note that these options are not available for Stellar AP Series Devices. As noted above to upgrade Stellar AP Series Devices, just click on the **Install Software** button.

Installation Options

- **Upgrade BMF Files -** Upgrade the BootROM, MiniBoot, or FPGA files (AOS switches only).
- **Upgrade Images Files -** Upgrade the image files on the switch(es) (Default) .
- **U-Boot Upgrade on all NIs -** Perform u-boot upgrade for all the NIs on the switch(es) (9000 series switches only).
- **In-Service Software Upgrade (ISSU) -** Upgrade the image files on redundant CMMs with minimal data interruption. This option is available (and displayed) for OS10K and OS6900 (7.3.1.R01 and later) and OS6860 (8.1.1.R01 and later). ISSU support for the OS10K is for both standalone and virtual chassis; ISSU support for the OS6900 and OS6860 is for Virtual Chassis configuration only.
- **Directory -** The Directory field is enabled when the Upgrade Image Files checkbox is selected and the images are for devices supporting the Multiple Working Directories Feature - OS10K (7.1.1.R01 and later), OS6900 (7.2.1.R01 and later) OS6860 - 8.1.1.R01 and later). The directory path must be either an absolute path (e.g. /flash/myimagedir) or a relative path to the flash (“/flash/” will be prefixed in this case). Validations will be done to ensure the directory path is valid before the images are sent to the switches. Note that if the user-specified directory does not exist on the switch, it is automatically created. Once the images are uploaded to the switch, if the user-specified directory does not contain any boot.cfg file, it is copied from the current running directory of the switch.

Note: The ISSU upgrade procedure for upgrading AOS from 8.1.1.xxx to 8.2.1.304.R01 on OS6860 and OS6860E Switches is different than the regular ISSU upgrade procedure. OmniVista does not support this ISSU upgrade path, please refer to APPENDIX C of the 8.2.1.304.R01 Release Notes for detailed instructions on the upgrade procedure.

6200 Devices Options

- **6200 Series Installation Options** (6200 Devices Only). If you are upgrading a stack of devices, the following options will be enabled.
- **Upgrade Master Unit Only** - Upgrade the image files on the master switch in the stack.
- **Upgrade All NIs in Stack** - Upgrade the image files on all switches in a stack.

When you have configured all of the applicable installation options, click on the **Install Software** button to initiate the upgrade process. When the install has successfully completed, click on the **Go to Topology to Reboot Device** link at the top of the screen. The Topology application will open with the device(s) highlighted. Click on **Reboot** in the Device Operations area to reboot the device(s) to load the restored configuration into flash memory.

> **Note:** You **must** reboot the device(s) to complete the upgrade. Remember that image files are installed into the working directory of AOS devices. After the installation completes, you should reboot AOS devices. You may also want to save the working directory to the certified directory.

ISSU Upgrade

The In-Service Software Upgrade (ISSU) feature is used to upgrade the CMM images running on supported devices with minimal disruption to data traffic. The CMM images can be upgraded only on fully synchronized, certified, and redundant systems. A minimum of size of mandatory images + 3MB flash space must be present in the device to accommodate the image files that are used to upgrade existing image files. The ISSU upgrade process is the same as the upgrade process detailed above. However, you cannot select individual files from the File Set. All of the files will be installed. You cannot select individual files in the File Details area. The following CMM images are ISSU capable.

Prior to FTPing the images to switches, Resource Manager performs the following checks to make sure the selected device is ready for ISSU:

- Ensures the device is redundant, fully certified, and synchronized.
- Ensures that sufficient flash space is available on the primary CMM (a minimum of size of mandatory images + 3MB flash file system space is required for the upgrade).

> **Note:** Although Resource Manager will make certain that the switch is ISSU capable, it will not perform any check whether selected ISSU images are compatible with the particular software version running on the switch. This information will be provided to customers by Customer Support when a new ISSU package is released.

If any of these checks fail for a device, Resource Manager logs the error message, and continues with the next device. Otherwise, Resource Manage checks for the existence of the /flash/issu directory on the primary CMM, and creates the directory if it is not present. If the directory already exists and is not empty, Resource Manager removes all files in the directory before replacing them with the new images.

When Resource Manager finishes issuing the ISSU command to the selected devices, the user is asked to perform "Copy Working to Certified" for each device. Make sure you also perform: "Flash-Synchro" for each device.

ISSU Upgrade Paths

AOS Release 7

	Upgrading From 7.3.4.R02 GA or 7.3.4.R02 Maintenance Release	Upgrading from any other 7.X Release
OS6900 - VC	ISSU - Supported Standard Upgrade - Supported	ISSU - Not Supported Standard Upgrade - Supported
OS6900 - Standalone	ISSU - N/A Standard Upgrade - Supported	ISSU - N/A Standard Upgrade - Supported
OS10K - VC	ISSU - Supported Standard Upgrade - Supported	ISSU - Not Supported Standard Upgrade - Supported
OS10K - Standalone (Dual-CMM)	ISSU - Supported Standard Upgrade - Supported	ISSU - Not Supported Standard Upgrade - Supported
OS10K - Standalone (Single-CMM)	ISSU - N/A Standard Upgrade - Supported	ISSU - N/A Standard Upgrade - Supported

AOS Release 8

	Upgrading From 8.2.1.R01 GA or 8.2.1.R01 Maintenance Release	Upgrading from any other 8.X
OS6860-VC	ISSU - Supported Standard Upgrade - Supported	ISSU - Not Supported Standard Upgrade - Supported
OS6860-Standalone	ISSU - N/A Standard Upgrade - Supported	ISSU - N/A Standard Upgrade - Supported

Important Information About Upgrades

If FTP User Names/Passwords are Undefined

If the FTP user names and passwords for the devices were not previously defined to OmniVista, the FTP User Name Password window displays. To supply the FTP user name and password for a device, select the device in the FTP User Name Password window and click the **Edit** button. Enter the FTP user name and password for the selected device in the appropriate fields. If the user name and password you enter also apply to the other devices, click the **Same for all Unspecified** checkbox. Then click the **OK** button.

If necessary, continue to enter FTP user names and passwords until they have been specified for all devices listed. When all user names and passwords have been specified, click Yes at the installation confirmation prompt to initiate the installation process.

If Version Numbers are Older

If the image files being installed have an older version number (or the same version number) than the image files currently resident on a device, a warning message will appear. Note that installing older versions of image files may result in a loss of functionality or, in the case of OmniStack devices, the resetting of device parameters. Click **Yes** if you wish to perform the installation anyway. Click **No** to cancel the installation.

File Sets Information

The individual upgrade files are contained in File Sets for each device type. The File Sets Table displays all of the File Sets stored in the Upgrade Image Repository on the OmniVista Server. The table displays basic information. Click on a file set to display detailed information for the files contained in the File Set.

Basic Information

- **Type -** The upgrade file set device type (e.g., Omniswitch6860).
- **Date -** The date the file set was imported into OmniVista.
- **Version -** The firmware version of the file set (e.g., 8.2.1.304.R01).
- **Description -** The file set description (e.g., AOS 8.2.1.304.R01).

Detailed Information

- **File Name -** The name of the file (e.g., Uos.img).
- **Version -** The firmware version of the file set (e.g., 8.2.1.304.R01).
- **Description -** The file description (e.g., Alcatel-Lucent OS).
- **Date -** The date the file was created.
- **File Size -** The file size, in bytes.
- **File Check Sum -** The upgrade file checksum value.

Inventory

The Resource Manager Inventory Screen is used to create Inventory Reports for AOS switches that enable you to examine a switch's configuration. A Switch Inventory Report includes system information, detailed module information, chassis data, and health information for an individual switch. You can request an Inventory Report for a single switch or for multiple switches simultaneously.

Note: Inventory Reports can only be created for AOS Switches.

Creating an Inventory Report

Select the switches and type of report you want to generate, then click on the **Create** button.

- **Select Device(s) -** Use the Switch Picker or Topology option to select the switch(es) for which you want to create the report. You can select up to 100 switches at a time.
- **Report Type -** Select the type of report you want to generate:
- **Condensed Content -** Generates a smaller, condensed report that is displayed when it is generated.

- **Detailed Content -** Generates a larger, detailed report. Select the information you want to include in the report (e.g., System Information, Chassis Information). This report is not immediately displayed. The report is generated as an HTML file and a link is displayed to access the report. Click on the link in the Detailed Inventory Report area at the bottom of the screen to display the report.

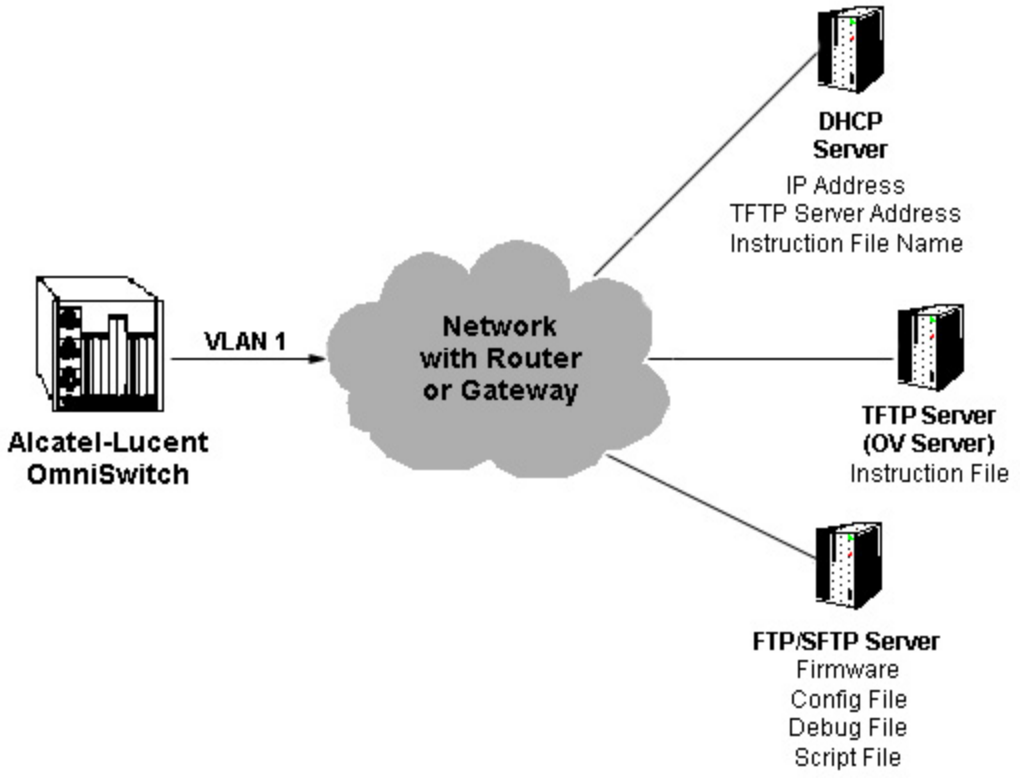
Auto Configuration

The Resource Manager Auto Configuration Screen is used to configure the Automatic Remote Configuration Feature. This feature provides automatic configuration or upgrade of an OmniSwitch without user intervention by pushing an Instruction File to the device. The Instruction File contains all of the information required to automatically locate and download all of the necessary files to configure a new device/upgrade an existing device on the network. When a device is initially deployed in a network, the Instruction File is sent to the device to download the applicable Image, Configuration, Debug, and Script Files from remote servers to bring the device online in the network. The Auto Configuration Screen displays all configured Instruction Files. It is also used to create, edit, and delete Instruction Files.

Auto Configuration Overview

The Auto Configuration Feature automatically configures a new switch and brings it online in the network. In addition, the feature can be used to automatically upgrade a switch with new Firmware, Configuration. And Debug files. As shown below, the Auto Configuration Feature requires a Default DHCP Server, a TFTP Server (the OmniVista Server) that contains the Instruction File, and a remote FTP/SFTP Server that contains the Firmware, Configuration, Debug, and Script Files.

- **DHCP Server -** Provides the switch with an IP address as well as the location of the TFTP Server and the name of the Instruction File. The switch must have at least one port with connectivity to the DHCP Server through Default VLAN 1.
- **TFTP Server -** Resides on the OmniVista Server and contains the Instruction File, which contains the file names and locations of the Firmware, Configuration, Debug, and Script Files stored on the FTP/SFTP Server. The OmniVista 2500 TFTP Server Code Library transfer limit file size is 4GB, per RFC 2347.
- **FTP/SFTP Server -** Contains the Firmware, Configuration, Debug, and Script files.



Auto Configuration on a New Switch

New OmniSwitches are shipped without a boot.cfg file. When the new switch is connected to the network as a new device with no boot.cfg file in the working directory, the Automatic Remote Configuration process is initiated. First, a DHCP client is automatically created on VLAN 1 on the switch and the switch obtains an IP address as well as the address of the TFTP Server and the name of the Instruction File. The switch then downloads the Instruction File. The Instruction File contains the file names and locations of the Firmware, Configuration, Debug, and Script Files which are then downloaded from the FTP/SFTP Server and saved as the boot.cfg file in the /flash/working directory. The DHCP Client on VLAN 1 is removed and the Script File is launched to configure the switch and the switch is automatically rebooted to load the image files from the /flash/working directory.

> **Note:** You must create an Instruction File for each switch model on your network. When the switch sends its initial request to the DHCP Server, the model name (e.g., 6850, 9000) is included in the Vendor Class Identifier Field (Option 60 Field). The DHCP Server will then return the Instruction File corresponding to the model listed in the field.

Automatic Configuration Updates

In addition to automatically configuring new switches on the network, the Auto Configuration Feature can be used to automatically update existing network switches upon reboot. To enable a switch to be automatically configured with the latest image files and configuration files on reboot, remove the boot.cfg file from the /flash/working directory. When the switch reboots and the network detects that there is no boot.cfg file, the Automatic Remote Configuration process is initiated. The Automatic Configuration software compares the current firmware version on the

switch with the version stored on the FTP/SFTP Server. If the version on the switch is older than the version on the FTP/SFTP Server, the Automatic Configuration process is launched, as described above.

Automatic Configuration Files

The files downloaded during the Automatic Configuration Process are detailed below.

- **Instruction File -** The initial file required for the automatic remote configuration process to occur. The file contains the names and location of the Firmware, Configuration, Debug and Script files, which are stored on a remote FTP/SFTP Server.
- **Firmware Files -** Image files that are used to initially configure or upgrade a switch. The firmware files, which differ for different OmniSwitch platforms, contain the executable code, which provides support for the system, Ethernet ports, and network functions.
- **Configuration File -** Bootup configuration information for the switch (network configuration parameters).
- **Debug Configuration File -** Default debug configuration.
- **Script File -** This file contains the commands to be performed on the switch so that appropriate actions can be taken on the downloaded files (Firmware, configuration and Debug Files). The Script File can be created using CLI commands, which are performed in the order in which they appear in the script. A Script File example is shown below:

```
reload working no rollback-timeout
copy working certified flash-synchro
```

Note: If a 'write memory' command is used in the script file, it overwrites the boot.cfg file. The

Script File should not contain the write memory command if it is downloaded along with the configuration file. For more information on configuring the Script File, See the "Managing Automatic Remote Configuration" chapter in the *Network Configuration Guide*.

Quick Steps for Automatic Remote Configuration

The steps below give a quick overview of configuring a switch for Auto Configuration. Follow the steps below to configure Automatic Remote Configuration for you network. Detailed instructions, including Script File Syntax and examples can be found in the "Managing Automatic Remote Configuration Download" chapter of the *Switch Management Guide*.

Note: The switch must have at least one port with connectivity to the DHCP Server through default VLAN 1.

1. Configure the default network DHCP Server with the TFTP Server address (Option 66) and Instruction File name (Option 67). For example:
   - **Option 66:** 128.251.17.224 (TFTP Server address. This is the OmniVista Server address)

- **Option 67:** os6855/instruction1.alu (Directory and Name of the Instruction File on the OmniVista Server).

Note: For details on how to configure the DHCP server, see the "Configuring DHCP Server" chapter in the *Network Configuration Guide*.

2. Configure a Script file. See the "Managing Automatic Remote Configuration Download Chapter" in the *Network Configuration Guide*.
3. Store the Firmware, Configuration, Debug and Script Files on the FTP/SFTP Server.
4. Create the Instruction File.

Creating an Instruction File

The Instruction File contains all of the information needed by a device to locate and download the applicable Image, Configuration, Debug, and Script Files from remote servers. The Firmware, Configuration, Debug and Script files, differ for different OmniSwitch platforms. You must create an Instruction file for each switch model on your network (e.g., 9000, 6850, 6855) . When a new switch comes online, the switch type is sent to the DHCP Server using Option 60 to select the Instruction File for that device type. To create an Instruction File, click on the Add icon and complete the Instruction Fields as described below.

Header/File Servers

- **Instruction File Path -** The Instruction File directory path. Enter the directory of the Instruction File on the OmniVista Server (e.g., os6855). Make sure you have configured Option 67 on the DHCP Server for the corresponding Instruction File (e.g., os6855/instruction1.alu).
- **Instruction File Name -** The Instruction File name. You can create multiple Instruction Files (e.g., Instruction Files for different models - 9000, 6850, 6855). When a new switch comes online, the switch model is sent to the DHCP Server using in the Vendor Class Identifier Field. The DHCP Server will then return the TFTP Server Address and Instruction File path for the corresponding Instruction File based on the information configured in the Option 66 Field. You must use the ".alu" extension for any Instruction Files you create (e.g., instruction1.alu).
- **Instruction File Header -** User-configured header for the Instruction File. This may contain any user information such as switch ID, file version, etc.
- **Primary File Server**
- **Primary Server IP Address -** The IP address of the Primary FTP/SFTP Server.
- **Primary Server Protocol -** The protocol used to communicate with the Primary Server (FTP, SFTP).
- **Primary Server User -** The user name of the primary user (e.g., admin).
- Secondary File Server (Optional)
- **Secondary Server IP Address -** The IP address of the Secondary FTP/SFTP Server. If OmniVista is unable to connect to the Primary Server after three (3) retries, OmniVista logs the error and connects to the Secondary File Server. A Secondary Server is not required. If you do not want to add a Secondary Server, make sure all of the Secondary Server fields are empty. The IP Address and User Fields must be empty and the Protocol Field must be set to "None".

- **Secondary Server Protocol -** The protocol used to communicate with the Secondary Server, if applicable (e.g., FTP). If a Secondary Server is not configured, this field must be set to "None".
- **Secondary Server User -** The user name of the secondary user (e.g., admin). If a Secondary Server is not configured, this field must be empty.

Software and Config Files

The only required fields in this section are the Firmware Version and Firmware Location fields. The remaining fields are not required and the fields can be left empty.

- **Firmware Version -** The version of the firmware to be downloaded from the FTP/SFTP Server (e.g., OS_6_4_6_101_R01). You must use the format shown in the example.
- **Firmware Location -** The directory location of the firmware on the FTP/SFTP Server (e.g., /ftproot/firmware).
- **Config File Name -** The name of the Configuration File (e.g., boot.cfg).
- **Config Location -** The location of the Configuration File on the FTP/SFTP Server (e.g., /ftproot/config).
- **Debug File Name -** The name of the Debug File on the FTP/SFTP Server (e.g., AlcatelDebug.cfg).
- **Debug Location -** The location of the Debug File on the on the FTP/SFTP Server (e.g., /ftproot/debug). **Script File Name -** The name of the Script File on the FTP/SFTP Server (e.g., OS6850_script.txt). If a script file is not specified in the Instruction File, or if it is not properly downloaded, the Automatic Remote Configuration Manager software automatically initiates a "reload working no rollback-timeout" command after firmware or bootup configuration files are downloaded.
- **Script File Location -** The location of the Script File on the FTP/SFTP Server, if applicable (e.g., /ftproot/script).
- **License File Name -** The name of the License File on the FTP/SFTP Server.
- **License File Location -** The location of the Script File on the FTP/SFTP Server, if applicable (e.g., /ftproot/ license).

Note: Since many of the fields for different Instruction Files will be the same (e.g., File Server Address, Firmware Location), a shortcut to creating additional Instruction Files is to select an existing file in the Instruction File List, click on the Add icon, and change only the fields that are different for the new file (e.g., Instruction File Path, Instruction File Name).

Editing an Instruction File

Select the file in the Instruction Files List and click on the Edit icon. Edit the necessary fields as described above, click on the **Apply** button, then click **OK** at the confirmation prompt to update the Instruction File on the TFTP Server.

Deleting an Instruction File

Select the file(s) in the Instruction Files List, click on the Delete icon, then click **OK** at the confirmation prompt.

The Instruction Files List

The Instruction Files List displays information about all Instruction Files stored on the OmniVista Server.

- **Instruction File Path -** The Instruction File directory path. The Instruction File is stored on the OmniVista Server (e.g., os6855).
- **Instruction File Name -** The Instruction File name. You can create multiple Instruction Files (e.g., Instruction Files for different models - 9000, 6850, 6855).
- **Instruction File Header -** User-configured header for the Instruction File. This may contain any user information such as switch ID, file version, etc.
- **Primary Server IP Address -** The IP address of the Primary FTP/SFTP Server.
- **Primary Server Protocol -** The protocol used to communicate with the Primary Server (FTP, SFTP).
- **Primary Server User -** The user name of the primary user (e.g., admin).
- **Secondary Server IP Address -** The IP address of the Secondary FTP/SFTP Server. If OmniVista is unable to connect to the Primary Server after three (3) retries, OmniVista logs the error and connects to the Secondary File Server. A Secondary Server is not required.
- **Secondary Server Protocol -** The protocol used to communicate with the Secondary Server, if applicable (e.g., FTP).
- **Secondary Server User -** The user name of the secondary user (e.g., admin).
- **Firmware Version -** The version of the firmware to be downloaded from the FTP/SFTP Server (e.g., OS_6_4_6_101_R01).
- **Firmware Location -** The directory location of the firmware on the FTP/SFTP Server (e.g., /ftproot/firmware).
- **Config File Name -** The name of the Configuration File (e.g., boot.cfg).
- **Config Location -** The location of the Configuration File on the FTP/SFTP Server (e.g., /ftproot/config).
- **Debug File Name -** The name of the Debug File on the FTP/SFTP Server (e.g., AlcatelDebug.cfg).
- **Debug Location -** The location of the Debug File on the on the FTP/SFTP Server (e.g., /ftproot/debug). **Script File Name -** The name of the Script File on the FTP/SFTP Server (e.g., OS6850_script.txt). If a script file is not specified in the Instruction File, or if it is not properly downloaded, the Automatic Remote Configuration Manager software automatically initiates a "reload working no rollback-timeout" command after firmware or bootup configuration files are downloaded.
- **Script File Location -** The location of the Script File on the FTP/SFTP Server, if applicable (e.g., /ftproot/script).
- **License File Name -** The name of the License File on the FTP/SFTP Server.
- **License File Location -** The location of the Script File on the FTP/SFTP Server, if applicable (e.g., /ftproot/ license).

Switch File Set

The Resource Manager Switch File Set Screen is used to create a command prompt Login Banner and/or Captive Portal Web Page file and assign the file to devices on the network. A Banner file is a .txt file that is displayed when a user first logs into a network device using the command line interface. Banner files can be customized to display a unique command line banner for all devices on the network. Captive Portal, a web-based user authentication option within the Access Guardian application. A Captive Portal file is an HTML file that is presented to the user with a web page for authentication. A Switch File Set contains Banner or Captive Portal files that can be assigned to network devices to be presented to users when they login to a device. The Switch File Set Screen displays all configured Switch File Sets and is used to create, edit, delete, and assign Switch File Sets.

> **Note:** Before assigning Banner or Captive Portal files to all devices in the network, it is recommended that you customize the file(s) and send the file(s) to a single switch on the network for verification. When you are satisfied with the customized file(s), you can then push the files to the network. Any subsequent changes to the files can be made on that same switch, and the new files imported and pushed to the network.

Overview

Below is a list of Banner and Captive Portal file names. These files are stored in OmniVista and will be the Banner and Captive Portal Web files (e.g., Login Page, Help Pages) that you will customize for your network. The files you create must use these file names. For example, if you create a Captive Portal Login Page, the file must be named *cpLoginWelcome.inc*. Once you have created all of the necessary files and verified them on a network device, you can then import those files from that device and "push" them other devices on the network. The file names and their use are described below.

- **banner.txt -** A Banner file is a .txt files that is displayed when a user first logs into a network device using the command line interface.
- **background.gif/.jpg/.png -** Use this file to provide a page background image that Captive Portal will display on all pages.
- **cpLoginHelp.html -** Use this file to customize the Captive Portal login help page. A question-mark ("?") button links to this HTML help page, which is displayed in a separate browser window
- **cpLoginWelcome/cpStatusWelcome/ cpFailWelcome/cpBypassWelcome.inc -** Use these files to customize the welcome message for the Captive Portal login, successful status, fail status, and bypass status page. **cpPolicy.html -** The User Acceptable Policy HTML file that is linked to the Captive Portal login page.
- The link provided opens a new browser window to display the policy information.
- **logo.gif/.jpg/.png -** Use these files to provide a company logo that Captive Portal will display on all pages.

Note: Create custom logo and background pages using the .gif, .jpg, or .png formats. Captive Portal checks the flash/switch directory on the switch for a .gif file, then a .jpg file, and finally a .png file. Whichever file type Captive Portal encounters first is the file used to display the custom logo or background.

The .inc files, which are used to present customized welcome messages, are partial HTML files that can include only text or text and other HTML tags, such as links. Note that these .inc files are wrapped in a paragraph HTML tag within the body of a Captive Portal default page.

Banner Files

A Banner file is a .txt file that is displayed when a user first logs into a network device using the command line interface (e.g., a company name, device name). You must first create the file, then assign ("push") the file to devices on the network.

Captive Portal Files

Captive Portal is a configurable option within the Access Guardian application that allows web-based clients to authenticate through switch using 802.1x or MAC authentication via a RADIUS Server. When the Captive Portal option is invoked, a Web page is presented to the user device to prompt the user to enter login credentials.

Creating a Switch File Set

A Switch File Set contains Banner or Captive Portal files that can be assigned to network devices to be presented to users when they login to a device. To create a Switch File Set, click on the Add icon to bring up the Create Switch File Set window. Enter a **File Set Name** and **File Set Description** and select the **File Set Type** from the drop-down menu (Captive Portal/Banner). All of the default files for that File Set Type are displayed in the Files Table. Select the file(s) you want to include in the Switch File Set and click on the **Create** button.

You can add custom files to the Switch File Set by adding files from your PC or importing the files from a network device. To add files from your PC, click on the **Add File** button, locate the file(s), and click **OK**. To import files from a network device, click on the **Import** button, select the switch from which you want to import the files, and click on the **Import** button. The files you add or import will appear in the Files Table. You can then select that file (or files) and add them to the Switch File Set. Remember, the files you add must have the same file name (e.g., banner.txt).

Once you have created the Switch File Set, you must assign it to device(s) on the network.

Assigning a Switch File Set

Select the Switch File Set that you want to assign from the Switch File Set Table and click on the **Assign** button. Select the device(s) to which you want to assign the Switch File Set, click the **Apply** button, then click **OK**.

> **Note:** Before assigning Banner or Captive Portal files to all devices in the network, it is recommended that you customize the file(s) and send the file(s) to a single switch on the network for verification. When you are satisfied with the customized file(s), you can then push the files to the network. Any subsequent changes to the files can be made on that same switch, and the new files imported and pushed to the network.

Editing a Switch File Set

Select the Switch File Set that you want to edit and click on the Edit icon. You can edit the **File Set Description** and **File Set Type**. When you are done editing, click on the **Apply** button. You can then assign the File Set to network devices.

Deleting a Switch File Set

Select the Switch File Set(s) that you want to delete and click on the Delete icon. Click **OK** at the confirmation prompt.

Settings

The Resource Manager Settings Screen is used to set the backup retention policy and the amount of space that must be available on the CMM before an upgrade is allowed.

Backup Retention Policy

These settings are used to specification of a maximum number of days and a minimum number of backups to keep per switch.

- **Minimum Backups -** The minimum number of backups you want to retain per switch. (Range = 1 365, Default = 365)
- **Maximum Days -** The maximum number of days that you want to retain those backups. (Range = 1 365, Default = 365)

If a backup for a switch is older than the maximum number of days, and the total number of backups is at least the minimum number specified, older backups will be deleted in accordance with the retention policy. The backup retention policy is applied when a new backup is successfully created.

For example, Let ‘b’ denote the minimum number of backups to retain, ‘d’ the retention period in days, and ‘n’ the number of backups that are less than ‘d’ days old. For each device, the larger of the two numbers, ‘b’ and ‘n’, shall be retained. If 'b' = 3 and 'd' = 60 days:

- Switch 1: There are 6 backups, 4 of them are more than 60 days old, 2 other builds are less than 60 days old: => 3 backups will be retained.
- Switch 2: There are 6 backups, 1 of them is more than 60 days old, 5 other builds are less than 60 days old: => 5 backups will be retained.

BMF Upgrade Settings

- **Minimum Space -** The amount of space that must be available on the CMM before an upgrade is allowed. (Default = 4.5 MB)

28.0 SAA

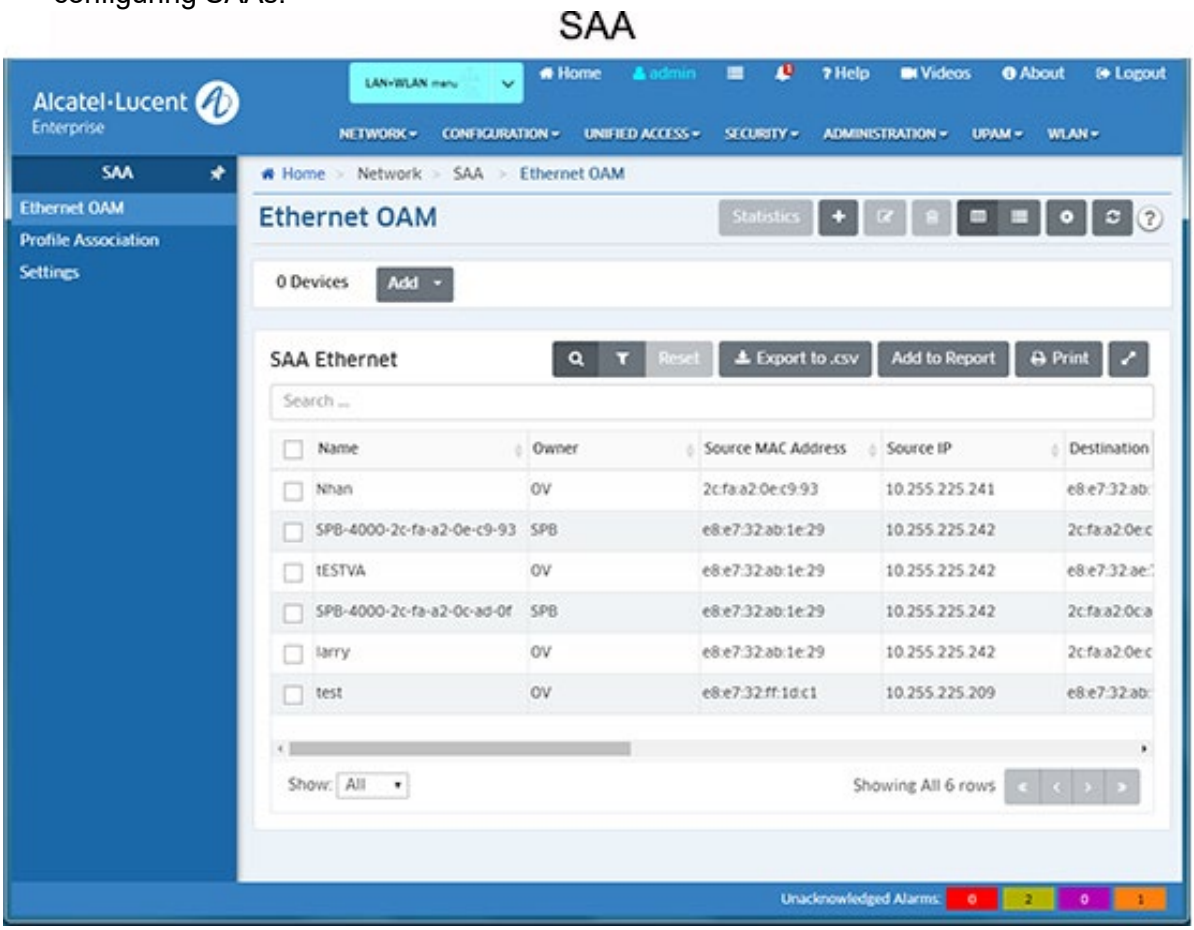
Service Assurance Agent (SAA) enables customers to assure business-critical applications, as well as services that utilize data, voice, and video. Ethernet Operations, Administration, and Maintenance (OAM) provides service assurance over a converged network that service providers required in an Ethernet network.

End-to-end monitoring of path Round-Trip-Times (RTT) and Delay Variation (jitter) between switch pairs and Virtual Machine (VM) pairs is provided by configuring Service Assurance Agents (SAA) between the endpoint switches. The OmniVista Ethernet OAM feature enables the user to easily configure SAAs between switch pairs and VM pairs on the network. Performance metrics monitored by these SAAs include: Packet

Loss, RTT or latency, Delay Variation (Jitter), and Latency and Delay Variation (Jitter) thresholds. SAA Traps (configured in the Notifications application) are sent when configured thresholds are exceeded for a configured metric.

SAA is supported on OS6900 and OS10K Switches running AOS 7.3.2.R01 or higher, OS6865 Switches running AOS 8.3.1.R01 and higher, and OS6860 Series Switches running AOS 8.1.1.R01 and higher.

> **Note:** You must first enable SAA Traps and configure default SAA metrics before configuring SAAs.



SAA Prerequisites

The following prerequisites must be met before configuring an SAA between switches/VMs:

- Enable SAA Traps
- Configure SAA Default Metrics

Enable SAA Traps

SAAs are basically monitoring agents that send traps to OmniVista when SAA metrics exceed user-configured Threshold values (e.g., RTT, Jitter). So for the SAA feature to work, SAA traps must be enabled in the Notifications application on applicable switches. The following traps must be enabled:

Trap ID	Trap Name
117	alaSaaIPIterationCompleteTrap
118	alaSaaEthIterationCompleteTrap
119	alaSaaMacIterationCompleteTrap
146	alaSaaPacketLossTrap
147	alaSaaJitterThresholdYellowTrap
148	alaSaaRTTThresholdYellowTrap
149	alaSaaJitterThresholdRedTrap
150	alaSaaRTTThresholdRedTrap

Configure SAA Metrics

Default SAAs metrics (e.g., RTT Threshold, Jitter Threshold, VLAN) are configured on the Settings Screen. These values will be used to automatically configure SAAs between VM pairs. They are also the default values displayed in the Ethernet SAA Creation Wizard. These default values can be modified on the Settings Screen or when creating an SAA using the Ethernet SAA Creation Wizard.

Configuring SAAs

SAAs are configured using the following screens in the SAA application:

- **Ethernet OAM -** Used to configure SAAs between switch pairs.
- **Profile Association -** Used to configure SAAs between VM pairs.
- **Settings -** Used to configure default SAA Profile settings as well as SAA data retention. Default SAA are used to automatically configure SAAs between VM pairs. They are also the default values displayed in the Ethernet SAA Creation Wizard.

Ethernet OAM

The SAA Ethernet OAM Screen displays information about all configured SAAs and is used to create, edit, and delete SAAs between switch pairs. It is also used to view statistics for configured SAAs. You can configure up to 127 SAAs. However, a maximum number of 50 is recommended to conserve system resources.

Note: You must first configure SAA traps in the Notifications application before configuring SAAs. See the SAA Overview help for more information on SAA Prerequisites.

Note: SAAs between VMs are configured on the Profile Association Screen.

Creating an SAA

Note: When an SAA is created on an AOS 8.x switch and the SAA test runs and collects statistics, if the switch is rebooted before the switch configuration is saved, the SAA test is removed from the switch but the OmniVista SAA instance is not cleared and cannot be modified or deleted. To clear the SAA instance from OmniVista, simply rediscover the switch.

Click on the Add icon to bring up the Create Ethernet SAA Wizard. Complete the screens as described below and click on the **Create** button.

Ethernet Config

The Ethernet Config Screen is used to create an SAA between switches and configure the basic metrics that will be monitored.

- **Name -** The user-defined SAA Name (up to 32 characters).
- **Description -** Optional description for the SAA (up to 32 characters).
- **Owner -** This will always be OV (OmniVista). This field is not configurable.
- **Test Mode -** The SAA Test type. Currently, only MAC Address Ping (MACSAA) is supported. This field is not configurable.
- **Source IP -** The source IP address of the switch pair.
- **Destination IP -** The destination IP address of the switch pair.
- **Admin Status -** The administrative status of the SAA (Start/Stop) (Default = Start).
- **RTT Threshold -** The round-trip time threshold, in microseconds. A trap is generated when this value is crossed (Range = 1 – 1,000,000, Default = 100).
- **Jitter Threshold -** The jitter threshold, in microseconds. A trap is generated when this value is crossed (Range = 1 – 1,000,000, Default = 100).
- **Packet Loss Threshold** - The packets lost threshold, in packets. A trap is generated when this value is crossed (Range - 1 - 100, Default = 5).
- **Interval -** The amount of time, in minutes, between two iterations of the SAA test (Range = from 1 1500, Default = 150).

MAC Config

The MAC Config Screen is used to configure the MAC parameters for the SAA.

- **VLAN -** The VLAN on which the SAA Packets are sent out (Range = 1 - 4094).
- **Inter Packet Delay -** The delay between packets sent during a ping iteration, in milliseconds (Range = 100 - 1000).
- **Number of Packets -** The number of packets to send in one ping iteration (Range = 1 – 100, Default = 5).
- **Payload Size -** The size of the ICMP payload to be used for the ping iteration, in bytes (Range = 24 – 1472, Default = 32).

- **Packet Data -** The size of the ICMP payload, in bytes, to be used for the ping iteration (Range = 36 – 1500).
- **ISID Check -** Enable this field to use the configured Service Instance Identifier (ISID) to identify the SPB service in a provider backbone bridge (PBB) network.
- **ISID -** If "ISID Check" is enabled. enter the ISID number (Range = 256 - 16777214).

Review

Review the configuration. If necessary, click on the **Back** button to make changes. When you are done, click on the **Create** button.

Editing an SAA

Select an SAA in the SAA Ethernet List and click on the Edit icon to bring up the Edit Ethernet SAA Wizard. Edit the available fields as described above and click on the **Apply** button. Note that you cannot edit the MAC Configuration.

Deleting an SAA

Select an SAA in the SAA Ethernet List and click on the Delete icon. Click **OK** at the Confirmation Prompt. Note that you cannot delete a running SAA. If an SAA is running, you must first stop the SAA before deleting it. Also note that you can only delete an SAA that was created in OmniVista

SAA Ethernet List

The SAA Ethernet List displays information about configured SAAs. To display SAA information for a device, click on the **ADD** or **EDIT** button at the top of the list, select the switch, and click **OK**. Click on the **EDIT** button again to display information about a different device.

- **Name -** The user-defined SAA Name. If the SAA is configured between VMs, the name will automatically be filled with the source and destination MAC addresses of the VMs.
- **Owner -** This will always be OV (OmniVista).
- **Source MAC Address -** The source MAC address of the switch/VM pair.
- **Source IP Address -** The source IP address of the switch pair. If the SAA is configured between VMs, the source address of the switch managing the VM is displayed.
- **Destination MAC Address -** The destination MAC address of the switch/VM pair.
- **Destination IP Address -** The destination IP address of the switch pair. If the SAA is configured between VMs, the destination address of the switch managing the VM is displayed.
- **Test Mode -** The SAA Test type. Currently, only MAC Address Ping (MACSAA) is supported.
- **RTT Threshold -** The round-trip time threshold, in microseconds. A trap is generated when this value is crossed (Range = 1 – 1,000,000, Default = 100).
- **Jitter Threshold -** The jitter threshold, in microseconds. A trap is generated when this value is crossed ((Range = 1 – 1,000,000, Default = 100).

- **Packets Loss Threshold -** The packets lost threshold, in packets. A trap is generated when this value is crossed (Range = 1 - 100, Default = 5).
- **Admin Status -** The administrative status of the SAA (Start/Stop) (Default = Start).
- **Interval -** The amount of time, in minutes, between two iterations of the SAA test (Range = from 1 1500, Default = 150).
- **Description -** Optional description for the SAA.
- **VLAN** - The VLAN on which the SAA Packets are sent out (Range = 1 - 4094).
- **ISID** - The configured Service Instance Identifier (ISID) to identify the SPB service in a provider backbone bridge (PBB) network.

Viewing SAA Statistics

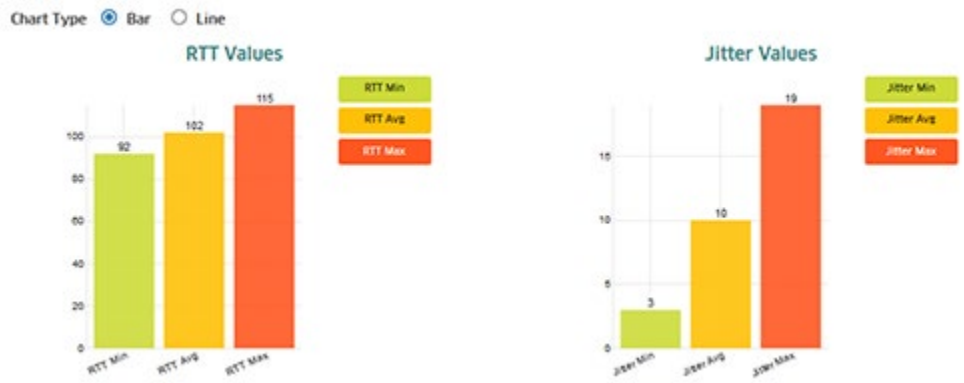
Select an SAA in the SAA Ethernet List then click on the **Statistics** button to view detailed statistics for the profile. Statistics are displayed in graphical and tabular format. The amount of data displayed in the graphical and table displays (and the length of time the profile will run) is configured on the Settings Screen (Range = 1 - 90 Days, default = 30 Days).

Graphical Display

By default, the graphical display for each is a Bar Chart Graph. Select the Line radio button to change the display to a Line Chart Graph.

Bar Chart Format

The Bar Charts show average RTT and Jitter values over the sampling period. The table below them shows values at each polling interval (shown in the Run Time Column). By default, the Bar Charts show the average values of all of the data in the table. You can get the average of a specific group of data points by selecting rows in the table. The Bar Charts will automatically reflect the averages for that select group of data points. De-select the rows to return to the default view.



Line Chart Format

The Line Chart shows the RTT and Jitter values in real time. Click on a data point to view specific values. Click the mouse in a chart and use the mouse button to scroll through the data on the timeline.

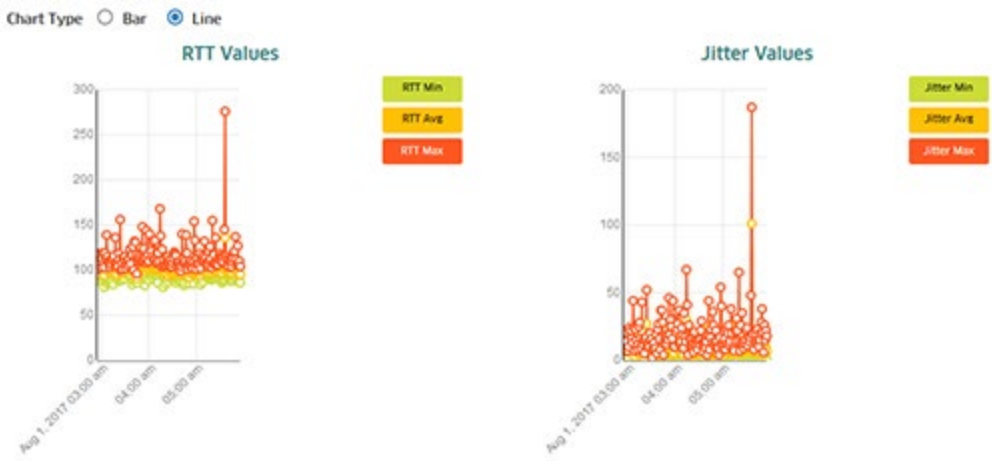


Table Display

The table below the graphical displays shows the following values at each polling interval (shown in the Run Time Column). Values exceeding Warning levels are highlighted in yellow; values exceeding Maximum levels are highlighted in red.

- **Name** - The user-defined SAA name.
- **VLAN** - The VLAN on which the SAA Packets are sent out.
- **ISID** - The configured Service Instance Identifier (ISID) to identify the SPB service in a provider backbone bridge (PBB) network.
- **Min RTT -** The minimum round-trip time, in microseconds.
- **Avg RTT -** The average round-trip time, in microseconds.
- **Max RTT -** The maximum round-trip time, in microseconds.
- **Min Jitter -** The minimum jitter, in microseconds.
- **Avg Jitter -** The average jitter, in microseconds.
- **Max Jitter -** The maximum jitter, in microseconds.
- **Pkts Lost -** The number of packets lost.
- **Run Time -** The polling interval.

Profile Association

The SAA Profile Association Screen displays a list of configured SAA Profiles, and is used to create and delete SAAs between Virtual Machines (VMs). It is also used to view statistics for SAA Profiles. SAA Profiles are created whenever you create an SAA between switches or VMs.

When you create an SAA between VMs, you don't actually configure SAAs between VM pairs. Rather, you associate VM pairs with an SAA by creating an SAA Profile. You create SAAs between VMs managed on different switches in your network, and the SAA application will continue to monitor these VMs even if they move to different switches in the network.

Creating an SAA VM Profile

Click on the Add icon to bring up the VM SAA Setup Screen. Complete the screens as described below and click on the **Create** button.

Virtual Machine Information

Select the switches and VMs for which you want to configure an SAA.

- **Device Selection -** Click on the **ADD** button and select switches that are managing the VM for which you want to configure an SAA.
- **Select Source VM -** Select a source VM from the drop-down menu.
- **Select Destination VM -** Select a destination VM from the drop-down menu.

SAA Setup

- **VLAN -** The VLAN on which the SAA Packets are sent out (Range = 1 - 4094).
- **ISID Check -** Enable this field to use the configured Service Instance Identifier (ISID) to identify the SPB service in a provider backbone bridge (PBB) network.
- **ISID -** If "ISID Check" is enabled. enter the ISID number (Range = 256 - 16777214).

If an SAA with the same SAA Ethernet and MAC configuration already exists between the switches hosting the VMs, the VMs are automatically assigned to that SAA. If an SAA on the specified SAA VLAN does not exist between the switches hosting the VMs, an SAA is automatically configured and started, using the SAAs default values (e.g., VLAN Priority, Drop Eligible, Inter Packet Delay) configured on the Settings Screen.

SAA VM Profiles and VM Movement

Once an SAA has been configured for one (or more) VM pairs, OmniVista automatically responds to VM moves. Because SAAs are configured between switches, if a VM moves to another host on the same switch, its existing SAA VM Profile remains unchanged. If a VM moves to a different switch, and an SAA with the same configuration exists on the switch, OmniVista will associate the VM with the existing SAA VM Profile on that switch. If an SAA with the same configuration does not exist on the new switch, OmniVista will create, and start, a new SAA VM Profile with the same configuration.

If a new SAA is created on VM movement, the new SAA Administrative State (Start/Stop) will be same as old SAA state that the SAA VM Profile was associated. However, if the VM is associated with an existing SAA, the Admin State is set as follows:

VM's Old SAA Profile State	Existing SAA Profile State	Final Admin State of Associated SAA
Stop	Stop	No change required.
Stop	Start	User is given warning - "State of associated SAA cannot be changed. User has to manually change the state".
Start	Stop	User is given warning - "State of associated SAA cannot be changed. User has to manually change the state".
Start	Start	No change required.

Deleting an SAA VM Profile

Select a profile in the SAA Profiles List and click on the Delete icon. Click **OK** at the Confirmation Prompt. Note that you cannot delete a running SAA. If an SAA is running, you

must first stop the SAA before deleting it. Also, you can only delete an SAA that was created in OmniVista.

SAA Profiles List

The SAA Profiles List displays basic configuration information about configured SAA Profiles. If an SAA was created on the Ethernet OAM Screen, the Profile Name will have the prefix "SAAExpertProfile". If the SAA was created on the Profile Association Screen, the Profile will have the prefix "SAAVMProfile".

Viewing SAA VM Profile Statistics

Select a profile in the SAA Profiles List and click on the **Statistics** button to display basic profile information.

- **SAA Profile -** The SAA Profile name. This is created automatically by OmniVista. If the profile was created between switch pairs on the Ethernet OAM Screen, the name will have the prefix "SAAExpertProfile". If the profile was created between VM pairs on the SAA Profile Association Screen, the Profile will have the prefix "SAAVMProfile".
- **Start At -** The VM movement start time.
- **Stop At -** The VM movement stop time.

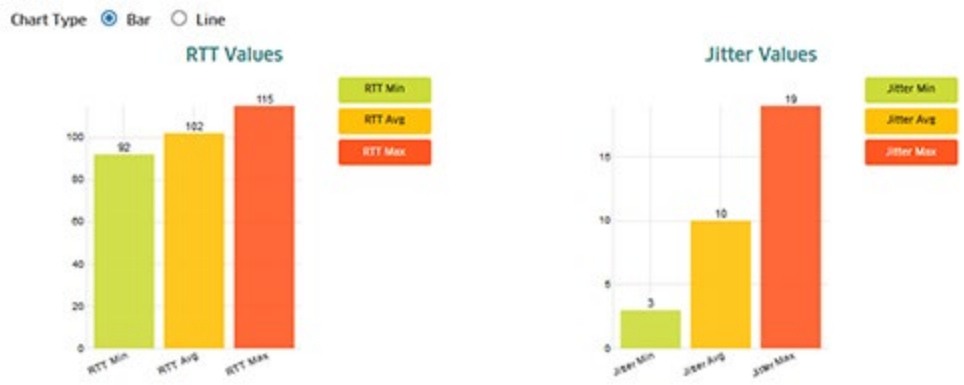
Click on an SAA Profile, then click on the **View Statistics Details** button to view detailed statistics for the profile. Statistics are displayed in graphical and tabular format. The amount of data displayed in the graphical and table displays (and the length of time the profile will run) is configured on the Settings Screen (Range = 1 - 90 Days, default = 30 Days).

Graphical Display

By default, the graphical display for each is a Bar Chart Graph. Select the Line radio button to change the display to a Line Chart Graph.

Bar Chart Format

The Bar Charts show average RTT and Jitter values over the sampling period. The table below them shows values at each polling interval (shown in the Run Time Column). By default, the Bar Charts show the average values of all of the data in the table. You can get the average of a specific group of data points by selecting rows in the table. The Bar Charts will automatically reflect the averages for that select group of data points. De-select the rows to return to the default view.



Line Chart Format

The Line Chart shows the RTT and Jitter values in real time. Click on a data point to view specific values. Click the mouse in a chart and use the mouse button to scroll through the data on the timeline.

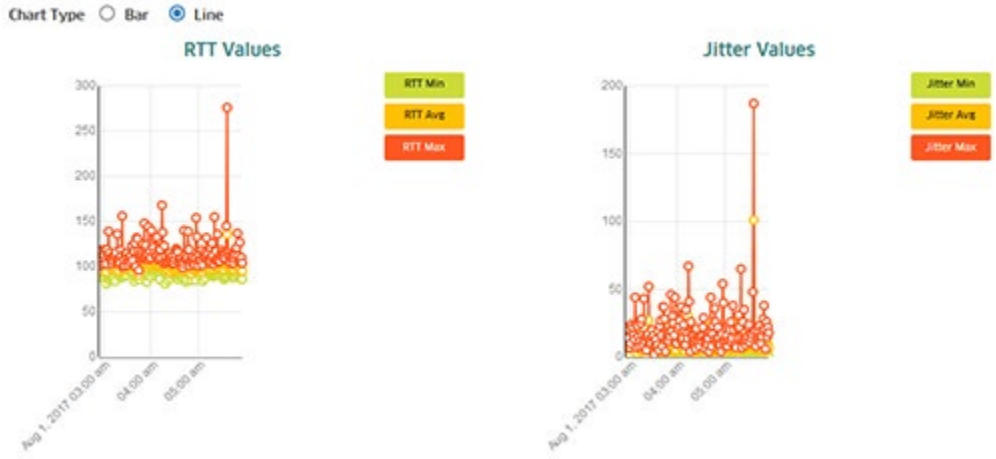


Table Display

The table below the graphical displays shows the following values at each polling interval (shown in the Run Time Column). Values exceeding Warning levels are highlighted in yellow; values exceeding Maximum levels are highlighted in red.

- **Name** - The user-defined SAA name
- **VLAN** - The VLAN on which the SAA Packets are sent out.
- **ISID** - The configured Service Instance Identifier (ISID) to identify the SPB service in a provider backbone bridge (PBB) network.
- **Min RTT -** The minimum round-trip time, in microseconds.
- **Avg RTT -** The average round-trip time, in microseconds.
- **Max RTT -** The maximum round-trip time, in microseconds.
- **Min Jitter -** The minimum jitter, in microseconds.
- **Avg Jitter -** The average jitter, in microseconds.
- **Max Jitter -** The maximum jitter, in microseconds.

- **Pkts Lost -** The number of packets lost.
- **Run Time -** The polling interval.

Settings

The SAA Settings Screen is used to configure default SAA Profile settings as well as SAA data retention. Default SAA are used to automatically configure SAAs between VM pairs. They are also the default values displayed in the Ethernet SAA Creation Wizard.

Ethernet Config

- **Owner -** This will always be OV (OmniVista). This field is not configurable.
- **Test Mode -** The SAA Test type. Currently, only MAC Address Ping (MACSAA) is supported. This field is not configurable.
- **Admin Status -** The administrative status of the SAA (Start/Stop) (Default = Start. It cannot be modified).
- **RTT Threshold -** The round-trip time threshold, in microseconds. A trap is generated when this value is crossed (Range = 1 – 1,000,000, Default = 100)
- **Jitter Threshold -** The jitter threshold, in microseconds. A trap is generated when this value is crossed (Range = 1 – 1,000,000, Default = 100).
- **Packets Loss Threshold** - The number of packets lost threshold. A trap is generated when this value is crossed (Range - 1 - 100, Default = 5).
- **Interval -** The amount of time, in minutes, between two iterations of the SAA test (Range = from 1 1500, Default = 150).

MAC Config

- VLAN - The VLAN on which the SAA Packets are sent out (Range = 1 - 4094).
- Inter Packet Delay - The delay between packets sent during a ping iteration, in milliseconds (Range = 100 - 1000).
- Number of Packets - The number of packets to send in one ping iteration (Range = 1 – 100, Default = 5).
- Payload Size - The size of the ICMP payload to be used for the ping iteration, in bytes (Range = 24 – 1472, Default = 32).
- Packet Data - The size of the ICMP payload, in bytes, to be used for the ping iteration (Range = 36 – 1500).
- ISID Check - Enable this field to use the configured Service Instance Identifier (ISID) to identify the SPB service in a provider backbone bridge (PBB) network.
- ISID - If "ISID Check" is enabled. enter the ISID number (Range = 256 - 16777214).

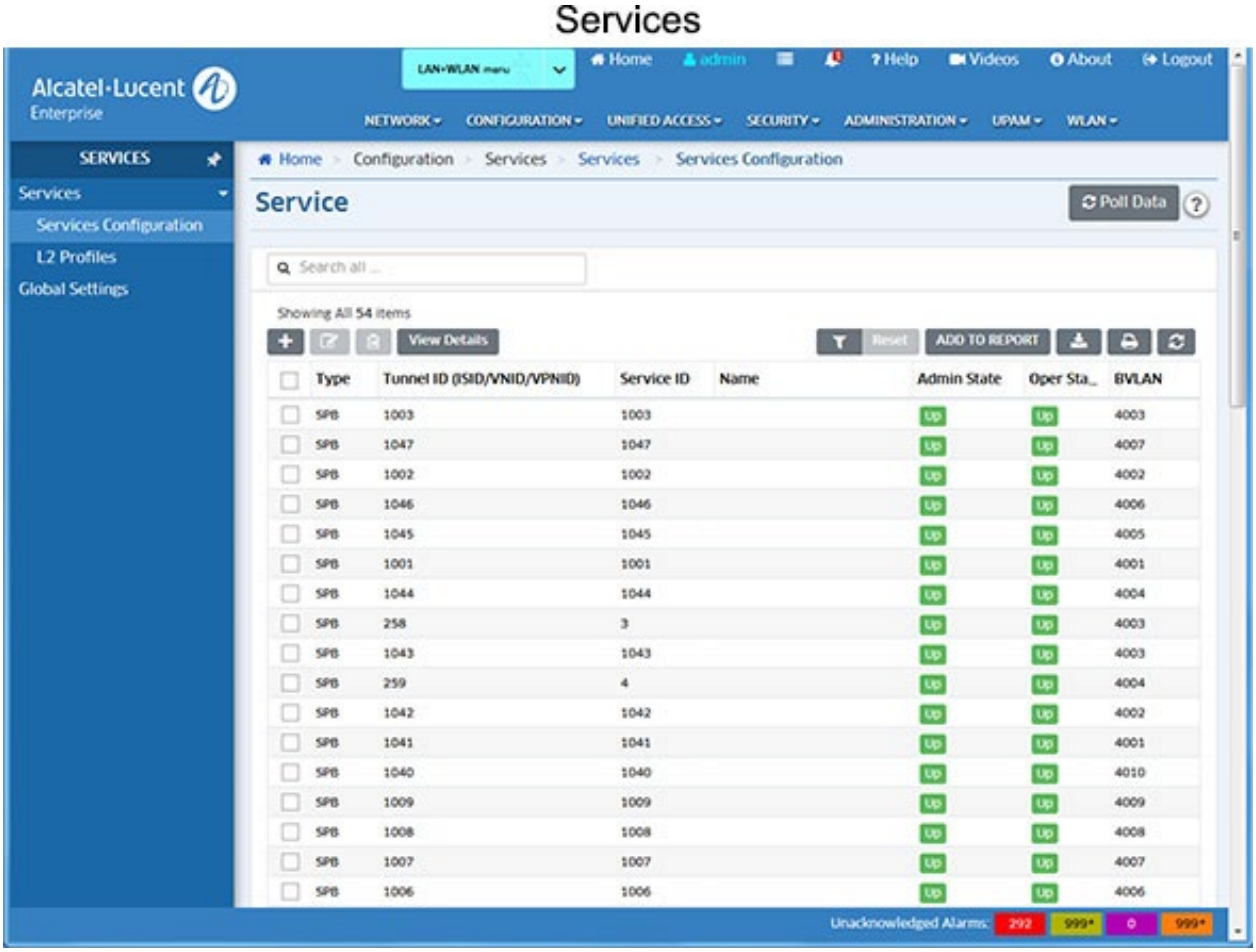
Ethernet Stats

- **Days to Retain -** The default maximum length of time, in days, that an SAA will run (and retain statistics data). If an SAA reaches this configured value, it is automatically stopped. If the user restarts the SAA, the data that exceeded the configured value is deleted (Range = 1 - 90, Default = 30).
- **Top N High Paths** - The number of paths with the highest values (High RTT, High Jitter, High Packets Lost).

- **Number of Records -** The total number of records since the last data purge. Click on the **Purge All** button to delete data that exceeded the configured "Days to Retain" value

29.0 Services

The Service Screen is used to view and configure Services on network devices. Currently, Shortest Path Bridging (SPB) Services are supported. You can view and configure SPB on new switches as well as existing switches in the network that are already configured for SPB (e.g., via the CLI).



Services are configured using the following screens:

- Services
- **Service Configuration -** Used to view/configure Services on network devices. Switches must first be selected on the Global Settings Screen before you can view/configure Services on those switches.
- **L2 Profiles -** Used to configure Layer 2 Profiles, which can be associated with an SPB Service Access Point (SAP).
- **Global Settings -** Used to select switches on which you want to view/configure a Service.

SPB Overview

The OmniSwitch supports Shortest Path Bridging MAC (SPBM), as defined in the IEEE 802.1aq standard. SPB-M uses the Provider Backbone Bridge (PBB) network model to encapsulate (using IEEE 802.1ah headers) and tunnel customer traffic through the network backbone. The shortest path trees (SPTs) upon which the PBB network infrastructure operates are determined using a version of the Intermediate System- to-Intermediate System (IS-IS) link state protocol that supports TLV extensions for SPB (ISIS-SPB).

The SPBM network topology consists of two layers: the backbone infrastructure (control plane) layer and the services (data plane) layer. ISIS-SPB builds the backbone layer by defining loop-free, SPTs through the backbone network. The service layer is based on the PBB framework as defined in the IEEE 802.1ah standard. SPBM supports the 802.1ah MAC-in-MAC method for data encapsulation. SPBM services transport the encapsulated traffic over the ISIS-SPB infrastructure.

Service

The Service Screen displays all Services configured on switches selected on the Global Settings Screen, and is used to create, edit, and delete Services on those network switches. Currently, Shortest Path Bridging (SPB) Services are supported. You can also poll switches for the latest SPB configuration information.

> **Note:** You must first select switches using the Service Global Settings Screen to view/configure Services on those switches.

Creating a Service

Click on the Add icon, complete the fields as described below, then click on the **Create** button.

Service Parameters

Complete the fields below to create a new Service.

Basic

- **Type -** The Service Type (SPB).
- **Service ID -** A unique numerical value that identifies the Service (Range = 1 - 32767). The field is pre-filled with a Service ID is auto-generated by OmniVista, based on the last highest Service ID configured (current highest value + 1). If you change it, you must avoid entering an Exiting ID.
- **ISID -** An ISID is required on a switch configured as a Backbone Edge Bridge (BEB). It identifies a backbone service instance that will tunnel the encapsulated data traffic through the network between BEBs. The ISID is bound to a BVLAN ID and a Service Manager SPB service ID when the service is created. The field is per-filled with a Service ID is auto-generated by OmniVista, based on the last highest ISID configured (current highest value + 1). If you change it, you must avoid entering an Exiting ID.
- **BVLAN -** Select the BVLAN for the Service. The drop-down displays BVLANs configured on the switch. BVLANs are configured on a switch using the CLI. For more information on configuring BVLANs using the CLI, see the *OmniSwitch AOS Network Configuration Guide*.
- **Admin State -** Enables/Disables the Service.

- **Description -** Enter an optional description for the Service.
- **Select Devices -** Click on the **ADD**/**EDIT** button to select devices on which you want to configure the Service.

Advanced

- **Multicast Mode -** The multicast replication mode for the Service. Make sure that the same Multicast Mode is used across all nodes for a given SPB BVLAN. Tandem nodes and head-end nodes cannot communicate with each other. Select a mode from the drop-down:
- **Headend -** A non-unicast packet received on an SPB access port is replicated once for each receiver in the provider backbone bridge (PBB) network using its unicast base MAC (BMAC) address. (Default)
- **Tandem -** A non-unicast packet received on an SPB access port is replicated once at each node using the multicast group address
- **VLAN Translation -** Enables/Disables VLAN Translation. VLAN Translation refers to the egress translation of VLAN tags on Service Access Points (SAPs). If VLAN Translation is enabled for a service, the VLAN tags for outgoing customer frames on SAPs associated with that service are processed according to the local SAP configuration (the SAP on which the frames will egress) and not according to the configuration of the SAP on which the frames were received. If VLAN Translation is disabled, frames simply egress without any modification of the VLAN tags. In other words, the frames are transparently bridged without tag modification. (Default - Disabled).
- **Remove Ing Tag -** Configures whether or not the customer VLAN tag is removed from ingress packets for the service (default = Disabled).
- **Stats -** Enables/Disables statistics collection for the Service.
- **VPN MTU -** Set the VPN MTU. This is the largest frame size, in octets, that the Service can handle. (Default = 1,500)
- **Select Devices -** Click on the **ADD**/**EDIT** button to select devices on which you want to configure the Service.

Configure SAP (Required for Backbone Edge Bridge)

Each Service is bound to at least one Service Access Point (SAP). A SAP identifies the point at which customer traffic enters the network. Creating a SAP on an SPB switch designates that switch as a Backbone Edge Bridge (BEB). An SPB switch that does not have a SAP but does have at least one BVLAN and an SPB interface is designated as Backbone Core Bridge (BCB).

- **Configure SAP -** Enable (On) to configure a SAP(s) on a switch.
- **Global SAP Settings -** Configure the global SAP settings below.

  Outer/Inner VLAN - Enter the Outer and/or Inner VLAN. Entering an Outer or Inner VLAN is a way to map traffic tagged with the VLAN to the Service.

  Description - Optional user description.

  Admin State - Enables/Disables the SAP.

  Stats - Enables/Disables ingress and egress statistics collection for packets flowing through the SAP.

  Priority - Select whether the SAP port is **Trusted** or is assigned a priority value (**Fixed**). If you select "Fixed", enter a value in the **Priority Number** field.

Automatic Access Interface Configuration - Enables/Disables automatic access interface configuration. If Enabled, OmniVista automatically creates an SPB interface.

- **Global Access Interface Config** - Enables/Disables Global Access Interface Configuration. If Enabled, OmniVista creates a SAP based on the configuration below:

  Description - Enter an optional user description.

  L2 Profile - Select a Layer 2 Profile from the drop-down menu, or click on the Add icon (+) to create a new profile. Layer 2 profiles specify how control packets are processed on SAPs.

  VLAN Translation - Enables/Disables VLAN Translation.
- **Select Ports -** Complete the fields below to designate an SAP Port(s).
- **Common Ports -** Enter ports to configure the same port(s) as SAPs on all selected switches; or select ports in List of Selected Devices.
- **List of Selected Devices -** Click on the "Add Port" link under a switch to designate the ports as SAPs.

Configure UNP Access Ports (Optional)

Complete the fields below to configure UNP Access Ports.

- **Configure UNP Access Ports -** Enable (On) to configure UNP Access Ports.
- **Access Auth Profile -** Select an Access Authentication Profile to be applied to traffic received on UNP Access Ports.
- **Common Ports -** Enter ports to configure the same UNP Access Port(s) on all selected switches; or select ports in List of Selected Devices.
- **List of Selected Devices -** Click on the "Add Port" link under a switch to designate the port(s) as UNP Access Ports.

Configure UNP Mapping (Optional)

- **Outer/Inner VLAN -** Enter the Outer and/or Inner VLAN to be checked for tagged traffic.
- **Access Role Profile -** Select an Access Role Profile to be applied to the traffic.

Editing a Service

Select a Service(s) in the table, click on the Edit icon, and edit a configuration field(s) as described above. To edit a field that is inconsistent, click on "Click to Overwrite" link below the field and edit the field.

To add/remove a Service to/from a device, go to the Selected Devices Section:

- **Add a Service to a Device** - Click on "Add Service To New Devices" link, click on the **ADD**/**EDIT** button and select a device (s). The device(s) will appear under "Add Service To New Devices".
- **Remove a Service From a Device -** Select a device(s) and click on the "Remove Service From Devices" link. The device will be moved under "Remove Service From Devices".

When you are finished editing, click on the **Apply** button.

Deleting a Service

Select a Service(s) in the table, click on the Delete icon, then click **OK** at the Confirmation Prompt.

Service Table

By default, information for all Services on all devices is displayed. For a more detailed information on all Services, click on the **View Details** button at the top of the table. You can also select a specific Service(s) in the table and click on the **View Details** button for detailed information about that Service (s). Three tables are displayed that display Device, SAP, or SDP information for the selected Service(s). Click on a tab to view information.

> **Note:** If you have a large number of Services, it is recommended that you select a specific Service or Services when using the **View Details** button. Viewing details on a large number of Services at the same time can cause delays in displaying the data.

Services Information

The Service Table displays general information about all Services configured on the network. Note that if a configuration for a Service is inconsistent, OmniVista displays an exclamation point next to the field. You can select that service and click on the **View Details** button to determine the inconsistency between devices.

- **Type -** The Service type (SPB).
- **Tunnel ID -** A backbone service instance that tunnels the encapsulated data traffic through the network between BEBs. A Tunnel ID is associated with a Service ID.
- **Service ID -** A unique numerical value that identifies the Service
- **Name -** A user-configured name for the Service. It can also be auto-generated by a dynamically created service.
- **Admin State -** The administrative state of the Service (Up/Down).
- **Oper State -** The operational state of the Service (Up/Down).
- **BVLAN -** The BVLAN associated with the Service.
- **Mcast Mode -** The multicast replication mode for the Service (Headend, Tandem).
- **VLAN Translation -** Whether VLAN Translation is enabled for the Service. (Yes/No).
- **Remove Ingress -** Whether " Remove Ingress Tag" is enabled for the Service (Yes/No).
- **Stats -** Whether statistics collection is enabled for the Service (Yes/No).
- **Router Interface -** The SPB interface.
- **VPN MTU -** Set the VPN MTU. This is the largest frame size, in octets, that the Service can handle. (Default = 1,500)
- **Port Isolation -** Whether port isolation is configured.

Device Information

The Device Table displays detailed information about devices on which the Service is configured.

- **Friendly Name -** The IP address of the device on which the Service is configured.

- **Service Type -** The Service type (SPB).
- **Tunnel ID -** The Tunnel ID used by the Service.
- **Service ID -** A unique numerical value that identifies the Service
- **Name -** A user-configured name for the Service. It can also be auto-generated by a dynamically created service.
- **Admin State -** The administrative state of the Service (Up/Down).
- **Oper State -** The operational state of the Service (Up/Down).
- **BVLAN -** The BVLAN associated with the Service.
- **Mcast Mode -** The multicast replication mode for the Service (Headend, Tandem).
- **VLAN Translation -** Whether VLAN Translation is enabled for the Service. (Yes/No).
- **Remove Ingress -** Whether " Remove Ingress Tag" is enabled for the Service (Yes/No).
- **Stats -** Whether statistics collection is enabled for the device (Yes/No).
- **Router Interface -** The SBP interface.
- **VPN MTU -** Set the VPN MTU. This is the largest frame size, in octets, that the Service can handle. (Default = 1,500)
- **NB SAPs -** The number of SAPs configured on the device.
- **NB SDPs -** The number of SDPs configured on the device.

SAP Information

The SAP Table displays detailed information for SAPs configured for the Service.

- **Friendly Name -** The IP address of the device on which the SAP is configured.
- **Service Type -** The Service type (SPB).
- **Tunnel ID -** The Tunnel ID used by the Service.
- **Outer/Inner VLAN -** The Inner/Outer VLAN configured for the SAP.
- **Service ID -** A unique numerical value that identifies the Service
- **Name -** A user-configured name for the Service. It can also be auto-generated by a dynamically created service.
- **Admin State -** The administrative state of the Service (Up/Down).
- **Oper State -** The operational state of the Service (Up/Down).
- **Description -** An optional user description.
- **SAP Type -** The SAP Priority setting (Trusted/Fixed)
- **Priority -** The Priority Value if the SAP Priority Type is "Fixed".
- **Stats -** Whether ingress and egress statistics collection for packets flowing through the SAP is enabled (Yes/No).

SDP Information

The SDP Table displays detailed information for Service Distribution Points (SDP) configured for the Service.

- **Friendly Name -**The IP address of the device on which the SAP is configured.
- **Service Type -**The Service type (SPB).

- **Tunnel ID -** The Tunnel ID used by the Service.
- **Interface -** The interface on which the SDP is configured.
- **SDP Type -** The SDP type (Dynamic).
- **Service ID -** A unique numerical value that identifies the Service.
- **SDP ID -** A unique numerical value that identifies the Service. This value is dynamically generated by OmniVista.
- **Admin State -** The administrative state of the SDP (Up/Down).
- **Oper State -**The operational state of the SDP (Up/Down).
- **Description -** The SDP description, if applicable.
- **SDP Name -** The SDP name.
- **SDP Info -** Additional SDP information, if applicable.
- **Stats -** Whether statistics collection for the SDP is enabled (Yes/No).
- **TTL -** The time-to-live (TTL) value for the SDP.

Polling Switches for SPB Information

By default, OmniVista is automatically scheduled to poll switches for Service information every 3 hours. To perform an immediate poll, click on the **Poll Data** button. OmniVista will poll the switches on the Global Settings Screen. When polling is complete, you can click on the "Results" Link to see the poll results for each switch (Success or Fail). The data on the Topology Screen - SBP View (Network - Topology) will also be updated with the latest information.

L2 Profiles

The Services L2 Profiles Screen displays configured Layer 2 Profile and is used to create, edit, and delete Layer 2 Profiles. Layer 2 Profiles determine how control frames ingressing on an access port (e.g., Service Access Port) are processed. For SPB, L2 Profiles are applied to SAP interfaces under the "Configure SAP" section when creating or editing a Service on the Services Screen.

Creating a Profile

Click on the Add icon, enter an **L2 Profile Name** and set the behavior for processing control frame types ingressing on an access port.

- **Tunnel -** Tunnel the PDU across the Provider Network.
- **Drop -** Discard the PDU.
- **Peer -** Allow the access port to participate in the specified protocol. Control packets are not sent to the network side of the node.

When you are finished, click on the **Create** button.

Editing a Profile

Select a profile(s) in the table, click on the Edit icon, edit a configuration field(s) as described above, then click on the **Apply** button.

Deleting a Profile

Select a profile in the table, click on the Delete icon, then click **OK** at the Confirmation Prompt. You cannot edit the default profiles (OV-unp-def-access-profile, OV-def-access-profile).

L2 Profiles Table

The L2 Profiles Table displays configuration details for all configure Layer 2 Profiles.

Polling Switches for SPB Information

By default, OmniVista is automatically scheduled to poll switches for Service information every 3 hours. To perform an immediate poll, click on the **Poll Data** button. OmniVista will poll the switches on the Global Settings Screen. When polling is complete, you can click on the "Results" Link to see the poll results for each switch (Success or Fail). The data on the Topology Screen - SBP View (Network - Topology) will also be updated with the latest information.

Global Settings

The Service Global Settings Screen is used to select switches on which you want to view/configure a Service. (Shortest Path Bridging Services (SPB) are supported at this time.) This is the first step in viewing/configuring Services. Only these selected switches will be available for SPB viewing/configuring on the Service Screen; and only these switches will be polled for Service information. Once switches are selected, you can go to the Service Screen to view/configure Services on the switches.

Selecting Switches for SPB Configuration

Click on the **ADD** or **EDIT** button to add or remove switches. When you are done, click on the **Save Settings** button. If you removed switches, Services on those switches will no longer be displayed on the Service Screen; and those switches will no longer be polled for Services information.

Polling Switches for SPB Information

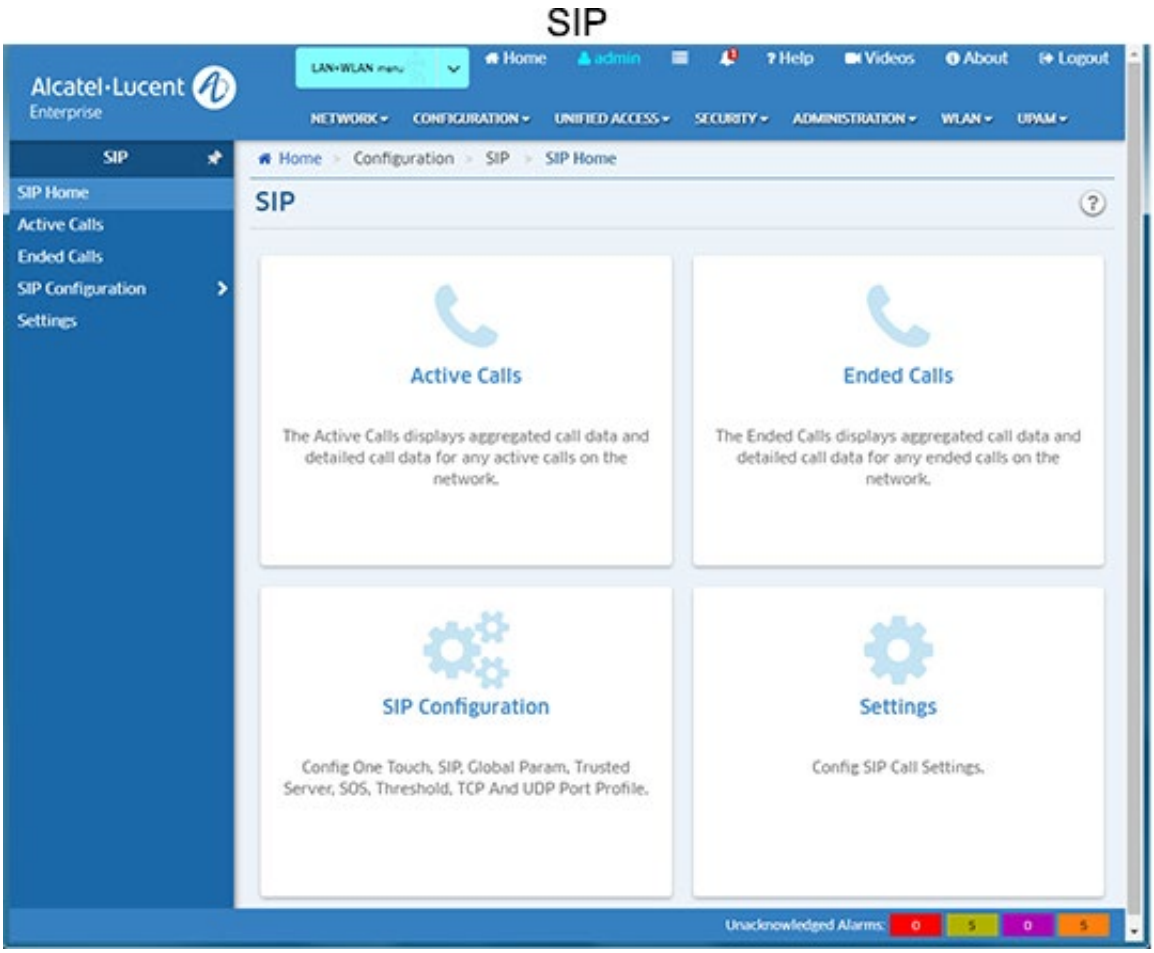
By default, OmniVista is automatically scheduled to poll switches for Service information every 3 hours. To perform an immediate poll, click on the **Poll Data** button. OmniVista will poll the switches on the Global Settings Screen. When polling is complete, you can click on the "Results" Link to see the poll results for each switch (Success or Fail). The data on the Topology Screen - SBP View (Network - Topology) will also be updated with the latest information.

30.0 SIP

Session Initiation Protocol (SIP) is an IETF-defined signaling protocol widely used for controlling communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating, modifying and terminating media sessions. SIP addresses the key challenge of real-time delivery and monitoring requirements for media streams from SIP devices. SIP Snooping prioritizes voice and video traffic over non-voice traffic. The OmniVista SIP Application automatically detects SIP data packets and enables you to configure SIP Profiles and apply QoS parameters for SIP packets; and monitor SIP traffic and create traps to alert you to SIP events. SIP Snooping:

- Identifies and marks the SIP and its corresponding media streams. Each media stream contains Real Time Protocol (RTP) and Real Time Control Protocol (RTCP) flows. Marking is done using the DSCP field in the IP header.
- Provides user configured QOS treatment for SIP/RTP/RTCP traffic flows based on its marking.
- Calculates QOS metric values of delay, jitter, round trip time, R factor and MOS values of media streams from its corresponding RTCP.

Note: The SIP snooping functions and the QOS actions require that the network paths used by the SIP signaling messages and the RTP/RTCP flows are the same and are “symmetric”. Therefore, MC-LAG, ECMP routing and VRRP topologies are not supported.



SIP monitoring and configuration functions are accessed by clicking on one of the widgets on the Home Page or links on the left side of the screen.

- **Active Calls -** The Active Calls Screen displays call data for any active calls on the network.
- **Ended Calls -** The Ended Calls Screen displays call data for any ended calls on the network.
- **SIP Configuration -** SIP Configuration Screens are used to configure global SIP parameters and custom SIP Profiles. One or more of the following sub-profiles profiles can be included in a custom SIP Profile.
  - **One Touch Profile -** The One Touch Profile Screen is used to configure all parameters for SIP packets with a single command.
  - **SIP Profile -** SIP Profile Screens are used to configure custom SIP Profiles and assign the profiles to switches/ports in the network to specify how SIP traffic is handled.
    - **Global Param Profile** - Used to configure global SIP Profile parameters (e.g., DSCP marking, call thresholds) and enable/disable SIP Snooping.
    - **Trusted Servers Profile -** Used to configure the IP addresses of the Trusted Servers. If a Trusted Server is configured, only the calls initiated through those servers are supported. If no Trusted Servers are configured, all SIP based calls using any call server are supported.
    - **Threshold Profile -** Used to configure SIP Snooping threshold parameters (e.g., jitter, packet loss).
    - **SOS Profile -** Used to configure SOS call strings.
    - **TCP Port Profile -** Used to configure a TCP port(s) for SIP Snooping.
    - **UDP Port Profile -** Used to configure a UDP port(s) for SIP Snooping.
  - **Device View -** The Device View Screen displays SIP Profile configuration for any SIP-enabled switch in the network.
- **Settings -** The Settings Screen is used to enable/disable and configure data retention parameters for SIP data.

SIP Overview

Ever increasing applications and their need for network resources keep demand on networks high. Critical applications like real-time voice, video and mission critical data applications continue to grow, and bandwidth needs are growing at a faster pace than the network technologies that need to address them. Therefore, it is essential to differentiate traffic, based on application, user and context, and provide applicable service levels for each. Voice and video traffic should be prioritized over non-voice traffic; and mission critical data traffic should be provided bandwidth guarantees for better performance. SIP is used for creating, modifying, and terminating media sessions; and applying QoS parameters to SIP traffic.

The SIP Snooping feature snoops voice quality metrics of media streams from their corresponding control packets and displays them to the user with knowledge of media reception quality in real time and helps to diagnose the problems on their quality. In addition, traps can be generated when voice/video/data quality parameters cross user configured thresholds.

Active Calls

The SIP Active Calls Screen is used to display Active Call Record data for selected SIP-enabled switches. To display Active Call Records, select an option from the drop-down menu (Use Switch Picker or Use Topology), then click on the **Select Devices** button to select the switches you want to view. The Active Call Records for the selected switches will be displayed in the table.

By default, the aggregated call records are displayed. The data is an aggregate of all Active Calls on SIP-enabled switches. You can also click on the **View Detailed Call** button at the top of the table to display detailed call records the selected switches.

Viewing Active Call Records

As described above, you can display aggregated or detailed call records in the table. You can also click on a switch(es) in the table to display a graphical representation of the call records.

Aggregated Records

Aggregated Records are call data for any active calls on the network. The data is an aggregate of all active calls on SIP-enabled switches.

- **Device -** The device name.
- **Start Time -** The call start date and time.
- **Calls Count -** The total number of calls processed for SIP Snooping.
- **RTCP Packet Count -** The total number of Real Time Control Protocol (RTCP) packets received by device.
- **RTP Packet Count -** The total number of Real Time Protocol (RTP) packet received by device.
- **Avg Pkt Loss -** The average number of SIP packet received by device.
- **Avg Jitter -** The average jitter, in milliseconds.
- **Avg RTD -** The average Round Trip Delay (RTD).
- **Avg RFactor -** The average RF Facto.
- **Avg MOS -** The average MOS.

Detailed Records

Detailed Records are detailed call data for any active calls on the network. The tab provides detailed data for each Active Call.

- **Device** - The Device name.
- **Call ID** - The call ID.
- **Tag A** - The call tag for call direction A to B.
- **Tag B** - The call tag for call direction B to A.
- **IP Addr A Type** - The IP type for call direction A to B type (e.g., IPv4).
- **IP Addr A** - The IP address for call direction A to B.
- **IP Addr B Type** - The IP type for call direction B to A type (e.g., IPv4).
- **IP Address B** - The IP address for call direction B to A.
- **L4 Port A** - The call L4 port for call direction A to B.

- **L4 Port B** - The call L4 port for call direction B to A.
- **SIP Medial Type** - The SIP Media Type (e.g., Voice, Video)
- **Start Time** - The call start date and time.
- **RTP Count A** - The call Real Time Protocol (RTP) packet count for call direction A to B.
- **RTCP Type A** - The call Real Time Control Protocol (RTCP) packet count for call direction A to B.
- **Rule Name A** - The policy rule name for call direction A to B.
- **RTP Count B** - The call Real Time Protocol (RTP) packet count for call direction B to A.
- **RTCP Count B** - The call Real Time Protocol (RTP) packet count for call direction B to A.
- **Rule Name B** - The policy rule name for call direction B to A.
- **Jitter Violations A** - The call RTCP jitter violations (%) for call direction A to B.
- **Jitter Violations B** - The call RTCP jitter violations (%) for call direction B to A.
- **RTD Violation A** - The call round trip delay violations (%) for call direction A to B.
- **RTD Violation B** - The call round trip delay violations (%) for call direction B to A.
- **Packet Loss Violations A** - Call packet loss violations (%) for call direction A to B.
- **Packet Loss Violations B** - The call packet loss violations (%) for call direction B to A.
- **MOS Violations A** - The call MOS violations (%) for call direction A to B.
- **MOS Violations B** - The call MOS violations (%) for call direction B to A.
- **RF Factor Violations A** - The call RF Factor Violation (%) for call direction A to B.
- **RF Factor Violations B** -
  The call RF Factor Violation (%) for call direction B to A.
- **Jitter Max A** - The call maximum jitter for call direction A to B.
- **Jitter Min A** - The call minimum jitter for call direction A to B.
- **Jitter Avg A** - The call average jitter for call direction A to B.
- **Jitter Max B** - The call maximum jitter for call direction B to A.
- **Jitter Min B** - The call minimum jitter for call direction B to A.
- **Jitter Avg B** - The call average jitter for call direction B to A.
- **RTD Max A** - The call maximum round trip delay for direction A to B.
- **RTD Min A** - The call minimum round trip delay for direction A to B.
- **RTD Avg A** - The call average round trip delay for direction A to B.
- **RTD Max B** - The call maximum round trip delay for direction B to A.
- **RTD Min B** - The call minimum round trip delay for direction B to A.
- **RTD Avg B** - The call average round trip delay for direction B to A.
- **Pkt Loss Max A -** The call maximum packet loss (%) for call direction A to B.
- **Pkt Loss Min A** - The call minimum packet loss (%) for call direction A to B.
- **Pkt Loss Avg A** - The call average packet loss (%) for call direction A to B.
- **Pkt Loss Max B** - The call maximum packet loss (%) for call direction B to A.
- **Pkt Loss Min B** - The call minimum packet loss (%) for call direction B to A.
- **Pkt Loss Avg B** - The call average packet loss (%) for call direction B to A.

- **RF Factor Max A** - The call maximum RF Factor for call direction A to B.
- **RF Factor Min A** - The call minimum RF Factor for call direction A to B.
- **RF Factor Avg A** - The call average RF Factor for call direction A to B.
- **RF Factor Max B** - The call maximum RF Factor for call direction B to A.
- **RF Factor Min B** - The call minimum RF Factor for call direction B to A.
- **RF Factor Avg B** - The call average RF Factor for call direction B to A.
- **MOS Max A** - The call maximum MOS for call direction A to B.
- **MOS Min A** - The call minimum MOS for call direction A to B.
- **MOS Avg A** - The call average MOS for call direction A to B.
- **MOS Max B** - The call maximum MOS for call direction B to A.
- **MOS Min B** - The call minimum MOS for call direction B to A.
- **MOS Avg B** - The call average MOS for call direction B to A.

Graphical View

You can view a graphical representation of Active Call Records by selecting a switch or switches in the table. By default, the data for "Jitter" is displayed in bar chart format. However, you can select a different variable from the **Variable** drop-down menu; and also change the display to a pie chart by selecting the "Pie" radio button in the **Chart Type** area.

Ended Calls

The SIP Ended Calls Screen is used to display Ended Call Record data for selected SIP-enabled switches. To display Ended Call Records, select an option from the drop-down menu (Use Switch Picker or Use Topology), then click on the **Select Devices** button to select the switches you want to view. You can also configure a Start Time and End Time to only display records from a specific time period.

By default, the aggregated call records are displayed. The data is an aggregate of all Active Calls on SIP-enabled switches. You can also click on the **View Detailed Call** button at the top of the table to display detailed call records the selected switches.

Viewing Ended Call Records

As described above, you can display aggregated or detailed call records in the table. You can also click on a switch(es) in the table to display a graphical representation of the call records.

Aggregated Records

Aggregated Records display call data for any ended calls on the network. The data is an aggregate of all ended calls on SIP-enabled switches.

- **Device -** The device name.
- **Start Time -** The call start date and time.
- **End Time -** The call end date and time.
- **Calls Count -** The total number of calls processed for SIP Snooping.
- **RTCP Packet Count -** The total number of Real Time Control Protocol (RTCP) packets received by device.

- **RTP Packet Count -** The total number of Real Time Protocol (RTP) packet received by device.
- **Avg Pkt Loss -** The average number of SIP packet received by device.
- **Avg Jitter -** The average jitter, in milliseconds.
- **Avg RTD -** The average Round Trip Delay (RTD).
- **Avg RFactor -** The average RF Facto.
- **Avg MOS -** The average MOS.

Detailed Records

Detailed Records are detailed call data for any ended calls on the network. The tab provides detailed data for each ended call. The data is an aggregate of all ended calls.

- **Device -** The Device name.
- **Call ID -** The call ID.
- **Tag A -** The call tag for call direction A to B.
- **Tag B -** The call tag for call direction B to A.
- **IP Address A -** The IP address for call direction A to B.
- **IP Address B -** The IP address for call direction B to A.
- **Port A -** The call L4 port for call direction A to B.
- **Port B -** The call L4 port for call direction B to A.
- **Medial Type -** The SIP Media Type (e.g., Voice, Video)
- **Start Date -** The call start date and time.
- **End Date -** The call end date and time.
- **RTP Count A -** The call Real Time Protocol (RTP) packet count for call direction A to B.
- **RTCP Count A -** The call Real Time Control Protocol (RTCP) packet count for call direction A to B.
- **Rule Name A -** The policy rule name for call direction A to B.
- **RTP Type B -** The RTP type for call direction B to A.
- **RTCP Count B -** The call Real Time Protocol (RTP) packet count for call direction B to A.
- **Rule Count B -** The call Real Time Protocol (RTP) packet count for call direction B to A.
- **Rule Name B -** The policy rule name for call direction B to A.
- **End Reason -** The end call reason.
- **Jitter Violation A -** The call RTCP jitter violations (%) for call direction A to B.
- **Jitter Violation B -** The call RTCP jitter violations (%) for call direction B to A.
- **RTD Violation A -** The call round trip delay violations (%) for call direction A to B.
- **RTD Violation B -** The call round trip delay violations (%) for call direction B to A.
- **Packet Loss Violation A -** The call packet loss violations (%) for call direction A to B.
- **Packet Loss Violation B -** The call packet loss violations (%) for call direction B to A.
- **MOS Violation A -** The call MOS violations (%) for call direction A to B.
- **MOS Violation B -** The call MOS violations (%) for call direction B to A.

- **RF Factor Violation A -** The call RF Factor Violation (%) for call direction A to B.
- **RF Factor Violation B -** The call RF Factor Violation (%) for call direction B to A.
- **Jitter Max A -** The call maximum jitter for call direction A to B.
- **Jitter Min A -** The call minimum jitter for call direction A to B.
- **Jitter Avg A -** The call average jitter for call direction A to B.
- **Jitter Max B -** The call maximum jitter for call direction B to A.
- **Jitter Min B -** The call minimum jitter for call direction B to A.
- **Jitter Avg B -** The call average jitter for call direction B to A.
- **RTD Max A -** The call maximum round trip delay for direction A to B.
- **RTD Min A -** The call minimum round trip delay for direction A to B.
- **RTD Avg A -** The call average round trip delay for direction A to B.
- **RTD Max B -** The call maximum round trip delay for direction B to A.
- **RTD Min B -** The call minimum round trip delay for direction B to A.
- **RTD Avg B -** The call average round trip delay for direction B to A.
- **Packet Loss Max A -** The call maximum packet loss (%) for call direction A to B.
- **Packet Loss Min A -** The call minimum packet loss (%) for call direction A to B.
- **Packet Loss Avg A -** The call average packet loss (%) for call direction A to B.
- **Packet Loss Max B -** The call maximum packet loss (%) for call direction B to A.
- **Packet Loss Min B -** The call minimum packet loss (%) for call direction B to A.
- **Packet Loss Avg B -** The call average packet loss (%) for call direction B to A.
- **RF Factor Max A -** The call maximum RF Factor for call direction A to B.
- **RF Factor Min A -** The call minimum RF Factor for call direction A to B.
- **RF Factor Avg A -** The call average RF Factor for call direction A to B.
- **RF Factor Max B -** The call maximum RF Factor for call direction B to A.
- **RF Factor Min B -** The call minimum RF Factor for call direction B to A.
- **RF Factor Avg B -** The call average RF Factor for call direction B to A.
- **MOS Max A -** The call maximum MOS for call direction A to B.
- **MOS Min A -** The call minimum MOS for call direction A to B.
- **MOS Avg A -** The call average MOS for call direction A to B.
- **MOS Max B -** The call maximum MOS for call direction B to A.
- **MOS Min B -** The call minimum MOS for call direction B to A.
- **MOS Avg B -** The call average MOS for call direction B to A.

Graphical View

You can view a graphical representation of Active Call Records by selecting a switch or switches in the table. By default, the data for "Jitter" is displayed in bar chart format. However, you can select a different variable from the **Variable** drop-down menu; and also change the display to a pie chart by selecting the "Pie" radio button in the **Chart Type** area.

One Touch Profile

The SIP One Touch Profile Screen displays all configured SIP One Touch Profiles, and is used to create, edit, delete, and apply One Touch Profiles. A Custom SIP Profile can be created and applied to switches on the network using the SIP Profile Tab. However, a SIP One Touch Profile is an easy way to automatically apply a default SIP Profile to traffic on SIP-enabled switches.

SIP One Touch Profile Parameters

When a SIP One Touch Profile is created and applied to a switch on the network, the following SIP configuration is applied to that switch:

Edge Devices

- The SIP Snooping Status is set to "Enabled" and the SOS Call Number values configured based on Media Type:
  - Voice - SOS Call Number 1 Field for the SOS Call Number.
  - Video - SOS Call Number 2 Field for the SOS Call Number.
  - Other - SOS Call Number 2 Field for the SOS Call Number.
- The Port Mode for all ports on the switch is set to "Automatic".
- The Port Status for all ports on the switch is set to "Enabled".
- A One Touch Policy Rule is created on the switch.

Non-Edge Devices

- The SIP Snooping Status is set to "Enabled" and the SOS Call Number values configured based on Media Type:
  - Voice - SOS Call Number 1 Field for the SOS Call Number.
  - Video - SOS Call Number 2 Field for the SOS Call Number.
  - Other - SOS Call Number 2 Field for the SOS Call Number.
- A One Touch Policy Rule is created on the switch.
- The user will have to manually set the Port Mode to Force-Edge/Force-Non-Edge from the CLI or by creating and assigning a custom SIP Profile using the SIP Profile Screen.

One Touch Policy Rule

The One Touch Policy Rule for different media types is detailed below.

- Voice
  - Policy Condition - sip audio
  - Policy Action - dscp 46
  - Policy Rule - OneTouchSIPRule$Voice condition OneTouchSIPCondition$Voice action OneTouchSIPAction$Voice
- Video
  - Policy Condition - sip video
  - Policy Action - dscp 34
  - Policy Rule - OneTouchSIPRule$Video condition OneTouchSIPCondition$Video action OneTouchSIPAction$Video

- Other
  - Policy Condition - sip other
  - Policy Action - dscp 24
  - Policy Rule - OneTouchSIPRule$Other condition OneTouchSIPCondition$Other action OneTouchSIPAction$Other

SIP One Touch Policy Rule Precedence

PolicyView enables you to define the precedence of policies created in PolicyView. A policy rule's precedence determines which policy will take effect in the rare case of a conflict.

- One Touch SIP Voice Policy Precedence is fixed at 50000.
- One Touch SIP Video Policy Precedence is fixed at 44000.
- One Touch SIP Other Policy Precedence is fixed at 44001.

Note the following for SIP Policies:

- Precedence for two policies can be the same.
- SIP Voice Precedence should be higher than Video/Other precedence.
- SIP Voice Precedence can overlap in One Touch Voice range.

  Note See the PolicyView Help for more information on Policy Precedence and Conflicts.

Creating a SIP One Touch Profile

SIP One Touch Profiles must be unique. You cannot create two profiles with the same name; and you cannot create duplicate profiles. Two profiles are considered duplicate if they have the same SIP Media Type and SOS Call Number. To create a SIP One Touch Profile, click on the Add icon. Click on one or more Media Types (Video, Voice, Other) and enter an SOS Call Number. When you are finished, click on the **Create** button. The profile will be created and stored in OmniVista.

After creating a profile, select the profile in the One Touch Profile List and click on the Apply to Devices button to apply the profile to specific network switches. The profile will be assigned to all ports on the selected switches.

> **Note:** The SIP snooping features allow the detection of emergency calls based on the “to” URI in the invite message. The SOS string must be the exact URI to be matched in the ‘to” URI; regular expressions are not supported.

Editing a SIP One Touch Profile

You can edit the SOS Call Numbers for a profile. Select a profile in the One Touch Profile List and click on the Edit icon. Edit the SOS Call Number(s) and click on the **Apply** button. The edited profile will be applied to any assigned switches/ports. Note that you cannot edit the profile name.

Deleting a SIP One Touch Profile

Select a profile in the One Touch Profile List, click on the Delete icon then click **OK** at the Confirmation Prompt. The profile will be deleted from the One Touch Profile List and from all assigned switches/ports.

Removing a SIP One Touch Profile

To remove an assigned One Touch Profile from specific switches/ports, select the profile in the SIP List and click on the **Apply to Devices** button. Select an option from the drop-down menu (Use Switch Picker or Use Topology) and click on the **Add/Remove Devices** button to select the switch(es) from which you want to remove the profile. Move the switch(es) from the Selected column and click on the **Apply** button.

> **Note:** Removing a SIP One Touch Profile from a switch does not change the global SIP Snooping Status, SOS call number, or port parameters.

Applying a SIP One Touch Profile

Select a profile in the One Touch Profile List and click on the **Apply to Devices** button. Select an option from the drop-down menu (Use Switch Picker or Use Topology) and click on the **Add/Remove Devices** button to select the switch(es) to which you want to apply the profile. Select a **Device Type** from the drop-down menu (Edge or Non-Edge) and click on the **Apply** button. The profile will be assigned to all ports on the selected switches.

> **Note:** You can only apply one (1) One Touch Policy to a switch. Only switches without an applied One Touch Policy will be available for selection. If you want to apply a new One Touch Policy to a switch, you must first remove the existing policy.
>
> **Note:** SIP Snooping is not supported in a Multi-Chassis configuration. If Multi-Chassis is configured on a 9000E Series device, that device will not be visible in the device list. If a device is configured in a Multi-Chassis configuration after opening the SIP application, assigning the device will result in an error Message. If Multi-Chassis is not configured and a device is not visible in the device list, the device must be polled so that its status is updated and it will appear in the list.

Viewing SIP One Touch Profiles

The One Touch Profile List displays information for all configured One Touch Profiles. Click on a profile in the list to display profile details, including the switches to which the profile was assigned, if applicable.

- **Profile Name -** The user-configured name for the profile
- **Video SOS Call -** The SOS Call Number for Video, if configured for the profile.
- **Voice SOS Call -** The SOS Call Number for Voice, if configured for the profile.
- **Other SOS Call -** The SOS Call Number for other media types, if configured for the profile.

SIP Profile

The SIP Profile Screen displays all configured SIP Profiles and is used create, edit, and delete SIP Profiles and apply profiles to switches/ports in the network. A SIP Profile is basically a "Master" Profile made up of "sub-profile" parameters configured using Global Params, Trusted Servers, Threshold, Threshold, TCP Port, UDP Port, and SOS Profile Screens.

Creating a SIP Profile

To create a SIP Profile, click on the Add icon, and enter a **SIP Profile Name**. Click on the "Add More Profiles" and select any sub-profile types you want to include. Select a sub-profile from a

drop-down. If necessary, click on the "Add New" link to go to a sub-profile page and create a new profile, then select the profile form the drop-down list. When you are finished, click on the **Create** button. The profile will be created and stored in OmniVista.

- **Global Params Profile -** Used to configure global SIP Profile parameters (e.g., DSCP marking, call thresholds) and enable/disable SIP Snooping.
- **Trusted Servers Profile -** Used to configure the IP addresses of the Trusted Servers. If a Trusted Server is configured, only the calls initiated through those servers are supported. If no Trusted Servers are configured, all SIP based calls using any call server are supported.
- **Threshold Profile -** Used to configure SIP Snooping threshold parameters (e.g., jitter, packet loss).
- **SOS Profile -** Used to configure SOS call strings.
- **TCP Port Profile -** Used to configure a TCP port(s) for SIP Snooping.
- **UDP Port Profile -** Used to configure a UDP port(s) for SIP Snooping.

After creating a profile, select the profile in the SIP Profile List and click on the Apply to Devices button to apply the profile to specific network switches/ports.

> **Note:** You can only have one of each sub-profile type in a SIP Profile. In other words, you cannot have two (2) different Trusted Server Profiles or two (2) different SOS Profiles.

Editing a SIP Profile

You can add/remove sub-profiles to/from a SIP Profile. Select a profile in the SIP Profile List and click on the Edit icon. You can select different sub-profiles, click on the Add More Profiles Link to add additional sub-profiles to the SIP Profile, or click on the "Remove" link next to a sub-profile to remove it from the SIP Profile. When you are finished, click on the **Apply** button. The profile will be updated and re-applied to any assigned switches/ports.

Deleting a SIP Profile

Select a profile in the SIP Profile List, click on the Delete icon then click **Yes** at the Confirmation Prompt. The profile will be deleted from the SIP Profile List and from all assigned switches/ports.

To remove an assigned SIP Profile from specific switches/ports, select the profile in the SIP List and click on the **Apply to Devices** button. Select an option from the drop-down menu (Use Switch Picker or Use Topology) and click on the **Add/Remove Devices** button to select the switch(es) from which you want to remove the profile. Move the switch(es) from the Selected column and click on the **Apply** button.

To remove the profile from specific ports, click on a switch and click on the **Add/Remove Ports** button to select the ports from which you want to remove the profile. Move the port(s) from the Selected column and click on the **Apply** button.

Applying a SIP Profile

Select a profile in the SIP Profile List and click on the **Apply to Devices** button. Select an option from the drop-down menu (Use Switch Picker or Use Topology) and click on the **Add/Remove Devices** button to select the switch(es) to which you want to apply the profile. Click on a switch

and click on the **Add/Remove Ports** button to select the ports to which you want to apply the profile. (You can also click on the "Add Port" link to bring up a list of ports for selection.)

By default, the Port Mode is set to "Automatic". To change the port mode, click on the "Device Config" Link for the switch to bring up the Device Configuration window and select a different Port Mode:

- **Automatic -** The port Edge/Non-Edge mode is derived from the switch based on LLDP received on the port.
- **Force Edge -** Media TCAM entries are created for dialogs that transverse the port.
- **Force Non-Edge -** Media TCAM entries are note created for dialogs that transverse the port.

Note that a port on a device will be considered as an Edge Port if:

- It is not connected through a link to any other port.
- It is connected through a link to another port on which LLDP is disabled.
- It has LLDP enabled and is connected through a link to another port on which LLDP is enabled and the remote capability advertised by that port is "None".

A port on a device will be considered as a Non-Edge port if:

- It has LLDP enabled and is connected through a link to another port on which LLDP is enabled and the remote capability advertised by that port is either "Bridge" or "Router".

When you are finished, click on the **Apply** button. The profile will be applied to the selected switch ports.

> **Note:** You can only apply one (1) SIP Policy to a switch. Only switches without an applied One Touch Policy will be available for selection. If you want to apply a new SIP Policy to a switch, you must first remove the existing policy.
>
> **Note:** SIP Snooping is not supported in a Multi-Chassis configuration. If Multi-Chassis is configured on a 9000E Series device, that device will not be visible in the device list. If a device is configured in a Multi-Chassis configuration after opening the SIP application, assigning the device will result in an error Message. If Multi-Chassis is not configured and a device is not visible in the device list, the device must be polled so that its status is updated and it will appear in the list.

Viewing SIP Profiles

The SIP Profile List displays information for all configured SIP Profiles. Click on a profile in the list to display profile details, including the switches to which the profile was assigned, if applicable.

- **SIP Profile Name -** The user-configured name for the SIP Profile.
- **SIP Profile Status**
  - **In Snyc -** The sub-profiles contained in the SIP Profile have not changed since the profile was created.
  - **Out of Sync -** A sub-profile contained in the SIP Profile as been edited since it was initially included in the SIP Profile. Any switches/ports to which the profile was initially applied will retain the original SIP Profile configuration until the profile is re-applied to the switches/ports.
  - **Unassigned -** The SIP profiled has not yet been applied to switches/ports.

- **Global Params Profile -** The name of the Global Parameters Profile contained in the SIP Profile. Global Parameters include SIP Snooping Enable/Disable, DSCP Marking, and Call Thresholds.
- **Trusted Servers Profile -** The name of the Trusted Servers Profile contained in the SIP Profile. A Trusted Server Profile contains IP addresses of Trusted Servers. If a Trusted Server is configured, only the calls initiated through those servers are supported. If no Trusted Servers are configured, all SIP based calls using any call server are supported.
- **UDP Ports Profile -** The name of the UDP Ports Profile contained in the SIP Profile. A UDP Ports Profile contains TCP Ports configured for SIP Snooping.
- **TCP Ports Profile -** The name of the TCP Ports Profile contained in the SIP Profile. A TCP Ports Profile contains TCP Ports configured for SIP Snooping.
- **Threshold Profile -** The name of the Threshold Profile contained in the SIP Profile. A Threshold Profile contains SIP Snooping threshold parameters (e.g., Jitter, Packet Loss).
- **SOS Profile -** The name of the SOS Profile contained in the SIP Profile. An SOS Profile contains a list of SOS call strings.

  Note: The SIP Profile Name only displays if a SIP Profile exists on the switch that completely matches the applied profile configuration; otherwise the SIP Profile Name field is blank.

Global Params Profile

The SIP Global Params Profile Screen displays all configured SIP Global Parameters Profiles and is used create, edit, and delete Global Parameter Profiles. A Global Parameters Profile can then be included in a SIP Profile and assigned to switches/ports in the network.

Creating a Global Parameters Profile

Global Parameter Profiles must be unique. You cannot create two profiles with the same name; and you cannot create duplicate profiles. Two Global Parameter Profiles are considered duplicate if they have the same DSCP Number, SOS Call DSCP Number, and Threshold Number of Calls values. To create a Global Parameters Profile, click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

- **Profile Name -** User-configured profile name (up to 32 characters).
- **DSCP Number-** The SIP Snooping DSCP number. By default, the packet gets its priority as normal packet (Range = 0 to 63). If the DSCP Number field is set to "0", the value is set as "NA" on switch.
- **SOS Call DSCP No. -** The SIP Snooping SOS Call DSCP No. (Range = 0 to 63)
- **Threshold No. of Calls -** The Number of call records that can be stored in flash (Range = 50 to 500)
- **Reserved Hardware Resource -** Reserved hardware resources required to program ACLs for media entries. Each value is a multiple of the default reserved hardware resources.
- **SIP CPU Rate Limit -** The rate limit of SIP PDUs trapping toward CPU (not applicable to SIP PDUs going towards network port).
- **SIP Snooping Status -** Use the drop-down menu to Enable/Disable SIP Snooping.

- **Clear Stats -** If set to "Yes", when the profile is assigned, existing SIP Statistics are cleared.

Editing a Global Parameters Profile

Select a profile in the Global Params Profile List and click on the Edit icon. Edit the fields as described above and click on the **Apply** button (note that you cannot edit the profile name). If you edit a Global Parameters Profile that is part of a SIP Profile, the SIP Profile will be labeled as "Out of Sync" on the SIP Profile Screen. Any device(s)/port(s) that the now-edited SIP Profile was applied to will retain its current SIP configuration until the SIP Profile is re-applied to those devices.

To apply the edited SIP Profile, go to the SIP Profiles Screen, select the SIP Profile that includes the edited Global Parameters Profile, and click on the **Apply to Devices** button. Select the device(s)s/port(s) to which you want to re-apply the updated SIP Profile, and click on the **Apply** button.

Deleting a Global Parameters Profile

Select a profile in the Global Params Profile List, click on the Delete icon then click **Yes** at the Confirmation Prompt. Note that you cannot delete a Global Parameters Profile that has been applied to a switch as part of a SIP Profile. You must first remove the SIP Profile from the switch.

Viewing Global Parameters Profiles

The Global Params Profile List displays information for all configured Global Parameter Profiles.

- **Profile Name -** User-configured profile name.
- **DSCP Number-** The SIP Snooping DSCP number. By default, the packet gets its priority as normal packet (Range = 0 to 63). If the DSCP Number field is set to "0", the value is set as "NA" on switch.
- **SOS Call DSCP No. -** The SIP Snooping SOS Call DSCP No. (Range = 0 to 63)
- **Threshold No. of Calls -** The Number of call records that can be stored in flash (Range = 50 to 500)
- **Clear Stats -** If set to "Yes", when the profile is assigned, existing SIP Statistics are cleared.
- **Reserved Hardware Resource -** Reserved hardware resources required to program ACLs for media entries. Each value is a multiple of the default reserved hardware resources.
- **SIP CPU Rate Limit -** The rate limit of SIP PDUs trapping toward CPU (not applicable to SIP PDUs going towards network port).

Trusted Servers Profile

The SIP Trusted Servers Profile Screen displays all configured Trusted Servers Profiles and is used create, edit, and delete Trusted Servers Profiles. If a Trusted Server is configured, only calls initiated through those servers are supported. If no Trusted Servers are configured, all SIP based calls using any call server are supported. You can configure up to eight (8) IP Addresses. A Trusted Server Profile can be included in a SIP Profile and assigned to switches/ports in the network.

Creating a Trusted Servers Profile

When creating a Trusted Servers Profile, the Profile Name, and at least one IP Address are required. Profiles must be unique. You cannot create two (2) profiles with the same name; and you cannot create duplicate profiles. Two Trusted Server Profiles are considered duplicate if they have the same IP Addresses in the same IP Address field. For example, if Profile 1 was created with IP Address 1 and IP Address 2 specified as 1.1.1.1 and 2.2.2.2; and Profile 2 was created with IP Address 1 and IP Address 2 specified as 1.1.1.1 and 2.2.2.2; and Profile 3 was created with IP Address 2 and IP Address 3 specified as 1.1.1.1 and 2.2.2.2; Profile 1 and Profile 2 would be duplicate profiles, but Profile 1 and Profile 3 would not.

> **Note:** When you apply a new Trusted Servers Profile as part of a SIP Profile it completely removes the previous Trusted Servers configuration on the switch and configures the Trusted Server IP Addresses provided in the new profile.

To create a Trusted Servers Profile, click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

- **Profile Name -** User-configured profile name (up to 32 characters).
- **IP Address List -** Enter a Trusted Server IP address and click on the Add icon. Repeat to add additional servers. You can configure up to eight (8) IP Addresses. At least one IP Address is required for the profile. “0.0.0.0” is considered as an invalid Trusted Server IP Address.

Editing a Trusted Servers Profile

Select a profile in the Trusted Servers Profile List and click on the Edit icon. Edit the fields as described above and click on the **Apply** button (note that you cannot edit the profile name). If you edit a Trusted Servers Profile that is part of a SIP Profile, the SIP Profile will be labeled as "Out of Sync" on the SIP Profile Screen. Any device(s)/port(s) that the now-edited SIP Profile was applied to will retain its current SIP configuration until the SIP Profile is re-applied to those devices.

To apply the edited SIP Profile, go to the SIP Profiles Screen, select the SIP Profile that includes the edited Trusted Servers Profile, and click on the **Apply to Devices** button. Select the device(s)s/port(s) to which you want to re-apply the updated SIP Profile, and click on the **Apply** button.

Deleting a Trusted Servers Profile

Select a profile in the Trusted Servers Profile List, click on the Delete icon then click **Yes** at the Confirmation Prompt. Note that you cannot delete a Trusted Servers Profile that has been applied to a switch as part of a SIP Profile. You must first remove the SIP Profile from the switch.

Viewing Trusted Servers Profiles

The Trusted Servers List displays information for all configured Trusted Servers Profiles.

- **Profile Name -** User-configured profile name.
- **IP Address List -** IP addresses of Trusted Servers included in the profile.

Threshold Profile

The SIP Threshold Profile Screen displays all configured Threshold Profiles and is used create, edit, and delete Threshold Profiles for SIP Snooping (e.g., jitter, packet loss). A Threshold Profile can be included in a SIP Profile and assigned to switches/ports in the network. (e.g., jitter, packet loss).

Creating a Threshold Profile

When creating a Threshold Profile, the Profile Name, at least one (1) medium (e.g., Audio, Video Other), and at least one of the performance parameter fields (e.g., Jitter, Packet Loss) are required. Profiles must be unique. You cannot create two profiles with the same name; and you cannot create duplicate profiles. Two Threshold Profiles are considered duplicate if they have the same values in the performance parameter fields (e.g., Jitter, Packet Loss). Follow the steps below to create a Threshold Profile.

To create a Threshold Profile, click on the Add icon and complete the fields for one or more medium as described below. When you are finished, click on the **Create** button.

- **Profile Name -** User-configured profile name (up to 32 characters).
- **Jitter -** The Jitter Threshold, in milliseconds (Range = 0 to 300, Defaults = Audio - 50, Video - 100, Other - 100).
- **Packet Loss -** The Packet Loss Threshold, in % (Range = 0 to 99, Defaults = Audio - 10, Video - 20, Other - 20).
- **Round Trip Delay -** The Round Trip Delay Threshold, in milliseconds (Range = 0 to 500, Defaults = 1Audio - 80, Video - 250, Other - 250).
- **R Factor -** The R-Factor Threshold, in milliseconds (Range = 0 - 100, Defaults = Audio - 70, Video - 80, Other - 80).
- **MOS** - The MOS Value Threshold (Range = 0 - 5, Defaults = Audio - 3.6, Video - 3.0, Other - 3.0). Note that the previous MOS range was 0 - 50. The current range of 0 - 5 represents 1/10th of the previous values.

  Note: Applying a new Threshold Profile will modify the threshold values for the specified performance parameter fields.

Editing a Threshold Profile

Select a profile in the Threshold Profile List and click on the Edit icon. Edit the fields as described above and click on the **Apply** button (note that you cannot edit the profile name). If you edit a Threshold Profile that is part of a SIP Profile, the SIP Profile will be labeled as "Out of Sync" on the SIP Profile Screen. Any device(s)/port(s) that the now-edited SIP Profile was applied to will retain its current SIP configuration until the SIP Profile is re-applied to those devices.

To apply the edited SIP Profile, go to the SIP Profiles Screen, select the SIP Profile that includes the edited Threshold Profile, and click on the **Apply to Devices** button. Select the device(s)s/port(s) to which you want to re-apply the updated SIP Profile, and click on the **Apply** button.

Deleting a Threshold Profile

Select a profile in the Threshold Profile List, click on the Delete icon then click **Yes** at the Confirmation Prompt. Note that you cannot delete a Threshold Profile that has been applied to a switch as part of a SIP Profile. You must first remove the SIP Profile from the switch.

Viewing Threshold Profiles

The Threshold Profile List displays information for all configured Threshold Profiles.

- **Profile Name -** User-configured profile name.
- **Jitter -** The Jitter Threshold, in milliseconds (Range = 0 to 300, Defaults = Audio - 50, Video - 100, Other - 100).
- **Packet Loss -** The Packet Loss Threshold, in % (Range = 0 to 99, Defaults = Audio - 10, Video - 20, Other - 20).
- **Round Trip Delay -** The Round Trip Delay Threshold, in milliseconds (Range = 0 to 500, Defaults = 1Audio - 80, Video - 250, Other - 250).
- **R Factor -** The R-Factor Threshold, in milliseconds (Range = 0 - 100, Defaults = Audio - 70, Video - 80, Other - 80).
- **MOS** - The MOS Value Threshold (Range = 0 - 5, Defaults = Audio - 3.6, Video - 3.0, Other - 3.0). Note that the previous MOS range was 0 - 50. The current range of 0 - 5 represents 1/10th of the previous values.

SOS Profile

The SIP SOS Profile Screen displays all configured SOS Profiles and is used create, edit, and delete SOS Profiles for SIP Snooping. A SOS Profile can be included in a SIP Profile and assigned to switches/ports in the network. (e.g., jitter, packet loss).

Creating an SOS Profile

When creating an SOS Profile, the Profile Name, and at least one SOS Call Number are required. Profiles must be unique. You cannot create two profiles with the same name; and you cannot create duplicate profiles. Two SOS Profiles are considered duplicate if they have the same SOS Call Number in the same SOS Call Number field. For example, if Profile 1 was created with SOS Call Number 1 and SOS Call Number 2 specified as abcd and 1234; and Profile 2 was created with SOS Call Number 1 and SOS Call Number 2 specified as abcd and 1234; and Profile 3 was created with SOS Call Number 2 and SOS Call Number 3 specified as abcd and 1234; Profile 1 and Profile 2 would be duplicate profiles, but Profile 1 and Profile 3 would not.

> **Note:** When you apply a new SOS Profile it completely removes the previous SOS Call Number configuration on the switch and configures the SOS Call Numbers provided in the new profile.

To create an SOS Profile, click on the Add icon and complete the fields for one or more medium as described below. When you are finished, click on the **Create** button.

- **Profile Name -** User-configured profile name (up to 32 characters).
- **SOS Call Number List -** Enter a call string for the profile and click on the Add icon. Repeat to add additional numbers. The SIP Snooping features allow the detection of emergency calls based on the “to” URI in the invite message. You can configure up to Configuration allows up to 4 SOS call strings. The string must be the exact URI to be

matched in the ‘to” URI; regular expression is not supported. By default, no SOS number is configured for SIP Snooping. (Allowed characters are a-z, A-Z, 0-9, @.)

Note: If the SOS Call Number field is left blank, when the profile is assigned to a switch, OmniVista will erase that SOS Call Number on the switch, if it existed previously.

Editing an SOS Profile

Select a profile in the SOS Profile List and click on the Edit icon. Edit the fields as described above. Click on Add icon and enter a number to add an additional number. Click on the Delete icon to remove an existing number. When you are finished, click on the **Apply** button (note that you cannot edit the profile name).

If you edit an SOS Profile that is part of a SIP Profile, the SIP Profile will be labeled as "Out of Sync" on the SIP Profile Screen. Any device(s)/port(s) that the now-edited SIP Profile was applied to will retain its current SIP configuration until the SIP Profile is re-applied to those devices.

To apply the edited SIP Profile, go to the SIP Profiles Screen, select the SIP Profile that includes the edited SOS Profile, and click on the **Apply to Devices** button. Select the device(s)s/port(s) to which you want to re-apply the updated SIP Profile, and click on the **Apply** button.

Deleting an SOS Profile

Select a profile in the SOS Profile List, click on the Delete icon then click **Yes** at the Confirmation Prompt. Note that you cannot delete an SOS Profile that has been applied to a switch as part of a SIP Profile. You must first remove the SIP Profile from the switch.

Viewing SOS Profiles

The SOS Profile List displays information for all configured SOS Profiles.

- **Profile Name -** User-configured profile name.
- **SOS Call Number List -** The SOS number(s) configured for the profile.

TCP Port Profile

The SIP TCP Port Profile Screen displays all configured TCP Port Profiles and is used create, edit, and delete TCP Port Profiles. A TCP Port Profile can be included in a SIP Profile and assigned to switches/ports in the network. You can configure up to eight (8) TCP Ports on SIP Snooping devices.

Creating a TCP Port Profile

When creating a TCP Port Profile, the Profile Name, and at least one TCP Port are required. Profiles must be unique. You cannot create two profiles with the same name; and you cannot create duplicate profiles. Two TCP Port Profiles are considered duplicate if they have the same TCP Port Number in the same TCP Port field. For example, if Profile 1 was created with TCP Port 1 and TCP Port 2 specified as 30 and 40; and Profile 2 was created with TCP Port 1 and TCP Port 2 specified as 30 and 40; and Profile 3 was created with TCP Port 2 and TCP Port 3 specified as 30 and 40; Profile 1 and Profile 2 would be duplicates, but Profile 1 and Profile 3 would not.

Note: When you apply a new TCP Port Profile it completely removes the previous TCP Ports configuration on the switch and configures the TCP Ports provided in the new profile.

To create a TCP Port Profile, click on the Add icon and complete the fields for one or more medium as described below. When you are finished, click on the **Create** button.

- **Profile Name -** User-configured profile name (up to 32 characters).
- **TCP Port List -** Enter a TCP Port Number for the profile and click on the Add icon. Repeat to add additional ports. You can configure up to eight (8) TCP Ports on SIP Snooping devices (Port Range 0 - 65535).

Editing a TCP Port Profile

Select a profile in the TCP Port Profile List and click on the Edit icon. Edit the fields as described above. Click on Add icon and enter a port to add an additional port. Click on the Delete icon to remove an existing port. When you are finished, click on the **Apply** button (note that you cannot edit the profile name).

If you edit a TCP Port Profile that is part of a SIP Profile, the SIP Profile will be labeled as "Out of Sync" on the SIP Profile Screen. Any device(s)/port(s) that the now-edited SIP Profile was applied to will retain its current SIP configuration until the SIP Profile is re-applied to those devices.

To apply the edited SIP Profile, go to the SIP Profiles Screen, select the SIP Profile that includes the edited TCP Port Profile, and click on the **Apply to Devices** button. Select the device(s)s/port(s) to which you want to re-apply the updated SIP Profile, and click on the **Apply** button.

Deleting a TCP Port Profile

Select a profile in the TCP Port Profile List, click on the Delete icon then click **Yes** at the Confirmation Prompt. Note that you cannot delete a TCP Port Profile that has been applied to a switch as part of a SIP Profile. You must first remove the SIP Profile from the switch.

Viewing TCP Port Profiles

The TCP Port Profile List displays information for all configured TCP Port Profiles.

- **Profile Name -** User-configured profile name.
- **TCP Port List -** The TCP Port(s) configured for the profile.

UDP Port Profile

The SIP UDP Port Profile Screen displays all configured UDP Port Profiles and is used create, edit, and delete UDP Port Profiles. A UDP Port Profile can be included in a SIP Profile and assigned to switches/ports in the network. You can configure up to eight (8) UDP Ports on SIP Snooping devices.

Creating a UDP Port Profile

When creating a UDP Port Profile, the Profile Name, and at least one UDP Port are required. Profiles must be unique. You cannot create two profiles with the same name; and you cannot create duplicate profiles. Two UDP Port Profiles are considered duplicate if they have the same UDP Port Numbers in the same UDP Port field. For example, if Profile 1 was created with UDP Port 1 and UDP Port 2 specified as 30 and 40; and Profile 2 was created with UDP Port 1 and

UDP Port 2 specified as 30 and 40; and Profile 3 was created with UDP Port 2 and UDP Port 3 specified as 30 and 40; Profile 1 and Profile 2 would be duplicates, but Profile 1 and Profile 3 would not.

> **Note:** When you apply a new UDP Port Profile it completely removes the previous UDP Ports configuration on the switch and configures the UDP Ports provided in the new profile.

To create a UDP Port Profile, click on the Add icon and complete the fields for one or more medium as described below. When you are finished, click on the **Create** button.

- **Profile Name -** User-configured profile name (up to 32 characters).
- **UDP Port List -** Enter a UDP Port Number for the profile and click on the Add icon. Repeat to add additional ports. You can configure up to eight (8) UDP Ports on SIP Snooping devices (Port Range 0 - 65535).

Editing a UDP Port Profile

Select a profile in the UDP Port Profile List and click on the Edit icon. Edit the fields as described above. Click on Add icon and enter a port to add an additional port. Click on the Delete icon to remove an existing port. When you are finished, click on the **Apply** button (note that you cannot edit the profile name).

If you edit an UDP Port Profile that is part of a SIP Profile, the SIP Profile will be labeled as "Out of Sync" on the SIP Profile Screen. Any device(s)/port(s) that the now-edited SIP Profile was applied to will retain its current SIP configuration until the SIP Profile is re-applied to those devices.

To apply the edited SIP Profile, go to the SIP Profiles Screen, select the SIP Profile that includes the edited UDP Port Profile, and click on the **Apply to Devices** button. Select the device(s)s/port(s) to which you want to re-apply the updated SIP Profile, and click on the **Apply** button.

Deleting a UDP Port Profile

Select a profile in the UDP Port Profile List, click on the Delete icon then click **Yes** at the Confirmation Prompt. Note that you cannot delete a UDP Port Profile that has been applied to a switch as part of a SIP Profile. You must first remove the SIP Profile from the switch.

Viewing UDP Port Profiles

The UDP Port Profile List displays information for all configured UDP Port Profiles.

- **Profile Name -** User-configured profile name.
- **UDP Port List -** The UDP Port(s) configured for the profile.

Device View

The SIP Device View Screen displays the SIP Profile configuration and SIP statistics for any SIP-enabled switch in the network. Select an option from the drop-down menu (Use Switch Picker/Use Topology) and click on the **Select Device** button to select a switch. Click on a profile type to view configuration information. The following SIP configuration information is displayed for the selected switch.

- SIP Profile
- TCP Port Profile
- UDP Port Profile
- Global Param Profile
- Trusted Server Profile
- Threshold Profile
- SOS Profile
- SIP Statistics

SIP Profile

- **SIP Profile Name -** The user-configured name for the SIP Profile.
- **SIP Profile Status**
  - **In Snyc -** The sub-profiles contained in the SIP Profile have not changed since the profile was created.
  - **Out of Sync -** A sub-profile contained in the SIP Profile as been edited since it was initially included in the SIP Profile. Any switches/ports to which the profile was initially applied will retain the original SIP Profile configuration until the profile is re-applied to the switches/ports.
  - **Unassigned -** The SIP profiled has not yet been applied to switches/ports.
- **Global Params Profile -** The name of the Global Parameters Profile contained in the SIP Profile. Global Parameters include SIP Snooping Enable/Disable, DSCP Marking, and Call Thresholds.
- **Trusted Servers Profile -** The name of the Trusted Servers Profile contained in the SIP Profile. A Trusted Server Profile contains IP addresses of Trusted Servers. If a Trusted Server is configured, only the calls initiated through those servers are supported. If no Trusted Servers are configured, all SIP based calls using any call server are supported.
- **UDP Ports Profile -** The name of the UDP Ports Profile contained in the SIP Profile. A UDP Ports Profile contains TCP Ports configured for SIP Snooping.
- **TCP Ports Profile -** The name of the TCP Ports Profile contained in the SIP Profile. A TCP Ports Profile contains TCP Ports configured for SIP Snooping.
- **Threshold Profile -** The name of the Threshold Profile contained in the SIP Profile. A Threshold Profile contains SIP Snooping threshold parameters (e.g., Jitter, Packet Loss).
- **SOS Profile -** The name of the SOS Profile contained in the SIP Profile. An SOS Profile contains a list of SOS call strings.

TCP Port Profile

- **Profile Name -** User-configured TCP Port Profile name.
- **TCP Port List -** The TCP Port(s) configured for the profile.

UDP Port Profile

- **Profile Name -** User-configured UDP Port Profile name (up to 32 characters).
- **UDP Port List -** The UDP Port(s) configured for the profile.

Global Param Profile

- **Profile Name -** User-configured Global Parameter Profile name.
- **DSCP Number-** The SIP Snooping DSCP number. By default, the packet gets its priority as normal packet (Range = 0 to 63). If the DSCP Number field is set to "0", the value is set as "NA" on switch.
- **SOS Call DSCP No. -** The SIP Snooping SOS Call DSCP No. (Range = 0 to 63)
- **Threshold No. of Calls -** The Number of call records that can be stored in flash (Range = 50 to 500)
- **Clear Stats -** If set to "Yes", when the profile is assigned, existing SIP Statistics are cleared.
- **Reserved Hardware Resource -** Reserved hardware resources required to program ACLs for media entries. Each value is a multiple of the default reserved hardware resources.
- **SIP CPU Rate Limit -** The rate limit of SIP PDUs trapping toward CPU (not applicable to SIP PDUs going towards network port).

Trusted Server Profile

- **Profile Name -** User-configured Trusted Server Profile name.
- **IP Address List -** IP addresses of Trusted Servers included in the profile.

Threshold Profile

- **Profile Name -** User-configured profile name.
- **Jitter -** The Jitter Threshold, in milliseconds (Range = 0 to 300, Defaults = Audio - 50, Video - 100, Other - 100).
- **Packet Loss -** The Packet Loss Threshold, in % (Range = 0 to 99, Defaults = Audio - 10, Video - 20, Other - 20).
- **Round Trip Delay -** The Round Trip Delay Threshold, in milliseconds (Range = 0 to 500, Defaults = 1Audio - 80, Video - 250, Other - 250).
- **R Factor -** The R-Factor Threshold, in milliseconds (Range = 0 - 100, Defaults = Audio - 70, Video - 80, Other - 80).
- **MOS** - The MOS Value Threshold (Range = 0 - 5, Defaults = Audio - 3.6, Video - 3.0, Other - 3.0). Note that the previous MOS range was 0 - 50. The current range of 0 - 5 represents 1/10th of the previous values.

SOS Profile

- **Profile Name -** User-configured profile name.
- **SOS Call Number List -** The SOS number(s) configured for the profile.

SIP Statistics

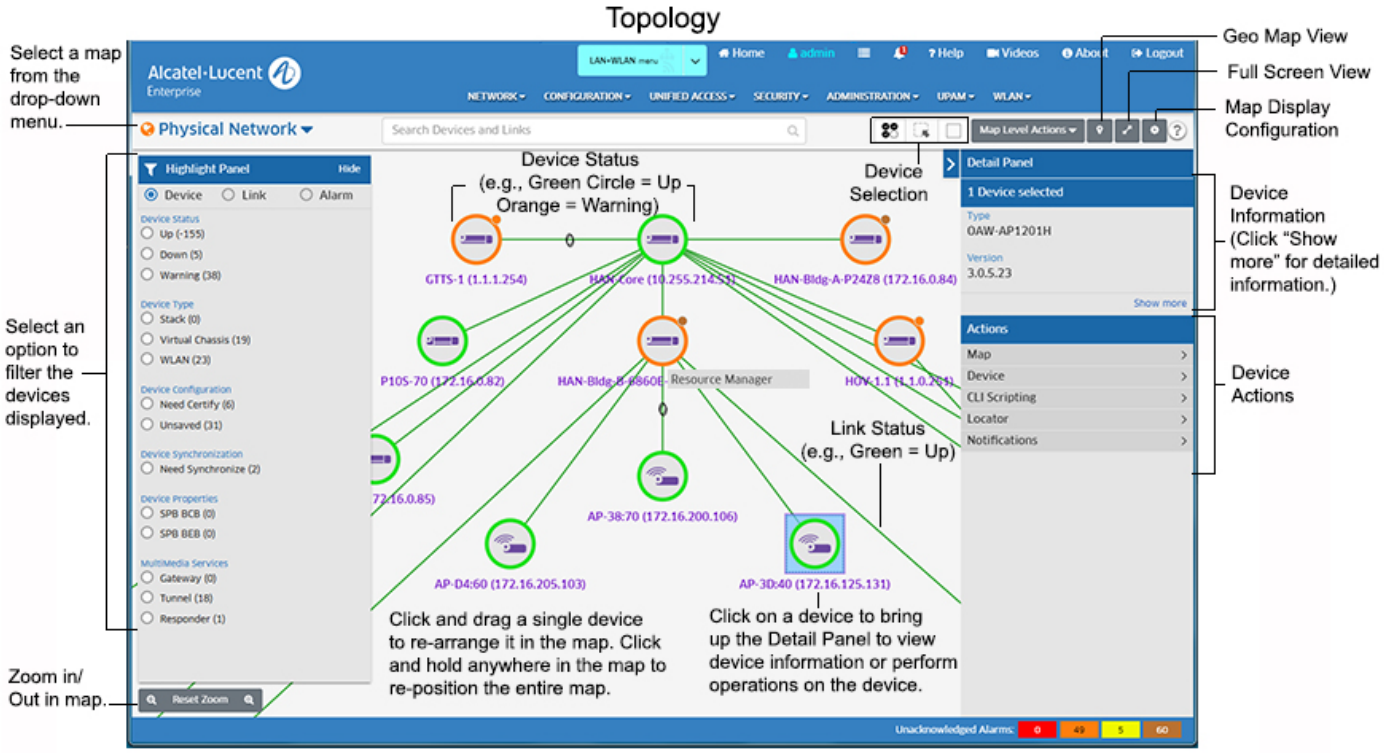
- **Total calls processed -** Total calls processed for SIP Snooping.
- **Total audio streams -** Total audio streams.
- **Total video streams -** Total video streams.

- **Total other streams -** Total other streams.
- **Total audio streams that crossed threshold -** Total audio streams that exceeded threshold.
- **Total video streams that crossed threshold -** Total video streams that exceeded threshold.
- **Total other streams that crossed threshold -** Total other streams that exceeded threshold.
- **Number of active calls -** Number of active calls.
- **Number of active audio streams -** Number of active audio streams.
- **Number of active video streams -** Number of active video streams.
- **Number of active other streams -** Number of active other streams.
- **Number of SIP packet received by hardware -** Number of SIP packets received by hardware.
- **Number of SIP packet received by software -** Number of SIP packets received by software.
- **Number of SIP packet received by per method -** Method by which the SIP packet was received (Invite, Ack, Bye, Update and Prack).
- **Number of SIP response packet received -** Number of SIP response packets received.
- **Number of discarded/malformed/unsupported SIP packets -** Number of discarded, malformed or unsupported SIP packets.
- **Number of discarded SIP packets not from/to trusted servers -** Number of discarded SIP packets not from or to trusted servers.
- **Number of dropped SIP packets due the software error -** Number of SIP packets dropped due the software error. (e.g., NI overflow, NI/CMM, CMM overflow).
- **Total Emergency Calls -** Total number of Emergency Calls.

31.0 Topology

The Topology application enables you to view the topology of all discovered devices in the network, view information about a specific device and perform certain actions on those devices (e.g., edit a device, telnet to a device, reboot a device). You can view devices in a topology map in various ways. For example, you can view devices in the Physical Network Map (default), and you can create custom maps that enable you to group and display devices in a way that is meaningful for your individual network configuration. You can also highlight specific devices or links, and re-arrange devices in a map and save that new map view. The figure below provides an overview of some of the functions that can be performed in the Topology application. Specific functions available when working with maps are detailed below. Devices must first be discovered using the Discovery application before they are displayed in Topology.

> **Note:** The default Topology Map view is the Geo Map view, which displays devices in their physical location on a geographical map. There are some device configuration options available in the Geo Map View; however most Topology device configuration options are available in the traditional Topology Map view shown below. When you first open OmniVista, the Geo Map view is displayed. Click on the Topology Map icon in the upper right corner of the Geo Map View to change to the traditional Topology view. You can also set the traditional Topology map view (shown below) as the default view on the Topology Configurations Screen.



The Physical Network Map (shown above) is the default map view. It is automatically created by OmniVista and displays all discovered network devices. The devices/maps you can see depend on your Role and permissions as configured in the Users and User Groups application (Security - Users and User Groups). You can also create maps, or configure dynamic maps. These maps are logical maps created from devices in the Physical Network Map.

Note: You can click on the **Map Level Actions** drop-down at the top of the screen and select **Go To Table View** to view a list all discovered devices on the Managed Devices Screen.

Note: If your network contains Stellar AP Series Devices, these devices are displayed in both the Physical Map and a Default AP Group Map that is also automatically created by OmniVista. See the AP Registration Help for more information.

Note: If any devices in the displayed map have unsaved configuration changes in their Working Directory, a number will appear in the Notification icon (Bell icon) at the top of the screen. The number of devices in this condition is displayed. Click on the **Save Now** button to save changes to the Working Directories of the devices. You can also click on the number of devices to highlight and view those devices in the map before saving the changes

Topology Maps

The Topology application not only provides an overview of the network, it can also be used to perform many functions that you can use to view and configure network devices. These functions are detailed in the following sections:

- Working with Topology Maps
- Viewing Map Information
  Devices
  Links
  Map Clusters
- Customizing Maps
  Customizing Map Colors
  Changing the Map Layout
  Adding Notes to Maps
- Selecting Devices
- Highlighting Devices/Links/Alarms
- Searching for Devices/Links
- Viewing Different Maps
- Viewing SPB Maps
- Viewing ERP Maps
- Working with Geo Maps
- Creating/Editing/Deleting Topology Maps
- Working with Network Devices
- Viewing Device Information
- Performing Device Actions

Working with Topology Maps

As mentioned earlier, the default Topology Map view is the Geo Map view, which displays devices in their physical location on a geographical map. There are some device configuration options available in the Geo Map View; however most Topology device configuration options are available in the traditional Topology Map view shown below. When you first open OmniVista, the Geo Map view is displayed. Click on the Topology Map icon in the upper right corner of the Geo Map View to change to the traditional Topology view. You can also set the traditional Topology map view (shown below) as the default view on the Topology Configurations Screen.

This section details the traditional Topology Map view. In this view, you can highlight devices or links by different criteria (e.g., device type, device admin state, link admin state, alarm severity), change the map layout, search for specific devices in the map, or create maps. Note that the maps that you can view and the tasks you can perform in Topology (e.g., creating maps, creating devices) depend on your User Role and User Group (e.g., Administrator, Network Administrator) as defined in the Users and User Groups application).

Viewing Map Information

Topology maps provide a visual representation of the network. The administrative status of the device or link is indicated by color (described below), and detailed information can be displayed by clicking on device or link.

You can click on the Map drop-down in the upper-left corner to view different maps. The "Globe" icon in the drop-down displays the status of the highest-level notification of any device in the map (e.g., if all devices in a map are "Up", the icon is green, if a device in a map is a "Warning" state, the icon is orange, if a device in a map is "Down", the icon is Red). Note that when you click on the Map drop-down, you can click on the Pin icon to keep the drop-down open. Click the Pin icon again to close it.

> **Note:** For a full screen view of Topology, click on the **Full Screen** icon in the top-right corner of the screen. Click the button again to return to the default view.

Devices

Each device type is displayed with a unique symbol as shown in the table below. Device status (e.g., Up, Down) is displayed by the device status circle around the device. Notifications status is displayed in a small circle in the upper-right corner of the device. This indicates the status of traps received for the device (e.g., Normal, Minor). Note that this Notifications status is only displayed if traps have been configured on the device.

Device Icons		
OS2260/OS2360	OS6560	OS9700/9700E
OS6200	OS6850/6850E	OS9900
OS6250	OS6855	OS10K
OS6350	OS6860/6860E/6865	Wireless Controller
OS6360	OS6900	Access Point
OS6400	OS9000/9000E	OAW Access Point
OS6450	Third-Party Device	

Hover the mouse over a device to display basic information. Click on a device to open the Detail Panel and view detailed information about the device.

Device Status

Device status is displayed by the device status circle around the device.

- **Green** = Device is "Up". For AOS devices, "Up" status does not necessarily mean that device is manageable from OmniVista. Refer to the "SNMP Status" column on

the Managed Devices page for management status. For Stellar APs and other devices, "Up" indicates that the device is "Up" and manageable from OmniVista.

- **Orange** = Warning (indicates that traps have been received from the device). The highest level of trap received by the device is displayed (Green, Orange, Red) in the Notifications Status).
- **Red** = Device is unreachable and cannot be managed by OmniVista. However, it may still be "Up" and functional in the network. Refer to the Device Status definition in the Manged Devices online help for more details.

Note: The colors above are the default Device Status colors. You can change the colors using the Network Status Screen in the Preferences application (Preferences - User Settings - Colors - Network Status).

Notifications Status

Notifications status displayed in the small circle in the upper right corner of the device, indicating the highest level of trap received by the device:

- **No Circle** = Alarm status is Normal.
- **Orange** = Alarm status is Warning.
- **Purple** = Alarm status is Minor.
- **Yellow** = Alarm status is Major.
- **Red** = Alarm status is Critical.

Note: The colors above are the default Notifications colors. You can change the colors using the Alarms Screen in the Preferences application (Preferences - User Settings - Colors - Alarms).

Note: If any device in a Child Map is in anything other than "Normal" status, a notifications status will be displayed on the Child Map icon. See Creating Maps for more information on Child Maps.

Links

Links between devices are displayed as a single line, whether there is a single link or multiple links.

- **Green -** Link is up. If there are multiple links, Green indicates **all** of the links are up.
- **Orange -** There are multiple links and at least one of the links is down. For example, only some of the ports of a linkagg are down while others are up; or one end of a link is up and the other end is down.
- **Red -** Link is down. If there are multiple links, Red indicates **all** of the links are down.
- **Blue -** Link status is unknown.

Note: After discovering devices via ping sweep, not all links will appear immediately. Some links may not be displayed. The links will be displayed after the next scheduled poll. To discover links immediately, you can manually poll links by selecting a device and using the Device - Poll Links action in the Actions Area of the Detail Panel.

Manual links are displayed as a dashed line if there is a single manual link or if there are multiple links and **all** of the links are manual. If there are multiple links and at least one is **not** a manual link, the link is displayed as a solid line. Aggregate links are displayed with an ellipse. Multi-Chassis links are displayed with a black border on the outer edge and an ellipse.

AP Mesh networks are displayed with Wi-Fi icons at endpoints between APs and a network symbol next to the Root AP in the network, as shown below.

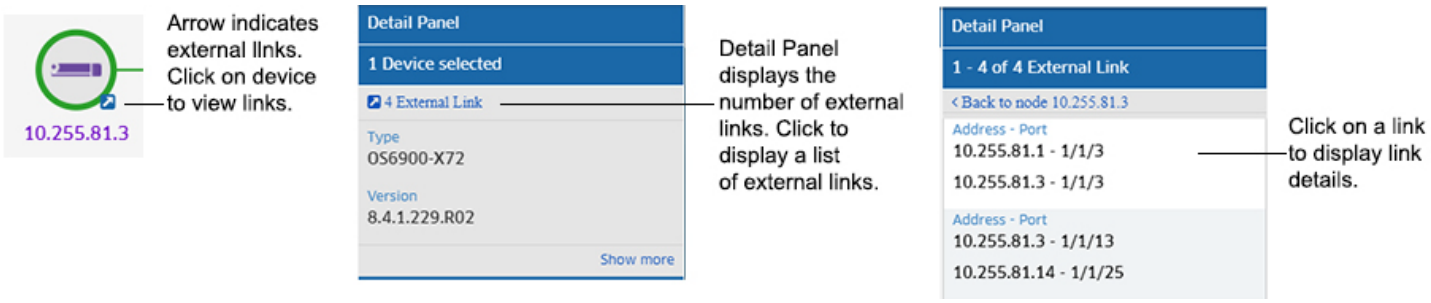
To display link information, move the mouse over the link until the pointer turns into a finger. Link information will be displayed in table form as shown below. The table displays information for all links.

You can also click on a link to display detailed link information. Move the mouse over the link until the pointer turns into a finger and click. The link is highlighted and link information is displayed in the Detail Panel. If it is a single link, the information is displayed for that link (as shown on the left below). If there are multiple links, a list of the links is displayed (as shown on the right). Click on a link to display details for the link. Click on the "Back" link to return to the list of links.

The information displayed varies depending on the link type.

- **Origin -** The origin of the link (LLDP, Manual).
- **IP Address 1-** The IP address of the first device in the link.
- **Slot/Port 1 -** The slot and port that connect the link on the first device, specified above.
- **LAG 1 -** If this is a link aggregation link, this field displays the Link Aggregation reference number assigned by the first device when the link aggregation group was created.
- **IP Address 2 -** The IP address of the second device in the link.
- **Slot/Port 2 -** The slot and port that connect the link on the second device, specified above.
- **LAG 2 -** If this is a link aggregation link, this field displays the Link Aggregation reference number assigned by the second device when the link aggregation group was created.
- **Ring ID -** The Ethernet Ring Protection (ERP) Ring ID, if applicable.
- **Link Type -** The link type (Copper or Fiber).
- **Speed -** The link speed.
- **Media Type -** The media type of the link.
- **Status -** The link status (Up, Down, Unknown).

Note that when viewing a map, devices linked to a device in another map display an External Link arrow icon, as shown below. When you click on one of these devices, a link to display a list of external links appears at the top of the Detail Panel (e.g., "1 External Link", "4 External Links"). Click to display a list of external links, then click on a link in the list to display link details.

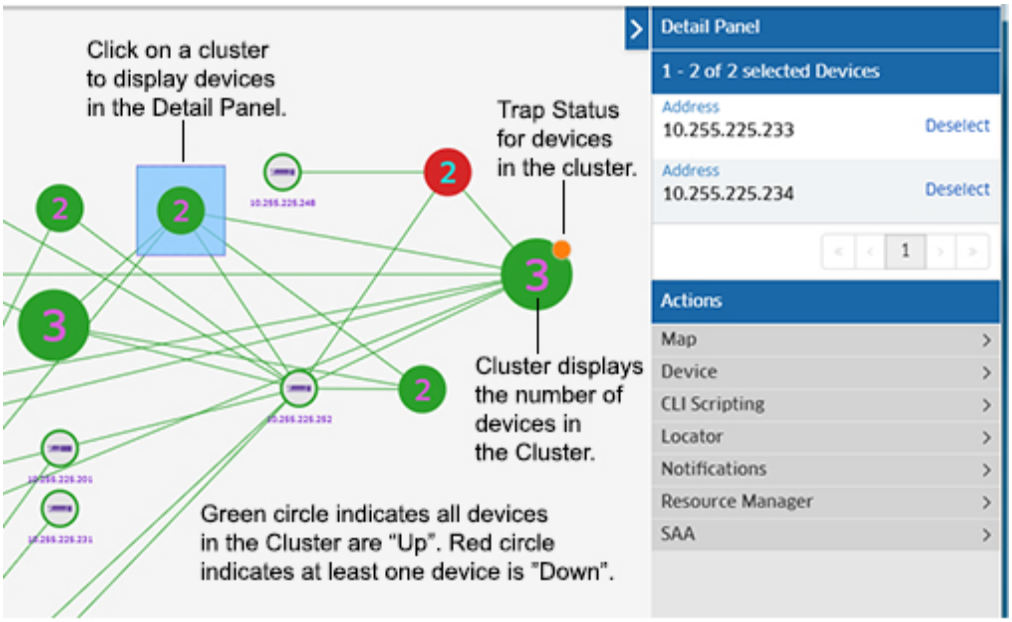


Note: The External Link detail display is not supported on Mesh AP Bridge External Links.

Map Clusters

When you zoom out for an overview of the network, devices are grouped into clusters, as shown below. Devices are grouped based on their proximity to each other in the map. Each cluster displays the status of devices in the cluster and the number of devices in the cluster, along with a Trap Status indicator at the top of the cluster. You can click on a cluster to display the devices contained in the cluster in the Detail Panel.

You can configure the minimum number of devices required to be displayed in a map to trigger the Clustering Feature. In other words, clustering will not be enabled unless there is this minimum number of devices in a map. The setting is found in the Topology Settings Screen.



If all devices in a cluster are "Up", the cluster circle displays in Green. If any device in the cluster is "Down", the cluster circle displays in Red. Click on a cluster to display all of the devices in the cluster in the Detail Panel. You can then click on a device to view device details or perform an action on the device.

The small circle at the top of the cluster displays the status of the highest severity trap generated by any device in the cluster. For example, if the highest-level severity trap for any device in the cluster is "Warning", the circle will be Orange. If the highest-level severity trap for any device in the cluster is "Critical", the circle will be Red. If all traps generated by all devices in

a cluster are "Normal", the Trap Status circle will not be displayed. The default trap status colors are shown below.

- **No Circle** = Alarm status is Normal.
- **Orange** = Alarm status is Warning.
- **Purple** = Alarm status is Minor.
- **Yellow** = Alarm status is Major.
- **Red** = Alarm status is Critical.

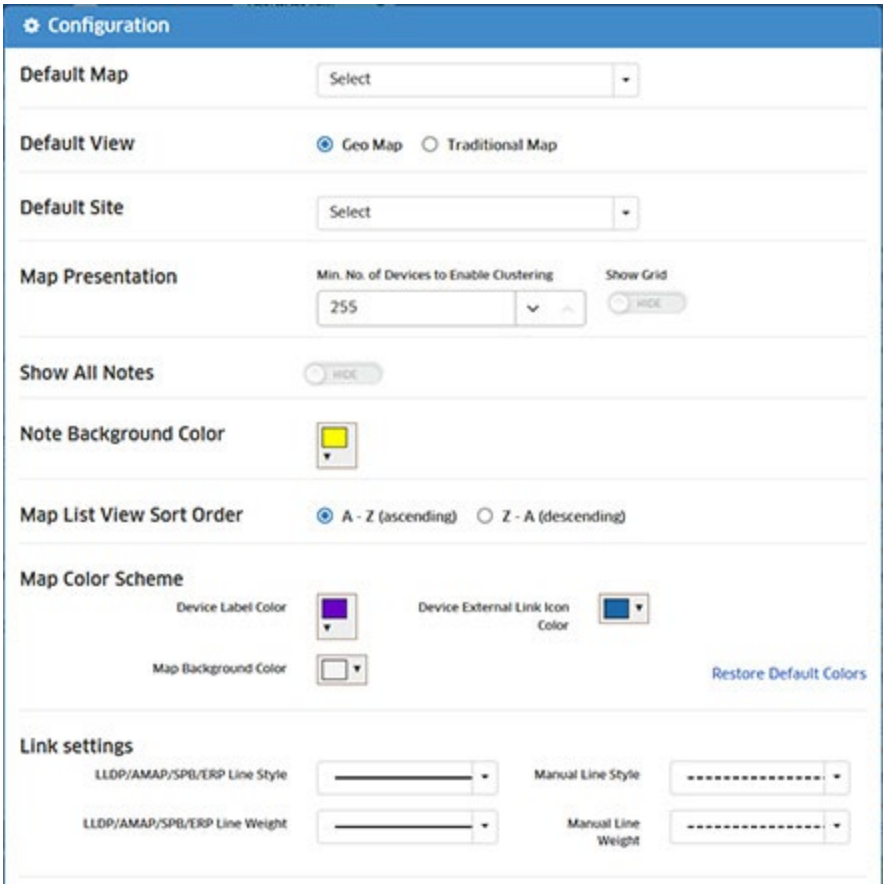
Note: You can change the default colors using the Alarms Screen in the Preferences application (Preferences - User Settings - Colors - Alarms).

Customizing Maps

You can customize the map display (e.g., Default Map, Map Color Scheme) and map layout.

Customizing the Map Display

You can change the default map preferences (e.g., Default View, map colors, link priority) by clicking on the Configuration icon at the top right corner of the map to bring up the Configuration Window (shown below). Set a preference(s) and click on the **Save** button. The changes will take effect immediately.



- **Default Map -** Used to set the default map displayed when you log into OmniVista. Select a map from the drop-down menu to set the default map. By default, the Geo Map is displayed.

- **Default View -** Used to set the default map view. You can set the default view or the Geo Map view. No matter which view you are in when using the Topology application, you can toggle between the views.
- **Default Site -** Used to set the default Geo Map Site that is displayed.
- **Map Presentation**
- **Min. No. of Devices to Enable Clustering -** The minimum number of devices that must be displayed on a map to trigger the Clustering Feature. In other words, clustering will not be enabled unless there is this minimum number of devices in a map. "1" will enable clustering for every map.
- **Show Grid -** Show or Hide the Topology Map Grid. When you move devices on a map, they snap to gridlines in the map to enable you to be more precise in your placement of the device in the map. By default, the gridlines are not shown. move the slider to Show, to display the gridlines on the map. Note that showing the gridlines will impact performance. It is recommended that the gridlines be shown only for arranging devices.
- **Show All Notes -** Set whether or not to display Map Notes.
- **List Map View Sort Order -** Used to set the default list order for maps in the Map drop-down menu alphabetically in ascending (A-Z) or descending (Z-A) order. You can always temporarily change the list order by clicking on the sort order in the Map drop-down menu. The order will return to the default setting when you navigate away from the Topology application.
- **Map Color Scheme -** Click on the arrow next to a field to configure a different color, click **Choose**, then click on the **Save** button. The changes take effect immediately.
- **Device Label Color -** The color of the label under a device (e.g., IP address).
- **Map Background Color -** The color of the background for all maps.
- **Device External Link Icon Color -** The color of the device external link icon. If a device in a map has a link to a device that is not in the currently-displayed map, a small arrow is displayed in the lower right corner of the device.
- **Link Settings -** Used to set the Line Style and Line Weight you want to use when displaying LLDP/AMAP/SPB/ERP Links and Manual Links.
- **Link Priority -** Used to set the order in which links are displayed in the Details Panel when a multiple link is selected on a map.
- **Ignore Manual Link -** If enabled, manual links will be hidden when LLDP and manual links exist between a set of ports when hovering the mouse over the link; and the manual links will not be displayed in the Detail Panel after clicking on the link.

Note: You can change the information e.g., IP address, Device Name, DNS Name) displayed under device on a map using the Device Naming Screen in the Preferences application (Administrator - Preferences - User Settings - Device Naming). This changes the how devices are identified and displayed in all applications in OmniVista.

Changing the Map Layout

You can change the basic layout of a map by clicking on the **Map Level Actions** drop-down and selecting one of the following:

- **Circular Layout -** Arranges all of the devices in a circular pattern.
- **Aligned Layout (Default) -** Arranges all of the devices in rows.

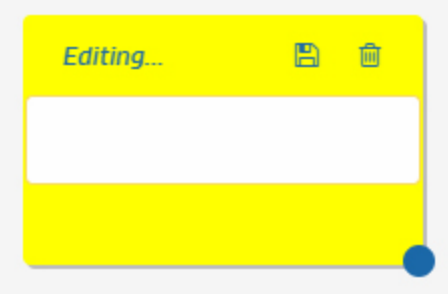
- **Circularize Connected Nodes -** Select a device in the map and click on this option to display all nodes connected to the selected device in a circular pattern.

You can also change the layout of a map by selecting a device and dragging it to a new location. You can also select multiple devices and move them. (Note that there is a built in gridline in all maps to enable you to be more precise in your placement of a device, and devices will snap to this gridline when moved.) Click on **Save Map** in the **Map Level Actions** drop-down to save the layout changes. You can also zoom in or out on a map using the Zoom control at the bottom of the map; and you can move an entire map on the screen by clicking anywhere outside the map and dragging the map to a new location on the screen.

> **Note:** If try to leave a map view or leave the Topology application without saving the new layout, you will be prompted to save it. Click **Save** at the confirmation prompt to save the new layout. The map will appear with the new layout the next time it is opened.

Adding Notes to Maps

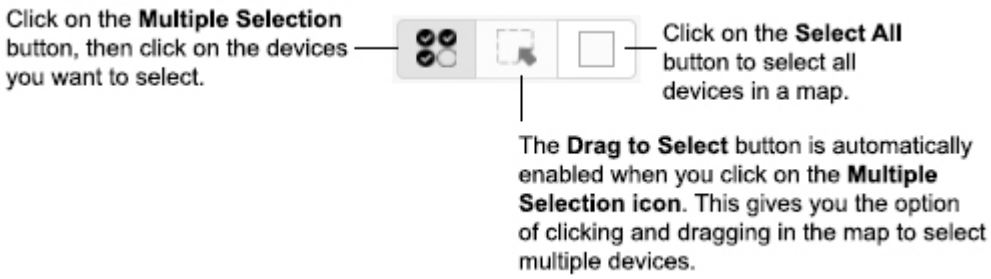
You can add notes to any Topology map. Click on the **Map Level Actions** drop-down and select **Add Note**.



Enter any text for the note, then click on the Save icon. You can resize the window and move the Note anywhere on the map. Once a Note has been added, you can edit it by clicking on the Edit icon in the Note. Click on the Delete icon, then click on **Delete This Note** at the Confirmation Prompt. You can hide notes by toggling the **Show All Notes** field on the Topology Configuration Window.

Selecting Devices

You can select a single device in a map to perform an action by clicking on the device. If you want to select multiple devices for an action, click on the **Multiple Selection** button at the top of the map, and click on the devices you want to select. When you click on the **Multiple Selection** button, the **Drag to Select** button is also enabled. At this point, you can either click on multiple devices to select them, or click and hold the mouse button to drag and select multiple devices. You can also select all devices in a map by clicking on the **Select All** button at the top of the map.



When you select multiple devices, the devices appear in a list in the Detail Panel on the right side of the screen (click on **Deselect** to remove a device from the list). You can then select an action (e.g., Copy Devices to Map, Poll for Traps, Reboot) to perform on the devices. Note that the actions available depend on the device type(s) selected and whether or not you select a single device or multiple devices.

Highlighting Devices/Links/Alarms

You can filter devices or links in a map by selecting one or more of Highlight criteria on the left side of the screen (Highlight Device, Highlight Link, Highlight Alarm). When you select one or more of the criteria (e.g., Status Up, Stack, Critical Alarm), only those devices/links matching the all of the selected criteria are displayed in the map. To return to the original map view, click on the "Clear" or "Clear All". You can filter devices/links based on the following criteria.

- **Device**
- Device Status
  Up
  Down
  Warning
- Device Type
  Stack
  Virtual Chassis
  WLAN
- Device Configuration
  Need Certify
  Unsaved
- Device Synchronization
  Need Synchronize
- Device Properties
  SPB BCB (Backbone Core Bridge)
  SPB BEB (Backbone Edge Bridge)
- Multimedia Services
  Gateway
  Tunnel
  Responder
- **Link**
- Link Status
  Up
  Down
- Link Type
  Aggregate
  Manual Link
  Discovered Link
  Mesh Link

- **Alarm**
- Critical
- Major
- Minor
- Warning
- Normal

Searching for Devices/Links

You can search for a device(s) or link(s) in the currently displayed map or in all maps. Click on the "Search Devices and Links" area at the top of the screen to see a list of search criteria that you can search on (e.g., IP address, MAC address, Link Title, IP address 1). By default, the "Limit search to the current map" checkbox is enabled. If you want to search in all maps, de-select the checkbox.

Enter the search information. Any device(s)/link(s) matching the criteria will be displayed in a list below the Search area. Click on an item to highlight the device/link in the map. Click on the x in the "Search" area to delete the search criteria and begin a new search.

Viewing Different Maps

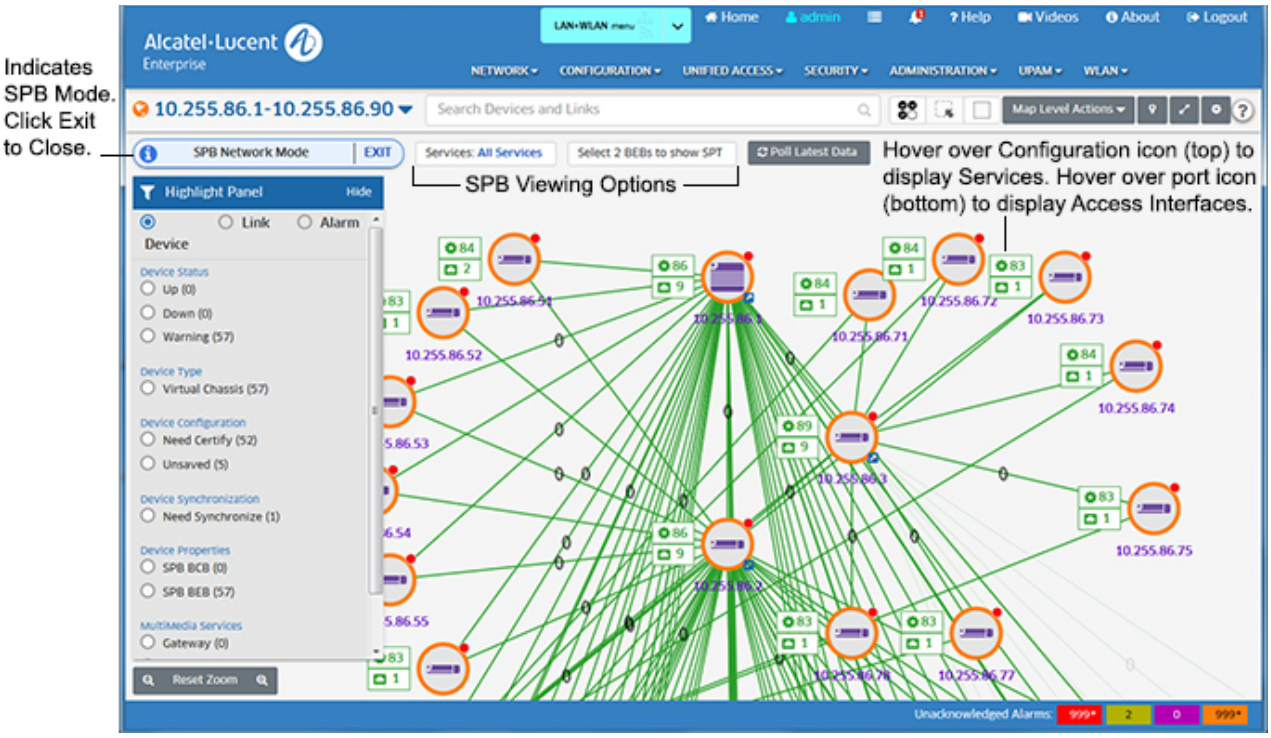
The Map drop-down in the upper-left corner of the screen displays the name of the current map. To change to a different map, select the map from the drop-down menu. You can also search for a specific map in the list.

Viewing SPB Maps

OmniSwitch 8.x Devices support Shortest Path Bridging MAC (SPBM) as defined in the IEEE 802.1aq standard. SPBM uses the Provider Backbone Bridge (PBB) network model to encapsulate (using IEEE 802.1ah headers) and tunnel customer traffic through the network backbone. The shortest path trees upon which the PBB network infrastructure operates are determined using a version of the Intermediate System-to-Intermediate System (IS-IS) link state protocol that supports TLV extensions for SPB (ISIS-SPB).

The SPBM network topology consists of two layers: the backbone infrastructure (control plane) layer and the services (data plane) layer. ISIS-SPB builds the backbone layer by defining loop-free, Shortest Path Trees (SPT) through the backbone network. The service layer is based on the PBB framework as defined in the IEEE 802.1ah standard. SPBM supports the 802.1ah MAC-in-MAC method for data encapsulation. SPBM services transport the encapsulated traffic over the ISIS-SPB infrastructure.

OmniVista displays SPB configurations on the network; however, SPB is configured on an OmniSwitch using the CLI. For more information on configuring SPB, see the *OmniSwitch AOS Network Configuration Guide*. Within the Topology application, you can view a map of all SPB-configured switches within a map, including SPB Services and SPT link information for devices by BVLAN. To bring up an SPB Map, click on the **Map Level Actions** drop-down at the top of the screen and select **SPB Network**. The map displays an overlay of the SPB-configured devices and links, as shown below.



As shown above, "SPB Network Mode" is displayed in the upper left corner. By default, all devices/links for all services are displayed (the "Services" link at the top of the screen displays "All Services"). The boxes next to each switch display the number of SPB Services (Configuration icon) and the number of Access Interfaces (Port icon) configured on the switch. You can hover the mouse over the boxes to view detailed information. In addition, each SPB Services and Access Interfaces box is color coded:

- **Green -** All SPB Services/Access Interfaces are up.
- **Orange -** If multiple SPB Services/Access Interfaces are configured, at least one is down.
- **Red -** If a single SPB Service/Access Interface is configured, it is down. Or, if multiple SPB Services/Access Interfaces are configured, all are down.

All of the map viewing and action options (e.g., highlight devices, view device/link information, perform actions on devices) are available on the SPB Map). To exit SPB Mode and return to the current map, click on **EXIT** in the "SPB Network Mode" bar (or click on the **Map Level Actions** drop-down and select **Exit SPB Network**).

> **Note:** If you zoom out on an SPB Map, clusters are created based on the current map. In other words, a cluster may contain both SPB devices and non-SPB devices.

SPB Configuration Viewing Options

When an SPB Map is displayed, different viewing options are available to display detailed configuration information. Hover the mouse over the Configuration icon (top icon) or the Port icon (bottom icon) next to a switch to display detailed information about SPB Services and Access Interfaces configured on a switch. Click on the "All Services" link and select a service to view SDP and SAP information for a specific SPB Service in the network. You can also view SPT links between devices for specific BVLANS, and view link information for Layer 2 Switches connected to a SAP.

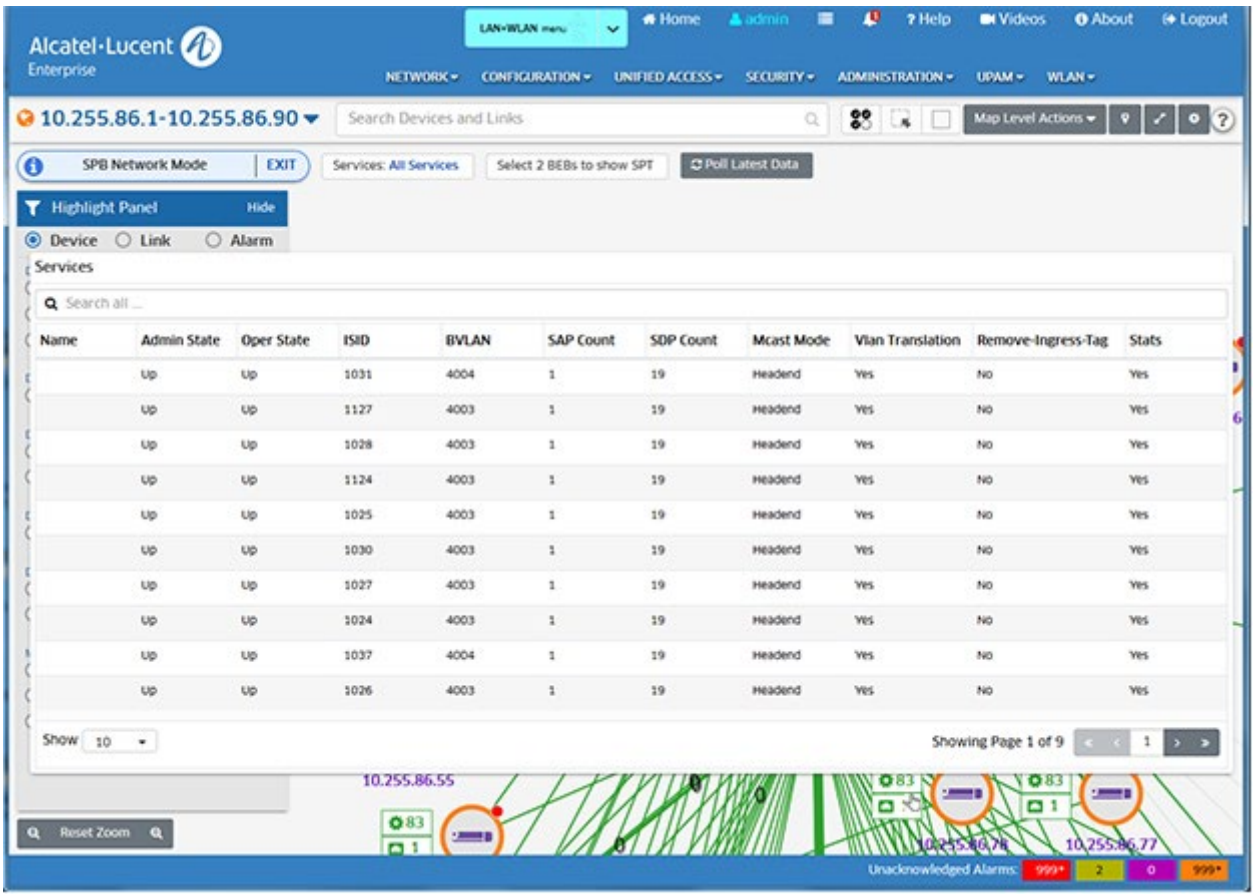
Note: By default, OmniVista is automatically scheduled to poll switches for SPB information every 3 hours. To perform an immediate poll, click on the Poll Latest Data button at the top of the screen to poll switches and update the SPB information displayed on the screen.

View SPB Service Information on a Device

You can quickly view information about SPB Services and Access Interfaces configured on a switch. The icons next to each switch in the map display the number of SPB Services (Configuration icon) and the number of Access Interfaces (Port icon) configured on the switch. Hover the mouse over the Configuration icon to display the Services Table. Hover the mouse over the Port icon to display the Access Interfaces Table.

Services Table

The Services Table displays information about all SPB Services configured on a switch. To view information, hover the mouse over the Configuration icon. The Services Table appears, as shown below. You can enter search criteria in the search field at the top of the table to search for specific information, or scroll through the pages in the table by clicking on the arrows at the bottom of the table.

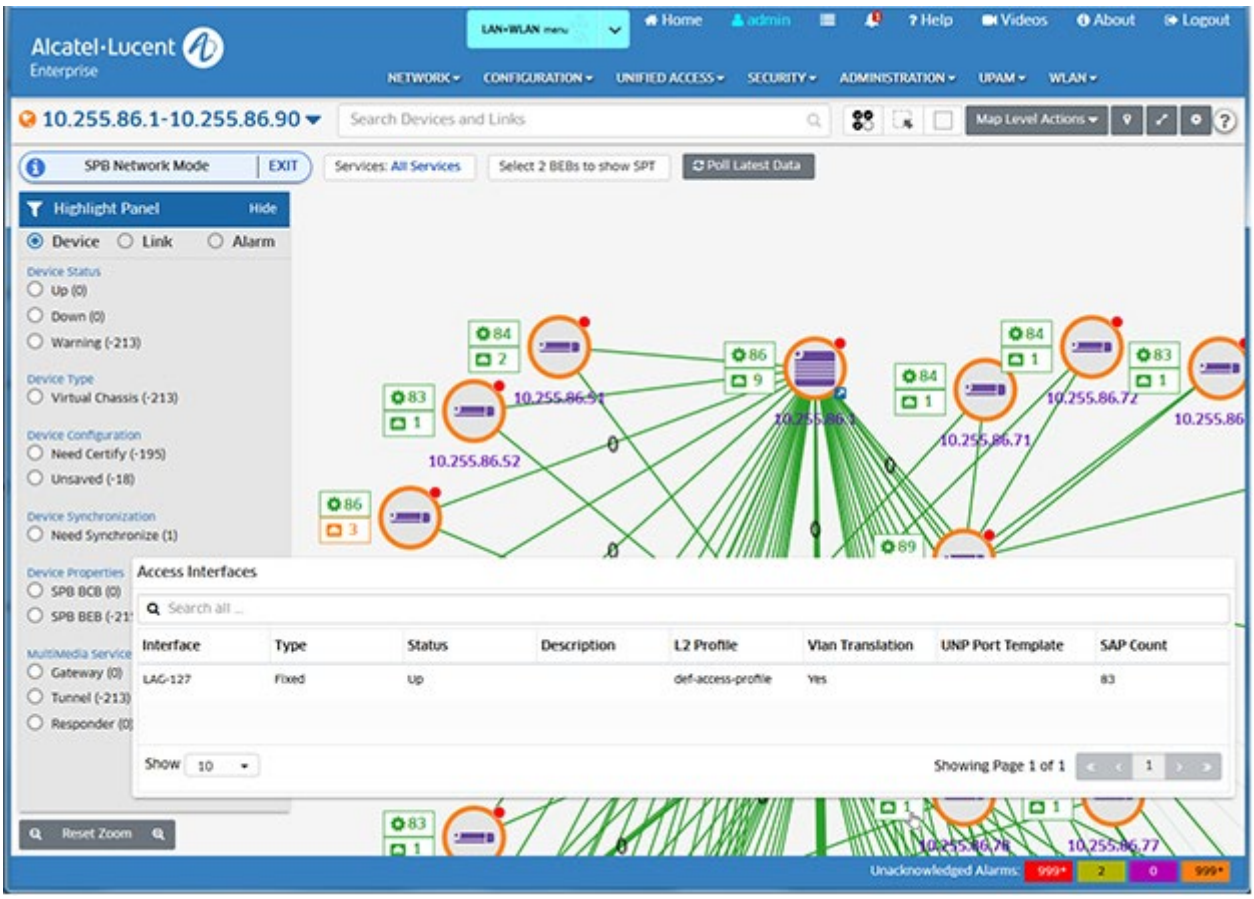


- **Name -** The name of the SPB Service.
- **Admin State -** The administrative state of the SPB Service (Up/Down).
- **Oper State -** The operational state of the SPB Service (Up/Down).

- **ISID -** The Service Instance Identifier that identifies the SPB service instance within the Provider Backbone Bridging (PBB) network.
- **BVLAN -** The VLAN ID number for the Backbone VLAN to which the SPB Service is mapped.
- **SAP Count -** The number of Service Access Points (SAPs) associated with the SPB Service.
- **SDP Count -** The number of Service Distribution Points (SDP) associated with the SPB Service.
- **Mcast Mode -** The multicast replication mode (Headend or Tandem) for the SPB Service.
- **VLAN Translation -** Whether or not VLAN translation is enabled for the SPB Service (Yes or No).
- **Remove Ingress Tag -** Whether or not the customer VLAN tag is removed before the packet is encapsulated for the SPB Service (Yes or No).
- **Stats -** Whether statistics collection is enabled for the SPB Service (Yes or No).

Access Interfaces Table

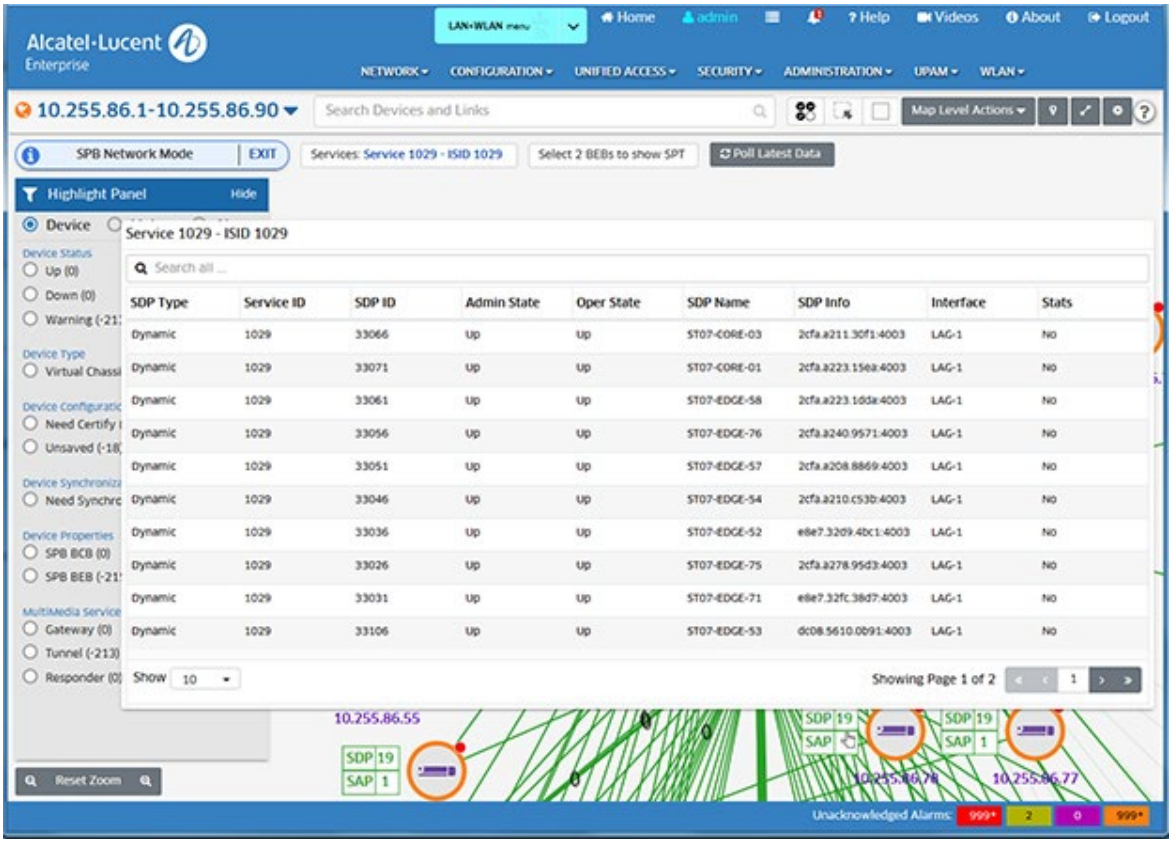
The Access Interfaces Table displays the access (customer-facing) port configuration for the switch. To view information about Access Interfaces configured on a switch, hover the mouse over the Port icon. The Access Interfaces Table appears, as shown below. You can enter search criteria in the search field at the top of the table to search for specific information, or scroll through the pages in the table by clicking on the arrows at the bottom of the table.



- **Interface -** The access slot/port number or link aggregate ID number.
- **Type -** Whether or not the SAP associated with the access port was created statically or dynamically (Fixed or Dynamic).
- **Status -** The status of the link connection to the access port (Up or Down).
- **Description -** An optional description configured for the access port. By default, the description is blank.
- **L2 Profile -** The Layer 2 profile associated with the access port.
- **VLAN Translation -** Whether or not VLAN translation is enabled on the access port (Yes or No).
- **UNP Port Template -** The UNP Port Template assigned to the interface.
- **SAP Count -** The number of Service Access Points (SAPs) that are associated with the access port.

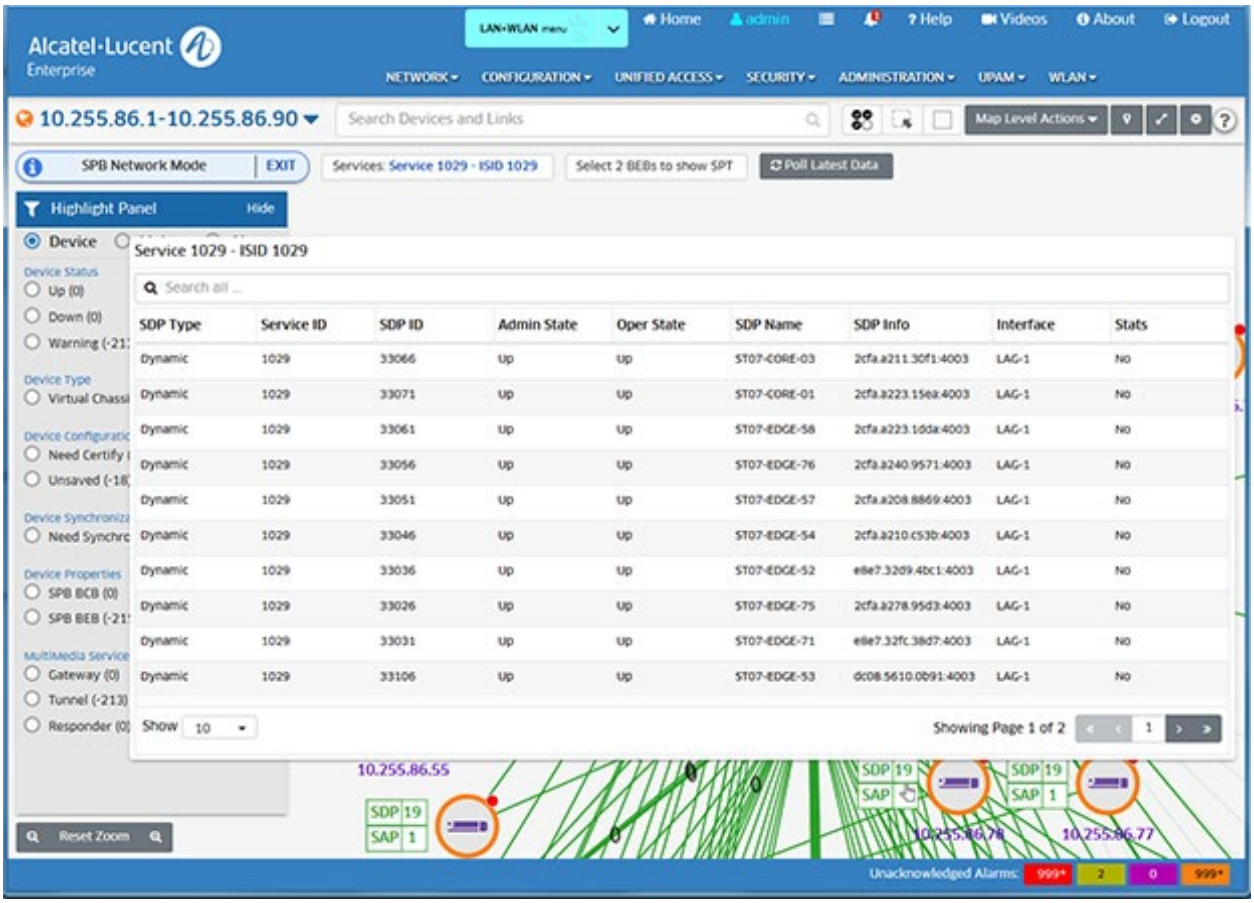
View SDP and SAP Information for a Service

You can view Service Distribution Point (SDP) and Service Access Point (SAP) information for a specific SPB Service on the network. Click on the "All Services" link at the top of the screen. A list of all SPB Services configured on the network is displayed. Select a service from the list. Switches on which the selected service is configured are displayed and other devices in the network are grayed out, as shown below. The boxes next to each switch now display the number of Service Distribution Points (SDP) and Service Access Points (SAP) configured on a switch. Hover the mouse over the SDP box to view Service Distribution Point information for the switch. Hover the mouse over the SAP box to view Service Access Point Information for the switch.



SDP Information

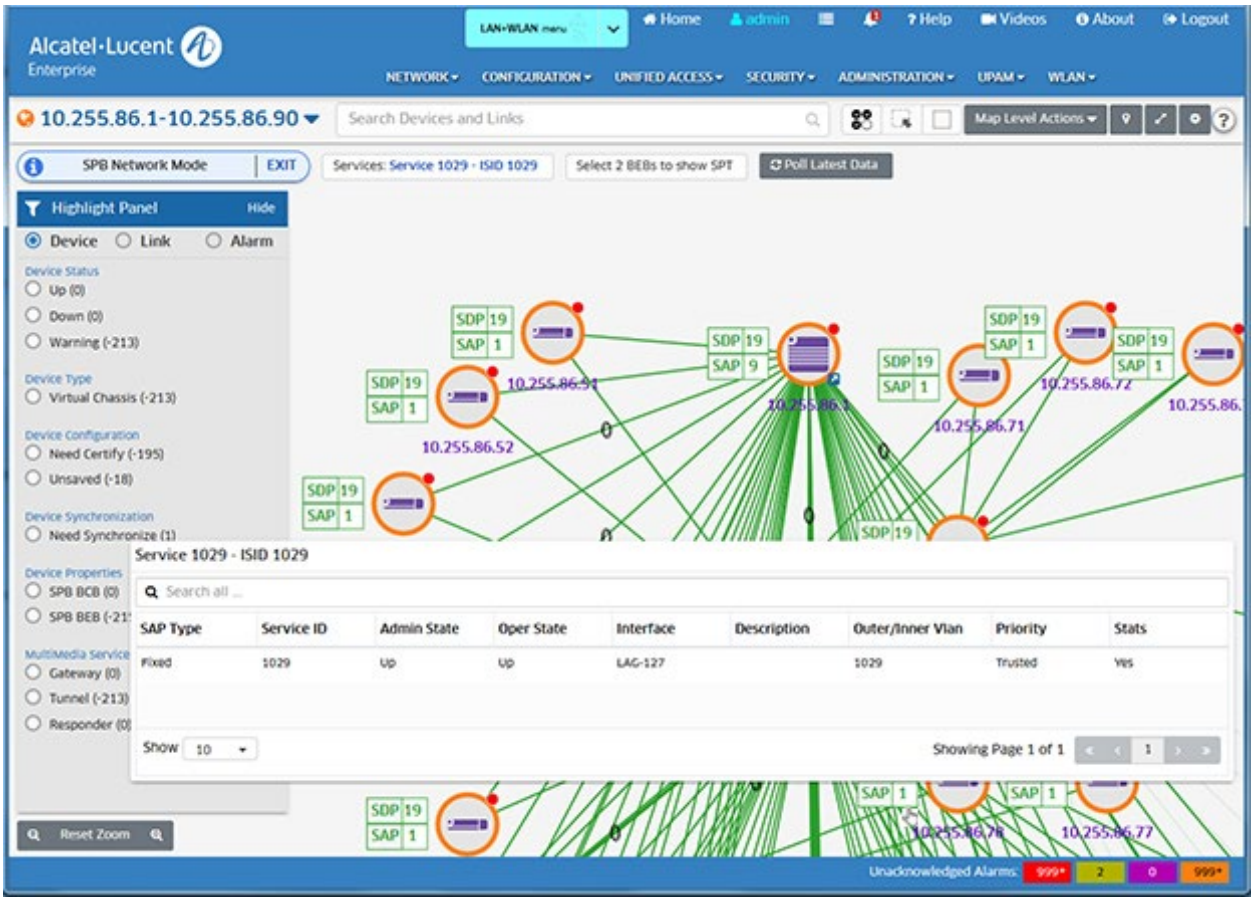
The SDP Table displays detailed Service Distribution Point (SDP) information for a switch. To view information, hover the mouse over the SDP box next to a switch. The SDP Table appears, as shown below. You can enter search criteria in the search field at the top of the table to search for specific information, or scroll through the pages in the table by clicking on the arrows at the bottom of the table.



- **SDP Type -** Whether or not the SDP was created statically or dynamically (Fixed or Dynamic).
- **Service ID -** The SPB Service ID.
- **SDP ID -** A unique, dynamically-generated SDP identification number.
- **Admin State -**The administrative status of the SDP (Up or Down).
- **Oper State -** The operational status of the SDP (Up or Down).
- **SDP Name -** User-configured name for the SDP.
- **SDP Info** - The System ID (BMAC) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.
- **Interface -** The SPB interface (network port) on which ISIS-SPB discovered the neighbor BMAC and BVLAN.
- **Stats -** Whether or not statistics collection is enabled for the SPB Service (Yes or No).

SAP Information

The SAP Table displays detailed information for the Service Access Point(s) (SAP) on a switch. To view information, hover the mouse over the SAP box next to a switch. The SAP Table appears, as shown below. You can enter search criteria in the search field at the top of the table to search for specific information, or scroll through the pages in the table by clicking on the arrows at the bottom of the table.

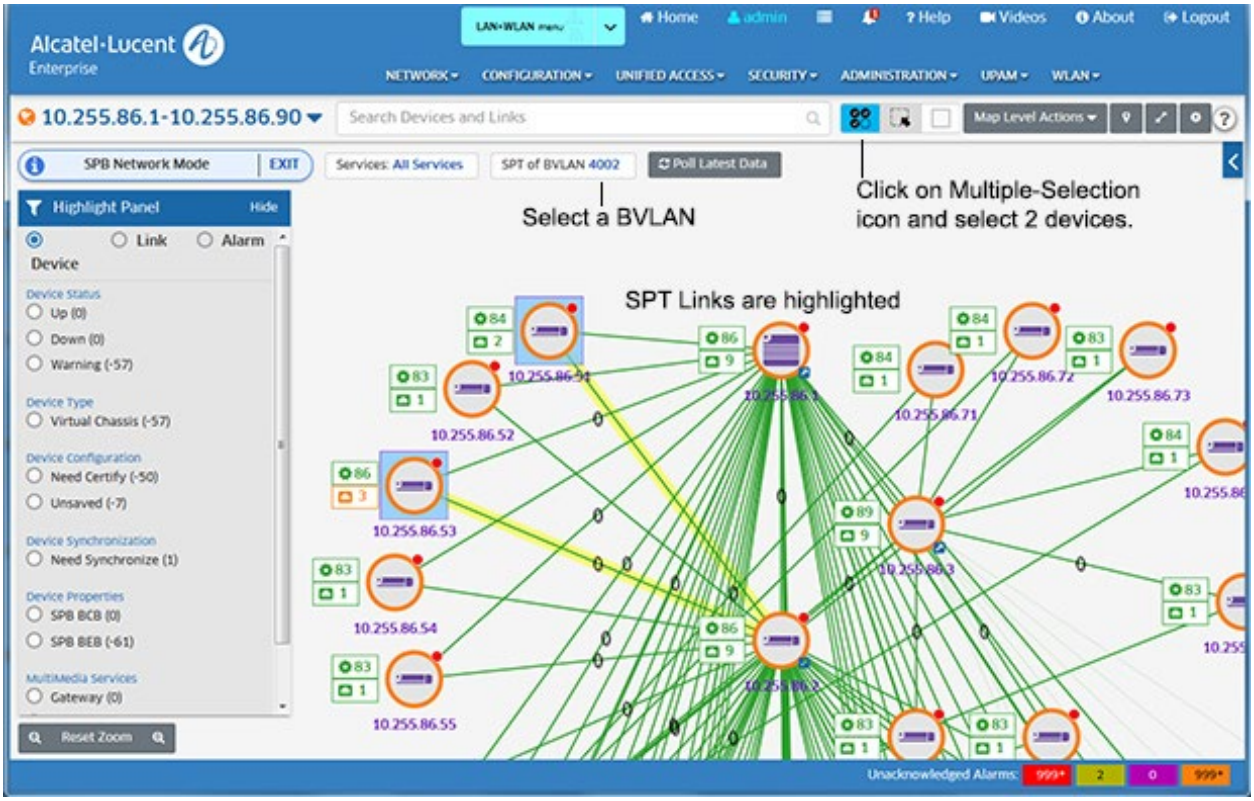


- **SAP Type -** Whether or not the SAP was created statically or dynamically (Fixed or UNP).
- **Service ID -** The SPB Service ID.
- **Admin State -** The administrative state of the SAP (Up or Down).
- **Oper State -** The operational state of the SAP (Up or Down).
- **Interface -** The bridge interface (port or link aggregate) of the virtual port that is associated with the service.
- **Description -** An optional description configured for the SPB Service.
- **Outer/Inner VLAN -** The Outer Tag (Service Tag)/the Inner Tag (Customer Tag). For a SAP, OmniVista can manage 1/1/X:0 or 1/1/x:Inner VLANs or 1/1/x:Inner VLANs. For Outer VLANs, a single VLAN is displayed if there is one Outer VLAN, two VLANs are displayed if there is an Inner and and Outer VLAN. No VLAN is displayed if the traffic is untagged.
- **Priority -** Whether or not the SAP virtual port associated with the service is trusted or assigns a priority value (Trusted or Untrusted).

- **Stats -** Whether or not statistics collection is enabled for the SPB Service (Yes or No).

View SPT Links

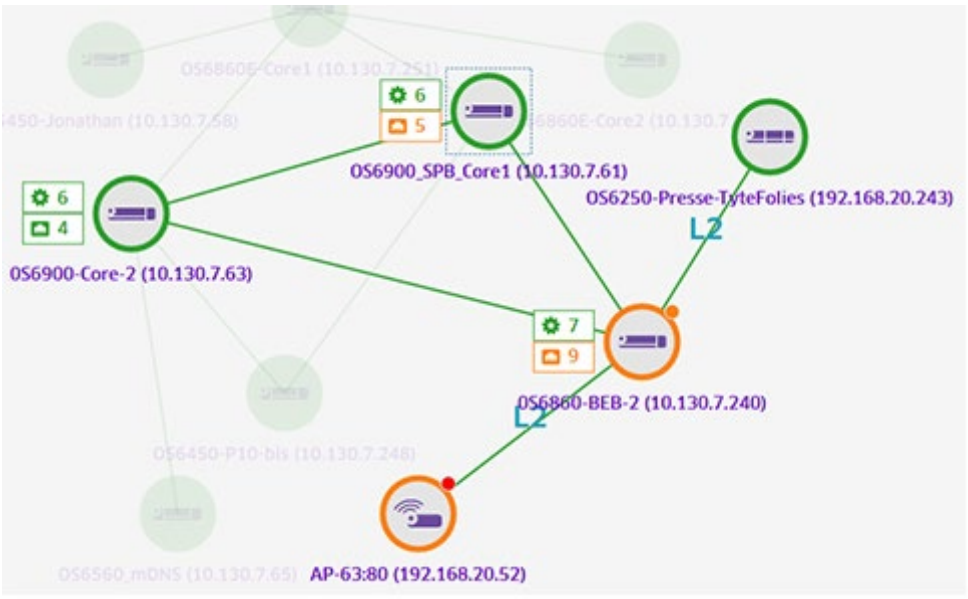
You can view SPT link information between switches. Click on the Multiple Selection icon at the top of the screen and select two switches. (Note that you can use the "SPB BEB" filter in the Highlight Panel to highlight all BEB Switches.) The "Select 2 Backbone Edge Bridges (BEB) to show SPT" field will display "SPT of BVLAN". Click on the "Select BVLAN" link and select a BVLAN. The link paths are highlighted in yellow, as shown below. You can hover over a link to display link information or click on the link to view link information in the Detail Panel.



Notes: SPT links are updated automatically based on the polling setting configured in the Discovery application (Discovery - Settings - Frequencies - Regular Updates). SPT links are also updated whenever you manually re-discover devices. Also note that if a device in an SPT is "down", OmniVista will continue to display the SPT through the "down" device until the next poll. Once the poll is complete, OmniVista will display the updated SPT between the switches. You can also perform a manual poll of all devices in the SPB network by clicking on the **Poll Latest Data** button.

View Link Information for Layer 2 Switches

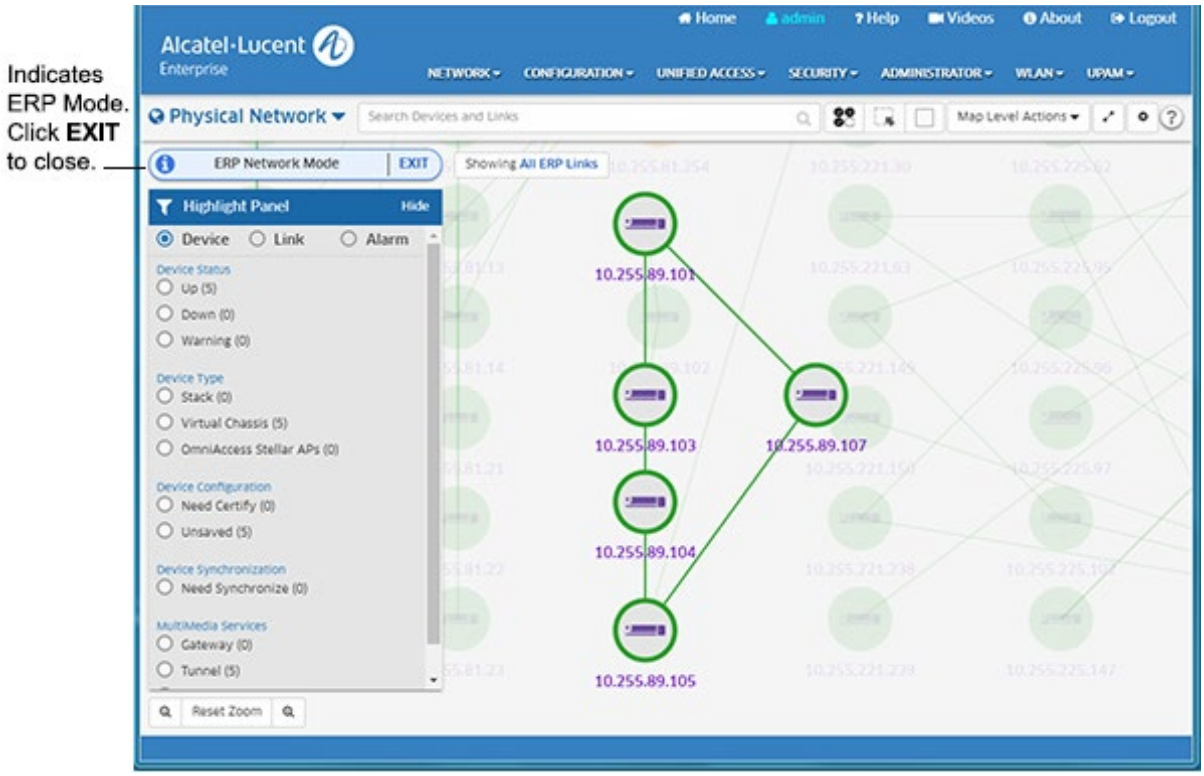
You can view link information for Layer 2 Switches connected to a SAP, even if the Layer 2 Switch does not run SPB. A switch must have a custom L2 Service Profile which enables 802.1ab (Peer), and the profile must be assigned to the SAP port on the switch. Hover over the link to display Customer VLAN information, as shown below.



Viewing ERP Maps

Ethernet Ring Protection (ERP) is a protection switching mechanism for Ethernet ring topologies, such as multi-ring and ladder networks. ERP uses the ring Automatic Protection Switching (APS) protocol to coordinate the prevention of network loops within a bridged Ethernet ring. Loop prevention is achieved by allowing the traffic to flow on all but one of the links within the protected Ethernet ring. This link is blocked and is referred to as the Ring Protection Link (RPL). When a ring failure condition occurs, the RPL is unblocked to allow the flow of traffic to continue through the ring. OmniVista displays ERP configuration on the network; however. ERP is configured using the CLI. For more information on ERP, see the *OmniSwitch AOS Network Configuration Guide*.

Within the Topology application, you can view a map of all Ethernet Ring Protection (ERP)-configured switches within a map. To bring up an ERP Map, click on the **Map Level Actions** drop-down at the top of the screen and select **ERP Network**.

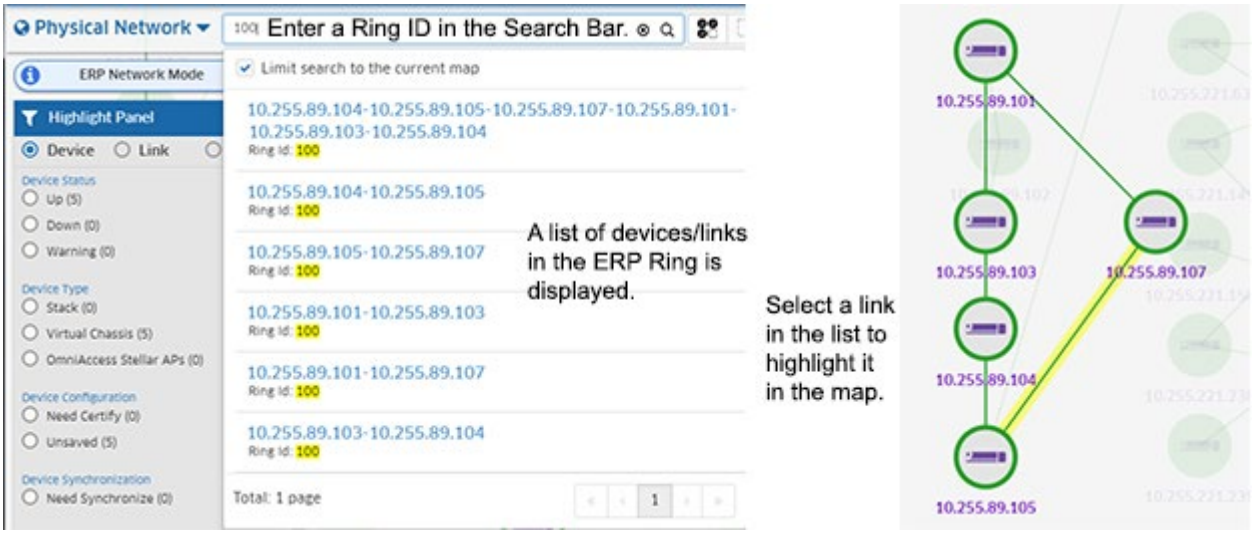


As shown above, "ERP Network Mode" is displayed in the upper left corner. Note that all of the map viewing and action options (e.g., highlight devices, view device/link information, perform actions on devices) are available on the ERP Map). To exit ERP Mode and return to the current map, click on **EXIT** in the "ERP Network Mode" bar (or click on the **Map Level Actions** drop-down and select **Exit ERP Network**).

> **Note:** If you zoom out on an ERP Map, clusters are created based on the current map. In other words, a cluster may contain both ERP devices and non-ERP devices.

ERP Configuration Viewing Options

By default, all links for all ERP Rings are displayed (as indicated by "All ERP Links" in the button at the top left corner of the map). However, you can view information about links on a specific ERP Ring. Enter a Ring ID (e.g., 100) in the Search Bar to bring up a list of devices/links in the ring. Click on a link to highlight the link in the map. You can hover over the link to display link information or click on the link to view link information in the Detail Panel.



Working with Geo Maps

The Topology application provides a Geo Map view to display devices in their physical location on a geographical map. You can edit a device to specify a Geo Map location for the device (either street address or Latitude/Longitude). The device will then be displayed in the Geo Map view in Topology. You can also create Map Sites (e.g., Street/City, Data Center, Campus Building), place them in a specific Geo Location and add devices to those sites. The sections below detail the steps for adding a Geo Map location for a single device, working with Geo Map Sites, and viewing Geo Maps.

Adding a Geo Map Location for a Single Device

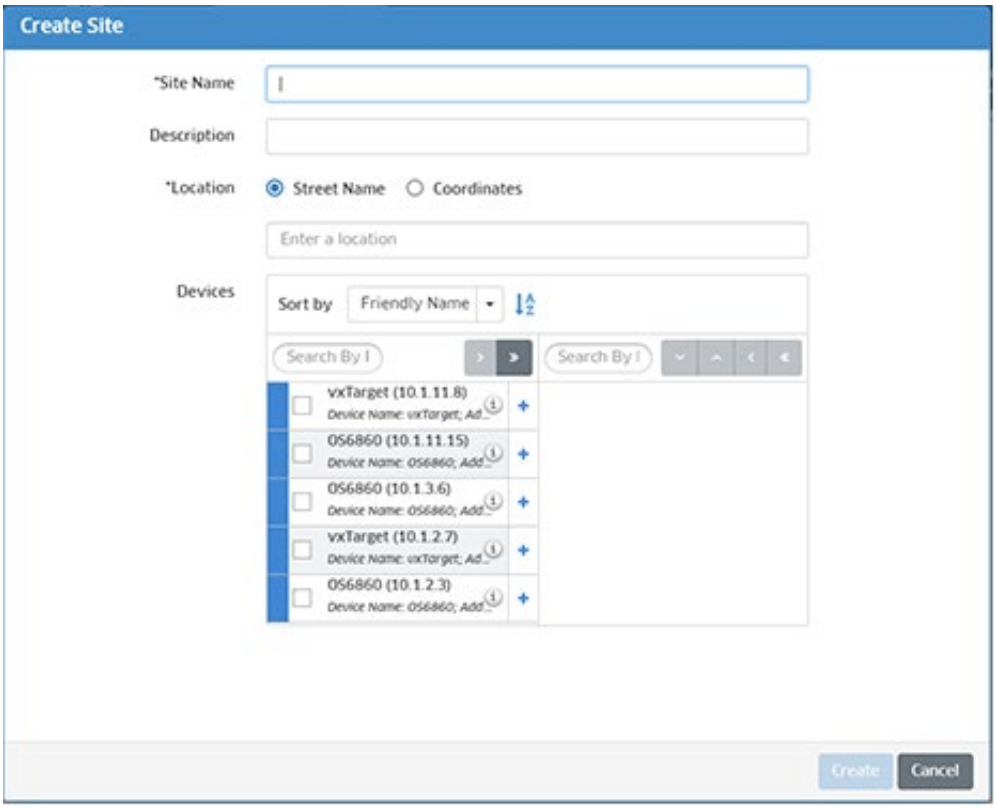
You can edit a device at any time on the Managed Devices - Edit Discovery Manager Entry Screen and specify a Geo Map location. Select the device in the Managed Devices Screen or in the Topology application and edit the device.

Geo Map Sites

You can create a Geo Map Site (e.g., Street/City, Data Center, Campus Building) and group devices in the site. When you create a Site, a logical map is automatically created for the Site. Note that you can create a Site without adding devices. Devices can be added/removed to/from a Site at any time. Also note that a device can only belong to one Site at time. To move a device to another Site, you must remove it from its current Site and add it to another Site. The sections below detail creating/editing/deleting Geo Map Sites.

Creating a Geo Map Site

Click on the **Create Site** button in the Topology Geo Map view; or click on the **Map Level Actions** drop-down in the traditional Topology view and select **New Site**. The Create Site Window will appear.



Complete the fields below and click on the **Create** button to create a new Site.

- **Site Name -** User-configured name for the Site.

- **Location**
  - **Street Name -** Enter a location beginning with the street name, city, etc. (OmniVista will offer suggestions as you type).
  - **Coordinates -** Enter Latitude and Longitude of the Site.
  - **Description -** Optional description for the Site.
  - **Devices -** Any devices that have not yet been assigned to a Site will be displayed on the left. Move the devices to the right to add them to the Site. Note that you can create a site without adding devices. Devices can be added later to the Site, or you can create Sub-Sites (e.g., building, floor) and add devices to the Sub-Sites. Also note that a device can only belong to one Site or Sub-Site. To move a device to another Site or Sub-Site, you must remove it before adding it to another Site or Sub-Site. If you remove a device that has a Geo Location specified and do not add it to another Site or Sub-Site, the device will be displayed individually on the Geo Map.

  Note: Remember that a device can only belong to one Site or Sub-Site at a time. If you are planning on creating Sub-Sites within a Site, it is recommended that you create a Site without assigned devices, then assign devices when you create the Sub-Sites (e.g., Floor 1, Floor 2).

Creating Sub-Sites

You create Sub-Sites within a Site (e.g., buildings, floors) by creating child maps from the logical Site map that is automatically created when you create a Site. To create a Sub-Site, go the Site map in the traditional Topology view. Click on the **Map Level Actions** drop-down at the top of

the screen and select **New Map**. The Create Custom Map window will appear. The name of the current Site map will be displayed in the **Parent Map** field. Enter a Sub-Site **Map Name** (e.g., Building 1, Floor 1), add devices to the map, and click on the **Create** button. Remember that just as in Sites, a device can only be assigned to one Sub-Site at a time.

The new Sub-Site map will appear as a sub-map under the Site in the Map drop-down at the upper-left corner of the screen. When you go to the Geo Map view, the total number of devices at the Site will be displayed in the Site circle (the total number of devices at the Site including all Sub-Sites), along with the device status and notifications status for all devices at the Site.

If all devices in a Site are "Up", the Site circle will be Green. If any device at the Site is in a "Warning" state, the Site circle will be Orange. If any device at the Site is "Down", the Site circle will be Red.

The small, solid circle in the upper-right corner of the Site circle displays the status of the highest severity trap generated by any device at the Site. For example, if the highest-level severity trap for any device at the Site is "Warning", the circle will be Orange. If the highest-level severity trap for any device at the Site is "Critical", the circle will be Red. If all traps generated by all devices at the Site are "Normal", the Trap Status circle will not be displayed. The default trap status colors are shown below.

- **No Circle** = Alarm status is Normal.
- **Orange** = Alarm status is Warning.
- **Purple** = Alarm status is Minor.
- **Yellow** = Alarm status is Major.
- **Red** = Alarm status is Critical.

Editing a Geo Map Site

You can edit a Geo Map Site by right-clicking on the site and selecting **Edit Site**. The Edit Site Window will appear. You can edit the Site Description or Location, and add/remove devices to/from the Site. If you remove a device, it will then be available for another Site. If you remove a device that has a Geo Location specified and do not add it to another Site, the device will be displayed individually on the Geo Map.

You can also go to the traditional Topology view to edit the Site. If you are in Geo Map view, hover the mouse over the Site on the Geo Map and click on **Go to Topology** to open the Site map in traditional Topology view. If you are in traditional Topology view, select the Site from the Map List drop-down in the upper left corner of the screen. Click on the **Map Level Actions** button at the top of the screen and select **Edit Site**.

You can edit a Sub-Site to add/remove devices. To edit a Sub-Site, open the Sub-Site map in traditional Topology view. Click on the **Map Level Actions** button at the top of the screen and select **Edit Map**. The Edit Map Window will appear. Add/Remove devices and click on the **Apply** button. The updated device count and status will be displayed in the Geo Map view. Note that you use the "Edit Map" function to edit a Sub-Site, not the "Edit Site" function.

> **Note:** Just as in the traditional Topology view, if you right-click on an individual device in a Geo Map, the Actions drop-down menu will appear, enabling you to perform any available device actions.

Deleting a Geo Map Site

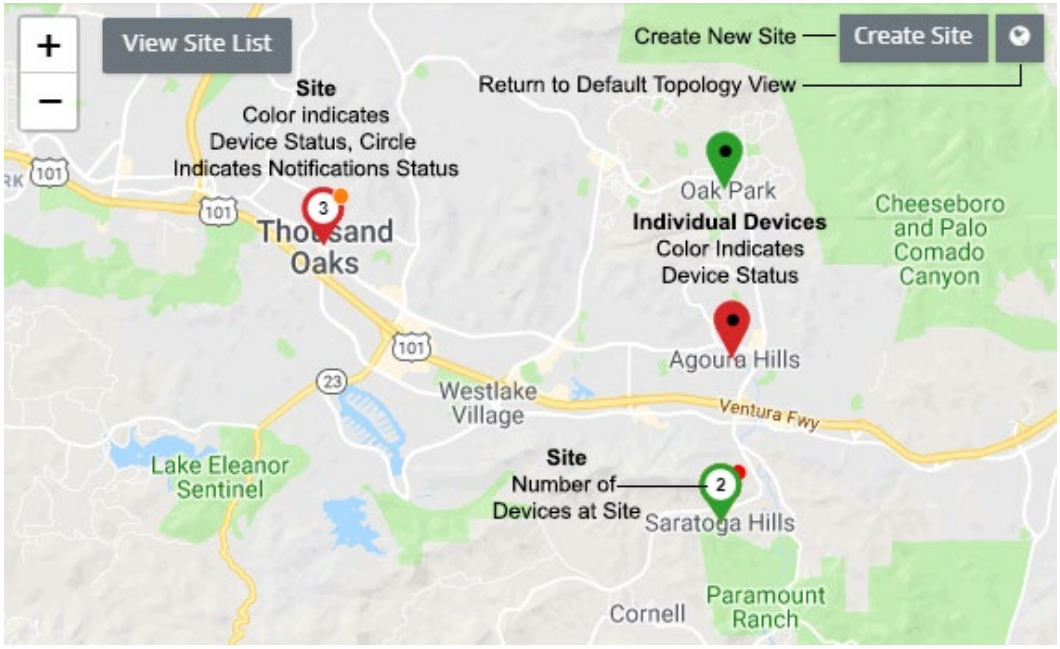
You can delete a Geo Map Site by right-clicking on the site and selecting **Delete Site**. Click on **Delete** at the Confirmation Prompt. All devices will be removed from the site. If a device had a Geo Location specified, once you remove it from the Site, it will be displayed individually on the Geo Map.

You can also go to the Logical Map for the Geo Map Site to delete the Site. If you are in the traditional Topology view, select the Site from the Map List drop-down in the upper left corner. If you are in Geo Map view, hover the mouse over the Site on the Geo Map and click on **Go to Topology** to open the Logical Map for the Site. On the Logical Map, click on the **Map Level Actions** button at the top of the screen and select **Delete Site**. Click on **Delete** at the Confirmation Prompt.

> **Note:** Just as in the traditional Topology view, if you right-click on an individual device in a Geo Map, the Actions drop-down menu will appear, enabling you to perform any available device actions.

Viewing Geo Maps

If you are in the traditional Topology view, click on the **Geo Location View** icon at the top-right corner of the screen to display the Geo Map view. Like any map application, you can zoom in/out and drag the map to change the view. Map Sites and individual devices are displayed as shown below. For individual devices, the device status is displayed by color (e.g., Green, Red), as is the Notifications status. For Geo Map Sites, the number of devices, device status, and Notifications Status are displayed for all devices in the Site. Links between Sites and devices are displayed, if configured. The links status is either "Up" (Green) or "Down" (Red).



For individual devices, the device status is displayed by color (Green, Orange, Red). For Sites, if all devices at a Site are "Up", the Site circle displays in Green. If any device at the Site is "Down", the Site circle displays in Red.

The small circle at the top of the device icon or the Site icon displays the Notifications Status. For an individual device, it displays the highest severity trap generated by the device. For a Site,

the Notifications Status displays the status of the highest severity trap generated by any device in the Site. For example, if the highest-level severity trap for any device at the Site is "Warning", the circle will be Orange. If the highest-level severity trap for any device at the Site is "Critical", the circle will be Red. If all traps generated by all devices at the Site are "Normal", the Notifications Status circle will not be displayed. The default Notifications status colors (for both sites and are shown below.

- **No Circle** = Alarm status is Normal.
- **Orange** = Alarm status is Warning.
- **Purple** = Alarm status is Minor.
- **Yellow** = Alarm status is Major.
- **Red** = Alarm status is Critical.

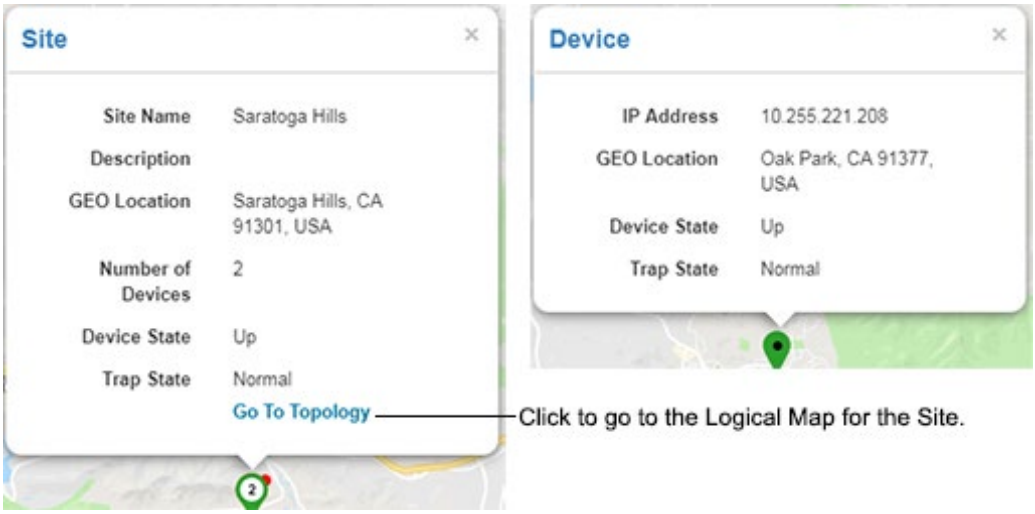
Note: You can change the default colors for alarm status using the Alarms Screen in the Preferences application (Preferences - User Settings - Colors - Alarms).

Note: You can change the default colors for device status using the Network Status Screen in the Preferences application (Preferences - User Settings - Colors - Network Status).

Click on the **+** or **-** symbol to zoom out or in on the map. Note that as you zoom out, Sites and devices that are close to each other on the map will display as a cluster with the number of Sites/devices displayed. When you zoom in, the individual Sites/devices will again be displayed.

Click on the **View Site List** button to view a list of Sites. You can then click on a Site in the list to center the map on the site. Click on the **Create Site** button to create a new Site (you can also click on the **+** icon at the top of the Site List to create a new Site). Click on the **Topology View** icon next to the **Create Site** button to return to the traditional Topology Map view.

You can hover the mouse over a Site or an individual device for more detailed information. When you hover over a Site, a "Go To Topology" link is also displayed. Click on the link to go the Logical Map for the Site. Sites can only be edited/deleted from the Logical Map.



Creating/Cloning/Editing/Deleting Maps

The Physical Network Map view (Default) displays all network devices. You can also create Custom Maps, or configure Dynamic Logical Maps. These maps are logical maps created from devices in the Physical Network Map. You can create multiple maps (Custom and Dynamic), and a device can be included in multiple maps.

> **Note:** Admin Users can create/clone/edit/delete maps. Netadmin and Write Users can edit maps.

Creating Maps

By default, all discovered devices are initially displayed in the Physical Network Map that is automatically created by OmniVista. New maps can be created by configuring a Child Map from a Parent map, or by creating a Logical Map that is not associated with a Parent Map.

- **Child Maps -** Child Maps are sub-maps created from a Parent Map. Any device you add to a Child Map is moved from the Parent Map to the Child Map. In general, you would create a series of Child Maps from the Physical Map to organize your network view. Child Maps are displayed in the Map drop-down under their Parent Map, and displayed in the Parent Map as a Globe icon (see below). You can click on the Map icon to view the devices in the map.
- **Logical Maps -** Logical Maps are not associated with a Parent Map. They are just logical groupings of devices that you can create to better visualize and manage your network. Since you are not using a Parent Map to create the Logical Map, devices you add to a Logical Map are not removed from any other map, and are displayed in both maps.

Child Map icon

To create a map, click on the **Map Level Actions** drop-down at the top of the screen and select **New Map**. The Create Custom Map window will appear. Complete the fields as described below to create a new map. When you are finished, click on the **Create** button to create the map.

- **Map Name -** Enter a unique name for the map. You cannot duplicate the name of an existing map.
- **Background -** If you want to change the default background for the map, select an image option, then select the background from the drop-down menu:
- **Upload New -** Click on the **Browse** button to locate a new background image, then select the image from the drop-down menu.
- **Existing Images -** Select an existing image from the drop-down menu.
- **Dynamic Map (to create a Dynamic Map) -** You can use a filter to create a Logical map that will dynamically add/remove devices to/from the map. Set the **Dynamic Map** slider to "On". Click on the **Filter** button to bring up the Filter Selection Window, and select a filter to apply to the map. If necessary, click on the Add icon to create a new filter. Select a condition(s) for the filter (e.g., IP address, Device Type, Device Location, AP Group.) Devices will now be added to/removed from the map dynamically based on the applied filter.

- **Parent Map -** If you want to create a **Child Map** of an existing map, select the **Parent Map** you want to use. Any devices you add to this map will be removed from the Parent Map and added to this map. If you want to create a **Logical Map**, select **None**. Selected devices will not be removed from the displayed map.
- **Devices -** Select the devices you want to include in the new map. Remember, if you are using a Parent Map to create a Child Map, the devices will be removed from the Parent Map and added to this new map.

Note: You can also copy devices from one map to another using the "Copy Device to Map" action. See Performing Device Actions for more information.

Note: If there are performance issues in rendering larger maps, you can reduce the number of devices in the map to improve performance.

Cloning Maps

You can also "clone" an existing map to quickly create a new Logical Map. Select a map that you want to clone from the Map drop-down menu at the top of the screen. Click on the **Map Level Actions** drop-down at the top of the screen and select **Clone Map**. The Clone Map window will appear with all of the devices in the map you are cloning pre-selected. Enter a **Map Name** and complete the fields as described above to create a new Logical Map.

Editing Maps

Go to the Map drop-down and select the map you want to edit. When the map is displayed, click on the **Map Level Actions** drop-down at the top of the screen and select **Edit Map**. Edit any of the fields as described above and click on the **Apply** button. You cannot edit the map name. You cannot change a Logical Map to a Dynamic Map or a Dynamic Map to a Logical Map; however, you can edit the filter for a Dynamic Map. You note that you cannot edit an AP Group Map.

Deleting Maps

To delete a Map, go to the Map drop-down in the upper-left corner of the screen and select the map you want to delete. When the map is displayed, click on the **Map Level Actions** drop-down at the top of the screen and select **Delete Map**. Click **OK** at the Confirmation Prompt. If you delete a Logical Map, the map and all devices (and child maps, if applicable) will be deleted. If you are deleting a Child Map created from the Physical Map, the map will be deleted and all devices will be moved back to the Physical Map. Note that you cannot delete the Physical Network Map or any AP Group Maps.

Working with Network Devices

You can view detailed information about a device or perform certain actions on a device by clicking on the device in the map. Actions can be performed on a single device or multiple devices. See Selecting Devices for instructions on selecting single or multiple devices. After selecting a device(s), you can perform one of the actions displayed in the Actions area. Note that the actions available depend on the device type(s) selected and whether or not you select a single device or multiple devices.

Note: The actions you can perform in Topology (e.g., performing backups, creating inventory reports) depend on your User Role and User Group configured in the Users and User Groups application.

Viewing Device Information

Click on a device to display detailed device information (IP address, MAC address, Backup information) in the Detail Panel on the right side of the screen. If you select multiple devices, the devices will be displayed in a list in the Detail Panel. Click on a device in the list to view information. Click on the “Back” link to return to the list. The information displayed may vary depending on the device.

- **Type -** The device type/model (e.g., OS6450-U24S)
- **Version -** The software version installed on the device (e.g., 6.7.2.107.R03).
- **Address -** The IP address of the device.
- **MAC Address -** The MAC address of the device.
- **Serial Number -** The serial number of the device.
- **Status -** The administrative status of the device:
- **Up -** Device is up and responding to polls.
- **Warning -** Device has sent at least one warning or critical trap and is thus in the warning state.
- **Down -** Device is down and not responding to polls.
- **Location -** The physical location of the device.
- **System Contact -** Contact information for the person responsible for the device.
- **Name -** The device name.
- **DNS Name -** The device DNS name, if applicable.
- **Last Upgrade Status -** The status of the last firmware upgrade on the switch:
- **Successful -** Successful BMF and Image upgrade performed.
- **Successful (BMF) -** Successful BMF upgrade performed.
- **Successful (Image) -** Successful Image upgrade is performed.
- **Failed (BMF, Image) -** BMF and Image upgrade failed.
- **Failed (BMF) -** BMF upgrade failed.
- **Failed (Image) -** Image upgrade failed.
- **Backup Date -** The date that the device's configuration and/or image files were last backed-up to the OmniVista Server.
- **Backup Version -** The firmware version of the configuration and/or image files that were last backed-up to the OmniVista Server.
- **Last Known Up At -** The date and time when the last successful poll was initiated on the device.
- **Description -** A description of the device, usually the vendor name and model.
- **Traps -** The status of trap configuration for the device
- **On -** Traps are enabled.
- **Off -** Traps are disabled.
- **Not Configurable -** Traps for this device are not configurable from OmniVista. (Note that traps may have been configured for such devices outside of OmniVista.)

- **Unknown -** OmniVista does not know the status of trap configuration on this device. OmniVista will read the switch's trap configuration when traps are configured for the switch via the Configure Traps Wizard.
- **No. of Licenses Used-** The total number of licenses being used. Generally, this will be 1. However, a device may use more than 1 license. For example, a stack of 4 switches would require 4 licenses, a VC of 6 would require 6 licenses. If a stack splits, the number of licenses reserved for the device before the split is maintained even though modules have been reduced to less than 5. This way, the license counts are reserved for the stack to recover.
- **License Type -** The type of license used by the device (e.g., Alcatel-Lucent Enterprise).
- **Running From -** For AOS devices, this field indicates whether the switch is running from the **certified** directory or the **working** directory. This field is blank for all other devices. For AOS devices, the directory structure that stores the switch's image and configuration files in flash memory is divided into two parts:
- **Certified Directory -** Contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory.
- **Working Directory -** Contains files that may or may not have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes to the working directory. You cannot save configuration changes directly to the certified directory.

Note: The files in the certified directory and in the working directory may be different from the running configuration of the switch, which is contained in RAM. The running configuration is the current operating parameters of the switch, which are originally loaded from the certified or working directory but may have been modified through CLI commands, WebView commands, or OmniVista. Modifications made to the running configuration must be saved to the working directory (or lost). The working directory can then be copied to the certified directory if and when desired.

Note: OmniVista supports the Multiple Working Directories Feature available on OS6900 Switches (AOS Release 7.2.1.R01 and later). This feature allows the user to create multiple Working Directories on the switch that can be used to save specific switch configurations. The user can create any name for these "Working" Directories (e.g., "Marketing Switch 05-10-19"). If the switch is running from one of these user-created directories, the directory name is displayed in this field.

- **Changes -** This field indicates the state of changes made to the switch's configuration. This field is blank for all other devices. This field can display the following values:
- **Certified -** Changes have been saved to the working directory, and but the working directory has been copied to the certified directory. The working directory and the certified directory are thus identical.
- **Uncertified -** Changes have been saved to the working directory, but the working directory has not been copied to the certified directory. The working directory and the certified directory are thus different.

- **Unsaved -** Changes have been made to the running configuration of the device that have not been saved to the working directory.
- **Blank -** When this field is blank, the implication is that OmniVista knows of no unsaved configuration changes and assumes that the working and certified directories in flash memory are identical.
- **Synchronized Status -** Indicates whether the primary CMM module's working directory is identical to the working directory on the other CMM module (if present):
- **Synchronized -** The primary CMM module's working directory is identical to the working directory on the other CMM module.
- **Not Synchronized -** The primary CMM module's working directory is not identical to the working directory on the other CMM module.
- **Not Applicable -** Only one CMM module is installed.
- **Unknown -** The synchronization state is unknown.

Performing Device Actions

You can perform the following actions on any device in a map. To execute one of the actions, click on a device(s) and select an action from the Actions area in Detail Panel. Note that the actions available are different for single device selection and multiple device selection. Available actions will also vary if you select different types of devices in multiple selection mode. Note that you can also perform actions on a device(s) by selecting a device(s) and right-clicking to bring up a menu of device actions. Click on a category, then click on an action. Note that you must right-click while the cursor is on a device to bring up the menu.

Map

- **Overlay View -** Provides detailed information for wireless, virtual chassis, and stack devices. Topology maps display a single icon for Virtual Chassis, Stacks, and Wireless devices. For example, topology maps display only the Master Chassis in a virtual chassis. You can select the device in the map and click on "Overlay View" to display the other the virtual chassis or stack. When the overlay view is displayed, you can click on any device in the overlay view for detailed information on the device. The following information is displayed:
- **Virtual Chassis Overlay -** Displays the devices in the Virtual Chassis and links between them. Click a node/link to view chassis/VFL link detail information.
- **Stack Overlay -** Displays each slot (chassis), and the links between them. Click on a node/link to view slot/link detail information.
- **Wireless Device Overlay -** Displays logical links between Controller and Access Points (APs). Click on a controller or AP for detailed information.
- **AP/Node Relationship Overlay -** Displays information about APs and LAN Devices, as well as the link between them. Click on an AP, switch or link for detailed information.
- **AOS Switch -** IP Address, MAC Address, Serial Number, Type, Status, SW Version, Location, System Contact, Name, DNS Name, Last Upgrade Status, Backup Date, Backup Version, Last Known Up At, Description, Traps, No. of Licenses Used, License Type, Running From, Changes, Synchronized Status.
- **AP Nodes -** IP Address, MAC Address, Serial Number, AP Type, Status, SW Version, Location, System Contact, Name, DNS Name, Last Upgrade Status, Backup Date, Backup Version, Last Known Up At, Description, Traps, No. of

Licenses Used, License Type, Running From, Changes, Synchronized Status, AP Group, SSIDs, Management VLAN, Data VLANs.

- **Link -** Origin, IP Address 1, Slot/Port 1, LAG 1, IP Address 2, Slot/Port 2, LAG 2, Ring Id, Media Type, Status, Local Port VLANs, Remote Port VLANs.
- **Copy Device to Map -** Copies the selected device(s) from the current map to a different map. Select a device(s), click on the "Copy Device to Map" action link, then select the new map location from the Map drop-down at the top-left of the screen. When the new map appears, click on the **Add devices to this map** button. The device(s) will appear in the new map.
- **Remove from the Map -** Removes the selected device(s) from the current map. Note that you cannot remove a device from the Physical Network Map, system-created maps (e.g., a map that is auto-created when a new discovery range is created), or a dynamic map.

Device

- **Edit Device -** Opens the Edit Discovery Manager Screen in the Discovery application for the selected device.
- **Delete Device -** Deletes the selected device the system. Note that when you delete a Stellar AP, the device is removed from the map and the Inventory Table in the Discovery application and placed into "Unmanageable" status on the Access Points Screen.
- **Copy as New Device - T**akes you to the Discovery application's "Add New Device" Screen, where you can add a new device based on the configuration (e.g., CLI/FTP Password, SNMP configuration) of selected device.
- **Ping Device -** Causes an immediate ping of the selected device(s), and launches the Managed Devices Screen in the Discovery application to display the results.
- **Poll Device -** Causes an immediate poll of the selected device(s), and launches the Managed Devices Screen in the Discovery application to display the results.
- **Poll Link -** Causes an immediate poll of any links on the device(s), and launches the Managed Devices Screen in the Discovery application to display the results.
- **Reboot -** Takes you the Discovery application's Managed Devices Screen where you can reboot the selected device(s). On LAN Devices, you have the option of rebooting from the Working, Certified, or Other Directory and setting a time for the reboot. Use the **Reboot From** drop-down to select the directory you want to reboot from. In the **Reboot Delay** drop-down, select when you want to reboot to occur (now, a specific number of minutes from now, or at a specific date and time). Note that when you reboot multiple devices, there is a minimum delay of 30 seconds before the devices reboot (even if you select the Reboot now option).
- **Copy Working/Running to Certified -** Copies the contents of the working/running directory in the primary CMM to the certified directory in the primary CMM. Note that the Copy Working to Certified command also automatically synchronizes the switch's CMMs after the copy action is completed.
- **Copy Certified to Working/Running -** Copies the contents of the certified directory in the primary CMM to the working/running directory in the primary CMM.
- **Save to Running -** Saves the primary CMM's current running configuration to the current running directory of the switch. OmniVista supports the Multiple Working Directories Feature on certain devices (OS6900). This feature allows the user to

create multiple "working" directories on the switch that can be used to save specific switch configurations. When the Save to Running Command is executed, the device(s) save the CMM's current running directory to the current user-defined "working" directory (Running Directory). Note that if you select a group of devices and some do not support multiple working directories, the devices will save the CMM's current running directory to the device's current "working" directory, whether it is a user-defined directory or the Working Directory.

Note: For Virtual Chassis stacks (running AOS 8.5R2 or higher or 6.7.3.R04 higher), if you attempt to save a configuration to the Running Directory and there has been a change in the Virtual Chassis stack topology since the last save, a warning prompt will appear listing the problem devices. You can proceed to save the configuration(s) on all devices, or make any necessary configuration updates to devices before saving. If you proceed with the save without addressing the changes, a trap will be generated (virtualchassisstatuschange) in the Notifications application.

- **Webpage -** Opens up a Web session with the selected device. The web session application varies depending on the device. For example, AOS devices will open a WebView session.
- **Configure Health Thresholds -** Opens the Configure Device Health Thresholds Screen in the Discovery application for the selected device. Thresholds are used to set limits for health traps. If a device has been configured to send health traps, a trap will be sent whenever a monitored item's current utilization exceeds the configured health threshold. Configure the CPU, Memory, or Temperature Threshold for the selected device(s) and click on the **Apply** button. Note that you cannot configure the Temperature Threshold. The Temperature Threshold is hard coded on devices.

CLI Scripting

- **SSH/Telnet -** Opens a Telnet (SSH) session with the selected device in the CLI Scripting application.

Locator

- **Locate End Stations -** Launches the Locator application and searches for all end stations/clients (Stellar APs) that are attached to the selected switch. All end stations/clients found are displayed in the Locator application's Browse Screen.

Notifications

- **View Traps -** Launches the Notifications Home Screen in the Notifications Application to display traps for the selected device.
- **Poll for Traps -** Causes an immediate poll of the selected devices for traps. Traps are reported in the Notifications application.
- **Configure Traps -** Launches the Trap Configuration Wizard in the Notifications application to enable you to configure traps for the selected devices.

Resource Manager

- **Backup Device -** Launches the Backup Wizard in the Resource Manager application, which enables you to perform a configuration backup of the selected devices
- **Upgrade Image -** Launches the Upgrade Image Screen in the Resource Manager application, which enables you to perform and image upgrade.

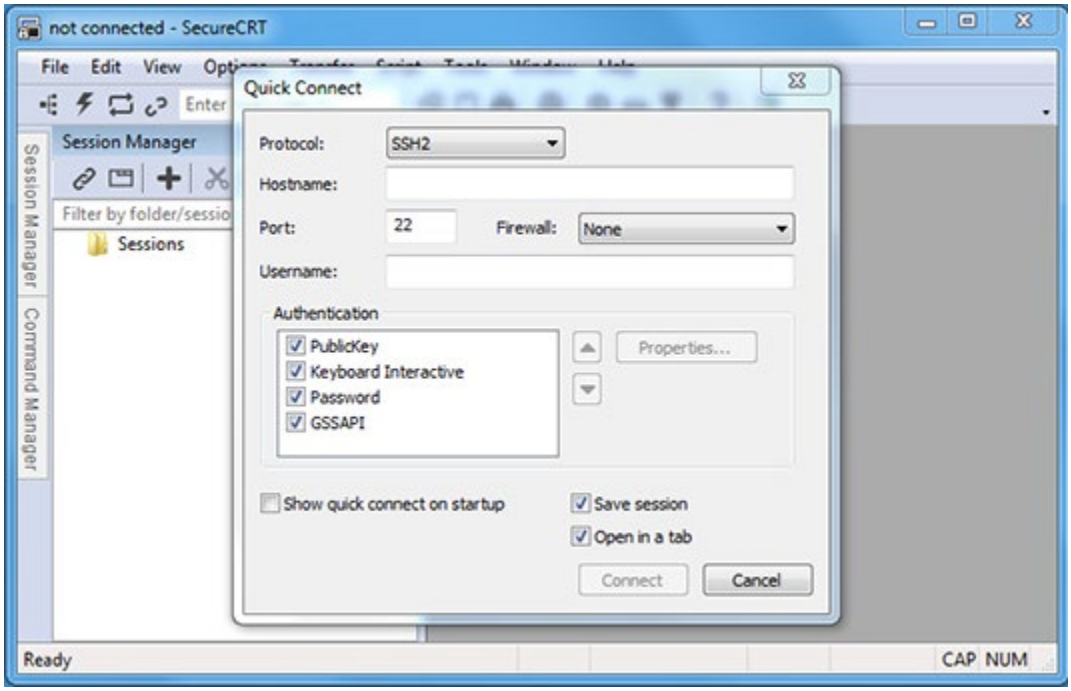
SAA

- **Ethernet -** Launches the Ethernet OAM Screen in the SAA application.

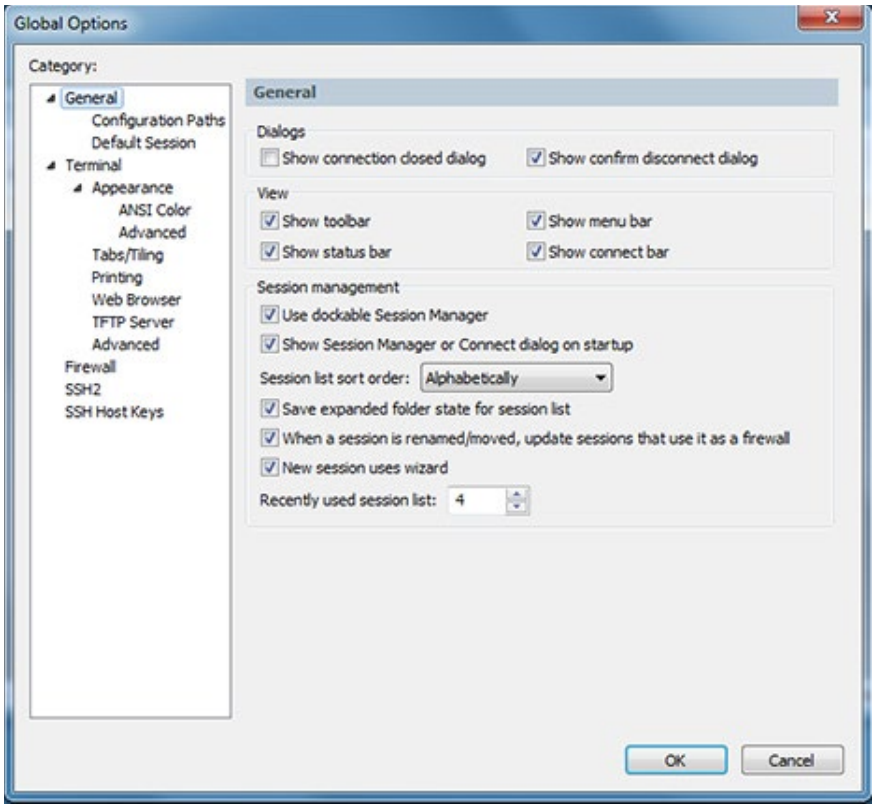
Installing/Configuring SecureCRT

1. Download and install SecureCRT on your OmniVista Client

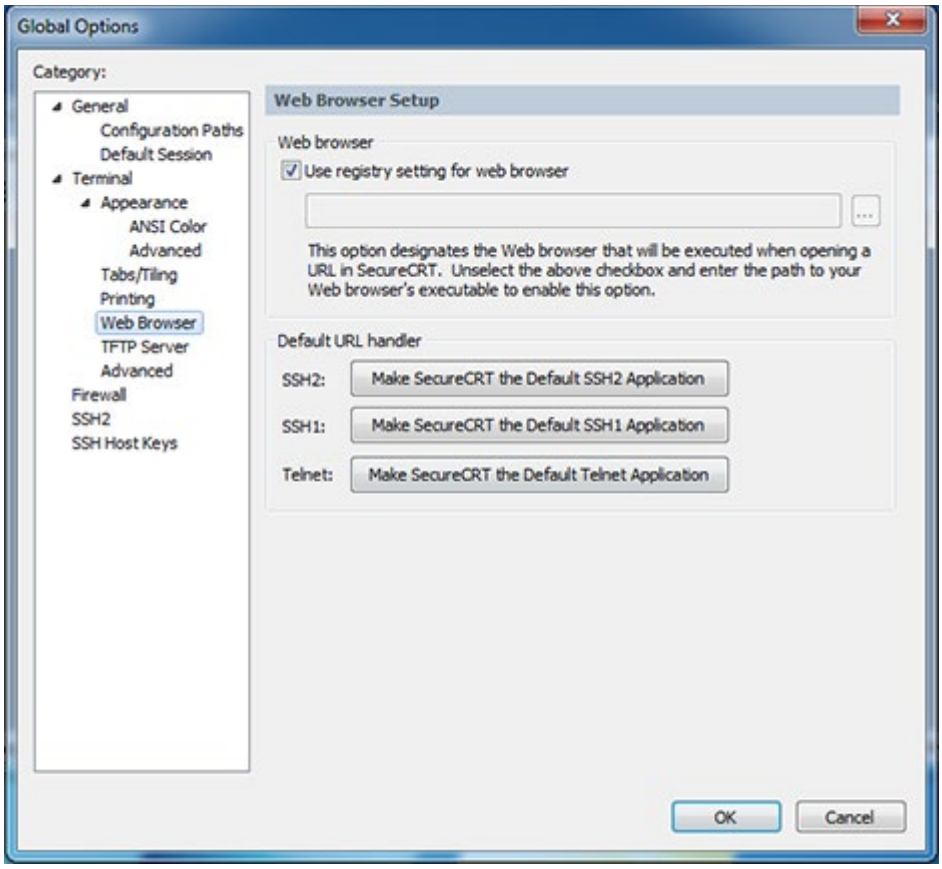
2. Open SecureCRT.



3. Close the Quick Connect Window. Click on the Options menu and select Global Options.



4. Click on Web Browser. Make sure “Use registry setting for web browser” is checked, and click **OK**. You can now open a Custom SSH session to a device from the Managed Devices Screen or in the Topology application.



Note: Your browser must be able to make SSH2 connections and SecureCRT must be set as your default SSH2 application to use the Custom SSH feature.

32.0 Unified Access

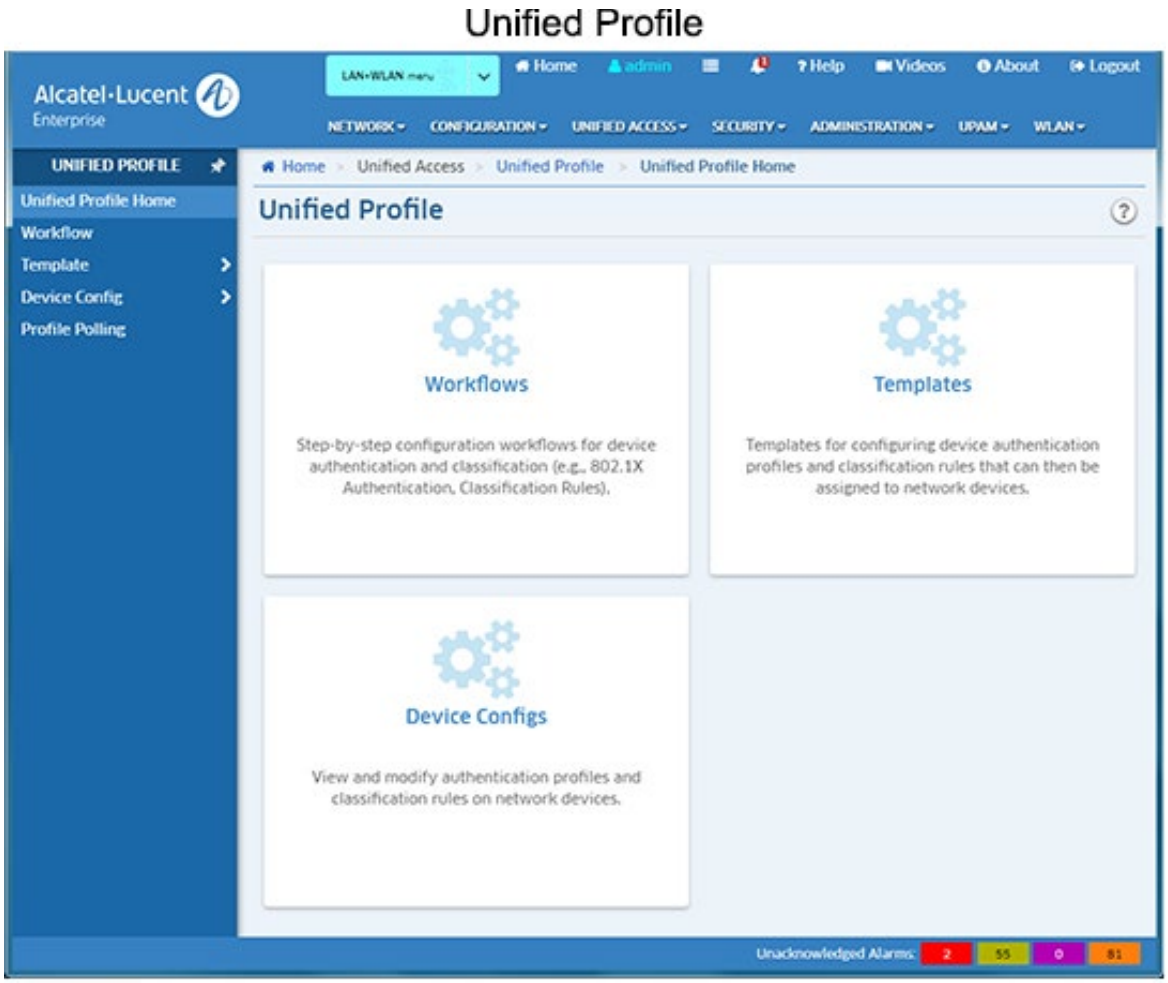
The Unified Access Application provides unified wirleline/wireless device configuration of security functions for Edge Ports and Access Points (APs) on OmniAccess Wireless devices. In addition to device authentication and classification, you can create Access Role Profiles (similar to User Network Profiles) to configure network access controls for one or more user devices. Unified Access contains applications that work together with the Authentication Servers application to seamlessly authenticate and configure QoS for both device types. It is configured using the following applications:

- **Unified Profile -** Provides unified security functions for Edge Ports for supported wireline and wireless devices.
- **Unified Policy -** Used to configure Unified Policies and Policy Lists, which enable the user to configure QoS policies for both wireline and wireless devices.
- **Multimedia Services (mDNS) -** Used to configure the Multicast Domain Name System (mDNS) protocol. mDNS is used by "Zero Configuration Networking" solutions such as Apple's Bonjour, Avahi LGPL, and Linux NSS-mDNS. mDNS is a resolution service that is used to discover services on a LAN.
- **Paid Services (BYOD) -** Used to configure the Bring Your Own Device (BYOD) feature. BYOD leverages Access Guardian features along with ClearPass Policy Manager (CPPM) to allow a wired or wireless guest, device, or authenticated user to connect to the network through an OmniSwitch edge device using the CPPM Server for unified authentication.

Unified Profile

The Unified Access Unified Profile application provides unified security functions for Edge Ports and AOS WLAN Devices. In addition to device authentication and classification, you can create Access Role Profiles (similar to User Network Profiles) to configure network access controls for one or more user devices. This is achieved using both Layer 2 and Layer 3 Authentication and Classification. Layer 2 Authentication and Classification provides the initial user authentication and Access Role Profile assignment. Layer 3 Authentication and Classification can dynamically change the QoS Policy List/Role for a user already authenticated and classified into the network. Based on the Access Role Profile (UNP) into which the user is initially classified, the user may undergo Quarantine Manager and Remediation (QMR), RADIUS based MAC Check Blacklisting, and Location or Time-Based validations that can restrict a user's network access or assign different Policy Lists/Roles to the user.

Unified Profile is configured using the links on the left side of the screen. An overview of each configuration function is provided below.



Authentication and Classification

Unified Profile provides network access and Quality of Service on a per user basis. This is achieved using both Layer 2 and Layer 3 Authentication and Classification.

Layer 2 Authentication and Classification

Unlike regular Layer 2 bridging, all users are learned through software. The user is learned "forwarding" or "filtering" based on Layer 2 authentication mechanisms configured on the port. The authentication mechanisms supported are 802.1x and MAC based authentication. Access Classification rules can also be used to learn a user in the forwarding state if no authentication mechanism is configured. Apart from determining the forwarding or filtering state, this stage also determines the UNP and VLAN to be assigned to the user. The UNP and VLAN assigned to the user do not change. The UNP provides an initial QoS Policy list/role to be assigned to the user.

A user is first authenticated using 802.1x or MAC based authentication (MAC authentication is used only if 802.1x authentication is disabled or the user is not a supplicant.) If the user passes authentication, and the RADIUS server returns a valid UNP name, the user is mapped to that Access Role Profile (UNP name) and VLAN. The RADIUS server may also return an explicit policy list name, which overrides the policy list associated with the UNP.

If authentication is not enabled or fails, or the Authentication Server does not return a valid UNP, and classification is enabled, the user is classified based on one of the following Access

Classification Rules - Port, Group ID, MAC, LLDP, Authentication Type, IP Address - and assigned a Default UNP.

Configuring Unified Profile

Unified Profile can be configured using Workflow windows and/or Templates. Unified Profile is configured using the links on the left side of the screen.

- **Workflow -** OmniVista provides guided workflows for configuring Unified Profile. These workflows can be used for an initial Unified Profile setup, which can then be fine-tuned using the Unified Profile Templates and Device Config editing. You can use the workflows to:
- Classify network traffic based on Access Classification Rules.
- Use RADIUS Servers to authenticate users using 802.1X.
- User RADIUS Servers to authenticate users using 802.1X or MAC Address.
- User RADIUS Servers to authenticate users using MAC Address or Captive Portal
- Use ClearPass to authenticate users using 802.1X, MAC Address or Web-based credentials.
- **Template -** Unified Profile Templates are used to configure Unified Profiles (e.g., Access Auth Profiles, Wireless Profiles) and apply them to multiple network devices.
- **Device Config -** Device Config screens enable you to view, edit, and delete Unified Profiles on specific network devices.
- **Profile Polling -** Used to set the polling interval at which device configuration information is updated, and perform immediate polls to update Unified Profile information.

Workflow

Unified Profile Workflows are guided workflows you can use to configure Unified Profile. These workflows can be used for setting up initial Unified Profiles on devices for specific use cases, which can then be fine-tuned using the Unified Profile Templates and Device Config editing. You can use the workflows to:

- **Traffic Based on Classification Rules -** Classify network traffic based on Access Classification Rules.
- **802.1X Authentication -** Use RADIUS Servers to authenticate users using 802.1X.
- **MAC Authentication -** Use RADIUS Servers to authenticate users using MAC Address.
- **802.1X and MAC Authentication -** Use RADIUS Servers to authenticate users using 802.1X or MAC Address.
- **MAC Authentication and Captive Portal -** Use RADIUS Servers to authenticate users using MAC Address or Captive Portal
- **802.1x MAC Authentication and Captive Portal with ClearPass -** Use ClearPass to authenticate users using 802.1X, MAC Address or Web-based credentials. Note that when you apply this workflow to a device, the ClearPass IP address will be automatically configured on the device based on the "unp redirect-server" configured on the device. If you want to change the ClearPass Server, go to the ClearPass Screen (Unified Access - Premium Services - BYOD - ClearPass) to create a new ClearPass Server and apply it to the device.

- **802.1x, MAC Authentication and Captive Portal with UPAM -** Use the 802.1x, MAC Authentication and Captive Portal with UPAM.
- **Setting up Edge Infrastructure for WLAN -** Classify AP traffic (management and client) to edge devices using Access Auth Profile and Classification Rules.

  Note: Captive Portal is not supported on OS6350 Switches. OS6350 Switches are not available for device selection in workflows involving Captive Portal.

Unified Profile Templates

Unified Profile Templates are used to configure Unified Access Profiles, which provide unified security functions for Edge Ports and AOS WLAN Devices. In addition to device authentication and classification, you can create Access Role Profiles (similar to User Network Profiles) to configure network access controls for one or more user devices. This is achieved using both Layer 2 and Layer 3 Authentication and Classification. Layer 2 Authentication and Classification provides the initial user authentication and Access Role Profile assignment. Layer 3 Authentication and Classification can dynamically change the QoS Policy List/Role for a user already authenticated and classified into the network. Based on the Access Role Profile (UNP) into which the user is initially classified, the user may undergo Quarantine Manager and Remediation (QMR), RADIUS based MAC Check Blacklisting, and Location or Time based validations that can restrict a user's network access or assign different Policy Lists/Roles to the user.

The first step in configuring Unified Profile is to configure an Access Auth Profile and assign it to ports/linkaggs on the network. You then configure Access Role Profiles and AAA Server Profiles to which a user is assigned based on the Access Auth Profile. The following links are used to access Unified Profile Templates:

- **Access Auth Profile -** An Access Auth Profile contains all of the UNP properties to be enabled on an Edge Port. The template can be applied to a port or linkagg to enable UNP Edge Port status and set the parameters for the authentication process for the port. The Access Auth Profile configures 802.1x and MAC authentication, Access Classification, the AAA Server Profile to be used for authentication specifying the default Access Role Profile (UNP), etc.
- **WLAN Service -** Used to create a WLAN Service and assign the service to devices on the network.
- **Access Role Profile -** Contains the various UNP properties, including the QoS Policy List attached to the UNP and Captive Portal Authentication for users assigned to into this UNP.
- **AAA Server Profile -** In addition to the global AAA configuration included in an Access Auth Profile, you can also create a AAA Server Profile that can be applied on a per Port/Linkagg basis. This enables you to configure different RADIUS Servers for different users on different ports and apply different RADIUS client attributes to them. AAA Server Profiles are only supported on 8.x and Wireless devices. 6.x and 7.x devices use Global AAA Configuration.
- **Access Policies -** Location and Period
- **Access Classification -** Used to configure Access Role Profile Classification Rules.
- **Customer Domain -** Used to configure Customer Domains. Customer Domains provide an additional method for segregating device traffic. A Customer Domain is identified by a numerical ID, which can be assigned to UNP ports and Access Classification Rules.

- **SPB Profile -** Used to create an SBP Profile. An SPB Profile contains SBP parameters that can be mapped to an Access Role Profile.
- **Far End IP -** Used to create Far End IP Lists. A Far End IP List is assigned to an Access Role Profile through the mapping of VXLAN service parameters to the profile. This allows multiple far-end nodes to be associated with the service created for the VXLAN Network ID (VNID) specified in a VXLAN Profile.
- **Static Service -** Used to configure a Static Service Profile. This can be used to configure the mapping of an existing SPB or VXLAN service ID to an Access Role Profile.
- **VXLAN Profile -** Used to configure a VXLAN Profile that can be mapped to an Access Role Profile.
- **Tunnel Profile -** Used to configure Tunnel Profiles. When you create a Tunnel Profile, you configure the parameters that can be mapped to an Access Role Profile to authenticate a Guest Client, and map the client to a Guest UNP profile that is mapped to an L2 GRE service.
- **Legacy Wireless Profiles -** Used to create the following OAW Wireless Device Profiles: 802.1x, Authentication, MAC Authentication, and AP Group.
- **Global Configuration -** global Settings, AAA, Redirect Allowed Profiles, and DHCP Option 82 sub-option information.

Access Auth Profile

The Unified Profile Access Auth Profile Screen displays all configured Access Auth Profiles and is used to create, edit, and delete Access Authentication Profiles. An Access Auth Profile enables you to assign a pre-defined UNP port configuration to a port or linkagg, or specify them individually on each port to enable UNP port status and set the parameters for the authentication process for the port. For IAP devices, an Access Auth Profile can be assigned to a WLAN identified by the SSID Profile. For wireless controller devices, an Access Auth Profile can be assigned to Virtual AP Profile, which is used to configure WLAN. The Access Auth Profile configures 802.1X and MAC authentication for both wired and wireless devices, Access Classification and the default AAA Server and/or UNP Profile to be used once a user is authenticated. The basic configuration for each configured Access Auth Profile is displayed. You can also click on a profile for a configuration view.

Creating an Access Auth Profile

Click on the Add icon. Enter a **Profile Name** and configure the profile as described below, then click on the **Create** button. When you are finished, select the checkbox next to the profile and click on the **Apply to Devices** button to assign the profile to switches/ports or wireless devices/virtual APs on the network.

Default Settings

This section is used to configure basic settings for the profile.

- **AAA Server Profile -** The AAA Server Profile used to authenticate users on the port. Select a profile from the drop-down list or click on the "Add New" link to go to the AAA Server Profile Screen and create a new profile. Note that this field is not supported for AOS 6x devices. To apply a AAA Profile to an AOS 6x device, go to the Global Configuration AAA Screen (Global Configuration - AAA), create a AAA Profile, and apply it to devices.

- **Port Bounce -** Enables/Disables Port Bounce. Always Enabled on wireless devices and AOS 6x switches. This feature is required to handle scenarios where a client is switched from one VLAN to other after COA. If port bounce is enabled, the port will be administratively shut down. This is to trigger DHCP renewal and re-authentication, if necessary.
- **MAC Auth -** Enables/Disables MAC Authentication for the port. Wireless devices do not contain this attribute in their configuration table. MAC Pass Alt attribute in the next section No Auth/Failure/Alternate is used for MAC Authentication on wireless devices.
- **802.1X Auth -** Enables/Disables 802.1X Authentication. Wireless devices do not contain this attribute in their configuration table. 802.1X Pass Alt attribute in the next section No Auth/Failure/Alternate is used for 802.1X Authentication on wireless devices.
- **Dynamic Service -** Select a dynamic mapping method for the profile, if applicable (SPB, VXLAN).
- **Customer Domain ID -** Select a Customer Domain ID for the profile, if applicable. If necessary, click on the "Add New" link to go to the Customer Domain Screen and create a Customer Domain.
- **L2 Profile -** Select an existing Layer 2 Profile from the drop-down menu. To create a new profile, go to the Layer 2 Profiles Screen (Configuration - Services - Layer 2 Profiles). Once a new profile is created, it will appear in the L2 Profile drop-down menu on this screen. Layer 2 profiles specify how control packets are processed on SAPs.
- **AP Mode -** Enables/Disables the Access Point Mode for the port. When enabled (the default), the switch automatically detects, learns, and manages a Stellar AP that is connected to the port. Wireless client traffic is then forwarded from the AP to the OmniSwitch onto the wired network.
- **Secure -** If the AP Mode is enabled, you can check this box to secure the AP Mode. The AP Mode is not secured by default (box is not checked). When an AP device is detected on a UNP port, the trust tag function is operationally enabled to trust the AP client traffic. If the AP device fails authentication but is still learned as forwarding, the client traffic is still trusted. When the AP Mode is secured (box is checked), the trust tag function is not enabled for client traffic until after the AP device successfully authenticates.

No Auth/Failure/Alternate

This section is used to configure the actions taken if a device assigned to the profile fails authentication.

- **Trust Tag -** Enables/Disables whether or not to trust the VLAN ID of a tagged packet to determine how the packet is classified. Enabling the trust VLAN ID tag option provides an implicit method of VLAN tag classification that will accept tagged traffic without the need to create specific classification rules for those profiles. (Default = Disabled)
- **Access Classification -** Enables/Disables device classification. Always Enabled on wireless devices (Default = Disabled).
- **Default Access Role Profile -** The Default Access Role Profile that users are assigned to if authentication or classification methods fail to match traffic with any

role. This is the last-resort role. Select a profile from the drop-down list or click on the "Add New" link to go to the Access Role Profile Screen and create a new profile. Note that for IAP devices the default Access Role Profile name must match the SSID Profile name in order for it to take effect.

- **Bypass VLAN -** Enter a Bypass VLAN (Range = 1 - 4094). The Bypass VLAN attribute is supported on Stellar AP1201H/1201HL (running AWOS 4.0.2 or later) and Stellar AP 1301H/1311 (running AWOS 4.0.5 or later). The feature improves wired port forwarding performance by skipping the CPU process. When a Bypass VLAN is configured, traffic from the AP uplink port to the downlink port, or vice versa, is forwarded directly through the switch chipset without CPU intervention. The Bypass VLAN has higher priority than Trust Tag. When a VLAN is configured as the Bypass VLAN and Trust Tag at the same time, the Bypass VLAN function is effective on that VLAN, while Trust Tag is not. Note that when Bypass VLAN is configured, Authentication/ACL/Policy etc. features cannot be applied to the traffic in the Bypass VLAN. When an Access Auth Profile is applied to an AP Group, OmniVista will pass the Bypass VLAN attribute to all APs in the AP Group. APs 1201H/1201HL and 1301/1311 will accept it, other APs in the group will silently ignore this attribute. Bypass VLAN is recommended for the use case of HD IPTV.
- **802.1X Pass Alt -** The user shall be assigned a Pass-Alternate UNP in case the 802.1X authentication does not result in a valid UNP for the pass branch. Select a profile from the drop-down list or click on the "Add New" link to go to the Access Role Profile Screen and create a new profile.
- **Bypass Status -** Enables/Disables 802.1X bypass. When 802.1X bypass is enabled, the user's 802.1X authentication method is skipped. The user directly enters mac-authentication or Access Classification based on the configuration on the UNP ports/Linkaggs. On wireless devices, this attribute corresponds to another attribute named l2-auth-fail-through, and this attribute must be combined with the MAC Allow EAP attribute to make l2-auth-fail-through attribute work (Default = Disabled).
    - **AOS Devices**
        - Bypass Status with Enabled status combined with MAC Allow EAP set to "None" will disable 802.1X authentication, and l2-auth-fail-through is not Enabled.
        - Bypass Status with Enabled status combined with l MAC Allow EAP set to "Fail" will enable l2-auth-fail-through.
        - Other configurations of Bypass Status and MAC Allow EAP cause l2-auth-fail-through to be ignored on wireless devices.
    - **Stellar APs**
        - If Bypass Status is Enabled, MAC Allow EAP will be considered. In the AP. There are only two options: Pass or Fail. When Bypass Status is Enabled, both MAC authentication and 802.1x authentication are performed - MAC authentication is performed first, then 802.1x authentication.
        - If Bypass Status is Disabled, OmniVista will always perform 802.1x authentication and ignore MAC authentication (unless both MAC and 802.1x authentication are enabled).
- **Failure Policy -** The authentication method used if 802.1X authentication fails. Note that MAC Authentication Failure Policy is not supported on AOS 6.x devices.

- **MAC Pass Alt -** The Access Role Profile the user is assigned to after passing authentication.
- **MAC Allow EAP -** MAC Allow EAP behavior can be configured on both AOS Device and certain Stellar AP Models (e.g., AP1201H).
    - **AOS Devices -** Normally, when we enable both MAC and 802.1x authentication, 802.1x authentication status is considered first. If 802.1x authentication is disabled or it is a non-supplicant client, MAC authentication will be performed. In some cases, you may want the AOS port to perform MAC authentication first. 802.1x authentication will be performed later or not based on the result of the MAC Authentication. Select one of the following options:
        - **Pass -** Allows 802.1x (EAP frame) authentication if the supplicant passes MAC authentication.
        - **Fail -** Allows 802.1x (EAP frame) authentication if the supplicant fails MAC authentication.
        - **No Auth -** Allows 802.1x (EAP frame) authentication if there is no MAC authentication configured on the port.
        - **None -** Prevents 802.1x Authentication. Only MAC authentication is performed on any device accessing this port.
    - **Stellar APs -** The Bypass Status setting (above) controls when the AP performs 802.1x Authentication on the downlink port. If the Bypass Status is set to Enable, select one of the following options:
        - **Pass -** 802.1x Authentication is only performed if MAC authentication passed.
          Fail - 802.1x Authentication is only performed if MAC authentication fails.

Advanced Settings

This section is used to configure advanced 802.1X authentication settings for the profile.

- **802.1X Tx Period Status -** Enables/Disables 802.1X Authentication Tx Period (Default = Disabled).
- **802.1X Tx Period -** Access Auth Profile 802.1X Tx period, in seconds.
- **802.1X Supp Timeout Status -** Enables/Disables802.1X Supp Timeout (Default = Disabled).
- **802.1X Supp Timeout -** 802.1X Authentication Supp Timeout, in seconds.
- **802.1X Request Status -** Enables/Disables 802.1X Authentication Max Request (Default = Disabled).
- **802.1X Request -** 802.1X Authentication Max Request number.
- **Port Controlled Directions -** Configures whether network access control is applied to both incoming and outgoing traffic, or only applied to incoming traffic (In/Both, Default = Both).

Wireless Settings

This section is used to configure a Virtual AP Profile (i.e., "wireless device" profile) and associate it with the Access Auth Profile.

- **Virtual AP Name -** User-configured name for the Virtual AP Profile.

- **SSID Profile -** The SSID Profile you want to associate with the Virtual AP Profile. Select a profile from the drop-down list or click on the "Add New" link to go to the SSID Profile Screen and create a new profile.
- **User Derivation Rules -** Select a User Derivation Rules from the drop-down list to specify a user attribute profile from which the user role or VLAN is derived. The user role can be derived from user attributes upon the client's association with an AP (this is known as a user-derived role). You can configure rules that assign a user role to clients that match a certain set of criteria. For example, you can configure a rule to assign the role VoIP-Phone to any client that has a MAC address that starts with bytes xx:yy:zz. User-derivation rules are executed before client authentication. Note that only wireless classification rules are listed in the drop-down menu.
- **Virtual AP Enable -** Enables/Disables the Wireless Authentication Profile.
- **Forward Mode -** Controls whether data is tunneled to the controller using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or using a combination of both depending on the destination (e.g., corporate traffic goes to the controller, and Internet access remains local). All forwarding modes support band steering, TSPEC/TCLAS enforcement, 802.11k and station blacklisting.
    - **Tunnel -** The AP handles all 802.11 association requests and responses, but sends all 802.11 data packets, action frames, and EAPOL frames over a GRE tunnel to the controller for processing. The controller removes or adds the GRE headers, decrypts or encrypts 802.11 frames, and applies firewall rules to the user traffic as usual. Both remote and campus APs can be configured in tunnel mode.
    - **Bridge -** 802.11 frames are bridged into the local Ethernet LAN. When a remote AP or campus AP is in bridge mode, the AP (and not the controller) handles all 802.11 association requests and responses, encryption/decryption processes, and firewall enforcement. The 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed.
    - **Split Tunnel -** 802.11 frames are either tunneled or bridged, depending on the destination (e.g., corporate traffic goes to the controller, and Internet access remains local).
    - **Decrypt Tunnel -** Both remote and campus APs can be configured in decrypt-tunnel mode. When an AP uses decrypt-tunnel forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the controller, which then applies firewall policies to the user traffic.
- **Allowed Band -** The band(s) on which to use the Virtual AP:
    - **a -** 802.11a band only (5 GHz)
    - **g -** 802.11b/g band only (2.4 GHz)
    - **all -** Both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz). (Default).
- **Band Steering -** Enables/Disables Band Steering. Band Steering encourages dual-band capable clients to stay on the 5GHz band on dual-band APs. This frees up resources on the 2.4GHz band for single band clients like VoIP phones. The feature supports both campus APs and remote APs that have a virtual AP profile set to tunnel , split-tunnel or bridge forwarding mode. Note, however, that if a campus or remote APs have virtual AP profiles configured in bridge or split-tunnel forwarding mode but no virtual APs in tunnel mode, those APs will gather information about 5G-

capable clients independently and will not exchange this information with other APs that only have bridge or split-tunnel virtual APs configured.

- **Steering Mode -** Band steering supports the following three band steering modes.
  - **Force-5GHz -** The AP will try to force 5Ghz-capable APs to use that radio band.
  - **Prefer-5GHz -**The AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts. (Default)
  - **Band Balancing -** The AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5Ghz band has more channels than the 2.4 GHz band, and that the 5Ghz channels operate in 40MHz while the 2.5Ghz band operates in 20MHz.
- **Dynamic Multicast Optimization -** Enables/Disables Dynamic Multicast Optimization.
- **Dynamic Multicast Optimization Threshold -** The maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops. (Range = 2 - 255, Default = 5)
- **Drop All Broadcast or Multicast Traffic -** If "Enabled", broadcast and multicast traffic is dropped. Do not enable this option for Virtual APs configured in bridge forwarding mode. This configuration parameter is only intended for use for Virtual APs in tunnel mode. In tunnel mode, all packets travel to the controller, so the controller is able to drop all broadcast traffic. When a Virtual AP is configured to use bridge forwarding mode, most data traffic stays local to the AP, and the controller is not able to filter out that broadcast traffic.
- **Convert Broadcast ARP Requests To Unicast -** If "Enabled", all broadcast ARP requests are converted to unicast and sent directly to the client. This configuration parameter is only intended for use for virtual APs in tunnel mode. In tunnel mode, all packets travel to the controller, so the controller is able to convert ARP requests directed to the broadcast address into unicast.

Assigning an Access Auth Profile

When you click the **Apply to Devices** button, the Access Auth Profile Assignments Screen appears. Follow the steps below to assign the profile to a Switch and/or an AP Group.

Assigning an Access Auth Profile to a Switch

An Access Auth Profile can be assigned to AOS Devices and/or Stellar APs.

Assigning an Access Auth Profile to AOS Devices

Click on the Devices **ADD/EDIT** buttons and select devices. The device(s) will appear in the List of Selected Devices. Click on the "Add Port" link under a device and select ports. Click on the "Port Type" link to select the port type (VLAN Port, SPB Access Port, VXLAN Access Port). (Default = VLAN Port).

If you are finished, click on the **Apply** button. The configuration will be applied and the assignment status displayed. Click **OK** to return to the Access Auth Profile Screen.

UNP VLANs for Silent Devices

When assigning an Access Authentication Profile, you can map a UNP VLAN to a UNP Port. This configures a Tagged or Untagged VLAN Port Association between the specified UNP Bridge Port and the VLAN This feature is useful when connecting "Silent" devices (e.g., printers) to Bridge Ports. The feature is supported on 6.x Switches (running AOS 6.7.1.R02 and higher) and 8.x Switches (running AOS 8.6R1 and higher).

Click on the Devices **ADD/EDIT** buttons and select devices. The device(s) will appear in the List of Selected Devices. Click on the "Add Port" link under a device and select ports. Click on the "Port Type" link to select the port type (VLAN Port, SPB Access Port, VXLAN Access Port).

Click on the "Add UNP VLANs" link under the device to bring up the UNP VLANs window.

- **6.x Switches -** Enter a VLAN and click on "+". Repeat to add additional VLANs. Click on **OK**.
- **8.x Switches -** Enter a VLAN, select a traffic type (Tagged or Untagged) and click on "+". Repeat to add additional VLANs. Click on **OK**.

If you are finished, click on the **Apply** button. The configuration will be applied and the assignment status displayed. Click **OK** to return to the Access Auth Profile Screen.

Assigning an Access Auth Profile to Stellar APs

You can assign an Access Auth Profile to Stellar APs with downlink ports (e.g., AP1201H). Click on the AP Groups **ADD/EDIT** buttons and select an AP Group(s). The AP Group(s) will appear in the List of Selected Groups. Three ports (Eth1, Eth2, Eth3) are displayed under the AP Group Name. Select a port(s). OmniVista will apply the profile to the selected ports on supported APs/ports in the AP Group. OmniVista will ignore unsupported APs/ports in the AP Group.

If you are finished, click on the **Apply** button. The configuration will be applied and the assignment status displayed. Click **OK** to return to the Access Auth Profile Screen.

Common Errors Seen When Assigning an Access Auth Profile

The following common errors may be seen in the Results page when attempting to assigning an Access Auth Profile to an AOS Switch. Possible causes are provided for each.

Error Message	Possible Cause(s)
"Failed to apply Access Auth Profile to port x/x/x"	• A member of Link-Agg, Port x/x/x is a Tagged Port.
"Port-Template applied to UNP Bridge Ports, cannot set L2 Profile on Bridge Ports"	• L2 Profile cannot be set when template is applied to UNP Bridge Ports. • UNP cannot be enabled on Tagged Port x/x/x. • UNP cannot be enabled on Service Access Port x/x/x. • VLAN ID xx does not exist. VLAN specified in "UNP VLANs" must exist on the switch. • VLAN ID xx is not a Standard VLAN. VLAN ID specified in "UNP VLANs" should be a Standard VLAN.

Editing an Access Auth Profile

Select the profile in the Access Auth Profile Screen and click on the Edit icon to bring up the Edit Access Auth Profile Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server. (Note that you cannot edit the Access Auth Profile Name.) If the Access Auth Profile has been applied to any devices, you will have to re-apply the profile to those devices. You can also go to the Device Config - Access Auth Profile Screen to edit a profile on any device.

To "unassign" an Access Auth Profile from a device, go the Device Config - Access Auth Profile Screen and delete the profile from the device. To "unassign" a profile from specific device ports, go the Device Config - Access Auth Profile Screen and delete the profile from the device. Then return to the Access Auth Profile Screen, select the profile and re-assign it to the device, selecting only those ports to which you want to assign the profile.

For example, if you had assigned Access Auth Profile 1 to ports 1/1, 1/2, 1/3, and 1/4 on a device and you want to remove it from ports 1/3 and 1/4. You would go to the Device Config - Access Auth Profile Screen and delete Access Auth Profile 1 from the device. Then return to the Access Auth Profile Screen, select Access Auth Profile 1 and re-assign it to the device, selecting only ports 1/1 and 1/2 on the Device Selection Screen.

Deleting an Access Auth Profile

Select the profile in the Access Auth Profile Screen and click on the Delete icon, then click **OK** at the confirmation prompt. This removes the profile from the server. If the profile has been assigned to any devices, go to the Device Config - Access Auth Profile Screen to remove the profile from the device(s). Select the applicable device(s) in the Devices - Access Auth Profile Table, click on the Delete icon, then click **OK** at the confirmation prompt.

WLAN Service Profile

The Unified Profile WLAN Service Profile Screen displays all configured WLAN Service Profiles and is used to create, clone, edit, and delete WLAN Services and assign the service to devices on the network.

Creating a WLAN Service Profile

Click on the Add icon. Enter a **Service Name** and configure the profile as described below, then click on the **Create** button. When you are finished, select the checkbox next to the profile and click on the **Apply to Devices** button to assign the profile to wireless devices on the network.

SSID Settings

Basic

- **ESSID -** User configured name that uniquely identifies a wireless network (up to 32 characters). If the ESSID includes spaces, you must enclose it in quotation marks.
- **Hide SSID -** Enables/Disables SSID in beacon frames. Note that hiding the SSID does very little to increase security. (Default = Disabled)
- **Enable SSID -** Enables/Disables the SSID.
- **Allowed Band -** The band(s) available on the service:
  - 2.4 GHz
  - 5 GHz

- All - 5 GHz and 2.4 GHz.

Security

- **Security Level -** Select the security level for the WLAN Service:
  - **Open -** The WI-FI will be unsecured. However, you can configure a default role or enable MAC Authentication to assign a role for clients (Default).
  - **Personal - T**he WI-FI will be protected by a key.
  - **Enterprise -** An authentication server will be used to authenticate the connecting client via 802.1x Authentication.
- **MAC Auth -** Enables/Disables MAC Authentication.
- **AAA Profile -** Select an AAA Profile to use for authentication. An AAA profile is required if the Security Level is set to "Enterprise" (to perform 802.1x authentication) or if MAC Authentication is enabled. This AAA Profile will be also used for Accounting purposes.
- **Classification Status -** Enables/Disabled classification. If classification is enabled, traffic will be classified to a role based on the configured classification rules. Note that the precedence of role assignment methods is important. Classification Rules are only used if 802.1x/MAC authentication does not return a role, or the returned role is not matched with any configured roles in the device.
- **MAC Pass Auth -** If MAC Authentication is enabled, select an Access Role Profile to assign to clients that pass MAC Authentication.
- **Default Access Role Profile -** Select the default Access Role Profile that will be applied to clients if a role cannot be assigned by other role assignment methods.
- **Client Isolation -** Enables/Disables Client Isolation. If enabled, traffic between clients on the same AP in the SSID is blocked; client traffic can only go toward the router. (Default = Disabled)

Advanced

Roaming Controls

- **L3 Roaming** - Enables/Disables Layer 3 roaming. Layer 3 roaming allows client to move between Access Points and connect to a new IP subnet and VLAN.
- **FBD Update on Association -** Enables/Disables FDB update on Association. If enabled, when a client roams to a new AP, the AP will send ARP packets to the uplink switch to notify the switch to change the downstream forwarding port for the wireless client's traffic.
- **802.11r -** Enables/Disables IEEE 802.11r (Fast BSS Transition). The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same group.
- **OKC -** Enables/Disables OKC Roaming. If OKC Roaming is enabled, a cached Pairwise Master Key (PMK) is used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1x authentication.
- **802.11k Status -** Enables/Disables 802.11k. The 802.11k protocol enables Stellar APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, Stellar APs and clients send neighbor reports, beacon reports, and link measurement reports to each other.

- **802.11v Status -** Enables/Disables 802.11v. 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an Instant AP to request a voice client to transition to a specific Stellar AP, or suggest a set of preferred Stellar APs to a client due to network load balancing or BSS termination. It also helps the client identify the best Stellar AP to transition to as they roam.

Client Controls

- **Max Number of Clients Per Band** - The maximum number of clients allowed in each band. (Range = 1 - 128, Default = 64)
- **802.11b Support -** Enables/Disables allowing 11b legacy clients connect to Stellar APs.
- **802.11g Support -** Enables/Disables allowing 11g legacy clients connect to Stellar APs.

Minimum Client Data Rate Controls

- **2.4GHz Minimum Client Data Rate Controller -** Enables/Disables 2.4G band access control based on client data rate.
- **2.4GHz Minimum Client Data Rate -** 2.4G band client with lower data speed will not be given access, recommended value 12.
- **5GHz Minimum Client Data Rate Controller -** Enables/Disables 5G band access control based on client data rate.
- **5GHz Minimum Client Data Rate -** 5G band client with lower data speed will not be given access, recommended value 24.

Minimum MGMT Rate Controls

- **2.4GHz Minimum MGMT Rate Controller -** Enables/Disables 2.4G band wireless management frame rate control.
- **2.4GHz Minimum MGMT Rate -** 2.4G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.
- **5GHz Minimum MGMT Rate Controller -** Enables/Disables 5G band wireless management frame rate control.
- **5GHz Minimum MGMT Rate -** 5G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.

High-Throughput Control

- **A-MSDU -** Enables/Disables Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.
- **A-MPDU -** Enables/Disables Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

QoS Settings

Configure the wireless QoS Settings for the profile as detailed below.

Bandwidth Contract

- **Upstream Bandwidth -** The maximum bandwidth for traffic from the switch to the client
- **Downstream Bandwidth -** The maximum bandwidth for traffic from the client to the switch.
- **Upstream Burst -** The maximum bucket size used for traffic from the switch to the client. The bucket size determines how much the traffic can burst over the maximum bandwidth rate
- **Downstream Burst -**The maximum bucket size used for traffic from the client to the switch. The bucket size determines how much the traffic can burst over the maximum bandwidth rate

Broadcast/Multicast Optimization

- **Broadcast Key Rotation -** Enables/Disables the broadcast key rotation function. If enabled, the broadcast key will be rotated after every interval time.
- **Broadcast Key Rotation Time Interval -** The interval, in minutes, to rotate the broadcast key (Range = 1 - 1440, Default = 15).
- **Broadcast Filter All -** This attribute is applicable to Stellar APs only. If enabled, all broadcast frames are dropped, except DHCP and Address Resolution Protocol (ARP) frames.
- **Broadcast Filter ARP -** This attribute is applicable to Stellar APs only. If enabled, the AP will act as an "ARP Proxy". If the ARP-request packet requests a client's MAC address and the AP knows the client's MAC and IP address, the AP will respond to the ARP-request but not forward the ARP-request (broadcast) to all broadcast domains. This reduces ARP broadcast packet forwarding and significantly improves network performance. Note that Stellar APs do not act as ARP proxy for Gratuitous ARP packets. When the station gets an IP from DHCP or IP release/ renew, the station will send Gratuitous ARP packets. AP will not respond to such special ARP packets and broadcast them normally.
- **Multicast Optimization -** Enable/Disables multicast traffic rate optimization.
- **Multicast Based Channel Utilization -** Configures based channel utilization optimization percentage. (Range = 0 - 100, Default = 90)
- **Number Of Clients -** Configure the threshold for multicast optimization. This is the maximum number of high-throughput stations.

802.1p Mapping

Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and 802.1p priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add icon. To remove a value, click on the "x" next to the value.

- **Background -** WMM Background will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 1)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 1, 2)

- **Best Effort -** WMM Best Effort will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 0)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 0, 3)
- **Video -** WMM Video will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 4)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 4, 5)
- **Voice -** WMM Voice will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 6)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 6, 7)

DSCP Mapping

Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and DSCP priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add icon. To remove a value, click on the "x" next to the value.

- **Background -** WMM Background will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 10)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 2, 10)
- **Best Effort -** WMM Best Effort will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 0)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 0, 18)
- **Video -** WMM Video will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 40)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 24, 36, 40)
- **Voice -** WMM Voice will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 46)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 46, 48, 56)

Legacy Wireless Settings

- **802.1x Authentication Profile -** The 802.1x Authentication Profile to use for legacy wireless devices.
- **MAC Authentication Profile -** The MAC Authentication Profile to use for legacy wireless devices.

- **User Derivation Rules -** Select a User Derivation Rule from the drop-down list to specify a user attribute profile from which the user role or VLAN is derived. The user role can be derived from user attributes upon the client's association with an AP (this is known as a user-derived role). You can configure rules that assign a user role to clients that match a certain set of criteria. For example, you can configure a rule to assign the role VoIP-Phone to any client that has a MAC address that starts with bytes xx:yy:zz. User-derivation rules are executed before client authentication. Note that only wireless classification rules are listed in the drop-down menu.
- **Virtual AP Enable -** Enables/Disables the Wireless Authentication Profile.
- **Forward Mode -** Controls whether data is tunneled to the controller using generic routingencapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or using a combination of both depending on the destination (e.g., corporate traffic goes to the controller, and Internet access remains local). All forwarding modes support band steering, TSPEC/TCLAS enforcement, 802.11k and station blacklisting.
  - **Tunnel -** The AP handles all 802.11 association requests and responses, but sends all 802.11 data packets, action frames, and EAPOL frames over a GRE tunnel to the controller for processing. The controller removes or adds the GRE headers, decrypts or encrypts 802.11 frames, and applies firewall rules to the user traffic as usual. Both remote and campus APs can be configured in tunnel mode.
  - **Bridge -** 802.11 frames are bridged into the local Ethernet LAN. When a remote AP or campus AP is in bridge mode, the AP (and not the controller) handles all 802.11 association requests and responses, encryption/decryption processes, and firewall enforcement. The 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed.
  - **Split Tunnel -** 802.11 frames are either tunneled or bridged, depending on the destination (e.g., corporate traffic goes to the controller, and Internet access remains local).
  - **Decrypt Tunnel -** Both remote and campus APs can be configured in decrypt-tunnel mode. When an AP uses decrypt-tunnel forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the controller, which then applies firewall policies to the user traffic.
- **Dynamic Multicast Optimization Threshold -** The maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops. (Range = 2 - 255, Default = 5)
- **Band Steering -** Enables/Disables Band Steering. Band Steering encourages dual-band capable clients to stay on the 5GHz band on dual-band APs. This frees up resources on the 2.4GHz band for single band clients like VoIP phones. The feature supports both campus APs and remote APs that have a virtual AP profile set to tunnel , split-tunnel or bridge forwarding mode. Note, however, that if a campus or remote APs have virtual AP profiles configured in bridge or split-tunnel forwarding mode but no virtual APs in tunnel mode, those APs will gather information about 5G-capable clients independently and will not exchange this information with other APs that only have bridge or split-tunnel virtual APs configured.
- **Steering Mode -** Band steering supports the following three band steering modes.
  - **Force-5GHz -** The AP will try to force 5Ghz-capable APs to use that radio band.

- **Prefer-5GHz -**The AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts. (Default)
- **Band Balancing -** The AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5Ghz band has more channels than the 2.4 GHz band, and that the 5Ghz channels operate in 40MHz while the 2.5Ghz band operates in 20MHz.

- **Broadcast Filter ARP** - Enables/Disables the Broadcast Filter ARP function. If enabled, broadcast ARP requests and responses are converted to unicast.

Cloning a WLAN Service Profile

You can quickly create an WLAN Service Profile by selecting a profile in the WLAN Service Profile List, clicking on the **Clone** button and modifying the profile to create a new one. Click on the **Copy** button to create the new profile.

Assigning a WLAN Service Profile

When you click the **Apply to Devices** button, the WLAN Service Assignments Screen appears. Click on the Devices **ADD** button and/or the AP Group **ADD** button to select devices. The device(s) will appear in the List of Selected Devices. If necessary, click on the Devices **EDIT** button and/or the AP Group **EDIT** button to add/remove devices from the list. When you are finished, click on the **Apply** button.

Editing a WLAN Service Profile

Select the profile in the WLAN Service Profile Screen and click on the Edit icon to bring up the Edit WLAN Service Profile Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server.

Deleting a WLAN Service Profile

Select the profile in the WLAN Service Profile Screen and click on the Delete icon, then click **OK** at the confirmation prompt. This removes the profile from the server.

Access Role Profile

The Unified Profile Access Role Profile Screen displays all configured Access Role Profiles and is used to create, clone, edit, and delete Access Role Profiles. An Access Role Profile contains the various UNP properties (e.g., QoS Policy List attached to the UNP, Captive Portal Authentication) for users assigned to the profile. In a wireless-centric network, an Access Role Profile is considered as a user role with which every client in the wireless-centric network is associated.

> **Note:** The Default WLAN Profile is a built-in profile for AOS Switches to set up edge infrastructure for a WLAN. Only the Auth Flag, Mobile Tag Status, and Policy List fields can be modified. However, you can clone the profile to create a new profile. Also note that the Default WLAN Profile cannot be deleted.

Creating an Access Role Profile

Click on the Add icon. Enter a **Profile Name** and configure the profile as described below, then click on the **Create** button. When you are finished, select the checkbox next to the profile and

click on the **Apply to Devices** button to assign the profile to switches/wireless devices on the network.

> **Note:** You can select a device type from the Highlight drop-down menu at the top of the screen to highlight configuration parameters for specific device types (6x, 7x, 8x). Selecting the "Highlight attributes applicable for 5x" option does not show a 5x indicator for any of the attributes, as only the profile name is applicable to 5x devices. In addition, 5x devices do not support dynamic VLAN configuration. Make sure the VLAN specified for the Access Role profile already exists.

Access Role Profile Attributes

General

- **Auth Flag -** Enables/Disables authentication (not supported on wireless devices and ignored when applied to those devices).
- **Mobile Tag Status -** Enables/Disables classification of tagged packets received on mobile ports (not supported on wireless devices and ignored when applied to those devices).
- **Redirect Status -** Enables/Disables Captive Portal Redirect (not supported on wireless devices and ignored when applied to those devices). Note that if Redirect Status is enabled, the Access Role Profile can only map to a VLAN when applying the profile to a device.
- **Policy List -** An Access Role Profile can also be configured with an existing Policy List. The set of rules within the Policy List are then applied to the traffic that passes though switches/wireless devices. Only one Policy List is allowed per profile, but multiple profiles may use the same Policy List. Select a Policy List for the profile from the drop-down menu. You can also click the "Add New" link to go to the Unified Policy Lists Screen to create a new one. An existing Policy List can be a Unified Policy List or a Policy List created in PolicyView - Expert Mode. See Note below for additional information.
- **Location Policy Name -** Select a Location Access Policy from the drop-down menu.
- **Period Policy Name -** Select a Period Policy from the drop-down menu.
- **Inactivity Interval -** The amount of time, in seconds, before an authenticated device is automatically logged out of the network due to inactivity (MAC address for the device has aged out). This timer value applies only to devices learned in the profile.

  Note: You can use a Unified Policy List or a Policy List created in PolicyView - Expert Mode in an Access Role Profile. If you use a Policy List in an Access Role Profile, you must apply the Access Role Profile to the same devices selected for the policies contained in the Policy List. Also note that policies created in PolicyView can only be applied to AOS Devices, not to APs.

Bandwidth Control Settings

- **Upstream Bandwidth -** The maximum bandwidth limit allocated for ingress traffic on UNP ports assigned to the profile. If the maximum ingress bandwidth value is set to zero, all ingress traffic is allowed on the UNP port. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)

- **Downstream Bandwidth -** The maximum bandwidth limit allocated for egress traffic on UNP ports assigned to the profile. If the maximum egress bandwidth value is set to zero, all egress traffic is allowed on the UNP port. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)
- **Upstream Burst -** The maximum ingress depth value that is applied to traffic on UNP ports that are assigned to the profile. This value determines how much the traffic can burst over the maximum ingress bandwidth rate. The maximum ingress depth value is configured in conjunction with the maximum ingress bandwidth parameter. When the ingress depth value is reached, the switch starts to drop packets. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)
- **Downstream Burst -** The maximum egress depth value that is applied to traffic on UNP ports that are assigned to profile. This value determines how much the traffic can burst over the maximum egress bandwidth rate. The maximum egress depth value is configured in conjunction with the maximum egress bandwidth parameter. When the egress depth value is reached, the switch starts to drop packets. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)

Client Session Logging

- **Client Session Logging -** Enables/Disables client session logging.
- **Client Connection Logging Level -** Select a logging level:
    - **Logging HTTP/HTTPs -** Log only the HTTP/HTTPs web session of wireless clients.
    - **Logging ALL -** Log all sessions of wireless clients, including HTTP/HTTPs.
    - **None -** Log only client online/offline behavior, without session details.

Web Content Filtering (WCF)

- **WCF Profile -** Select a WCF Profile from the drop-down to include in the Access Role Profile. If necessary, click on **Add New** to bring up the WCF Profile Screen to add a new profile. An Access Role Profile can only contain one WCF Profile.

Walled Garden

- **Wireless Client Social Login Vendor -** Select a vendor(s) to allow a wireless client to authenticate through a social media vendor (Facebook, Google, and Rainbow are supported). OmniVista will automatically configure the Allowlist Domains for the selected vendor(s). This will allow the user to connect over the Internet to the selected vendor(s) for authentication.
- **Allowlist Domains -** In addition to Facebook, Google, and Rainbow login, you can enter any Allowlist Domain to allow a user to connect to sites over the Internet without authentication. For example, a hotel may want to allow a guest to connect to their website without authentication. Enter the Allowlist Domain and click on the Add icon to allow access to the site. Repeat to add additional domains. Domains must be entered in Fully Qualified Domain Name (FQDN) format (e.g., www.marriot.com, www.bbc.com). IP Addresses and http/https prefixes should **not** be used.

Client Isolation: Allowed Contacts List

- **Allowed list of devices for an isolated client** - When Client Isolation is enabled for the client SSID or the Access Authentication Profile for the switch port to which the AP is connected, traffic between clients on the same AP in the SSID is blocked; client traffic can only go toward the default gateway. To identify the devices a client is allowed to contact when Client Isolation is enabled, enter the MAC address for each device. You can manually specify or copy and paste the device MAC address using any of the following formats:
  - 00:80:0f:33:33:24
  - 00-80-0f-33-33-24
  - 00800f333324
  - 008.00f.333.324
  - 00800f.333324
  - 00:d0:95* (trailing wildcard character "*" specifies all MAC addresses beginning with 00:d0:95) This wildcard format is particularly useful for entering a vendor OUI only and not the full MAC address for all the vendor devices.

Captive Portal Attributes

- **Captive Portal Auth -** To configure Captive Portal Authentication, select **None**, **Internal**, or **External** authentication and complete the required fields for the selected authentication type.
- **None**
  - **Redirect URL -** Redirect URL is only used for ClearPass Servers. Make sure a ClearPass server exists on the system before entering the URL.
- **Internal**
  - **Captive Portal Profile -** A Captive Portal Profile can be applied to AOS devices. Only one Captive Portal Profile is allowed per profile, but multiple profiles may use the same Captive Portal Profile. Select a Captive Portal Profile for the profile from the drop-down menu. You can also click the "Add New" link to go to the **Captive Portal Profile** Screen to create a new one. (Not supported on wireless devices and ignored when applied to those devices.)
- **External**
  - **Portal Server -** The FQDN/IP address of the external captive portal server.
  - **Redirect URL -** The redirect URL for the captive portal authentication.
  - **HTTPS Redirection -** Specify whether the redirect portal page is using HTTPS protocol.
  - **AAA Server Profile -** The AAA Server used for Captive Portal Authentication.
  - **Custom Profile -** The External Captive Portal Config File used for communication between APs and the External Portal Server. The External Captive Portal Config File is configured on the AP Groups Screen in the AP Registration application.

Advanced

- **DHCP Option 82 -** Enables/Disabled the DHCP Option 82 Feature. If necessary, click on the link to go to the DHCP Option 82 Screen to configure the feature.

Cloning an Access Role Profile

You can quickly create an Access Role Profile by selecting a profile in the Access Role Profile List, clicking on the **Clone** button and modifying the profile to create a new one. Click on the **Copy** button to create the new profile.

Assigning an Access Role Profile

When you click the **Apply To Devices** button, the Access Role Profile Assignments Wizard appears. Complete the screens as described below, then click on the **Apply** button.

Select Devices

Configure the mapping method and select devices.

Configure the Mapping Method

You can map the Access Role Profile to a specific VLAN or service. Select a **Mapping Method**, then make a selection from the drop-down menu. Note that you can only use one mapping method for a profile.

- **Map to VLAN -** Maps the profile to a specific VLAN on network devices. Select a VLAN from the **VLANs** drop-down. For APs, you can map an Access Role Profile to untagged traffic. In the **VLANs** drop-down, select **Untagged VLAN**. Then click on the **ADD** button to select an AP Group(s) (the Devices ADD button will be grayed out). To map the same Access Role Profile to AOS Devices, you will have to repeat the process and specify a VLAN. Note that for Stellar APs, the VLAN ID must be between 1 and 4094 or "untagged". If any other value is configured, the device will ignore the VLAN configuration. Also note that for Stellar APs you can select a VLAN Pool, by entering multiple VLANs. You can enter VLANs as a range (e.g., 10-20), as individual VLANs (21, 23, 25), or both (10-20, 21,23, 25). Note that you can map an Access Role Profile to a dynamically-created VLAN on 6.x and 8.x Switches.
- **Map to SPB -** Maps the profile to an SPB Profile.
- **Map to VXLAN -** Maps the profile to a VXLAN Profile.
- **Map to Static Service -** Maps the profile to a Static Service.
- **Map to Tunnel -** Maps the profile to a Guest Tunnel (supported on OS6860, 6860E, OS6900-Q32/X72, OS9900, OS6560, OS6865 Switches).
- **Map to VLAN and Tunnel -** Maps the profile to a VLAN and a Tunnel, allowing VLAN tagging inside the GRE.

Dynamic VLAN Mapping

On 6.x Switches (running 6.7R08 and higher) and 8.x Switches (running 8.6R1 and higher) you can map an Access Role Profile to a dynamically-created VLAN. On 6.x Switches, you can map an Access Role Profile to a VLAN learned by a dynamic protocol (e.g., MVRP). The VLAN must be present on the switch. On 8.x Switches you can map an Access Role Profile to any VLAN

even if the VLAN does not yet exist on the switch. The switch will create a UNP Dynamic VLAN. In both cases, the switch will decide whether it will permit the mapping.

> **Important Note:** For dynamic VLAN mapping, you must **first** configure a Unified Access Global Configuration Setting with Global Dynamic UNP VLAN creation enabled, and assign that Global Configuration to network switches. Global Configurations are configured on the Unified Access Global Configuration Setting Screen (Unified Access - Unified Profile - Template - Global Configuration - Setting). See the Global Configuration Setting Screen online help for more information. You can also enable dynamic VLAN mapping on a device by editing a device on the Unified Access Unified Profile – Device Config - Global Configuration Setting Screen (Unified Access - Unified Profile – Device Config - Global Configuration - Setting). See the Device Config Global Configuration Setting Screen online help for more information.

Select Devices

After configuring the Mapping Method, click on the Devices **ADD** button and/or the AP Group **ADD** button to select devices. The device(s) will appear in the List of Selected Devices. If necessary, click on the Devices **EDIT** button and/or the AP Group **EDIT** button to add/remove devices from the list. See Common Errors When Assigning an Access Role Profile if you receive an error message when assigning a profile.

> **Note:** If the Access Role Profile contains a Policy List, you must assign the profile to the same devices that are included in the Policies contained in the Policy List.
>
> **Note:** You can also assign an Access Role Profile to a ClearPass Server. If a ClearPass Server is configured and connectivity established, the server will appear in the Device Selection Window in Blue.

Click on the **Next** button to configure a Period Policy.

Configure a Period Policy

You can specify the days and times during which a client can access devices. Select a Period Policy, then click on the **Next** button to configure a Location Policy.

Configure a Location Policy

You can specify the location of clients that can access devices. Select a Location Policy, then click on the **Next** button to review the configuration.

Review

Review the configuration and click on the **Apply** button to apply the policy to appendices Groups.

Common Errors When Assigning an Access Role Profile

The following common errors may be seen in the Results page when attempting to assign an Access Role Profile.Possible causes are provided for each.

Error Message	Possible Cause(s)
"Failed to apply Access Role Profile to VLAN ID 4094"	• VLAN ID xx is not a standard VLAN.

"VLAN ID xx does not exist"	• The VLAN specified must exist on the switch.
"VLAN ID xx is not a standard VLAN"	• The specified VLAN should be a Standard VLAN.

Editing an Access Role Profile

Select the profile in the Access Role Profile List and click on the Edit icon to bring up the Edit Access Role Profile Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server. (Note that you cannot edit the Access Role Profile Name.) If the Access Role Profile has been applied to any devices, you must re-apply the profile to those devices. You can also go to the Device Config - Access Role Profile Screen to edit a profile on any device.

> **Note:** The Default WLAN Profile is a built-in profile for AOS Switches to set up edge infrastructure for a WLAN. Only the Auth Flag, Mobile Tag Status, and Policy List fields can be modified. However, you can clone the profile to create a new profile.

Deleting an Access Role Profile

Select the profile in the Access Role Profile Screen and click on the Delete icon, then click **OK** at the confirmation prompt. This removes the profile from the server. If the profile has been assigned to any devices, go to the Device Config - Access Role Profile Screen to remove the profile from the device(s). Select the applicable device(s) in the Devices - Access Role Profile Table, click on the Delete icon, then click **OK** at the confirmation prompt.

> **Note:** You cannot delete the Default WLAN Profile.

AAA Server Profile

The Unified Profile AAA Server Profile Screen displays all configured AAA Server Profiles and is used to create, edit, and delete AAA Server Profiles for AOS 8.x Switches and Server Groups for Wireless Controllers. AAA Server Profiles are used to define specific AAA parameters that can be used in an Access Auth Profile or Captive Portal Profile.

> **Note:** When an AAA Server Profile is assigned to a UNP Edge port/virtual AP through an Access Auth Profile, the parameter values defined in the profile will override any existing global AAA configuration for users authenticating on that port/virtual AP.

Creating an AAA Server Profile

Click on the Add icon. Enter a **Profile Name** and configure the Profile as described below, then click on the **Create** button.

Authentication Servers

- **802.1X Primary -** Select a Primary 802.1X Authentication Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the Add icon to go to the Authentication Servers Application and create a new server. The Link takes you to the RADIUS Server Management Screen in the Authentication Server application. You can click on one of the other links on the left side of the screen to create a different Authentication Server type (LDAP, ACE, TACACS+).

For wireless devices, 802.1x Primary and Secondary Server configurations will help you to create 802.1x Authentication Server Group which will be used by Access Auth Profiles (Wireless AAA Server Profiles).

- **Captive Portal Primary -** Select a Primary Captive Portal Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the Add icon to go to Authentication Servers Application and create a new Server. The Link takes you to the RADIUS Server Management Screen in the Authentication Server application. You can click on one of the other links on the left side of the screen to create a different Authentication Server type (LDAP, ACE, TACACS+).

  Note: Captive Portal Primary and Secondary Server configurations are ignored for wireless devices.

- **MAC Primary-** Select a Primary MAC Authentication Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the Add icon to go to Authentication Servers Application and create a new Server. The Link takes you to the RADIUS Server Management Screen in the Authentication Server application. You can click on one of the other links on the left side of the screen to create a different Authentication Server type (LDAP, ACE, TACACS+).

  Note: For wireless devices, MAC Primary and Secondary Server configurations will help you to create a MAC Authentication Server Group that will be used by Access Auth Profiles (Wireless AAA Server Profiles). For IAP Devices, there is not a separate server for MAC Authentication. 802.1x Primary and Secondary Servers are used instead.

Accounting Servers

- **802.1X Primary -** Select a Primary 802.1X Accounting Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the "Add New" link to go to the RADIUS Server Management Screen and create a new Server.
- **Captive Portal Primary -** You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the "Add New" link to go to the RADIUS Server Management Screen and create a new Server.
- **MAC Primary -** Select a Primary MAC Accounting Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the "Add New" link to go to the RADIUS Server Management Screen and create a new Server.

  Note: For wireless devices, Accounting Servers will help you to create an Accounting Radius Server Group that will be used in Access Auth Profiles (Wireless AAA Server Profiles). Captive Portal Primary and Secondary Servers are ignored. Wireless Devices only accept Radius servers for Accounting. If you select another type, an error will occur when you try to apply the configuration to Wireless Controllers.

Advanced Settings

Advanced settings are not supported on wireless devices and will be ignored when applied to those devices.

MAC Auth

- **Session Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for MAC Authenticated users. If Enabled, the switch will use the Session Timeout attribute received from the Authentication Server in an Accept-Accept message. If Disabled, the switch uses the locally configured timeout interval value (Default = Disabled).
- **Session Timeout Status -** Enables/Disables the Session Timeout option for MAC Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Session Timeout Interval. (Default = Disabled).
- **Session Timeout Interval -** The Session Timeout value, in seconds. When the Session Timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed. Note that when the Session Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again (Range = 12000 - 86400, Default = 43200).
- **Inactivity Timeout Status -** Enables/Disables the Inactivity Timeout option for MAC Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Inactivity Timeout Interval (Default = Disabled).
- **Inactivity Timeout Interval -** The Inactivity Timeout value, in seconds. Make sure the configured value is value greater than the MAC address aging time for the switch. If the Timeout Value is exceeded, the user is not logged out of the network if the MAC address aging time expires before the configured timeout value. Also note that when the Inactivity Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.(Range = 60 - 1200, Default = 600)
- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for MAC Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- **Accounting Interim Interval -** The amount of time between each interim accounting update for MAC accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

802.1X

- **Re-Authentication Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for 802.1x Authenticated users. If Enabled, the Session-Timeout attribute value received from the RADIUS server overrides the locally configured value for the switch. (Default = Disabled).

- **Re-Authentication Timeout -** Enables/Disables the automatic re-authentication of authenticated 802.1X users (Default = Disabled).
- **Re-Authentication Interval -** The amount of time the switch waits, in seconds, before triggering re-authentication of 802.1X users. Note that when the re-authentication time interval is changed, the new value does not apply to existing authenticated 802.1X users until the user is flushed out or when the user is authenticated again. Any new 802.1X users are re-authenticated based on the current time interval setting. (Range = 600 - 7200, Default = 3600)
- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for 802.1X authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- **Accounting Interim Interval -** The amount of time between each interim accounting update for 802.1x accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

Captive Portal

- **Session Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for Captive Portal Authenticated users. If Enabled, the switch will use the Session Timeout attribute received from the RADIUS server in an Accept-Accept message. If Disabled, the switch to use the locally configured timeout interval value (Default = Disabled).
- **Session Timeout Status -** Enables/Disables the Session Timeout option for Captive Portal Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Session Timeout Interval. (Default = Disabled).
- **Session Timeout Interval -** The Session Timeout value, in seconds. When the Session Timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed. Note that when the Session Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again (Range = 12000 - 86400, Default = 43200).
- **Inactivity Timeout Status -** Enables/Disables the Inactivity Timeout option for Captive Portal Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Inactivity Timeout Interval (Default = Disabled).
- **Inactivity Timeout Interval -** The Inactivity Timeout value, in seconds. Make sure the configured value is value greater than the MAC address aging time for the switch. If the Timeout Value is exceeded, the user is not logged out of the network if the MAC address aging time expires before the configured timeout value. Also note that when the Inactivity Timeout Interval is changed, the new value does not apply to existing authenticated

users until the user is flushed out or when the user is authenticated again. (Range = 60 - 1200, Default - 600)

- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for Captive Portal Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- **Accounting Interim Interval -** The amount of time between each interim accounting update for Captive Portal accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

RADIUS

- **NAS Port ID -** The RADIUS client NAS-Port attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to define a NAS-Port identifier for the NAS-Port attribute. "Default" sets the NAS-Port attribute value to the chassis/slot/port of the user. The NAS-Port attribute value specified with this command is used in Account-Request messages and in Accounting-Request messages.
- **NAS ID -** The RADIUS client NAS-Identifier attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to identify the switch (RADIUS client) in the NAS-Identifier attribute. "Default" sets the NAS-Identifier attribute to the system name of the switch. The NAS-Identifier attribute value specified with this command is used in both Account-Request and Accounting-Request messages.
- **Username Delimiter -** The delimiter character used to separate fields within a RADIUS Server User Name.
- **Password Delimiter -** The delimiter character used to separate fields within a RADIUS Server Password.
- **Calling Station Delimiter -** The delimiter character used to separate fields within a Calling Station ID.
- **Called Station Delimiter -** The delimiter character used to separate fields within a Called Station ID.
- **Username Case -** Indicates if the RADIUS Server User Name must be in Upper Case or Lower Case.
- **Password Case -** Indicates if the RADIUS Server Password must be in Upper Case or Lower Case.
- **Calling Station ID Case -** Indicates if the Calling Station ID must be in Upper Case or Lower Case.
- **Called Station ID Case -** Indicates if the Called Station ID must be in Upper Case or Lower Case.

Editing an AAA Server Profile

Select the profile in the AAA Server Profile Screen and click on the Edit icon to bring up the Edit AAA Server Profile Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server. Note that if the AAA Server Profile has been applied to any devices through an Access Auth Profile or Captive Portal Profile, you will have to re-apply the associated Access Auth Profile or Captive Portal Profile to those devices to update the profile on the device(s).

Deleting an AAA Server Profile

Select the profile in the AAA Server Profile Screen and click on the Delete icon, then click **OK** at the confirmation prompt.

- If the profile has **not** been associated with an Access Auth Profile or Captive Portal Profile, the update will be applied and the status displayed. Click **OK** to return to the AAA Server Profile Screen.
- If the profile has been associated with an Access Auth Profile or Captive Portal Profile, the "Delete AAA Server Profile" confirmation prompt will appear listing any associated profiles. You must delete the AAA Server Profile from any associated profile(s) before returning to the AAA Server Profile Screen to delete the AAA Profile.

Location Policy

The Unified Profile Location Policy Screen displays all configured Location Policies is used to create, clone, edit, and delete Location Policies. A Location Policy defines a specific location where a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.

Creating a Location Policy

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Apply** button.

- **Location Policy Name -** User-configured Location Policy Name.
- **System Location -** The configured system location for the switch from which the device can access the network.
- **System Name -** The configured system name for the switch from which the device can access the network.

Cloning a Location Policy

You can clone an existing Location Policy and edit it to quickly create a new policy. Select a profile in the Location Policy List and click on the **Clone** button. Enter a new Location Policy Name, edit the fields as necessary and click on the **Clone** button.

Editing a Location Policy

Select the policy in the Location Policy List and click on the Edit icon to bring up the Edit Location Policy Screen. Edit the fields as described above then click on the **Apply** button to save the changes. Note that you cannot edit the profile name.

Deleting a Location Policy

Select the policy in the Location Policy List and click on the Delete icon, then click **OK** at the confirmation prompt.

Period Policy

The Unified Profile Period Policy Screen displays all configured Period Policies is used to create, clone, edit, and delete Period Policies. A Period Policy specifies the days and times during which a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.

Creating a Period Policy

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Apply** button.

- **Period Policy Name -** User-configured Period Policy Name.
- **Date/Time** - Click on the Days/Months, Date/Time, and Time of Day sliders to configure the time when the devices can access the network.
- **Timezone -** Select the in which the Period Policy is active.

Cloning a Period Policy

You can clone an existing Period Policy and edit it to quickly create a new policy. Select a profile in the Period Policy List and click on the **Clone** button. Enter a new Period Policy Name, edit the fields as necessary and click on the **Clone** button.

Editing a Period Policy

Select the policy in the Period Policy List and click on the Edit icon to bring up the Edit Period Policy Screen. Edit the fields as described above then click on the **Apply** button to save the changes. Note that you cannot edit the profile name.

Deleting a Period Policy

Select the policy in the Period Policy List and click on the Delete icon, then click **OK** at the confirmation prompt.

Access Classification

The Unified Profile Access Classification Screen displays all Access Classification Rules configured for Access Role Profiles and is used to create edit, and delete Access Classification Rules (Access Classification Rules in AOS Switches and User Rules in wireless devices). Access Classification Rules are defined and associated with an Access Role Profile to provide an additional method for classifying a device into an Access Role Profile. If authentication is not available or does not return a profile name for whatever reason, Access Classification rules are applied to determine the profile assignment.

Creating an Access Classification Rule

Click on the Add icon. Select a **Rule Type** from the drop-down menu. Configure the Rule as described below, select the **Access Role Profile** for which you want to configure the rule, then

click on the **Create** button. When you are finished, click on the **Apply to Devices** button to assign the Rule to switches/ports on the network.

Access Classification Rules

- **MAC Rule (Both AOS and Wireless Devices) -** Defines a MAC Address Access Classification Rule for the specified UNP Access Role Profile. If the source MAC address of the device traffic matches the MAC address defined for the rule, the specified Access Role Profile is applied. Note that when a MAC Access Classification Rule is removed or modified, all MAC addresses classified with that rule are flushed.
  - **Name -** User-configured name for the MAC Rule.
  - **MAC Address -** The MAC address to be used for the rule. If the source MAC address of the device traffic matches the MAC address defined for the rule, the specified Access Role Profile is applied.
  - **VLAN Tag -** An optional VLAN Tag. If configured, traffic must also match this VLAN Tag in addition to the source MAC address.
  - **Customer Domain ID -** An optional Customer Domain ID to which this rule will apply. When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.
  - **Access Role Profile -** Select the Access Role Profile to use for the rule.
- **MAC Range Rule (AOS Devices only) -** Defines a MAC Address Range Access Classification Rule for the specified UNP Access Role Profile. If the source MAC address of the device traffic matches any of the MAC address within the range of MAC addresses, the specified profile is applied. Note that when a MAC Access Classification Rule is removed or modified, all MAC addresses classified with that rule are flushed.
  - **MAC Low Address -** MAC address that defines the low end of the range (e.g., 00:00:39:59:f1:00).
  - **MAC High Address -** MAC address that defines the high end of the range (e.g., 00:00:39:59:f1:90).
  - **VLAN Tag -** An optional VLAN Tag. If configured, traffic must also match this VLAN Tag in addition to the source MAC address.
  - **Customer Domain ID -** An optional Customer Domain ID to which this rule will apply. When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.
  - **Access Role Profile -** Select the Access Role Profile to use for the rule.
- **IP Address Rule (AOS Devices only) -** Defines an IP Address Access Classification Rule for the specified UNP Access Role Profile. If the source IP address of the device traffic matches the IP address defined for the rule, the specified Access Role Profile is applied.
  - **IP Network Address -** The IPv4 network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0).
  - **IP Mask -** An IP address mask to identify the IP subnet for the interface (supports class-less masking).

  - **VLAN Tag -** An optional VLAN Tag. If configured, traffic must also match this VLAN Tag in addition to the source MAC address.
  - **Customer Domain ID -** An optional Customer Domain ID to which this rule will apply. When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.
  - **Access Role Profile -** Select the Access Role Profile to use for the rule.
- **VLAN Tag Rule -** Defines a VLAN Tag for the specified Access Classification Rule. If the source VLAN Tag of the device traffic matches the VLAN Tag defined for the rule, the specified Access Role Profile is applied.
  - **VLAN Tag -** The VLAN Tag used for the rule.
  - **Tag Position (7x only) -** The VLAN Tag position - Inner Tag (Default), Outer Tag.
  - **Customer Domain ID -** An optional Customer Domain ID to which this rule will apply. When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.
  - **Access Role Profile -** Select the Access Role Profile to use for the rule.
- **Location (Wireless Devices only) -** Defines a Location rule for the specified Access Role Profile. The specified Access Role Profile will be applied if the user location (AP name) matches with the value defined in the rule. Note that this rule applies only to Legacy AP devices; Stellar APs do not support Location-based rules.
  - **Name -** The rule name.
  - **Location -** The AP location.
  - **Access Role Profile -**Select the Access Role Profile to use for the rule.
- **ESSID (Wireless Devices only) -** Defines an Extended Service Set Identifier (ESSID) for the specified Access Role Profile. The specified Access Role Profile will be applied if the ESSID of AP (which client is associating) matches with the defined ESSID in the rule.
  - **Name -** The rule name.
  - **ESSID Value -** The ESSID of AP.
  - **Access Role Profile -**Select the Access Role Profile to use for the rule.
- **DHCP Option (Wireless Devices only) -** Defines a DHCP signature ID rule for the specified Access Role Profile.
  - **Name -** The rule name.
  - **Signature ID -** The DHCP signature ID.
  - **Access Role Profile -**Select the Access Role Profile to use for the rule.
- **DHCP Option 77 (Wireless Devices only) -** Defines a DHCP Option 77 rule for the specified Access Role Profile. The specified Access Role Profile will be applied if the user class identifier returned by DHCP server matches with the value defined in the rule.
  - **Name -** The rule name.
  - **Value -** The user class identifier returned by DHCP server.
  - **Access Role Profile -**Select the Access Role Profile to use for the rule.

- **Encryption Type (Wireless Devices only) -** Defines an Encryption Type rule for the specified Access Role Profile. The specified Access Role Profile will be applied if the encryption type used by the client matches with the value defined in the rule.
  - **Name -** The rule name.
  - **Encryption Type -** The encryption type used by the client (e.g., WPA/WPA2 AES, Dynamic WEP).
  - **Access Role Profile -**Select the Access Role Profile to use for the rule.

Editing an Access Classification Rule

Select the profile in the Classification Profile List and click on the Edit icon to bring up the Edit Access Classification Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server. Note that if the Access Role Profile has been applied to any devices, you will have to re-apply the profile to those devices. You can also go to the Device Config - Access Classification Screen to edit a profile on any device.

> **Note:** You cannot edit an Access Classification Rule Name.

Assigning an Access Classification Rule

When you click the **Apply To Devices** button, the Access Classification Assignments Screen appears. Select a Mapping Method, then select devices. When you are finished, click on the **Apply** button. Note that a VLAN must exist on a switch/wireless device to configure VLAN Mapping.

Select Mapping Methods

You can map the Access Classification Rule to a specific VLAN or service. Select a **Mapping Method**, then make a selection from the drop-down menu. Note that you can only use one mapping method for a profile.

- **Map to VLAN -** Maps the profile to a specific VLAN on network devices.
- **Map to SPB -** Maps the profile to an SPB Profile.
- **Map to VXLAN -** Maps the profile to a VXLAN Profile.
- **Map to Static Service -** Maps the profile to a Static Service.

Select Devices

After configuring the Mapping Method, click on the Devices **ADD** button and/or the AP Group **ADD** button to select devices. The device(s) will appear in the List of Selected Devices. If necessary, click on the Devices **EDIT** button and/or the AP Group **EDIT** button to add/remove devices from the list.

The devices presented will vary according to your Mapping Method. For example, if you selected VLAN Number 3, only those devices on which VLAN 3 is configured would be displayed. After selecting devices, click on the **Apply** button to assign the Access Classification Rule.

> **Note:** During assignment of **Extended Rule**, port selection is offered, but it is optional. The rule can only be assigned to UNP Ports. Select **Port Range** and use the **From Port** and **To Port** options to assign the rule to a port(s). A port range can only be populated with consecutively higher numbered ports. Select Group Port to assign the rule to a port group, instead of a port(s).

Deleting an Access Classification Rule

To delete a rule(s), select the Rule(s) in the table and click on the Delete icon, then click **OK** at the confirmation prompt. This removes the profile from the server. If the profile has been assigned to any devices, go to the Device Config - Access Classification Screen to remove the profile from the device(s). Select the applicable device(s) in the Devices - Classification Profile List, click on the Delete icon, then click **OK** at the confirmation prompt.

Customer Domain

The Unified Profile Customer Domain Screen displays all configured Customer Domains create, edit, and delete Customer Domains. Customer Domains provide an additional method for segregating device traffic. A Customer Domain is identified by a numerical ID, which can be assigned to UNP ports and Access Classification Rules. By default, all UNP ports (bridge and access) and profile rules are assigned to domain 0. The main benefit of Customer Domains is that they provide the ability to group physical UNP ports or link aggregates into one logical domain. Once a UNP port is assigned to a specific Customer Domain ID, only classification rules associated with the same ID are applied to that port.

An example of using customer domains would be to group UNP ports carrying traffic for a specific customer into the same domain (all Customer A ports assigned to Domain 2). Then assign VLAN and/or service profiles tailored for that customer to the same Domain ID (all profiles for Customer A assigned to Domain 2).

Creating a Customer Domain

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

- **Customer Domain ID -** An ID number for the Customer Domain.
- **Customer Domain Description -** A description for the Customer Domain Profile.

Editing a Customer Domain

Select the profile in the Customer Domain List and click on the Edit icon to bring up the Edit Customer Domain Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server. Note that if the Customer Domain Profile has been applied to any devices through an Access Classification Profile, you will have to re-apply the associated Access Classification Profile to those devices to update the profile on the device(s).

Deleting a Customer Domain

Select the profile in the Customer Domain List and click on the Delete icon, then click **OK** at the confirmation prompt. If the Customer Domain Profile has been applied to any devices through an Access Classification Profile, you will have to re-apply the associated Access Classification Profile to any devices to update the profile on the device(s).

- If the Customer Domain has **not** been associated with an Access Classification Profile, the update will be applied and the status displayed. Click **OK** to return to the AAA Server Profile Screen.
- If the Customer Domain has been associated with an Access Classification Profile, the "Delete" confirmation prompt will appear listing any associated profiles. You must delete the Customer Domain Profile from any associated profile(s) before returning to the Customer Domain Screen to delete the Customer Domain Profile.

SPB Profile

The Unified Profile SPB Profile Screen displays all configured Shortest Path Bridging (SPB) Profiles and is used to create, edit, and delete SPB Profiles. When you create an SPB Profile, you configure the parameters that can be mapped to an Access Role Profile. When a device is dynamically assigned to the profile through authentication or classification, and SPB Service Access Point (SAP) is automatically created using the specified profile parameters. Traffic from the device is then forwarded on the SAP.

Creating an SPB Profile

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

- **SPB Profile Name -** The SPB Profile name.
- **Tag Value -** The VLAN tag information from classified traffic used to create the Service Access Point (SAP) for the traffic. If the traffic is untagged, the SAP is created with 0 as the encapsulation value (for example, 1/12:0).
- **ISID -** A service instance identifier (ISID) that is used to identify an SPB service in a provider backbone bridge (PBB) network. The valid range is 256 - 16777214.
- **BVLAN -** The VLAN ID number of an existing SPB backbone VLAN (BVLAN).
- **VLAN Translation -** Enables/Disables egress VLAN translation for the service.
- **Multicast Mode -** Select the multicast mode from the drop-down menu:
  - **Headend** - Specifies the head-end replication mode for the service.
  - **Tandem -** Specifies the tandem replication mode for the service.

Editing an SPB Profile

Select the profile in the SPB Profile List and click on the Edit icon to bring up the Edit SPB Profile Screen. Edit the fields as described above then click on the **Apply** button. Note that you cannot edit the profile name.

Deleting an SPB Profile

Select the profile in the SPB Profile List and click on the Delete icon, then click **OK** at the confirmation prompt.

Far End IP

The Unified Profile Far End IP Screen displays all configured Far End IP Lists and is used to create, edit, and delete Far End IP Lists. Each IP address in a list is assigned to the Loopback0 interface of a far-end VXLAN node. The list name is assigned to an Access Role Profile through the mapping of VXLAN service parameters to the profile. This allows multiple far-end nodes to be associated with the service created for the VXLAN Network ID (VNID) specified in a VXLAN Profile.

Creating a Far End IP List

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Apply** button.

- **Name -** The Far End IP List name

- **IP Address -** Enter an IP address and click on the Add icon. Repeat to add additional IP addresses. Click on the Delete icon to remove an IP address.

Editing a Far End IP List

Select the list in the Far End IP Table and click on the Edit icon to bring up the Edit Far End IP Screen. Edit the IP Address field as described above then click on the **Apply** button to save the changes. Note that you cannot edit the profile name.

Deleting a Far End IP List

Select the profile in the Far End IP Table and click on the Delete icon, then click **OK** at the confirmation prompt.

Static Service

The Unified Profile Static Service Screen displays all configured Static Service mapping and is used to create, edit, and delete Static Service mapping. When you configure a Static Service, it is used to configure the mapping of an existing SPB or VXLAN service ID to an Access Role Profile. This type of profile mapping is only valid if the specified SPB or VXLAN service is already configured; the switch does not dynamically create the service. The specified service ID is then used to dynamically create a service access point (SAP) based on the specified tag value.

Creating a Static Service

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Add** button.

- **Name -** The SPB Profile name.
- **Tag Value -** The VLAN tag information from classified traffic used to create the Service Access Point (SAP) for the traffic. If the traffic is untagged, the SAP is created with 0 as the encapsulation value (for example, 1/12:0).
- **Service ID -** An existing (statically configured) numerical value that identifies a specific SPB or VXLAN service. The valid service ID range is 1–32767.

Editing a Static Service

Select the profile in the Static Service List and click on the Edit icon to bring up the Edit Screen. Edit the fields as described above then click on the **Apply** button. Note that you cannot edit the profile name.

Deleting a Static Service

Select the profile in the Static Service List and click on the Delete icon, then click **OK** at the confirmation prompt.

VXLAN Profile

The Unified Profile VXLAN Profile Screen displays all configured VXLAN Profiles and is used to create, edit, and delete VXLAN Profiles. When you create a VXLAN, you configure the parameters that can be mapped to an Access Role Profile. When a device is dynamically assigned to the profile through authentication or classification, a VXLAN service access point

(SAP) is automatically created using the specified profile parameters. Traffic from the device is then forwarded on the SAP.

Creating a VXLAN Profile

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

- **Name -** The VXLAN Profile name.
- **Tag Value -** The VLAN tag information from classified traffic used to create the Service Access Point (SAP) for the traffic. If the traffic is untagged, the SAP is created with 0 as the encapsulation value (for example, 1/12:0).
- **VNID -** The VXLAN network identifier that identifies the VLAN segment form where the frames originate. This value is used to create the VXLAN service that is required to dynamically create the SAP.
- **Far End IP -** Select a Far End IP that contains the IP addresses for the far end VXLAN Tunnel End Points (VTEPs). The IP addresses in this list are used to dynamically create service distribution points (SDPs) for the VXLAN service.
- **Multicast IP Address -** The multicast IP address of the group to which this service will join.
- **VLAN Translation -** Enables/Disables egress VLAN translation for the service.
- **Multicast Mode -** Select the multicast mode from the drop-down menu:
  - **Headend** - Specifies the head-end replication mode for the service.
  - **Tandem -** Specifies the tandem replication mode for the service.
  - **Hybrid -** Specifies the hybrid replication mode for this service. This mode uses both the headend and tandem methods.

Editing a VXLAN Profile

Select the profile in the VXLAN Profile List and click on the Edit icon to bring up the Edit VXLAN Profile Screen. Edit the fields as described above then click on the **Apply** button to save the changes. Note that you cannot edit the profile name.

Deleting a VXLAN Profile

Select the profile in the VXLAN Profile List and click on the Delete icon, then click **OK** at the confirmation prompt.

Tunnel Profile

The Unified Profile Tunnel Profile Screen displays all configured Tunnel Profiles and is used to create, edit, and delete Guest Tunnel Profiles. When you create a Tunnel Profile, you configure the parameters that can be mapped to an Access Role Profile to authenticate a Guest Client, and map the client to a Guest UNP profile that is mapped to an L2 GRE service.

The Guest Tunnel feature is supported on OS6860, 6860E, and 6865 (AOS 8.4.1.R02 and later), and Stellar APs OAW-AP1101, OAW-AP1221, OAW-AP1222, OAW-AP1231, OAW-AP1232, OAW-AP1251 (AWOS 3.0.2.x and later), OAW-1201 (AWOS 3.0.5MR2 and later), and OAW-AP1201L (AWOS 3.0.7.x and later).

Creating a Tunnel Profile

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button. Each tunnel should have a unique Tunnel ID - GRE Tunnel Server/Data VPN Server pairing.

- **Name -** The Tunnel Profile name.
- **Tunnel ID -** The VPN ID used for Access Role Profile mapping. (Range = 0 - 16777215, suggested range of 64001 - 65000). If the Tunnel ID is set to "0", no GRE Key is sent.
- **GRE Tunnel Server IP Address/Data VPN Server -** The IP Address of the Tunnel Termination Switch (GRE Tunnel Server/Data VPN Server) used for mapping to the Access Role Profile. Select a switch from the drop-down or enter an IP address.
- **Backup GRE Tunnel Server IP Address** - The IP address of a backup GRE Tunnel Server to provide GRE tunnel redundancy between an AP and GRE Tunnel Server. Select a switch from the drop-down or enter an IP address. When the primary GRE Tunnel Server IP address goes down, the backup Tunnel Server takes over. Note that configuring a backup tunnel between an AP and the GRE Tunnel Server is supported on AWOS 4.0.5.15 or later.
- **Keepalive Interval** - The time interval, in seconds, for APs to check the status of the far-end IP address for the GRE Tunnel Server. (Range = 2 - 5 seconds, Default = 5 seconds)
- **Response Timeout** - The amount of time, in seconds, to wait for a response from the GRE Tunnel Server to keepalive requests. (Default = 2 seconds)
- **Retries** - The number of times to retry after a failed Keepalive request. (Range = 3 - 5, Default = 3). A failover to the backup GRE Tunnel Server IP address occurs after the last retry has failed.
- **Preemption** - Enables/Disables whether to go back to the primary GRE Tunnel Server. (Default = Disabled). When enabled:
    - **Preemption Countdown Timer** - Specify the amount of time to wait, in seconds, after a failover to the backup GRE Tunnel Server before attempting to go back to the primary GRE Tunnel Server. The countdown timer restarts on every switchover to the backup server. (Default = 300 seconds)
- **MTU** - Specify the MTU value for the GRE Tunnel. The recommended value is 1476 for Raw GRE and 1416 for GRE over wireguard interface. Leave this value blank if you do not want to set a specific value.
- **TCPMSS** - Specify the TCPMSS value for the GRE Tunnel (Range = 500 - 1426, Default = 1250).
- **Support of Entropy -** Enables/Disables entropy. An ALE Switch acting as a GRE Tunnel Server requires Entropy; however, some third-party GRE Tunnel Servers (e.g., Linux) require no Entropy.
- **Allow Local Breakout -** Enables/Disables Local Breakout on the tunnel. If enabled, enter the Static Route(s) to be used for entering the Tunnel. All other traffic will go out through the local network. Make sure you have applied the relevant Data VPN Server to AP Groups in the SSID **before** choosing Data VPN Server as the Tunnel endpoint. To apply a Data VPN Server to an AP Group, go to the AP Groups page (Network - AP Registration - AP Group) and edit the Data VPN Setting for the group.

Note that only one VLAN inside the tunnel (tunnel ID different from 0 if tagged, 0 if untagged) can be enabled with Local Breakout.

- **Static Routes -** Specify the static routes to be used for entering the tunnel. All other traffic will go out through the local network.

  Avoid specifying static routes pertaining to the VLAN ID of the traffic that enters the Tunnel. For example, if VLAN ID = 41 is specified to be carried within the Tunnel and if the network subnet that corresponds to VLAN 41 is 192.168.41.0, the AP will automatically set up this route and make sure traffic destined for 192.168.41.0 will enter the Tunnel. The AP will automatically set up this route and make sure traffic with VLAN ID = 41 will enter the Tunnel. **Do not specify an explicit Route** with Destination = 192.168.41.0, as that will confuse the AP and lead to poor performance.

  The static routes specified will be accumulated on an AP across all SSIDs assigned to the AP. For example, if you have two SSIDs configured on the same AP and configure SSID1 to use Tunnel Profile T1 with Static Routes A and B, and configure SSID2 to use Tunnel Profile T2 with Static Routes C and D, all of the routes (A, B, C, and D) will be applicable for SSID 1 and SSID 2.

  Across all of the routes applied on an AP from the different SSIDs, make sure any destination IP subnet is specified only once. Each route applied on an AP should be for a different IP subnet, even across the SSIDs. Also, avoid specifying static routes pertaining to the VLAN ID of the traffic that enters the tunnel. The AP will automatically set up such routes. If a route to IP subnet X already exists in an SSID and that SSID is applied to an AP, another route to the same IP subnet X must not be specified in the same or a different SSID that is applied to the same AP.

  Note: If you create two tunnel profiles with the same Remote IP and Tunnel ID, the "Support of Entropy" status **must** be the same on both tunnels (both must be "enabled" or "disabled"). Choose the value based on what use case you plan to deploy. The following are the four possible use cases that are supported:

1. GRE Tunnel from AP to AOS Switch - This is the typical Guest Tunnel uses case where AOS acts as the Guest Tunnel Termination Switch. The AOS Switch expects the Tunnel ID to be non-0 and "Support of Entropy" must be "Enabled".

2. GRE Tunnel from AP to Non-AOS Switch/Server (e.g., Nokia 7750 SR/Standard Linux Tunnel Server) - This is the Guest Tunnel use case with a non-AOS switch. The Tunnel ID must be 0 and "Support of Entropy" must be "Disabled", as the Key field in L2GRE header is not expected by the Switch/Server.

3. GRE Tunnel Between AP and OV VPN Server Appliance - This is the regular Data VPN tunnel use case between Remote APs and an OV VPN Server acting as the Data VPN Server. The Tunnel ID must be 0 and "Support of Entropy" must be "Disabled", as the Key field in L2GRE header is not expected by OV VPN Server.

4. GRE Tunnel from AP to AOS Switch, Over the Data VPN tunnel Between AP and OV VPN Server Appliance - This is a rare use case of using the Data VPN tunnel to reach from a remote site where the AP is located, to the Central Site where the AOS Switch is located. The AOS Switch expects the Tunnel ID to be non-0 and "Support of Entropy" must be "Enabled".

The following combinations of values are not supported:

- Tunnel ID > 0 and Support of Entropy = Disabled

- Tunnel ID = 0 and Support of Entropy = Enabled.

Editing a Tunnel Profile

Select the profile in the Tunnel Profile List and click on the Edit icon to bring up the Edit Tunnel Profile Screen. Edit the fields as described above then click on the **Apply** button to save the changes. Note that you cannot edit the profile name.

Deleting a Tunnel Profile

Select the profile in the Tunnel Profile List, click on the Delete icon, then click **OK** at the confirmation prompt.

Tunnel Profile List

- **Name -** The Tunnel Profile name.
- **Tunnel ID -** The VPN ID used for Access Role Profile mapping.
- **GRE Tunnel Server IP Address/Data VPN Server -** The IP Address of the Tunnel Termination Switch (GRE Tunnel Server/Data VPN Server) used for mapping to the Access Role Profile.
- **Backup GRE Tunnel Server IP Address** - The IP address of a backup GRE Tunnel Server to provide GRE tunnel redundancy between an AP and the GRE Tunnel Server. Note that configuring a backup tunnel between an AP and the GRE Tunnel Server is supported on AWOS 4.0.5.15 or later.
- **Keepalive Interval** - The time interval, in seconds, for APs to check the status of the far-end IP address for the GRE Tunnel Server.
- **Response Timeout** - The amount of time, in seconds, to wait for a response from the GRE Tunnel Server to keepalive requests.
- **Retries** - The number of times to retry after a failed Keepalive request.
- **Preemption** - The administrative status on whether to go back to the primary GRE Tunnel Server (Enabled/Disabled).
- **Preemption Countdown Timer** - If Preemption is enabled, this timer specifies the amount of time to wait after a failover to the backup GRE Tunnel Server before attempting to go back to the primary GRE Tunnel Server.
- **Entropy Status -** The administrative status of Entropy on the tunnel (Enabled/Disabled).
- **Local Breakout Status -** The administrative status of Local Breakout on the tunnel (Enabled/Disabled).
- **Static Routes -** The Local Breakout Static Route(s), if applicable.
- **MTU -** The MTU value for the GRE Tunnel.
- **TCPMSS -** The TCPMSS value for the GRE Tunnel.

802.1X Authentication Profile

The Unified Profile 802.1X Authentication Profile Screen displays all configured Wireless 802.1X Authentication Profiles and used to create, clone, edit, and delete 802.1X Authentication Profiles. An 802.1X Profile can be created and included in an Access Authentication Profile that can be assigned to wireless devices on the network.

802.1X is an Institute of Electrical and Electronics Engineers (IEEE) standard that provides an authentication framework for WLANs. 802.1x uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1X framework that are suitable for wireless networks include EAP-Transport Layer Security (EAP-TLS), Protected EAP (PEAP), and EAPTunneled TLS (EAP-TTLS). These protocols allow the network to authenticate the client while also allowing the client to authenticate the network. 802.1x authentication consists of three components:

- **Client -** The device attempting to gain access to the network.
- **Authenticator -** The gatekeeper to the network and permits or denies access to the clients. The wireless controller acts as the authenticator, relaying information between the authentication server and the client. Note that the EAP type must be consistent between the authentication server and supplicant, and is transparent to the controller.
- **Authentication Server -** Provides a database of information required for authentication, and informs the Authenticator to deny or permit access to the client. The 802.1X authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS) Server which can authenticate either users (through passwords or certificates) or the client computer.

Creating an 802.1X Authentication Profile

Click on the Add icon and enter a **Profile Name**. Configure the Profile as described below, then click on the **Create** button.

Settings

Complete the fields below to configure the basic settings for the profile.

- **Max Authentication Failures -** The number of times a user can try to log in with the wrong credentials after which the user is blacklisted as a security threat. Set to 0 to disable blacklisting, otherwise enter a non-zero integer to blacklist the user after the specified number of failures. (Range = 0 - 5, Default = 0)
- **Reauthentication -** Enables/Disables re-authentication. If enabled, the client must perform an 802.1X re-authentication after the expiration of the default timer for re-authentication (default value of the timer is 24 hours). If the user fails to re-authenticate with valid credentials, the state of the user is cleared. If derivation rules are used to classify 802.1x-authenticated users, the re-authentication timer per role overrides this setting. (Default = Disabled)
- **Max Reauthentication Attempts -** The number of times a user can try to re-authenticate. (Range = 1 - 10, Default = 3)
- **Termination -** Enables/Disables 802.1X authentication termination on the controller. (Default = Disabled)
- **Termination EAP-Type -** If you enable termination, click either EAP-PEAP or EAP-TLS to select an Extensible Authentication Protocol (EAP) method.
- **Termination Inner EAP-Type -** If you use EAP-PEAP as the EAP method, select one of the following inner EAP types:
  - **EAP-GTC -** Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or

RADIUS as the user authentication server. You can also enable caching of user credentials on the controller as a backup to an external authentication server.

- **EAP MSCHAPV2 -** Described in RFC 2759, this EAP method is widely supported by Microsoft clients.

- **Enforce Machine Authentication -** Enables/Disables Machine Authentication. If enabled, machine authentication is enforced before user authentication, and either the machine-default-role or the user-default-role is assigned to the user, depending on which authentication is successful. (Default = Disabled)
- **Default Machine Role -** The default role (Access Role Profile) assigned to the user after completing only machine authentication. Select an Access Role Profile from the drop-down menu or click on the Add icon to go to the Access Role Profile Screen and create a new one. The default role for this setting is the “guest” role.
- **Default User Role -** The default role (Access Role Profile) assigned to the user after 802.1x authentication. Select an Access Role Profile from the drop-down menu or click on the Add icon to go to the Access Role Profile Screen and create a new one. The default role for this setting is the “guest” role.

Instant Access Authentication Settings

Complete the fields below to configure RADIUS accounting settings for the profile.

- **Radius Accounting Mode -** The RADIUS Accounting Mode (User Authentication/User Association).

Cloning an 802.1X Authentication Profile

To save time in creating an 802.1X Authentication Profile, you can copy and modify an existing profile. Select the profile you want to copy and click on the **Clone** button. Enter a **Profile Name**, configure the settings you want to change, then click on the **Copy** button to save the changes to the server.

Editing an 802.1X Authentication Profile

Select the Profile in the 802.1X Authentication Profile Screen and click on the Edit icon to bring up the Edit Access 802.1X Authentication Profile Screen. Edit the fields as described above then click on the **Save** button to save the changes to the server. Note that you cannot edit the profile name. To edit the name, copy the profile and configure a new name.

Deleting an 802.1X Authentication Profile

To delete a profile(s), select the Profile(s) in the table and click on the Delete icon, then click **OK** at the confirmation prompt. If the profile is associated with an Access Authentication Profile, you will be presented with warning prompt that you must remove the 802.1X Authentication Profile(s) from the Access Authentication Profile before it can be deleted. Remove the 802.1X Authentication Profile(s) from the Access Authentication Profile, and then delete the profile(s).

MAC Authentication Profile

The Unified Profile MAC Authentication Profile Screen displays all configured Wireless MAC Authentication Profiles and used to create, clone, edit, and delete MAC Authentication Profiles. A MAC Profile can be created and included in an Access Authentication Profile that can be assigned to wireless devices on the network.

MAC-based authentication authenticates devices based on their physical Media Access Control (MAC) address. While not the most secure and scalable method, MAC-based authentication implicitly provides an addition layer of security authentication devices. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to the rest. For example, if clients are allowed access to the network via station A, then one method of authenticating station A is MAC-based. Clients may be required to authenticate themselves using other methods depending on the network privileges required.

Creating a MAC Authentication Profile

Click on the Add icon. Configure the Profile as described below, then click on the **Create** button.

MAC Authentication Profile

- **Profile Name -** User-configured name for the profile.
- **Max Authentication Failures -** The number of times a client can fail to authenticate before it is blacklisted. A value of zero disables blacklisting. (Range = 0 - 10, Default = 0)
- **Delimeter -** The Delimiter used in the MAC string:
  - **Colon -** Specifies the format XX:XX:XX:XX:XX:XX
  - **Dash -** Specifies the format XX-XX-XX-XX-XX-XX
  - **None -** Specifies the format XXXXXXXXXXXX (Default)
- **Case -** The case (Upper or Lower) used in the MAC string. (Default = Lower).

Cloning a MAC Authentication Profile

To save time in creating a MAC Authentication Profile, you can copy and modify an existing profile. Select the profile you want to copy and click on the Copy icon. Enter a **Profile Name**, configure the settings you want to change, then click on the **Copy** button to save the changes to the server.

Editing a MAC Authentication Profile

Select the Profile in the MAC Authentication Profile Screen and click on the Edit icon to bring up the Edit MAC Authentication Profile Screen. Edit the fields as described above then click on the **Save** button to save the changes to the server. Note that you cannot edit the profile name. To edit the name, copy the profile and configure a new name.

Deleting a MAC Authentication Profile

To delete a profile(s), select the profile(s) in the table and click on the Delete icon, then click **OK** at the confirmation prompt. If the profile is associated with an Access Authentication Profile, you will be presented with warning prompt that you must remove the MAC Authentication Profile(s) from the Access Authentication Profile before it can be deleted. Remove the MAC Authentication Profile(s) from the Access Authentication Profile, and then delete the profile(s).

AP Group

The Unified Profile AP Group Screen displays all configured AP (Access Point) Groups and used to create, edit, assign, and delete AP Groups.

Creating an AP Group

Click on the Add icon. Configure the Group as described below, then click on the **Create** button. After creating the AP Group, assign the group to a controller.

- **Group Name-** User-configured name for the group.
- **Access Auth Profiles -** The Access Authentication Profile(s) associated with the group. Selecting an Access Auth Profile will allow for association of the AP Group to the correct Virtual AP Profile inside the Access Auth Profile. Select an Access Auth Profile from the drop-down menu or click on the Add icon to go to the Access Auth Profile Screen and create a new one.

Editing an AP Group

Select the group in the AP Group Screen and click on the Edit icon to bring up the Edit AP Group Screen. Edit the fields as described above then click on the **Save** button to save the changes to the server. Note that you cannot edit the group name.

Assigning an AP Group

Select a group and click on the **Apply To Wireless Controllers** button. The AP Group Assignments Screen appears. Click on the Devices **ADD** button and select a controller(s). The controller(s) will appear in the List of Selected Devices. If necessary, click on the Devices **EDIT** button to add/remove devices from the list. When you are finished, click on the **Apply** button.

Deleting an AP Group

To delete a group(s), select the group(s) in the table and click on the Delete icon, then click **OK** at the confirmation prompt.

Global Configuration - Setting

The Unified Profile Global Configuration Setting Screen displays all configured Access Guardian Global configurations and used to create, clone, edit, delete, and assign Unified Profile Global configurations. This Global Configuration can be assigned and automatically applied to all UNP ports which have not been assigned an Access Authentication Profile.

Creating a Global Configuration

Click on the Add icon. Enter a **Global Config Name** and configure it as described below, then click on the **Create** button. When you are finished, select the checkbox next to the profile and click on the **Apply to Devices** button to assign the configuration to switches/wireless devices on the network.

Global Configuration Attributes

- **Redirect Pause Timer -** Configures the global pause timer value, in seconds, for the switch. Use this command to configure the amount of time the switch filters traffic from a non-supplicant (non-802.1X device) on a UNP port. This is done to allow enough time for the switch to clear the authentication state of the non-supplicant, at which time the device is re-authenticated. The pause timer is triggered when a COA request is received that requires a VLAN change for a non-supplicant (non-802.1X device) and the port bounce action is not triggered for the device. (Range = 60 – 65535, Default = 0)

- **Auth Server Down Timeout -** The authentication server down timer value, in seconds. When the timer runs out for a particular device, the switch clears the device from the Auth Server Down Access Role Profile and triggers another authentication attempt for that device. If authentication fails again, the device is classified back into the Auth Server Down Access Role Profile. The switch will repeat this process until the device authentication is completed. (Range = 10 to 1000, Default = 60)
- **Redirect Port Bounce -** Enables/Disables Port Bounce. This feature is required to handle scenarios where a client is switched from one VLAN to other after a Change of Authorization (COA) request. If port bounce is enabled, the port will be administratively put down. This is to trigger DHCP renewal and re-authentication, if necessary. (Default = Enabled, always "Enabled" on wireless devices)
- **UNP Dynamic VLAN Configuration -** Enables/Disables UNP Dynamic VLAN configuration when assigning Access Role Profiles to 8.x Devices running AOS 8.6R1 and higher.
- **Auto-Create Dynamic VLANs on Switch Reload -** Enables/Disables Dynamic UNP VLAN configuration when assigning Access Role Profiles to 6.x Devices running AOS 6.7R08 and higher.
- **Auth Server Down Access Role Profile -** The configuration can include an Authentication Server Down Access Role Profile. This is the profile to which a device is classified if MAC or 802.1X authentication fails because the RADIUS-capable server is unreachable. If necessary, you can also click the Add icon to go to the Access Role Profile Screen to create a new profile to include in the Global Configuration.
- **Redirect Proxy Server Port -** The HTTP proxy port number to use for redirection to UPAM or the CPPM Server.
- **Redirect Server IP -** The IP address used for redirection of HTTP traffic to UPAM or the CPPM Server. Specify the address that is associated with the dynamic URL returned from UPAM or the CPPM Server.

Cloning a Global Setting Profile

You can clone an existing profile and edit it to quickly create a new profile. Select a profile in the Setting List and click on the **Clone** button. Enter a new Global Config Name, edit the fields as necessary and click on the **Clone** button. After creating the profile, assign the profile to network devices.

Assigning a Global Setting Profile

Select a profile in the Setting List and click on the **Apply to Devices** button. Click on the Devices **ADD** button and/or the AP Group **ADD** button to select devices. The device(s) will appear in the List of Selected Devices. If necessary, click on the Devices **EDIT** button and/or the AP Group **EDIT** button to add/remove devices from the list. When you are finished, click on the **Apply** button.

Editing a Global Configuration

Select the configuration on the Global Configuration Setting Screen and click on the Edit icon to bring up the Edit Global Configuration Setting. Edit the fields as described above then click on the **Apply** button.

- If the edited configuration has **not** yet been assigned to switches/wireless devices, the update will be applied and the status displayed. Click **OK** to return to the Global

Configuration Setting Screen. If you want to assign the configuration to network switches/wireless devices, select the configuration on the Global Configuration Setting Screen and click on the **Apply to Devices** button to assign the configuration to switches/wireless switch on the network.

- If the edited configuration **has** already been assigned to switches/wireless devices, the Update Global Configuration confirmation prompt will appear (you can click on **Devices** to view the switches/wireless devices). Click on the **Process** button. The update will be applied and the status displayed. Click **OK** to return to the Global Configuration Setting Screen.

  Note: You cannot edit a Global Configuration Name.

Deleting a Global Configuration

Select the configuration in the Global Configuration Setting Screen and click on the Delete icon, then click **OK** at the confirmation prompt.

- If the configuration has **not** yet been assigned to switches/wireless devices, the update will be applied and the status displayed. Click **OK** to return to the Global Configuration Setting Screen.
- If the configuration **has** already been assigned to switches/wireless devices, the Delete Global Configuration Setting confirmation prompt will appear (you can click on **Devices** to view the switches/wireless devices). Click on the **Process** button. The update will be applied and the status displayed. Click **OK** to return to the Global Configuration Setting Screen.

Removing a Global Configuration From a Switch

To remove a Global Configuration from a switch, select the configuration in the table and click on the **Apply To Devices** button. The switches/wireless devices to which the configuration has been assigned will appear in the Assigned Switches area. Remove the switch(es)/wireless device(s) from the right-hand column and click **OK**. Click the **Apply** button. The configuration will be applied and the assignment status displayed. Click **OK** to return to the Global Configuration Setting Screen.

Global Configuration – AAA

The Unified Profile Global Configuration AAA Screen displays all configured Global AAA Profiles and used to create, edit, delete, and assign a Global AAA Profile. AAA Profiles are used to define specific AAA parameters that can be used in an Access Auth Profile or an Captive Portal Profile. This Global AAA Profile can be assigned and automatically applied to all UNP ports which have not been assigned an AAA Profile. In the absence of port template's AAA profile, the Global AAA Profile can be applied on AOS 8.x Switches.

An AAA Profile can be created to configure user access to the network as well as user access to network devices. The following use cases are supported:

- Using the UPAM local database for both network/switch authentication and client authentication.
- Using the UPAM local database for network/switch authentication (ASA) and an external RADIUS Server for client authentication.
- Using an external RADIUS Server for both network/switch authentication (ASA) and client authentication.

The following use case is **not** supported:

- Using an external RADIUS Server for network/switch authentication (ASA) and UPAM local database for client authentication.

Creating a Global AAA Profile

Click on the Add icon to bring up the Create AAA Screen. Enter a profile name in the **AAA Name** field, then follow the instructions below to configure a profile for Network Access or Switch Access.

User's Access to Network

If necessary, click on "User's Access To Network" to open the configuration window. Configure a profile for network access as described below, then click on the **Create** button.

Authentication Servers

- **802.1X -** Select a Primary 802.1X Authentication Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the click on the "Add New" link to go to the Authentication Servers Application and create a new Server. (The Link takes you to the RADIUS Server Management Screen. You can click on one of the other links to create a different server type (ACE, TACACS+).

  Note: For wireless devices, 802.1x Primary and Secondary Server configurations will help you to create 802.1x Authentication Server Group which will be used by Access Auth Profiles (Wireless AAA Server Profiles).

- **Captive Portal -** Select a Primary Captive Portal Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the click on the "Add New" link to go to the Authentication Servers Application and create a new Server. (The Link takes you to the RADIUS Server Management Screen. You can click on one of the other links to create a different server type (LDAP, ACE, TACACS+).

  Note: Captive Portal Primary and Secondary Server configurations are ignored for wireless devices.

- **MAC Auth -** Select a Primary MAC Authentication Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the click on the "Add New" link to go to the Authentication Servers Application and create a new Server. (The Link takes you to the RADIUS Server Management Screen. You can click on one of the other links to create a different server type (LDAP, ACE, TACACS+).

  Note: For wireless devices, MAC Primary and Secondary Server configurations will help you to create a MAC Authentication Server Group that will be used by Access Auth Profiles (Wireless AAA Server Profiles).

Accounting Servers

- **802.1X -** Select a Primary 802.1X Accounting Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the click on the "Add New" link to go to the **RADIUS Server Management** Screen and create a new Server.

- **Captive Portal -** Select a Primary Captive Portal Accounting Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the click on the "Add New" link to go to the **RADIUS Server Management** Screen and create a new Server.
- **MAC Auth -** Select a Primary MAC Accounting Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server. You can also click on the click on the "Add New" link to go to the **RADIUS Server Management** Screen and create a new Server.

Note: For wireless devices, Accounting Servers will help you to create an Accounting Radius Server Group that will be used in Access Auth Profiles (Wireless AAA Server Profiles). Captive Portal Primary and Secondary Servers are ignored. Wireless Devices only accept Radius servers for Accounting. If you select another type, an error will occur when you try to apply the configuration to Wireless Controllers.

Advanced Settings

Advanced settings are not supported on wireless devices and will be ignored when applied to those devices.

MAC Auth

- **Session Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for MAC Authenticated users. If Enabled, the switch will use the Session Timeout attribute received from the Authentication Server in an Accept-Accept message. If Disabled, the switch uses the locally configured timeout interval value (Default = Disabled).
- **Session Timeout Status -** Enables/Disables the Session Timeout option for MAC Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Session Timeout Interval. (Default = Disabled).
- **Session Timeout Interval -** The Session Timeout value, in seconds. When the Session Timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed. Note that when the Session Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again (Range = 12000 - 86400, Default = 43200).
- **Inactivity Timeout Status -** Enables/Disables the Inactivity Timeout option for MAC Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Inactivity Timeout Interval (Default = Disabled).
- **Inactivity Timeout Interval -** The Inactivity Timeout value, in seconds. Make sure the configured value is value greater than the MAC address aging time for the switch. If the Timeout Value is exceeded, the user is not logged out of the network if the MAC address aging time expires before the configured timeout value. Also note that when the Inactivity Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.(Range = 60 - 1200, Default - 600)
- **Accounting Interim Trust RADIUS Status -** Enables/Disables the Accounting Interim Trust Radius option for MAC Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again. (Default = Disabled)

- **Accounting Interim Interval -** The amount of time between each interim accounting update for MAC accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Calling Station ID Type -**The RADIUS Calling Station ID attribute for MAC accounting sessions (MAC - sets the Calling Station ID to the MAC address of the user. IP - sets the Calling Station ID to the IP address of the user).

802.1X

- **Re-Authentication Timeout Trust RADIUS Status -** Enables/Disables the Session Timeout Trust RADIUS option for 802.1x Authenticated users. If Enabled, the Session-Timeout attribute value received from the RADIUS server overrides the locally configured value for the switch. (Default = Disabled).
- **Re-Authentication Timeout Status -** Enables/Disables the automatic re-authentication of authenticated 802.1X users (Default = Disabled).
- **Re-Authentication Timeout Interval -** The amount of time the switch waits, in seconds, before triggering re-authentication of 802.1X users. Note that when the re-authentication time interval is changed, the new value does not apply to existing authenticated 802.1X users until the user is flushed out or when the user is authenticated again. Any new 802.1X users are re-authenticated based on the current time interval setting. (Range = 600 - 7200, Default = 3600)
- **Accounting Interim Trust RADIUS Status -** Enables/Disables the Accounting Interim Trust RADIUS option for MAC Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again. (Default = Disabled)
- **Accounting Interim Interval -** The amount of time between each interim accounting update for 802.1x accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Calling Station ID Type -**The RADIUS Calling Station ID attribute for MAC accounting sessions (MAC - sets the Calling Station ID to the MAC address of the user. IP - sets the Calling Station ID to the IP address of the user).

Captive Portal

- **Session Timeout Trust RADIUS Status -** Enables/Disables the Session Timeout Trust RADIUS option for Captive Portal Authenticated users. If Enabled, the switch will use the Session Timeout attribute received from the RADIUS server in an Accept-Accept message. If Disabled, the switch to use the locally configured timeout interval value (Default = Disabled).
- **Session Timeout Status -** Enables/Disables the Session Timeout option for Captive Portal Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Session Timeout Interval. (Default = Disabled).
- **Session Timeout Interval -** The Session Timeout value, in seconds. When the Session Timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed. Note that when the Session Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again (Range = 12000 - 86400, Default = 43200).

- **Inactivity Timeout Status -** Enables/Disables the Inactivity Timeout option for Captive Portal Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Inactivity Timeout Interval (Default = Disabled).
- **Inactivity Timeout Interval -** The Inactivity Timeout value, in seconds. Make sure the configured value is value greater than the MAC address aging time for the switch. If the Timeout Value is exceeded, the user is not logged out of the network if the MAC address aging time expires before the configured timeout value. Also note that when the Inactivity Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again. (Range = 60 - 1200, Default - 600)
- **Accounting Interim Trust RADIUS Status -** Enables/Disables the Accounting Interim Trust RADIUS option for Captive Portal Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again. (Default = Disabled)
- **Accounting Interim Interval -** The amount of time between each interim accounting update for Captive Portal accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Calling Station ID Type -**The RADIUS Calling Station ID attribute for MAC accounting sessions (MAC - sets the Calling Station ID to the MAC address of the user. IP - sets the Calling Station ID to the IP address of the user).

RADIUS

- **NAS Port ID -** The RADIUS client NAS-Port attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to define a NAS-Port identifier
  for the NAS-Port attribute. "Default" sets the NAS-Port attribute value to the chassis/slot/port of the user. The NAS-Port attribute value specified with this command is used in Account-Request messages and in Accounting-Request messages.
- **NAS ID -** The RADIUS client NAS-Identifier attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to identify the switch (RADIUS
  client) in the NAS-Identifier attribute. "Default" sets the NAS-Identifier attribute to the system name of the switch. The NAS-Identifier attribute value specified with this command is used in both Account-Request and Accounting-Request messages.
- **Username Delimiter -** The delimiter character used to separate fields within a RADIUS Server User Name.
- **Password Delimiter -** The delimiter character used to separate fields within a RADIUS Server Password.
- **Calling Station Delimiter -** The delimiter character used to separate fields within a Calling Station ID.
- **Called Station Delimiter -** The delimiter character used to separate fields within a Called Station ID.
- **Username Case -** Indicates if the RADIUS Server User Name must be in Upper Case or Lower Case.

- **Password Case -** Indicates if the RADIUS Server Password must be in Upper Case or Lower Case.
- **Calling Station ID Case -** Indicates if the Calling Station ID must be in Upper Case or Lower Case.
- **Called Station ID Case -** Indicates if the Called Station ID must be in Upper Case or Lower Case.

User's Access to Switches

If necessary, click on "User's Access To Switches" to open the configuration window. Select the Authentication Server(s) for the different types of switch access, and select an Accounting Server. If necessary, click on the "Add New" link to go to the RADIUS Server Management Screen and create a new Authentication Server. You can also select a UPAM RADIUS Server for Authentication and Accounting.

- **Authentication Servers**
- **Default Authentication -** Configures Authenticated Switch Access for any port using any service (e.g., Telnet, SSH, FTP). .
- **Telnet Authentication -** Configures Authenticated Switch Access for any port used for Telnet.
- **SSH Authentication -** Configures Authenticated Switch Access for any port used for Secure Shell.
- **HTTP Authentication -** Configures Authenticated Switch Access for any port used for Web-based management.
- **FTP Authentication -** Configures Authenticated Switch Access for any port used for FTP.
- **Console Authentication -** Configures Authenticated Switch Access through the console port.
- **Accounting Server**
- **Session Accounting -** Configures an Accounting Server for authenticated switch sessions. Accounting servers keep track of network resources (e.g., time, packets, bytes) and user activity.

UPAM RADIUS Server Use Cases

An AAA Profile can be created to configure user access to the network, as well as user access to network devices. The following use cases are supported for UPAM Radius Server.

Use Case	Database for ASA	Database for 802.1X/ MAC Authentication	Setting to be Used in UPAM - Authentication Access Policy Page	Sample Policy That Could Be Used in UPAM - Authentication Access Policy Page
UPAM for Network/Switch Authentication/Client Authentication	UPAM DB	UPAM DB	Enable ASA	• No explicit Access Policy needed for ASA • Any other Access Policy as required for 802.1x/MAC

UPAM for Network/Switch Authentication (ASA), External RADIUS for Client Authentication.	UPAM DB	External RADIUS DB (UPAM acts as Proxy to External RADIUS Server)	Enable ASA	• No explicit Access Policy needed for ASA • For 802.1x - Network Type = Wired + Authentication Type = 802.1X • For MAC - Network Type = Wired + Authentication Type = MAC
External RADIUS for Network/Switch Authentication (ASA), UPAM for Client Authentication	Use Case Not Supported	Use Case Not Supported	Use Case Not Supported	• Use Case Not Supported
External RADIUS for both Network/Switch Auth (ASA) and Client Authentication	Use Case Not Supported	Use Case Not Supported	Use Case Not Supported	• Use Case Not Supported

Editing a Global AAA Profile

Select the profile in the AAA Screen and click on the Edit icon to bring up the Edit AAA Screen. Edit the fields as described above then click on the **Apply** button.

Note: You cannot edit the Profile Name.

Assigning a Global AAA Profile

When you click the **Apply To Devices** button, the Assign AAA Screen appears. Click on on the Devices **ADD** button to select devices. The device(s) will appear in the List of Selected Devices. If necessary, click on the Devices **EDIT** button to add/remove devices from the list. When you are finished, click on the **Apply** button.

Deleting a Global AAA Profile

Select the profile in the AAA Screen, click on the Delete icon, then click **OK** at the confirmation prompt.

Global Configuration - Redirect Allowed Profile

The Unified Profile Global Configuration Redirect Allowed Profile Screen displays all configured Redirect Allowed Profiles and is used to create, clone, edit, delete, and assign Global Setting Profile Profiles. Configures an additional IP address to that a host can access. This allows traffic to reach additional subnets other than that of UPAM or the CPPM Server.

Creating a Redirect Allowed Profile

Click on the Add icon to bring up the Create Redirect Allowed Screen. Complete the fields as described below, then click on the **Create** button.

- **Profile Name -** User-configured profile name.

- **Redirect Allowed IP -** Redirect IP address.
- **Redirect Allowed Mask -** Redirect IP address mask.

Cloning a Redirect Allowed Profile

You can clone an existing profile and edit it to quickly create a new profile. Select a profile in the Redirect Allowed Profile List and click on the **Clone** button. Enter a new Profile Name, edit the fields as necessary and click on the **Clone** button. After creating the profile, assign the profile to network devices

Assigning a Redirect Allowed Profile

Select a profile in the Redirect Allowed Profile List and click on the **Apply to Devices** button. Click on the Devices **ADD** button and/or the AP Group **ADD** button to select devices. The device(s) will appear in the List of Selected Devices. If necessary, click on the Devices **EDIT** button and/or the AP Group **EDIT** button to add/remove devices from the list. When you are finished, click on the **Apply** button.

Editing a Redirect Allowed Profile

Select the profile in Redirect Allowed Profile List and click on the Edit icon to bring up the Edit Redirect Allowed Profile Screen. Edit the fields as described above and click on the **Apply** button.

Deleting a Redirect Allowed Profile

Select the profile in the Redirect Allowed Profile List and click on the Delete icon, then click **OK** at the confirmation prompt.

Global Configuration - DHCP Option 82

The Unified Profile Global Configuration DHCP Option 82 is used to configure the DHCP Option 82 Feature for Stellar APs. DHCP Option 82 allows a DHCP Relay Agent to insert specific information into a request that is being forwarded to a DHCP Server. Specifically, the option works by setting two sub-options: Circuit ID and Remote ID. The Option 82 Feature is enabled/disabled as part of an Access Role Profile. Configure the options as described below, then click on the **Apply** button.

Note: The DHCP Option 82 Feature is supported on Stellar APs AWOS 3.0.6.x and higher.

- **Delimiter** - The character to use as a delimter between values specified in the Circuit ID sub-option. Click on the drop-down menu to select the delimiter character.
- **Circuit ID -** The Circuit ID sub-option is used to include information about the network device the client request came in on.
    - **SSID -** The SSID of the network to which the client is connecting.
    - **AP Model -** The model of the AP to which the client is connecting.
    - **AP Name -** The name of the AP to which the client is connecting.
    - **AP MAC -** The MAC address of the AP to which the client is connecting.
    - **AP Location -** The location of the AP to which the client is connecting.
    - **VLAN-ID -** The VLAN to which the client is connecting.
    - **AP-Port -** The AP downlink port to which the client is connecting.

    - **Input -** A user-customized definition of the Circuit ID.
    - **Format of Circuit ID** - Displays the format of the selected Circuit ID sub-option information with the specified delimiter character. For example, "AP Name - AP MAC - SSID - AP Location" if a dash is the specified delimiter.
- **Remote ID -** The Remote ID sub-option is used to include the client information.
    - **Client-MAC -** The MAC address of the client connecting to the network.
    - **Input -** A user-customized definition of the Remote ID.

Device Config

Unified Profile Device Config Screens enable you to edit and delete Unified Profiles on specific network devices. When you select a profile on the left side of the screen (e.g., Access Auth Profile, Access Role Profile), click on the Devices or AP Groups **ADD**/**EDIT** buttons to display devices to which that profile type has been assigned. You can select a device and edit the profile parameters on the device, or select a device(s) and delete the profile from the device(s). The following screens are available:

- **Access Auth Profile -** Edit/Delete Access Authentication Profiles. An Access Auth Profile enables you to assign a pre-defined UNP port configuration to a port or linkagg, or specify them individually on each port to enable UNP port status and set the parameters for the authentication process for the port.
- **WLAN Service -** Create a WLAN Service for Stellar APs.
- Access Role Profile - Edit/Delete Access Role Profiles. An Access Role Profile contains the various UNP properties (e.g., QoS Policy List attached to the UNP, Captive Portal Authentication) for users assigned to the profile.
- **AAA Server Profile -** Edit/Delete AAA Server Profiles. AAA Server Profiles are used to define specific AAA parameters that can be used in an Access Auth Profile or Captive Portal Profile.
- **Access Policies -** Edit/Delete Location/Period Policies.
- **Access Classification -** Edit/Delete Access Classification Rules. Access Classification Rules are defined and associated with an Access Role Profile to provide an additional method for classifying a device into an Access Role Profile. If authentication is not available or does not return a profile name for whatever reason, Access Classification rules are applied to determine the profile assignment.
- **Far End IP -** Edit/Delete Far End IP Lists. Far End IP Lists allow multiple far-end nodes to be associated with the service created for the VXLAN Network ID (VNID) specified in a VXLAN Profile.
- **Diagnostics -** The Diagnostics Screen displays Unified Profile information for an end station which can be used to diagnose UNP Profile problems.
- **Legacy Wireless Profiles**
    - **802.1x Authentication Profile -** Edit/Delete 802.1x Authentication Profile. An 802.1X Profile can be created and included in an Access Authentication Profile that can be assigned to wireless devices on the network.
    - **MAC Authentication Profile -** Edit/Delete MAC Authentication Profile. MAC-based authentication authenticates devices based on their physical Media Access Control (MAC) address.

- **SSID Profile -** Edit/Delete SSID Profiles. Wireless Profiles can be created and included in an Access Authentication Profile that can be assigned to wireless devices on the network.
- **AP Group -** Edit/Delete AP Group Profiles. Wireless Profiles can be created and included in an Access Authentication Profile that can be assigned to wireless devices on the network.
- **Virtual AP -** Edit/Delete Virtual AP Profiles. Wireless Profiles can be created and included in an Access Authentication Profile that can be assigned to wireless devices on the network.
- **AAA Server Group -** Edit/Delete AAA Server Group Profiles.

- **Global Configuration**
  - **Setting -** Create and apply Global Unified Profile Settings to network devices.
  - **AAA Profile -** Edit/Delete Global AAA Profiles. AAA Profiles are used to define specific AAA parameters that can be used in an Access Auth Profile or an Captive Portal Profile.
  - **Redirect Allowed Profile** - Create and apply Global Redirect Allowed Profiles.

Device Config - Access Auth Profile

The Unified Profile Device Config Access Auth Profile Screen displays information about all devices to which an Access Auth Profile has been assigned. You can edit the Access Auth Profile on an AOS device or AP Group, or delete the profile from an AOS Device or AP Group. To display AOS Device information, click on the Devices **ADD** button and select device(s). To display AP Group information, click on the AP Group **ADD** button and select an AP Group(s). To add/remove devices/AP Groups from the display, click on the **EDIT** button.

Important Note: Any configuration updates applied in the Device Config application are **only** applied to the selected devices/AP Groups. The updates will not affect the corresponding SSIDs, Unified Access Profiles/Templates.

Editing an Access Auth Profile

Select a device/AP Group in the Access Auth Profile List and click on the Edit icon to edit the field(s) as described below. When you are finished, click on the **Apply** button. Note that support for different parameters varies by device type. You can select an option from the "Highlight" drop-down menu at the top of the screen to highlight the parameters supported by specific devices (6x, 7x, 8x)

Default Settings

This section is used to configure basic settings for the profile.

- **AAA Server Profile -** The AAA Server Profile used to authenticate users on the port.
- **Port Bounce -** Enables/Disables Port Bounce. Always Enabled on wireless devices. This feature is required to handle scenarios where a client is switched from one VLAN to other after COA. If port bounce is enabled, the port will be administratively put down. This is to trigger DHCP renewal and re-authentication, if necessary.

- **MAC Auth -** Enables/Disables MAC Authentication for the port. Wireless devices do not contain this attribute in their configuration table. MAC Pass Alt attribute in the next section No Auth/Failure/Alternate is used for MAC Authentication on wireless devices.
- **802.1X Auth -** Enables/Disables 802.1X Authentication. Wireless devices do not contain this attribute in their configuration table. 802.1X Pass Alt attribute in the next section No Auth/Failure/Alternate is used for 802.1X Authentication on wireless devices.
- **Dynamic Service -** Select a dynamic mapping method, if applicable (SPB, VXLAN).
- **Customer Domain ID -** Select a Customer Domain ID for the profile, if applicable.
- **L2 Profile -** Select an existing Layer 2 Profile from the drop-down menu. To create a new profile, go to the Layer 2 Profiles Screen (Configuration - Services - Layer 2 Profiles). Once a new profile is created, it will appear in the L2 Profile drop-down menu on this screen. Layer 2 profiles specify how control packets are processed on SAPs.
- **AP Mode -** Enables/Disables the Access Point Mode for the port. When enabled (the default), the switch automatically detects, learns, and manages a Stellar AP that is connected to the port. Wireless client traffic is then forwarded from the AP to the OmniSwitch onto the wired network.
- **Secure -** If the AP Mode is enabled, you can check this box to secure the AP Mode. The AP Mode is not secured by default (box is not checked). When an AP device is detected on a UNP port, the trust tag function is operationally enabled to trust the AP client traffic. If the AP device fails authentication but is still learned as forwarding, the client traffic is still trusted and forwarded on the port. When the AP Mode is secured (box is checked), the trust tag function is not enabled for client traffic until after the AP device successfully authenticates.

No Auth/Failure/Alternate

This section is used to configure the actions taken if a device assigned to the profile fails authentication.

- **Trust Tag -** Enables/Disables whether or not to trust the VLAN ID of a tagged packet to determine how the packet is classified. Enabling the trust VLAN ID tag option provides an implicit method of VLAN tag classification that will accept tagged traffic matching any of the existing UNPs without the need to create specific classification rules for those profiles. (Default = Disabled)
- **Access Classification -** Enables/Disables device classification. Always Enabled on wireless devices (Default = Disabled).
- **Default Access Role Profile -** The Default Access Role Profile that users are assigned to after authentication. Note that for IAP devices the default Access Role Profile name must match the SSID Profile name in order for it to take effect.
- **Bypass VLAN -** Enter a Bypass VLAN (Range = 1 - 4094). The Bypass VLAN attribute is supported on Stellar AP 1201H/1201HL (running AWOS 4.0.2 or later) and Stellar AP 1301H/1311 (running AWOS 4.0.5 or later). The feature improves wired port forwarding performance by skipping the CPU process. When a Bypass VLAN is configured, traffic from the AP uplink port to the downlink port, or vice versa, is forwarded directly through the switch chipset without CPU intervention.
- **802.1X Pass Alt -** The user shall be assigned a Pass-Alternate UNP in case the 802.1X authentication does not result in a valid UNP for the pass branch.
- **Bypass Status -** Enables/Disables 802.1X bypass. When 802.1X bypass is enabled, the user's 802.1X authentication method is skipped. The user directly enters mac-

authentication or Access Classification based on the configuration on the UNP ports/Linkaggs. On wireless devices, this attribute corresponds to another attribute named l2-auth-fail-through, and this attribute must be combined with the MAC Allow EAP attribute to make l2-auth-fail-through attribute work (Default = Disabled).

- **AOS Devices**
  - Bypass Status with Enabled status combined with MAC Allow EAP set to "None" will disable 802.1X authentication, and l2-auth-fail-through is not Enabled.
  - Bypass Status with Enabled status combined with l MAC Allow EAP set to "Fail" will enable l2-auth-fail-through.
  - Other configurations of Bypass Status and MAC Allow EAP cause l2-auth-fail-through to be ignored on wireless devices.
- **Stellar APs**
  - If Bypass Status is Enabled, MAC Allow EAP will be considered. In the AP. There are only two options: Pass or Fail. When Bypass Status is Enabled, both MAC authentication and 802.1x authentication are performed - MAC authentication is performed first, then 802.1x authentication.
  - If Bypass Status is Disabled, OmniVista will always perform 802.1x authentication and ignore MAC authentication (unless both MAC and 802.1x authentication are enabled).

- **Failure Policy -** The authentication method used if 802.1X authentication fails.
- **MAC Pass Alt -** The Access Role Profile the user is assigned to after passing authentication.
- **MAC Allow EAP -** Enables/Disables Extensible Authentication Protocol (EAP).

Advanced Settings

This section is used to configure advanced 802.1x authentication settings for the profile.

- **802.1X Tx Period -** Access Auth Profile 802.1x Tx period, in seconds.
- **802.1X Supp Timeout -** 802.1X Authentication Supp Timeout, in seconds.
- **802.1X Request -** 802.1X Authentication Max Request number.
- **Port Controlled Directions -** Configures whether network access control is applied to both incoming and outgoing traffic, or only applied to incoming traffic.
- **Client Isolation** - Enables/Disables Client Isolation (Default = Disabled). When enabled, traffic between clients on the same AP in the SSID is blocked; client traffic can only go toward the default gateway. You can create a list of device MAC addresses that a client can still access when Client Isolation is enabled. This list is configured for the Access Role Profile to which a client is assigned.

Configuration Information

This section displays current port configurations, if applicable; and and is used to create/edit port configurations for the profile.

- **Ports -** The switch port(s) configured for the profile.
- **Port Type -** The port type (VLAN Port, SPB Access Port, VXLAN Access Port).

- **UNP VLANs -** The VLANS configured for dynamically-created UNP VLANs. For 8.x Devices, select a traffic type (Tagged, Untagged).

Deleting an Access Auth Profile

Select a profile(s) in the Access Auth Profile List and click on the Delete icon, then click **OK** at the confirmation prompt.

Device Config - SSID/WLAN Service

The Unified Profile Device Config SSID/WLAN Service Screen displays information about all AP Groups to which an SSID/WLAN Service Profile has been assigned. You can edit a WLAN Service Profile on an AP Group, or delete a profile from an AP Group. To display AP Group information, click on the AP Groups **ADD** button and select devices. To add/remove AP Groups from the display, click on the **EDIT** button.

> **Important Note:** Any configuration updates applied in the Device Config application are only applied to the selected devices/AP Groups. The updates will not affect the corresponding SSIDs, Unified Access Profiles/Templates.

Editing a WLAN Service

Select an AP Group in the WLAN Service List and click on the Edit icon to edit the field(s) as described below. When you are finished, click on the **Apply** button. Note that you cannot edit a WLAN Service Profile that was created in the SSIDs application (Origin = SSIDs). You can only edit the profile from the SSIDs application.

SSID Settings

Basic

- **Service Name -** User-configured SSID.
- **SSID -** User configured name that uniquely identifies a wireless network (up to 32 characters).
- **Origin -** The application used to create the WLAN Service (WLAN (Expert) or SSIDs).
- **Hide SSID -** Enables/Disables SSID in beacon frames. Note that hiding the SSID does very little to increase security. (Default = Disabled)
- **Enable SSID -** Enables/Disables the SSID.
- **Allowed Band -** The band(s) available on the service:
  - 2.4 GHz
  - 5 GHz
  - All - 5 GHz and 2.4 GHz.

Security

- **Security Level -** Select the security level for the WLAN Service:
  - **Open -** The WI-FI will be unsecured. However, you can configure a default role or enable MAC Authentication to assign a role for clients (Default).

- **Enterprise -** An authentication server will be used to authenticate the connecting client via 802.1x Authentication. Select an **Enryption Type** from the drop-down menu:
  - DYNAMIC_WEP - WEP with dynamic keys.
  - WPA_TKIP - WPA with TKIP encryption and dynamic keys using 802.1X.
  - WPA_AES - WPA with AES encryption and dynamic keys using 802.1X.
  - WPA2_TKIP - WPA2 with TKIP encryption and dynamic keys using 802.1X.
  - WPA2_AES - WPA2 with AES encryption and dynamic keys using 802.1X.
  - WPA3_AES256 - WPA3 with CNSA (Suite B) using 802.1X. Note that when WPA3_AES256 encryption is applied to an AP that does not support it, the encryption will automatically fall back to WPA2_AES. OAW-AP1101 full band, OAW-AP1201H 2.4G band do not support WPA3_AES256 authentication.
  - WPA_AES - WPA3 with AES encryption and dynamic keys using 802.1X.
- **Personal -** The WI-FI will be protected by a key. Select an **Enryption Type** from the drop-down menu, then enter a **Passphrase**.
  - STATIC_WEP - Authentication with Static Wired Equivalent Privacy security algorithm.
  - WPA_PSK_TKIP - WPA with TKIP encryption using a preshared key.
  - WPA_PSK_AES - WPA with AES encryption using a preshared key.
  - WPA_PSK_AES_TKIP - WPA with TKIP and AES mixed encryption using a preshared key.
  - WPA2_PSK_TKIP - WPA2 with TKIP encryption using a preshared key.
  - WPA2_PSK_AES - WPA2 with AES encryption using a preshared key.
  - WPA3_SAE_AES - WPA3 with AES encryption using a preshared key, which ONLY allow WPA3 capable client accessing.
  - WPA3_PSK_SAE_AES - WPA3 and WPA2 mixed mode, which allow both WPA3 capable client as well as ONLY WPA2 capable client accessing.

- **MAC Auth -** Enables/Disables MAC Authentication.
- **AAA Profile -** Select an AAA Profile to use for authentication. An AAA profile is required if the Security Level is set to "Enterprise" (to perform 802.1x authentication) or if MAC Authentication is enabled. This AAA Profile will be also used for Accounting purposes.
- **Classification Status -** Enables/Disabled classification. If classification is enabled, traffic will be classified to a role based on the configured classification rules. Note that the precedence of role assignment methods is important. Classification Rules are only used if 802.1x/MAC authentication does not return a role, or the returned role is not matched with any configured roles in the device.

- **MAC Pass Auth -** If MAC Authentication is enabled, select an Access Role Profile to assign to clients that pass MAC Authentication.
- **Default Access Role Profile -** Select the default Access Role Profile that will be applied to clients if a role cannot be assigned by other role assignment methods.
- **Client Isolation -** Enables/Disables Client Isolation. If enabled, traffic between clients on the same AP in the SSID is blocked; client traffic can only go toward the router. (Default = Disabled)
- **Protected Management Frame -** Configures whether connections are accepted from clients supporting Protected Management Frame for certain Security Levels/Encryption Types (Enterprise - WPA2_AES/WPA3_AES256/ WPA3AES, Personal - WPA2_PSK_AES/WPA3_SAE_AES/WPA3_PSK_SAE_AES)
    - **Disabled -** Disables Protected Management Frame requirements.
    - **Optional -** Allows connections from clients supporting Protected Management Frame and clients that do not.
    - **Required -** Only allows connections from clients supporting Protected Management Frame.

Hotspot 2.0

- **Hotspot 2.0 -** Enables/Disables Hotspot 2.0. Hotspot 2.0 is a new standard for public-access Wi-Fi that enables seamless roaming among Wi-Fi networks and between Wi-Fi and cellular networks. Hotspot 2.0 was developed by the Wi-Fi Alliance and the Wireless Broadband Association to enable seamless hand-off of traffic without requiring additional user sign-on and authentication. Note that Hotspot 2.0 is only supported with Enterprise WPA2_AES or Enterprise WPA3_AES256 Encryption. You must first select one of these Encryption types before you can enable Hotspot 2.0.
- **Operator Name -** The operator providing the Hotspot service (0 - 252 characters).
- **Venue Name -** The venue where the Hotspot is hosted (0 - 252 characters).
- **Venue Type -** The type of venue hosting the Hotspot.
- **Network Detail -** The type of Hotspot network.
- **Domain List -** The list of Hotspot Domains. You can have up to 16 Domain Names (1 - 255 characters each).
- **Roaming OIs** - The Roaming Organization Identifier. You can have up to 16 OIs. Each OI field is 3 characters in length if the organizationally unique identifier is an OUI, or 5 octets in length if the organizationally unique identifier is an OUI-36.

Roaming Controls

- **802.11r -** Enables/Disables 802.11r fast roaming. 802.11r is a roaming standard defined by IEEE. When enabled, 802.11r reduces roaming delay by pre-authenticating clients with multiple target APs before a client roams to an AP.
- **OKC** - Enables/Disables OKC (Opportunistic Key Caching) fast roaming. AP stores one PMK per client, which is derived from the last 802.1X authentication completed by the client in the network. The cached PMK is used when a client roams to a new AP. This allows faster roaming of clients between the APs, without requiring a complete 802.1X authentication.

- **L3 Roaming** - Enables/Disables Layer 3 roaming. Layer 3 roaming allows client to move between Access Points and connect to a new IP subnet and VLAN.
- **802.11k Status -** Enables/Disables 802.11k. The 802.11k protocol enables Stellar APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, Stellar APs and clients send neighbor reports, beacon reports, and link measurement reports to each other.
- **802.11v Status -** Enables/Disables 802.11v. 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an Instant AP to request a voice client to transition to a specific Stellar AP, or suggest a set of preferred Stellar APs to a client due to network load balancing or BSS termination. It also helps the client identify the best Stellar AP to transition to as they roam.

Client Controls

- **Max Number of Clients Per Band** - The maximum number of clients allowed in each band. (Range = 1 - 256, Default = 64)
- **802.11b Support -** Enables/Disables allowing 11b legacy clients to connect to Stellar APs.
- **802.11a/g Support -** Enables/Disables allowing 11a/g legacy clients to connect to Stellar APs. ?

Minimum Client Data Rate Controls

- **2.4GHz Minimum Client Data Rate Controller -** Enables/Disables 2.4G band access control based on client data rate.
- **2.4GHz Minimum Client Data Rate -** 2.4G band client with lower data speed will not be given access, recommended value 12.
- **5GHz Minimum Client Data Rate Controller -** Enables/Disables 5G band access control based on client data rate.
- **5GHz Minimum Client Data Rate -** 5G band client with lower data speed will not be given access, recommended value 24.

Minimum MGMT Rate Controls

- **2.4GHz Minimum MGMT Rate Controller -** Enables/Disables 2.4G band wireless management frame rate control.
- **2.4GHz Minimum MGMT Rate -** 2.4G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.
- **5GHz Minimum MGMT Rate Controller -** Enables/Disables 5G band wireless management frame rate control.
- **5GHz Minimum MGMT Rate -** 5G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.

High Throughput Control

- **A-MSDU -** Enables/Disables Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

- **A-MPDU -** Enables/Disables Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

QoS Settings

Configure the wireless QoS Settings for the profile as detailed below.

Bandwidth Contract

- **Upstream Bandwidth -** The maximum bandwidth for traffic from the switch to the client
- **Downstream Bandwidth -** The maximum bandwidth for traffic from the client to the switch.
- **Upstream Burst -** The maximum bucket size used for traffic from the switch to the client. The bucket size determines how much the traffic can burst over the maximum bandwidth rate
- **Downstream Burst -**The maximum bucket size used for traffic from the client to the switch. The bucket size determines how much the traffic can burst over the maximum bandwidth rate

Broadcast/Multicast Optimization

- **Broadcast Key Rotation -** Enables/Disables the broadcast key rotation function. If enabled, the broadcast key will be rotated after every interval time.
- **Broadcast Key Rotation Time Interval -** The interval, in minutes, to rotate the broadcast key (Range = 1 - 1440, Default = 15).
- **Broadcast Filter All -** If enabled, all multicast and broadcast traffic will be dropped.
- **Multicast Optimization -** Enable/Disables multicast traffic rate optimization.
- **Multicast Based Channel Utilization -** Configures based channel utilization optimization percentage. (Range = 0 - 100, Default = 90)
- **Number Of Clients -** Configure the threshold for multicast optimization. This is the maximum number of high-throughput stations.

802.1p Mapping

Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and 802.1p priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add icon. To remove a value, click on the "x" next to the value.

- **Background -** WMM Background will be mapped to the 802.1p value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 1)
    - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 1, 2)
- **Best Effort -** WMM Best Effort will be mapped to the 802.1p value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 0)

  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 0, 3)
- **Video -** WMM Video will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 4)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 4, 5)
- **Voice -** WMM Voice will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 6)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 6, 7)

DSCP Mapping

Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and DSCP priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add icon. To remove a value, click on the "x" next to the value.

- **Trust Original DSCP -** If enabled, the original DSCP mapping for uplink traffic is trusted (Default = Disabled).
- **Background -** WMM Background will be mapped to the DSCP value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 10)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 2, 10)
- **Best Effort -** WMM Best Effort will be mapped to the DSCP value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 0)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 0, 18)
- **Video -** WMM Video will be mapped to the DSCP value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 40)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 24, 36, 40)
- **Voice -** WMM Voice will be mapped to the DSCP value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 46)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 46, 48, 56)

Deleting a WLAN Service

Select an AP Group(s) in the WLAN Service List, click on the Delete icon, then click **OK** at the confirmation prompt. This removes the profile from the server. Note that you cannot delete a

WLAN Service that was created in the SSIDs application (Origin = SSIDs). You can only delete the profile from the SSIDs application.

Device Config - Access Role Profile

The Unified Profile Device Config Access Role Profile Screen displays information about all devices/AP Groups to which an Access Role Profile has been assigned. You can edit the Access Role Profile on an AOS Device or AP Group, or delete the profile from an AOS Device or AP Group. To display AOS Device information, click on the Devices **ADD** button and select an AP Group(s). To add/remove devices/AP Groups from the display, click on the applicable **EDIT** button.

> **Important Note:** Any configuration updates applied in the Device Config application are **only** applied to the selected devices/AP Groups. The updates will not affect the corresponding SSIDs, Unified Access Profiles/Templates.

Editing an Access Role Profile

Select a device/AP Group in the Access Role Profile List and click on the Edit icon to edit the field(s) as described below. When you are finished, click on the **Apply** button. Note that support for different parameters varies by device type.

Access Role Profile Attributes

- **Policy List -** An Access Role Profile can also be configured with an existing Unified Policy List. The set of rules within the Unified Policy List are then applied to the traffic that passes though switches/wireless devices. Only one Unified Policy List is allowed per profile, but multiple profiles may use the same Policy List. Select a Unified Policy List for the profile from the drop-down menu.
- **Max Ingress Bandwidth -** The maximum bandwidth limit allocated for ingress traffic on UNP ports assigned to the profile. If the maximum ingress bandwidth value is set to zero, all ingress traffic is allowed on the UNP port. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)
- **Max Egress Bandwidth -** The maximum bandwidth limit allocated for egress traffic on UNP ports assigned to the profile. If the maximum egress bandwidth value is set to zero, all egress traffic is allowed on the UNP port. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)
- **Max Ingress Depth or Max Default Depth (AOS 6) -** The maximum ingress depth value that is applied to traffic on UNP ports that are assigned to the profile. This value determines how much the traffic can burst over the maximum ingress bandwidth rate. The maximum ingress depth value is configured in conjunction with the maximum ingress bandwidth parameter. When the ingress depth value is reached, the switch starts to drop packets. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)

Deleting an Access Role Profile

Select a device(s)/AP Group(s) in the Access Role Profile List and click on the Delete icon, then click **OK** at the confirmation prompt.

Access Role Profile Information

- **Device Friendly Name** - The user-defined name for the device.
- **Profile Name** - The name assigned to the Access Role Profile
- **VLAN(s) Number** - The VLAN mapping for the profile.
- **Auth Flag** -Enables/Disables authentication (not supported on wireless devices and ignored when applied to those devices).
- **Mobile Tag Status** - Enables/Disables classification of tagged packets received on mobile ports (not supported on wireless devices and ignored when applied to those devices).
- **Redirect Status** - Enables/Disables Captive Portal Redirect (not supported on wireless devices and ignored when applied to those devices). Note that if Redirect Status is enabled, the Access Role Profile can only map to a VLAN when applying the profile to a device.
- **Policy List -** The name of the Policy List assigned to the profile. The set of rules within the Policy List are applied to the traffic that passes though switches/wireless devices. Only one Policy List is allowed per profile, but multiple profiles may use the same Policy List.
- **Location Policy Name -** The name of the Location Access Policy assigned to the profile.
- **Period Policy Name -** The name of the Period Policy assigned to the profile..
- **Captive Portal Auth -** The type of Captive Portal Authentication (**None**, **Internal**, or **External**).
- **External Captive Portal Auth** - Enables/Disables external Captive Portal.
- **Portal Server -** The FQDN/IP address of the external captive portal server.
- **Redirect URL -** The redirect URL for the captive portal authentication.
- **HTTPS Redirection -** Specify whether the redirect portal page is using HTTPS protocol.
- **AAA Server Profile -** The AAA Server used for Captive Portal Authentication.
- **Custom Profile -** The External Captive Portal Config File used for communication between APs and the External Portal Server. The External Captive Portal Config File is configured on the AP Groups Screen in the AP Registration application.
- **Captive Portal Profile -** A Captive Portal Profile can be applied to AOS devices. Only one Captive Portal Profile is allowed per profile, but multiple profiles may use the same Captive Portal Profile.
- **Inactivity Interval -** The amount of time, in seconds, before an authenticated device is automatically logged out of the network due to inactivity (MAC address for the device has aged out). This timer value applies only to devices learned in the profile.
- **Client Session Logging -** Enables/Disables client session logging.
- **Client Connection Logging Level:**
  - **Logging HTTP/HTTPs -** Log only the HTTP/HTTPs web session of wireless clients.
  - **Logging ALL -** Log all sessions of wireless clients, including HTTP/HTTPs.
  - **None -** Log only client online/offline behavior, without session details.
- **WCF Profile** - The specified WCF Profile for the Access Role Profile. An Access Role Profile can only contain one WCF Profile.
- **Wireless Client Social Login Vendor -** The vendor(s) selected to allow a wireless client to authenticate through a social media vendor (Facebook, Google, and Rainbow are supported). OmniVista automatically configures the Allowlist Domains for the selected vendor(s). This allows the user to connect over the Internet to the selected vendor(s) for authentication.

- **Allowlist Domains -** Facebook, Google, Rainbow login, or any user-specified Allowlist Domain that allows a user to connect to sites over the Internet without authentication. For example, a hotel may want to allow a guest to connect to their website without authentication. Domains must be in Fully Qualified Domain Name (FQDN) format (e.g., www.marriot.com, www.bbc.com). IP Addresses and http/https prefixes should **not** be used.
- **Allowed list of devices for an isolated client** - The MAC addresses of devices that a client is allowed to access when the Client Isolation mode is enabled. When Client Isolation is enabled for the client SSID or the Access Authentication Profile for the switch port to which the AP is connected, traffic between clients on the same AP in the SSID is blocked; client traffic can only go toward the default gateway.
- **Upstream Bandwidth -** The maximum bandwidth limit allocated for ingress traffic on UNP ports assigned to the profile. If the maximum ingress bandwidth value is set to zero, all ingress traffic is allowed on the UNP port. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)
- **Downstream Bandwidth -** The maximum bandwidth limit allocated for egress traffic on UNP ports assigned to the profile. If the maximum egress bandwidth value is set to zero, all egress traffic is allowed on the UNP port. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)
- **Upstream Burst -** The maximum ingress depth value that is applied to traffic on UNP ports that are assigned to the profile. This value determines how much the traffic can burst over the maximum ingress bandwidth rate. The maximum ingress depth value is configured in conjunction with the maximum ingress bandwidth parameter. When the ingress depth value is reached, the switch starts to drop packets. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)
- **Downstream Burst -** The maximum egress depth value that is applied to traffic on UNP ports that are assigned to profile. This value determines how much the traffic can burst over the maximum egress bandwidth rate. The maximum egress depth value is configured in conjunction with the maximum egress bandwidth parameter. When the egress depth value is reached, the switch starts to drop packets. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)
- **Mapping Type** - Whether the Access Role Profile is mapped to a VLAN or service.
- **Mapping Name** - The VLAN, service, or tunnel ID to which the profile is mapped.
- **MIB set** - The Mibset List that applies to this profile.
- **DHCP Option 82 -** Enables/Disabled the DHCP Option 82 Feature.

Device Config - AAA Profile

The Unified Profile Device Config AAA Profile Screen displays information about all devices to which an AAA Profile has been assigned. You can edit the AAA Profile on a device, or delete the profile from a device(s). To display device information, click on the Devices **ADD** button and select devices. To add/remove devices from the display, click on the **EDIT** button.

Editing a AAA Profile

Select a device in the AAA Profile List and click on the Edit icon to edit the field(s) as described below. When you are finished, click on the **Apply** button.

Authentication Servers

- **802.1X Primary -** Select a Primary 802.1X Authentication Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.

  For wireless devices, 802.1x Primary and Secondary Server configurations will help you to create 802.1x Authentication Server Group which will be used by Access Auth Profiles (Wireless AAA Server Profiles).

- **Captive Portal Primary -** Select a Primary Captive Portal Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.

  Note: Captive Portal Primary and Secondary Server configurations are ignored for wireless devices.

- **MAC Primary-** Select a Primary MAC Authentication Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.

  Note: For wireless devices, MAC Primary and Secondary Server configurations will help you to create a MAC Authentication Server Group that will be used by Access Auth Profiles (Wireless AAA Server Profiles). For IAP Devices, there is not a separate server for MAC Authentication. 802.1x Primary and Secondary Servers are used instead.

Accounting Servers

- **802.1X Primary -** Select a Primary 802.1X Accounting Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.
- **Captive Portal Primary -** Select a Primary Captive Portal Accounting Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.
- **MAC Primary -** Select a Primary MAC Accounting Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.

  Note: For wireless devices, Accounting Servers will help you to create an Accounting Radius Server Group that will be used in Access Auth Profiles (Wireless AAA Server Profiles). Captive Portal Primary and Secondary Servers are ignored. Wireless Devices only accept Radius servers for Accounting. If you select another type, an error will occur when you try to apply the configuration to Wireless Controllers.

Advanced Settings

Advanced settings are not supported on wireless devices and will be ignored when applied to those devices.

MAC Auth

- **Session Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for MAC Authenticated users. If Enabled, the switch will use the Session Timeout attribute received from the Authentication Server in an Accept-Accept message. If Disabled, the switch uses the locally configured timeout interval value (Default = Disabled).

- **Session Timeout Status -** Enables/Disables the Session Timeout option for MAC Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Session Timeout Interval. (Default = Disabled).
- **Session Timeout Interval -** The Session Timeout value, in seconds. When the Session Timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed. Note that when the Session Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again (Range = 12000 - 86400, Default = 43200).
- **Inactivity Timeout Status -** Enables/Disables the Inactivity Timeout option for MAC Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Inactivity Timeout Interval (Default = Disabled).
- **Inactivity Timeout Interval -** The Inactivity Timeout value, in seconds. Make sure the configured value is value greater than the MAC address aging time for the switch. If the Timeout Value is exceeded, the user is not logged out of the network if the MAC address aging time expires before the configured timeout value. Also note that when the Inactivity Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.(Range = 60 - 1200, Default = 600)
- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for MAC Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- **Accounting Interim Interval -** The amount of time between each interim accounting update for MAC accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

802.1X

- **Re-Authentication Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for 802.1x Authenticated users. If Enabled, the Session-Timeout attribute value received from the RADIUS server overrides the locally configured value for the switch. (Default = Disabled).
- **Re-Authentication Timeout -** Enables/Disables the automatic re-authentication of authenticated 802.1X users (Default = Disabled).
- **Re-Authentication Interval -** The amount of time the switch waits, in seconds, before triggering re-authentication of 802.1X users. Note that when the re-authentication time interval is changed, the new value does not apply to existing authenticated 802.1X users until the user is flushed out or when the user is authenticated again. Any new 802.1X

users are re-authenticated based on the current time interval setting. (Range = 600 - 7200, Default = 3600)

- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for 802.1X authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- **Accounting Interim Interval -** The amount of time between each interim accounting update for 802.1x accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

Captive Portal

- **Session Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for Captive Portal Authenticated users. If Enabled, the switch will use the Session Timeout attribute received from the RADIUS server in an Accept-Accept message. If Disabled, the switch to use the locally configured timeout interval value (Default = Disabled).
- **Session Timeout Status -** Enables/Disables the Session Timeout option for Captive Portal Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Session Timeout Interval. (Default = Disabled).
- **Session Timeout Interval -** The Session Timeout value, in seconds. When the Session Timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed. Note that when the Session Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again (Range = 12000 - 86400, Default = 43200).
- **Inactivity Timeout Status -** Enables/Disables the Inactivity Timeout option for Captive Portal Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Inactivity Timeout Interval (Default = Disabled).
- **Inactivity Timeout Interval -** The Inactivity Timeout value, in seconds. Make sure the configured value is value greater than the MAC address aging time for the switch. If the Timeout Value is exceeded, the user is not logged out of the network if the MAC address aging time expires before the configured timeout value. Also note that when the Inactivity Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again. (Range = 60 - 1200, Default - 600)
- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for Captive Portal Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply

to existing authenticated users until the user is flushed out or when the user is authenticated again.

- **Accounting Interim Interval -** The amount of time between each interim accounting update for Captive Portal accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

RADIUS

- **NAS Port ID -** The RADIUS client NAS-Port attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to define a NAS-Port identifier for the NAS-Port attribute. "Default" sets the NAS-Port attribute value to the chassis/slot/port of the user. The NAS-Port attribute value specified with this command is used in Account-Request messages and in Accounting-Request messages.
- **NAS ID -** The RADIUS client NAS-Identifier attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to identify the switch (RADIUS client) in the NAS-Identifier attribute. "Default" sets the NAS-Identifier attribute to the system name of the switch. The NAS-Identifier attribute value specified with this command is used in both Account-Request and Accounting-Request messages.
- **Username Delimiter -** The delimiter character used to separate fields within a RADIUS Server User Name.
- **Password Delimiter -** The delimiter character used to separate fields within a RADIUS Server Password.
- **Calling Station Delimiter -** The delimiter character used to separate fields within a Calling Station ID.
- **Called Station Delimiter -** The delimiter character used to separate fields within a Called Station ID.
- **Username Case -** Indicates if the RADIUS Server User Name must be in Upper Case or Lower Case.
- **Password Case -** Indicates if the RADIUS Server Password must be in Upper Case or Lower Case.
- **Calling Station ID Case -** Indicates if the Calling Station ID must be in Upper Case or Lower Case.
- **Called Station ID Case -** Indicates if the Called Station ID must be in Upper Case or Lower Case.

Deleting a AAA Server Profile

Select a device(s) in the AAA Server Profile List and click on the Delete icon, then click **OK** at the confirmation prompt.

Device Config - Location Policy

The Unified Profile Device Config Location Policy Screen displays information about all devices to which a Location Policy has been assigned. You can edit a Location Policy on a device, or delete the policy from a device(s). To display device/AP Group information, click on the Devices/AP Groups **ADD** button and select devices/groups. To add/remove devices/AP Groups from the display, click on the applicable **EDIT** button.

Editing a Location Policy

Select the policy in the Location Policy List and click on the Edit icon. Edit the fields as described below and click on the **Apply** button to save the changes. Note that you cannot edit the profile name.

- **Location Policy Name -** User-configured Location Policy Name.
- **System Location -** The configured system location for the switch from which the device can access the network.
- **System Name -** The configured system name for the switch from which the device can access the network.

Deleting a Location Policy

Select the policy in the Location Policy List and click on the Delete icon, then click **OK** at the confirmation prompt.

Device Config - Period Policy

The Unified Profile Device Config Period Policy Screen displays information about all devices to which an Period Policy has been assigned. You can edit a Period Policy on a device, or delete the policy from a device(s). To display device/AP Group information, click on the Devices/AP Groups **ADD** button and select devices/groups. To add/remove devices/AP Groups from the display, click on the applicable **EDIT** button.

Editing a Period Policy

Select a device/AP Group in the Period Policy List and click on the Edit icon. Edit the field(s) as described below. When you are finished, click on the **Apply** button.

- **Period Policy Name -** User-configured Period Policy Name.
- **Date/Time** - Click on the Days/Months, Date/Time, and Time of Day sliders to configure the time when the devices can access the network.
- **Timezone -** Select the in which the Period Policy is active.

Deleting a Period Policy

Select the policy in the Period Policy List and click on the Delete icon, then click **OK** at the confirmation prompt.

Device Config - Access Classification

The Unified Profile Device Config Access Classification Screen displays information about all devices/AP Groups to which an Access Classification Profile has been assigned. You can edit the Access Classification Rule on a device, or delete the profile from a device(s). To display device/AP Group information, click on the Devices **ADD** button or AP Groups **ADD** button and

select devices/AP Groups. To add/remove devices/AP Groups from the display, click on the applicable **EDIT** button.

Editing an Access Classification Profile

Select a device in the Access Classification Profile List and edit the field(s) as described below. When you are finished, click on the **Apply** button. Note that the parameters you can edit depend on the Access Classification Profile assigned to the device.

- **MAC Rule (Both AOS and Wireless Devices) -** Defines a MAC Address Access Classification Rule for the specified UNP Access Role Profile. If the source MAC address of the device traffic matches the MAC address defined for the rule, the specified Access Role Profile is applied. Note that when a MAC Access Classification Rule is removed or modified, all MAC addresses classified with that rule are flushed.
  - **Name -** User-configured name for the MAC Rule.
  - **MAC Address -** The MAC address to be used for the rule. If the source MAC address of the device traffic matches the MAC address defined for the rule, the specified Access Role Profile is applied.
  - **VLAN Tag -** An optional VLAN Tag. If configured, traffic must also match this VLAN Tag in addition to the source MAC address.
  - **Customer Domain ID -** An optional Customer Domain ID to which this rule will apply. When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.
  - **Access Role Profile -** Select the Access Role Profile to use for the rule.
- **MAC Range Rule (AOS Devices only) -** Defines a MAC Address Range Access Classification Rule for the specified UNP Access Role Profile. If the source MAC address of the device traffic matches any of the MAC address within the range of MAC addresses, the specified profile is applied. Note that when a MAC Access Classification Rule is removed or modified, all MAC addresses classified with that rule are flushed.
  - **MAC Low Address -** MAC address that defines the low end of the range (e.g., 00:00:39:59:f1:00).
  - **MAC High Address -** MAC address that defines the high end of the range (e.g., 00:00:39:59:f1:90).
  - **VLAN Tag -** An optional VLAN Tag. If configured, traffic must also match this VLAN Tag in addition to the source MAC address.
  - **Customer Domain ID -** An optional Customer Domain ID to which this rule will apply. When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.
  - **Access Role Profile -** Select the Access Role Profile to use for the rule.
- **IP Address Rule (AOS Devices only) -** Defines an IP Address Access Classification Rule for the specified UNP Access Role Profile. If the source IP address of the device traffic matches the IP address defined for the rule, the specified Access Role Profile is applied.

  - **IP Network Address -** The IPv4 network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0).
  - **IP Mask -** An IP address mask to identify the IP subnet for the interface (supports class-less masking).
  - **VLAN Tag -** An optional VLAN Tag. If configured, traffic must also match this VLAN Tag in addition to the source MAC address.
  - **Customer Domain ID -** An optional Customer Domain ID to which this rule will apply. When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.
  - **Access Role Profile -** Select the Access Role Profile to use for the rule.
- **VLAN Tag Rule -** Defines a VLAN Tag for the specified Access Classification Rule. If the source VLAN Tag of the device traffic matches the VLAN Tag defined for the rule, the specified Access Role Profile is applied.
  - **VLAN Tag -** The VLAN Tag used for the rule.
  - **Tag Position (7x only) -** The VLAN Tag position - Inner Tag (Default), Outer Tag.
  - **Customer Domain ID -** An optional Customer Domain ID to which this rule will apply. When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.
  - **Access Role Profile -** Select the Access Role Profile to use for the rule.
- **Location (Wireless Devices only) -** Defines a Location rule for the specified Access Role Profile. The specified Access Role Profile will be applied if the user location (AP name) matches with the value defined in the rule. Note that this rule applies only to Legacy AP devices; Stellar APs do not support Location-based rules.
  - **Name -** The rule name.
  - **Location -** The AP location.
  - **Access Role Profile -**Select the Access Role Profile to use for the rule.
- **ESSID (Wireless Devices only) -** Defines an Extended Service Set Identifier (ESSID) for the specified Access Role Profile. The specified Access Role Profile will be applied if the ESSID of AP (which client is associating) matches with the defined ESSID in the rule.
  - **Name -** The rule name.
  - **ESSID Value -** The ESSID of AP.
  - **Access Role Profile -**Select the Access Role Profile to use for the rule.
- **DHCP Option (Wireless Devices only) -** Defines a DHCP signature ID rule for the specified Access Role Profile.
  - **Name -** The rule name.
  - **Signature ID -** The DHCP signature ID.
  - **Access Role Profile -**Select the Access Role Profile to use for the rule.

- **DHCP Option 77 (Wireless Devices only) -** Defines a DHCP Option 77 rule for the specified Access Role Profile. The specified Access Role Profile will be applied if the user class identifier returned by DHCP server matches with the value defined in the rule.
  - **Name -** The rule name.
  - **Value -** The user class identifier returned by DHCP server.
  - **Access Role Profile -**Select the Access Role Profile to use for the rule.
- **Encryption Type (Wireless Devices only) -** Defines an Encryption Type rule for the specified Access Role Profile. The specified Access Role Profile will be applied if the encryption type used by the client matches with the value defined in the rule.
  - **Name -** The rule name.
  - **Encryption Type -** The encryption type used by the client (e.g., WPA/WPA2 AES, Dynamic WEP).
  - **Access Role Profile -**Select the Access Role Profile to use for the rule.

Deleting an Access Classification Profile

Select a device(s) in the Access Classification Profile List and click on the Delete icon, then click **OK** at the confirmation prompt.

Device Config - Far End IP

The Unified Profile Device Config Far End IP Screen displays information about all devices to which a Far End IP List has been assigned. You can edit the Far End IP List on a device, or delete the it from a device(s). To display device information, click on the Devices **ADD** button and select devices. To add/remove devices from the display, click on the **EDIT** button.

Editing a Far End IP List

Select a device in the Far End IP List and edit the field(s) as described below. When you are finished, click on the **Apply** button.

- **IP Address -** Enter an IP address and click on the Add icon to add an address. Repeat to add additional IP addresses. Click on the Delete icon to remove an IP address.

Deleting a Far End IP List

Select a device(s) in the Far End IP List and click on the Delete icon, then click **OK** at the confirmation prompt.

Device Config - Diagnostic

he Unified Profile Device Config Diagnostics Screen displays Unified Profile information for an end station connected to UNP Ports which can be used to diagnose UNP Profile problems. You can view information for a device by IP Address or MAC Address by selecting the applicable **Search by** criteria, entering the address and clicking on the **Locate** button.

Diagnostic List

- **Device Address -** The IP address of the device.
- **Port -** The slot/port on which the device was learned.
- **MAC Address -** The MAC address of the device.

- **Access Timestamp -** The login timestamp of the device.
- **User Name -** The name used to authenticate the device.
- **IP Address -** The IP address from which the device is sending packets.
- **VLAN -** The device VLAN.
- **Classification Source -** The Classification policy under which the device was learned.
- **Authentication Type -** The authentication type used to authenticate the device (e.g., MAC).
- **Authentication Status -** The status of authentication:
  - Idle
  - In Progress
  - Authenticated
  - Failed
  - Failed Timeout
  - Failed No Server
  - Failed No Resources
- **IP Address Type -** The user IP address type. Currently, only IPv4 is supported.
- **Auth Server IP Used-** The IP address of the Authentication Server used to authenticate the device.
- **Auth Server IP Type -** The Authentication Server IP address type. Currently, only IPv4 is supported.
- **UNP Used -** The UNP used to classify the device.
- **User Role -** The UNP used to classify the device role.
- **User Role Source -** The UNP user role source.
- **Auth Fail Reason -** The authentication failure reason.
- **Auth Fail Retry Count -** The authentication failure retry count (number of times re-authentication is attempted after an authentication failure).
- **Classif Profile Rule -** The Classification Policy from which the device was learned.
- **Rest Access Status -** The MAC VLAN user Authentication Server status.
- **Role Rule -** The Classification Policy Rule used to classify the device.
- **Loc Policy Status -** The Location Policy status (Not Applicable/Pass/Fail).
- **Time Policy Status -** The Time Policy status (Not Applicable/Pass/Fail).
- **Cap Portal Status -** The Captive Portal status (Not Applicable/Pass/Fail).
- **Auth Server Used -** The name of the Authentication Server name used for the latest authentication session of the device.
- **Server Message -** The RADIUS server message displayed to the user.
- **Redirection URL -** The Redirect Server URL.
- **UNP From Auth Server -** The UNP returned by the Authentication Server for the device.
- **QMR Status -** The QMR status (Enabled/Disabled).
- **MC LAG Learning -** The Multi-Chassis Link Aggregate status (Enabled/Disabled).
- **SIP Call Type -** The SIP Call Type for the device (Normal Call/Emergency Call/Not In Call).

- **SIP Media Type -** The SIP Media Type for the device (Other/Audio/Video/None).

Device Config - 802.1X Authentication Profile

The Unified Profile Device Config 802.1X Authentication Profile Screen displays information about all devices to which an 802.1X Authentication Profile has been assigned. You can edit the 802.1X Authentication Profile on a device, or delete the profile from a device(s). To display device/AP Group information, click on the Devices **ADD** button and select devices/groups. To add/remove devices from the display, click on the applicable **EDIT** button.

Editing an 802.1X Authentication Profile

Select a device in the 802.1X Authentication Profile List and edit the field(s) as described below. When you are finished, click on the **Apply** button. Note that the parameters you can edit depend on the 802.1X Authentication Profile assigned to the device.

- **Max Authentication Failures -** The number of times a user can try to log in with the wrong credentials after which the user is blacklisted as a security threat. Set to 0 to disable blacklisting, otherwise enter a non-zero integer to blacklist the user after the specified number of failures. (Range = 0 - 5, Default = 0)
- **Reauthentication -** Enables/Disables re-authentication. If enabled, the client must perform an 802.1X re-authentication after the expiration of the default timer for re-authentication (default value of the timer is 24 hours). If the user fails to re-authenticate with valid credentials, the state of the user is cleared. If derivation rules are used to classify 802.1x-authenticated users, the re-authentication timer per role overrides this setting. (Default = Disabled)
- **Max Reauthentication Attempts -** The number of times a user can try to re-authenticate. (Range = 1 - 10, Default = 3)
- **Termination -** Enables/Disables 802.1X authentication termination on the controller. (Default = Disabled)
- **Termination EAP-Type -** If you enable termination, click either EAP-PEAP or EAP-TLS to select an Extensible Authentication Protocol (EAP) method.
- **Termination Inner EAP-Type -** If you use EAP-PEAP as the EAP method, select one of the following inner EAP types:
  - **EAP-GTC -** Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the controller as a backup to an external authentication server.
  - **EAP MSCHAPV2 -** Described in RFC 2759, this EAP method is widely supported by Microsoft clients.
- **Enforce Machine Authentication -** Enables/Disables Machine Authentication. If enabled, machine authentication is enforced before user authentication, and either the machine-default-role or the user-default-role is assigned to the user, depending on which authentication is successful. (Default = Disabled)
- **Default Machine Role -** The default role (Access Role Profile) assigned to the user after completing only machine authentication. Select an Access Role Profile from the drop-down menu or click on the Add icon to go to the Access Role Profile Screen and create a new one. The default role for this setting is the “guest” role.

- **Default User Role -** The default role (Access Role Profile) assigned to the user after 802.1x authentication. Select an Access Role Profile from the drop-down menu or click on the Add icon to go to the Access Role Profile Screen and create a new one. The default role for this setting is the “guest” role.
- **Radius Accounting Mode -** The RADIUS Accounting Mode (User Authentication/User Association).

Device Config - MAC Authentication Profile

The Unified Profile Device Config MAC Authentication Profile displays information about all devices to which a MAC Authentication Profile has been assigned. You can edit the MAC Authentication Profile on a device, or delete the profile from a device(s). To display device information, click on the Devices **ADD** button select device. To add/remove devices/AP Groups from the display, click on the applicable **EDIT** button.

Editing an 802.1X Authentication Profile

Select a device in the MAC Authentication Profile List and edit the field(s) as described below. When you are finished, click on the **Apply** button. Note that the parameters you can edit depend on the MAC Authentication Profile assigned to the device.

- **Profile Name -** User-configured name for the profile.
- **Max Authentication Failures -** The number of times a client can fail to authenticate before it is blacklisted. A value of zero disables blacklisting. (Range = 0 - 10, Default = 0)
- **Delimeter -** The Delimiter used in the MAC string:
  - **Colon -** Specifies the format XX:XX:XX:XX:XX:XX
  - **Dash -** Specifies the format XX-XX-XX-XX-XX-XX
  - **None -** Specifies the format XXXXXXXXXXXX (Default)
- **Case -** The case (Upper or Lower) used in the MAC string. (Default = Lower).

SSID Profile

The Unified Profile SSID Profile Screen displays all configured SSID Profiles and used to create, edit, assign, and delete SSID Profiles. An SSID Profile can be created and included in an Access Authentication Profile that can be assigned to wireless devices on the network.

Creating an SSID Authentication Profile

Click on the Add icon. Configure the Profile as described below, then click on the **Create** button.

SSID Authentication Profile

- **Profile Name -** User-configured profile name.
- **ESSID -** User configured name that uniquely identifies a wireless network (up to 32 characters). If the ESSID includes spaces, you must enclose it in quotation marks.
- **Hide SSID -** Enables/Disables the SSID name in beacon frames. Note that hiding the SSID does very little to increase security. (Default = Disabled)
- **Enable SSID -** Enables/Disables the SSID Profile.
- **Encryption -** The layer-2 authentication and encryption type used on this ESSID.
- DYNAMIC_WEP - WEP with dynamic keys.

- OPENSYSTEM - No authentication and encryption.
- STATIC_WEP - WEP with static keys.
- WPA_AES - WPA with AES encryption and dynamic keys using 802.1X.
- WPA_PSK_AES - WPA with AES encryption using a preshared key.
- WPA_PSK_TKIP - WPA with TKIP encryption using a preshared key.
- WPA_TKIP - WPA with TKIP encryption and dynamic keys using 802.1X.
- WPA2_AES - WPA2 with AES encryption and dynamic keys using 802.1X.
- WPA2_PSK_AES - WPA2 with AES encryption using a preshared key.
- WPA2_PSK_TKIP - WPA2 with TKIP encryption using a preshared key.
- WPA2_TKIP - WPA2 with TKIP encryption and dynamic keys using 802.1X.
- WPA3_SAE_AES - Need definition? Note that when WPA3_SAE_AES encryption is applied to an AP that does not support it, the encryption will automatically fall back to WPA2_PSK_AES.

Editing an SSID Authentication Profile

Select the Profile in the SSID Authentication Profile Screen and click on the Edit icon to bring up the Edit SSID Authentication Profile Screen. Edit the fields as described above then click on the **Save** button to save the changes to the server. Note that you cannot edit the profile name.

Assigning an SSID Profile

When you click the **Apply To IAP Devices** button, the SSID Profile Assignments Screen appears. Click on the Add/Remove button to select device(s) and click the **Apply** button. The configuration will be applied and the assignment status displayed. Click **OK** to return to the SSID Profile Screen.

Deleting an SSID Authentication Profile

To delete a Profile(s), select the Profile(s) in the table and click on the Delete icon, then click **OK** at the confirmation prompt. If the profile is associated with an Access Authentication Profile, you will be presented with warning prompt that you must remove the SSID Profile(s) from the Access Authentication Profile before it can be deleted. Remove the SSID Profile(s) from the Access Authentication Profile, and then delete the profile(s).

AP Group

The Unified Profile AP Group Screen displays all configured AP (Access Point) Groups and used to create, edit, assign, and delete AP Groups.

Creating an AP Group

Click on the Add icon. Configure the Group as described below, then click on the **Create** button. After creating the AP Group, assign the group to a controller.

- **Group Name-** User-configured name for the group.
- **Access Auth Profiles -** The Access Authentication Profile(s) associated with the group. Selecting an Access Auth Profile will allow for association of the AP Group to the correct Virtual AP Profile inside the Access Auth Profile. Select an Access Auth Profile from the

drop-down menu or click on the Add icon to go to the Access Auth Profile Screen and create a new one.

Editing an AP Group

Select the group in the AP Group Screen and click on the Edit icon to bring up the Edit AP Group Screen. Edit the fields as described above then click on the **Save** button to save the changes to the server. Note that you cannot edit the group name.

Assigning an AP Group

Select a group and click on the **Apply To Wireless Controllers** button. The AP Group Assignments Screen appears. Click on the Devices **ADD** button and select a controller(s). The controller(s) will appear in the List of Selected Devices. If necessary, click on the Devices **EDIT** button to add/remove devices from the list. When you are finished, click on the **Apply** button.

Deleting an AP Group

To delete a group(s), select the group(s) in the table and click on the Delete icon, then click **OK** at the confirmation prompt.

Device Config - Virtual AP

The Unified Profile Device Config Virtual AP Screen displays information about all devices to which a Virtual AP Profile has been assigned. You can edit the Virtual AP Profile on a device, or delete the it from a device(s). To display device information, click on the Devices **ADD** button and select devices. To add/remove devices from the display, click on the **EDIT** button.

Editing a Virtual AP Profile

Select a device in the Virtual AP List and edit field(s) as described below. When you are finished, click on the **Apply** button.

- **Access Auth Profile -** The Access Auth Profile associated with the Virtual AP Profile.
- **VLAN -** The VLAN the to which the profile is assigned.
- **SSID Profile -** The SSID Profile associated with the Virtual AP Profile.
- **Allowed Band -** The band(s) on which to use the Virtual AP:
  - **a -** 802.11a band only (5 GHz)
  - **g -** 802.11b/g band only (2.4 GHz)
  - **all -** Both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz). (Default).
- **Band Steering -** Enables/Disables Band Steering. Band Steering encourages dual-band capable clients to stay on the 5GHz band on dual-band APs. This frees up resources on the 2.4GHz band for single band clients like VoIP phones. The feature supports both campus APs and remote APs that have a virtual AP profile set to tunnel, split-tunnel or bridge forwarding mode. Note, however, that if a campus or remote APs have virtual AP profiles configured in bridge or split-tunnel forwarding mode but no virtual APs in tunnel mode, those APs will gather information about 5G-capable clients independently and will not exchange this information with other APs that only have bridge or split-tunnel virtual APs configured.
- **Dynamic Multicast Optimization -** Enables/Disables Dynamic Multicast Optimization.

- **Dynamic Multicast Optimization Threshold -** The maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops. (Range = 2 - 255, Default = 5)
- **Drop All Broadcast or Multicast Traffic -** If "Enabled", broadcast and multicast traffic is dropped. Do not enable this option for Virtual APs configured in bridge forwarding mode. This configuration parameter is only intended for use for Virtual APs in tunnel mode. In tunnel mode, all packets travel to the controller, so the controller is able to drop all broadcast traffic. When a Virtual AP is configured to use bridge forwarding mode, most data traffic stays local to the AP, and the controller is not able to filter out that broadcast traffic.
- **Convert Broadcast ARP Requests To Unicast -** If "Enabled", all broadcast ARP requests are converted to unicast and sent directly to the client. This configuration parameter is only intended for use for virtual APs in tunnel mode. In tunnel mode, all packets travel to the controller, so the controller is able to convert ARP requests directed to the broadcast address into unicast.
- **Forward Mode -** Controls whether data is tunneled to the controller using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or using a combination of both depending on the destination (e.g., corporate traffic goes to the controller, and Internet access remains local). All forwarding modes support band steering, TSPEC/TCLAS enforcement, 802.11k and station blacklisting.
  - **Tunnel -** The AP handles all 802.11 association requests and responses, but sends all 802.11 data packets, action frames, and EAPOL frames over a GRE tunnel to the controller for processing. The controller removes or adds the GRE headers, decrypts or encrypts 802.11 frames, and applies firewall rules to the user traffic as usual. Both remote and campus APs can be configured in tunnel mode.
  - **Bridge -** 802.11 frames are bridged into the local Ethernet LAN. When a remote AP or campus AP is in bridge mode, the AP (and not the controller) handles all 802.11 association requests and responses, encryption/decryption processes, and firewall enforcement. The 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed.
  - **Split Tunnel -** 802.11 frames are either tunneled or bridged, depending on the destination (e.g., corporate traffic goes to the controller, and Internet access remains local).
  - **Decrypt Tunnel -** Both remote and campus APs can be configured in decrypt-tunnel mode. When an AP uses decrypt-tunnel forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the controller, which then applies firewall policies to the user traffic.
- **Steering Mode -** Band steering supports the following three band steering modes.
  - **Force-5GHz -** The AP will try to force 5Ghz-capable APs to use that radio band.
  - **Prefer-5GHz -**The AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts. (Default)
  - **Band Balancing -** The AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5Ghz band has more channels than the 2.4 GHz band, and that the 5Ghz channels operate in 40MHz while the 2.5Ghz band operates in 20MHz.
- **Virtual AP Enable -** Enables/Disables the Wireless Authentication Profile.

Deleting a Virtual AP Profile

Select a device(s) in the Virtual AP List and click on the Delete icon, then click **OK** at the confirmation prompt.

Device Config - AAA Profile

The Unified Profile Device Config AAA Profile Screen displays information about all devices to which an AAA Profile has been assigned. You can edit the AAA Profile on a device, or delete the profile from a device(s). To display device information, click on the Devices **ADD** button and select devices. To add/remove devices from the display, click on the **EDIT** button.

Editing a AAA Profile

Select a device in the AAA Profile List and click on the Edit icon to edit the field(s) as described below. When you are finished, click on the **Apply** button.

Authentication Servers

- **802.1X Primary -** Select a Primary 802.1X Authentication Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.

  For wireless devices, 802.1x Primary and Secondary Server configurations will help you to create 802.1x Authentication Server Group which will be used by Access Auth Profiles (Wireless AAA Server Profiles).

- **Captive Portal Primary -** Select a Primary Captive Portal Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.

  Note: Captive Portal Primary and Secondary Server configurations are ignored for wireless devices.

- **MAC Primary-** Select a Primary MAC Authentication Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.

  Note: For wireless devices, MAC Primary and Secondary Server configurations will help you to create a MAC Authentication Server Group that will be used by Access Auth Profiles (Wireless AAA Server Profiles). For IAP Devices, there is not a separate server for MAC Authentication. 802.1x Primary and Secondary Servers are used instead.

Accounting Servers

- **802.1X Primary -** Select a Primary 802.1X Accounting Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.
- **Captive Portal Primary -** Select a Primary Captive Portal Accounting Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.
- **MAC Primary -** Select a Primary MAC Accounting Server for the Profile. You can also select Secondary, Tertiary, and Quaternary Backups, however each must be a different server.

Note: For wireless devices, Accounting Servers will help you to create an Accounting Radius Server Group that will be used in Access Auth Profiles (Wireless AAA Server Profiles). Captive Portal Primary and Secondary Servers are ignored. Wireless Devices only accept Radius servers for Accounting. If you select another type, an error will occur when you try to apply the configuration to Wireless Controllers.

Advanced Settings

Advanced settings are not supported on wireless devices and will be ignored when applied to those devices.

MAC Auth

- **Session Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for MAC Authenticated users. If Enabled, the switch will use the Session Timeout attribute received from the Authentication Server in an Accept-Accept message. If Disabled, the switch uses the locally configured timeout interval value (Default = Disabled).
- **Session Timeout Status -** Enables/Disables the Session Timeout option for MAC Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Session Timeout Interval. (Default = Disabled).
- **Session Timeout Interval -** The Session Timeout value, in seconds. When the Session Timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed. Note that when the Session Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again (Range = 12000 - 86400, Default = 43200).
- **Inactivity Timeout Status -** Enables/Disables the Inactivity Timeout option for MAC Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Inactivity Timeout Interval (Default = Disabled).
- **Inactivity Timeout Interval -** The Inactivity Timeout value, in seconds. Make sure the configured value is value greater than the MAC address aging time for the switch. If the Timeout Value is exceeded, the user is not logged out of the network if the MAC address aging time expires before the configured timeout value. Also note that when the Inactivity Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.(Range = 60 - 1200, Default = 600)
- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for MAC Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- **Accounting Interim Interval -** The amount of time between each interim accounting update for MAC accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).

- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

802.1X

- **Re-Authentication Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for 802.1x Authenticated users. If Enabled, the Session-Timeout attribute value received from the RADIUS server overrides the locally configured value for the switch. (Default = Disabled).
- **Re-Authentication Timeout -** Enables/Disables the automatic re-authentication of authenticated 802.1X users (Default = Disabled).
- **Re-Authentication Interval -** The amount of time the switch waits, in seconds, before triggering re-authentication of 802.1X users. Note that when the re-authentication time interval is changed, the new value does not apply to existing authenticated 802.1X users until the user is flushed out or when the user is authenticated again. Any new 802.1X users are re-authenticated based on the current time interval setting. (Range = 600 - 7200, Default = 3600)
- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for 802.1X authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- **Accounting Interim Interval -** The amount of time between each interim accounting update for 802.1x accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

Captive Portal

- **Session Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for Captive Portal Authenticated users. If Enabled, the switch will use the Session Timeout attribute received from the RADIUS server in an Accept-Accept message. If Disabled, the switch to use the locally configured timeout interval value (Default = Disabled).
- **Session Timeout Status -** Enables/Disables the Session Timeout option for Captive Portal Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Session Timeout Interval. (Default = Disabled).
- **Session Timeout Interval -** The Session Timeout value, in seconds. When the Session Timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed. Note that when the Session Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is

flushed out or when the user is authenticated again (Range = 12000 - 86400, Default = 43200).

- **Inactivity Timeout Status -** Enables/Disables the Inactivity Timeout option for Captive Portal Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Inactivity Timeout Interval (Default = Disabled).
- **Inactivity Timeout Interval -** The Inactivity Timeout value, in seconds. Make sure the configured value is value greater than the MAC address aging time for the switch. If the Timeout Value is exceeded, the user is not logged out of the network if the MAC address aging time expires before the configured timeout value. Also note that when the Inactivity Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again. (Range = 60 - 1200, Default - 600)
- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for Captive Portal Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- **Accounting Interim Interval -** The amount of time between each interim accounting update for Captive Portal accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

RADIUS

- **NAS Port ID -** The RADIUS client NAS-Port attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to define a NAS-Port identifier for the NAS-Port attribute. "Default" sets the NAS-Port attribute value to the chassis/slot/port of the user. The NAS-Port attribute value specified with this command is used in Account-Request messages and in Accounting-Request messages.
- **NAS ID -** The RADIUS client NAS-Identifier attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to identify the switch (RADIUS client) in the NAS-Identifier attribute. "Default" sets the NAS-Identifier attribute to the system name of the switch. The NAS-Identifier attribute value specified with this command is used in both Account-Request and Accounting-Request messages.
- **Username Delimiter -** The delimiter character used to separate fields within a RADIUS Server User Name.
- **Password Delimiter -** The delimiter character used to separate fields within a RADIUS Server Password.
- **Calling Station Delimiter -** The delimiter character used to separate fields within a Calling Station ID.

- **Called Station Delimiter -** The delimiter character used to separate fields within a Called Station ID.
- **Username Case -** Indicates if the RADIUS Server User Name must be in Upper Case or Lower Case.
- **Password Case -** Indicates if the RADIUS Server Password must be in Upper Case or Lower Case.
- **Calling Station ID Case -** Indicates if the Calling Station ID must be in Upper Case or Lower Case.
- **Called Station ID Case -** Indicates if the Called Station ID must be in Upper Case or Lower Case.

Deleting a AAA Server Profile

Select a device(s) in the AAA Server Profile List and click on the Delete icon, then click **OK** at the confirmation prompt.

Device Config - AAA Server Group

The Unified Profile Device Config AAA Server Group Screen displays information about AAA Authentication Server Group Profiles configure for devices. You can edit the AAA Servers for an Authentication Server Group Profiles assigned to a device, or delete the profile from a device(s). To display AAA Server Group information for a device, click on the Devices **ADD** button or AP Groups **ADD** button and select devices/AP Groups. To add/remove devices/AP Groups from the display, click on the applicable **EDIT** button.

Editing a AAA Server Group

Select a device in the AAA Server Group List and click on the Edit icon to edit the field(s) as described below. When you are finished, click on the **Apply** button.

- **Profile Name -** The AAA Server Group Profile associated with the device.
- **Primary Server -** The primary authentication server used for the profile.
- **Secondary Server -** The primary authentication server used for the profile.
- **Tertiary Server -** The primary authentication server used for the profile.
- **Quaternary Server -** The primary authentication server used for the profile.

Deleting a AAA Server Group

Select a device(s) in the AAA Server Group List and click on the Delete icon, then click **OK** at the confirmation prompt.

Profile Polling

The Unified Profile Profile Polling Screen is used to set the interval for polling devices the latest Unified Profile configurations. The current configured interval is displayed at the top of the screen. To change the interval, click on the "Reconfigure Poll Interval" link, set the new interval and click on the **Apply** button. (Range = 10 minutes to 24 hours, Default = 1 Hour).

You can also perform an immediate poll of devices. Select an option from the drop-down menu (Use Switch Picker/Use Topology) and click on the **Select Devices** button to choose the devices you want to poll (you can poll up to 512 devices at a time). Click on the **Poll Now** button to poll the devices. When polling is complete, OmniVista will be updated with the latest Unified

Profile information. Note that when polling is complete, you can click on the on the "Show More" link, then click on the "Details" link next to a device for detailed information on the polling operation.

33.0 UPAM

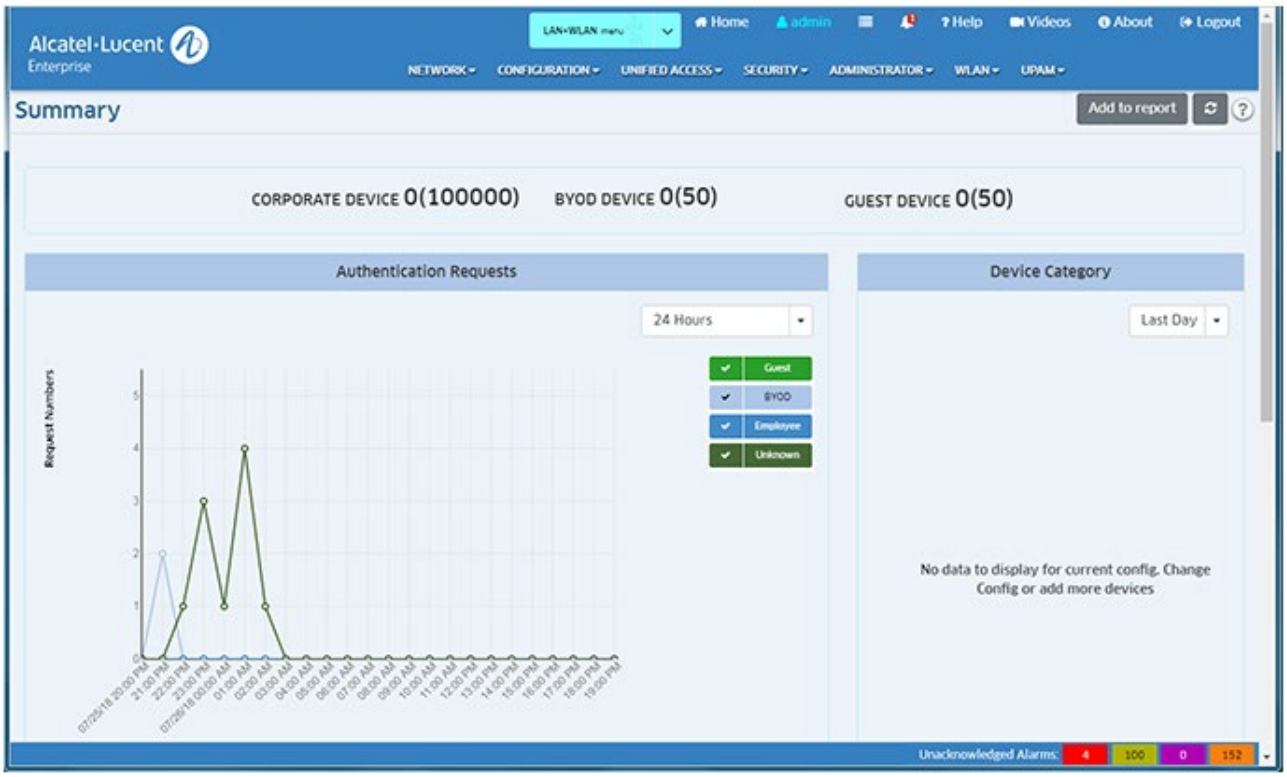
Unified Policy Authentication Manager (UPAM) is a unified access management platform for both AOS Switch Series devices and Stellar AP Series devices. UPAM supports both captive portal server and RADIUS server; and can be used to implement multiple authentication methods, such as MAC authentication, 802.1X authentication, and captive portal authentication. User Profiles can be supported in the OmniVista database or on external servers. The following applications are used to monitor and configure UPAM:

- **Summary -** Provides an overview of UPAM activity on the network.
- **Authentication -** Used to monitor and configure authentication for wired and wireless devices. network.
- **Guest Access -** Used to manage the guest user accessing the network.
- **BYOD Access -** Used to manage the BYOD devices of employee. BYOD service is based on Captive Portal authentication.
- **Settings -** Used to configure UPAM components (e.g., Email Server, External Log Server, External RADIUS Server).

Summary

The UPAM Summary application provides an overview of UPAM activity on the network.

UPAM Summary



The screen provides the following information:

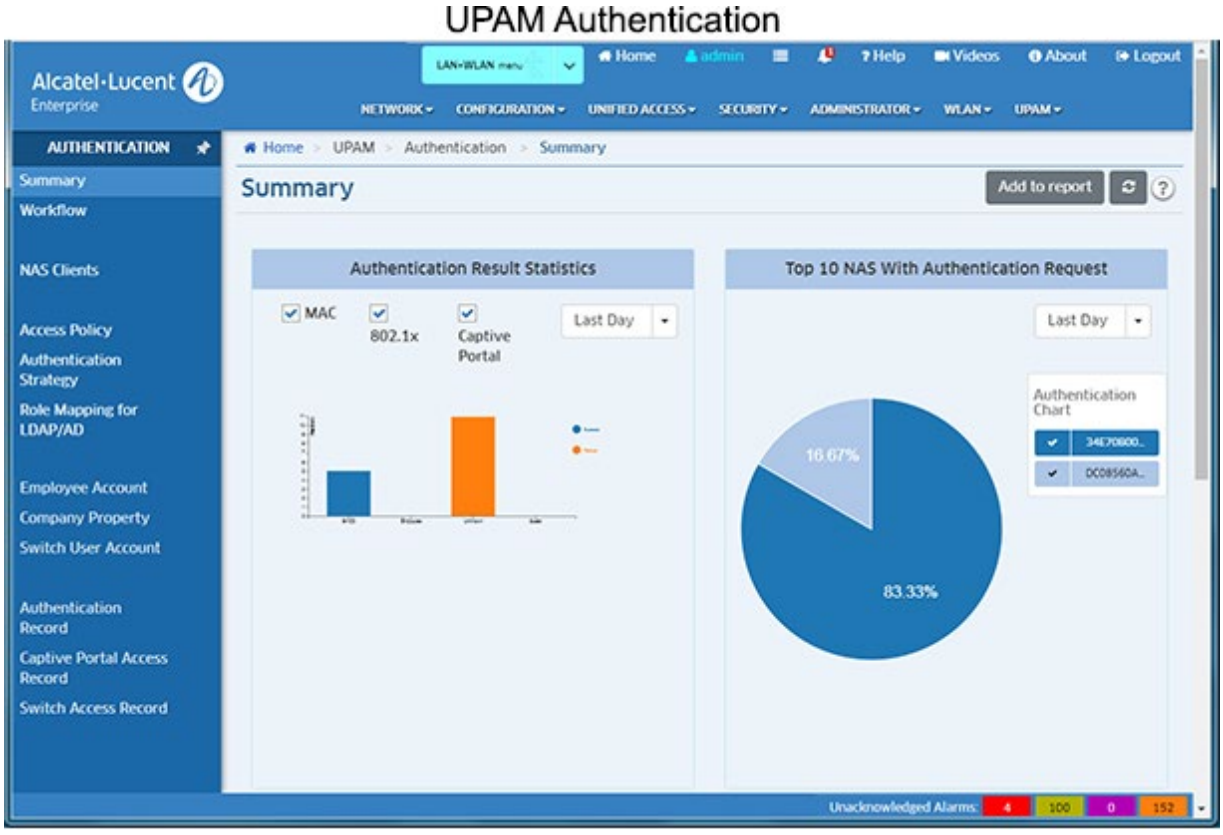
- **Device Statistics -** The top of the Summary Screen displays the number devices/licenses. For Corporate Devices, the first number represents the number of devices being authenticated through UPAM; the number in parenthesis represents

the maximum number of devices allowed. For BYOD and Guest Devices, the first number represents the number of licenses being used; the number in parenthesis represents total allowed devices (based on the Guest and On-Boarding Licenses purchased).

- **Authentication Request -** Displays a line chart depicting authentication requests from all types of users to UPAM, including Guest Users, BYOD Users, Employee Users or other Unknown Users (wired BYOD/Guest Devices that complete MAC authentication but do not complete the portal authentication it is an intermediate state). Use the drop-down to display information from the last 24 Hours or the Last 30 Days. Click and drag in the display to scroll through the data.
- **Device Category -** Displays information by device category (e.g., Computer. Mobile, Tablet) in a pie chart format. Use the drop-down to display information from the last Day, Week, or Month.
- **Connected Device -** Displays a line chart depicting online devices by Guest User, BYOD User, and Employee User. Use the drop-down to display information from the last 24 Hours or the Last 30 Days. Click and drag in the display to scroll through the data.
- **Device Family -** Displays information by device family (e.g., Alcatel Lucent Enterprise, Apple, IBM) in a pie chart format. Use the drop-down to display information from the last Day, Week, or Month.

Authentication

The UPAM Authentication application is used to monitor and configure authentication for wired and wireless devices.



The following screens are used to monitor and configure the Authentication application:

- **Summary -** Provides an overview of authentication activity for the network.
- **Workflow -** Authentication application workflows provide system-defined workflows that can be used to create wired or wireless service for both employees and guest users
- **NAS Clients -** Used to configure NAS Clients. A client connects to the NAS, and the NAS then connects to a AAA Server to determine whether or not the client's supplied credentials are valid.
- **Access Policy -** Used to configure Authentication Access Policies. Authentication Access Policies are used to define the mapping conditions for an authentication strategy.
- **Authentication Strategy -** Authentication Strategy is used to set up a user profile source and login method (web page or not) for authentication, as well as the network attributes applied after passing the authentication.
- **Role Mapping for LDAP -** Authentication Role Mapping enables you to assign different Access Role Profiles and Policy Lists to different sub-user groups by creating mapping rules based on user attributes.
- **Employee Account -** Used to create login accounts for employee users in the local UPAM Database. Company Property - Used to create a Company Property List containing information on devices owned by a company and assigned to an employee (e.g., printers, IP phones, laptops, tablets).
- **Company Property -** Used to create a Company Property List containing information on devices owned by a company and assigned to an employee (e.g., printers, IP phones, laptops, tablets).
- **Switch User Account -** Used to configure user Authenticated Switch Access through UPAM.
- **Authentication Record -** Displays authentication information for all devices authenticated through UPAM.
- **Captive Portal Access Record -** Displays captive portal information for all devices authenticated through UPAM.
- **Switch Access Record -** Displays information about user authentication access to network switches.

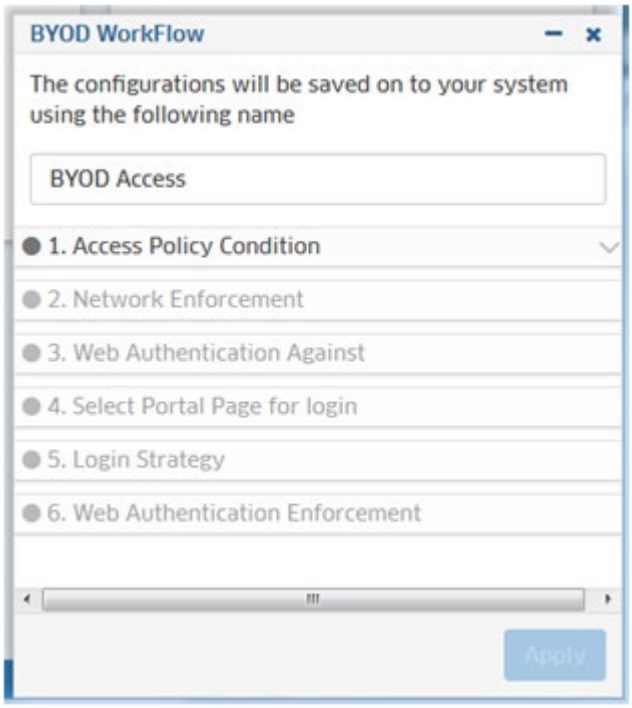
Summary

The Authentication Summary Screen provides an overview of authentication activity for the network. The screen provides the following information:

- **Authentication Result Statistics -** Authentication results statistics for all requests.
- **Top 10 NAS with Authentication Request -** Top 10 NAS with most authentication request sent to UPAM.
- **Top 10 NAS with Authentication Failure -** Top 10 NAS with most failure authentication request rejected by UPAM.
- **Top 10 Reason of Authentication Failure -** Top 10 failure reasons for authentication by UPAM.

Workflow

Authentication application workflows provide system-defined workflows that can be used to create wired or wireless service for both employees and guest users, supporting company devices as well as BYOD devices. Select a workflow (e.g., BYOD Access with MAC and Captive Portal), click on **Begin Now,** and complete the steps in the workflow. When you have completed all of the steps, click on the **Apply** button at the bottom of the workflow to complete the configuration. The BYOD Access with MAC and Captive Portal Workflow is shown below. The configuration process is the same for all workflows.



Workflows can be used to configure:

- BYOD Access
- Guest Access
- MAC or 802.1x Authentication.

BYOD Access

The BYOD Access Workflow uses UPAM to authenticate BYOD users using MAC Address and Captive Portal against a local or external database. Complete the steps as described below, then click on the **Apply** button.

1. Access Policy Condition - Create an SSID.
2. Network Enforcement - Specify an Access Role Profile and Policy List for MAC authentication
3. Web Authentication Against - Specify an authentication source.
4. Select Portal Page for Login - Specify the portal page for login.
5. Login Strategy - Specify success redirect URL.
6. Web Authentication Enforcement - Specify the Access Role Profile and Policy List for web authentication.

Guest Access with MAC and Captive Portal

The Guest Access Workflow uses UPAM to authenticate Guest Users using MAC Address and Captive Portal against the Guest Account Database. Complete the steps as described below, then click on the **Apply** button.

1. **Access Policy Condition -** Create an SSID.
2. **Network Enforcement -** Specify an Access Role Profile and Policy List for MAC authentication.
3. **Select Portal Page for Login -** Specify the portal page for login.
4. **Login Strategy -** Select a login method and specify success redirect URL.
5. **Web Authentication Enforcement -** Specify the Access Role Profile and Policy List for web authentication.
6. **Enable Self-Registration -** Enable the self-registration function.

MAC or 802.1x Authentication

The MAC or 802.1x Authentication Workflow uses UPAM to authenticate users using MAC authentication or 802.1x authentication against a local or external database without Captive Portal. Complete the steps as described below, then click on the **Apply** button.

1. **Access Policy Condition -** Create an SSID.
2. **Web Authentication Against -** Specify an authentication source.
3. **Network Enforcement -** Specify an Access Role Profile and Policy List for MAC authentication.

NAS Clients

The Authentication NAS Clients Screen displays all configured NAS Clients and is used to create, edit, and delete NAS Clients. NAS acts as a gateway to guard access to a network resource. A client connects to the NAS, and the NAS then connects to a AAA Server to determine whether or not the client's supplied credentials are valid. The NAS then allows or denies access to the network resource. The network device in the infrastructure attaching with wired or wireless clients will act as a NAS client, communicating to UPAM which acts as a AAA Server.

Creating a NAS Client

Click on the Add icon to bring up the Create NAS Client Item Screen. Complete the fields as described below, then click on the **Create** button.

- **NAS Name -** The name of the NAS Client.
- **Start IP Address -** The starting IP of the NAS Client segment.
- **End IP Address -** The ending IP of the NAS Client segment.
- **Shared Secret -** The shared secret used by the NAS client to communicate with the Authentication Server.
- **Description -** An optional description for the NAS Client.
- **DM-Attribute -** The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes (User Name/Calling Station ID) to identify the subscriber session.
- **User Name -** The value should exactly match the subscriber name of the session.
- **Calling Station ID -** The value should match the subscriber ID.

In UPAM, there is a system-defined NAS Client Item (All Managed Devices). It cannot be deleted and is used to indicate that all the devices managed by OmniVista are automatically added into the NAS Client Database of UPAM every 15 minutes and perform the AAA process.

The shared secret in the system-defined “All Managed Devices” NAS profile is “123456”. The “All Managed Devices” NAS profile works together with UPAM RADIUS Server, which is downloaded into the devices and applied if configured as a WLAN Service in the Unified Profile application.

System-Defined UPAM Example		
WLAN Service setting (Unified Profile)	Radius Server setting (Security app)	NAS setting (UPAM app)
Apply “UPAMRadiusServer” in AAA profile	UPAMRadiusServer	All Managed Devices

You can create a new NAS Item in UPAM and map it to specific device for authentication. In this use case, a corresponding RADIUS Server and AAA Profile must to be created and applied to the device.

Important Notes:

- A NAS device (AOS Switch) can use multiple IP addresses to communicate with other network elements. The NAS IP that carries the user authentication request should be the same as the NAS device management IP in OmniVista. If not, you can manually create a NAS Client with the correct NAS IP address.
- For external RADIUS use cases, UPAM acts as a RADIUS proxy. The shared secret must be the same for the NAS Client, the UPAM RADIUS Server, the UPAM External RADIUS Server, and the third-party External RADUIS Server (e.g., ClearPass). The shared secret for each is configured as follows:
- NAS Client - Configured on the NAS Clients Screen (UPAM – Authentication – NAS Clients)
- UPAM RADIUS Server - Configured on the RADIUS Server Management Screen (Security – Authentication Servers - Radius)
- UPAM External RADIUS Server - Configured on the External Radius Screen (UPAM – Setting – External Radius)
- Third-Party External RADIUS Server - Configured on the Third-Party RADIUS Server.

  In other words, if for example you create a NAS Client with “alcatel” as the shared secret, you must make sure the shared secret on all of the above RADIUS Servers is “alcatel”.

Editing a NAS Client

Select a NAS Client in the NAS Clients Registration List and click on the Edit icon. Edit the field(s) as described above, and click on the **Apply** button. Note that you cannot edit the NAS IP Address or NAS Name.

Deleting a NAS Client

Select a NAS Client in the NAS Clients Registration List and click on the Delete icon. Click **OK** at the Confirmation Prompt. Note that you cannot delete the “All Managed Devices” Client.

NAS Clients Registration List

The NAS Clients Registration List displays information about all configured NAS Clients.

- **NAS Name -** The name of the NAS Client.
- **Start IP Address -** The starting IP of the NAS Client segment.
- **End IP Address -** The ending IP of the NAS Client segment.
- **Description -** An optional description for the NAS Client.
- **DM-Attribute -** The DM message is used to disconnect subscriber sessions in the system from a RADIUS server.
- **User Name -** The value should exactly match the subscriber name of the session.
- **Calling Station ID -** The value should match the subscriber ID.

Access Policy

Authentication Access Policies are used to define the mapping conditions for an authentication strategy. Through Access Policy configuration, authentication strategy is can be applied to different user groups, which can be divided by SSID or other attributes. The Access Policy Screen displays all configured UPAM Access Policies and is used to create, edit, and delete Access Policies.

Creating an Access Policy

Click on the Add icon to bring up the Create Access Policy Screen. Complete the fields as described below, then click on the **Create** button.

- **Policy Name -** User-configured policy name.
- **Priority -** Access Policy Priority. A user requesting authentication may match several access policies and the one with highest priority will take effect after passing the authentication. (Range = 1 - 99, 1 is the highest priority and 99 is the lowest)
- **Mapping Condition -** Select "Show Basic Attribute Selection" to display basic conditions, select Show Advanced Attribute Selection" to show advanced conditions. Select an Attribute and corresponding Operator, then select or enter a Value.
- **Basic Attributes**

  Authentication Type

  802.1X - 802.1X authentication

  MAC - MAC authentication.

  Network Type

  Wired - Wired network

  Wireless - Wireless network.

  SSID

  Wireless network SSID.

  NAS IP

  Enter the NAS IP address.

  NAS Identifier

  Enter the NAS Identifier.

  NAS Port ID

Enter NAS Port ID.

Port Desc/WLAN Name

Enter a port description of the switch, WLAN name of the wireless network. Note that "WLAN Name" refers either to the "SSID Service Name" in the “SSIDs” application or to the "WLAN Service Name" in the WLAN Service (Expert) application.

NAS Device Name - Enter the NAS device name.

NAS Device Location

Enter the NAS Device location.

AP Group

Enter the AP Group defined in the AP Registration application.

- **Advanced Attributes**

NAS IP Address

Enter the NAS IP address.

Service Type - This attribute indicates the type of service the user has requested, or the type of service to be provided. It may be used in both Access-Request and Access-Accept packets. A NAS is not required to implement all of these service types, and must treat unknown or unsupported Service-Types as though an Access-Reject had been received instead.

Login User - The user should be connected to a host.

Call Check - Used by the NAS in an Access-Request packet to indicate that a call is being received and that the RADIUS Server should send back an Access-Accept to answer the call, or an Access-Reject to not accept the call, typically based on the Called-Station-Id or Calling-Station-Id attributes. It is recommended that such Access-Requests use the value of Calling-Station-Id as the value of the User-Name.

Call Back Administrative - The user should be disconnected and called back, then granted access to the administrative interface to the NAS from which privileged commands can be executed.

Voice - Voice service type.

Fax - Fax service type.

Modem Relay - Modem Relay service type.

IAPP Register - IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, IEEE 802.11F, June 2003.

IAPP AP Check - IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, IEEE 802.11F, June 2003.

Framed User - A Framed Protocol should be started for the User, such as PPP or SLIP.

- **EAP Type Restriction -** Enables/Disables EAP Protocol Type Restriction. If enabled, you can restrict authentication to the selected EAP Protocol(s) below.
  - **EAP-PEAP -** Restricts authentication to EAP-PEAP Protocol.

- **EAP-TLS -** Restricts authentication to EAP-TLS Protocol

Callback Login User - The user should be disconnected and called back, then connected to a host.

Callback Framed User - The user should be disconnected and called back, then a Framed Protocol should be started for the User, such as PPP or SLIP.

Outbound User - The user should be granted access to outgoing devices.

Administrative User - The user should be granted access to the administrative interface to the NAS from which privileged commands can be executed. (IETF rfc2865)

NAS Prompt User - The user should be provided a command prompt on the NAS from which non-privileged commands can be executed. (IETF rfc2865)

Authenticate Only - Only Authentication is requested, and no authorization information needs to be returned in the Access-Accept (typically used by proxy servers rather than the NAS itself). (IETF rfc2865)

Callback NAS Prompt - The user should be disconnected and called back, then provided a command prompt on the NAS from which non-privileged commands can be executed. (IETF rfc2865)

NAS Identifier

Enter the NAS Identifier and click on the Add icon.

NAS Port Type - This attribute indicates the type of physical port of the NAS that is authenticating the user. It can be used instead of, or in addition to, the NAS-Port attribute. It is only used in Access-Request packets. Either NAS-Port or NAS-Port-Type or both should be present in an Access-Request packet if the NAS differentiates among its ports.

NAS Port ID

Enter the NAS port ID.

Alcatel Port Description

Enter the Alcatel Port Description.

Alcatel Device Name

Enter the Alcatel Device Name

Alcatel Device Location

Enter the Alcatel Device Location and click on the Add icon.

Alcatel AP Group

Enter the Alcatel AP Group Name and click on the Add icon.

- **Authentication Strategy -** Authentication strategy that will be utilized when the Access Policy is matched.

Editing an Access Policy

Select a policy in the Access Policy List and click on the Edit icon. Edit the field(s) as described above, and click on the **Apply** button. Note that you cannot edit a Policy Name.

Deleting an Access Policy

Select a policy in the Access Policy List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Access Policy List

The Access Policy List displays information about all configured UPAM Access Policies.

- **Policy Name -** User-configured policy name.
- **Authentication Strategy -** Authentication strategy that will be utilized when the Access Policy is matched.
- **Mapping Condition -** The mapping condition configured for the policy.
- **Priority -** The Access Policy Priority. (Range = 1 - 99, 1 is the highest priority and 99 is the lowest)

Authentication Strategy

Authentication Strategy is used to set up a user profile source and login method (web page or not) for authentication, as well as the network attributes applied after passing the authentication. The Authentication Strategy Screen displays all configured authentication strategies and is used to create, edit, and delete Authentication Strategies.

Creating an Authentication Strategy Policy

Click on the Add icon to bring up the Create Authentication Strategy Screen. Complete the fields as described below, then click on the **Create** button.

General

- **Strategy Name -** User-configured name for the authentication strategy.
- **Authentication Source -** Specify the source of the user profile (Account/Password). The user profile can reside different servers and is required to specified so that UPAM is able to obtain the user profile for authentication.
- **None -** Authenticate against “None”. This is only supported for MAC authentication, which requires captive portal authentication. 802.1x Authentication is not supported. In this case, a user needs to pass captive portal authentication first (authentication method could be by Account + Password/Access Code/Terms of Use/etc.), the MAC address of the user will be stored and the user will complete the MAC authentication. For a guest user, the devices will be displayed in UPAM - Guest Access - Guest Device - Remembered Device Screen. For an Employee user, the devices will be displayed in UPAM - BYOD Access - BYOD Device - Remember Device Screen.
- **Local Database -** Authenticate against the user profile in the local UPAM database. An Employee or Guest user must be created before authentication. An Employee Guest User is created on the UPAM – Authentication - Employee Account Screen. A Guest User is created on the UPAM Guest Access - Guest Account Screen.
- **External LDAP/AD -** Authenticate against the user profile in an external LDAP/AD sever. The server is configured on the UPAM – Setting - LDAP/AD Configuration Screen.
- **External Radius -** Authenticate against the user profile in an external RADIUS server. The server is configured on the UPAM – Setting - External Radius Screen.

Network Enforcement Policy

- **Enable Role Mapping** (External LDAP/AD Server Only) **-** Enables/Disables Role Mapping. If enabled, Role Mapping allows you to restrict network access to specific User Groups authenticated with 802.1x authentication using Windows AD. If enabled, select an "Unmatched Action" below.
- **Role Mapping Unmatched Action** (External LDAP/AD Server Only) **-** Select the action to take for User Groups that do not match any Role Mapping Policies (Accept/Reject).
- **Company Property Check** - Whether or not OmniVista will check to see if the device MAC address is in the Company Property database. When check MAC address is enabled, you have the option to specify an Access Role Profile, Policy List, or other attributes for when the check is successful (MAC address is in the database) and for when the check fails (MAC address is not in the Company Property database).
- **Default Access Role Profile** - Default Access Role Profile for the authentication strategy.
- **Default Policy List** - Default Access Policy for the authentication strategy.
- **Other Attributes** - Select an attribute from the drop-down, enter a value and click on the Add icon to add the attribute. Repeat the process to add additional attributes.
    - **Session Timeout -** The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default = 43200)
    - **Accounting Interim Interval -** Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 – 1200, Default = 600)
    - **WISPr Bandwidth Max Up -** The user upstream bandwidth, in kbit/s. By default, it is not limited.
    - **WISPr Bandwidth Max Down -** The user downstream bandwidth, in kbit/s. By default, it is not limited.

Web Redirection Enforcement Policy

- **Web Authentication -** Specify whether or not web redirection is required and which web login page is going to be used during the authentication.
    - **None -** No web redirection during the authentication.
    - **Guest -** Redirect to the guest login page during the authentication.
    - **Employee -** Redirect to the employee login page during the authentication.
    - **Guest and Employee -** Redirect to the guest and employee login page during the authentication (only applicable for wired access).
- **Access Strategy -** Specify the access strategy for each user group.
- **Guest Access Strategy -** Specify the access strategy for guest users.
- **BYOD Access Strategy -** Specify the access strategy for employee users with BYOD devices.

- **Location Policy -** Specify whether to change the enforcement policy when the location is different.
    - **New Enforcement Policy -** Always apply new enforcement policy to clients when connecting.
    - **Remember New Enforcement Policy -** Always apply the remembered enforcement policy to clients when connecting.

Recommended Combinations of Authentication Source and Web Authentication			
	Authentication Source	**Web Authentication**	**Use Case**
Combination 1	None	Guest/Employee/Guest and Employee	Captive Portal Authentication
Combination 2	Local Database	None	MAC/802.1x Authentication
Combination 3	External LDAP/AD	None	802.1x Authentication
Combination 4	External RADIUS	None	802.1x Authentication

Editing an Authentication Strategy

Select a strategy in the Authentication Strategy List and click on the Edit icon. Edit the field(s) as described above and click on the **Apply** button. Note that you cannot edit a Strategy Name.

Deleting an Authentication Strategy

Select a strategy in the Authentication Strategy List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Authentication Strategy List

The Authentication Strategy List displays information about all configured Authentication Strategies.

- **Strategy Name -** User-configured name for the authentication strategy.
- **Authentication Source -** Specify the source of the user profile (Account/Password). The user profile can reside different servers and is required to specified so that UPAM is able to obtain the user profile for authentication.
- **Enable Role Mapping -** Enables/Disables the "Role Mapping for LDAP/AD" function for authentication sources with external LDAP/AD.
- **Company Property Check** - Enables/Disables MAC address check. If enabled, the Company Property database is checked to see if it contains the device MAC address.
- **Default Access Role Profile -** Default Access Role Profile for the authentication strategy.
- **Default Policy List -** Default Access Policy for the authentication strategy.
- **Web Authentication -** The Web Authentication configuration (None, Guest, Employee, Guest and Employee).
- **Guest Account Strategy -** The name of the Guest Access Strategy used.

- **BYOD Access Strategy -** The name of the BYOD Access Strategy used.
- **Session Timeout Status -** Enables/Disables session timeout attribute. The Session Timeout attribute as defined in RFC 2865 is included in the Access-Accept message and sets the maximum number of seconds of service to be provided to the user before termination of the session. If disabled, an empty value will be transferred to the NAS device and the device's default session timeout policy will take effect.
- **Session Timeout Interval -** Maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. (Range = 12000 - 86400, Default = 43200)
- **Account Interim-Interval Status -** Enables/Disables the accounting attribute. If disabled, an empty value will be transferred to NAS device and the device's default accounting policy will take effect. **Accounting Interim Interval -** Interval for RADIUS accounting, in seconds. (Range = 60 – 1200, Default = 600)

Attribute for LDAP

The Attribute for LDAP Screen is used to manage the LDAP/AD attributes for AP authentication through an external LDAP/AD Server. The attributes can be used as mapping conditions for assigning Role/Access Role Profiles. You can fetch the attributes from the UPAM LDAP/AD Server or create attributes if auto fetch is not successful. Attributes in the list can be selected as mapping conditions on the Role Mapping for LDAP/AD Screen.

Fetching LDAP/AD Attributes

Click on the **Fetch** button to pull attributes from the UPAM LDAP/AD Server. The attributes will be displayed in the LDAP Attribute List.

Creating LDAP/AD Attributes

Click on the Add icon to create new attributes. Enter the attribute in the Name field and click on the **Create** button.

Deleting LDAP/AD Attributes

Select the attribute(s) in the LDAP Attribute List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Role Mapping for LDAP/AD

Authentication Role Mapping for LDAP/AD enables you to assign different Access Role Profiles and Policy Lists to different sub-user groups by creating mapping rules based on user attributes. For example, you could assign a Premium Access Role Profile with larger bandwidth to the VIP group in LDAP/AD. The Role Mapping for LDAP/AD Screen displays all configured mappings and is used to create, edit, and delete mappings.

Creating a Mapping

Click on the Add icon to bring up the Create Role Mapping for LDAP/AD Screen. Complete the fields as described below, then click on the **Create** button.

- **Name -** User-configured name for the mapping rule.

- **Priority -** Priority of the role mapping rule. A user requesting LDAP/AD authentication may match several role mapping rules; the one with highest priority will take effect after passing authentication. (Range = 1 - 99, 1 is the highest priority and 99 is the lowest)
- **LDAP/AD Attributes Condition**
- **Attribute -** LDAP/AD attributes used as role mapping rule key.
- **Value -** Role mapping rule value.

Note: You can also click on the **Fetch** button to fetch attributes from the LDAP/AD Server to specify mapping conditions.

- **Default Access Role Profile -** Access Role Profile applied to the user after matching the role mapping rule.
- **Default Policy List -** Policy List applied to the user after matching the role mapping rule.
- **Other Attributes -** Select an attribute from the drop-down, enter a value and click on the Add icon to add the attribute. Repeat the process to add additional attributes.
- **Session Timeout -** The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default =43200)
- **Accounting Interim Interval -** Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 – 1200, Default = 600)
- **WISPr Bandwidth Max Up -** The user upstream bandwidth, in kbit/s. By default, it is not limited.
- **WISPr Bandwidth Max Down -** The user downstream bandwidth, in kbit/s. By default, it is not limited.

Editing a Mapping

Select a mapping Role Mapping List and click on the Edit icon. Edit the field(s) as described above, and click on the **Apply** button. Note that you cannot edit a Mapping Name.

Deleting a Mapping

Select a mapping in the Role Mapping List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Role Mapping List

The Role Mapping List displays information about all configured mappings.

- **Condition -** The mapping condition.
- **Default Access Role Profile -** Access Role Profile applied to the user after matching the role mapping rule.
- **Default Policy List -** Policy List applied to the user after matching the role mapping rule.
- **Name -** User-configured name for the mapping rule.

- **Priority -** Priority of the role mapping rule. A user requesting LDAP/AD authentication may match several role mapping rules; the one with highest priority will take effect after passing authentication. (Range = 1 - 99, 1 is the highest priority and 99 is the lowest).

Employee Account

The Authentication Employee Account Screen is used to create login accounts for employee users in the local UPAM Database. The Employee Account Screen displays all configured employee accounts and is used to create, edit, and delete employee accounts.

Creating an Employee Account

Click on the Add icon to bring up the Create Employee Account Screen. Complete the fields as described below, then click on the **Create** button.

- **Username -** User name for the employee account.
- **Password -** Password for the employee account.
- **Repeat Password –** Re-enter to confirm the employee password.
- **Telephone -** Optional telephone number of the employee.
- **Email -** Optional Email address of the employee.
- **Access Role Profile -** Access Role Profile that is bound to the employee account. It is prior to the Access Role Profile configured in Authentication Strategy.
- **Policy List** – Policy List that is bound to the employee account. It is prior to the Policy List configured in an Authentication Strategy.
- **Other Attributes -** Select an attribute from the drop-down, enter a value and click on the Add icon to add the attribute. Repeat the process to add additional attributes.
- **Session Timeout -** The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default =43200)
- **Accounting Interim Interval -** Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 – 1200, Default = 600)
- **WISPr Bandwidth Max Up -** The user upstream bandwidth, in kbit/s. By default, it is not limited.
- **WISPr Bandwidth Max Down -** The user downstream bandwidth, in kbit/s. By default, it is not limited.
- **Full Name -** Full name of the employee.
- **Department -** Department of the employee.
- **Position -** Employee position in the company.
- **Description -** Description of the employee account.

Note: You can automatically import a xls/csv/xlsx file containing Employee Account information by clicking on the **Import** button at the top of the screen. You can also download a template by clicking on the **Import** button then clicking on the **Template Download** button.

Editing an Employee Account

Select an employee in the Employee Account List and click on the Edit icon. Edit the field(s) as described above and click on the **Apply** button. Note that you cannot edit a Username.

Deleting an Employee Account

Select an employee in the Employee Account List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Employee Account List

The Employee Account List displays information about all configured Employee accounts.

- **Username -** User name for the employee account.
- **Telephone -** Optional telephone number of the employee.
- **Email -** Optional Email address of the employee.
- **Effective Date -** The date and time the account was created.
- **Full Name -** Full name of the employee.
- **Department -** Department of the employee.
- **Position -** Employee position in the company.
- **Description -** Description of the employee account.
- **Access Role Profile -** Access Role Profile that is bound to the employee account. It is prior to the Access Role Profile configured in Authentication Strategy.
- **Policy List -** Policy List that is bound to the employee account. It is prior to the Policy List configured in an Authentication Strategy.

Company Property

The Authentication Company Property Screen displays information on devices owned by a company that can be assigned to an employee for daily use (e.g., printers, IP phones, laptops, tablets), and is used to create, edit, and delete property information. If a device is configured as a Device Specific PSK device, you can also print out a PSK Passphrase or QR Code for a user to enable them to log into the network.

Creating a Company Property List Entry

Click on the Add icon to bring up the Create Company Property Screen. Complete the fields as described below, then click on the **Create** button to add a device. Note that you can also add multiple devices at once by importing the information in an Excel or CSV file.

- **Device MAC -** MAC address of the company device.
- **Device Name -** System name of the company device.
- **Employee Account -** The employee account to which the company device is associated.
- **Device Category -** Category of the company device:
- Computer
- Mobile
- Tablet

- Game console
- Digital media receiver
- Others
- **Device Family -** Production vendor of the company device:
- Alcatel-Lucent Enterprise
- Apple
- Samsung
- Huawei
- Microsoft
- LG
- Lenovo
- HP
- IBM
- Nokia
- MI
- HTC
- Sony
- Blackberry
- Others
- **Device OS -** Operation system of the company device:
- Linux
- Windows
- MacOS
- Android
- IOS
- Others
- **Enable Device Specific PSK -** Enables/Disables Device Specific PSK. Device Specific PSK provides more security than traditional PSK. If Device Specific PSK is enabled on a wireless network and a device is configured for Device Specific PSK, when the AAA Server sends the Radius Access Accept for MAC Authentication for the device, it will also send the specific pre-shared key for that device, differentiated by the device's MAC Address. This means that each device will have a different key. If enabled:
- **Device Specific Passphrase -** The Device Specific Passphrase.
- **Device Specific Passphrase Retype -** Re-enter the Passphrase.
- **Device Specific Passphrase Validity Period -** Select the duration for the Device Specific Passphrase.

  Note: Device Specific PSK must be enabled on a wireless network as well as the device. Device Specific PSK is enabled on either the WLAN - SSIDs Screen or the WLAN - Service (Expert) Screen.

- **Access Role Profile -** Access Role Profile that is bound to the company device. It is prior to the ARP configured in authentication strategy.
- **Policy List -** Policy List that is bound to the company device. It is prior to the policy list configured in authentication strategy.
- **Other Attributes -** Select an attribute from the drop-down, enter a value and click on the Add icon to add the attribute. Repeat the process to add additional attributes.
- **Session Timeout -** The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default =43200)
- **Accounting Interim Interval -** Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 – 1200, Default = 600)
- **WISPr Bandwidth Max Up -** The user upstream bandwidth, in kbit/s. By default, it is not limited.
- **WISPr Bandwidth Max Down -** The user downstream bandwidth, in kbit/s. By default, it is not limited.

Note: You can automatically import a xls/csv/xlsx file containing Company Property information by clicking on the **Import** button at the top of the screen. You can also download a template by clicking on the **Import** button then clicking on the **Template Download** button.

Importing Multiple Devices

You can add multiple devices at once to the Company Property list by importing the devices in an Excel or CSV File. Click on the **Import** button at the top of the screen. The Import File Window will appear. Click on the **Browse** button to locate the Excel or CSV File, then click on **Import**. The devices in the file will be populated in the Company Properties List.

You can download an Excel or CSV Template that you can use to create an import file. Click on the **Import** button at the top of the screen. The Import File Window will appear. Click on the **Template** button to download a Zip File containing an Excel Template File and a CSV Template File. Use the template file to create a list of devices that you can import into the Company Property List.

Editing a Company Property Entry

Select an employee account in the Company Property List and click on the Edit icon. Edit the field(s) as described above, and click on the **Apply** button. Note that you cannot edit a Device MAC address.

Deleting a Company Property Entry

Select an employee account in the Company Property List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Printing a PSK Passphrase or QR Code

If a device in the Company Property List has Device Specific PSK enabled, you can print the PSK Passphrase or a QR Code version of the Passphrase to give to a user to enable them to

log into the network. Select a device(s) in the Company Property List and click on one of the buttons at the top of the screen:

- **Print PSK -** Prints the PSK Passphrase.
- **Print QR Code -** Prints a QR Code version of the PSK Passphrase that the user can scan to obtain the Passphrase.

Company Property List

The Company Property List displays information about company property that can be assigned to employees. The Online Devices List displays information about devices associated with an Employee account that have been authenticated and accessed the network.

Company Property

The Company Property List displays information about company property that can be assigned to employees.

- **Employee Account -** The employee account to which the company device is associated.
- **Device MAC -** MAC address of the company device.
- **Device Name -** System name of the company device.
- **Device Category -** Category of the company device (e.g., Computer, Mobile Tablet).
- **Device Family -** Production vendor of the company device (e.g., Alcatel Lucent Enterprise, Apple IBM).
- **Device OS -** Operation system of the company device (e.g., Linux, Windows, IOS).
- **Effective Date -** The date and time the company device information was first entered.
- **Last Authentication Time -** The date and time the company device was last authenticated.
- **Last Access Location -** The date and time the company device last accessed the network.
- **Status -** Device status.
- **Access Role Profile -** Access Role Profile that is bound to the company device. It is prior to the ARP configured in authentication strategy.
- **Policy List -** Policy List that is bound to the company device. It is prior to the policy list configured in authentication strategy.

Online Devices

The Online Devices List displays information about devices assiciated with an Employee account that have accessed the network. You can also select a device(s) in the list and click on the **Kick Off** button to immediately log the user out of the network. The user will have to log in again to connect to the network again.

- **Account Name -** The employee account to which the company device is associated.
- **Client IPv4 -** The IPv4 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses.

- **Client IPv6 -** The IPv6 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses.
- **Device MAC -** MAC address of the company device.
- **Session Start -** The time when the user passed authentication and a connection session was created.
- **Session Stop -** The time when the connection session ended.
- **Acct Status Type -** Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop). Values: Start (1), Stop (2), Interim-Update (3), Accounting-On (7) Accounting-Off (8).
- **Acct Terminate Cause -** Indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
- 1 - User Request: User logout.
- 4 - Idle Timeout: User activity logout (only applicable for MAC based or Captive Portal users).
- 6 - Admin Reset: Operator logout/flush operation.
- 7 - Admin Reboot: Operator reboot operation.
- 8 - Port Error: Port down, NI down.
- 9 - NAS-Error: Any software notification that the user is no longer authenticated.
- **Acct Session Time -** Indicates how many seconds the user has received service, and can only be present in Accounting-Request records where the Acct Status Type is set to Stop.
- **Session Timeout Interval -** The maximum number of seconds of service provided prior to session termination.
- **Account Session ID** - Unique Accounting ID that makes it easy to match start and stop records in a log file. The start and stop records for a given session MUST have the same Acct Session ID.
- **Acct Interim Interval -** The number of seconds between each interim update, in seconds, for this specific session.
- **Final Access Role Profile -** The Access Role Profile assigned by NAS in effect on the user device, but it is not Access Role Profile returned by UPAM.
- **Tunnel Private Group ID -** Used to support the legacy VLAN assignment from RADIUS (ID = VLAN ID).
- **Authentication Method -** The method used to authenticate the device (e.g., EAP-PEAP).
- **Access Device SSID -** The wireless service broadcast by the NAS and connected by user device (only valid for wireless access).
- **Access Device Location -** The location of the NAS.
- **Access Device Name -** The system name of the NAS to which the user device is attached.
- **Auth Resource -** The user profile database used in authentication (e.g., None, Local Database, LDAP/AD, external RADIUS server); can refer to the authentication strategy definition.

- **Access Device MAC -** The MAC address of the NAS to which the user device is attached.
- **Called Station ID -** Allows the NAS to send the phone number the user called, using Dialed Number Identification (DNIS) or similar technology inside the Access-Request packet:
- For Switch - Switch MAC Address.
- For AP - radio_MAC_address: SSID_NAME.
- **NAS Port Type -** The type of physical port type of the NAS authenticating the user:
- Wireless-IEEE 802.11
- Ethernet.
- **NAS IP Address -** The identifying IP Address of the NAS.
- **NAS Port -** The physical port number of the NAS authenticating the user.
- For Switch - if index
- For AP - Wireless radio index.
- **Authentication Type -** The authentication type from the user requesting authentication (MAC authentication, 802.1x authentication, and Captive Portal authentication).
- **Framed MTU -** The Maximum Transmission Unit to be configured for the user when it is not negotiated by some other means (e.g., PPP). It is a fixed value = 1400.
- **NAS ID -** The NAS identifier, identify the NAS originating the Access-Request. (The attribute can be configured in Unified Access - Unified Profile – Template - AAA Server Profile.)
- **Access Role Profile -** The Access Role Profile that is bound to the employee account. It is prior to the Access Role Profile configured in Authentication Strategy.
- **Policy List -** The Policy List that is bound to the employee account. It is prior to the Policy List configured in an Authentication Strategy.
- **Slot/Port -** The slot/port number on the switch to which the device is connected (only for wired access).
- **Port Desc/WLAN Service**
- For Switch - if index
- For AP - Wireless radio index.
- **NAS Port ID -** The NAS authenticating the user (the attribute can be configured in Unified Access - Unified Profile – Template - AAA Server Profile):
- For Switch - chassis/slot/port
- For AP - WLAN service.
- **Access Policy -** The name of the Access Policy for the user.
- **Authentication Strategy** - The name of the Authentication Strategy for the user.
- **Termination Action -** Fixed with “Radius-Request”. When the session is timed out, the user needs to be re-authenticated.
- **Upstream Bandwidth -** Device upstream bandwidth, in kbit/s.
- **Downstream Bandwidth -** Device downstream bandwidth, in kbit/s.

- **Acct Input Packets -** Indicates how many packets have been received from the port over the course of this service being provided to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop".
- **Acct Output Packets -** Indicates how many packets have been sent to the port in the course of delivering this service to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop"..
- **Acct Input Octets -** Indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop".
- **Acct Output Octets -** Indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop".
- **Acct Input Gigawords -** Indicates how many gigawords have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop".
- **Acct Output Gigawords -** Indicates how many gigawords have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop".
- **Acct Multi-Session ID -** A unique Accounting ID to make it easy to link together multiple related sessions in a log file.
- **Roaming Information -** Client roaming historical information (indicates the client roamed a path from AP to AP).
- **Web Access Strategy -** Guest Strategy or BYOD Strategy.
- **Access AP Group -** AP Group through which the user accesses the network.

Switch User Account

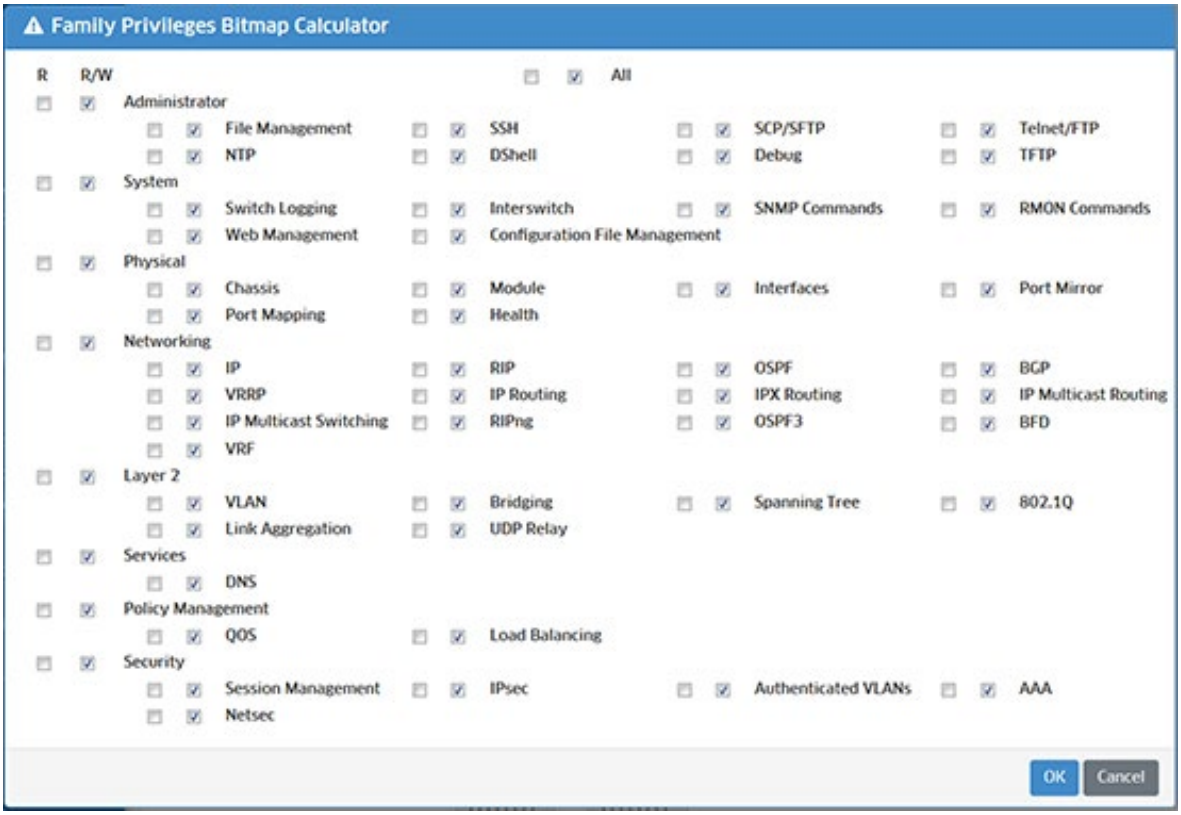
The Switch User Account Screen displays all users configured for Authenticated Switch Access (ASA) through UPAM and is used to create, edit, and delete switch user accounts. You can also enable/disable the UPAM local database for ASA, and enable/disable an existing Switch User Account. After creating a switch user, you create a AAA Profile for the user, setting UPAM as the server used for switch access, and assign the AAA Profile to network switches. See UPAM Authenticated Switch Access Workflow for more details.

Creating a User

Complete the fields as described below and click on the **Create** button to create a new user. You can also create multiple accounts by importing an Excel or .CSV file.

- **Username -** The user's username to access a switch.
- **Description -** Optional description for the user.
- **First Name -** The user's first name (optional).
- **Last Name -** The user's last name (optional).
- **Email -** The user's contact email (optional).
- **Password -** The user password to access a switch.
- **Repeat Password -** Re-enter the user password.
- **Privileges -** Select the access level for the user:

- **Read/Write -** Read/Write access for all Domain Families (e.g., System Domain, Physical Domain) on the switch. (Default)
- **Read Only -** Read Only access for all for all Domain Families.
- **Advanced -** Enables you to customize privileges for a user. When you select "Advance", BitMap representations of user privileges are displayed (e.g., Read 1, Read 2). Click on the "BitMap Calculator" link for AOS 8 and/or AOS 6 to bring up the Family Privileges Bitmap Calculator Screen (the AOS 6 screen is shown below). By default, all operations are configured as "Read/Write". Select/unselect items to customize privileges. When you are done, click **OK** to return to the Switch User Account Screen.



The **All** checkboxes at the top-center of the screen can be used to set all privileges for all groups to "Read-Only" (left checkbox) or "Read/Write" (right checkbox, selected by default). You can also set all privileges by group (e.g., Administrator, System) by selecting a checkbox next to the group name, or select individual privileges within a group. The AOS 8 screen is the same. However, instead of the All checkbox at the top-center of the screen, you have the option to select **All** or **All Support**. "All" will select all privileges, "All Support" will select all supported privileges. It is recommended that you select "All" (default). All privileges will be selected, but OmniVista will just ignore any unsupported privileges.

Importing Users

You can create multiple user accounts by importing an Excel or .CSV file containing multiple users. Click on the **Import** button at the top of the screen to bring up the Import File Window. If necessary, you can download a Template by clicking on the **Template** button. All of the necessary fields are provided in the Template. Complete the fields as described above. To

import a file to OmniVista, click on the **Browse** button to locate the file, then click on the **Import** button at the bottom of the window. The users defined in the file will be added to the Switch User Account List with the default privilege of "Read/Write". You can edit the privileges as described above.

Editing a User

Select a user and click on the Edit icon. Edit the fields as described above, then click on the **Apply** button. You cannot edit the Username.

Deleting a User

Select a user and click on the Delete icon, then click **OK** at the Confirmation Prompt.

Enable/Disable the UPAM Local Database for ASA

You can enable/disable switch user authentication through the local Switch User Account Database in UPAM. By default, this option is disabled, and switch user accounts are authenticated through an external authentication server. To enable ASA using the local UPAM Database, select a username(s) and click on the **Enable ASA** button. To disable it, select a username(s) and click on the **Disable ASA** button.

The following use cases are supported:

- Using the UPAM local database for both network/switch authentication and client authentication.
- Using the UPAM local database for network/switch authentication (ASA) and an external RADIUS Server for client authentication.
- Using an external RADIUS Server for both network/switch authentication (ASA) and client authentication.

The following use case is **not** supported:

- Using an external RADIUS Server for network/switch authentication (ASA) and UPAM local database for client authentication.

Enable/Disable a Switch User Account

When a Switch User Account is created, it is enabled by default. You can disable a user account by selecting the account(s) and clicking on the **Disable** icon at the top of the screen. The user(s) will no longer have access to network switches through UPAM. To enable a disabled account, select the disabled account(s) and click on the **Enable** icon at the top of the screen. The user(s) will again have access to network switches through UPAM.

Switch User Account List

- **Username -** The user's username to access a switch.
- **Description -** Optional description for the user.
- **First Name -** The user's first name (optional).
- **Last Name -** The user's last name (optional).
- **Email -** The user's contact email (optional).
- **Effective Date -** The date the user account was created.
- **Status -** The account administrative status (Enabled/Disabled).

UPAM Authenticated Switch Access Workflow

Follow the steps below to configure UPAM Authenticated Switch Access (ASA) for a user and assign UPAM ASA to network switches.

1. Create a Switch User as described above.

2. Go to the AAA Profile Screen (Unified Access - Unified Profile - Template - Global Configuration - AAA).

3. Enter the Switch User's Username in the **AAA Name** field.

4. Click on "User's Access to Switches" enable ASA and open the configuration pane.

5. In the Authentication Servers section, set the UPAM Server as the ASA Server for each type of switch access. Setting the Default Authentication to the UPAM Server configures the UPAM Server for all access types.

6. Click on the **Create** button.

7. Select the User you just created in the AAA Profile List and click on the **Apply to Devices** button. The Assign AAA Screen will appear.

8. Click on the **Add** button and select switches.

9. Click on the **Assign** button.

Note: See the AAA Profile Online Help for more information.

Authentication Record

The Authentication Record Screen displays authentication information for all devices authenticated through UPAM. The Authentication Record List provides basic information. Click on an entry for detailed information. You can also select a record(s) and click on the **Generate** button at the top of the screen to quickly generate a PSK for a device(s), create an Employee Account(s), or add a device(s) to the Company Property List.

Authentication Record List

The Authentication Record List displays basic information for all Authentication Records. Click on an entry for the detailed information described below.

Basic

- **Account Name -** Indicates the user name of the user to be authenticated
- MAC Authentication - Account name is the MAC address of the user device.
- 802.1X Authentication - Account name is the user name of the employee user.
- Captive Portal Authentication - Account name is user name of the guest user or employee user.
- **Account Type -** Group to which the requesting authentication user belongs:
- Guest
- Employee
- BYOD
- Unknown (MAC authentication without captive portal)

- **Client IPv4 -** The IPv4 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses.
- **Client IPv6 -** The IPv6 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses.
- **Device MAC -** MAC address of the user device requesting authentication.
- **Authentication Type -** Authentication type from the user requesting authentication, including: MAC authentication, 802.1x authentication and Captive Portal authentication.
- Service Type -
- **Auth Resource -** User profile database used in authentication, including None, Local Database, LDAP/AD and external RADIUS server, can refer to the authentication strategy definition.
- **Access Policy -** Name of the Access Policy for the user.
- **Authentication Strategy -** Name of the Authentication Strategy for the user.
- **Web Access Strategy -** Guest Strategy or BYOD Strategy.
- **Authentication Result -** Result for the user authentication request:
- Pass
- Fail.
- **Session Start -** The time when the user passed authentication and a connection session was created.
- **Session Stop -** The time when the connection session was terminated.
- **Redirect URL -** Redirect URL returned to NAS by UPAM when Captive Portal authentication is required.

Enforcement Policy

- **Access Role Profile -** Access Role Profile used to authenticate the device.
- **Policy List -** Policy List used to authenticate the device.
- **Final Access Role Profile -** Access Role Profile assigned by NAS and in effect on the user device, but not the Access Role Profile returned by UPAM.
- **Termination Action -** Indicates what action should be taken when the service is completed. "RADIUS-Request (1)" indicates that re-authentication should occur on expiration of the Session-Time. "Default (0)" indicates that the session should terminate.
- **Session Timeout -** Specifies the maximum number of seconds of service provided prior to session termination.
- When sent along in an Access-Accept without a Termination-Action attribute or with a Termination-Action attribute set to Default, the Session-Timeout attribute specifies the maximum number of seconds of service provided prior to session termination.
- When sent in an Access-Accept along with a Termination-Action value of RADIUS-Request, the Session-Timeout attribute specifies the maximum number of seconds

of service provided prior to re-authentication. In this case, the Session-Timeout attribute is used to load the reAuthPeriod constant within the Re-authentication Timer state machine of 802.1X. When sent with a Termination-Action value of RADIUS-Request, a Session-Timeout value of zero indicates the desire to perform another authentication (possibly of a different type) immediately after the first authentication has successfully completed.

- When sent in an Access-Challenge, this attribute represents the maximum number of seconds that an IEEE 802.1X Authenticator should wait for an EAP-Response before retransmitting. In this case, the Session-Timeout attribute is used to load the suppTimeout constant within the backend state machine of IEEE 802.1X
- **Acct Interim Interval -** The number of seconds between each interim update, in seconds, for this specific session.
- **Upstream Bandwidth -** Device upstream bandwidth, in kbit/s.
- **Downstream Bandwidth -** Device downstream bandwidth, in kbit/s.

Authenticate

- **Authentication Method -** The method used to authenticate the device (e.g., PAP, EAP-MD5, EAP-PEAP, EAP-TLS).
- **Access Device MAC -** MAC address of the NAS to which the user device is attached.
- **Access Device Name -** System name of the NAS to which the user device is attached.
- **Access Device SSID -** Wireless service broadcast by the NAS and connected by user device (only valid for wireless access).
- **Access Device Location -** Location of the NAS.
- **Called Station ID -** Allows the NAS to send the phone number the user called, using Dialed Number Identification (DNIS) or similar technology inside the Access-Request packet:
- For Switch - Switch MAC Address.
- For AP - radio_MAC_address:SSID_NAME.
- **Access AP Group -** AP Group through which the user accesses the network
- **NAS Port Type -** The type of physical port type of the NAS authenticating the user:
- Wireless-IEEE 802.11
- Ethernet.
- **NAS Port -** The physical port number of the NAS authenticating the user.
- For Switch - if index
- For AP - Wireless radio index
- **NAS Port ID -** The NAS authenticating the user (The attribute can be configured in Unified Access - Unified Profile – Template - AAA Server Profile):
- For Switch - chassis/slot/port
- For AP - WLAN service.
- **NAS ID** – NAS Identifier, identify the NAS originating the Access-Request. (The attribute can be configured in Unified Access - Unified Profile – Template - AAA Server Profile.)

- **NAS IP Address -** The identifying IP Address of the NAS.
- **Slot Port -** Port number on the switch slot to which the device is connected (only for wired access).
- **Port Desc/Wlan Service**
- For Switch - Port description
- For AP - WLAN service
- **Framed MTU -** The Maximum Transmission Unit to be configured for the user when it is not negotiated by some other means (e.g., PPP). It is a fixed value = 1400.
- **Reject Reason -** Reason for rejecting the authentication request from user device:
- Overdue license
- Invalid username or password
- Cannot match access policy according to the authentication request.
- **Roaming Information -** Client roaming historical information (indicates the client roamed a path from AP to AP).

COA

CoA-Request packets contain information for dynamically changing session authorizations. This is typically used to change Access Role Profile or Policy List for the user.

- **COA Status -** The NAS responds to a CoA-Request sent by UPAM with a CoA-ACK if the NAS can successfully change the authorizations for the user session, or a CoA-NAK if the request is unsuccessful.
- **COA Error Cause -** It is possible that the NAS cannot honor Disconnect-Request or CoA-Request messages for some reason. The COA Error Cause Attribute provides more detail on the cause of the problem. It may be included within Disconnect-ACK, Disconnect-NAK and CoA-NAK messages.

Accounting

- **Acct Status Type -** Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop). Values: Start (1), Stop (2), Interim-Update (3), Accounting-On (7) Accounting-Off (8).
- **Acct Session Time -** Indicates how many seconds the user has received service, and can only be present in Accounting-Request records where the Acct Status Type is set to "Stop".
- **Acct Session ID -** Unique Accounting ID that makes it easy to match start and stop records in a log file. The start and stop records for a given session MUST have the same Acct Session ID.
- **Acct Input Packets -** Indicates how many packets have been received from the port over the course of this service being provided to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop".
- **Acct Output Packets -** Indicates how many packets have been sent to the port in the course of delivering this service to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop"..
- **Acct Input Octets -** Indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop".

- **Acct Output Octets -** Indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop".
- **Acct Input Gigawords -** Indicates how many gigawords have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop".
- **Acct Output Gigawords -** Indicates how many gigawords have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to "Stop".
- **Acct Terminate Cause -** The reason the connection session was terminated.
- **Acct Multi Session ID -** This attribute is a unique Accounting ID to make it easy to link together multiple related sessions in a log file.

Using the Generate Button

You can quickly generate a PSK for a device(s), create an Employee Account(s), or add a device(s) to the Company Property List. Select a record(s) in the Authentication Record List and select an option as described below.

- **PSK -** Select the record(s) in the Authentication Record List. Click on the **Generate** button, click on **PSK**, then then click **Save** at the Confirmation Prompt. The device(s) associated with the record(s) will be added to the Company Property List as Device Specific PSK Devices. The PSK Passphrase for the device(s) is automatically generated by OmniVista based on the device MAC Address and Session Time. The PSK Passphrase can be obtained and printed from the Company Property Screen. You can generate a PSK for any Authentication Record. See the Company Property online help for more information.
- **Employee Account -** Select the record(s) in the Authentication Record List and click on the **Generate** button. Click on **Employee Account**, then then click **Save** at the Confirmation Prompt. OmniVista will create an Employee Account(s) for the selected Authentication Record(s). See the Employee Account online help for more information. The following conditions must be met to generate an Employee Account for an Authentication Record. If these conditions are not met, the **Employee Account** option will be grayed out.
- Authentication Result = Fail
- Auth Resource = Local Database
- Service Type = 802.1X or Voice (User Account Authentication)
- **Company Property -** Select the record(s) in the Authentication Record List and click on the **Generate** button. Click on **Company Property**, then then click **Save** at the Confirmation Prompt. The device(s) associated with the selected record(s) will be added to the Company Property List. See the Company Property online help for more information. The following conditions must be met to generate an Company Property entry for an Authentication Record. If these conditions are not met, the **Company Property** option will be grayed out.
- Authentication Result = Fail
- Auth Resource = Local Database
- Service Type = Call Check (MAC Authentication)

Captive Portal Access Record

The Authentication Captive Portal Access Record Screen displays captive portal information for all devices authenticated through UPAM. The Captive Portal Access Record List provides basic information. Click on an entry for detailed information, as shown below.

- **Device MAC -** MAC address of the user device requesting captive portal authentication.
- **Account -** User name of the device requesting authentication.
- **Auth Result -** Result for the user authentication request:
- Access - Accept
- Access - Reject
- Empty Value - Captive portal authentication is not activated.
- **Device Family -** Production vendor of the user device.
- **Browser Type -** The browser on the device that used to login the network by user.
- **Access Time -** The time the device sent the access request.
- **Device OS -** Operating system of the user device.
- **Device Category -** Category of the user device.
- **Association SSID -** Wireless network to which the user device is associated.
- **Reject Reason -** The the reason UPAM reject the access request.
- **Portal Type -** The Captive Portal usage (BYOD/Guest).
- **Portal Page -** The Captive Portal template name.
- **Success Redirect -** The redirect URL to which the browser goes after successful Captive Portal authentication.
- **User Agent -** The browser and device used to access the network.

Note: Custom attributes will show if you configured Custom Attributes in Guest Access Strategy.

Switch Access Record

The Switch Access Record screen displays information about user authentication access to network switches through UPAM.

Switch Access Record List

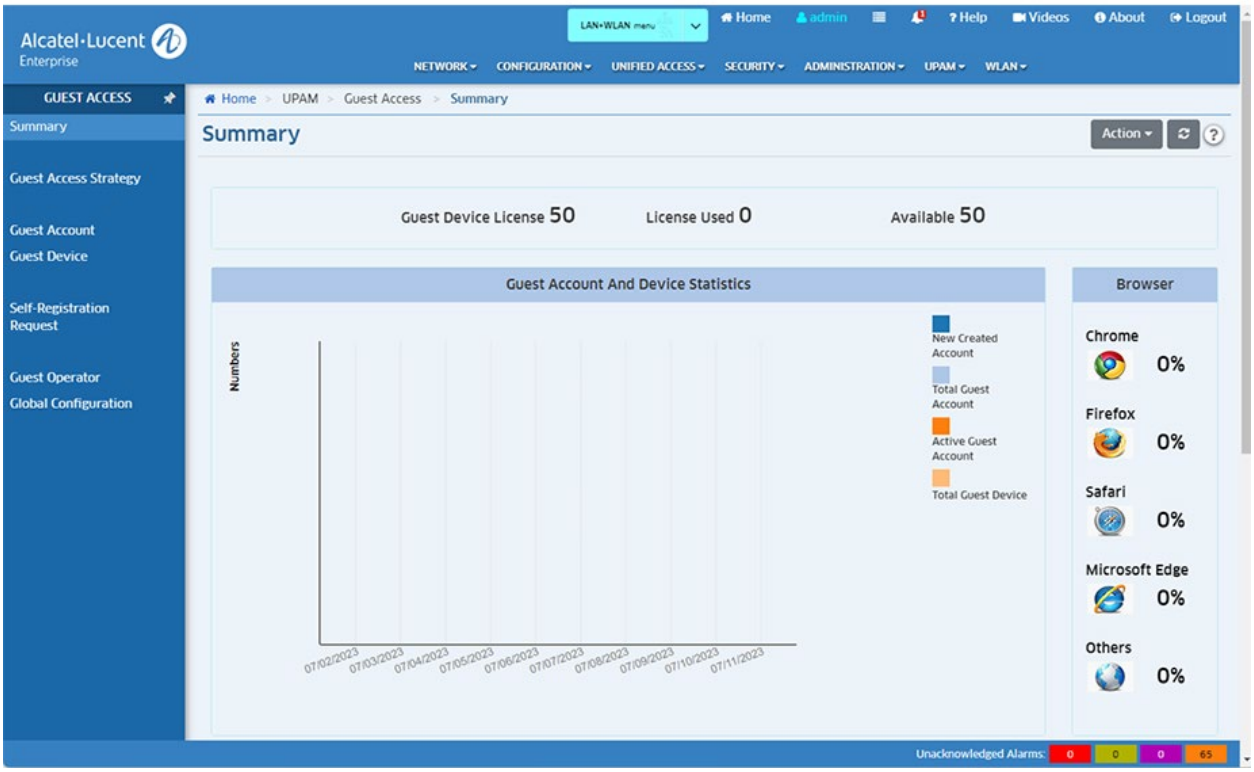
- **Account Name -** The Switch User Account name.
- **Alcatel Client IP Address -** The IP address of the client that accessed the AOS switch through SSH/FTP/HTTP.
- **Service Type -** The Service Type attribute in the Radius Access-Request message (Default = Framed User)
- **Authentication Result -** Whether the user passed or failed authentication (Pass/Fail).
- **Reject Reason -** The reason the user failed authentication, if applicable (e.g., Invalid Username or Password).

- **Session Start -** The time when the user passed authentication and a connection session was created.
- **Session Stop -** The time when the user session on the switch ended.
- **ASA AOS Version -** The AOS switch type (AOS6/AOS8).
- **Authentication Method -** The method used to authenticate the user (e.g., PAP).
- **NAS Port Type -** The physical port type of the NAS authenticating the user (e.g., Wired).
- **NAS Port -** The port number of the NAS authenticating the user.
- **NAS Port ID -** The client NAS-Port attribute for authentication and accounting sessions.
- **NAS IP Address -** The IP address of the NAS.
- **Alcatel Port Description -** The configured port description/alias.
- **Account Status Type -** The account status for the entry (Start/Stop)
- **Account Session Time -** The number of seconds the user received service. This is only displayed in Accounting-Request records where the Acct Status Type is set to "Stop".
- **Account Session ID -** A Unique Accounting ID that makes it easy to match start and stop records in a log file. The start and stop records for a given session must have the same Acct Session ID.
- **Slot/Port -** The port number on the switch slot to which the device is connected.

Guest Access

The UPAM Guest Access application is used to manage guest users accessing the network. Guest Access service is based on the captive portal authentication.

UPAM Guest Access



The following screens are used to monitor and configure the Guest Access application:

- **Summary -** Provides an overview of Guest Access on the network.
- **Guest Access Strategy -** Used to configure access attributes for guest users.
- **Guest Account -** The Guest Account Screen used to configure Guest Accounts. If self-registration is not enabled, you can manually create a login account for a guest user and relay the information to the guest user.
- **Guest Device -** Displays all authenticated online devices as well as all devices that were previously on the network and are stored in UPAM.
- **Self-Registration Request -** Used to review, approve or reject self-registration requests from Guest Users.
- **Guest Operator -** Used to configure a Guest Operator. A Guest Operator is a network operator who manages the guest user network access.
- **Global Configuration** - Used to set global configurations for Guest Access Strategy and Guest Accounts.

Summary

The Guest Access Summary Screen provides an overview of Guest Access on the network. The screen provides the following information:

- **Guest License Information**
    - **Guest Device License -** Total number of Guest Licenses available.
    - **License Used -** Total number of Guest Licenses used.
    - **Available -** Currently available Guest Licenses.
- **Guest Account And Device Statistics**
    - **New Created Account -** Guest Accounts created on that day.
    - **Total Guest Account -** Total number of Guest Accounts.
    - **Active Guest Account** - The Guest Accounts that have been activated by a guest device by logging into the network.
    - **Total Guest Device** - The total number of Guest Devices registered in UPAM.
- **Browser -** Guest Device browser usage as a percentage of total Guest browser usage.
- **Remembered Guest Device Category -** Displays information by device category (e.g., Computer, Mobile, Table) in a pie chart format.
- **Guest Account Creation Mode -** Displays the method used to create the Guest Account (e.g., created by administrator, or guest self-registration) in a pie chart format.

Guest Access Strategy

The Guest Access Strategy Screen displays information about configured Guest Access Strategies and is used to configure access attributes for guest users. The screen can be used to create, edit, and delete Guest Access Strategies. There is a pre-configured Default Guest Access Strategy that you can edit, or you can create new Guest Access Strategies (up to a maximum of 32).

Creating a Guest Access Strategy

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

General

Configure redirect and authentication attributes.

- **Strategy Name -** The Guest Access Strategy Name.
- **Redirect Strategy -** The captive portal page template used for guest user login.
- **Mode -** The http protocol used to redirect the captive portal page (https/http).
- **IP/FQDN -** The displayed URL format for redirection to the captive portal page (FQDN/IP).
- **Current FQDN -** The FQDN used for the captive portal page redirection.
- **Authentication Resource -** The guest user profile database, which is the local UPAM database (Local Database). Guest user accounts can be added on the UPAM - Guest Access - Guest Account Screen.

Login Strategy

Configure guest user login.

- **Login By -** Specify the login method:
  - **Username & Password -** Guest user login by their credential (Username and Password).
  - **Terms & Condition -** Guest user login by accepting the Terms and Conditions. When this login method is selected, additional Registration Strategy information is required.
  - **Access Code -** Guest user login by a unified access code.
  - **Simple Persona** - Guest user login by email address. When this login method is selected, additional Registration Strategy information is required.
- **Reset Password -** If enabled, this option allows a guest user to change their login password without Administrator operation. Select one of the options from the drop-down to allow the guest to receive a Verification Code through e-mail, SMS, or both. The user will be able to click on the "Forget Password?" link on the login screen for their account to request a Verification Code to change their password.
- **Social Media Account -** Guest user login by social media account (Facebook, Google, Rainbow, WeChat). Complete the fields below for social media login. Note that you must also configure the Social Login Settings in an Access Role Profile for the applicable Social Media account (Facebook, Google, Rainbow, WeChat).
  - **Portal Server Domain -** Social Media website domain. Domains must be entered in Fully Qualified Domain Name (FQDN) format (e.g., www.upam.com). Note that you must configure your local DNS Server to resolve this Hostname to the correct UPAM IP address.
  - **Facebook OAuth Client ID -** The OAuth Client ID provided by Facebook (see Configuring the Facebook API for more information).
  - **Google Plus OAuth Client ID -** The OAuth Client ID provided by Google (see Configuring the Google API for more information).
  - **Rainbow OAuth Client ID -** The OAuth Client ID provided by Rainbow (see Configuring the Rainbow API for more information).
  - **WeChat Open APP ID -** The WeChat APP ID provided by the WeChat Official Accounts Platform (see Configuring the WeChat API for more information).
    - **APP Secret -** The APP secret key for the wireless service provider.
- **Success Redirect URL -** Specify the redirect URL for the browser after the guest user passes captive portal authentication:
  - **None -** No redirect URL. Remain on the “Success” login page configured by the Administrator.
  - **Go to Initial URL -** Redirect to the guest-user-input URL after passing authentication
  - **Go to Fixed URL -** Redirect to a fixed web page specified by the Administrator.
- **Custom Attributes -** Allow the Administrator to customize the attributes for guest self-registration to collect the guest user information. The Administrator can configure up to 20 attributes (max length 32 characters each). The configured attributes will be displayed in the self-registration page where the guest user can input 1 - 255 character(s) for each attribute. To make this option visible for configuration, the login method must be specified in the Terms & Conditions.

Note: If you are configuring Custom Attributes, then the Administrator can get all user information in the Captive Portal Access Record.

Note: If you are configuring **Social Media Login** you **must** configure and obtain Google and Facebook tokens using the Google and Facebook Developer APIs as detailed below.

Registration Strategy

The following Registration Strategy fields are required when "Terms & Condition" or "Simple Persona" is selected as the user login method. This section is not displayed for the other login methods (Username & Password, Access Code).

- **Remeber Device** - Specify whether to remember the device MAC address and make it valid after successful authentication (Enabled/Disabled). If the remembered device is valid, the MAC address check will be performed first and the device allowed access without re-authentication.
- **Period Unit** - The unit used for the Account Validity Period Attribute (Days, Hours, Minutes).
- **Device Validity Period** - The length of time that the user device is valid. This value is entered based on the selected Period Unit. For example, if Days is selected, enter the number of days the user device is valid; if Hours is selected, enter the number of hours, etc. By default, Days = 30, Hours = 24, and Minutes = 60.

Post Portal Authentication Enforcement

Configure post-authentication enforcement for guest users.

- **Fixed Access Role Profile -** The Access Role Profile assigned to the guest user after passing authentication (required for AOS Switches).
- **Fixed Policy List -** The Policy List assigned to the guest user after passing authentication.
- **Data Quota Status -** Specify whether to control guest access based on user data quota (Enabled/Disabled). If enabled, the Data Quota limit is applied only to a user who logs in with username and password credentials. It will not be applied to a user who logs in with an access code or a user who just accepts the terms and conditions.
- **Quota Exhausted URL -** The redirect URL to which the accessing device will be guided after the user reaches their data quota limitation.
- **Other Attributes -** Select an attribute from the drop-down, enter a value and click on the Add icon to add the attribute. Repeat the process to add additional attributes.
    - **Session Timeout -** The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device’s default session timeout policy will take effect. (Range = 12000 - 86400, Default = 43200)
    - **Accounting Interim Interval -** Interval for RADIUS accounting, in seconds. If not configured, the device’s default accounting policy will take effect. (Range = 60 - 1200, Default = 600)
    - **WISPr Bandwidth Max Up -** The user upstream bandwidth, in kbit/s. By default, it is not limited.

- **WISPr Bandwidth Max Down -** The user downstream bandwidth, in kbit/s. By default, it is not limited.

Self-Registration Strategy

Configure the self-registration attributes for guest user login when the guest user is required to perform self-registration and approval before accessing the network. In this case, the guest user account is automatically created and send to the guest user through e-mail by UPAM. The self-registration strategy is only applicable for login by Username and Password.

- **Self-Registration -** Enables/Disables the self-registration function.
- **Account Name Created By -** The field from which the guest user account is retrieved, the information is entered by the guest user in the self-registration login page:
  - **Guest Name -** Login account for the guest user
  - **Email Address –** Email address of the guest user
  - **Phone Number -** Phone number of the guest user.
- **Password Creation -** Password creation method:
  - **Manually -** Password for guest user account is set by guest user in the self-registration web page.
  - **Automatically -** Password for guest user account is automatically generated by UPAM and sent to guest user through E-mail.
- **Success Account Notification -** If enabled, the user must specify an e-mail address as part of the Self-Registration Strategy, and the login details are sent to the user.
- **Approval -** Specify whether the guest registration request is required to be approved by a sponsor in the company or a guest operator. The employee sponsor could be an Administrator or employee the guest going to visit.
  - **Disabled -** Approval by an employee or guest operator in not required.
  - **Approved by Employee Sponsor -** Approval by the employee specified in the Self-Registration Request Screen is required.
    - **Email Suffix Restriction -** Enter the employee sponsor e-mail suffix(es) and click on the Add icon. This is the e-mail suffix used by the company employee, which will be combined with a specific employee e- mail ID to form a full e-mail address. The registration request will be sent to this e-mail address.
    - **Full Email -** Enter the full employee e-mail address.
  - **Approved by Guest Operator -** Approval by a guest operator specified on the Guest Operator Screen is required.
    - **Location-Based Notification -** Enables/Disables location-based notification. When enabled, send the guest request to guest operators for the specific location. When disabled, send the guest request to all operators.
- **Required Attributions -** Customize the information fields that the guest user is required to input during self-registration. Certain fields are required and pr-configured for employee sponsor or guest operator approval.
- **Guest Name -** Login account for the guest user.

  - **Password -** Login password for the guest user. If the password creation method is set to “Automatically”, the guest user does not have to enter this field.
  - **Full Name -** Full name of the guest user.
  - **Email ID-** Email address of the guest user.
  - **Phone Number -** Phone number of the guest user.
  - **Company -** Name of the company the guest user is representing.
  - **Position -** Position of the guest user in their company.
  - **Department –** Department of the guest user in their company.
  - **Country or Region -** Country or region of the guest user’s company.
  - **Employee Visited -** The employee being visited by the guest user.
  - **Employee Email ID -** Email address of the employee being visited.
  - **Employee Phone Number -** Phone number of the employee being visited.
  - **Reason Visited -** The purpose of the guest user’s visit.
- **Custom Attributes -** Allow the Administrator to customize the attributes for guest self-registration to collect the guest user information. The Administrator can configure up to 20 attributes (max length 32 characters each). The configured attributes will be displayed in the self-registration page where the guest user can input 1 - 255 character(s) for each attribute.
- **Authorize By Verification Code -** If the e-mail or phone number is required, Enables/Disables whether to send a verification code to specified address to ensure the e-mail or phone number is correct.
- **Password Visibility -** Enables/Disables whether to display account information such as name and password on the Registration Result Page.
- **Service Level -** When Service Level is set to "None", settings of Registration Strategy in Global Configuration will take effect for guest self registration.

Note: If you are configuring Custom Attributes, then the Administrator can get all user information in the Guest Account, Self-Registration Request, or via a guest operator email.

Service Level (Optional)

Configure the different service levels for the guest account by binding various levels of Access Roles and Policies. The guest user can select an appropriate service level when logging into the network. Enable and configure applicable Service Levels as described in the Service Level section of Global Configuration.

WiFi4EU

WiFi4EU provides free access to public Wi-Fi in parks, schools, public buildings, and health centers throughout Europe.

- **WiFi4EU -** Enables/Disables WiFi4EU. To use the WiFi4EU feature, the “RedirectStrategy“ must use the specified WiFi4EU template for the Captive Portal page. In addition, the validity period for Captive Portal authentication must be no more than 24

hours per the WiFi4EU requirement. This value can be changed in Registraton Strategy from the Global Configuration screen.
- **Network Identifier -** The Network Identifier received from the WiFi4EU portal as part of Installation report.
- **Self-Test Modus -** The WiFi4EU portal self-test mode.

Editing a Guest Access Strategy

Select a strategy in the Guest Access Strategy List and click on the Edit icon. Edit any fields as described above and click on the **Apply** button. Note that you cannot edit the Strategy Name.

Deleting a Guest Access Strategy

Select a strategy(ies) in the Guest Access Strategy List and click on the Delete icon. Click **OK** at the Confirmation Prompt. You cannot delete the Default Guest Access Strategy.

Guest Access Strategy List

- **Strategy Name -** The Guest Access Strategy name.
- **Redirect Strategy -** The captive portal page template used for guest user login.
- **Mode -** The http protocol used to redirect the captive portal page (https/http).
- **IP/FDQN -** The displayed URL format for redirection to the captive portal page (FQDN/IP).
- **Authentication Resource -** The guest user profile database, which is the local UPAM database (Local Database).
- **Login By -** User login method (e.g., Username & Password, Social Media Account).
- **Social Media Account -** Indicates whether Social Media login is enabled/disabled.
- **Portal Server Domain -** The Social Media website domain.
- **Facebook OAuth Client ID -** The OAuth Client ID provided by Facebook.
- **Facebook Authorized Origins** - The Facebook Authorized Origins URL that is copied into the Valid OAuth redirect URLs field when configuring the Facebook API.
- **Google OAuth Client ID -** The OAuth Client ID provided by Google.
- **Google Authorized Origins** - The Google Authorized Origins URL that is copied into the Authorized redirect URLs field when configuring the Google API.
- **Success Redirect URL -** The redirect URL for the browser after the guest user passes captive portal authentication.
- **Fixed URL -** The redirect URL to a fixed web page specified by the Administrator, if applicable.
- **Fixed Access Role Profile -** The Access Role Profile assigned to the guest user after passing authentication.
- **Fixed Policy List -** The Policy List assigned to the guest user after passing authentication.
- **Session Timeout Interval -** The maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device’s default session timeout policy will take effect.

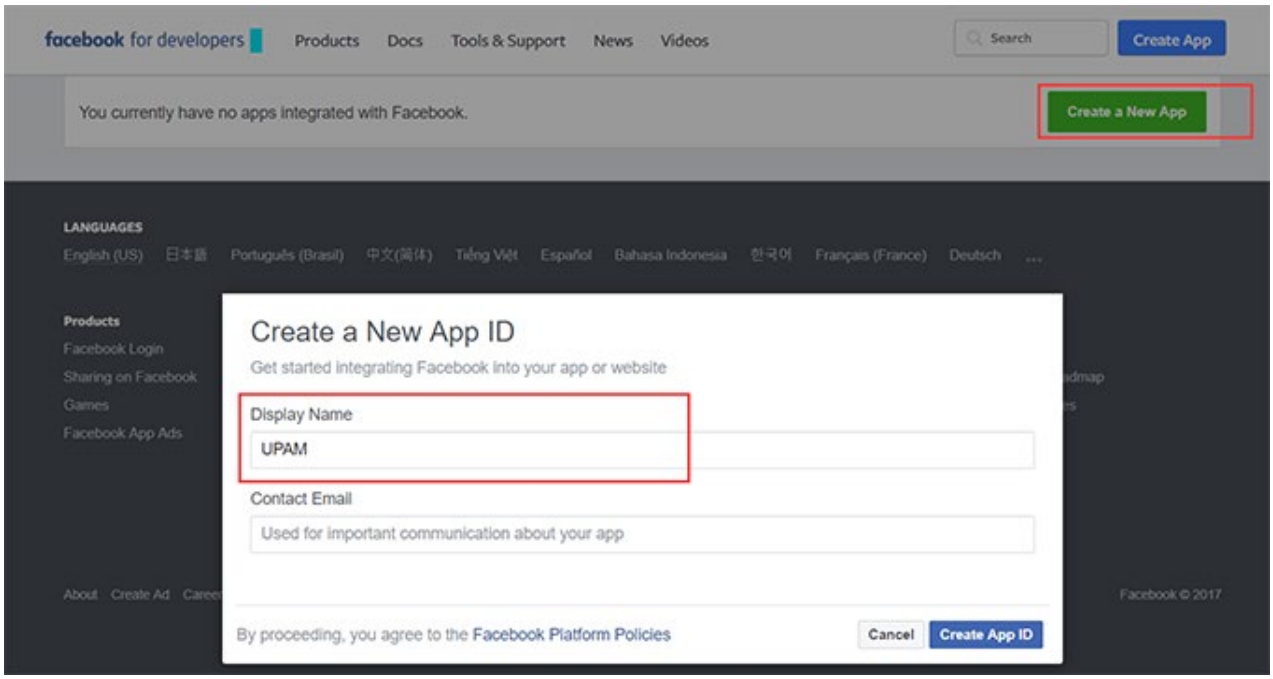
- **Accounting Interim Interval -** Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 - 1200, Default = 600)
- **Upstream Bandwidth -** The user upstream bandwidth, in kbit/s. By default, it is not limited.
- **Downstream Bandwidth -** The user downstream bandwidth, in kbit/s. By default, it is not limited.
- **Self-Registration -** The administrative state of guest user self registration (Enabled/Disabled).
- **Use Name Created By -** Method used to create an account name for the guest user in the self-registration workflow.
- **Password Creation -** Whether the password for the Guest User Account is set by the user "Manually" on the self-registration page or "Automatically" generated by UPAM and sent to the user via e-mail.
- **Approval -** The administrative state of the approval requirement for a guest registration request (Enabled/Disabled).
- **Full Email Address -** The full employee e-mail address if approval is required.
- **Required Attributes -** Information the guest user is required to input during self-registration.
- **Password Visibility -** The administrative status of password visibility on the Registration Result page (Enabled/Disabled).
- **Location-Based Notification -** Administrative status of Location-Based Notification (Enabled/Disabled).
- **Remeber Device** -Indicates whether the online device was remembered by UPAM and added into the Remembered Devices List.
- **Data Quota Status -** The administrative state of the data quota limitation (Enabled/Disabled).
- **Quota Exhausted URL -** The redirect URL to which the accessing device will be guided after the user reaches their data quota limit, if applicable.
- **Service Level -** The service level defined in the self-registration strategy. If the service level in Global Configuration is disabled or the service level assigned to the strategy is disabled, the service level content in table and detail will be marked in red color “Disabled”.
- **Reset Password -** The User Reset Password administrative status (Enabled/Disabled). If enabled, the user can reset their Guest Account password without Administrative action.

Configuring Facebook, Google, Rainbow, and WeChat Developer APIs for Social Login

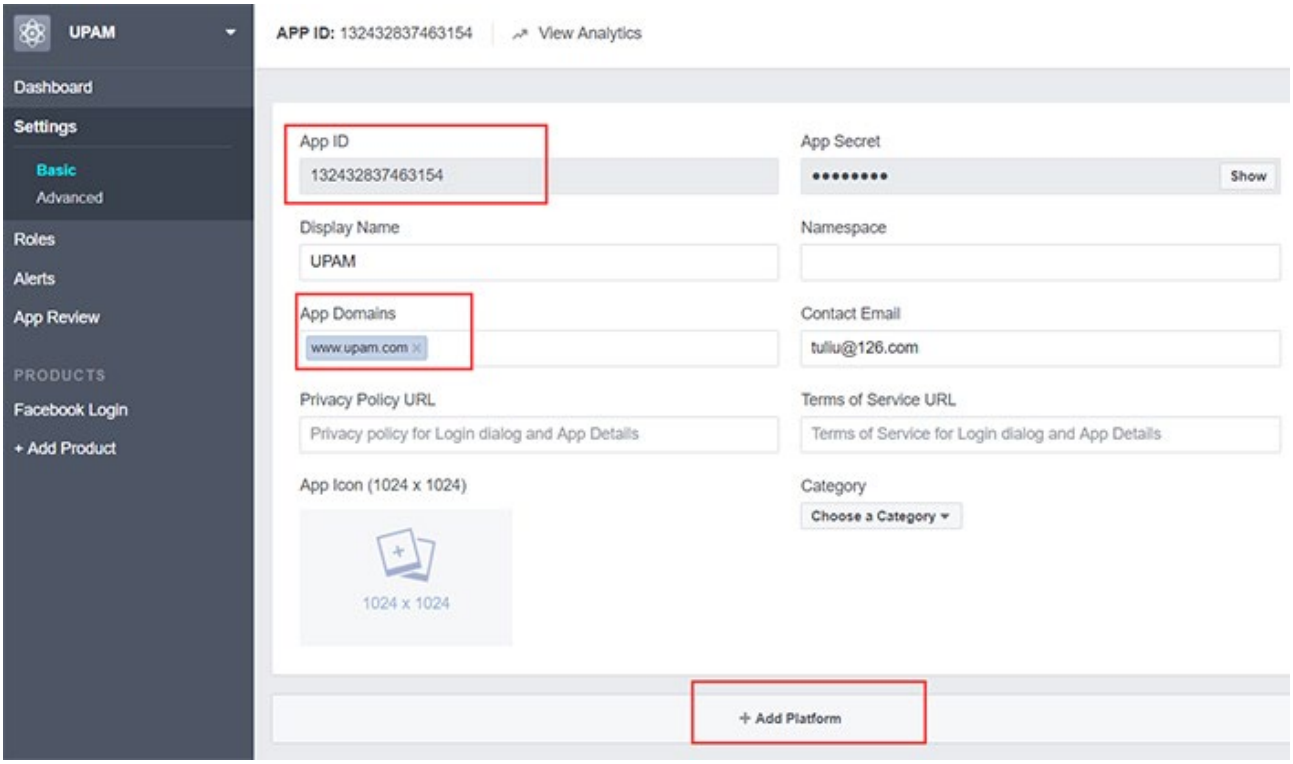
The sections below provide detailed instructions for configuring the Facebook, Google, Rainbow, and WeChat APIs and obtaining the necessary tokens for Social Login.

Configuring the Facebook API

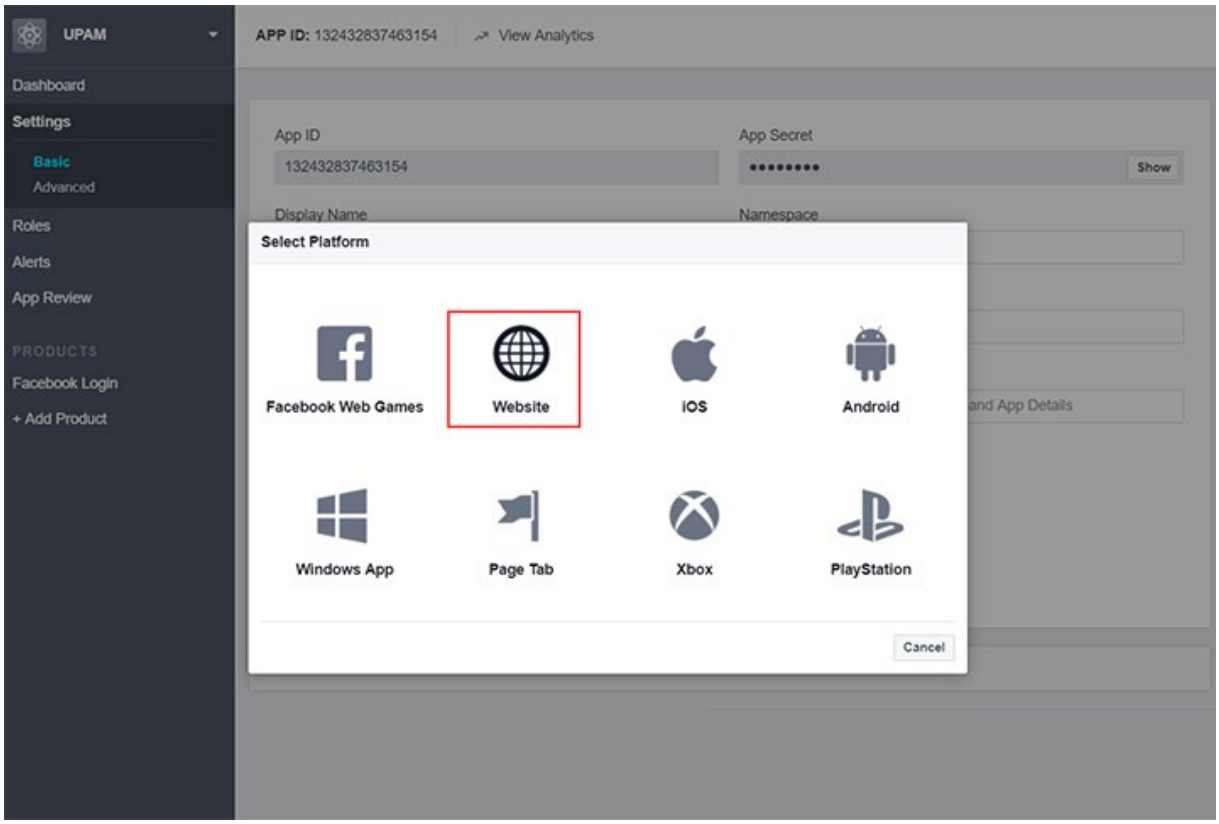
1. Go to https://developers.facebook.com/apps. Click on the **Create New App** button to bring up the Create a New App ID window. Enter the **Display Name** (e.g., UPAM) and your **Contact Email** and click on the **Create App ID** button.



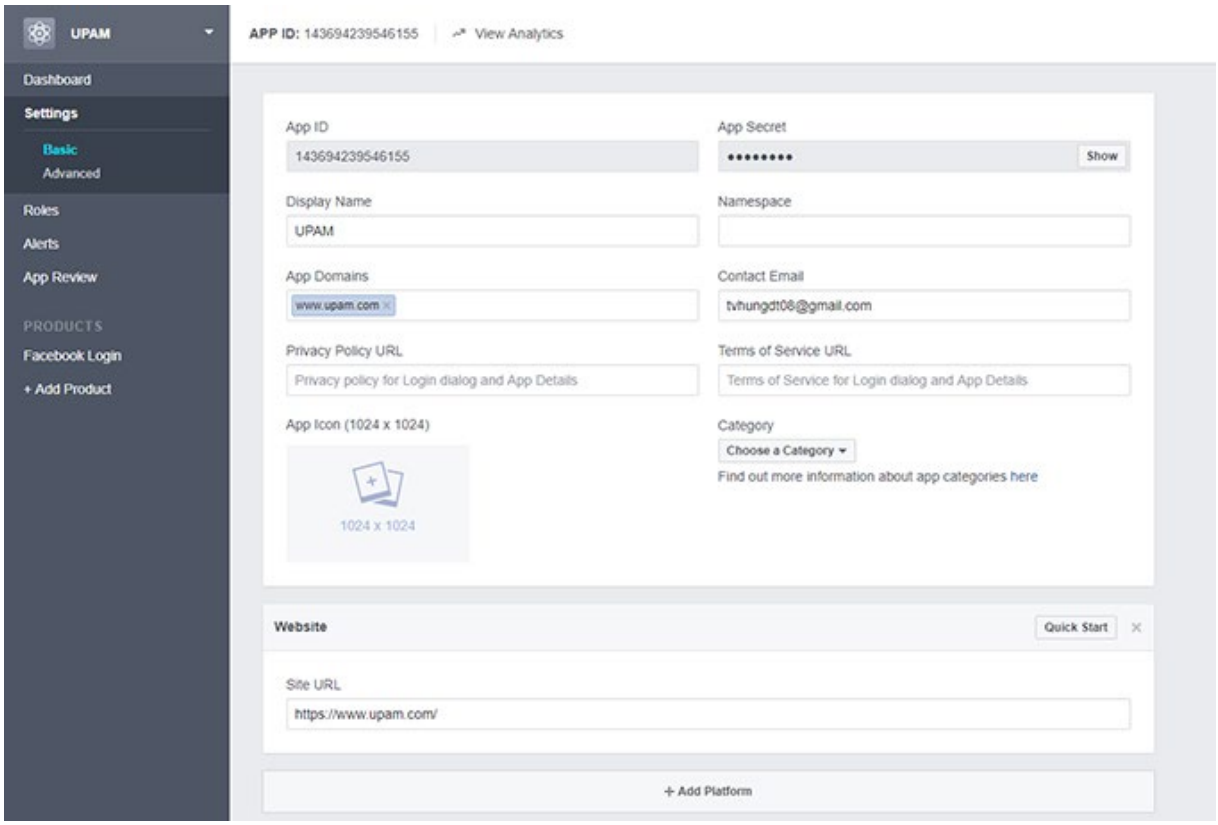
2. Click on **Settings - Basic** in the Navigation Tree on the left side of the screen to display the basic App settings.



3. Click on the **+ Add Platform** button at the bottom of the screen to bring up the Select Platform Screen.



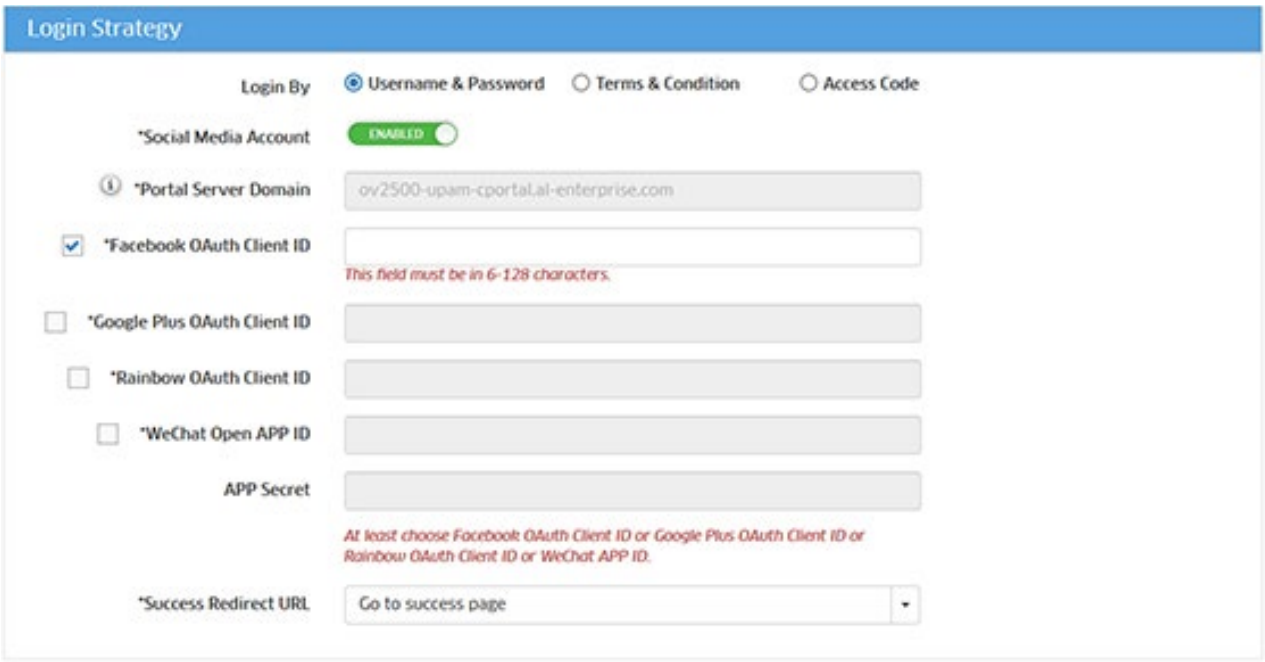
4. Click on **Website**.



5. Complete the App Domain and Site URL Fields as follows, then click on the **Save Changes** button.

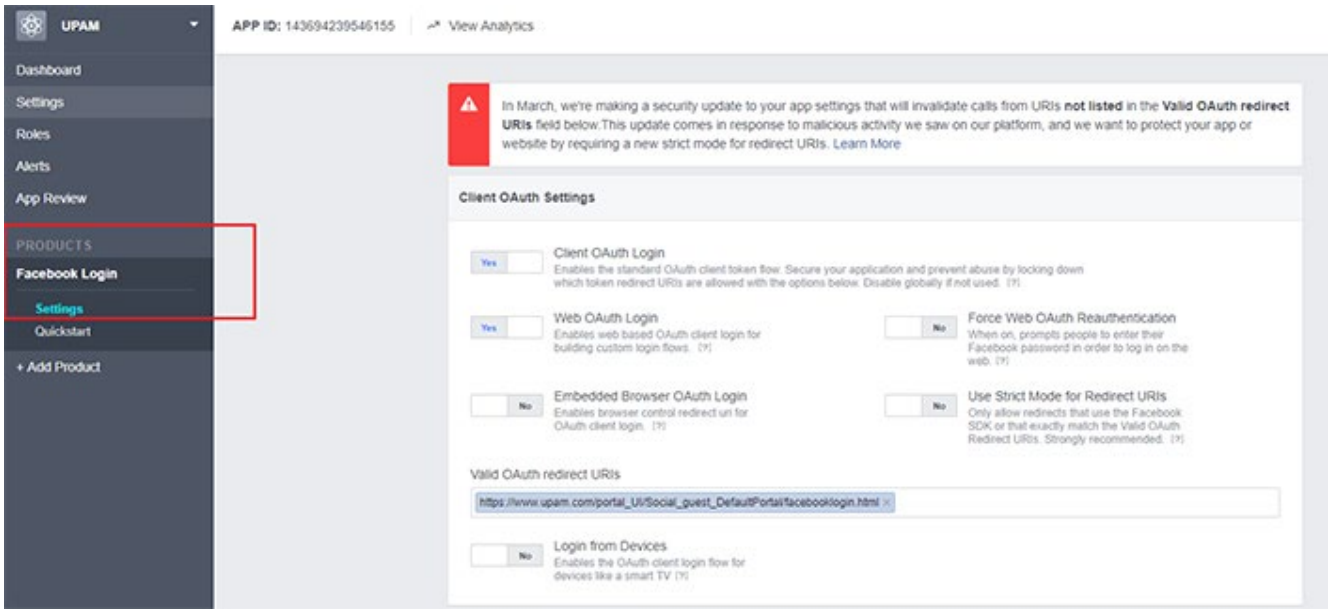
- **App Domains -** Enter the Portal Server Domain you entered in your Guest Access Strategy (e.g., www.upam.com)
- **In Site URL:** Enter the full web URL (e.g., https://www/upam.com/)

6. Go to the Guest Access Strategy Screen in OmniVista (UPAM - Guest Access - Guest Access Strategy).



7. In the **Facebook OAuth Client ID** field, enter the App ID you received from Facebook.

8. Return to the Facebook API Configuration Screen and click on Facebook Login - Settings in the Navigation Tree on the left side of the screen.



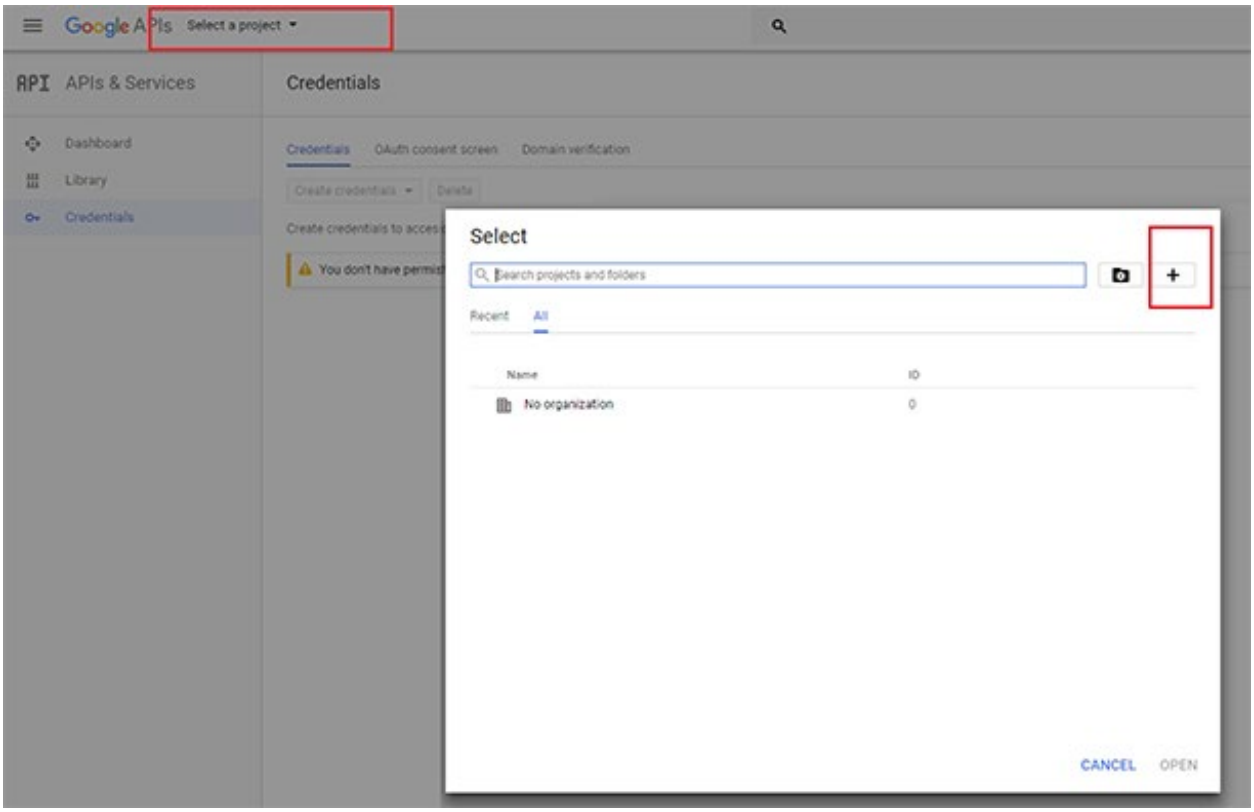
9. Paste the Facebook Authorized Origins information as directed into the **Valid OAuth redirect URLs** Field.

10. Save all changes.

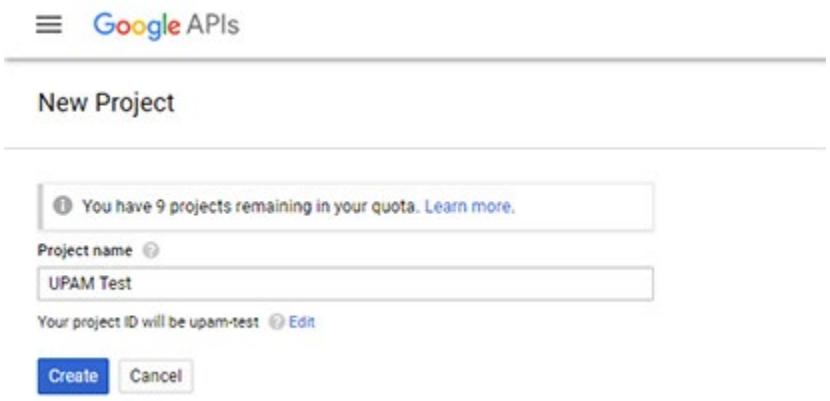
You can now use Facebook for UPAM Authentication.

Configuring the Google API

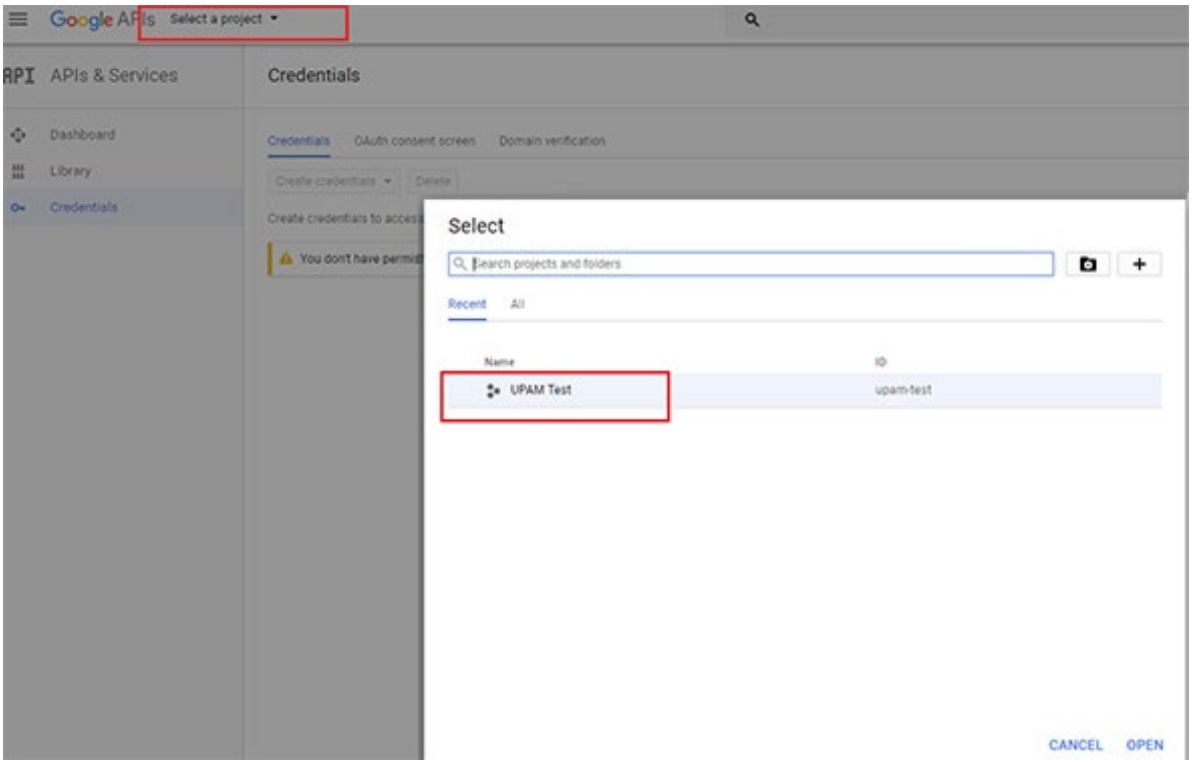
1. Go to https://console.developers.google.com/apis/credentials?project=mimetic-surf-155906. Click on the **Select a project** drop-down at the top of the screen, then click on the Add icon on the Select window.



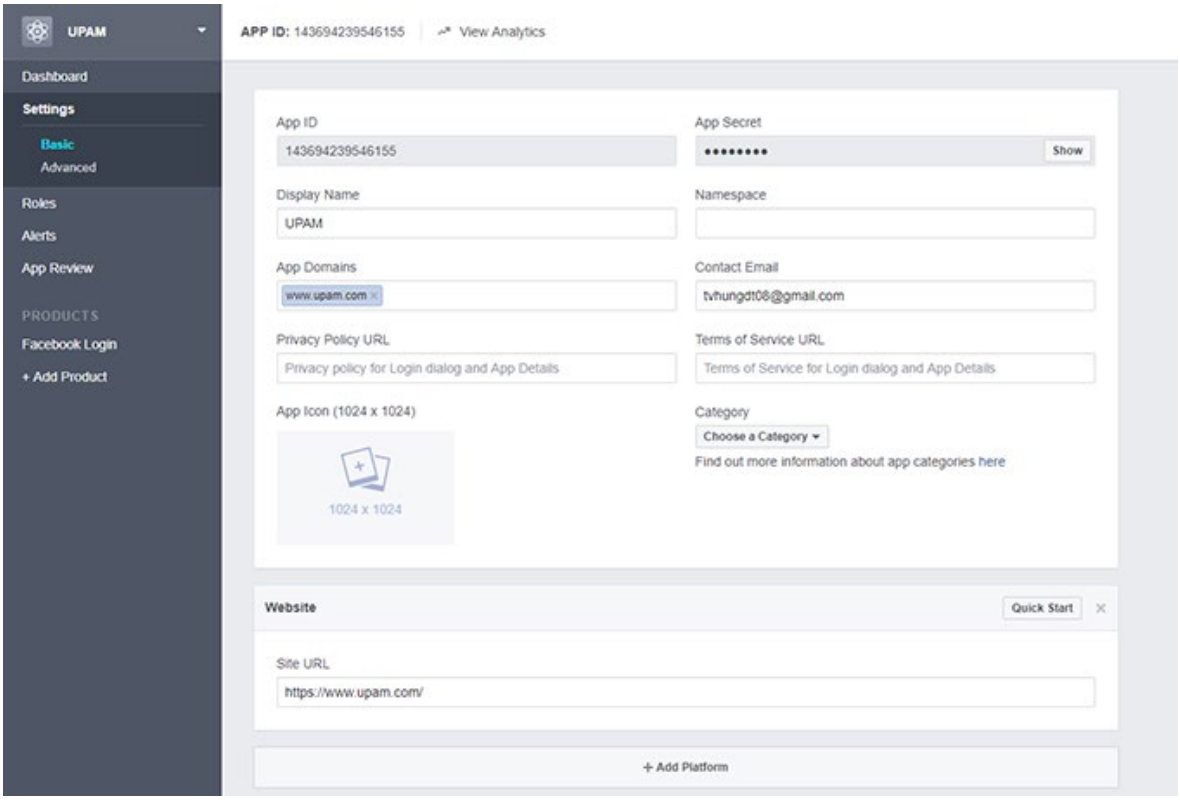
2. On the New Project Screen, enter the name of your project (e.g., UPAM Test) and click **Create**.



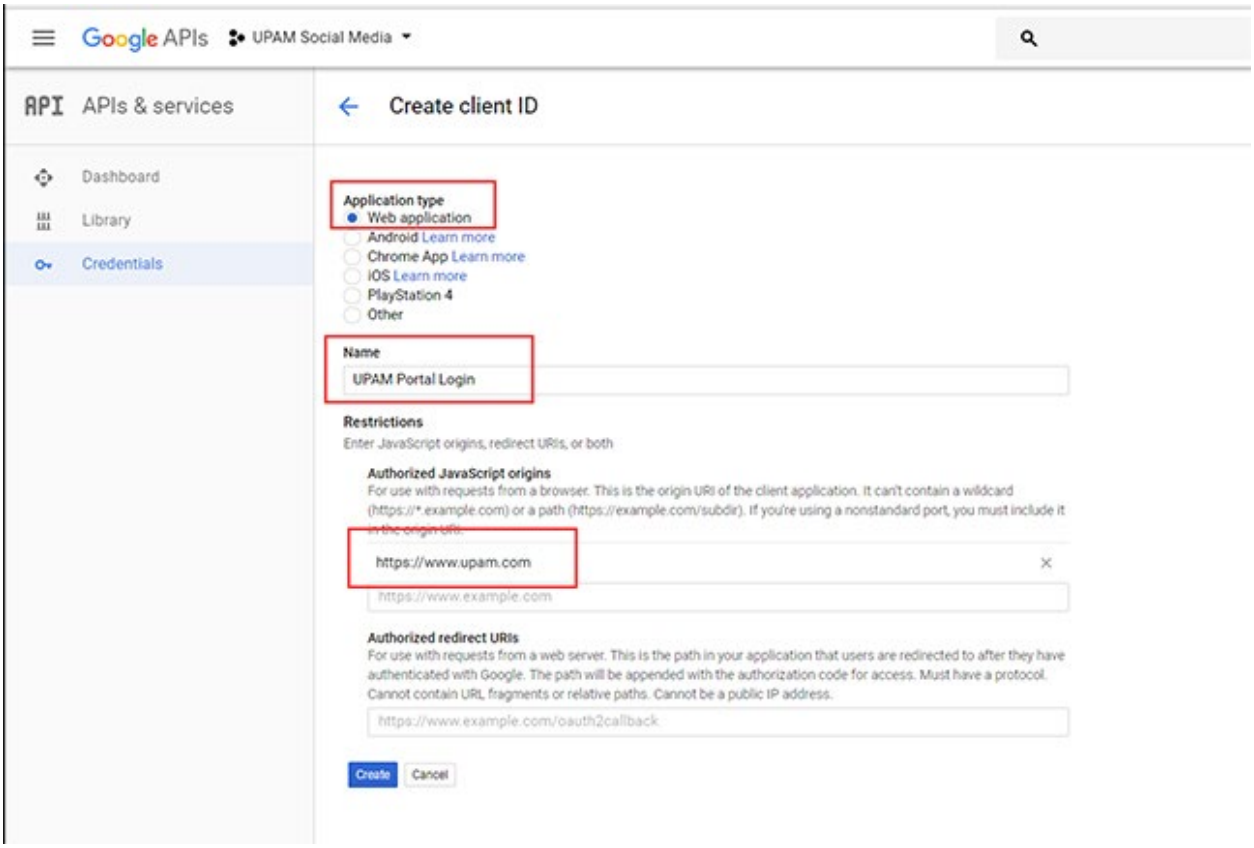
3. Click on the **Select a project** drop-down at the top of the screen, then click on the project you just created (e.g., UPAM Test).



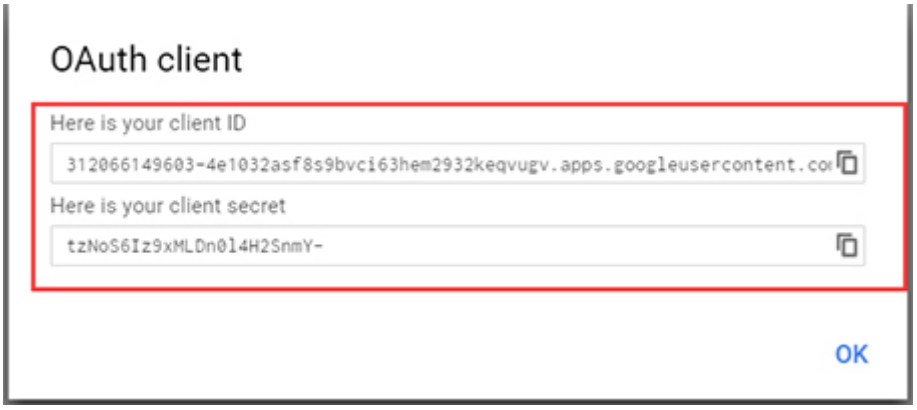
4. Click on **Create credentials** and select **OAuth client ID**, as shown as below.



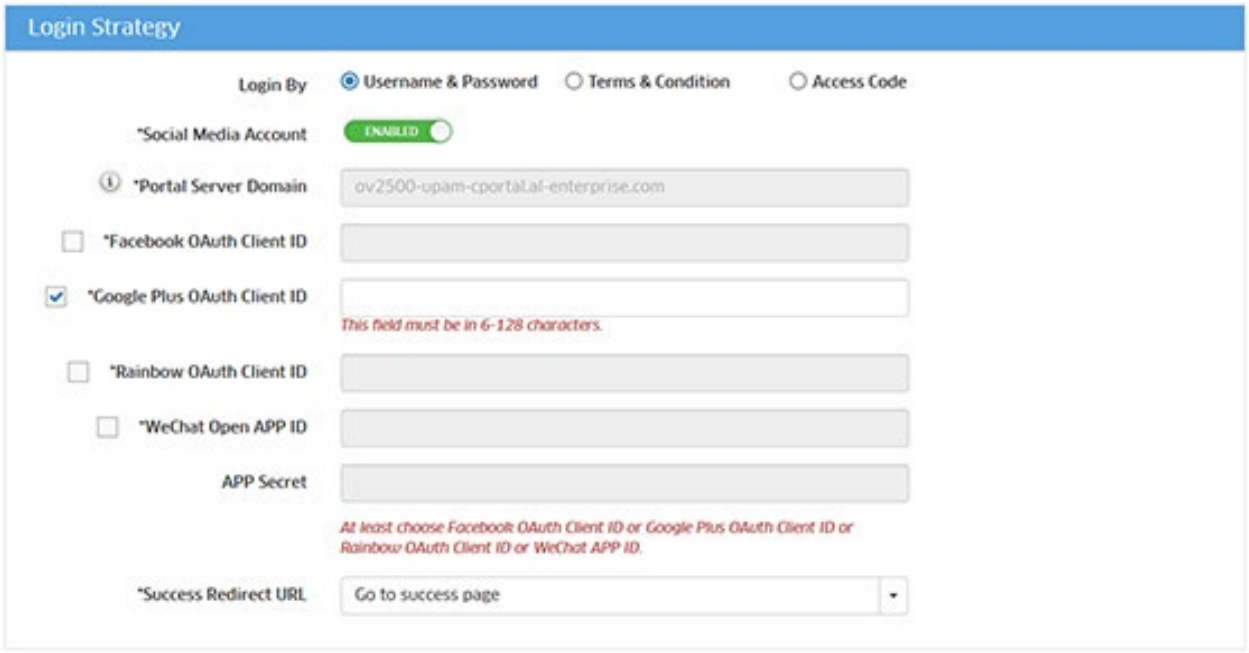
5. On the Create Client ID Screen, select “Web Application”. Enter the Project Name and Authorized JavaScript origins. (Defined in the local DNS, directed to the UPAM Portal IP, it is the Portal Server Domain name in the Guest Access Strategy.) Click **Create**.



The Client ID and Client Secret are displayed.

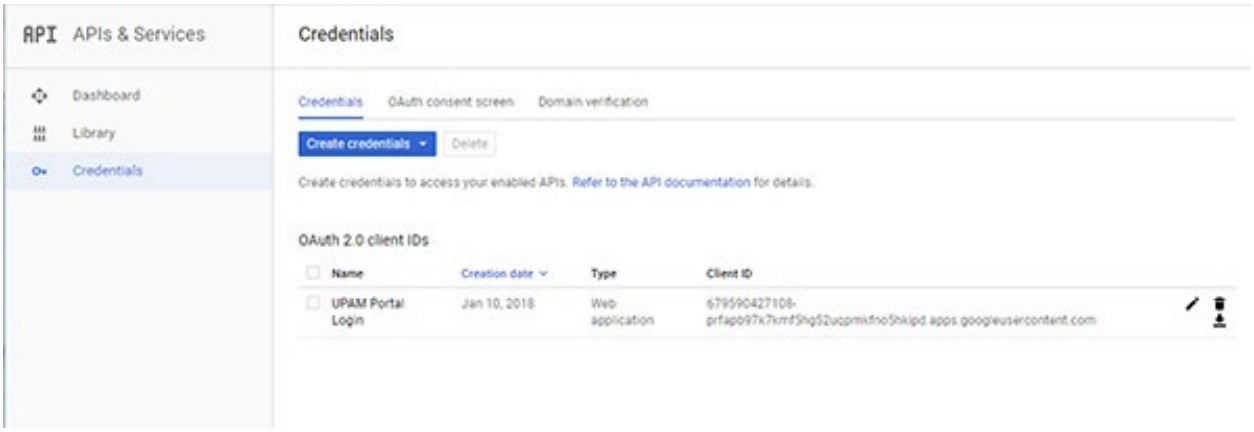


6. Go to the Guest Access Strategy Screen in OmniVista (UPAM - Guest Access - Guest Access Strategy)

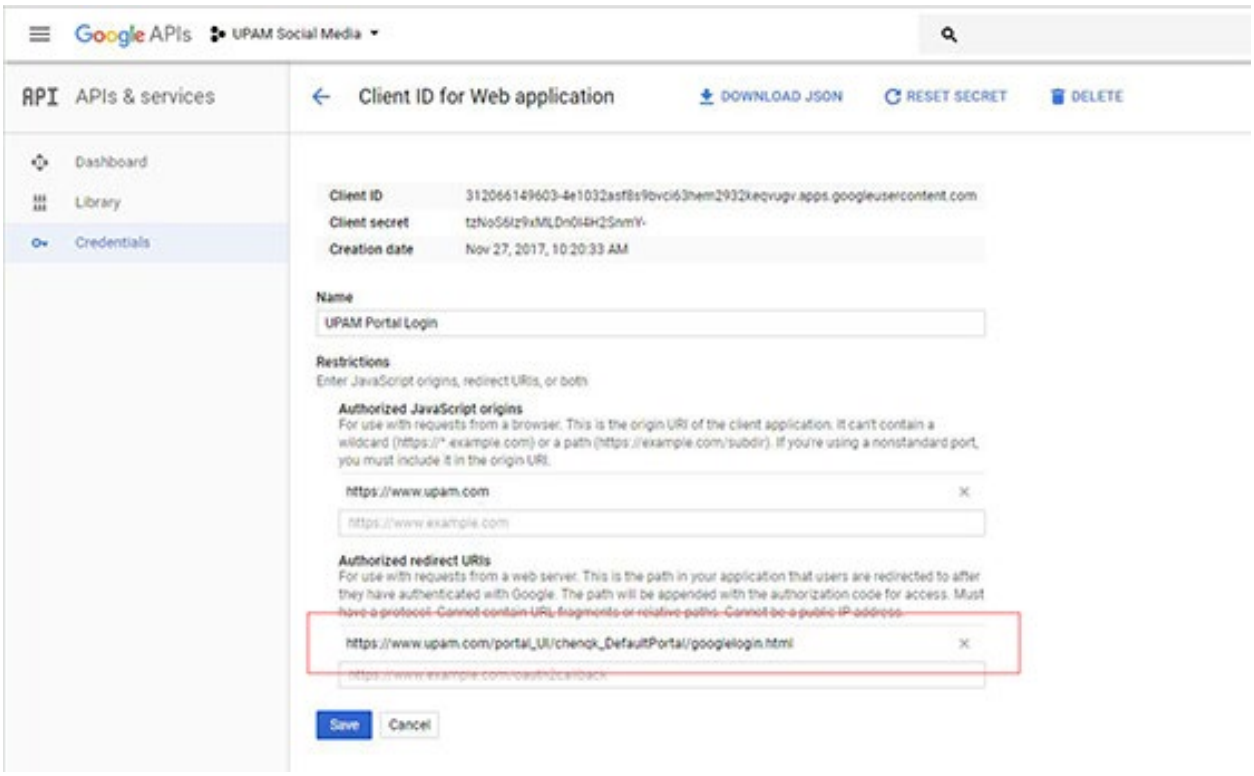


7. In the **Google Plus OAuth Client ID** field, enter the Client ID you received from Google.

8. Return to the Google API Configuration Screen.

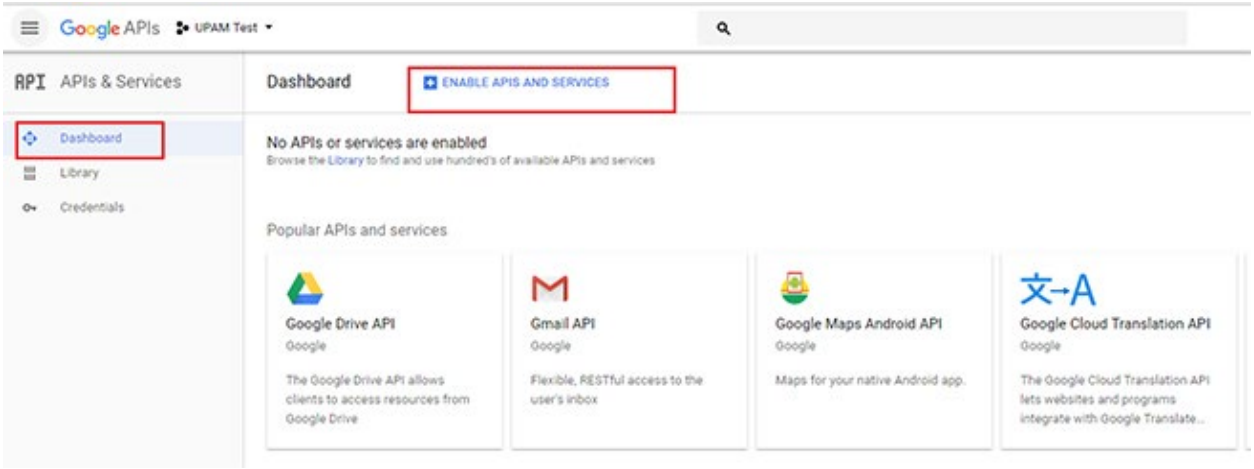


9. Click on the Edit icon next to the OAuth 2.0 client ID you just created.

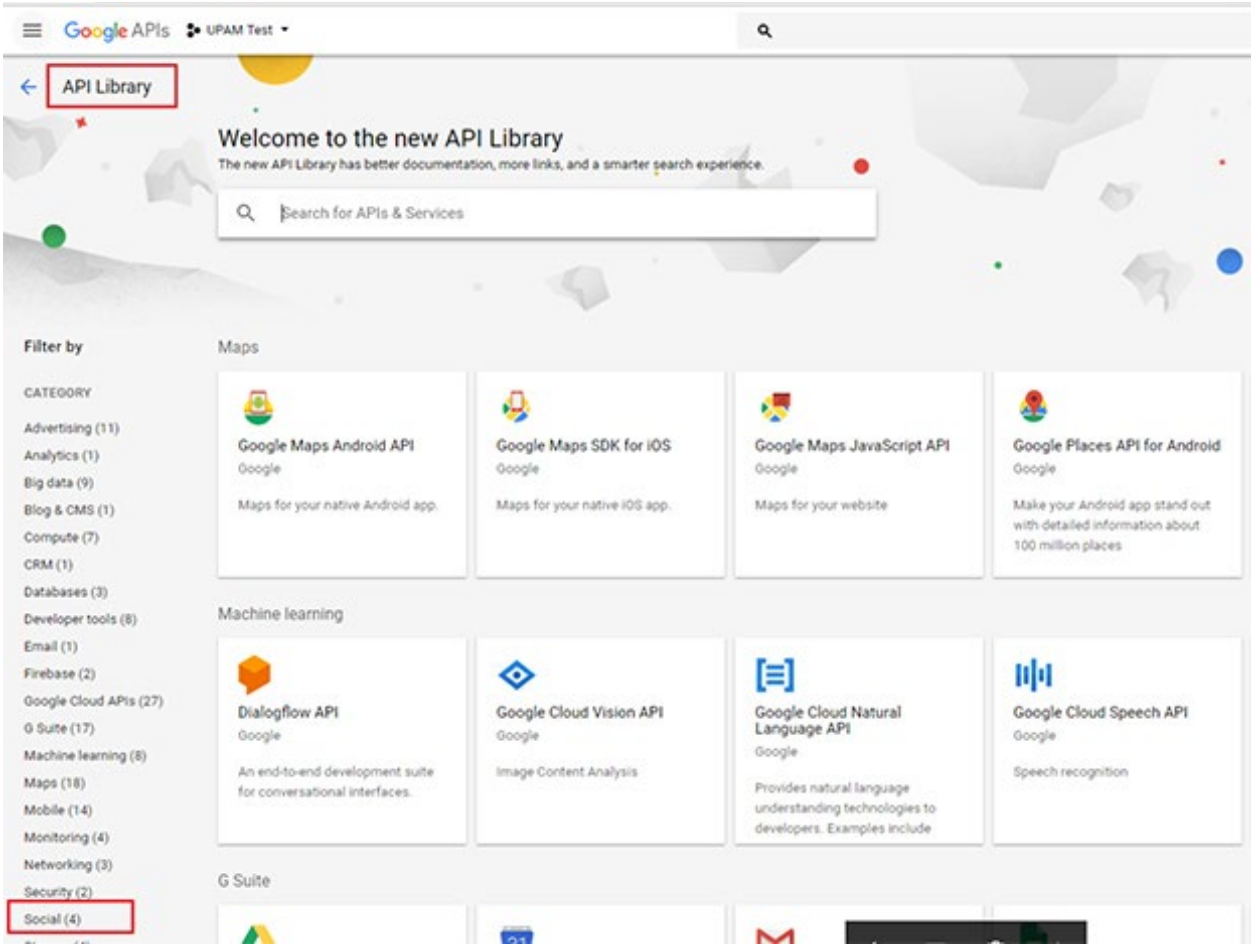


10. Paste the Google Authorized Origins information as directed into the **Authorized redirect URLs** Field and click **Save**.

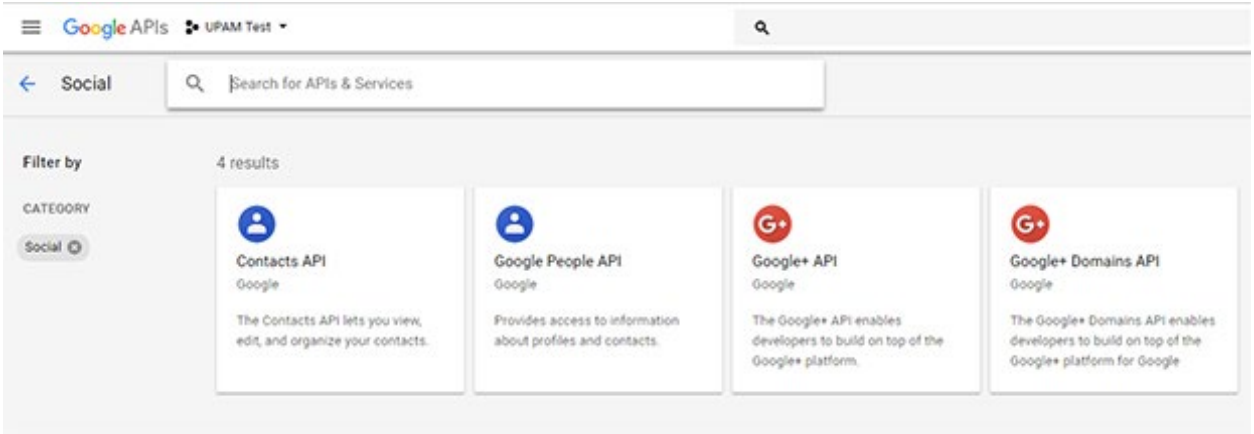
11. Enable Google + API service on Google API developer to receive requests from OV during UPAM authentication. Click on **Dashboard** in the Navigation Tree, then click on **Enable APIs and Services**.



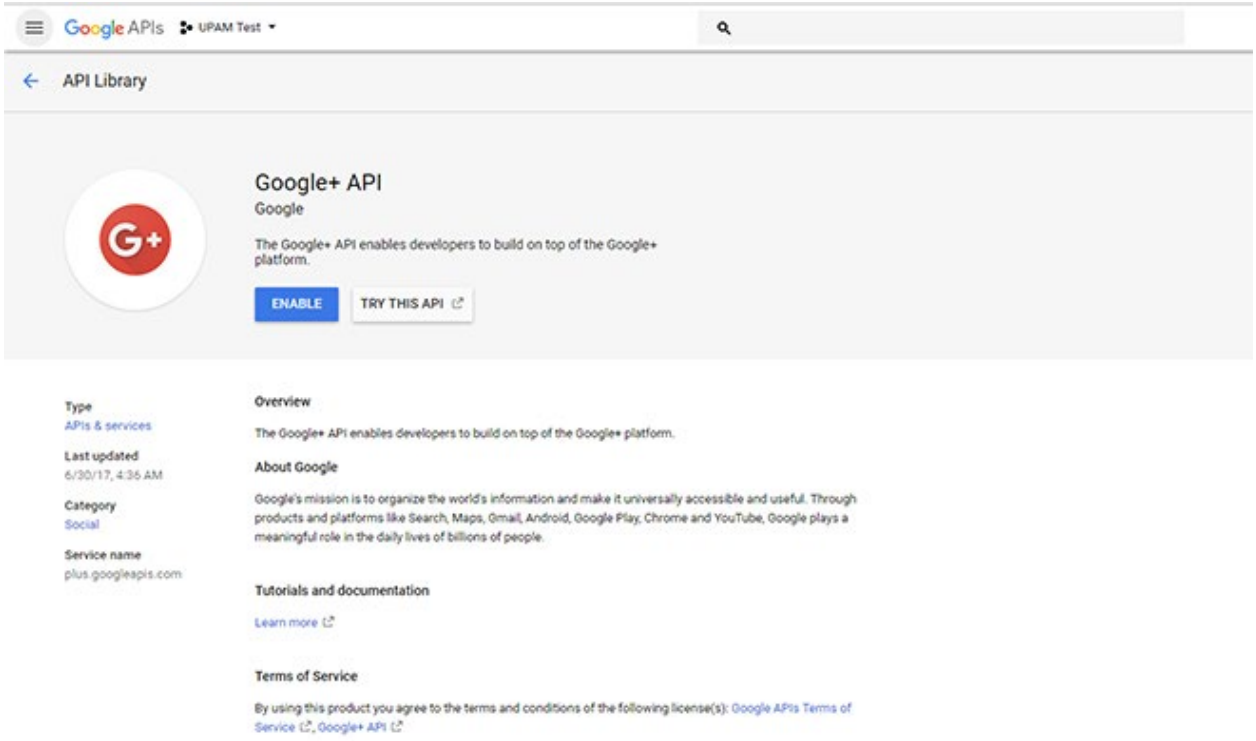
12. Select **Social** in the "Filter by" List on the right side of the screen.



13. Select **Google+ API**.



14. Click **Enable**.



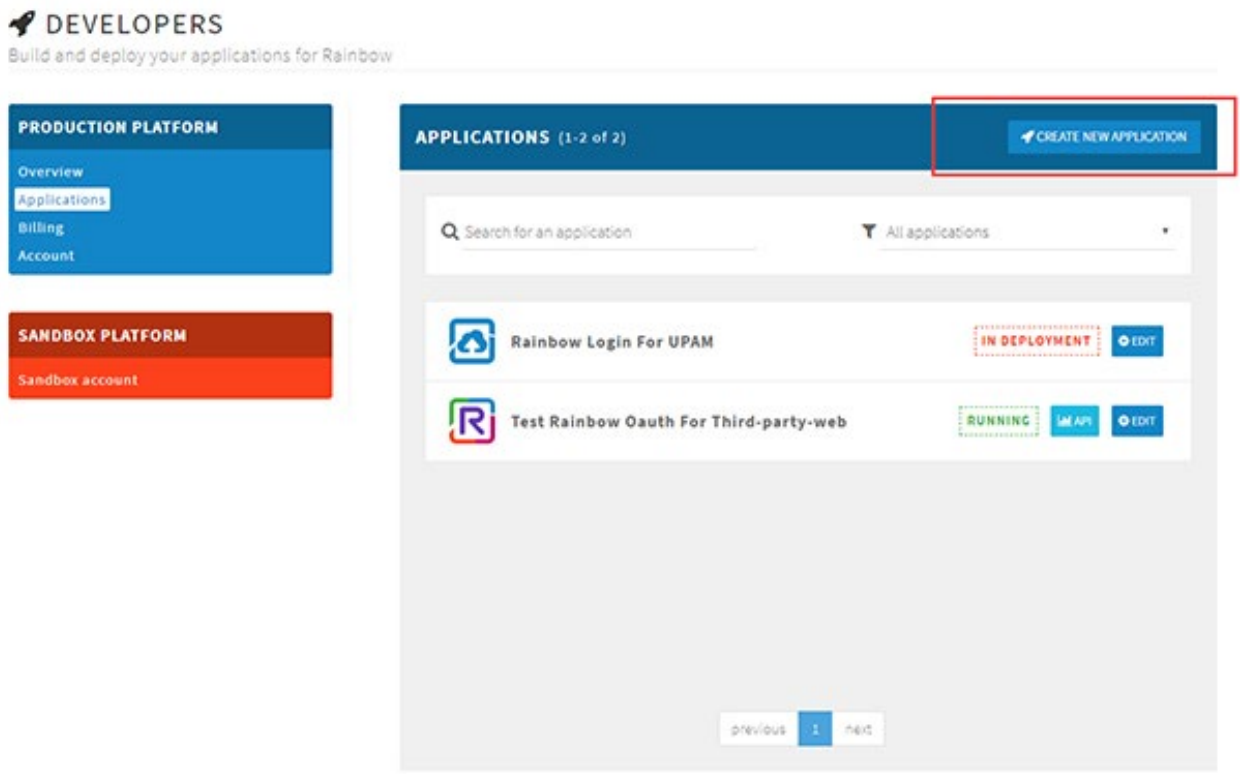
You can now use Google for UPAM Authentication.

Configuring the Rainbow API

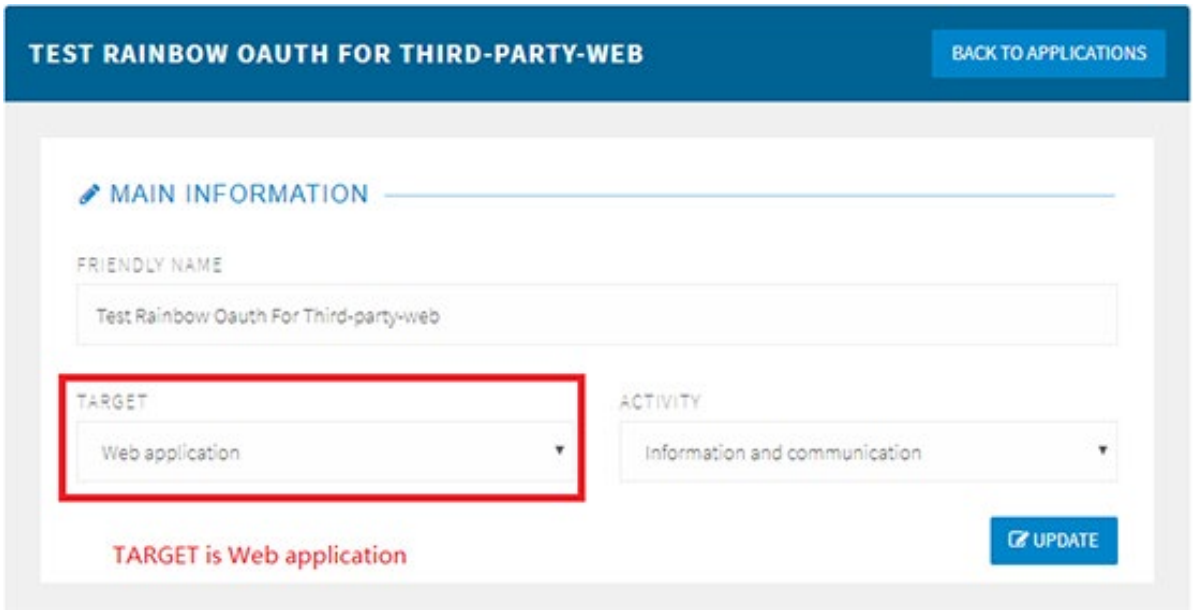
1. Set https://www.openrainbow.com and https://web.openrainbow.com in the Whitelist in OmniVista.

2. If you do not have a Rainbow account, go to https://hub.openrainbow.com/#/dashboard/overview and create one.

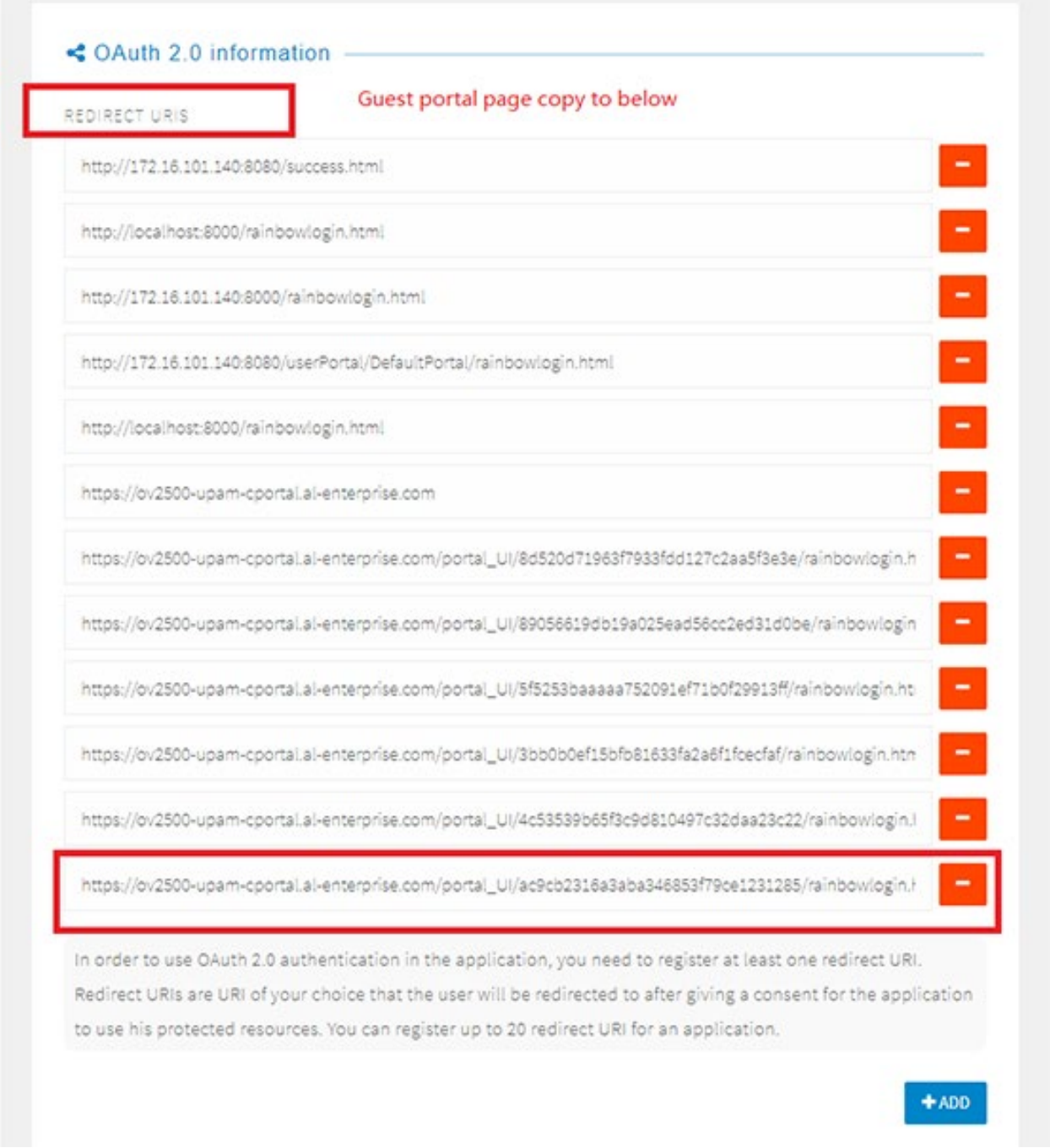
3. After creating an account, go to the Developers Applications page and click on the **Create New Application** button.



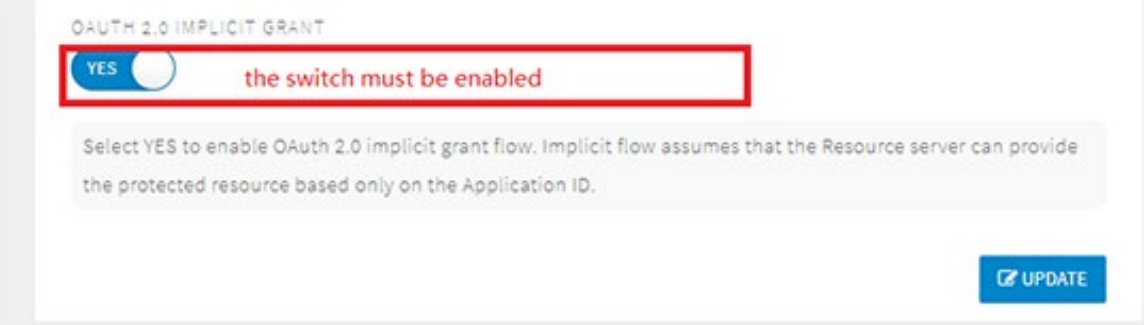
4. In the **Main Information** section go to the **Target** drop-down and select **Web application**.



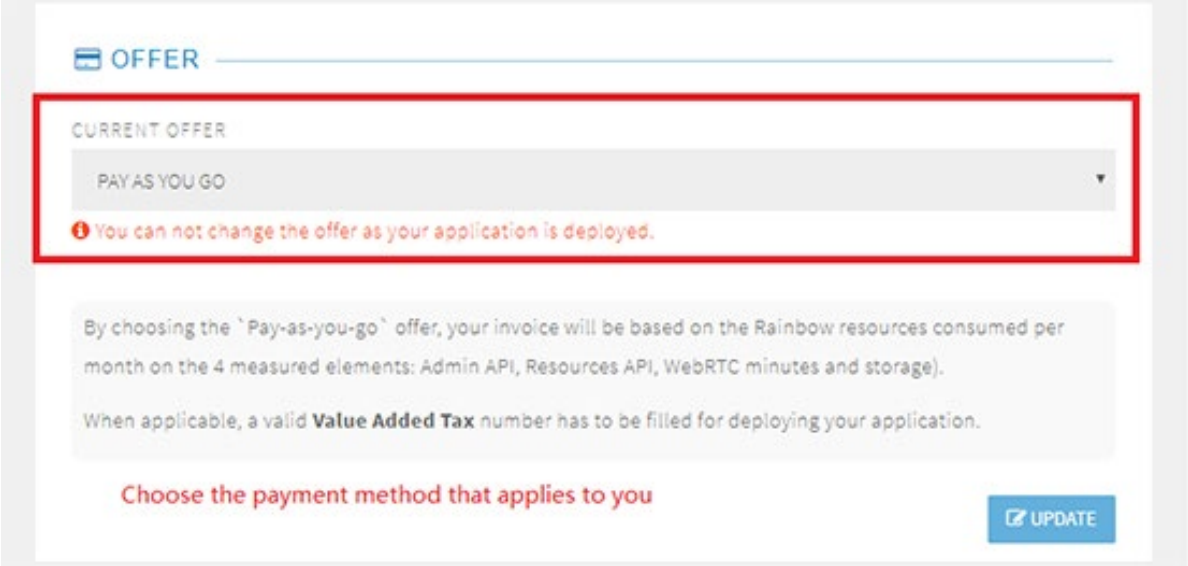
5. In the **OAOTH 2.0 Information** section, add the Guest Portal page URL.



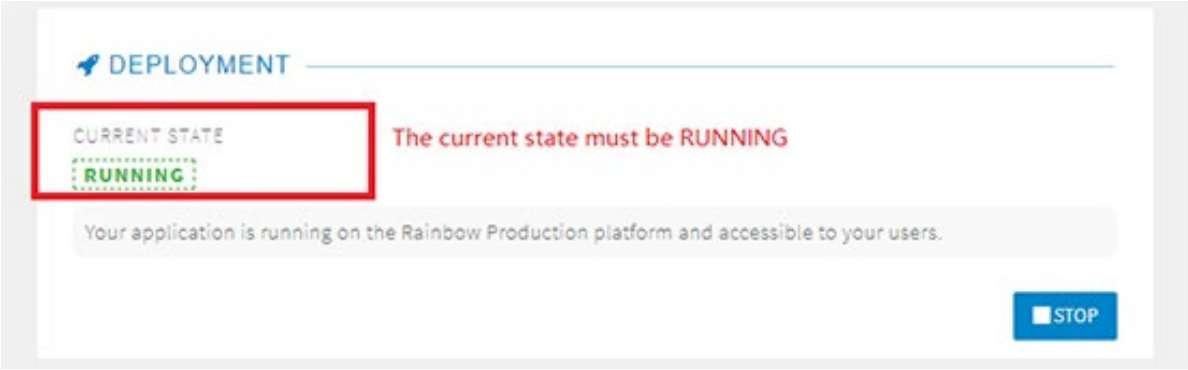
6. Under **OAUTH 2.0 Implicit Grant** section, enable OAUTH 2.0 Implicit Grant.



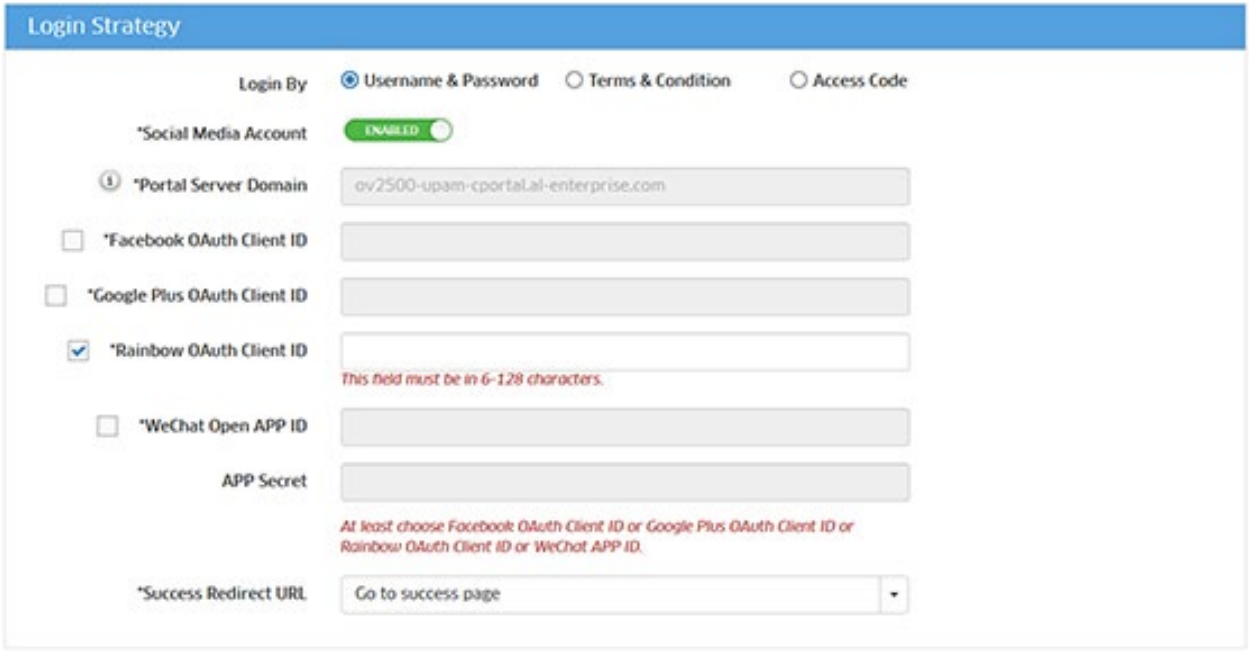
7. In the **Offer** section, choose a payment method.



8. In the **Deployment** section, make sure the **Current State** is **Running**.

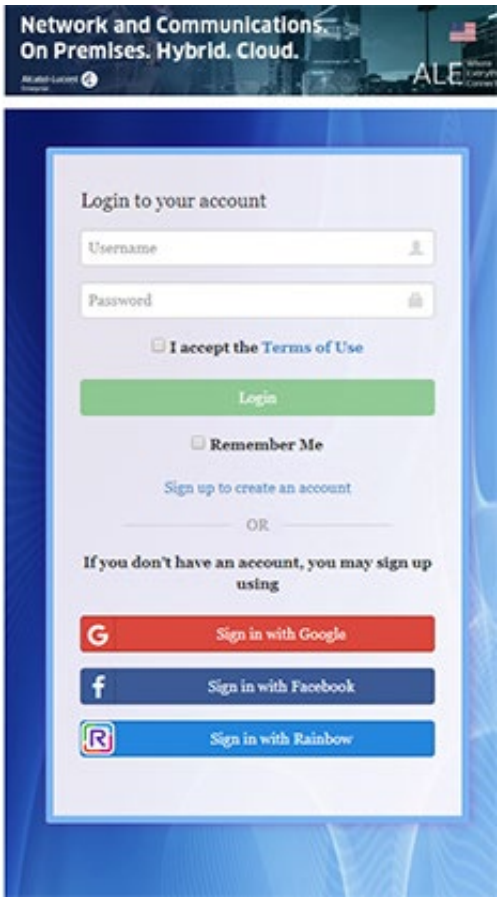


9. Go to the Guest Access Strategy Screen in OmniVista (UPAM - Guest Access - Guest Access Strategy).

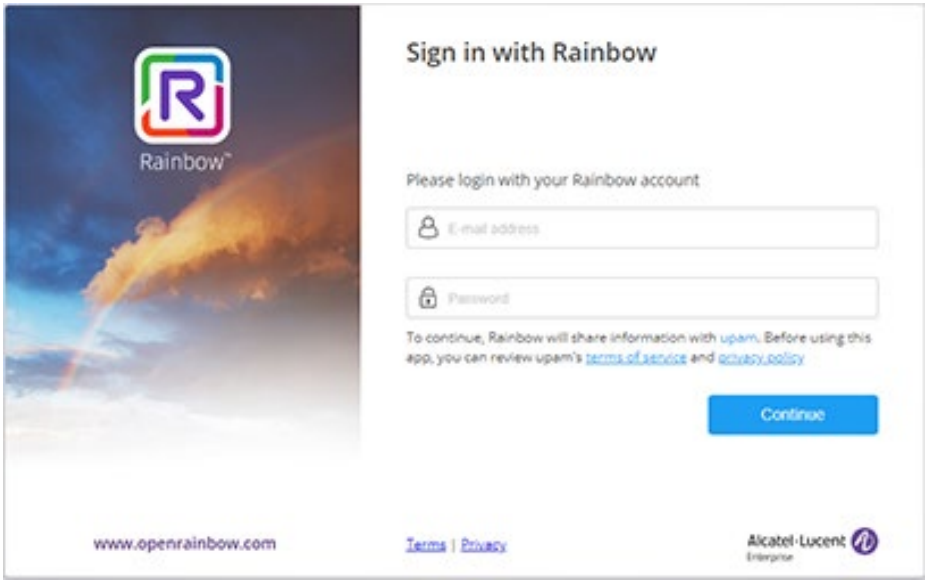


10. In the **Rainbow 0Auth Client ID** field, enter the Rainbow App ID that you receive from Rainbow.

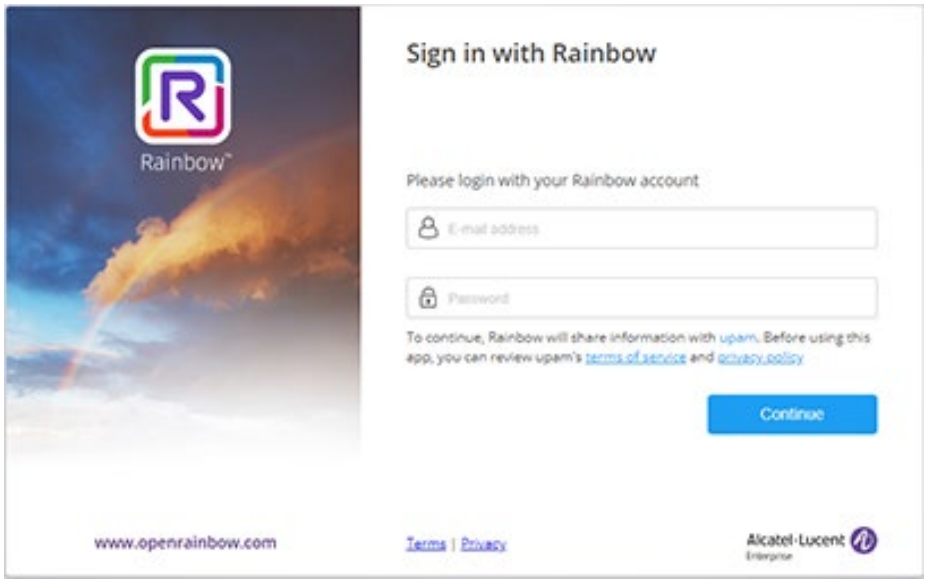
11. Open the Portal page and login using Rainbow.



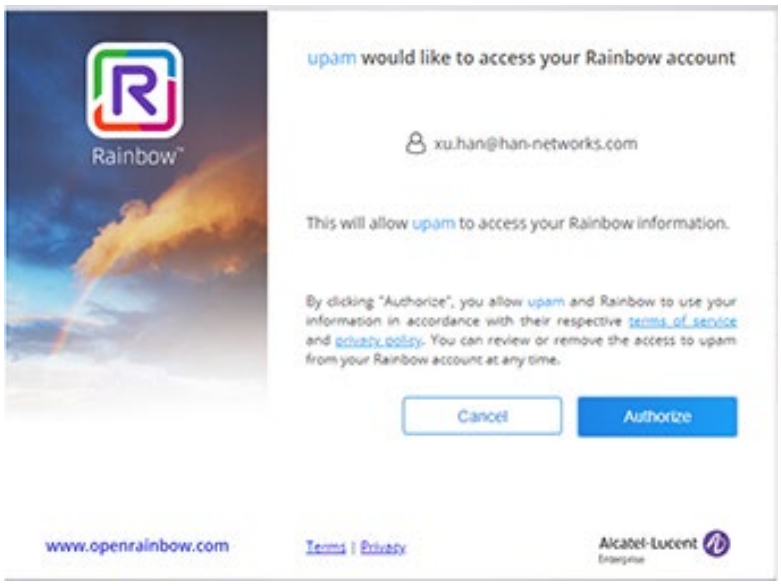
12. Enter the Rainbow App ID in the **Rainbow Application** field on the Guest Access Strategy page in OmniVista.



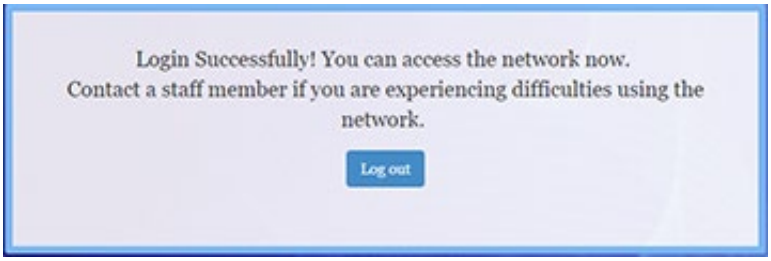
13. When you open the Portal Page, click on **Sign in with Rainbow** and sign into your Rainbow account.



14. On the UPAM Authorization page, click on **Authorize**.



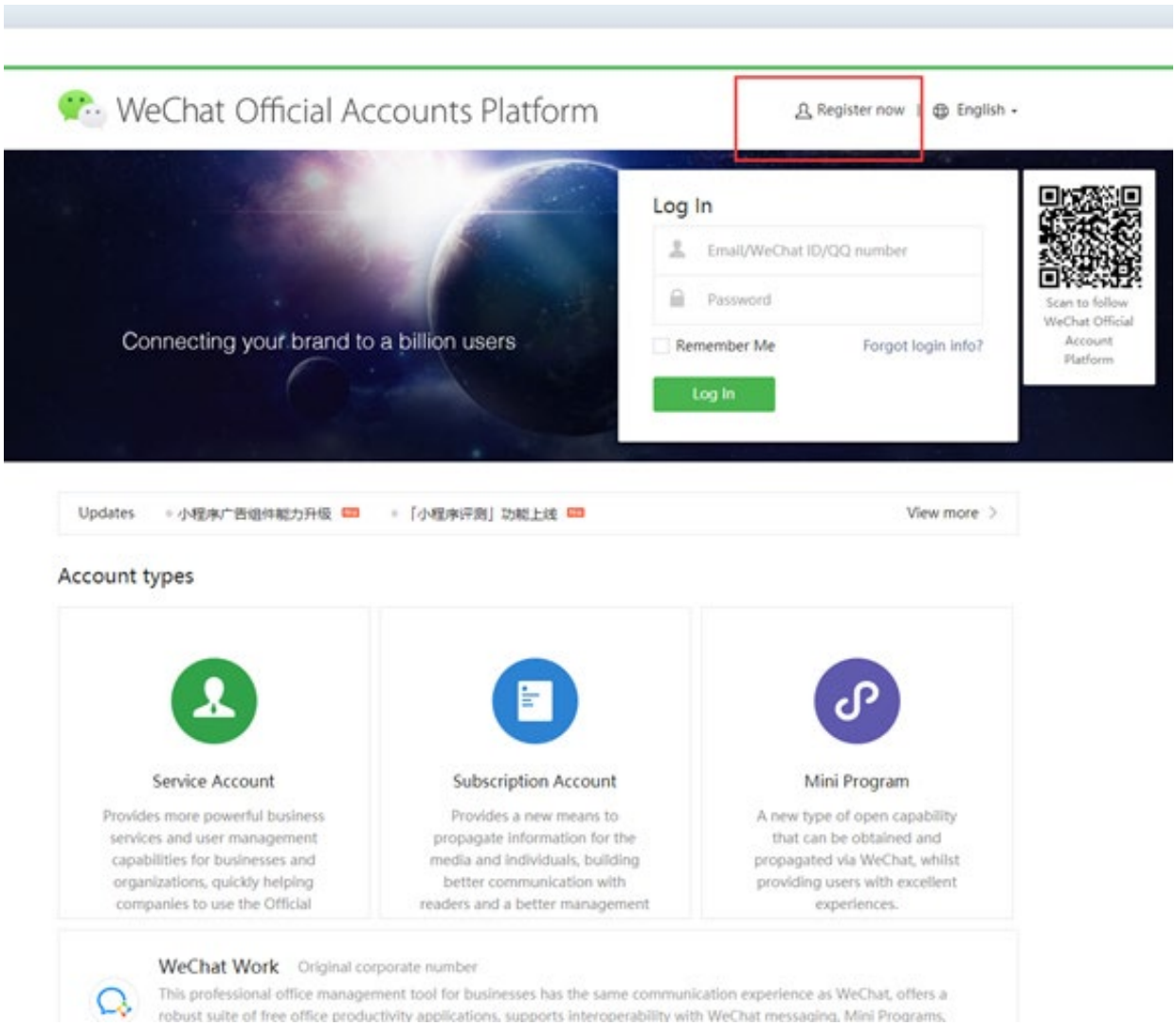
The following login message will appear.



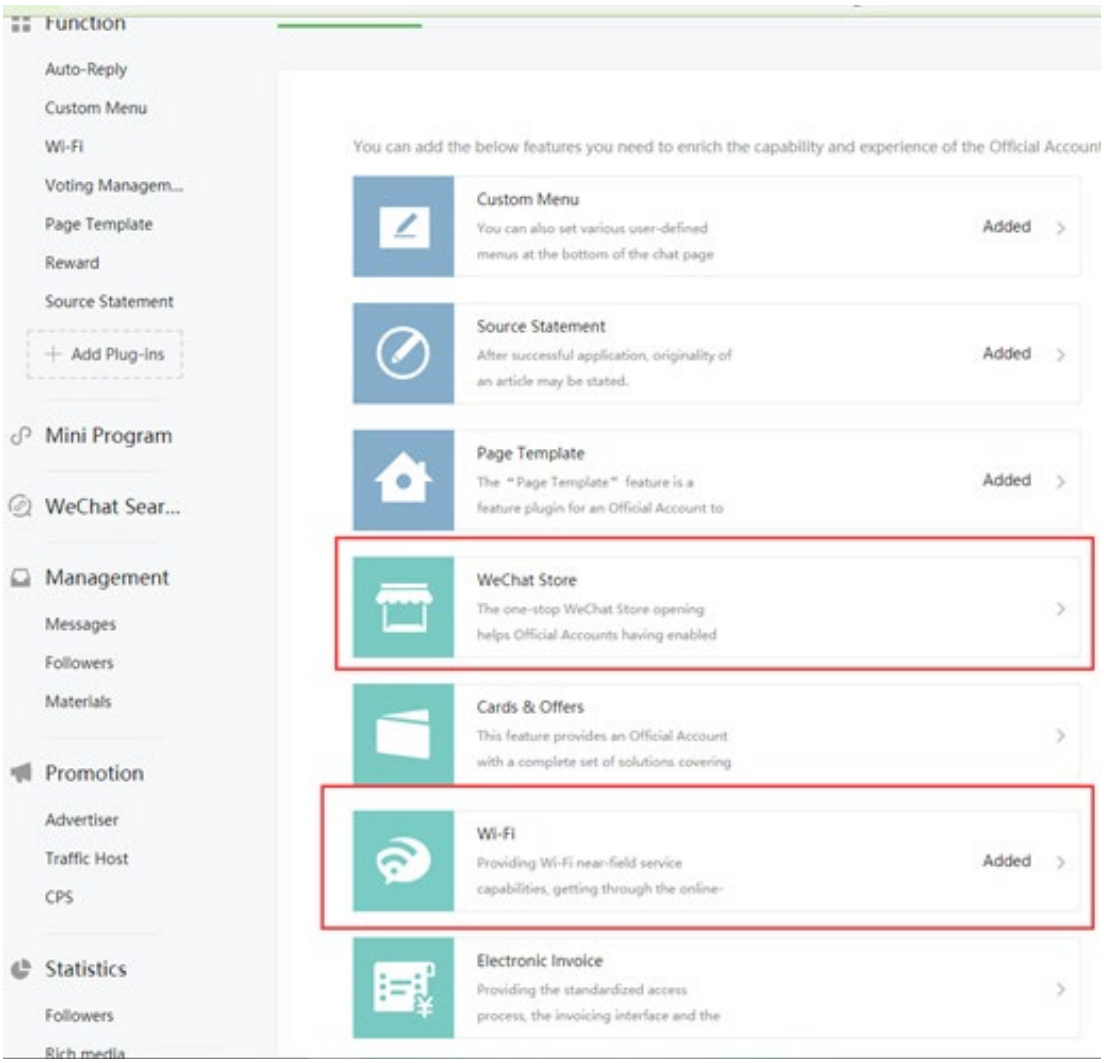
You can now use Rainbow for UPAM Authentication. For more information, go to the Rainbow Documentation Core Concepts page.

Configuring the WeChat API

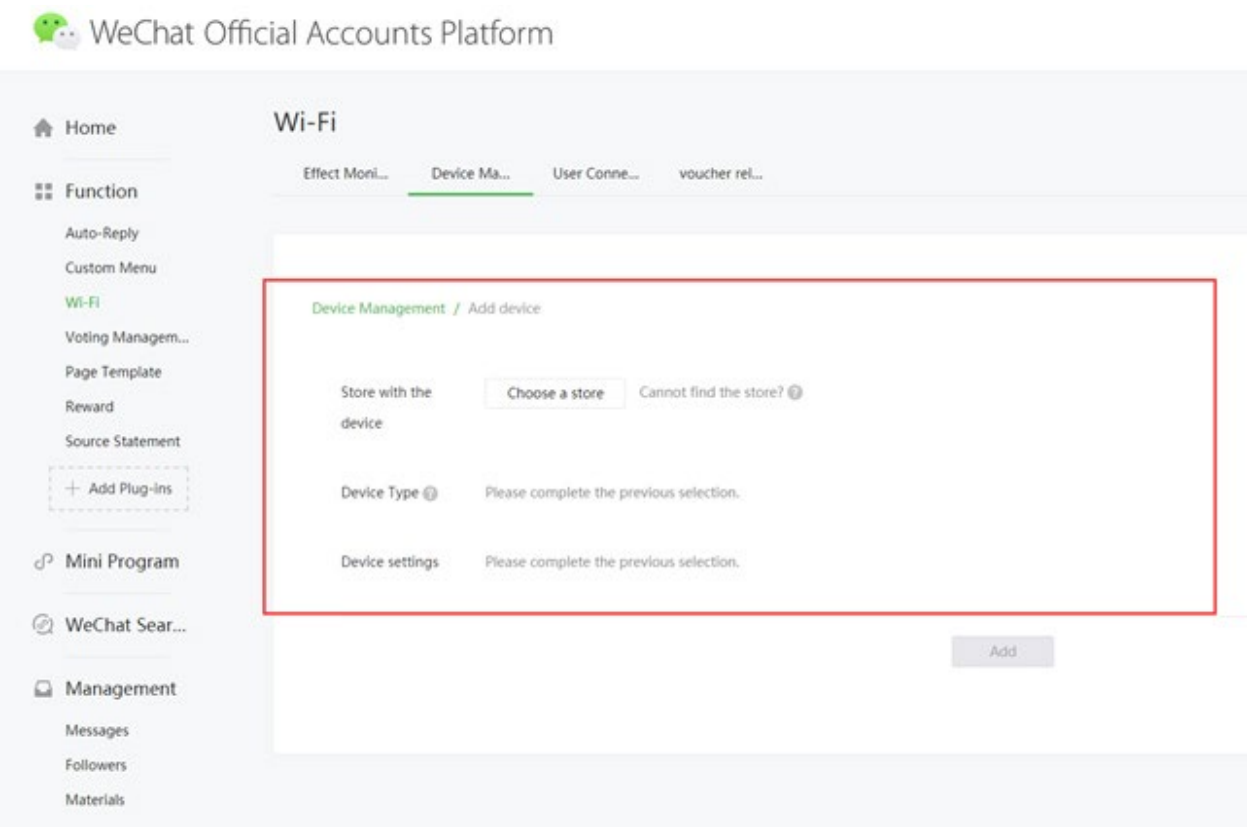
1. Go to the WeChat website (https://mp.weixin.qq.com) and click on **Register Now** to create a Service Account.



2. After creating the account, login and add plug-ins from the **WeChat Store** and **WiFi**.



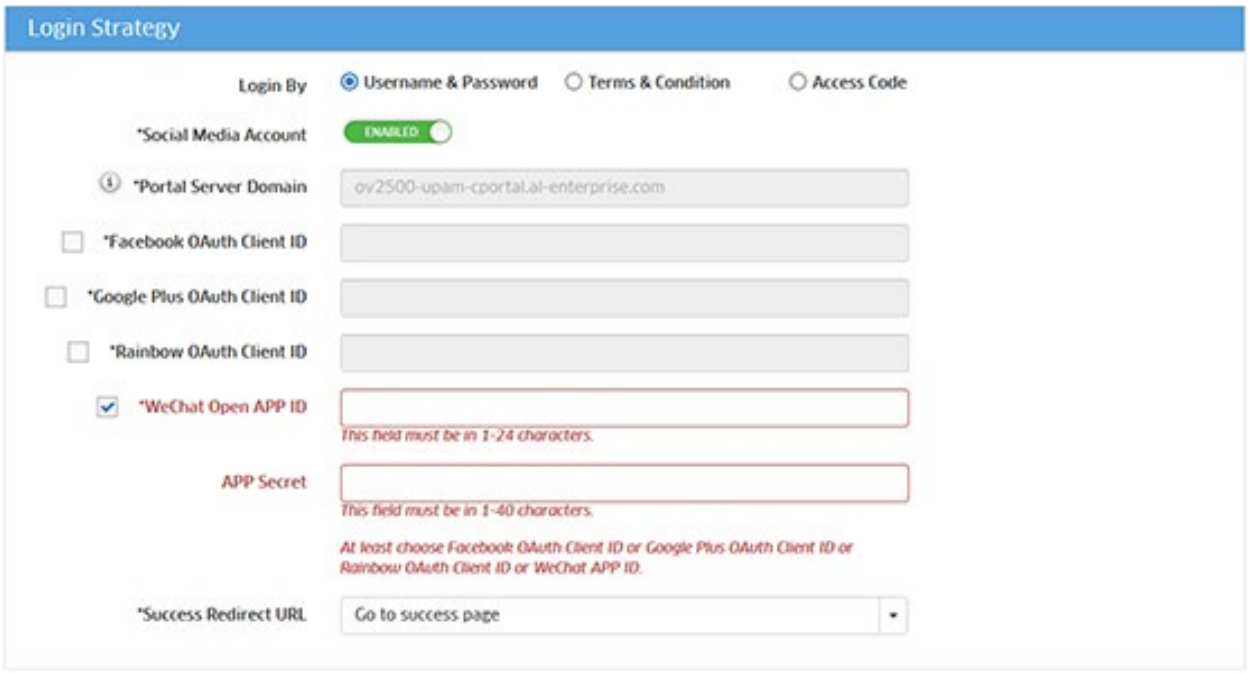
3. To use WiFi, you must create a store In the WeChat Store Plugins.



4. You will receive the WeChat social login parameters that must be entered into the UPAM Guest Access Strategy Screen:

- Store Name
- SSID
- shopId
- appId
- secrectKey

5. Go to the Guest Access Strategy Screen in OmniVista (UPAM - Guest Access - Guest Access Strategy).

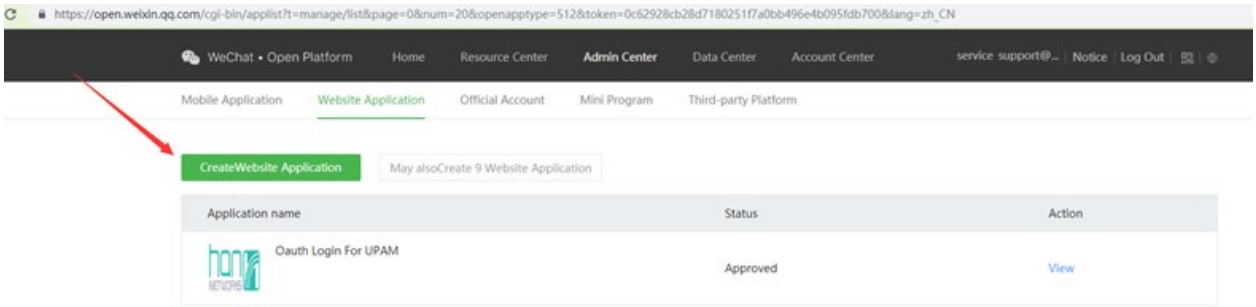


6. Enter the required WeChat information on the Guest Access Strategy Screen in OmniVista.

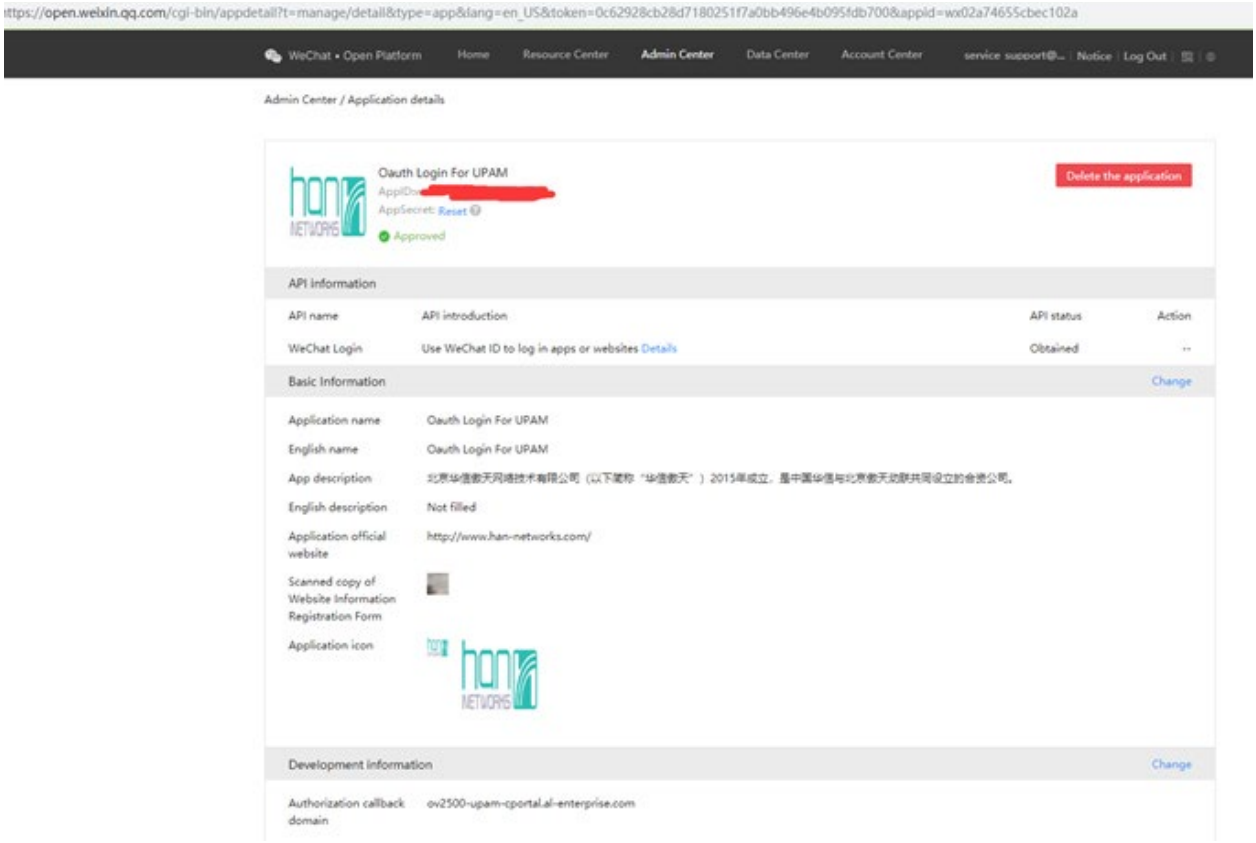
You can now use WeChat for UPAM Authentication on Smartphone and iPad devices. If want to use WeChat authentication on PCs/Laptops, you must complete Steps 6 - 10.

7. Login to WeChat (https://mp.weixin.qq.com).

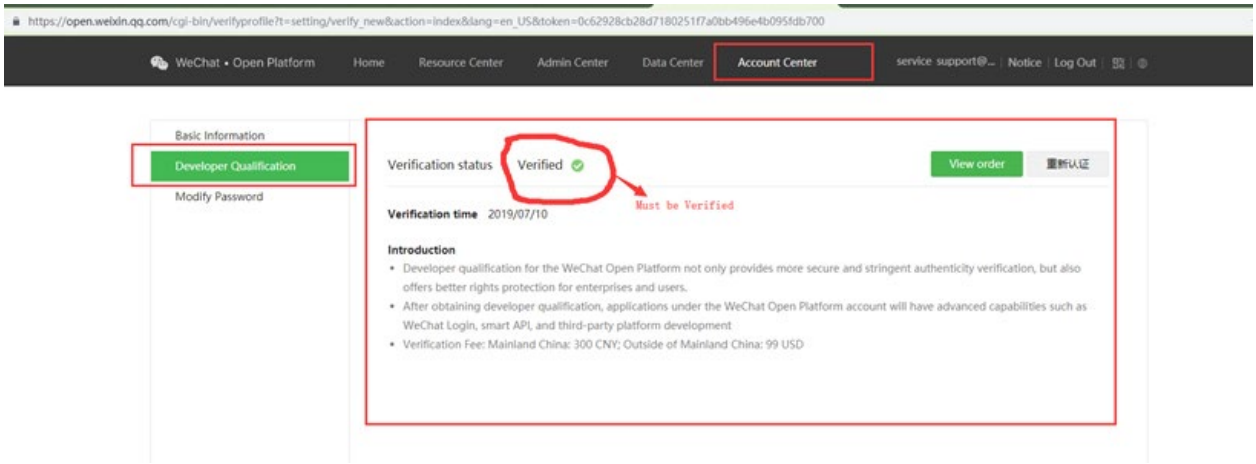
8. Create a website application.



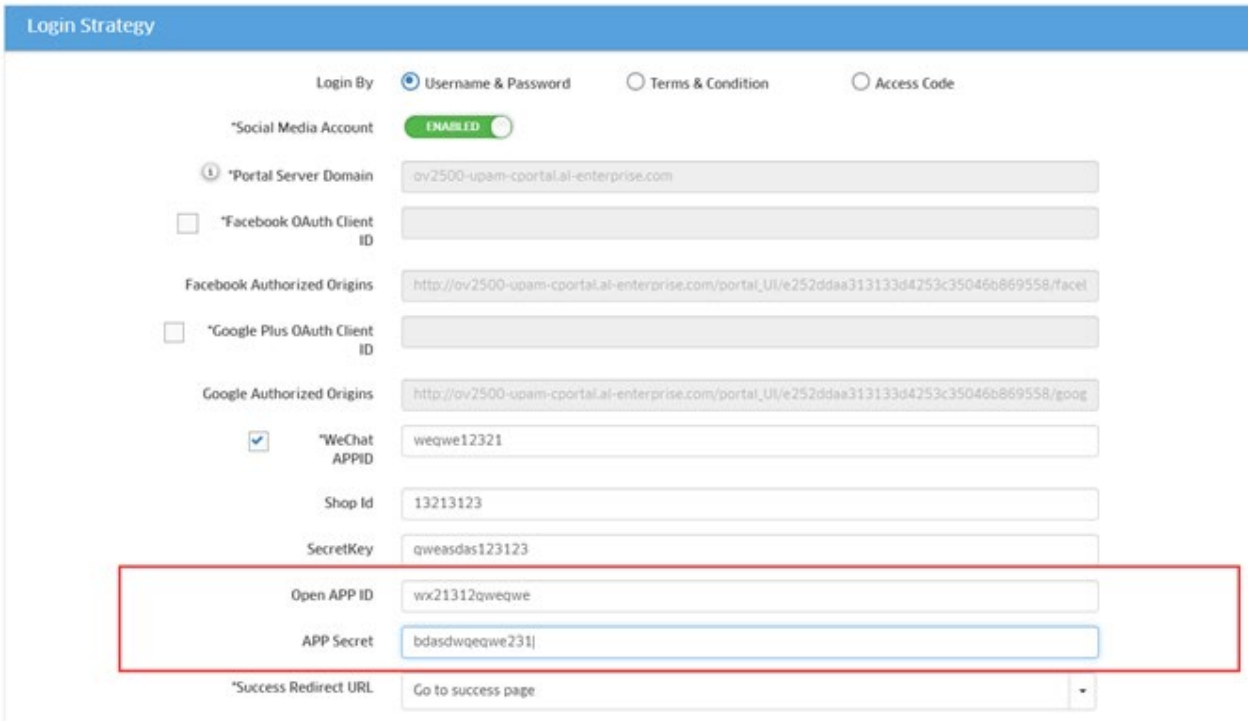
9. You will receive an application.



10. If API status is not obtained, you must pay to receive "Verified" status.



11. The Authorization callback domain of the WeChat website application should be populated with your portal server domain (Current FQDN of the Guest Strategy, which is the UPAM server). Then copy AppID and AppSecret in your WeChat web app to the Guest Strategy page, as shown below.



Guest Account

The Guest Access Guest Account Screen displays all configured Guest Accounts and is used to create, edit, and delete Guest Accounts. If self-registration is not enabled, you can manually create a login account for a Guest User and relay the information to the Guest User. In addition, you can manually add a device for the Guest Account to the Remembered Devices List on the Guest Device Screen.

There are two tabs on the Guest Account Screen: " Account" displays all configured Guest Accounts. "Access Code" displays all configured Guest Access Code Accounts. The "Account" tab is used to create Guest Acounts by name and the "Access Code" tab is used to create Guest Accounts by access code.

Creating a Guest Account

Click on the Add icon to bring up the Create Guest Account Screen. Complete the fields as described below, then click on the **Create** button. When an account is created, it is automatically enabled. To disable and account, select the account and click on the Disable icon at the top of the screen.

- **User Name -** Account identifier (e.g., name of the guest).
- **Password -** Password for the account.
- **Repeat Password -** Re-enter and confirm the Guest Account password.
- **Service Level -** Specify the service level for the Guest Account. Service Levels are configured on the UPAM - Guest Access - Global Configuration page.
- **Data Quota -** Enable and set the maximum data usage allowed for the Guest Account, in MB. By default, this field is set to 1MB. You can set a different Data Quota by assigning a Service Level to the Guest Account. Service Levels are configured on the UPAM - Guest Access - Global Configuration page.

- **Account Validity Period -** The length of time that the Guest Account is valid. The initial date and time displayed reflects the Account Validity Period configured on the Global Configuration page (UPAM - Guest Access - Global Configuration). You can change that range here by clicking on the Calendar icon and setting a new date and time. However, the Account Validity Period you set cannot be longer than the length set on the Global Configuration page. For example, if you set the Global Validity Period to 180 days, the longest period you will be able to set will be up to 180 days.
- **Full Name -** Full name of the Guest User.
- **Company -** Company name of the Guest User.
- **Telephone -** Telephone number of the Guest User.
- **Email -** Email address of the Guest User.
- **Description -** Optional description for the account

Note: You can automatically import a xls/csv/xlsx file containing Guest Account information by clicking on the **Import** button at the top of the screen. You can also download a template by clicking on the **Import** button then clicking on the **Template Download** button.

Note: To print a ticket for a Guest User containing login information, click on the **Create and Print** button when creating the account. If the account has already been created, select the account and click on the **Print Tickets** button to immediately print a ticket.

Batch Creation

You can quickly create multiple Guest Accounts by clicking on the **Batch Creation** button at the top of the screen. Complete the fields as described below then click on the **Create** button. To print tickets for the Guest Users containing login information, click on the **Create and Print** button.

- **Guest Account Name Prefix -** Enter a prefix for the accounts you are creating. When created, the account name will consist of the prefix and incremented number (e.g., Guest1, Guest2).
- **Number of Clients to Create -** Enter the number of Guest Accounts you want to create. (Range = 1 – 5000)
- Service Level - Specify the service level for the account. Service Levels are configured on the UPAM - Guest Access - Global Configuration page.
- **Data Quota -** Enable and set the maximum data usage allowed for the Guest Account.
- **Account Validity Period -** Length of time, in days, that the Guest Account is valid. The range available depends on the range set on the Global Configuration Screen (UPAM - Guest Access - Global Configuration). For example, if you set the Global Validity Period to 180 days, the longest period you will be able to set will be up to 180 days. (Range = 1 – 365, Default = 90)
- **Description -** Optional description for the account

Note: The Batch Creation Feature is enabled on the Global Configuration Screen (UPAM - Guest Account - Global Configuration). Once it is enabled, the **Batch Creation** button is enabled.

Editing a Guest Account

Select a Guest Account in the Guest Account List and click on the Edit icon. Edit the field(s) as described above, and click on the **Apply** button. Note that you cannot edit an Account Name.

Deleting a Guest Account

Select a Guest Account in the Guest Account List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Adding a Device to the Guest Account Remebered Devices List

Select a Guest Account in the Guest Account List and click on the **Add Device** button at the top of the screen to bring up the Create Guest Device Screen. Complete the fields as described below, then click on the **Create** button. The device is added to the Remebered Devices List on the Guest Device screen.

- **Device MAC** - Enter the MAC address of the guest device.
- **Device Category** - Optionally select a category for the device (Default = Others):
  - Computer
  - Mobile
  - Tablet
  - Game console
  - Digital media receiver
  - Others
- **Device Family** - Optionally select a production vendor of the guest device (Default = Others):
  - Alcatel-Lucent Enterprise
  - Apple
  - Samsung
  - Huawei
  - Microsoft
  - LG
  - Lenovo
  - HP
  - IBM
  - Nokia
  - MI
  - HTC

  - Sony
  - Blackberry
  - Others
- **Device OS -** Optionally select the OS running on the guest device (Default = Others):
  - Linux
  - Windows
  - MacOS
  - Android
  - IOS
  - Others
- **Description** - Enter an optional description for this device.

Guest Account List

The Guest Account List displays information about all configured Guest Accounts. The list displays basic information. Click on an account in the list for more detail.

Basic

- **User Name -** Account identifier (e.g., name of the guest).
- **Data Quota -** Whether or not the Data Quota feature is Enabled/Disabled.
- **Data Quota Amount -** The maximum data traffic allowed for the Guest User if configured.
- **Account Validity Period -** The length of time, in days, that the account is valid.
- **Service Level -** The the service level for the account.
- **Full Name -** Full name of the Guest User.
- **Company -** Company name of the Guest User.
- **Telephone -** Telephone number of the Guest User.
- **Email -** Email address of the Guest User.
- **Online Devices -** The number of online devices are logged in with the account.
- **Sponsor Name -** Sponsor who created the account or approved it for self-registration.
  - **Admin-XXX -** Indicates the sponsor belongs to the Administrator group; XXX indicates the account in the group.
  - **EmployeeSponsor-YYY -** Indicates the sponsor belongs to the Employee group; YYY indicates the employee account in the group.
  - **GuestSponsor-ZZZ -** Indicates the sponsor belongs to the Guest Operator group; ZZZ indicates the Guest Operator account in the group.
  - **SelfRegister-AAA -** Indicates no sponsor is involved and there is no need approval for the self-registration request; AAA indicates the login password is guest-user-defined (Manually) or UPAM-defined (Automatically).
- **Description -** Optional description for the account.

- **Effective Date -** The date and time the account was created.
- **Status -** The administrative status of the account (Enabled/Expired/Disabled).
- **Guest Account Deletion Policy -** The number of days after the Account Validity Period expires before Guest Accounts are automatically deleted:
  - **Never -** Guest Account will **not** be deleted at the end of the Account Validity Period (Default).
  - **Immediately -** Guest Account will be automatically deleted at the end of the Account Validity Period.
  - **Number of Days -** Guest Account will be automatically deleted on the configured number of days after the end of the Account Validity Period (Range = 1 - 90).

Detailed

- **Guest Type -** The login method for the guest.
- **User Name -** Account identifier (e.g., name of the guest).
- **Telephone -** Telephone number of the Guest User.
- **Email -** Email address of the Guest User.
- **Full Name -** Full name of the Guest User.
- **Company -** Company name of the Guest User.
- **Effective Date -** The date and time the account was created.
- **Expire Time -** The time when the account is going to expire.
- **Service Level -** The the service level for the account.
- **Data Quota -** Whether or not the Data Quota feature is Enabled/Disabled.
- **Data Quota Amount -** The maximum data traffic allowed for the Guest User if configured.
- **Guest Account Deletion Policy -** The number of days after the Account Validity Period expires before Guest Accounts are automatically deleted:
  - **Never -** Guest Account will **not** be deleted at the end of the Account Validity Period (Default).
  - **Immediately -** Guest Account will be automatically deleted at the end of the Account Validity Period.
  - **Number of Days -** Guest Account will be automatically deleted on the configured number of days after the end of the Account Validity Period (Range = 1 - 90).
- **Sponsor Name -** Sponsor who created the account or approved it for self-registration.
  - **Admin-XXX -** Indicates the sponsor belongs to the Administrator group; XXX indicates the account in the group.
  - **EmployeeSponsor-YYY -** Indicates the sponsor belongs to the Employee group; YYY indicates the employee account in the group.
  - **GuestSponsor-ZZZ -** Indicates the sponsor belongs to the Guest Operator group; ZZZ indicates the Guest Operator account in the group.
  - **SelfRegister-AAA -** Indicates no sponsor is involved and there is no need approval for the self-registration request; AAA indicates the login password is guest-user-defined (Manually) or UPAM-defined (Automatically).

- **Online Devices -** The number of online devices are logged in with the account.
- **Status -** The administrative status of the account (Enabled/Disabled).
- **Description -** Optional description for the account.

Note: Custom attributes will show if you configured **Custom Attributes** in Guest Access Strategy.

Creating a Guest Access Code Account

To create a new Guest Access Code Account, click on the “Access Code” tab on the Guest Accounts screen then click on the Add icon to access the Create Guest Account screen. Complete the fields as described below, then click on the **Create** button.

- **Access Code -** The Access Code of the Guest Account.
- **Service Level -** Specify the service level for the Guest Account. Service Levels are configured on the UPAM - Guest Access - Global Configuration page.
- **Account Validity Period -** The length of time that the Guest Account is valid. The initial date and time displayed reflects the Account Validity Period configured on the Global Configuration page (UPAM - Guest Access - Global Configuration). You can change that range here by clicking on the Calendar icon and setting a new date and time. However, the Account Validity Period you set cannot be longer than the length set on the Global Configuration page. For example, if you set the Global Validity Period to 180 days, the longest period you will be able to set will be up to 180 days.
- **Description** - Optional description for the account.

Note: You can automatically import a xls/csv/xlsx file containing Guest Account information by clicking on the **Import** button at the top of the screen. You can also download a template by clicking on the **Import** button then clicking on the **Template** button.

Note: To print a ticket for a Guest User containing login information, click on the **Create&Print** button when creating the account. If the account has already been created, select the account and click on the **Print Tickets** button to immediately print a ticket.

Batch Account Creation by Access Code

You can quickly create multiple Guest Accounts by clicking on the **Batch Creation** button at the top of the screen. Complete the fields as described below then click on the **Create** button. To print tickets for the Guest Users containing login information, click on the **Create and Print** button.

- **Number of Clients to Create -** Enter the number of Guest Accounts you want to create. (Range = 1 - 5000)
- **Service Level -** Specify the service level for the account. Service Levels are configured on the UPAM - Guest Access - Global Configuration page.
- **Account Validity Period -** Length of time, in days, that the Guest Account is valid. The range available depends on the range set on the Global Configuration Screen (UPAM - Guest Access - Global Configuration). For example, if you set the Global Validity Period

to 180 days, the longest period you will be able to set will be up to 180 days. (Range = 1 – 365, Default = 90)

- **Description -** Optional description for the account.

  Note: The Batch Creation Feature is enabled on the Global Configuration Screen (UPAM - Guest Account - Global Configuration). Once it is enabled, the **Batch Creation** button is enabled.

Editing a Guest Access Code Account

Select a Guest Access Code Account in the Access Code List and click on the Edit icon. Edit the field(s) as described above and click on the Apply button. Note that you cannot edit an Account Name.

Deleting a Guest Account

Select a Guest Access Code Account in the Access Code List and click on the Delete icon. Click OK at the Confirmation Prompt.

Extend a Guest Access Code Account

You can extend the expiration date for a Guest Access Code Account in the Access Code List by accessing the Extend Account Screen. Select a Guest Access Code Account in the Access Code List and click on the Extend button. Select a new Account Validity Period then click on the Save button.

Access Code List

The Access Code List displays information about all configured Guest Access Code Accounts. The list displays basic information. Click on an account in the list for more detail.

Basic

- **Access Code -** The Access Code of the Guest Account.
- **Status -** The administrative status of the account (Enabled/Expired/Disabled).
- **Effective Date -** The date and time the account was created.
- **Account Validity Period -** The date and time the Account Validity Period ends.
- **Service Level -** The Service Level for the Guest Account, if configured.
- **Guest Account Deletion Policy -** The number of days after the Account Validity Period expires before Guest Accounts are automatically deleted:
  - **Never -** Guest Account will **not** be deleted at the end of the Account Validity Period (Default).
  - **Immediately -** Guest Account will be automatically deleted at the end of the Account Validity Period.
  - **Number of Days -** Guest Account will be automatically deleted on the configured number of days after the end of the Account Validity Period (Range = 1 - 90).
- **Sponsor Name -** Sponsor who created the Guest Account or approved it for self-registration.
  - **Admin-XXX -** Indicates the sponsor belongs to the Administrator group; XXX indicates the account in the group.

  - **EmployeeSponsor-YYY -** Indicates the sponsor belongs to the Employee group; YYY indicates the employee account in the group.
  - **GuestSponsor-ZZZ -** Indicates the sponsor belongs to the Guest Operator group; ZZZ indicates the Guest Operator account in the group.
  - **SelfRegister-AAA -** Indicates no sponsor is involved and there is no need approval for the self-registration request; AAA indicates the login password is guest-user-defined (Manually) or UPAM-defined (Automatically).
- **Description -** Optional description for the account.

Detailed

- **Guest Type -** The login method for the Guest Account (Access Code)
- **Access Code -** The Access Code of the Guest Account.
- **Effective Date -** The date and time the Guest Account was created.
- **Expire Time -** The date and time the Guest Account expires.
- **Service Level -** The Service Level for the Guest Account, if configured.
- **Guest Account Deletion Policy -** The number of days after the Account Validity Period expires before Guest Accounts are automatically deleted:
  - **Never -** Guest Account will **not** be deleted at the end of the Account Validity Period (Default).
  - **Immediately -** Guest Account will be automatically deleted at the end of the Account Validity Period.
  - **Number of Days -** Guest Account will be automatically deleted on the configured number of days after the end of the Account Validity Period (Range = 1 - 90).
- **Sponsor Name -** Sponsor who created the account or approved it for self-registration.
  - **Admin-XXX -** Indicates the sponsor belongs to the Administrator group; XXX indicates the account in the group.
  - **EmployeeSponsor-YYY -** Indicates the sponsor belongs to the Employee group; YYY indicates the employee account in the group.
  - **GuestSponsor-ZZZ -** Indicates the sponsor belongs to the Guest Operator group; ZZZ indicates the Guest Operator account in the group.
  - **SelfRegister-AAA -** Indicates no sponsor is involved and there is no need approval for the self-registration request; AAA indicates the login password is guest-user-defined (Manually) or UPAM-defined (Automatically).
- **Online Devices -** The number of online devices are logged in with the account.
- **Status -** The administrative status of the account (Enabled/Disabled).
- **Description -** Optional description for the account.

Guest Device

The Guest Access Guest Device Screen displays all authenticated online guest devices as well as all guest devices that were previously on the network and are stored in UPAM.

Online Device List

The Online Device List displays all authenticated online guest devices.

Basic

- **Account Name -** User name of the guest account.
  - For MAC authentication - Account name is the MAC address of the guest device.
  - For Captive Portal Authentication - Account name is user name of the guest user.
- **Client IPv4 -** IPv4 address of the guest device.
- **Client IPv6 -** IPv6 address of the guest device.
- **Remembered -** Indicates whether the online device was remembered by UPAM and added into the Remembered Device List. A remembered device can be utilized for MAC authentication.
- **Device Category -** Category of the guest device:
  - Computer
  - Mobile
  - Tablet
  - Game console
  - Digital media receiver
  - Others
- **Device Family -** Production vendor of the guest device:
  - Alcatel-Lucent Enterprise
  - Apple
  - Samsung
  - Huawei
  - Microsoft
  - LG
  - Lenovo
  - HP
  - IBM
  - Nokia
  - MI
  - HTC
  - Sony
  - Blackberry
  - Others
- **Device OS -** OS running on the guest device.

  - Linux
  - Windows
  - MacOS
  - Android
  - IOS
  - Others
- **Authentication Type -** Authentication type used to login by the guest user (MAC authentication or Captive Portal authentication).
- **Auth Resource -** Guest account database used for authentication (None or Local Database).
- **Session Start -** The date and time when the user was online and the connection session created.
- **Access Role Profile -** Access Role Profile applied on the guest device.
- **Final Access Role Profile -** Access Role Profile assigned by NAS before the Access Role Profile returned by UPAM.
- **Policy List -** Policy List applied on the guest device.
- **Redirect URL -** Redirect URL returned to the guest device by UPAM.

Authenticate

- **Authentication Method -** The method used to authenticate the device (e.g., PAP, EAP-MD5, EAP-PEAP, EAP-TLS).
- **Access Device MAC -** MAC address of the NAS to which the guest device is attached.
- **Access Device Name -** System name of the NAS to which the guest device is attached
- **Access Device SSID -** Wireless service broadcast by the NAS and connected by guest device (only valid for wireless access).
- **Access Device Location -** Location of the NAS.
- **Called Station ID -** Allows the NAS to send the phone number that the user called in the Access-Request packet, using Dialed Number Identification (DNIS) or similar technology.
  - For Switch - The switch MAC address.
  - For AP: radio_MAC_address:SSID_NAME
- **NAS Port Type -** Type of port of the NAS is authenticating the user:
  - Wireless-IEEE 802.11
  - Ethernet.
- **NAS Port -** Physical port number of the NAS is authenticating the user.
  - For Switch - if index
  - For AP - Wireless radio index
- **NAS Port ID -** NAS port authenticating the user. (The attribute can be configured in Unified Access - Unified Profile – Template - AAA Server Profile).
  - For switch: chassis/slot/port
  - For AP: WLAN service
- **NAS ID -** NAS originating the Access-Request.
- **NAS IP Address -** NAS IP address.

- **Slot Port -** Port number on the switch slot to which the device is connected (only for wired accessing).
- **Port Desc/Wlan Service**
  - For Switch - Port description
  - For AP - WLAN service
- **Framed MTU -** Maximum Transmission Unit to be configured for the user when it is not negotiated by some other means (e.g., PPP). It is a fixed value = 1400.
- **Reject Reason -** Reason for rejecting the authentication request from the user device
  - Overdue license
  - Invalid username or password
  - Cannot match access policy according to the authentication request

Account

- **Acct Status Type -** Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop). Values: Start (1), Stop (2), Interim-Update (3), Accounting-On (7) Accounting-Off (8).
- **Acct Session Time -** Indicates how many seconds the user has received service, and can only be present in Accounting-Request records where the Acct Status Type is set to Stop.
- **Acct Session ID -** Unique Accounting ID that makes it easy to match start and stop records in a log file. The start and stop records for a given session must have the same Acct Session ID.
- **Termination Action -** Fixed with “Radius-Request”. When the session is timed out, the user needs to be re-authenticated.
- **Session Timeout -** Maximum number of seconds of service provided prior to session termination.
- **Acct Interim Interval -** Number of seconds between each interim update in seconds for this specific session.
- **Tunnel Private Group ID -** Used to support the legacy VLAN assignment from RADIUS (ID=VLAN ID).
- **Acct Terminate Cause -** Indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
  - 1 - User Request: User logout
  - 4 - Idle Timeout: User activity logout (only applicable for MAC based or Captive Portal users)
  - 6 - Admin Reset: Operator logout/flush operation
  - 7 - Admin Reboot: Operator reboot operation
  - 8 - Port Error: Port down, NI down
  - 9 - NAS-Error: Any software notification that the user is no longer authenticated

Remembered Device List

The Remembered Device List displays all authenticated guest devices saved in UPAM and can be utilized for MAC authentication.

- **User Name -** Account used by the guest user for login.
  - For MAC authentication - Account name is MAC address of the user device.
  - For 802.1X authentication - Account name is user name of the employee user.
  - For Captive Portal authentication - Account name is user name of the guest user or employee user.
- **Device MAC -** MAC address of the guest device.
- **Device Category -** Category of the guest device:
  - Computer
  - Mobile
  - Tablet
  - Game console
  - Digital media receiver
  - Others
- **Device Family -** Production vendor of the guest device:
  - Alcatel-Lucent Enterprise
  - Apple
  - Samsung
  - Huawei
  - Microsoft
  - LG
  - Lenovo
  - HP
  - IBM
  - Nokia
  - MI
  - HTC
  - Sony
  - Blackberry
  - Others
- **Device OS -** OS running on the guest device:
  - Linux
  - Windows
  - MacOS
  - Android
  - IOS
  - Others
- **Browser Type -** Browser of the guest device
- **Activity Status -** Indicate whether the guest device is online or offline.

- **Expiry Time -** Indicate the expiry time of the guest device. When it is expired, the guest device will be deleted from the remembered list in UPAM.
- **Remembered Time -** Time when the guest device is remembered by UPAM
- **Last Access Time -** Time when the guest device latest accesses to the network
- **Last Access Device Location -** Location of the NAS to which guest device last access
- **Last Access Device MAC -** MAC address of the NAS to which guest device last access
- **Last Access Device Name -** System Name of the NAS to which guest device last access
- **Last Access Device SSID -** SSID of the NAS to which guest device last access.
- **Web Access Strategy -** The Access Strategy used for the device. One device can login through multiple Guest Access Strategies.
- **Remember Method -** Indicates whether the device was manually added to the list (Static) or automatically added through Captive Portal Authentication (Auto).
- **Active Status -** Indicates whether the remembered device was ever logged into the network. " Actived" means the device was. at one time, logged into the network. :Inactive means the device was manually added, but never logged into the network. Only " Actived" devices consume a Guest license.

Self-Registration Request

The Guest Access Self-Registration Request Screen is used to review, approve or reject self-registration requests from Guest Users. If “Self Registration” and “Approved by Sponsor” are enabled in the Guest Access Strategy, a guest user must summit a request email to enroll personal with the required information. The self-registration request sent by guest user can be taken care of by the Administrator, Guest Operator or Employee sponsor, using the Approve or Reject operation.

To approve or reject a Self-Registration Request, select the request in the Self-Registration Request List and click on the **Approve** or **Reject** button at the top of the screen.

Self-Registration Request List

- **Guest Name -** Name of the guest user. If the self-registration request is approved, the guest name will be used as the login account for the guest user.
- **Full Name -** Full name of the guest user.
- **Company -** Company name of the guest user.
- **Register Time -** Date and Time when the guest user submitted the self-registration request.
- **Employee Email -** Email address of the employee being visited.
- **Employee Visited -** Name of the employee being visited.
- **Employee Phone Number -** Phone number of the employee being visited.
- **Visited Reason -** The purpose for this visit by the guest.
- **Status -** Status for the guest self-registration request.
    - **Unchecked -** The request needs to be checked by the Administrator or Guest Operator.
    - **Approved -** The request is approved by the Administrator/Guest Operator/Employee Sponsor and the approval message has been send to the guest through email.

  - **Rejected -** The request is rejected by Administrator/Guest Operator/Employee Sponsor and the rejection message has been send to the guest through email.
- **Approver Name -** The person who approves the self-registration request.
  - **Admin-XXX -** Admin indicates the sponsor belongs to The Administrator group; XXX indicates the account for the group.
  - **EmployeeSponsor-YYY -** EmployeeSponsor indicates the sponsor belongs to the employee group; YYY indicates the employee account for the group.
  - **GuestSponsor-ZZZ -** GuestSponsor indicates the sponsor belongs to the Guest Operator group; ZZZ indicates the Guest Operator account for the group.
- **Approval Time -** The date and time when the self-registration request was approved.
- **Email -** Email address of the guest user.
- **Telephone -** Telephone number of the guest user.
- **Guest Access Strategy -** Guest Access Strategy assigned to the guest user after approval.
- **Description -** Optional description information provided by the guest.

Note: Custom attributes will show if you configured **Custom Attributes** in Guest Access Strategy.

Guest Operator

The Guest Access Guest Operator Screen displays all configured Guest Operators and is used to create, edit, and delete a Guest Operator. A Guest Operatory is a network operator who manages the guest user network access. A Guest Operator can create guest user accounts and approve guest user self-registration requests.

Creating a Guest Operator

Click on the Add icon to bring up the Create Guest Operator Screen. Complete the fields as described below, then click on the **Create** button.

- **Username -** User name of the Guest Operator account.
- **Full Name -** Full name of the Guest Operator.
- **Password -** Password of the Guest Operator account.
- **Repeat Password -** Re-enter to confirm the account password.
- **Telephone -** Telephone of the Guest Operator.
- **Email -** Email address of the Guest Operator.
- **Location -** Location/Site of the Guest Operator. Guest requests are sent to the operator for this location.
- **Description -** Optional description information for the Guest Operator account.

Editing a Guest Operator

Select a Guest Operator in the Guest Operator List and click on the Edit icon. Edit the field(s) as described above and click on the **Apply** button. Note that you cannot edit a User Name.

Deleting a Guest Operator

Select a Guest Operator in the Guest Operator List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Guest Operator List

The Guest Operator displays information about all configured mappings.

- **Username -** User name of the Guest Operator account.
- **Full Name -** Full name of the Guest Operator.
- **Telephone -** Telephone of the Guest Operator.
- **Email -** Email address of the Guest Operator.
- **Location -** Location/Site of the Guest Operator. Guest requests are sent to the operator for this location.
- **Description -** Optional description information for the Guest Operator account.
- **Last Login Time -** Latest login time for the Guest Operator account.
- **Login URL -** The management interface for Guest Operator. It uses the secondary IP address of OmniVista

Global Configuration

The Guest Access Global Configuration Screen is used to set global configurations for Guest Access Strategy and Guest Accounts. Complete the fields as described below and click on the **Apply** button.

Batch Account Creation

Batch Account creation enables you quickly create batch accounts for Guest Users. Guest Accounts are configured on the Guest Account page (UPAM- Guest Access - Guest Account).

- **Batch Account Creation -** Enable/Disable the batch Guest Account creation function on the Guest Account page.
- **Default Prefix For Account -** Enter a default prefix used for batch Guest Account creation.
- **Effective at First Login -** If enabled, the Guest Accounts created will begin their Validity Period the first time the user logs in. If disabled, the Validity Period begins when the Guest Account is created (Enabled/Disabled, Default = Disabled)
- **Access Code Length -** If Batch Account Creation is Enabled, you can set the Access Code Length for the created Guest Accounts (Range = 6 - 16, Default = 6).

Registration Strategy

Configure basic Guest Account Registration strategy.

- **Period Unit -** The unit used for the Account Validity Period Attribute (Days, Hours, Minutes).
- **Account Validity Period -** The length of time that Guest Accounts are valid. (Range = 1 – 365 Days, Default = 90 Days). You can customize the Guest Account Validity Period for a specific account on the Guest Account page (UPAM - Guest Access - Guest Account). However, the range you can set on the Guest Account page cannot be longer than the length set here. For example, if you set the Global Validity Period to 180 days, the longest period you will be able to set on the Guest Account page will be up to 180 days.

- **Guest Account Deletion Policy -** Configure how long expired Guest Accounts are retained before they are automatically deleted:
- **Never -** Guest Accounts will **not** be deleted at the end of the Account Validity Period (Default).
- **Immediately After Expiration -** Guest Accounts will be automatically deleted at the end of the Account Validity Period.
- **Set Days After Expiration -** Guest Accounts will be automatically deleted on the configured number of days after the end of the Account Validity Period (Range = 1 - 90). Note that you can click on the **Other Options** button to return to list of original options.
- **Remember Device -** Specify whether to remember the device MAC address and make it valid after successful authentication. If the remembered device is valid, the MAC address check will be performed first and the device allowed access without re-authentication.
- **Device Validity Period -** The length of time that the user device is valid. (Range = 1 – 365 Days, Default = 30 Days).
- **Max Device Number Per Account -** The maximum number of devices that can access the network with one single account. (Range = 1 – 500,000, Default = 10)

Data Quota

Specify the guest traffic quota for the Guest Strategy. The Administrator can customize the data quota for different guest when creating accounts.

Service Level

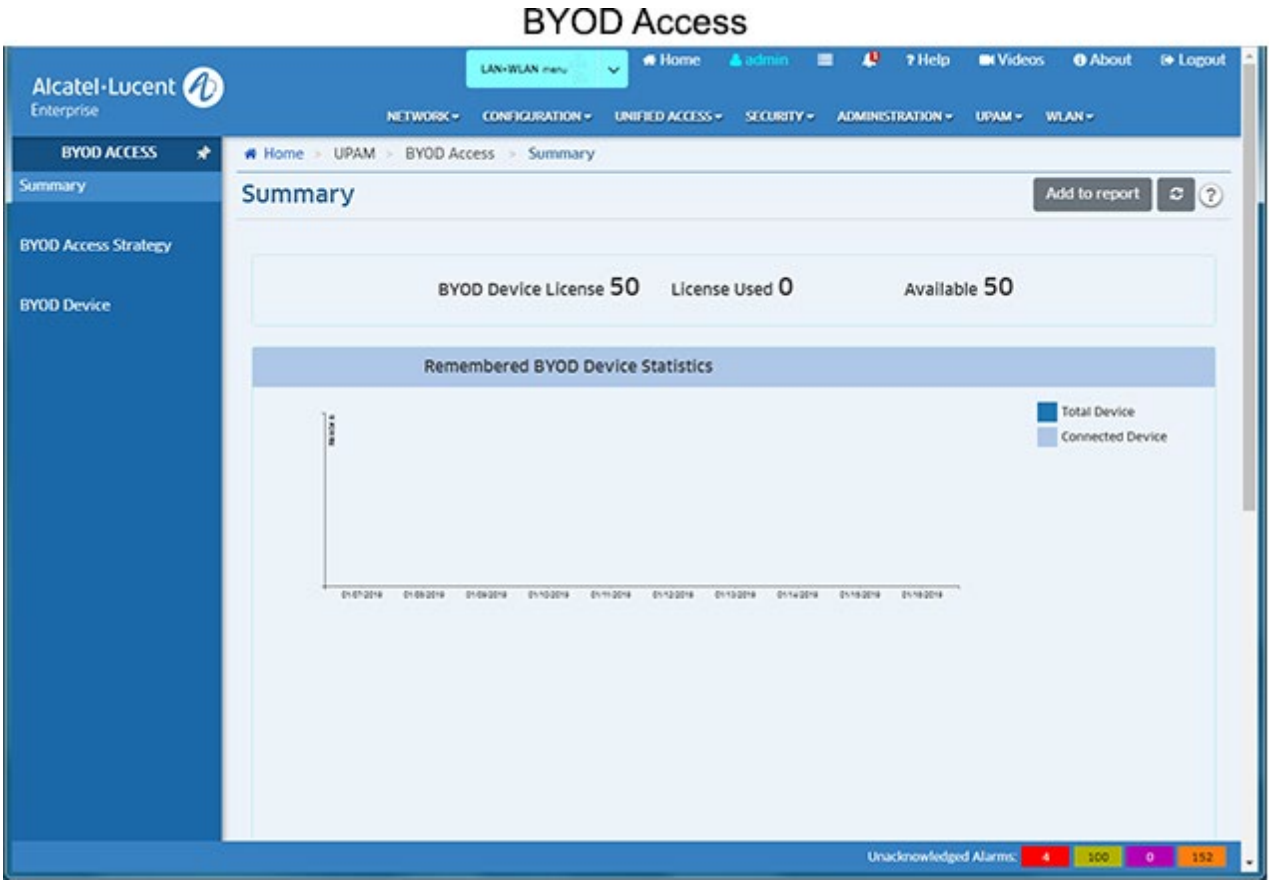
You can configure the different service levels for Guest Accounts by binding various levels of Access Roles and Policies. The Administrator can customize service level for different guest when creating account.

- **Enable Service -** Enables/Disables Service for the Level.
- **Service Name -** Service Name.
- **Access Role Profile -** Access Role Profile defined for the Service Level.
- **Policy List -** Policy List defined for the Service Level.
- **Data Quota -** Specify the guest traffic quota, in MB, for the Service Level.
- **Period Unit -** Specify the unit for account validity period attribute (Days, Hours, Minutes).
- **Account Validity Period -** The length of time that Guest Accounts are valid. (Range = 1 – 365 Days, Default = 90 Days). You can customize the Guest Account Validity Period for a specific account on the Guest Account page (UPAM - Guest Access - Guest Account). However, the range you can set on the Guest Account page cannot be longer than the length set here. For example, if you set the Global Validity Period to 180 days, the longest period you will be able to set on the Guest Account page will be up to 180 days.
- **Guest Account Deletion Policy -** The number of days after the Account Validity Period expires before Guest Accounts are automatically deleted:
- **Never -** Guest Accounts will **not** be deleted at the end of the Account Validity Period (Default).

- **Immediately After Expiration -** Guest Accounts will be automatically deleted at the end of the Account Validity Period.
- **Set Days After Expiration -** Guest Accounts will be automatically deleted on the configured number of days after the end of the Account Validity Period (Range = 1 - 90). Note that you can click on the **Other Options** button to return to list of original options.
- **Remember Device -** Specify whether to remember the device MAC address and make it valid after successful authentication. If the remembered device is valid, the MAC address check will be performed first and the device allowed access without re-authentication.
- **Device Validity Period -** The length of time that the user device is valid. (Range = 1 – 365 Days, Default = 30 Days).
- **Max Device Number Per Account -** The maximum number of devices that can access the network with one single account. (Range = 1 – 500,000, Default = 10).
- **Description -** Optional description for the Service Level.

BYOD Access

The UPAM BYOD Access application is used to manage employee BYOD devices. BYOD service is based on Captive Portal authentication.



The following screens are used to monitor and configure the BYOD Access application:

- **Summary -** Provides an overview of BYOD usage.

- **BYOD Access Strategy -** Used to configure access attributes for BYOD users.
- **BYOD Device -** Displays all authenticated online BYOD devices as well as all BYOD devices that were previously on the network and are stored in UPAM.

Summary

The BYOD Access Summary Screen provides an overview of BYOD usage.

- **BYOD License Information**
- **BYOD Device License -** Total number of BYOD Licenses available.
- **License Used -** Total number of BYOD Licenses used.
- **Available -** Currently available BYOD Licenses.
- **Remembered BYOD Device Statistics**
- **Total Device -** Total number of remembered BYOD devices.
- **Online Device -** Total number of online BYOD device.
- **Remembered BYOD Device Category -** Displays remembered BYOD information by device category (e.g., Computer. Mobile, Table) in a pie chart format.
- **Remembered BYOD Device Family -** Displays remembered BYOD information by device family (e.g., Alcatel Lucent Enterprise, Apple, IBM) in a pie chart format.

BYOD Access Strategy

The BYOD Access Strategy Screen is used to configure access attributes for BYOD users. The screen can be used to create, edit, and delete BYOD Access Strategies. There is a pre-configured Default BYOD Access Strategy that you can edit, or you can create new Guest Access Strategies (up to a maximum of 32).

Creating a BYOD Access Strategy

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

General

Configure redirect and authentication attributes.

- **Strategy Name -** Name of the BYOD access strategy.
- **Redirect Strategy -** Specify the captive portal page template to be used for BYOD service.
- **Mode -** The http protocol used to redirect the captive portal page (https/http).
- **IP/FQDN -** The displayed URL format for redirection to the captive portal page (FQDN/IP).
- **Current FQDN -** The FQDN used for the captive portal page redirection.
- **Authentication Source**
- **Local Database -** The employee account utilized for BYOD service is stored in the local database of UPAM.

- **External LDAP/AD -** The employee account utilized for BYOD service is stored in an external LDAP/AD Server (configured on the UPAM – Setting - LDAP/AD Configuration Screen).
- **External Radius -** The employee account utilized for BYOD service is stored in the local database of UPAM.
- **On-Premise LDAP -** The employee account utilized for BYOD service is stored in an on-premise LDAP/AD Server (configured on the Security - Authentication Servers - LDAP Screen). If selected, a private LDAP/AD Server is used instead of one in cloud for AP authentication. In this scenario, user authentication requests are communicated directly between an AP and the LADP/AD server and are not exposed in the public network.

Registration Strategy

Configure BYOD user account attributes.

- **Period Unit -** Select a unit for the Account and Device Validity Periods (Days, Hours, Minutes).
- **Remember Device -** Specify whether to remember the device MAC addresss and make it valid after authentication success (Enabled/Disabled). If the remembered device is valid, the MAC address check will be performed first and the device allooed access without re-authentication.
- **Expire Setting** - Specify the rules for remembered device.
- **Never Expire -** User remembered device will always be valid after authentication success.
- **Customization -** Customize the valid period for the remembered devices.

  Device Validity Period - Length of time that the guest user device is valid. Ranges and default values are shown below. (Range = 1 – 365, Default = 90, -1 = never expires)

  Max Device Number Per Account - Maximum number of devices that can access the network with one single guest account. (Range = 1 – 10, Default = 5)

Login Strategy

Configure BYOD user login.

- **Success Redirect URL**
- **Go Initially URL -** Redirect to the guest-user-input URL after passing authentication
- **Go Fixed URL -** Redirect to a fixed webpage specified by the Administrator.

Post Portal Authentication Enforcement

Configure post-authentication enforcement for BYOD users.

- **Fixed Access Role Profile -** The Access Role Profile assigned to the BYOD device after it is authorized.
- **Fixed Policy List -** The Policy List assigned to the BYOD device after it is authorized.

- **Other Attributes -** Select an attribute from the drop-down, enter a value and click on the Add icon to add the attribute. Repeat the process to add additional attributes.
- **Session Timeout -** The Session Timeout Interval is the - maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default = 43200)
- **Accounting Interim Interval -** Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 - 1200, Default = 600)
- **WISPr Bandwidth Max Up -** The user upstream bandwidth, in kbit/s. By default, it is not limited.
- **WISPr Bandwidth Max Down -** The user downstream bandwidth, in kbit/s. By default, it is not limited.

Editing a BYOD Access Strategy

Select a strategy in the Guest Access Strategy List and click on the Edit icon. Edit any fields as described above and click on the **Apply** button. Note that you cannot edit the Strategy Name.

Deleting a BYOD Access Strategy

Select a strategy in the Guest Access Strategy List and click on the Delete icon. Click **OK** at the Confirmation Prompt. You cannot delete the Default BYOD Access Strategy.

BYOD Device

The BYOD Access BYOD Device Screen displays all authenticated online BYOD devices as well as all BYOD devices that were previously on the network and are stored in UPAM.

Online Device List

The Online Device List displays all authenticated online BYOD devices.

Basic Info

- **Account Name -** User name of the employee account. For MAC authentication, Account Name will be device MAC.
- **Device MAC -** MAC address of the employee device.
- **Client IPv4 -** IPv4 address of the employee device.
- **Client IPv6 -** IPv6 address of the employee device.
- **Remembered -** Indicates whether the online device was stored by UPAM and added into the BYOD remembered list. A remembered item can be utilized for MAC authentication.
- **Device Category -** Category of the BYOD device:
  - Computer
  - Mobile
  - Tablet
  - Game console
  - Digital media receiver

    - Others
- **Device Family -** Production vendor of the BYOD device:
    - Alcatel-Lucent Enterprise
    - Apple
    - Samsung
    - Huawei
    - Microsoft
    - LG
    - Lenovo
    - HP
    - IBM
    - Nokia
    - MI
    - HTC
    - Sony
    - Blackberry
    - Others
- **Device OS -** OS running o**n** the BYOD device
    - Linux
    - Windows
    - MacOS
    - Android
    - IOS
    - Others
- **Authentication Type -** Authentication type from the user requesting access, including: MAC authentication and Captive Portal authentication
- **Auth Resource -** User profile database used in the authentication, including: None, Local Database, LDAP/AD and external RADIUS server.
- **Authentication Strategy -** Authentication strategy applied to the BYOD device.
- **Access Policy -** Access Policy that the BYOD device matches.
- **Session Start -** The date and time when the device connection session was created.
- **Access Role Profile -** Access Role Profile applied to the BYOD device.
- **Final Access Role Profile -** Access Role Profile assigned to the BYOD device by NAS, before the Access Role Profile returned by UPAM.
- **Policy List -** Policy List applied to the BYOD device.
- **Redirect URL -** Redirect URL returned to the BYOD device by UPAM.

Authenticate

- **Access Device MAC -** MAC address of the NAS to which the BYOD device is attached.

- **Access Device Name -** System name of the NAS to which the BYOD device is attached
- **Access Device SSID -** Wireless service broadcast by the NAS and used for connection to the BYOD device (only valid for wireless access).
- **Access Device Location -** Location of the NAS.
- **Called Station ID -** Allows the NAS to send the phone number that the user called in the Access-Request packet, using Dialed Number Identification (DNIS) or similar technology.

  For Switch - The switch MAC Address

  For AP - radio_MAC_address:SSID_NAME
- **NAS Port Type -** The type of physical port on the NAS that authenticated the device

  Wireless-IEEE 802.11

  Ethernet
- **NAS Port -** The physical port number of the NAS which authenticated the device.

  For Switch - if index

  For AP - Wireless radio index
- **NAS Port ID –** Port of the NAS that authenticated the device. The attribute can be configured on the Unified Access - Unified Profile – Template - AAA Server Profile Screen

  For Switch - Chassis/slot/port

  For AP - WLAN service
- **NAS ID -** NAS identifier, identifying the NAS originating the Access-Request. (Can be configured on the Unified Access - Unified Profile – Template - AAA Server Profile Screen)
- **NAS IP Address -** IP Address of the NAS
- **Slot Port -** Port number on the switch slot to which the device is connected (only for wired access).
- **Port Desc/Wlan Service**

  For Switch: Port description

  For AP: WLAN service
- **Framed MTU -** Maximum Transmission Unit to be configured for the user, when it is not negotiated by some other means (e.g., PPP). It is a fixed value = 1400.
- **Reject Reason -** Reason for rejecting the request from the BYOD device:

  Overdue license

  Invalid username or password

  Cannot match access policy according to the authentication request

Account

- **Acct Status Type -**Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop). Values: Start (1), Stop (2), Interim-Update (3), Accounting-On (7) Accounting-Off (8).

- **Acct Session Time -** Indicates how many seconds the user has received service, and can only be present in Accounting-Request records where the Acct Status Type is set to Stop.
- **Acct Session ID -** A unique Accounting ID that makes it easy to match start and stop records in a log file. The start and stop records for a given session MUST have the same Acct Session ID.
- **Termination Action -** Fixed with “Radius-Request”. When the session is timeout, user needs to be re-authenticated.
- **Session Timeout -** Maximum number of seconds of service provided prior to session termination.
- **Acct Interim Interval -** Number of seconds between each interim update for this specific session.
- **Tunnel Private Group ID -** Used to support the legacy VLAN assignment from RADIUS (ID=VLAN ID).
- **Acct Terminate Cause -** Indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

  1 - User Request: User logout

  4 - Idle Timeout: User activity logout (only applicable for MAC based or Captive Portal users)

  6 - Admin Reset: Operator logout/flush operation

  7 - Admin Reboot: Operator reboot operation

  8 - Port Error: Port down, NI down

  9 - NAS-Error: Any software notification that the user is no longer authenticated

Remembered Device List

The Remembered Device List displays all authenticated BYOD devices saved in UPAM and can be utilized for MAC authentication.

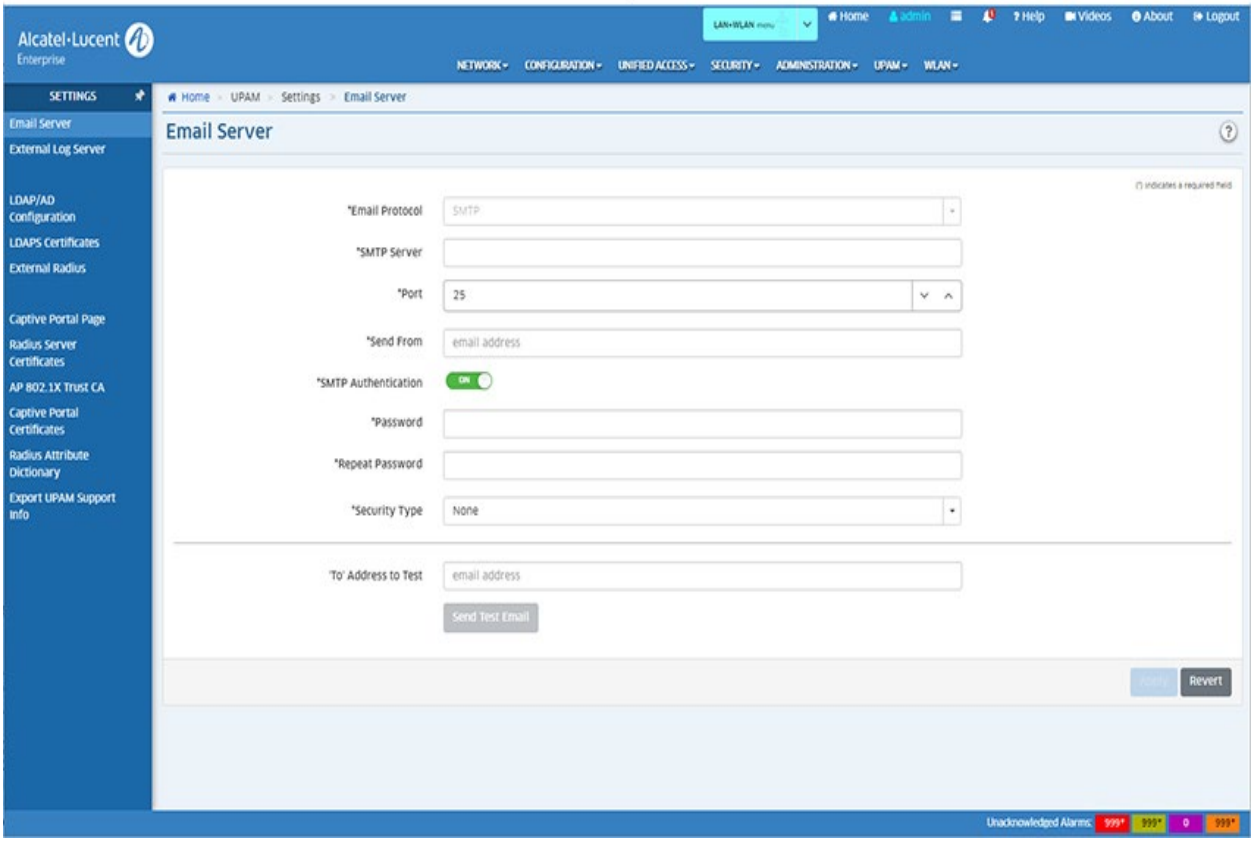
- **Employee Account -** The account used for login by the BYOD device
- **Device MAC -** MAC address of the BYOD device
- **Device Category -** Category of the BYOD device:
- Computer
- Mobile
- Tablet
- Game console
- Digital media receiver
- Others
- **Device Family -** Production vendor of the BYOD device:
- Alcatel-Lucent Enterprise
- Apple
- Samsung
- Huawei
- Microsoft

- LG
- Lenovo
- HP
- IBM
- Nokia
- MI
- HTC
- Sony
- Blackberry
- Others
- **Device OS -** OS running on the BYOD device.
- Linux
- Windows
- MacOS
- Android
- IOS
- Others
- **Browser Type -** Browser of the BYOD device
- **Activity Status -** Indicates whether the BYOD device is online or offline.
- **Expire Time -** The expiration time of the BYOD device. When it is expired, the device will be deleted from the BYOD remembered list in UPAM.
- **Remembered Time -** Date and time when the BYOD device was first connected to the network.
- **Last Access Time –** Date and time when the BYOD device latest accessed the network.
- **Last Access Device Location -** Location of the NAS that the BYOD device last accessed.
- **Last Access Device MAC -** MAC address of the NAS that the BYOD device last accessed.
- **Last Access Device Name -** System Name of the NAS that the BYOD device last accessed.
- **Last Access Device SSID -** SSID of the NAS that the BYOD device last accessed.
- **Web Access Strategy -** The Access Strategy used for the device. One device can login through multiple BYOD Access Strategies.
- **Remember Method -** Indicates whether the device was manually added to the list (Static) or automatically added through Captive Portal Authentication (Auto).
- **Active Status -** Indicates whether the remembered device was ever logged into the network. " Active" means the device was. at one time, logged into the network. Inactive means the device was manually added, but never logged into the network. Only " Active" devices consume a BYOD license.

Settings

The UPAM Settings application is used to configure UPAM components (e.g., Email Server, External Log Server, External RADIUS Server).

UPAM Settings



The following screens are used to monitor configure the Settings application:

- **Email Server -** Used to configure the integrated UPAM Email client function.
- **External Log Server -** Used to configure a connection to an external server to collect UPAM authentication logs.
- **LDAP/AD Configuration -** Used to configure a connection to an LDAP Server for UPAM.
- **LDAPS Certificates -** Used to configure a LDAPS Certificates. An LDAPS Certificate is used for secure communication between UPAM and the LDAP Sever.
- **External RADIUS -** Used to configure an External RADIUS Server for UPAM.
- **Captive Portal Page -** Used to configure the UPAM Captive Portal Page.
- **Additional Trust CA -** Used to configure a UPAM RADIUS Server Certificate for 802.1X authentication of an 802.1X AP device.
- **Captive Portal Certificates -** Used to configure Captive Portal Certificates. A Captive Portal Certificate is used to implement the HTTPS login when UPAM is used as a Captive Portal Server.
- **RADIUS Server Certificates -** Used to configure UPAM RADIUS Server Certificates.

- **RADIUS Attribute Dictionary -** Displays all RADIUS Attributes stored on the RADIUS Server and is used to configure attributes

Email Server

The Setting Email Server Screen is used to configure the integrated UPAM Email client function. When the email server parameters are configured, UPAM can act as a client to send system-defined emails to specific users:

- UPAM will send emails to guest user to notify their credentials for login.
- UPAM will send emails with approve link to administrator or employee for authorization.

Configuring the Email Server

Complete the fields as described below and click on the **Apply** button. To edit the email server configuration, update the field(s) and click the **Apply** button.

- **Email Protocol -** The protocol used to send emails. By default, SMTP protocol is used.
- **Service URL -** The URL of the email sever used to send system-defined emails.
- **Port -** TCP port used for mail transmission.
- **Send From -** Email account used to log into the email server and send system-defined emails (10 – 64 characters)
- **SMTP Authentication -** Enable(On)/Disable (Off) SMTP authentication. If enabled, SMTP will be allowed without authentication to accommodate e-mail servers that internally relay e-mail without a password.
- **Password -** Email password used log into the email server and send system-defined emails. (8 – 64 characters)
- **Repeat -** Re-enter to confirm the password.
- **Security Type -** Encryption method used in the connection between UPAM and the email server.
- **None -** No encryption method is used in the connection.
- **SSL -** Secure Socket Layer encryption method is used in the connection.
- **TLS -** Transport Layer Security encryption method is used in the connection.
- **'To' Address to Test -** A test account used to receive the system-defined email to verifying the email server configuration.
- **Send Test Email -** Click to send a test email.

External Log Server

The Setting External Log Server Screen is used to configure a connection to an external server to collect UPAM authentication logs. By default, Authentication Logs are stored in UPAM for one month. To retain historical logs generated by UPAM, configure an external server.

Configuring the External Log Server

Complete the fields as described below and click on the **Apply** button. To edit the external Log Server configuration, update the field(s) and click the **Apply** button.

- **Send Log to External Server -** Enables/Disables sending logs to an external server.
- **Server Type**
- **Database-MySQL -** External MySQL server
- **Database-MSSQL -** External Microsoft SQL server
- **Syslog -** External syslog server
- **Host Name/IP Address -** IP address of the external server.
- **Backup Host Name/IP Address -** IP address of backup server, if applicable.
- **Port -** TCP/UDP port that UPAM will use to communicate with the external server. (Range = 1 – 65535)
- **Username -** Username that UPAM will use to communicate with the external server. (1 - 64 characters)
- **Password -** Password that UPAM will use to communicate with the external server. (6 - 64 characters)
- **Repeat -** Re-enter to confirm the password.
- **DB Name –** Name of the external server. <3-64 characters>

Note: After configuring the server, you can click on the **Test Connection** button to test the connection from UPAM to the server. A message will appear indicating whether or not the connection was successful.

LDAP/AD Configuration

The Settings LDAP/AD Configuration Screen is used to configure a connection to an LDAP Server or an Active Directory (AD) Server (Windows NT LAN Manager - NTLM) for UPAM.

Configuring an LDAP Server

Enable the **LDAP/AD Server** field, complete the fields as described below and click on the **Apply** button. To edit the configuration, update the field(s) and click the **Apply** button.

- **Server Name -** Pre-filled with “Default Server” (cannot be modified).
- **Server Type -** Select LDAP.
- **Host Name/IP Address -** LDAP Server host name/IP address. (4 - 64 characters)
- **Backup Host Name/IP Address -** Backup LDAP server host name/IP address, if applicable. (4 - 64 characters)
- **Retries -** Number of times UPAM will attempt to reconnect to the LDAP server when the connection timeout occurs before concluding that the LDAP server is unreachable. (range = 1 – 3, Default = 3)
- **Timeout -** The amount of time, in seconds, that UPAM will attempt a connection to the LDAP server before timing out. (Range = 1 - 30, Default = 5)
- **TLS -** Select a TLS encryption type from the drop-down:
    - **NS -** Non-secure encryption between UPAM and the LDAP Server.
    - **LDAPS -** Use LDAPS protocol as the secure communication method between UPAM and the LDAP Server.
    - **Start TLS Extension -** Use Start TLS Extension mechanism as the secure communication method between UPAM and the LDAP Server.

- **Certificate for TLS -** Select an LDAP Certificate from the drop-down. You can also click on the "Add New" link to go to the LDAPS Certificate Screen and create a new certificate.
- **Port -** TCP/UPD port used by UPAM to communicate with the LDAP server (1 – 65535, Default - 389, Default for TLS = 636).
- **Admin Name -** Administrator account used to login into the LDAP server. Format: cn=,DC= (8 - 64 characters).
- **Admin Password -** Administrator password used to login into the LDAP server. (1 - 32 characters)
- **Search Base -** The starting point for the search in the LDAP server directory tree.
- **Username Attribution -** The field in an LDAP entry that represents the username used for authentication. (1 - 32 characters)
- **Password Attribution -** The field in an LDAP entry that represents the password used for authentication. (1 - 128 characters)
- **Object Class -** Define named collections of attributes and classify them into sets of required and optional attributes. (1 - 32 characters)

Note: You can click on the **Test Connection** button to verify the configuration. A message will appear indicating whether or not the connection was successful.

Configuring Active Directory Authentication

Enable the **LDAP/AD Server** field, complete the fields as described below and click on the **Apply** button. To edit the configuration, update the field(s) and click the **Apply** button.

- **Server Name -** Pre-filled with “Default Server” (cannot be modified).
- **Server Type -** Select AD.
- **TLS -** Select a TLS encryption type from the drop-down:
- **NS -** Non-secure encryption between UPAM and the LDAP Server.
- **LDAPS -** Use LDAPS protocol as the secure communication method between UPAM and the LDAP Server.

  Certificate for TLS - Select an LDAP Certificate from the drop-down. You can also click on the "Add New" link to go to the LDAPS Certificate Screen and create a new certificate.
- **Start TLS Extension -** Use Start TLS Extension mechanism as the secure communication method between UPAM and the LDAP Server.
- **Netbios Domain Name -** The Netbios Domain Name of the Domain Controller which is used to perform authentication.
- **DNS Domain Name -** The DNS Domain Name of the Domain Controller which is used to perform authentication
- **FQDN/IP Address of Domain Controller -** The FQDN/IP address of the AD Server.
- **Username -** Username used to access the AD Server.
- **Password -** Password used to access AD Server.
- **AD Port -** Port used to access the AD Server.

Note: You can click on the **Test Connection** button to verify the configuration. A message will appear indicating whether or not the connection was successful.

LDAPS Certificates

The Settings LDAPS Certificates Screen displays about all configured LDAPS Certificates and is used to create and delete LDAPS Certificates. You can also download an imported certificate. The LDAPS Certificate is used for secure communication between UPAM and the LDAP Sever. UPAM will use the LDAPS Certificate to establish an encrypted connection with the LDAP Server.

Creating an LDAPS Certificate

Click on the Add icon to bring up the Create LDAPS Server Certificates Screen. Click on the **Upload** button to upload a **CA File,** then click on the **Import** button to import the file into UPAM. Repeat the process to upload and import the **Server File** and **Server Key File**.

Enter a **Name** for the Certificate and **Private Key Password** to encrypt the key file when generating the CA File, then click on the **Create** button. After creating the file, select the file in the RADUIS Server Certificates List and click on the **Download** button to download the file to the RADIUS Server. The certificate can now be activated.

Note: If you use the default certificate, the password is "password".

Activating an LDAPS Certificate

Select a certificate in the LDAPS Certificates List and click on the **Activate** button. You can have only one active certificate at a time. If you activate a new certificate, it replaces the previously-activated certificate.

Deleting an LDAPS Certificate

Select a user and click on the Delete icon, then click **OK** at the Confirmation Prompt.

LDAPS Certificates List

The LDAPS Certificate List displays information about all imported LDAPS Certificates.

- **Name -** Identifier for the certificate item in UPAM.
- **CA File Name -** The name of the CA file uploaded.
- **Server File Name -** Name of certificate file.
- **Key File Name -** Name of Key File.
- **Issued By -** The certification authority (CA) that issued the certificate.
- **Issued To -** The entity to which the certificate is assigned.
- **Validity Start Time -** The start date and time when the certificate is valid.
- **Validity Stop Time -** The end date and time when the certificate is valid.
- **Using Status -** Indicates whether the certificate is effective. Can be activated by the administrator.
- **Expiry Status -** Indicates whether the certificate is Expired or Unexpired.

External RADIUS

The Setting External RADIUS Screen displays information about all configured UPAM External RADIUS Servers and is used to create, edit, and delete a server.

Configuring an External RADIUS Server

Complete the fields as described below and click on the **Apply** button. To edit the External RADIUS Server configuration, update the field(s) and click the **Apply** button.

- **Server Name -** Pre-filled with “Default Server” (cannot be modified).
- **Host Name/IP Address -** External Radius Server host name/IP address (4 - 64 characters)
- **Back Host Name/IP Address -** Back up external radius server host name/IP address, if applicable (4 64 characters)
- **Retries -** Number of times UPAM will attempt to reconnect to the External Radius Server when the connection timeout occurs before concluding that the External Radius Server is unreachable. (range = 1 – 3, Default = 3)
- **Timeout -** The amount of time, in seconds, that UPAM will attempt a connection to the External Radius Server before timing out. (Range = 1 – 30, Default = 5)
- **Shared Secret -** Shared key that UPAM uses to communicate with External Radius Server. (4 - 64 characters)
- **Confirm Secret –** Re-enter to confirm the shared secret key. (4 - 64 characters)
- **Authentication Port -** TCP/UDP port used to perform authentication. (Range – 1 – 65535, Default = 1812)
- **Accounting Port -** TCP/UDP port used to perform accounting. (Range – 1 – 65535, Default = 1813)

Editing an External RADIUS Server

Select a server in the External RADUIS List and click on the Edit icon. Edit the fields as described above, then click on the **Apply** button.

Deleting an External RADIUS Server

Select a server(s) in the External RADUIS List and click on the Delete icon. Click on **OK** at the Confirmation Prompt.

External RADUIS List

The External RADIUS Server List displays information about all configured UPAM External RADIUS Servers.

- **Server Name -** Pre-filled with “Default Server” (cannot be modified).
- **Host Name/IP Address -** External Radius Server host name/IP address (4 - 64 characters)
- **Back Host Name/IP Address -** Back up external radius server host name/IP address, if applicable (4 - 64 characters)
- **Retries -** Number of times UPAM will attempt to reconnect to the External Radius Server when the connection timeout occurs before concluding that the External Radius Server is unreachable. (range = 1 – 3, Default = 3)
- **Timeout -** The amount of time, in seconds, that UPAM will attempt a connection to the External Radius Server before timing out. (Range = 1 – 30, Default = 5)
- **Authentication Port -** TCP/UDP port used to perform authentication. (Range – 1 – 65535, Default = 1812)

- **Accounting Port -** TCP/UDP port used to perform accounting. (Range – 1 – 65535, Default = 1813)

Captive Portal Page

The Setting Captive Portal Page is presented to the user for Guest and BYOD login.
The Captive Portal Page Screen displays all configured Captive Portal Pages and is used to create, edit, and delete Captive Portal Pages. There is a system-defined page template in UPAM called “Default Portal”, which can be used and customized, or you can create a new portal page template and customize it.

Creating a Captive Portal

Click on the Add icon to bring up the Create Captive Portal Screen. Complete the fields as described below then click on the **Create** button to create a template. Once you have created the basic template, you can customize the page with different images and welcome messaging as described below. The web page will automatically adjust the display size according to the device type (e.g., computer screen, smart phone screen).

- **Page Name -** Name for the template.
- **Template Name -** Select a layout from the drop-down menu for the Welcome Layout and Success Layout pages. There are six system-defined layouts to choose from, as well as a European Union (EU) WiFi layout. When you select a layout, the pages are previewed at the bottom of the screen.
- **Description -** Enter an optional description for the template.

Editing a Captive Portal Page

Select a Captive Portal Page in the Captive Portal Pages List and click on the Edit icon. Edit the fields as described above and click on the **Apply** button. You can also customize the page after editing.

Deleting a Captive Portal Page

Select a Captive Portal Page in the Captive Portal Pages List and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Customizing a Captive Portal Page

To customize a Captive Portal page, click on the page in the Captive Portal Pages List, then click on the **Customization** button at the top of the screen to bring up the User Customization Screen. Customize one or both of the pages as described below. When you are finished, click on the **Apply** button.

After customizing the page(s), you can click on the **Welcome Preview** button to preview the customized Welcome Page or the **Success Preview** button to preview the customized Success Page.

Edit the Welcome Layout

- **Logo Panel**
  - **Upload Picture -** Click on the **Browse** button to locate a background image for the Logo area at the top of the screen.

  - **Linked URL -** Enter a URL to link to a background image for the Logo area at the top of the screen.
- **Function Panel**
  - **Upload Picture -** Click on the **Browse** button to locate a background image for the Function area at the bottom of the screen.
  - **Opacity Setting -** Use the slider to set the opacity of the Function color (slider ranges from 1 - Dark to 10 - Light).
  - **Function Color -** Enter the background color for the Function area of the page (where the user enters username, login).
- **Advertisement Picture Panel** (available if included as part of the selected Captive Portal Page Layout)
  - **Upload Picture -** Click on the **Browse** button to locate a background image for the “Advertisement” area.
- **Advertisement Broadcast Panel** (available if included as part of the selected Captive Portal Page Layout)
  - **Upload Picture -** Click on the **Browse** button to locate a background image for the “Broadcast” area.
- **Advertisement Video Panel** (available if included as part of the selected Captive Portal Page Layout)
  - **Upload Video -** Click on the **Browse** button to locate a video file for the “Video” area.

Edit the Success Layout

- **Logo Panel**
  - **Upload Picture -** Click on the **Browse** button to locate a background image for the Logo area at the top of the screen.
  - **Linked URL -** Enter a URL to link to a background image for the Logo area at the top of the screen.
- **Function Panel**
  - **Upload Picture -** Click on the **Browse** button to locate a background image for the Function area at the bottom of the screen.
  - **Opacity Setting -** Use the slider to set the opacity of the Function color (slider ranges from 1 - Dark to 10 - Light).
  - **Function Color -** Enter the background color for the Function area of the page (the "results" area on the screen).
- **Advertisement Picture Panel** (available if included as part of the selected Captive Portal Page Layout)
  - **Upload Picture -** Click on the **Browse** button to locate a background image for the “Advertisement” area.
- **Advertisement Broadcast Panel** (available if included as part of the selected Captive Portal Page Layout)
  - **Upload Picture -** Click on the **Browse** button to locate a background image for the “Broadcast” area.
- **Advertisement Video Panel** (available if included as part of the selected Captive Portal Page Layout)

- **Upload Video -** Click on the **Browse** button to locate a video file for the "Video" area.

RADIUS Server Certificates

The Setting RADIUS Server Certificates Screen displays information about all RADIUS Server Certificates and is used to add, activate, and delete a certificate in the RADIUS Server in UPAM for 802.1X or TLS authentication. You can also download an imported certificate to your computer.

Adding a Certificate

Click on the Add icon to bring up the Create RADIUS Server Certificates Screen. Click on the **Upload** button to upload a **CA File**, then click on the **Import** button to import the file into UPAM. Repeat the process to upload and import the **Server File** and **Server Key File**.

Enter a **Name** for the Certificate and a **Private Key Password** to encrypt the key file when generating the Server File, then click on the **Create** button. The certificate can now be activated.

Note: If you use the default certificate, the password is "password".

Note: If necessary, you can generate a new RADIUS Server Certificate.

Activating a Certificate

Select a certificate in the RADIUS Server Certificates List and click on the **Activate** button. You can have only one active certificate at a time. If you activate a new certificate, it replaces the previously-activated certificate.

Deleting a Certificate

Select a Certificate in the RADIUS Server Certificates List and click on the Delete icon. Click **OK** at the Confirmation Prompt. Note that you cannot delete an active certificate. You must first activate a different certificate before you can delete it.

Downloading a Certificate

You can download an imported certificate from the RADIUS Server Certificates List to your machine. Select the certificate in the list and click on the **Download** button. The certificate will be downloaded to your designated Download folder.

Generating a Certificate

Follow the steps below to generate a RADIUS Server Certificate.

1. Generate the root key: *openssl genrsa -out rootCA.key 2048*.

2. Generate the root CA certificate: *openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 3560 -out rootCA.pem*.

3. Generate a private Key for RADIUS: *openssl genrsa -des3 -out radius_server.key 2048* (enter password "switch" or any desired password).

4. Generate a CSR (Certificate Signing Request): *openssl req -new -key radius_server.key -out radius_server.csr -sha256*.

5. Sign and generate RADIUS certificate using the root CA key created at the Step 1: *openssl x509 -req -in radius_server.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out radius_server.crt -days 3560 -sha256*.

6. Add and activate the certificate.

RADIUS Certificate List

The RADIUS Certificate List displays information about all imported RADIUS Certificates.

- **Name -** Identifier for the certificate in UPAM.
- **CA File Name -** The name of the uploaded CA Certificate file.
- **Server File Name -** The name of certificate file in the RADIUS server. The Server File contains the contents of the Sever Certificate file and the Server Key file.
- **Type -** The type of certificate file stored in the RADIUS server.
- **Issued By -** The certification authority (CA) that issued the certificate.
- **Issued To -** The entity to which the certificate is assigned.
- **Validity Start Time -** The start date and time when the certificate is valid.
- **Validity Stop Time -** The end date and time when the certificate is valid.
- **Using Status -** Indicates whether the certificate is effective in the RADIUS server. Can be activated by administrator.
- **Expiry Status -** Indicates whether the certificate is Expired or Unexpired.

Additional Trust CA

The Settings Additional Trust CA Screen displays information about all AP 802.1x Trust CA certificates and is used to add, trust, and delete a certificate in the UPAM RADIUS Server for client authentication and/or AP as an 802.1X client authentication. You can also download an imported certificate to your computer.

Adding a Certificate

There is a "Built-in_CA" certificate file that is available to use by default and appears in the list of certificates on the Additional Trust CA Screen. If using this certificate for AP 802.1x authentication, there is no need to add a custom certificate file. However, if you want to add your own custom certificate file, complete the following steps to add the file to the UPAM RADIUS Server:

1. Click on the Add icon to bring up the Create Additional Trust CA Screen.

2. Click on the **Upload** button to upload a **CA File**, then click on the **Import** button to import the file into UPAM.

3. Enter a **Name** for the Certificate, then click on the **Create** button. The certificate is now available and appears in the list of certificates on the Additional Trust CA Screen.

Note: When using the "Built_in_CA" certificate file or a custom certificate file, make sure the AP Group to which the AP 802.1x client belongs has the 802.1x Supplicant option enabled and specifies the same certificate file.

Trust a Certificate

The "Built_in_CA" certificate file is trusted by default. However, custom certificate files are untrusted by default. To trust a custom certificate, select the custom certificate in the Additional Trust CA List and click on the **Trust** button. The Result Screen displays the results of the trust operation. Click the **OK** button to close the Result Screen and return to the Additional Trust CA List.

Deleting a Certificate

Select a certificate in the Additional Trust CA List and click on the Delete icon. Click **OK** at the Confirmation Prompt. Note that you cannot delete the "Built_in_CA" certificate or a trusted custom certificate. You must first untrust a custom certificate before you can delete it.

Downloading a Certificate

You can download an imported certificate from the Additional Trust CA List to your machine. Select the certificate in the list and click on the **Download** button. The certificate will be downloaded to your designated Download folder.

Additional Trust CA List

The Additional Trust CA List displays information about all of the imported Trust Certificates.

- **Name -** Identifier for the certificate in UPAM.
- **CA File Name -** The name of the uploaded CA Certificate file.
- **Issued By -** The certification authority (CA) that issued the certificate.
- **Issued To -** The entity to which the certificate is assigned.
- **Validity Start Time -** The start date and time when the certificate is valid.
- **Validity Stop Time -** The end date and time when the certificate is valid.
- **Status -** Indicates the trust status for the certificate (Trust or UnTrust).

Captive Portal Certificates

The Setting Captive Portal Certificates Screen displays information about all Captive Portal Certificates and is used to add, activate, edit, delete, certificates. Captive Portal Certificates are utilized to implement the https login when UPAM is used as a Captive Portal server. During authentication, the certificate is used to establish the SSL secure connection between the client and UPAM. UPAM provides a default certificate with the specific redirect URL of the Captive Portal page. You can customize the portal page redirect URL, and upload and activate a custom certificate.

Adding a Certificate

Click on the Add icon to bring up the Create Captive Portal Certificates Screen. Click on the **Upload** button to upload a **Server Certificate File**, then click on the **Import** button to import the file into UPAM. Repeat the process to upload and import the **Server Key File**.

Enter a **Name** for the Certificate, a **Private Key Password** to encrypt the key file when generating the Server File and enter a **Selected FQDN**. Click on the **Create** button. The certificate can now be activated.

Notes:

- The Certificate Files only support PEM or DER encoded certificates (e.g., .pem., .cer, .der, .crt).
- If the certificate has a long certificate chain, please include them all in the .crt file. The order should be the root certificate at the start, the intermediate certificates in the middle, and the user's certificate at the end. To find out which certificates are which, please contact your certificates vendor.
- If you use the default certificate, the password is "password".
- If necessary, you can generate a new Captive Portal Certificate.

Activating a Certificate

Select a Certificate in the Captive Portal Certificates List and click on the **Activate** Button. You can only have one active certificate. If you activate a new certificate, it replaces the previously-activated certificate.

Editing a Certificate

You can edit the Selected FQDN for a certificate. Select a Certificate in the Captive Portal Certificates List and click on the Edit icon. Edit the Selected FQDN field and click **Apply**.

Deleting a Certificate

Select a Certificate in the Captive Portal Certificates List and click on the Delete icon. Click **OK** at the Confirmation Prompt. Note that you cannot delete an active certificate. You must first activate a different certificate before you can delete it.

Generating a Certificate

Follow the steps below to generate a Captive Portal Certificate.

1. Generate the root key: *openssl genrsa -out rootCA.key 2048.*

2. Generate the root CA certificate: *openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 3560 -out rootCA.pem*.

Note: Please ignore Steps 1 and 2 if you have a Root CA.

3. Generate a private Key for Captive Portal: *openssl genrsa -des3 -out cp_server.key 2048* (enter password "switch" or any desired password).

4. Generate a CSR (Certificate Signing Request): *openssl req -new -key cp_server.key -out cp_server.csr sha256*. You must provide the ULR of Captive Portal in the FQDN field, as shown in the example below.

```
C:\OpenSSL-Win64\bin>openssl req -new -key cp_server.key -out cp_server.csr -sha256
Enter pass phrase for cp_server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:VN
State or Province Name (full name) [Some-State]:D12
Locality Name (eg, city) []:HCM
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TMA
Organizational Unit Name (eg, section) []:OVSUS
Common Name (e.g. server FQDN or YOUR name) []:ov2500-upam-cportal.al-enterprise.com
Email Address []:pitnhan@tma.com.vn

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:switch
An optional company name []:TMA
```

5. Provide the DNS name and IP address in the v3.ext file using the commands shown below:

v3.ext

```
1  authorityKeyIdentifier=keyid,issuer
2  basicConstraints=CA:FALSE
3  keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
4  subjectAltName = @alt_names
5
6  [alt_names]
7  DNS.1 = ov2500-upam-cportal.al-enterprise.com
8  IP.1 = 192.168.71.123
9  IP.2 = 192.168.71.124
```

cat > v3.ext <<-EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names
[alt_names]
DNS.1=<replace-with-FQDN>
IP.1=<IP address>
IP.2=<IP address - if more than one IP>
EOF

6. Sign and generate the Captive Portal Certificate using the Root CA key created at Step 1 and the v3.ext file created at Step 5: *openssl x509 req -in cp_server.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out cp_server.crt -days 3560 sha256 -extfile v3.ext.*

7. Add and activate the certificate.

Captive Portal Certificates List

The Captive Portal Certificates List displays information about all imported RADUIS Certificates.

- **Name -** Identifier for the certificate item in UPAM.
- **CA File Name -** The name of the CA file uploaded.
- **Server File Name -** The name of certificate file in the RADIUS server.
- **Key File Name -** The name of the Key File uploaded.
- **Issued By -** The certification authority (CA) that issued the certificate.
- **Issued To -** The entity to which the certificate is assigned.
- **Validity Start Time -** The start date and time when the certificate is valid. **Validity Stop Time -** The end date and time when the certificate is valid.
- **Using Status -** Indicates whether the certificate is effective in the RADIUS server. Can be activated by administrator.
- **Expiry Status -** Indicates whether the certificate is Expired or Unexpired.
- **Selected FQDN -** The FQDN presented in the captive portal redirect URL instead of captive portal server IP address.

RADIUS Attribute Dictionary

The Setting RADIUS Attribute Dictionary Screen displays all RADIUS Attributes stored on the RADIUS Server and is used to add, edit, and delete attributes. The RADIUS Attribute Dictionary Feature enables UPAM to integrate with other vendor's network infrastructure, and allows UPAM to act as a RADIUS Server to authenticate user requests from Third-Party devices.

> **Note:** Click on the **Sync to RADIUS** button to add any custom attributes you have created to the RADIUS Server. The server will restart after the sync.

Adding a RADIUS Attribute

Click on the Add icon, complete the fields as described below, then click on the **Create** button to add a RADIUS Attribute.

- **Vendor -** Select a vendor (IETF, Alcatel, Other)
- **Vendor Name -** The vendor name (pre-filled for IETF and Alcatel).
- **Vendor ID -** The vendor ID ((pre-filled for IETF and Alcatel).
- **Radius Attribute Name -** Select a Radius attribute for IETF or Alcatel from the drop-down. For other vendors, enter the attribute name.
- **Attribute Code -** The attribute code is automatically populated if the Radius Attribute Name is selected from the drop-down list. Otherwise, it needs to be manually entered (Attribute code of same vendor is not repeatable).
- **Value Type -** The type of value allowed for the attribute.
- **Available In -** The configuration step in which the attribute can be applied.
- **Access Policy -** The attribute can be utilized for Access Policy configuration.
- **Authentication Enforcement Policy -** The attribute can be utilized for Authentication Enforcement Policy configuration.
- **Radius-DM -** The attribute can be utilized for NAS Client configuration.

Editing a RADIUS Attribute

Select an attribute in the RADIUS Attribute Dictionary List and click on the Edit icon. Edit any necessary fields as described above, then click on the **Apply** button.

Deleting a RADIUS Attribute

Select an attribute(s) in the RADIUS Attribute Dictionary List and click on the Delete icon. Click **OK** at the Confirmation Prompt. You cannot delete the standard attributes, only attributes that you have added.

RADIUS Attribute Dictionary List

The RADIUS Attribute Dictionary List displays all available RADIUS attributes.

- **Attribute Name -** The name of the vendor attribute
- **Attribute Code -** The attribute code.
- **Vendor Name -** The vendor name.
- **Vendor ID -** The vendor ID.
- **Value Type -** The type of value allowed for the attribute.
- **Access Policy -** Whether or not the attribute is available in an Access Policy (True/False).
- **Enforcement Policy -**Whether or not the attribute is available in an Enforcement Policy (True/False).
- **RADIUS-DM -** Whether or not the attribute is available in NAS Client configuration (True/False).
- **Sync to RADIUS -** Whether or not the attribute has been synced to the RADIUS Server. When synced, the attribute is available in the UPAM RADIUS server. (True/False).

Web Content Filtering

The UPAM Web Content Filtering (WCF) Profile Screen displays all configured WCF Profiles and is used to create, edit, and delete WCF Profiles. WCF Profiles can be configured to allow/deny client access through Stellar APs to web sites based on specific security or content conditions (e.g., Malware Sites, Gambling). When a client tries to access a restricted website, the page will fail to load, and the browser will display an error. A single WCF profile can contain multiple filtering conditions. To configure Web Content Filtering on an AP, you create a WCF Profile, configure an Access Role Profile or SSID with the WCF Profile, and then apply the Access Role Profile or SSID to APs. The basic Web Content Filtering Workflow is shown below.

Web Content Filtering is supported on Stellar APs running AWOS 4.0.2.x and higher (except AP1101, AP1201H, AP1201L, and AP1201HL models). You must have a Web Content Filtering License installed to use this feature. Licenses are purchased for a set number of APs, and you can only enable the feature on APs up to the number of licenses purchased.

Web Content Filtering is enabled on APs at the AP or AP Group level. You can only enable the feature on APs up to the number of APs in the license purchased. Note that if you enable Web Content Filtering at the AP Group level, it is enabled on all APs in the group that support Web Content Filtering (supported APs running AWOS 4.0.2.x and higher), and a license is consumed for each of those APs. If necessary, you can disable the feature on individual APs to reduce the number of licenses consumed.

Web Content Filtering OmniVista connects to a cloud-based Web Content Filtering Service to determine access to filtered URLs. The OmniVista Server must be able to connect to the

Internet to access this service to perform Web Content Filtering. The status of the OmniVista connection to this service is displayed at the top of the screen - **WCF Cloud Service**.

- **In Service -** Connection to WCF Filtering Service is up. OmniVista is connected to the Internet and to the Web Content Filtering Service site.
- **Not in Service -** Connection to WCF Filtering Service is down. Click on the tooltip for more information. You can also check the brightcloud.log for additional information (Administration - Audit - System).

Web Content Filtering Workflow

To configure Web Content Filtering on APs:

1. Enable Web Content Filtering on APs using the Access Points Screen (Network - AP Registration - Access Points) or AP Group Screen (Network - AP Registration - AP Group).

- **Access Points Screen -** Select an AP(s) in the Managed APs List, click on the Edit icon, select **Web Content Filtering** and enable the **Use Private Config** and **Web Content Filtering** fields. See the Access Points online help for more information.
- **AP Group Screen** - Create a new AP Group and set the Web Content Filtering slider to "On"; or select an existing AP Group in the AP Group List, click on the Edit icon, and set the Web Content Filtering slider to "On". See the AP Group online help for more information.

2. Create a WCF Profile as shown below.

3. Configure an Access Role Profile (Unified Access - Template - Access Role Profile) or SSID (WLAN - SSIDs) with a WCF Profile.

- In the **WCF Profile** field, select a WCF Profile from the drop-down. See the Access Role Profile online help or the SSID online help for more information.

4. Apply the Access Role Profile or SSID to AP(s) or AP Group(s).

Note: As mentioned earlier, if you enable Web Content Filtering at the AP Group level, all supported APs in the group are enabled, and each AP consumes a license. You can reduce the number of APs consuming a license by disabling Web Content Filtering on individual APs in the group. Select an AP(s) in the Managed APs List, click on the Edit icon, select **Web Content Filtering**, then disable the **Use Private Config** and **Web Content Filtering** fields. See the AP Group online help for more information.

Creating a WCF Profile

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

- **Name -** Enter a name for the WCF Profile.
- **Conditions -** In the first drop-down, select a condition to be included in the profile (e.g., Malware Sites, Gambling). In the second drop-down select whether to Accept or Reject access to a website based on the selected condition. When you are finished configuring a condition, click on the Add icon. Repeat to add additional conditions.

Editing a WCF Profile

Select a profile in the WCF Profile List and click on the Edit icon. Edit the condition(s) for the profile as described above, then click on the **Apply** button. You cannot edit the Profile Name.

> **Note:** When you edit a WCF Profile, the profile changes will not take effect until you enable Web Content Filtering again for the AP Group. See the AP Group online help for more information.

Deleting a WCF Profile

Select a profile(s) in the WCF Profile List, click on the Delete icon, then click **OK** at the Confirmation Prompt. You cannot delete a profile that is part of an Access Role Profile or SSID. To delete the profile, you must remove it from the Access Role Profile or SSID, and then delete the profile from the WCF Profile List.

WCF Profile List

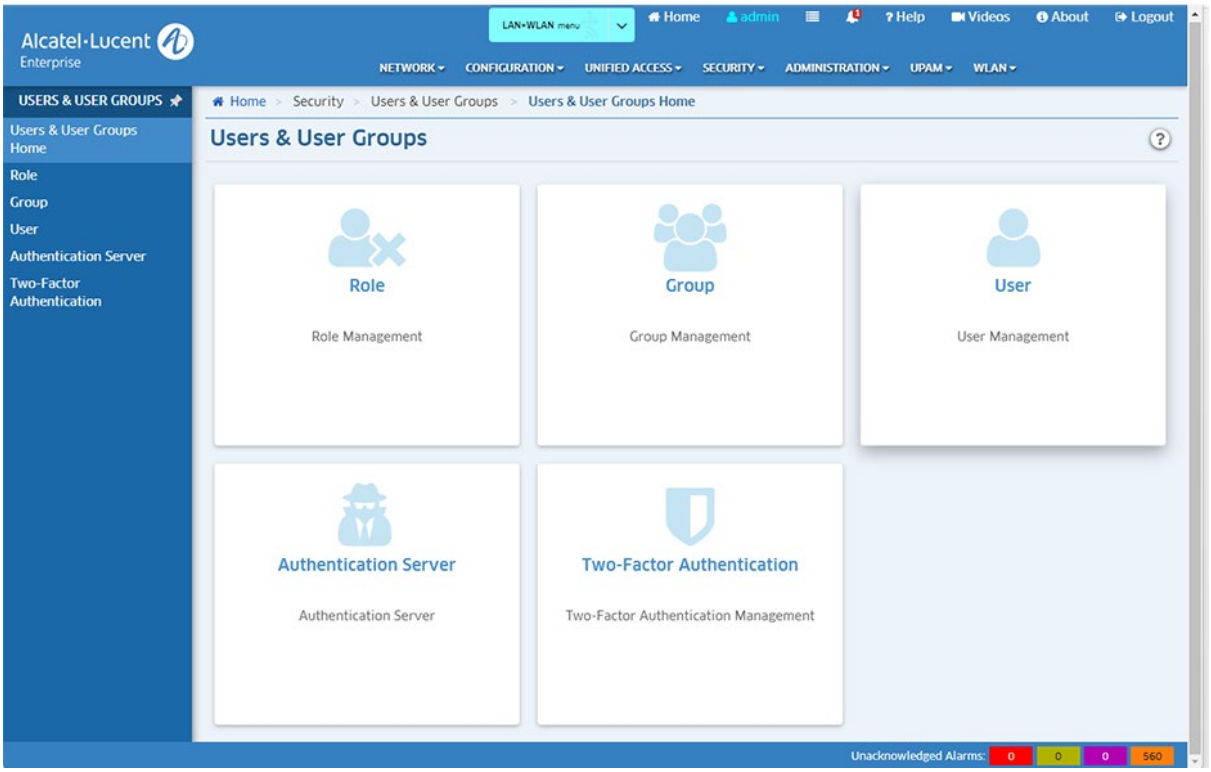
- **Name -** The user-configured name for the WCF Profile.
- **Conditions -** The conditions included in the WCF Profile.

34.0 Users and User Groups

The Users and User Groups application enables you to control user access to OmniVista and to network devices. Access to OmniVista is controlled through the definition of user logins and passwords. Access to network switches is controlled through the use of User Groups, which have specified levels of access to switches. You can further define access with the User Role feature, which can be used to specify read/write access to specific OmniVista applications and network devices.

All OmniVista users must be assigned to at least one User Group, which defines the access rights and roles for its members. User Groups and user logins are configured from the Users and User Groups application and constitute one level of network security. Users can also be configured for Two-Factor Authentication, based on User Role. Other levels of security are summarized below.

Users and User Groups



User Groups, Users, and User Roles are configured using the following screens:

- Role Management - Used to configure User Roles to restrict user access/rights to specific devices and OmniVista applications.
- Group Management - Used to configure User Groups to define access to OmniVista, network devices. A User Role is associated with a User Group to specify read/write access to specific devices and OmniVista applications.
- User Management - Used to configure users and assign the user to a User Group.
- Authentication Server - Used to specify the OmniVista Login Server.
- Two-Factor Authentication - Used to enable/disable Two-Factor Authentication for user login based on User Role.

Note: A User Role is an option that enables you to provide user access/rights to specific applications and network devices. For the most part, configuring Users and User Groups is all that will be required.

Security Levels

Security levels are configured in the Users and User Groups application, and through the Command Line Interface (CLI):

- **SNMP Get and Set Community Names -** Get and Set Community names act as read and write passwords that define whether any OmniVista user is allowed to read or write the switch's configuration information. Get and Set Community names are configurable only from the switch itself. Configured through the Console Port or CLI.
- **OmniVista User Groups -** User Groups in OmniVista provide different level of access to switches. An OmniVista user's access rights are based on the access rights of his/her assigned User Group. Configured in the Users and User Groups application.

Default Groups, Users, Roles

OmniVista security uses a combination of user logins, User Groups, and User Roles to control access to OmniVista, network switches, and applications. OmniVista is shipped with the pre-configured user logins, passwords, and User Groups described below. The Users and User Groups application enables you to modify these User Groups, Users, and passwords, or create new ones. Note that the pre-configured user **admin** is the only user that has permission to change the user logins and User Groups defined by the Users and User Groups application. The pre-configured User Groups, Users, and Roles shipped with OmniVista are as follows:

Group	User	Role	Access
Administrators	admin	Account Admin	Full administrative rights to all devices in the network and full administrative rights to the following features. These features are only available to this user: • User Management • License Management • Write Operations of System Settings • Control Panel Watchdog, Scheduler Management, and Session Management The default password for this user is **switch**.
Network Administrators	netadmin	Network Admin	Full administrative rights to all devices in the network. The default password for this user is **switch**.
Writers	writer	Write	Read/Write access to all devices in the network. The default password for this user is **switch**.
Default	user	Read	Read access to all devices in the network. The default password for this user is **switch**.

Note: A User Role is an option that enables you to provide user access/rights to specific OmniVista applications and network devices. For the most part, configuring Users and User Groups is all that will be required. The User Roles feature is configured on the Role

Management Screen. This feature enables you to specify access to specific applications, as well as devices using Topology maps. You can also limit user access to specific devices for VLAN and VXLAN configuration. You create a User Role to specify user access, associate it with a User Group, and then create a user in that User Group.

Working with User Groups, Users, and User Roles

You can use one of the pre-configured User Groups or use the Group Management Screen to create a new group or edit one of the pre-configured groups. You can use one of the pre-configured users or use the User Management Screen to create a new user or one of the edit pre-configured users. And you can use the Role Management Screen to create a new role.

> **Note:** All pre-configured users have the same default password, **switch**. At a minimum, it is recommended that you redefine the passwords.

The User Role feature allows you to limit users to specific network devices and applications. For example, OmniVista users with Admin rights can view and manage every device in the network and have read/write access for all applications. With the User Role feature, you can limit the devices a user can manage and the applications the user can configure by creating a User Role with access to a specific Topology map.

To utilize the User Role feature, you create a User Role with access to a specific Topology map and read/write access to a specific application(s). You then create a User Group and associate that group with that User Role. And finally, you create a user and associate it with that User Group. The user would then have full administrative rights to the specified applications for all devices in the specified map.

For example, you could create a User Role (User Role 1) with access to devices in Map 1 and read/write access to the Application Visibility application. A user with this role would be able to access all devices in Map 1 and configure Application Visibility on those devices. And since a user can have multiple roles, you could create a second User Role (User Role 2) with access to Map 2 and read/write access to the CLI Scripting and assign it to the same user. That user could now configure Application Visibility on devices in Map 1, and CLI Scripting on devices in Map 2.

Two-Factor Authentication

Two-Factor Authentication uses the Google Authenticator App to generate a time-based, 6-digit code that must be entered in addition to a user's login/password to log into OmniVista Cirrus. Two-Factor Authentication is configured for a user based on User Role. Once Two-Factor Authentication is set up for a user, the user will be required to enter their username/login, and then the 6-digit code generated by Google Authenticator to log into OmniVista Cirrus.

Role Management

The Users and User Groups Role Management Screen displays all currently configured User Roles. The screen is used to create, edit, or delete User Roles. The User Role feature enables you to specify user rights for specific OmniVista applications and devices. A User Role is associated with a User Group to define access for users assigned to the group. OmniVista is shipped with four pre-configured User Roles:

- **Account Admin** - This User Role can access all maps and has full administrative access rights to all devices in the network. This User Role also has full administrative rights to edit the groups and users defined in the Users and Groups Application.
- **Network Admin** - This User Role can access all maps and has full administrative access rights to all devices in the network. This User Role can view/add/import licenses, Trust/Untrust APs, and create/edit/delete AP Groups. This User Role can only perform "Edit" operations on accessible Topology maps, and does **not** have administrative rights to edit the groups and users defined in the Users and Groups Application.
- **Write** - This User Role can access all maps and has Read/Write access to all devices in the network.
- **Read -** This User Role can access all maps and has Read access to all devices in the network.

  Note: Specific rights for each OmniVista application for the above system-defined Roles can be viewed by clicking on a Role in the Existing Roles Table to view the Details window.

Creating a User Role

Click on the Add icon to launch the Role Management Wizard and configure and create a User Role. Complete the fields as described below. Click on the **Next** button to move to the next window. When you are finished, click on the **Create** button.

Role Info and Map Access

Complete the fields below to specify which Topology maps a user can access.

- **Role Name -** Enter a name for the User Role.
- **Description -** Enter an optional description for the User Role.
- **Accessible Maps -** Select an option from the drop-down menu to specify the maps the user can access. The user will only have access to devices in the selected map(s).
- **All Maps -** The user can access all maps.
- **No Maps -** The user cannot access any maps. The user will only have access to non-network OmniVista applications (e.g., Audit, Preferences).
- **Selected Maps -** Select this option, then click on the **Add/Remove Maps** button to select maps the user can access.

Application Access Control

Select the OmniVista application access for the user. Only those applications you configure (either Read or Write access) will be available to the user. By default, Read access is pre-selected for Topology (if map access is configured), System Preferences and Users and User Groups. Read/Write access is pre-selected for User Preferences and Report.

Object Restrictions

Specify the VLANs and or VXLANs the user can access for VLAN/VXLAN configuration. The user will be able to perform VLAN/VXAN operations on these VLANs/VXLANs for devices specified in the Role Info and Map Access window above. This parameter is optional.

Review

Review the configuration. Click on the **Back** button to make any changes.

Editing a User Role

Click on a User in the Existing Users Table and click on the Edit icon. Edit any fields as necessary and/or edit the User Groups at the bottom of the screen to re-assign the User to a different User Group. When you are done, click **Apply**. You will be returned to the User Management Screen. Note that you cannot edit the User Login field. Note that you cannot edit a system-defined User Role.

Deleting a User Role

Select a User(s) in the Existing Users Table, click on the Delete icon, then click **OK**. Note that you cannot delete a system-defined User Role.

Existing Roles Table

The Existing Roles Table displays all configured Users. Click on a User Role in the table for more details.

- **Role Name -** Role Name.
- **Description -** Role Description.
- **System Defined -** Whether the role is a system-defined role or a user-defined role.
- **Accessible Maps -** The maps a user assigned to this role can access.
- **Access Control -** The access/rights to OmniVista applications for a user assigned to this role.

User Role Feature

Basically, the User Role feature allows you to limit users to specific network devices and OmniVista applications. For example, OmniVista users with Admin rights can view and manage every device in the network and have read/write access for all applications. With the User Role feature, you can limit the devices a user can manage and the applications the user can configure by creating a User Role with access to a specific Topology map and write access to specific applications.

To utilize the User Role feature, you create a User Role with access to a specific Topology map and read/write access to a specific application(s). You then create a User Group and associate that group with that User Role. And finally, you create a user and associate it with that User Group. The user would then have full administrative rights to the specified applications for all devices in the specified map.

For example, you could create a User Role (User Role 1) with access to devices in Map 1 and read/write access to the Application Visibility application. A user with this role would be able to access all devices in Map 1 and configure Application Visibility on those devices. And since a user can have multiple roles, you could create a second User Role (User Role 2) with access to Map 2 and read/write access to the CLI Scripting and assign it to the same user. That user could now configure Application Visibility on devices in Map 1, and CLI Scripting on devices in Map 2.

The table below provides some use case samples for assigning multiple User Roles to a User.

Scenario	User Role 1	User Role 2	User Role 3	Device/Application Access
Using Topology Maps to limit access to devices	Map 1 Read Access for Topology	Map 2 Write Access for Topology	Map 3 Read Access for Topology	Read Access for devices in Maps 1 and 3. Write Access for devices in Map 2
Using a combination of Topology Maps and an application, such as Application Visibility.	Map 1 Read Access for Application Visibility	Map 2 Read Access for Application Visibility	Map 3 Write Access for Application Visibility	Read Access for Application Visibility for devices in Maps 1 and 2. Write Access for Application Visibility for devices in Map 3.
Using a combination of Topology Maps and an Object (VLAN)	Map 1 VLAN 10 Read Access for Application Visibility	Map 2 VLAN 20 Read Access for Application Visibility	Map 3 VLAN 30 Write Access for Application Visibility	Read Access for Application Visibility for devices in Maps 1 and 2; and VLAN configuration allowed on those devices in VLANs 10 and 20. Write Access for Application Visibility for devices in Maps 1 and 2; and VLAN configuration allowed on those devices in VLAN 30.

Group Management

The Users and User Groups Group Management Screen displays all currently-configured User Groups (along with a brief description). You can click on a User Group in the list for more information about the group. The screen is used to create, edit, or delete User Groups; and add or delete Users from a User Group. OmniVista is shipped with four pre-configured User Groups:

- **Administrators** - This User Group has full administrative access rights to all devices in the network AND full administrative rights to edit the groups and users defined in the Users and Groups Application.
- **Network Administrators** - This User Group has full administrative access rights to all devices in the network. Members of this group are the users who are responsible for management of parts of the network (Site Administrators). This group can manually add, delete, or modify devices.
- **Writers** - This User Group has Read/Write access to all devices in the network.
- **Default -** This User Group has Read access to all devices in the network.

  Note: Specific rights for each OmniVista Application for the above system-defined Groups can be viewed by clicking on a Group in the Existing Groups Table to view the Details window.

Creating a User Group

Click on the Add icon and complete the fields as described below. When you are finished, click on the **Create** button.

- **Name** - Enter a name for the group.
- **Description** - Enter an optional description for the group.
- **Assigned Roles** - Select a User Role for the group.
- **User Members** - Select a User(s) for the group.

Note that users may belong to more than one group at a time, in which case their access rights are defined by the most privileged group to which they belong. Also note that you do not have to add users to the User Group at this time. When you create a user, you can add them to any existing User Group as a member. You can also edit a User Group later to add members.

Editing a User Group

Click on a Group on the Group Management Screen to bring up the User Group Detail Screen. Click on the Edit icon. You can edit the **Description**, **Assigned Roles**, and **User Members** fields. When you are done, click the **Apply** button. You will be returned to the Group Management Screen. Note that you cannot edit the Group Name field. Also note that you can only edit the Description field of the Administrators Group.

Deleting a User Group

Select a User Group(s) on the Group Management Screen by clicking in the checkbox, click on the Delete icon, then click **OK**. Note that you cannot delete the Administrators Group or the Default Group.

Existing Groups Table

The Existing Groups Table displays all configured User Groups. Click on a group in the table for more details.

- **Name -** Group Name.
- **Description -** Group Description.
- **Assigned Roles -** The User Roles assigned to the group.

User Management

The Users and User Groups User Management Screen displays all currently-configured Users by login name (along with a brief description). The screen is used to create, edit, or delete Users. Note that a User's access rights are determined by the User Group in which the user is a member. OmniVista is shipped with four pre-configured Users and four pre-configured User Groups. The default password for all four pre-configured Users is **switch**. For security reasons, it is recommended that you redefine the default passwords. The default Users and their default pre-configured User Group memberships are as follows:

- **admin -** This user belongs to the Administrators User Group and has full administrative rights to all switches on the network AND full administrative rights to the Users and Groups Application. The default password for this user is **switch**.

- **netadmin -** This user belongs to the Network Administrators User Group and has full administrative rights to all devices in the network. This user has read/write access to the License Screen and can also create/edit/delete AP Groups, Trust/Untrust APs, create/delete maps/sites, and modify the accessible maps of role. The default password for this user is **switch**.
- **writer -** This user belongs to the Writers User Group and has Read/Write access to all devices in the network. The default password for this user is **switch**.
- **user -** This user belongs to the Default User Group and has read access to all devices in the network. The default password for this user is **switch**.

  Note: Specific rights for each OmniVista Application for the above system-defined Users can be viewed by clicking on a User in the Existing Users Table to view the Details window.

Creating a User

Click on the Add icon and complete the fields as described below. The **User Login** and **Password** fields are **mandatory**. The user will use this User Login and Password to log into OmniVista. You can complete additional fields (e.g. Name, Description) to provide a more detailed description of the User. Select one of the User Groups at the bottom of the screen to assign the User to a specific User Group and click on the **Create** button. Note that users may belong to more than one User Group at a time, in which case their access rights are defined by the most privileged group to which they belong.

Editing a User

Click on a User in the Existing Users Table and click on the Edit icon. Edit any fields as necessary and/or edit the User Groups at the bottom of the screen to re-assign the User to a different User Group. When you are done, click **Apply**. You will be returned to the User Management Screen. Note that you cannot edit the User Login field.

Deleting a User

Select a User(s) in the Existing Users Table, click on the Delete icon, then click **OK**. Note that you cannot delete the user admin.

Existing Users Table

The Existing Users Table displays all configured Users. Click on a user in the table for more details.

- **Login -** User login.
- **Description -** User Description.
- **Assigned Roles -** The User Roles assigned to the user. This tab also displays the Application Access Control configuration for the user (the user's read/write access for OmniVista applications).
- **Assigned Groups -** The User Group(s) to which the user belongs.

Authentication Server

The Users and User Groups Authentication Server Screen is used to select the Login Authentication Server. You can select the local OmniVista Server (Local) or a remote RADIUS

Server. Select the server from the **Authentication Serve**r drop-down list and click on the **Apply** button. If necessary, click on the "Add New RADIUS Server" link or the "Add New LDAP Server" link to go the RADIUS Server Management Screen or the LDAP Server Management screen and configure a remote RADIUS or LDAP Server. (After creating the server, you will automatically be returned to the Authentication Server Screen.)

Select the server from the **Authentication Server** drop-down list. If you select a server other than "Local", select an **Authentication Method** for communication between the remote server and OmniVista (PAP, CHAP, MSCHAP, MSCHAPV2, EAP - MSCHAPV2, or LDAP Server - SIMPLE).

If you select a remote server, you must also verify connectivity to that server by clicking on the **Test Radius Server Connection** or **Test LDAP Server Connection** button and entering your RADIUS User Name and Password for the selected server. (You can also enter the User Name and Password of any user configured on the selected Server.) This is to ensure that the selected RADIUS Server is reachable and is configured correctly for OmniVista remote authentication. Enter your RADIUS Server **User Name** and **Password** and click **OK**. OmniVista will ping the server and verify connectivity and configuration. If successful, the **Apply** button will activate. Click on the **Apply** button to set the new server. If the server is unreachable or not configured correctly, the **Apply** button will not activate and you will not be able to change the server.

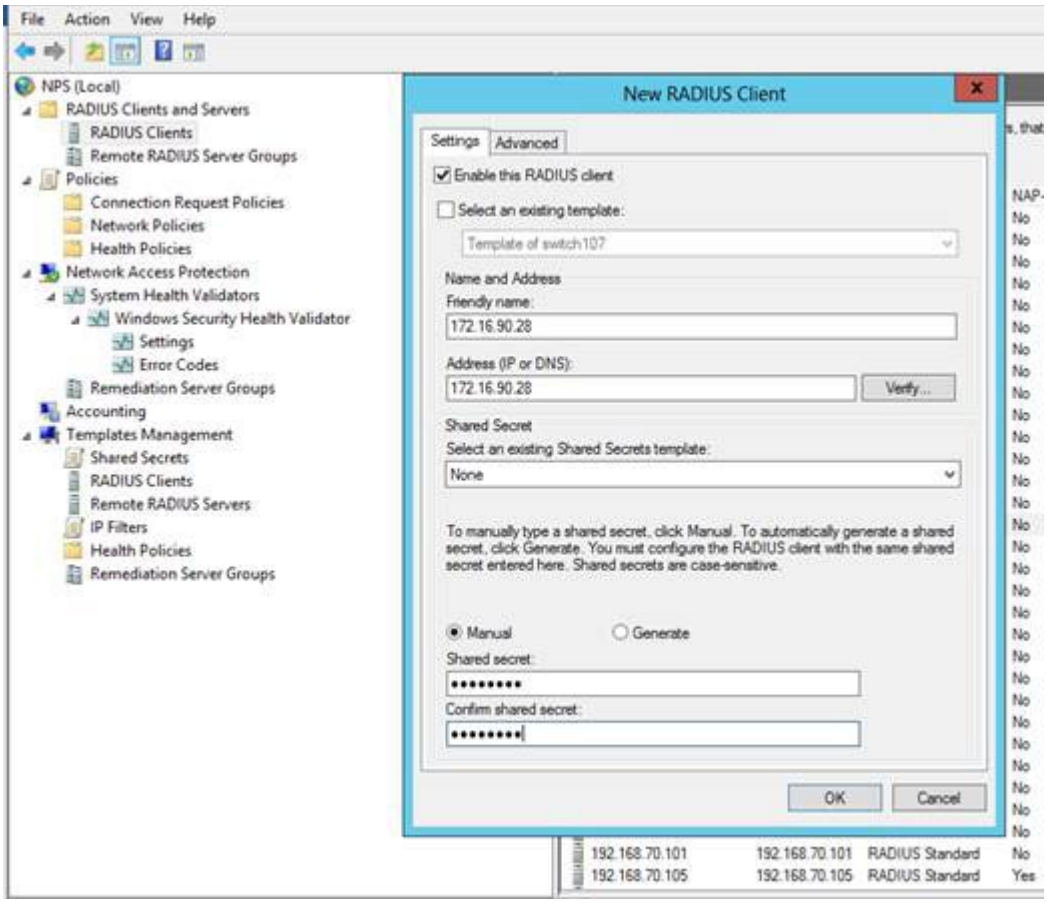
Notes:

- Only a remote RADIUS Server or the OmniVista Server (Local Database) can be used for OmniVista login. If a remote Authentication Server is used, and that remote server and the remote backup server are not available, users cannot log into OmniVista. If necessary, the Administrator may change the Authentication Server using the Virtual Appliance Menu on the VA.
- If a remote LDAP Server is selected, note that you can enable SSL (SSL = True) for OmniVista login authentication. See the LDAP Server Management online help for more information.
- You can also view/change the Authentication Server using the Virtual Appliance Menu on the VA. Open a Console on the VA. On **The Virtual Appliance Menu**, enter **7** to go to the **Login Authentication Server Screen**.
- If a remote authentication server is selected, and that remote server and the remote backup server are not available, users can login from the local OmniVista Server.
- If the Administrator changes the Login Server, current users will remain logged in. However, if the users attempt to login/re-login, they will be logged in using the new Login Server.

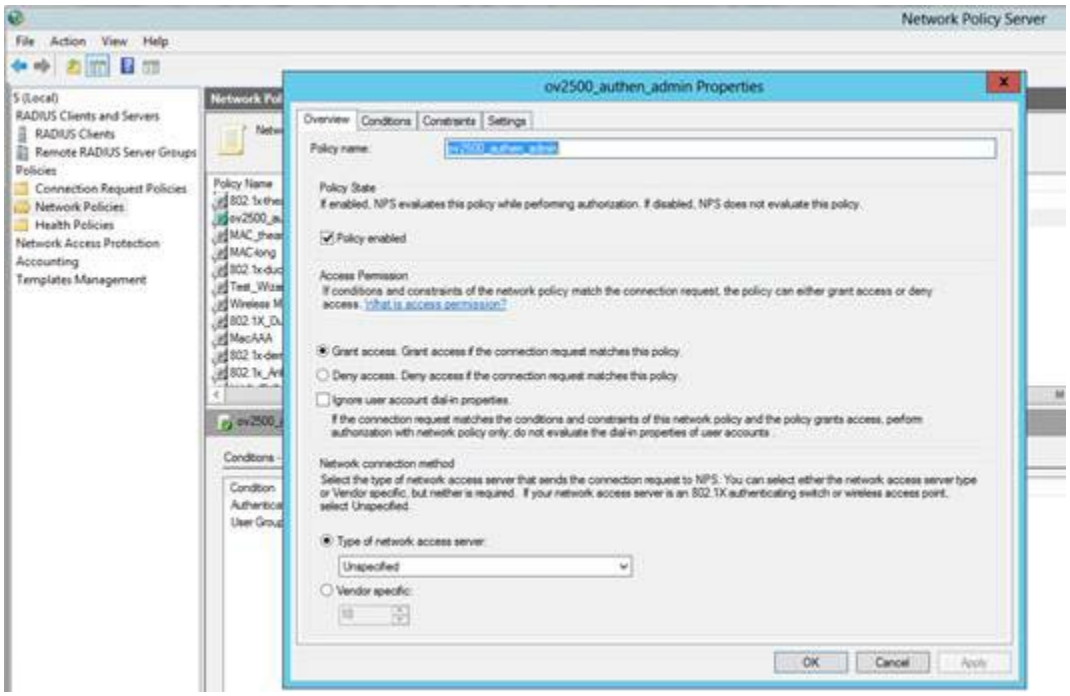
See the sections below for steps on configuring an External RADIUS Server or a CPPM RADIUS Server for authentication.

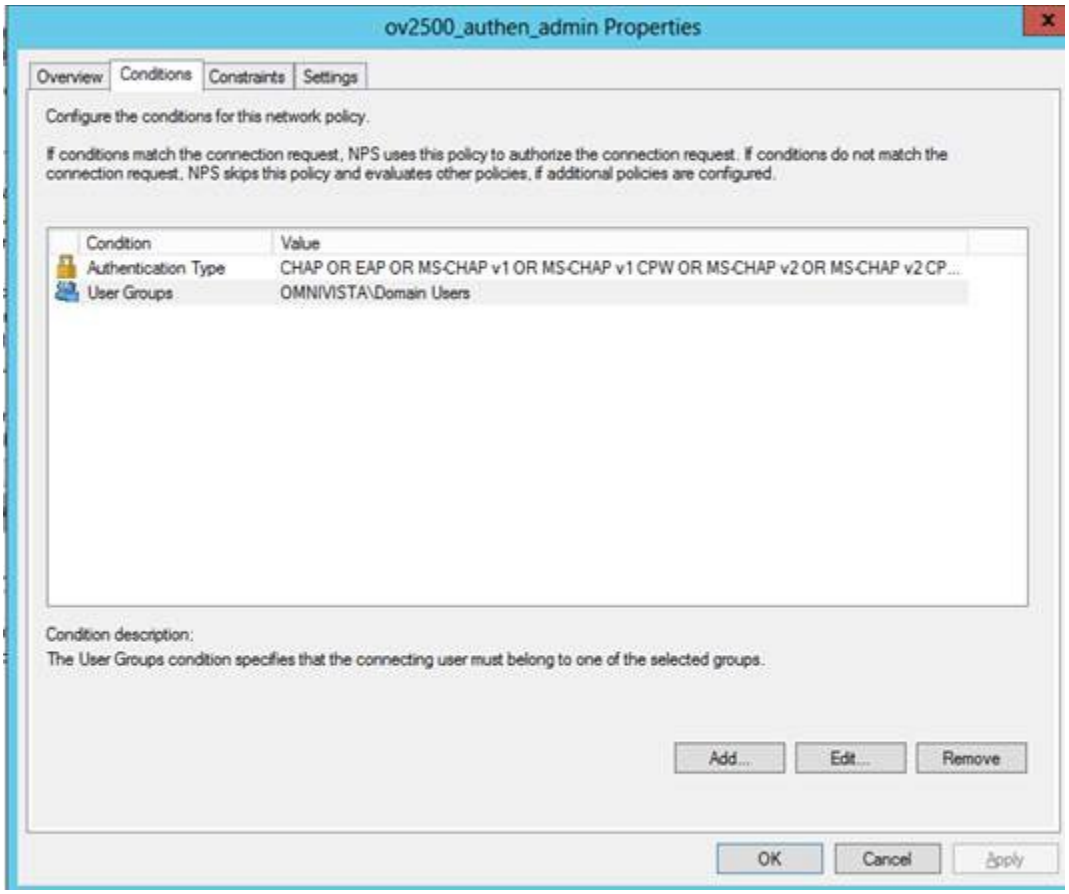
Configuring External RADIUS Server Authentication

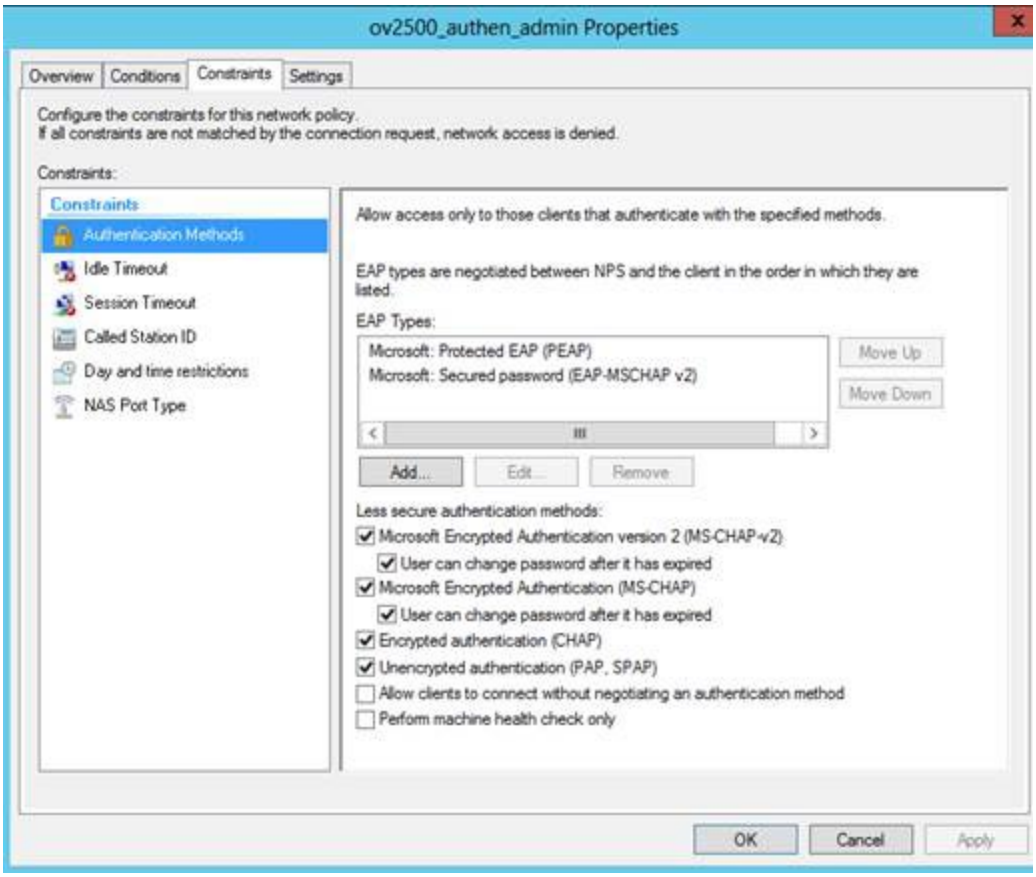
1. Add a new RADIUS Client (e.g., 172.16.90.28).

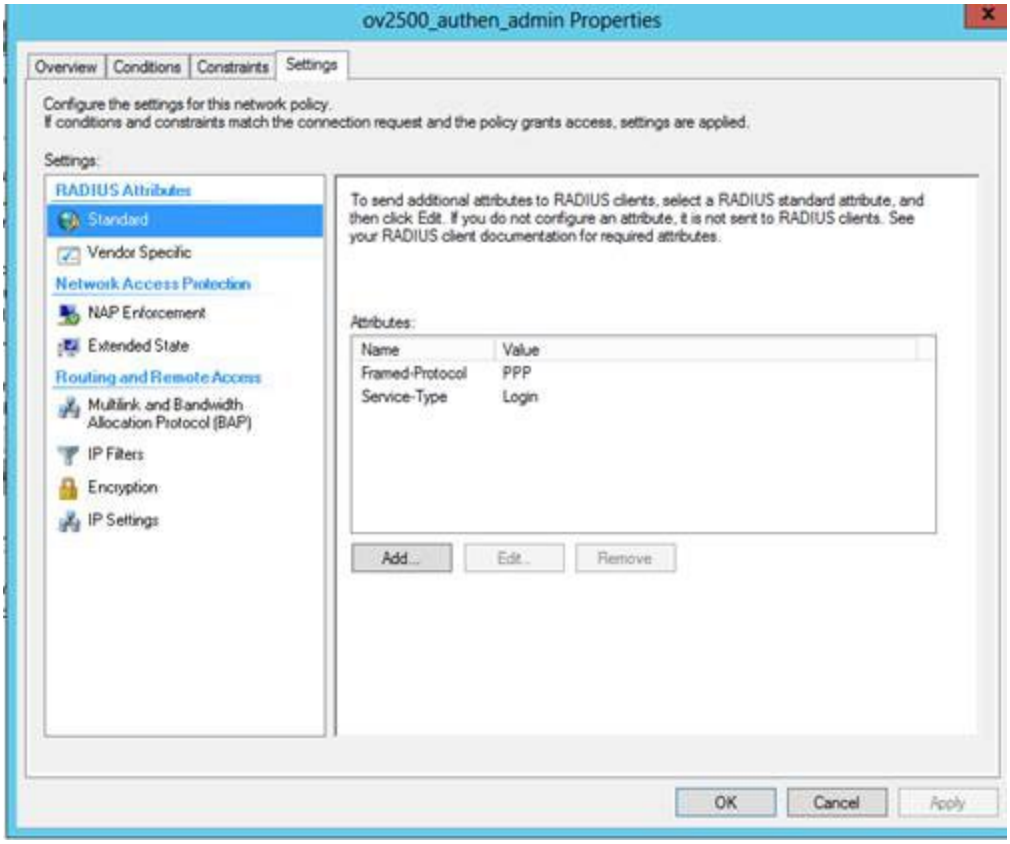


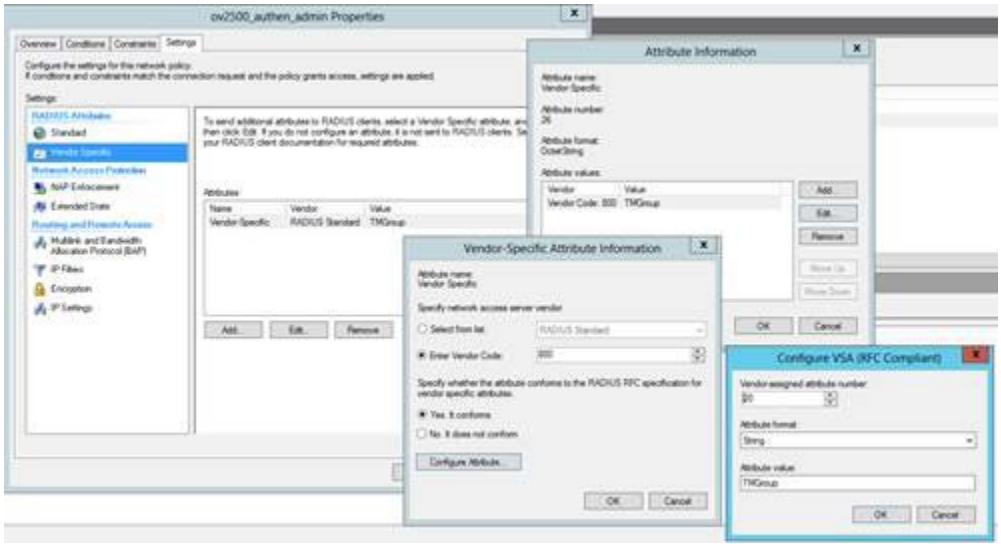
2. Configure some conditions for this Network Policies.



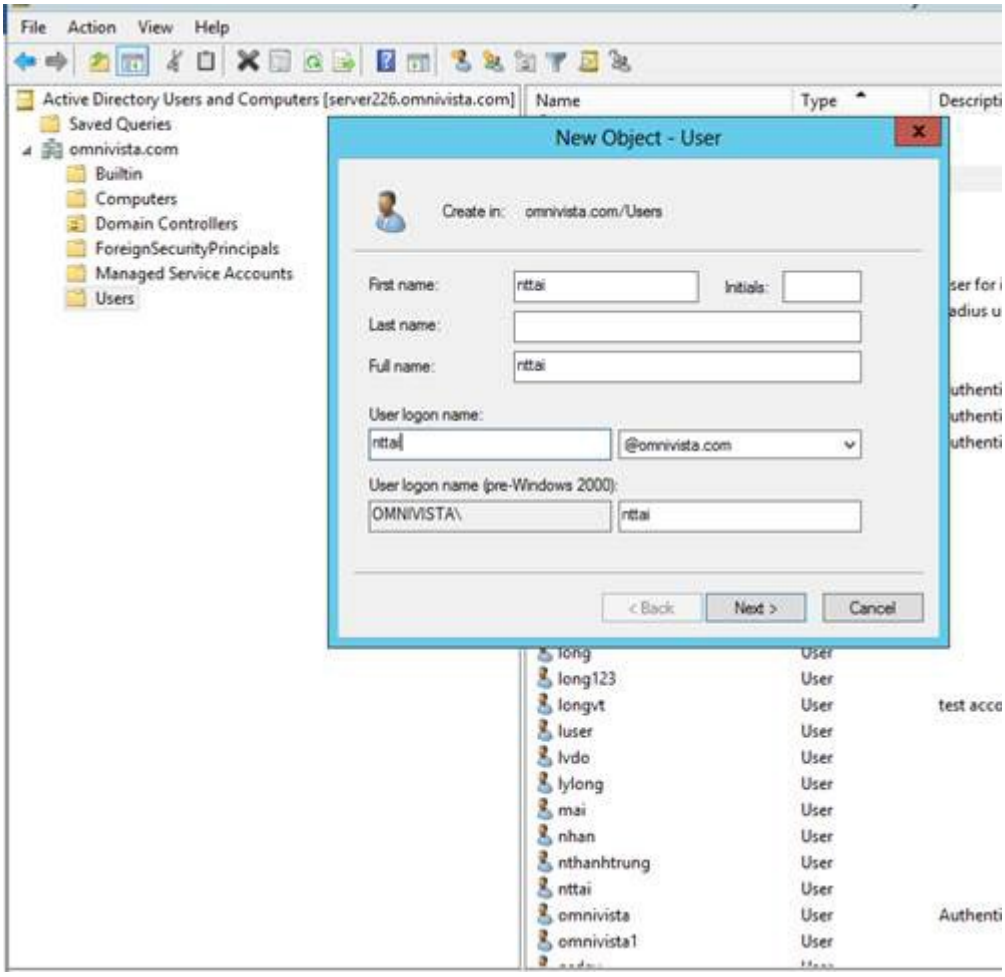

ov2500_authen_admin Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
Authentication Type
CHAP OR EAP OR MS-CHAP v1 OR MS-CHAP v1 CPW OR MS-CHAP v2 OR MS-CHAP v2 CP...
User Groups
OMNIVISTA\Domain Users
Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.
Add...
Edit...
Remove
OK
Cancel
Apply


ov2500_authen_admin Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to those clients that authenticate with the specified methods.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Protected EAP (PEAP)
Microsoft: Secured password (EAP-MSCHAP v2)
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method
Perform machine health check only
OK
Cancel
Apply


ov2500_authen_admin Properties
Overview
Conditions
Constraints
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Network Access Protection
NAP Enforcement
Extended State
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Framed-Protocol
PPP
Service-Type
Login
Add...
Edit...
Remove
OK
Cancel
Apply

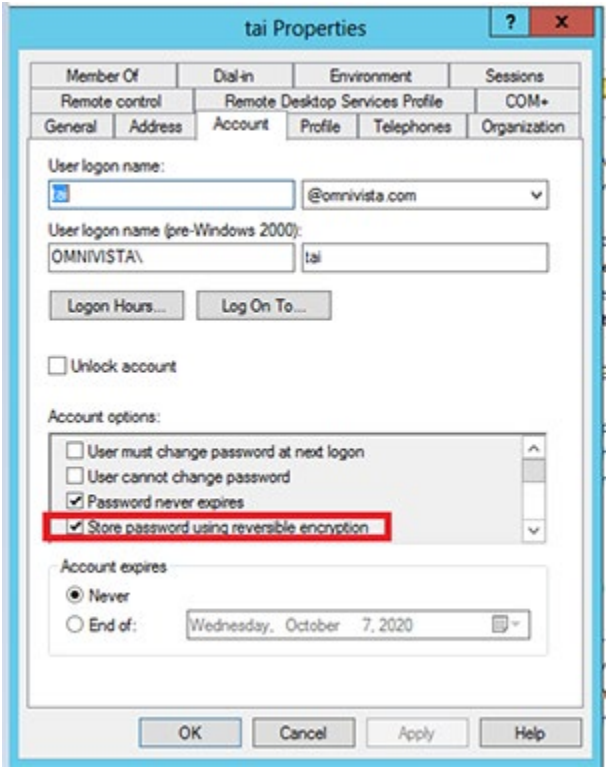


3. Create user.



Note that users need to enable storage of a reversibly-encrypted form of the user's password for authentication using CHAP.

- Go to Active Directory Domain Services - Active Directory Users and Computers - Domain (e.g., scc.seeg.com) - Users.
- Double click the user who is going to use the CHAP Authentication Protocol. Click on the Account Tab. Select Store password using reversible encryption. Click OK.



Configuring CPPM RADIUS Authentication

1. Update the RADIUS Dictionary Alcatel-Lucent Enterprise by adding attributes:

- Export Alcatel-Lucent Enterprise Dictionary of CPPM.
- Edit using notepad.
- Import it in to CPPM.

<Attribute profile="in out" type="String" name="Alcatel-Nms-Group" id="20"/>
<Attribute profile="in out" type="String" name="Alcatel-Nms-First-Name" id="21"/>
<Attribute profile="in out" type="String" name="Alcatel-Nms-Last-Name" id="22"/>
<Attribute profile="in out" type="String" name="Alcatel-Nms-Description" id="23"/>

2. Configure an Enforcement Profile for the Administrators Group.

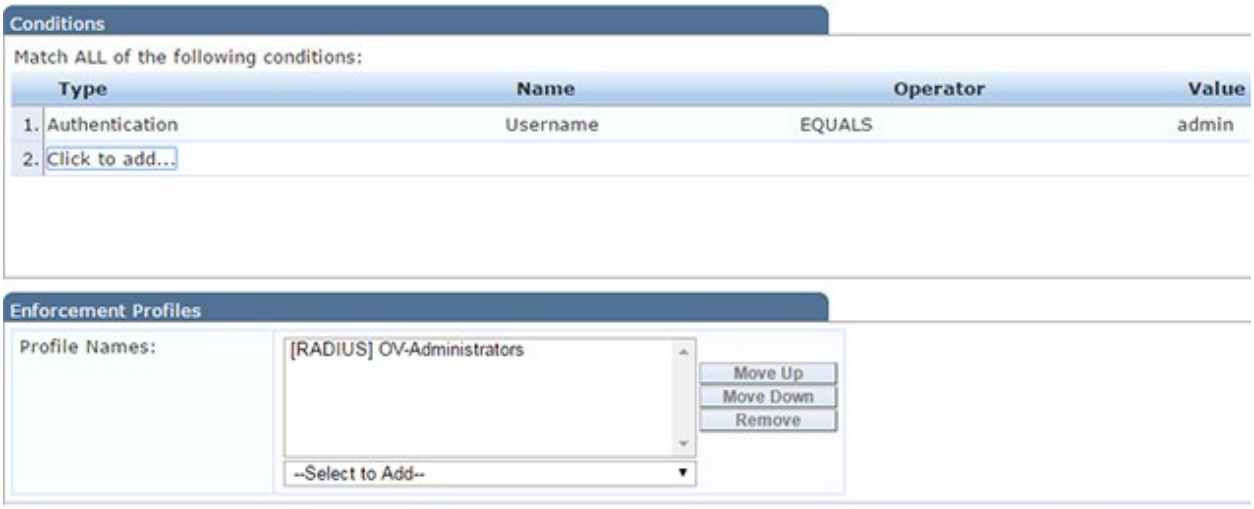
Profile:

Name:	OV-Administrators
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

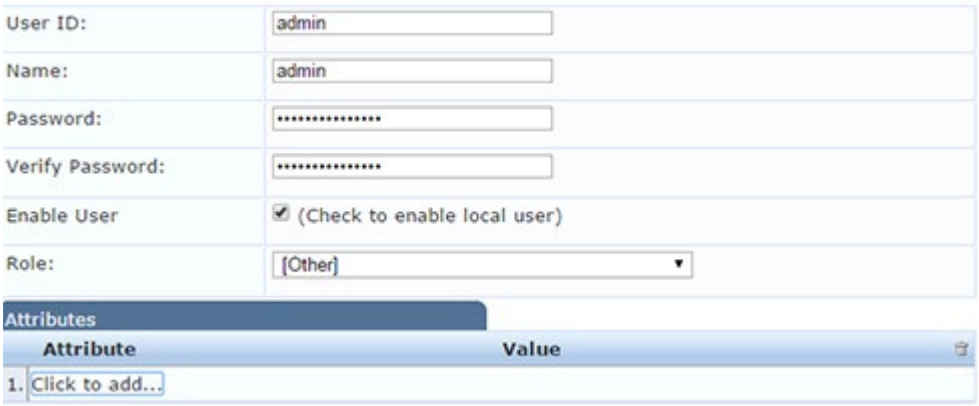
Attributes:

	Type	Name		
1.	Radius:Alcatel-Lucent-Enterprise	Alcatel-Nms-Group	=	A

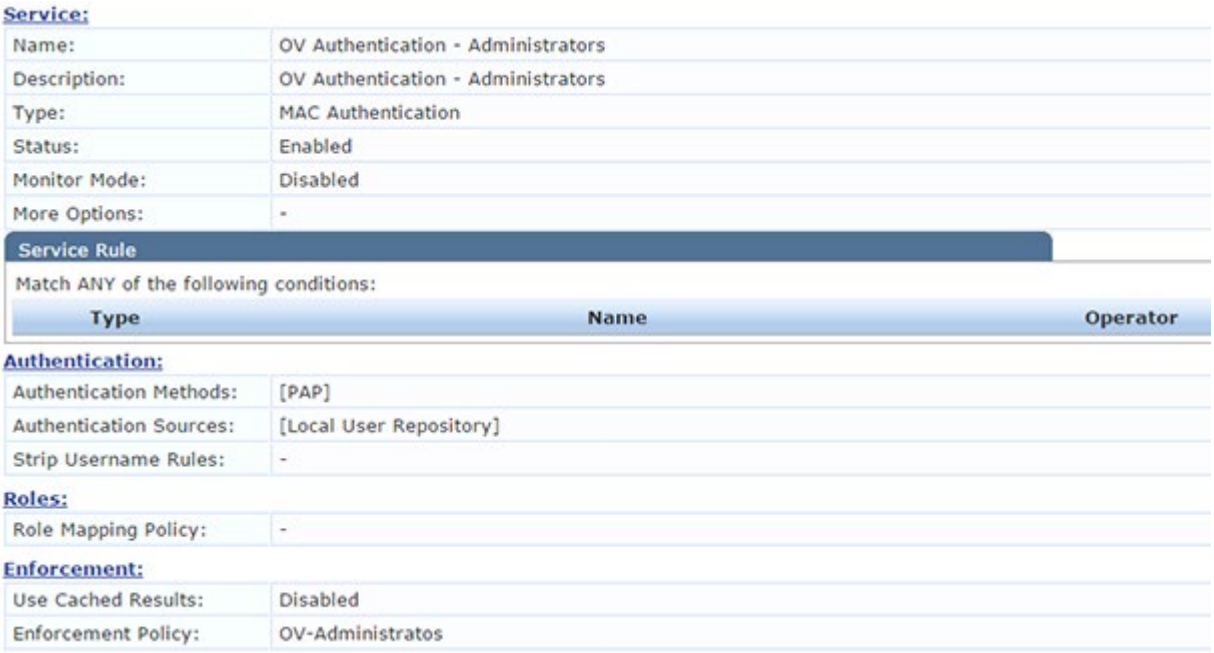
. **3.** Configure an Enforcement Policy for the Administrators Group.



4. Create a Local User “admin” with any password on CPPM.



5. Create an Authentication Service on CPPM with “PAP” Protocol, “Local User Database”, and Enforcement Policy for the Administrators Group.



Service:

Name:	OV Authentication - Administrators
Description:	OV Authentication - Administrators
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ANY of the following conditions:

Type	Name	Operator

Authentication:

Authentication Methods:	[PAP]
Authentication Sources:	[Local User Repository]
Strip Username Rules:	-

Roles:

Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	OV-Administratos

6. Configure as RADIUS Client for OmniVista on CPPM and RADIUS Server on OmniVista.

7. Choose CPPM RADIUS as the Authentication Server for OmniVista and try to login with a user from CPPM.

Two-Factor Authentication

The Users and User Groups Two-Factor Authentication Server Screen displays Two-Factor Authentication Status by User Role and is used to globally enable/disable Two-Factor Authentication for all user logins. Two-Factor Authentication requires a user to enter an authentication code after entering their login/password to access OmniVista. The authentication code is a time-based, 6-digit code that is generated using the Google Authenticator App.

When Two-Factor Authentication is globally enabled/disabled, the configuration is applied to all users assigned to each Role through their User Group. You cannot have different login settings for different users in a User Group. Two-Factor Authentication is enabled for all Roles, so all users will be required to use Two-Factory Authentication to log in.

To enable/disable Two-Factor Authentication for all Roles, click on the **Enable Globally** or **Disable Globally** button at the top of the screen, then click **OK** at the Confirmation Prompt. The setting will be applied to all users. Note that if a user is configured for Two-Factor Authentication, the user will receive an auto-generated email any time Two-Factor Authentication is enabled/disabled, informing them that Two-Factor Authentication has been enabled or disabled for their account.

> **Note:** When you enable/disable Two-Factor Authentication, the setting is applied to all current users, as well as all future users that you create. Two-Factor Authentication is not applied based on User Role; it is only applied globally to all users.

Two-Factor Authentication User Set Up and Login

This section details the steps required for a user to set up and use Two-Factor Authentication. Two-Factor Authentication uses the Google Authenticator App to generate a time-based, 6-digit code that must be entered in addition to a user's login/password to log into OmniVista.

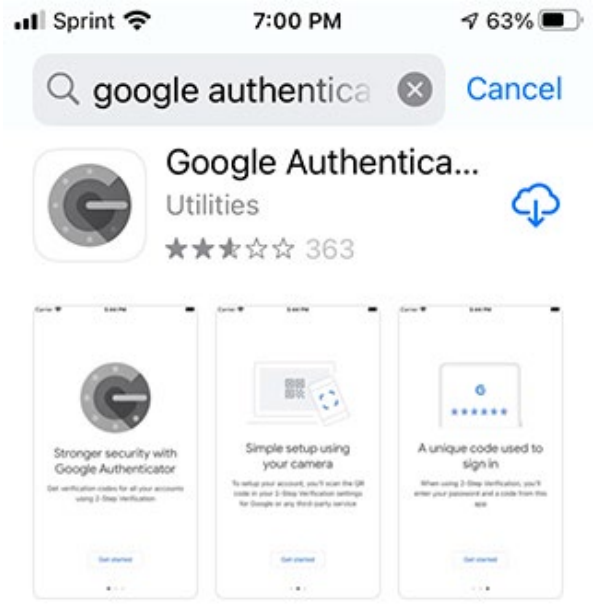
The first time a user logs into OmniVista after being configured for Two-Factor Authentication, they will be presented with a second login screen to set up Two-Factor Authentication using the Google Authenticator App. Once Two-Factor Authentication is set up, the user will be required to enter their username/login, and then the 6-digit code generated by Google Authenticator to log into OmniVista.

The following sections detail the steps for initial user setup and login, as well as returning user login for Two-Factor Authentication.

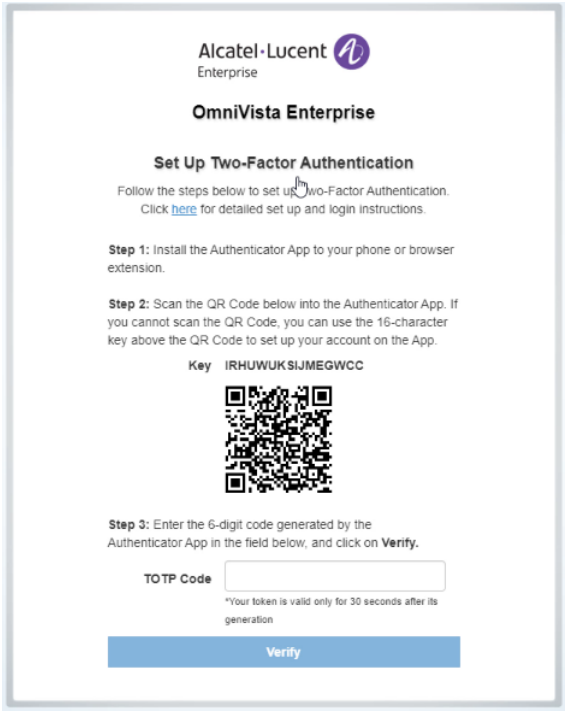
First Time Two-Factor Authentication Setup and Login

Two-Factor Authentication uses the Google Authenticator App to generate a time-based, 6-digit code that is used to log into OmniVista. To log into OmniVista using Two-Factor Authentication, you must first download the Google Authenticator App to your phone. The steps below detail downloading the App, setting up the user account on Google Authenticator, and logging into OmniVista.

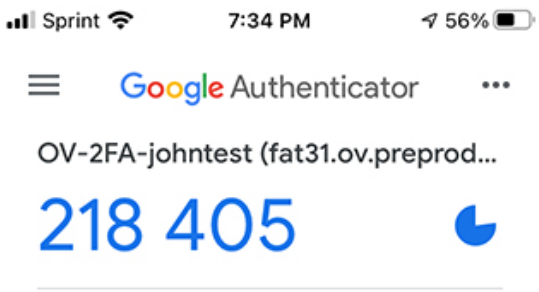
1. Go to the Google Play App Store or the Apple App Store and download the Google Authenticator App to you phone.



2. After entering your login/password on the OmniVista Login Screen, the following Two-Factor Authentication Screen will appear.



3. Open the Google Authenticator App on your phone and use your phone to scan the QR Code on the login screen into the App. Click on the **+** icon at the bottom of the Google Authenticator App Screen, then click on the **Scan a QR Code** option to bring up the camera. Hold the phone up to the screen to scan the QR Code on the login page. When the scan is complete, the following screen will appear in the Google Authenticator App.



When you scan the QR Code into the Google Authenticator App, the App sets up your account and stores your username (e.g., OV-2FA-johntest) and the URL of the machine you are logging into (fat31.ov.preprod.com). As shown above, a 6-digit login code is displayed under your username and URL. Note that the code is good for 30 seconds. A countdown clock is shown to the right of the code. When then timer is close to expiring, the code numbers will turn red. When the countdown is complete, a new code will be displayed for 30 seconds.

> **Note:** If you cannot scan the QR Code as described above, you can use the 16-digit key above the QR Code to set up your account in the Google Authenticator App. To enter this code, click on **Enter a setup key** instead of **Scan a QR Code**. Enter your Account (e.g., OV-2FA-johntest), enter the Key, then click on the **Add** button.

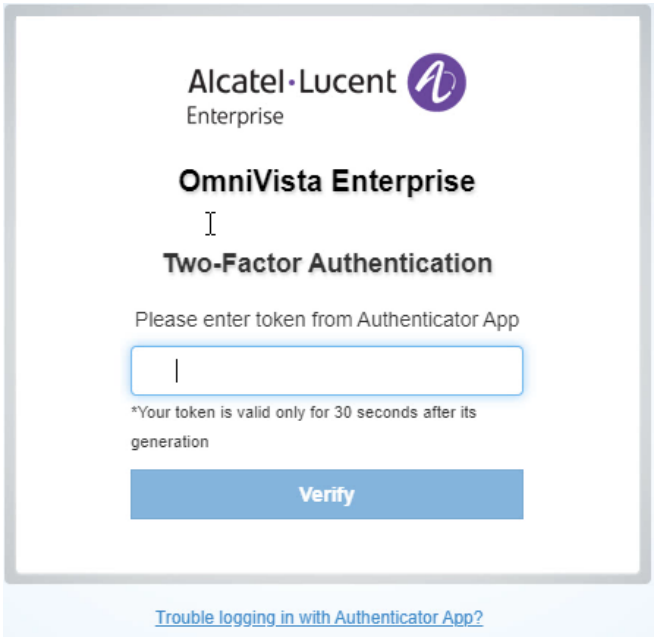
4. Enter the code for your user account into the **TOTP Code** Field on the OmniVista Login Screen and click **Verify** to log into OmniVista. If you have more than one user account set up in the Google Authenticator App, make sure you are entering the code for the correct account.

> **Note:** If a User configured for Two-Factor Authentication is unable to successfully log in (e.g., unable to set up Two-Factor Authentication, repeatedly inputting an invalid authentication code), a warning message is presented to the user and the user is redirected to the login page. The User's "2FA State" will display "Verified" in the Existing Users Table the User Management Screen. Select the User in the table, click on the Reset 2FA button at the top of the screen, then click OK at the Confirmation Prompt. The user will then be required to set up Two-Factor Authentication again.

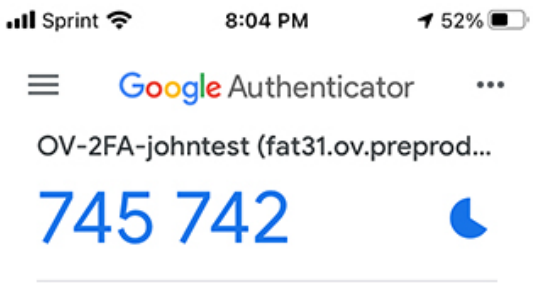
Returning User Two-Factor Authentication Login

Once you set up your user account in the Google Authenticator App as described above, log in using the 6-digit code provided by the Google Authenticator App.

1. After entering your OmniVista login/password, the following screen will appear.



2. Open the Google Authenticator App on your phone. The app will open to the Login Code Screen displaying the current codes for any user account you have set up in the App.



3. Enter the code for your user account (e.g., OV-2FA-johntest - fat31.ov.preprod.com) and click **Verify** to log into OmniVista. If you have more than one user account set up in the Google Authenticator App, make sure you are entering the code for the correct account.

> **Note:** If a User configured for Two-Factor Authentication is unable to successfully log in (e.g., repeatedly inputting an invalid authentication code), a warning message is presented to the user and the user is redirected to the login page. The User's "2FA Status" will display "Verify" in the Existing Users Table the User Management Screen. Select the User in the table, click on the **Reset 2FA** button at the top of the screen, then click **OK** at the Confirmation Prompt. The user will then be required to set up Two-Factor Authentication again.

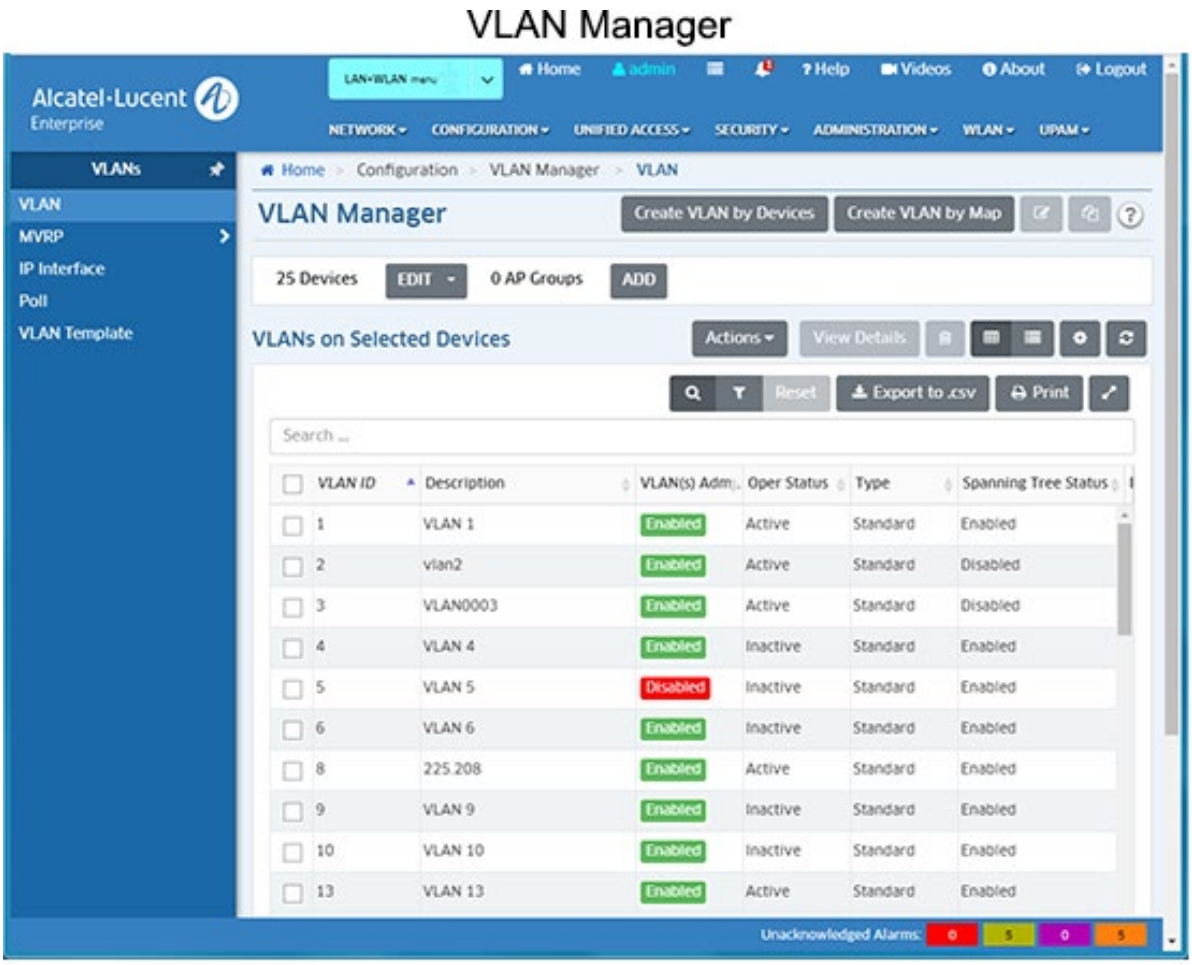
Two-Factor Authentication Table

The Two-Factor Authentication Table displays Two-Factor Authentication status for all configured User Roles. It can also be used to globally enable/disable Two-Factor Authentication for all Role(s). Click on the **Enable Globally** or **Disable Globally** button, then click **OK** at the Confirmation Prompt.

- **Role Name** - The User Role.
- **Status** - The administrative status of Two-Factor Authentication for the User Role:
  - **Enabled** - Two-Factor Authentication is enabled for the user.
  - **Disabled** - Two Factor Authentication is disabled for the user. The user can log into OmniVista using only their login/password.

35.0 VLAN Manager

The VLAN Manager Screen displays information about all VLANs configured on AOS Devices and Stellar APs; and is used to create, edit, copy, and delete VLANS on AOS Devices. It is also used to perform certain actions on a VLAN (e.g., enable/disable VLANs, view/edit Spanning Tree parameters, view/configure an IP Router, and view VLAN details). Links on the left side of the screen are used to view/configure MVRP and IP interfaces; and poll network devices.



Note: You can create, edit, delete, VLANs on AOS Switches and OAW Controllers using the VLAN Manager application. Information about VLANs configured on Stellar APs is displayed in the VLAN Manager application; however, VLANs are created on Stellar APs by mapping an AP Group to a VLAN in an Access Role Profile.

VLAN Overview

One of the main benefits of using VLANs to segment network traffic is that VLAN configuration and port assignment is handled through software. This eliminates the need to physically change a network device connection or location when adding or removing devices from the VLAN broadcast domain.

The initial configuration for all Alcatel-Lucent Enterprise (ALE) switches consists of a default VLAN 1 and all device ports are initially assigned to this VLAN. If additional VLANs are not

configured on the switch, then the entire switch is treated as one large broadcast domain. All ports will receive all traffic from all other ports.

In compliance with the IEEE 802.1Q standard, each VLAN is identified by a unique number, referred to as the VLAN ID. The user specifies a VLAN ID to create, modify or remove a VLAN and to assign switch ports to a VLAN. When a packet is received on a port, the VLAN ID for that port is inserted into the packet. The packet is then bridged to other ports that are assigned to the same VLAN ID. In essence, the VLAN broadcast domain is defined by a collection of ports and packets assigned to its VLAN ID.

The operational status of a VLAN remains inactive until at least one active switch port is assigned to the VLAN. This means that VLAN properties, such as Spanning Tree and/or router interfaces, also remain inactive. Ports are considered active if they are connected to an active network device. Non-active port assignments are allowed, but do not change the VLAN's operational state.

When using the OmniVista VLAN Manager application to configure VLANs in your network, consider the following:

- There is no staging of VLAN configuration changes. When you make a change to a VLAN, changes are sent directly to the device and are processed in real time.
- If an error occurs when changes are applied to a device, any changes successfully made to that point are maintained and not backed out of the switch configuration.
- The parameter values displayed in the VLANs Table, except for the VLAN ID field, are the values obtained from the switch polled that has the lowest IP host address. For example, if VLAN 5 exists on three different switches with IP addresses of 10.0.0.1, 10.0.0.2, and 10.0.0.3 and each instance of the VLAN has a different description, the VLAN 5 description from switch 10.0.0.1 is displayed in this window.
- When you modify VLAN parameters, however, the changes are applied across all switches in the topology that have this VLAN configured. For example, if you selected VLAN 10 and changed the description to "Marketing Department", all switches that contain VLAN 10 would receive this new description value.

VLANs Table

The VLANs Table displays VLANs configured on the network. To view VLANs configured on network devices, click on the Devices **ADD** button and select devices. The VLANs configured on those devices are displayed. To view VLANs configured on Stellar APs, click on the AP Groups **ADD** button and AP Groups. To add/remove devices/AP Groups from the display, click on the **EDIT** button to add/remove devices/AP Groups.

The VLANs Table displays basic information about each VLAN as shown below. To view detailed information about a VLAN, double click on the VLAN in the VLANs Table or select the VLAN and click the **View Details** button at the top of the VLANs Table.

- **VLAN ID -** In compliance with the IEEE 802.1Q standard, each VLAN is identified by a unique number, referred to as the VLAN ID. This number is assigned by the user at the time the VLAN is created and is not a modifiable parameter. When a network device packet is received on a port, the port's VLAN ID is inserted into the packet. The packet is then bridged to other ports that are assigned to the same VLAN ID. In essence, the VLAN broadcast domain is defined by a collection of ports and packets assigned to its VLAN ID. (Range = 1 - 4094)

- **Description -** A text string up to 32 characters. This parameter defaults to the VLAN ID number (e.g., VLAN 10) if a description is not specified at the time the VLAN is created.
- **VLAN Admin Status -** The administrative status of the VLAN (Enabled/Disabled). By default, the administrative status is enabled when a VLAN is created. When a VLAN is administratively disabled, static port and dynamic mobile port assignments are retained but traffic on these ports is not forwarded. However, VLAN rules remain active and continue to classify mobile port traffic for VLAN membership.
- **Oper Status -** The VLAN operational status (Active/Inactive). This parameter is not modifiable; switch software determines if the VLAN is operationally active or inactive and sets the appropriate field value. A VLAN's operational status remains inactive until at least one active switch port is assigned to the VLAN and the VLAN's administrative status is enabled. This means that VLAN properties, such as Spanning Tree or router ports, also remain inactive. Ports are considered active if they are connected to an active network device. Non-active port assignments are allowed, but do not change the VLAN's operational state.
- **VLAN Type -** The type of VLAN is determined at the time the VLAN is created (e.g., Standard, BVLAN, Control BVLAN).
- **Spanning Tree Status -** The Spanning Tree Status (Enabled/Disabled) for the VLAN. When a VLAN is created, an 802.1D standard Spanning Tree Algorithm and Protocol (STP) instance is enabled for the VLAN by default. STP evaluates VLAN port connections to determine if there are redundant data paths between the same VLAN on other switches. If a redundant path does exist, STP determines which path to block in order to provide a loop-free network topology. In this manner, STP ensures that there is always only one active data path between any two switches (VLANs). When a change occurs, such as a path is disconnected or a path cost change, the Spanning Tree Algorithm activates the blocked path to restore the network connection.
- **Router Protocol -** The protocol for the VLAN virtual router port. If no router port is configured for the VLAN, then "none" appears in this field. A VLAN is available for routing when a virtual router port is defined for that VLAN and at least one active port has joined the VLAN. If a VLAN does not have a router port, its ports are in essence firewalled from other VLANs.

  Note: The basic information displayed in the VLANs Table, except for the VLAN ID field, is the information obtained from the switch polled that has the lowest IP host address. For example, if VLAN 9 exists on three different switches with IP addresses of 10.0.0.1, 10.0.0.2, and 10.0.0.3 and each instance of the VLAN has a different description, the VLAN 9 description from switch 10.0.0.1 is displayed in this window. You can view detailed information on each device in the VLAN by double-clicking on a VLAN in the VLANs Table, or selecting a VLAN and clicking on the **View Details** button at the top of the VLANs Table.

Creating a VLAN

VLANs are created using a wizard that guides you through each of the steps needed to create the VLAN. You can create VLANs by Device or by Topology Map. The Create VLAN Wizard will then guide you through the process.

Creating VLANs by Device

Click on the **Create VLAN by Devices** button and complete the following screens in the VLAN Wizard, to create VLANs by selecting specific devices.

- **Device Selection -** Basic VLAN configuration parameters (e.g. VLAN ID, Description, administrative status) and device selection.
- **VLAN Configuration -** Review VLAN device selection and review/modify VLAN administrative status.
- **Default Ports Assignment -** Configure VLAN Ports on selected device(s).
- **Q-Tagged Ports Assignment -** Configure Q-Tagged Ports on selected device(s).
- **Review -** Review VLAN configuration and create VLAN.

  Note: When creating a VLAN, you can select up to 200 devices. If necessary, once the VLAN is created you can edit the VLAN to add additional devices. Again, for each edit, you can add up to 200 devices. Repeat to add additional devices. Also note that you can use the wizard to create a single VLAN or multiple VLANs.

Device Selection

The Device Selection Screen is used to configure basic VLAN configuration parameters and select devices to be included in the VLAN. You can create a single VLAN or create multiple VLANS. When you have completed all of the parameters, click the **Next** button at the bottom of the screen or click on VLAN Configuration on the left side of the screen to move to the next step.

- **VLAN Overwrite -** Enables/Disables VLAN Overwrite. When the Overwrite option is enabled, the VLANs which will be overridden are notified when the user inputs a new range. All current configuration discovered by OV will be replaced with new VLAN configuration, including devices or ports configured with the VLANs.
- **VLAN Template -** Select a VLAN Template from the drop-down menu.
- **VLAN IDs -** The VLAN ID number (Range = 2 - 4094). To create a single VLAN, enter a single VLAN ID and click on the Add icon. Repeat to create multiple VLANS, or enter a range of VLANs (e.g., 500-505) and click on the Add icon. Note that you cannot enter a VLAN ID for a VLAN that has already been created. If you want to add additional devices to an existing VLAN, return to the VLANs Table and edit the VLAN to add the additional devices.
- **VLAN Configuration Template -** The VLAN Configuration Template contents are applied to all selected devices, subject to availability of ports on devices. Users can override these settings.
  - **VLAN(s) Admin Status -** The administrative status of the VLAN (Enabled/Disabled).
  - **Default VLAN ID** (Multiple VLAN Configuration Only) **-** If you are configuring multiple VLANs, enter the VLAN ID of one of the VLANs. This will be the default VLAN for the configured ports.
  - **Default Ports Template -** Used to configure default (untagged) ports for all selected devices. The configuration will be added to selected devices if the port is available on device. For example, if you enter port 1/5 as a default port when creating VLAN 100, port 1/5 will be added as a default port for all devices having port 1/5. If a selected device does not have port 1/5, the default port will not be created on the device. Ports or Link Aggregates must be entered in the format shown (e.g., LAG-1, lag-1,

1/1, 1/2a, 1/1-1/7, 1/1/1, 1/1/1a, 1/1/1-1/1/7). Note that you will be able to add additional ports (or remove ports) on the Default Ports Assignment Screen later in the wizard.

- **Q Tagged Ports Template -** Used to configure Q-Tagged ports for all selected devices. The configuration will be added to selected devices if the port is available on device. For example, if you enter port 1/3 as a Q-Tagged Port when creating VLAN 100, port 1/3 will be added as a Q-Tagged port for all devices having port 1/3. If a selected device does not have port 1/3, the Q-Tagged port will not be created on the device. Ports or Link Aggregates must be entered in the format shown (e.g., LAG-1, lag-1, 1/1, 1/2a, 1/1-1/7, 1/1/1, 1/1/1a, 1/1/1-1/1/7). Note that you will be able to add additional ports (or remove ports) on the Q-Tagged Ports Assignment Screen later in the wizard. Also note that for wireless devices, Q-Tagged Port configuration is supported on trunk ports.
- **VLAN(s) Description -** Enter an optional description for the VLAN(s). If you do not enter a description, the VLAN ID is used.
- **Device Selection -** Select an option from the drop-down menu (Use Switch Picker/ Use Topology) and click **Add Remove Device** button to select devices for the VLAN.

  Note: When creating a VLAN, you can select up to 200 devices. If necessary, once the VLAN is created you can edit the VLAN to add additional devices. Again, for each edit, you can add up to 200 devices. Repeat to add additional devices. Also note that you can use the wizard to create a single VLAN or multiple VLANs.

VLAN Configuration

The VLAN Configuration Screen is used to review VLAN device selection and review/modify VLAN administrative status. If necessary, click the **Back** button to modify the device selection, or click on the **Admin state configuration** button to change the VLAN administrative state. When you are finished, click the **Next** button at the bottom of the screen or click on Default Ports Assignment on the left side of the screen to move to the next step.

Default Ports Assignment

The Default Ports Assignment Screen is used to configure ports on the selected device(s) to be included in the VLAN. Click on a device in the list and click on the **Add Ports for Device ...** button (or just click on the "Add Port" link under a device) to bring up the Port Selection Window. Select the device ports to be included in the VLAN and click **OK**. Repeat to add ports for additional devices.

Note that ports added on the Device Selection Screen of the wizard in the VLAN Configuration Template will be "pre-selected" on the Default Ports Selection window. You can add additional ports or remove ports. Also note that Q-Tagged Ports will not be available for selection.

After selecting ports for each device, click the **Next** button at the bottom of the screen or click on Q Tagged Ports Assignment on the left side of the screen to move to the next step.

Q Tagged Ports Assignment

The Q Tagged Ports Assignment Screen is used to configure Q-Tagged Ports on the selected device(s) to be included in the VLAN. Click on a device in the list and click on the **Add Q Tagged Ports for Device ...** button (or just click on the "Add Port" link under a device) to bring up the Port Selection Window. Select the device ports to be included in the VLAN and click **OK**. Repeat to add ports for additional devices.

Note that ports added on the Device Selection Screen of the wizard in the VLAN Configuration Template will be "pre-selected" on the Tagged Ports Selection window. You can add additional ports or remove ports. Also note that ports selected on Default Port Assignment Screen will not available for selection.

After selecting ports for each device, click the **Next** button at the bottom of the screen or click on Review on the left side of the screen to move to the next step.

Review

The Review Screen is used to review the VLAN configuration. VLAN Configuration Template information is displayed at the top of the window; and a list of devices contained in the configured VLAN is displayed. By default, the List of Switches displays device configuration information. Click on a link at the top of the table to display Port, or Link Aggregate information. If you have created VLANs by map, the Map Name is displayed. You can click on the map name to go to the Topology application and view the map.

After reviewing the configuration, click the **Create** button to create the VLAN. You can also click the **Back** button to return to a previous screen and modify the configuration before returning to this screen to create it.

Creating VLANs by Maps

Click on the **Create VLAN by Map** button and complete the following screens in the VLAN Wizard, to create VLANs on all devices in a specific Topology Map.

- **Map Selection -** Select devices contained in a Topology Map.
- **Review -** Review VLAN configuration and create VLAN.

Map Selection

The Map Selection Screen is used to configure basic VLAN configuration parameters on devices contained in a Topology Map. You can create a single VLAN or create multiple VLANS. When you have completed all of the parameters, click the **Next** button at the bottom of the screen or click on Review on the left side of the screen to move to the next step.

- **VLAN Overwrite -** Enables/Disables VLAN Overwrite. When the Overwrite option is enabled, the VLANs which will be overridden are notified when the user inputs a new range. All current configuration discovered by OV will be replaced with new VLAN configuration, including devices or ports configured with the VLANs.
- **VLAN Template -** Select a VLAN Template from the drop-down menu.
- **VLAN IDs -** The VLAN ID number (Range = 2 - 4094). To create a single VLAN, enter a single VLAN ID and click on the Add icon. Repeat to create multiple VLANS, or enter a range of VLANs (e.g., 500-505) and click on the Add icon. Note that you cannot enter a VLAN ID for a VLAN that has already been created. If you want to add additional devices to an existing VLAN, return to the VLANs Table and edit the VLAN to add the additional devices.
- **VLAN Configuration Template** - The VLAN Configuration Template contents are applied to all selected devices, subject to availability of ports on devices. Users can override these settings.
  - **VLAN(s) Admin Status -** The administrative status of the VLAN (Enabled/Disabled).
  - **Map Name -** Select a map from the drop-down menu.

- **VLAN(s) Description -** Enter an optional description for the VLAN(s). If you do not enter a description, the VLAN ID is used.

  Note: If a device in a map has LLDP links that were created by a mobile port(s), the VLAN(s) will not be created on that device.

Review

The Review Screen is used to review the VLAN configuration. VLAN Configuration Template information is displayed at the top of the window; and the Map Name is displayed. You can click on the map name to go to the Topology application and view the map.

Editing a VLAN

Select the VLAN in the VLANs Table and click on the Edit icon. The Edit VLAN Wizard appears. Use the wizard to make any edits. When you are done, go the Review Window in the wizard and click on the **Apply** button to update the VLAN. Note that you cannot edit the VLAN ID.

Copying a VLAN

You can save time creating a new VLAN by copying an existing VLAN and modifying the configuration. Select a VLAN in the VLANs Table and click on the Copy icon. The Create VLAN Wizard will appear. Enter a new VLAN ID and use the wizard to create the new VLAN.

Deleting a VLAN

You can delete a VLAN(s) completely - delete the VLAN(s) and delete them from all devices; or you can delete a VLAN(s) from specific devices.

- To delete a VLAN(s) completely, select the VLAN(s) in the VLANs Table, click on the Delete icon, and click **OK** at the confirmation prompt. The VLAN(s) will be removed from OmniVista and from all network devices to which it was assigned.
- To delete a VLAN from specific devices, select the VLAN in the VLANs Table and click on the Edit icon. The Edit VLAN Wizard appears. On the Device Selection Screen, click on the **Add/Remove Devices** button and user the Switch Picker or Topology application to remove devices from the VLAN. Go to the Review Screen to review the devices and click on the **Apply** button.

  Note: You cannot delete a VLAN from more than 200 devices at a time.

VLAN Actions

You can perform the following actions on VLANs by selecting a VLAN(s) in the VLANs Table and clicking on the **Actions** button at the top of the screen: enable/disable VLANs, view/modify Spanning Tree parameters, view/configure an IP Router, and view VLAN details.

Enabling/Disabling VLANs

To enable/disable a VLAN(s), select one or more VLANs in the table, click on the **Actions** button and select **Enable** or **Disable**. The Results Screen displays the operation results. Click **OK** to return to the VLAN Manager Screen.

Viewing/Modifying Spanning Tree

The Spanning Tree Screen in the VLANs application is used to view Spanning Tree configuration information for devices in a VLAN, and to modify Spanning Tree Bridge or Port Parameters. To view/edit Spanning Tree information for a VLAN, select the VLAN in the VLANs Table, then select **Spanning Tree** from the **Actions** drop-down menu at the top of the screen.

Viewing Spanning Tree Configuration

The VLAN Manager Spanning Tree Screen is used to view Spanning Tree configuration information for devices in a VLAN; and to edit Spanning Tree Bridge and Port parameters. By default, a Summary view is displayed. Click on the Bridge or Port link at the top of the to view bridge or port information.

Summary View

The Summary View displays a summary of the Spanning Tree information for devices in the selected VLAN.

- **Device Friendly Name -** The user-defined name for the device.
- **Device IP -** The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.
- **Protocol -** The VLAN spanning tree algorithm protocol. The algorithm determines the state and role of a port within the spanning tree topology:
  - **STP (802.1D) -** Standard Spanning Tree Algorithm and Protocol (Default).
  - **RSTP (802.1W) -** Rapid Spanning Tree Algorithm and Protocol. RSTP is based on the 802.1D standard algorithm and is designed to provide quick recovery in the event of a link, port or device failure.
  - **MSTP (802.1S) -** Multiple Spanning Tree Protocol. MSTP is an enhancement to 802.1Q Common Spanning Tree Instance (CST). When the switch is running in Flat Mode, a single Spanning Tree instance is applied across all VLAN port connections. MSTP allows the configuration of Multiple Spanning Tree Instances (MSTI) in addition to the CST instance. Each MSTI is mapped to a set of VLANs. As a result, Flat Mode can now support the forwarding of VLAN traffic over separate data paths. Note that MSTP in VLAN spanning tree view is only displayed for Instance 0 under VLAN 1. None of the other instances will be displayed.
- **Priority -** The bridge priority value (0 - 65535) for the VLAN. The lower the number, the higher the priority value. The bridge priority value is used by the spanning tree algorithm to determine which VLAN should serve as the root of the spanning tree. (Default = 32768)
- **Maximum Age -** The amount of time, in seconds, that spanning tree information learned from BPDUs received on VLAN ports is retained. When this information has aged beyond the maximum age value, the information is discarded. (Range = (6- 40, Default = 20)
- **Path Cost -** The cost of the path to the root for this Spanning Tree instance.
- **Mode -** The Spanning Tree operating mode for the switch:

    - **Flat Mode (Single Spanning Tree) -** The Spanning Tree Algorithm is applied across all VLANs. For example, if a port belonging to VLAN 10 and a port belonging to VLAN 20 both connect to the same switch, then Spanning Tree Algorithm will block one of these ports.
    - **1x1 (One Spanning Tree per VLAN) -** A single Spanning Tree instance is enabled for each VLAN configured on the switch. For example, if there are five VLANs configured on the switch, then there are five separate Spanning Tree instances. In essence, a VLAN is a virtual bridge in that it will have its own bridge ID and configurable STP parameters, such as protocol, priority, hello time, max age and forward delay. Note: By default, the Spanning Tree operating mode is set to One Spanning Tree Per VLAN (available only on AOS switch platforms).
- **Bridge ID -** The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the bridge MAC address.
- **Root ID-** The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Algorithm and Protocol.
- **Time Since Last Topology Change -** The amount of time, in hundredths of a second, since the last topology change was detected by this Spanning Tree instance.
- **Total Topology Change -** The number of topology changes detected by this spanning tree instance since the management entity was last reset or initialized.
- **Root Port -** The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.
- **Next Best Root Cost -** The cost of the next best root port for this Spanning Tree instance.
- **Next Best Root Port -** The port that offers the next best (second lowest) cost path to the root bridge for this Spanning Tree instance.
- **Network Maximum Age -** The Maximum Age time value for the root bridge.
- **Network Hello Time -** The Hello Time value for the root bridge.
- **Network Hold Time -** The amount of time, in hundredths of a second, in which this spanning tree instance can transmit no more than two Configuration Bridge Protocol Data Units (BPDU).
- **Network Forward Delay -** The forward delay time value for the root bridge.

Bridge View

The Bridge View List displays a Spanning Tree bridge information for devices in the selected VLAN.

- **Device Friendly Name -** The user-defined name for the device.
- **Device IP -** The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.
- **Protocol -** The VLAN spanning tree algorithm protocol. The algorithm determines the state and role of a port within the spanning tree topology:
    - **STP (802.1D) -** Standard Spanning Tree Algorithm and Protocol (Default).

  - **RSTP (802.1W) -** Rapid Spanning Tree Algorithm and Protocol. RSTP is based on the 802.1D standard algorithm and is designed to provide quick recovery in the event of a link, port or device failure.
  - **MSTP (802.1S) -** Multiple Spanning Tree Protocol. MSTP is an enhancement to 802.1Q Common Spanning Tree Instance (CST). When the switch is running in Flat Mode, a single Spanning Tree instance is applied across all VLAN port connections. MSTP allows the configuration of Multiple Spanning Tree Instances (MSTI) in addition to the CST instance. Each MSTI is mapped to a set of VLANs. As a result, Flat Mode can now support the forwarding of VLAN traffic over separate data paths. Note that MSTP in VLAN spanning tree view is only displayed for Instance 0 under VLAN 1. None of the other instances will be displayed.
- **Priority -** The bridge priority value (0 - 65535) for the VLAN. The lower the number, the higher the priority value. The bridge priority value is used by the spanning tree algorithm to determine which VLAN should serve as the root of the spanning tree. (Default = 32768)
- **Maximum Age -** The amount of time, in seconds, that spanning tree information learned from BPDUs received on VLAN ports is retained. When this information has aged beyond the maximum age value, the information is discarded. (Range = 6- 40, Default = 20)
- **Hello Time -**The Hello Time value for the root bridge.
- **Forward Delay -**The forward delay time value for the root bridge.

Port View

The Port View List displays a Spanning Tree port information for devices in the selected VLAN.

- **Device Friendly Name -** The user-defined name for the device.
- **Device IP -** The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.
- **Port -** The slot/port number.
- **Priority -**The port priority value for the VLAN. The lower the number, the higher the priority value. The port priority is used to determine which port offers the best path to the root when multiple paths have the same path cost. If the priority values are the same for all ports in the path, then the port with the lowest physical switch port number is selected. (Range = (0 - 15, Default = 7)
- **Oper Status -** The operational state of the port as determined by the spanning tree algorithm:
  - **Disabled -** Physical port is down or administratively disabled.
  - **Blocking or Discarding -** Port does not transmit or receive data to prevent a network loop.
  - **Listening -** Port is preparing to transmit data.
  - **Learning -** Port is learning MAC addresses seen on the port.
  - **Forwarding -** Port is transmitting and receiving data.

- **Admin Status -** The Spanning Tree status for the port (Enabled/Disabled). If disabled, the port state is set to forwarding for the VLAN Spanning Tree instance. This status value, however, is ignored if Spanning Tree is disabled for the associated VLAN. By default, Spanning Tree is enabled on all switch ports.
- **Path Cost -** The path cost value for the port. This value specifies the contribution of a port to the path cost towards the root bridge that includes the port. If the path cost is set to 0, then a default value based on link speed is used. (Range = (0 - 65535).
- **Manual Mode -** The mode used for managing the port's state:
  - **Blocking or Forwarding (Manually Set) -** If the port state is manually set to Blocking or Forwarding, the port remains in that state until it is changed and does not participate in the spanning tree algorithm.
  - **No (Dynamic) -** Dynamic mode defers configuration of the port state to the spanning tree algorithm. By default, this parameter is set to No (Dynamic).
- **Admin Connection -** The port's administratively set connection type. This parameter is used by the 802.1w Rapid Spanning Tree Protocol (RSTP) to determine if a port is eligible for rapid transition to the forwarding state.
  - **No Point to Point -** Port connects to multiple switches.
  - **Point to Point -** Port connects directly to another switch.
  - **Auto Point to Point -** Connection type is automatically defined to No Point to Point or Point to Point based on the port's operational status. (Default)
  - **Edge Port -** Port is at the edge of a bridged LAN, does not receive BPDU, and has only one MAC address learned. Edge ports, however, will operationally revert to a No Point to Point connection type if a BPDU is received on the port.
- **Port Role -** The role of the port for this Spanning Tree instance (e.g., Root, Designated, Alternate, Backup).
- **Oper Connection -** The operational connection type for the port:
  - **No Point to Point -** Port connects to multiple switches.
  - **Point to Point -** Port connects directly to another switch.
  - **Auto Point to Point -** Connection type is automatically defined to No Point to Point or Point to Point based on the port's operational status. (Default)
  - **Edge Port -** Port is at the edge of a bridged LAN, does not receive BPDU, and has only one MAC address learned. Edge ports, however, will operationally revert to a No Point to Point connection type if a BPDU is received on the port.
  - **Non-Significant -** Port is inactive.

Editing an STP Configuration

You can edit Spanning Tree Bridge or Port parameters on switches in a VLAN. Select the VLAN in the VLANs Table, then select Spanning Tree from the **Actions** drop-down menu at the top of the screen to bring up the Spanning Tree Summary View Table for the VLAN. Click on the Bridge or Port link at the top of the table to bring up the Bridge or Port Table. Select a switch/port in a table then click on the Edit icon. Edit the Bridge or Port parameters as described below and click on the **Apply** button. Repeat to edit additional Bridge or Port parameters.

> **Note:** Spanning Tree software is active on all switches by default. As a result, a loop-free network topology is automatically calculated based on default Spanning Tree switch, VLAN (bridge), and port parameter values. It is only necessary to configure

Spanning Tree bridge parameters to change how the topology is calculated and maintained.

STP Bridge Parameters

- **Protocol -** The VLAN spanning tree algorithm protocol. The algorithm determines the state and role of a port within the spanning tree topology:
  - **STP (802.1D) -** Standard Spanning Tree Algorithm and Protocol (Default).
  - **RSTP (802.1W) -** Rapid Spanning Tree Algorithm and Protocol. RSTP is based on the 802.1D standard algorithm and is designed to provide quick recovery in the event of a link, port or device failure.
  - **MSTP (802.1S) -** Multiple Spanning Tree Protocol. MSTP is an enhancement to 802.1Q Common Spanning Tree Instance (CST). When the switch is running in Flat Mode, a single Spanning Tree instance is applied across all VLAN port connections. MSTP allows the configuration of Multiple Spanning Tree Instances (MSTI) in addition to the CST instance. Each MSTI is mapped to a set of VLANs. As a result, Flat Mode can now support the forwarding of VLAN traffic over separate data paths. Note that MSTP in VLAN spanning tree view is only displayed for Instance 0 under VLAN 1. None of the other instances will be displayed.
- **Priority -** The bridge priority value (0 - 65535) for the VLAN. The lower the number, the higher the priority value. The bridge priority value is used by the spanning tree algorithm to determine which VLAN should serve as the root of the spanning tree. (Default = 32768)
- **Maximum Age -** The amount of time, in seconds, that spanning tree information learned from BPDUs received on VLAN ports is retained. When this information has aged beyond the maximum age value, the information is discarded. (Range = (6- 40, Default = 20)
- **Hello Time -**The Hello Time value for the root bridge.
- **Forward Delay -**The forward delay time value for the root bridge.

STP Port Parameters

- **Priority -**The port priority value for the VLAN. The lower the number, the higher the priority value. The port priority is used to determine which port offers the best path to the root when multiple paths have the same path cost. If the priority values are the same for all ports in the path, then the port with the lowest physical switch port number is selected. (Range = (0 - 15, Default = 7)
- **Admin Status -** The Spanning Tree status for the port (Enabled/Disabled). If disabled, the port state is set to forwarding for the VLAN Spanning Tree instance. This status value, however, is ignored if Spanning Tree is disabled for the associated VLAN. By default, Spanning Tree is enabled on all switch ports.
- **Path Cost -** The path cost value for the port. This value specifies the contribution of a port to the path cost towards the root bridge that includes the port. If the path cost is set to 0, then a default value based on link speed is used. (Range = (0 - 65535).
- **Admin Connection -** The port's administratively set connection type. This parameter is used by the 802.1w Rapid Spanning Tree Protocol (RSTP) to determine if a port is eligible for rapid transition to the forwarding state.
  - **No Point to Point -** Port connects to multiple switches.

- **Point to Point -** Port connects directly to another switch.
- **Auto Point to Point -** Connection type is automatically defined to No Point to Point or Point to Point based on the port's operational status. (Default)
- **Edge Port -** Port is at the edge of a bridged LAN, does not receive BPDU, and has only one MAC address learned. Edge ports, however, will operationally revert to a No Point to Point connection type if a BPDU is received on the port.

Viewing/Configuring IP Routers

The IP Router Screen in the VLANs application is used to view/configure IP Routers on a VLAN. To configure an IP router for a VLAN, select the VLAN in the VLANs Table, then select **IP Router** from the **Actions** drop-down menu at the top of the screen. The IP Router Screen will appear. Click on the Add icon to create an IP router for the VLAN.

IP Router Screen

The VLAN Manager IP Router Screen displays all configured IP router interfaces for the selected VLAN. It is also used to create, edit, and delete IP router interfaces on devices in the VLAN. Network device traffic is bridged (switched) at the Layer 2 level between ports that are assigned to the same VLAN. However, if a device needs to communicate with another device that belongs to a different VLAN, you must configure an IP router interface on a device in the VLAN to enable Layer 3 routing to transmit traffic between VLANs. A VLAN is available for routing when at least one IP router interface is defined for that VLAN and at least one active port is associated with the VLAN. If a VLAN does not have a router interface, the ports associated with that VLAN are in essence firewalled from other VLANs.

Creating an IP Router Interface

Click on the Add icon to create an IP router interface on a device in a VLAN. Complete the fields as described below, then click on the **Create** button.

- **Device -** Select an option from the drop-down menu (Use Switch Picker/Use Topology) and click on the **Select Device** button. A list of devices that are members of the VLAN is displayed. Select the device on which you want to create an IP router interface and click **OK**.
- **Router IP Address -** The IP address of the IP router interface. Router interface IP addresses must be unique. You cannot have two router interfaces with the same IP address.
- **Router IP Mask -** The IP router subnet mask value. The default value for this field is based on which network class range the IP address falls within; Class A, B, or C. (255.0.0.0, 255.255.0.0, or 255.255.255.0).
- **IP Encapsulation -** The IP router interface frame encapsulation value (Ethernet 2 or SNAP). The frame encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. (Default = Ethernet 2)
- **IP Forwarding -** The router interface forwarding status (Enabled/Disabled). A forwarding router interface sends IP frames to other subnets. A "no forwarding" router interface acts as a host only. It receives IP frames from other router interfaces. (Default = Enabled).
- **Interface Name -** The user-defined interface name (up to 20 characters).

- **VRF ID -** The VRF ID. If configured, select a VRF from the drop-down menu to assign the interface to a configured VRF instance (by default all interfaces are assigned to the Default VRF). You can assign a new interface to a VRF; however, you cannot edit the VRF ID of an existing interface. If the feature is not available on the device, the column will display "Default", indicating that the switch is operating as a single routing instance. VRF instances are created on the switch through the CLI or WebView application. See the "Configuring Multiple VRF" Chapter in the applicable *OmniSwitch AOS Network Configuration Guide* for detailed instructions on configuring VRF instances.

Editing an IP Router Interface

To edit an IP router interface on a device, select the interface in the IP Router Table and click on the Edit icon. Edit any fields as described above and click on the **Apply** button. Note that you cannot edit the Interface Name or VRF fields.

Deleting an IP Router Interface

To delete an IP router interface, select the interface in the IP Router Table, click on the Delete icon, then click **OK** at the Confirmation Prompt.

Viewing IP Router Interfaces

The Router Screen displays all configured IP router interfaces for the selected VLAN. The fields are defined below.

- **Device Name -** The user-configured name for the device on which the interface is configured.
- **Device Friendly Name -** The IP address of the device.
- **Device IP Address -** The IP address of the device.
- **Router IP Address -** The IP address of the IP router interface.
- **Router IP Mask -** The IP router subnet mask value. The default value for this field is based on which network class range the IP address falls within; Class A, B, or C. (255.0.0.0, 255.255.0.0, or 255.255.255.0).
- **IP Encapsulation -** The IP router interface frame encapsulation value (Ethernet 2 or SNAP). The frame encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. (Default = Ethernet 2)
- **IP Forwarding -** The router interface forwarding status (Enabled/Disabled). A forwarding router interface sends IP frames to other subnets. A "no forwarding" router interface acts as a host only. It receives IP frames from other router interfaces. (Default = Enabled).
- **Interface Name -** The user-defined interface name (up to 20 characters).
- **VRF ID -** The VRF ID. If multiple VRFs are configured on the device, the VRF ID is displayed. If none are configured, or if the feature is not available on the device, the column will display "Default", indicating that the switch is operating as a single routing instance.

VLAN Details

The VLANs Table displays VLANs configured on the network. To view VLANs configured on network devices, click on the Devices **ADD** button and select devices. The VLANs configured on those devices are displayed. To view VLANs configured on Stellar APs, click on the AP Groups **ADD** button and AP Groups. To add/remove devices/AP Groups from the display, click on the **EDIT** button.

The VLANs Table displays basic information about each VLAN. To view detailed information about a VLAN, select the VLAN, click on the **View Details** button at the top of the VLANs Table.

Basic Information

The VLANs Table displays basic information about each VLAN.

- **VLAN ID -** In compliance with the IEEE 802.1Q standard, each VLAN is identified by a unique number, referred to as the VLAN ID. This number is assigned by the user at the time the VLAN is created and is not a modifiable parameter. When a network device packet is received on a port, the port's VLAN ID is inserted into the packet. The packet is then bridged to other ports that are assigned to the same VLAN ID. In essence, the VLAN broadcast domain is defined by a collection of ports and packets assigned to its VLAN ID. (Range = 1 - 4094)
- **Description -** A text string up to 32 characters. This parameter defaults to the VLAN ID number (e.g., VLAN 10) if a description is not specified at the time the VLAN is created.
- **Admin Status -** The administrative status of the VLAN (Enabled/Disabled). By default, the administrative status is enabled when a VLAN is created. When a VLAN is administratively disabled, static port and dynamic mobile port assignments are retained but traffic on these ports is not forwarded. However, VLAN rules remain active and continue to classify mobile port traffic for VLAN membership.
- **Oper Status -** The VLAN operational status (Active/Inactive). This parameter is not modifiable; switch software determines if the VLAN is operationally active or inactive and sets the appropriate field value. A VLAN's operational status remains inactive until at least one active switch port is assigned to the VLAN and the VLAN's administrative status is enabled. This means that VLAN properties, such as Spanning Tree or router ports, also remain inactive. Ports are considered active if they are connected to an active network device. Non-active port assignments are allowed, but do not change the VLAN's operational state.
- **VLAN Type -** The type of VLAN is determined at the time the VLAN is created (e.g., Standard, BVLAN, Control BVLAN).
- **Spanning Tree Status -** The Spanning Tree Status (Enabled/Disabled) for the VLAN. When a VLAN is created, an 802.1D standard Spanning Tree Algorithm and Protocol (STP) instance is enabled for the VLAN by default. STP evaluates VLAN port connections to determine if there are redundant data paths between the same VLAN on other switches. If a redundant path does exist, STP determines which path to block in order to provide a loop-free network topology. In this manner, STP ensures that there is always only one active data path between any two switches (VLANs). When a change occurs, such as a path is disconnected or a path cost change, the Spanning Tree Algorithm activates the blocked path to restore the network connection.
- **Router Protocol -** The protocol for the VLAN virtual router port. If no router port is configured for the VLAN, then "none" appears in this field. A VLAN is available for

routing when a virtual router port is defined for that VLAN and at least one active port has joined the VLAN. If a VLAN does not have a router port, its ports are in essence firewalled from other VLANs.

Detailed View

The VLAN Details Screens provide detailed information about devices in the selected VLAN. By default, the Device View is displayed. Click on a link at the top of the screen to display Device, Port, AP Group, or Link Aggregate information.

Devices

- **Friendly Name -** The IP address of the device.
- **Device Name -** The user-configured name for the device.
- **Device IP Address -** The IP address of the device.
- **Device MAC Address -** The MAC address of the device.
- **Device Version -** The version number of the device software. OmniVista may not be able to determine the software version on some third-party devices. In these cases, the field will be blank.
- **Device Location -** The physical location of the device (user-defined, up to 255 characters). If the user did not specify a location the field displays "Unknown".
- **Device Status -** This field displays the operational status of the device:
  - Up - Device is up and responding to polls.
  - Down - Device is down and not responding to polls.
  - Warning - Device has sent at least one warning or critical trap
- **Device Type -** The device model (e.g., OS6900-X72).
- **VLAN ID -** The VLAN ID number (e.g., VLAN 10).
- **VLAN Description -** A text string up to 32 characters. This parameter defaults to the VLAN ID number (e.g., VLAN 10) if a description is not specified at the time the VLAN is created.
- **VLAN Admin Status -** The administrative status of the VLAN (Enabled/Disabled). By default, the administrative status is enabled when a VLAN is created. When a VLAN is administratively disabled, static port and dynamic mobile port assignments are retained but traffic on these ports is not forwarded. However, VLAN rules remain active and continue to classify mobile port traffic for VLAN membership.
- **VLAN Type -** The type of VLAN is determined at the time the VLAN is created (e.g., Standard, BVLAN, Control BVLAN).
- **Spanning Tree Status -** The Spanning Tree Status for the VLAN (Enabled/Disabled). When a VLAN is created, an 802.1D standard Spanning Tree Algorithm and Protocol (STP) instance is enabled for the VLAN by default. STP evaluates VLAN port connections to determine if there are redundant data paths between the same VLAN on other switches. If a redundant path does exist, STP determines which path to block in order to provide a loop-free network topology. In this manner, STP ensures that there is always only one active data path between any two switches (VLANs). When a change occurs, such as a path is disconnected or a path cost change, the Spanning Tree Algorithm activates the blocked path to restore the network connection.

- **Mobility -** The mobile status for the VLAN (Enabled/Disabled). On AOS switches, mobility is not enabled or disabled at the VLAN level. Instead, switch ports are designated as mobile or non-mobile.
- **Oper Status -** The VLAN operational status (Active/Inactive). This parameter is not modifiable; switch software determines if the VLAN is operationally active or inactive and sets the appropriate field value. A VLAN's operational status remains inactive until at least one active switch port is assigned to the VLAN and the VLAN's administrative status is enabled. This means that VLAN properties, such as Spanning Tree or router ports, also remain inactive. Ports are considered active if they are connected to an active network device. Non-active port assignments are allowed, but do not change the VLAN's operational state.
- **Authentication -** The authentication status for the VLAN (Enabled/Disabled). By default, authentication is disabled when a VLAN is created. Once authentication is enabled on a VLAN, however, then only authenticated mobile port devices can join the VLAN after completing the appropriate log-in process. Layer 2 authentication uses VLAN membership to grant access to network resources. Authenticated VLANs control membership through a log-in process; this is sometimes called user authentication. A VLAN must have authentication enabled before it can participate in the Layer 2 authentication process.
- **Voice Status -** Administrative status (Enabled/Disabled) of voice usage for the current VLAN (supported on 6.x devices only).
- **Router Protocol -** The protocol for the VLAN virtual router port. If no router port is configured for the VLAN, then "N/A" appears in this field. A VLAN is available for routing when a virtual router port is defined for that VLAN and at least one active port has joined the VLAN. If a VLAN does not have a router port, its ports are in essence firewalled from other VLANs.

AP Groups

- **AP Group Name -** The name of the AP Group associated with the VLAN.

Port View

- **Device Friendly Name -** The IP address of the device.
- **Device IP Address -** The IP address of the device.
- **Port -** The VLAN slot/port number.
- **Port Description -** A user-configured port description, if applicable.
- **Port Type -** The Port Type parameter indicates how the port assignment to the current VLAN was made.
  - **Default -** The port is a fixed port that was statically assigned to the VLAN, which is now the configured default VLAN for the port.
  - **Q Tagged -** The port is a fixed port that was statically assigned to the VLAN using the 802.1Q tagging feature. The VLAN is a static secondary VLAN assignment for the 802.1Q tagged port.
  - **Mobile -** The port is a mobile port that was dynamically assigned to the VLAN when traffic received on the port match traffic rules defined for the VLAN. The VLAN is a dynamic secondary VLAN assignment for the mobile port.
- **Port State -** The status of the VLAN port assignment.

- **Forwarding -** Port is active and forwarding traffic on this VLAN.
- **Inactive -** Port is not active (administratively disabled, down, or nothing is connected to the port).
- **Blocking -** Port is active, but not forwarding any traffic on this VLAN.
- **Filtering -** Mobile port traffic is filtered for the VLAN; only traffic received on the port that matches VLAN rules is forwarded. Occurs when a mobile port's VLAN is administratively disabled or the port's default VLAN status is disabled. Does not apply to fixed ports.

Link Aggregate View

- **Friendly Name -** The IP address of the device.
- **Device IP Address -** The IP address of the device.
- **Link Aggregate ID-** The ID of the link aggregate group of ports. This number was assigned when the aggregate was created.
- **Link Aggregate -** An optional textual description (up to 32 characters) for the link aggregate.
- **Port Type -** The Port Type parameter indicates how the port assignment to the current VLAN was made.
  - **Default -** The port is a fixed port that was statically assigned to the VLAN, which is now the configured default VLAN for the port.
  - **Q Tagged -** The port is a fixed port that was statically assigned to the VLAN using the 802.1Q tagging feature. The VLAN is a static secondary VLAN assignment for the 802.1Q tagged port.
  - **Mobile -** The port is a mobile port that was dynamically assigned to the VLAN when traffic received on the port match traffic rules defined for the VLAN. The VLAN is a dynamic secondary VLAN assignment for the mobile port.
- **Description -** The standard MIB name for this dynamic aggregate group.

MVRP

Multiple VLAN Registration Protocol (MVRP) provides a mechanism for dynamic maintenance of the contents of dynamic VLAN registration entries for each VLAN, and for propagating the information they contain to other bridges. This information allows MVRP-aware devices to dynamically establish and update their knowledge of the set of VLANs that currently have active members, and through which ports those members can be reached. The main purpose of MVRP is to allow switches to automatically discover some of the VLAN information that would otherwise have to be manually configured.

To configure MVRP, click on the link on the left side of the screen. The MVRP Configuration Wizard guides you through the steps to configure MVRP on network switches/ports.

> **Note:** Dynamic VLAN configuration is not supported on 5x devices; only standard (static) VLAN configuration is supported.

Summary View

The MVRP Summary View Screen displays an overview of MVRP switch and port configuration on the network. MVRP provides a mechanism for dynamic maintenance of the contents of

dynamic VLAN registration entries for each VLAN, and for propagating the information they contain to other bridges. This information allows MVRP-aware devices to dynamically establish and update their knowledge of the set of VLANs that currently have active members, and through which ports those members can be reached. The main purpose of MVRP is to allow switches to automatically discover some of the VLAN information that would otherwise have to be manually configured.

MVRP acts as an MRP application, sending and receiving MVRP information encapsulated in an ethernet frame on a specific MAC address. MVRP allows both end stations and bridges in a bridged local area network to issue and revoke declarations relating to membership of VLANs. Each MVRP device that receives the declaration in the network creates or updates a dynamic VLAN registration entry in the filtering database to indicate that the VLAN is registered on the reception port.

Switches List

The Switches List provides an overview of MVRP configuration on network switches.

- **Device Friendly Name -** The IP address of the device.
- **Device IP -** The IP address of the device.
- **MVRP Status -** The MVRP administrative status on the switch (Enabled/Disabled)
- **Transparent Switch -** The administrative status of MVRP transparent switching on the switch. If enabled, when MVRP is globally disabled on the device, MVRP frames are flooded transparently. If disabled, the device will discard received MVRP frames. (Default = Disabled)
- **Max VLAN Limit -** The maximum number of dynamic VLANs that can be created by MVRP on the switch. (Range = 32 - 4094, Default = 256)
- **Registration Protocol -** The registration protocol running on the switch (MVRP/GVRP). (Default = MVRP)

Ports Configuration

Click on a switch in the Switches List to view MVRP port information for the switch.

- **Port -** The slot/port number of the MVRP interface. MVRP can be enabled on switch ports regardless of whether it is globally enabled on the switch. However, for the port to become an active participant in the MVRP operation, MVRP must be enabled globally on the switch. When MVRP is globally enabled on the switch and is not enabled on the port, that port is excluded from the MVRP protocol operation.
- **MVRP Status -** MVRP status for the port (Enabled/Disabled). MVRP can be enabled on switch ports regardless of whether it is globally enabled on the switch. However, for the port to become an active participant in the MVRP operation, MVRP must be enabled globally on the switch. When MVRP is globally enabled on the switch and is not enabled on the port, that port is excluded from the MVRP protocol operation. Note: MVRP can be enabled only on fixed ports, 802.1 Q ports, aggregate ports, and VLAN Stacking Network ports. Other ports (e.g., mirroring ports, VLAN Stacking User ports) do not support MVRP.
- **Registrar Mode -** The MVRP Registration Mode of the port:
  - **Normal -** Specifies that both registration and de-registration of VLANs is allowed. VLANs can be mapped either dynamically (through MVRP) or statically (through management application). (Default)

  - **Fixed -** Specifies that only static mapping of VLANs is allowed on the port, but de-registration of previously created dynamic or static VLANs is not allowed.
  - **Forbidden -** Specifies that dynamic VLAN registration or de-registration is not allowed on the port. Any dynamic VLANs created earlier are de-registered.
- **Applicant Mode -** The Applicant Mode of the port. This configures whether MVRP PDU exchanges are allowed on the port, depending on the port's Spanning Tree state:
  - **Participant -** MVRP PDU exchanges are only allowed when the port is in the STP forwarding state.
  - **Non-Participant -** MVRP PDUs are not sent in this mode, and PDUs received are processed as expected.
  - **Active -** MVRP PDU exchanges are allowed when the port is in the STP forwarding state or STP blocking state.
- **Periodic Timer -** The MVRP periodic-timer time interval, in seconds, for dynamically registering VLANs on the switch. The default timer setting is used unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP. (Default = 1).
- **Periodic Transmission -** The periodic transmission status on the port (Enabled/Disabled). (Default = Disabled)

Configuring MVRP

To configure MVRP, click on the link on the left side of the screen. The MVRP Configuration Wizard guides you through the steps to configure MVRP on network switches/ports.

Global Parameters

The MVRP Configuration Wizard Global Parameters Screen is used to configure global MVRP parameters on a switch. You can apply the existing global configuration to switches by selecting the **Keep Existing Global Configuration** radio button or you can select the **Apply New Configuration** radio button and change the global MVRP parameters as described below. When you are finished, click on the **Next** button or select **Port Parameters** on the left side of the screen to move to the next screen.

> **Note:** To view the current global configuration, click on the **Apply New Configuration** radio button.

- **MVRP Status -** Enables/Disables MVRP globally on the switch. To enable MVRP on a port, MVRP must be enabled on the switch. Disabling MVRP globally deletes all VLANs learned through MVRP. MVRP is supported only when the switch is operating in the flat Spanning Tree mode.
- **Transparent Switching -** Enables/Disables transparent switching for MVRP. If enabled, when MVRP is globally disabled on the device, MVRP frames are flooded transparently. If disabled, the device will discard received MVRP frames. (Default = Disabled)
- **Max VLAN Limit -** The maximum number of dynamic VLANs that can be created by MVRP. The Max VLAN Limit can be configured even if MVRP is not enabled on the switch. However, MVRP must be enabled on the switch for creating dynamic VLANs. If you set the VLAN limit to less than the current number of dynamically learned VLANs, the new configuration takes effect only after MVRP is disabled and re-enabled on the switch. The VLANs learned earlier are retained if this operation is not performed. (Range = 32 - 4094, Default = 256)

- **Registration Protocol -** The registration protocol running on the switch. (Default = MVRP)

Port Parameters

The MVRP Configuration Wizard Port Parameters Screen is used to configure global MVRP port parameters. You can apply the existing MVRP port parameters to switches by selecting the **Keep Existing Port Configuration** radio button or you can select the **Apply New Configuration** radio button and change the MVRP port parameters as described below. When you are finished, click on the **Next** button or select **Devices/Ports** on the left side of the screen to move to the next screen.

> **Note:** To view the current MVRP port parameters, click on the **Apply New Configuration** radio button.

- **MVRP Status -** The MVRP port status (Enabled/Disabled). MVRP can be enabled on switch ports regardless of whether it is globally enabled on the switch. However, for the port to become an active participant in the MVRP operation, MVRP must be enabled globally on the switch. When MVRP is globally enabled on the switch and is not enabled on the port, that port is excluded from the MVRP protocol operation. Note that MVRP can only be enabled on fixed ports, 802.1 Q ports, aggregate ports, and VLAN Stacking Network ports. Other ports (e.g., mirroring ports, VLAN Stacking User ports) do not support MVRP.
- **Registrar Mode -** The MVRP Registration Mode of the port:
  - **Normal -** Both registration and de-registration of VLANs is allowed. VLANs can be mapped either dynamically (through MVRP) or statically (through management application). (Default)
  - **Fixed -** Only static mapping of VLANs is allowed on the port, but de-registration of previously created dynamic or static VLANs is not allowed.
  - **Forbidden -** Dynamic VLAN registration or de-registration is not allowed on the port. Any dynamic VLANs created earlier are de-registered.
- **Applicant Mode -** The Applicant Mode of the port. This configures whether MVRP PDU exchanges are allowed on the port, depending on the port's Spanning Tree state:
  - **Participant -** MVRP PDU exchanges are only allowed when the port is in the STP forwarding state.
  - **Non-Participant -** MVRP PDUs are not sent in this mode, and PDUs received are processed as expected.
  - **Active -** MVRP PDU exchanges are allowed when the port is in the STP forwarding state or STP blocking state. (Default)
- **Periodic Timer -** The MVRP periodic-timer time interval, in seconds, for dynamically registering VLANs on the switch. Use default timer setting unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP. (Default = 1)
- **Periodic Transmission -** Enables/Disables the periodic transmission status on the port. (Default = Disabled)

Devices/Ports

The MVRP Configuration Wizard Devices/Ports Screen is used to apply the MVRP global/port parameters to specific switches/ports). In the Devices area, select an option from the drop-down

menu to select switches, then click on the Add/Remove Devices button. The selected switches will be listed. Select a switch in the list and click on the Add/Remove Ports button to select specific ports on the switch. Repeat the process for additional switches.

When you are finished, click on the **Next** button or select **Review** on the left side of the screen to move to the next screen.

Review

The MVRP Configuration Wizard Review Screen is used to review your MVRP configuration before applying it to the selected switches/ports. If necessary, click on the **Back** button to return to a screen to make any changes to the configuration. When you are finished, click on the **Apply** button to apply the configuration.

The operation will be displayed on the Results Screen. Click **OK** to return to the top of the MVRP Configuration Wizard.

IP Interface

Network device traffic is bridged (switched) at the Layer 2 level between ports that are assigned to the same VLAN. However, if a device needs to communicate with another device that belongs to a different VLAN, you must configure an IP interface on a device in the VLAN to enable Layer 3 routing to transmit traffic between VLANs. A VLAN is available for routing when at least one IP interface is defined for that VLAN and at least one active port is associated with the VLAN. If a VLAN does not have an IP interface, the ports associated with that VLAN are in essence firewalled from other VLANs.

The VLAN Manager IP Interface Screen is used to view configured IP interfaces on a device; and to create, edit, and delete IP interfaces on devices You can configure up to eight (8) IP interfaces per VLAN on OS6800/6850/9000/9000E Switches (Release 6.1.1 and later); and up to sixteen (16) IP interfaces per VLAN on OS6860, OS6900 (Release 7.2.1 and later), OS9900, and OSOS10K Switches (Release 7.1.1 and later).

Creating an IP Interface

To create an IP interface on a device, click on the Add icon, complete the fields as described below, then click on the **Create** button.

- **Name -** The user-configured interface name.
- **IP Address -** The IP address of the IP interface.
- **Subnet Mask -** The IP interface subnet mask value. The default value for this field is based on which network class range the IP address falls within; Class A, B, or C. (255.0.0.0, 255.255.0.0, or 255.255.255.0).
- **MTU -** The Maximum Transmission Unit size set for the interface.
- **Device Type -** The type of device bound to the interface:
  - **Unbound -** No device is bound to the interface.
  - **VLAN -** Associates a VLAN with the interface. You must enter the VLAN ID in the VLAN ID field.
  - **EMP -** The Ethernet Management Port is bound to the interface.
  - **Loopback -** A loopback interface configured for testing.

  - **GRE Tunnel -** A GRE Tunnel is configured for the interface. You must enter the Tunnel Source and Destination.
  - **IPIP Tunnel -** An IPIP Tunnel is configured for the interface. You must enter the Tunnel Source and Destination.
- **VRF -** The VRF ID. If the device supports the Multiple VRF feature, select a VRF from the drop-down menu to assign the interface to a configured VRF instance (by default all interfaces are assigned to the Default VRF). You can assign a new interface to a VRF; however, you cannot edit the VRF ID of an existing interface. If the feature is not available on the device, the column will display "Default", indicating that the switch is operating as a single routing instance. VRF instances are created on the switch through the CLI or WebView application. See the "Configuring Multiple VRF" Chapter in the applicable *OmniSwitch AOS Network Configuration Guide* for detailed instructions on configuring VRF instances.
- **IP Encapsulation -** The IP interface frame encapsulation value (Ethernet 2 or SNAP). The frame encapsulation determines the framing type the interface uses when generating frames that are forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. (Default = Ethernet 2)
- **Admin State -** The administrative state of the interface (Enable/Disabled). (Default = Enabled)
- **IP Forward -** The interface forwarding status (Enabled/Disabled). A forwarding interface sends IP frames to other subnets. A "no forwarding" interface acts as a host only. It receives IP frames from other interfaces. (Default = Enabled).
- **Local Proxy ARP -** Local Proxy ARP status (Enabled/Disabled). The Local Proxy ARP feature is an extension of the Proxy ARP feature, but is enabled on an IP interface and applies to the VLAN bound to that interface. When Local Proxy ARP is enabled, all ARP requests received on VLAN member ports are answered with the MAC address of the IP interface that has Local Proxy ARP enabled. In essence, all VLAN traffic is now routed within the VLAN instead of bridged. (Default = Disabled)
- **Primary Interface -** If set to "True", designates the IP interface as the primary interface for the VLAN. If set to "False", the first interface bound to the VLAN becomes the primary by default. (Default = False)
- **Devices -** Use the Switch Picker or Topology application to select the device on which you want to configure the interface.

Editing an IP Interface

To edit an IP interface, select the interface in the IP Interface List and click on the Edit icon. Edit any fields as described above and click on the **Apply** button. Note that you cannot edit the Interface Name, Device Type, or VRF fields.

Deleting an IP Interface

To delete an IP interface, select the interface in the IP Interface List, click on the Delete icon, then click **OK** at the Confirmation Prompt.

Viewing IP Interfaces

The Interface List displays basic information for all configured IP interfaces for a selected device. To view IP interfaces on a device, select an option from the drop-down menu (Use

Switch Picker/Use Topology) and click on the **Select Device** button. Select a device and click **OK**. Information for all IP interfaces configured on the device is displayed in the IP Interface List as described below. Click on an entry in the list to view detailed information about an interface.

Basic Information

- **Name -** The user-configured interface name.
- **IP Address -** The IP address of the IP interface.
- **Subnet Mask -** The IP interface subnet mask value.
- **Admin State -** The administrative state of the interface (Enable/Disabled).
- **Oper State -** The operational state of the interface.
- **Device Type -** The type of device bound to the interface:
  - **Unbound -** No device is bound to the interface.
  - **VLAN -** Associates a VLAN with the interface. You must enter the VLAN ID in the VLAN ID field.
  - **EMP -** The Ethernet Management Port is bound to the interface.
  - **Loopback -** A loopback interface configured for testing.
  - **GRE Tunnel -** A GRE Tunnel is configured for the interface. You must enter the Tunnel Source and Destination. The GRE Tunnel devices are supported only on OS10K Switches.
- **IP Forward -** The interface forwarding status (Enabled/Disabled). A forwarding interface sends IP frames to other subnets. A "no forwarding" interface acts as a host only. It receives IP frames from other interfaces. (Default = Enabled).
- **MTU -** The Maximum Transmission Unit size set for the interface.

Detailed Information

- **Name -** The user-configured interface name.
- **IP Address -** The IP address of the IP interface.
- **Subnet Mask -** The IP interface subnet mask value. The default value for this field is based on which network class range the IP address falls within; Class A, B, or C. (255.0.0.0, 255.255.0.0, or 255.255.255.0).
- **Admin State -** The administrative state of the interface (Enable/Disabled). (Default = Enabled)
- **Device Type -** The type of device bound to the interface:
  - **Unbound -** No device is bound to the interface.
  - **VLAN -** Interface is associated with a VLAN. (The VLAN ID will be displayed in the next field.)
  - **EMP -** The Ethernet Management Port is bound to the interface.
  - **Loopback -** A loopback interface configured for testing.
  - **GRE Tunnel -** A GRE Tunnel is configured for the interface. (The GRE Tunnel Source and Destination will be displayed in the next field.)
- **IP Forward -** The interface forwarding status (Enabled/Disabled). A forwarding interface sends IP frames to other subnets. A "no forwarding" interface acts as a host only. It receives IP frames from other interfaces. (Default = Enabled).

- **IP Encapsulation -** The IP interface frame encapsulation value (Ethernet 2 or SNAP). The frame encapsulation determines the framing type the interface uses when generating frames that are forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. (Default = Ethernet 2)
- **VRF - VRF ID -** The VRF ID. If multiple VRFs are configured on the device, the VRF ID is displayed. If none are configured, or if the feature is not available on the device, the column will display "Default", indicating that the switch is operating as a single routing instance.
- **MTU -** The Maximum Transmission Unit size set for the interface.
- **Local Proxy ARP -** Local Proxy ARP status (Enabled/Disabled). (Default = Disabled)
- **Primary Interface -** If set to "True", designates the IP interface as the primary interface for the VLAN. If set to "False", the first interface bound to the VLAN becomes the primary by default. (Default = False)
- **Oper State -** The operational status of the router interface; Active or Inactive. An IP router interface is not operationally active until at least one active switch port is assigned to the VLAN. This is not a configurable parameter; switch software automatically determines the operational status of the VLAN and router interface.
- **Oper Reason -** An explanation of the operational state. If the interface is up the field will indicate "Interface Up". If the interface is down, an explanation is displayed:
  - **Unbound -** No device is bound to the interface.
  - **Device Down -** Device bound to the interface is down.
  - **Admin Down -** The admin state of the interface is down.
  - **No Such Device -** Device does not exist.
  - **No Router MAC -** No MAC address available for the interface.
  - **Tunnel Source Invalid -** The source IP address of the tunnel is invalid.
  - **Tunnel Destination Unreachable -** The destination IP address of the tunnel is not reachable.
- **Router MAC -** The switch MAC address assigned to the interface. Each interface assigned to the same VLAN shares the same switch MAC address.
- **Broadcast Address -** The default broadcast address value. The default value for this field is based on the default network class range of the IP address assigned to the router interface. For example, a class A IP address, such as 10.0.0.2, has a default broadcast address of 10.255.255.255. A class C address, such as 198.181.10.2, has a default broadcast address of 198.181.10.255.
- **Actual Primary -** Indicates if the interface is the configured and/or actual primary interface for the device (True/False).

Poll

Network devices are polled every 30 minutes for VLAN information update. The VLAN Manager Poll Screen can be used at any time to manually poll devices VLAN updates. Select an option from the drop-down menu (Use Switch Picker/User Topology), click on the **Select Devices** button, then click on the **Start Polling** button. A Result Screen will appear to indicate if the poll was successful. Click **OK** to return to the Poll Screen. VLAN information displayed in the VLAN Manager application will be updated for the selected devices.

VLAN Template

The VLAN Manager VLAN Template Screen displays all configured VLAN Templates and is used to create, edit, and delete VLAN Templates. A VLAN Templates specifies a range of VLANS that can be used when creating VLANS in the Create VLAN Wizard.

Creating a VLAN Template

Click on the Add icon, complete the fields as described below, then click on the **Create** button.

- **Name -** User-configured VLAN Template Name.
- **Description -** Optional VLAN Template Description.
- **Ranges -** Enter a VLAN range.

Editing a VLAN Template

Select a template in the VLAN Template List and click on the Edit icon. Edit any fields as described above and click on the **Apply** button.

Deleting a VLAN Template

Select a template in interface in the VLAN Template List, click on the Delete icon, then click **OK** at the Confirmation Prompt. Note that you cannot edit the template name.

VLAN Template List

The VLAN Template list displays all configured VLAN Templates.

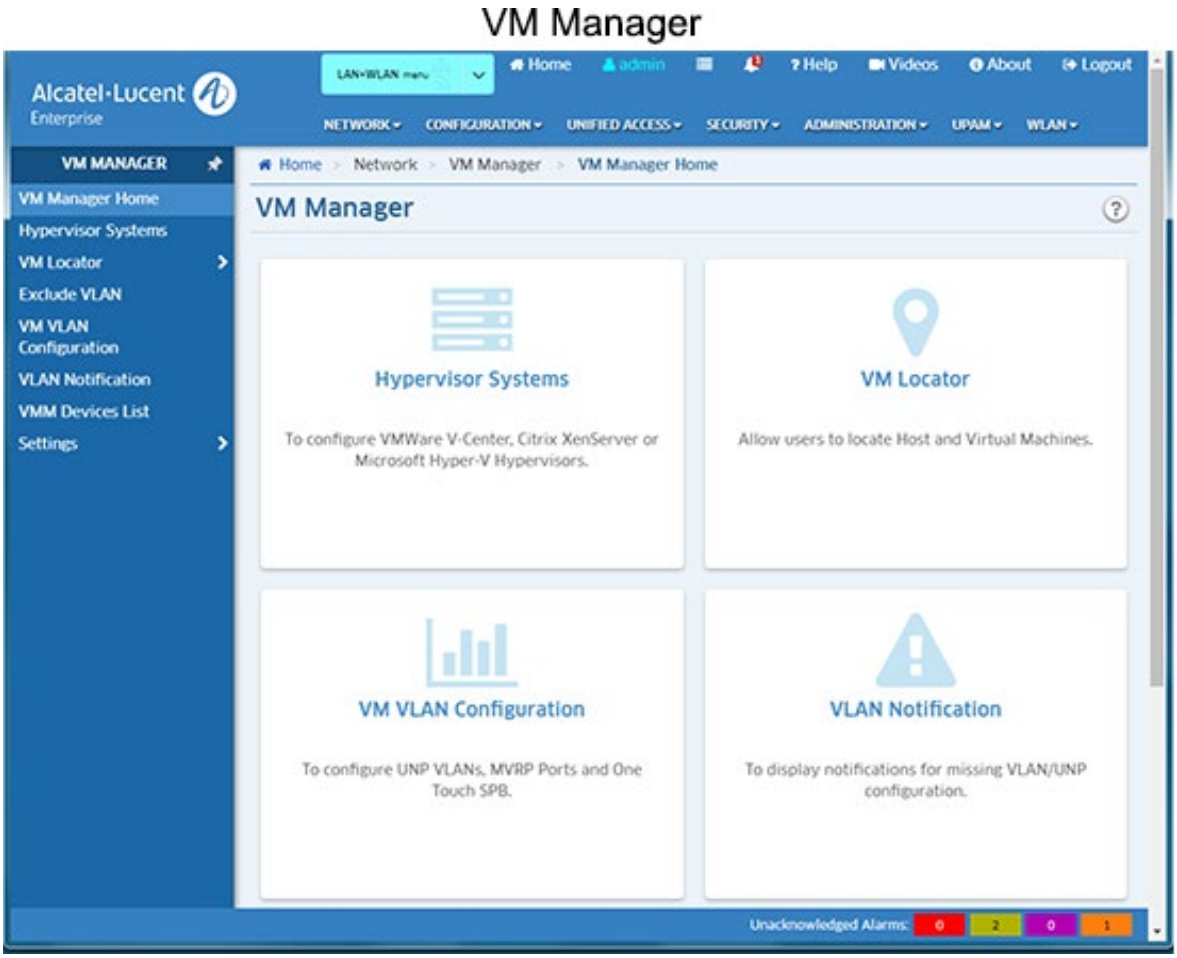
- **Name -** User-configured VLAN Template Name.
- **Description -** Optional VLAN Template Description.
- **Ranges –** The VLAN Template VLAN range.

36.0 VM Manager

Virtualization allows multiple Virtual Machines to run in isolation, side-by-side on the same physical machine (Host Server). Each virtual machine can interact independently with other devices, applications, data and users as though it were a separate physical resource. This enables much more efficient and reliable use of server resources because different Virtual Machines can run different operating systems and multiple applications while sharing the resources of a single physical machine. And because each Virtual Machine is isolated from other Virtual Machines, if one crashes, it does not affect the others. Moreover, Virtual Machines can dynamically migrate between Hosts to better utilize server resources.

Virtual Machines are configured using third-party software (VMware's vSphere or Microsoft Hyper-V). The OmniVista Virtual Machine (VM) Manager application interfaces with vSphere, or Hyper-V to provide a single GUI interface to easily monitor Virtual Machines, including tracking Virtual Machines and their network associations if the machines move to a different Host on the network. Moreover, VM Manager interfaces with the Universal Network Profile (UNP) feature within OmniVista's Access

Guardian application to shape Virtual Machine traffic based on user-configured UNP rules (e.g., VLAN Tag Rules, IP Rules, MAC Range Rules).



Note: VM Manager supports a mixture of vCenters and Hyper-V Servers in the same configuration. You can manage up to a total of 5,000 Virtual Machines (i.e., 5,000 VMs total on all Hypervisors).

Note: The OmniVista Server can run on a Virtual Machine. However, Virtual Machine movement can cause OmniVista to lose UDP traffic (e.g., SNMP Queries or Traps).

The VM Manager application is configured by clicking on one of the following tiles on the Home Page or links on the left side of the screen:

- **Hypervisor Systems -** Used to configure a Hypervisor (vCenter or Hyper-V).
- **VM Locator –** Enables the user to search and browse for VM Host Machines and Virtual Machines, and view Host Machine and Virtual Machine configurations.
- **Exclude VLAN –** Enables the user to configure a list of VM VLANs that VM Manager can ignore when polling Virtual Machine configurations.
- **VM VLAN Configuration –** Enables the user to configure VM VLANs and associate those VLANs with Universal Network Profiles (UNP) to monitor and manage Virtual Machines on the network.
- **VLAN Notification -** This panel displays a list of instances where Virtual Machines are mis-configured.
- **VMM Devices List -** Used to display information for switches connected to a Host Machine. Switches on this list are polled by VM Manager for VM Locator updates. Any switches connected to a Host Machine should be added to the VM Devices List to ensure the latest VM Locator information.
- **Settings -** Used to configure VM Polling and SBP configuration.

Virtualization/VM Manager Overview

The following sections provide an overview of virtualization and VM Manager's role in monitoring and managing Virtual Machines on the network.

Virtualization

Virtualization is a way to use software (e.g., VMware) to create multiple Virtual Machines on a single Host Server to make better use of storage and server resources (CPU power, memory). These Virtual Machines run in isolation, side-by-side on the same physical machine. Each virtual machine can interact independently with other devices, applications, data and users as though it were a separate physical resource. This enables much more efficient and reliable use of server resources because different virtual machines can run different operating systems and multiple applications while sharing the resources of a single physical machine. And because each virtual machine is isolated from other virtualized machines, if one crashes, it does not affect the others. Moreover, Virtual Machines can dynamically migrate between Hosts to better utilize server resources.

Virtualization has a profound impact on the efficiency of the server farm. Without virtualization technology, the average server usage is about 10-20%, with virtualization, the average usage goes up to 40 - 60%. The introduction of virtualization in the data center has had a transforming effect on the way server farms are designed and operated. It also has implications for the network infrastructure.

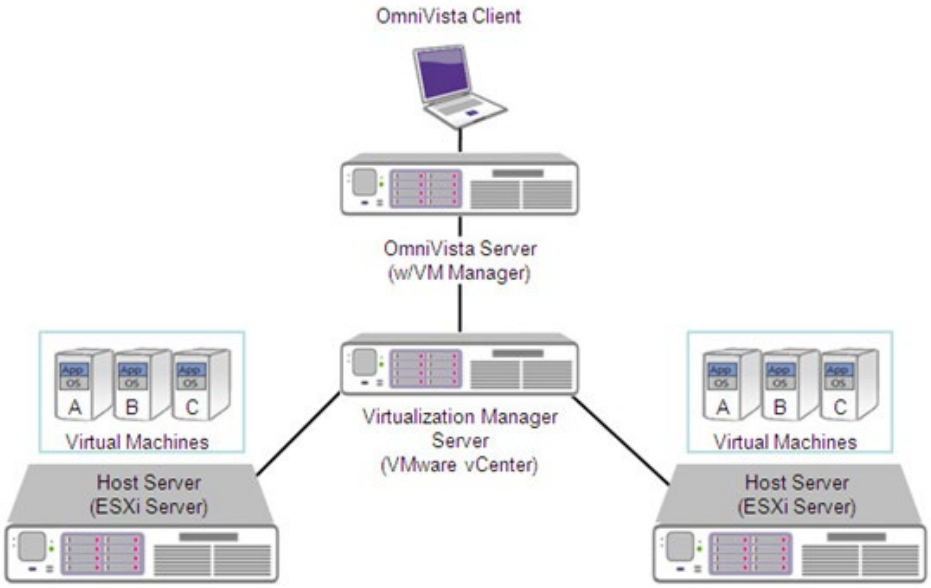
VM Manager and Virtualization

vCenter and Hyper-V provide a central location to monitor and manage Virtual Machines. OmniVista's VM Manager interacts with them to provide a unified view of virtual machines on the network. Although similar in operation, their configurations are slightly different. The sections

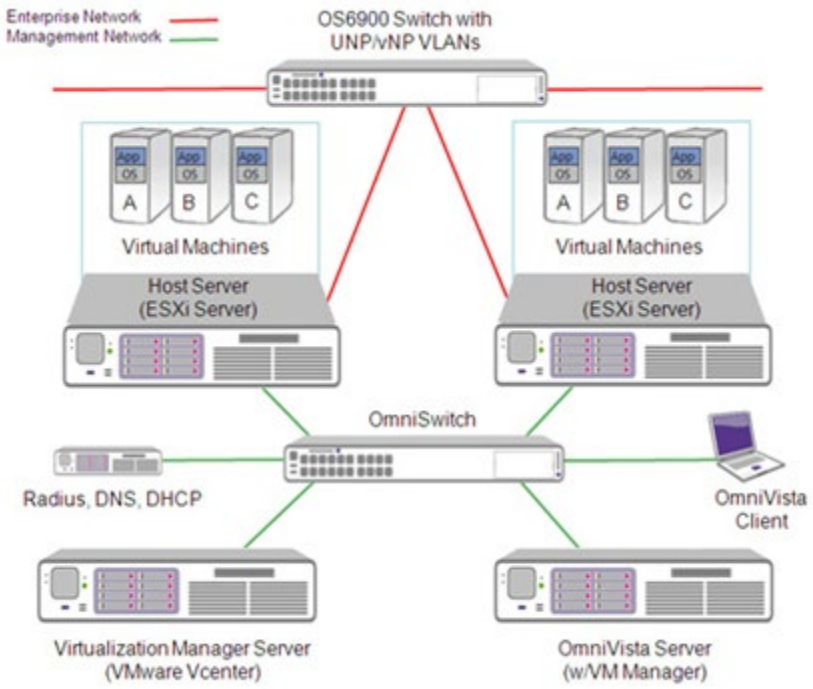
below provide a high-level overview of their configuration and operation within the context of OmniVista's VM Manager. For detailed vCenter configuration instructions, refer to the applicable vendor documentation.

VMware vCenter

As shown below, the VM Manager application interfaces with VMware's vCenter to provide a unified view of Virtual Machines, their configurations, and designated switch configurations that, together enable proper traffic flows. Virtual Machines are configured on physical Host Servers that provide computing resources for the Virtual Machines. VMware's vCenter is a central service configured on its own physical server that interfaces with multiple Host Servers and the OmniVista Server through an OS6900 Switch. The diagram below shows a configuration with a single vCenter. VM Manager will support up to two (2) vCenters.



The diagram below provides a high-level view of an OmniVista/vCenter network configuration.



Microsoft Hyper-V

The VM Manager application interfaces with Hyper-V to provide a unified view of Virtual Machines, their configurations, and designated switch configurations that, together enable proper traffic flows. Virtual Machines are configured on physical Host Servers that provide computing resources for the Virtual Machines.

VM Manager and Traffic Shaping

VM Manager also interfaces with the Universal Network Profile (UNP) feature within OmniVista's Access Guardian application. The UNP Tag Rule feature enables you to assign VM VLANs to traffic shaping profiles based on UNP Classification Rules or Policy Lists. Any traffic matching the UNP Tag rule will have a UNP profile applied and will be forwarded to a VLAN.

To utilize the VM Manager application, you first create Virtual Machine Port Groups inside the Host's networking configuration. The Virtual Machine Port Group is assigned a VLAN (VM VLAN) per your specification. Using UNP Tag rules on the switches, you can then associate VM VLANs with different UNPs (and their VLANs). Once a Virtual Machine is assigned a Virtual Machine Port Group, its network traffic is tagged with a VLAN number and the switch will know how handle the tagged packets based on the UNP Tag rule. This rule translates a VM VLAN to its corresponding UNP profile and VLAN on the switch.

If UNP Tag rules are consistently defined on all of the switches that carry VM network traffic, a Virtual Machine can move between Hosts connected to different switches without changes to its switch VLAN and traffic shaping parameters. The new switch will pick up the VM VLAN tag and know how to properly handle the VM network traffic. To help with consistency, the VM Notifications feature within VM Manager monitors Virtual Machine configurations and sends a notification if a Virtual Machine configuration is missing.

> **Note:** It is recommended that the 'Management Network' that used to handle traffic for Host management, VM movement (vMotion), NFS, etc. be on a separate physical switch

port and a separate UNP Tag rule or that the VLAN is defined differently from those defined for Virtual Machines. This requires a Host server with multiple NIC cards. This way, misconfigurations on a Virtual Machines' switch port will not cause any interruptions VMware's vCenter, Host Server, or OmniVista communications, and you can still use vSphere Client to manage Virtual Machines.

When Virtual Machines are created, you must also create a VLAN Tag for that machine. (Any traffic originating from that Virtual Machine will be tagged with that VLAN tag). To utilize the VM Manager application, you first create a UNP with a VLAN Tag Rule. Any traffic matching that VLAN tag is then routed to the VLAN associated with that UNP. You then create a VM VLAN and associate it with that UNP Profile and VLAN.

Configuring VM Manager

OmniVista's VM Manager application interfaces with a Hypervisor System (vCenter, Hyper-V) to enable you to monitor Virtual Machines on your network. VM Manager also utilizes the Universal Network Profile (UNP) feature within OmniVista's Access Guardian application to apply UNP Rules to VM traffic. These UNP rules, which can be associated with QoS Policy Lists, are applied to UNP VLANs, and the traffic is then assigned to the applicable VLAN.

VM Manager Configuration Quick Steps

Configure Virtual Machines and vCenter as instructed by VMware. When you configure a Virtual Machine you must configure a VLAN Tag for the machine to enable VM Manager to monitor the machine and manage VM traffic. After configuring Virtual Machines and vCenter, follow the Quick Steps below to configure OmniVista's VM Manager. Generally, VM Manager configuration should use the following guidelines:

- Virtual Machines are tagged.
- Configure one UNP per VM VLAN.
- Configure a VLAN Tag Rule for each VM VLAN. (You can configure additional Classification Rules UNP or associate the UNP with Policy List, to further shape traffic.)

Note: VM Manager requires that the link discovery protocol be turned off on the port connecting the Hypervisor (ESXi Server), or on the Hypervisor itself. Some Hypervisors may introduce LLDP packets which make it seem to have another physical bridging device, rather than an end station.

The recommended way to manage Virtual Machines in a data center using VM Manager is to have the Virtual Machines communicate using tagged VLAN packets, and provisioning the network using UNP VLAN Tag Classification rules over UNP Ports. Once all Virtual Machines are associated by VLAN tag with VM VLANs, any Virtual Machine movement will not require further adjustment to the configuration. This also ensures that OmniVista will notify the user through VM VLAN Notifications when a Virtual Machine and its VM VLAN are mis-configured.

1. In the VM Manager application, go to the Hypervisor Systems Screen to configure VM Manager's connection to a Hypervisor (vCenter, Hyper-V).

   Important Note: The system time on all hypervisors must be correctly set and synchronized with the time on the OmniVista Server.

2. Go to the Unified Access application and create a VXLAN Mapping Template (Unified Access - Unified Profile - Template - VXLAN Mapping).
3. In the Unified Access application, create an Access Classification Rule for the VLAN (Unified Access Unified Profile - Template - Access Classification).
4. Assign the UNP Policy to network switches.

Hypervisor Systems

The VM Manager Hypervisor Systems Screen displays a list of all VM Servers connected to OmniVista; and is used to configure the connection from OmniVista to a VM Server. You can also edit and delete VM Servers. OmniVista supports VMware's vCenter and Microsoft Hyper-V.

If no VM Servers have been configured, the Hypervisor Systems Table is not displayed. Click on a link (VMware's vCenter, Microsoft Hyper-V) at the top of the screen to bring up the Create Hypervisor Systems Screen to create a VM Server.

> **Important Note:** The system time on all hypervisors must be correctly set and synchronized with the time on the OmniVista Server.

Creating a VM Server

To configure the connection from OmniVista to a VM Server, click on the Create icon **+** and complete the fields as described below. The fields differ slightly depending on the server type selected (VMware's vCenter, Microsoft Hyper-V). When you have finished completing the fields, click on the **Create** button.

> **Note:** You can test the connection to the VM Server before creating it by clicking on the **Test Connection** button after completing the fields.

VMware vCenter

- **VM Server Type -** Select **VMware vCenter** from the drop-down menu).
- **URL -** The IP address of the VM Server. For a vCenter Server, enter the IP address, followed by "/sdk" (e.g., https://10.255.11.1/sdk).
- **Name -** User-configured name for the VM Server.
- **User -** Administrator's User Name.
- **Password -** The password needed to access the VM Server.
- **Re-Type Password -** Re-Type password needed to access the VM Server.

Microsoft Hyper-V

- **VM Server Type -** Select **Microsoft Hyper-V** from the drop-down menu). The server type you selected on the previous screen will automatically be selected. However, you can also select a different server type from this drop-down menu.
- **IP Address -** The IP address of the VM Server (e.g., https://10.255.11.1).
- **Name -** User-configured name for the VM Server.
- **Domain -** The Hyper-V Domain.
- **User -** Administrator's User Name.
- **Password -** The password needed to access the VM Server.

- **Re-Type Password -** Re-Type password needed to access the VM Server.

Editing a VM Server

Select a VM Server in the table and click on the Edit icon . Edit the field(s) as described above and click on the **Apply** button. You can only edit the server password.

Deleting a VM Server

Select a VM Server(s) in the table, click on the Delete icon then click **OK** at the Confirmation Prompt.

Hypervisor Systems Table

The Hypervisor Systems Table displays a list of all VM Servers connected to OmniVista.

- **Name -** User-configured name for the VM Server.
- **URL -** The IP address of the VM Server.
- **VM Server Type -** The VM Server type (VMware's vCenter, and Microsoft Hyper-V).
- **User -** Administrator's User Name.
- **Status -** The administrative status of the Server (Up, Down, Unknown).

VM Locator - Host Networks

The VM Manager Host Networks Screen is used to search for and display information on the Host Machines on which the Virtual Machines reside. You can view information for all Host Machines or enter search criteria to view specific Host Machines. The information displayed is based on the most recent search. To refresh the information with the most recent data, repeat the search.

Searching for Host Machines

Select an option from the **Search By** drop-down menu (e.g., Host MAC Address, Host IP Address) and enter the search criteria. (You can also just select "All Hosts" to search for all Host Machines.) By default, OmniVista will conduct an historical search. If you want to do a live search, set the **Live Search** slider to **Enabled**. You can also enable "Stop after 1st Match" to stop the search after finding the first match. When you are done, click on the **Apply** button. The results are displayed in the Host Networks Table.

> **Note:** If you enable the "Stop after 1st Match" option, OmniVista will stop searching after at least one match is found; however more than one match may be displayed.

Host Network Table

The Host Networks Table displays basic information about all configured VM Server networks. To view detailed information, click on an entry in the table.

Basic Information

- **Hypervisor Host -** The user-configured name for the Host Machine. If none is configured, the IP address of the Host is displayed.
- **VM Server -** The user-configured name of the VM Server (vCenter, Hyper-V).

- **IP Address -** The Host Machine IP address.
- **Network Mask -** The corresponding network mask of the Host Machine.
- **Network Name -** The VM VLAN that the Virtual Machine's network interface is associated with. The network traffic for a Port Group may be tagged or untagged.
- **Number of Networks -** The number of networks (also known as Physical Interfaces (PIFs) on the Host Machine.
- **Switch IP Address -** The IP address of the switch to which the Host Machine is connected.
- **Slot/Port -** The slot/port of the switch to which the Host Machine is connected.
- **Port VLAN -** The VLAN or SPB Service ID that the switch uses to classify Virtual Machine network traffic.
- **UNP -** The UNP associated with the Host Machine's interface.
- **Locator Time -** The time the Virtual Machine's network traffic was detected on the switch port.
- **Last Update -** The date and time the Host Machine configuration was last updated.

Detailed Information

- **Hypervisor Host -** The user-configured name for the Host Machine. If none is configured, the IP address of the Host is displayed.
- **VM Server -** The user-configured name of the VM Server (vCenter, Hyper-V).
- **IP Address -** The Host Machine IP address.
- **Network Mask -** The corresponding network mask of the Host Machine.
- **Network Name -** The VM VLAN that the Virtual Machine's network interface is associated with. The network traffic for a Port Group may be tagged or untagged.
- **Number of Networks -** The number of networks (also known as Physical Interfaces (PIFs) on the Host Machine.
- **Switch IP Address -** The IP address of the switch to which the Host Machine is connected.
- **Slot/Port -** The slot/port of the switch to which the Host Machine is connected.
- **Port VLAN -** The VLAN or SPB Service ID that the switch uses to classify Virtual Machine network traffic.
- **UNP -** The UNP associated with the Host Machine 's interface.
- **Locator Time -** The time the Virtual Machine's network traffic was detected on the switch port.
- **Last Update -** The date and time the Host Machine configuration was last updated.
- **Uptime -** The amount of time the Host Machine has been up (time since last reboot).
- **CPU Count -** The number of processors on the Host Machine.
- **CPU Model -** The model name of the Host Machine CPU.
- **Service ID -** The Service ID that the switch uses to classify Virtual Machine network traffic.
- **ISID -** The ISID that the switch uses to classify Virtual Machine network traffic.
- **Port Status -** The operational status of the Host port connected to the switch.

- **Port Speed -** The speed of the Host port connected to the switch.
- **Duplex -** The duplex mode (half duplex, full duplex, or auto duplex) of the Host port connected to the switch.
- **Disposition -** The switch port's disposition (Bridging/Filtering).
- **Classification Source -** The Classification Policy under which the device was learned.
- **Data Center -** The name of the Data Center to which the Virtual Machine is assigned.
- **Cluster -** The Cluster in which the Virtual Machine resides.
- **Memory Usage -** The amount of RAM currently being used by the Host Machine, in MB.
- **Vendor -** The Manufacturer of the Host Machine (e.g., HP).
- **Status -** The administrative status of the Host Machine.
- **VM Motion Enabled -** Whether or not VM Motion is enabled. If enabled, Virtual Machines can be moved from one Host to another and the VM configuration will be dynamically updated.
- **CPU -** The speed of the Host Machine CPU, in MHz.
- **Memory Size -** The amount of RAM on the Host Machine, in MB.
- **Num of CPU Pkgs -** Number of physical CPU packages on the Host Machine.
- **Num of Threads -** The number of threads.
- **Num of HBAs -** The number of Host Bus Adapters (HBA).
- **CPU Usage -** The amount of CPU currently being used by the Host Machine, in MHz.
- **Power -** The Power status of the Host Machine (Powered On, Powered Off, Suspended).
- **DNS Name -** The name of the DNS associated with the Host Machine (if applicable).

VM Locator - VM Networks

The VM Manager VM Networks Screen is used to search for and display information on the Virtual Machines residing on the Host Machine. You can view information for all Virtual Machines or enter search criteria to view specific Virtual Machines. The information displayed is based on the most recent search. To refresh the information with the most recent data, repeat the search.

Searching for Virtual Machines

Select an option from the **Search By** drop-down menu (e.g., VM MAC Address, VM IP Address) and enter the search criteria. (You can also just select "All VMs" to search for all Virtual Machines.) By default, OmniVista will conduct an historical search. If you want to do a live search, set the **Live Search** slider to **Enabled**. You can also enable Stop after 1st Match to stop the search after finding the first match. When you are done, click on the **Apply** button. The results are displayed in the VM Networks Table.

> **Note:** "Live Search" locates the most recent location of VMs by doing live query against known switches. If a location is found for a VM's MAC address, information is displayed with the latest timestamp. If a live search does not result in a match, the last historical location and past timestamp is displayed. Historical location will produce multiple results from the past for tracing purposes. Historical search results can also display "false positive" information. For example, a non-uplink port used to connect an end station that has become an uplink port can still be displayed. Furthermore, uplink status that may be

learned later will not be used to determine location. This condition will correct itself but historical data will be persistent regardless. Use the Locator timestamp to determine if the information is noteworthy.

Note: If you enable the "Stop after 1st Match" option, OmniVista will stop searching after at least one match is found; however more than one match may be displayed.

VM Networks Table

The VM Networks Table displays basic information about all configured Virtual Machines. To view detailed information, click on an entry in the table. As indicated below, the information varies slightly depending on server type (vCenter, Hyper-V).

Basic Information

- **VM Name -** The user-configure Virtual Machine name.
- **DNS Name -** The name of the DNS associated with the Virtual Machine (if applicable).
- **MAC Address -** The MAC address of the Virtual Machine.
- **IP Address -** The IP address of the Virtual Machine.
- **Network Name -** The VM VLAN that the Virtual Machine's network interface is associated with. The network traffic for a Port Group may be tagged or untagged.
- **VM Server -** The user-configure name for the VM Server.
- **Hypervisor Host -** The IP address of the Host Machine on which the Virtual Machine resides.
- **Switch IP Address -** The IP address of the switch to which the Host Machine is connected.
- **Slot/Port -** The slot/port of the switch to which the Host Machine is connected.
- **VM VLAN -** The Tag Value for the VM VLAN in the Host System.
- **UNP -** The UNP associated with the Virtual Machine.
- **Locator Time -** The time the Virtual Machine's network traffic was detected on the switch port.
- **Last Update -** The date and time the Host Machine configuration was last updated.

Detailed Information

- **VM Name -** The user-configure Virtual Machine name.
- **DNS Name -** The name of the DNS associated with the Virtual Machine (if applicable).
- **MAC Address -** The MAC address of the Virtual Machine.
- **IP Address -** The IP address of the Virtual Machine.
- **Network Name -** The VM VLAN that the Virtual Machine's network interface is associated with. The network traffic for a Port Group may be tagged or untagged.
- **VM Server -** The user-configure name for the VM Server.
- **Hypervisor Host -** The IP address of the Host Machine on which the Virtual Machine resides.
- **Switch IP Address -** The IP address of the switch to which the Host Machine is connected.

- **Slot/Port -** The slot/port of the switch to which the Host Machine is connected.
- **VM VLAN -** The Tag Value for the VM VLAN in the Host System.
- **UNP -** The UNP associated with the Virtual Machine.
- **Locator Time -** The time the Virtual Machine's network traffic was detected on the switch port.
- **Last Update -** The date and time the Host Machine configuration was last updated.
- **Address Type -** The Virtual Machine address type (Assigned/Unassigned).
- **Guest OS -** The operating system of the Virtual Machine.
- **Power -** The Power status of the Virtual Machine (Powered On, Powered Off, Suspended).
- **Up Time -** The amount of time the Virtual Machine has been up (time since last reboot).
- **Port VLAN -** The VLAN that the switch uses to classify Virtual Machine network traffic.
- **Service ID -** The SPB Service ID that the switch uses to classify Virtual Machine network traffic.
- **ISID -** The ISID that the switch uses to classify Virtual Machine network traffic.
- **Port Status -** The operational status of the Virtual Machine port connected to the Host Machine.
- **Port Speed -** The speed of the Virtual Machine port connected to the Host Machine.
- **Duplex -** The duplex mode (half duplex, full duplex, or auto duplex) of the Virtual Machine port connected to the Host Machine.
- **Disposition -** The switch port's disposition (Bridging/Filtering).
- **Classification Source -** The Classification Policy under which the device was learned.
- **Status -** The operating status of the Virtual Machine.
- **Network Usage -** The percentage of network resource being used by the Virtual Machine.

Exclude VLAN

The VM Manager Exclude VLAN Screen displays a list of all Exclude VM VLANs. It is also used to create, edit and delete Exclude VLANs. When OmniVista polls a VM Server, it checks the Virtual Machine configuration and sends a notification to VM Manger if there is a problem with the configuration (displayed on the VLAN Notifications Screen). The Exclude VLAN Screen is used to define VM VLANs that should be ignored by OmniVista when conducting VM polling (e.g., the VM Network Management VLAN). VLANs listed here will be ignored during support checks.

Creating an Exclude VLAN

Create icon **+** and complete the fields as described below.

- **VLAN ID -** Enter a VLAN ID, multiple VLAN IDs or a range of VLANs.
- **Description -** Enter a description for the Exclude VLAN(s).

Editing and Exclude VLAN

Select a VLAN in the Exclude VLAN List and click on the Edit icon . You can only edit the "Description" field. Edit the field and click on the **Apply** button.

Deleting an Exclude VLAN

Select a VLAN(s) in the Exclude VLAN List, click on the Delete icon , the click on **OK** at the Confirmation prompt.

Exclude VLAN List

The Exclude VLAN List displays all configured Exclude VLANs.

- **VLAN ID -** The VLAN ID.
- **Description -** User configured description for the VLAN.

VM VLAN Configuration

The VM Manager VM VLAN Configuration Screens are used to associate VM VLANs with Universal Network Profiles (UNP), and enable MVRP Ports and One-Touch SPB on network switches/ports.

The recommended way to manage Virtual Machines in a data center using VM Manager is to have the Virtual Machines communicate using tagged VLAN packets, and provisioning the network using UNP VLAN Tag Classification rules over UNP Ports. Once all Virtual Machines are associated by VLAN tag with VM VLANs, any Virtual Machine movement will not require further adjustment to the configuration. This also ensures that OmniVista will notify the user through VM VLAN Notifications when a Virtual Machine and its VM VLAN are mis-configured.

> **Note:** SPB is supported on OS10K and OS6900 Switches running AOS 7.3.1.R01 and later, with an *Advanced* License. To support a mixture of devices using the same screen, OmniVista only pushes configurations which are applicable for specific device types, skipping the rest. For SPB-capable devices, all attributes are applicable. For non-SPB devices, SPB-specific attributes will be skipped and only regular bridging UNP changes will be updated.

VM VLAN Configuration - Apply UNP VLAN

The VM Manager Apply UNP VLAN Screen is used to apply VLAN Tag Rules to network switches/ports. The recommended way to manage Virtual Machines in a data center using VM Manager is to have the Virtual Machines communicate using tagged VLAN packets, and provisioning the network using UNP VLAN Tag Classification rules over UNP Ports. Once all Virtual Machines are associated by VLAN tag with VM VLANs, any Virtual Machine movement will not require further adjustment to the configuration. This also ensures that OmniVista will notify the user through VM VLAN Notifications when a Virtual Machine and its VM VLAN are mis-configured.

Complete the fields as described below and click on the **Apply** button to apply VLAN Tag Rules to network switches/ports.

- **Select VLAN Tag Rules -** Select an existing VLAN Tag Rule(s) from the drop-down list. You can also click on the Add icon to go to the Access Guardian application and create a new rule(s).

- **Enable UNP Ports -** Enables/Disables UNP on the selected ports. By default, UNP Ports are enabled when you create UNP Port Policies.
- **Select UNP Port Policy -** Select as UNP Port Policy from the drop-down menu. You can also click on the Add icon to go to the Access Guardian application and create a new policy. You can only select one policy.
- **Select Devices -** Select an option from the drop-down menu "Use Switch Picker" or "Use Topology" and click on the **Add/Remove Devices** button to select the device(s) on which you want to apply the VLAN Tag Rule(s).
- **Select Ports -** Click on a device and click on the **Add/Remove Ports** button to select the port(s) on which you want to apply the VLAN Tag Rule(s).

VM VLAN Configuration - Enable MVRP Ports

The VM Manager Enable MVRP Ports Screen is used to enable MVRP Ports on network switches. Select an option from the drop-down menu "Use Switch Picker" or "Use Topology" and click on the **Add/Remove Devices** button to select the device(s) on which you want to enable MVRP Ports. Then select a device and click on the **Add/Remove Ports** button to enable MVRP on those ports.

VM VLAN Configuration - Enable One-Touch SPB

The VM Manager Enable One-Touch SPB Screen is used to enable SPB Interfaces on network switches. One-Touch SPB configures switches for backbone communication to transport VM traffic that is classified to service domain using UNP for SPB. UNP for SPB specifies which Service Access Port and which Policy List will be used. Subsequently, it will determine the correct layer 2 domain for VM data.

Select an option from the drop-down menu "Use Switch Picker" or "Use Topology" and click on the **Add/Remove Devices** button to select the device(s) on which you want to enable MVRP Ports. Then select a device and click on the **Add/Remove Interfaces** button to enable SPB on those interfaces.

VLAN Notification

The VM Manager VLAN Notification Screen displays VM VLAN Notifications generated by the VMM Service for missing VLAN/UNP configuration on a switch slot/port where VMs are connected. The notifications briefly describe the problem and enable you to resolve it. Ideally, you want to have no notifications in this panel. You can also resolve configuration problems using the Resolve Feature. There are two links on the screen:

- **Active Notifications -** Displays all active notifications. Note that a user can move a notification to the Ignored Notifications List selecting the notification(s) in the Active Notifications List and clicking on the **Ignore** Button.
- **Ignored Notifications -** Displays any notifications that the user has moved to the tab because they may describe alternate configurations that are known by the user to work. Generally, a user will move notifications to the Ignored List because they have alternate configurations (e.g., MAC, MAC Range, IP) which are known to work, in addition to the supported UNP VLAN Tag configurations. Note that a user can also move the Ignored notifications back to the Active list by highlighting the notification(s) on the Ignored Tab and clicking on the **Activate** Button.

You can also select the notification and click on the **Resolve** button to open the UNP VLAN Wizard and resolve the problem.

Resolving a VM Configuration Problem

When a mis-configuration notification appears in the VLAN Notification window, select the notification and click the **Resolve** button to bring up the UNP VLAN Configuration Wizard. Use the Wizard to correct the configuration problem described in the notification (e.g., missing tag rule, slot/port).

If a VM discovered on a UNP or SPB access port and OmniVista's VLAN tag rule has not been created on the switch(es), OmniVista create an entry in the Active Notifications List. The "Resolve" button will guide you through the necessary configuration steps to resolve the problem and clear the Notification.

For SPB configurations, OmniVista may generate a new profile with an ISID derived from the VM VLAN and associate this value into one of the 4 pre-configured SBP BVLANs, if it has not been created. This profile is used to classify the VLAN's traffic into the provider backbone's BVLAN. OmniVista uses a round-robin mechanism to associate BVLAN to a VM VLAN and pushes these parameters into an SPB profile. A VM VLAN will have a uniquely associated ISID created by adding the VM VLAN ID to the starting ISID number defined in SPB Settings Screen.

If a VLAN Tag rule already exists as it may pertain to regular bridging UNP, OmniVista will append an additional SPB Profile name using the corresponding SPB Profile, which was auto-generated for the VLAN. With that in mind, "ag Position' will be specified as "Outer" and the SPB Profile will be the one generated based on the VM VLAN. The Customer Domain ID will be based on the ports' Customer Domain ID. For example, If VLAN 31 is detected on SPB ports with Customer Domains of 1 and 2, 2 entries of UNP VLAN will be created - VLAN 31, Customer Domain 1> and VLAN 31, Customer Domain 2 - and corresponding SPB Profiles will be created in Access Guardian.

UNP Profiles with blank policy lists will be created if necessary to resolve a UNP VLAN tag rule and the rule will be specified in the UNP VLAN List. If the UNP Profile already exists, it will be automatically picked up in creating UNP VLAN List entry. Auto-generated UNP Profiles have the name UNP XX where XX is the VLAN ID. The Default UNP Profile is named UNP1 and its VLAN ID is 1. This UNP will be used to resolve "Default UNP" notifications for regular UNP ports.

> **Note:** In both cases where bridging-domain UNP Profiles or SPB Profiles are generated, the Policy List is left blank. Having these profiles will only facilitate connectivity. You can later decide to modify the UNP Profile to that rule by clicking on Edit button and reassigning the policy list.
>
> **Note:** SPB Profiles that are auto-generated using the Resolve function require that "One Touch SPB" is configured successfully on the switch(es) and the same default configuration parameters exist that existed when "One Touch SPB" was first configured. If this configuration has changed, "One Touch SPB" needs to be re-invoked.

Notification List

The following fields are displayed on both the Active and Ignored Notifications Lists.

- **VLAN -** The VM VLAN ID.
- **Host Name -** The name of the Host Machine hosting the Virtual Machine.
- **Switch -** The switch connected to the Host Machine.
- **Slot/Port -** The slot/port number of the port connecting the Host Machine to the switch.
- **Missing Configuration -** A brief description of the configuration problem.
- **Missing Configuration Slot/Port -** The port(s) missing from the configuration.
- **Port Groups -** The port groups missing from the configuration.
- **Last Update -** The time the notification was last updated.
- **Create Time -** The time the notification was created.

VMM Devices List

The VM Manager VMM Devices List Screen displays information for switches connected to a Host Machine. Switches on this list are polled by VM Manager for VM Locator updates. Any switches connected to a Host Machine should be added to the VM Devices List to ensure the latest VM Locator information. You can add/remove switches from the list by clicking on the **Select Devices** button at the top of the screen and selecting devices for the list.

VMM Devices List

- **Friendly Name -** User-configured name for the device.
- **Name -** The name of the device.
- **Address -** The address of the device.
- **Status-** The operational status of the device. It displays "Up" if the device is up and responding to polls. It displays "Down" if the device is down and not responding to polls. It displays "Warning" if the switch has sent at least one warning or critical trap and is thus in the warning state.
- **DNS Name -** The DNS name of the device.
- **Type -** The type of device chassis (e.g., OS6850-24).
- **Version -** The version number of the device software (e.g., 6.6.5.96.R02). OmniVista may not be able to determine the software version on some third-party devices. In these cases, the field will be blank.
- **Location -** The physical location of the device (e.g., Test Lab).
- **NOD -** Whether or not the device is an NOD device (Yes/No).
- **Activated Licenses -** Activated optional licenses on the device.
- **FTP User Name -** The CLI/FTP user name for the device.
- **SNMP Version -**The SNMP version that OmniVista uses to communicate with the device.
- **v1/2 Read Community -** The device's SNMP v1/2 "get" community name, if applicable.
- **v1/2 Write Community -** The device's SNMP v1/2 "set" community name, if applicable.
- **v3 User Name -** The device's SNMP v3 user name, if applicable.

- **Last Upgrade Status -** The status of the last firmware upgrade on the device.
  - "Successful" - Successful BMF and Image upgrade performed.
  - "Successful (BMF)" - Successful BMF upgrade performed.
  - "Successful (Image)" - Successful Image upgrade is performed.
  - "Failed (BMF, Image)" - BMF and Image upgrade failed.
  - "Failed (BMF)" - BMF upgrade failed.
  - "Failed (Image)" - Image upgrade failed.
- **Backup Date -** The date that the device's configuration and/or image files were last backed-up to the OmniVista Server.
- **Backup Version -** The firmware version of the configuration and/or image files that were last backed-up to the OmniVista Server.
- **Last Known Up At -** The date and time when the last poll was initiated on the device.
- **Description** - A description of the device, usually the vendor name and model.
- **Traps -** The status of trap configuration for the device. "On" means that traps are enabled. "Off" means that traps are disabled. "Not Configurable" means that traps for this device are not configurable from OmniVista. (Note that traps may have been configured for such devices outside of OmniVista.) "Unknown" means that OmniVista does not know the status of trap configuration on this device.
- **Seen By -** The User Groups that are able to view the device. OmniVista is shipped with the following pre-defined user groups Default, Writers, Network Administrators, Administrators) that have different security permissions.
- **Running From -** For AOS devices, this field indicates whether the switch is running from the Certified directory or from the Working directory. This field is blank for all other devices. For AOS devices, the directory structure that stores the switch's image and configuration files in flash memory is divided into two parts:
  - The Certified directory contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory.
  - The Working directory contains files that may or may not have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes to the working directory. You cannot save configuration changes directly to the certified directory.

  Note that the files in the certified directory and in the working directory may be different from the running configuration of the switch, which is contained in RAM. The running configuration is the current operating parameters of the switch, which are originally loaded from the certified or working directory but may have been modified through CLI commands, WebView commands, or OmniVista. Modifications made to the running configuration must be saved to the working directory (or lost). The working directory can then be copied to the certified directory if and when desired.

  > **Note:** OmniVista supports the Multiple Working Directories Feature available on OS10K and OS6900 Switches (AOS Release 7.2.1.R01 and later). This feature allows the user to create multiple Working Directories on the switch that can be used to save specific switch configurations. The user can create any name for these "Working" Directories (e.g., "Marketing Switch 05-23-15"). If the switch is

running from one of these user-created directories, the directory name is displayed in this field.

- **Changes -** For AOS devices, this field indicates the state of changes made to the switch's configuration. This field is blank for all other devices. This field can display the following values:
  - **Certified -** Changes have been saved to the working directory, and but the working directory has been copied to the certified directory. The working directory and the certified directory are thus identical.
  - **Uncertified -** Changes have been saved to the working directory, but the working directory has not been copied to the certified directory. The working directory and the certified directory are thus different.
  - **Unsaved -** Changes have been made to the running configuration of the switch that have not been saved to the working directory.
  - **Blank -** When this field is blank for an AOS device, the implication is that OmniVista knows of no unsaved configuration changes and assumes that the working and certified directories in flash memory are identical.
- **Discovered -** The date and time when OmniVista successfully pings or polls the switch for the first time. This value remains unchanged until the switch entry is deleted. This field will remain blank if OmniVista does not ping or poll the switch at all.
- **No. of Licenses Used -** The total number of Core (AOS) or Third-Party licenses being used. For example, a stack of 4 switches would require 4 licenses, a VC of 6 would require 6 licenses. If a stack splits, the number of licenses reserved for the device before the split is maintained even though modules have been reduced to less than 5. This way, the license counts are reserved for the stack to recover.
- **License Type -** The type of license used by the device (e.g., AOS, Third Party).

Settings - VM Polling

The VM Manager VM Polling Screen is used to set the interval at which OmniVista will poll VM Servers. The interval you set should be determined based on the number of Virtual Machines you are managing. The more machines you are managing, the more resource-intensive the operation will be. The Polling Interval should generally be the same as the interval set for "Regular Updates" in the Setting Frequencies Screen in the Discovery Application.

Select an option from the drop-down menu (Minutes, Hours, Days), enter a Polling Interval and click on the **Apply** button. You can also click on the **Poll Now** button to perform an immediate poll of all connected VM Servers.

Settings - SBP

The VM Manager Settings Screen enables you to modify the default "One Touch SPB" configuration. You can overwrite the system-chosen starting ISID and create a value unique to an OmniVista Server. This enables you to create different L2 tunneling domains for Virtual Machines (VMs). VMs associated with the same VLAN/Network in the Hypervisor’s environment but placed on different ISIDs will not communicate with each other. Other attributes can also be customized, including Control BVLAN, BVLANs 2 - 4, and ECT ID 1 - 4, which are tie-breaking algorithms. Update any fields as described below and click on the **Apply** button.

- **Starting ISID -** Used in the auto-generation of SPB Profiles to resolve any notification that is raised when the user clicks on the "Resolve" button in the VM Manager VLAN Notification node. To keep consistent mappings of VLAN-to-ISID, the VM VLAN number is added to the starting ISID number to determine the ISID for each VLAN.
- **Control BVLAN -** One of the four (4) BVLANs created in "One-Touch SPB" to take advantage of shortest path bridging topology from the source. Used for traffic as well as control information.
- **ECT ID 1 -** Cost Tree Identifier (ECT ID) assigned to Control BVLAN. The ECT ID assigns a tie-breaking algorithm to the BVLAN that is used for Shortest Path Tree (SPT) calculations
- **Additional BVLAN 2 -** One of the four (4) BVLANs created in "One-Touch SPB" to take advantage of shortest path bridging topology from the source. Used only for traffic.
- **ECT ID 2 -** Cost Tree Identifier (ECT ID) assigned to BVLAN 2. The ECT ID assigns a tie-breaking algorithm to the BVLAN that is used for Shortest Path Tree (SPT) calculations
- **Additional BVLAN 3 -** One of the four (4) BVLANs created in "One-Touch SPB" to take advantage of shortest path bridging topology from the source.
- **ECT ID 3 -** Cost Tree Identifier (ECT ID) assigned to BVLAN 3. The ECT ID assigns a tie-breaking algorithm to the BVLAN that is used for Shortest Path Tree (SPT) calculations
- **Additional BVLAN 4 -** One of the four (4) BVLANs created in "One-Touch SPB" to take advantage of shortest path bridging topology from the source.
- **ECT ID 4 -** Cost Tree Identifier (ECT ID) assigned to BVLAN 4. The ECT ID assigns a tie-breaking algorithm to the BVLAN that is used for Shortest Path Tree (SPT) calculations.

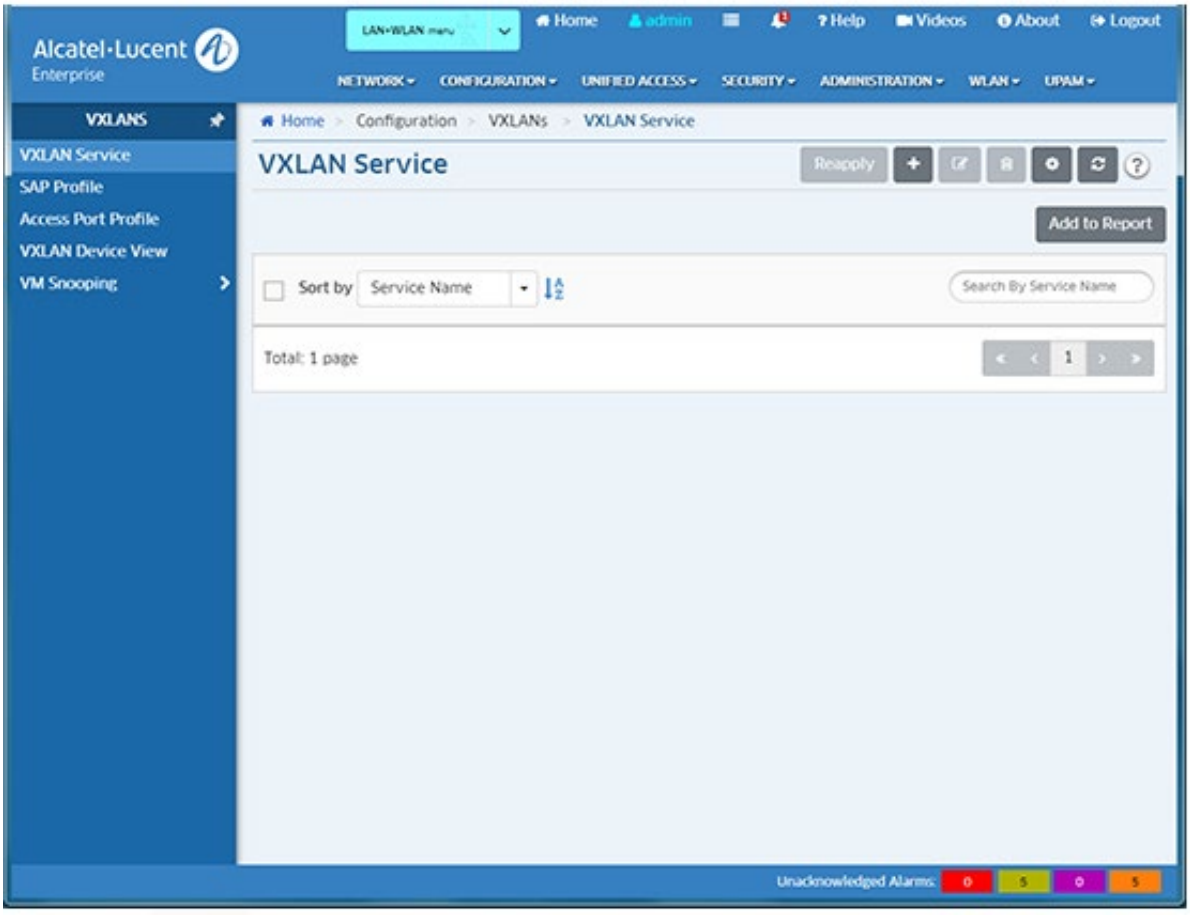
37.0 VXLANs

Virtual Extensible LAN (VXLAN) is a network virtualization scheme tailored to address the evolving trends such as server virtualization and cloud computing in the current data center deployments. Legacy Layer 2 (L2) bridging using VLANs to segregate user traffic is no longer sufficient to meet the scale of current and future requirements. VXLAN uses a L2 over L3 encapsulation technique to overlay L2 network segments on L3 network infrastructure. Basically, a MAC frame received is encapsulated in an IP packet with a UDP header and sent out over the L3 network. Use of L3 as the transport network automatically allows use of ECMP routes, thus increasing utilization of the network infrastructure that cannot be matched by bridged networks using STP.

VXLAN supports up to 16 million virtualized L2 segments called VXLAN segments. Only servers, or more precisely VMs residing in the servers, that are attached to the same VXLAN segment can communicate with each other. Each VXLAN segment is identified by a 24 bit segment ID called VXLAN Network Identifier (VNI). The VNI identifies the scope of the inner MAC frame originated by the individual VM. Thus, we can have overlapping MAC addresses across segments but never have traffic "crossover" since the traffic is isolated using the VNI. The VNI is in an outer header which encapsulates the inner MAC frame originated by the VM. The VMs themselves are completely unaware of the VXLAN and VNI and communicate with each other as if connected directly over a VLAN-based L2 network.

Note: VXLANs are only supported on OS6900-Q32 and OS6900-X72 Switches.

VXLANs



VXLAN Service

The VXLAN Service Screen displays all configured VXLAN Services, and is used to create, edit, and delete VXLAN Services. A VXLAN Service defines a Virtual Forwarding Instance (VFI) that is capable of learning device MAC addresses from the access side and from the network side and then switching the traffic based on this information. Each VXLAN Service is basically an VFI that is capable of learning customer MAC addresses from the access side (Service Access Points - SAP) and from the network side (mesh Service Distribution Point - SDP) and then switching traffic based on this information.

Creating a VXLAN Service

Click on the Create icon **+** and complete the fields as described below to create the VXLAN Service.

- **Service Name -** The name of the VXLAN Service (up to 32 characters).
- **VNID -** The Virtual Network Identifier (VNID) is a 24-bit segment ID (also referred to as a VXLAN Segment ID) that is used to identify encapsulated frames. A VNID is bound to a VXLAN Service when the service is created. OmniVista will auto-generate a unique VNID for VXLAN Service if VNID is set to zero (0).
- **VXLAN Network Profile -** The VXLAN Network Profile associated with the VXLAN Service. The profile specifies the UDP Port and VRF Name. If necessary, create a VXLAN Network Profile.
- **VLAN Translation -** Enables/Disables egress VLAN translation for all SAPs associated with the VXLAN Service. Enabling translation at the service level is only applicable if the corresponding access ports for the SAPs also have VLAN translation enabled.
- **Admin Status -** Enables/Disables the administrative status of the VXLAN Service. Disable the administrative status of the service and any associated SAPs and SDPs before deleting a service.

  Note: The **Reapply** button is enabled and can be used (in certain cases) when a VXLAN Service create/edit fails.

Creating a VXLAN Network Profile

Click on the Create icon **+** and complete the fields as described below to create the VXLAN Network Profile.

- **Profile Name -** The VXLAN Network Profile Name. Select a profile from the drop-down menu, or click on the Add icon ☐ to go to the Screen and create a profile. A “Default” profile with default parameters is available. This profile cannot be modified or deleted; however, if a VXLAN Service is deleted, this profile will be deleted if no other service is using it.
- **VRF Name -** The VRF instance associated with the profile.
- **UDP Port -** The UDP Port used by the VXLAN Service.

Creating an Service Distribution Point (SDP) Tunnel

Click on the Create icon **+**. Complete the fields as described below to create an SDP Tunnel. You can configure a Unicast or Multicast tunnel. Note that you can only configure a tunnel on a device configured with Loopback0 interface. If necessary, click on the **Create Loopback0** button to open the VLANs application and create a Loopback0 interface on a device. You can create either a Unicast or Multicast Tunnel. Select the corresponding button and complete the fields as described below. Click on the **Browse** button to create the tunnel on available devices. Note that only supported devices with a Loopback0 interface and the selected VXLAN Network Profile or no profile assigned will be available for selection during SDP tunnel configuration.

- **SDP Name -** The name of the SDP Tunnel.
- **Device IP** (Unicast) **-** The Unicast IP address of the far-end node to which customer traffic will be directed.
- **Group Address** (Multicast) **-** The PIM Multicast Group for the SDP Tunnel. Note that all neighbor nodes have to participate in the same multicast group to receive the VXLAN tunnel traffic from other members of the group.
- **Direction** (Unicast) **-** Traffic direction (Bidirectional/Unidirectional). When the service is assigned to switches, note that for Unidirectional mode, OmniVista will create SDP(s) on selected switches on the Device IP. For Bidirectional mode, OmniVista will create SDP(s) on switches selected on both the Device IP and Far End IPs. There will be one SDP created on all switches in the Far End IPs list.
- **Far End IPs** (Unicast) **-** The Unicast IP address(es) of the far-end node(s) to which customer traffic will be directed.
- **Device IPs** (Multicast) **-** The devices to include in the Multicast Tunnel. If the one or more devices selected for Multicast tunnel do not have PIM IPv4 sparse admin state enabled and PIM Bi-Direction enabled, a warning will appear listing any devices that need to be configured for PIM. Click on **Yes**, to apply the default PIM configuration profile to those devices. If you select **No**, a second warning will appear prompting you to either configure PIM on the devices or remove the devices from the configuration before proceeding.

  Note: Creation of Multicast VXLAN Services requires PIM configuration on devices in the VXLAN.

Re-Applying a VXLAN Service

The **Reapply** button is enabled and can be used (in certain cases) when a VXLAN Service create/edit fails. The process of creating a VXLAN Service involves several steps (creating the SDP Tunnel, applying the VXLAN Network Profile, creating a VXLAN, binding the SDP with the VXLAN). The **Reapply** button is activated and can be used to re-apply the configuration if one of the intermediate steps fails during the process. Complete failure scenarios are not considered for re-apply. For example:

- In a Multicast Configuration - If a user applies the configuration to 3 devices, and SDP creation succeeds but VXLAN Service creation fails, the Reapply button will be enabled. But if the configuration succeeds on 2 devices completely, but the initial configuration (e.g., SDP) fails on the 3rd device, the third device will be removed from list and the Reapply button will not be enabled.
- In a Unicast Configuration - If a user configures a device and list of far end IPs, and SDP and VXLAN configuration succeed on the far end IPs but fail on the device IP, the

Reapply button will be enabled. If configuration fails on the far end IP, the far end IP will be removed from list and the Reapply button will not be enabled.

Editing a VXLAN Service

Select the service and click on the Edit icon to bring up the Edit VXLAN Service Screen. Edit the fields as described above then click on the **Save** button to save the changes to the server.

- If the edited VXLAN Service has **not** yet been assigned to switches/ports, the update will be applied and the status displayed. Click **OK** to return to the VXLAN Service Screen.
- If the edited profile **has** already been assigned to switches/ports, a confirmation prompt will appear (you can click on **Devices** to view the switches/ports). Click on the **Update** button. The update will be applied and the status displayed. Click **OK** to return to the VXLAN Service Screen.

  Note: You cannot edit the Service Name. To edit the name, delete the service and re-configure the service with a new name.

Deleting a VXLAN Service

Select the service and click on the Delete icon, then click **OK** at the confirmation prompt.

SAP Profile

The VXLAN Service Access Point (SAP) Profile Screen is used to create, edit, delete, and assign SAP Profiles to switches/ports on the network. The SAP Profile is associated with a VXLAN service. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of network traffic to map to the associated service. You can configure up to eight (8) SAPs per port on a switch.

Creating a SAP Profile

Click on the Create icon **+**. Complete the fields as described below and click on the **Create** button.

- **Profile Name -** A unique name for the profile (up to 32 characters)
- **VXLAN Service -** The VXLAN Service associated with the profile.
- **Trusted -** Sets the Trust Mode for the SAP Profile. If set to "True", the SAP port uses the priority value obtained from tagged packets received on the port. Untagged packets use the default port priority value. If set to "False", the priority value is set to the value configured in the Priority fields for tagged and untagged packets received on the port. (Default = Trusted)
- **Priority -** The priority value to set for tagged and untagged packets received on an untrusted SAP. (Range = 0 (lowest priority) to 7 (highest priority)).
- **Description -** A user-defined description for the SAP.

Assigning a SAP Profile

After creating a profile, select the profile and click on the **Apply to Devices** button to assign the profile to switches/ports on the network. Specify only ports or link aggregates that are

configured as service access ports (see service access). This command does not apply to network ports.

After selecting the ports, configure the encapsulation value for the port(s) and select an Access Port Profile to associate with the SAP Profile (if applicable):

- **Encapsulation Values -** Configure the encapsulation value for the port(s). Only traffic matching this encapsulation value will be mapped to the SAP Profile.
  - **:0 -** Specifies a null encapsulation value. Only untagged traffic is mapped to the profile. (Default)
  - **:all -** Specifies a wildcard SAP. All tagged traffic that is not classified into another profile is mapped to the wildcard profile.
  - **:qtag[-qtag2] -** Specifies a VLAN ID tag for ingress traffic on the access port. Only traffic with this tag is mapped to this profile.
  - **:outer_qtag.inner_qtag -** Specifies an outer VLAN ID tag and an inner VLAN tag for ingress traffic on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this profile.
- **Access Port Profile -** Click on the **Browse** button and select an Access Port Profile to associate with the SAP Profile. Note that ports that have been already assigned to one Access Port Profile, cannot be assigned another profile unless all SAP profile assignments on the port are removed.

When you have completed the assignment configuration, click on the **Apply** button. The configuration will be applied and the assignment status displayed. Click **OK** to return to the SAP Profile Screen.

Editing a SAP Profile

Select the profile and click on the Edit icon to bring up the Edit SAP Profile Screen. Edit the fields as described above then click on the **Update** button to save the changes to the server. Note that you can only edit the Priority and Description Fields. Note that if any devices are assigned to a profile, the following prompt will appear - "Update also synchronizes the changes to the device". When you click **OK**, the profile is edited and changes are synced to devices.

Deleting a SAP Profile

Select a profile and click on the Delete icon, then click **OK** at the confirmation prompt. Note that this will also delete all the corresponding SAPs on devices assigned to the profile.

Access Port Profile

The VXLAN Access Port Profile Screen is used to create, edit, and delete Access Port Profiles. An Access Port Profile is a Layer 2 Profile that is applied to an access (customer facing) port. This profile is used to specify how to process Layer 2 control frames ingressing on the access port. If an Access Port Profile is not associated with an access port, the default access profile is used to process control packets that ingress on the port. An Access Port Profile is associated with a SAP Profile using the SAP Profile Screen.

Creating an Access Port Profile

Click on the Create icon. Complete the fields as described below and click on the **Create** button.

- **Profile Name -** A unique name for the profile (up to 32 characters)
- **VLAN Translation -** Enables/Disables egress VLAN translation for all Service Access Points (SAPs) associated with the profile. Enabling translation at the service level is only applicable if the corresponding access ports for the SAPs also have VLAN translation enabled.
- **L2 Profile Name -** A Layer 2 profile name for the Access Port Profile. You cannot use the default profile name ("default", "def-access-profile").
- **L2 Profile Attributes** - The Layer 2 attributes (e.g., STP BDU, L2 802.1x) are listed with the available behavior for each traffic type (Tunnel, Drop, Peer). The default configuration for each traffic type is pre-selected. Select the Layer 2 attributes for the profile by clicking on the desired behavior.

Editing an Access Port Profile

Select the profile and click on the Edit icon to bring up the Edit Access Profile Screen. Edit the fields as described above then click on the **Update** button to save the changes to the server. Note that you cannot edit the Profile Name or L2 Profile Name fields. Note that if any devices are assigned to a profile, the following prompt will appear - "Update also synchronizes the changes to the device". When you click **OK**, the profile is edited and changes are synced to devices.

Deleting an Access Port Profile

Select a profile and click on the Delete icon, then click **OK** at the confirmation prompt.

VXLAN Device View

The VXLAN Device View Screen is used to view the VXLAN configuration for devices in the network. Select and option from the drop-down menu (User Switch Picker/User Topology) and click on the **Select a Device** button to select the device you want to view. The VXLAN configuration for the switch is displayed.

VXLAN Information

The following VXLAN information is displayed for the selected switch: Network Profile, VXLAN Services, SDP Tunnels, SDP Binding, SAP).

Network Profile

Displays VXLAN Network Profile information for the switch.

- **VRF Name -** The VRF instance associated with the profile.
- **UDP Port -** The UDP Port used by the VXLAN Service.
- **Loopback 0 -** The Loopback 0 address for the VRF.

VXLAN Services

Displays general information about the VXLAN Services configured on the switch.

- **VNID -** The Virtual Network Identifier VNID is a 24-bit segment ID (also referred to as a VXLAN Segment ID) that is used to identify encapsulated frames. A VNID is bound to a VXLAN Service when the service is created. OmniVista will auto-generate a unique VNID for VXLAN Service if VNID is set to zero (0).
- **Service ID -** The VXLAN Service ID number.
- **Type -** The type of VXLAN Service (SPB or VXLAN is supported).
- **Description -** An optional, user-configured description for the VXLAN Service.
- **Multicast Mode -** The multicast replication mode for the VXLAN Service (Headend, Tandem, or Hybrid).
- **Admin Status -** The administrative status (Enabled/Disabled) of the VXLAN Service.
- **VLAN Translation-** The administrative status (Enabled/Disabled) of VLAN translation for all Service Access Points (SAPs) associated with the VXLAN Service. VLAN translation at the service level is only applicable if the corresponding access ports for the SAPs also have VLAN translation enabled.

SDP Tunnels

Displays the Service Distribution Point (SDP) configuration for the VXLAN Service.

- **ID -** The SDP identification number.
- **Far End ID -** The IP address (loopback0) or multicast group IP address associated with the far-end VXLAN node of the SDP.
- **Description -** An optional user-configured description for the SDP Tunnel.
- **Admin Status -** The administrative state of the SDP (Up or Down).
- **TTL -** The Time-to-Live (TTL) value for the SDP.

Binding

Displays the SDP binding configuration for the switch.

- **Service ID -** The ID number of the VXLAN Service that is bound to the SDP.
- **SDP Bind ID -** The unique SDP identification number that is bound to the VXLAN Service ID.

SAP

Displays the configuration information for the specified Service Access Point (SAP) associated with the VXLAN Service.

- **SAP ID -** The access port and encapsulation associated with the VXLAN Service.
- **Service ID -** The VXLAN Service ID number.
- **Description -** An optional description configured for the SAP. By default, the description is blank.
- **Trusted -** Whether or not the SAP is trusted (Yes or No).
- **Priority -** The 802.1p priority assigned to traffic mapped to this SAP. Applied only when the SAP is not trusted and a priority is specified.

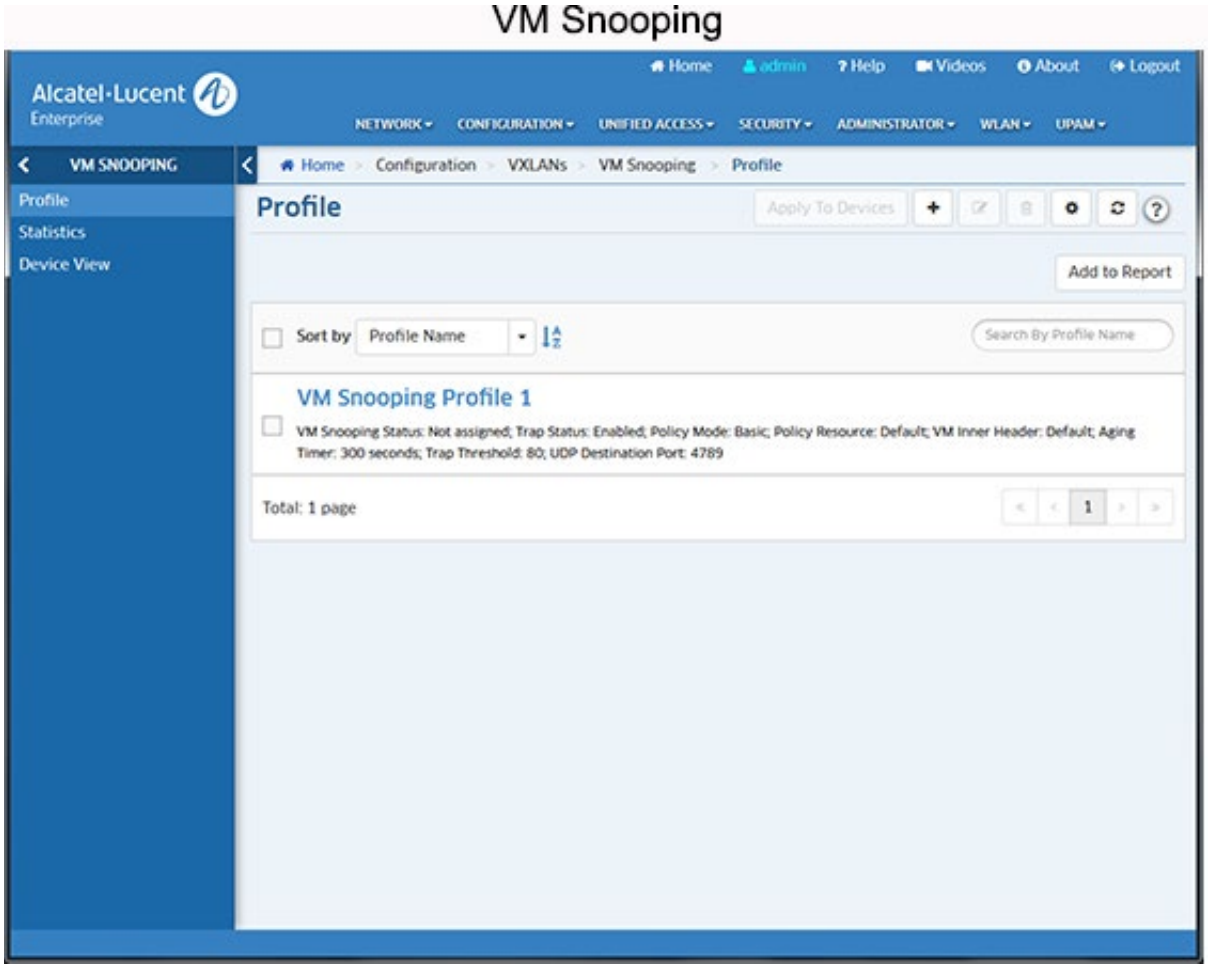
Service Access Ports

Displays Service Access Port information for the switch.

- **Port -** The slot/port number of the service access port.
- **VLAN Translation -** The administrative status of VLAN translation for the port (Enabled/Disabled).
- **L2 Profile Name -** The Layer 2 profile name for the Access Port Profile.

VM Snooping Overview

The Virtual Machine (VM) Snooping feature detects and identifies Virtual Extensible LAN (VXLAN) traffic by inspecting packets to determine if they are VXLAN encapsulated packets. Once VXLAN traffic is identified, VM Snooping collects and stores information about the VM flows in a database on the local switch. In addition to monitoring VM traffic, you can apply QoS policy list rules to the identified flows and generate SNMP traps when a new VM is learned.



To enable VM Snooping, you must create a VM Snooping Profile and assign it to switches/ports on the network. VM information can then be displayed on the VM Snooping Statistics Screen. You can also view VM Snooping Profile information for specific switches using the Device View Screen.

VM Snooping Profile

The VM Snooping Profile Screen displays all configured VM Snooping Profiles, and is used to create, edit, assign, and delete VM Snooping Profiles. A VM Snooping Profile contains global VM Snooping parameters. When a profile is created and assigned to switches/ports, VM Snooping is enabled on those switches/ports with the configured global parameters.

Creating a VM Snooping Profile

Click on the Create icon **+**. Enter a **Profile Name** and configure the profile as described below, then click on the **Create** button. When you are finished, select the checkbox next to the profile and click on the **Apply to Devices** button to assign the profile to switches/ports on the network.

- **Profile Name -** User-configured name for the profile.
- **Trap Status -** Enables/Disables traps for VM discovery or timeout. If Enabled, a trap is sent to the trap manager when a new VM is learned, or when a VM ages out and is removed from the system (Default = Disabled).
- **Policy Mode -** The policy lookup mode:
  - **Basic -** VXLAN UDP Port, VNI, inner source MAC, and inner IPv4 address are used for lookup (Default).
  - **Advanced -** VXLAN UDP Port, VNI, inner IPv4 source address, IP protocol, and L4 source and destination ports are used for policy lookup. In advanced IPv6 mode, VXLAN UDP Port, VNI, inner IPv6 source address, and L4 source and destination ports are used for lookup.
- **Policy Resource -** Used for configuring the hardware resources for VM Snooping:
  - **Default -** Specifies the default number of VM Policies.
  - **Extended -** Doubles the number of VM Policies.
- **VM Inner Header -** Optional inner header parameter used to specify if the header of the inner VM packet (Tagged, Untagged, Default). If you select "Default", the inner header option is set to the following values based on the current Policy Mode: Basic Mode - untagged and tagged VM packet header; Advanced Mode - tagged VM packet header.
- **Aging Timer -** The aging time value, in seconds, for VMs learned on the switch. Once a VM is discovered, it is added to the VM Snooping Database. If no flows are detected from a VM during the aging timer period, the VM is deleted from the VM Snooping Database. Information from this VM will no longer be available for display on the VM Snooping Statistics Screen (until flows are again detected and the VM is added to the VM Snooping Database. (Range = 60 - 86400, **or** 0 - *if set to "0" VMs will never age out*, Default = 300).
- **Trap Threshold -** The threshold percentage at which the switch generates a trap to indicate that VM Snooping has utilized the specified level of system resources (Range = 60 - 90, Default = 80).
- **UDP Destination Port -** The UDP destination port number(s) to look for when the switch inspects packets received on VM Snooping ports. This value is used to identify VXLAN encapsulated packets. The default port number is 4789. You can configure up to seven (7) additional UDP ports, however, configuring multiple UDP ports may slow down the VM Snooping process. Avoid using the well-known UDP ports that are already reserved by IANA for other applications.

Assigning a VM Snooping Profile

Select a profile and click on the **Apply To Devices** button. Select an option from the drop-down menu (Use Switch Picker/Use Topology and click on the **Add Remove Switch** button. Select the switch(es) to which you want to assign the profile. If VM Snooping has not already been enabled on the switch, a message will appear ("VM snooping is not enabled on ports") along with an "Add Port' link. Click on the link to bring up the port picker and select the ports to which you want to assign the profile and click **OK**. Repeat to assign the profile to additional switches/ports (select the switch, click on the **Add/Remove Ports** button, select the ports to which you want to assign the profile and click **OK**). When you have selected all of the switches/ports, click the **Apply** button. The Apply To Devices Results Screen will appear, displaying the status of the operation. Click **OK** to return to the Profile Screen.

Editing a VM Snooping Profile

Select the profile and click on the Edit icon to bring up the Edit VM Snooping Profile Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server.

- If the edited profile has already been assigned to switches/ports, the "Update VM Snooping Profile" confirmation prompt will appear (you can click on the **Device** link to view the devices). Click **OK** to apply the update. The update will be applied and the status displayed. Click **OK** to return to the Profile Screen.

  Note: You cannot edit the Profile Name. To edit the name, delete the profile and configure a new one.

Deleting a VM Snooping Profile

Select the profile and click on the Delete icon , then click **OK** at the confirmation prompt.

- If the edited profile has already been assigned to switches/ports, the "Update VM Snooping Profile" confirmation prompt will appear (you can click on **Device** link to view the devices). Click OK to delete the profile. The update will be applied and the status displayed. Click **OK** to return to the Profile Screen.

Removing a VM Snooping Profile From a Switch/Port

To remove a VM Snooping Profile from a switch, select the profile in the table and click on the **Apply To Devices** button. The switches to which the profile has been assigned will appear in the Assigned Switches area. Click on the **Add/Remove Switches** button to bring up the switch picker. The switches to which the profile has been assigned will appear on the right. Remove the switch(es) from the right-hand column and click **OK**. You will be returned to the Profile Screen. Click the **Apply** button. The configuration will be applied and the assignment status displayed. Click **OK** to return to the Profile Screen.

To remove a VM Snooping Profile from a port, select the profile in the table and click on the **Apply To Devices** button. The switches to which the profile has been assigned will appear in the Assigned Switches area. Select a switch and click on **Add/Remove Ports** button to bring up the port picker. The ports to which the profile has been assigned will appear on the right. Remove the port(s) from the right-hand column and click **OK** then click on the **Apply** button. The configuration will be applied and the assignment status displayed. Click **OK** to return to the Profile Screen.

VM Snooping Statistics

The VM Snooping Statistics Screen is used to display VM Snooping information for Virtual Machine (VM) traffic flows on a VM Snooping port or link aggregate. Once VM Snooping is enabled on ports, the packets flowing from the configured ports are snooped and upon matching configured UDP port, flow details are written to the VM Snooping Database. The VM Snooping Statistics Screen enables you to search for and display VM snooping information based on VM IP Address, VM MAC Address, VXLAN VNI, Destination Port, or Policy Name.

> **Note:** OmniVista collects VM Snooping statistics from a device via an FTP session. The Telnet/FTP User Name and Password must be configured on a device for OmniVista to collect statistics. If necessary, go to the Topology application, right-click select a device(s), right click and select Edit to configure the Telnet/FTP User Name and password. If the “Prefer SSH” option is enabled in Device properties, statistics will be collected via SFTP.
>
> Also note that by default there is a scheduler job performed every 15 minutes for collecting VM Snooping statistic data from the all supported switches (VSnoop Purge Scheduler). You can modify the interval time on the Scheduler Jobs Screen.

Searching for VM Information

You can search for VM information from a number of different sources and for different time periods. Enter the search criteria as described below, then click on the Search button. The information will be displayed in the Statistics Data Table.

- **From Date -** The start date for the VM information you want to view.
- **To Date -** The end date for the VM information you want to view.
- **Search By -** The search option to use. Select a search option, then enter the specific search criteria (e.g., VM IP Address, MAC Address).
  - **VM IP Address -** The VM IP address you want to search for.
  - **MAC Address -** The MAC address you want to search for.
  - **VXLAN VNI -** The VXLAN VNI you want to search for.
  - **Destination Port** - The destination port you want to search for.
  - **Policy Name -** The QoS Policy you want to search for.
- **Limit -** The number of rows of data to display (Range = 500 - 5,000, Default = 1,000).

VM Information

By default, all of the columns defined below appear in the Statistics Data Table. However, you can configure Custom Templates to view specific information. To configure a template, click on the Configuration icon next to one of the templates (**Custom Template 1**, **Custom Template 2**), select the column headings you want to display for that template, and click **OK**. You can configure two (2) Custom Templates. The headings you select when you configure a template will be displayed until you change them again.

- **Chassis/Slot/Port -** The physical port on which snooping is performed.
- **VTEP Source IP -** The VXLAN Tunnel end point source IP address.
- **VTEP Destination IP -** The VXLAN Tunnel end point destination IP address.
- **VXLAN VNI -** The VXLAN network identifier.

- **VTEP VLAN -** The VXLAN Tunnel end point VLAN.
- **VM Source MAC -** The source MAC of VM that is participating in the flow.
- **VM Source IP -** The source IP Address of VM that is participating in the flow.
- **VM Source Port -** The source port of the VM that is participating in the flow.
- **VM Destination MAC -** The VM destination MAC address.
- **VM Destination IP -** The VM destination IP address.
- **VM Destination Port -** The VM destination port.
- **VM IP Protocol -** The protocol that is being used by VMs in the flow (IPv4/IPv6).
- **Flow Learned Time -** The time at which the VM was identified during snooping.
- **Flow Update Time -** The most recent time verified, whether the flow is live or not.
- **Policy Name -** The name of the QoS policy rule applied to the VM flow.
- **Policy List -** The flow that is passing through by matching indicated policy list.
- **VM VLAN -** The VLAN on which the VM is learned and forwarded.
- **Sampled Packets -** The number of packets considered for snooping.

Device View

The VM Snooping Device View Screen is used to view VM Snooping Profile and port information for switches in the network. Click on the **Browse** button to select a switch then click **OK**. The VM Snooping configuration for the switch is displayed.

VM Snooping Profile Information

Displays VM Snooping Profile information for the selected switch.

- **Trap Status -** The VM discovery/timeout trap status. If Enabled, a trap is sent to the trap manager when a new VM is learned, or when a VM ages out and is removed from the system (Default = Disabled).
- **Policy Mode -** The policy lookup mode:
  - **Basic -** VXLAN UDP Port, VNI, inner source MAC, and inner IPv4 address are used for lookup (Default).
  - **Advanced -** VXLAN UDP Port, VNI, inner IPv4 source address, IP protocol, and L4 source and destination ports are used for policy lookup. In advanced IPv6 mode, VXLAN UDP Port, VNI, inner IPv6 source address, and L4 source and destination ports are used for lookup.
- **Policy Resource -** Used for configuring the hardware resources for VM Snooping:
  - **Default -** Specifies the default number of VM Policies.
  - **Extended -** Doubles the number of VM Policies.
- **VM Inner Header -** Optional inner header parameter used to specify if the header of the inner VM packet (Tagged, Untagged, Both) (Default = Both). By default, the inner header option is set to the following values based on the current policy lookup mode: Basic Mode—untagged and tagged VM packet header; Advanced Mode—tagged VM packet header.
- **Aging Timer -** The aging time value, in seconds, for VMs learned on the switch. Once a VM is discovered, it is added to the VM Snooping Database. If no flows are detected to/from a VM during the aging timer period, the VM is deleted from the VM Snooping

Database. Information from this VM will no longer be available for display on the VM Snooping Statistics Screen (until flows are again detected and the VM is added to the VM Snooping Database. (Range = 0 - 86400, Default = 300). If set to "0", VMs will never age out.

- **Trap Threshold -** The threshold percentage at which the switch generates a trap to indicate that VM Snooping has utilized the specified level of system resources (Range = 60 - 80, Default = 80).
- **UDP Destination Port -** The UDP destination port number(s) to look for when the switch inspects packets received on VM Snooping ports. This value is used to identify VXLAN encapsulated packets. The default port number is 4789. You can configure up to seven (7) additional UDP ports, however, configuring multiple UDP ports may slow down the VM Snooping process. Avoid using the well-known UDP ports that are already reserved by IANA for other applications.
- **Hardware Allocation Status -** The hardware resource allocation status for VM Snooping.

Enabled VM Snooping Port Information

Displays basic information for VM Snooping-enabled ports for the selected switch.

38.0 WLAN

The new Wireless LAN (WLAN) group of applications are used to configure wireless networks, AP Policies to prevent attacks on Stellar AP Series Wireless Devices, and RF Profiles for devices. It is also used to create Heat Maps and Floor Plans to design and troubleshoot Stellar AP networks. The following applications are used to monitor and configure WLAN:

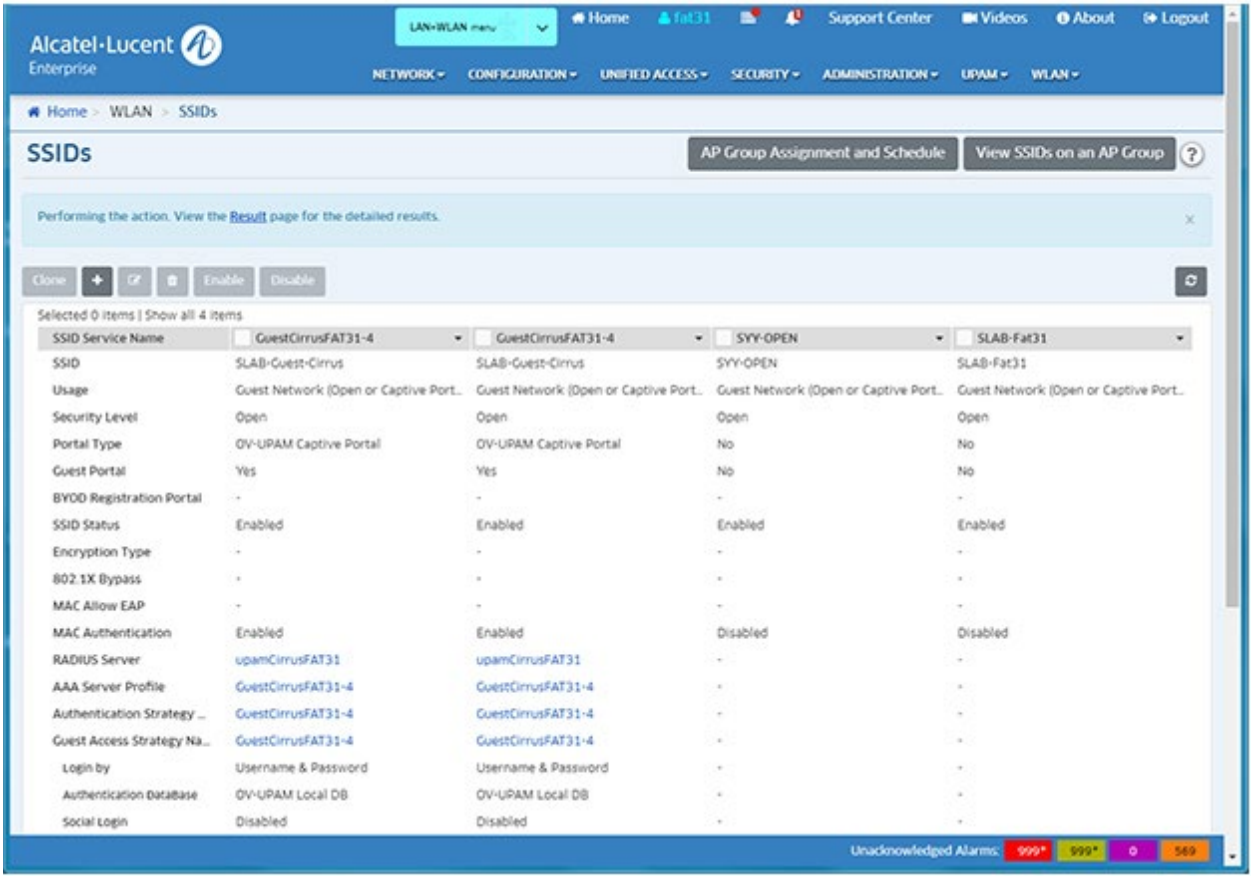
- **SSIDs -** The SSIDs application is used to configure wireless networks. The SSIDs option simplifies wireless network configuration with one-step provisioning, including SSID setup as well as authentication and policy configuration. The WLAN Service (Expert) can be used for more complex configurations.
- **WIPS -** The WIPS application is used to monitor the wireless radio spectrum for the presence of unsafe access points and clients, and is used to configure policies to classify rogue APs/wireless attacks and take countermeasures to mitigate the impact of foreign intrusions.
- **RF -** The RF application is used to create wireless RF Profiles for Stellar APs and AP Groups. RF Profiles enable the user to ensure that transmit power and operating frequencies meet the requirements of global regulatory agencies and individual countries. A user can also use the profiles to adjust the wireless parameters and functions according to real network environment to improve the user experience of wireless network.
- **Heat Map -** The Heat Map application is a design, verification, and troubleshooting tool for installed Stellar Wi-Fi networks. The application provides a way to create and organize Heat Maps from multiple locations, from Campus level to Building level and Floor level to give a comprehensive view of Wi-Fi coverage.
- **Floor Plan -** The Floor Plan application is a design, verification, and troubleshooting tool for Stellar WiFi networks. Floor Plan can be used to determine optimal placement of Stellar APs in a location. The application can also automatically determine AP placement and configurations for optimal set-up.
- **Client -** The Client application displays real time information for clients associated with Stellar APs, as well as clients that have been blacklisted. The application can also be used to manually blacklist a client.

SSIDs

The SSID application simplifies wireless network configuration with one-step provisioning, including SSID setup as well as authentication and policy configuration. When you create an SSID, relevant related default configurations (Access Role Profile, Access Policy, Authentication Strategy, Guest Access Strategy, BYOD Access Strategy, AAA Server Profile, Tunnel Profile, and Global Configuration) are automatically created and linked to the SSID using a name derived from the SSID. As you go through the creation/customization process you can customize these default SSID configurations to fit your network requirements.

The SSIDs screen displays information about all configured SSIDs. The screen displays up to 15 SSIDs at a time. Scroll to view additional SSIDs. If you have more than 15 SSIDs, you can choose which 15 SSIDs to display on the screen by customizing the display order. The screen is used to Enable/Disable SSIDs, create, edit, and delete SSIDs, and modify an SSID's AP Group Assignment and AP Availability Schedule.

SSIDs



Note: SSIDs can also be configured in the WLAN Service (Expert) application. Note that WLAN Name and WLAN Service Name refer to the SSID Service Name.

Creating an SSID

Click on the Add icon to create and customize a new SSID. Complete the fields on the Create SSID Screen and the Customize SSID Screen to customize the SSID configuration.

Create an SSID

Complete the fields as described below to create an SSID, then click on the **Create & Customize** button to customize the configuration. After completing the configuration, click on the **Save and Apply to AP Group** button to apply the SSID to AP Groups.

- **SSID Service Name -** A unique name that identifies a specific wireless service. You can have multiple SSID Services using the same SSID. For example, you could define an SSID called "Student" and have two SSID Services at different locations - "School 1" and "School 2".
- **SSID -** A name that uniquely identifies the wireless network (up to 31 characters).
- **Usage -** The SSID's usage. When you select a Usage, relevant related default configurations such as Access Policy, Authentication Strategy, Guest Access Strategy, and BYOD Access Strategy are automatically created and linked to the SSID using a name derived from the SSID. These configurations can then be customized for your network.

- **Guest Network (Open or Captive Portal) -** Create a network for Guest Users. Suitable for setting up an Open Network with or without a Captive Portal. This is typically used for Guests.
- **Employee BYOD Network -** Create a network for employees connecting with their own devices. Suitable for setting up an Open Network for Employee BYOD devices. Access to the network is granted after BYOD portal authentication.
- **Enterprise Network for Employees (802.1X) -** Create a network for employees connecting with known devices. Suitable for setting up an Enterprise Network for Employees accessing the network with Company Property or BYOD devices.
- **Protected Network (Pre-Shared Key & an Optional Captive Portal) -** Create a Protected Network for Guest Users. Suitable for setting up a Personal network that requires a PSK/Passphrase, with or without a Captive Portal. This is typically used for Guests.
- **Protected Network for Employees (Pre-Shared Key & BYOD Registration Portal) -** Create Protected Network for employees connecting with their own devices. Suitable for setting up a Personal Network that requires a PSK/Passphrase for employee BYOD devices. Access to the network is granted after BYOD portal authentication.
- **Captive Portal/BYOD -** Depending on the Usage selected, you can enable/configure Captive Portal or BYOD authentication for the SSID.
- **BYOD -** Enable/Disable BYOD authentication for the SSID.
- **Captive Portal -** Enable/Disable Captive Portal Authentication for the SSID.

  OV-UPAM Captive Portal - Authenticate through OmniVista Cirrus UPAM Captive Portal.

  External Captive Portal - Authenticate through an external Captive Portal.

Customize an SSID

As mentioned earlier, when you create an SSID, relevant related default configurations (e.g., Access Role Profile, Access Policy, Authentication Strategy) are automatically created and linked to the SSID using a name derived from the SSID. As you go through the creation/customization process you can customize these SSID configurations to fit your network requirements.

When you create an SSID, the default configuration is displayed on the Customize SSID Screen. Complete the fields as described below to customize these defaults as well as additional SSID configurations. Note that the fields displayed depend on the Usage that you selected in the previous screen.

General

- **SSID Service Name (Pre-Filled) -** A unique name that identifies the wireless service.
- **SSID -** A name that uniquely identifies the wireless network (up to 31 characters).
- **Usage - (Pre-Filled)** The Usage selected for the network (e.g., Guest Network, Employee BYOD Network).
- **Security Level (Pre-Filled) -** The Security Level for the network based on the Usage selected (e.g., Open, Personal, Enterprise)

- **Guest Portal/BYOD Registration (Pre-Filled) -** Whether or not Captive Portal/BYOD Registration are configured (Yes/No).
- **Portal Type - (Pre-Filled) -** The type of Captive Portal/BYOD Portal configured (e.g., OV-UPAM Captive Portal).
- **Allowed Band -** The band(s) available on the network:
  - GHz
  - GHz
  - GHz
  - All - 6.0 GHz, 5.0 GHz, and 2.4 GHz
- **Enhanced Open** - Enables/Disables the use of Wi-Fi Enhanced Open™ to secure an open SSID. Wi-Fi Enhanced Open™ is a security standard that is based on Opportunistic Wireless Encryption (OWE). When enabled, OWE is used to ensure that communication between each pair of endpoints is protected from other endpoints. Data sent between a client and an AP is provided individualized data protection. Wi-Fi Enhanced Open™ offers improved data privacy, while maintaining convenience and ease-of-use. This functionality is particularly useful for provisioning a secure open SSID in public spaces. Configuring the status of this attribute is based on the following:
  - If 2.4 GHz and/or 5.0 GHz is the allowed band (not 6.0 GHz), you can enable or disable Enhanced Open status
  - If 6.0 GHz is the allowed band, then Enhanced Open is automatically enabled whether or not 2.4 GHz or 5.0 GHz is selected. You cannot disable the Enhanced Open status.
- **Encryption Type -** The Encryption Type rule for the specified Access Role Profile. The specified Access Role Profile will be applied if the encryption type used by the client matches with the value defined in the rule. The types available depend on the Usage selected (e.g., Protected Network, Enterprise Network).
- **Protected Network** - The WI-FI will be protected by a key.
  - STATIC_WEP - Authentication with Static Wired Equivalent Privacy security algorithm.
  - WPA_PSK_TKIP - WPA with TKIP encryption using a preshared key.
  - WPA_PSK_AES - WPA with AES encryption using a preshared key.
  - WPA_PSK_AES_TKIP - WPA with TKIP and AES mixed encryption using a preshared key.
  - WPA2_PSK_TKIP - WPA2 with TKIP encryption using a preshared key.
  - WPA2_PSK_AES - WPA2 with AES encryption using a preshared key.
  - AUTO_WPA_WPA2- WPA or WPA2 mixed mode, which allows both WPA capable client and WPA2 capable client access.
  - WPA3_SAE_AES - WPA3 with AES encryption using a preshared key, which ONLY allow WPA3 capable client accessing.
  - WPA3_PSK_SAE_AES - WPA3 and WPA2 mixed mode, which allow both WPA3 capable client as well as ONLY WPA2 capable client accessing.
- **Enterprise Network** - An authentication server will be used to authenticate the connecting client via 802.1x Authentication.
  - DYNAMIC_WEP - WEP with dynamic keys.

  - WPA_TKIP - WPA with TKIP encryption and dynamic keys using 802.1X.
  - WPA_AES - WPA with AES encryption and dynamic keys using 802.1X.
  - WPA2_TKIP - WPA2 with TKIP encryption and dynamic keys using 802.1X.
  - WPA2_AES - WPA2 with AES encryption and dynamic keys using 802.1X.
  - AUTO_WPA_WPA2- WPA or WPA2 mixed mode, which allows both WPA capable client and WPA2 capable client access.
  - WPA3_AES256 - WPA3 with CNSA (Suite B) using 802.1X. Note that when WPA3_AES256 encryption is applied to an AP that does not support it, the encryption will automatically fall back to WPA2_AES. OAW-AP1101 full band, OAW-AP1201H 2.4G band, and OAW-AP1201L 2.4G band do not support WPA3_AES256 authentication.
  - WPA3_AES - WPA3 with AES encryption and dynamic keys using 802.1X. Note that Stellar AP Models AP1101, AP1201H, and AP1201L do not support WPA3 authentication.

- **802.1X Bypass -** 802.1X bypass administrative status (Enabled/Disabled). When 802.1X bypass is enabled, the user's 802.1X authentication method is performed conditionally based on the result of MAC Authentication. (Default = Disabled).
- **MAC Authentication -** MAC Authentication administrative status (Enabled/Disabled).
- **MAC Allow EAP -** Extensible Authentication Protocol (EAP) administrative status (Enabled/Disabled).
- **Encryption Type -** The encryption type used by the client (e.g., WPA/WPA2 AES).
- **Key Format -** PSK format.
- **PSK/Passphrase -** Enter a PSK Passphrase for authentication.
- **Confirm PSK/Passphrase -** Re-enter the PSK Passphrase.
- **Device Specific PSK -** Enables/Disables Device Specific PSK. Device Specific PSK provides more security than traditional PSK. If Device Specific PSK is enabled and a device is configured for Device Specific PSK, when the AAA Server sends the Radius Access Accept for MAC Authentication for the device, it will also send the specific pre-shared key for that device, differentiated by the device's MAC Address. This means that each device will have a different key. If enabled:
  - **Prefer Device Specific PSK -** If the AAA Server sends the "AES-CBC-128" attribute along with the Radius Access Accept response, this value will be used. If the AAA server does NOT send the "AES-CBC-128" attribute, the key configured in the SSID will be used.
  - **Force Device Specific PSK -** The value of "AES-CBC-128" attribute returned by AAA Server will be always used, whether it exists or not.

  Note: Device Specific PSK will only work with a UPAM RADIUS Server. Devices are configured for Device Specific PSK on the Company Property Screen (UPAM - Authentication - Company Property). See the Company Property online help for more information. You can also configure a device for Device Specific PSK from the Authentication Record List (UPAM - Authentication - Authentication Record). See the Authentication Record online help for more information.

Private Group PSK

When enabled SSID is created, you can either create a static PSK or enforce Device Specific PSK. This provides a common Passphrase key, which is suitable for networks requiring network-wide common PSK. Enabling Private Group PSK (PPSK) allows you to create private groups of client devices based on a PPSK Entry. Each client device specifies a Passphrase when connecting to an SSID. If the passphrase matches any of the PPSK Entry, the client is placed in the specified Access Role Profile.

Configuring the Private Group PSK attribute is offered only when Device Specific PSK is Disabled or set to "Prefer Device Specific PSK". When the Device Specific PSK is set to "Force Device Specific PSK", OmniVista will not display the Private Group PSK attribute because the Passphrase specified in Company Property is used instead.

Complete the following fields to configure PPSK Entries:

- **Private Group PSK** - Enables/Disables the grouping of Device Specific PSKs. When enabled:
    - **PPSK Entries** - At least one Private Group PSK (PPSK) Entry is required with the following parameters:
        - **Name** - Enter a unique name to identify the PPSK Entry. No two Entries can have the same Name.
        - **Passphrase** - Enter a unique PSK Passphrase for authentication. No two Entries can have the same Passphrase.
        - **Access Role Profile** - Select the name of an Access Role Profile.

    Note: Each SSID can have upto 16 PPSK Entries. The total number of entries across all SSIDs that exist on an AP cannot exceed 64 on any AP.

Authentication Strategy

- **MAC Authentication -** MAC Authentication administrative status on the network. If enabled:
    - **RADIUS Server -** RADIUS Server used for authentication. Select an existing server from the drop-down or click on the Add icon to create a new server to select. Note the following when selecting the RADIUS Server:
        - If you select a TLS-enabled RADIUS Server, the AAA profile generated for the SSID will specify only a Primary 802.1x Authentication Server and a Primary 802.1x Accounting Server, but other servers will be empty.
        - If you select a TLS-disabled RADIUS Server, the AAA Server Profile generated for the SSID assigns the server for Captive Portal and MAC authentication. However, editing the TLS-disabled RADIUS Server for the SSID to enable TLS will fail. A TLS-enabled RADIUS Server does not support Captive Portal and MAC authentication in the AAA Server Profile.
- **Guest Authentication Database -** The database used for Guest Authentication.

The following configuration options may be available, depending on the Usage you selected:

- **Advanced Configuration -** Click on this link to go to the UPAM - Authentication Strategy Screen to customize your MAC Authentication configuration.

- **Manage Employee Devices -** Click on this link to open the UPAM Company Property window to view/manage devices owned by your company and assigned to an employee for daily use.
- **Manage Guest Devices -** Click on this link to open the UPAM Company Property window to view/manage known devices of Guests.
- **Manage Employee Accounts -** Click on this link to open the UPAM Local Employee Accounts window to view/manage Employee Accounts.
- **Edit Server Attributes -** Click on this link to open the RADIUS Server Management window to view/edit the selected RADIUS Server.

Note: The automatically generated AAA Server Profile is given the same name as the SSID. Do not make changes to this profile through the AAA Server Profile Page. For example, if you want to change the RADIUS server, edit the SSID and select a different RAIUS server. Alternatively, go to the AAA Server Profile page and select the corresponding profile row to make the edit.

Access Policy

- **Default Access Policy -** A default Access Policy is automatically created with the SSID Name. You can customize the default Access Policy by creating the SSID and then editing it. After creating the SSID, select the SSID on the SSIDs Screen and click on the Edit icon. The Default Access Policy will now display a "Customize" link. Click on the link to customize the Default Access Policy.
- **Existing Access Policy -** If you do not want to use the Default Access policy, you can select an existing policy from the drop-down menu. If necessary, you can create a new policy by going to the the UPAM - Authentication - Access Policy Screen. After creating the new policy, return to this screen to select the new policy.

Note: The "WLAN Name" Mapping Condition refers either to the "SSID Service Name" in the “SSIDs” application or to the "WLAN Service Name" in the WLAN Service (Expert) application.

Guest Access Strategy

- **Portal Page -** The name of the Captive Portal Page being used for guest access.
- **Login By -** The Captive Portal login method (e.g., Username and Password).
- **Social Login -** Administrative status of the Social Login feature (Enabled/Disabled). If enabled, a guest user can log into the network through a social media account (e.g., Facebook)
- **Self-Registration Strategy -** Administrative status of self-registration (Enabled/Disabled). If enabled, a guest user is required to perform self-registration and approval before accessing the network.
- **URL to Redirect to on Success -** the redirect URL for the browser that is presented after a guest user passes Captive Portal authentication.

The following configuration options may be available, depending on the Usage you selected:

- **Customize -** Click on this link to go to the UPAM Guest Access Strategy Screen and customize the Guest Access configuration.
- **Customize Portal Page -** Click on this link to go to the UPAM Custom Portal Screen and customize the Captive Portal Page presented to users.

- **Manage Guest Accounts -** Click on this link to open the UPAM Guest Accounts window, where you can view/manage Guest Accounts.

BYOD Access Strategy

- **Portal Page -** The name of the Captive Portal Page being used for BYOD access.
- **Employee Database -** The database used for employee records.
- **URL to Redirect to on Success -** The redirect URL for the successful BYOD authentication.

The following configuration options may be available, depending on the Usage you selected:

- **Customize -** Click on this link to go to the UPAM BYOD Access Strategy Screen and customize the BYOD Access configuration.
- **Customize Portal Page -** Click on this link to go to the UPAM Custom Portal Screen and customize the Captive Portal Page presented to users.
- **Manage Employee Accounts -** Click on this link to open the UPAM Local Employee Accounts window, to view/manage Employee Accounts.

Default VLAN/Network

A Default Access Role Profile will be applied to clients joining this SSID if a role cannot be assigned by other role assignment methods. In this section, you can configure the Default VLAN/Network and other attributes of this Default Access Role Profile. You can either create a new Access Role Profile or use an existing Access Role Profile for this SSID.

Configure Access Role Attributes

- **General**
  - **Default VLAN/Network**
    - **VLAN(s) -** Maps the profile to a specific VLAN(s) on network devices. For AOS Devices, a VLAN must exist on a switch to configure VLAN Mapping. However, for Stellar APs, you can map an Access Role Profile to untagged traffic (the VLAN ID must be between 1 and 4094 or "untagged"). Also note that for Stellar APs you can configure a VLAN Pool by entering multiple VLANs. You can enter VLANs as a range (e.g., 10-20), as individual VLANs (21, 23, 25), or both (10 - 20, 21, 23, 25). In addition, the number of WLANs the following Stellar AP models can support based on a configuration of 256 VLANs per WLAN/SSID varies:
      - AP1301H - Maximum 2 WLANs/SSIDs can supported 256 VLANs; total 2x256 VLANs can be assigned to all WLAN on the device.
      - AP1311/AP1301/AP1431/AP1411 - Maximum 4 WLANs/SSIDs can supported 256 VLANs; total 4x256 VLANs can be assigned to all WLAN on the device.
      - AP1320/AP1331/AP1351/AP1451- Maximum 7 WLANs/SSIDs can supported 256 VLANs; total 7x256 VLANs can be assigned to all WLAN on the device.
  - **Use Tunnel** (see Tunnel Guidelines below)

- **Tunnel ID -** The VPN ID used for Access Role Profile mapping. (Range = 0 - 16777215, suggested range of 64001 - 65000). If the Tunnel ID is set to "0", no GRE Key is sent.
- **GRE Tunnel Server IP Address/Data VPN Server -** The IP Address of the Tunnel Termination Switch (GRE Tunnel Server/Data VPN Server) used for mapping to the Access Role Profile. Select a switch from the drop-down or enter an IP address.
- **Backup GRE Tunnel Server IP Address** - The IP address of a backup GRE Tunnel Server to provide tunnel redundancy between an AP and the GRE Tunnel Server. Select a switch from the drop-down or enter an IP address. When the primary GRE Tunnel Server IP address goes down, the backup Tunnel Server takes over. Note that configuring a backup tunnel between an AP and the GRE Tunnel Server is supported on AWOS 4.0.5.15 or later.
- **Keepalive Interval** - The time interval, in seconds, for APs to check the status of the far-end IP address for the GRE Tunnel Server. (Range = 2 - 5 seconds, Default = 5 seconds)
- **Response Timeout** - The amount of time, in seconds, to wait for a response from the GRE Tunnel Server to keepalive requests. (Default = 2 seconds)
- **Retries** - The number of times to retry after a failed Keepalive request. (Range = 3 - 5, Default = 3). A failover to the backup GRE Tunnel Server IP address occurs after the last retry has failed.
- **Preemption** - Enables/Disables whether to go back to the primary GRE Tunnel Server. (Default = Disabled). When enabled:
    - **Preemption Countdown Timer** - Specify the amount of time to wait, in seconds, after a failover to the backup GRE Tunnel Server before attempting to go back to the primary GRE Tunnel Server. The countdown timer restarts on every switchover to the backup server. (Default = 300 seconds)
- **MTU** - Specify the MTU value for the GRE Tunnel. The recommended value is 1476 for Raw GRE and 1416 for GRE over wireguard interface. Leave this value blank if you do not want to set a specific value.
- **TCPMSS** - Specify the TCPMSS value for the GRE Tunnel (Range = 500 - 1426, Default = 1250).
- **Support of Entropy -** Enables/Disables entropy. An ALE Switch acting as a GRE Tunnel Server requires Entropy; however, some third-party GRE Tunnel Servers (e.g., Linux) require no Entropy.
- **Allow Local Breakout -** Enables/Disables Local Breakout on the tunnel. If enabled, enter the Static Route(s) to be used for entering the Tunnel. All other traffic will go out through the local network. Make sure you have applied the relevant Data VPN Server to AP Groups in the SSID **before** choosing Data VPN Server as the Tunnel endpoint. To apply a Data VPN Server to an AP Group, go to the AP Groups page (Network - AP Registration - AP Group) and edit the Data VPN Setting for the group. Note that only one VLAN inside the tunnel (tunnel ID

different from 0 if tagged, 0 if untagged) can be enabled with Local Breakout.

- **Static Routes -** Specify the static routes to be used for entering the tunnel. All other traffic will go out through the local network.
  - Avoid specifying static routes pertaining to the VLAN ID of the traffic that enters the Tunnel. For example, if VLAN ID = 41 is specified to be carried within the Tunnel and if the network subnet that corresponds to VLAN 41 is 192.168.41.0, the AP will automatically set up this route and make sure traffic destined for 192.168.41.0 will enter the Tunnel. The AP will automatically set up this route and make sure traffic with VLAN ID = 41 will enter the Tunnel. **Do not specify an explicit Route** with Destination = 192.168.41.0, as that will confuse the AP and lead to poor performance.
  - The static routes specified will be accumulated on an AP across all SSIDs assigned to the AP. For example, if you have two SSIDs configured on the same AP and configure SSID1 to use Tunnel Profile T1 with Static Routes A and B, and configure SSID2 to use Tunnel Profile T2 with Static Routes C and D, all of the routes (A, B, C, and D) will be applicable for SSID 1 and SSID 2.
  - Across all of the routes applied on an AP from the different SSIDs, make sure any destination IP subnet is specified only once. Each route applied on an AP should be for a different IP subnet, even across the SSIDs. Also, avoid specifying static routes pertaining to the VLAN ID of the traffic that enters the tunnel. The AP will automatically set up such routes. If a route to IP subnet X already exists in an SSID and that SSID is applied to an AP, another route to the same IP subnet X must not be specified in the same or a different SSID that is applied to the same AP.

- **ACL/QoS -** ACL/QoS Policy to be applied to traffic on the SSID. Click on the Add icon to configure a new policy.

- **External Captive Portal**
  - **Portal Server -** The FQDN/IP address of the external captive portal server.
  - **Redirect URL -** The redirect URL for the captive portal authentication.
  - **HTTPS Redirection -** Specify whether the redirect portal page is using HTTPS protocol.
  - **AAA Server Profile -** The AAA Server used for Captive Portal Authentication.
  - **Custom Profile -** The External Captive Portal Config File used for communication between APs and the External Portal Server. The External Captive Portal Config File is configured on the AP Groups Screen in the AP Registration application.
- **Web Content Filtering**

- **WCF Profile -** Select a WCF Profile from the drop-down to include in the SSID. If necessary, click on **Add New** to bring up the WCF Profile Screen to add a new profile. An SSID can only contain one WCF Profile. Note that an AP will allow any URL to be accessed by the first time a user visits that URL, while the AP tries to determine whether this URL is to be restricted for this Access Role Profile or not. If the URL is to be restricted, subsequent users belonging to the same Access Role Profile will then be blocked from visiting this restricted URL. So, on any given AP, Web Content Filtering will not be effective for the first visitor of a restricted URL. Web Content Filtering rules will be effective for such first visitors only after DNS cache expires on the user device.

- **Walled Garden**
  - **Wireless Client Social Login Vendor -** Select a vendor(s) to allow a wireless client to authenticate through a social media vendor (Facebook, Google, and Rainbow are supported). OmniVista will automatically configure the Allowlist Domains for the selected vendor(s). This will allow the user to connect over the Internet to the selected vendor(s) for authentication.
  - **Allowlist Domains -** In addition to Facebook, Google, and Rainbow login, you can enter any Allowlist Domain to allow a user to connect to sites over the Internet without authentication. For example, a hotel may want to allow a guest to connect to their website without authentication. Enter the Allowlist Domain and click on the Add icon to allow access to the site. Repeat to add additional domains. Domains must be entered in Fully Qualified Domain Name (FQDN) format (e.g., www.marriot.com, www.bbc.com). IP Addresses and http/https prefixes should not be used.

Tunnel Guidelines

If you create two tunnel profiles with the same Remote IP and Tunnel ID, the "Support of Entropy" status **must** be the same on both tunnels (both must be "enabled" or "disabled"). Choose the value based on what use case you plan to deploy. The following are the four possible use cases that are supported:

1. GRE Tunnel from AP to AOS Switch - This is the typical Guest Tunnel use case where AOS acts as the Guest Tunnel Termination Switch. The AOS Switch expects the Tunnel ID to be non-0 and "Support of Entropy" must be "Enabled".

2. GRE Tunnel from AP to Non-AOS Switch/Server (e.g., Nokia 7750 SR/Standard Linux Tunnel Server) - This is the Guest Tunnel use case with a non-AOS switch. The Tunnel ID must be 0 and "Support of Entropy" must be "Disabled", as the Key field in L2GRE header is not expected by the Switch/Server.

3. GRE Tunnel Between AP and OV VPN Server Appliance - This is the regular Data VPN tunnel use case between Remote APs and and an OV VPN Server acting as the Data VPN Server. The Tunnel ID must be 0 and "Support of Entropy" must be "Disabled", as the Key field in L2GRE header is not expected by OV VPN Server.

4. GRE Tunnel from AP to AOS Switch, Over the Data VPN tunnel Between AP and OV VPN Server Appliance - This is a rare use case of using the Data VPN tunnel to reach from a remote site where the AP is located, to the Central Site where the AOS Switch is located. The AOS Switch expects the Tunnel ID to be non-0 and "Support of Entropy" must be "Enabled".

The following combinations of values are not supported:

- Tunnel ID > 0 and Support of Entropy = Disabled
- Tunnel ID = 0 and Support of Entropy = Enabled.

Choose an Existing Access Role Profile

- **General**
  - **Default VLAN/Network**
    - **VLAN(s) -** Maps the profile to a specific VLAN(s) on network devices. For AOS Devices, a VLAN must exist on a switch to configure VLAN Mapping. However, for Stellar APs, you can map an Access Role Profile to untagged traffic (the VLAN ID must be between 2 and 4090 or "untagged"). Also note that for Stellar APs you can configure a VLAN Pool by entering multiple VLANs. You can enter VLANs as a range (e.g., 10-20), as individual VLANs (21, 23, 25), or both (10 - 20, 21, 23, 25). In addition, the number of WLANs the following Stellar AP models can support based on a configuration of 256 VLANs per WLAN/SSID varies:
      - AP1301H - Maximum 2 WLANs/SSIDs can supported 256 VLANs; total 2x256 VLANs can be assigned to all WLAN on the device.
      - AP1311/AP1301/AP1431/AP1411 - Maximum 4 WLANs/SSIDs can supported 256 VLANs; total 4x256 VLANs can be assigned to all WLAN on the device.
      - AP1320/AP1331/AP1351/AP1451- Maximum 7 WLANs/SSIDs can supported 256 VLANs; total 7x256 VLANs can be assigned to all WLAN on the device.
  - **Use Tunnel** (see Tunnel Guidelines above.)
    - **Tunnel ID -** The VPN ID used for Access Role Profile mapping. (Range = 0 - 16777215, suggested range of 64001 - 65000). If the Tunnel ID is set to "0", no GRE Key is sent.
    - **GRE Tunnel Server IP Address/Data VPN Server -** The IP Address of the Tunnel Termination Switch (GRE Tunnel Server/Data VPN Server) used for mapping to the Access Role Profile. Select a switch from the drop-down or enter an IP address.
    - **Backup GRE Tunnel Server IP Address** - The IP address of a backup GRE Tunnel Server to provide GRE tunnel redundancy between an AP and the GRE Tunnel Server. Select a switch from the drop-down or enter an IP address. When the primary GRE Tunnel Server IP address goes down, the backup Tunnel Server takes over. Note that configuring a backup tunnel between an AP and the GRE Tunnel Server is supported on AWOS 4.0.5.15 or later.
    - **Keepalive Interval** - The time interval, in seconds, for APs to check the status of the far-end IP address for the GRE Tunnel Server. (Range = 2 - 5 seconds, Default = 5 seconds)

- **Response Timeout** - The amount of time, in seconds, to wait for a response from the GRE Tunnel Server to keepalive requests. (Default = 2 seconds)
- **Retries** - The number of times to retry after a failed Keepalive request. (Range = 3 - 5, Default = 3). A failover to the backup GRE Tunnel Server IP address occurs after the last retry has failed.
- **Preemption** - Enables/Disables whether to go back to the primary GRE Tunnel Server. (Default = Disabled). When enabled:
- **Preemption Countdown Timer** - Specify the amount of time to wait, in seconds, after a failover to the backup GRE Tunnel Server before attempting to go back to the primary GRE Tunnel Server. The countdown timer restarts on every switchover to the backup server. (Default = 300 seconds)
- **MTU** - Specify the MTU value for the GRE Tunnel. The recommended value is 1476 for Raw GRE and 1416 for GRE over wireguard interface. Leave this value blank if you do not want to set a specific value.
- **TCPMSS** - Specify the TCPMSS value for the GRE Tunnel (Range = 500 - 1426, Default = 1250).
- **Support of Entropy -** Enables/Disables entropy. An ALE Switch acting as a GRE Tunnel Server requires Entropy; however, some third-party GRE Tunnel Servers (e.g., Linux) require no Entropy.
- **Allow Local Breakout -** Enables/Disables Local Breakout on the tunnel. If enabled, enter the Static Route(s) to be used for entering the Tunnel. All other traffic will go out through the local network. Make sure you have applied the relevant Data VPN Server to AP Groups in the SSID **before** choosing Data VPN Server as the Tunnel endpoint. To apply a Data VPN Server to an AP Group, go to the AP Groups page (Network - AP Registration - AP Group) and edit the Data VPN Setting for the group. Note that only one VLAN inside the tunnel (tunnel ID different from 0 if tagged, 0 if untagged) can be enabled with Local Breakout.
  - **Static Routes -** Specify the static routes to be used for entering the tunnel. All other traffic will go out through the local network.
    - Avoid specifying static routes pertaining to the VLAN ID of the traffic that enters the Tunnel. For example, if VLAN ID = 41 is specified to be carried within the Tunnel and if the network subnet that corresponds to VLAN 41 is 192.168.41.0, the AP will automatically set up this route and make sure traffic destined for 192.168.41.0 will enter the Tunnel. The AP will automatically set up this route and make sure traffic with VLAN ID = 41 will enter the Tunnel. **Do not specify an explicit Route** with Destination = 192.168.41.0, as that will confuse the AP and lead to poor performance.
  - The static routes specified will be accumulated on an AP across all SSIDs assigned to the AP. For example, if you have two SSIDs configured on the same AP and configure SSID1 to use Tunnel Profile T1 with Static Routes A and B, and configure SSID2 to use

Tunnel Profile T2 with Static Routes C and D, all of the routes (A, B, C, and D) will be applicable for SSID 1 and SSID 2.

- Across all of the routes applied on an AP from the different SSIDs, make sure any destination IP subnet is specified only once. Each route applied on an AP should be for a different IP subnet, even across the SSIDs. Also, avoid specifying static routes pertaining to the VLAN ID of the traffic that enters the tunnel. The AP will automatically set up such routes. If a route to IP subnet X already exists in an SSID and that SSID is applied to an AP, another route to the same IP subnet X must not be specified in the same or a different SSID that is applied to the same AP.

- **Default Access Role Profile -** Select the default Access Role Profile that will be applied to clients if a role cannot be assigned by other role assignment methods.

Advanced Access Role Configuration

- **Location Policy -** Select a Location Policy. A Location Policy defines a specific location where a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.
- **Period Policy -** Select a Period Policy. A Period Policy specifies the days and times during which a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.
- **Bandwidth Control Settings**
  - **Upstream Bandwidth -** The maximum bandwidth limit allocated for ingress traffic on UNP ports assigned to the profile. If the maximum ingress bandwidth value is set to zero, all ingress traffic is allowed on the UNP port. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)
  - **Downstream Bandwidth -** The maximum bandwidth limit allocated for egress traffic on UNP ports assigned to the profile. If the maximum egress bandwidth set to zero, all egress traffic is allowed on the UNP port. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)
  - **Upstream Burst -** The maximum ingress depth value that is applied to traffic on UNP ports that are assigned to the profile. This value determines how much the traffic can burst over the maximum ingress bandwidth rate. The maximum ingress depth value is configured in conjunction with the maximum ingress bandwidth parameter. When the ingress depth value is reached, the switch starts to drop packets. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)
  - **Downstream Burst -** The maximum egress depth value that is applied to traffic on UNP ports that are assigned to profile. This value determines how much the traffic can burst over the maximum egress bandwidth rate. The maximum egress depth value is configured in conjunction with the maximum egress bandwidth parameter. When the egress depth value is reached, the switch starts to drop packets. (Not supported on AOS 7.3.4 switches and ignored when applied to those devices.)

- **Client Session Logging -** Enables/Disables client session logging.
  - **Client Connection Logging Level** - Select a logging level:
    - **Logging HTTP/HTTPs** - Log only the HTTP/HTTPs web session of wireless clients.
    - **Logging ALL -** Log all sessions of wireless clients, including HTTP/HTTPs.
    - **None -** Log only client online/offline behavior, without session details.
- **DHCP Option 82 -** Enables/Disabled the DHCP Option 82 Feature. If necessary, click on the link to go to the DHCP Option 82 Screen to configure the feature.

Advanced WLAN Service Configuration

SSID Setting

- **Basic**
  - **Hide SSID -** Enables/Disables SSID in beacon frames. Note that hiding the SSID does very little to increase security. (Default = Disabled)
  - **UAPSD -** Enables/Disables Unscheduled Automatic Power Save Delivery (UAPSD) on the SSID. UAPSD is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow that is delivered over the wireless media. Because UAPSD does not require the client to poll each individual packet that is buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. (Default = Enabled)
- **Security**
  - **Classification Status -** Enables/Disables classification. If classification is enabled, traffic will be classified to a role based on the configured classification rules. Note that the precedence of role assignment methods is important. Classification Rules are only used if 802.1x/MAC authentication does not return a role, or the returned role is not matched with any configured roles in the device.
  - **MAC Pass Alt -** If MAC Authentication is enabled, select an Access Role Profile to assign to clients that pass MAC Authentication.
  - **Client Isolation -** Enables/Disables Client Isolation. If enabled, traffic between clients on the same AP in the SSID is blocked; client traffic can only go toward the router. (Default = Disabled)
  - **Protected Management Frame -** Configures whether connections are accepted from clients supporting Protected Management Frame for certain Security Levels/Encryption Types (Enterprise - WPA2_AES/WPA3_AES256/ WPA3AES, Personal - WPA2_PSK_AES/WPA3_SAE_AES/WPA3_PSK_SAE_AES)
  - **Disabled -** Disables Protected Management Frame requirements.
  - **Optional -** Allows connections from clients supporting Protected Management Frame and clients that do not.
  - **Required -** Only allows connections from clients supporting Protected Management Frame.

- **Hotspot 2.0**
  - **Hotspot 2.0 -** Enables/Disables Hotspot 2.0. Hotspot 2.0 is a new standard for public-access Wi-Fi that enables seamless roaming among Wi-Fi networks and between Wi-Fi and cellular networks. Hotspot 2.0 was developed by the Wi-Fi Alliance and the Wireless Broadband Association to enable seamless hand-off of traffic without requiring additional user sign-on and authentication. Note that Hotspot 2.0 is only supported with Enterprise WPA2_AES or Enterprise WPA3_AES256 Encryption. You must first select one of these Encryption types before you can enable Hotspot 2.0.
  - **Operator Name -** The operator providing the Hotspot service (0 - 252 characters).
  - **Venue Name -** The venue where the Hotspot is hosted (0 - 252 characters).
  - **Venue Type -** The type of venue hosting the Hotspot.
  - **Network Detail -** The type of Hotspot network.
  - **Domain List -** The list of Hotspot Domains. You can have up to 16 Domain Names (1 - 255 characters each).
  - **Roaming OIs** - The Roaming Organization Identifier. You can have up to 16 OIs. Each OI field is 3 characters in length if the organizationally unique identifier is an OUI, or 5 octets in length if the organizationally unique identifier is an OUI-36.
- **Advanced**
  - **Roaming Controls**
    - **L3 Roaming -** Enables/Disables Layer 3 roaming. Layer 3 roaming allows client to move between Access Points and connect to a new IP subnet and VLAN.
    - **FBD Update on Association -** Enables/Disables FDB update on Association. If enabled, when a client roams to a new AP, the AP will send ARP packets to the uplink switch to notify the switch to change the downstream forwarding port for the wireless client's traffic.
    - **802.11r -** Enables/Disables IEEE 802.11r (Fast BSS Transition). The Fast BSS Transition mechanism minimizes the delay when a a client transitions from one BSS to another within the same group.
    - **OKC -** Enables/Disables OKC Roaming. If OKC Roaming is enabled, a cached Pairwise Primary Key is used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1x authentication.
    - **802.11k Status -** Enables/Disables 802.11k. The 802.11k protocol enables APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other.
    - **802.11v Status -** Enables/Disables 802.11v. 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an Instant AP to request a voice client to transition to a specific AP, or suggest a set of preferred

APs to a client due to network load balancing or BSS termination. It also helps the client identify the best AP to transition to as they roam.

- **Client Controls**
  - **Max Number of Clients Per Band -** The maximum number of clients allowed in each band. (Range = 1 - 256, Default = 64)
  - **802.11b Support -** Enables/Disables allowing 11b legacy clients connect to APs.
  - **802.11a/g Support** - Enables/Disables allowing 11a/g legacy clients connect to APs.
- **Minimum Client Date Rate Controls**
  - **2.4GHz Minimum Client Data Rate Controller -** Enables/Disables 2.4G band access control based on client data rate.
  - **2.4GHz Minimum Client Data Rate -** 2.4G band client with lower data speed will not be given access, recommended value 12.
  - **5GHz Minimum Client Data Rate Controller -** Enables/Disables 5G band access control based on client data rate.
  - **5GHz Minimum Client Data Rate -** 5G band client with lower data speed will not be given access, recommended value 24.
  - **6GHz Minimum Client Data Rate Controller -** Enables/Disables 6G band access control based on client data rate.
  - **6GHz Minimum Client Data Rate -** 6G band client with lower data speed will not be given access.
  - **Notes:**
    - Disabling lower bands has an impact on the coverage area.
    - Depending on the environment, we recommend 12 Mbps or 24 Mbps setting for minimum client data rates.
    - Higher Mbps value means less coverage; lower value means larger coverage.
- **Minimum MGMT Rate Controls**
  - **2.4GHz Minimum MGMT Rate Controller -** Enables/Disables 2.4G band wireless management frame rate control.
  - **2.4GHz Minimum MGMT Rate -** 2.4G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.
  - **5GHz Minimum MGMT Rate Controller -** Enables/Disables 5G band wireless management frame rate control.
  - **5GHz Minimum MGMT Rate -** 5G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.
  - **6GHz Minimum MGMT Rate Controller -** Enables/Disables 6G band wireless management frame rate control.
  - **6GHz Minimum MGMT Rate -** 6G band wireless management frame transmit rate.
  - **Notes:**
    - Disabling lower bands has an impact on the coverage area.
    - Depending on the environment, we recommend 12 Mbps or 24 Mbps setting for minimum management rates.

        - Higher Mbps value means less coverage; lower value means larger coverage.
    - **High-Throughput Control**
        - **A-MSDU -** Enables/Disables Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.
        - **A-MPDU -** Enables/Disables Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.
    - **Power Save Control**
        - **DTIM Interval -** The Delivery Traffic Indication Message (DTIM) period in beacons. The DTIM interval determines how often the AP should deliver the buffered broadcast and multicast frames to associated clients in the "power save" mode. The default value is 1, which means the client checks for buffered data on the OAW-IAP at every beacon. You can configure a higher DTIM value for power saving (Range = 1 - 255).
    - **802.11 Frame Controls**
        - **Advertise AP Name** - Enables/Disables the advertising of the AP name in the standard 802.11 beacon frame with a vendor-specific tag. When enabled, the AP name is displayed instead of the AP MAC address.

QoS Settings

- **Bandwidth Contract**
    - **Upstream Bandwidth -** The maximum bandwidth for traffic from the switch to the client
    - **Downstream Bandwidth -** The maximum bandwidth for traffic from the client to the switch.
    - **Upstream Burst -** The maximum bucket size used for traffic from the switch to the client. The bucket size determines how much the traffic can burst over the maximum bandwidth rate
    - **Downstream Burst -**The maximum bucket size used for traffic from the client to the switch. The bucket size determines how much the traffic can burst over the maximum bandwidth rate.
- **Broadcast/Multicast Optimization**
    - **Broadcast Key Rotation -** Enables/Disables the broadcast key rotation function. If enabled, the broadcast key will be rotated after every interval time.
    - **Broadcast Key Rotation Time Interval -** The interval, in minutes, to rotate the broadcast key (Range = 1 - 1440, Default = 15).
    - **Broadcast Filter All -** Enables/Disables broadcast filtering. If enabled, all broadcast frames are dropped, except DHCP and Address Resolution Protocol (ARP) frames.
    - **Broadcast Filter ARP -** Enables/Disables broadcast filtering for ARP. If enabled, the AP will act as an "ARP Proxy". If the ARP-request packet requests a client's MAC address and the AP knows the client's MAC and IP address, the AP will respond to the ARP-request but not forward the ARP-

request (broadcast) to all broadcast domains. This reduces ARP broadcast packet forwarding and significantly improves network performance. Note that APs do not act as ARP proxy for Gratuitous ARP packets. When the station gets an IP from DHCP or IP release/ renew, the station will send Gratuitous ARP packets. AP will not respond to such special ARP packets and broadcast them normally.

- **Multicast Optimization -** Enable/Disables multicast traffic rate optimization.
- **Multicast Based Channel Utilization -** Configures based channel utilization optimization percentage. (Range = 0 - 100, Default = 90)
- **Number of Clients -** Configure the threshold for multicast optimization. This is the maximum number of high-throughput.

- **802.1p Mapping** - Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and 802.1p priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add icon. To remove a value, click on the "x" next to the value.
  - **Background -** WMM Background will be mapped to the 802.1p value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 1)
    - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 1, 2)
  - **Best Effort -** WMM Best Effort will be mapped to the 802.1p value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 0)
    - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 0, 3)
  - **Video -** WMM Video will be mapped to the 802.1p value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 4)
    - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 4, 5)
  - **Voice -** WMM Voice will be mapped to the 802.1p value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 6)
    - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 6, 7)
- **DSCP Mapping** - Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and DSCP priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add icon. To remove a value, click on the "x" next to the value.

- **Trust Original DSCP -** If enabled, the original DSCP mapping for uplink traffic is trusted (Default = Disabled).
- **Background -** WMM Background will be mapped to the DSCP value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 10)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 2, 10)
- **Best Effort -** WMM Best Effort will be mapped to the DSCP value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 0)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 0, 18)
- **Video -** WMM Video will be mapped to the DSCP value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 40)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 24, 36, 40)
- **Voice -** WMM Voice will be mapped to the DSCP value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 46)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 46, 48, 56)

Editing an SSID

Select an SSID by clicking on the checkbox in the upper-left corner of the SSID column, then click on the Edit icon. The Customize SSID Screen appears. Edit the configuration as described above and click on the **Save and Apply to AP Group** button. The new configuration will be saved and applied to the AP Groups on which the SSID was previously applied.

If you edit an SSID that was created in a previous release of OmniVista Cirrus, there is an extra step in the edit process. When you click on the Edit icon, the Upgrade SSID Screen appears. Depending on the type of Security Level configured for the WLAN Service (Personal/Open), only certain Usages will be available for editing. Select a Usage and Captive Portal/BYOD configuration and click on the **Upgrade & Customize** button. The Customize SSID Screen appears. Edit the configuration as described above and click on the **Save and Apply to AP Group** button to apply the edited SSID to AP Groups.

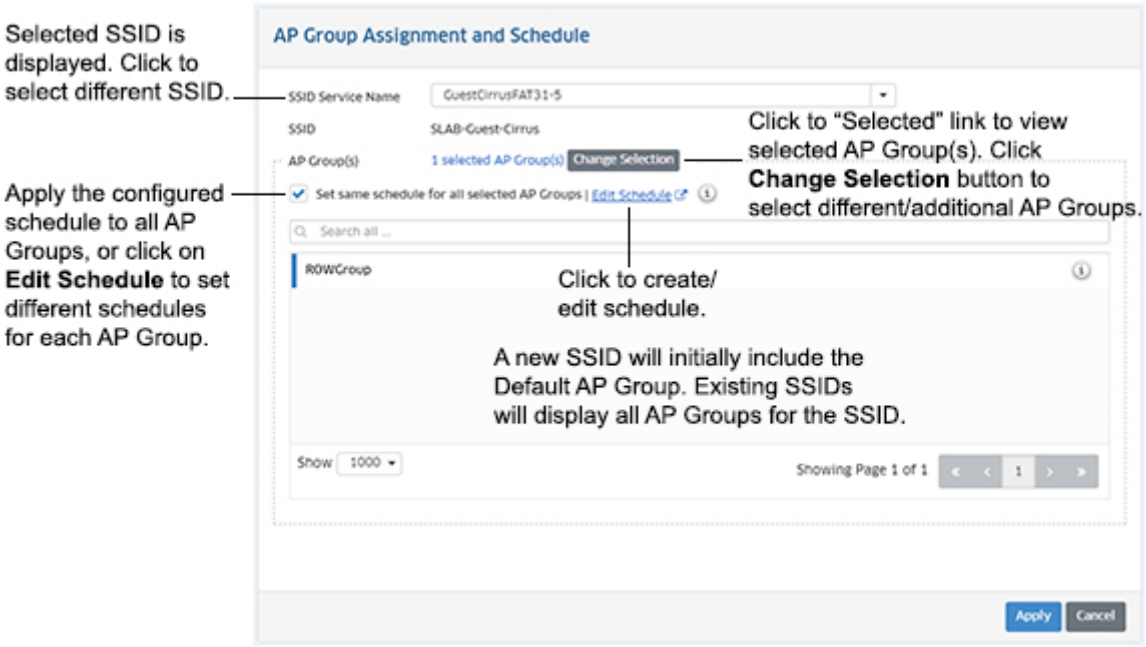
Note: You can only edit one SSID at a time. You cannot edit the SSID Name.

Deleting an SSID

Select an SSID(s) by clicking on the checkbox in the upper-left corner of the SSID column, click on the Delete icon, then click **OK** at the Confirmation Prompt. Note that when you delete an SSID you delete the relevant related configurations created for the SSID (e.g., Access Role Profile, Access Policy, Authentication Strategy), unless those configurations are in use outside of this SSID.

Applying an SSID

The AP Group Assignment and Schedule Screen is used to apply SSIDs to AP Groups. You can also set an availability schedule for APs in a group. Select AP Groups as described below, set a schedule, and click on the **Apply** button.



Note: If you have just created an SSID, the SSID Name is displayed in the **SSIDs** field (as shown above). If you clicked on the **AP Group Assignment and Schedule** button to modify an existing SSID's AP Group assignment or AP Schedule, select an SSID from the **SSID's** drop-down menu.

Note: The maximum number of SSIDs per band that an AP can support is based on the AP model and whether the Extended SSID Scale option is enabled for the AP Group to which the AP belongs.

- **Extended SSID Scale option is disabled (the default)** - AP allows a maximum of 7 SSIDs per band. This means up to 7 SSIDs with Allowed Band = 2.4GHz, up to 7 SSIDs with Allowed Band = 5GHz, and up to 7 SSIDs with Allowed Band = 6GHz. Alternatively, you can have up to 7 SSIDs with Allowed Band = All. If you apply an SSID to an AP Group and it causes a breach of this maximum limit, the "Apply" operation will fail on that AP Group.
- **Extedned SSID Scale option is enabled** - AP models that support more than 7 SSIDs per band will allow a maximum of 14 SSIDs per band. This means up to 14 SSIDs with Allowed Band = 2.4GHz, up to 14 SSIDs with Allowed Band = 5GHz, and up to 14 SSIDs with Allowed Band = 6GHz. Alternatively, you can have up to 14 SSIDs with Allowed Band = All. If you apply an SSID to an AP Group and it causes a breach of this maximum limit, the "Apply" operation will fail on that AP Group.

Applying an SSID to AP Groups

If you are creating a new SSID, the Default AP Group is pre-selected by default and is displayed in the AP Group area. Click on the **Change Selection** button to add/remove AP Groups.

Note: You do not have to apply the SSID to an AP Group when you create it. Click on the **Cancel** button to create the SSID without any AP Group assignment. You can apply AP Groups to the SSID at any time by selecting the SSID in the SSIDs Table and clicking on the **AP Group Assignment and Schedule** button.

If you are editing an SSID, all of the AP Groups to which the SSID was applied are displayed as pre-selected. Click on the **Change Selection** button to bring up the AP Group Selection window to add/remove AP Groups.

Scheduling AP Availability

By default, the schedule you set is applied to all selected AP Groups, however set different schedules for each selected AP Group, as described below:

- **Set the Same Schedule For All Selected Groups -** By default, **the Set same schedule for all selected AP Groups** checkbox is enabled. If selected, the schedule you configure is applied to all selected AP Groups. Click on the **Edit Schedule** button to bring up the Timer Dialog window and set the schedule. By default, the "Always Available" radio button is selected. Select the "Specific Timer" radio button to set a specific schedule for all selected AP Groups. You can set the start and stop (From/To) availability hours for all days of the week or for specific days of the week. Set the schedule and click **OK**.
- **Set a Different Schedule for Selected AP Groups -** To set a different schedule for selected AP Groups, uncheck the **Set same schedule for all selected AP Groups** checkbox. Click on the **Edit Schedule** link next to an AP Group in List of Selected AP Groups to bring up the Timer Dialog window and set the schedule for the group. By default, the "Always Available" rad button is selected. Select the "Specific Timer" radio button to set a specific schedule for all selected AP Groups. You can set the start and stop (From/To) availability hours for all days of the week or for specific days of the week. Set the schedule and click **OK**. Repeat the process for each AP Group.

Editing an SSID AP Group/Schedule

To edit an SSID's AP Group assignment or AP Schedule, select the SSID and click on the **AP Group Assignment and Schedule** button at the top of the SSIDs Screen. The AP Group Assignment and Schedule Screen appears with the selected SSID displayed in the **SSIDs** field. Edit the AP Groups and/or AP Schedule as described above and click on the **Apply** button.

Note that you can also just click on the **AP Group Assignment and Schedule** button and select the SSID you want to modify from the **SSIDs** drop-down menu.

Enabling/Disabling an SSID

Click on the checkbox next to an SSID(s) and select the **Enable** or **Disable** button to enable/disable an SSID. When you disable an SSID, the SSID stops broadcasting; the configuration remains on the AP. When you enable an SSID, it begins broadcasting again.

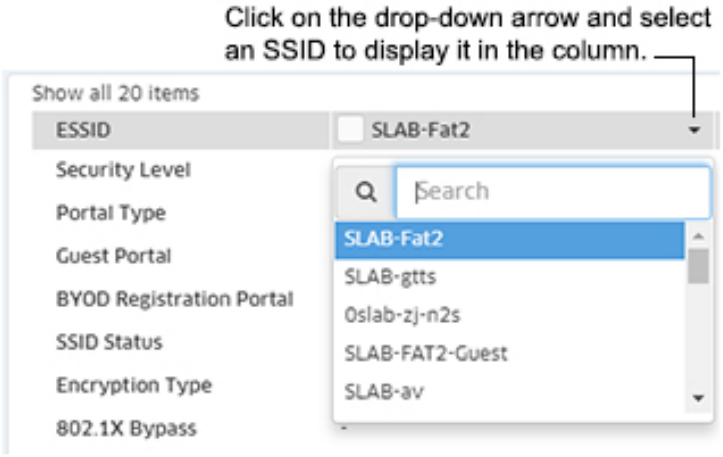
SSIDs Table

The SSIDs Screen displays information about all configured SSIDs. If a specific parameter has not been configured for an SSID, the field is blank. The screen displays up to 15 SSIDs at time. Scroll to view configured SSIDs. You can also customize the display order of the SSIDs on the

screen. The screen can also be used to quickly edit relevant related SSID configurations (e.g., Access Role Profile, Access Policy, Authentication Strategy).

Customizing the Display

You can customize the order in which SSIDs are displayed on the screen, prioritizing them so that specific SSIDs are shown in the first columns. Click on the drop-down arrow at the top of a column to display a list of all configured SSIDs and select an SSID. The selected SSID will be displayed in that column.



The SSID that was previously displayed will not be "moved" to another location. To re-display that SSID, go to another column and repeat the procedure to re-display that SSID in that column.

If you have fewer than 15 SSIDs configured and create a new SSID, the new SSID will be displayed in the last column. However, if you have reached the maximum display of 15 SSIDs and create a new SSID, the SSID will not replace an existing SSID in the display. To display the SSID you must click on the drop-down at the top of one of the columns and select the new SSID.

Editing an SSID's Related Configurations

You can quickly edit relevant related SSID configurations (e.g., Access Role Profile, Access Policy, Authentication Strategy) from the SSIDs Screen. The names of these configurations are displayed as a hyperlink. Click on the link to open a configuration window. The configuration will be pre-selected with the Detailed Configuration information displayed. Click on the Edit icon on the window to edit the configuration. Click on the **Apply** button to apply the update, then click on the **Close** button to close the window and return to the SSIDs Screen.

> **Note:** If you edit the Access Role Profile for an SSID, you must re-apply the profile to the SSID. After editing the Access Role Profile, select the SSID on the SSIDs Screen, and click on the **AP Group Assignment and Schedule** button. The AP Group Assignment and Schedule Screen appears. Click on the **Apply** button to apply the new configuration.
>
> **Note:** When an SSID is created with a RADIUS Server, the auto-generated AAA Server Profile for the SSID assigns the RADIUS Server for Captive Portal and MAC authentication. If TLS was disabled for the RADIUS Server configured for the SSID, enabling TLS for the server will fail because a TLS-enabled RADIUS Server does not support Captive Portal and MAC authentication in the AAA Server Profile.

WLAN Service (Expert)

The Unified Profile WLAN Service (Expert) Screen displays all configured WLAN Service Profiles and is used to create, clone, edit, and delete WLAN Services and assign the service to devices on the network.

Creating a WLAN Service Profile

Click on the Add icon. Enter a **Service Name** and configure the profile as described below, then click on the **Create** button. When you are finished, select the checkbox next to the profile and click on the **Apply to Devices** button to assign the profile to wireless devices on the network.

SSID Settings

Basic

- **SSID -** User configured name that uniquely identifies a wireless network (up to 32 characters).
- **Hide SSID -** Enables/Disables SSID in beacon frames. Note that hiding the SSID does very little to increase security. (Default = Disabled)
- **UAPSD -** Enables/Disables Unscheduled Automatic Power Save Delivery (UAPSD) on the SSID. UAPSD is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow that is delivered over the wireless media. Because UAPSD does not require the client to poll each individual packet that is buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. (Default = Enabled)
- **Enable SSID -** Enables/Disables the SSID.
- **Allowed Band -** The band(s) available on the service:
    - 2.4 GHz
    - 5.0 GHz
    - 6.0 GHz
    - All - 6.0 GHz, 5.0 GHz and 2.4 GHz.

Security

- **Security Level -** Select the security level for the WLAN Service:
    - **Open -** The Wi-Fi will be unsecured. However, you can configure a default role or enable MAC Authentication to assign a role for clients (Default).
    - **Enhanced Open** - Enables/Disables the use of Wi-Fi Enhanced Open™ to secure an open SSID. Wi-Fi Enhanced Open™ is a security standard that is based on Opportunistic Wireless Encryption (OWE). When enabled, OWE is used to ensure that communication between each pair of endpoints is protected from other endpoints. Data sent between a client and an AP is provided individualized data protection. Wi-Fi Enhanced Open™ offers improved data privacy, while maintaining convenience and

ease-of-use. This functionality is particularly useful for provisioning a secure open SSID in public spaces. Configuring the enabled/disabled status of this attribute is based on the following:

- If 2.4 GHz and/or 5.0 GHz is the allowed band (not 6.0 GHz), you can enable or disable Enhanced Open status
- If 6.0 GHz is the allowed band, then Enhanced Open is automatically enabled, whether or not 2.4 GHz or 5.0 GHz is selected. You cannot disable the Enhanced Open status.

- **Enterprise -** An authentication server will be used to authenticate the connecting client via 802.1x Authentication. Select an **Encryption Type** from the drop-down menu:
  - DYNAMIC_WEP - WEP with dynamic keys.
  - WPA_TKIP - WPA with TKIP encryption and dynamic keys using 802.1X.
  - WPA_AES - WPA with AES encryption and dynamic keys using 802.1X.
  - WPA2_TKIP - WPA2 with TKIP encryption and dynamic keys using 802.1X.
  - WPA2_AES - WPA2 with AES encryption and dynamic keys using 802.1X.
  - WPA3_AES256 - WPA3 with CNSA (Suite B) using 802.1X. Note that when WPA3_AES256 encryption is applied to an AP that does not support it, the encryption will automatically fall back to WPA2_AES. OAW-AP1101 full band, OAW-AP1201H 2.4G band, and OAW-AP1201L 2.4G band do not support WPA3_AES256 authentication.
  - WPA3_AES - WPA3 with AES encryption and dynamic keys using 802.1X. Note that Stellar AP Models AP1101, AP1201H, and AP1201L do not support WPA3 authentication.
- **Personal -** The Wi-Fi will be protected by a key. Select an **Encryption Type** from the drop-down menu, then enter a **Passphrase**.
  - STATIC_WEP - Authentication with Static Wired Equivalent Privacy security algorithm.
  - WPA_PSK_TKIP - WPA with TKIP encryption using a preshared key.
  - WPA_PSK_AES - WPA with AES encryption using a preshared key.
  - WPA_PSK_AES_TKIP - WPA with TKIP and AES mixed encryption using a preshared key.
  - WPA2_PSK_TKIP - WPA2 with TKIP encryption using a preshared key.
  - AUTO_WPA_WPA2- WPA or WPA2 mixed mode, which allows both WPA capable client and WPA2 capable client access.
  - WPA2_PSK_AES - WPA2 with AES encryption using a preshared key.
  - WPA3_SAE_AES - WPA3 with AES encryption using a preshared key, which ONLY allow WPA3 capable client accessing.

        - WPA3_PSK_SAE_AES - WPA3 and WPA2 mixed mode, which allow both WPA3 capable client as well as ONLY WPA2 capable client accessing.

- **MAC Auth -** Enables/Disables MAC Authentication.
- **Device Specific PSK -** Enables/Disables Device Specific PSK. Device Specific PSK provides more security than traditional PSK. If Device Specific PSK is enabled and a device is configured for Device Specific PSK, when the AAA Server sends the Radius Access Accept for MAC Authentication for the device, it will also send the specific pre-shared key for that device, differentiated by the device's MAC Address. This means that each device will have a different key. This option is available when the Security Level is set to "Personal" with a "PSK" Encryption Type. If enabled:
    - **Prefer Device Specific PSK -** If the AAA Server sends the "AES-CBC-128" attribute along with the Radius Access Accept response, this value will be used. If the AAA server does NOT send the "AES-CBC-128" attribute, the key configured in the SSID will be used.
    - **Force Device Specific PSK -** The value of "AES-CBC-128" attribute returned by AAA Server will be always used, whether it exists or not.

    Note: Device Specific PSK will only work with a UPAM RADIUS Server. Devices are configured for Device Specific PSK on the Company Property Screen (UPAM - Authentication - Company Property). See the Company Property online help for more information. You can also configure a device for Device Specific PSK from the Authentication Record List (UPAM - Authentication - Authentication Record). See the Authentication Record online help for more information.
- **Private Group PSK** - Enables/Disables the grouping of Device Specific PSKs. When a PSK-enabled SSID is created, you can either create a static PSK or enforce Device Specific PSK. This provides a common Passphrase key, which is suitable for networks requiring network-wide common PSK. Enabling Private Group PSK (PPSK) allows you to create private groups of client devices based on a PPSK Entry. Each client device specifies a Passphrase when connecting to an SSID. If the passphrase matches any of the PPSK Entry, the client is placed in the specified Access Role Profile. Configuring the Private Group PSK attribute is offered only when Device Specific PSK is Disabled or set to "Prefer Device Specific PSK". When the Device Specific PSK is set to "Force Device Specific PSK", OmniVista will not display the Private Group PSK attribute because the Passphrase specified in Company Property is used instead. If Private Group PSK is enabled, complete the following fields to configure a PPSK Entry:
    - **PPSK Entries** - At least one PPSK Entry is required with the following parameters defined. Note that each SSID can have up to 16 PPSK Entries. The total number of entries across all SSIDs that exist on an AP cannot exceed 64 on any AP.
        - **Name** - Enter a unique name to identify the PPSK Entry. No two Entries can have the same Name.
        - **Passphrase** - Enter a unique PSK Passphrase for authentication. No two Entries can have the same Passphrase.
        - **Access Role Profile** - Select the name of an Access Role Profile.

- **AAA Profile -** Select an AAA Profile to use for authentication. An AAA profile is required if the Security Level is set to "Enterprise" (to perform 802.1x authentication) or if MAC Authentication is enabled. This AAA Profile will be also used for Accounting purposes.
- **Classification Status -** Enables/Disabled classification. If classification is enabled, traffic will be classified to a role based on the configured classification rules. Note that the precedence of role assignment methods is important. Classification Rules are only used if 802.1x/MAC authentication does not return a role, or the returned role is not matched with any configured roles in the device.
- **MAC Pass Auth -** If MAC Authentication is enabled, select an Access Role Profile to assign to clients that pass MAC Authentication.
- **Default Access Role Profile -** Select the default Access Role Profile that will be applied to clients if a role cannot be assigned by other role assignment methods.
- **Client Isolation -** Enables/Disables Client Isolation. If enabled, traffic between clients on the same AP in the SSID is blocked; client traffic can only go toward the router. (Default = Disabled)
- **Protected Management Frame -** Configures whether connections are accepted from clients supporting Protected Management Frame for certain Security Levels/Encryption Types (Enterprise - WPA2_AES/WPA3_AES256/ WPA3AES, Personal - WPA2_PSK_AES/WPA3_SAE_AES/WPA3_PSK_SAE_AES)
    - **Disabled -** Disables Protected Management Frame requirements.
    - **Optional -** Allows connections from clients supporting Protected Management Frame and clients that do not.
    - **Required -** Only allows connections from clients supporting Protected Management Frame.

Hotspot 2.0

- **Hotspot 2.0 -** Enables/Disables Hotspot 2.0. Hotspot 2.0 is a new standard for public-access Wi-Fi that enables seamless roaming among Wi-Fi networks and between Wi-Fi and cellular networks. Hotspot 2.0 was developed by the Wi-Fi Alliance and the Wireless Broadband Association to enable seamless hand-off of traffic without requiring additional user sign-on and authentication. Note that Hotspot 2.0 is only supported with Enterprise WPA2_AES or Enterprise WPA3_AES256 Encryption. You must first select one of these Encryption types before you can enable Hotspot 2.0.
- **Operator Name -** The operator providing the Hotspot service (0 - 252 characters).
- **Venue Name -** The venue where the Hotspot is hosted (0 - 252 characters).
- **Venue Type -** The type of venue hosting the Hotspot.
- **Network Detail -** The type of Hotspot network.
- **Domain List -** The list of Hotspot Domains. You can have up to 16 Domain Names (1 - 255 characters each).
- **Roaming OIs** - The Roaming Organization Identifier. You can have up to 16 OIs. Each OI field is 3 octets in length if the organizationally unique identifier is an OUI, or 5 octets in length if the organizationally unique identifier is an OUI-36.

Advanced

Roaming Controls

- **L3 Roaming -** Enables/Disables Layer 3 roaming. Layer 3 roaming allows client to move between Access Points and connect to a new IP subnet and VLAN.
- **FBD Update on Association -** Enables/Disables FDB update on Association. If enabled, when a client roams to a new AP, the AP will send ARP packets to the uplink switch to notify the switch to change the downstream forwarding port for the wireless client's traffic.
- **802.11r -** Enables/Disables IEEE 802.11r (Fast BSS Transition). The Fast BSS Transition mechanism minimizes the delay when a a client transitions from one BSS to another within the same group.
- **OKC -** Enables/Disables OKC Roaming. If OKC Roaming is enabled, a cached Pairwise Primary Key is used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1x authentication.
- **802.11k Status -** Enables/Disables 802.11k. The 802.11k protocol enables APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other.
- **802.11v Status -** Enables/Disables 802.11v. 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an Instant AP to request a voice client to transition to a specific AP, or suggest a set of preferred APs to a client due to network load balancing or BSS termination. It also helps the client identify the best AP to transition to as they roam.

Client Controls

- **Max Number of Clients Per Band** - The maximum number of clients allowed in each band. (Range = 1 - 256, Default = 64)
- **802.11b Support -** Enables/Disables allowing 11b legacy clients to connect to Stellar APs.
- **802.11a/g Support -** Enables/Disables allowing 11a/g legacy clients to connect to Stellar APs.

Minimum Client Data Rate Controls

- **2.4GHz Minimum Client Data Rate Controller -** Enables/Disables 2.4G band access control based on client data rate.
- **2.4GHz Minimum Client Data Rate -** 2.4G band client with lower data speed will not be given access, recommended value 12.
- **5GHz Minimum Client Data Rate Controller -** Enables/Disables 5G band access control based on client data rate.
- **5GHz Minimum Client Data Rate -** 5G band client with lower data speed will not be given access, recommended value 24.

- **6GHz Minimum Client Data Rate Controller -** Enables/Disables 6G band access control based on client data rate.
- **6GHz Minimum Client Data Rate -** 6G band client with lower data speed will not be given access.
- **Notes:**
    - Disabling lower bands has an impact on the coverage area.
    - Depending on the environment, we recommend 12 Mbps or 24 Mbps setting for minimum client data rates.
    - Higher Mbps value means less coverage; lower value means larger coverage.

Minimum MGMT Rate Controls

- **2.4GHz Minimum MGMT Rate Controller -** Enables/Disables 2.4G band wireless management frame rate control.
- **2.4GHz Minimum MGMT Rate -** 2.4G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.
- **5GHz Minimum MGMT Rate Controller -** Enables/Disables 5G band wireless management frame rate control.
- **5GHz Minimum MGMT Rate -** 5G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.
- **6GHz Minimum MGMT Rate Controller -** Enables/Disables 6G band wireless management frame rate control.
- **6GHz Minimum MGMT Rate -** 6G band wireless management frame transmit rate.
- **Notes:**
    - Disabling lower bands has an impact on the coverage area.
    - Depending on the environment, we recommend 12 Mbps or 24 Mbps setting for minimum management rates.
    - Higher Mbps value means less coverage; lower value means larger coverage.

High-Throughput Control

- **A-MSDU -** Enables/Disables Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.
- **A-MPDU -** Enables/Disables Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

Power Save Controls

- **DTIM Interval -** The Delivery Traffic Indication Message (DTIM) period in beacons. The DTIM interval determines how often the AP should deliver the buffered broadcast and multicast frames to associated clients in the "power save" mode. The default value is 1, which means the client checks for buffered data on the OAW-IAP at every beacon. You can configure a higher DTIM value for power saving (Range = 1 - 255).

802.11 Frame Controls

- Advertise AP Name - Enables/Disables the advertising of the AP name in the standard 802.11 beacon frame with a vendor-specific tag. When enabled, the AP name is displayed instead of the AP MAC address.

QoS Settings

Configure the wireless QoS Settings for the profile as detailed below.

Bandwidth Contract

- **Upstream Bandwidth -** The maximum bandwidth for traffic from the switch to the client
- **Downstream Bandwidth -** The maximum bandwidth for traffic from the client to the switch.
- **Upstream Burst -** The maximum bucket size used for traffic from the switch to the client. The bucket size determines how much the traffic can burst over the maximum bandwidth rate
- **Downstream Burst -**The maximum bucket size used for traffic from the client to the switch. The bucket size determines how much the traffic can burst over the maximum bandwidth rate

Broadcast/Multicast Optimization

- **Broadcast Key Rotation -** Enables/Disables the broadcast key rotation function. If enabled, the broadcast key will be rotated after every interval time.
- **Broadcast Key Rotation Time Interval -** The interval, in minutes, to rotate the broadcast key (Range = 1 - 1440, Default = 15).
- **Broadcast Filter All -** This attribute is applicable to Stellar APs only. If enabled, all broadcast frames are dropped, except DHCP and Address Resolution Protocol (ARP) frames.
- **Broadcast Filter ARP -** This attribute is applicable to Stellar APs only. If enabled, the AP will act as an "ARP Proxy". If the ARP-request packet requests a client's MAC address and the AP knows the client's MAC and IP address, the AP will respond to the ARP-request but not forward the ARP-request (broadcast) to all broadcast domains. This reduces ARP broadcast packet forwarding and significantly improves network performance. Note that Stellar APs do not act as ARP proxy for Gratuitous ARP packets. When the station gets an IP from DHCP or IP release/ renew, the station will send Gratuitous ARP packets. AP will not respond to such special ARP packets and broadcast them normally.
- **Multicast Optimization -** Enable/Disables multicast traffic rate optimization.
- **Multicast Based Channel Utilization -** Configures based channel utilization optimization percentage. (Range = 0 - 100, Default = 90)
- **Number Of Clients -** Configure the threshold for multicast optimization. This is the maximum number of high-throughput stations.

802.1p Mapping

Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and 802.1p priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add icon . To remove a value, click on the "x" next to the value.

- **Background -** WMM Background will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 1)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 1, 2)
- **Best Effort -** WMM Best Effort will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 0)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 0, 3)
- **Video -** WMM Video will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 4)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 4, 5)
- **Voice -** WMM Voice will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 6)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 7, Default = 6, 7)

DSCP Mapping

Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and DSCP priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add icon . To remove a value, click on the "x" next to the value.

- **Trust Original DSCP -** If enabled, the original DSCP mapping for uplink traffic is trusted (Default = Disabled).
- **Background -** WMM Background will be mapped to the DSCP value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 10)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 2, 10)
- **Best Effort -** WMM Best Effort will be mapped to the DSCP value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 0)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 0, 18)

- **Video -** WMM Video will be mapped to the DSCP value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 40)
    - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 24, 36, 40)
- **Voice -** WMM Voice will be mapped to the DSCP value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 63, Default = 46)
    - **Downlink -** Maps downlink traffic (from network to AP). (Range = 0 - 63, Default = 46, 48, 56)

Legacy Wireless Settings

- **802.1x Authentication Profile -** The 802.1x Authentication Profile to use for legacy wireless devices.
- **MAC Authentication Profile -** The MAC Authentication Profile to use for legacy wireless devices.
- **802.1x Pass Alt -** The user shall be assigned a Pass-Alternate UNP in case the 802.1X authentication does not result in a valid UNP for the pass branch. Select a profile from the drop-down list or click on the "Add New" link to go to the Access Role Profile Screen and create a new profile.
- **User Derivation Rules -** Select a User Derivation Rule from the drop-down list to specify a user attribute profile from which the user role or VLAN is derived. The user role can be derived from user attributes upon the client's association with an AP (this is known as a user-derived role). You can configure rules that assign a user role to clients that match a certain set of criteria. For example, you can configure a rule to assign the role VoIP-Phone to any client that has a MAC address that starts with bytes xx:yy:zz. User-derivation rules are executed before client authentication. Note that only wireless classification rules are listed in the drop-down menu.
- **Virtual AP Enable -** Enables/Disables the Wireless Authentication Profile.
- **Forward Mode -** Controls whether data is tunneled to the controller using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or using a combination of both depending on the destination (e.g., corporate traffic goes to the controller, and Internet access remains local). All forwarding modes support band steering, TSPEC/TCLAS enforcement, 802.11k and station blocklisting.
    - **Tunnel -** The AP handles all 802.11 association requests and responses, but sends all 802.11 data packets, action frames, and EAPOL frames over a GRE tunnel to the controller for processing. The controller removes or adds the GRE headers, decrypts or encrypts 802.11 frames, and applies firewall rules to the user traffic as usual. Both remote and campus APs can be configured in tunnel mode.
    - **Bridge -** 802.11 frames are bridged into the local Ethernet LAN. When a remote AP or campus AP is in bridge mode, the AP (and not the controller) handles all 802.11 association requests and responses, encryption/decryption processes, and firewall enforcement. The 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed.

  - **Split Tunnel -** 802.11 frames are either tunneled or bridged, depending on the destination (e.g., corporate traffic goes to the controller, and Internet access remains local).
  - **Decrypt Tunnel -** Both remote and campus APs can be configured in decrypt-tunnel mode. When an AP uses decrypt-tunnel forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the controller, which then applies firewall policies to the user traffic.

- **Dynamic Multicast Optimization Threshold -** The maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops. (Range = 2 - 255, Default = 5)
- **Band Steering -** Enables/Disables Band Steering. Band Steering encourages dual-band capable clients to stay on the 5GHz band on dual-band APs. This frees up resources on the 2.4GHz band for single band clients like VoIP phones. The feature supports both campus APs and remote APs that have a virtual AP profile set to tunnel, split-tunnel or bridge forwarding mode. Note, however, that if a campus or remote APs have virtual AP profiles configured in bridge or split-tunnel forwarding mode but no virtual APs in tunnel mode, those APs will gather information about 5G-capable clients independently and will not exchange this information with other APs that only have bridge or split-tunnel virtual APs configured.
- **Steering Mode -** Band steering supports the following three band steering modes.
  - **Force-5GHz -** The AP will try to force 5Ghz-capable APs to use that radio band.
  - **Prefer-5GHz -**The AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts. (Default)
  - **Band Balancing -** The AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5Ghz band has more channels than the 2.4 GHz band, and that the 5Ghz channels operate in 40MHz while the 2.5Ghz band operates in 20MHz.

Cloning a WLAN Service Profile

You can quickly create an WLAN Service Profile by selecting a profile in the WLAN Service Profile List, clicking on the **Clone** button and modifying the profile to create a new one. Click on the **Copy** button to create the new profile.

Assigning a WLAN Service Profile

When you click the **Apply to Devices** button, the WLAN Service Assignments Screen appears. Click on the Devices **ADD** button and/or the AP Group **ADD** button to select devices. The device(s) will appear in the List of Selected Devices. If necessary, click on the Devices **EDIT** button and/or the AP Group **EDIT** button to add/remove devices from the list. When you are finished, click on the **Apply** button.

> **Note:** The maximum number of SSIDs per band that an AP can support is based on the AP model and whether the Extended SSID Scale option is enabled for the AP Group to which the AP belongs.

- **Extended SSID Scale option is disabled (the default)** - AP allows a maximum of 7 SSIDs per band. This means up to 7 SSIDs with Allowed Band = 2.4GHz, up to 7 SSIDs with Allowed Band = 5GHz, and up to 7 SSIDs with Allowed Band = 6GHz. Alternatively, you can have up to 7 SSIDs with Allowed Band = All. If you apply an SSID to an AP Group and it causes a breach of this maximum limit, the "Apply" operation will fail on that AP Group.
- **Extedned SSID Scale option is enabled** - AP models that support more than 7 SSIDs per band will allow a maximum of 14 SSIDs per band. This means up to 14 SSIDs with Allowed Band = 2.4GHz, up to 14 SSIDs with Allowed Band = 5GHz, and up to 14 SSIDs with Allowed Band = 6GHz. Alternatively, you can have up to 14 SSIDs with Allowed Band = All. If you apply an SSID to an AP Group and it causes a breach of this maximum limit, the "Apply" operation will fail on that AP Group.

Editing a WLAN Service Profile

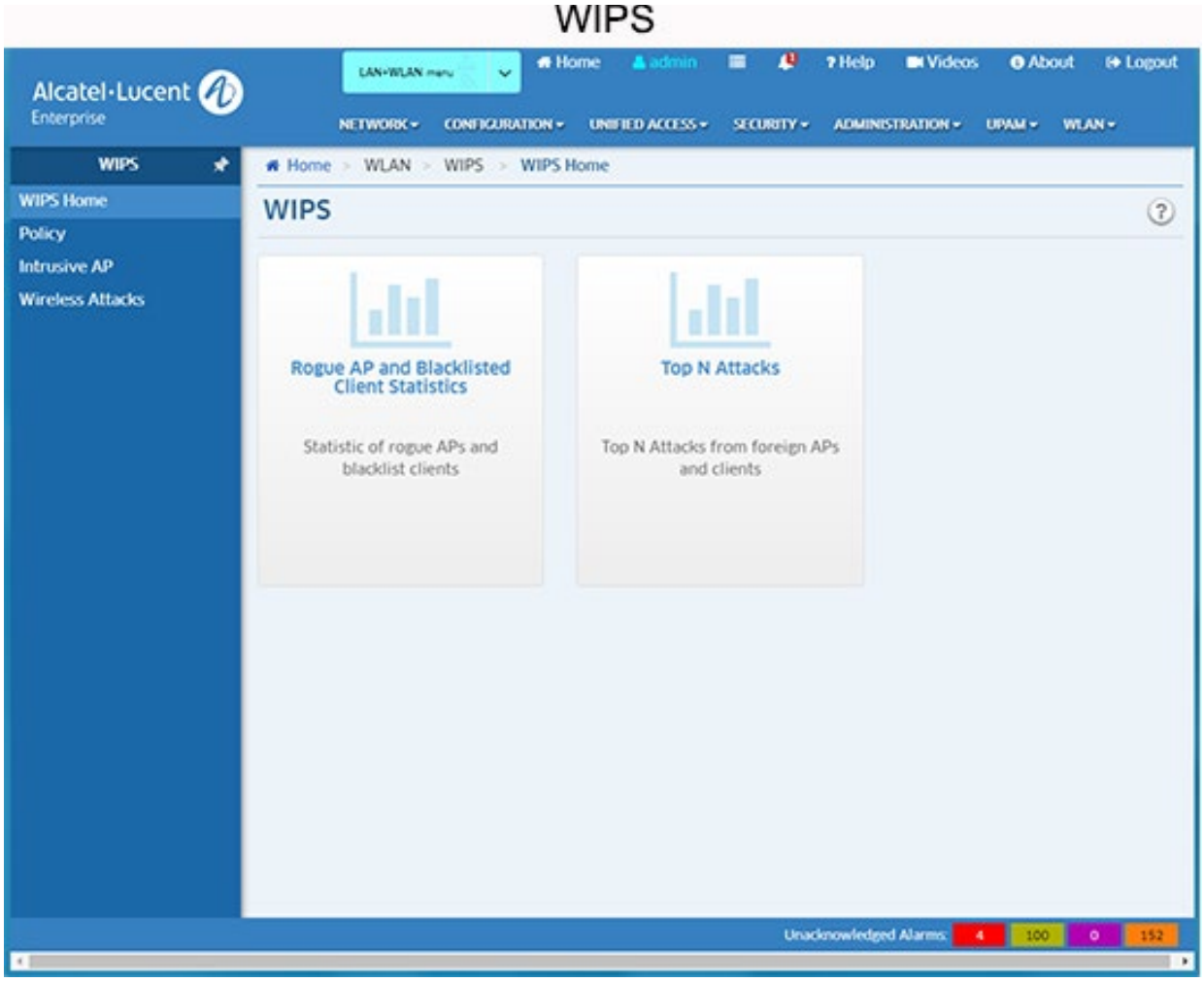
Select the profile in the WLAN Service Profile Screen and click on the Edit icon to bring up the Edit WLAN Service Profile Screen. Edit the fields as described above then click on the **Apply** button to save the changes to the server.

Deleting a WLAN Service Profile

Select the profile in the WLAN Service Profile Screen, click on the Delete icon, then click **OK** at the confirmation prompt. This removes the profile from the server.

WIPS

An 802.11 network is open and borderless, making it vulnerable to attack (e.g., rogue APs, unauthorized clients, DoS attacks). The Wireless Intrusion Protection System (WIPS) application monitors the wireless radio spectrum for the presence of unsafe access points and clients, and can take countermeasures to mitigate the impact of foreign intrusions. WIPS provides an overview of wireless network threats/intrusions for Stellar APs, and enables users to set up policies to detect threats and take countermeasures.



Network Overview

The WIPS Home Page provides links to an overview of network threats and intrusions for Stellar APs, including Rogue APs and Blacklisted Clients, as well as network attacks over a 24 hour or one-week period.

Rogue APs and Blacklist Clients

Click on the Rogue APs and Blacklist Clients widget on the Home Page and select **Rogue Client Association** for an overview of detected Rogue APs and Clients. Click on **Blacklist Clients** to for an overview of clients that have been automatically and manually added to the Blacklist.

Top N Attacks

Click on the Top N Attacks widget to view a list of attacks from foreign APs and Clients, Click on the Settings icon to configure the number of attacks to display (Top 5, 10, 20), as well as the monitoring period (24 Hours, 1 Week).

WIPS Views and Policies

In addition to the overview provided on the WIPS Home Page, you can view detailed information on intrusive APs and wireless attacks, and create policies to detect and react to the attacks. Detailed views and policies are configured using the links on the left side of the WIPS Home Page:

- **Policy -** Define rules for classifying rogue AP/wireless attacks, and specify the measures that will be taken to react to the threats.
- **Intrusive AP -** Display detailed information about interfering APs and rogue APs, as well as clients connecting to the intrusive AP.
- **Wireless Attacks -** Display detailed wireless attack information.

Policy

The WIPS Policy Screen is used to configure policies for rogue AP and wireless attacks on the network. You can configure one overall policy for the Stellar wireless network. When an attack is detected based on the policy, the detected device is banned from the network and is displayed on the Intrusive AP or Wireless Attacks Screens for review. After creating a policy as described below, click on the **Apply** button to activate the policy for the wireless network.

Creating Rogue AP Policies

A rogue AP is an unauthorized AP connected to the wired side of the network, that is considered a security threat to the wireless network. An interfering AP is an AP seen in the wireless environment but not connected to the wired network, which is not considered a direct security threat. However, some interfering APs may have an impact on network quality and can interfere with valid client access to the network. Complete the fields below to configure rules to classify interfering APs as rogue APs.

Recognition Policy

- **Signal Strength Threshold -** If enabled, an interfering AP with greater RSSI than the setting value will be classified as rogue (Range = 50 - 95 dBm). By default, the RSSI matching rule is disabled.
- **Detect Valid SSID -** If enabled, a foreign AP broadcasting the same SSID with valid Stellar network SSIDs will be classified as rogue. By default, the Detected Valid SSID rule is enabled.
- **Detect Rogue SSID Keyword -** If enabled, an interfering AP broadcasting and SSID that matches the characteristic specified by the user will be classified as rogue. The matching condition can be equal to or contain the configured keyword.
- **Rogue OUI -** If enabled, interfering APs matching this MAC OUI will be classified as rogue.

Friendly AP

- **Friendly MAC -** An AP classified as interfering or rogue can be trusted to be a "Friendly" AP by entering the MAC OIU of the AP - essentially creating a Vendor "Whitelist". These interfering APs will never be classified as rogue.

Note: The default MAC OUIs (34:e7:0b and dc:08:56) are required for Stellar APs. Also note that you can have a **maximum** of 32 Friendly MAC OUIs/MAC addresses, including the two default Stellar AP MAC OUIs

Containment Policy

- **Rogue AP Containment -** If enabled, the rogue AP containment function reduces the impact of the rogue AP on valid clients.

Creating Wireless Attack Policies

A rogue AP is not the only threat to the wireless network, other wireless attacks can be detected and mitigated for both APs and Clients. To create Wireless Attack Policies, you must enable **Wireless Detection**. When configuring a policy, each detection policy can be set to one of the following levels. When a level is selected, all detection policies included in that level are displayed and selected.

- **High -** Enables all applicable detection mechanisms, including all the options of low and medium level settings.
- **Medium -** Enables important detection mechanisms. This includes all the options of the low-level settings.
- **Low (Default) -** Enables only the most critical detection mechanisms.
- **Custom -** Enables only the selected detection mechanisms. When this level is selected, all detection mechanisms are displayed. Select the ones you want to include in the policy.

The sections below describe each of the Wireless Attack Policies.

AP Attack Detection Policy

An AP Attack Detection Policy detects multiple attacks originating from foreign APs. The following detection methods are available depending on the level selected.

- **Detect AP Spoofing -** An AP Spoofing attack involves an intruder sending forged frames that are made to look like they are from a valid AP.
- **Detect Broadcast De-authentication -** A de-authentication broadcast attempts to disconnect all clients in range. Rather than sending a spoofed de-authentication frame to a specific MAC address, this attack sends the frame to a broadcast address.
- **Detect Broadcast Disassociation -** By sending disassociation frames to the broadcast address (FF:FF:FF:FF:FF:FF), an intruder can disconnect all stations on a network for a widespread DoS.
- **Detect Adhoc Networks using VALID SSID -** If an unauthorized ad hoc network is using the same SSID as an authorized network, a valid client may be tricked into connecting to the wrong network. If a client connects to a malicious ad hoc network, security breaches or attacks can occur.
- **Detect Long SSID -** Detects long SSIDs with more than 32 characters in the name.
- **Detect AP Impersonation -** In AP impersonation attacks, an AP assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for man-in-the-middle attacks, a rogue AP attempting to bypass detection, or a Honeypot attack.

- **Detect Adhoc Networks -** An ad hoc network is a collection of wireless clients that form a network among themselves without the use of an AP. If the ad hoc network does not use encryption, it may expose sensitive data to outside eavesdroppers. If a device is connected to a wired network and has bridging enabled, an ad-hoc network may also function like a rogue AP. Additionally, ad-hoc networks can expose client devices to viruses and other security vulnerabilities.
- **Detect Wireless Bridge -** Wireless bridges are normally used to connect multiple buildings together. However, an intruder could place (or have an authorized person place) a wireless bridge inside the network that would extend the corporate network somewhere outside the building. Wireless bridges are somewhat different from rogue APs in that they do not use beacons and have no concept of association. Most networks do not use bridges. In these networks, the presence of a bridge is a signal that a security problem exists.
- **Detect Null Probe Response -** A null probe response attack has the potential to crash or lock up the firmware of many 802.11 NICs. In this attack, a client probe-request frame will be answered by a probe response containing a null SSID. Many popular NIC cards will lock up upon receiving such a probe response.
- **Detect Invalid Address Combination -** In this attack, an intruder can cause an AP to transmit de-authentication and disassociation frames to its clients. Triggers that can cause this condition include the use of broadcast or multicast MAC address in the source address field.
- **Detect Reason Code Invalid of De-authentication -** De-authentication packets with invalid reason code will be classified as an attack.
- **Detect Reason Code Invalid of Disassociation -** Disassociation packets with invalid reason code will be classified as an attack.

Client Attack Detection Policy

A Client Attack Detection Policy detects attacks originating from wireless clients. The following detection methods are available depending on the level selected.

- **Detect Valid Station Misassociation** - This feature does not detect attacks, but rather monitors valid wireless clients and their association within the network. Valid client mis-association is potentially dangerous to network security. The four types of mis-association monitored are:
- **Valid Client Associated to a Rogue -** A valid client that is associated to a rogue AP
- **Valid Client Associated to an Interfering AP -** A valid client that is associated to an interfering AP
- **Valid Client Associated to a Honeypot AP -** A honeypot is an AP that is not valid but is using an SSID that has been designated as valid
- **Valid Client in Ad Hoc Connection Mode -** A valid client that has joined an ad hoc network
- **Detect Omerta Attack -** Omerta is an 802.11 DoS tool that sends disassociation frames to all clients on a channel in response to data frames. The Omerta attack is characterized by disassociation frames with a reason code of 0x01. This reason code is “unspecified” and is not be used under normal circumstances.
- **Detect Unencrypted Valid Client -** A valid client that is passing traffic in unencrypted mode is a security risk. An intruder can sniff unencrypted traffic (also

known as packet capture) with software tools known as sniffers. These packets are then reassembled to produce the original message.

- **Detect 802.11 40MHZ Intolerance Setting -** When a client sets the HT capability “intolerant bit” to indicate that it is unable to participate in a 40MHz BSS, the AP must use lower data rates with all of its clients. Network administrators often want to know if there are devices that are advertising 40MHz intolerance, as this can impact the performance of the network.
- **Detect Active 802.11n Greenfield Mode -** When 802.11 devices use the HT operating mode, they can’t share the same channel as 802.11a/b/g clients. Not only can they not communicate with legacy devices, the way they use the transmission medium is different, which would cause collisions, errors and retransmissions.
- **Detect DHCP Client ID -** A client which sends a DHCP DISCOVER packet containing a Client-ID tag (Tag 61) which doesn't match the source MAC of the packet may be doing a DHCP denial-of-service to exhaust the DHCP pool.
- **Detect DHCP Conflict -** Clients which receive a DHCP address and continue to use a different IP address may indicate a mis-configured or spoofed client.
- **Detect DHCP Name Change -** The DHCP configuration protocol allows clients to optionally put the hostname in the DHCP Discover packet. This value should only change if the client has changed drastically (such as a dual-boot system). Changing values can often indicate a client spoofing/MAC cloning attack.
- **Detect Too Many Auth Failure Client -** Client which attempts to connect to Stellar AP but fails to pass the authentication for too many times, indicating an attack client.
- **Detect Malformed Frame-Assoc Request -** Some wireless drivers used in access points do not correctly parse the SSID information element tag contained in association request frames. A malicious association request with a null SSID can trigger a DoS or potential code execution condition on the targeted device.
- **Detect Long SSID At Client -** Detect long SSID in the wireless environment based on packets sent by clients.
- **Detect Reason Code Invalid of De-authentication -** Detect invalid De-authentication Reason Code. **Detect Reason Code Invalid of Disassociation -** Detect invalid Disassociation Reason Code.

Client Blacklist Policy

There are two sources for the Client Blacklist: created manually by user or added dynamically by system. If the **Dynamic Client Blacklist** is enabled, intruders discovered by WIPS are dynamically added into the Client Blacklist and prevented from associating with the network. The following detected items are added to the Client Blacklist by system: List of Client Attack Detection, ad hoc clients, Clients associated to rogue AP.

- **Aging Time -** Aging time for the Client Blacklist. Once expired, a client will be removed from the blacklist and allowed to be associated to the valid network until it is detected as a threat again. (Range = 1 hour to 365 days, Default = 1 Day).
- **Max Auth Failure Times -** Authentication failure times threshold. When a client fails to pass the authentication in the associated phase for too many times in a brief period, it will be classified as an attack and added into the Client Blacklist. (Range = 3 - 10 times per 5 - 3600 seconds, Default = 10 times per 60 seconds.

Intrusive AP

The WIPS Intrusive AP Screen displays information about Intrusive APs on the network including Interfering APs, Rogue APs, Friendly APs, Clients Associated to an Interfering AP, and Clients Associated to a Rogue AP. By default, the Interfering AP List is displayed. Click on a link at the top of the list to see additional lists.

> **Note:** Devices can automatically be moved to the Friendly AP List through an OUI filter, or manually moved by selecting the device(s) and clicking on the **Friendly** button at the top of the screen.

Interfering APs

- **Interfering AP BSSID -** BSSID of the interfering AP.
- **SSID -** ESSID broadcast by the interfering AP.
- **Channel -** Working channel of radio frequency on the interfering AP.
- **Scanning AP Name -** Name of the valid AP that detected the interfering AP.
- **Scanning AP MAC -** MAC address of the valid AP that detected the interfering AP.
- **Scanning AP Location -** Location of the valid AP that detected the interfering AP.
- **Distance -** Estimated distance between the interfering AP and the valid detecting AP.
- **Encryption Type -** Encryption method of ESSID broadcast by the interfering AP.
- **Attached Clients -** Clients associated to the interfering AP.
- **Signal Strength -** RSSI of the interfering AP.
- **Last Detected Time -** The latest time that the interfering AP was seen by the valid AP.

Rogue APs

- **Rogue AP BSSID -** BSSID of the rogue AP.
- **SSID -** ESSID broadcast by the rogue AP.
- **Channel -** Working channel of the radio frequency on the rogue AP.
- **Scanning AP Name -** Name of the valid AP that detected the rogue AP.
- **Scanning AP MAC -** MAC address of the valid AP that detected the rogue AP.
- **Scanning AP Location -** Location of the valid AP that detected the rogue AP.
- **Distance -** Estimated distance between the rogue AP and the valid detecting AP.
- **Encryption Type -** Encryption method of ESSID broadcast by the rogue AP.
- **Attached Clients -** Clients associated to the rogue AP.
- **Signal Strength -** RSSI of the rogue AP.
- **Last Detected Time -** The latest time that the rogue AP was seen by the detecting AP. **Rogue Reason - I**ndicates the reason for classifying the foreign AP as a rogue AP:
- Grabing Legal Accessing Client
- Signal Strength is Too Stronger, Reducing Network Performance
- Channel Switching is Too Often

- Broadcasting Conflicted SSID, Misleading User Connection
- Matching the Keyword of Suspected SSID
- Matching the Suspected MAC OUI.

Friendly APs

- **Friendly AP BSSID -** BSSID of the friendly AP.
- **SSID -** ESSID broadcasting by the friendly AP.
- **Channel -** Working channel of the radio frequency on the friendly AP.
- **Scanning AP MAC -** MAC address of the valid AP that detected the friendly AP.
- **Scanning AP Location -** Location of the valid AP that detected the friendly AP.
- **Distance -** Estimated distance between the friendly AP and the valid detecting AP.
- **Encryption Type -** Encryption method of ESSID broadcast by the friendly AP.
- **Attached Clients -** Clients associated to the friendly AP.
- **Signal Strength -** RSSI of the friendly AP.
- **Last Detected Time -** The latest time that the friendly AP was seen by the detecting AP.

Clients Associated to an Interfering AP

- **Interfering Client MAC -** MAC address of the interfering client.
- **SSID -** ESSID to which the interfering client is associated.
- **In Blacklist -** Indicates whether the client was added into the blacklist automatically and banned from accessing the network.
- **Channel -** Working channel of the interfering client.
- **Interfering AP MAC -** MAC address of the interfering AP to which the client is associated.
- **Distance -** Distance between the interfering client and the detecting AP.
- **Encryption Type -** Encryption method of the SSID to which the interfering client is associated.
- **Signal Strength -** RSSI of the interfering client.
- **Last Detected Time -** The latest time that the interfering client was seen by the detecting AP.

Clients Associated to a Rogue AP

- **Rogue Client MAC -** MAC address of the rogue client.
- **SSID -** ESSID to which the rogue associated.
- **In Blacklist -** Indicates whether the client was added into the blacklist automatically and banned from accessing the network.
- **Channel -** Working channel of the rogue client.
- **Rogue AP MAC -** MAC address of the rogue AP to which the client is associated.
- **Distance -** Distance between the rogue client and the detecting AP.
- **Encryption Type -** Encryption method of the SSID to which the rogue client is associated.

- **Signal Strength -** RSSI of the rogue client.
- **Last Detected Time -** The latest time that the rogue client was seen by the detecting AP.

Wireless Attacks

The WIPS Wireless Attacks Screen displays information about wireless attacks on the network including AP attacks and Client attacks.

AP Attack Detected

- **Attack AP BSSID -** BSSID of the attack AP.
- **SSID -** ESSID broadcast by the attack AP.
- **Channel -** Working channel of the radio frequency of the attack AP.
- **Scanning AP Name -** Name of the valid AP that detected the attack AP.
- **Scanning AP MAC -** MAC address of valid AP that detected the attack AP.
- **Scanning AP Location -** Location of valid AP that detected the attack AP.
- **Distance -** Estimated distance between the attack AP and the valid detecting AP.
- **Encryption Type -** Encryption method of the ESSID broadcast by the attack AP.
- **Attached Clients -** Clients associated to the attack AP.
- **Signal Strength -** RSSI of the attack AP.
- **Last Detected Time -** The latest time that the attack AP was seen by the detecting AP.
- **Attack Detection -** The Attack Detection Policy used (e.g., Detect Valid Station Misassociation).

Client Attack Detected

- **Attack Client MAC -** MAC address of the attack client.
- **In Blacklist -** Whether or not the client is in the Blacklist.
- **SSID -** ESSID to which the attack client is associated.
- **Channel -** Working channel of the attack client.
- **Attack AP MAC -** MAC address of the attack AP to which the client is associated.
- **Distance -** Distance between the attack client and the detecting AP.
- **Encryption Type -** Encryption method of the SSID to which the attack client is associated.
- **Signal Strength -** RSSI of the attack client.
- **Last Detected Time -** The latest time that the attack client was seen by the detecting AP.
- **Attack Detection -** The Attack Detection Policy used (e.g., Detect Valid Station Misassociation).

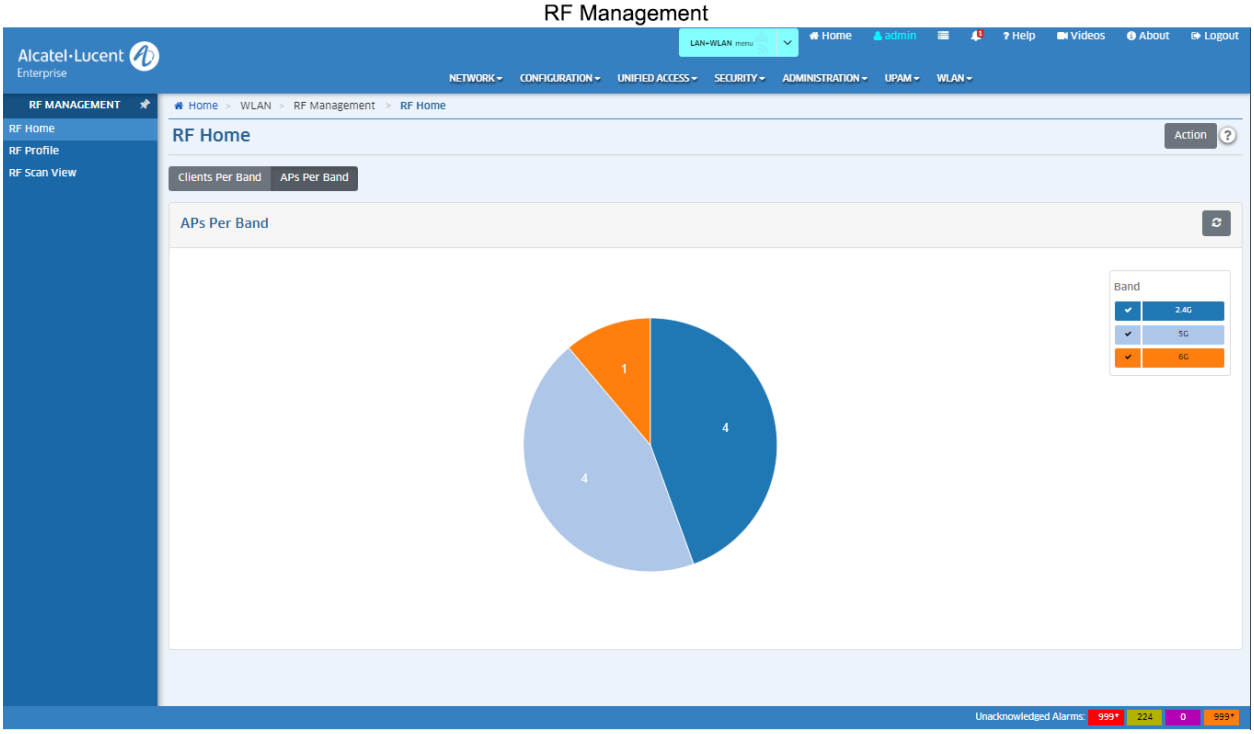
RF Management

The RF Management application allows users to create and apply wireless RF Profiles for Stellar Access Points (APs) and AP Groups. RF Profiles enable the user to ensure that transmit

power and operating frequencies meet the requirements of global regulatory agencies and individual countries. A user can also use the profiles to adjust the wireless parameters and functions according to real network environment to improve the user experience of wireless network. When Stellar APs initially register with OmniVista, they are assigned to the Default AP Group, which is configured based on the Default RF Profile. However, you can create custom RF Profiles and assign them to individual APs or AP Groups.

The Home Page (shown below) provides an overview of the clients and Stellar APs on the wireless network. Pie Charts display the number of clients and APs by bandwidth (2.4G and 5G, and 6G). Click on the **Clients Per Band** or **APs Per Band** buttons to view the information. Click on a Bandwidth in one of the pie charts for more information on the clients and APs utilizing that bandwidth.

RF Management



RF Profile

The RF Management RF Profile Screen displays all configured RF Profiles and is used to create, edit, and delete RF Profiles. Once a profile is created, it must be assigned to an AP or AP Group. To assign an RF Profile you must go to the Access Points Screen in the AP Registration application and edit the RF Profile field for an AP or AP Group by selecting the RF Profile from the drop-down menu.

> **Note:** Do not assign the same RF Profile to all APs if the APs do not support common RF parameters. For example, if some APs support 160 MHz Channel Width and others do not, then create two AP Groups and two RF Profiles. Group APs supporting 160MHz channel width into their own AP group and assign a 160 MHz RF profile to that AP group.

Creating an RF Profile

Click on the Create icon and complete the fields as described below. When you are finished, click on the **Create** button.

General Information

- **Name -** Enter a name for the RF Profile.
- **Description -** Enter an optional profile description.
- **Country/Region -** Select a Country Code. A Country Code is a short alphabetic or numeric geographical code that represent a country or dependent area and is used data processing and communications. The wireless transmitting power and operating frequencies (channels) vary by country/region. Select the country code where the APs are located.

Smart Load Balance

Smart Load Balance (SLB) is a feature improves the user experience when accessing wireless connectivity by guiding a user's client device to connect to a free wireless channel or AP and denying access to APs with weak signal. Smart Load Balance includes:

- **Band Steering -** Enables/Disables Band Steering. Band Steering controls the behavior of dual band clients according to the utilization of a wireless channel and users connected to the AP, and guides a client accessing the network to the optimal AP.

- **Force 5GHz/ Force 6GHz** Dual-band wireless clients are directed to the appropriate AP radio based on the following Force 5GHz/Force6GHz settings:
    - Force 5GHz is disabled and Force 6GHz is enabled:
        - If a client supports 6G, then client is forced to connect to the 6G radio of the AP.
        - If a client supports 2.4G and 5G but not 6G, the client is not forced to connect to 5G.
    - Force 5GHz is enabled and Force 6G is enabled:
        - If a client supports 2.4G, 5G, and 6G, the AP will prevent the client from connecting to the 2.4G radio. The client will then try to connect to the 5G or 6G radio, which the AP will allow.
        - If a client supports 2.4G and 5G but not 6G, the AP will prevent the client from connecting to the 2.4G radio. The client will then try to connect to the 5G radio, which the AP will allow.
    - Force 5Ghz is enabled and Force 6GHz is disabled:
        - If a client supports 2.4G, 5G, and 6G, the client is forced to connect to the 5G radio and not allowed to connect the 2.4G radio. If the AP supports 6G, then the client can try to connect to the 6G radio, which the AP will allow.

- **Exclude MAC OUI -** Excludes MAC OUI for band-steering. If Band Steering is enabled, enter a MAC OUI for a client, then click on the Add icon. The client will not utilize Band Steering and will be allowed to connect to the wireless band. This setting may be preferable for certain legacy and latency sensitive clients (e.g., scanners, MIPT Phones).
- **Association RSSI Threshold -** Used to set thresholds to optimize connectivity when associating with an AP by forbidding client access to networks with a weak wireless

signal (RSSI). Clients with an RSSI value lower than the Association RSSI Threshold will not be allowed to connect to the AP. By default, RSSI threshold is disabled (0). RSSI threshold can be applied to 2.4G band, 5G band, or 6G band separately. Recommend 2.4G (5), 5G (10). RSSI Threshold is recommended to be deployed in high density scenario.

- **Roaming RSSI Threshold -** Used to set thresholds to optimize connectivity when roaming by forbidding client access to networks with a weak wireless signal (RSSI). The ability to define a Roaming RSSI Threshold helps to improve the client experience in harsh RF environments. Roaming RSSI can be applied to 2.4G band, 5G band, or 6G band separately and is used in conjunction with the 802.11k and 802.11v protocols.
    - When 802.11k and 802.11v functionality is enabled on the AP, clients that support these protocols will be informed on which AP to roam to when the threshold is breached. The client will then decide whether or not to roam to another AP.
    - Clients that do not support 802.11k or 802.11v will be dropped if their RSSI value is less than the Roaming RSSI Threshold.
    - If both 802.11k and 802.11v functionality is not enabled on the AP, then all of the clients will be treated as non-802.11k or non-802.11v clients and will be dropped if their RSSI value is less than the Roaming RSSI Threshold.

  Recommended threshold settings: 2.4G (10), 5G (15). By default, Roaming RSSI is disabled (0).
- **Dynamic Load Balance -** Enables/disables client load balancing among APs in a group or groups in the same wireless network. The client information such as client number is synchronized in the wireless network so that an AP can know the load of its neighbor AP and decide whether or not to permit client access.
- **Airtime Fairness -** Enables/Disables the Airtime Fairness feature on 2.4G and/or 5G bands. The Airtime Fairness feature provides equal access to all wireless clients, regardless of client type, capability (802.11ac or 802.11n or 802.11a or 802.11g or 802.11b), thus delivering uniform performance to all clients. This feature prevents the clients from monopolizing resources. It is disabled by default. You must reboot the AP after the function enabled to make it take effect.
- **Background Scanning -** Enables/Disables Background Scanning. Background Scanning is used to examine the radio frequency environment in which the wireless network is operating, discover neighbor APs, and identify interference and attacks. Background scanning is the basis of some advanced features such as: MIPS, RDA (ACS/APC) etc. If want these advanced functions to be utilized, make sure it is enabled. By default, background scanning is enabled.
- **Scanning Channel -** Specify the channel(s) on which the wireless background scanning is executed. For a highly-sensitive packet delay use case, it is recommended that you enable background scanning only for the Working Channel.
- **Scanning Interval -** The Background Scanning interval, in seconds. (Default = 20)
- **Scanning Duration -** The Background Scanning duration in milliseconds. During the specified duration, APs examine the radio frequency through all channels on both the 2.4G band, 5G band, and 6G band (Default = 50)

- **Voice and Video Awareness -** Enables/Disables Voice and Video Awareness. Background scanning must be aware of existing traffic on APs. If there is an ongoing voice/video service, scanning should not be performed to ensure uninterrupted traffic; and scanning should resume there is no active voice/video session.
- **DRM Time Control** - Enables/Disables DRM Time Control. Enable to specify a start time for DRM automatic channel selection. When disabled, channel selection occurs at the specified DRM Interval (Default = 6 hours).
- **DRM Start Time** - If DRM Time Control is enabled (On), specify any hour of the day between 0 - 23 hours. Note that DFS radar detection change will take effect immediately.
- **DRM Interval** - If DRM Time Control is disabled (Off), specify a time interval for DRM channel selection. (Range = 0.5 hour - 12 hours, Default = 6 hours)

Radio Setting

Configures the radio options for the AP-1411. The AP-1411 is a dual-radio, tri-band (2.4G, 5G, 6G) Access Point with configurable radio options.

- **Model** - Select the AP model (OAW-AP1411).
- **Band** - Select one of the following radio band options from the drop-down menu:
  - 2.4G, 5G Full (the default)
  - 2.4G, 6G
  - 5G Full, 6G

Per Band Info

Configures the wireless setting for each radio band on an AP, such as working channel, transmit power, and short guard interval of the radio.

- **Default Setting -** Enables/Disables Band Default Settings. Disable to set custom bandwidth settings. Enable to reset bandwidth settings to default values.
- **Band -** Configure the working radio for the AP.
  - **2.4G -** 2.4G band radio will be activated.
  - **5G All -** 5G band radio will be activated. It is used to set the full band 5G radio on other AP series.
  - **5G Low -** 5.2G band radio will be activated. It is used to set the 5.2G radio on OAW AP-123x.
  - **5G High -** 5.8G band radio will be activated. It is used to set the 5.8G radio on OAW AP-123x.
  - **6G** - 6G band radio will be activated.
- **Channel Setting -** Configure the working channel of the radio.
  - Auto - Dynamically assigns the 2.4G working channel by ACS (Auto Channel Selection).
  - Manually specify the channel (allowed channels vary by country/region).
- **Client Aware -** Enables/Disables Client Aware Feature. When enabled, Auto Channel Selection does not change channels for Stellar APs with connected clients, except for high-priority events such as RADAR detected. If "Client Aware" is Disabled, the Stellar

AP may change to a more optimal channel, which may temporarily disrupt current client traffic.

- **Channel DRM -** Specify the channel scope for DRM. In some regions, specific unwanted channels can be scoped out automatic channel selection to avoid conflicts or law violation. Not supported on 2.4G Band.
- **CSA -** Enables/Disables Channel Switch Announcement. When enabled, the AP announces to clients that it is going to switch to a new channel. This allows clients that support CSA to move to the new channel and limit downtime.
- **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel. (Default = 4)
- **Channel List -** Specify the available channel(s) that can be selected by DRM. Not supported on 2.4G Band.
- **Channel Width -** Configures the channel width. Channel width is used to control how broad the signal is for transferring data. By increasing the channel width, you can increase the speed and throughput of a wireless broadcast. However, larger channel width brings more unstable transmission in crowded areas with a lot of frequency noise and interference. The 2.4G channel width support is different between 2.4G, 5G, and 6G.
    - **2.4G -** 20MHz/40MHz
    - **5G -** 20MHz/40MHz/80MHz/160MHz. Note that some high-frequency channels (e.g., 165) do not support 40MHz/80MHz/160MHz. If an AP is using these channels, a Channel Width of 40MHz/80MHz/160Mhz will not be available. For example, 160MHz is only supported on channel settings 36 through 128. Wi-Fi 6 Access Points AP132X, AP136X and new AP1351 all support 160Mhz channels.
    - **6G -** 20MHz/40MHz/80MHz/160MHz
- **Power Setting -** Configures the transmit power of the wireless radio. Power range varies from different radios.
    - **2.4G -** Configure the power setting for 2.4G radio.
        - Auto - Dynamically assigned the 2.4G transmit power by APC (Auto Power Control)
        - Manually specify the power setting (3dBm - 20dBm)
    - **5G -** Configure the power setting for 5G radio.
        - Auto - Dynamically assigned the 5G transmit power by APT (Auto Power Control)
        - Manually specify the power setting (3dBm - 23dBm)
    - **6G -** Configure the power setting for 6G radio.
        - Auto - Dynamically assigns the 6G transmit power by APC (Auto Power Control)
        - Manually specify the power setting
- **Minimum Tx Power -** Specify the minimum transmit power for auto power setting. This can prevent the AP from selecting a low transmit power resulting in poor quality transmission.
- **Maximum Tx Power -** Specify the maximum transmit power for auto power setting.

- **External Antenna Gain -** Specify the gain value for the external AP antenna. Only those AP Groups containing APs with external antennas (OAW-AP1222, OAW-AP1232) need to be configured with this attribute. It is recommended that you divide APs into several AP Groups when using different types of external antenna (e.g., Group A with an antenna gain value of 3-dBi, and Group B with an antenna gain value of 6-dBi).
- **Beacon Interval -** Specify the Beacon period for the AP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the AP. (Range = 60 - 500, Default = 100)
- **Short Guard Interval -** Enables/Disables Short Guard Interval. In IEEE 802.11 OFDM-based communications, Guard Interval is used to ensure that distinct transmissions occur between the successive data symbols transmitted by a device. The standard symbol Guard Interval used in 802.11 OFDM is 800 nanoseconds in duration. To increase data rates, the 802.11n standard added optional support for a 400 nanoseconds guard interval (Short Guard Interval). This would provide approximately an 11% increase in data rates. However, using the Short Guard Interval will result in higher packet error rates when the delay spread of the RF channel exceeds the Short Guard Interval, or if timing synchronization between the transmitter and receiver is not precise. By Default, Short Guard Interval is disabled on the wireless radio.
- **MU-MIMO -** Enables/Disables Multi-User, Multiple-Input, Multiple-Output (MU-MIMO) feature. If enabled, the AP can communicate with multiple devices simultaneously. This decreases the time each device has to wait for a signal and speeds up the network.
- **High-Efficiency -** Enables/Disables 802.11ax high efficiency wireless functionality. If Disabled, an HE mode capable AP will downgrade to VHT (Very High Throughput) mode. For 6GHz band, this functionality is enabled by default and cannot be disabled.

Editing an RF Profile

Select an RF Profile in the Profile List and click on the Edit icon. Edit any fields as described above, then click on the **Apply** button. Note that you cannot edit the Profile Name.

Deleting an RF Profile

Select an RF Profile(s) in the Profile List, click on the Delete icon, and click on **OK** at the Confirmation Prompt. Note that you cannot delete a profile that has been assigned to an AP or AP Group.

RF Profile Information

General

- **Name -** The RF Profile name.
- **Description -** Optional RF Profile description.
- **Country/Region -** The Country Code for the profile. A Country Code is a short alphabetic or numeric geographical code that represent a country or dependent area and is used data processing and communications. The wireless transmitting power and operating frequencies (channels) vary by country/region. Select the country code where the APs are located.
- **Associated AP/Associated Group -** The AP/AP Group associated with the profile.

Smart Load Balance

- **Band Steering -** The administrative status of Band Steering for the profile (On/Off).
- **Force 5Ghz** - The administrative status of the "Force 5GHz" feature (On/Off).
- **Force 6Ghz -** The administrative status of the "Force 6GHz" feature (On/Off).
- **Exclude MAC OUI -** The "Exclude MAC OUI", if configured.
- **Association RSSI Threshold 2.4G -** The RSSI setting for 2.4G radio.
- **Association RSSI Threshold 5G All -** The Association RSSI setting for 5G radio.
- **Association RSSI Threshold5G Low -** The Association RSSI setting for 5.8G band radio.
- **Association RSSI Threshold 5G High -** The Association RSSI setting for 5.2G band radio.
- **Association RSSI Threshold 6G -** The Association RSSI setting for 6G radio.
- **Roaming RSSI Threshold 2.4G -** The Roaming RSSI setting for 5G radio.
- **Roaming RSSI Threshold 5G All -** The Roaming RSSI setting for 5G radio.
- **Roaming RSSI Threshold 5G Low -** The Roaming RSSI setting for 5.8G band radio.
- **Roaming RSSI Threshold 5G High -** The Roaming RSSI setting for 5.2G band radio.
- **Roaming RSSI Threshold 6G -** The Roaming RSSI setting for 6G radio.
- **Dynamic Load Balance -** The administrative status of Dynamic Load Balancing for the profile (On/Off). If enabled, this feature performs client load balancing among APs in a group or groups in the same wireless network.
- **Airtime Fairness 2G -** The administrative status of the Airtime Fairness feature for 2G band radio (On/Off).
- **Airtime Fairness 5G -** The administrative status of the Airtime Fairness feature for 5G band radio (On/Off).
- **Background Scanning -** The administrative status of Background Scanning for the profile (On/Off). Background Scanning is used to examine the radio frequency environment in which the wireless network is operating, discover neighbor APs, and identify interference and attacks.
- **Scanning Interval -** The Background Scanning interval, in seconds.
- **Scanning Duration -** The Background Scanning duration in milliseconds. During the specified duration, APs examine the radio frequency through all channels on both the 2.4G band and 5G band.
- **Voice and Video Awareness -** The administrative status of Voice and Video Awareness (On/Off). Background scanning must be aware of existing traffic on APs. If there is an ongoing voice/video service, scanning should not be performed to ensure uninterrupted traffic; and scanning should resume there is no active voice/video session.

Per Band Info

- **Default Setting -** Indicates whether or not Band Settings are customized, the Default setting = "Off". If the Default Band Settings are being used, Default setting = "On".

- **2.4G -** Indicates whether or not the 2.4G Band Settings are configured for the profile (On/Off).
    - **Power Setting -** The 2.4G Power setting for the profile.
    - **Minimum Tx Power 2.4G -** The minimum transmit power for auto power setting, if configured.
    - **Maximum Tx Power 2.4G -** The maximum transmit power for auto power setting, if configured.
    - **Channel Setting -** The 2.4G Channel setting for the profile.
    - **Client Aware -** Client Aware Feature administrative status (On/Off)
    - **CSA -** Channel Switch Announcement administrative status (On/Off).
    - **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel.
    - **Channel Width -** The 2.4G Channel Width setting for the profile.
    - **External Antennas Gain -** The gain value of 2.4G band for the external antennas used by the APs mapping to this RF profile.
    - **Short Guard Interval -** The administrative status of the Short Guard Interval feature for 2.4G radio.
    - **MU-MIMO -** The administrative status of the MU-MIMO feature for 2.4G radio.
    - **High Efficiency -** The administrative status of the "High Efficiency" feature for 2.4G radio.
    - **Beacon Interval -** The 2.4G radio Beacon Interval.
- **5G All -** Indicates whether or not the 5G Band Settings are configured for the profile (On/Off).
    - **Power Setting -** The 5G Power setting for the profile.
    - **Minimum Tx Power 5G All -** The minimum transmit power for auto power setting, if configured.
    - **Maximum Tx Power 5G All -** The maximum transmit power for auto power setting, if configured.
    - **Channel Setting -** The 5G Channel setting for the profile.
    - **Client Aware -** Client Aware Feature administrative status (On/Off).
    - **Channel DRM -** The Channel DRM administrative status (On/Off).
    - **CSA -** Channel Switch Announcement administrative status (On/Off).
    - **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel.
    - **Channel List -** If enabled, the available channel(s) that can be selected by DRM.
    - **Channel Width -** The 5G Channel Width setting for the profile.
    - **External Antennas Gain -** The gain value of 5G band for the external antennas used by the APs mapping to this RF profile.
    - **Short Guard Interval -** The administrative status of the Short Guard Interval feature for 5G radio.

  - **MU-MIMO -** The administrative status of the MU-MIMO feature for 5G radio.
  - **High Efficiency -** The administrative status of the "High Efficiency" feature for 5G radio.
  - **Beacon Interval -** The 5G radio Beacon Interval.
- **5G High -** Indicates whether or not the 5.8G Band Settings are configured for the profile (On/Off).
  - **Power Setting -** The 5.8G Power setting for the profile.
  - **Minimum Tx Power 5G High -** The minimum transmit power for auto power setting, if configured.
  - **Maximum Tx Power 5G High -** The maximum transmit power for auto power setting, if configured.
  - **Channel Setting -** The 5.8G Channel setting for the profile.
  - **Client Aware -** Client Aware Feature administrative status (On/Off)
  - **Channel DRM -** The Channel DRM administrative status (On/Off).
  - **CSA -** Channel Switch Announcement administrative status (On/Off).
  - **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel.
  - **Channel List -** If enabled, the available channel(s) that can be selected by DRM.
  - **Channel Width -** The 5.8G Channel Width setting for the profile.
  - **External Antennas Gain -** Configure the gain value of 5.8G band for the external antennas used by AP1232(s) mapping to this RF profile.
  - **Short Guard Interval -** The administrative status of the Short Guard Interval feature for 5.8G radio.
  - **MU-MIMO -** The administrative status of the MU-MIMO feature for 5.8G radio.
  - **High Efficiency -** The administrative status of the "High Efficiency" feature for 5.8G radio.
  - **Beacon Interval -** The 5.8G radio Beacon Interval.
- **5G Low -** Indicates whether or not the 5.8G Band Settings are configured for the profile (On/Off).
  - **Power Setting -** The 5.2G Power setting for the profile.
  - **Minimum Tx Power 5G Low -** The minimum transmit power for auto power setting, if configured.
  - **Maximum Tx Power 5G Low -** The maximum transmit power for auto power setting, if configured.
  - **Channel Setting -** The 5.2G Channel setting for the profile.
  - **Client Aware -** Client Aware Feature administrative status (On/Off)
  - **Channel DRM -** The Channel DRM administrative status (On/Off).
  - **CSA -** Channel Switch Announcement administrative status (On/Off).

  - **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel.
  - **Channel List -** If enabled, the available channel(s) that can be selected by DRM.
  - **Channel Width -** The 5.2G Channel Width setting for the profile.
  - **External Antennas Gain -** Configure the gain value of 5G band for the external antennas used by the APs mapping to this RF profile.
  - **Short Guard Interval -** The administrative status of the Short Guard Interval feature for 5.2G radio.
  - **MU-MIMO -** The administrative status of the MU-MIMO feature for 5.2G radio.
  - **High Efficiency -** The administrative status of the "High Efficiency" feature for 5.2G radio.
  - **Beacon Interval -** The 5.2G radio Beacon Interval.
- **6G -** Indicates whether or not the 6G Band Settings are configured for the profile (On/Off).
  - **Power Setting -** The 6G Power setting for the profile.
  - **Minimum Tx Power 6G Low -** The minimum transmit power for auto power setting, if configured.
  - **Maximum Tx Power 6G Low -** The maximum transmit power for auto power setting, if configured.
  - **Channel Setting -** The 6G Channel setting for the profile.
  - **Client Aware -** Client Aware Feature administrative status (On/Off)
  - **Channel DRM -** The Channel DRM administrative status (On/Off).
  - **CSA -** Channel Switch Announcement administrative status (On/Off).
  - **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel.
  - **Channel List -** If enabled, the available channel(s) that can be selected by DRM.
  - **Channel Width -** The 6G Channel Width setting for the profile.
  - **External Antennas Gain -** Configure the gain value of 6G band for the external antennas used by the APs mapping to this RF profile.
  - **Short Guard Interval -** The administrative status of the Short Guard Interval feature for 6G radio.
  - **MU-MIMO -** The administrative status of the MU-MIMO feature for 6G radio.
  - **High Efficiency -** The administrative status of the "High Efficiency" feature for 6G radio.
  - **Beacon Interval -** The 6G radio Beacon Interval.

RF Scan View

The RF Management RF Scan View Screen is used to view Scanning Mode data for APs. Wireless networks operate in environments with electrical and radio frequency devices that can interfere with network communications. APs can examine the radio frequency environment in which the Wi-Fi network is operating, identify interference, and classify its sources. An analysis of the results can then be used to quickly isolate issues with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel.

> **Note:** To view Scanning Mode data for an AP, the AP must be in "Scanning Mode". If necessary, go to the Access Points Screen (Network - AP Registration - Access Points),

select the AP, click on the Edit icon and select **Edit Dedicated Scanning Mode**. Note that when an AP is in Scanning Mode, no clients can associate with the AP.

Viewing Scanning Mode Data

Click on the **Select Device** button and select an AP. The "real time" Scanning Mode data for the AP will be displayed. Repeat to view data on other APs. You can only view data for one AP at a time.

Click on the **Show History Data** button to display historical data. In the historical data display, you can view data by Band (2.4G, 5G), Channel Width (20MHz, 40MHz), Channel, and Time Period (last 24 hours, 3 days, 7 days).

Scanning Mode Data

By default, "real time" data is displayed. Click on the **Show History Data** button to display historical data.

Real Time Data

By default, OmniVista Cirrus displays "real time" data for the selected AP for both the 2.4G and 5G Bands. Hover the mouse over a data point for more detailed data.

- **Radio -** The wireless band of the network
- **Utilization -** The percentage of the channel being used.
- **Channel Width -** The width of the channel
- **Frequency Range -** The frequency range of the channel.
- **Noise -** Noise is the measure of the wireless signal created from the sum of all the noise sources and unwanted signals.
- **Known APs -** The number of valid APs identified on the channel.
- **Unknown APs -** The number of interfering or rogue APs identified on the channel.

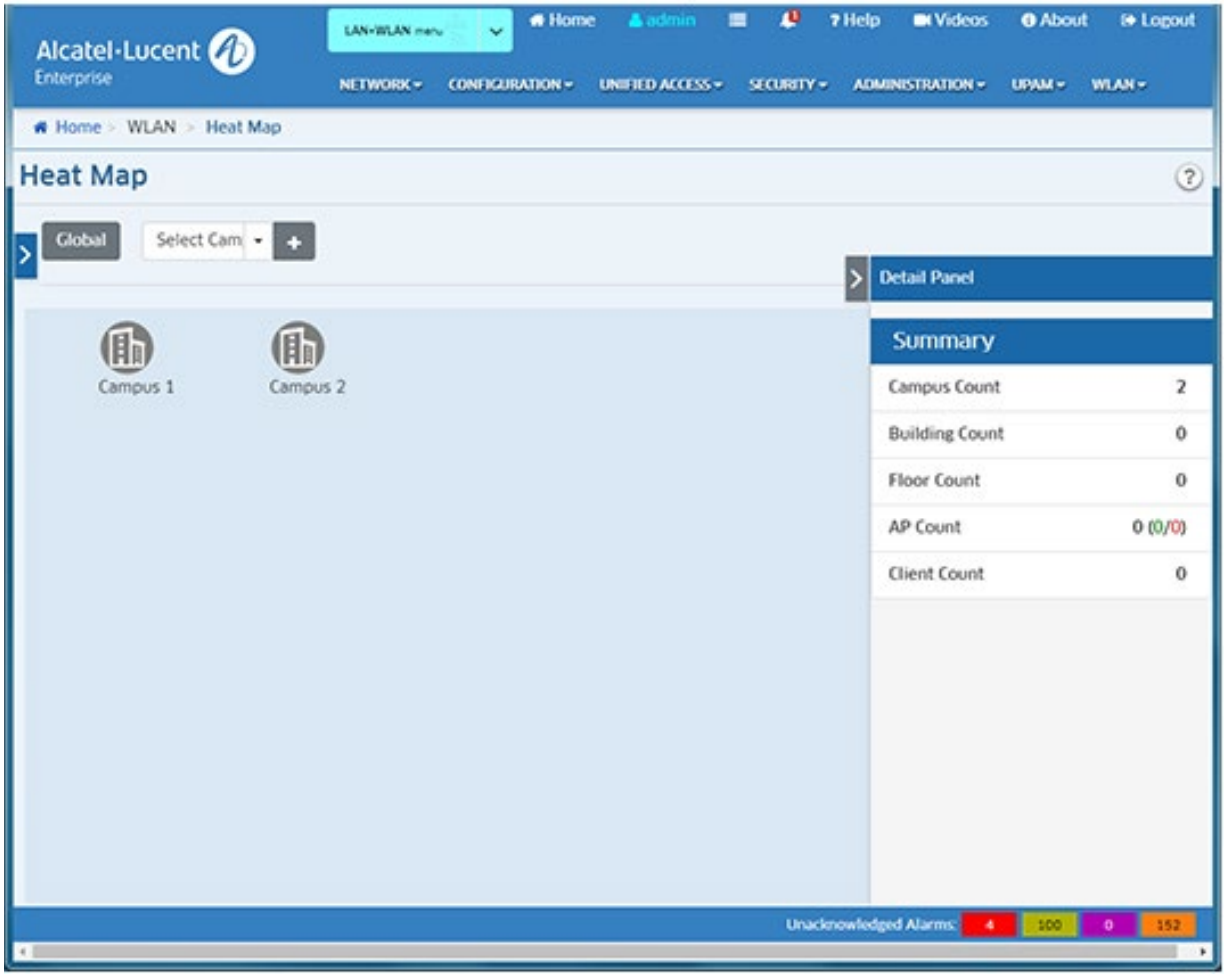
Historical Data

Click on the **Show History Data** button to display historical data. In the historical data display, you can view data by Band (2.4G, 5G), Channel Width (20MHz, 40MHz), Channel, and Time Period (last 24 hours, 3 days, 7 days).

Heat Map

The Heat Map application is a design, verification, troubleshooting tool for installed Stellar Wi-Fi networks. The application provides a way to create and organize Heat Maps from multiple locations, from Campus level to Building level and Floor level to give a comprehensive view of Wi-Fi coverage. The Heat Map Screen (shown below) is used to create, edit, delete, and organize Wi-Fi Heat Maps.

Heat Map



Creating a Heat Map

The hierarchy for creating heat maps in the Heat Map application is Campus - Building - Floor - Heat Map. You must first create a Campus location, then create buildings within the campus, then create floors for the building. Once you create the floors in the building, you create Heat Maps for each floor based on the current Wi-Fi configuration for the floor.

Creating a Campus

On the Global Screen, click on the Add icon next to the "Select Campus" drop-down to bring up the Add Campus Screen. Complete the fields as described below, then click on **OK**.

- **Campus Name -** User-configured name for the Campus.
- **Campus Address -** Optional address for the Campus.
- **Campus Description -** Optional description information for the Campus.

Repeat to create additional Campuses. When you are done, create a Building(s) for the Campus(es). To edit basic Campus information, click on the Campus icon and click on the "Modify Campus" link in the Operation Pane of the Detail Panel. To delete a Campus, click on

the Campus icon, click on the Delete icon next to the "Select Campus" drop-down and click **OK** at the Confirmation Prompt.

Creating a Building

Double-click on a Campus, then click on the Add Icon next to the "Select Building" drop-down to bring up the Add Building Screen. Complete the fields as described below, then click on **OK**.

- **Campus Name -** Pre-filled with the name of the Campus.
- **Building Name -** User-configured name for the Building
- **Building Address -** Optional address for the Building.
- **Building Description -** Optional description information for the Building.

Repeat to create additional Buildings. When you are done, create a floor(s) for the Building(s). To edit basic Building information, click on the Building icon and click on the "Modify Building" link in the Operation area of the Detail Panel. To delete a Building, click on the Building icon, click on the Delete icon next to the "Select Building" drop-down and click **OK** at the Confirmation Prompt.

Creating a Floor

Double-click on a Building, then click on the Add icon next to the "Select Floor" drop-down to bring up the Add Floor Screen. Complete the fields as described below, then click on **Apply**.

- **Building Name -** Pre-filled with the name of the Building.
- **Floor Name -** User-configured name for the Floor.
- **Floor Number -** Floor number (e.g., 1, 2. 3).
- **Floor Description -** Optional description information for the Floor.
- **File Name -** Import a basic floor plan image (jpeg or png file). You can import an existing floor plan image for a location that you can use as a guide, or create a blank image (.jpg or .png). Note that you can also select the "Clone" radio button to use an existing Floor Map image.

Repeat to create additional Floors. When you are done, create a Heat Map(s) for the floor(s). To edit basic Floor information, click on the Floor icon and click on the "Modify Floor Basic Info" link in the Operation area of the Detail Panel. To delete a Floor, click on the Floor icon, click on the Delete icon next to the "Select Floor" drop-down and click **OK** at the Confirmation Prompt.

Creating a Heat Map for a Floor

To create a Heat Map for a floor, double-click on the Floor icon to bring up the Heat Map Screen. The floor plan image you imported when you created the floor will be displayed along with the Detail Panel for the Heat Map.

Click on the "Edit Floor Map" link in the Operation Pane of the Detail Panel to bring up the Edit Floor Map Pane. The Edit Pane is used to scale the map, draw obstacles in the map, and place APs in the map.

After creating the map using the Edit Pane options, click on "Stop" at the top of the Edit Pane or the "Stop Edit Mode" link in the Operation Pane, then click on **Yes** at the Save the Layout prompt to save the map and view the Heat Map.

Detail Panel

The Detail Panel contains the following areas, which are used to display basic map parameters, perform operations on a map (e.g., edit a map, modify basic map information), edit a map (e.g., add obstacles, add APs), and change map displays (e.g., display obstacles/APs, display APs by frequency). You can also click on an AP in the map for detailed information about the AP.

Summary Pane

The Summary Pane displays basic information about the map.

- **Floor Name -** User configured name for the floor.
- **Floor Number -** Floor number (e.g., 1, 2. 3).
- **Floor Description -** Optional description information for the floor.
- **AP Count -** APs deployed in the floor map. Green indicates online AP, Red indicates offline AP, and Black indicates the number of APs deployed on the floor.
- **Client Count -** The number of clients connected to APs on the floor.

Operation Pane

The Operation Pane is used to perform specific operations on the map (e.g., edit the map, modify basic map information, create/edit/delete obstacles in the map).

- **Edit Floor Map -** Click to bring up the Edit Floor Map Pane to create/edit a floor map as described below. After creating a floor, click on the Edit Floor Map link to bring up the Edit Floor Map Panel and add obstacles and APs to the map.
- **Modify Floor Basic Info -** Brings up the Modify Floor Basic window to modify basic floor information.
- **Upload Floor Background -** Used to change the background image. If you upgrade the background image, all of the obstacles and map scaling are removed. The AP(s) remain in the map, however, their original placement is eliminated.
- **Obstacle Manage -** Used to create/edit/delete custom obstacles. You can create a custom obstacle when system-defined ones are not sufficient for deployment. Click on the "Obstacle Manage" link to bring up the Obstacle List. To add a custom obstacle, click on the Add icon, complete the following fields on the Add Obstacle window, and click **OK**. You can then add the custom obstacle to the map.
- **Obstacle Name -** User-configured name for the obstacle.
- **Signal Decline -** Typical Wi-Fi signal attenuation caused by the obstacle (<1~90>).
- **Color -** Color of the line that represent the obstacle in the floor plan.
- **Width -** Width of the line that represent the obstacle in the floor plan.
- **Remove All The APs -** Used to remove all APs in a floor plan.
- **Remove All The Obstacles -** Used to remove all obstacles in a floor plan.

Note: To edit a custom obstacle, select the obstacle in the Obstacle List and click on the Edit icon. Edit the fields as described above, then click **OK**. To delete a custom obstacle, select the obstacle in the Obstacle List, click on the Delete icon, then click **OK** at the Confirmation Prompt. You can only edit/delete custom obstacles.

Edit Pane

The Edit Pane is used to customize a map by adding obstacles and APs to the map.

- **Scale the Map -** Click on this option to set the scale of the floor map. Click on the **Scale The Map** button and move the cursor to the map. The cursor will turn into a ruler. Drag the cursor across an area of the map. The Scale Distance window will appear. Enter the length of the line drawn in meters or feet. Click again to set the scale.
- **Adding AP to the Floor -** Click on **Laying AP To The Floor** button to add APs to the Heat Map. All available registered APs are displayed. Select the APs that have been installed on the floor and click **OK**. After the AP(s) are added to the map, you can click and drag the AP(s) to their proper location on the map. An AP can only be placed in one map at a time. Once an AP is added to a map, it will no longer be available for selection in a new map. If you want to add an AP that has been placed in another map, you must first remove it from that map.
- **Draw -** Next to the **Draw** button, click on the down arrow to display a list of pre-configured obstacles (e.g., Cubicle, WallsHeavy). Click on an obstacle to select it. The obstacle will appear in the **Draw** button. Click on the Draw button to activate the drawing tool for that obstacle (button will turn blue), then click on the map to draw the obstacle (much like any drawing tool). Repeat to add additional objects. The following objects and are available:
- **Walls Heavy -** Represents a thick wall (e.g., concrete wall in the building floor). One heavy wall typically causes 13dB Wi-Fi signal attenuation.
- **Cubicle -** Represents cubicle material, such as a thin wall in a building. One cubicle wall typically causes 1dB Wi-Fi signal attenuation.
- **Door Heavy -** Represents a thick, solid door, such as an iron door. One heavy door typically causes 12dB Wi-Fi signal attenuation.
- **Glass -** Represents a glass window or similar material in a building. One glass obstacle typically causes 3dB Wi-Fi signal attenuation.

  Note: You can also create custom obstacles using the Obstacle Manage function in the Operation Pane. After creating a map using the Edit Pane options, click on "Stop" at the top of the Edit Pane or the "Stop Edit Mode" link in the Operation Pane, then click on **Yes** at the Save the Layout prompt to save the map and view the Heat Map.

Survey Toggle Pane

The Survey Toggle Pane is used to quickly customize the map display. Select a Display or Frequency checkbox to add/remove items from the display. Select a signal from the Coverage Area drop-down to display areas of the map with a specific signal. This pane is not displayed when the map is in Edit Mode.

- **Display -** Add/remove obstacles or all APs
- **Frequency -** Add/remove 2.4 and/or 5G APs
- **Coverage Area -** Display the area of the map for the selected signal.
- **Display Neighbor AP -** Select an AP and click on this link to display neighbor APs for the selected AP. An AP icon with purple text background color represents a static

neighbor AP, and a pink background represents an automatic discovery neighbor AP.

- **Display All APs -** If you click on the Display Neighbor APs link, click on this link to toggle to the previous view.

AP Details Pane

- **Model -** The model type of the AP (e.g., OAW-AP1221, OAW-AP1251).
- **MAC -** The MAC address of the AP.
- **IP -** The IP address of the AP.
- **Group -** The AP Group to which the AP belongs.
- **Uptime -** The amount of time the AP has been up since the last reboot.
- **Location -** The AP physical location (set in the AP Registration application).
- **Status -**The AP status:
- **Up -** AP is reachable.
- **Down -** AP is not reachable.
- **Unknown -** The AP has not been seen yet (AP was manually created/imported).
- **Registration Status -** The AP management status in OmniVista.
- **Normal -** AP is managed by OmniVista.
- **Untrusted -** AP cannot be managed by OmniVista because it is "Untrusted". The Administrator can set the AP to "Trusted" status, if needed.
- **Unlicensed -** AP cannot be managed by OmniVista because it is unlicensed. The Administrator can allocate a license to the AP and turn it to Normal status, if needed.
- **Error Country Code -** The AP cannot be managed by OmniVista because it has the wrong country code configuration. The Administrator can change the AP's country code and turn it to Normal status, if needed.
- **Channel -** The working channel of the 2.4GHz band and 5GHz band on the AP.
- **EIRP -** The Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power for the AP. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the AP.
- **Client Count -** The number of clients currently connected to the AP.
- **Channel Utilization -** The utilization of the AP working channel.

Editing a Heat Map for a Floor

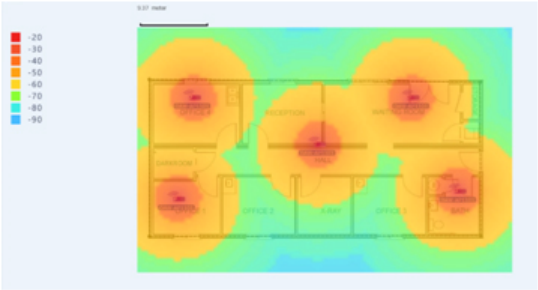
To edit a Heat Map for a floor, double-click on the Floor icon to bring up the Heat Map Screen. The floor plan image you imported when you created the floor will be displayed along with the Detail Panel for the Heat Map. Click on the "Edit Floor Map" link in the Operation Pane of the Detail Panel to bring up the Edit Floor Map Pane. Edit the map as described above, click on "Stop" at the top of the Edit Pane or the "Stop Edit Mode" link in the Operation Pane, then click on **Yes** at the Save the Layout prompt to save the map and view the Heat Map.

Deleting a Heat Map

To delete a map, click on the Delete icon next to the **Floor** drop-down list at the top of the screen, then click **OK** at the Confirmation prompt.

Viewing Heat Maps

After creating a Heat Map, the map displays the Wi-Fi coverage quality within the floor plan. Wi-Fi coverage areas are displayed by color depending on the quality of the coverage, as shown in the figure below.



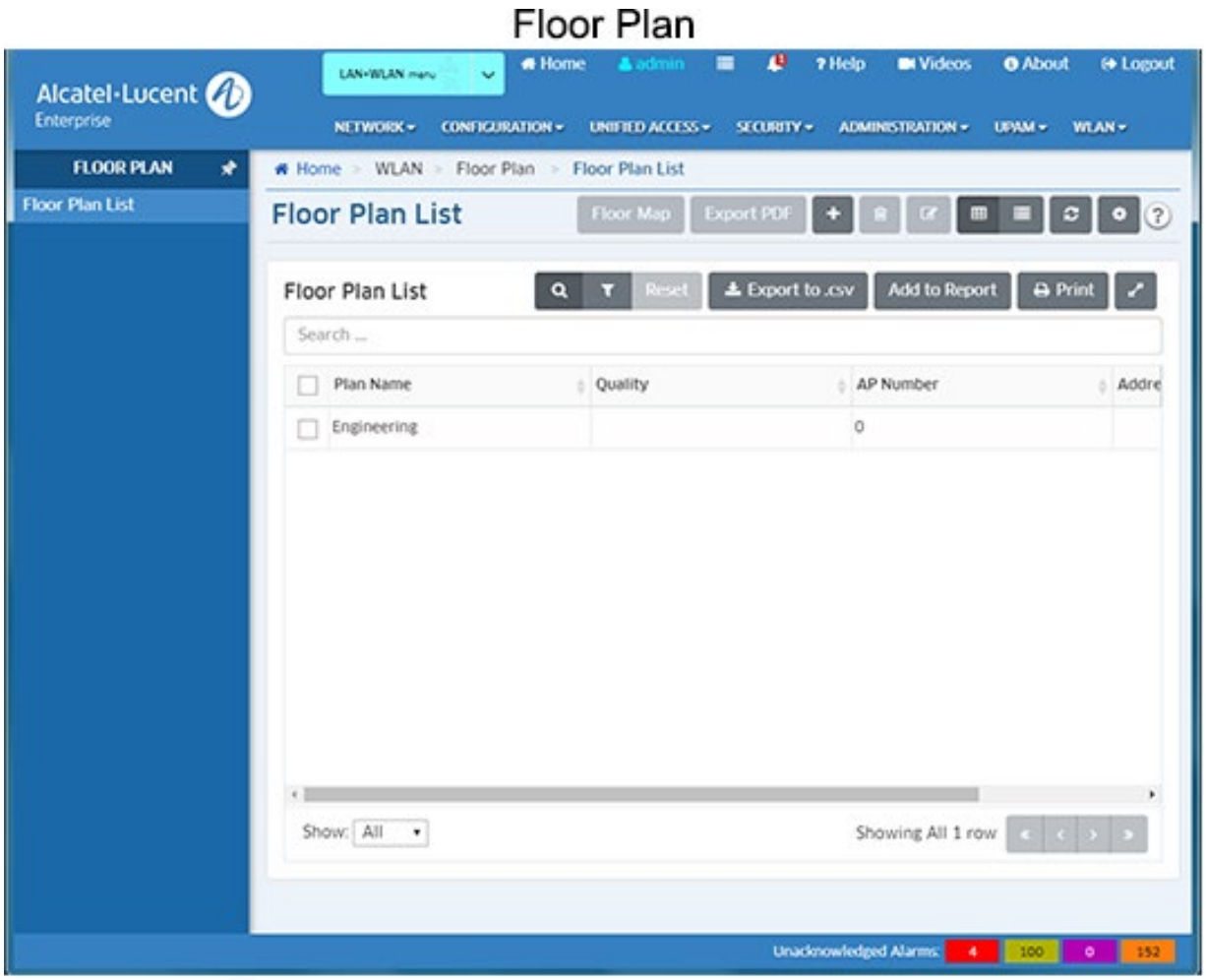
Wi-Fi Coverage Legend	
-20	Wi-Fi signal is stronger than -20dBm.
-30	Wi-Fi signal is stronger than -30dBm.
-40	Wi-Fi signal is stronger than -40dBm.
-50	Wi-Fi signal is stronger than -50dBm.
-60	Wi-Fi signal is stronger than -60dBm.
-70	Wi-Fi signal is stronger than -70dBm.
-80	Wi-Fi signal is stronger than -80dBm.
-90	Wi-Fi signal is stronger than -90dBm.

Floor Plan

The Floor Plan application is a design, verification, troubleshooting tool for Stellar Wi-Fi networks. Floor Plan can be used to determine optimal placement of Access Points (APs) in a location. The application can also automatically determine AP placement and configurations for optimal set-up.

The application enables you to create a floor plan for a location and manually place Stellar APs on the floor plan to view the effective Wi-Fi coverage within the floor plan. You can also set up an expected coverage area on the floor plan and the application will automatically identify the optimal number and location of APs within the floor plan to use as a guide when installing APs on site.

The Floor Plan List Screen (below) displays all configured floor plans and is used to create, edit, and delete floor plans. You can also export a Floor Plan as a PDF File.



Creating a Floor Plan

To create a floor plan, you must first create a basic floor plan by importing a floor plan image. You then customize the floor plan by adding obstacles (e.g., Walls, Cubicles) and APs to the floor plan so that the Floor Plan application can display Wi-Fi coverage quality within the floor plan.

Creating a Basic Floor Plan

Click on the Add Icon to bring up the Create Floor Plan Screen. With the "New" radio button selected (Default), complete the fields as described below, then click on the **Create** button to create a basic floor plan.

- **Floor Plan Name -** User-created name for the floor plan.
- **Address -** Optional physical location and description for the floor plan.
- **File Name -** Import a basic floor plan image (jpg or png file). You can import an existing floor plan image for a location that you can use as a guide, or create a blank image (.jpg or .png). Note that once the basic image is imported, you must customize it as described below.

Note: You can also select the "Clone" radio button to create a new floor plan using the same floor plan image.

Customizing a Floor Plan

Click on the "Edit Floor Map" link in the Operation Pane of the Detail Panel to bring up the Edit Floor Map Pane. The Edit Pane is used to scale the map, draw obstacles in the map, and place APs in the map.

After creating the map using the Edit Pane options, click on "Stop" at the top of the Edit Pane or the "Stop Edit Mode" link in the Operation Pane, then click on **Yes** at the Save the Layout prompt to save the map and view the effective Wi-Fi coverage within the floor plan.

Detail Panel

The Detail Panel contains the following areas, which are used to display basic map parameters, perform operations on a map (e.g., edit a map, modify basic map information), and create/edit a map (e.g., add obstacles, add APs).

Summary Pane

The Summary Pane displays basic information about the map.

- **Plan Name -** User-configured name for the floor plan.
- **Address -** User-configured location of the floor plan.
- **Quality -** Expected wireless network quality. (Specified by user for Auto Deployment only.)
- **AP Number -** The number of APs in the floor plan.

Operation Pane

The initial Operation Pane that is displayed is used to perform specific operations on the map (e.g., edit the map, modify basic map information, create/edit/delete obstacles in the map). When you are in edit mode, the Operation Pane contains additional editing functions.

- **Edit Floor Map -** Click to bring up the Edit Floor Map Pane to create/edit a floor map as described below. After creating a floor, click on the Edit Floor Map link to bring up the Edit Floor Map Panel and add obstacles and APs to the map.
- **Obstacle Manage -** Used to create/edit/delete custom obstacles. You can create a custom obstacle when system-defined ones are not sufficient for deployment. Click on the "Obstacle Manage" link to bring up the Obstacle List. To add a custom obstacle, click on the Add icon, complete the following fields on the Add Obstacle window, and click **OK**. You can then add the custom obstacle to the map.

  Obstacle Name - User-configured name for the obstacle.

  Signal Decline - Typical Wi-Fi signal attenuation caused by the obstacle (<1~90>).

  Color - Color of the line that represent the obstacle in the floor plan.

  Width - Width of the line that represent the obstacle in the floor plan.
- **Export PDF** - Downloads the current Floor Plan as a PDF to your PC.

Note: To edit a custom obstacle, select the obstacle in the Obstacle List and click on the Edit icon. Edit the fields as described above, then click **OK**. To delete a custom obstacle, select the obstacle in the Obstacle List, click on the Delete icon, then click **OK** at the Confirmation Prompt. You can only edit/delete custom obstacles.

Note that when the Edit Floor Plan Pane is activated, the following functions are also available in the Operation Pane.

- **Stop Edit Mode -** Exit edit mode. After exiting edit mode, you can save your floor plan changes or cancel the updates.
- **Auto Deployment -** Used to activate the "Auto Deployment" feature. Click on the "Auto Deployment" link to bring up the Auto Deployment window. Select the AP Model you want to deploy and desired coverage quality and click **OK**. The optimal number of APs will be placed on the floor plan based on the coverage quality selected:

  General - Expected coverage(RSSI>-65) greater than 50%.

  Good - Expected coverage(RSSI>-65) greater than 70%.

  Excellent - Expected coverage(RSSI>-65) greater than 85%.
- **Remove the Polygon -** Used to remove a polygon from the floor plan.
- **Remove All The Obstacles -** Used to remove all obstacles in a floor plan.
- **Remove All The APs -** Used to remove all APs in a floor plan.
- **Set Default Power of Each AP Model -** Used to set the default Tx power for each AP Model. Click on the link to bring up the Set Default Power For Each AP Model window, then set the default power for an AP Model. Repeat to set defaults for additional AP Models. This sets the default Tx power for any subsequent APs you add to the floor plan. The power settings on APs that have already been placed on the map will not change.

Edit Pane

The Edit Pane is used to customize a map by adding obstacles and APs to the map.

- **Polygon (Auto Deployment Only) -** Used to add a coverage area with expected wireless quality. Click on the Polygon icon, then click a beginning and end point in the floor plan. When you select "Auto Deployment", the Floor Plan application will place the APs in the coverage area based on the wireless quality selected for Auto Deployment. Note that you can only have one polygon in a floor plan. Click on the Delete icon next to the Polygon icon to delete it.
- **Scale the Map -** Click on this option to set the scale of the floor map. Click on the **Scale The Map** button and move the cursor to the map. The cursor will turn into a ruler. Drag the cursor across an area of the map. The Scale Distance window will appear. Enter the length of the line drawn in meters or feet. Click again to set the scale.
- **Draw -** Next to the **Draw** button, click on the down arrow to display a list of pre-configured obstacles (e.g., Cubicle, WallsHeavy). Click on an obstacle to select it. The obstacle will appear in the **Draw** button. Click on the Draw button to activate the drawing tool for that obstacle (button will turn blue), then click on the map to draw the obstacle (much like any drawing tool). Repeat to add additional objects. The following objects and are available:

  Walls Heavy - Represents a thick wall (e.g., concrete wall in the building floor). One heavy wall typically causes 13dB Wi-Fi signal attenuation.

  Cubicle - Represents cubicle material, such as a thin wall in a building. One cubicle wall typically causes 1dB Wi-Fi signal attenuation.

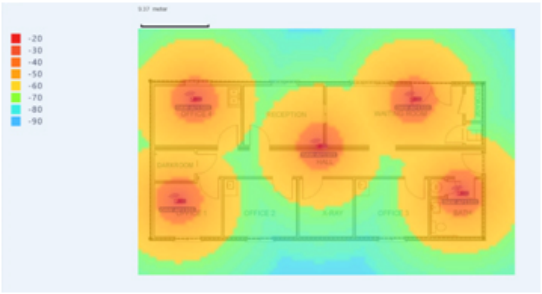
Door Heavy - Represents a thick, solid door, such as an iron door. One heavy door typically causes 12dB Wi-Fi signal attenuation.

Glass - Represents a glass window or similar material in a building. One glass obstacle typically causes 3dB Wi-Fi signal attenuation.

- **Add APs -** Click on the down arrow to display a list of AP Models. Select an AP model from the list to move it into the AP field. Click on the AP Model to activate the field (field turns blue), then move the cursor to the floor plan and click to place the AP. Repeat to add additional APs.

Viewing Wi-Fi Coverage

After creating and customizing a floor plan, or using the "Auto Deployment" feature, the floor plan will display the Wi-Fi coverage quality within the floor plan. Wi-Fi coverage areas are displayed by color depending on the quality of the coverage, as shown in the figure below.



Wi-Fi Coverage Legend	
-20	Wi-Fi signal is stronger than -20dBm.
-30	Wi-Fi signal is stronger than -30dBm.
-40	Wi-Fi signal is stronger than -40dBm.
-50	Wi-Fi signal is stronger than -50dBm.
-60	Wi-Fi signal is stronger than -60dBm.
-70	Wi-Fi signal is stronger than -70dBm.
-80	Wi-Fi signal is stronger than -80dBm.
-90	Wi-Fi signal is stronger than -90dBm.

Editing a Floor Plan

You can edit the Address field of any floor plan in the Floor Plan List. Select the floor plan and click on the Edit icon. Edit the field and click on the **Apply** button.

> **Note:** To edit the elements in an existing floor plan (e.g., Walls, Cubicles, APs), select the floor plan in the Floor Plan List and click on the **Floor Map** button. Click on the "Edit Floor Plan" link in the Operation Pane. Edit any objects as described above, then click on the "Save The Layout" link in the Operation area of the Detail Panel.

Deleting a Floor Plan

Select a floor plan and click on the Delete icon. Click **OK** at the Confirmation Prompt.

Exporting a Floor Plan as a PDF

Select a Floor Plan in the Floor Plan list and click on the **Export PDF** button. The Floor Plan will be saved as a PDF and downloaded to your PC.

Floor Plan List

The Floor Plan List displays all configured floor plans.

- **Plan Name -** User-created name for the floor plan.
- **Quality -** The Wi-Fi quality level used when configuring an "Auto Deployment, if applicable.
- **AP Number -** The number of APs included in the floor plan.
- **Address -** Optional physical location and description for the floor plan.

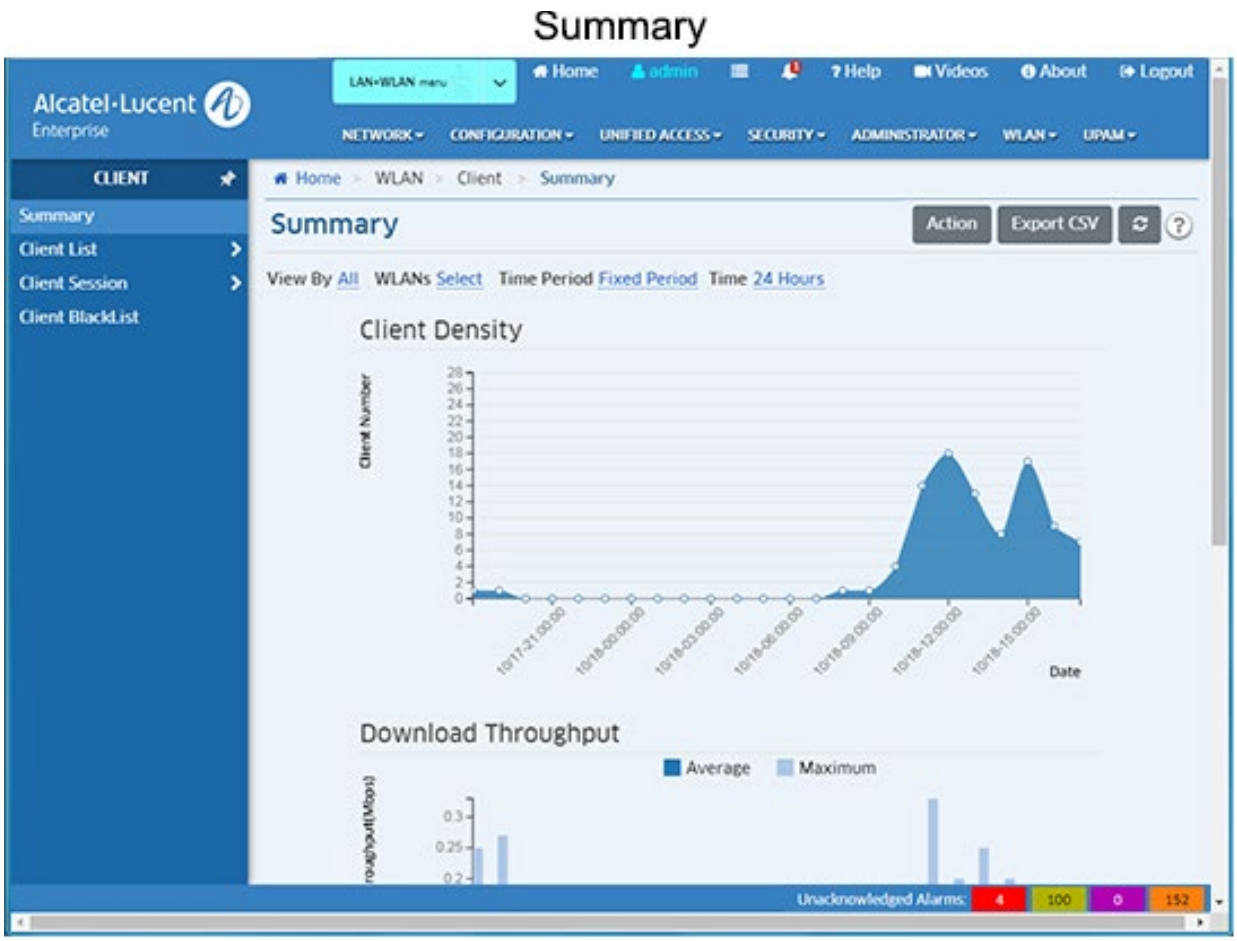
Client

The Client application can be used to view Client information and Client Blacklist information and to manually blacklist a Client.

Client Summary

The Client Summary Screen provides a graphical view of the number of clients and system throughput on your network. The following viewing options are available by clicking on one of the drop-down lists at the top of the page:

- **View By -** View information by AP/AP Group/Physical Map/Logical Map. Select "All" to view information for all APs. Select "APs", then select an AP to view information about a specific AP. Select "AP Group", then select an AP Group to view information about APs in a specific AP Group. Select "Physical Map", then select a physical map to view information about APs in a specific physical map. Select "Logical Map", then select a logical map to view information about APs in a specific logical map.
- **WLANs -** View the information by WLAN. Select "All" to view information for all WLANs; or select a specific WLAN from the drop-down. Note that deleted WLANs (SSIDs) may still be displayed in the drop-down since the data retention period may still be valid. These deleted WLANs (SSIDs) will be indicated with an (*) next to the WLAN (SSID) name.
- **Time Period -** View information for a specific time period. Select "Fixed Period" to view information for the time period configured in the "Time" drop-down. Select "Custom Period" to view information for a specific date range. The "Custom Period" is used to view historical data; you cannot configure dates in the future. The "Time" option is not available if you configure a Custom Period.
- **Time -** View information over different time periods (24 Hours, Last 7 Days, 30 Days, 90 Days). This option is available for a "Fixed Period".



Data is displayed in the following charts:

- **Client Density -** The number of clients connected to the network for the configured AP/AP Group and time period.
- **Download Throughput -** The average and maximum download throughput, in Mbps, for the configured AP/AP Group and time period.
- **Upload Throughput -** The average and maximum upload throughput, in Mbps, for the configured AP/AP Group and time period.

Wireless Client List

The Wireless Client List Screen displays real time information for wireless clients associated with APs. The Distribution of Clients per AP chart at the top of the screen provides a graphical overview of the number of clients associated with each AP. The All APs List provides information for each AP in the network. And the List of Clients on All APs provides information for all clients associated with an AP. It can also be used to manually "Blacklist" a client.

All APs List

- **AP Name -** Name of the AP.
- **Group Name -** The AP Group to which the associated AP belongs.
- **AP MAC -** The MAC address of the AP.

- **IP Address -** The IP address of the AP.
- **IP Mode -** The mode used to obtain the AP IP address (DHCP or Static).
- **Default Gateway -** The default gateway used for AP forwarding.
- **Subnet Address -** The IP subnet address of the AP.
- **AP Location -** The AP location currently assigned in the AP. There are two location modes:

  LLDP Mode (Default) - The location is retrieved from the LLDP ALE TLV.

  Fixed/User String Mode - The location is hard coded with a user sting.
- **Status -**The AP status:

  Up - AP is reachable.

  Down - AP is not reachable.

  Unknown - The AP has not been seen yet (AP was manually created/imported).
- **Registration Status -** The registration status of the AP (e.g., Normal).
- **Country Code -** The AP Country Code.
- **Management VLAN ID -** The VLAN used to manage the AP.
- **AP Model -** The model type of the AP (e.g., OAW-AP1221, OAW-AP1251).
- **AP Version -** The AP OS version.
- **RF Profile -** The RF Profile applied to the AP.
- **Client Count -** The number of clients currently connected to the AP.
- **Neighbor AP -** The neighbor AP to which the connected wireless client might roam.
- **Saved/Unsaved -** Indicates whether or not the current AP configuration has been saved to OmniVista (Saved/Unsaved).
- **LED Model -** The LED Mode configured for the AP.
- **DNS -** The IP address of the DNS Server used by the AP.
- **Channel -** The radio frequency working channel for the AP.
- **EIRP -** The Effective Isotopically Radiated Power radio frequency for the AP.
- **LACP Status -** Indicates whether or not the AP supports link aggregation (Supported/Unsupported).
- **Link Status -** The LACP link status (Up/Down).
- **Work Mode -** The AP Work Mode:
- **AP Mode -** AP serving wireless clients
- **Mesh Mode -** AP is working as a wireless mesh node.
- **Bridge Mode -** AP is working as a wireless bridge node.

List of Clients on All APs

- **Client Name -** The name of the client. It is derived from the client's system.
- **Group Name -** The name of the AP Group to which the associated AP belongs.
- **AP MAC -** The MAC address of the AP to which the client associated.
- **Associated SSID -** The WLAN to which the client is associated.
- **Working Mode -** The wireless working mode of the client.

- **Attached Band -** The radio band through which the client attached to the AP (2.4GHz or 5GHz). **Client MAC -** The MAC address of the client.
- **Client IP -** The IP address of the client.
- **Device Category -** The Client device type, including PC, Mobile, Tablet.
- **Device OS -** The operating system of the client.
- **AP Name -** The Name of AP to which the client associated.
- **Associate Time -** The time when the client associated to the wireless network.
- **Channel -** The working channel of the client.
- **RSSI -** The Received Signal Strength Indicator of the client (Range = 0 - 99).
- **Rx Total -** The total number of packets received by the client.
- **Tx Total -** The total number of packets sent by the client.
- **Rx Rate -** The packet receive rate of the client.
- **Tx Rate -** The packet sending rate of the client.
- **PHY Rx Rate -** The physical receive rate of the client.
- **PHY Tx Rate -** The physical sending rate of the client.
- **Access Role Profile -** The Access Role Profile applied to the client after authentication.
- **VLAN -** The VLAN through which the client accesses the network.
- **Tunnel -** The VPN Tunnel through which the client accesses the network. **Far End IP -** The IP address of the far end tunnel termination.

Blacklisting a Client

To blacklist a client, select the client(s) in the List of Clients on All APs and click on the Add to Blacklist button. Click OK at the Confirmation Prompt. The client will no longer be able to access the network and will be displayed on the Client Blacklist Screen.

Wired Client List

The Wired Client List Screen displays real time information for wired clients associated with APs. By default, all wired clients are displayed in the list. Click on the "Filter" link and select a criteria to filter the list of clients (e.g., Group Name, Client IP, Physical Map).

- **User Name -** The user name of the client (802.1X or Captive Portal users only).
- **Group Name -** The AP Group to which the associated AP belongs.
- **AP MAC -** The MAC address of the AP.
- **Access Role Profile -** The Access Role Profile applied to the client after authentication.
- **Access Auth Profile -** The Access Authentication Profile applied to the client after authentication.
- **VLAN ID -** The VLAN to which the client is assigned.
- **Client MAC -** The MAC address of the client.
- **Client IPv4 Address -** The IPv4 address of the client, if applicable.
- **Client IPv6 Adress -** The IPv6 address of the client, if applicable.
- **Port -** The port through which the client connected to the network.

- **Port Name -** The name of port through which the client connected.
- **Auth Type -** The user authentication type (8021X, Portal, MAC, None).
- **Online Time -** The length of time the client has been online.
- **Rx Bytes -** The client receive traffic, in bytes.
- **Tx Bytes -** The client transmit traffic, in bytes.

Wireless Client Session

The Wireless Client Session Screen displays information about current wireless clients associated with APs. By default, all wireless client sessions are displayed in the list. Click on the "Filter" link and select a criteria to filter the list of clients (e.g., Group Name, Client IP, Physical Map). You can also filter all sessions by date range by selecting "All" in the filter and setting a time range. The screen can also be used to show the roaming history of a client and its signal strength, and export the Wireless Client Session List to a .csv file.

- **User Name -** The user name of the client. It is derived from the client's system.
- **Group Name -** The name of the AP Group to which the associated AP belongs.
- **AP MAC -** The MAC address of the AP to which the client associated.
- **Associated SSID -** The WLAN to which the client is associated.
- **Working Mode -** The wireless working mode of the client.
- **Attached Band -** The radio band through which the client attached to the AP (2.4GHz or 5GHz).
- **Client MAC-** The MAC address of the client.
- **Client IP -** The IP address of the client.
- **Device Category -** The Client device type, including PC, Mobile, Tablet.
- **Device OS -** The operating system of the client.
- **VLAN -** The VLAN to which the client is assigned.
- **AP Name -** The Name of AP to which the client associated.
- **Associate Time -** The date and time when the client associated to the wireless network.
- **Online Time -** The amount of time the client was connected to the wireless network.
- **Channel -** The working channel of the client.
- **RSSI -** The Received Signal Strength Indicator of the client (Range = 0 - 99).

Show Roaming History for a Client

To display roaming data for a client, select a client in the list and click on the **Show Roaming and RSSI History** button. A graphical history of the client's signal strength is displayed. By default, the past 24 Hours is displayed. Click on the **Time Period** field at the top of the screen to view data for the past 3 days. Use the slider at the bottom of the scree for a more detailed view of a specific time period. Click on the **Show Client Session List** button at the top of the screen to return to the original screen view.

> **Note:** To collect roaming data for a client, the following traps must be configured on APs: **apStationAssociation** and **apStationDeassociation**. Go to the Notifications application and configure the traps (Network - Notifications - Trap Configuration). See the Trap Configuration online help for more information.

Exporting The Wireless Client Session List

You can export the Wireless Client Session List to a CSV File. Click on the **Export** button and select **All** or **Current**.

Wired Client Session

The Wired Client Session Screen displays information about current wired clients associated with APs. By default, all wired client sessions are displayed in the list. Click on the "Filter" link and select a criteria to filter the list of clients (e.g., Group Name, Client IP, Physical Map).

- **User Name -**The user name of the client (802.1X or Captive Portal users only).
- **Group Name -**The AP Group to which the associated AP belongs.
- **AP MAC -**The MAC address of the AP.
- **Access Role Profile -** The Access Role Profile used to authenticate the client.
- **Access Auth Profile -** The Access Authentication Profile used to authenticate the client.
- **VLAN ID -** The VLAN to which the client is assigned.
- **Client MAC -** The MAC address of the client.
- **Client IP -** The IP address of the client.
- **Port -** The port through which the client connected to the network.
- **Port Name -** The name of port through which the client connected.
- **Auth Type -** The user authentication type (8021X, Portal, MAC, None).
- **Connect Time -** The time when the client connected to the network.
- **Online Time -** The length of time the client has been online.

Client Blacklist

The Client Blacklist Screen displays information about all clients that have been blacklisted. It is also used to manually add clients to the Blacklist.

Client Blacklist

- **Client MAC -** MAC address of the client in the blacklist.
- **Start Date -** The starting date for the blacklisting. During the duration, the client is not allowed to access to the wireless network.
- **Expiry Date -** The expiration date for the blacklisting. The client can access the wireless network after the expiration date.
- **Reason -** The reason why the client was added to blacklist.

  Manually Add - Added into the Blacklist by the user.

  Garbing Legal Accessing Client - Dynamically added by the WIPS policy.

  Signal Strength is Too Strong, Reducing Network Performance - Dynamically added by the WIPS policy.

  Channel Switching Too Often - Dynamically added by the WIPS policy.

  Broadcasting Conflicted SSID, Misleading User Connection - Dynamically added by the WIPS policy.

  Matching the Keyword of Suspected SSID - Dynamically added by the WIPS policy.

Matching the Suspected MAC OUI - Dynamically added by the WIPS policy.

Have Attacking Behavior - Dynamically added by the WIPS policy.

- **Status -** Indicates whether the blacklist policy effective date has expired.

Manually Adding a Client to the Blacklist

Click on the Add icon to bring up the Add Client to Blacklist window. Enter the client's MAC address, then click on the **Apply** button. Repeat to add additional clients.

Deleting a Client from the Blacklist

Select the client(s) in the Blacklist and click on the Delete icon. Click **OK** at the confirmation prompt.