



# Alcatel-Lucent OmniVista 2500 UPAM and Fortinet Single Sign-On Application Note

March 2021

**Application Note**

OmniVista 2500 UPAM and Fortinet Single Sign-On

Alcatel-Lucent   
Enterprise

## Table of Contents

About this Application Note.....	3
The Zero-Trust paradigm.....	3
About Fortinet Single Sign-On.....	3
About OmniVista 2500 UPAM.....	3
Use case.....	4
Mechanism.....	5
Procedure overview.....	5
OmniVista: Registering the FortiGate or FortiAuthenticator as a RADIUS Server .....	6
OmniVista: Configuring the AAA profile.....	7
OmniVista: Configuring UPAM Access Policy and Authentication Strategy.....	8
OmniVista: Configuring and applying the Access Auth Profile.....	9
Fortinet: Enabling RADIUS Accounting on the Network Interface .....	10
Fortinet: Creating a RADIUS Single Sign-On connector .....	11
Fortinet: Specifying RADIUS Attributes for User-Name and Role (Filter-Id).....	12
Fortinet: Creating user groups .....	13
Fortinet: Creating role-based firewall rules.....	14
Fortinet: Verifying user and role mappings.....	15
Fortinet: Verifying user-based policies .....	16
Conclusion.....	17

## About this Application Note

The purpose of this application note is to help Alcatel-Lucent Enterprise Business Partners and customers integrate the Alcatel-Lucent OmniVista® 2500 Unified Policy Authentication Management (UPAM) with the Fortinet next-generation firewall single sign-on feature. With this integration, users or devices authenticated to the LAN and/or WLAN networks can also be simultaneously and seamlessly authenticated to the Fortinet firewall. Alcatel-Lucent OmniVista 2500 UPAM can share user or device connection status, as well as identity or role information, with the firewall for enhanced visibility, finer policy control and improved logging, reporting and forensic analysis. In the sample runs the code segment is now different between runs.

## The Zero-Trust paradigm

In a legacy firewall, the “trust” boundary is based on the point of connection: “inside” users are implicitly trusted and “outside” users are not. In an airport analogy, this would be equivalent to allowing land-side passengers to go through security unchecked. With trends such as mobility and Internet of Things (IoT), that notion of “trust” is completely outdated. For example: a Bring Your Own Device (BYOD) may bring malware into the organization, an IoT device may be intrinsically vulnerable and become an attack vector, and even corporate users could be outright malicious.

**The paradigm today is “Zero Trust”: No matter where the user or device is connected, never trust and always verify.** Establishing identity is at the core of the zero-trust paradigm.

Going back to the airport analogy, the first thing an immigration officer will do is check the passport. Other checks such as visa check, database checks and so on, are done after identity is established using a passport, a matching fingerprint, among others. And, since establishing identity is a fundamental check at the core of the zero-trust paradigm, next-generation firewalls have multiple mechanisms to determine identity.

## About Fortinet Single Sign-On

Fortinet Single Sign-On (FSSO) is a mechanism by which users can transparently authenticate to FortiGate, FortiAuthenticator, and FortiCache devices. Users are identified to the Fortinet device based on their authentication to a third system. Knowing users’ identities and/or roles, rather than just their IP address, provides several benefits. These include: improved visibility into usage patterns, finer policy control by only allowing application and/or resource access to those users/roles with a legitimate need for it (principle of least privilege). It also allows for enhanced logging, reporting and forensics by referencing the user identity or role rather than just the IP address. Please refer to Fortinet documentation for further information on the FSSO feature.

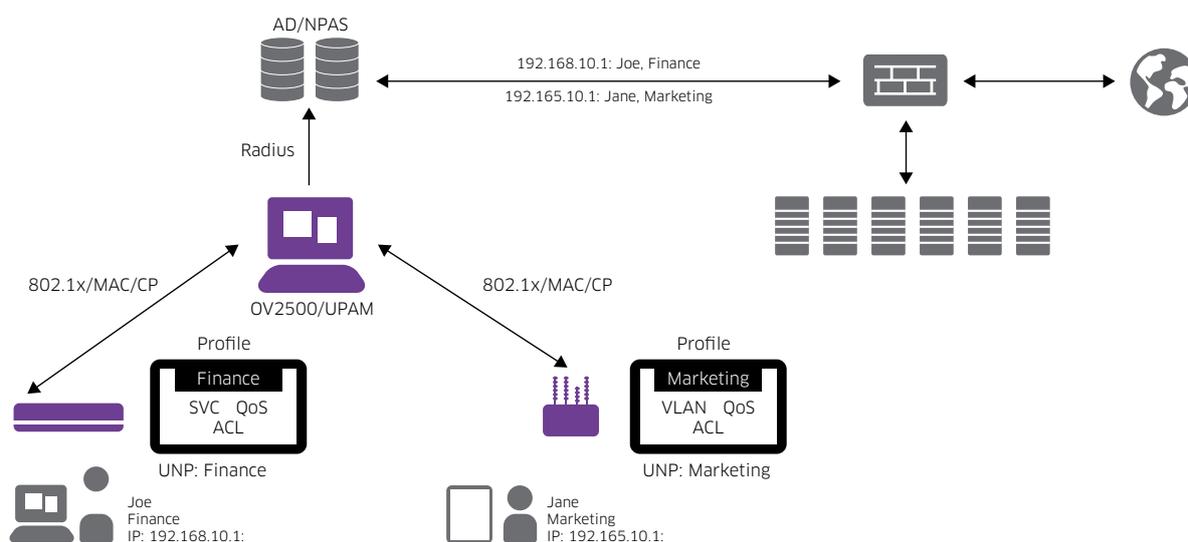
## About OmniVista 2500 UPAM

The Alcatel-Lucent OmniVista 2500 Unified Policy Authentication Management module is a unified access management platform for Alcatel-Lucent OmniSwitch® Ethernet switches, and Alcatel-Lucent OmniAccess® Stellar access points. OmniVista 2500 UPAM includes both a captive portal and a RADIUS server and can implement multiple authentication methods such as MAC authentication, 802.1x authentication, and captive portal authentication. Users can authenticate against the UPAM local database or against external databases including Microsoft Active Directory, LDAP, and external RADIUS. **The OmniVista 2500 UPAM customizable captive portal can implement flexible authentication strategies for Guest and BYOD users with integrated credential management through email, SMS and social login (for example, Facebook, Google, WeChat and Rainbow™ by Alcatel-Lucent Enterprise).**

## Use case

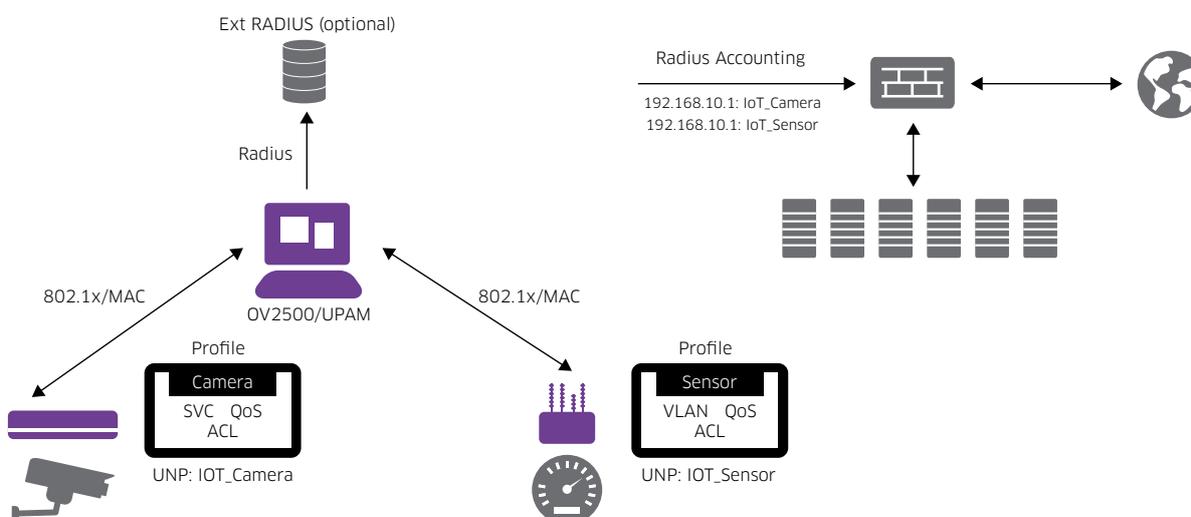
There are two main use cases when it comes to wired and wireless users: Corporate (AD) devices, and BYOD or IoT devices. For corporate devices, such as a corporate user on a corporate laptop, OmniVista UPAM can proxy authentication to AD and the preferred point of integration is directly on AD, not on UPAM. This application note will not elaborate further on this use case. For details on the AD-based integration please refer to the Fortinet documentation.

Figure 1 - AD-Based Integration



In this document, we will focus on the second use case in **which a BYOD or IoT device is authenticated directly against the UPAM database or proxied to an external RADIUS database (other than Microsoft® Network Policy and Access Services or NPAS) because these devices may not be associated with an AD account.** This use case is shown in Figure 2, using IoT as an example. This document focuses on this use case because the point of integration is directly on the OmniVista 2500 UPAM.

Figure 2 - Radius Accounting-based Integration



### Application Note

## Mechanism

The AAA server profile is configured such that network devices authenticate users against the UPAM database (which can in turn proxy authentication to an external server) and send RADIUS accounting logs to either FortiGate or FortiAuthenticator. Sending logs to FortiAuthenticator is convenient in a deployment with multiple firewalls otherwise, multiple AAA profiles would be required. It's important to understand that accounting messages will be sent directly from the switch or access point and that they are not proxied by UPAM.

The FortiGate or FortiAuthenticator extracts username and role information from RADIUS accounting messages. Firewall policies can be based on the user's role instead of solely the IP address. Firewall logs also include username and role, not just the client's IP address.

Note, in this document we provide instructions on a FortiGate. However, when multiple FortiGates are associated to a FortiAuthenticator, RADIUS accounting messages can be sent to the FortiAuthenticator instead.

## Procedure overview

Following is a summary of the steps required on both OmniVista 2500 UPAM and the PAN firewall.

### OmniVista 2500 UPAM

1. Register the FortiGate or FortiAuthenticator as a RADIUS Server
2. Configure the AAA profile
3. Configure the UPAM Access Policy and Authentication Strategy
4. Create Access Auth profile for MAC/802.1x authentication against UPAM

### FortiGate

1. Enable RADIUS accounting on network interface
2. Create a RADIUS single sign-on connector
3. Specify RADIUS Attributes for username and role (filter-id)
4. Create user groups
5. Create role-based firewall rules
6. Verify user and role mappings
7. Verify user-based policies

## OmniVista: Registering the FortiGate or FortiAuthenticator as a RADIUS Server

In OmniVista, go to Security -> Authentication Server -> RADIUS and click “+”.

Complete the FortiGate or FortiAuthenticator IP or name, and shared secret.

Then click on “Create”.

**It's important to note that if you configure a name instead of an IP address, the switch or AP will need to resolve that address to an IP.** If the switch or AP does not have access to a DNS server, you should configure the IP address instead. In addition, since accounting messages flow directly from the network device, any intermediate firewall should be configured to allow this traffic (UDP port 1813).

Figure 3 - Registering the FortiGate or FortiAuthenticator as a RADIUS Server

The screenshot displays the 'Create RADIUS Server' configuration page in the Alcatel-Lucent Enterprise OmniVista web interface. The page is titled 'RADIUS Server Management' and 'Create RADIUS Server'. The configuration fields are as follows:

Field	Value
* Server Name	FortiGate
* Host Name/IP Address	10.0.0.1
Backup Host Name/IP Address	Enter Backup Host Name/IP Address (v4   v6)
Retries	3
Timeout	2
* Shared Secret	*****
* Confirm Secret	*****
Authentication Port	1812
Accounting Port	1813
VRF Name	default

At the bottom right, there are 'Create' and 'Cancel' buttons. A status bar at the bottom indicates 'Unacknowledged Alarms' with counts: 399 (red), 212 (yellow), 0 (green), and 471 (orange).

### Application Note

## OmniVista: Configuring the AAA profile

In OmniVista, go to Unified Access->Template->AAA Server Profile and click “+”.

Create a new AAA Server Profile pointing to the UPAMRADIUServer for Authentication and the newly registered FortiGate or FortiAuthenticator for Accounting. You will do this for the required authentication methods: 802.1x, MAC or Captive Portal. In the example below, only 802.1x and MAC are shown as IoT devices do not normally use Captive Portal authentication.

Figure 4 - AAA Server Profile – Authentication and Accounting

Authentication Servers		Accounting Servers	
<b>802.1X</b>			
802.1X Primary	UPAMRadiusServer	802.1X Primary	FortiGate
Secondary	Tertiary	Secondary	Tertiary
	Quaternary		Quaternary
<b>Captive Portal</b>			
Captive Portal Primary	Secondary	Captive Portal Primary	Secondary
	Tertiary		Tertiary
	Quaternary		Quaternary
<b>MAC</b>			
MAC Primary	UPAMRadiusServer	MAC Primary	FortiGate
Secondary	Tertiary	Secondary	Tertiary
	Quaternary		Quaternary

You may also specify the Accounting Interim Interval (600 seconds by default) or alternatively, trust the accounting interim interval set by the RADIUS server (UPAM or external) in which case, the accounting interim interval must be configured on the RADIUS server. In most cases, the first accounting message sent shortly after successful authentication will contain the device IP address and allow the firewall to identify the user. In other cases, however, the device IP address will only be present in the second and subsequent accounting messages. In such case, setting a lower interim interval will result in this information being updated quicker on the firewall.

Figure 5 - MAC - Accounting Interim Interval

Advanced Settings (Optional)

---

**MAC Auth**

Session Timeout Trust RADIUS Status:  DISABLED

Session Timeout Status:  DISABLED

Session Timeout Interval: 43200 second(s)

Inactivity Timeout Status:  DISABLED

Inactivity Timeout Interval: 600 second(s)

Accounting Interim Trust RADIUS Status:  DISABLED

Accounting Interim Interval: 600 second(s)

Syslog Accounting Server IP Address:

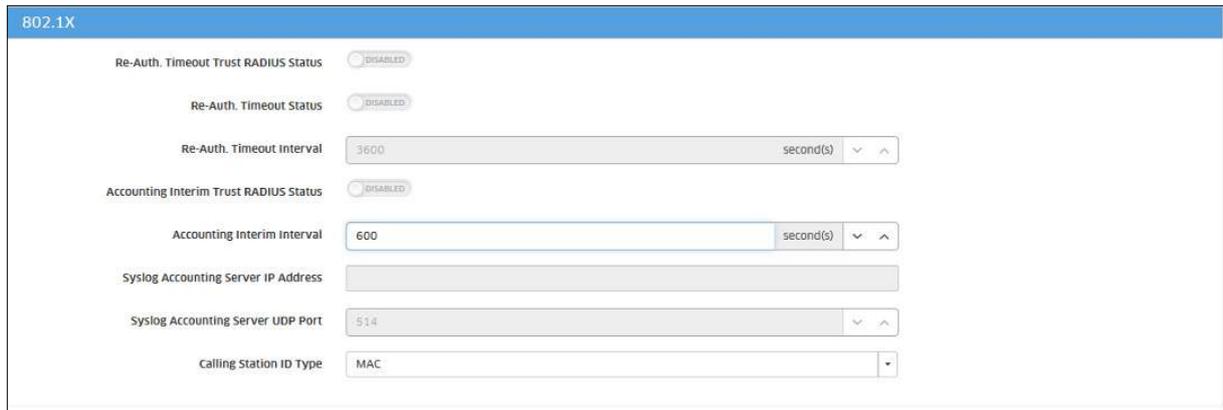
Syslog Accounting Server UDP Port: 514

Calling Station ID Type: MAC

### Application Note

OmniVista 2500 UPAM and Fortinet Single Sign-On

Figure 6 - 802.1x Accounting Interim Interval



The screenshot shows the configuration page for 802.1X. It includes several settings:

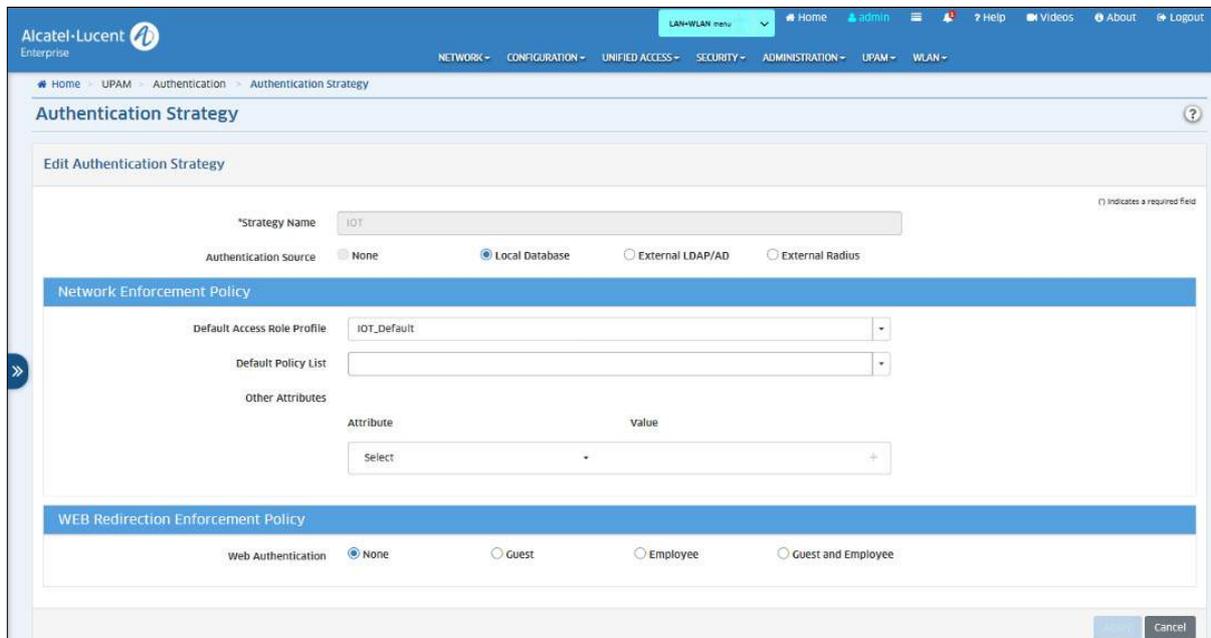
- Re-Auth. Timeout Trust RADIUS Status:  DISABLED
- Re-Auth. Timeout Status:  DISABLED
- Re-Auth. Timeout Interval: 3600 second(s)
- Accounting Interim Trust RADIUS Status:  DISABLED
- Accounting Interim Interval: 600 second(s)
- Syslog Accounting Server IP Address: (empty field)
- Syslog Accounting Server UDP Port: 514
- Calling Station ID Type: MAC

## OmniVista: Configuring UPAM Access Policy and Authentication Strategy

**As a reminder, the Authentication Strategy defines which authentication database will be used and other parameters while the Access Policy routes authentication requests to the right strategy based on criteria such as the SSID or the switch NAS IP.**

To create an Authentication Strategy, go to UPAM->Authentication->Authentication Strategy and click "+". A sample Authentication Strategy using the UPAM internal database is shown below. The default Access Role Profile (ARP) is the role to be applied in case no specific role is assigned to the device or the specified role is not locally defined on the switch or AP group. Note: The default ARP must be created before creating the Authentication Strategy. In addition, all relevant ARPs must be created and mapped to switches and AP groups. These steps will not be shown in this guide.

Figure 7 - Authentication Strategy



The screenshot shows the "Authentication Strategy" configuration page. It includes the following sections and settings:

- Edit Authentication Strategy**
- \*Strategy Name: IOT
- Authentication source:  Local Database,  External LDAP/AD,  External Radius
- Network Enforcement Policy**
- Default Access Role Profile: IOT\_Default
- Default Policy List: (empty field)
- Other Attributes: (empty table with columns Attribute and Value)
- WEB Redirection Enforcement Policy**
- Web Authentication:  None,  Guest,  Employee,  Guest and Employee

To create an Access Policy, go to UPAM->Authentication->Access Policy and click "+". The Access Policy maps authentication requests to the previously created Authentication Strategy based on criteria such as SSID (shown in the example), NAS IP, Location.

### Application Note

**Figure 8 - Access Policy**

The screenshot shows the 'Edit Access Policy' configuration page in the Alcatel-Lucent Enterprise web interface. The breadcrumb navigation is Home > UPAM > Authentication > Access Policy. The page title is 'Access Policy'. Below the title is a sub-header 'Edit Access Policy'. The configuration fields are as follows:

- \*Policy Name:** IOT
- \*Priority:** 4
- \*Mapping Condition:** Basic Attribute (selected), Advanced Attribute (unselected)
- Attribute Operator Value Table:**

Attribute	Operator	Value
SSID	Equals	IoT
- \*Authentication Strategy:** IOT

Buttons for 'Apply' and 'Cancel' are located at the bottom right. A note indicates that an asterisk (\*) denotes a required field.

## OmniVista: Configuring and applying the Access Auth Profile

Go to Unified Access-> Unified Profile -> Templates -> Access Auth Profile and click on “+”. Select the previously defined UPAM AAA Server Profile and configure MAC/802.1x authentication options as required. The example below shows MAC authentication with the “IOT\_Default” profile used as the default and pass-alternate (used when the returned attribute does not match a locally defined profile on the switch or AP group). When done, apply it to the required switches and AP groups.

**Figure 9 - Access Auth Profile**

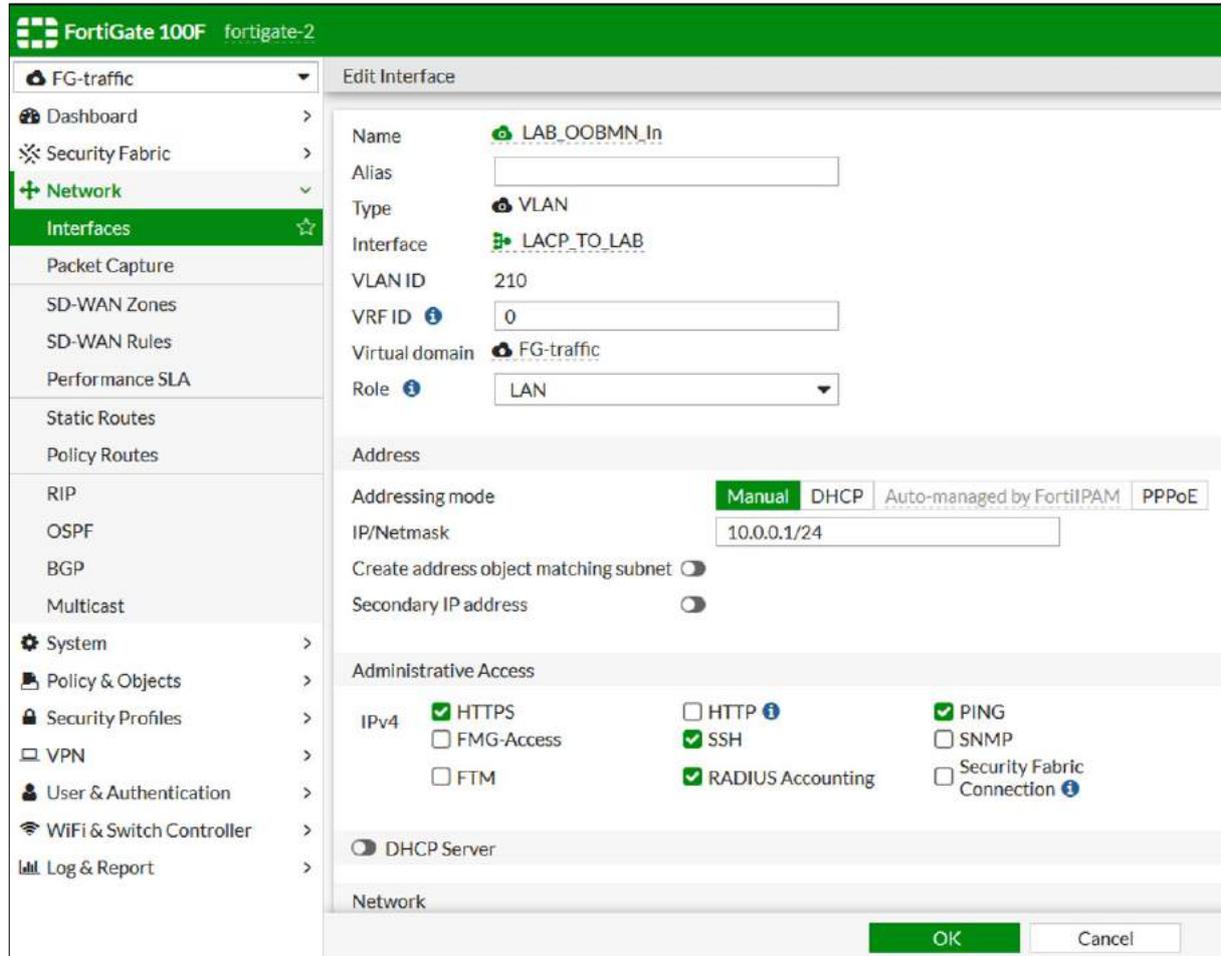
Default Settings		No Auth/Failure/Alternate	
AAA Server Profile	AAAProfile	Trust Tag	Enable
Port-Bounce	Enable	Access Classification	Disable
MAC Auth	Enable	Default Access Role Profile	IOT_Default
802.1X Auth	Enable	<b>802.1X Authentication</b>	
Customer Domain ID	0	802.1X Pass Alt	
		By-pass Status	Disable
		Failure Policy	Default
		<b>MAC Authentication</b>	
		MAC Pass Alt	IOT_Default
		MAC Allow EAP	None

### Application Note

## Fortinet: Enabling RADIUS Accounting on the Network Interface

In the FortiGate firewall, go to Network->Interfaces, and double click on the interface that will receive RADIUS accounting messages. In the Administrative Access section, select the RADIUS Accounting checkbox and click "OK". The interface will start listening on port 1813 and be ready to receive the RADIUS accounting messages.

Figure 10 - Enabling RADIUS Accounting on Network Interface



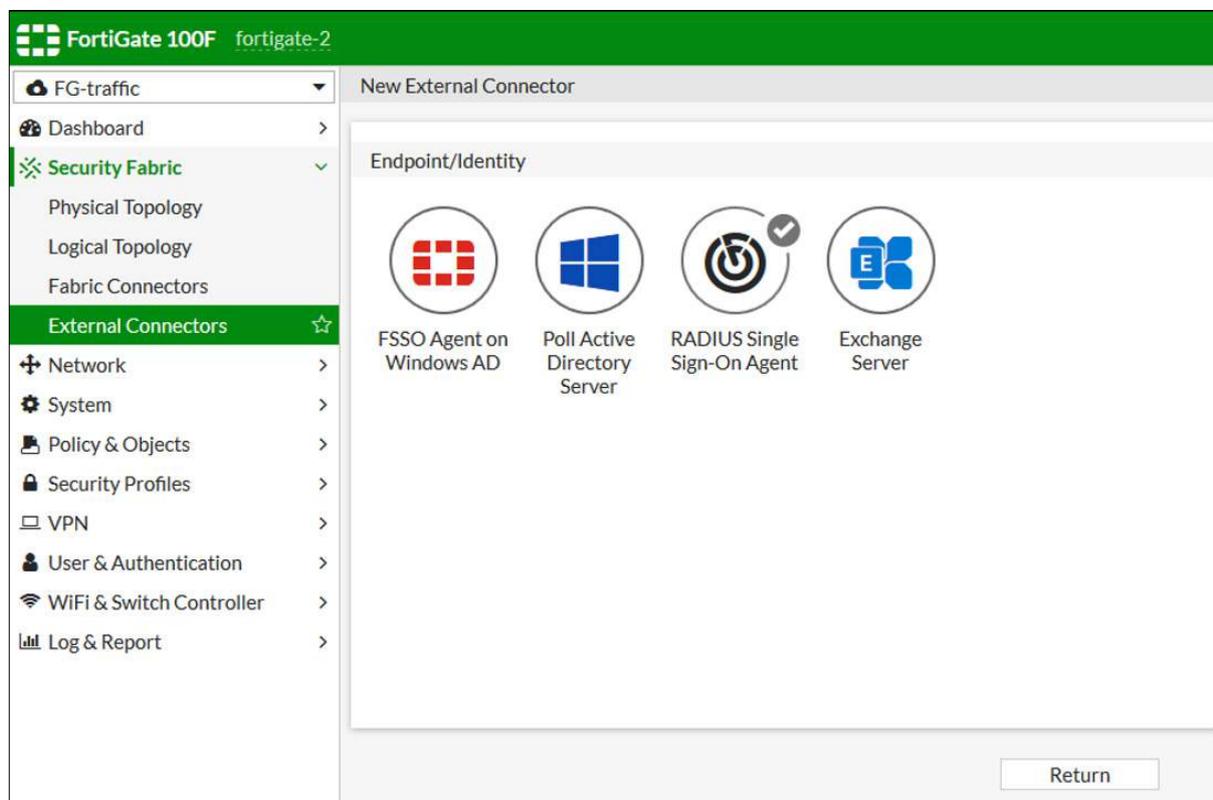
### Application Note

OmniVista 2500 UPAM and Fortinet Single Sign-On

## Fortinet: Creating a RADIUS Single Sign-On connector

In the FortiGate firewall, go to Security Fabric -> External Fabric Connectors. Click “Create New”. Select “RADIUS Single Sign-On Agent”.

Figure 11 - Creating RSSO external connector

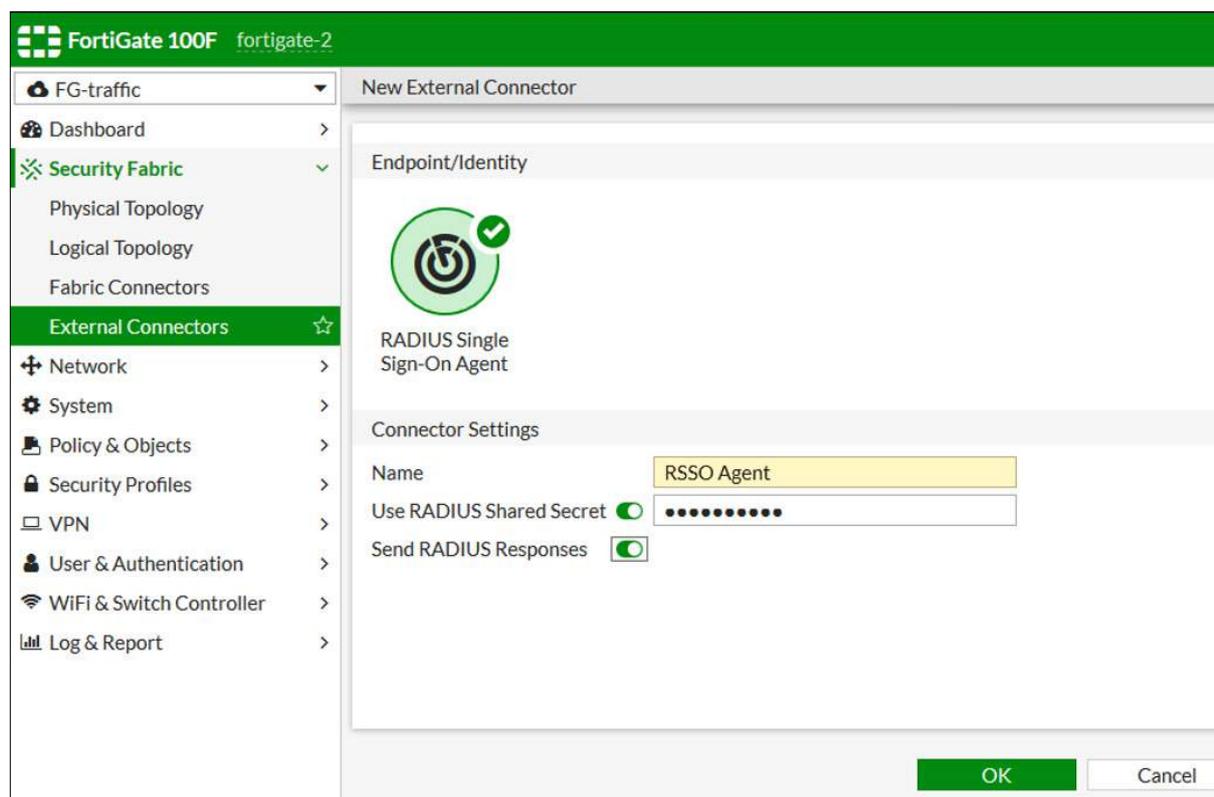


Create an RSSO Agent name. Select “Use RADIUS Shared Secret” and enter the same key that was defined in the OmniVista (Step 1). Enable “Send RADIUS responses” and click “OK”.

### Application Note

OmniVista 2500 UPAM and Fortinet Single Sign-On

Figure 12 - Configuring RSSO Agent



## Fortinet: Specifying RADIUS Attributes for User-Name and Role (Filter-Id)

This step must be completed through the CLI. SSH to the firewall and edit the RADIUS SSO connector as shown in the image below.

Figure 13 - Specifying RADIUS Attributes for User-Name and Role (Filter-Id)

```
fortigate-2 # config vdom
fortigate-2 (vdom) # edit FG-traffic
current vf=FG-traffic:1
fortigate-2 (FG-traffic) # config user radius
fortigate-2 (radius) # edit RSSO\ Agent
fortigate-2 (RSSO Agent) # set rso-endpoint-attribute User-Name
fortigate-2 (RSSO Agent) # set sso-attribute Filter-Id
fortigate-2 (RSSO Agent) # end
fortigate-2 (FG-traffic) #
```

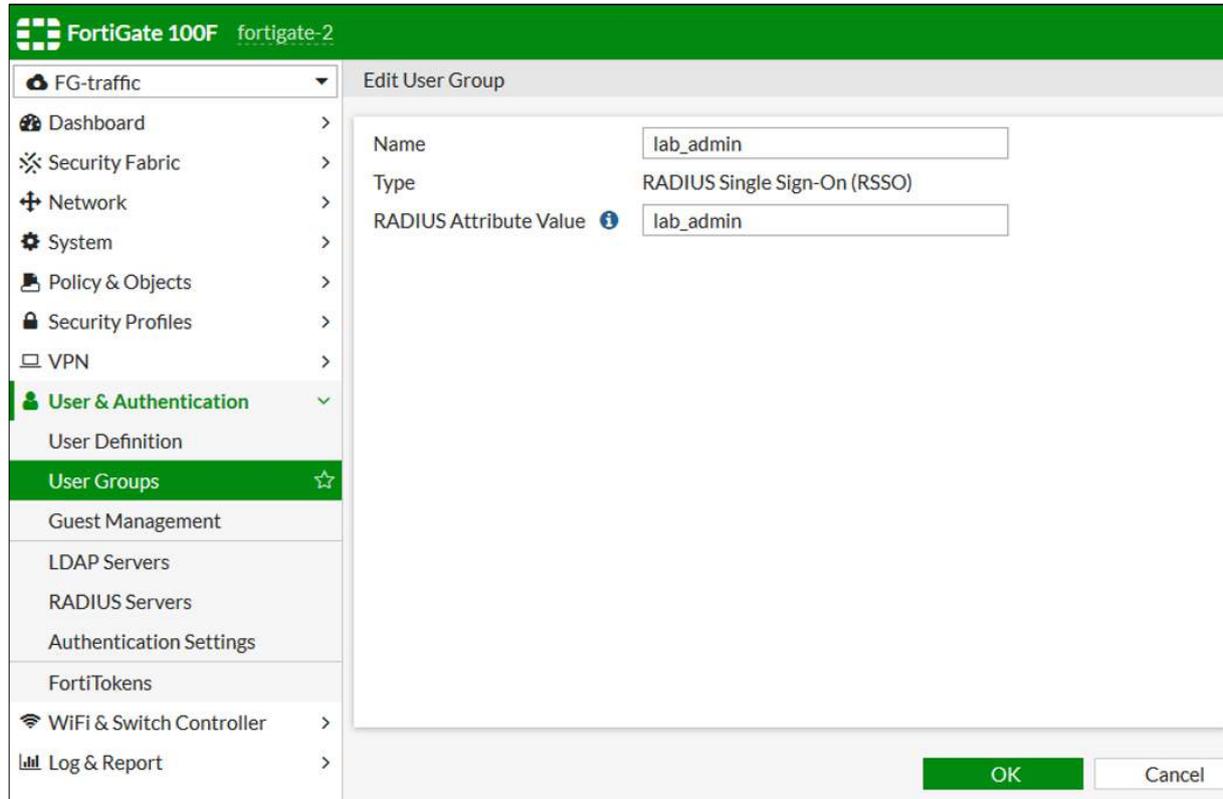
### Application Note

OmniVista 2500 UPAM and Fortinet Single Sign-On

## Fortinet: Creating user groups

In the firewall, go to User & Authentication->User Groups, and click on “Create New”. Enter a group for the name and select “RADIUS Single Sign-On (RSSO)” type. In the “RADIUS Attribute Value” textbox, enter the value of the Access Role Profile associated to the user role in the UPAM database or on an external RADIUS server. This value is the Filter-Id. Click “OK” and repeat as required for other roles.

Figure 14 - Creating user groups



### Application Note

OmniVista 2500 UPAM and Fortinet Single Sign-On

## Fortinet: Creating role-based firewall rules

In the firewall, go to Policy & Objects -> Firewall Policy, and click on “Create New”. Define the required policy attributes. In the “Source” drop-down menu, select the source address, or address object, and the user group or groups created in the previous step. Complete all other fields as required and click “OK”.

Figure 15 - Creating role-based firewall policies

The screenshot displays the 'New Policy' configuration interface in the FortiGate 100F management console. The left sidebar shows the navigation menu with 'Policy & Objects' and 'Firewall Policy' selected. The main configuration area includes the following fields and options:

- ID:** 0
- Name:** lab\_admin\_policy
- Incoming Interface:** (empty dropdown)
- Outgoing Interface:** (empty dropdown)
- Source:** List containing 'all' and 'lab\_admin' with a '+' button to add more.
- Negate Source:**
- Destination:** (empty dropdown with '+')
- Negate Destination:**
- Schedule:** always
- Service:** (empty dropdown with '+')
- Action:**  ACCEPT,  DENY,  IPsec
- Inspection Mode:** Flow-based (selected), Proxy-based
- Firewall / Network Options:**
  - NAT:**
  - IP Pool Configuration:** Use Outgoing Interface Address (selected), Use Dynamic IP Pool
  - Preserve Source Port:**
  - Protocol Options:** PROT default

At the bottom right, there are 'OK' and 'Cancel' buttons.

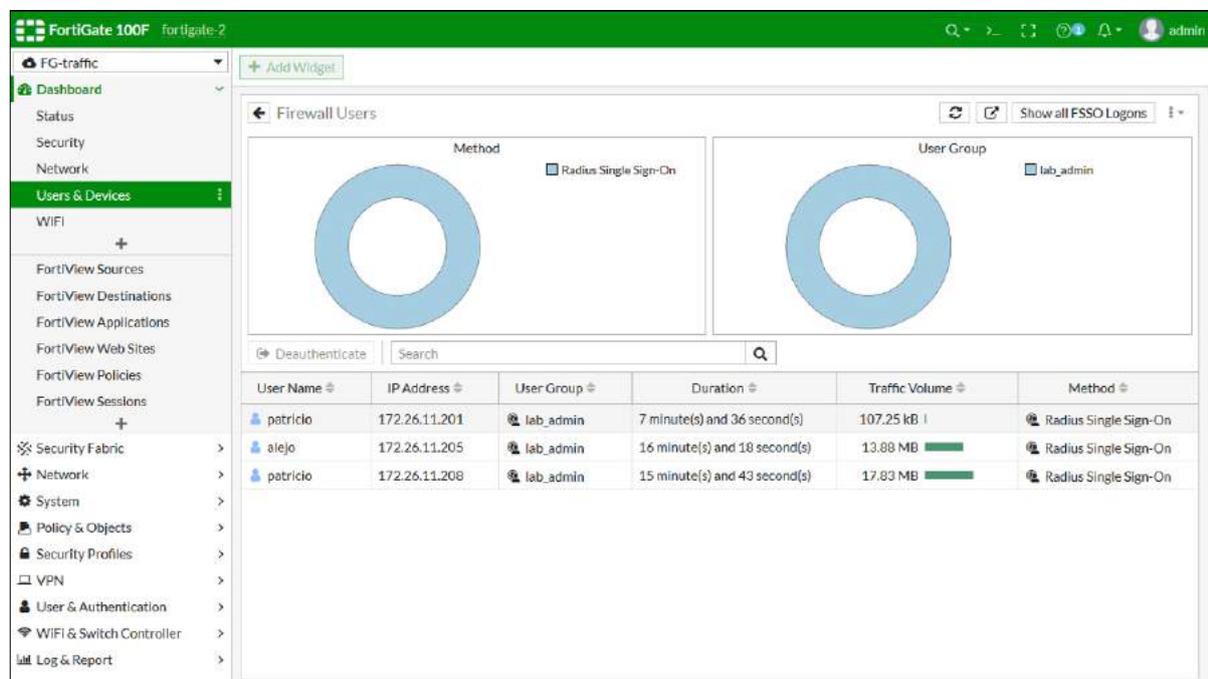
### Application Note

OmniVista 2500 UPAM and Fortinet Single Sign-On

## Fortinet: Verifying user and role mappings

User mappings can be verified through the GUI by going to Dashboard->Users & Devices->Firewall Users.

Figure 16 - Verifying user and role mappings through the GUI



In addition, user and role mappings can be verified through the CLI by entering the “diagnose firewall auth list” command.

### Application Note

Figure 17 - Verifying user and role mappings through the CLI

```

fortigate-2 # config vdom
fortigate-2 (vdom) # edit FG-traffic
current vf=FG-traffic:1
fortigate-2 (FG-traffic) # diagnose firewall auth list

172.26.11.201, patricio
  type: rso, id: 0, duration: 1591, idled: 97
  flag(10): radius
  server: FG-traffic
  packets: in 553 out 565, bytes: in 99975 out 266364
  group_id: 1
  group_name: lab_admin

172.26.11.205, alejo
  type: rso, id: 0, duration: 2113, idled: 18
  flag(10): radius
  server: FG-traffic
  packets: in 33634 out 5276, bytes: in 48946319 out 828224
  group_id: 1
  group_name: lab_admin

172.26.11.208, patricio
  type: rso, id: 0, duration: 2078, idled: 0
  flag(10): radius
  server: FG-traffic
  packets: in 34496 out 48305, bytes: in 6345602 out 61457853
  group_id: 1
  group_name: lab_admin

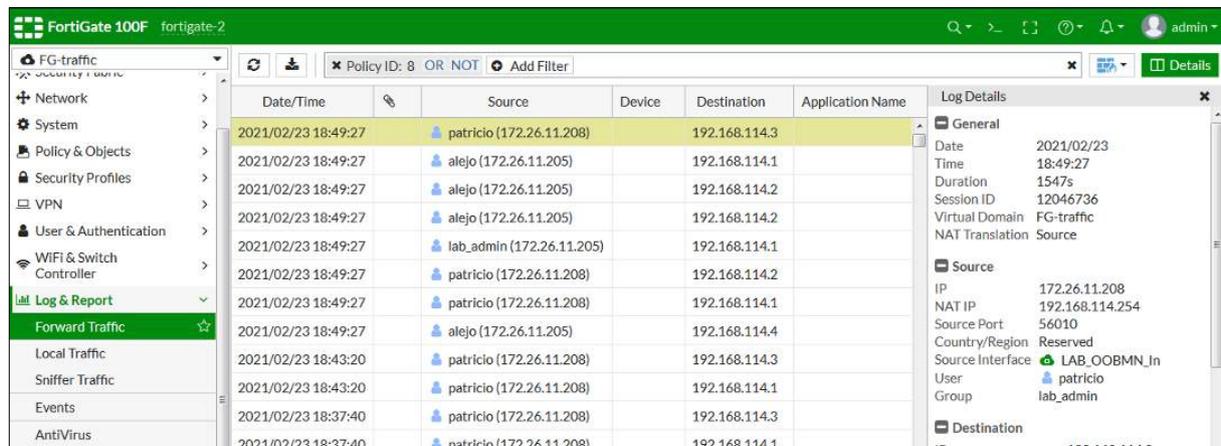
----- 3 listed, 0 filtered -----

```

## Fortinet: Verifying user-based policies

To verify that firewall policies are identifying users correctly, go to Log & Report -> Forward Traffic. Configure a filter if required. Select an entry and verify that user and group are identified correctly on the right side panel.

Figure 18 - Verifying user-based policies



### Application Note

OmniVista 2500 UPAM and Fortinet Single Sign-On



## Conclusion

**Integrating OmniVista 2500 UPAM with Fortinet's SSO feature provides better visibility into wired and wireless users and devices and the resources and applications that they consume.**

It enables finer control, by allowing access only to those users and devices with a legitimate business need, thus reducing the attack surface. Logging and reporting is enhanced with user and role information.

Reporting can be improved by filtering activity for a specific user, role, or device, and forensic analysis can quickly identify the username or role, not just the IP address.

