UCOPIA

TURN YOUR WI-FI UP

Out-Of-Band Alcatel-Lucent Enterprise OmniAccess Stellar architecture

Table of contents

Table of figures

1 Introduction

This document describes the Out-of-Band architecture with Alcatel-Lucent Enterprise OmniAccess Stellar Access Points (AP) on premise. This architecture is composed of a central controller (Advance license), and OmniAccess Stellar AP(s) that are connected to the central controller. The central controller is typically in a datacentre, and the APs at customer sites (e.g. hotel, restaurant, agency, etc.).

The goal of the Out-of-Band architecture is to build a centralized architecture over your existing OmniAccess Stellar Wi-Fi infrastructure, allowing centralized management of the main UCOPIA features: captive portals, authentication server, provisioning, user directory, user logs' traceability but without the need to centralize user traffic. The local Internet access of each site is used for the user traffic.

The on premise OmniAccess Stellar APs ensure portal redirection to the centralized UCOPIA controller, authentication process, and redirection of the user traffic's logs.
The central controller can be a high availability cluster (Advance product line).

The following schema presents the global Out-of-Band OmniAccess Stellar architecture.

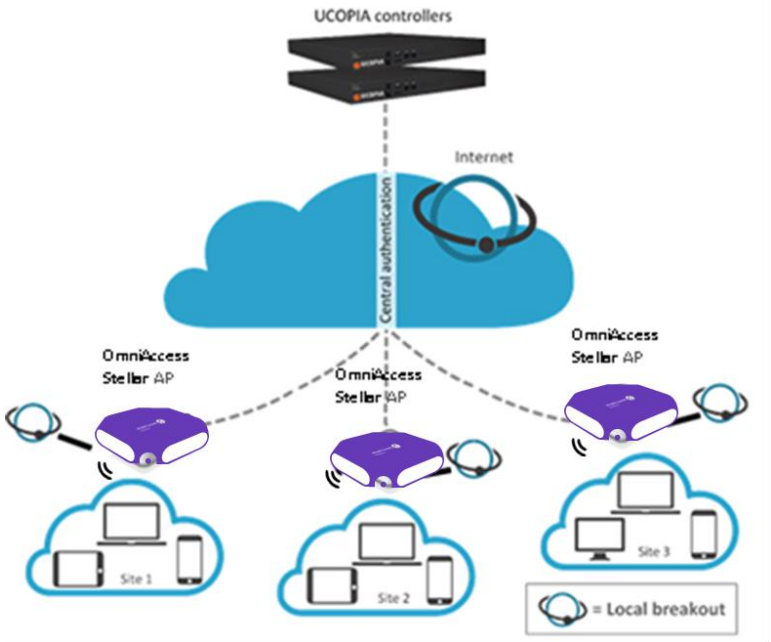

Figure 1 : Global Out-of-Band OmniAccess Stellar architecture

2 User experience workflow

Let's consider a Guest user trying to get a Wi-Fi Internet connection on a site (site A) where an OmniAccess Stellar AP is installed. The user will use the captive portal to connect with SMS registration.

The workflow is as follows:

1. Once associated to the Wi-Fi, the user launches his (her) Web browser.
2. The OmniAccess Stellar AP detects that the user is not connected yet and redirects him to the central controller. The URL used for the redirection contains the name of the zone associated to the site A.
3. The central controller displays the portal associated to the zone corresponding to the site A.
4. The user fills in the form (phone number, etc.), receives his (her) credentials by SMS and connects on the portal.
5. The request is analysed by the central controller. If the credentials entered by the user are correct, the authentication process is performed between the OmniAccess Stellar AP and the central controller through the RADIUS protocol.
6. Once the user is authenticated, he can browse using the local Internet access (on the site A).

The user traffic flow is summarized by the following schema.

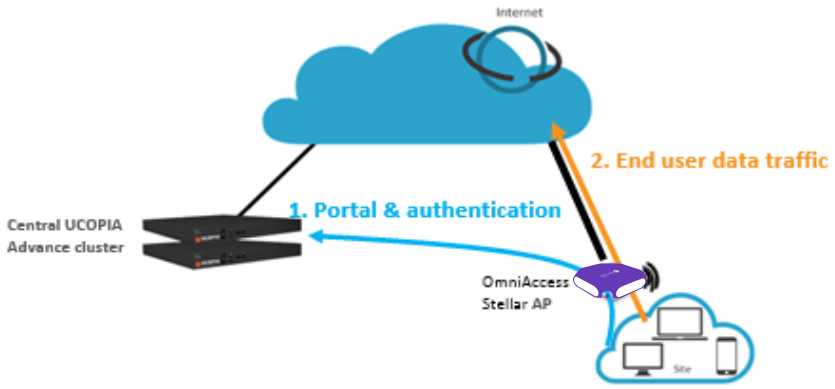

Figure 2 : User traffic flow

3 Advantages and recommendations

3.1 Advantages

3.1.1 Centralization of the user directory

User accounts are centralized on the central controller. The architecture allows a user to login with the same account on all sites and ensures the user roaming function.

3.1.2 Centralization of captive portals

Captive portals are centralized and therefore configured on the central controller.

The modification of a captive portal on the central site is taken into account for all sites. Of course, it's also possible to have a specific portal for one site or a group of sites.

3.1.3 Centralization of user profiles

UCOPIA user profiles are configured and centralized on the central controller.

- When an unauthenticated user comes on the network and tries to connect, the UCOPIA controller checks his validity settings, the time- and device- based criteria of the profile, and also the allowed zones.

- If the user is successfully connected, the UCOPIA controller sends some information to the OmniAccess Stellar AP via RADIUS exchanges such as the profile name, the expiration date, the session timeout in case of time credit so that the AP can enforce time validity checking before letting the user access the network.

3.1.4 Local Internet breakout

Each local site uses its own Internet access for connecting users and avoids to centralize the user traffic toward the central Internet access.

3.2 Restrictions and recommendations

3.2.1 Supported OmniAccess Stellar APs and UCOPIA versions

The Out-Of-Band OmniAccess Stellar architecture requires access points in version 3.0.3.22 or higher, and UCOPIA controller version 5.1.13 or higher. OmniAccess Stellar WLAN can be deployed in Wi-Fi Express mode managed through a Web Interface or it can be deployed in Wi-Fi Enterprise mode wherein the APs are managed either from OmniVista 2500 NMS (on premise) or OV Cirrus (cloud platform). Integration with UCOPIA is supported in all modes of operation. In this document Wi-Fi Express mode is elaborated.

For user traffic logging in the central UCOPIA controller, OmniAccess Stellar access points require firmware version 3.0.6.27 or higher, and UCOPIA controller requires version 6.0.2 or higher.

3.2.2 Supported authentication / registration modes

With the Out-Of-Band OmniAccess Stellar architecture, most authentication / registration modes are available, with a few exceptions or limitations listed below:

- 802.1x
- Shibboleth
- Automatic connection
- Limited email registration as users have to wait for the end of their session with temporary profile to be able to either click on the autoconnect/autofilllink or to enter their received credentials on the splash page
- Limited social network authentication as the customer must:
  → either control the DNS server that the end user devices will use and resolve “central.access.network” or “controller.access.network” with the IP address of his central UCOPIA controller
  → or change the domain name of his UCOPIA controller, create a new certificate and create his own social network application

3.2.3 Supported UCOPIA features on user management

As described in 3.1.3, during an authentication, the UCOPIA controller checks all the settings of the user account and its corresponding profile before allowing the user to get connected.

But, once connected, as the user traffic doesn’t go through UCOPIA, the OmniAccess Stellar AP is in charge with enforcing the policy on the user. However, the AP isn’t aware of the entire profile configuration on UCOPIA as only some information is sent by UCOPIA to the AP during the RADIUS exchanges. Here are the profile settings that can be enforced by AP:

- Time-based criteria:

- Time validity from creation/1st connection
- Preconfigured end date
- Time credit

Other configurations like authorized services, web filtering, limitation of bandwidth and quota are not sent by the UCOPIA to the OmniAccess Stellar AP.

3.2.4 User disconnection

Some disconnection mechanisms are not available in the Out-Of-Band OmniAccess Stellar architecture, as explained below:

	Supported in the Out-Of-Band OmniAccess Stellar architecture?
Increased security	**Yes,** if RADIUS accounting is enabled on the access point
UCOPIA automatic disconnection	**No** *Description: because user traffic doesn't go through the UCOPIA controller, the automatic disconnection feature doesn't make sense. So, as soon as an Out-Of-Band architecture is configured, the central controller disables its automatic disconnection feature.* *Only the automatic disconnect on the AP will be able to disconnect a user after a given network inactivity period.*
Manual disconnection	**No** *Description: The OmniAccess Stellar API doesn't allow such a disconnection request. The disconnection button is not displayed on the portal feedback page in this Out-Of-Band architecture.*
Reached max quota	**No**
Expired credit time	**Yes**
Reached ending validity date	**Yes**
Forced disconnection	**Yes**

3.2.5 Network failure

The user directory is centralized and used by all OmniAccess Stellar APs on local sites. In case of network failure between the APs and the central controller, the user directory and captive portal will not be available, so new users will not be able to connect. It is therefore recommended to set up a redundant cluster on the central site.

4 Licensing

The central UCOPIA controller handles the concurrent connections of all sites. Therefore, an ADVANCE license for managing multi-sites is needed.

You can configure a license limitation per zone or per profile to make sure that the mutualized license is not completely consumed by a given site.

5 Configuration

5.1 Prerequisites

5.1.1 Time synchronization

The central controller and OmniAccess Stellar AP should share the same time source. It is advised to use the NTP protocol for that purpose. OmniAccess Stellar AP can be configured in different time zones from one another and from the central controller.

On OmniAccess Stellar AP: configure the NTP server in “System > System Time”.

On UCOPIA: configure the NTP server in the administration interface “Configuration > Network > Time server”.

5.1.2 Communication between remote sites and central site (on UCOPIA and firewall)

The central controller has to be reachable by all the users on the remote sites as well as the remote OmniAccess Stellar APs (see Annex 1: detailed flow diagram). Local users reach the central portal through the Internet, which is available on the OUT interface. The central controller default route should use the OUT interface, or any OUT VLAN, to reach the Internet.

The ports used for the communication between the remote sites and the central site are the following.

Source	Destination	Port
User’s equipment on remote site	Central controller	TCP/443
OmniAccess Stellar AP	Central controller	TCP/443, UDP/1812, UDP/1813, UDP/514

5.1.3 Auto disconnection settings (on OmniAccess Stellar)

As the user traffic goes through the OmniAccess Stellar AP and not the UCOPIA controller, the AP is responsible for detecting an inactive user and disconnecting him. As soon as a device disassociate from a SSID, the AP will send a RADIUS Accounting-Stop message to inform the UCOPIA central controller that the session has to be ended.

5.2 Central controller configuration

Before starting the central controller configuration, check that the prerequisites are met (time server, routing and communication ports).

5.2.1 Zone

An incoming zone must be created for one or several remote sites and a portal must be associated to this zone. The profiles that are going to be used on these sites must allow this zone as available incoming zone. This zone will be used in the redirection URL configured on the on premise OmniAccess Stellar AP.

A zone can be added from the page ***Administration->Zones.***

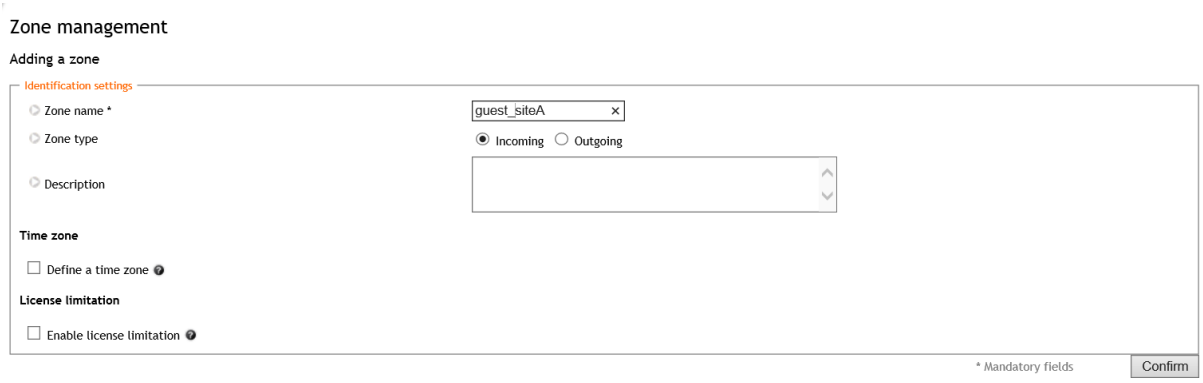

Figure 3 : Adding an incoming zone

5.2.2 Captive portal

The captive portal can be configured from the page ***Configuration->Customization->Portal***

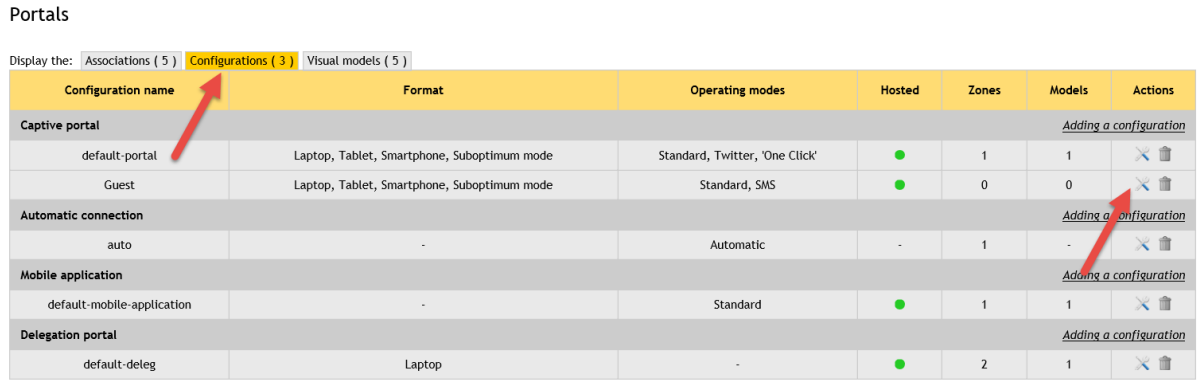

Figure 4 : Configuring a captive portal

For example, a portal with self-registering by SMS

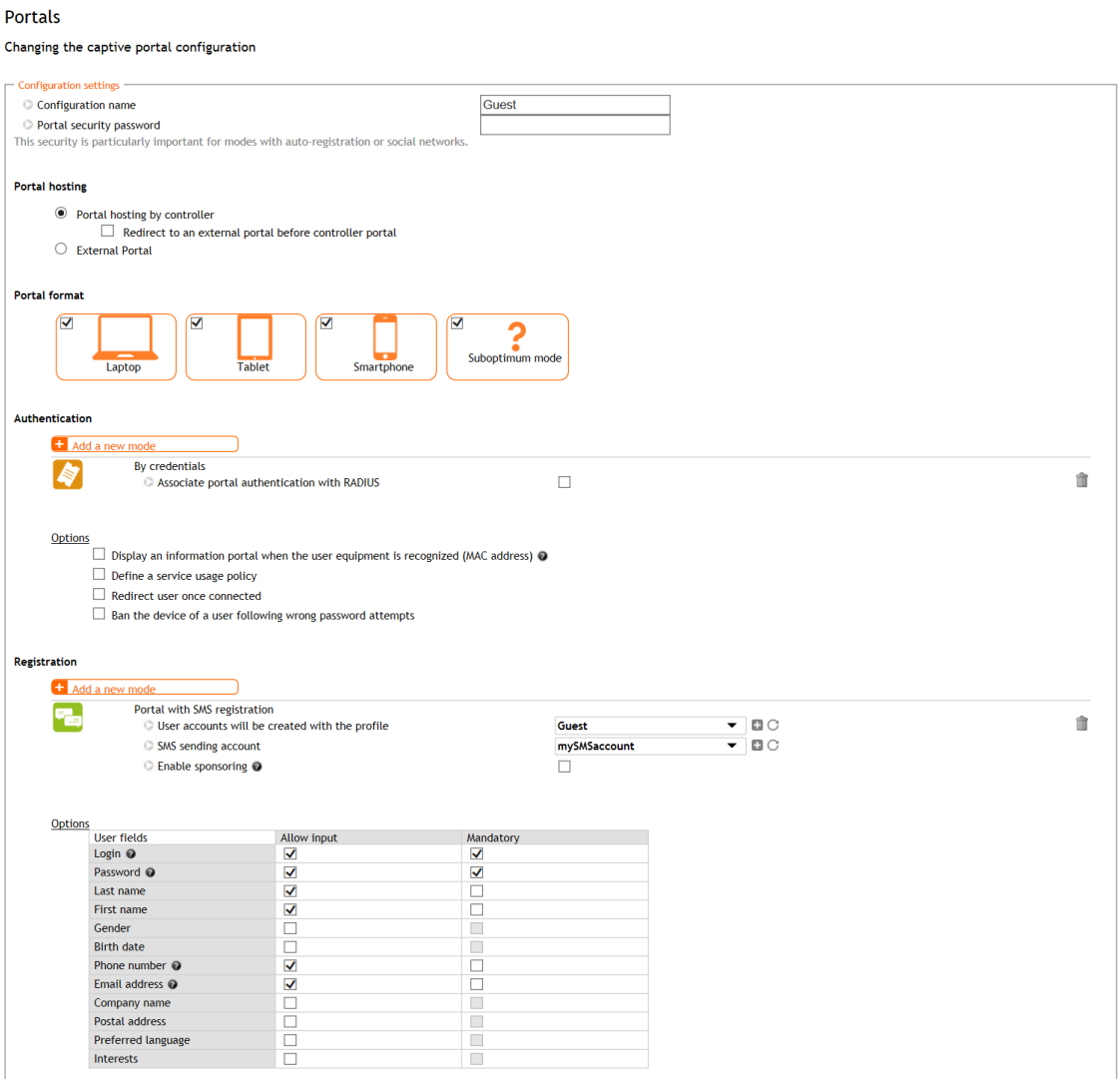

Figure 5 : Example of portal configuration with self-registering by SMS

Then, you have to associate the zone previously created to the portal configuration. A portal visual model must be chosen for this association.

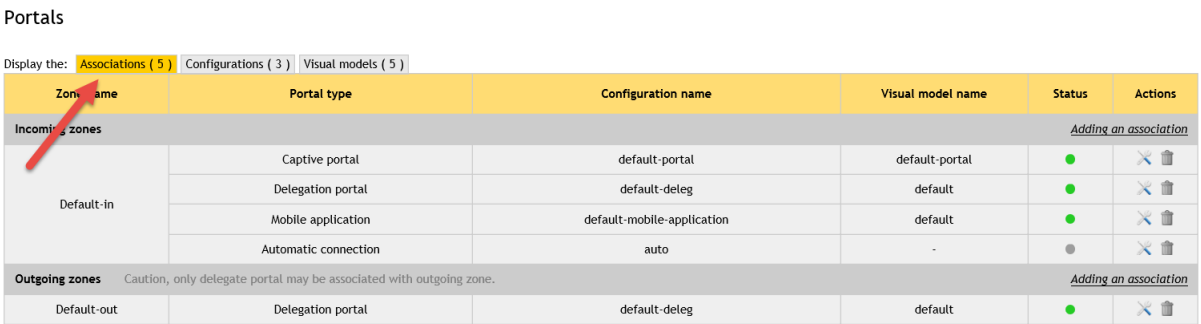

Figure 6 : Association between portal and zone

5.2.3 RADIUS authentication

The OmniAccess Stellar APs perform user authentication through the RADIUS protocol.

The RADIUS configuration on the UCOPIA controller is done from the page ***Configuration->Authentication->RADIUS***.

Add a new NAS, as the OmniAccess Stellar AP must be defined as a NAS for the central controller.

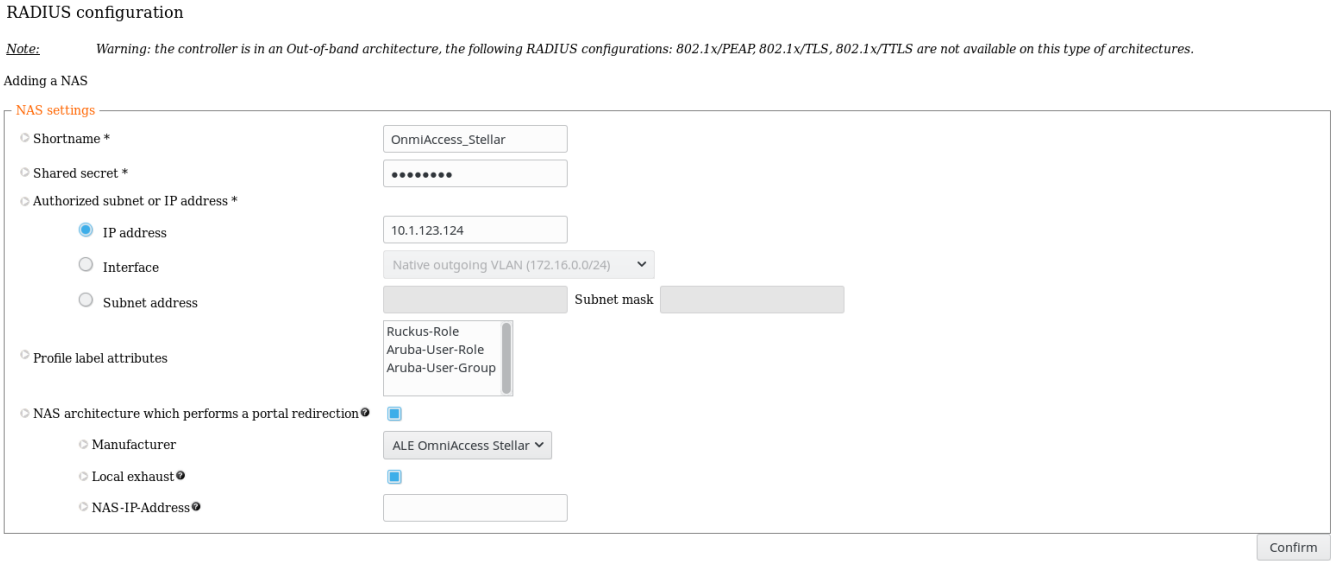

Figure 7 : Adding a NAS

To configure the NAS, you have to go through the following steps:

- Define the name of the NAS.
- Define the shared secret. This same shared secret will be defined on the AP as well.
- Define the AP IP address. If the AP is behind a NAT, you have to configure an IP addressing containing the IP address seen by the central controller. A subnet IP address can also be defined. When using several APs, all their IP addresses has to be allowed, as each AP sends RADIUS messages independently from one another.
- Tick the box “NAS architecture which performs a portal redirection”
- Select “ALE OmniAccess Stellar” as Manufacturer
- Tick the box “Local exhaust” for local Internet breakout architecture.

5.2.4 User profile

Define your user profiles, their time- and MAC- based settings (refer to 3.2.3. to have the list of supported UCOPIA features).

5.2.5 User traffic logging

User traffic logs are sent from OmniAccess Stellar APs to the central UCOPIA controller through syslog messages over UDP/514. To allow these messages to reach the UCOPIA controller, a rule has to be opened in ***Configuration > Network > Filtering***.

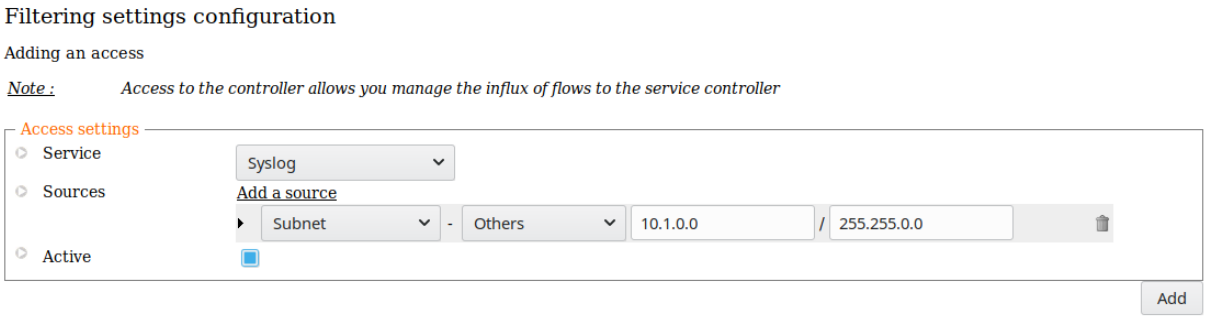

Figure 8 Opening rule for Syslog traffic

Note: Ensure that any active element in the network (Firewall, …) will not block this traffic between the access points and the central controller.

5.2.6 [Optional] New domain name and certificate

By default, the FQDN (Fully Qualified Domain Name) of a UCOPIA controller is "controller.access.network". A signed certificate is installed matching this FQDN. This certificate is also valid for the FQDN "central.access.network".

When using social network authentication on the portal, end-user devices must be able to resolve "controller.access.network" or "central.access.network" with the IP address of the central UCOPIA controller. So new DNS entries has to be added in the DNS server that will answer the end-user devices requests so that these FQDN are correctly resolved.

Another solution is to have a new FQDN that will be resolved to the IP address of the central UCOPIA controller. This solution has drawbacks, as a TLS certificate matching that new FQDN must be purchased, and new social networks applications have to be created for that new FQDN.

Note: The new certificate must be consistent with the FQDN and must be purchased from a Certification Authority

- Add a new certificate: to install the certificate for the captive portal, go to the page ***Configuration->Authentication>Certificates.***

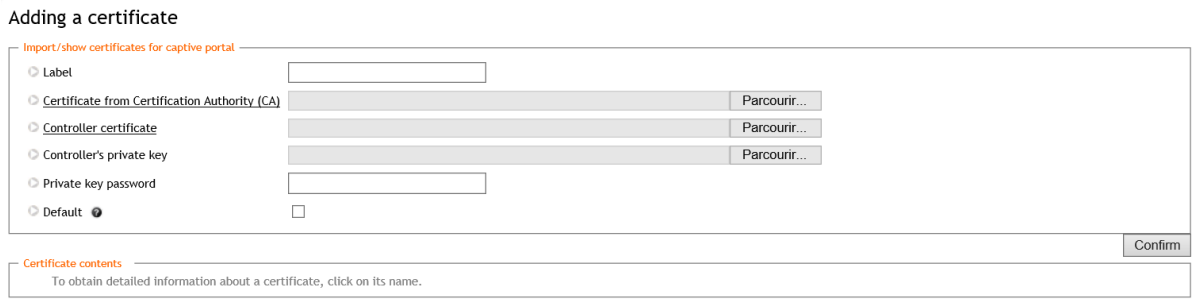

Figure 9 : Adding a new certificate for the captive portal

- Modify the controller domain name: the name of the controller must be changed according to the new certificate. The controller name can be modified from the page ***Configuration->Network->Controller.***

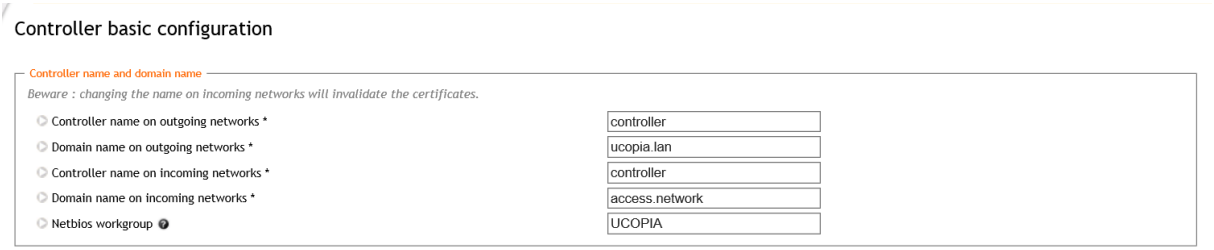

Figure 10 : Modifying a controller name

5.3 OmniAccess Stellar AP configuration

Connect to the Web management tool of your access point.

5.3.1 Creation of a new SSID

Click on "**New**" in the WLAN tile.

Figure 11 Creation of a new WLAN

Give a name to the new WLAN, select "Open" as security level to enable the "Captive Portal" option, and tick Yes for Captive portal.

Then, click on Advance and configure as follows:

- MAC authentication: Optional, it should be enabled when authentication bypass based on MAC address is to be used. This bypass is performed through a RADIUS Access-Request sent to the UCOPIA controller when a new device associate with the WLAN. The profile used on UCOPIA should have the appropriate configuration set: MAC remembering and automatic connection in the "Recognition of user equipment" section. The zone name used on the UCOPIA controller should be the same as the WLAN name, as zone authorization will be performed based on the WLAN name set in the RADIUS request. When this option is enabled, the following parameters should be configured:
- Server IP/Hostname: the central UCOPIA controller
- Port: 1812, or any other when using port forwarding
- Secret: the RADIUS shared secret, the same as defined in NAS configurations on the UCOPIA controller
- Account: to enable RADIUS accounting. This has to be checked to ensure an Accounting-Start/Stop message is sent upon device connection/ disconnection to the UCOPIA controller.

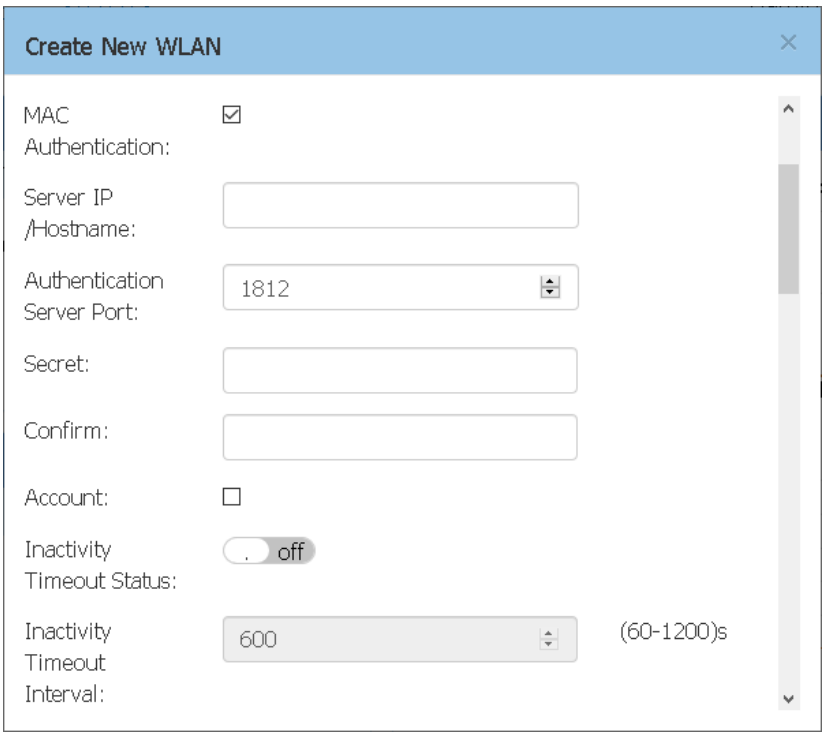

Figure 12 MAC authentication

- Fill the remaining fields according to your needs.
- Click on "**Save**".

5.3.2 External captive portal

Expand the menu "**Access**" and click on "**Authentication**".

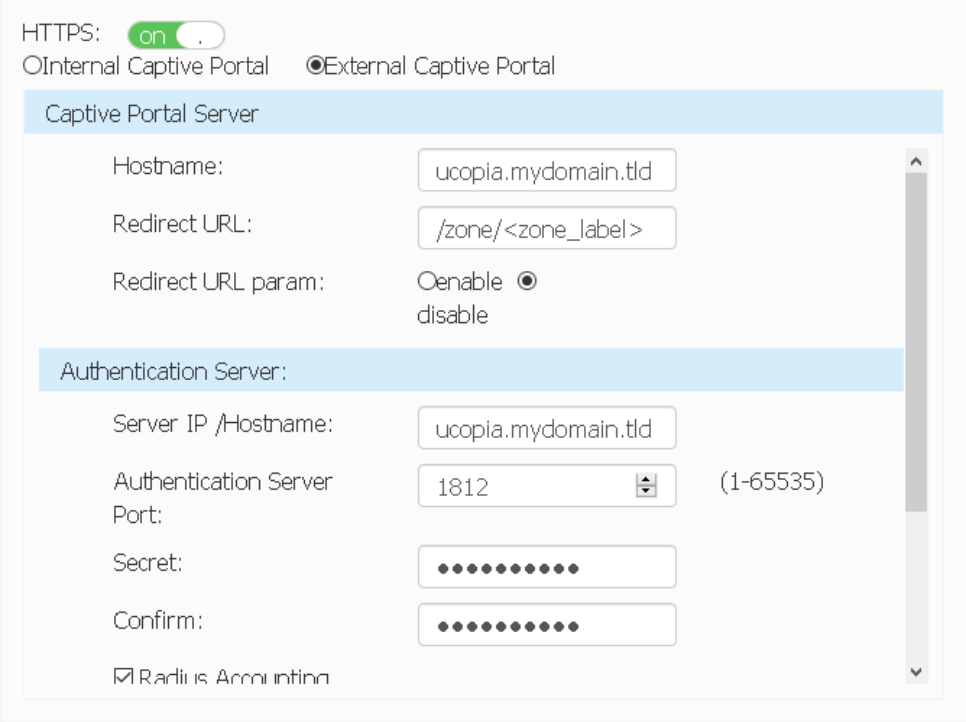

Figure 13 External captive portal

Configure the external captive portal as follows:

- HTTPS: on
- Internal/External captive portal: External
- Captive portal server:
- Hostname: the fully qualified domain name of the UCOPIA controller
- Redirect URL: /zone/<zone_label> where zone_label is the label of the zone on the UCOPIA controller
- Authentication server: this part of for the RADIUS configuration
- Server IP/Hostname: the fully qualified domain name or IP address of the UCOPIA controller
- Port: 1812, or any other when using port forwarding
- Secret: the RADIUS shared secret, the same as defined in NAS configurations on the UCOPIA controller
- RADIUS Accounting: enable. This is mandatory to get Accounting-Stop messages to disconnect end-user devices on the central UCOPIA controller.
- Port: 1813, or any other when using port forwarding
- Interval: 600 seconds. This controls the interval of Accounting-Interim messages.

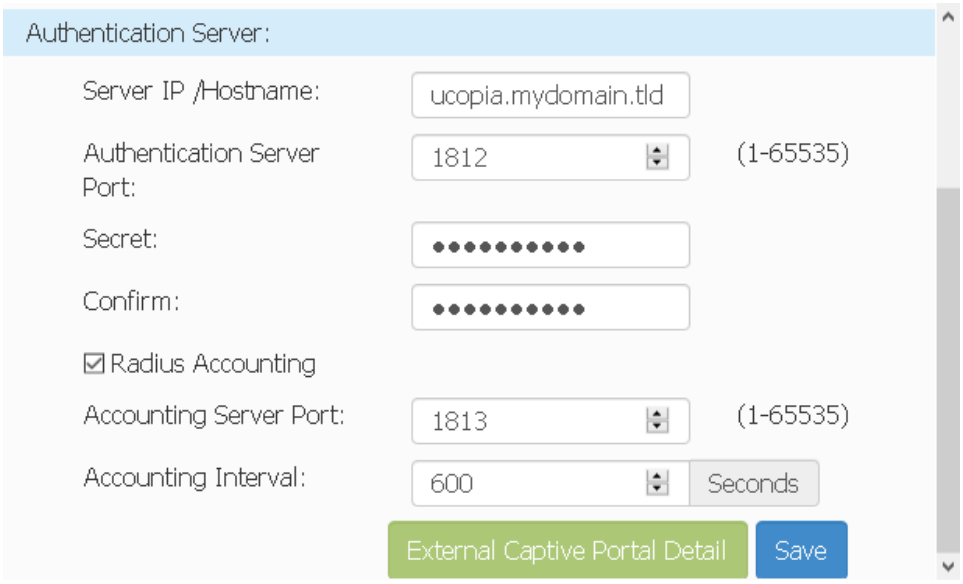

Figure 14 Authentication server configuration for external captive portal

To finish, click on "**Save**".

5.3.3 User traffic logging

In the same menu, below the authentication server configuration, the **Client Behavior Tracking** can be enabled. Both options "**HTTP/HTTPS**" and "**ALL**" should be selected to sent Web domains and IP traffic logs. The second parameter should be set to "**Syslog Server**" to send these logs to the central controller syslog server.

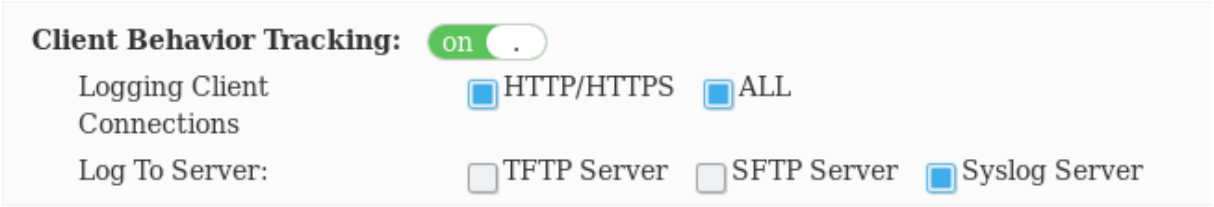

Figure 15 Configuring user traffic logging

The syslog server parameters can then be defined in the fields displayed on the right, as shown in figures below.

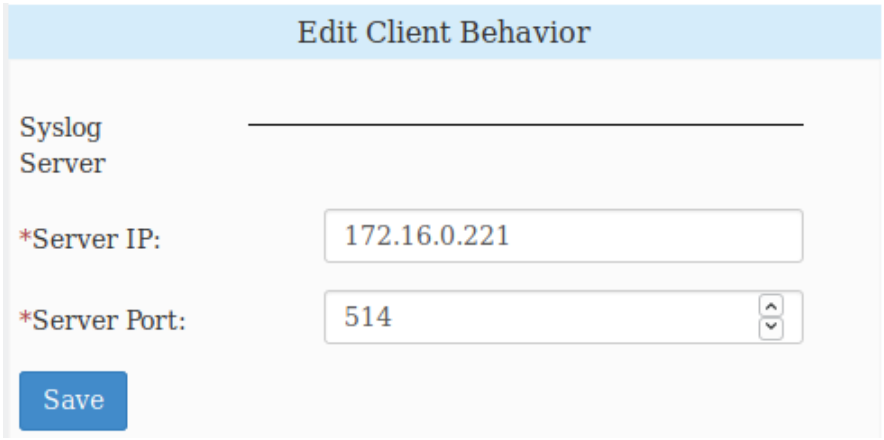

Figure 16 Syslog server parameters

Finally, in the “Syslog & SNMP” part of the “System” menu, it should be ensured that the log levels are not set to a too verbose value (below Warning level). This will avoid overloading the central controller with messages that would be dropped anyway.

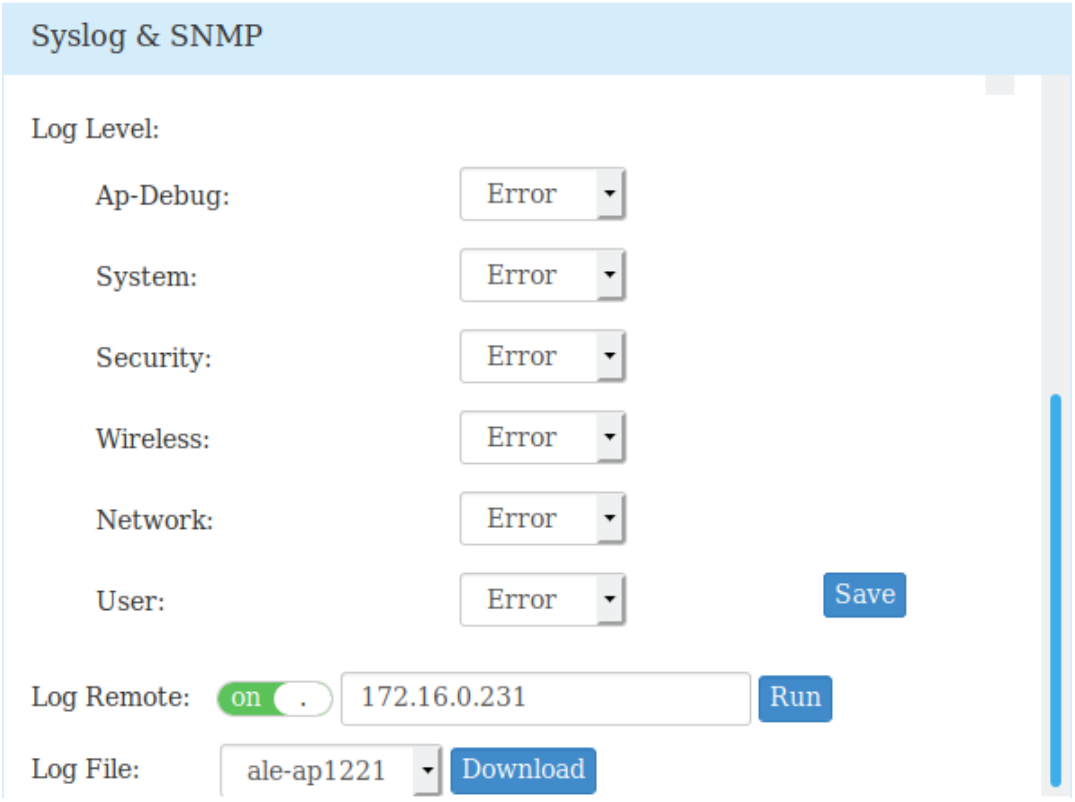

Figure 17 Syslog log levels

5.3.4 Walled garden

End-user devices must have access to the external captive portal before any authentication. For that purpose, a walled garden URL has to be configured as follows:

- Expand the “Access” menu and click on “Walled garden” in the “Black list & White list” tile.

- Select domain, enter the fully qualified domain name of the central UCOPIA controller and click “Add”.

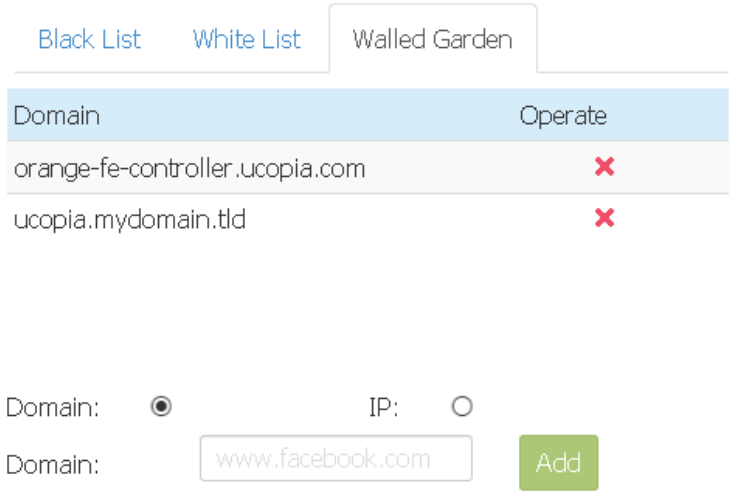

Figure 18 Walled garden configuration

When using portal authentication modes with social network logins, some additional walled garden URLs have to be configured. The URL lists are available in Annex 2.

6 Annex 1: detailed flow diagram

The following diagram describes in detail the flows between the user at remote site, the OmniAccess Stellar AP and the central controller for authentication process.

6.1 Portal authentication

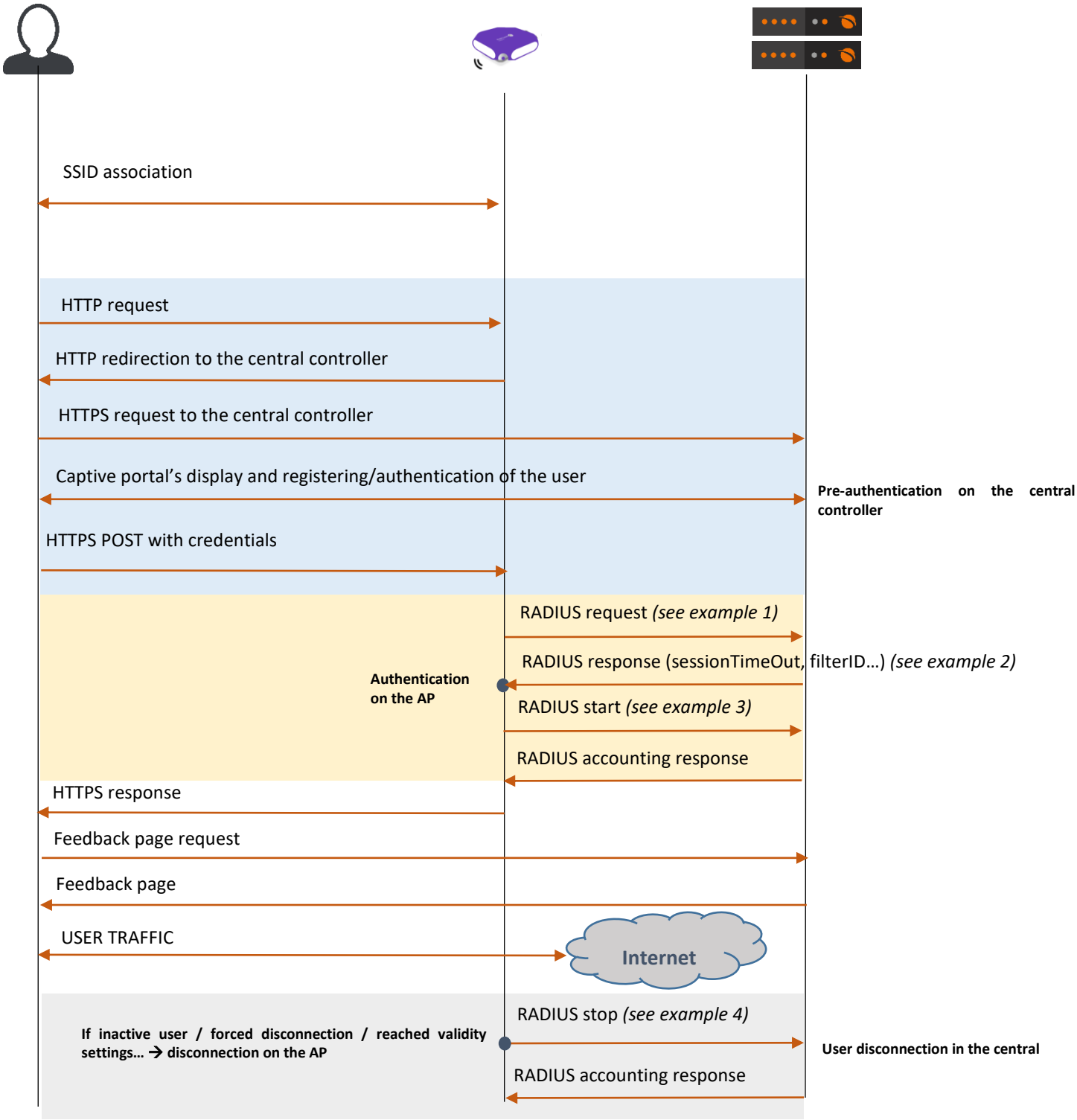

Figure 19 : Detailed flow diagram

7 Annex 2: Walled garden for social networks

7.1 Facebook, Twitter, Google, LinkedIn

The following open-access URLs must be opened.

Facebook	www.facebook.com
	fbstatic-a.akamaihd.net
	graph.facebook.com
	fbcdn-profile-a.akamaihd.net
	m.facebook.com
	fbcdn-photos-a-a.akamaihd.net
	fbcdn-photos-b-a.akamaihd.net
	fbcdn-photos-c-a.akamaihd.net
	fbcdn-photos-d-a.akamaihd.net
	fbcdn-photos-e-a.akamaihd.net
	fbcdn-photos-f-a.akamaihd.net
	fbcdn-photos-g-a.akamaihd.net
	fbcdn-photos-h-a.akamaihd.net
	static.xx.fbcdn.net
	edge-star-shv-01-cdg2.facebook.com
	xx-fbcdn-shv-01-cdg2.fbcdn.net
Google	clients1.google.com
	accounts.google.com
	accounts.google.fr
	accounts.youtube.com
	ssl.gstatic.com
	fonts.googleapis.com
	themes.googleusercontent.com
	sb-ssl.google.com
LinkedIn	api.linkedin.com
	static.licdn.com
	www.linkedin.com
Twitter	api.twitter.com
	abs.twimg.com
	abs-0.twimg.com
	pbs.twimg.com
	api.twitter.com

7.2 OpenID Connect

The following open-access URLs must be opened.

- **Authorization endpoint:** URL of the OpenID Connect application authorization endpoint. Example: https://server.example.com/connect/authorize.
- **Token endpoint:** URL of the OpenID Connect application Token Endpoint. Example: https://server.example.com/connect/token
- **Userinfo endpoint:** URL of the OpenID Connect application UserInfo Endpoint. Example: https://server.example.com/connect/userinfo

8 Annex 3: Summary table on available features

The following table is provided as a summary of the supported features in the Out-Of-Band OmniAccess Stellar architecture:

Features	OOB OmniAccess Stellar	Comments
SECURITY		
Authentication		
- Web captive portal	✓	Hosted by central UCOPIA
- 802.1x (PEAP/TTLS/TLS)	✗	
- Social networks (Facebook, Twitter, G+, LinkedIn, OpenID Connect)	✓	- If new DNS entries for resolving "controller.access.network" or "central.access.network" with the IP address of the central UCOPIA controller have been created, or - if the domain name /certificate has been changed and publicly declared, and new social network applications are created
- Automatic @MAC address authentication	✓	
- Shibboleth	✗	
Redirection on corporate web portal	✓	
URL/domain filtering (HTTP and HTTPS)	✗	Not ensured by UCOPIA controller as the traffic won't go though it
Access permissions on basis of user profile	✗	
Controller's incoming VLANs/subnets	✓	
Pre-authentication charter acceptance	✓	
Private information charter acceptance (opt-in marketing)	✓	
Password policies and password recovery	✓	
Quarantine after N wrong password attempts	✓	
Connection break between two sessions	✓	
Connections traceability and logs	✓	
- User sessions	✓	

- Traffic	✓	TCP/UDP flow data available on AP and can be sent to the central UCOPIA controller through Syslog
- URL	✓	URL domain available on AP and can be sent to the central UCOPIA controller through Syslog
- Automatic logs backup via FTP(S)	✓	
Audit logs (Syslog)	✓	
MOBILITY		
QoS (by service, by user)	✓	Policy controls per service via AP management
Data volume quota	✗	No quota applied by UCOPIA as the traffic won't go though it
Time based access control	✓	
- Configured ending validity date	✓	
- Time credit	✓	
Location based access control	✓	Based on zones
Multi-portal	✓	One portal per zone
Conditional profile	✓	Only for the supported features of the profile
Memorization and limitation of devices per user	✓	
Automatic disconnection	✗	Disabled on the central controller as soon as an Out-Of-Band architecture is set up. Has to be performed by the AP
Manual disconnection (thanks to Logout button on the portal)	✗	
ADMINISTRATION		**Done on central**
License per zone or user profile	✓	
SMS registration	✓	
Mail registration	✓	Limited mail registration as users have to wait for the end of their temporary session to be able to either click on the autoconnect/autofilllink or to enter their received credentials on the splash page
Sponsoring by email	✓	
User account refill by code or online payment	✓	Same limitation as email registration, as a temporary session is needed to perform the payment
Automatic user accounts purging (global or per profile)	✓	

Manual/automatic user account export via CSV	✓	
Delegated provisioning	✓	
- Customization	✓	
- Multi zones	✓	
- Connection ticket printing (or sending by SMS or email)	✓	
- Bulk account creation from CSV file	✓	
- User account refill by code	✓	
Supervision of connected users	✓	
Statistics	✓	
- Predefined graphs	✓	
- Manual/automatic CSV export	✓	
Reporting (PDF)	✓	
Customizable web portal	✓	
Customizable connection ticket per zone or profile	✓	
SNMP	✓	
External Syslog	✓	
CLI	✓	
Multi zone administration	✓	
Physical Administration port	✓	For hardware US2000 and above
BILLING		
Online payment (PayPal, Ingenico)	✓	
PMS connector	✓	Only one PMS server can be configured and integrated with the central UCOPIA
INTEGRATION		
Integration with a corporate LDAP directory (OpenLDAP, Active Directory)	✓	
Integration with one or more directories	✓	
Integration with external RADIUS (proxy)	✓	
Integration with secondary RADIUS (failover or load-balancing)	✓	

Web proxy integration	✓	
ICAP compliant	✓	
API for third party tool integration	✓	