



Out-Of-Band Edge Architecture

Version 6.0



Table of contents

Table of figures	4
1 Introduction	5
2 How does it work?	6
2.1 User experience workflow	6
2.2 Synchronization mechanism between central controller and Edge	7
2.3 Synchronization mechanism between central controller and Analytics Platform	7
3 Advantages and recommendations	8
3.1 Advantages	8
3.1.1 Centralization of the user directory	8
3.1.2 Centralization of captive portals	8
3.1.3 Centralization of user profiles	8
3.1.4 Centralization of outgoing policies	8
3.1.5 Local Internet breakout	8
3.2 Recommendations	9
3.2.1 User logs	9
3.2.2 Network or Central controller failure	9
3.2.3 Control of users' time and quota consumption	9
4 Licensing	10
5 UCOPIA configuration	11
5.1 Prerequisites	11
5.1.1 Certificate	11
5.1.2 DNS	12
5.1.3 Time synchronization	12
5.1.4 Communication between remote sites and central site	13
5.1.5 Version consistency between Edge controller and Central controller	13
5.2 Central controller configuration	14
5.2.1 Certificate	14
5.2.2 Controller name	15
5.2.3 Zone	15
5.2.4 Captive portal	16
5.2.5 Using a specific HTTPS port	19
5.2.6 RADIUS authentication	20
5.2.7 User profile	20
5.2.8 Administrator account	21
5.2.9 Social network authentication	22
5.3 Edge configuration	23
5.3.1 Association to the central controller	23
5.3.2 Using a specific HTTPS port	24
5.3.3 Portal redirection	25
5.3.4 RADIUS authentication	26
5.3.5 Additional networks and VLANs reachable through outgoing policies (optional)	27
5.3.6 Automatic MAC address authentication (optional)	28
5.3.7 High Availability on Edge controllers (optional)	30
5.4 Edge administration from the central controller	31
6 Annex 1: detailed flow diagram	32
6.1 Portal authentication	32
6.2 Automatic MAC address authentication	33
7 Annex 2: Walled garden for social networks	34
7.1 Facebook, Twitter, Google, LinkedIn	34
7.2 OpenID Connect	34

8 Annex 3: Check-List 35

Table of figures

Figure 1: Global Out-of-Band Edge architecture.....	5
Figure 2: User traffic flow	6
Figure 3: Synchronization between central controller and Edge	7
Figure 4: Synchronization UWS for Analytics service	7
Figure 5: License management in Out-of-Band Edge architecture	10
Figure 6: Out-of-Band Edge architecture certificates.....	11
Figure 7: Adding a new certificate for the captive portal	14
Figure 8: Modifying a controller name	15
Figure 9: Adding an incoming zone	15
Figure 10: Configuring a captive portal	16
Figure 11: Example of portal configuration with self-registering by SMS	17
Figure 12: Association between portal and zone.....	18
Figure 13: Creation of a port redirection.....	19
Figure 14: Adding a NAS	20
Figure 15: Adding an administrator profile.....	21
Figure 16: Adding an administrator account.....	22
Figure 17: Edge Association to the central controller.....	23
Figure 18: Creation of a port opening	24
Figure 19: Configuring a portal redirection to the central controller	25
Figure 20: Configuring the NULL RADIUS realm	26
Figure 21: Configuring the DEFAULT RADIUS realm	27
Figure 22: Adding a network reachable through outgoing policies	28
Figure 23: Adding an automatic connection	28
Figure 24: Configuring an automatic connection	29
Figure 25: Association between automatic connection and zone	29
Figure 26: Two associated Edge controllers in High Availability architecture	30
Figure 27: Edge administration from the central controller.....	31
Figure 28: Detailed flow diagram	32
Figure 29: Flow diagram for automatic MAC address authentication	33

1 Introduction

This document describes the Out-of-Band architecture with UCOPIA Edge on premise. This architecture is composed of a central controller (Advance Global license), and UCOPIA Edge(s) (Edge license) that are connected to the central controller. The central controller is typically in a datacentre, and the Edges at customer sites (e.g. hotel, restaurant, agency, etc.).

The goal of the Out-of-Band architecture is to build a centralized architecture allowing centralized management of the main UCOPIA features: captive portals, user profiles, authentication server, provisioning, user directory, but without the need to centralize the user traffic. The local Internet access of each site is used for the user traffic.

On-premise, the Edge ensures portal redirection to the centralized UCOPIA controller, authentication process, user traffic traceability and optionally Proximity services.

The central controller and Edge can be a high availability cluster.

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

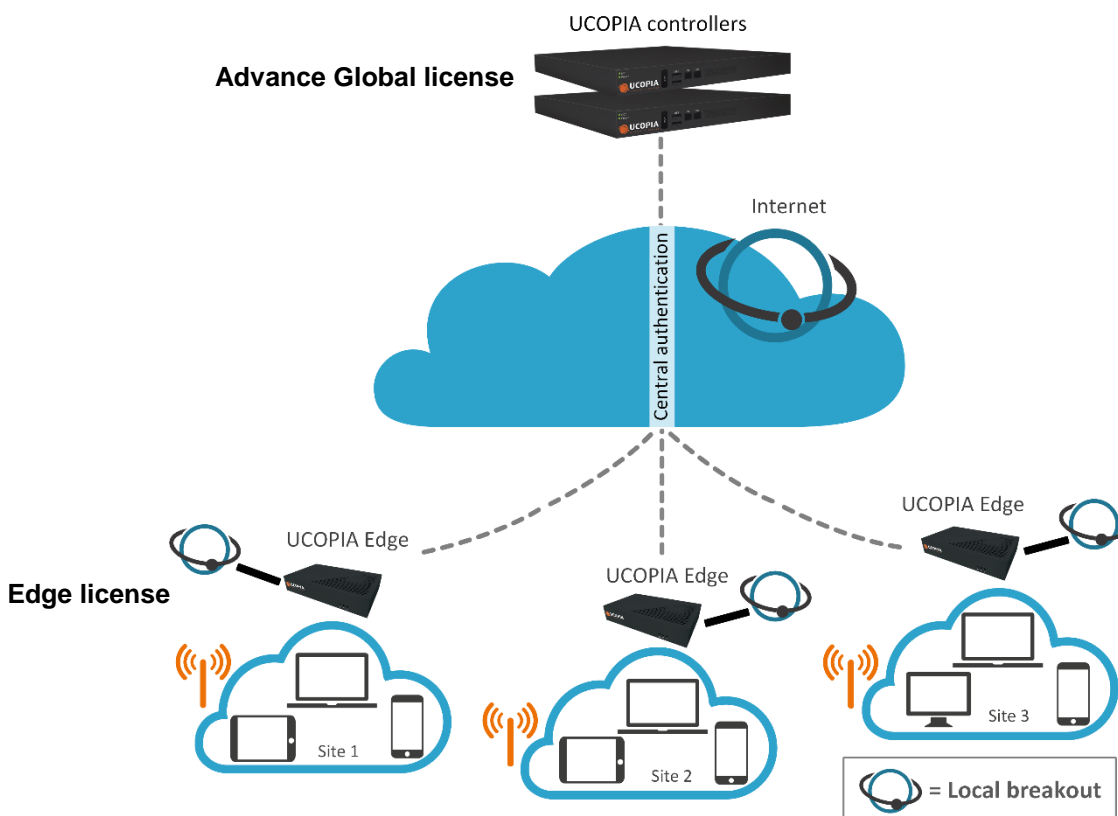


Figure 1: Global Out-of-Band Edge architecture

2 How does it work?

2.1 User experience workflow

Let's consider a Guest user trying to get a Wi-Fi Internet connection on a site (site A) where an UCOPIA Edge 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 Edge, as the user is not yet connected, makes an HTTPS redirection 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 presents the portal associated to the zone corresponding to the site A.
4. The user fills the form (phone number, etc.) correctly, his user account is created on the central controller only, and (s)he receives his (her) credentials by SMS and enters his login and password on the captive portal from the central controller.
5. The login and password are analyzed by the central controller, and if they are correct, the authentication process is performed between the Edge and the central controller through the RADIUS protocol. The user profile is sent to the Edge in order to locally apply policies related to the profile, a RADIUS attribute is used for that.
6. Once the user authenticated, the user can browse using the local Internet access (site A).

The user traffic flow is summarized by the following schema.

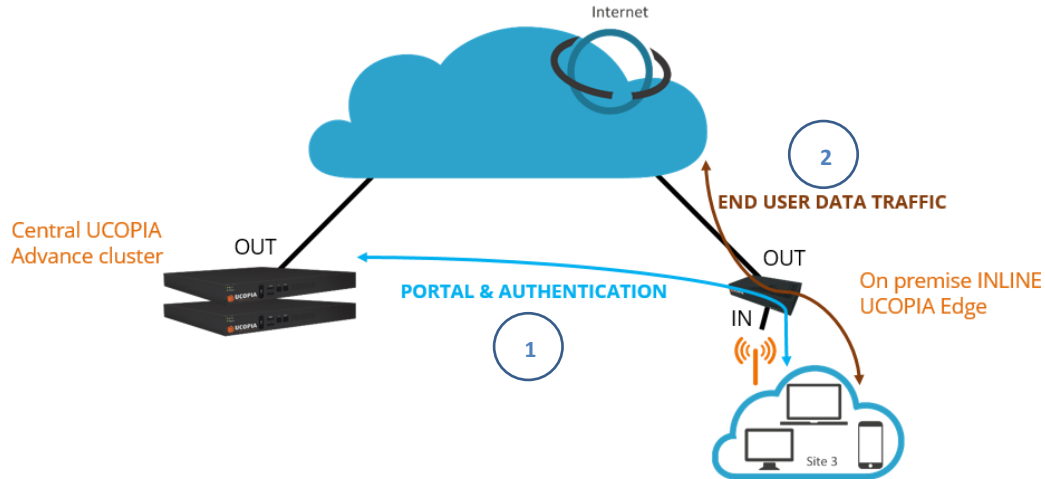


Figure 2: User traffic flow

2.2 Synchronization mechanism between central controller and Edge

The user profiles, services, zones, password policies and URL categories are configured only at the central controller level and are automatically replicated on the Edge in order to centralize administration.

Each time one of these components is modified on the central controller, it is replicated on the Edge. This synchronization process relies on the zone defined on the Edge for the central portal redirection. **It will only synchronize components necessary for that zone** (All zones of the central controller are replicated on the Edge. But, regarding the other components (profiles, services and password policies), the Edge will only synchronize those necessary on his zone. **It is possible to declare multiple zones on the edge. Just manually create the Open-Access URL in the Edge and used in a configuration of external portal.**

In case of network failure, synchronization restarts when Edge/central controller link is up again.

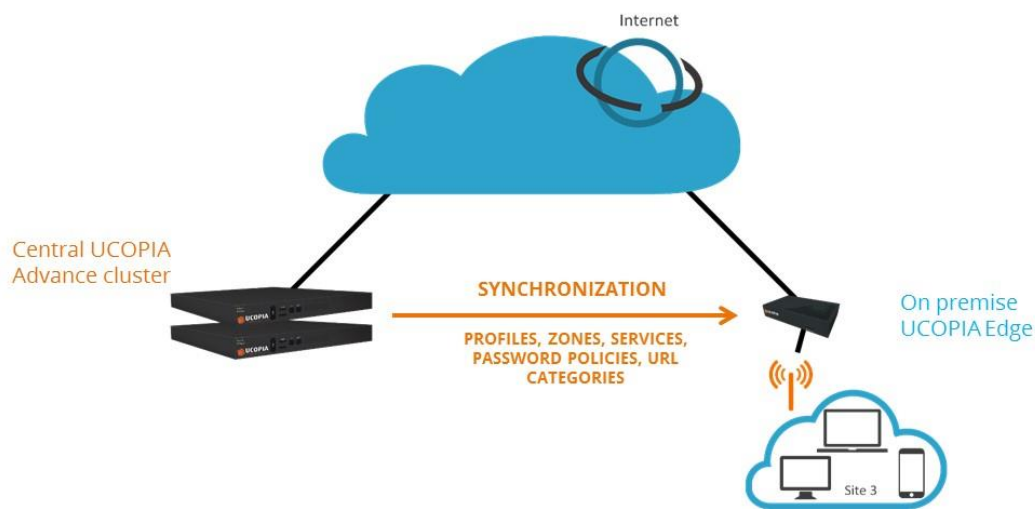


Figure 3: Synchronization between central controller and Edge

2.3 Synchronization mechanism between central controller and Analytics Platform

In case of a subscription to the analytics platform, only UCOPIA central sessions must be sent to the analysis platform (not Edge sessions).

To export the sessions, go, on the central controller, to the page « Exploitation ► Maintenance ► UWS », and click on the “Enable” button.

UWS synchronization

Synchronization with UCOPIA Web Services platform

Send data like the profiles and the zones to the UCOPIA Web Services platform.
This data is required to use this controller in the multi-tenant mode.

▶ Immediately trigger the sending data

Send

Export sessions to the Wi-Fi Analytics service

▶ Instant export of sessions to the Wi-Fi Analytics service

Enable

▶ Synchronize the sessions

Synchronization

▶ Collect URL

Apply

Figure 4: Synchronization UWS for Analytics service

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 capability. Note that this can be restricted by configuration on the profiles on the central controller.

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

User profiles are centralized and therefore configured on the central controller. However, the profiles are used by the Edge controller in order to apply profile policies. To simplify administration, the user profiles are automatically replicated on the Edge controller. In order to replicate only the needed profiles, the replication process is selective. The selection is done by matching the zones allowed for the profiles and the zones used by the Edge controller. Only profiles allowed to authenticate on the zones used by an Edge controller will be synchronized to it. On the Edge side, user profiles settings cannot be modified.

3.1.4 Centralization of outgoing policies

The outgoing policies configured on the central controller are also synchronized on the Edge controllers. Once this synchronization is done, the policies can be modified on the Edge controller to use NAT or routing, and be applied on another VLAN.

3.1.5 Local Internet breakout

Each local site, and so each Edge controller, uses its own Internet access for connecting users and avoids centralizing the user traffic toward the central Internet access. The central UCOPIA controller does not see the user traffic (this explains the "out-of-band" name of this architecture).

3.2 Recommendations

3.2.1 User logs

User sessions logs are centralized on the central controller. However, due to “3.1.5 Local Internet breakout traffic” logs and visited URLs are only stored on the Edge. It is therefore recommended to set up an automatic backup via external FTP.

3.2.2 Network or Central controller failure

The user directory is centralized on the central controller and used by all Edge controllers on local sites. In case of network failure between the Edge controller and the central controller or in case of Central controller failure, the user directory will not be available for the Edge controllers. It is therefore recommended to set up a redundant cluster on the central site.

3.2.3 Control of users' time and quota consumption

When time credit/validity or quota are configured on a profile, the Edge will regularly send RADIUS Interim Accounting Updates to the central controller, so that the central controller can regularly update the information of time and quota consumption in its database.

On the contrary, if no time or quota limitations are configured on a profile, the users won't be regularly updated (the table “Connected users” on the central controller won't display updated information) until their disconnection.

That is why it is recommended to follow the users' time or quota consumption on the Edge instead of the central controller, as the information are not always up-to-date on the latest.

4 Licensing

The Edge license doesn't take into account the number of concurrent connections. Only the central controller handles the concurrent connections.

However, the server with the Edge license must be properly sized according to the user traffic on the remote site.

Licenses « Edge LR » and « Edge R » are for High Availability architecture between two Edge controllers (see § [High Availability on Edge controllers](#)).

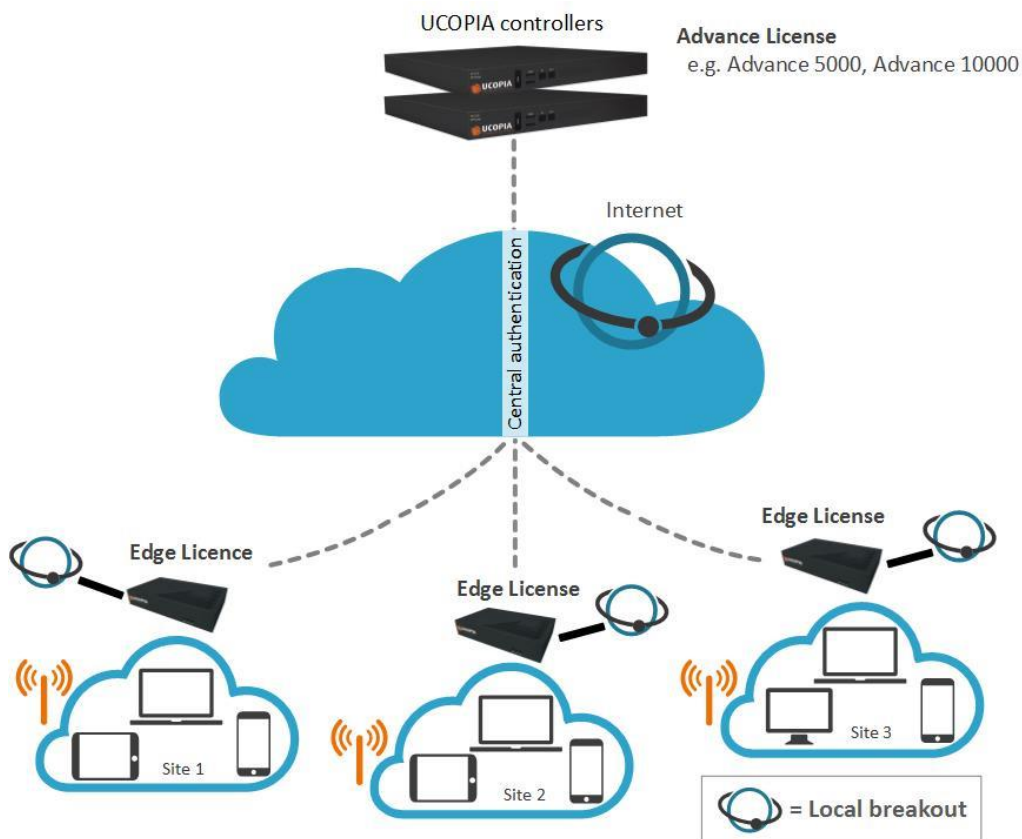


Figure 5: License management in Out-of-Band Edge architecture

5 UCOPIA configuration

5.1 Prerequisites

5.1.1 Certificate

By default, 2 FQDNs (Fully Qualified Domain Name) are configured on a UCOPIA controller:

- controller.access.network
- central.access.network

The signed certificate including these two FQDNs is also installed by default.

For the end user browser to be able to make the difference between the edge controller and the central controller, the central controller FQDN has to be different from the one of the edge controllers.

You can configure your FQDNs in 2 ways:

- either use the default certificate pre-configured on UCOPIA
 - controller.access.network for the Edge controllers
 - central.access.network for the central controllers

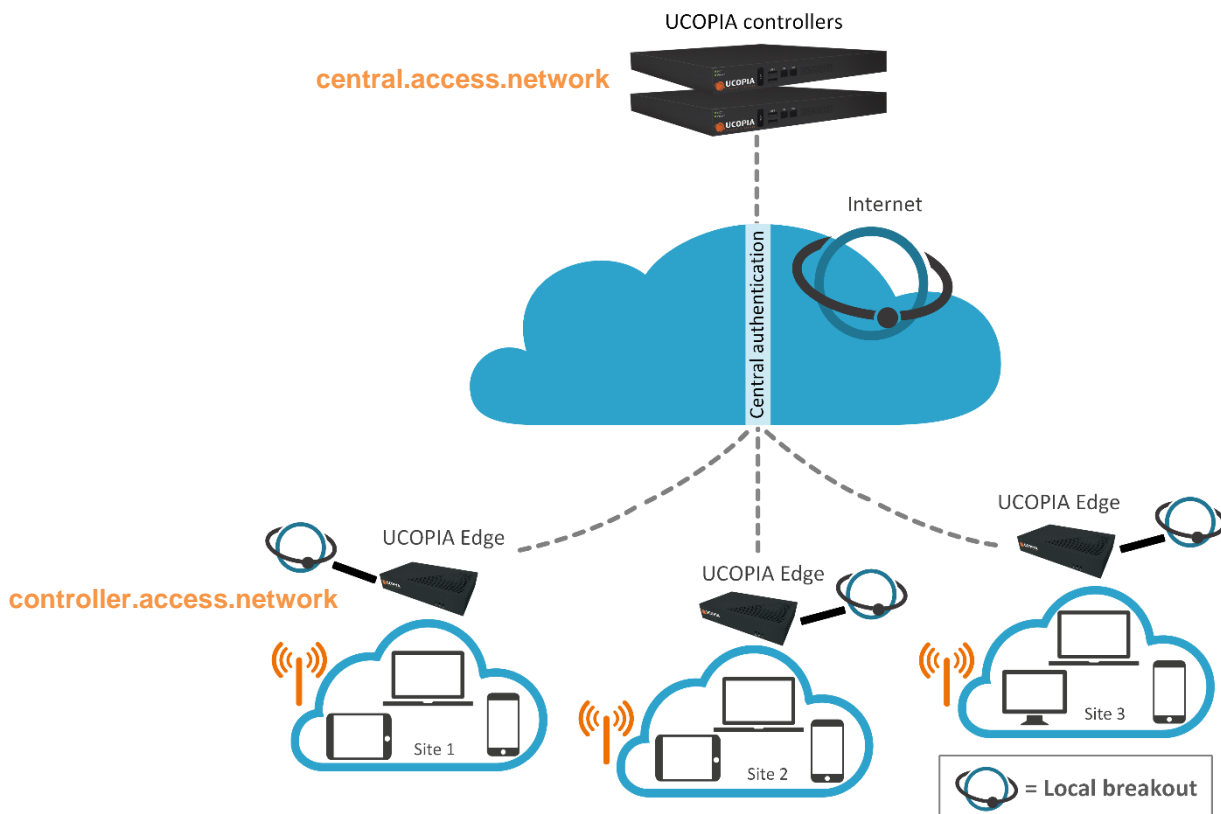


Figure 6: Out-of-Band Edge architecture certificates

- either buy, create, and sign your own customized certificates from [a trusted certificate authority](#)

**Note**

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

Since 5.1.11 version, even if UCOPIA controller FQDN remains « controller.access.network », the embedded certificate has become a multi domains and allow « central.access.network » as FQDN too.

The social network authentication method, natively proposed in the portal configuration (both the Neutral and UCOPIA), are based on these 2 FQDN « controller.access.network » and « central.access.network ». If you change the FQDN of your central UCOPIA controller, then not only do you need to change the certificate but also to create and declare your own social network application, (see § [Social network authentication](#)).

5.1.2 DNS

The central controller must have an URL that can be resolved by the end user's equipment on the remote site. A DNS entry (FQDN) must be created on a DNS server (private or public) or on the Edge DNS server so that the user can log in to the central controller.

5.1.3 Time synchronization

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

5.1.4 Communication between remote sites and central site

The central controller communicates with all the users on the remote sites as well as with the remote Edges (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.

Local users reach the central portal on its OUT interface (either via Internet, a private network like MPLS...).

If the default route is already defined on an outgoing VLAN (OUT interface), no additional configuration is needed.

If the default route is already defined on an incoming VLAN (IN interface), the default route must be modified.

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

Source	Destination	Protocol	Destination port	Description	Frequency
End user device	@IP central controller	TCP (HTTPS)	443	Portal redirection	Permanently (ex: when a user opens the portal)
@IP Edge controller	@IP central controller	TCP (HTTPS)	Chosen port	Synchronization of UCOPIA conf	Permanently (ex: when a profile is modified)
@IP Edge controller	@IP central controller	UDP (RADIUS)	1812	RADIUS exchange for authentication	Permanently (ex: when a user connects/disconnects)
@IP Edge controller	@IP central controller	UDP (RADIUS)	1813	RADIUS exchange for accounting	Permanently (ex: when time credit to track)

5.1.5 Version consistency between Edge controller and Central controller

The Out-of-band architecture requires that all the UCOPIA controllers, Central and Edge, have the exact same version, or that the Central controller is not ahead of more than 1 minor version from the Edge controllers.

An example:

Central controller version	Edge controller version	Authentication	Synchronization
6.0.0	6.0.0	✓	✓
6.0.0	6.0.1	✗	✗
6.0.1	6.0.0	✓	✓
6.0.1	6.0.1	✓	✓

5.2 Central controller configuration

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




5.2.1 Certificate

Please read 5.1.1 Certificate to choose the appropriate certificates for your edge and central controllers.


To view the default certificate for the captive portal, go to the page « **Configuration ► Authentication ► Certificates** ».

Certificate management

For the certificate of Radius, please click this link: [RADIUS server certificates](#)

SSL stored certificates list							
<input type="checkbox"/>	Label	Server name	Validity start	Validity end	Alternative alias names	Default	Actions
<input type="checkbox"/>	ucopia	controller.access.network	08/30/2017 01:39 PM	08/30/2020 01:39 PM	controller.access.network central.access.network	<input checked="" type="checkbox"/>	  

Page 1 of 1 10

In this menu, to install a new certificate that you have purchased for the captive portal, click on the  icon at the bottom of the certificates table:

Adding a certificate

Import/show certificates for captive portal

Label
 Certificate from Certification Authority (CA) Aucun fichier choisi
 Controller certificate Aucun fichier choisi
 Controller's private key Aucun fichier choisi
 Private key password
 Default

Certificate contents

To obtain detailed information about a certificate, click on its name.

Figure 7: Adding a new certificate for the captive portal

Note

UCOPIA requires certificate files with a .pem or .crt extension and format.

If ever you also have a certificate from an intermediate authority, it can be installed on UCOPIA by merging it with the root authority certificate in a single .pem or .crt file.

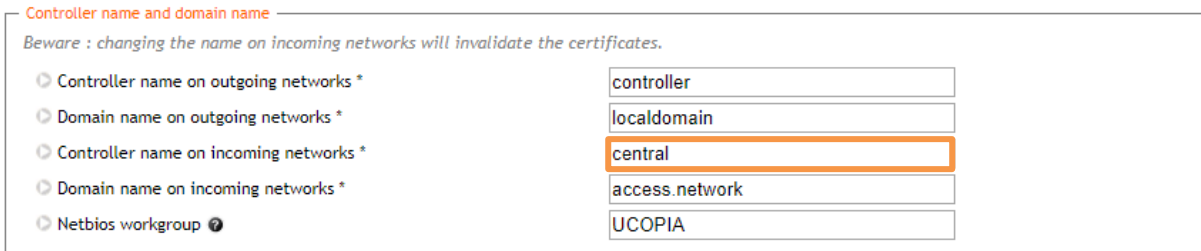


5.2.2 Controller name

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** », where you have to change the “Controller name on incoming networks”.

For example, if you use the default UCOPIA configuration, on the central controller you will have to change the “Controller name on incoming networks” to “central”:



Controller name and domain name

Beware : changing the name on incoming networks will invalidate the certificates.

Controller name on outgoing networks *	controller
Domain name on outgoing networks *	localdomain
Controller name on incoming networks *	central
Domain name on incoming networks *	access.network
Netbios workgroup ⓘ	UCOPIA

Figure 8: Modifying a controller name

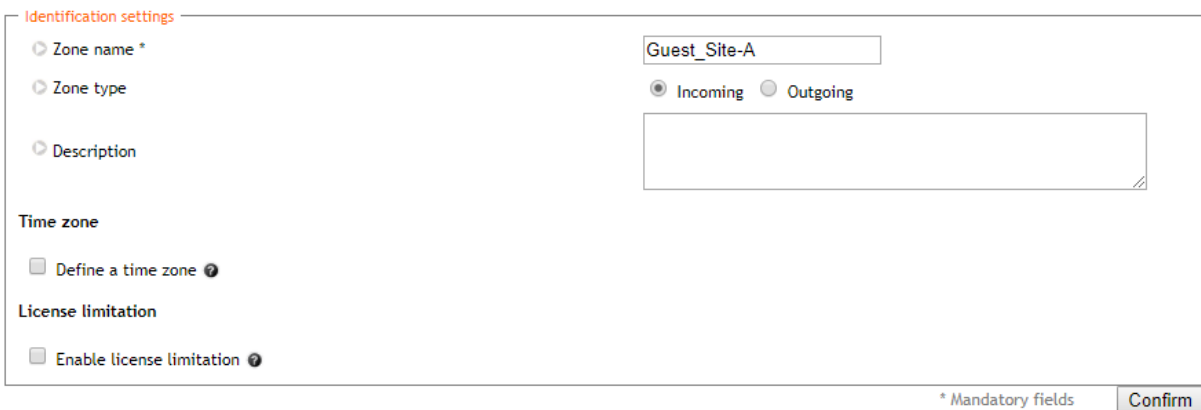
5.2.3 Zone

An incoming zone must be created for each remote site and a portal must be associated to this zone. The profile must allow this zone as “available input zone”. This zone will be used to redirect URL on the on-premise equipment. For each remote site, an incoming zone must be added. However, a site can be associated to several zones.

A zone can be added from the page « **Management ► Policies ► Zones** ».

Zone management

Adding a zone



Identification settings

Zone name *	Guest_Site-A
Zone type	<input checked="" type="radio"/> Incoming <input type="radio"/> Outgoing
Description	

Time zone

Define a time zone ⓘ

License limitation

Enable license limitation ⓘ

* Mandatory fields Confirm

Figure 9: Adding an incoming zone

Note

It is possible to define a license limitation in order to limit the number of simultaneous connections to a defined number or to a percentage of the license.



5.2.4 Captive portal

The captive portal can be configured from the page « **Configuration** ► **Customization** ► **Portals** ».

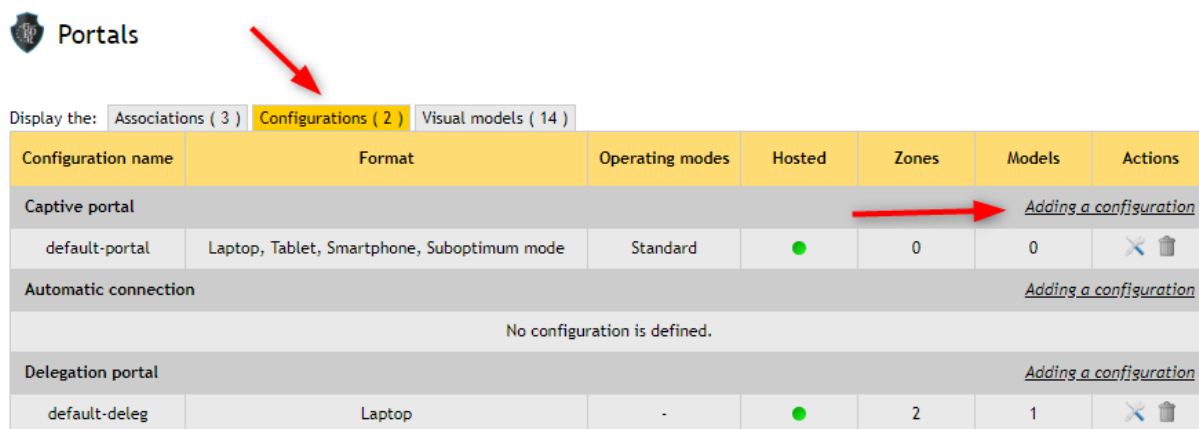


Figure 10: Configuring a captive portal

For example, a portal with self-registering by SMS.

Portals

Adding a captive portal configuration

Configuration settings

Configuration name
 Portal security password
This security is particularly important for modes with auto-registration or social networks.

Portal hosting

Portal hosting by controller
 Redirect to an external portal before controller portal
 External Portal

Portal format

Laptop Tablet Smartphone Suboptimum mode

Global options

Display subscription modes first
 Enable smart by-pass for Android CNA
 Define a policy governing the use of personal data

Authentication

[+ Add a new mode](#)

By credentials
 Associate portal authentication with RADIUS

Options

Display an information portal when the user equipment is recognized (MAC address)
 Define a service usage policy
 Redirect user once connected
 Ban the device of a user following wrong password attempts

Registration

[+ Add a new mode](#)

Portal with SMS registration
 User accounts will be created with the profile
 SMS sending account
 Enable sponsoring

Options

Warning: you have configured mandatory personal data input

User fields	Allow input	Mandatory
Login	<input type="checkbox"/>	<input type="checkbox"/>
Password	<input type="checkbox"/>	<input type="checkbox"/>
Last name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
First name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Gender	<input type="checkbox"/>	<input type="checkbox"/>
Birth date	<input type="checkbox"/>	<input type="checkbox"/>
Phone number	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Email address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Company name	<input type="checkbox"/>	<input type="checkbox"/>
Postal address	<input type="checkbox"/>	<input type="checkbox"/>
Preferred language	<input type="checkbox"/>	<input type="checkbox"/>
Interests	<input type="checkbox"/>	<input type="checkbox"/>

Figure 11: 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.

Portals

Display the: **Associations (3)** Configurations (3) Visual models (14)

Zone name	Portal type	Configuration name	Visual model name	Status	Actions
Incoming zones Adding an association					
Default-in	Captive portal	Guest	default	●	
	Delegation portal	default-deleg	default	●	
Outgoing zones Caution, only delegate portal may be associated with outgoing zone. Adding an association					
Default-out	Delegation portal	default-deleg	default	●	

Portals

Adding an association to an incoming zone

Association settings

- Zone
- Captive portal configuration
- Automatic connection configuration
- Delegation portal configuration
- Visual model
- Active

Figure 12: Association between portal and zone

5.2.5 Using a specific HTTPS port

The central controller expects the synchronization and portals and synchronization requests only to its 443 ports and on its outgoing networks. If the network cannot send the traffic to this port, you can still configure an internal port redirection on UCOPIA:

- In « **Configuration** ► **Network** ► **Filtering** ► **Port redirection** » tab add a new port redirection for the desired port (in the below example, the central controller has IP 78.91.234.56 and receives synchronization and portals traffic on port 1443)



Filtering settings configuration

Display the: Access to the controller (4) Opening port (1) Port redirection (1) Add

Source	Initial destination	Modified destination	Protocol	Initial ports	Modified ports	Status	Actions
Outgoing interface : out (Native)	The controller	78.91.234.56	TCP/UDP	1443	443	●	✕ 🗑️



Filtering settings configuration

Redirection modification

Note : Port redirection enables you to forward data to a resource, going through the controller.

Redirection settings

Source *	Outgoing interface	-	out (Native)
Initial destination *	The controller		
Modified destination host *	78.91.234.56		
Protocols	TCP/UDP		
Initial ports	1443		
Modified port	443		
Active	<input checked="" type="checkbox"/>		

* Mandatory fields Modify

For range of ports, use a dash '-'. Ex.: 2000-2050.

Figure 13: Creation of a port redirection

The same kind of configuration works for the RADIUS traffic to be received by the central controller on ports 1812/1813 and for syslog traffic to be received by the central controller on port 514.

Note

Default Facebook applications require the use of standard port 443 for HTTPs redirection. When using a different port, new Facebook applications have to be created.




5.2.6 RADIUS authentication

The on-premise Edge performs user authentication through the RADIUS protocol.

The RADIUS configuration is done from the page « **Configuration** ► **Authentication** ► **Radius** ».

Add a new NAS. Indeed, the Edge must be defined as a NAS for the central controller.

 **RADIUS configuration**
Adding a NAS

NAS settings

- Shortname *
- Shared secret *
- Authorized subnet or IP address *
 - IP address
 - Interface
 - Subnet address Subnet mask
- Profile label attributes
 -
 -
 -
- NAS architecture which performs a portal redirection
 - Manufacturer
 - Local exhaust
 - NAS-IP-Address




Figure 14: 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 Edge as well.
- Define the IP addressing containing the Edge IP address. If the Edge is behind a NAT, you have to configure an IP addressing containing the IP address seen by the central controller.
- Tick the box “**NAS architecture which performs a portal redirection**”
- Select “**Ucopia**” as Manufacturer
- Tick the box “**Local exhaust**” for local Internet breakout architecture.
- The field “**NAS IP-address**” is only useful in case of several Edge NATed with the same IP address. Defining this field overwrites the IP address of the RADIUS request and allows to differentiate the Edges. Otherwise, all the Edges are seen with the same IP address.

5.2.7 User profile

User profiles (and zones, services, password policies and URL categories) are configured on the central controller and automatically replicated on the Edge. Therefore, user profiles and other replicated components are read-only on the Edge.

5.2.8 Administrator account

To associate the Edge to the central controller, you need an administrator profile and account. The default administrator account can be used but it is recommended that you create an administrator on the central controller with limited privileges for security reasons. You can even create an administrator account with no right at all (read-only access, and disable access to all tabs).

You can create an administrator profile from the page « **Management** ► **Administrators** ► **Profiles** ».

Administrator profile management

Global settings

▶ Name

▶ Personal data rights

- Personal data read right ⓘ
- Personal data write right ⓘ

▶ Tools accesses

- Administration tool
- Delegation tool ⓘ

Administration rights

▶ Allowed menus

- Configuration
 - Network
 - Authentication
 - Zero configuration
 - Customization
 - Logging
 - High availability
 - Out-of-band
 - External services
 - Interfaces with the controller
- Management
 - Users
 - Administrators
 - Packages & Vouchers
 - Policies
- Monitoring
 - Real-time
 - User logs
 - System logs
- Operations
 - Backups
 - Reports
 - Maintenance
- Options
 - Documentation
 - Restart
 - Shut down

Allow visualization only for the above menus

▶ Allow administrator account management for the following profiles :

Allowed	<input type="button" value=" <<< Add"/> <input type="button" value=" Delete >>>"/>	Not allowed
		profil_admin_maintenance profil_super.deleg profil_deleg profil_admin profil_admin_deleg

* Mandatory fields

Figure 15: Adding an administrator profile

Then, you can create an administrator account from the page « **Management** ► **Administrators** ► **Accounts** ».

Administrator account management

User identity

Login *
 Last name

Password *
 First name

Confirm password *
 Mail

Phone number
 Duty

Profile

Available profiles *

profil_admin_mainten.
profil_super_deleg
profil_deleg
profil_admin
profil_admin_deleg
profil_edge_sync_adn

Administration tool **Yes**
 Delegation tool **No**
 Personal data read right **No**
 Personal data write right **No**

* Mandatory fields

Figure 16: Adding an administrator account

5.2.9 Social network authentication

Since 5.1.11 version and the new supported FQDN « central.access.network », user authentication is easiest with native social network applications. Adding specific customers applications is no more mandatory but change controller name on incoming network to “central” instead of “controller” that matches the embedded certificate.

5.3 Edge configuration

5.3.1 Association to the central controller

First of all, you must configure the association to the central controller. When launching the administration tool, you will be prompted with the following page.

Central controller configuration

Central controller association

<input type="radio"/> Central controller *	<input type="text" value="central.access.network"/>
<input type="radio"/> HTTPS Port *	<input type="text" value="443"/>
<input type="radio"/> Remote login *	<input type="text" value="edge_sync_admin"/>
<input type="radio"/> Remote password *	<input type="password" value="*****"/>
<input type="radio"/> Zone label *	<input type="text" value="Guest_Site-A"/>

* Mandatory fields

Figure 17: Edge Association to the central controller

Note

Until the association with the central controller is done, most menus of the administration tool will not be available.

You have to specify the **FQDN** of the central controller and the credentials of the administrator account (previously created on the central controller). **Do not use an IP address instead of the FQDN.**

The zone label must be specified as well, if the zone is not yet defined on the central controller, the zone will be automatically created.

The open-access URL used for the portal redirection (see next Section) will be automatically created with the following syntax.

https://<central_controller_FQDN>/zone/<zone_label>

Once the association successfully done, the menus of the administration tool will be available. However, user profiles, services, password policies and URL categories will be read-only (automatic synchronization with the central controller).

Note

The synchronization is scheduled to run every 5 minutes.

Please note that the very first synchronization can take some time and so profiles and zones will not appear in their dedicated menus on the edge controller, just after a successful association.

5.3.2 Using a specific HTTPS port

Due to network restrictions (e.g. if another application already uses port 443), you might need to redirect the HTTPS traffic flows from the edge controllers (captive portals and synchronization), to a different destination port to the central controller. Here is how to configure this:

- In « **Configuration** ► **Out-of-band** ► **Central controller** » enter the desired HTTPS port and validate the synchronization.
- In « **Configuration** ► **Customization** ► **Open-access URLs** » modify the automatically created URL in “HTTPS protocol” to

https://FQDN_central:<your new port HTTPS>/zone/<zone name>



(You need to enter the FQDN and not the IP address of the central controller in the Open-access URL, otherwise your customer will always see security messages displayed before the captive portal)

- **[Optional]** Only if other ports than 443 is used for the communication with the central by end users: In « **Configuration** ► **Network** ► **Filtering** ► **Opening port** » add a new port opening for the desired port (in the below example we try to reach the central controller on 78.91.234.56 on port 1443)



Filtering settings configuration

Display the: Access to the controller (4) Opening port (1) Port redirection (0) Add

Source	Destination	Protocol	Source ports	Destination ports	Logging	Status	Actions
Input interface : All	Host : 78.91.234.56	TCP/UDP	All	1443	●	●	 



Filtering settings configuration

Opening modification

Note :

The opening port allows the use of a port through the controller without authentication or access control.

Warning :

Opening for the following ports **80, 443, 8080, 3128** will be operational only if the destination type is **Subnet, Host or All destinations**

Opening settings

- Source *
- Log this opening traffic
- Open a predefined access
- Destination
- Protocols
- Source ports
- Destination ports
- Active

-
 Yes No
 Yes No
 -

To specify multiple ports, separate them with commas ',' . For ranges, use a dash '-'. Ex.: 2000-2050, 3000, 4000. To define all ports, let the field empty.

* Mandatory fields Modify

Figure 18: Creation of a port opening

The same kind of configuration works for the RADIUS traffic to be sent to the central controller ports 1812/1813.

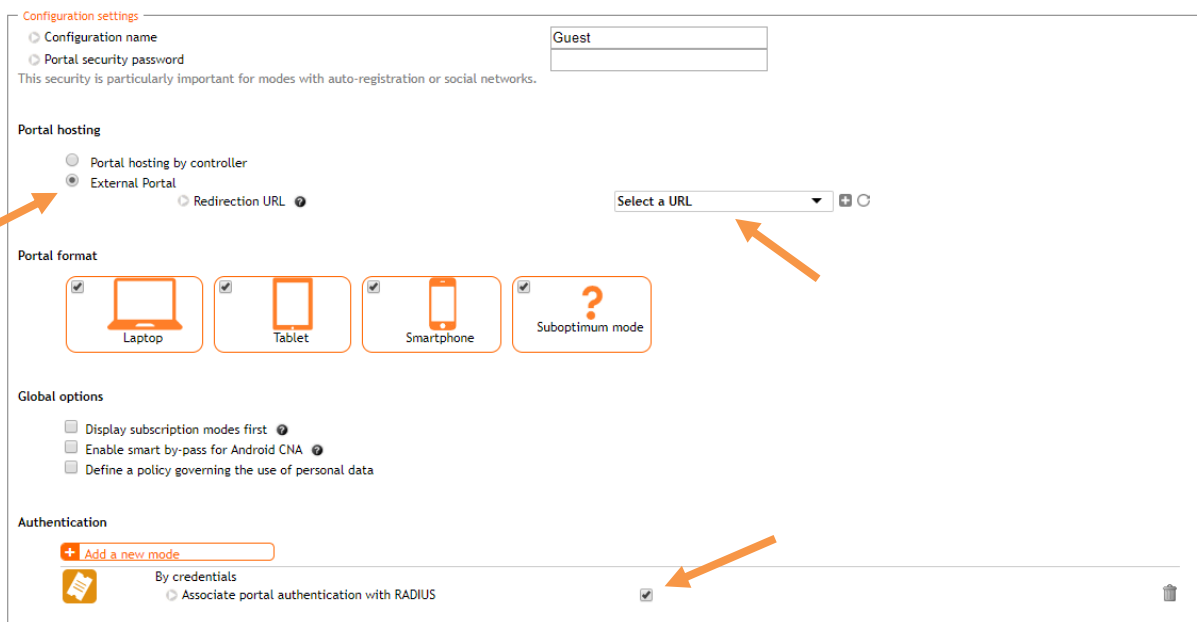
5.3.3 Portal redirection

From the page « **Configuration ► Customization ► Portals** », add a new portal configuration as follows.

- Select « **External portal** » option and choose for the redirection the **open-access URL automatically created** by the association process.
- Add the mode « Authentication by credentials » and tick the box « Associate portal authentication with RADIUS ».

Portals

Adding a captive portal configuration



Configuration settings

- Configuration name: Guest
- Portal security password: [Empty field]
- This security is particularly important for modes with auto-registration or social networks.

Portal hosting

- Portal hosting by controller
- External Portal**
- Redirection URL: Select a URL

Portal format

- Laptop
- Tablet
- Smartphone
- Suboptimum mode

Global options

- Display subscription modes first
- Enable smart by-pass for Android CNA
- Define a policy governing the use of personal data

Authentication

- [+ Add a new mode](#)
- By credentials
- Associate portal authentication with RADIUS


Figure 19: Configuring a portal redirection to the central controller

Associate the configuration to the zone previously created. A portal visual model must be chosen for this association.

5.3.4 RADIUS authentication

Go to the RADIUS page configuration « **Configuration** ► **Authentication** ► **Radius** », and configure both the realm NULL and realm DEFAULT in remote mode as follows.

- Optionally you can enable the accounting mechanism which is mandatory when using quota or time credit. Activating the replication on other realms allows to replicate the traffic associated to the realm on other realms.
- A default user profile can be defined if the central controller doesn't send any profile information.
- A default user profile can be defined if the profile sent by the central controller doesn't exist on the Edge.
- The IP address of the central controller is automatically filled, according to the FQDN of the central controller.
- The authentication port is UDP/1812.
- The RADIUS secret must be the same as the central controller.

 **RADIUS configuration**
 Realm modification *NULL*

Realm settings

LOCAL RADIUS

Remote RADIUS

Enable accounting

Enable accounting replication

Default profile in case of missing attribute

Default profile in case of wrong attribute

WISPr provider

Main RADIUS authority server

Authority RADIUS server IP address *

RADIUS server authentication port *

RADIUS server secret *

Secondary RADIUS authority server (optional)

Secondary RADIUS authority server IP address

Secondary RADIUS server authentication port

Secondary RADIUS server secret

Working choice fail-over load-balance

* Mandatory fields

Figure 20: Configuring the NULL RADIUS realm

RADIUS configuration

Realm modification *DEFAULT*

Realm settings

LOCAL RADIUS

Remote RADIUS

Enable accounting

Enable accounting replication

Default profile in case of missing attribute

Default profile in case of wrong attribute

Send the realm to the remote RADIUS

WISPr provider

Main RADIUS authority server

Authority RADIUS server IP address *

RADIUS server authentication port *

RADIUS server secret *

Secondary RADIUS authority server (optional)

Secondary RADIUS authority server IP address

Secondary RADIUS server authentication port

Secondary RADIUS server secret

Working choice fail-over load-balance

* Mandatory fields

Figure 21: Configuring the DEFAULT RADIUS realm

5.3.5 Additional networks and VLANs reachable through outgoing policies (optional)

You need to create the outgoing networks in the EDGE controller that will be used for Internet connection by the connected users but also to communicate with the Central controller.

If you have 2 different subnets (n°1 for Internet access; n°2 for communication between the Edge and the central), note that:

- The user, once connected on the Edge, will be assigned the policy with outgoing network n°1
- Thus, in order for the user to be able to see the feedback page (post-connection page), the connected user must be able to communicate to the Central controller. So, you must add in the default outgoing policy the available VLAN "network n°2" (and the associated static routes to reach the Central controller if the central controller is in a remote subnet). See an example below where the central controller is in a distant network 192.168.193.0/24 and reachable through the default VLAN OUT:

Configuration Management Monitoring Operations Documentation Restart Shut

Configuration of outgoing networks

Delete	VLAN number	Subnet address	Subnet mask	Controller IP address	Addressing mode	Outgoing zones	Administration access	Delegation access	Default output	Add
<input type="checkbox"/>	out	192.168.38.0	255.255.255.0	192.168.38.4	Fixed	Interconnection_Central	●	●	●	
<input type="checkbox"/>	5	10.0.1.0	255.255.255.0	10.0.1.2	Fixed	Internet_out	●	●	●	

Outgoing addressing policies configuration

Addressing policies for logged-in users

Delete	Policy name	Profiles affected	Mode	Outgoing network	NAT IP address	NAT netmask	Add
<input type="checkbox"/>	Default outgoing policy	WIFI_INVITE	NAT	5	10.0.1.2	255.255.255.0	

Caution, users supported by the zero-configuration IP will be NATed even if their profile using an outgoing addressing policy routed.
When web traffic is redirected to the controller proxy, whatever the outgoing policies, these will inevitably apply an address translation (NAT).

Figure 22: Adding a network reachable through outgoing policies

(to understand the flow exchanges, see the matrix in Annex 1)

5.3.6 Automatic MAC address authentication (optional)

In order to activate the automatic MAC address authentication, you have to configure an automatic connection with the « **RADIUS MAC authorization** » mode enabled.

You can add an automatic connection from the page « **Configuration ► Customization ► Portals** ».

Portals

Display the: Associations (4) Configurations (3) Visual models (14)

Configuration name	Format	Operating modes	Hosted	Zones	Models	Actions
Captive portal Adding a configuration						
default-portal	Laptop, Tablet, Smartphone, Suboptimum mode	Standard	●	0	0	
Guest	Laptop, Tablet, Smartphone, Suboptimum mode	Standard, SMS	●	2	1	
Automatic connection Adding a configuration						
No configuration is defined.						
Delegation portal Adding a configuration						
default-deleg	Laptop	-	●	2	1	

Figure 23: Adding an automatic connection

Tick/Check the box « **Enable RADIUS MAC authorization** ».

Configuration settings

Configuration name auto-mac_Guest_Site-A

Enable RADIUS MAC authorization

- Select RADIUS MAC realm

Enable RADIUS LOGIN authorization

Figure 24: Configuring an automatic connection

Associate the automatic connection to the right zone.

Portals

Display the: Associations (4) Configurations (3) Visual models (14)

Zone name	Portal type	Configuration name	Visual model name	Status	Actions
Incoming zones				Adding an association	
Default-in	Captive portal	Guest	default	●	
	Delegation portal	default-deleg	default	●	
Guest_Site-A	Captive portal	Guest	default	●	
Outgoing zones <small>Caution, only delegate portal may be associated with outgoing zone.</small>				Adding an association	
Default-out	Delegation portal	default-deleg	default	●	



Portals

Adding an association to an incoming zone

Association settings

Zone Guest_Site-A ▼

Captive portal configuration No configuration ▼

Automatic connection configuration auto-mac_Guest_Site-A ▼

Delegation portal configuration No configuration ▼

Visual model default ▼

Active

Add

Figure 25: Association between automatic connection and zone

5.3.7 High Availability on Edge controllers (optional)

From 5.1.11 version, two Edge controllers can be associated in a High Availability architecture. This architecture can only be set with one active controller and one passive controller.

No configuration is needed on the passive Edge as everything will be synchronized right after the High Availability association.

Once the future master Edge is correctly associated to the central and configured, you will need to go to « **Configuration ► High availability ► Redundancy and load balancing** » page to enable High Availability.

Redundancy and load balancing

Enable

Warning, this controller have an 'Edge' license, so the configuration is limited to two controllers (active/passive) only.

Label of the cluster *

Communication interface between controllers

Number of controllers

IP addresses of the controllers

Controller	IP address	License type	Status
# 1	<input type="text" value="10.1.66.102"/>	Load balancing 250 connections	Active manages the node(s) 1
# 2	<input type="text" value="10.1.255.167"/>	Redundancy 250 connections	Passive

Initial VRID

VRRP interval

Number of active controllers

Enable preemption

Virtual addresses

on incoming VLANs:

VLAN 1 (192.168.100.0/255.255.255.0) for the node 1 (VMAC: 00-00-5E-00-01-42)

on outgoing VLANs:

VLAN 1 (10.1.0.0/255.255.0.0) for the node 1 (VMAC: 00-00-5E-00-01-43)

Routing

If routing mode is enabled, network routing is required :
- 192.168.100.0/24 to outgoing virtual IP address 1

Figure 26: Two associated Edge controllers in High Availability architecture

Only the master Edge data are synchronized with the central controller. The passive Edge data is synchronized through High Availability synchronization mechanism.

The High Availability cluster label is sent to the central controller in order to see, on central, the Edge controllers that belongs to a cluster.

5.4 Edge administration from the central controller

From the page « **Configuration** ► **Out-of-Band** ► **Edge** », you can visualize all the Edges associated to the central.

The page shows information about communication between the Edge and the central controller and additional information such as UCOPIA version inconsistency.


You can dissociate an Edge controller by clicking on the corresponding garbage icon. A warning message will appear on the Edge to indicate that the Edge is no longer associated to the central controller.

Edge administration

Search filter

Select a field

Reinit match all rules (AND) Search

Edge controller list							
<input type="checkbox"/>	Serial number	IP address	Version (build)	Last communication time	Status	Additional information	Actions
<input type="checkbox"/>	R2401623	10.1.45.3	5.1 (build 16012504)	2016-09-12 10:30:12	●		

Page 1 of 1 View 1 - 1 of 1

Figure 27: Edge administration from the central controller

6 Annex 1: detailed flow diagram

The following diagram describes in detail the flows between the user at remote site, the Edge and the central controller for authentication and logout processes.

6.1 Portal authentication

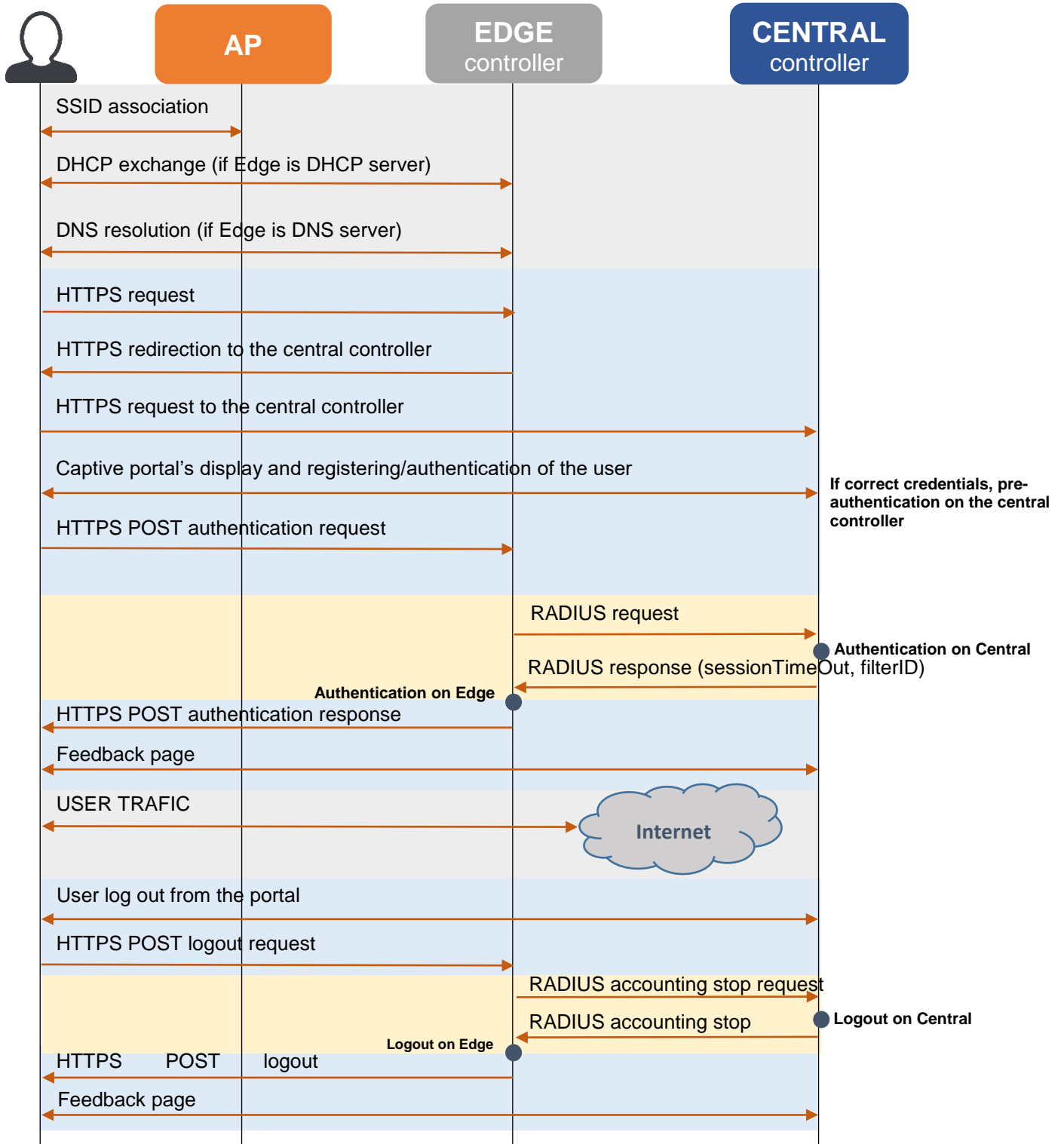


Figure 28: Detailed flow diagram

6.2 Automatic MAC address authentication

If a user has already successfully connected to the network and comes back with the same device, you can decide to automatically recognize and connect the user device on UCOPIA.

In this case, the Edge initiates a connection request, in the form of a RADIUS Access-Request, to the central controller whenever it detects a MAC address arriving on the network. If the central controller recognizes the MAC address, then the device is automatically connected with the associated profile and the central controller sends a RADIUS Access-Accept. All this exchange is called the MAB (MAC Auth Bypass).

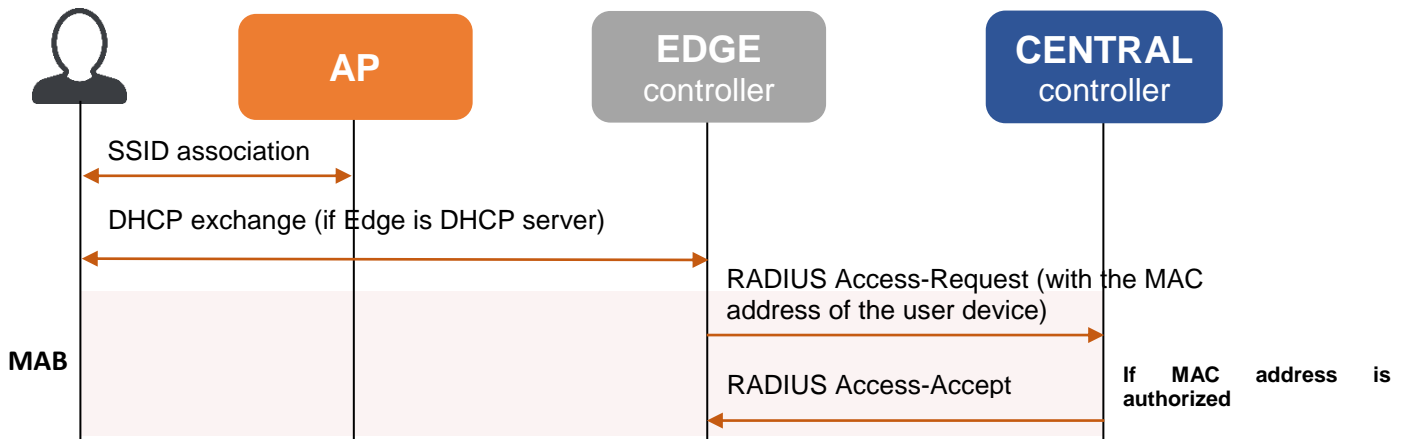


Figure 29: Flow diagram for automatic MAC address authentication

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	http://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: Check-List

Central

- | | |
|---|-----------|
| <input type="checkbox"/> Prepare firewall to allow internet access and ports 443, 1812 and 1813 | Optional |
| <input type="checkbox"/> Prepare certificate | Optional |
| <input type="checkbox"/> Change admin password | Mandatory |
| <input type="checkbox"/> Configure OUT network | Mandatory |
| <input type="checkbox"/> Configure DNS | Mandatory |
| <input type="checkbox"/> Install license online / offline | Mandatory |
| <input type="checkbox"/> Update to defined version | Mandatory |
| <input type="checkbox"/> Disable updates | Optional |
| <input type="checkbox"/> Create named admin profile and account (do not use 'admin' any more) | Mandatory |
| <input type="checkbox"/> Create profile and admin for edge sync | Mandatory |
| <input type="checkbox"/> Enable maintenance tunnel | Optional |
| <input type="checkbox"/> Configure time server (same as on edge) | Mandatory |
| <input type="checkbox"/> Change controller name | Mandatory |
| <input type="checkbox"/> Insert new certificate | Optional |
| <input type="checkbox"/> Create zones | Mandatory |
| <input type="checkbox"/> Create profiles | Mandatory |
| <input type="checkbox"/> Create / import visual models | Mandatory |
| <input type="checkbox"/> Create captive portal configuration | Mandatory |
| <input type="checkbox"/> Bind zones and visual models | Mandatory |
| <input type="checkbox"/> Configure RADIUS NAS | Mandatory |

When Edge is ready:

- | | |
|---|-----------|
| <input type="checkbox"/> Disable maintenance tunnel | Optional |
| <input type="checkbox"/> Disable useless access to CLI, admin tool and delegation | Mandatory |

Edge

<input type="checkbox"/> Prepare firewall to allow internet access, and access to central	Optional
<input type="checkbox"/> Prepare certificate	Optional
<input type="checkbox"/> Change admin password	Mandatory
<input type="checkbox"/> Configure OUT network	Mandatory
<input type="checkbox"/> Configure DNS	Mandatory
<input type="checkbox"/> Install license online / offline	Mandatory
<input type="checkbox"/> Update to the same version as the central	Mandatory
<input type="checkbox"/> Disable updates	Optional
<input type="checkbox"/> Enable maintenance tunnel	Optional
<input type="checkbox"/> Configure time server (same as on central)	Mandatory
<input type="checkbox"/> Change controller name	Optional
<input type="checkbox"/> Insert new certificate	Optional
<input type="checkbox"/> Configure DNS entry for central	Optional
<input type="checkbox"/> Sync with central	Mandatory
<input type="checkbox"/> Configure zone on incoming networks	Mandatory
<input type="checkbox"/> Configure Radius realms	Mandatory
<input type="checkbox"/> Create captive portal configuration (external portal)	Mandatory
<input type="checkbox"/> Enable « Associate portal authentication with RADIUS » in portal configuration for credentials authentication	Mandatory
<input type="checkbox"/> Create automatic portal configuration for MAC authentication	Optional
<input type="checkbox"/> Bind zones, configurations and visual models	Mandatory
<input type="checkbox"/> Disable maintenance tunnel	Optional
<input type="checkbox"/> Disable useless access to CLI, admin tool and delegation	Mandatory