UCOPIA

TURN YOUR WI-FI UP

Out-Of-Band Cisco WLC architecture

Version 5.1

Table of contents

Table of figures

1 Introduction

This document describes the Out-of-Band architecture with Cisco Wireless LAN Controllers (WLC) on premise. This architecture is composed of a UCOPIA central controller with an ADVANCE Global license (designed as “central controller” in this document), one or more Cisco WLCs that is/are connected to the central controller and one or more Access Points (AP) that are connected to the WLC. The central controller is typically in a datacenter, and the WLCs at customer sites (e.g. hotel, restaurant, agency, etc.).

Commenté [CL1]: One or more ?
Prendre le cas le plus général avec WLC avec :
-Un WLC sur site distant
-[Possible ?] une cascade de WLC

The goal of the Out-of-Band Cisco WLC architecture is to build a centralized architecture over your existing Cisco Wi-Fi infrastructure, allowing centralized management of the main UCOPIA features: captive portals, authentication server, provisioning, user directory. The local Internet access of each site is used for the user traffic.

The on-premise Cisco WLCs ensure portal redirection to the centralized UCOPIA controller and authentication process.
The central controller can be a high availability cluster (Advance product line).

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

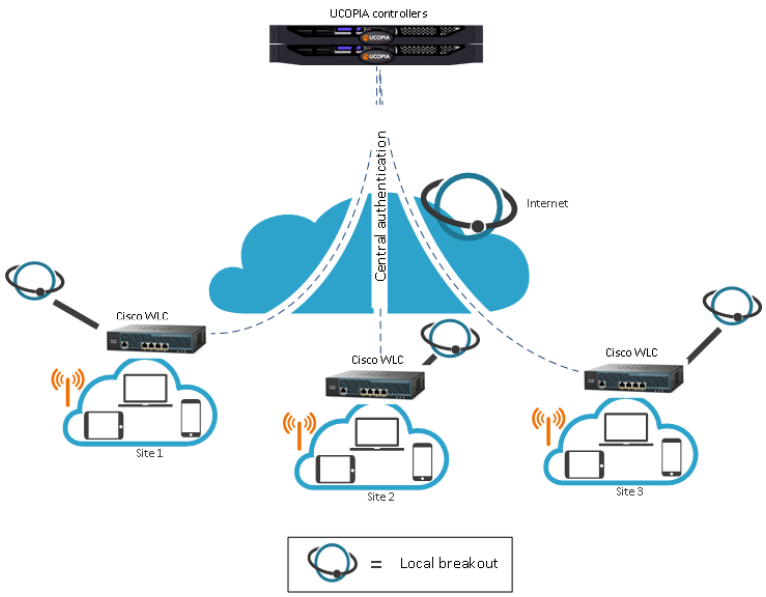


Figure 1 : Global Out-of-Band Cisco WLC architecture

2 User experience workflow

Let's consider a Guest user trying to get a Wi-Fi Internet connection on a site (site A) where a Cisco WLC 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 Cisco WLC 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 Cisco WLC and the central controller through the RADIUS protocol. The user's validity settings are sent to the Cisco WLC in order for it to locally apply these validity policies related to the user (RADIUS attributes are used for that purpose).
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.

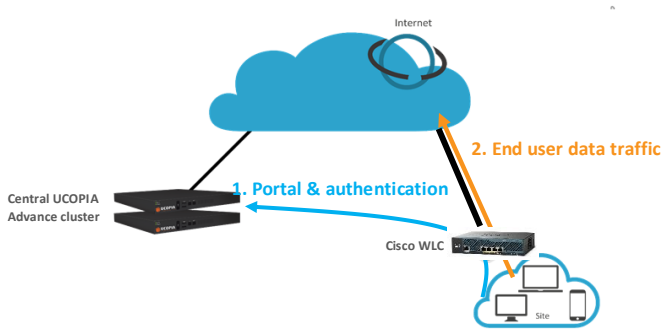


Figure 2 : User traffic flow

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…

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

Note: The Cisco WLC supports only one profile per SSID. As Cisco WLCs don't have a full knowledge of the profile settings on UCOPIA controller (such as starting validity date, bandwidth limitation …) via the authentication exchanges with the UCOPIA controller, these settings should be locally configured on the profile created and used by the Cisco WLC

Commenté [CL2]: Partial centralization of user profiles :
-Seul le profil du WLC est utilisé (un profil unique pour un SSID, défini ds WLC)
-Par contre, prise en compte du crédit-temps et du quota par le WLC, choppé dans les infos RADIUS

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 Cisco WLC and UCOPIA versions

The Out-Of-Band Cisco WLC architecture requires a version ≥ 8.3.102.0 to configure walled gardens (previous versions don't support this feature). Note that all Cisco WLCs are not compatible with this feature (please refer to the Cisco release notes for a full list of compatible hardware).

Only UCOPIA controllers from version 5.1.11 can set up an Out-Of-Band Cisco WLC configuration.

3.2.2 Supported authentication / registration modes

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

- 802.1x
- Shibboleth
- Limited mail 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

3.2.3 Centralization of user logs

Unlike other Cisco hardware, the Cisco WLC does not log wireless traffic, so it is not possible to retrieve user logs such as connected users, sessions, visited URLs, …

3.2.4 Profile differentiation

As the user traffic doesn't go through UCOPIA, the Cisco WLC is in charge with enforcing the right policy on the user.

However, the Cisco WLC supports only one profile per SSID (the RADIUS field "Filter-Id" is not supported), so it is not possible to differentiate a user from another.

3.2.5 User disconnection

Some disconnection mechanisms aren't available in the Out-Of-Band Cisco WLC architecture, as explained below:

	Supported in the Out-Of-Band Cisco WLC architecture?
Increased security	**No** *Description: the user will be disconnected from UCOPIA controller but not on Cisco WLC. That can be problematic for users with time credit as no time will be deducted from the time credit on UCOPIA while the user will access the Internet.*
UCOPIA auto disconnect	**No** *Description: because user traffic doesn't go through the UCOPIA controller, the autodisconnect feature doesn't make sense. So, as soon as an Out-Of-Band architecture is configured, the central controller disables its autodisconnect feature.* *Only the autodisconnect on Cisco WLC will be able to disconnect a user after a given inactivity period.*
Manual disconnection	**No** *Description: The Cisco WLC doesn't properly redirect to the UCOPIA controller portal after receiving a disconnection request. The disconnection button has been deleted from the feedback page in the Out-Of-Band Cisco WLC.*
Reached max quota	**No**

	Description: The Cisco WLC only sends the information of the number of packets consumed by the user when the user is disconnected, via a RADIUS Accounting Stop. There is no regular RADIUS Interim Accounting message sent to UCOPIA, which means that UCOPIA ignores what the user has consumed in terms of quota until the user session is over.
Expired credit time	**Yes**
Reached ending validity date	**Yes**
Forced disconnection	**Yes**
User deletion from the delegation tool	**Yes**

3.2.6 Network failure

The user directory is centralized and used by all Cisco WLCs on local sites. In case of network failure between the Cisco WLCs and the central controller, the user directory and captive portal will not be available, so no new user will 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 Global 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 isn't completely consumed by a given site.

5 UCOPIA configuration

5.1 Prerequisites

5.1.1 Time synchronization (on UCOPIA and Cisco)

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

This time synchronization is particularly important for profiles with expiration date as the central UCOPIA controller will send to the Cisco WLC an explicit end date for the user connection. If the time isn't similarly between the Cisco WLC and UCOPIA controller, it will directly impact the authorized time connection of users.

On Cisco: configure the NTP server in the Cisco WLC Advanced configuration interface "Controller > NTP > Server"

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 communicates with all the users on the remote sites as well as with the remote Cisco WLC (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.

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.

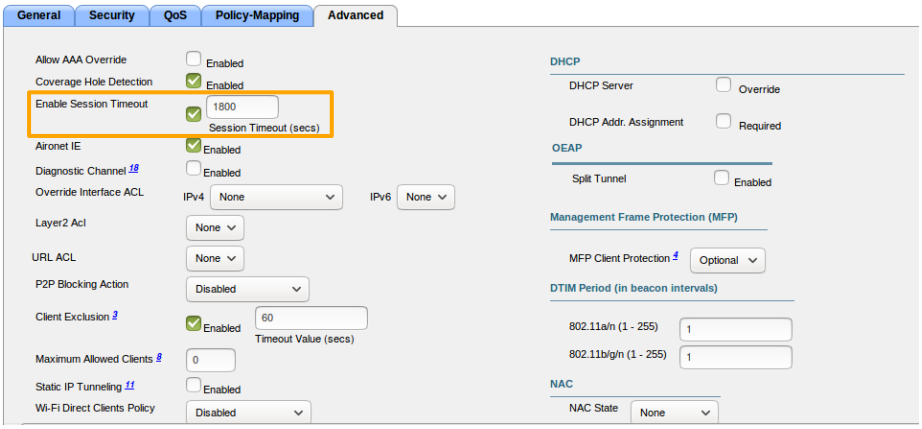
Source @IP	Destination @IP	Port
User's equipment on remote site	Central controller	TCP/443
Cisco WLC	Central controller	TCP/443, UDP/1812, UDP/1813, UDP/514 (for syslog)

These are the flows that should be opened from the Cisco WLC to the central in order to enable the Cisco WLC to communicate with their central.

5.1.3 Auto disconnection settings (on Cisco WLC)

As the user traffic goes through the Cisco WLC and not the UCOPIA controller, the Cisco WLC is responsible for detecting an inactive user and disconnecting him.

This "auto disconnection" feature on Cisco WLC is specific to each WLAN. It can be configured on the Advanced configuration interface in "WLANs > *Your WLAN name* > Advanced > Enable Session Timeout".



If a user has a limited time credit, then it is recommended to choose the lowest possible value for the auto disconnection so that, when the user isn't active on the network, he is quickly disconnected from Cisco WLC and then from UCOPIA (and he doesn't unnecessarily consume his time credit).

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 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 in the redirection URL configured on the on-premise Cisco WLCs. 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 ***Administration->Zones.***

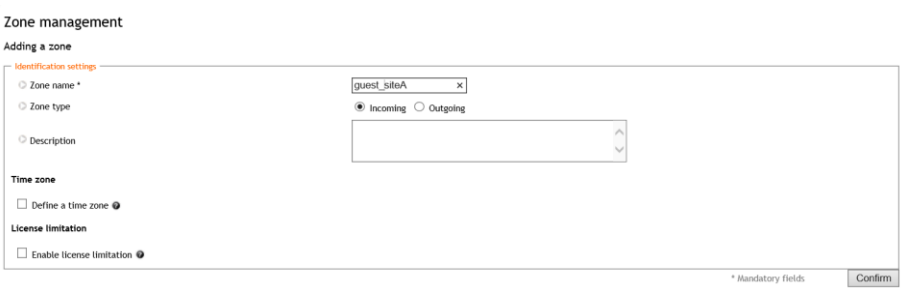


Figure 3 : Adding an incoming zone

5.2.2 Captive portal

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

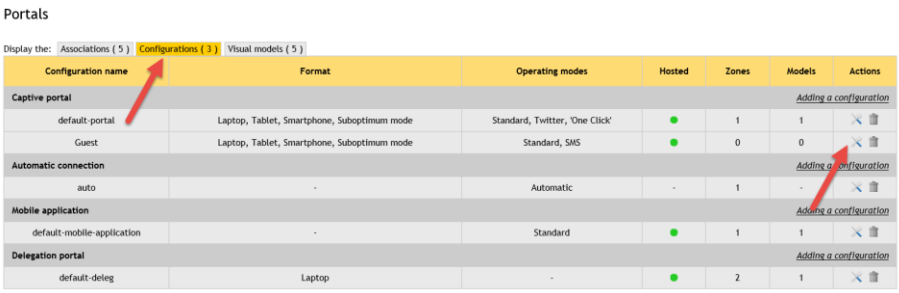


Figure 4 : Configuring a captive portal

For example, a portal with self-registering by SMS

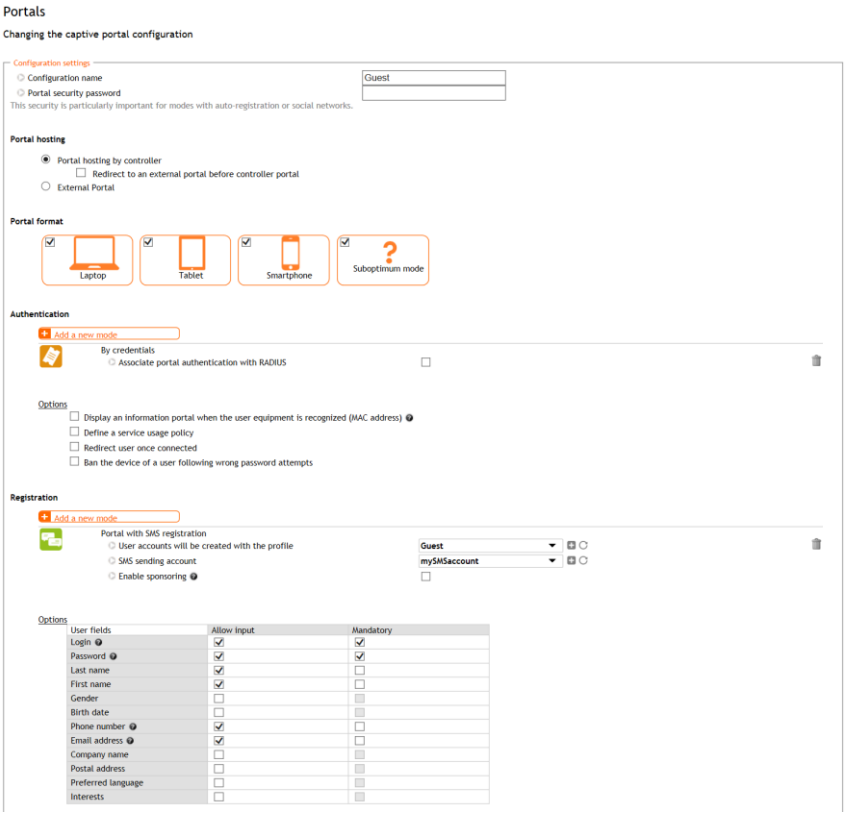


Figure 5 : Example of portal configuration with self-registering by SMS

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

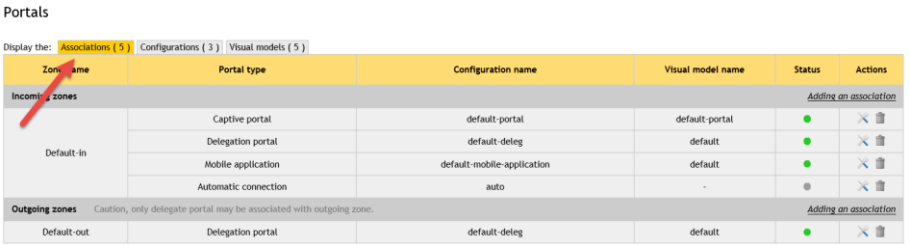


Figure 6 : Association between portal and zone

5.2.3 RADIUS authentication

The Cisco WLC can perform user authentication through the RADIUS protocol.

The RADIUS configuration is done from the page ***Configuration>Authentication>Radius***.

Add a new NAS, as the Cisco WLC must be defined as a NAS for the central controller.

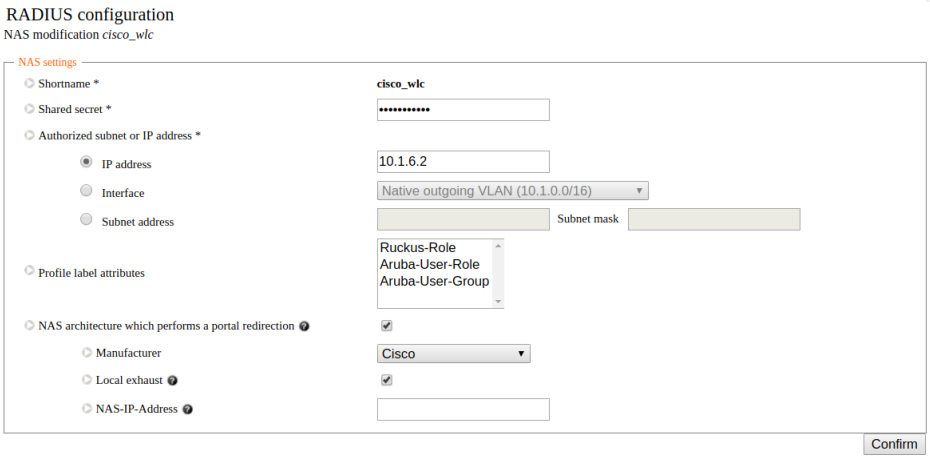


Figure 7 : Adding a NAS

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 Cisco WLC as well.

- Define the IP addressing containing the Cisco WLC IP address. If the WLC 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 “Cisco” as Manufacturer
- Tick the box “Local exhaust” for local Internet breakout architecture.

The field “NAS IP-address” is only useful in case of several Cisco WLCs NATed with the same IP address. Defining this field overwrites the IP address of the RADIUS request and allows to differentiate the Cisco WLCs. Otherwise, all the Cisco WLCs are seen with the same IP address.

5.2.4 User profile

Define your user profiles, their time- and MAC- based settings (refer to 3.2.4. to have the list of supported UCOPIA features).

5.2.5 [Optional] New domain name and certificate

By default, the FQDN (Fully Qualified Domain Name) of an UCOPIA controller is “controller.access.network”. A signed certificate is installed matching this FQDN.

If the customer doesn’t have control on his DNS server and can’t create a DNS entry in order to resolve the domain name “controller.access.network” with the IP address of its own UCOPIA controller.

Then, both the FQDN and the certificate must be modified on the central controller, so that the user clicking on the social network button isn’t redirected to our UCOPIA public IP address.

Commenté [MB3]: Also add « central.access.network » ?

Commenté [MB4]: This certificate should not be used in production

Commenté [MB5]: Syntax issue

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

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

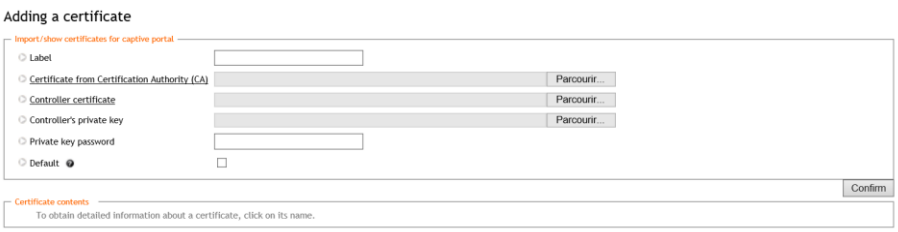


Figure 8 : Adding a new certificate for the captive portal

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.***

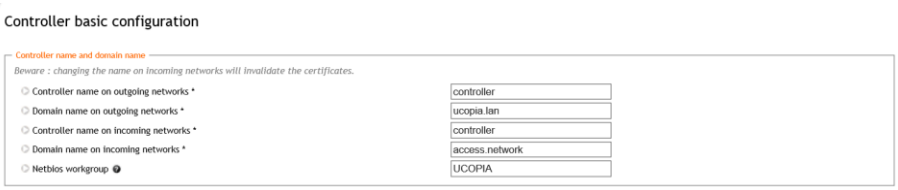


Figure 9 : Modifying a controller name

5.3 Cisco WLC configuration

Connect on your Cisco WLC Advanced configuration interface.

5.3.1 Creation of a WLAN and its associated SSID

Go to section “WLANs > WLANs > WLANs”, select “Create New” then “Go”

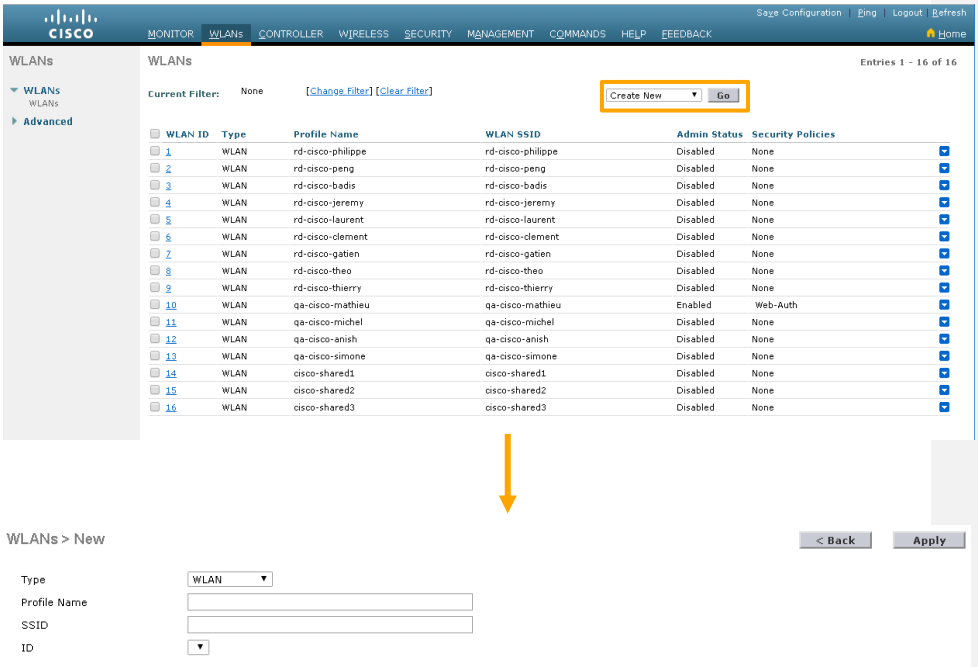


Figure 10 : Creation of a WLAN

Note: A WLAN is associated to one profile and one SSID only. If you need another SSID, you have to create a new WLAN.

5.3.2 Creation of an Access Control List

Create a new ACL to allow a communication between the Cisco WLC and the UCOPIA central controller. Go to section “Security > Access Control Lists > Access Control Lists” and add a new IPv4 ACL.

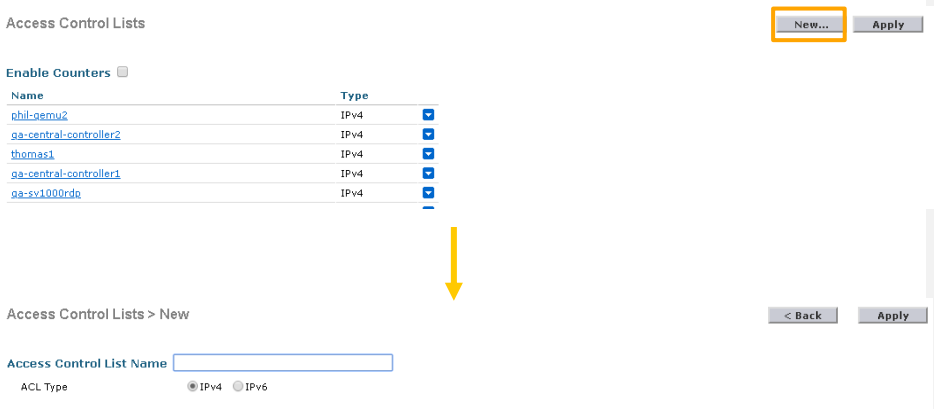


Figure 11 : Add a new Access Control List

Edit the created ACL and add 2 rules for the UCOPIA central:

- For incoming traffic
  - Source: IP address + add the IP address of the UCOPIA central
  - Destination: Any
  - Protocol: Any
  - DSCP: Any
  - Direction: Outbound
  - Action: Permit

- For outgoing traffic
  - Source: Any
  - Destination: IP address + add the IP address of the UCOPIA central
  - Protocol: Any
  - DSCP: Any
  - Direction: Inbound
  - Action: Permit

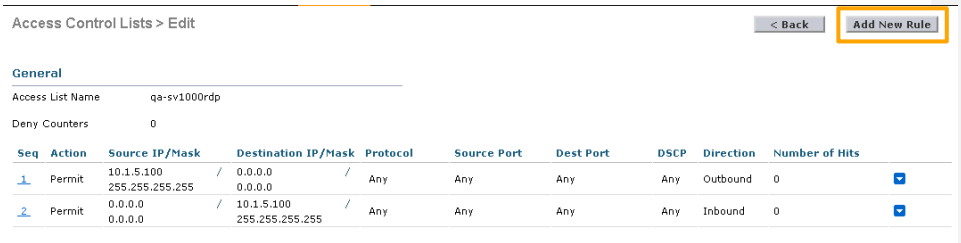


Figure 12 : Configuration of the new Access Control List

Then edit your WLAN and configure it as following:

- Go to section “Security > Layer 3”
- Select the Layer 3 security “Web Policy” and the mode “Authentication”
- In section “Preauthentication ACL IPv4”, select your previously created ACL

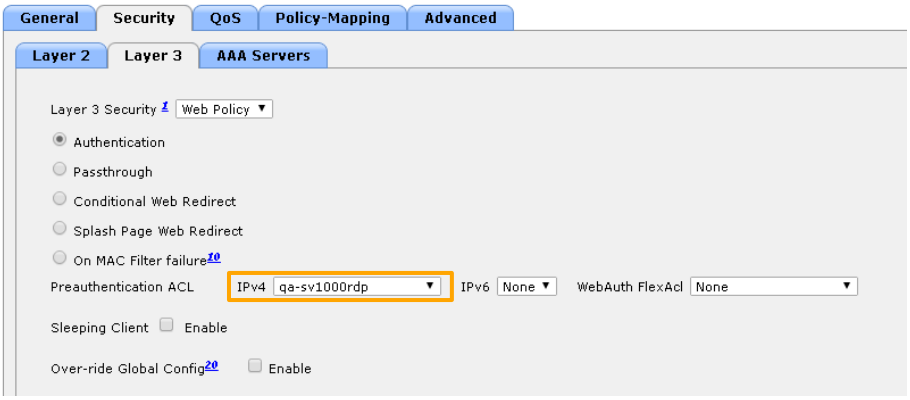


Figure 13 : Association of the ACL to the WLAN

5.3.3 Redirection to a captive portal

In order to define the redirection URL to the UCOPIA central controller:

- Go to section “Security > WebAuth > WebAuth Login Page” and define your default captive portal:
- Web Authentication Type = External
- External Webauth URL = https://<central controller FQDN>/zone/<zone label>
- Redirect URL after login = <your welcome page>

If needed, you can configure walled garden to open the access to certain URL even for unauthenticated users.

Note that if you have changed the default controller FQDN "controller.access.network", then the certificate must be modified on the central controller and you must ensure that the new FQDN can be correctly resolved)

Figure 14 : Configuration of the Web Login Page

5.3.4 Configuration of the external RADIUS server

Create a new RADIUS server:

- Go to section “Security > AAA > RADIUS > Authentication”
- Add an entry and provide the following information:
  - The server IP Address (Ipv4/Ipv6)
  - The port number to be used (default port 1812)
  - The shared RADIUS secret must be the same as the central controller

- Go to section “Security > AAA > RADIUS > Accounting”
- Add an entry and provide the following information:
  - The server IP Address (Ipv4/Ipv6)
  - The port number to be used (default port 1813)
- The shared RADIUS secret must be the same as the central controller

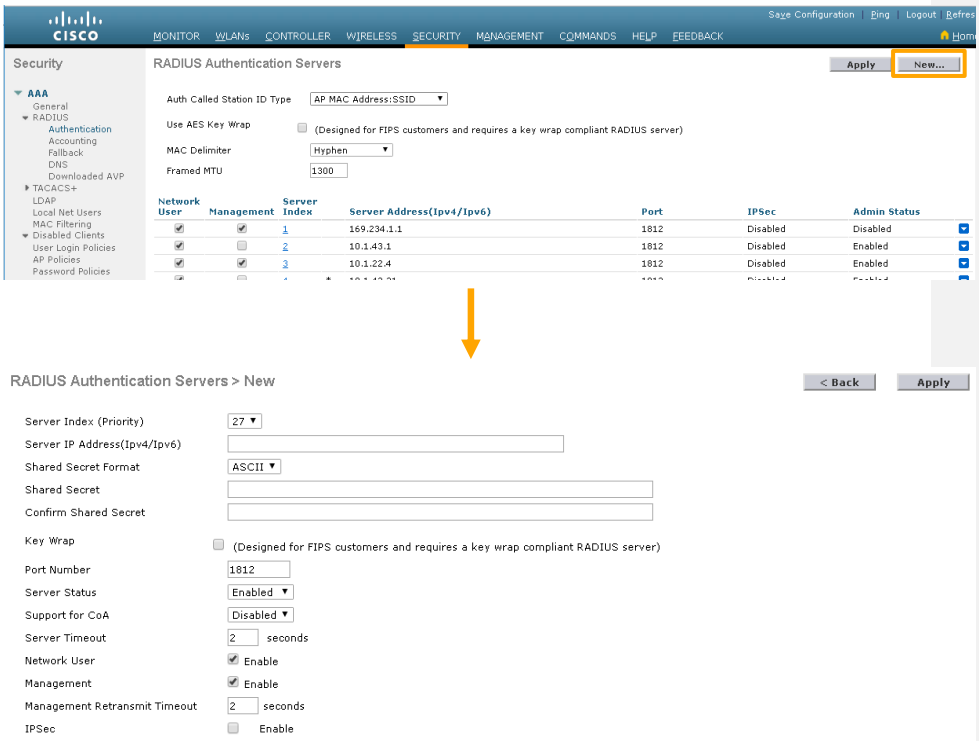


Figure 15 : Creation of a RADIUS Authentication server

Then associate the RADIUS server to your WLAN:

- Edit your WLAN and go to section “Security > AAA Servers”
- Enable “Authentication Servers” and select your RADIUS authentication server
- Enable “Accounting Servers” and select your RADIUS accounting server

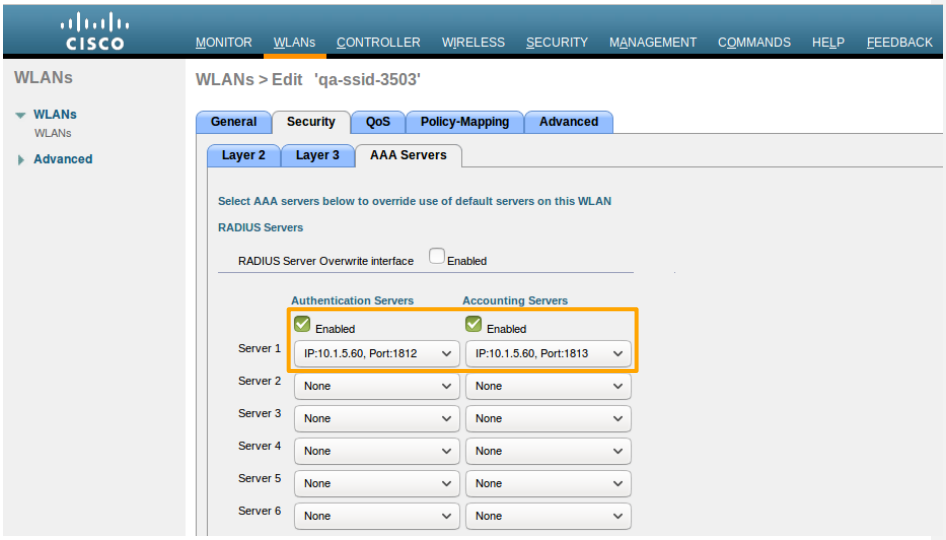


Figure 166: Association of the RADIUS configuration to the WLAN

5.3.5 Configuration of a user profile

The Cisco WLC supports only one profile per SSID, so profiles per user are not supported.

5.3.6 Configuration of the syslog server

In order to configure the syslog export:

- Go to section “Management > Logs > Config”

<missing part>

Commenté [CL6]: Mettre l’info qqpart que cette archi ne permet pas de collecter les journaux de connexion requis par la loi 2006 anti-terroriste

+ préciser que le client peut utiliser un serveur syslog externe pour récupérer des informations de WLC (pour récupérer des infos sur l’état du WLC…), par contre, le WLC ne renvoie pas les infos de journaux de connexion

Commenté [MB7]: To add

5.3.7 Configuration of a certificate for 1.1.1.1

<missing part>

Commenté [MB8]: To add?

5.3.8 Activation of the SSID

Edit your WLAN and ensure that the box “Status” is checked. Apply your modifications in order to activate the SSID.

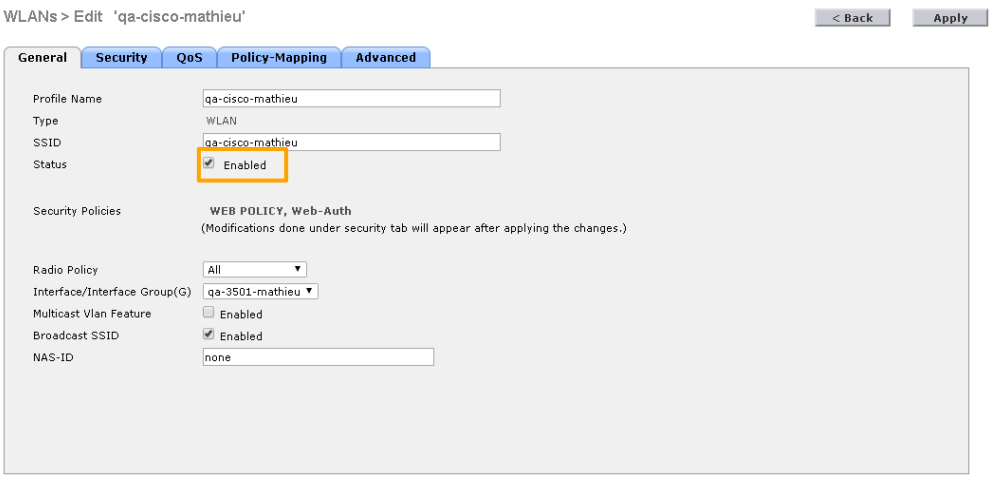


Figure 177: Activation of the SSID

6 Annex 1: detailed flow diagram

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

6.1 Portal authentication

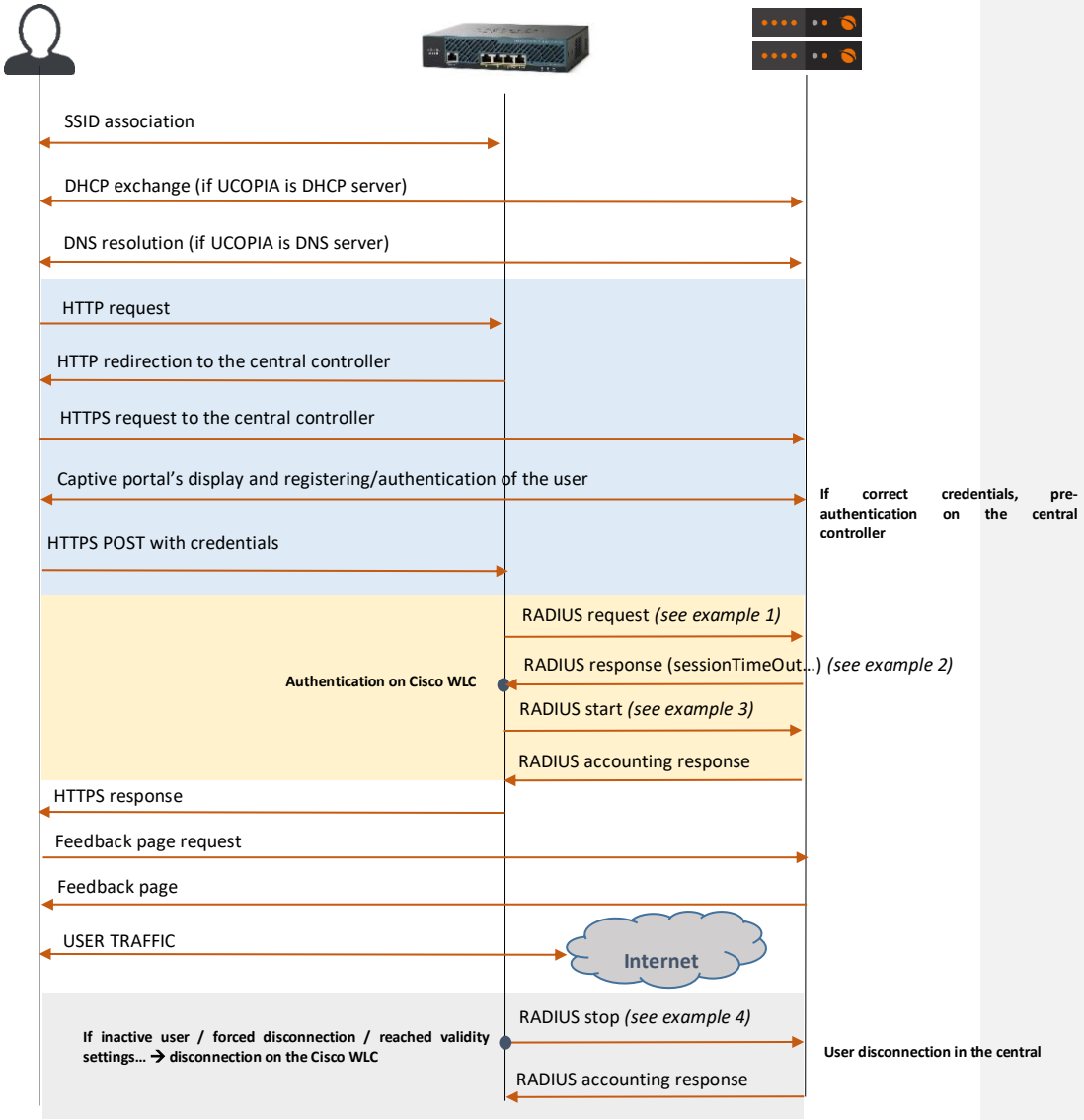


Figure 18: Detailed flow diagram

Example 1: RADIUS Access-Request

```
Thu Jan 18 17:19:47 2018
        Packet-Type = Access-Request
        User-Name = "hi2o6zt"
        Service-Type = Login-User
        NAS-IP-Address = 10.1.6.2
        NAS-Port = 3
        Cisco-AVPair = "audit-session-id=0a01060200000b055a60c879"
        Framed-IP-Address = 10.1.255.98
        Acct-Session-Id = "5a60c923/40:d3:ae:fa:3a:ce/493"
        NAS-Identifier = "rd-cisco-2504-controller"
        NAS-Port-Type = Wireless-802.11
        Airespace-Wlan-Id = 14
        Calling-Station-Id = "40-d3-ae-fa-3a-ce"
        Called-Station-Id = "04-da-d2-4f-f0-f0:qa-ssid-3503"
        Message-Authenticator = 0x22d06088e3b98f865c93f6ba0f167bb7
```

Example 2: RADIUS Access-Accept

```
Thu Jan 18 17:19:47 2018
        Packet-Type = Access-Accept
        Ucopia-Ldap-Id = "1"
        Ucopia-validitytype = "inherited"
        Ucopia-ProfileId := "2"
        Ruckus-Role := "2"
        Filter-Id := "2"
        Ucopia-Group := "oneclick"
        User-Name := "hi2o6zt"
        Session-Timeout = 7200
```

Example 3: RADIUS Accounting Start

```
Thu Jan 18 17:19:48 2018
        User-Name = "hi2o6zt"
        NAS-Port = 3
        NAS-IP-Address = 10.1.6.2
        Framed-IP-Address = 10.1.255.98
        NAS-Identifier = "rd-cisco-2504-controller"
        Airespace-Wlan-Id = 14
        Acct-Session-Id = "5a60c923/40:d3:ae:fa:3a:ce/493"
        NAS-Port-Type = Wireless-802.11
        Cisco-AVPair = "audit-session-id=0a01060200000b055a60c879"
        Acct-Authentic = RADIUS
        Event-Timestamp = "Jan 18 2018 17:19:47 CET"
        Acct-Status-Type = Start
        Calling-Station-Id = "40:d3:ae:fa:3a:ce"
        Called-Station-Id = "68-9c-e2-be-da-40"
        Acct-Unique-Session-Id = "0b3f860f62aaedd5"
        Stripped-User-Name = "hi2o6zt"
        Realm = "NULL"
        Timestamp = 1516292388
```

Example 4: RADIUS accounting stop

```
Thu Jan 18 17:27:28 2018
        User-Name = "hi2o6zt"
        NAS-Port = 3
        NAS-IP-Address = 10.1.6.2
        Framed-IP-Address = 10.1.255.98
        NAS-Identifier = "rd-cisco-2504-controller"
        Airespace-Wlan-Id = 14
        Acct-Session-Id = "5a60c923/40:d3:ae:fa:3a:ce/493"
        NAS-Port-Type = Wireless-802.11
        Cisco-AVPair = "audit-session-id=0a01060200000b055a60c879"
        Acct-Authentic = RADIUS
        Event-Timestamp = "Jan 18 2018 17:27:28 CET"
        Acct-Status-Type = Stop
        Acct-Input-Octets = 8579185
        Acct-Input-Gigawords = 0
        Acct-Output-Octets = 75523858
        Acct-Output-Gigawords = 0
        Acct-Input-Packets = 27172
        Acct-Output-Packets = 56956
        Acct-Terminate-Cause = Idle-Timeout
        Acct-Session-Time = 461
        Acct-Delay-Time = 0
        Calling-Station-Id = "40:d3:ae:fa:3a:ce"
        Called-Station-Id = "68-9c-e2-be-da-40"
        Acct-Unique-Session-Id = "0b3f860f62aaedd5"
        Stripped-User-Name = "hi2o6zt"
        Realm = "NULL"
        Timestamp = 1516292848
```

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
	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 Cisco architecture:

Features	OOB Cisco WLC	Comments
SECURITY		
Authentication		
- Web captive portal	✓	Hosted by central UCOPIA
- 802.1x/PEAP - 802.1x/TTLS - 802.1x/TLS		
- Social networks (Facebook, Twitter, G+, LinkedIn, OpenID Connect)	✓	- Only if the domain name /certificate has been changed and publicly declared, and a new social network application is created, or -If the customer has control on the DNS server and created a new DNS entry for resolving "controller.access.network" with the outgoing IP address of his UCOPIA controller
- Fixed MAC address or IP address	✓	
- 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		The Cisco WLC applies the same profile for every user connected to the same AP
Controller's incoming VLANs/subnets	✓	
WPA, 802.11i compliance	✓	

URLs available before authentication	✓	
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 - URL - Automatic logs backup via FTP(S) - Automatic logs compression		
Audit logs (Syslog)	✓	
MOBILITY		
QoS (by service, by user) **Data volume quota**		No BW limitation / reservation possible on UCOPIA as the traffic won't go though it No quota applied by UCOPIA as the traffic won't go though it
Time based access control		
- Configured ending validity date	✓	
- Configured ending validity date		
- Time credit	✓	
Location based access control: Localization on incoming and outgoing zones	✓	
Multi-portal (one portal per zone)	✓	
Conditional profile	✓	Only for the supported features of the profile
Memorization and limitation of devices per user	✓	
Auto disconnection	N/A	Disabled on the central controller as soon as an Out-Of-Band architecture is set up
Possibility for the user to disconnect from the captive portal (thanks to a "Disconnection" button) **Increased security**		The disconnection button is hidden in an OOB Cisco WLC architecture because the WLC intercepts the disconnection request and doesn't redirect the user to the UCOPIA 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 session with temporary profile to be able to either click on the autoconnect/autofill link or to enter their received credentials on the splash page
Sponsoring by email	✓	
User account refill by code or online payment	✓	
Automatic user accounts purging (global or per profile)	✓	
Manual user account exportation via CSV	✓	
Automatic user account exportation via CSV	✓	
Delegated provisioning	✓	
- Customization	✓	
- Multi zones	✓	
- Connection ticket printing (or sending by SMS or email)	✓	
- Creating accounts in mass from a CSV file	✓	
- User account refill by code	✓	
Supervision of connected users	✓	
Statistics	✓	
- Predefined graphs	✓	
- Manual CSV export	✓	
- Automatic CVS export	✓	
Reporting (PDF), send by email or FTP	✓	
Customizable web portal	✓	
Customizable connection ticket per zone or profile	✓	
SNMP – MIB II	✓	
External Syslog	✓	
CLI	✓	
Multi zone administration	✓	
Physical Administration port	✓ (>=5000)	
BILLING		

Online payment (credit card, PayPal, Ingenico)	✓	
PMS connector	✓	Only one PMS can be configured and integrated with the central UCOPIA
INTEGRATION		
Integration with a corporate LDAP directory (OpenLDAP, ActiveDirectory)	✓	
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	✓	