



Out-Of-Band Aruba architecture

Version 5.1



Table of contents

Table of contents.....	2
Table of figures.....	3
1 Introduction	4
2 User experience workflow	6
3 Advantages and recommendations	7
3.1 Advantages	7
3.1.1 Centralization of the user directory	7
3.1.2 Centralization of captive portals	7
3.1.3 Centralization of user profiles	7
3.1.4 Centralization of user logs	7
3.1.5 Local Internet breakout	8
3.2 Restrictions and recommendations.....	8
3.2.1 Supported Aruba and UCOPIA versions.....	8
3.2.2 Supported authentication / registration modes	8
3.2.3 Profile differentiation	8
3.2.4 Supported UCOPIA features on user management.....	9
3.2.5 User disconnection	10
3.2.6 Network failure.....	11
4 Licensing.....	11
5 UCOPIA configuration	11
5.1 Prerequisites	11
5.1.1 Time synchronization (on UCOPIA and Aruba).....	11
5.1.2 Communication between remote sites and central site (on UCOPIA and firewall)	12
5.1.3 New FQDN and certificate on the Aruba devices	12
5.1.4 New FQDN and certificate on the UCOPIA controller	12
5.1.5 Auto disconnection settings	13
5.2 Central controller configuration	15
5.2.1 Zone	15
5.2.2 Captive portal	16
5.2.3 RADIUS authentication	17
5.2.4 User profile	18
5.2.5 Administrator account.....	18
5.2.6 Access to the syslog service.....	18
5.2.7 [Optional] New domain name and certificate.....	19
5.3 Aruba Controller configuration.....	21
5.3.1 Configuration of the external RADIUS server	21
5.3.2 Configuration of the server group	22
5.3.3 Configuration of the external Captive portal	23
5.3.4 Configuration of the User Profile.....	25
5.3.5 Configuration of the AAA Profile	29
5.3.6 Configuration of a WLAN	30
5.3.7 Role differentiation.....	33
5.3.8 Configuration of the syslog server.....	33
5.4 Aruba IAP configuration.....	34
5.4.1 Creation of a WLAN Setting.....	34
5.4.2 Configure Client IP & VLAN Assignment	36

5.4.3	Configuration of the external RADIUS server	37
5.4.4	Configuration of the captive portal profile.....	38
5.4.5	Configuring Security Level	39
5.4.6	Access Rules.....	39
5.4.7	Configuration of the syslog server.....	42
6	Annex 1: detailed flow diagram	44
6.1	Portal authentication	44
6.2	RADIUS exchanges	45
7	Annex 2: Walled garden for social networks	49
7.1	Facebook, Twitter, Google, LinkedIn	49
7.2	OpenID Connect.....	49
8	Annex 3: Summary table on available features	49

Table of figures

Figure 1	: Global Out-of-Band Aruba architecture	4
Figure 2	: User traffic flow	6
Figure 3	: Adding an incoming zone	15
Figure 4	: Configuring a captive portal	16
Figure 5	: Example of portal configuration with self-registering by SMS.....	17
Figure 6	: Association between portal and zone	17
Figure 7	: Adding a NAS	17
Figure 8	: Adding an administrator account.....	18
Figure 9	: Adding an access to the syslog service from Aruba AP	19
Figure 10	: Creation of a network policy	21
Figure 10	: Naming of your network policy	21
Figure 11	: Creation of a new SSID	Erreur ! Signet non défini.
Figure 12	: Configuration of the new SSID > Authentication	22
Figure 13	: Configuration of the Captive Web Portal Settings	Erreur ! Signet non défini.
Figure 14	: Creation of a RADIUS server configuration	29
Figure 15	: Configuration of the external RADIUS server	29
Figure 16	: Creation of the default user profile.....	30
Figure 17	: Configuration of the default user profile	Erreur ! Signet non défini.
Figure 18	: Creation of the syslog server	33
Figure 19	: Association of the created syslog server in the network policy	Erreur ! Signet non défini.
Figure 20	: Deployment of the network policy.....	Erreur ! Signet non défini.

1 Introduction

This document describes the Out-of-Band architecture with Aruba Access Points on premise. Aruba has multiple architectures whose main ones are Aruba controller mode and Aruba IAP mode.

- **Aruba controller mode:** This architecture is composed of a central Aruba controller who manages a cluster of APs, and of controller-managed AP's that are the thin AP's which is configured and managed by the central controller.
- **Aruba IAP mode:** Aruba Instant is a controllerless Wi-Fi solution. They eliminate the need for additional controller hardware by distributing controller functionality such as configuration to the access points (AP). One of AP (out of all deployed) works as virtual controller and managed all the other AP's.

This Out-Of-Band Aruba enables to have a central UCOPIA solution (with an ADVANCE global license) communicating with Aruba AP(s) or Controller. The UCOPIA central controller is typically in a datacenter, and the APs at customer sites (e.g. hotel, restaurant, agency, etc.).

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

The on premise Aruba Aps or controller ensure portal redirection to the centralized UCOPIA controller, participates in the authentication process, and redirect the user traffic's logs to the central UCOPIA controller.

The central controller can be a high availability cluster (Advance product line).

The following schemes presents the global Out-of-Band Aruba architecture.

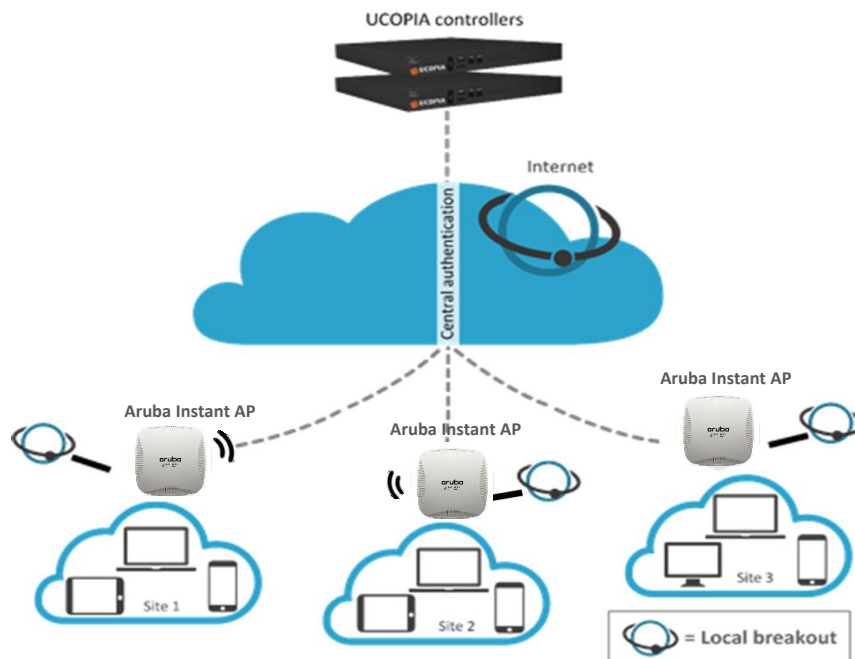


Figure 1.a : Global Out-of-Band Instant AP Aruba architecture

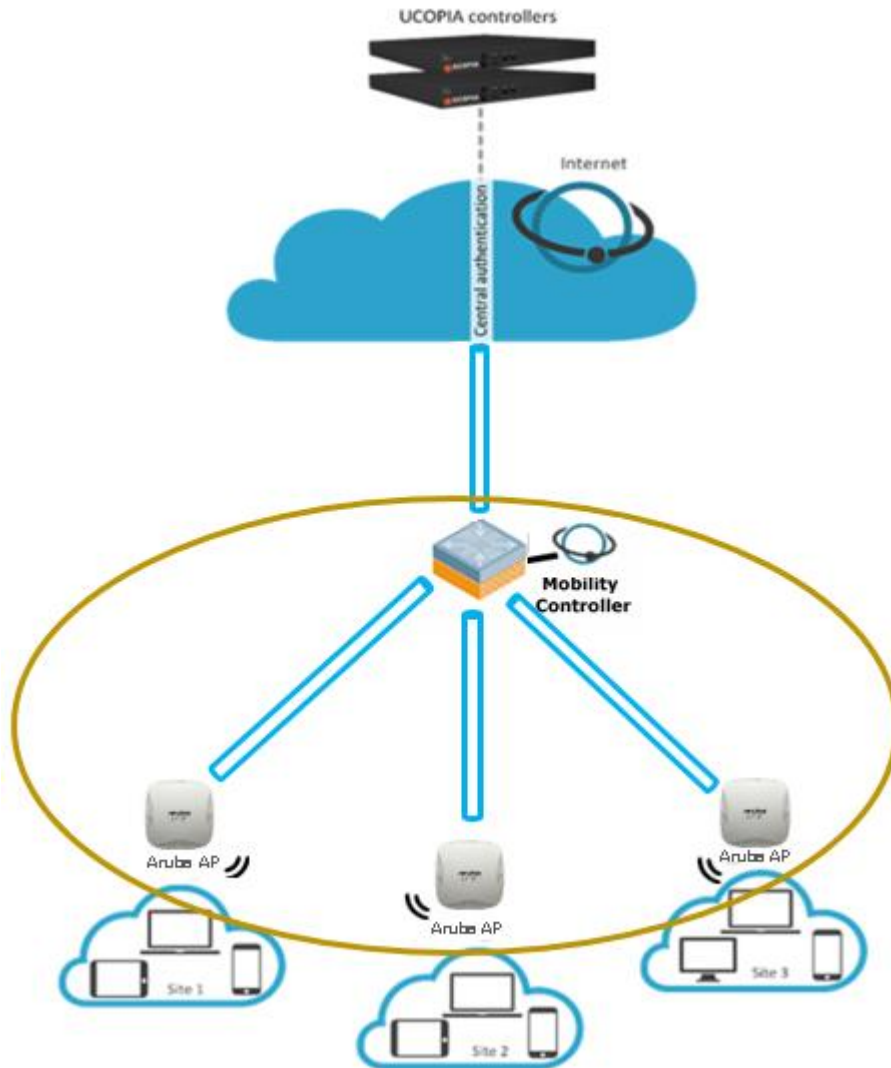


Figure 2.b : Global Out-of-Band Instant AP Aruba architecture

2 User experience workflow

Let's consider a guest trying to connect on the Wi-Fi on a site A where an Aruba AP is installed. The user will register on the captive portal to connect with SMS registration.

The workflow (described only in the case of IAP architecture) is as follows:

1. Once associated to the Wi-Fi, the user launches his (her) Web browser.
2. The Aruba 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 Aruba AP and the central controller through the RADIUS protocol. The user's validity settings are sent to the Aruba AP through timestamp RADIUS attribute. And Aruba is not able to interpret in Time-credit, so the disconnection is done by the Ucopia Controller answer to the Interim-Update.
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.

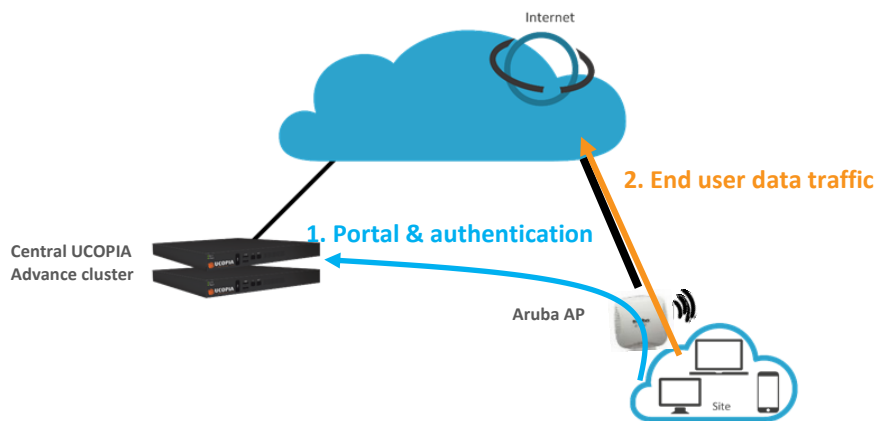


Figure 3 : User traffic flow

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.

You can configure a single captive portal for all sites, or 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 Aruba AP via RADIUS exchanges such as the profile Id, the user name, the expiration date, the session timeout in case of time credit...so that the Aruba AP can enforce time validity checking before letting the user access the network.

Note: As Aruba APs don't have a full knowledge of the profile settings on UCOPIA controller (such as starting validity date, bandwidth limitation, quota...) via the authentication exchanges with the UCOPIA controller, these settings should be locally configured on the profile created and used by the Aruba AP

3.1.4 Centralization of user logs

All Aruba APs in the Out-Of-Band architecture send in real-time all event log entries to the central UCOPIA controller, so that logs from different sites are centralized in the central UCOPIA controllers. This logs exchange is done via the standard Syslog (UDP / port 514).

All Aruba logs sent to UCOPIA are to be seen on the Aruba Cloud Services Controller GUI, in "Monitoring > DEBUG > Process Logs".

The central UCOPIA controller doesn't store all syslog information sent by the Aruba APs and only keeps the ones that feed its SQL database. Here are the logs recorded by the UCOPIA controller:

- Connected users
- Sessions (user @IP and @MAC...)
- Traffic (except for the source MAC address. Only the user IP address and not his MAC address is stored in the traffic logs)

But, URLs aren't logged in the UCOPIA controller.

3.1.5 Local Internet breakout

Each local site can use its own Internet access for connecting users, thus avoiding to centralize the user traffic toward the central Internet access.

3.2 Restrictions and recommendations

3.2.1 Supported Aruba and UCOPIA versions

The Out-Of-Band Aruba architecture requires:

- For controller-based architecture: a version $\geq 6.4.3$ and a license with the module authorizing firewalling features
- For IAPs: a version $\geq 6.3.3$

Only UCOPIA controllers from version 5.1.11 support the Out-Of-Band Aruba configuration.

3.2.2 Supported authentication / registration modes

With the Out-Of-Band Aruba 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
- Limited social network authentication as the customer must:
 - either change controller name on incoming networks to “central” and then control his DNS server and resolve “central.access.network” with the IP address of his UCOPIA controller (if you have a full controller on the DNS server of your guests)
 - or change the domain name of his UCOPIA controller, create a new certificate and create his own social network application

3.2.3 Profile differentiation

As the user traffic doesn't go through UCOPIA, the Aruba AP is in charge of enforcing the right policy on the user.

Aruba can apply different profiles depending on various RADIUS attributes, the OS type, the location, the MAC address or the schedule. Thus, it is possible for Aruba to reuse the UCOPIA profile of the user, indicated in the RADIUS field “Filter-Id”, in order to apply a distinct policy and QoS for each profile.

3.2.4 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 Aruba AP is in charge of enforcing the policy on the user. However, the Aruba AP isn't aware of the entire profile configuration on UCOPIA as only some information is sent by UCOPIA to the Aruba AP during the RADIUS exchanges. Here are the profile settings that can be enforced by Aruba AP:

- Time-based criteria:

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

- **MAC-based criteria:**

- Limitation of the number of authorized devices for a user account
- Limitation of the number of simultaneously connected devices with a user account
- Memorization of user devices
- Automatic reconnection...

- **Others:**

All other configurations like authorized services, web filtering, limitation of bandwidth and quota, web marketing injection...are not sent by the UCOPIA to the Aruba. So, any desired QoS policy should be directly configured and set up in the Aruba AP.

3.2.5 User disconnection

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

Supported in the Out-Of-Band Aruba architecture?	
Increased security	<p>No</p> <p><i>Description: the user will be disconnected from UCOPIA controller but not on Aruba AP. 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.</i></p>
UCOPIA auto disconnect	<p>No</p> <p><i>Description: because user traffic doesn't go through the UCOPIA controller, the autodisconnect feature doesn't make sense. So, as soon as an Ou-Of-Band architecture is configured, the central controller disable its autodisconnect feature.</i></p> <p><i>Only the autodisconnect on Aruba will be able to disconnect a user after a given inactivity period.</i></p>
Manual disconnection	<p>No</p> <p><i>Description: The Aruba API doesn't allow such disconnection request. The disconnection button has been deleted from the feedback page in the Out-Of-Band Aruba.</i></p>
Reached max quota	<p>Yes</p> <p><i>Description: The Aruba AP sends the information of the number of packets consumed by the user via the RADIUS Interim-Update send every 5 minutes.</i></p>
Expired credit time	Yes
Reached ending validity date	Yes
Forced disconnection	Yes
User deletion from the central UCOPIA controller	Yes

3.2.6 Network failure

The user directory is centralized and used by all Aruba APs on local sites. In case of network failure between the Aruba APs 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 Aruba)

The central controller and Aruba AP should share the same time source. It is advised to use the NTP protocol for that purpose. Aruba AP 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 Aruba AP an explicit end date for the user connection. If the time isn't similarly between the Aruba AP and UCOPIA controller, it will directly impact the authorized time connection of users.

On Aruba: configure the NTP server in the Cloud Controller Services GUI "Configuration > MANAGEMENT>Clock"

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 Aruba AP (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
Aruba AP	Central controller	TCP/443, UDP/1812, UDP/1813, UDP/514

These are the flows that should be opened from the Aruba AP to the central in order to enable the Aruba APs to communicate with their central.

5.1.3 New FQDN and certificate on the Aruba devices

It is mandatory to import on an Aruba controller/APs a certificate coming from a known certification authority, for a complete FQDN (no wildcard). This requirement is to avoid certificate errors or warnings to the clients.

Indeed, when an Aruba AP/controller redirects users to the central UCOPIA portal, it tells the user to include the name and domain name of the Aruba AP/controller, so that the user will be able to make a POST request on the AP/controller to be connected on the Wi-Fi equipment.

Nowadays, Aruba AP/controller have a self-generated certificate not signed by recognized Certification Authority, generating error messages on the user browser.

Hence the necessity to import a certificate on the Aruba AP/controller.

5.1.4 New FQDN and certificate on the UCOPIA controller

In this architecture, a new public certificate is necessary on the central UCOPIA if no control on the client's DNS server (resolving UCOPIA default certificates with the outgoing IP address of the central UCOPIA).

The default certificates « **controller.access.network** » or « **central.access.network** » are only present for the purpose of feature demonstrations and convenience and are not intended for long-term use in a production environment. Users are urged to change and use their own certification when in production.

5.1.5 Auto disconnection settings

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

This “auto disconnection” feature on Aruba AP can be configured on the Virtual Controller Instant in “Networks > New > Show advanced options”

Figure 1.1: Configuring inactivity timeout (IAP mode)

The screenshot shows a configuration interface for WLAN Settings. At the top, there are four tabs: 1 WLAN Settings (highlighted in green), 2 VLAN, 3 Security, and 4 Access. Below the tabs, the 'WLAN Settings' section is visible. It contains a 'Name & Usage' section with a 'Name:' label and an empty text input box. Underneath, there is a 'Primary usage:' label followed by three radio button options: 'Employee' (which is selected), 'Voice', and 'Guest'. At the bottom left of the configuration area, there is a link labeled 'Show advanced options' which is highlighted with a blue rectangular box. At the bottom right, there are two buttons: 'Next' and 'Cancel'.

Then, change the value of “Inactivity timeout”.

Figure 1.2: Configuring inactivity timeout (IAP mode)

The screenshot shows the 'WLAN Settings' configuration page. The 'Inactivity timeout' field is highlighted with a blue box and is set to 1000 seconds. Other visible settings include:

- Name: anish
- Primary usage: Guest
- Broadcast filtering: ARP
- Multicast transmission optimization: Disabled
- Dynamic multicast optimization: Disabled
- DMO channel utilization threshold: 90%
- Transmit Rates: 2.4 GHz (Min: 1, Max: 54), 5 GHz (Min: 6, Max: 54)
- Band: All
- DTIM interval: 1 beacon
- Min RSSI for probe request: 0
- Min RSSI for auth request: 0
- Bandwidth Limits: Airtime, Each radio (unchecked)
- Downstream/Upstream: kbps, Per user (unchecked)
- WMM: Background, Best effort, Video, Voice (all 0%)
- Traffic Specification (TSPEC): 2000 Kbps
- Spectralink Voice Protocol (SVP): (unchecked)
- Miscellaneous: Content filtering: Disabled

Figure 1.2: Configuring inactivity timeout (Controller mode)

The screenshot shows the 'Security > Authentication > Profiles' configuration page. The 'User idle timeout' field is highlighted with a blue box and is set to 60 seconds. Other visible settings include:

- Initial role: logon
- MAC Authentication Default Role: guest
- 802.1X Authentication Default Role: guest
- Download Role from CPPM: (unchecked)
- Set username from dhcp option 12: (unchecked)
- L2 Authentication Fail Through: (unchecked)
- Multiple Server Accounting: (unchecked)
- User idle timeout: Enable, seconds: 60
- Max IPv4 for wireless user: 2
- RADIUS Roaming Accounting: (unchecked)
- RADIUS Interim Accounting: (unchecked)
- User derivation rules: --NONE--
- Wired to Wireless Roaming:
- SIP authentication role: --NONE--
- Device Type Classification:
- Enforce DHCP: (unchecked)
- PAN Firewall Integration: (unchecked)
- Open SSID radius accounting: (unchecked)

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 Aruba and then from UCOPIA (and he doesn't unnecessarily consume his time credit).

*Auto disconnection after a maximum period of inactivity = **Inactive timeout***

Inactive timeout: This is the time to age out inactive clients and automatically disassociate them. By default, Aruba devices age out a client after 1000 seconds of inactivity but you can assign it a smaller value.

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 Aruba AP. 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**.



The screenshot shows the 'Zone management' interface with the 'Adding a zone' form. The form is titled 'Zone management' and 'Adding a zone'. It has a section for 'Identification settings' with the following fields:

- Zone name ***: A text input field containing 'guest_siteA'.
- Zone type**: Radio buttons for 'Incoming' (selected) and 'Outgoing'.
- Description**: A text area with a scroll bar.

Below the 'Identification settings' are two sections:

- Time zone**: A checkbox labeled 'Define a time zone'.
- License limitation**: A checkbox labeled 'Enable license limitation'.

At the bottom right of the form, there is a small asterisk indicating '* Mandatory fields' and a 'Confirm' button.

Figure 4 : Adding an incoming zone

5.2.2 Captive portal

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

Portals

Display the: Associations (5) **Configurations (3)** Visual models (5)

Configuration name	Format	Operating modes	Hosted	Zones	Models	Actions
Captive portal Adding a configuration						
default-portal	Laptop, Tablet, Smartphone, Suboptimum mode	Standard, Twitter, 'One Click'	●	1	1	✕ 🗑️
Guest	Laptop, Tablet, Smartphone, Suboptimum mode	Standard, SMS	●	0	0	✕ 🗑️
Automatic connection Adding a configuration						
auto	-	Automatic	-	1	-	✕ 🗑️
Mobile application Adding a configuration						
default-mobile-application	-	Standard	●	1	1	✕ 🗑️
Delegation portal Adding a configuration						
default-deleg	Laptop	-	●	2	1	✕ 🗑️

Figure 5 : Configuring a captive portal

For example, a portal with self-registering by SMS

Portals

Changing the 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

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

User fields	Allow input	Mandatory
Login	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Password	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Last name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
First name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Gender	<input type="checkbox"/>	<input type="checkbox"/>
Birth date	<input type="checkbox"/>	<input type="checkbox"/>
Phone number	<input checked="" type="checkbox"/>	<input 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 6 : 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 (5)** | Configurations (3) | Visual models (5)

Zone name	Portal type	Configuration name	Visual model name	Status	Actions
Incoming zones Adding an association					
Default-in	Captive portal	default-portal	default-portal	●	✕ 🗑️
	Delegation portal	default-deleg	default	●	✕ 🗑️
	Mobile application	default-mobile-application	default	●	✕ 🗑️
	Automatic connection	auto	-	●	✕ 🗑️
Outgoing zones <small>Caution, only delegate portal may be associated with outgoing zone.</small> Adding an association					
Default-out	Delegation portal	default-deleg	default	●	✕ 🗑️

Figure 7 : Association between portal and zone

5.2.3 RADIUS authentication

The Aruba APs perform user authentication through the RADIUS protocol.

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

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

RADIUS configuration

NAS modification *Aerohive*

NAS settings

Shortname *	Aerohive
Shared secret *	●●●●●●
Authorized subnet or IP address *	
<input checked="" type="radio"/> IP address <input type="radio"/> Interface <input type="radio"/> Subnet address	10.1.255.212
	Native outgoing VLAN (10.0.0.0/23)
	Subnet mask
NAS architecture which performs a portal redirection	<input checked="" type="checkbox"/>
Manufacturer	Aerohive
Local exhaust	<input checked="" type="checkbox"/>
NAS-IP-Address	

Confirm

Figure 8 : 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 Aruba AP as well.
- Define the IP addressing containing the Aruba 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.
- Tick the box “NAS architecture which performs a portal redirection”
- Select “Aruba” as Manufacturer
- Tick the box “Local exhaust” for local Internet breakout architecture.

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

5.2.4 User profile

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

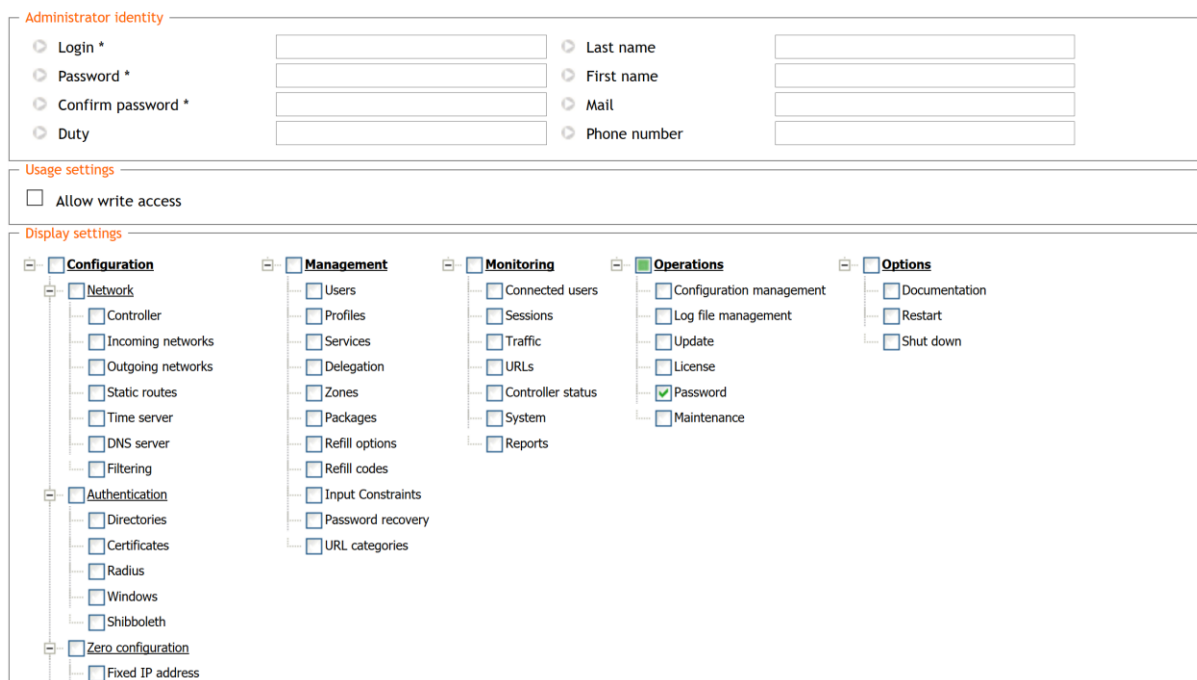
5.2.5 Administrator account

To associate the Aruba AP to the central controller, you need an administrator 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 + access to no tab).

You can create an administrator account from the page **Management->Administrators**.

Administrator management

Adding an administrator



The screenshot shows a web form for adding an administrator account, divided into three sections:

- Administrator identity:** Contains two columns of input fields. The left column includes Login *, Password *, Confirm password *, and Duty. The right column includes Last name, First name, Mail, and Phone number.
- Usage settings:** Contains a single checkbox labeled "Allow write access".
- Display settings:** A tree view of system tabs with checkboxes. The tabs are:
 - Configuration:** Network (Controller, Incoming networks, Outgoing networks, Static routes, Time server, DNS server, Filtering), Authentication (Directories, Certificates, Radius, Windows, Shibboleth), Zero configuration (Fixed IP address).
 - Management:** Users, Profiles, Services, Delegation, Zones, Packages, Refill options, Refill codes, Input Constraints, Password recovery, URL categories.
 - Monitoring:** Connected users, Sessions, Traffic, URLs, Controller status, System, Reports.
 - Operations:** Configuration management, Log file management, Update, License, Password (checked), Maintenance.
 - Options:** Documentation, Restart, Shut down.

Figure 9 : Adding an administrator account

5.2.6 Access to the syslog service

In order to allow the Aruba APs to send to the UCOPIA controller user logs, then you need to open the access to the Syslog service from the desired subnet / hosts.

Go to “Configuration > Network > Filtering > Access to the controller” and add a filtering setting configuration for the syslog service:

Filtering settings configuration

Access modification

Note : Access to the controller allows you manage the influx of flows to the service controller



Figure 10 : Adding an access to the syslog service from Aruba AP

5.2.7 [Optional] New domain name and certificate

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

If the customer:

- wants to use social networks on his splash page
- doesn't have control on his DNS server and can't create a DNS entry in order to resolve the domain name “central.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.



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**.

Adding a certificate

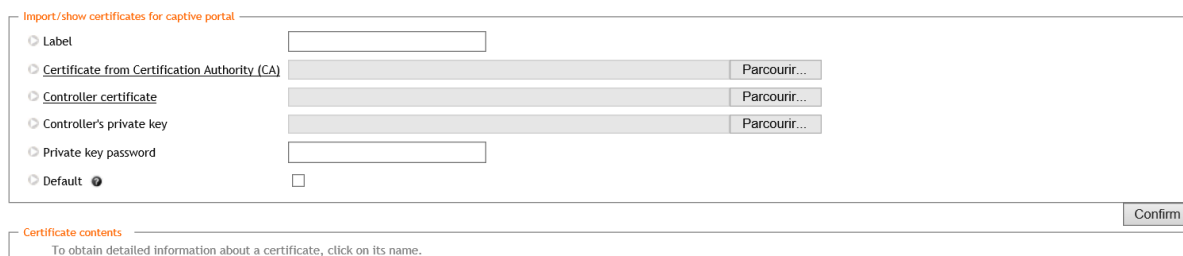


Figure 11 : Adding a new certificate for the captive portal

- 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**.

Controller basic configuration

Controller name and domain name

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


<input type="radio"/> Controller name on outgoing networks *	<input type="text" value="controller"/>
<input type="radio"/> Domain name on outgoing networks *	<input type="text" value="ucopia.lan"/>
<input type="radio"/> Controller name on incoming networks *	<input type="text" value="controller"/>
<input type="radio"/> Domain name on incoming networks *	<input type="text" value="access.network"/>
<input type="radio"/> Netbios workgroup 	<input type="text" value="UCOPIA"/>

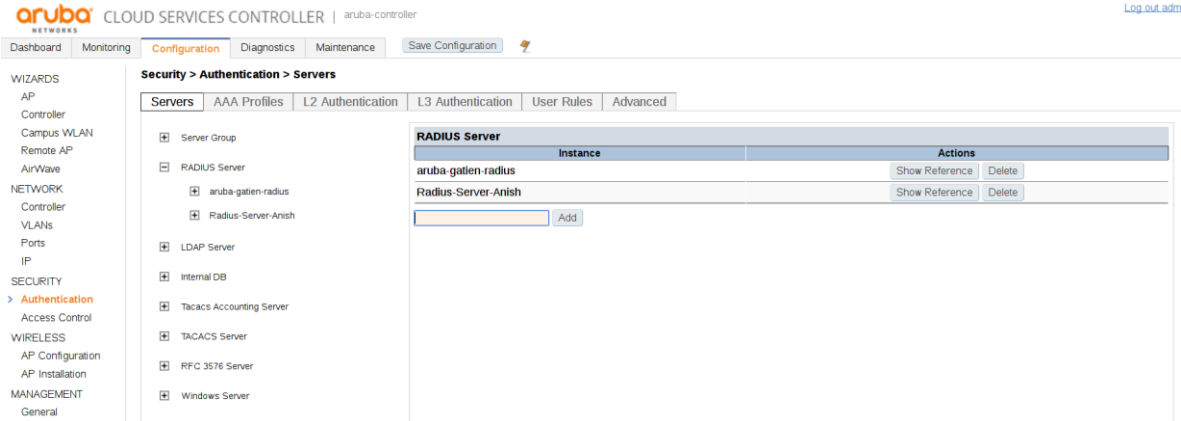
Figure 12 : Modifying a controller name

5.3 Aruba Controller configuration

Connect on your Aruba-controller

5.3.1 Configuration of the external RADIUS server

Go to “Configuration > SECURITY > Authentication > Servers (tab) > RADIUS Server” and then Name your radius server and press “ADD”.

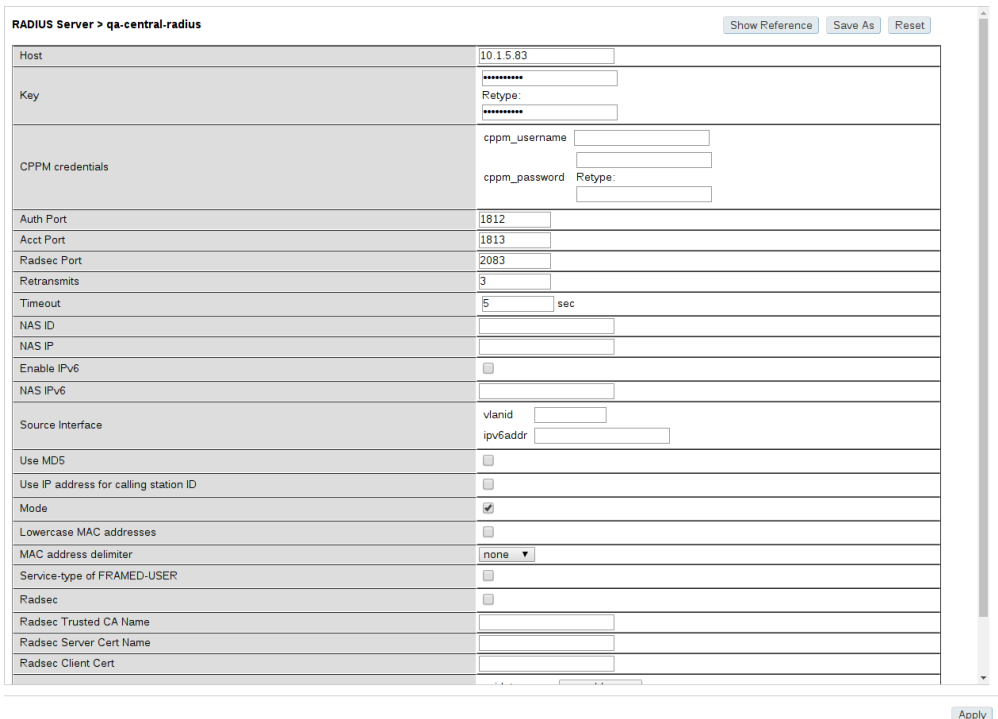


The screenshot shows the Aruba Cloud Services Controller web interface. The breadcrumb navigation is Configuration > SECURITY > Authentication > Servers. The 'Servers' tab is active, showing a list of RADIUS servers. One server, 'aruba-gatien-radius', is selected. The 'Add' button is visible at the bottom of the list.

Instance	Actions
aruba-gatien-radius	Show Reference Delete
Radius-Server-Anish	Show Reference Delete
<input type="text"/>	Add

Figure 13 : Creation of a RADIUS Server

Click on the Radius server you just created to edit it



The screenshot shows the configuration page for a RADIUS server named 'qa-central-radius'. The page contains various fields for configuration, including Host, Key, CPM credentials, Auth Port, Acct Port, Radsec Port, Retransmits, Timeout, NAS ID, NAS IP, Enable IPv6, NAS IPv6, Source Interface, Use MDS, Use IP address for calling station ID, Mode, Lowercase MAC addresses, MAC address delimiter, Service-type of FRAMED-USER, Radsec, Radsec Trusted CA Name, Radsec Server Cert Name, and Radsec Client Cert.

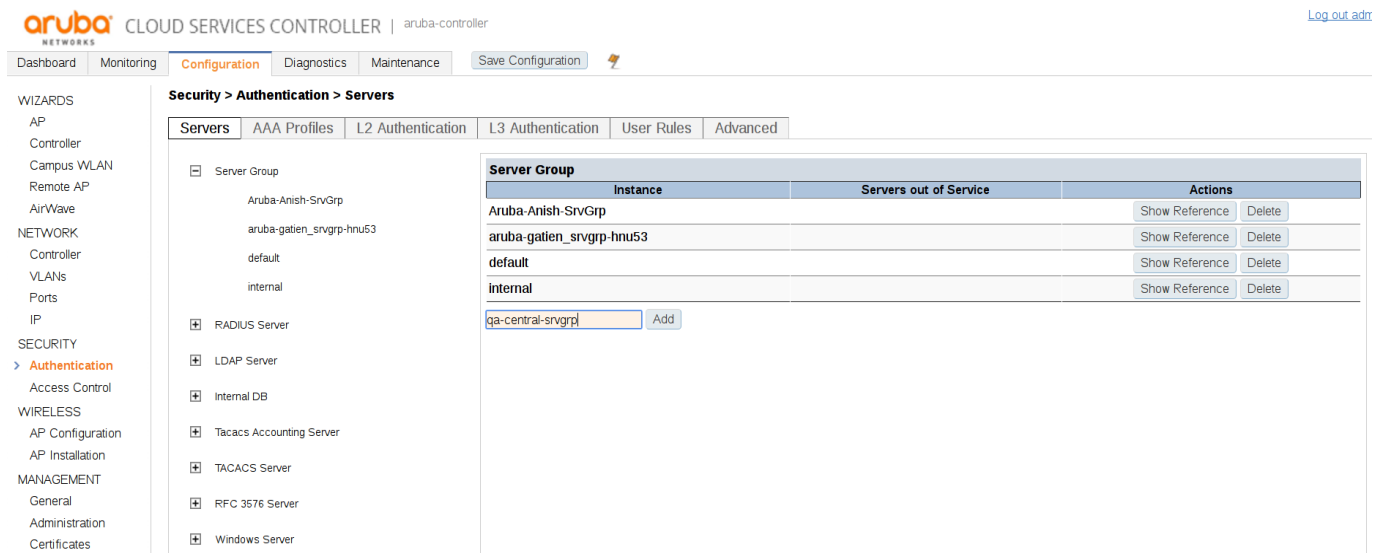
Host	10.15.83
Key	Retype: *****
CPM credentials	cppm_username: <input type="text"/> cppm_password: Retype: <input type="text"/>
Auth Port	1812
Acct Port	1813
Radsec Port	2083
Retransmits	3
Timeout	5 sec
NAS ID	<input type="text"/>
NAS IP	<input type="text"/>
Enable IPv6	<input type="checkbox"/>
NAS IPv6	<input type="text"/>
Source Interface	vlanid: <input type="text"/> ipv6addr: <input type="text"/>
Use MDS	<input type="checkbox"/>
Use IP address for calling station ID	<input type="checkbox"/>
Mode	<input checked="" type="checkbox"/>
Lowercase MAC addresses	<input type="checkbox"/>
MAC address delimiter	none
Service-type of FRAMED-USER	<input type="checkbox"/>
Radsec	<input type="checkbox"/>
Radsec Trusted CA Name	<input type="text"/>
Radsec Server Cert Name	<input type="text"/>
Radsec Client Cert	<input type="text"/>

Figure 14 : Radius server configuration

- The key must be the same as the shared RADIUS secret on the central controller.
- Host as [UCOPIA Controller IP address on out]
- Define the ports to be used
- The key must be the same as the shared RADIUS secret on the central controller.
- Click on “Apply”

5.3.2 Configuration of the server group

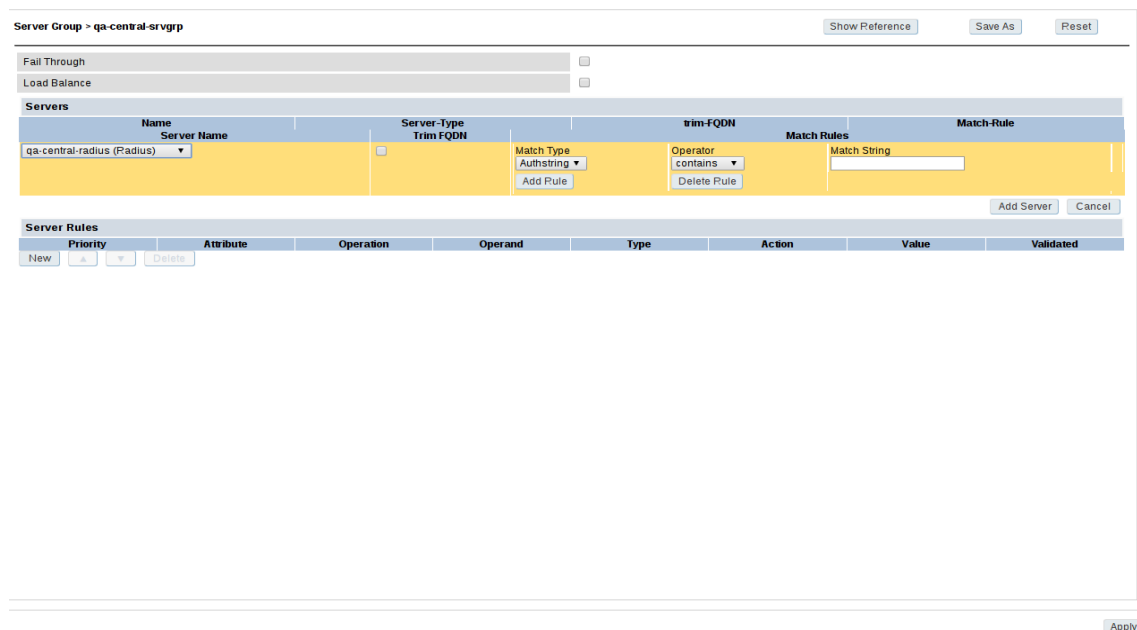
Go to “Configuration > SECURITY > Authentication > Servers (tab) > Server Group” and then Name your server group and press “ADD”.



The screenshot shows the Aruba Cloud Services Controller interface. The navigation menu on the left includes WIZARDS, NETWORK, SECURITY, and WIRELESS. The main content area is titled 'Security > Authentication > Servers'. A table lists existing server groups: Aruba-Anish-SrvGrp, aruba-gatien_srvgrp-hnu53, default, and internal. A new entry 'qa-central-srvgrp' is being added to the table. The 'Add' button is visible next to the input field.

Figure 154: Adding a Server group

Click on the Server group you just created to edit it



The screenshot shows the configuration page for the 'qa-central-srvgrp' server group. The 'Servers' section contains a table with the following data:

Name	Server Name	Server-Type	Trim FQDN	Match Type	Operator	Match String	Match-Rule
qa-central-radius (Radius)				Authstring	contains		

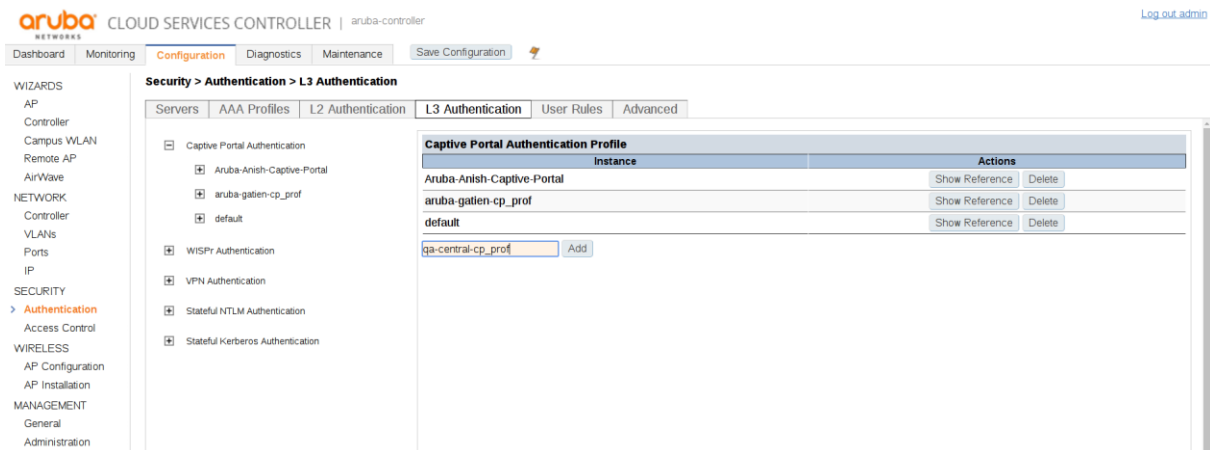
The 'Server Rules' section shows a table with the following columns: Priority, Attribute, Operation, Operand, Type, Action, Value, Validated. There is a 'New' button and a 'Delete' button in the 'Priority' column.

Figure 165: Configuration of the Server group

- Under servers, click on new
- Choose the Radius server created in section 5.3.1 for the Server Name column
- Leave all other values as default
- Click on “Add Server”
- Click on “Apply”

5.3.3 Configuration of the external Captive portal

Go to “Configuration > SECURITY > Authentication > L3 Authentication (tab) > Captive Portal Authentication” and then Name your Captive portal and press “ADD”.

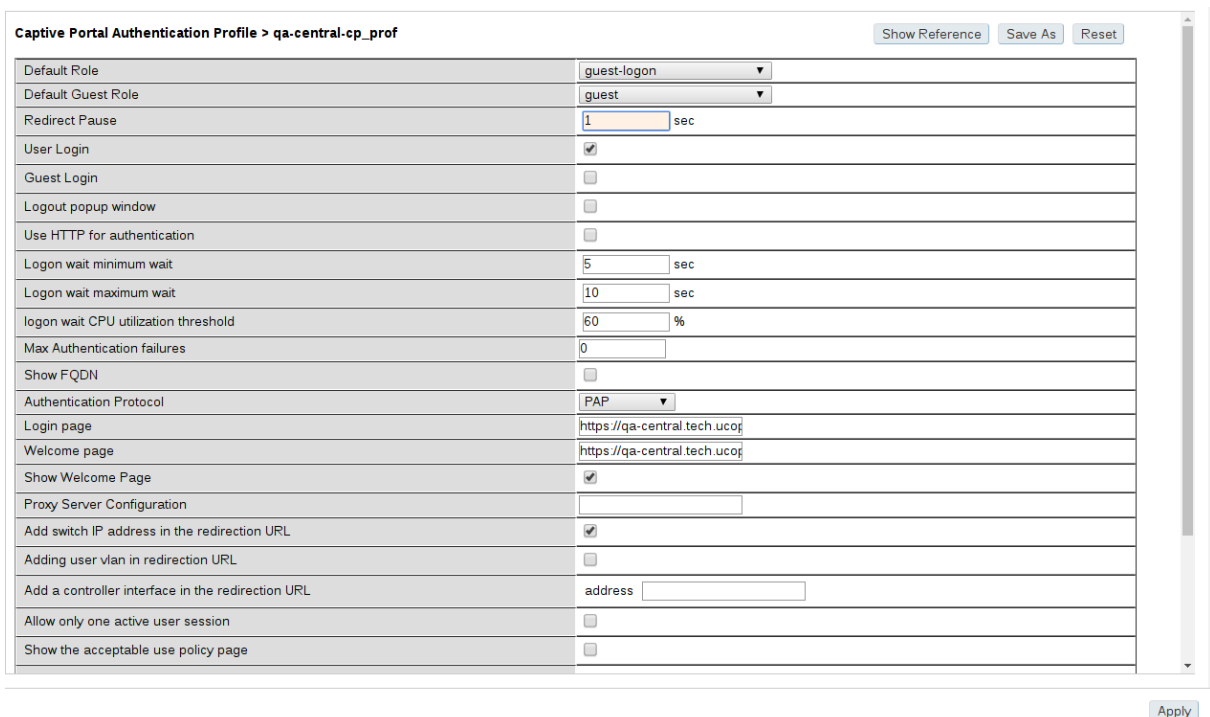


The screenshot shows the Aruba Cloud Services Controller interface. The navigation menu on the left includes WIZARDS, NETWORK, SECURITY, and WIRELESS. The main content area is titled "Security > Authentication > L3 Authentication". Under the "Captive Portal Authentication" section, there is a table of existing profiles:

Instance	Actions
Aruba-Anish-Captive-Portal	Show Reference Delete
aruba-gatien-cp_prof	Show Reference Delete
default	Show Reference Delete
qa-central-cp_prof	Add

Figure 176: Adding a new Captive portal

Click on the Captive portal you just created to edit it



The screenshot shows the configuration page for the Captive Portal Authentication Profile "qa-central-cp_prof". The page includes various settings for the profile, such as Default Role, Default Guest Role, Redirect Pause, User Login, Guest Login, Logout popup window, Use HTTP for authentication, Logon wait minimum wait, Logon wait maximum wait, logon wait CPU utilization threshold, Max Authentication failures, Show FQDN, Authentication Protocol, Login page, Welcome page, Show Welcome Page, Proxy Server Configuration, Add switch IP address in the redirection URL, Adding user vlan in redirection URL, Add a controller interface in the redirection URL, Allow only one active user session, and Show the acceptable use policy page.

Default Role	guest-logout
Default Guest Role	guest
Redirect Pause	1 sec
User Login	<input checked="" type="checkbox"/>
Guest Login	<input type="checkbox"/>
Logout popup window	<input type="checkbox"/>
Use HTTP for authentication	<input type="checkbox"/>
Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec
logon wait CPU utilization threshold	60 %
Max Authentication failures	0
Show FQDN	<input type="checkbox"/>
Authentication Protocol	PAP
Login page	https://qa-central.tech.ucoj
Welcome page	https://qa-central.tech.ucoj
Show Welcome Page	<input checked="" type="checkbox"/>
Proxy Server Configuration	
Add switch IP address in the redirection URL	<input checked="" type="checkbox"/>
Adding user vlan in redirection URL	<input type="checkbox"/>
Add a controller interface in the redirection URL	address <input type="text"/>
Allow only one active user session	<input type="checkbox"/>
Show the acceptable use policy page	<input type="checkbox"/>

Figure 187: Configuration of the Captive Web Portal Settings

Define your default captive portal:

- Default Role = < Role to assign when user is connected ('guest' by default) >
- Default Guest Role = < Role to assign when guest user is connected ('guest' by default) >
- Redirect pause = '1' (the higher the value the higher the time pause when the user wants to connect)
- Check "User Login"
- Uncheck "Logout popup window"
- login page = https://<central controller FQDN>/zone/<zone label>
- Welcome page = https://<central controller FQDN>/zone/<zone label>
- Check "Show Welcome page"
- Check "Add switch IP address in redirection URL"
- Click on "Apply"
- Click on "Server Group" at the left menu under the captive portal profile you just created

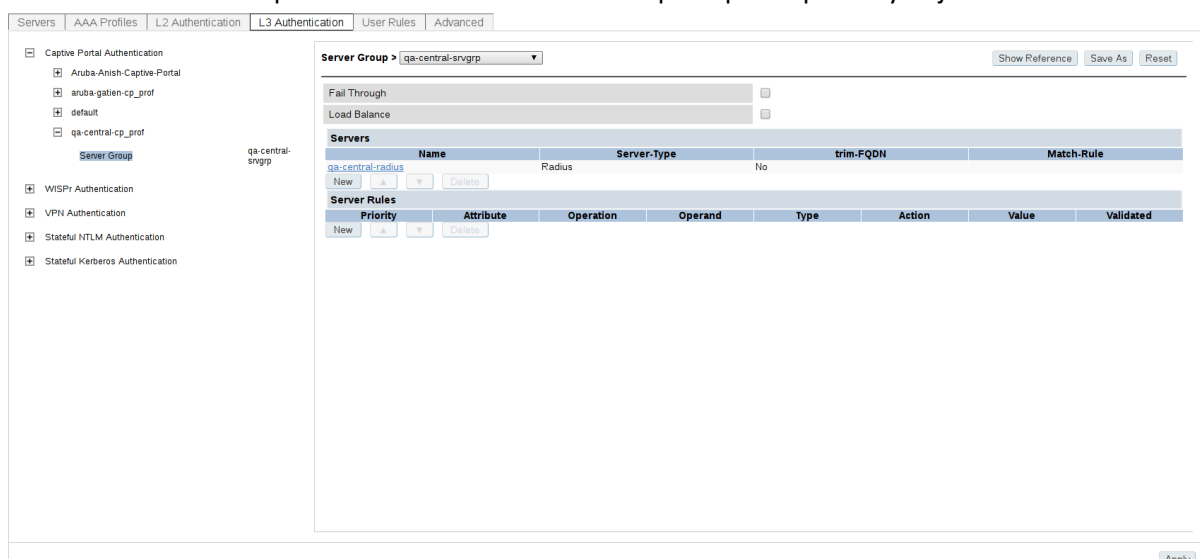


Figure 198: Server group association to captive portal

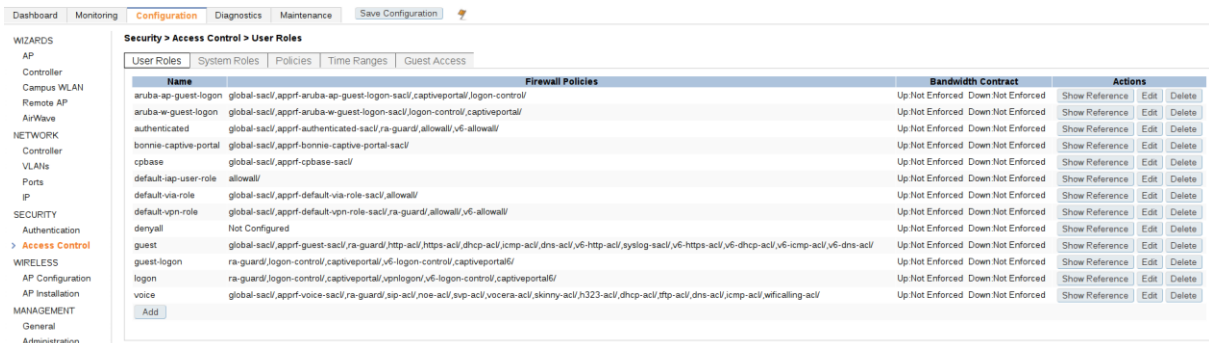
- Choose the server group created in section 5.3.2
- Click on "Apply"

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)

5.3.4 Configuration of the User Profile

Go to “Configuration > SECURITY > Access Control > User Roles (tab)” and press “ADD”.



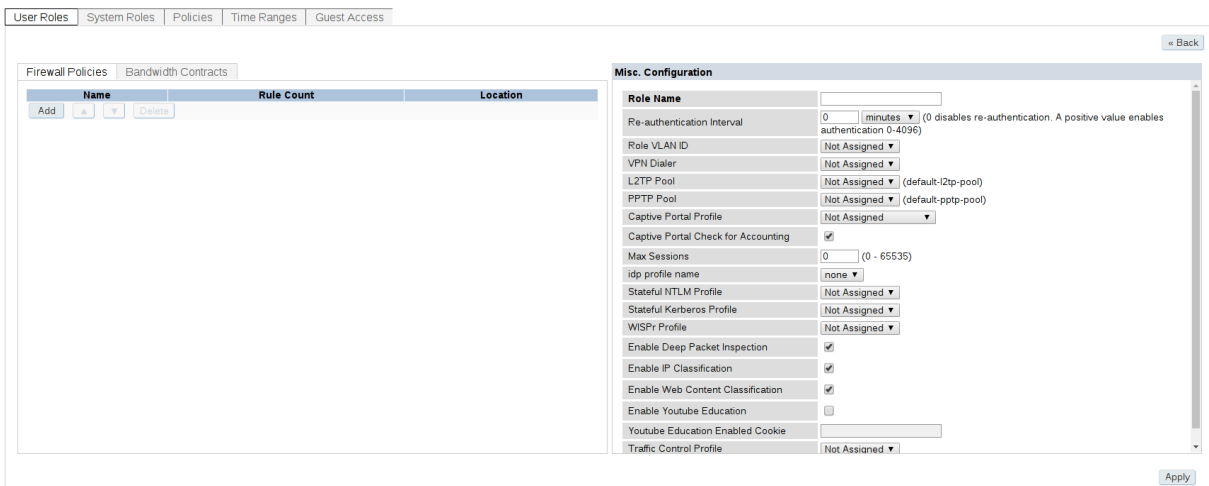
Name	Firewall Policies	Bandwidth Contract	Actions
aruba-ap-guest-logon	global-sacl/appf-aruba-ap-guest-logon-sacl/captiveportal/jogon-control/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
aruba-w-guest-logon	global-sacl/appf-aruba-w-guest-logon-sacl/jogon-control/captiveportal/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
authenticated	global-sacl/appf-authenticated-sacl/ra-guard/allowall/v6-allowall/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
bonnie-captive-portal	global-sacl/appf-bonnie-captive-portal-sacl/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
cpbase	global-sacl/appf-cpbase-sacl/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
default-iap-user-role	allowall/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
default-via-role	global-sacl/appf-default-via-role-sacl/allowall/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
default-vpn-role	global-sacl/appf-default-vpn-role-sacl/ra-guard/allowall/v6-allowall/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
deryall	Not Configured	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
guest	global-sacl/appf-guest-sacl/ra-guard/http-acli/https-acli/dhcp-acli/jcmp-acli/dns-acli/v6-http-acli/v6-https-acli/v6-dhcp-acli/v6-icmp-acli/v6-dns-acli/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
guest-logon	ra-guard/jogon-control/captiveportal/v6-logon-control/captiveportal/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
logon	ra-guard/jogon-control/captiveportal/vpnlogon/v6-logon-control/captiveportal/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete
voice	global-sacl/appf-voice-sacl/ra-guard/sip-acli/noe-acli/svp-acli/vocera-acli/skny-acli/h323-acli/dhcp-acli/ftp-acli/dns-acli/jcmp-acli/wfcalling-acli/	Up/Not Enforced Down/Not Enforced	Show Reference Edit Delete

Figure 209: User roles list

You have to create 2 user profiles.

- A user role (Preauth): This first user role is to use for users not authenticated
- A user role (authUser): This second user role is to assign to users after authentication

Each user profiles can be associated to a specific firewall policy to limit or allow a user to perform a specific action.



Name	Rule Count	Location
Add		

Misc. Configuration	
Role Name	
Re-authentication Interval	0 (minutes) (0 disables re-authentication. A positive value enables authentication 0-4096)
Role VLAN ID	Not Assigned
VPN Dialer	Not Assigned
L2TP Pool	Not Assigned (default-l2tp-pool)
PPTP Pool	Not Assigned (default-pptp-pool)
Captive Portal Profile	Not Assigned
Captive Portal Check for Accounting	<input checked="" type="checkbox"/>
Max Sessions	0 (0 - 65535)
idp profile name	none
Stateful NTLM Profile	Not Assigned
Stateful Kerberos Profile	Not Assigned
WISPr Profile	Not Assigned
Enable Deep Packet Inspection	<input checked="" type="checkbox"/>
Enable IP Classification	<input checked="" type="checkbox"/>
Enable Web Content Classification	<input checked="" type="checkbox"/>
Enable Youtube Education	<input type="checkbox"/>
Youtube Education Enabled Cookie	
Traffic Control Profile	Not Assigned

Figure 20: New user role

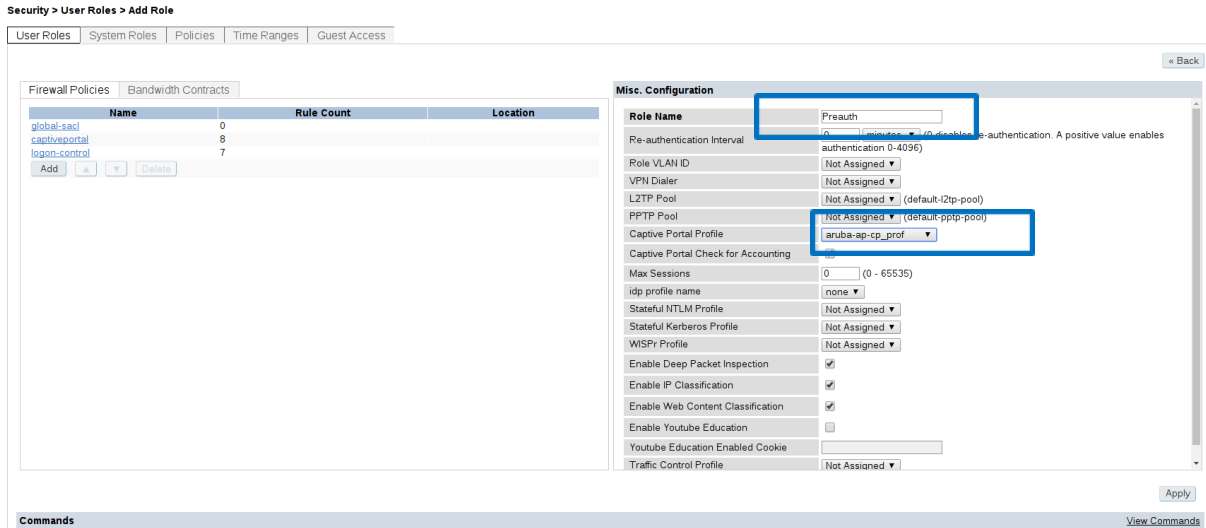


Figure 21: User Role Preauth with policies

The firewall Policies to use for a preauth Profile can be:

- Role Name = < name can be 'Preauth' >
- Captive Portal Profile = < select your external captive portal >
- Click on add, then You can either use an existing policy or create a new one.
- You can select the following existing policies (I not exist You can create a new one)
 - o Global-sacl: For global rules.
 - o Logon-control: This policy is to limit user’s connections. It contains the rules shown in figure 25
 - o Captive portal: this policy is used to redirect all user’s request to a specific captive portal and allow ucofia controller url. It contains the rules shown in figure 24
 - Here, if not yet configured, create an alias for the ucofia central urls and IP. Use them as on figure 23

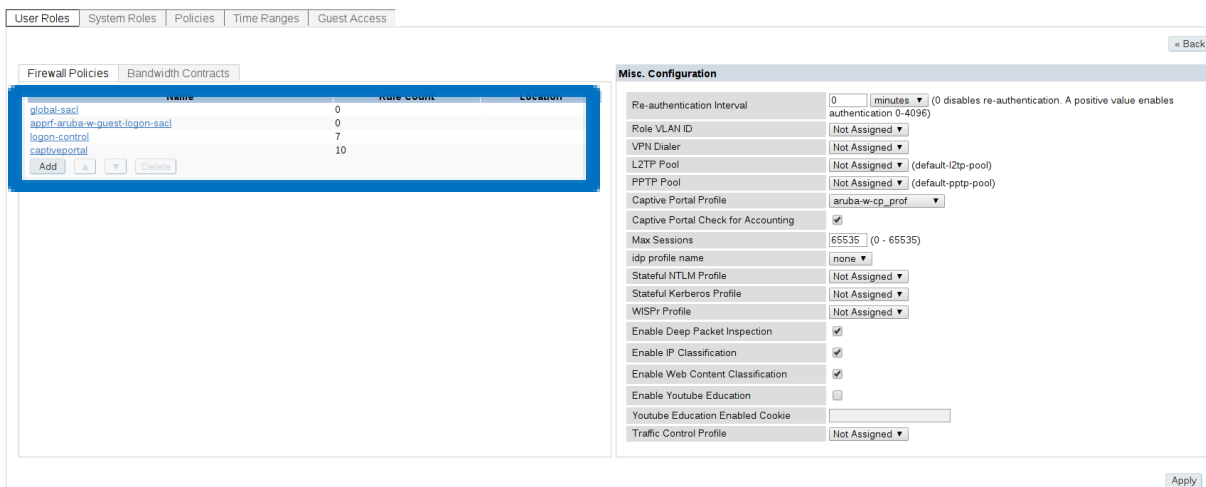


Figure 22: User Role Preauth with policies and custom rules

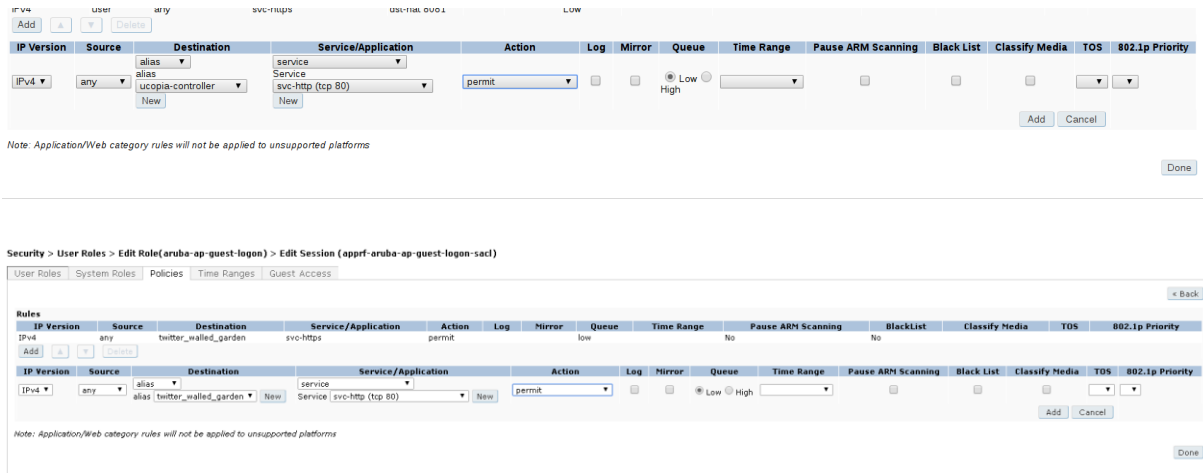


Figure 23: Adding a new rule / Twitter walled garden rules

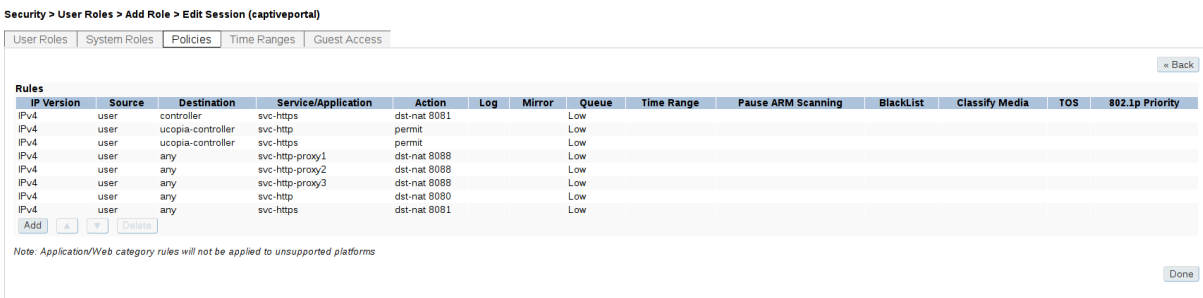


Figure 24: List of rules for captive Portal Policy

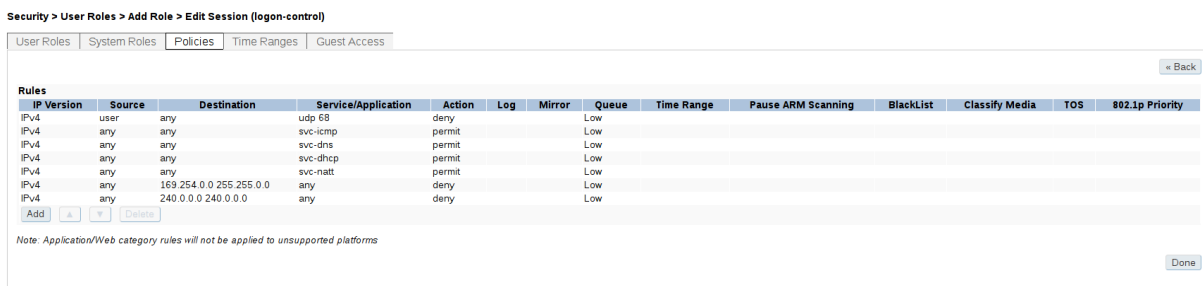


Figure 25: List of rules for logon-control Policy

The firewall Policies to use for an authUser profile can be :

- Click on add
- Role Name = < name can be 'authUser' >
- Add all the existing firewall policies in the figure 26
- Click on Apply

Security > User Roles > Edit Role(guest)

User Roles	System Roles	Policies	Time Ranges	Guest Access
Firewall Policies	Bandwidth Contracts			
Name	Rule Count	Location		
global-sacl	0			
apprf-guest-sacl	0			
ra-guard	1			
http-acl	1			
https-acl	1			
dhcp-acl	1			
icmp-acl	1			
dns-acl	1			
v6-http-acl	1			
syslog-sacl	1			
v6-https-acl	1			
v6-dhcp-acl	1			
v6-icmp-acl	1			
v6-dns-acl	1			
<input type="button" value="Add"/>	<input type="button" value="▲"/>	<input type="button" value="▼"/>	<input type="button" value="Delete"/>	

Figure 26: List of policies for a guest role

5.3.5 Configuration of the AAA Profile

Go to “Configuration > SECURITY > Authentication > AAA Profiles (tab) > AAA” and Press “ADD” then Name your AAA profile and press “ADD”.

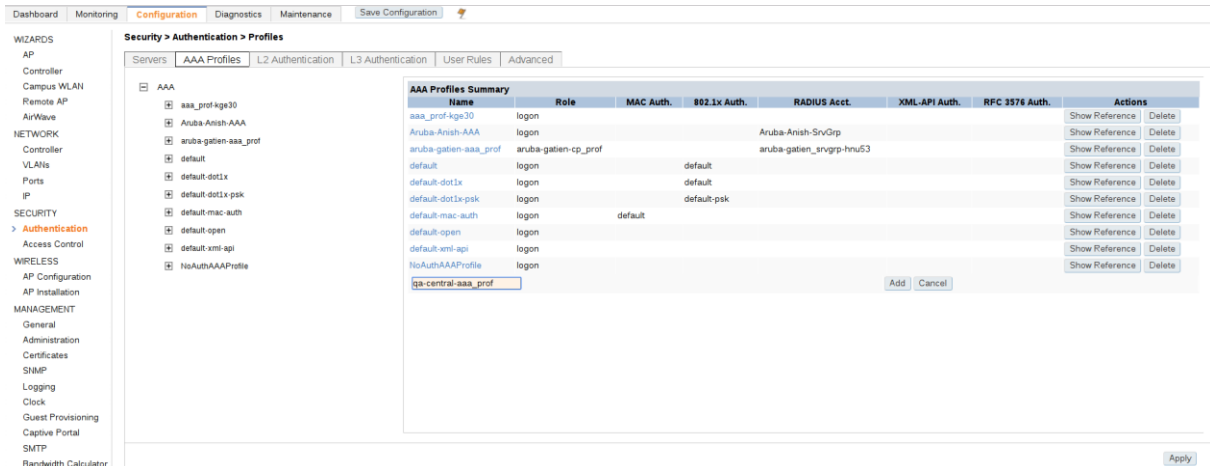


Figure 19: Creation of a AAA profile

Double click on the AAA profile you just created

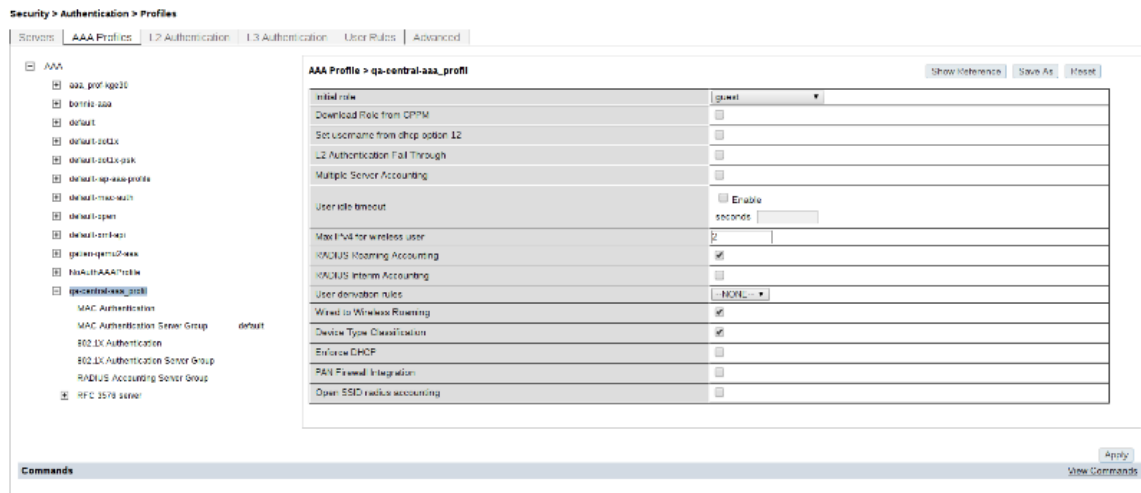


Figure 20: Configuration of the AAA profile

- Initial role = < Role to use for users not connected on the network >
- Uncheck “Wired to Wireless Roaming”
- Check “RADIUS Roaming Accounting”
- Check “RADIUS Interim Accounting”
- Click on “Apply”
- Click on “RADIUS Accounting Server Group” at the left menu under the AAA Profile you just created

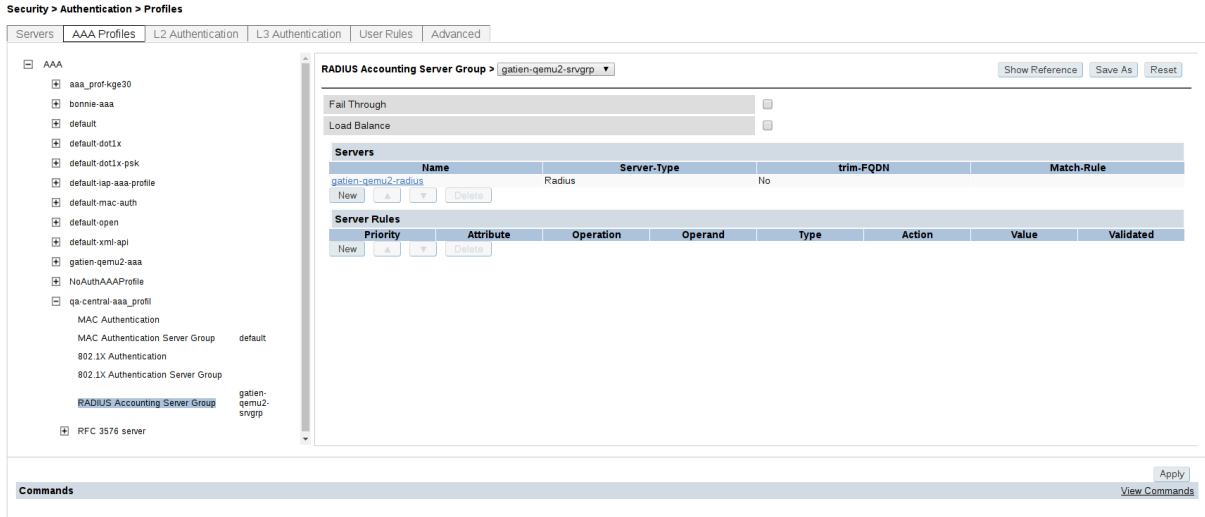


Figure 21: Configuration Radius Accounting on the AAA profile

Choose the server group created on section 5.3.2 and press « Apply »

5.3.6 Configuration of a WLAN

Go to “Configuration > WIRELESS > AP Configuration > AP Group” and click on one AP Group to Access more configuration.

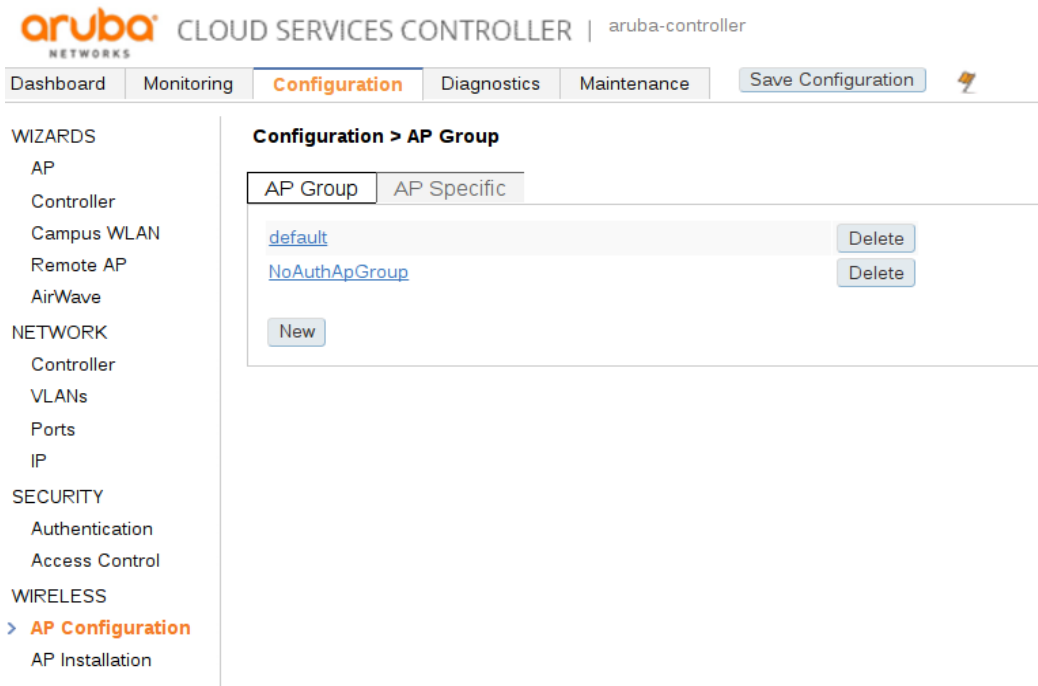
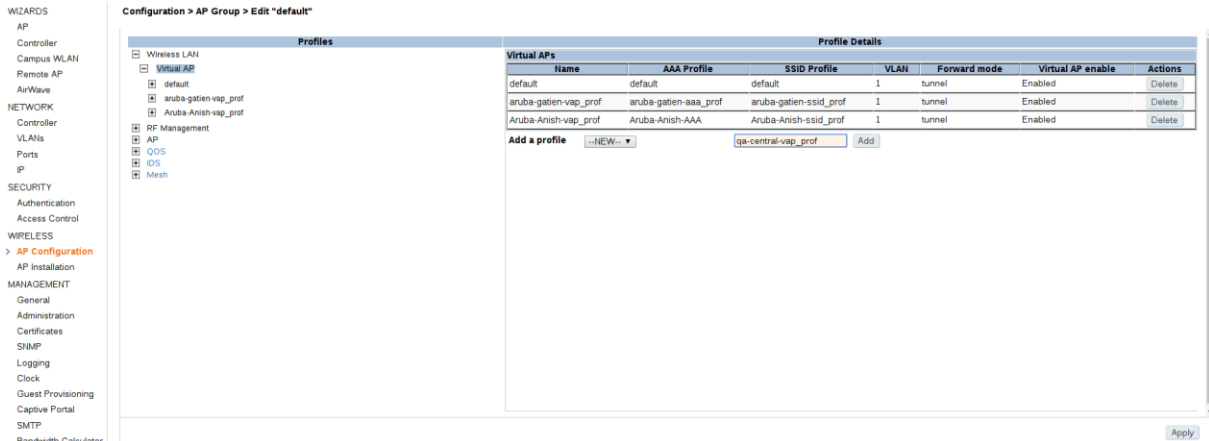


Figure 21 : AP Group configuration page

Click on “Wireless LAN” and then on “Virtual AP”.



Configuration > AP Group > Edit "default"

Profiles

- Wireless LAN
 - Virtual AP
 - default
 - aruba-galien-vap_prof
 - Aruba-Anish-vap_prof
 - RF Management
 - AP
 - QoS
 - IDS
 - Mesh

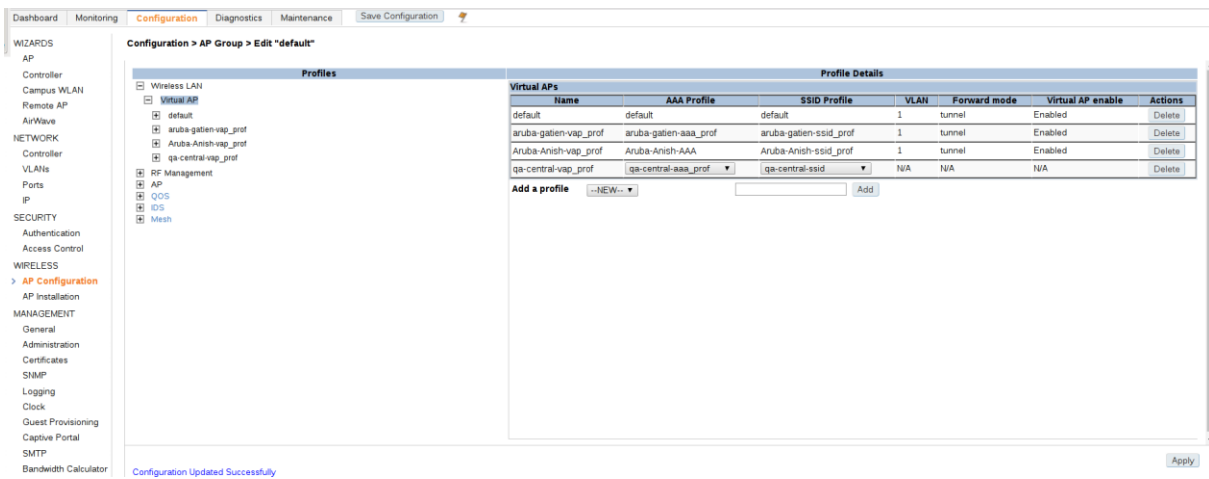
Profile Details

Name	AAA Profile	SSID Profile	VLAN	Forward mode	Virtual AP enable	Actions
default	default	default	1	tunnel	Enabled	Delete
aruba-galien-vap_prof	aruba-galien-aaa_prof	aruba-galien-ssid_prof	1	tunnel	Enabled	Delete
Aruba-Anish-vap_prof	Aruba-Anish-AAA	Aruba-Anish-ssid_prof	1	tunnel	Enabled	Delete

Add a profile: --NEW-- [qa-central-vap_prof] Add

Figure 22 : AP Group configuration page

- Add a new profile
- Choose your AAA profile created in step 5.3.5



Configuration > AP Group > Edit "default"

Profile Details

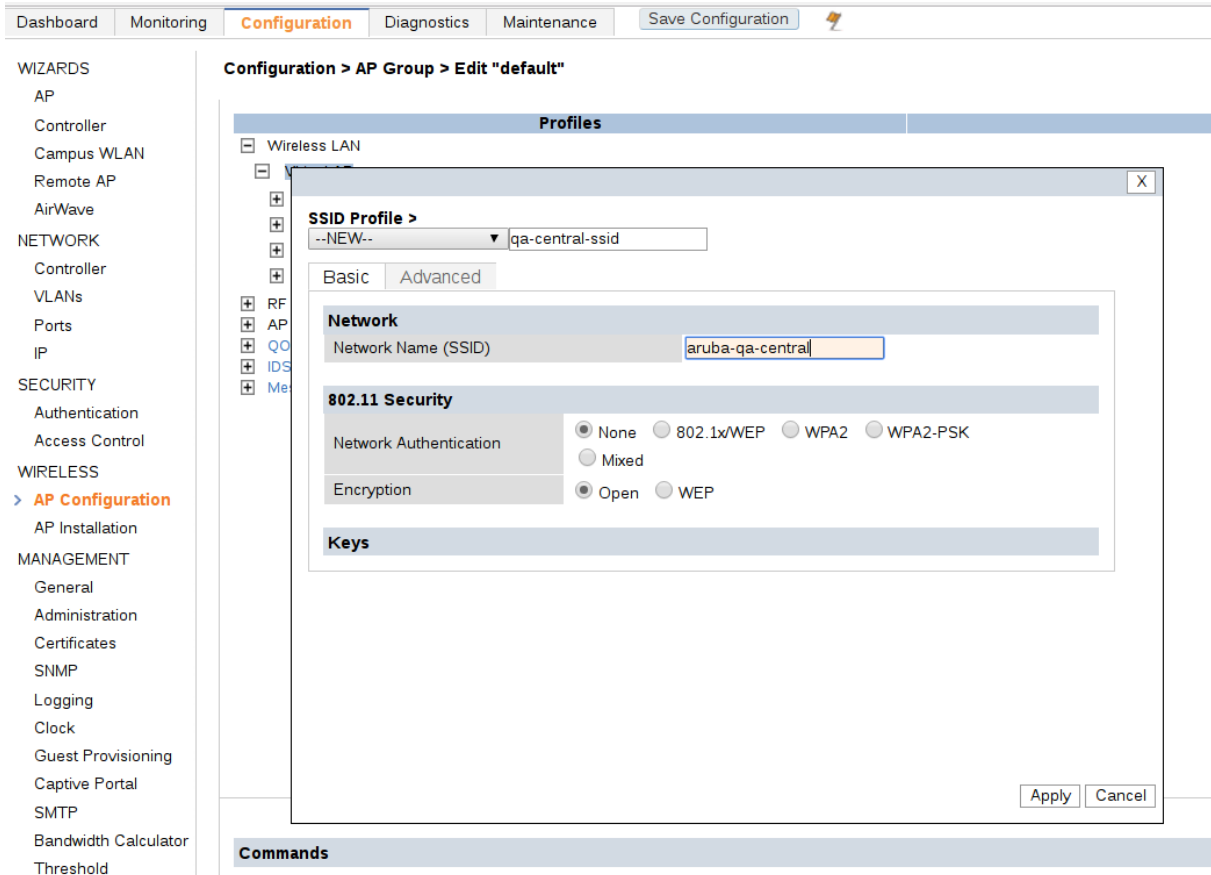
Name	AAA Profile	SSID Profile	VLAN	Forward mode	Virtual AP enable	Actions
default	default	default	1	tunnel	Enabled	Delete
aruba-galien-vap_prof	aruba-galien-aaa_prof	aruba-galien-ssid_prof	1	tunnel	Enabled	Delete
Aruba-Anish-vap_prof	Aruba-Anish-AAA	Aruba-Anish-ssid_prof	1	tunnel	Enabled	Delete
qa-central-vap_prof	qa-central-aaa_prof	qa-central-ssid	N/A	N/A	N/A	Delete

Add a profile: --NEW-- [] Add

Configuration Updated Successfully

Figure 23 : Virtual AP configuration

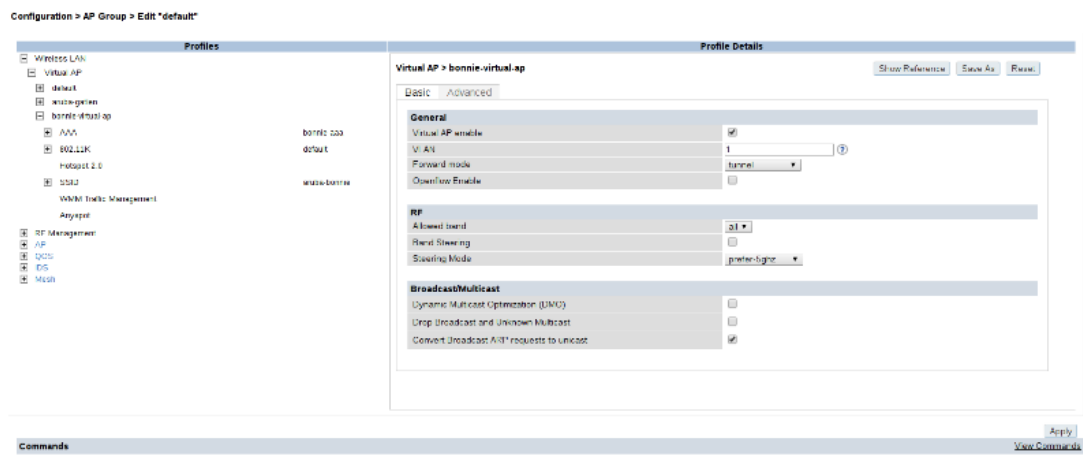
- Create your new SSID profile (--NEW--) to attach to this config
 - o Name you SSID Profile (Name must not already exist)
 - o Modify the "Network Name (SSID)" to create a new one (Choose a Network name that does not yet exists)
 - o Click on "Apply"



The screenshot shows the Aruba configuration interface with the 'Configuration > AP Group > Edit "default"' path selected. A 'Profiles' window is open, showing the 'SSID Profile >' configuration for 'qa-central-ssid'. The 'Network' section has 'Network Name (SSID)' set to 'aruba-qa-central'. The '802.11 Security' section has 'Network Authentication' set to 'None' and 'Encryption' set to 'Open'. The 'Keys' section is empty. 'Apply' and 'Cancel' buttons are visible at the bottom right of the popup.

Figure 24 : SSID creation popup

- If an error message occurs, click on the left menu <Name of the Virtual AP you just created>/AAA and change it again there. Click on apply
- Click on the Virtual AP you just created to edit it



The screenshot shows the Aruba configuration interface with the 'Configuration > AP Group > Edit "default"' path selected. The 'Profiles' window is open, showing the 'Virtual AP > bonnie-virtual-ap' configuration. The 'Basic' tab is selected. The 'General' section has 'Virtual AP enable' checked, 'VLAN' set to '1', and 'Forward mode' set to 'tunnel'. The 'RF' section has 'Allowed band' set to '31', 'Rend Steering' checked, and 'Scheduling Mode' set to 'prefer-higher'. The 'Broadcast/Multicast' section has 'Dynamic Multicast Optimization (DMO)' checked, 'Drop Broadcast and Unknown Multicast' checked, and 'Convert Broadcast ARP requests to unicast' checked. 'Apply' and 'View Commands' buttons are visible at the bottom right of the window.

Figure 25 : Virtual AP configuration

- VLAN = <select one existing Vlan>
- Press on "Apply"
- Press on "Save configuration"

5.3.7 Role differentiation

If you want to define, in addition to your default profile “guest”, a profile “VIP” with specific rules, QoS... when this information is received by Aruba from UCOPIA, in the RADIUS response, then you can configure this as shown below:

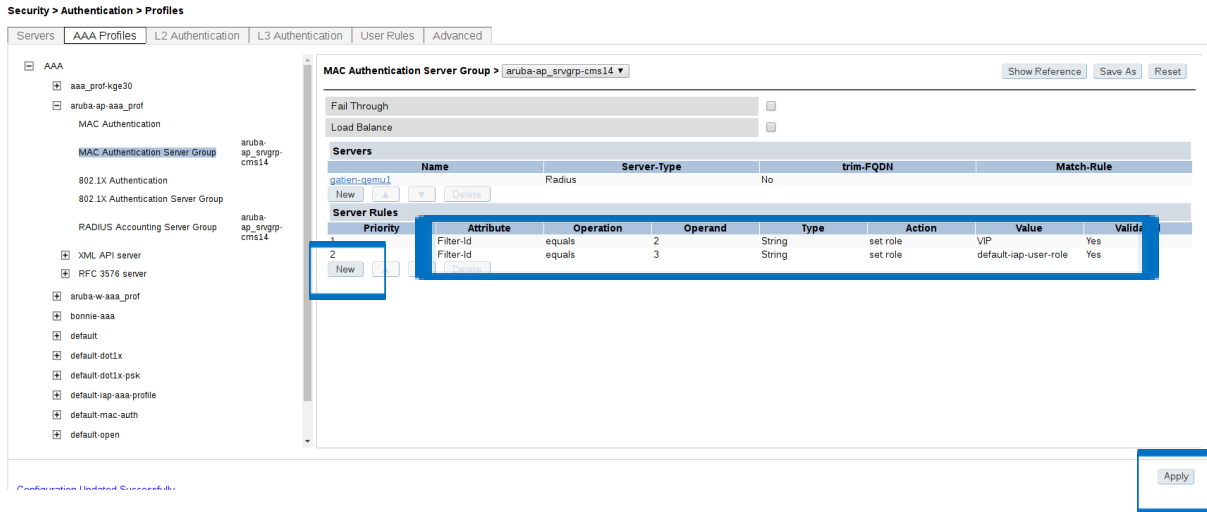


Figure 26 : Dynamic assignment of profile by Aruba

In this example, when Aruba receives the value 2 in the RADIUS field “Filter-Id”, then it will assign the profile “VIP” to the user with given QoS, data/time limit...

5.3.8 Configuration of the syslog server

Go to “Configuration > MANAGEMENT > Logging” and press “New”

Define the syslog configuration

- Define the external syslog server with IP address = OUT IP of the central UCOPIA controller
- Category = user
- Let the default logging facility (local 6)
- Choose the severity = Informational

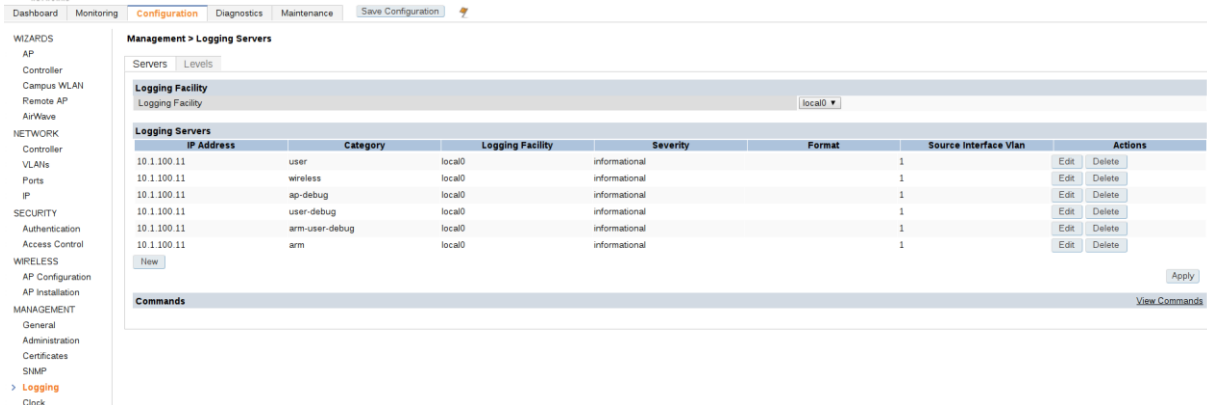


Figure 27 : Creation of the syslog server

5.4 Aruba IAP configuration

Connect on your Aruba Instant AP.

5.4.1 Creation of a WLAN Setting

Under the Network section, press “New”

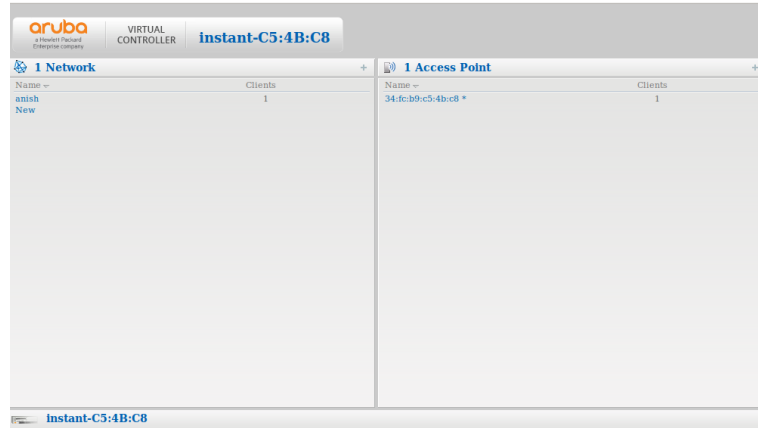


Figure 28 : Aruba iap admin panel

- Name = <name of the network>
- Primary usage = Guest

New WLAN
[Help](#)

1 WLAN Settings

2 VLAN

3 Security

4 Access

WLAN Settings

Name & Usage

Name:

Primary usage:

Employee

Voice

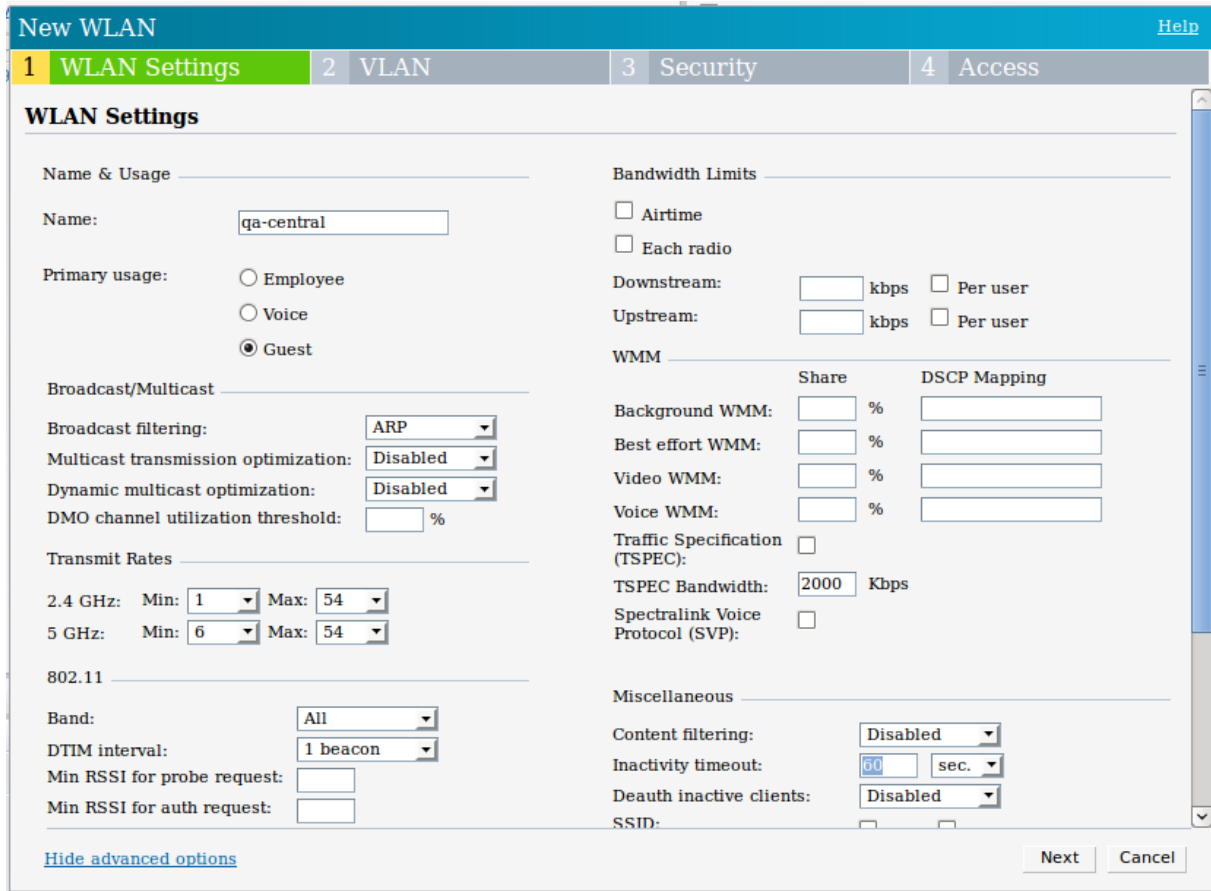
Guest

[Show advanced options](#)

Next

Cancel

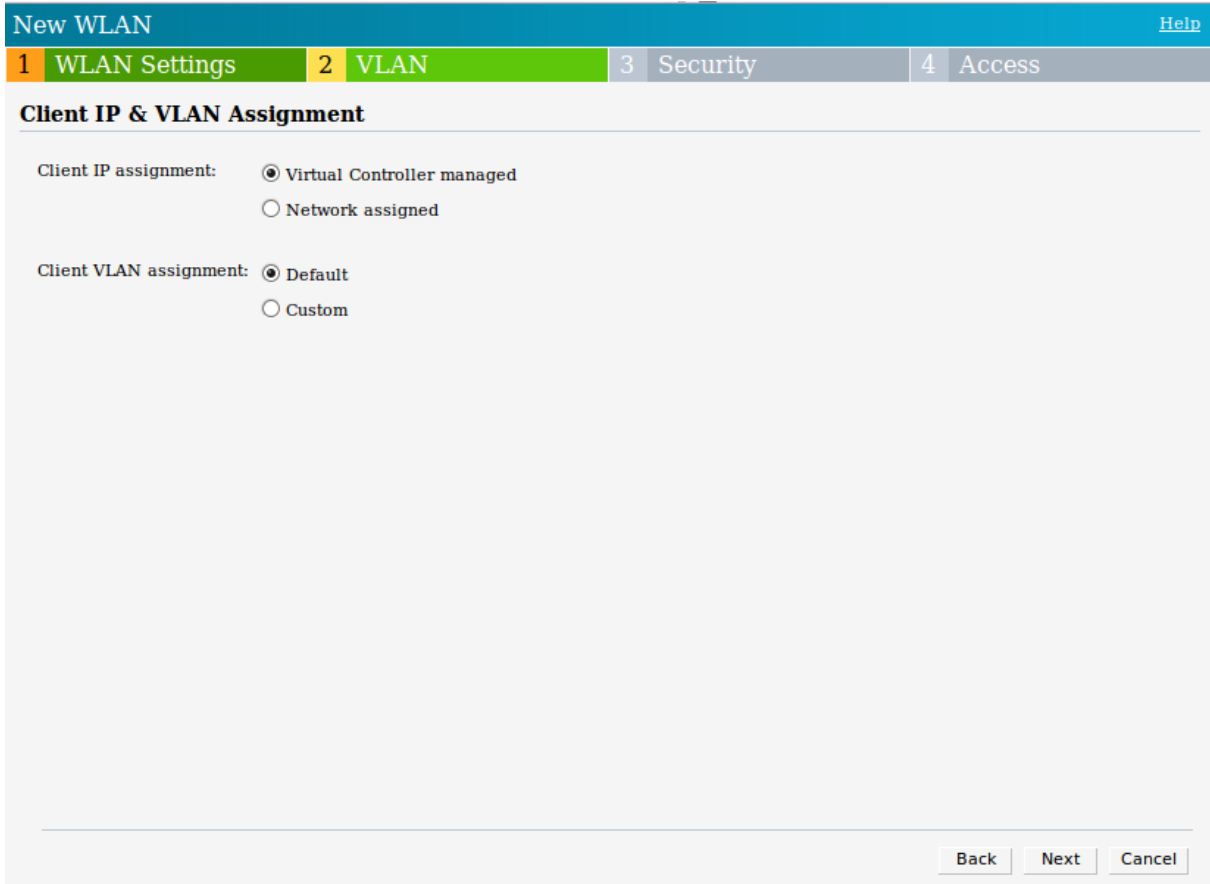
To change the user's inactivity time period, press "Show advanced options" and change inactivity timeout (minimum is 60 s).



The screenshot shows the 'New WLAN' configuration window with the 'WLAN Settings' tab selected. The 'Name' is 'qa-central' and 'Primary usage' is 'Guest'. Under 'Broadcast/Multicast', 'Broadcast filtering' is 'ARP', 'Multicast transmission optimization' is 'Disabled', and 'Dynamic multicast optimization' is 'Disabled'. 'Transmit Rates' are set to 1-54 for 2.4 GHz and 6-54 for 5 GHz. The 'Band' is 'All' and 'DTIM interval' is '1 beacon'. In the 'Miscellaneous' section, 'Content filtering' is 'Disabled', 'Inactivity timeout' is '60 sec', and 'Death inactive clients' is 'Disabled'. The 'Next' button is visible at the bottom right.

Press "Next"

5.4.2 Configure Client IP & VLAN Assignment



New WLAN [Help](#)

1 WLAN Settings 2 **VLAN** 3 Security 4 Access

Client IP & VLAN Assignment

Client IP assignment: Virtual Controller managed
 Network assigned

Client VLAN assignment: Default
 Custom

[Back](#) [Next](#) [Cancel](#)

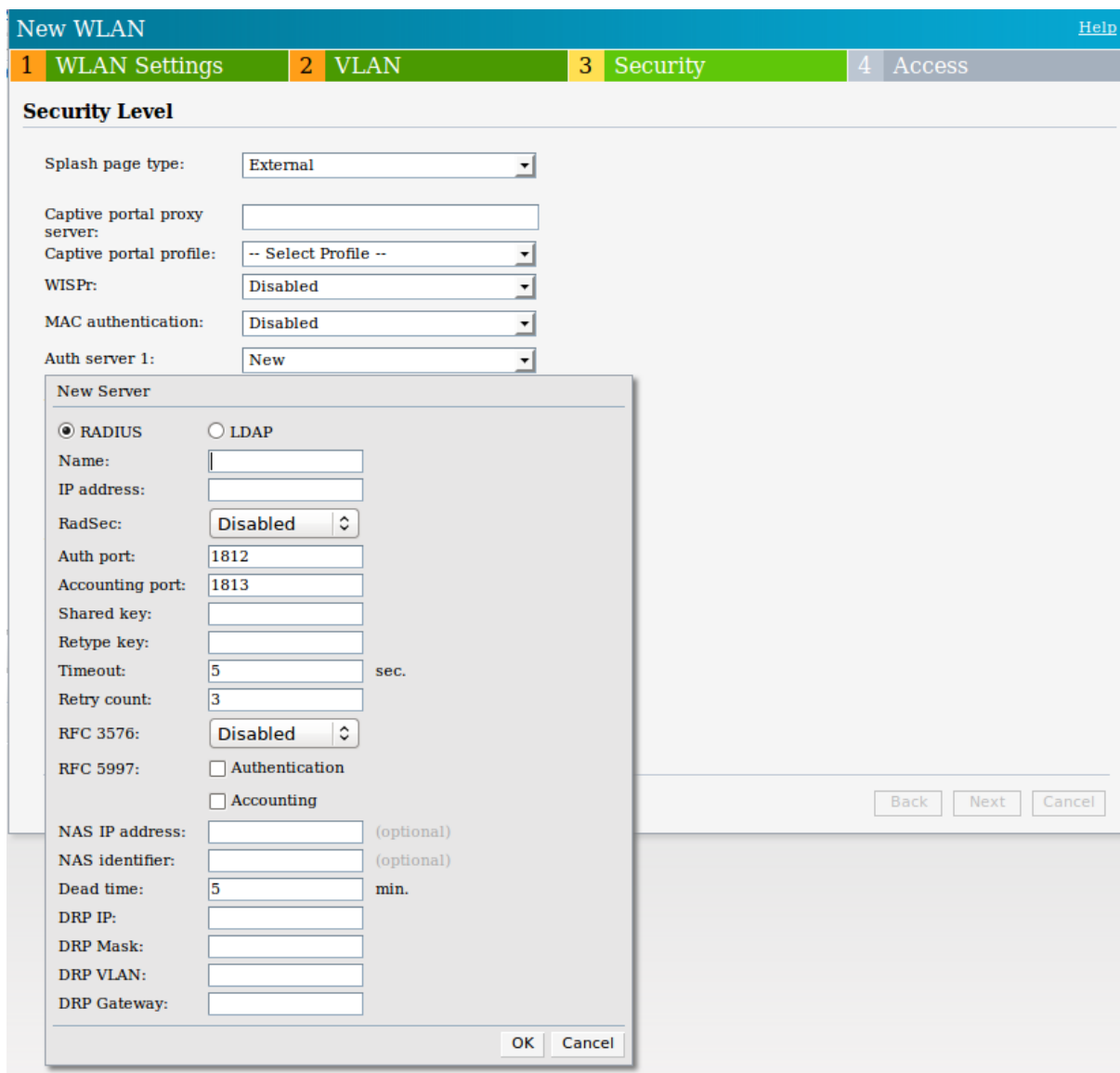
Here you can allow the virtual controller to manage the client IP or let the Network to assign an IP to the client.

Therefore, you can configure your client VLAN (create a VLAN by choosing “custom”)

- Click Next

5.4.3 Configuration of the external RADIUS server

Under the “Security” tab, select Auth server 1: and add a new server

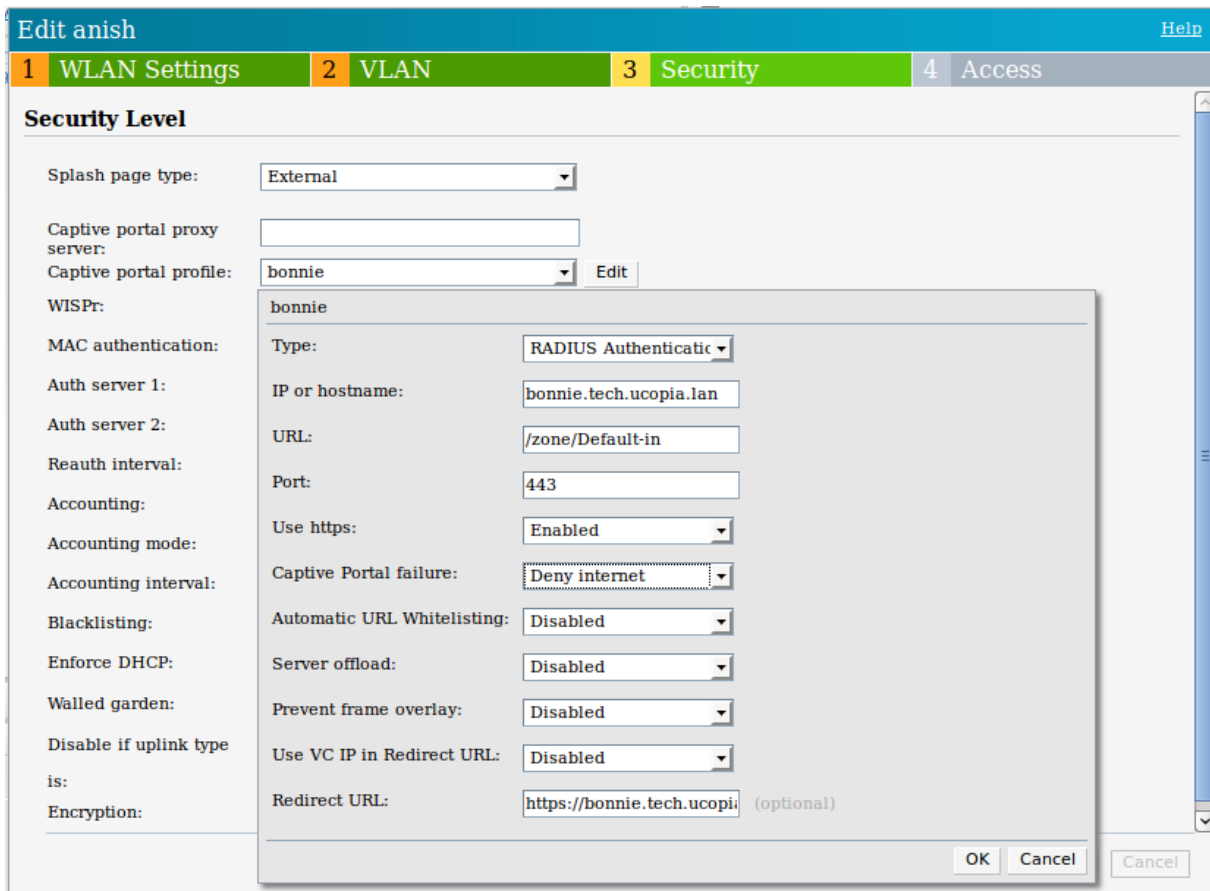


The screenshot shows the 'New WLAN' configuration page with the 'Security' tab selected. The 'Security Level' section includes fields for 'Splash page type' (External), 'Captive portal proxy server', 'Captive portal profile' (-- Select Profile --), 'WISPr' (Disabled), 'MAC authentication' (Disabled), and 'Auth server 1' (New). A 'New Server' dialog box is open, allowing the user to configure a RADIUS server. The dialog has radio buttons for 'RADIUS' (selected) and 'LDAP'. Fields include Name, IP address, RadSec (Disabled), Auth port (1812), Accounting port (1813), Shared key, Retype key, Timeout (5 sec), Retry count (3), RFC 3576 (Disabled), RFC 5997 (Authentication and Accounting checkboxes), NAS IP address (optional), NAS identifier (optional), Dead time (5 min), and various DHCP-related fields (DRP IP, Mask, VLAN, Gateway). 'OK' and 'Cancel' buttons are at the bottom of the dialog.

- Choose Radius radio button
- Name = <Name of the radius server>
- Ip address as [UCOPIA Controller IP address on out]
- Define the ports to be used
- The Shared key must be the same as the shared RADIUS secret on the central controller.
- Retype key [same as shared key]
- Press “OK”

5.4.4 Configuration of the captive portal profile

Under the “Security” tab, select “Captive portal profile”: and add a new Captive portal



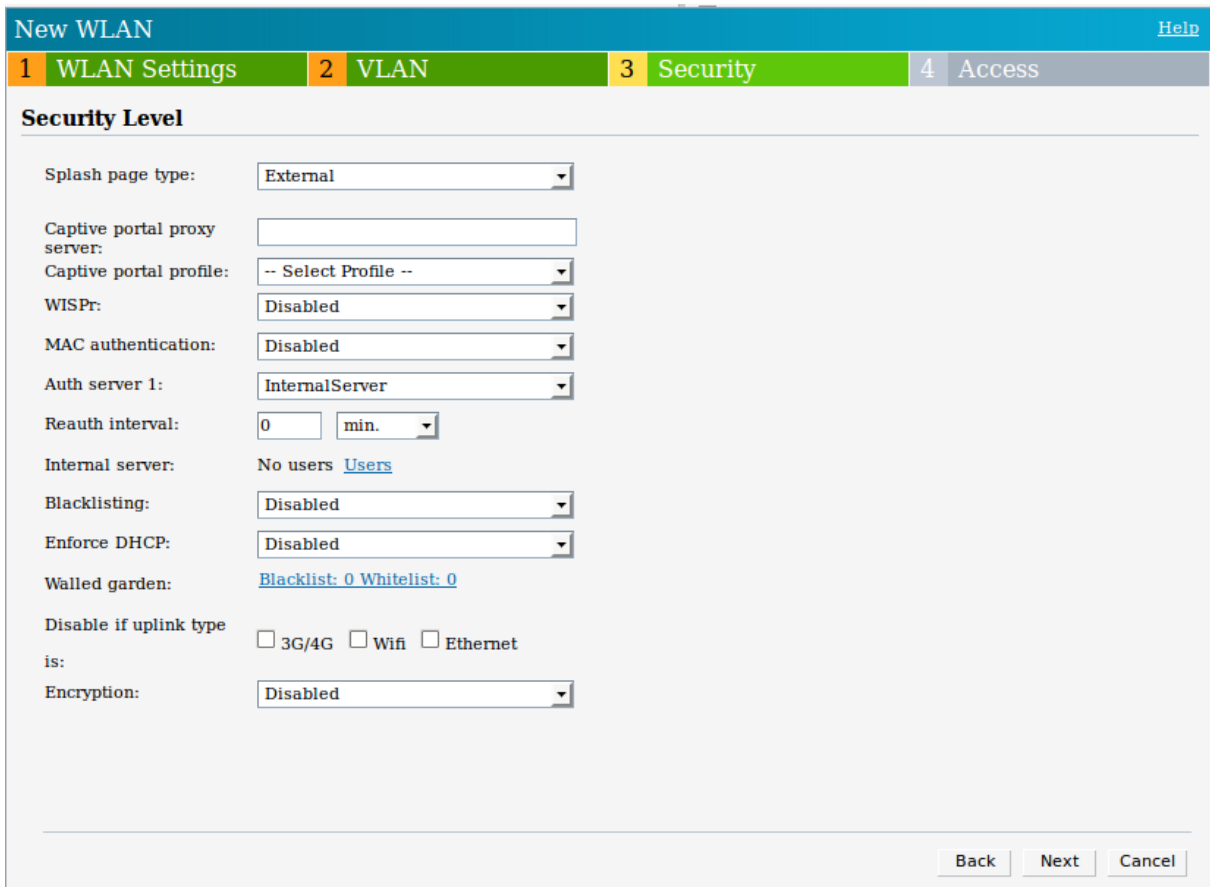
The screenshot shows the 'Edit anish' configuration window with the 'Security' tab selected. The 'Security Level' section is expanded to show the configuration for the 'bonnie' captive portal profile. The configuration is as follows:

Field	Value
Splash page type:	External
Captive portal proxy server:	
Captive portal profile:	bonnie (with Edit button)
WISPr:	bonnie
MAC authentication:	Type: RADIUS Authentication
Auth server 1:	IP or hostname: bonnie.tech.ucopia.lan
Auth server 2:	URL: /zone/Default-in
Reauth interval:	Port: 443
Accounting:	Use https: Enabled
Accounting mode:	Captive Portal failure: Deny internet
Accounting interval:	Automatic URL Whitelisting: Disabled
Blacklisting:	Server offload: Disabled
Enforce DHCP:	Prevent frame overlay: Disabled
Walled garden:	Use VC IP in Redirect URL: Disabled
Disable if uplink type is:	Redirect URL: https://bonnie.tech.ucopi (optional)
Encryption:	

- Name = <the captive portal profile name>
- Type = “RADIUS Authentication”
- IP or hostname = <central controller FQDN>
- URL = /zone/<zone label>
- Port = 443
- Use https = Enabled
- Captive Portal failure = Deny internet
- Automatic URL Whitelisting = Disabled
- Server offload = Disabled
- Prevent frame overlay = Disabled
- Use VC IP in Redirect URL = Disabled
- Redirect URL = https://<central controller FQDN>/zone/<zone label>
- Press “OK”

5.4.5 Configuring Security Level

Under the “Security” tab



New WLAN [Help](#)

1 **WLAN Settings** 2 **VLAN** 3 **Security** 4 **Access**

Security Level

Splash page type:

Captive portal proxy server:

Captive portal profile:

WISPr:

MAC authentication:

Auth server 1:

Reauth interval:

Internal server: No users [Users](#)

Blacklisting:

Enforce DHCP:

Walled garden: [Blacklist: 0](#) [Whitelist: 0](#)

Disable if uplink type is: 3G/4G Wifi Ethernet

Encryption:

- Splash page type as “External”
- Captive portal profile = [Captive portal profile created in section 5.4.4]
- WisPr = Disabled
- MAC Authentication = Disabled
- Auth server 1 = [Radius server created in section 5.4.3
- Accounting = Use authentication servers
- Accounting mode = Authentication
- Accounting interval = 0
- Press “Next”

5.4.6 Access Rules

Choose a role-based access rule.

Here, you can create the desired role to assign to all clients who connect to a network

Edit anish Help

1 WLAN Settings 2 VLAN 3 Security 4 Access

Access Rules

More Control

Role-based

Network-based

Unrestricted

Less Control

Roles

- wired-instant
- anish
- PreAuth

New Delete

Access Rules for PreAuth

- Allow any to domain controller.access.network.
- Allow any to domain central.access.network.
- Allow any to domain bonnie.tech.ucopia.lan.

New Edit Delete ↑ ↓

Role Assignment Rules

Default role: anish

New Edit Delete ↑ ↓

Assign pre-authentication role: PreAuth

Back Finish Cancel

1 WLAN Settings 2 VLAN 3 Security 4 Access

Access Rules

More Control

Role-based

Network-based

Unrestricted

Less Control

Roles

- wired-instant
- anish
- PreAuth

New Delete

Access Rules for PreAuth

- Allow any to domain controller.access.network.
- Allow any to domain central.access.network.
- Allow any to domain bonnie.tech.ucopia.lan.

New Edit Delete ↑ ↓

Role Assignment Rules

Default role: anish

New Edit Delete ↑ ↓

Assign pre-authentication role: PreAuth

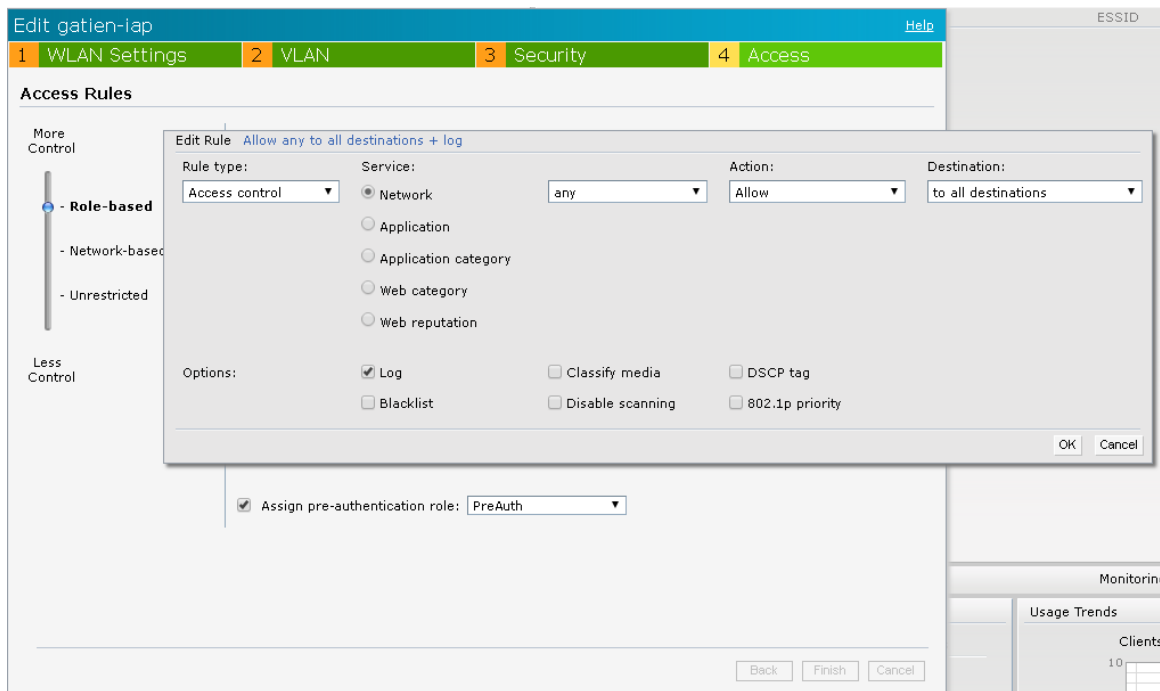
Back Finish Cancel

Once a role is created by following the steps below,

- Press “New” under the Roles section
- Enter a new role
- Click OK

Then, you can assign access rules to the role. To do so, you have to

- Click on the role you just created
- Press “New” under the “Access Rules for” section



Then configure the rule you want by choosing the desired Rule type.

You can also define a specific rule before assigning a role to a connected user.

- Go to the “Role Assignment Rules” section
- Press “New” to add a new condition
- Under Attribute, you can select to attribute to compare. Here we choose the Filter-Id attribute.
- Under Role, select the role to assign to the user if the condition is respected.
- Press “OK”

The « Role Assignment Rules » can enable you to make rules as:

- If Filter-Id equal 2 Assign Role “Bandwidth-limit”
- If Filter-Id equal 3 Assign Role “limited-category-profile”

1 WLAN Settings 2 VLAN 3 Security 4 Access

Access Rules

More Control

Less Control

Role-based
 Network-based
 Unrestricted

Roles

- wired-instant
- anish
- PreAuth

New Delete

Access Rules for PreAuth

- Allow any to domain .twitter.com.
- Allow any to domain .twimg.com.
- Allow any to domain controller.access.network.

New Edit Delete ↑ ↓

Role Assignment Rules

Default role: anish

New Role Assignment Rule

Attribute:	Operator:	String:	Role:
Filter-Id	equals	2	wired-instant

OK Cancel

Assign pre-authentication role: PreAuth

Press 'Finish'

5.4.7 Configuration of the syslog server

Define the syslog configuration

- Press System, then "show advanced option"
- Press "Monitoring" tab
- Define the syslog server with IP address = <the central UCOPIA controller IP>
- Choose the Facility Levels = INFO

Then edit your Network configuration to allow the user to send its logs to an external server. To do that, click on your network to edit it.

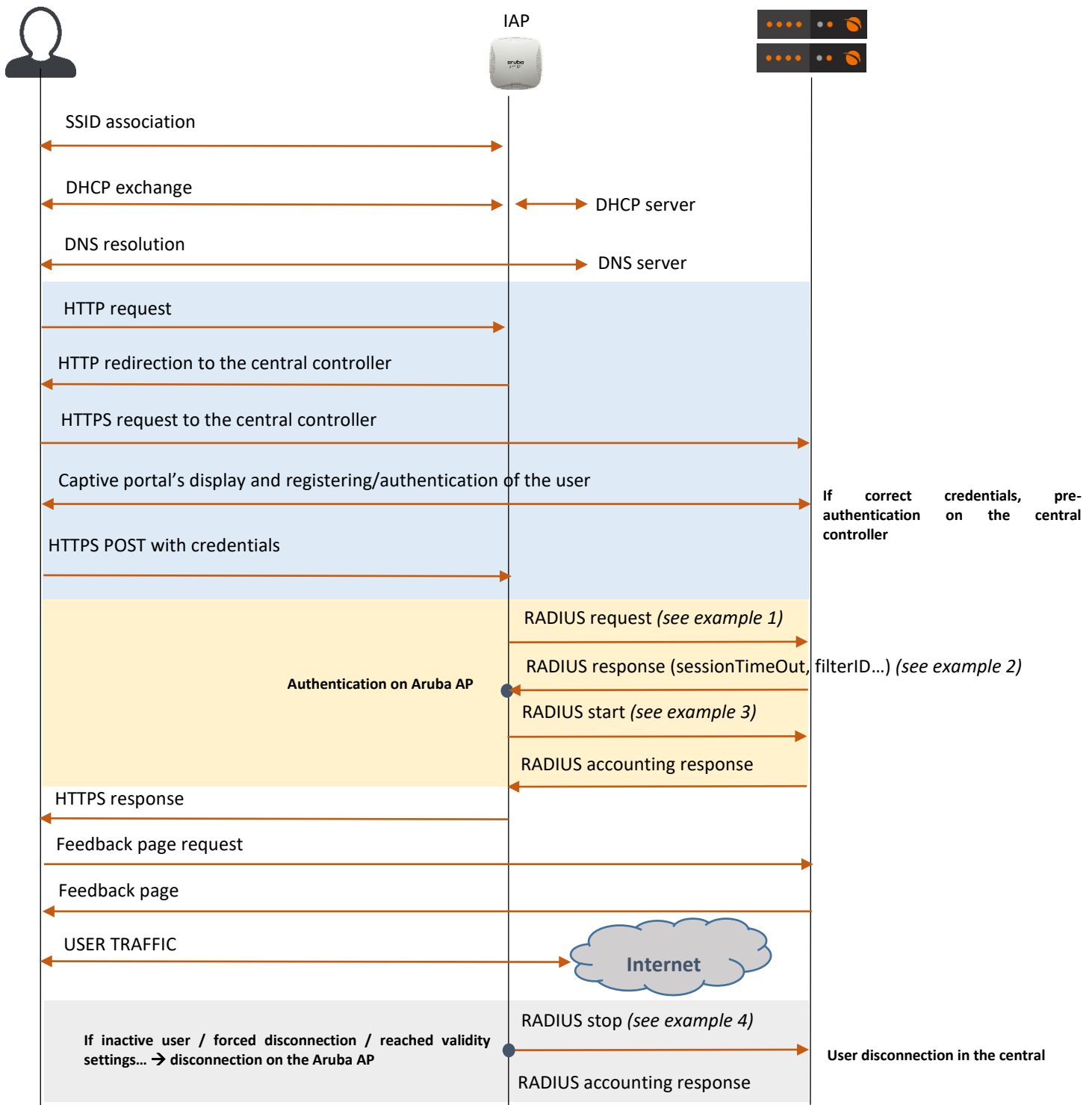
- Go to the Access tab
- Edit the user's role and add a new Access rule (At least one access rule must allow syslog to your central ucopia controller).
- For your traffic to be logged, check the log option. This will log info when rule matches.

Click on OK

6 Annex 1: detailed flow diagram

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

6.1 Portal authentication



T

This diagram illustrates the exchanges in case of an Aruba IAP architecture. In the case of controller-based APs, then the IAP should be replaced by the Aruba controller (which initiates the redirection and RADIUS exchanges with the UCOPIA controller. The light APs never communicate with the UCOPIA controller).

6.2 RADIUS exchanges

Example 1: RADIUS Access-Request

Aruba Instant AP Access-Request

```
Thu Nov 30 11:03:18 2017
Packet-Type = Access-Request
NAS-IP-Address = 10.1.2.6
NAS-Port = 0
NAS-Port-Type = Wireless-802.11
User-Name = "a"
Service-Type = Login-User
Calling-Station-Id = "446d6cb61a82"
Called-Station-Id = "34fcb9c54bc8"
Framed-IP-Address = 172.31.99.117
Aruba-Essid-Name = "gatien-iap"
Aruba-Location-Id = "34:fc:b9:c5:4b:c8"
Aruba-AP-Group = "instant-C5:4B:C8"
Aruba-Attr-12 = 0x416e64726f6964
Message-Authenticator = 0xfd6fb6c7c927398c460df0a437fcffbf
```

Calling-Station-Id = MAC address of the end user

Called-Station-Id = MAC address of the NAS (configurable)

Framed-IP-Address = IP address of the user after authentication

Aruba Controller Access-Request

```
Thu Nov 30 12:37:18 2017
Packet-Type = Access-Request
NAS-IP-Address = 10.1.2.5
NAS-Port = 0
NAS-Port-Type = Wireless-802.11
User-Name = "A"
Service-Type = Login-User
Calling-Station-Id = "C486E95E99EB"
Called-Station-Id = "204C0303CCF8"
Framed-IP-Address = 10.1.255.29
Aruba-Essid-Name = "aruba-ap"
Aruba-Location-Id = "AP1"
Aruba-AP-Group = "default"
Aruba-Attr-12 = 0x416e64726f6964
Message-Authenticator = 0x279c0d47c12e0d602ce12c1109b16a69
```

Example 2: RADIUS Access-Accept

Aruba Instant AP Access-Accept

```
Thu Dec 21 17:52:36 2017
Packet-Type = Access-Accept
Ucopia-Ldap-Id = "1"
Ucopia-validitytype = "inherited"
Ucopia-ProfileId := "3"
Ruckus-Role := "3"
Filter-Id := "3"
Ucopia-Group := "Fin_valid_15min"
User-Name := "s"
Session-Timeout = 900
```

Aruba Controller Access-Accept

```
Thu Dec 21 19:02:27 2017
Packet-Type = Access-Accept
Ucopia-Ldap-Id = "1"
Ucopia-validitytype = "inherited"
Ucopia-ProfileId := "4"
Ruckus-Role := "4"
Filter-Id := "4"
Ucopia-Group := "Cred_15min"
User-Name := "d"
Session-Timeout = 900
```

Example 3: RADIUS Accounting Start

Aruba Instant AP Accounting Start

```
Thu Nov 30 11:03:18 2017
Acct-Status-Type = Start
NAS-IP-Address = 10.1.2.6
User-Name = "a"
NAS-Port = 0
NAS-Port-Type = Wireless-802.11
Calling-Station-Id = "44:6d:6c:b6:1a:82"
Called-Station-Id = "34fcb9c54bc8"
Framed-IP-Address = 172.31.99.117
Acct-Multi-Session-Id = "446D6CB61A82-1512036171"
Acct-Session-Id = "34FCB9D4BC91-446D6CB61A82-5A1FD767-852C0"
Acct-Delay-Time = 0
Aruba-Essid-Name = "gatien-iap"
Aruba-Location-Id = "34:fc:b9:c5:4b:c8"
Aruba-User-Vlan = 3333
Aruba-Attr-12 = 0x416e64726f6964
Acct-Authentic = 0
Acct-Unique-Session-Id = "e61652bb7eebce3b"
Stripped-User-Name = "a"
Realm = "NULL"
Timestamp = 1512036198
```

Aruba Controller Accounting Start

```
Thu Nov 30 12:11:23 2017
User-Name = "A"
NAS-IP-Address = 10.1.2.5
NAS-Port = 0
NAS-Port-Type = Wireless-802.11
Acct-Session-Id = "A446D6CB61A82-5A1FE75B-844AB"
Event-Timestamp = "Nov 30 2017 12:11:23 CET"
Acct-Multi-Session-Id = "446D6CB61A82-0000000106"
Framed-IP-Address = 10.1.255.89
Calling-Station-Id = "44:6d:6c:b6:1a:82"
Called-Station-Id = "204C0303CCF8"
Acct-Delay-Time = 0
Aruba-Essid-Name = "aruba-ap"
Aruba-Location-Id = "AP1"
Aruba-AP-Group = "default"
Aruba-User-Role = "guest-logon"
Aruba-User-Vlan = 1
Aruba-Attr-12 = 0x416e64726f6964
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Acct-Unique-Session-Id = "6a693451b7df255a"
Stripped-User-Name = "A"
Realm = "NULL"
Timestamp = 1512040283
```

Aruba Controller Interim update

```
Thu Nov 30 12:11:35 2017
User-Name = "A"
NAS-IP-Address = 10.1.2.5
NAS-Port = 0
NAS-Port-Type = Wireless-802.11
Acct-Session-Id = "A446D6CB61A82-5A1FE75B-844AB"
Event-Timestamp = "Nov 30 2017 12:11:35 CET"
Acct-Multi-Session-Id = "446D6CB61A82-0000000106"
Framed-IP-Address = 10.1.255.89
Calling-Station-Id = "44:6d:6c:b6:1a:82"
Called-Station-Id = "204C0303CCF8"
Acct-Delay-Time = 0
Aruba-Essid-Name = "aruba-ap"
Aruba-Location-Id = "AP3"
Aruba-AP-Group = "default"
Aruba-User-Role = "guest-logon"
Aruba-User-Vlan = 1
Aruba-Attr-12 = 0x416e64726f6964
Acct-Status-Type = Interim-Update
Acct-Unique-Session-Id = "6a693451b7df255a"
Stripped-User-Name = "A"
Realm = "NULL"
Timestamp = 1512040295
```

Example 4: RADIUS accounting stop

Aruba Instant AP accounting stop

```
Thu Nov 30 11:04:13 2017
Acct-Status-Type = Stop
NAS-IP-Address = 10.1.2.6
User-Name = "a"
NAS-Port = 0
NAS-Port-Type = Wireless-802.11
Calling-Station-Id = "44:6d:6c:b6:1a:82"
Called-Station-Id = "34fcb9c54bc8"
Framed-IP-Address = 172.31.99.117
Acct-Multi-Session-Id = "446D6CB61A82-1512036171"
Acct-Session-Id = "34FCB9D4BC91-446D6CB61A82-5A1FD767-852C0"
Acct-Delay-Time = 0
Aruba-Essid-Name = "gatien-iap"
Aruba-Location-Id = "34:fc:b9:c5:4b:c8"
Aruba-User-Vlan = 3333
Aruba-Attr-12 = 0x416e64726f6964
Acct-Input-Octets = 62063
Acct-Output-Octets = 1070333
Acct-Input-Packets = 575
Acct-Output-Packets = 969
Acct-Terminate-Cause = Admin-Reset
Acct-Session-Time = 55
Acct-Unique-Session-Id = "e61652bb7eebce3b"
Stripped-User-Name = "a"
Realm = "NULL"
Timestamp = 1512036253
```

Aruba Controller Accounting stop

```
Thu Nov 30 12:25:31 2017
User-Name = "a"
NAS-IP-Address = 10.1.2.5
NAS-Port = 0
NAS-Port-Type = Wireless-802.11
Acct-Session-Id = "a206274B4AF18-5A169921-CA508"
Event-Timestamp = "Nov 23 2017 12:28:17 CET"
Acct-Multi-Session-Id = "206274B4AF18-0000000099"
Framed-IP-Address = 10.1.255.242
Calling-Station-Id = "20:62:74:b4:af:18"
Called-Station-Id = "204C0303CCF8"
Acct-Delay-Time = 0
Aruba-Essid-Name = "aruba-ap"
Aruba-Location-Id = "AP3"
Aruba-AP-Group = "default"
Aruba-User-Role = "gatien-qemu2-cp_prof"
Aruba-User-Vlan = 1
Aruba-Attr-12 = 0x57696e646f77732050686f6e65
Acct-Status-Type = Stop
Acct-Input-Octets = 434487
Acct-Output-Octets = 2681478
Acct-Input-Packets = 2204
Acct-Output-Packets = 3019
Acct-Terminate-Cause = Admin-Reset
Acct-Session-Time = 6064
Acct-Unique-Session-Id = "ca28b7e4926843f8"
Stripped-User-Name = "a"
Realm = "NULL"
Timestamp = 1512041131
```


7 Annex 2: Walled garden for social networks

7.1 Facebook, Twitter, Google, LinkedIn

The following open-access URLs must be opened.

Facebook	facebook.com
	facebook.net
	akamaihd.net
	fbcdn.net
Google	google.com We recommend you to add also your local Google domain (e.g. "*google.us" for USA, "*google.it" for Italy, "*google.co.uk" for UK, etc.).
	googleapis.com
	gstatic.com
LinkedIn	linkedin.com
	licdn.com
Twitter	*.twitter.com
	*.twimg.com
	abs.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 Aruba architecture:

Features	OOB Aruba	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 "central.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 through it
Access permissions on basis of user profile	✓	Aruba profile management based on RADIUS attributes, the OS type, the location, the MAC address or the schedule. Aruba can use the information of UCOPIA profile provided that no dynamic VLAN is used.
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	-	Sent by Aruba AP to UCOPIA in real-time
- User sessions	-	
- Traffic	-	
- URL		
- Automatic logs backup via FTP(S)	-	
- Automatic logs compression	-	
Audit logs (Syslog)	-	
MOBILITY		

QoS (by service, by user)		No BW limitation / reservation possible on UCOPIA as the traffic won't go through it
Data volume quota		No quota applied by UCOPIA as the traffic won't go through 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)		The disconnection button is hidden in an OOB Aruba architecture because the Aruba API won't support such a disconnection request from the user browser
Increased security		
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/autofillink 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	✓	