UCOPIA

TURN YOUR WI-FI UP

Out-Of-Band Aerohive architecture

Version 5.1

Table of contents

Table of figures

1 Introduction

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

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

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

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

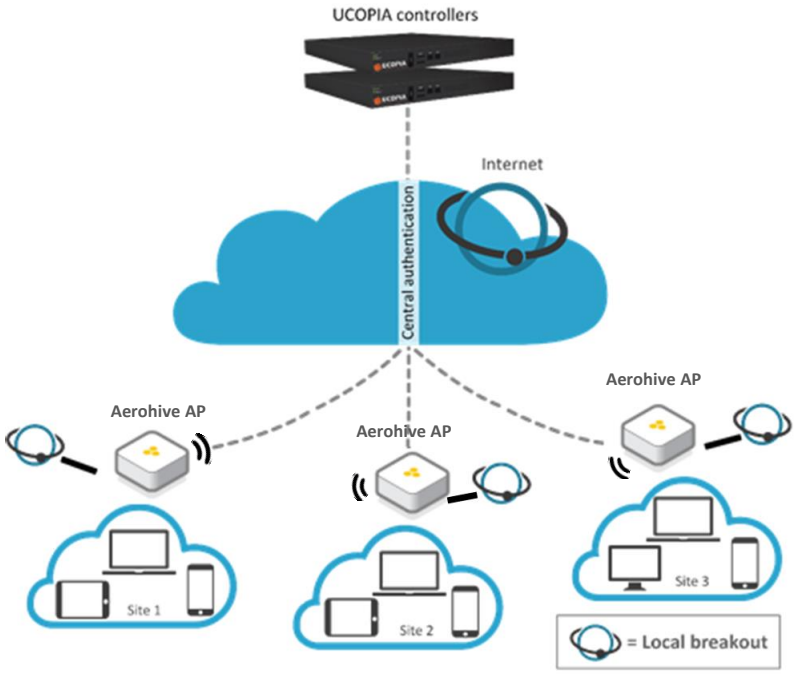


Figure 1 : Global Out-of-Band Aerohive architecture

2 User experience workflow

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

The workflow is as follows:

1. Once associated to the Wi-Fi, the user launches his (her) Web browser.
2. The Aerohive 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 analyzed by the central controller. If the credentials entered by the user are correct, the authentication process is performed between the Aerohive AP and the central controller through the RADIUS protocol. The user's validity settings are sent to the Aerohive AP 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.

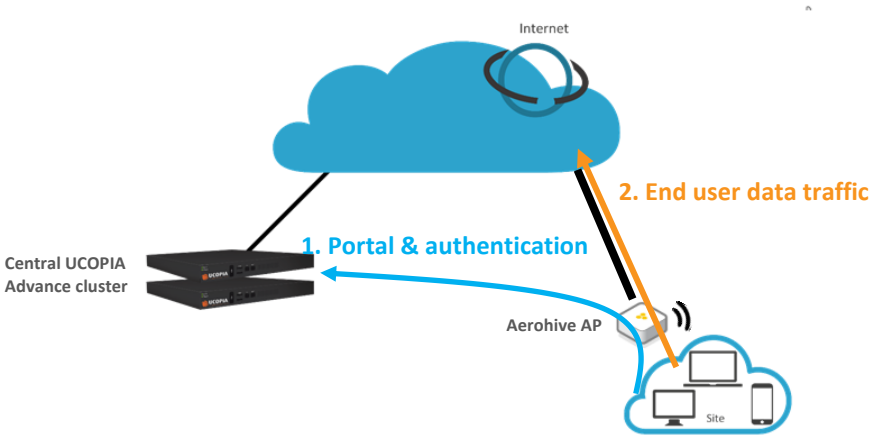


Figure 2 : User traffic flow

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 Aerohive AP via RADIUS exchanges such as the profile name, the user name, the expiration date, the session timeout in case of time credit…so that the Aerohive AP can enforce time validity checking before letting the user access the network.

Note: As Aerohive 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 Aerohive AP

3.1.4 Centralization of user logs

All Aerohive 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 UCOPIA controllers. This logs exchange is done via the standard Syslog (UDP / port 514).
All Aerohive logs sent to UCOPIA are to be seen on the HiveManager GUI, in "Monitor > Devices > Select your AP > Utilities > Diagnostics > Show Log".

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

- Connected users
- Sessions
- Traffic

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

3.1.5 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 Aerohive and UCOPIA versions

The Out-Of-Band Aerohive architecture requires a HiveOS version ≥ 6.1r3 in order to guarantee the logs' externalization (previous versions can't be used for log exploitation).

Only UCOPIA controllers from version 5.1.6 enable to set up an Out-Of-Band Aerohive configuration.

3.2.2 Supported authentication / registration modes

With the Out-Of-Band Aerohive 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 control his DNS server and resolve "controller.access.network" with the IP address of his UCOPIA controller
  → or change the domain name of his UCOPIA controller, create a new certificate and create his own social network application

3.2.3 Profile differentiation

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

Aerohive 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 Aerohive 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.

Attention: The profile differentiation based on the UCOPIA profile information (in the RADIUS field "Filter-Id") do not work if dynamic VLAN is used. If you use dynamic VLAN assignment, then, the profile differentiation based on RADIUS field can only be done using the tuple "Tunnel-Type", "Tunnel-Medium-Type" and "Tunnel-Private-Group-Id" which is used with dynamic VLAN. Indeed, Aerohive doesn't even try to interpret the other RADIUS attributes when this tuple is in the RADIUS response.

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

- Time-based criteria:

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

Configuration of a later starting validity date and the increased security aren't supported in this architecture.

- 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 Aerohive. So, any desired QoS policy should be directly configured and set up in the Aerohive AP.

3.2.5 User disconnection

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

	Supported in the Out-Of-Band Aerohive architecture?
Increased security	**No** *Description: the user will be disconnected from UCOPIA controller but not on Aerohive 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.*
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 Ou-Of-Band architecture is configured, the central controller disable its autodisconnect feature.* *Only the autodisconnect on Aerohive will be able to disconnect a user after a given inactivity period.*
Manual disconnection	**No** *Description: The Aerohive API doesn't allow such disconnection request. The disconnection button has been deleted from the feedback page in the Out-Of-Band Aerohive.*
Reached max quota	**No** *Description: The Aerohive AP 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 Aerohive APs on local sites. In case of network failure between the Aerohive 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 license for managing multi-sites is needed.

You can configure a license limitation per zone or per profile to make sure that the mutualized licence isn't completely consumed by a given site.

5 UCOPIA configuration

5.1 Prerequisites

5.1.1 Time synchronization (on UCOPIA and Aerohive)

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

On Aerohive: configure the NTP server in the HiveManager GUI "Configuration > (Your Network Policy) > Additional Settings > Management Server Settings > 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 Aerohive 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.

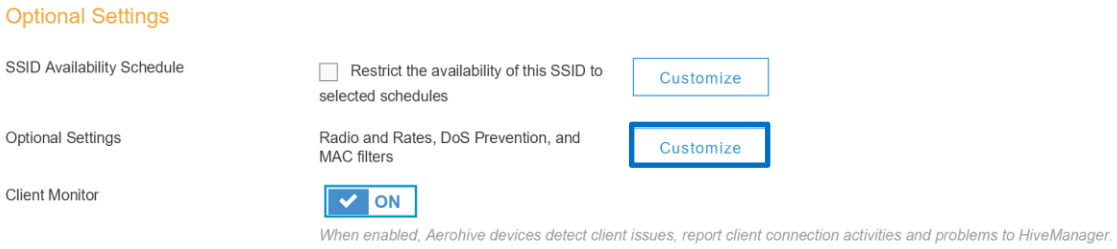
Source @IP	Destination @IP	Port
User's equipment on remote site	Central controller	TCP/443
Aerohive AP	Central controller	TCP/443, UDP/1812, UDP/1813, UDP/514

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

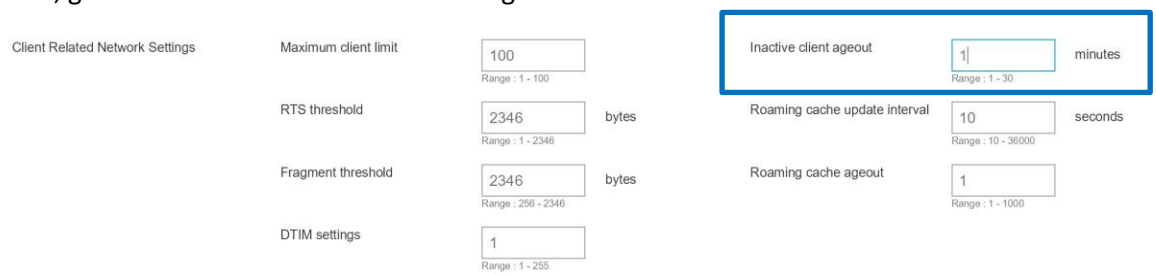
5.1.3 Auto disconnection settings (on Aerohive)

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

This "auto disconnection" feature on Aerohive AP can be configured on the HiveManager in "Configure > Network Policies > *Your Policy name* > Wireless Settings > *Your SSID name* > Optional settings"



Then, go to "Client Related Network Settings".



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

*Auto disconnection after a maximum period of inactivity = **Inactive client ageout** + **Roaming cache update interval** * **Roaming cache ageout***

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

Roaming cache update interval: *By default, an Aerohive AP sends updates to its neighbors about the clients currently associated with it every 60 seconds. The neighboring APs use this information to update their roaming caches—if necessary—with the most up-to-date client information from their neighboring APs.*

Roaming cache ageout: By default, an Aerohive device removes an entry from its roaming cache if it is absent from 60 consecutive updates from a neighbor. You can change how many times an entry must be absent from a neighbor's updates before removing it from the roaming cache from just once to 1000 consecutive times.

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 Aerohive 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.***

Figure 3 : Adding an incoming zone

5.2.2 Captive portal

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

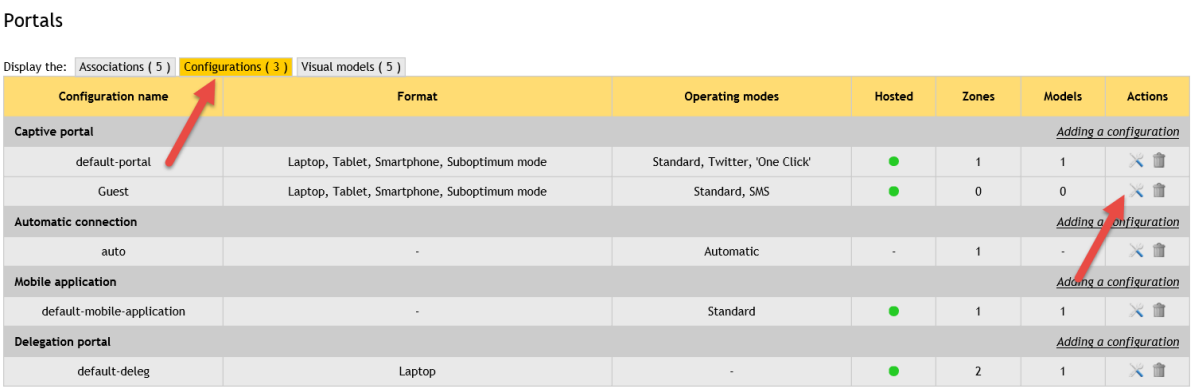


Figure 4 : Configuring a captive portal

For example, a portal with self-registering by SMS

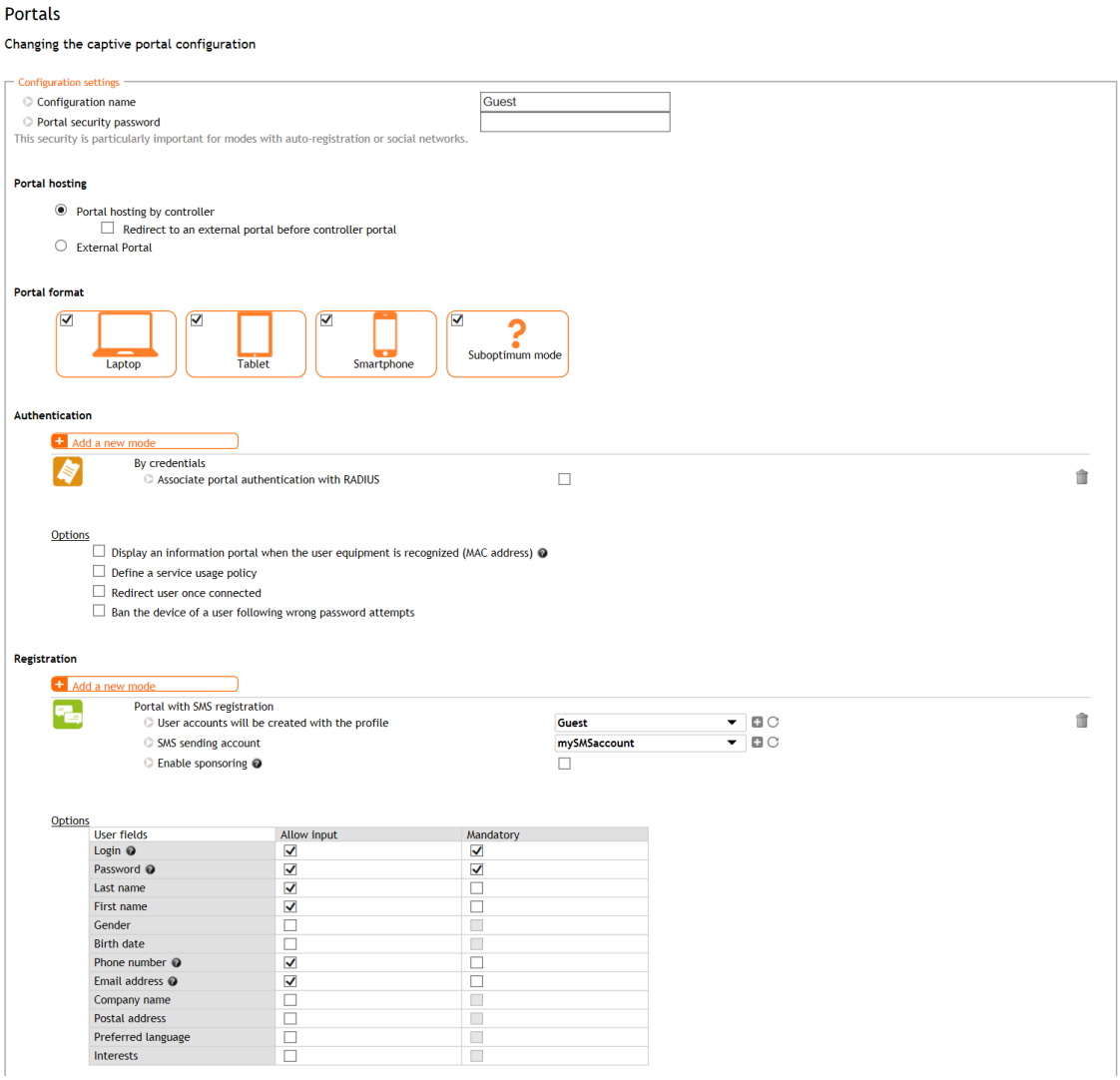


Figure 5 : Example of portal configuration with self-registering by SMS

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

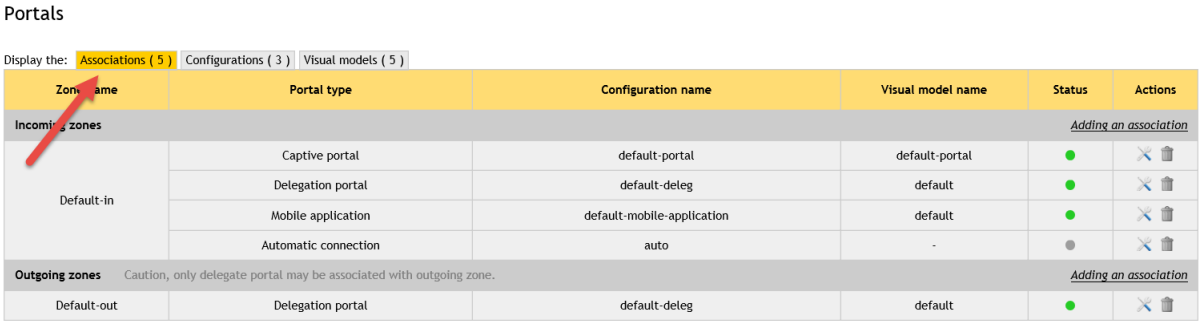


Figure 6 : Association between portal and zone

5.2.3 RADIUS authentication

The Aerohive 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 Aerohive AP must be defined as a NAS for the central controller.

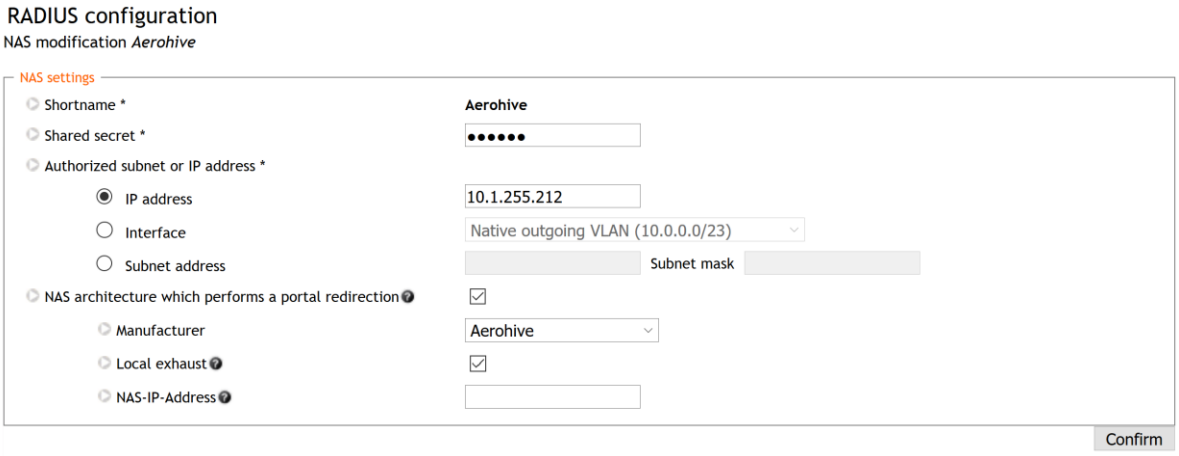


Figure 7 : Adding a NAS

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

- Define the name of the NAS.
- Define the shared secret. This same shared secret will be defined on the Aerohive AP as well.
- Define the IP addressing containing the Aerohive 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 “Aerohive” as Manufacturer

- Tick the box “Local exhaust” for local Internet breakout architecture.

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

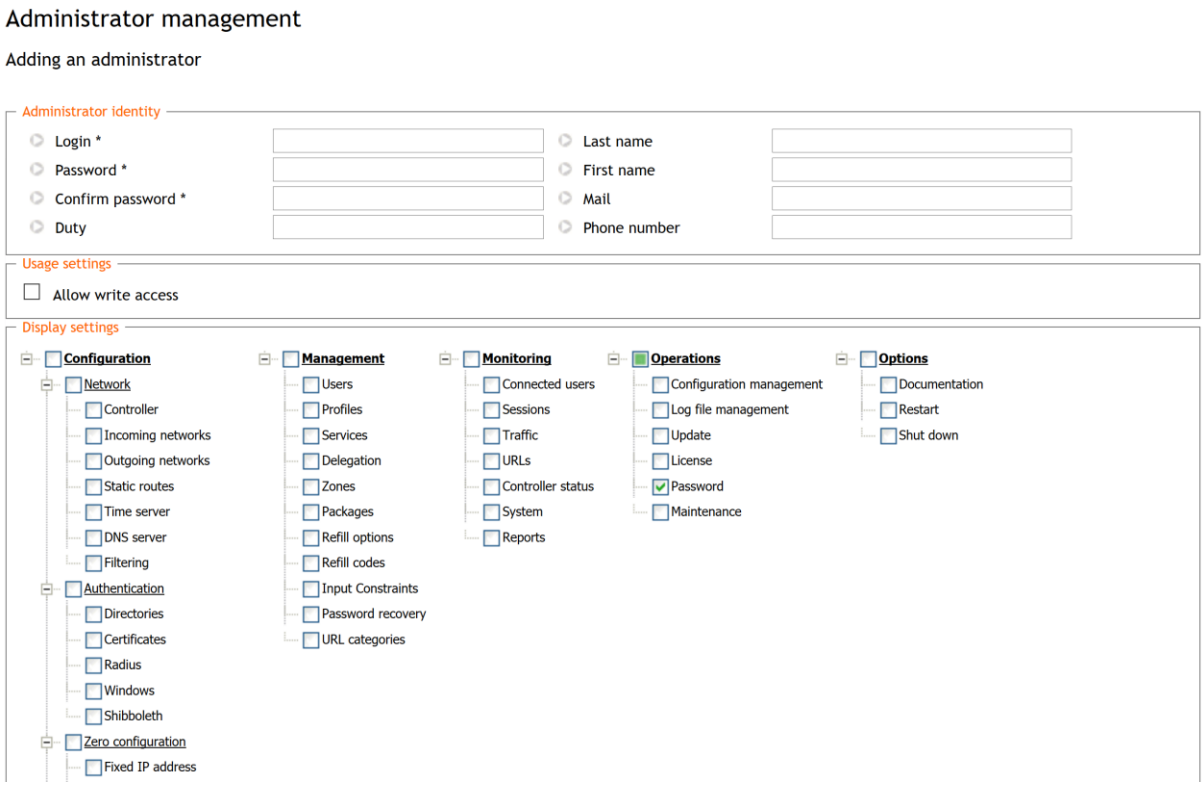


Figure 8 : Adding an administrator account

5.2.6 Access to the syslog service

In order to allow the Aerohive 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:

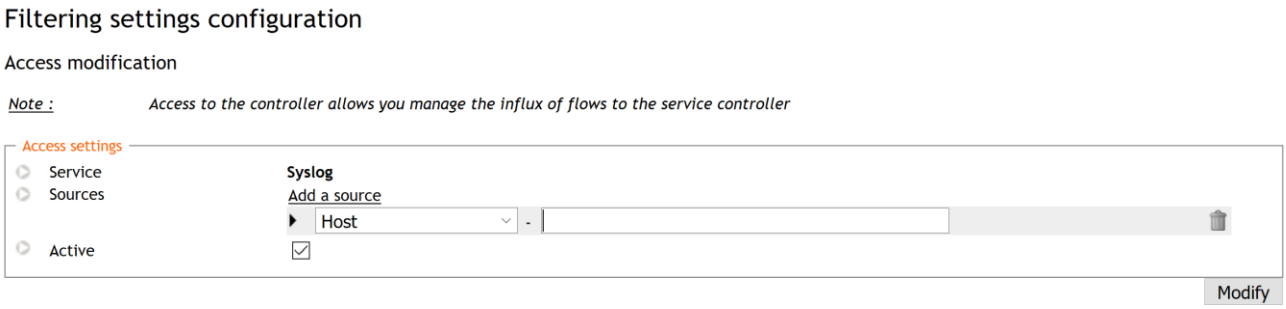


Figure 9 : Adding an access to the syslog service from Aerohive AP

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”. 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
- wants to use social networks on his splash page

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.***

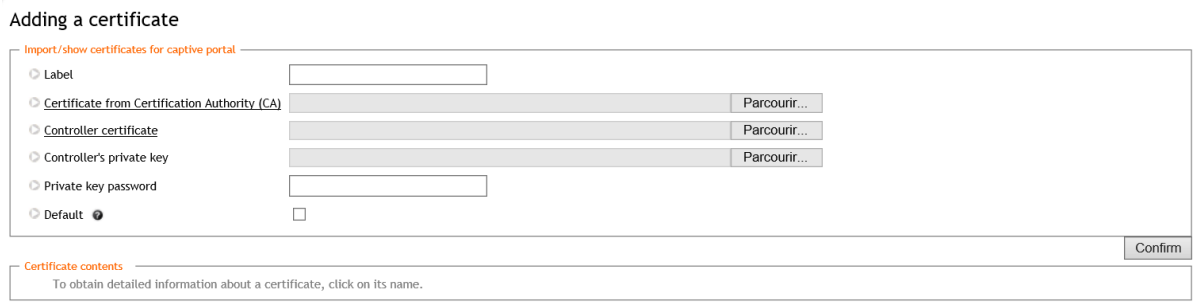


Figure 10 : Adding a new certificate for the captive portal

- 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.***

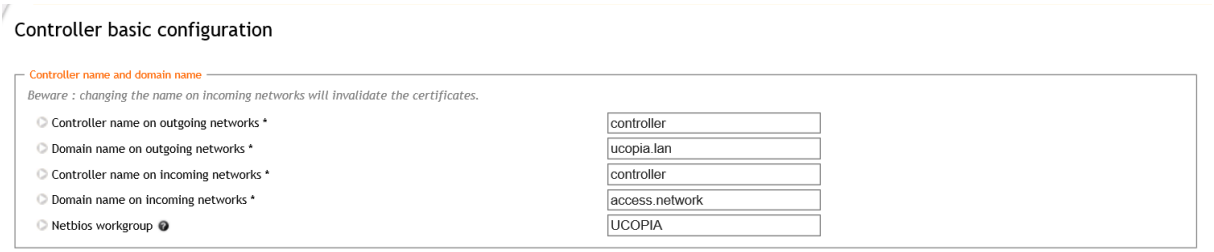


Figure 11 : Modifying a controller name

5.3 Aerohive AP configuration

Connect on your HiveManager.

5.3.1 Creation of a network policy and its associated SSID

Go to “Configure > Network Policies” and then press “ADD NETWORK POLICY“.

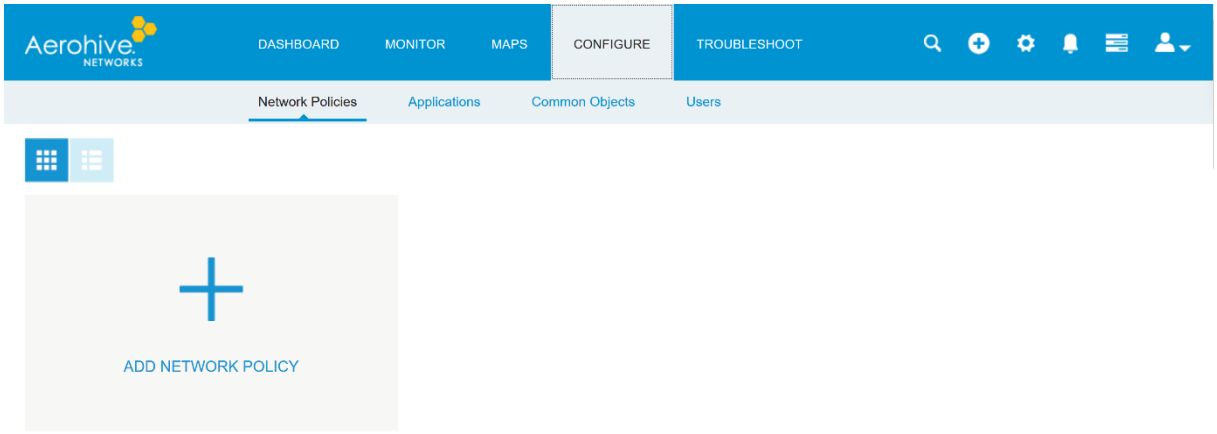


Figure 12 : Creation of a network policy

Name it

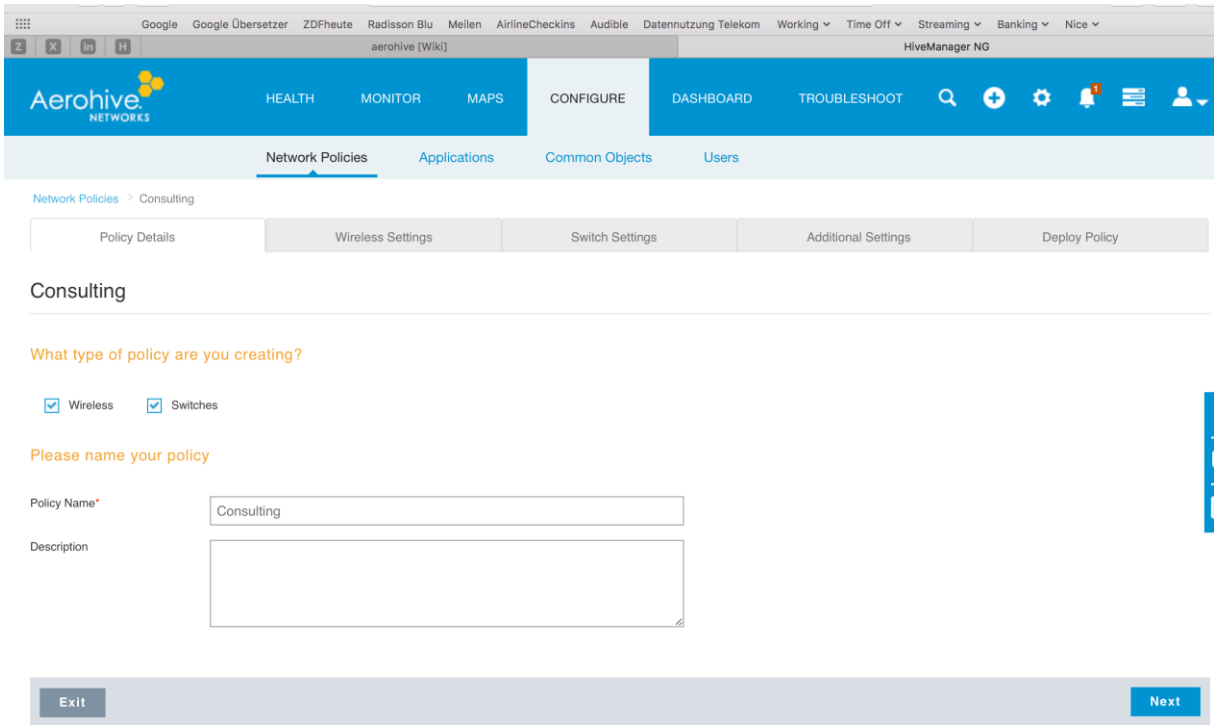


Figure 13 : Naming of your network policy

Add your SSID, in the menu “Wireless Settings > Add > All other SSID”

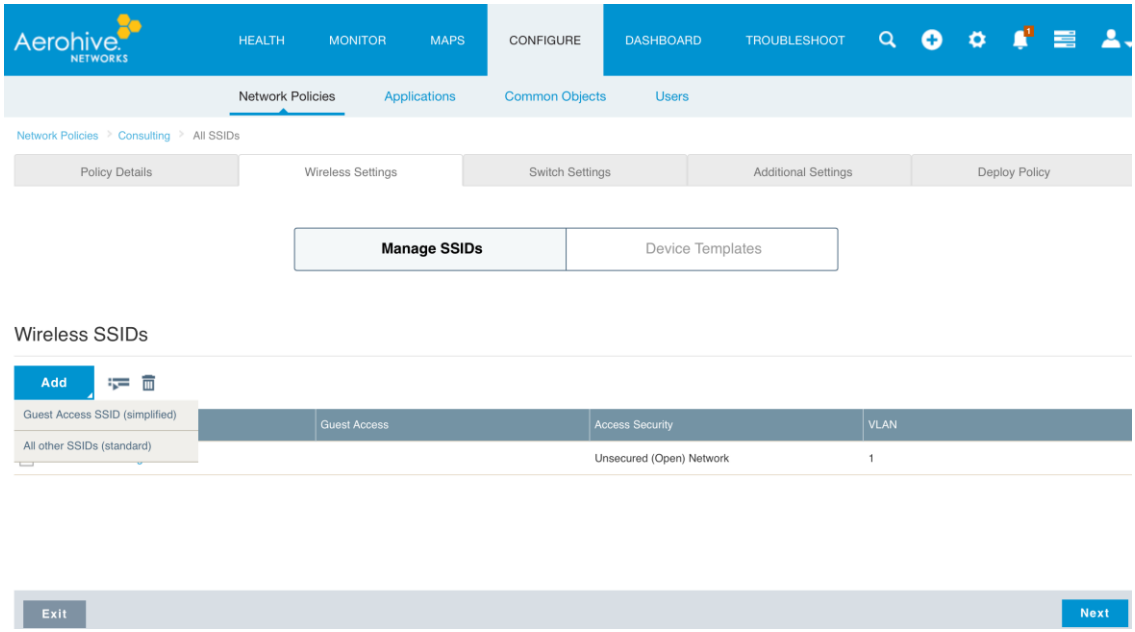


Figure 14 : Creation of a new SSID

5.3.2 Redirection to a captive portal

Configure this new SSID as following:

- Enable the Captive Web Portal
- Select User Auth on Captive Web Portal
- Choose the redirection to an External URL

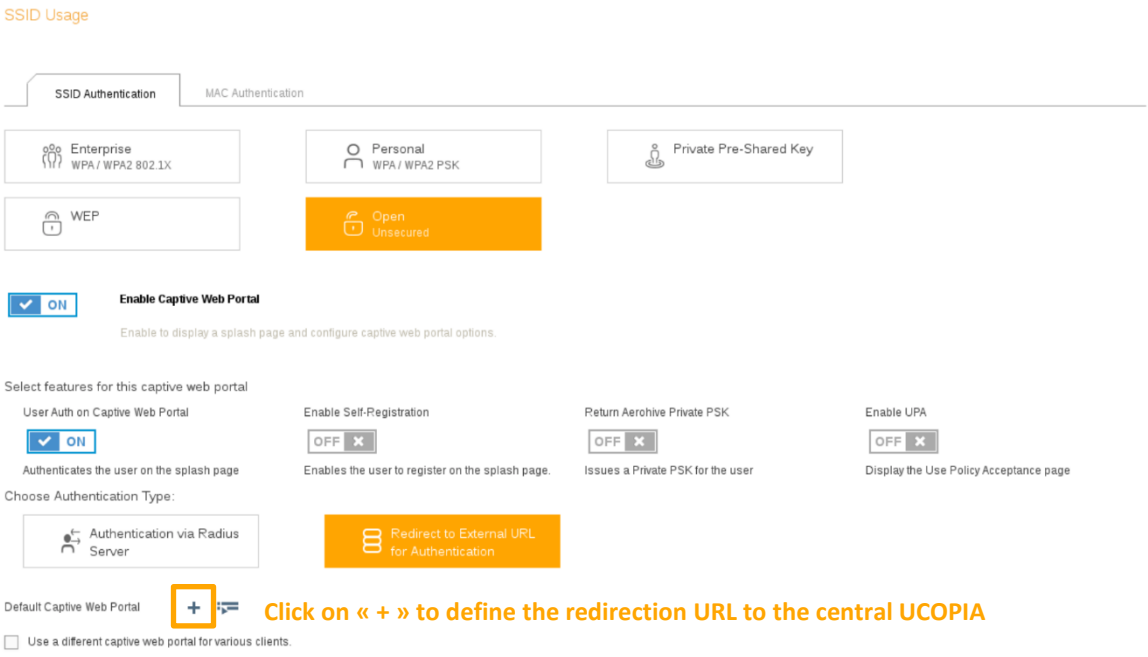


Figure 15 : Configuration of the new SSID > Authentication

Define your default captive portal:

- Login URL = https://<central controller FQDN>/zone/<zone label>
- Success page = https://<central controller FQDN>/zone/<zone label>
- Failure page = https://<central controller FQDN>/zone/<zone label>

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)

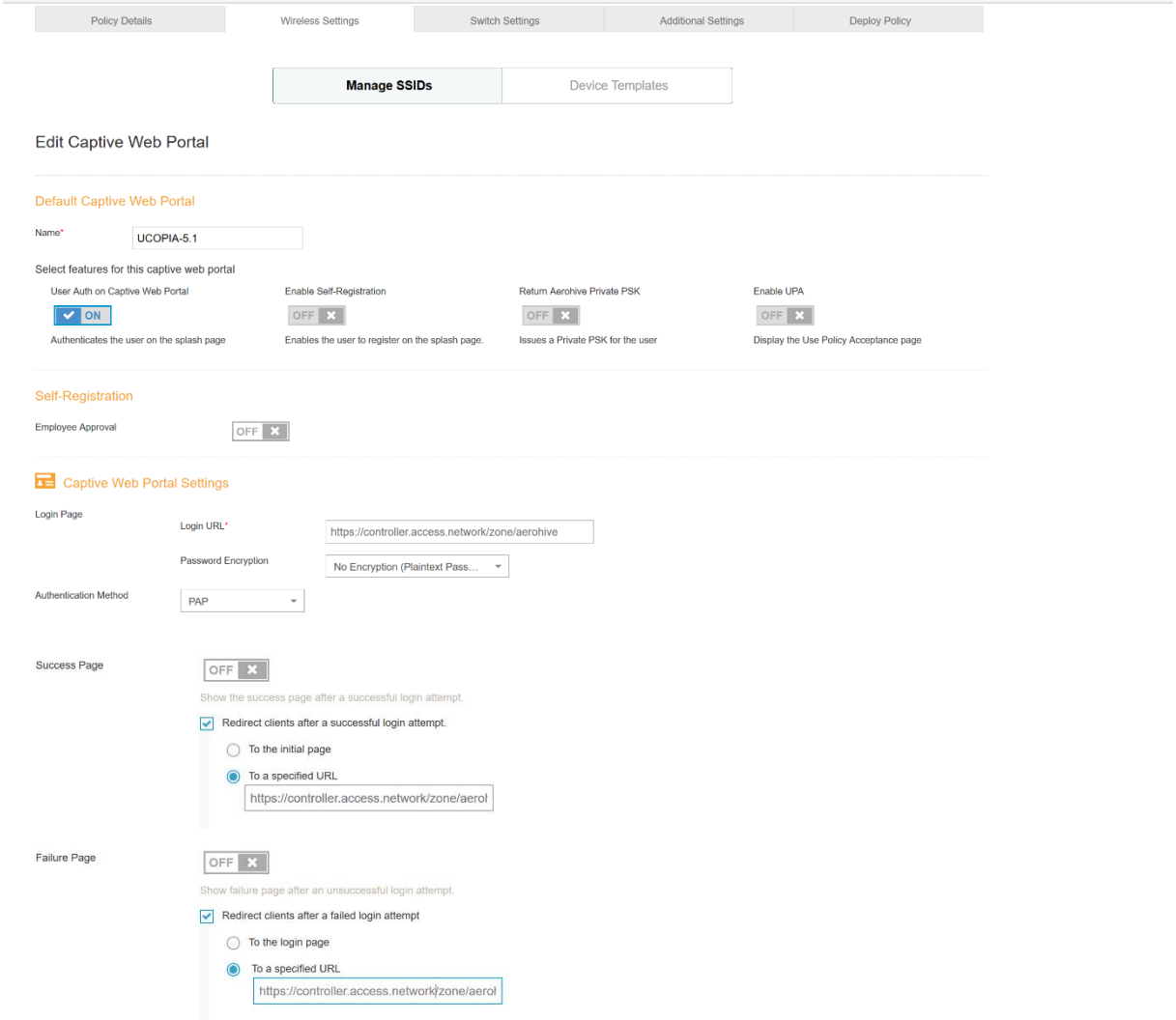


Figure 16 : Configuration of the Captive Web Portal Settings

5.3.3 Configuration of the external RADIUS server

Define the RADIUS configuration of your SSID

- Create the RADIUS server of your choice
- Define the ports to be used
- The shared RADIUS secret must be the same as the central controller.

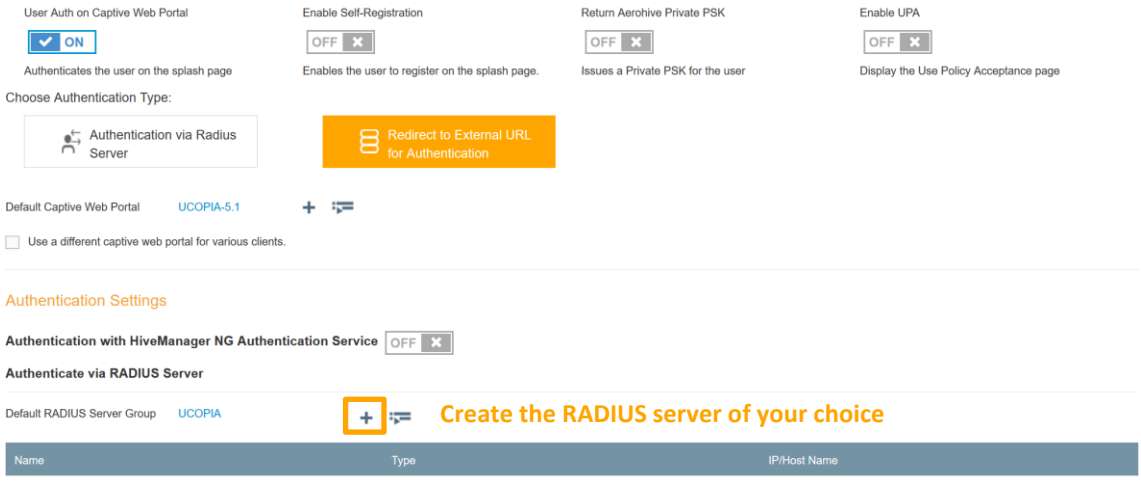


Figure 17 : Creation of a RADIUS server configuration

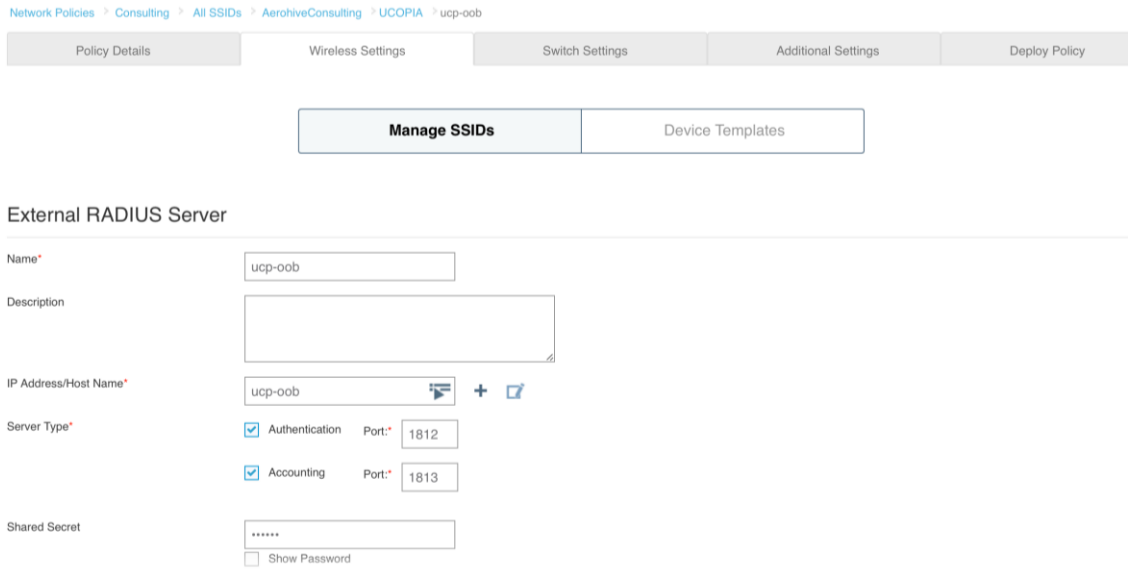


Figure 18 : Configuration of the external RADIUS server

5.3.4 Configuration of a user profile

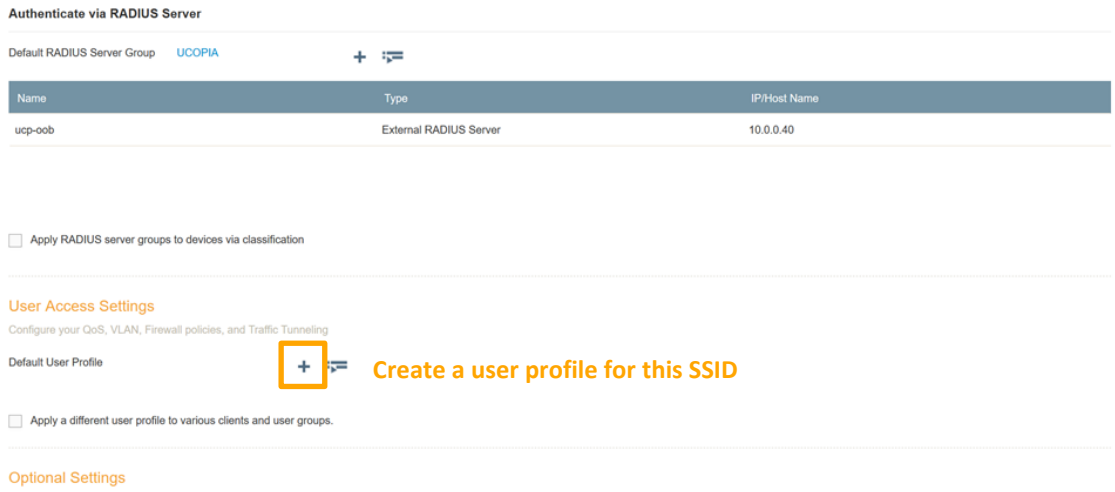


Figure 19 : Creation of the default user profile

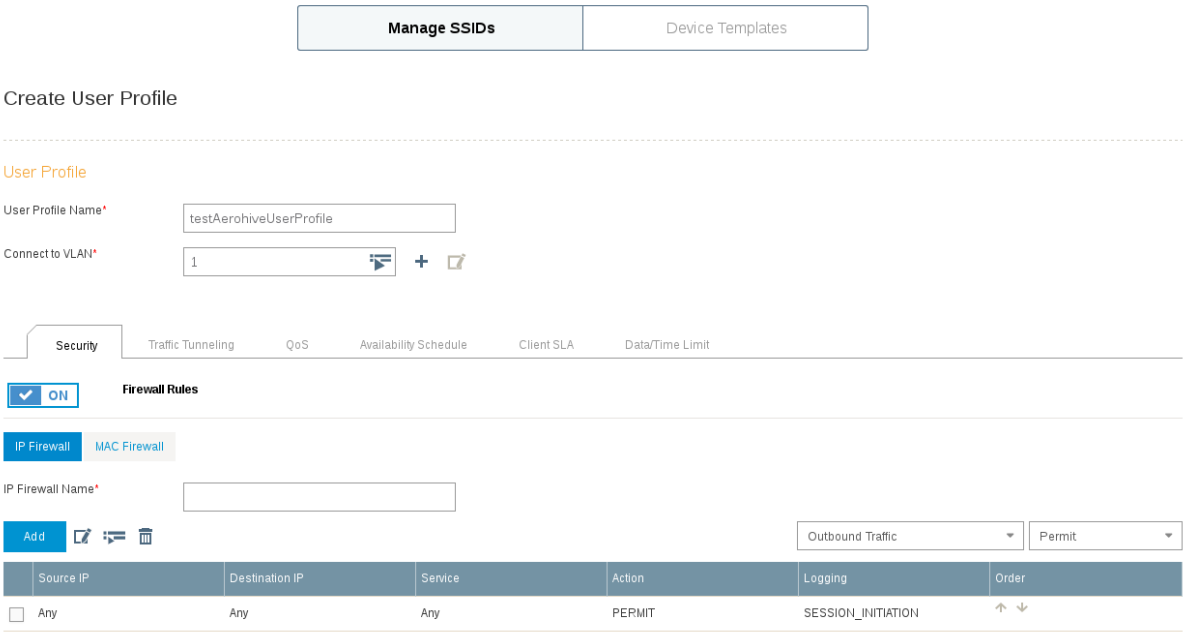


Figure 20 : Configuration of the default user profile

5.3.5 Profile differentiation

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

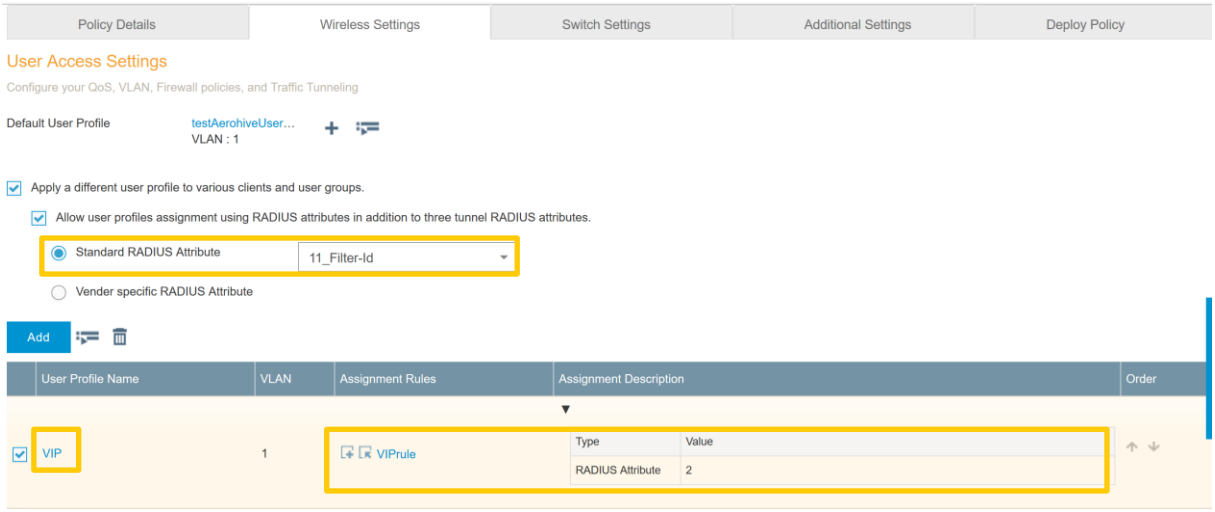


Figure 21 : Dynamic assignment of profile by Aerohive

In this example, when Aerohive 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…

5.3.6 Configuration of the syslog server

Define the syslog configuration

- Define the external syslog server with IP address = OUT IP@ of the central UCOPIA controller
- Let the default syslog facility (local 6 and local 7)
- Choose the severity = INFO

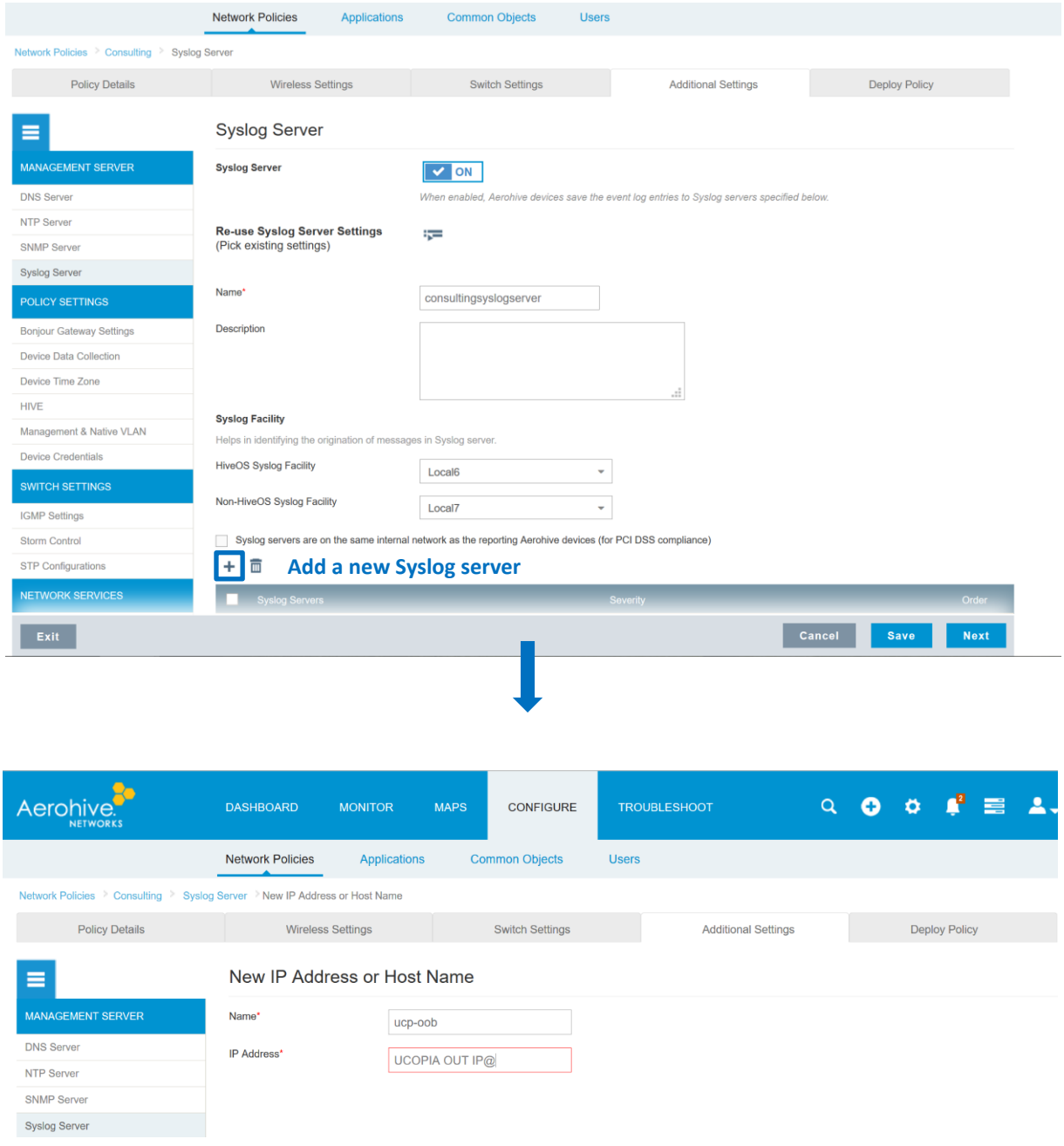


Figure 22 : Creation of the syslog server

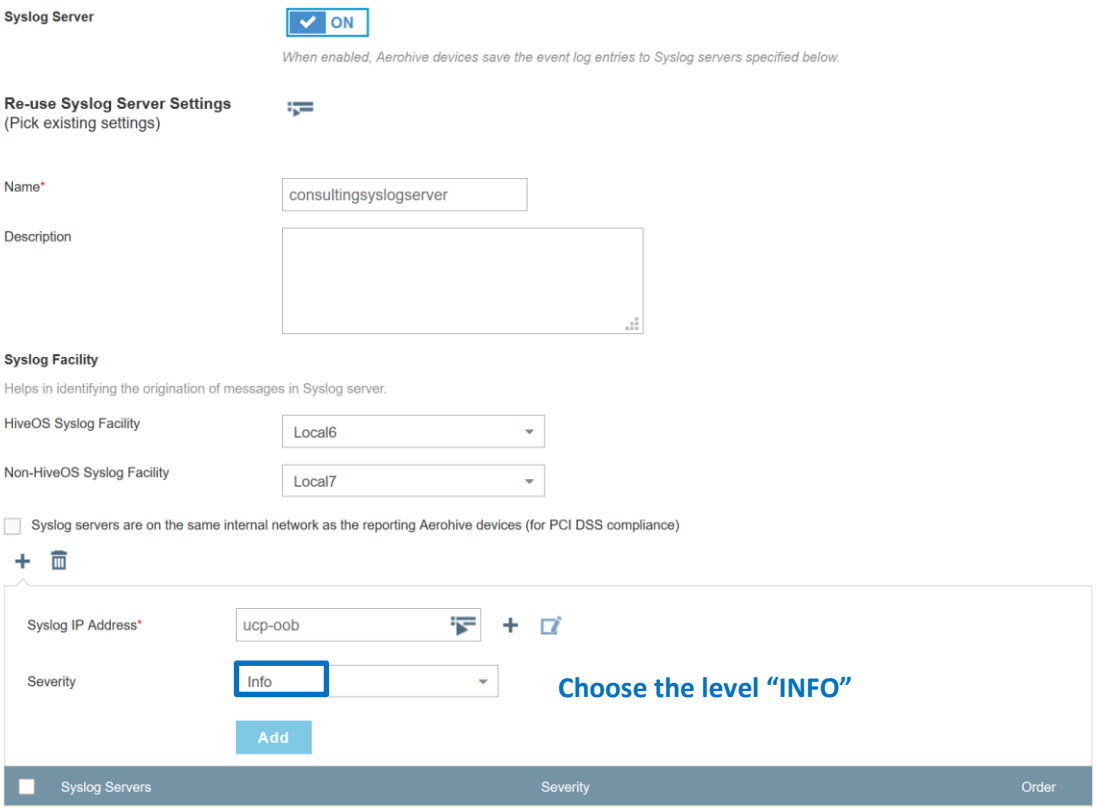


Figure 23 : Association of the created syslog server in the network policy

5.3.7 Deployment of the network policy

Finally, deploy the configured network policy on the AP of your choice.

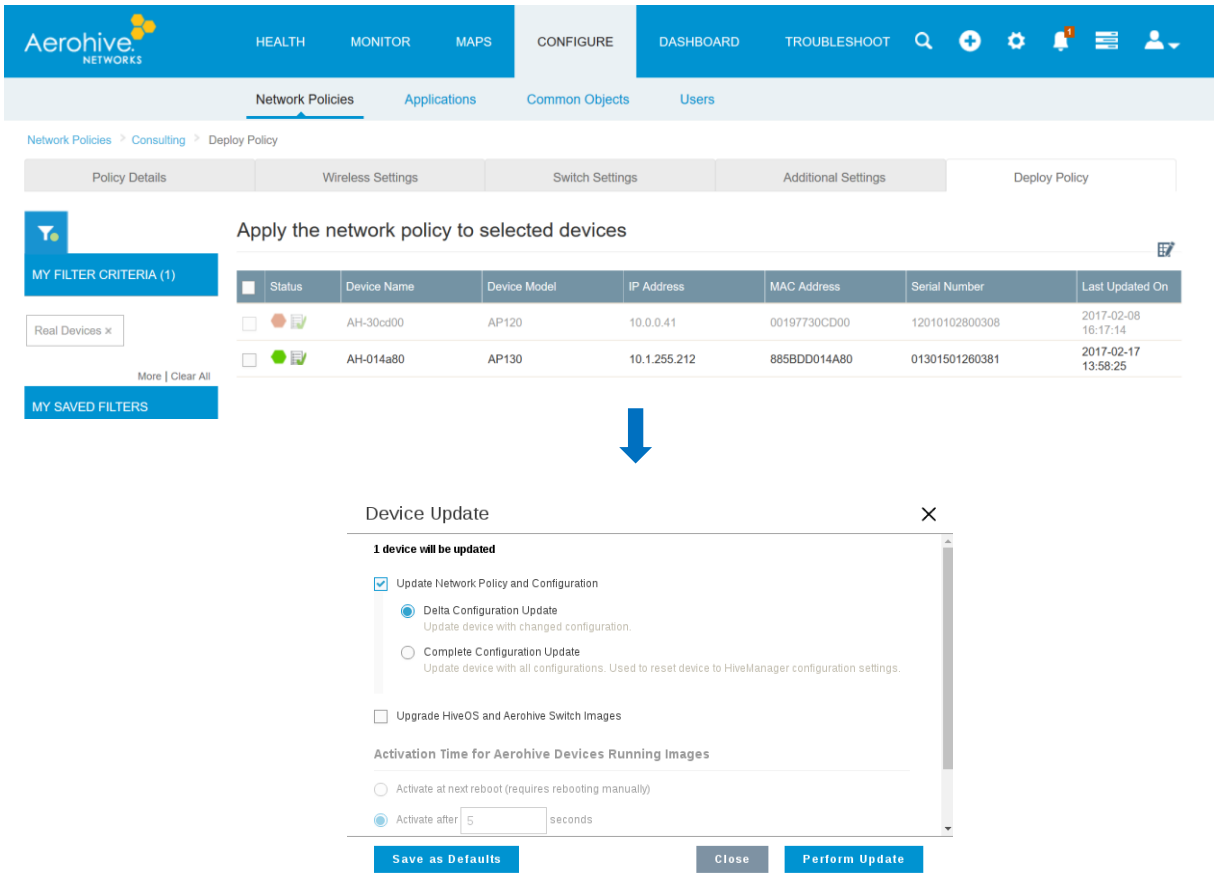


Figure 24 : Deployment of the network policy

6 Annex 1: detailed flow diagram

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

6.1 Portal authentication

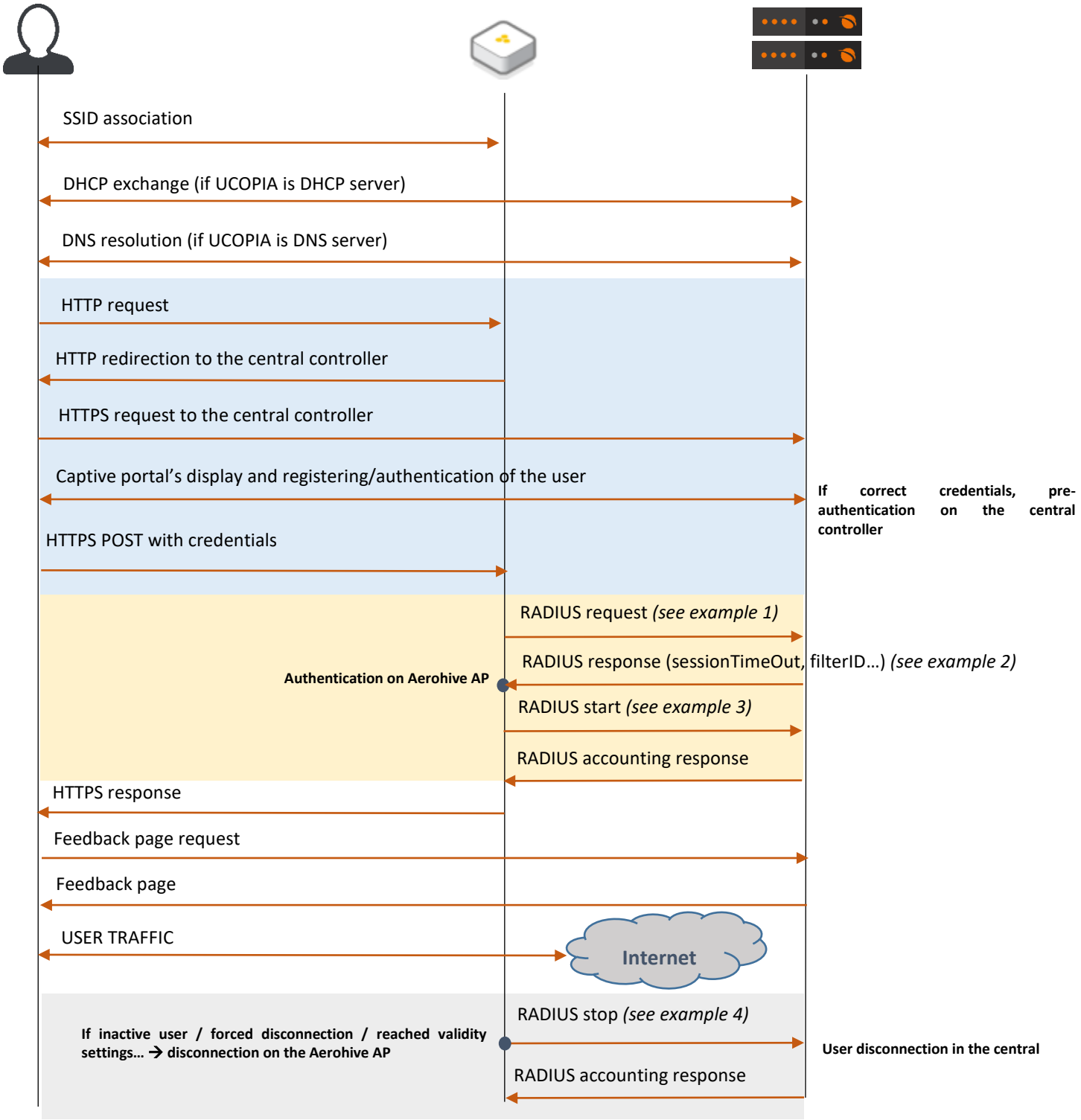


Figure 25 : Detailed flow diagram

Example 1: RADIUS Access-Request

```
Wed Apr  5 17:23:49 2017
        Packet-Type = Access-Request
        Service-Type = Login-User
        NAS-Port-Type = Wireless-802.11
        Framed-IP-Address = 10.1.255.11
        User-Name = "lolo2"
        Calling-Station-Id = "C0-F2-FB-C4-65-18"
        Called-Station-Id = "88-5B-DD-01-4A-94:AerohiveConsulting"
        Vendor-26928-Attr-212 = 0x38382d35422d44442d30312d34412d383000
        NAS-Port = 0
        NAS-IP-Address = 10.1.255.212
        NAS-Identifier = "AH-014a80"
```

Example 2: RADIUS Access-Accept

```
Wed Apr  5 17:23:49 2017
        Packet-Type = Access-Accept
        Ucopia-Ldap-Id = "1"
        Ucopia-startdate = "1491405798"
        Ucopia-validitytype = "inherited"
        Ucopia-ProfileId := "3"
        Ruckus-Role := "Guest"
        Filter-Id := "Guest"
        Ucopia-Group := "Guest"
        User-Name := "lolo2"
        Session-Timeout = 60
        Tunnel-Type:0 = VLAN
        Tunnel-Medium-Type:0 = IEEE-802
        Tunnel-Private-Group-Id:0 = "-1"
```

Example 3: RADIUS Accounting Start

```
Wed Apr  5 17:23:50 2017
        Acct-Session-Id = "0AF779BB-00000000"
        Acct-Status-Type = Start
        Event-Timestamp = "Apr  5 2017 17:23:50 CEST"
        Acct-Delay-Time = 0
        Acct-Authentic = Local
        User-Name = "lolo2"
        NAS-IP-Address = 10.1.255.212
        NAS-Identifier = "AH-014a80"
        NAS-Port = 0
        Called-Station-Id = "88-5B-DD-01-4A-94:AerohiveConsulting"
        Vendor-26928-Attr-1 = 0x00000001
        Vendor-26928-Attr-6 = 0x00000001
        Framed-IP-Address = 10.1.255.11
        Acct-Multi-Session-Id = "c0f2fbc46518885bdd014a9458e50bee737b8ddc"
        Service-Type = Framed-User
        Calling-Station-Id = "c0:f2:fb:c4:65:18"
        NAS-Port-Type = Wireless-802.11
        Connect-Info = "11ng"
        Acct-Unique-Session-Id = "e6e3f4019a52db4c"
        Stripped-User-Name = "lolo2"
        Realm = "NULL"
        Timestamp = 1491405830
```

Example 4: RADIUS accounting stop

```
Wed Apr  5 17:24:50 2017
        Acct-Session-Id = "0AF779BB-00000000"
        Acct-Status-Type = Stop
        Event-Timestamp = "Apr  5 2017 17:24:50 CEST"
        Acct-Delay-Time = 0
        Acct-Authentic = Local
        User-Name = "lolo2"
        NAS-IP-Address = 10.1.255.212
        NAS-Identifier = "AH-014a80"
        NAS-Port = 0
        Called-Station-Id = "88-5B-DD-01-4A-94:AerohiveConsulting"
        Vendor-26928-Attr-1 = 0x00000001
        Vendor-26928-Attr-6 = 0x00000001
        Framed-IP-Address = 10.1.255.11
        Acct-Multi-Session-Id = "c0f2fbc46518885bdd014a9458e50bee737b8ddc"
        Service-Type = Framed-User
        Calling-Station-Id = "c0:f2:fb:c4:65:18"
        NAS-Port-Type = Wireless-802.11
        Connect-Info = "11ng"
        Acct-Session-Time = 60
        Acct-Input-Packets = 427
        Acct-Input-Octets = 50376
        Acct-Input-Gigawords = 0
        Acct-Output-Octets = 550525
        Acct-Output-Gigawords = 0
        Acct-Output-Packets = 459
        Acct-Terminate-Cause = User-Request
        Acct-Unique-Session-Id = "e6e3f4019a52db4c"
        Stripped-User-Name = "lolo2"
        Realm = "NULL"
        Timestamp = 1491405890
```

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
	Aerohive AP-star-shv-01-cdg2.facebook.com
	xx-fbcdn-shv-01-cdg2.fbcdn.net
Google	http://clients1.google.com
	accounts.google.com
	accounts.google.fr
	accounts.youtube.com
	ssl.gstatic.com
	fonts.googleapis.com
	themes.googleusercontent.com
	sb-ssl.google.com
LinkedIn	api.linkedin.com
	static.licdn.com
	www.linkedin.com
Twitter	api.twitter.com
	abs.twimg.com
	abs-0.twimg.com
	pbs.twimg.com
	api.twitter.com

7.2 OpenID Connect

The following open-access URLs must be opened.

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

8 Annex 3: Summary table on available features

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

Features	OOB Aerohive	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	✓	Aerohive profile management based on RADIUS attributes, the OS type, the location, the MAC address or the schedule. Aerohive 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 Aerohive 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 though it
Data volume quota		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)		The disconnection button is hidden in an OOB Aerohive architecture because the Aerohive 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/autofilllink 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	✓	