



## Out-Of-Band Aerohive architecture

---

Version 5.1



## Table of contents

---

Table of contents.....	2
Table of figures.....	3
1 Introduction .....	4
2 User experience workflow .....	5
3 Advantages and recommendations .....	6
3.1 Advantages .....	6
3.1.1 Centralization of the user directory .....	6
3.1.2 Centralization of captive portals .....	6
3.1.3 Centralization of user profiles .....	6
3.1.4 Centralization of user logs.....	6
3.1.5 Local Internet breakout .....	7
3.2 Restrictions and recommendations.....	7
3.2.1 Supported Aerohive and UCOPIA versions.....	7
3.2.2 Supported authentication / registration modes .....	7
3.2.3 Profile differentiation .....	7
3.2.4 Supported UCOPIA features on user management.....	8
3.2.5 User disconnection .....	9
3.2.6 Network failure.....	10
4 Licensing.....	10
5 UCOPIA configuration .....	10
5.1 Prerequisites .....	10
5.1.1 Time synchronization (on UCOPIA and Aerohive).....	10
5.1.2 Communication between remote sites and central site (on UCOPIA and firewall) .....	10
5.1.3 Auto disconnection settings (on Aerohive) .....	11
5.2 Central controller configuration .....	12
5.2.1 Zone .....	12
5.2.2 Captive portal .....	13
5.2.3 RADIUS authentication .....	14
5.2.4 User profile .....	15
5.2.5 Administrator account.....	15
5.2.6 Access to the syslog service.....	15
5.2.7 [Optional] New domain name and certificate.....	16
5.3 Aerohive AP configuration.....	18
5.3.1 Creation of a network policy and its associated SSID.....	18
5.3.2 Redirection to a captive portal .....	19
5.3.3 Configuration of the external RADIUS server .....	21
5.3.4 Configuration of a user profile .....	22
5.3.5 Configuration of the syslog server.....	23
5.3.6 Deployment of the network policy.....	26
6 Annex 1: detailed flow diagram .....	27
6.1 Portal authentication .....	27
7 Annex 2: Walled garden for social networks .....	30
7.1 Facebook, Twitter, Google, LinkedIn .....	30
7.2 OpenID Connect.....	31

8	Annex 3: Summary table on available features .....	31
---	--	----

## Table of figures

---

Figure 1 : Global Out-of-Band Aerohive architecture .....	4
Figure 2 : User traffic flow .....	5
Figure 3 : Adding an incoming zone .....	12
Figure 4 : Configuring a captive portal .....	13
Figure 5 : Example of portal configuration with self-registering by SMS.....	14
Figure 6 : Association between portal and zone .....	14
Figure 7 : Adding a NAS .....	14
Figure 8 : Adding an administrator account.....	15
Figure 9 : Adding an access to the syslog service from Aerohive AP .....	16
Figure 10 : Creation of a network policy .....	18
Figure 10 : Naming of your network policy .....	18
Figure 11 : Creation of a new SSID .....	19
Figure 12 : Configuration of the new SSID > Authentication .....	19
Figure 13 : Configuration of the Captive Web Portal Settings .....	20
Figure 14 : Creation of a RADIUS server configuration .....	21
Figure 15 : Configuration of the external RADIUS server .....	21
Figure 16 : Creation of the default user profile.....	22
Figure 17 : Configuration of the default user profile .....	22
Figure 18 : Creation of the syslog server.....	24
Figure 19 : Association of the created syslog server in the network policy .....	25
Figure 20 : Deployment of the network policy.....	26

# 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.

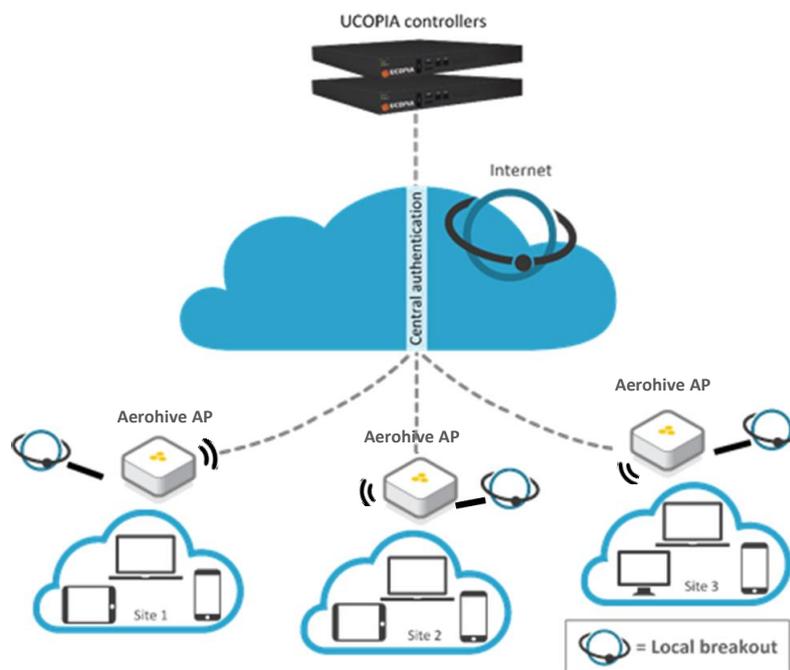


Figure 1 : Global Out-of-Band Aerohive architecture

## 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.

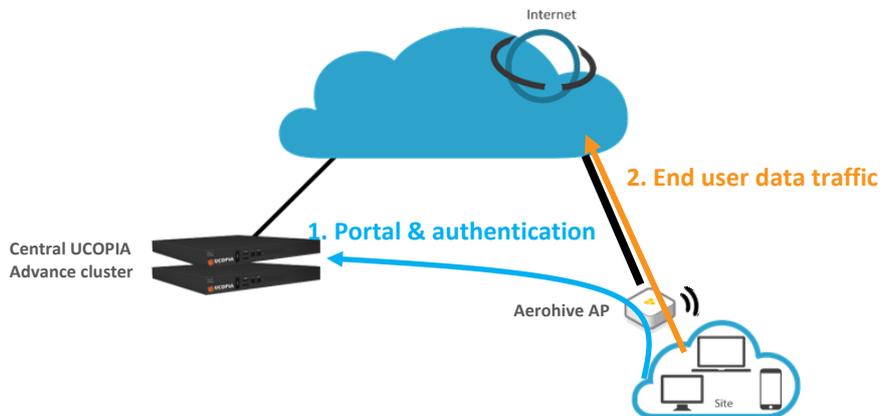


Figure 2 : User traffic flow

## 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  $\geq 6.1r3$  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/autofillink 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/1<sup>st</sup> 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	<p><b>No</b></p> <p><i>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.</i></p>
UCOPIA auto disconnect	<p><b>No</b></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 Aerohive will be able to disconnect a user after a given inactivity period.</i></p>
Manual disconnection	<p><b>No</b></p> <p><i>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.</i></p>
Reached max quota	<p><b>No</b></p> <p><i>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.</i></p>
Expired credit time	<b>Yes</b>
Reached ending validity date	<b>Yes</b>
Forced disconnection	<b>Yes</b>
User deletion from the delegation tool	<b>Yes</b>

### 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”

#### Optional Settings

SSID Availability Schedule  Restrict the availability of this SSID to selected schedules [Customize](#)

Optional Settings Radio and Rates, DoS Prevention, and MAC filters [Customize](#)

Client Monitor  ON

When enabled, Aerohive devices detect client issues, report client connection activities and problems to HiveManager.

Then, go to “Client Related Network Settings”.

Client Related Network Settings

Maximum client limit  Range : 1 - 100

RTS threshold  bytes Range : 1 - 2346

Fragment threshold  bytes Range : 256 - 2346

DTIM settings  Range : 1 - 255

Inactive client ageout  minutes Range : 1 - 30

Roaming cache update interval  seconds Range : 10 - 36000

Roaming cache ageout  Range : 1 - 1000

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**.



The screenshot shows the 'Zone management' interface with the 'Adding a zone' form. The form is titled 'Adding a zone' and is divided into several sections:

- Identification settings:**
  - Zone name \***: A text input field containing 'guest\_siteA'.
  - Zone type:** Radio buttons for 'Incoming' (selected) and 'Outgoing'.
  - Description:** A large text area for entering a description.
- Time zone:**
  - Define a time zone
- License limitation:**
  - Enable license limitation

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

Figure 3 : 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
<b>Captive portal</b> <a href="#">Adding a configuration</a>						
default-portal	Laptop, Tablet, Smartphone, Suboptimum mode	Standard, Twitter, 'One Click'	●	1	1	<a href="#">✕</a> <a href="#">🗑️</a>
Guest	Laptop, Tablet, Smartphone, Suboptimum mode	Standard, SMS	●	0	0	<a href="#">✕</a> <a href="#">🗑️</a>
<b>Automatic connection</b> <a href="#">Adding a configuration</a>						
auto	-	Automatic	-	1	-	<a href="#">✕</a> <a href="#">🗑️</a>
<b>Mobile application</b> <a href="#">Adding a configuration</a>						
default-mobile-application	-	Standard	●	1	1	<a href="#">✕</a> <a href="#">🗑️</a>
<b>Delegation portal</b> <a href="#">Adding a configuration</a>						
default-deleg	Laptop	-	●	2	1	<a href="#">✕</a> <a href="#">🗑️</a>

Figure 4 : 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

Guest   
 mySMSaccount

**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 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.

#### Portals

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

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

**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.

#### RADIUS configuration

NAS modification *Aerohive*

**NAS settings**

Shortname \*

Shared secret \*

Authorized subnet or IP address \*

IP address

Interface

Subnet address

NAS architecture which performs a portal redirection

Manufacturer

Local exhaust

NAS-IP-Address

**Confirm**

**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**.

#### Administrator management

Adding an administrator

**Administrator identity**

<input type="text" value="Login *"/>	<input type="text"/>	<input type="text" value="Last name"/>	<input type="text"/>
<input type="text" value="Password *"/>	<input type="text"/>	<input type="text" value="First name"/>	<input type="text"/>
<input type="text" value="Confirm password *"/>	<input type="text"/>	<input type="text" value="Mail"/>	<input type="text"/>
<input type="text" value="Duty"/>	<input type="text"/>	<input type="text" value="Phone number"/>	<input type="text"/>

**Usage settings**

Allow write access

**Display settings**

<p><input type="checkbox"/> <b>Configuration</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Network           <ul style="list-style-type: none"> <li><input type="checkbox"/> Controller</li> <li><input type="checkbox"/> Incoming networks</li> <li><input type="checkbox"/> Outgoing networks</li> <li><input type="checkbox"/> Static routes</li> <li><input type="checkbox"/> Time server</li> <li><input type="checkbox"/> DNS server</li> <li><input type="checkbox"/> Filtering</li> </ul> </li> <li><input type="checkbox"/> Authentication           <ul style="list-style-type: none"> <li><input type="checkbox"/> Directories</li> <li><input type="checkbox"/> Certificates</li> <li><input type="checkbox"/> Radius</li> <li><input type="checkbox"/> Windows</li> <li><input type="checkbox"/> Shibboleth</li> </ul> </li> <li><input type="checkbox"/> Zero configuration           <ul style="list-style-type: none"> <li><input type="checkbox"/> Fixed IP address</li> </ul> </li> </ul>	<p><input type="checkbox"/> <b>Management</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Users</li> <li><input type="checkbox"/> Profiles</li> <li><input type="checkbox"/> Services</li> <li><input type="checkbox"/> Delegation</li> <li><input type="checkbox"/> Zones</li> <li><input type="checkbox"/> Packages</li> <li><input type="checkbox"/> Refill options</li> <li><input type="checkbox"/> Refill codes</li> <li><input type="checkbox"/> Input Constraints</li> <li><input type="checkbox"/> Password recovery</li> <li><input type="checkbox"/> URL categories</li> </ul>	<p><input type="checkbox"/> <b>Monitoring</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Connected users</li> <li><input type="checkbox"/> Sessions</li> <li><input type="checkbox"/> Traffic</li> <li><input type="checkbox"/> URLs</li> <li><input type="checkbox"/> Controller status</li> <li><input type="checkbox"/> System</li> <li><input type="checkbox"/> Reports</li> </ul>	<p><input checked="" type="checkbox"/> <b>Operations</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Configuration management</li> <li><input type="checkbox"/> Log file management</li> <li><input type="checkbox"/> Update</li> <li><input type="checkbox"/> License</li> <li><input checked="" type="checkbox"/> Password</li> <li><input type="checkbox"/> Maintenance</li> </ul>	<p><input type="checkbox"/> <b>Options</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Documentation</li> <li><input type="checkbox"/> Restart</li> <li><input type="checkbox"/> Shut down</li> </ul>
---	---	---	---	---

**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:

### Filtering settings configuration

Access modification

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



**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

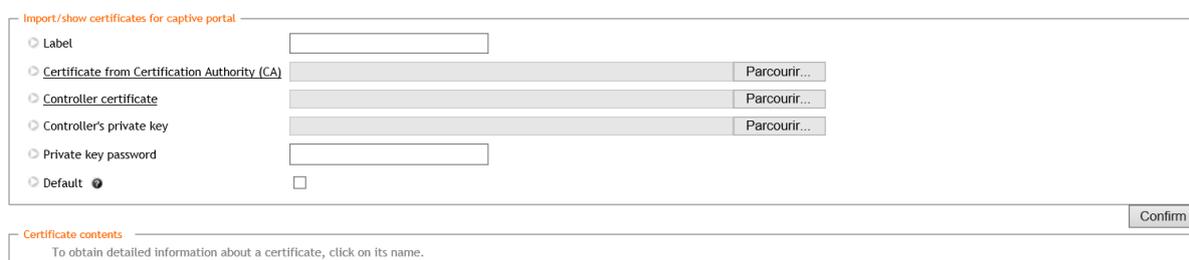
Then, both the FQDN and the certificate must be modified on the central controller, so that the user clicking on the social network button isn't redirected to our UCOPIA public IP address.



*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.**

#### Adding a certificate



**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**.

#### 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 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”.

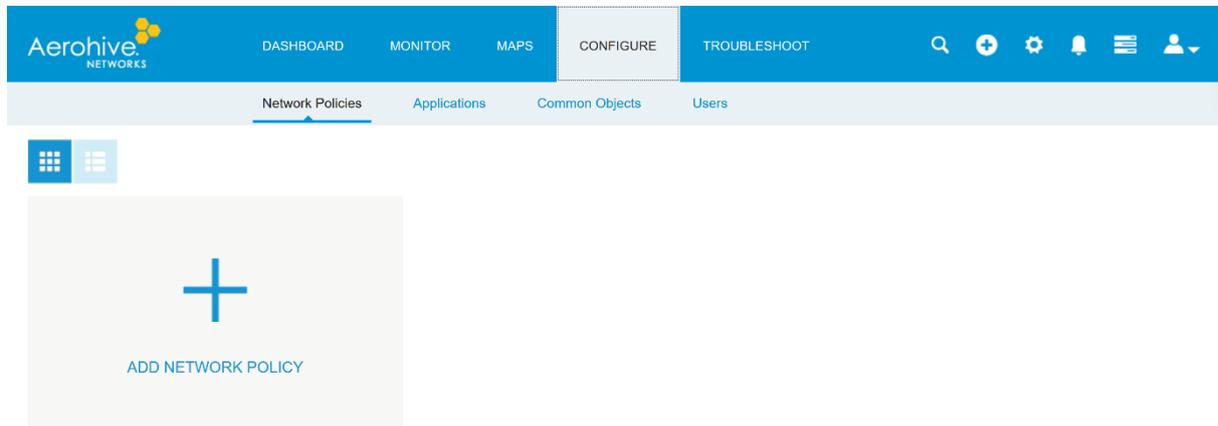


Figure 12 : Creation of a network policy

Name it

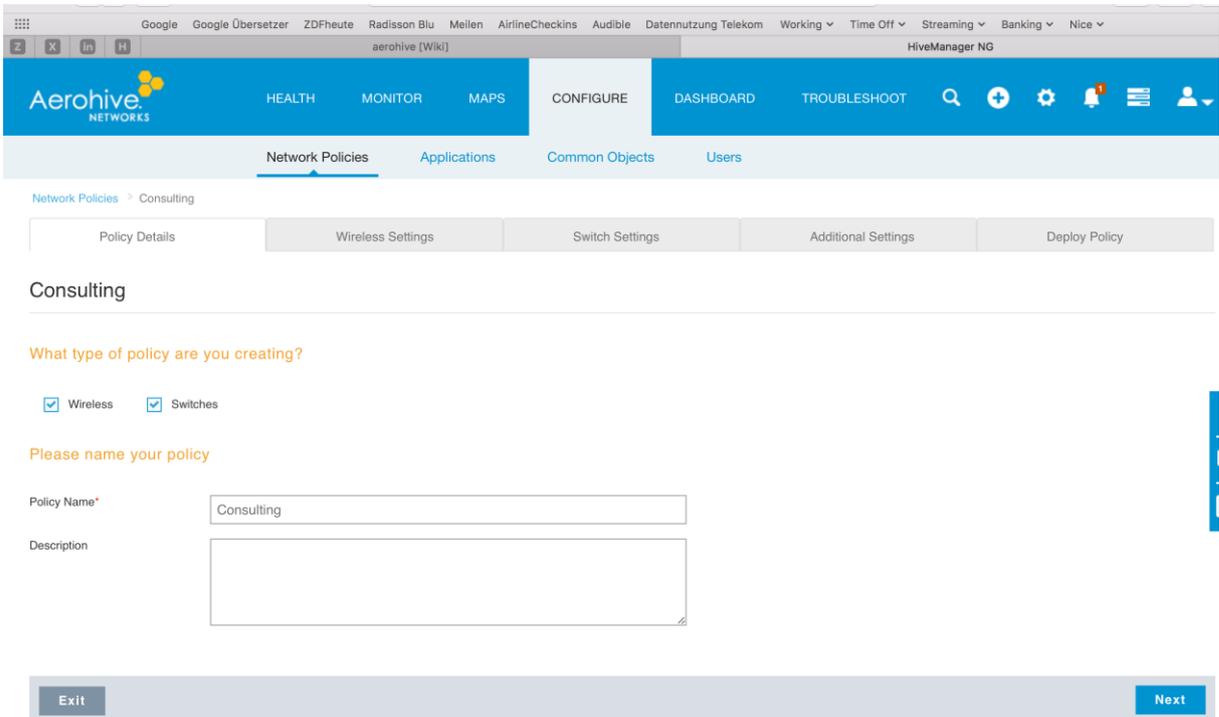
The screenshot shows the 'Consulting' page in the Aerohive Networks interface. The top navigation bar is blue and contains the Aerohive logo, menu items for HEALTH, MONITOR, MAPS, CONFIGURE, DASHBOARD, and TROUBLESHOOT, and utility icons for search, add, settings, notifications, and user profile. Below the navigation bar, there are sub-menu items for Network Policies, Applications, Common Objects, and Users. The main content area shows the 'Consulting' page with a breadcrumb 'Network Policies > Consulting'. Below the breadcrumb, there are tabs for Policy Details, Wireless Settings, Switch Settings, Additional Settings, and Deploy Policy. The 'Policy Details' tab is active. The form asks 'What type of policy are you creating?' with checkboxes for 'Wireless' and 'Switches', both of which are checked. Below this, it asks 'Please name your policy' with a text input field for 'Policy Name\*' containing the text 'Consulting' and a larger text area for 'Description'. At the bottom of the form, there are 'Exit' and 'Next' buttons.

Figure 13 : Naming of your network policy

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

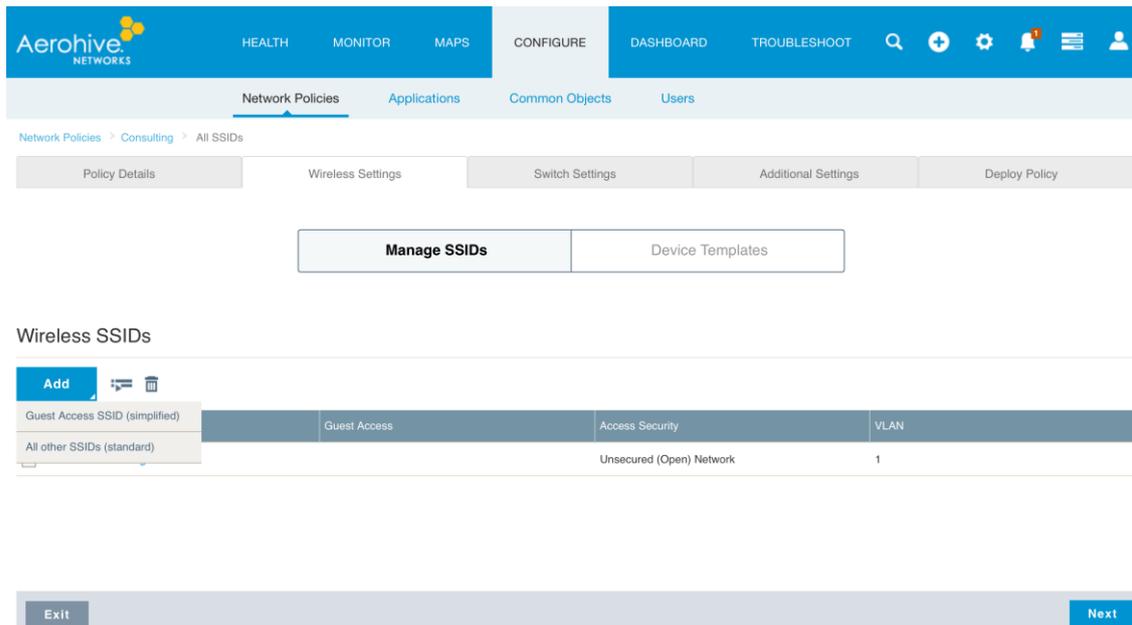


Figure 14 : Creation of a new SSID

### 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

#### SSID Usage

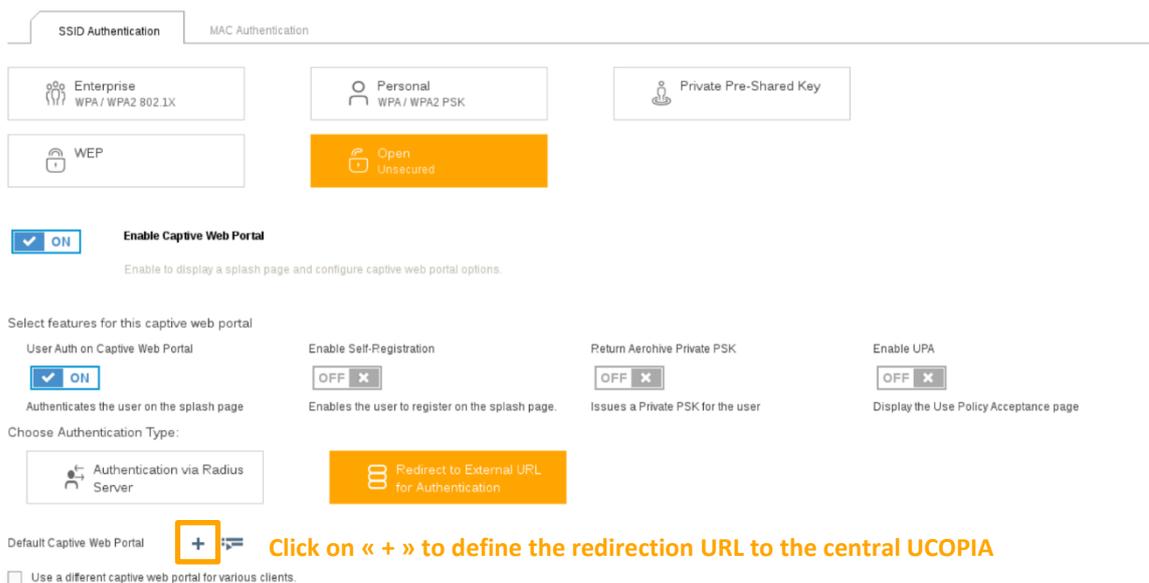


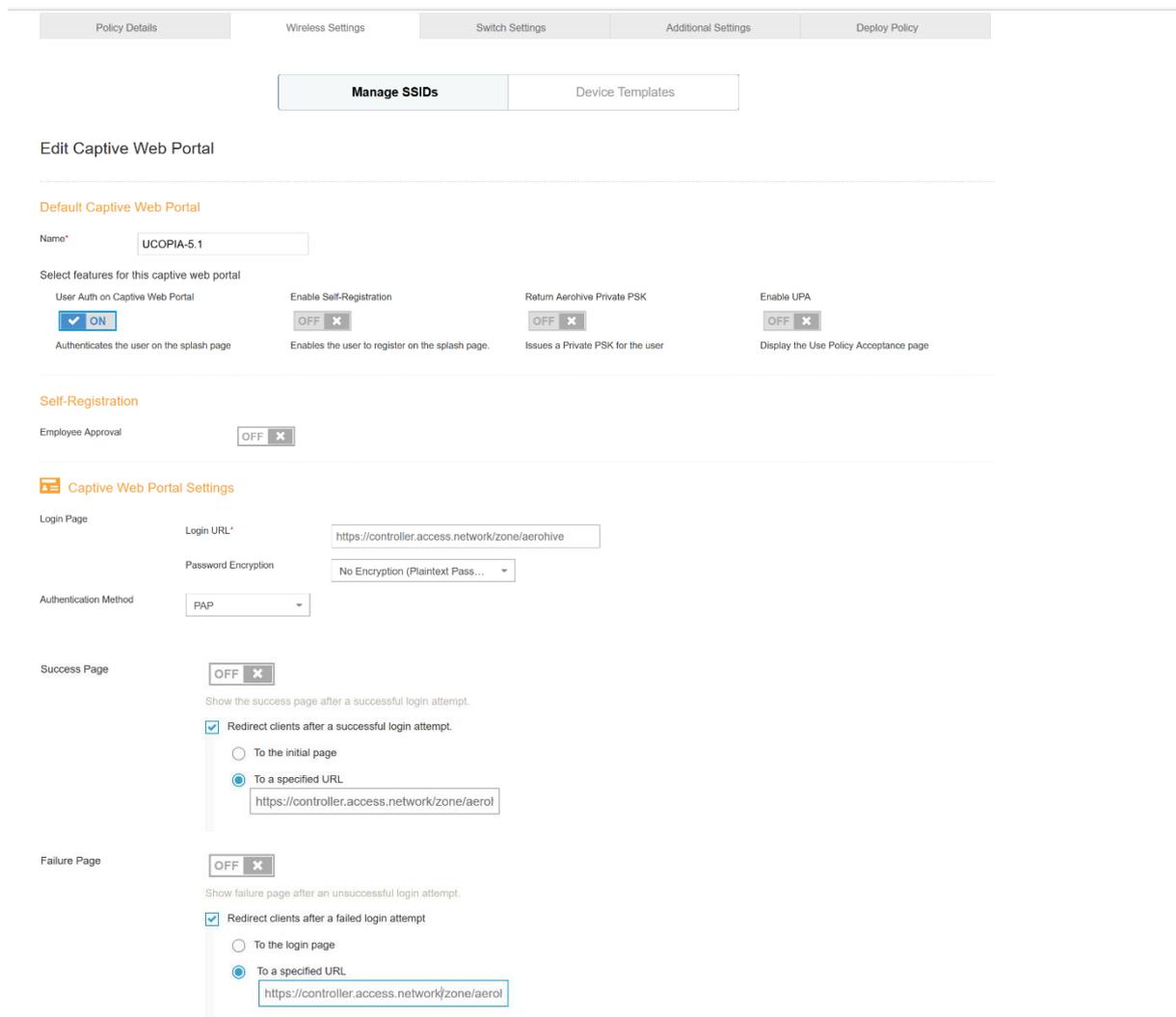
Figure 15 : Configuration of the new SSID > Authentication

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)*



The screenshot shows the configuration page for the Captive Web Portal. The page is divided into several sections:

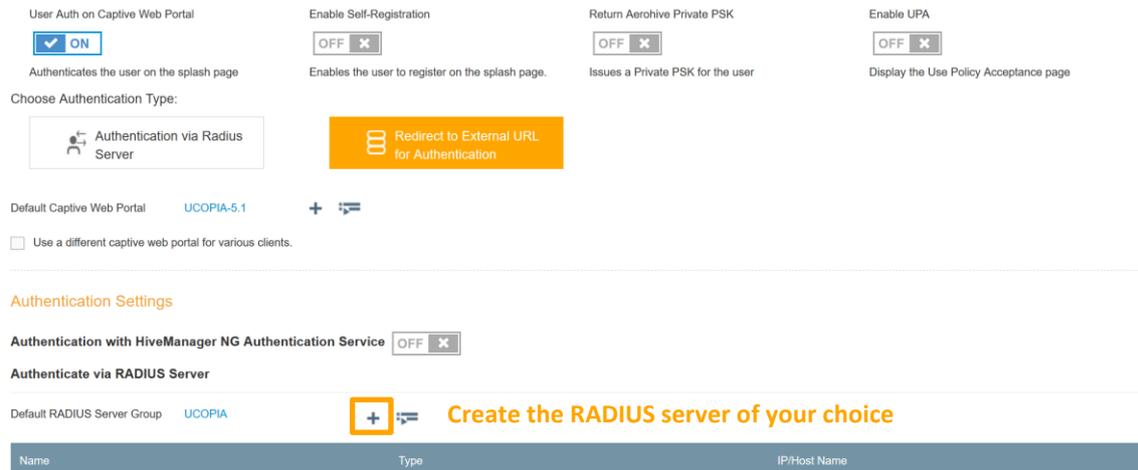
- Policy Details:** Includes tabs for Policy Details, Wireless Settings, Switch Settings, Additional Settings, and Deploy Policy. Below these are buttons for **Manage SSIDs** and **Device Templates**.
- Edit Captive Web Portal:**
  - Default Captive Web Portal:** Name is set to "UCOPIA-5.1".
  - Select features for this captive web portal:**
    - User Auth on Captive Web Portal:** ON (checked)
    - Enable Self-Registration:** OFF
    - Return Aerohive Private PSK:** OFF
    - Enable UPA:** OFF
- Self-Registration:** Employee Approval is OFF.
- Captive Web Portal Settings:**
  - Login Page:** Login URL is `https://controller.access.network/zone/aerohive`. Password Encryption is set to "No Encryption (Plaintext Pass...)". Authentication Method is PAP.
  - Success Page:** OFF. "Redirect clients after a successful login attempt" is checked. The selected option is "To a specified URL" with the URL `https://controller.access.network/zone/aerol`.
  - Failure Page:** OFF. "Redirect clients after a failed login attempt" is checked. The selected option is "To a specified URL" with the URL `https://controller.access.network/zone/aerol`.

**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.



User Auth on Captive Web Portal  ON  
Authenticates the user on the splash page

Enable Self-Registration  OFF  X  
Enables the user to register on the splash page.

Return Aerohive Private PSK  OFF  X  
Issues a Private PSK for the user

Enable UPA  OFF  X  
Display the Use Policy Acceptance page

Choose Authentication Type:

Authentication via Radius Server

Redirect to External URL for Authentication

Default Captive Web Portal [UCOPIA-5.1](#)

Use a different captive web portal for various clients.

---

Authentication Settings

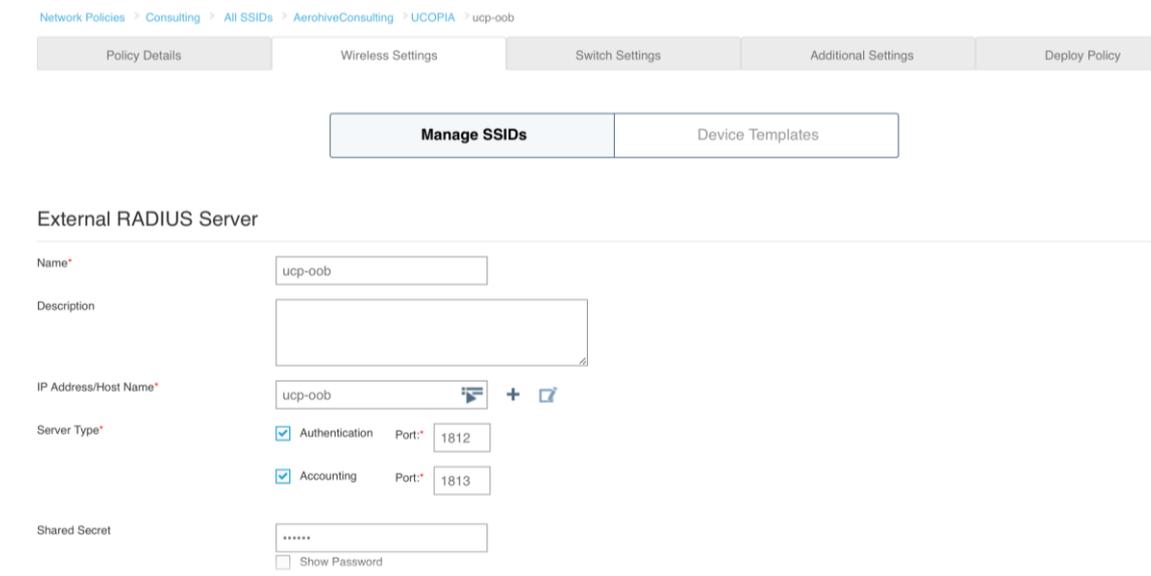
Authentication with HiveManager NG Authentication Service  OFF  X

Authenticate via RADIUS Server

Default RADIUS Server Group [UCOPIA](#)    **Create the RADIUS server of your choice**

Name	Type	IP/Host Name
------	------	--------------

Figure 17 : Creation of a RADIUS server configuration



Network Policies > Consulting > All SSIDs > AerohiveConsulting > UCOPIA > ucp-oob

Policy Details | Wireless Settings | Switch Settings | Additional Settings | Deploy Policy

Manage SSIDs | Device Templates

External RADIUS Server

Name\*

Description

IP Address/Host Name\*

Server Type\*

Authentication Port.\*

Accounting Port.\*

Shared Secret   Show Password

Figure 18 : Configuration of the external RADIUS server

### 5.3.4 Configuration of a user profile

**Authenticate via RADIUS Server**

Default RADIUS Server Group **UCOPIA** +

Name	Type	IP/Host Name
ucp-oob	External RADIUS Server	10.0.0.40

Apply RADIUS server groups to devices via classification

---

**User Access Settings**  
Configure your QoS, VLAN, Firewall policies, and Traffic Tunneling

Default User Profile **Create a user profile for this SSID**

Apply a different user profile to various clients and user groups.

---

**Optional Settings**

Figure 19 : Creation of the default user profile

Manage SSIDs
Device Templates

#### Create User Profile

**User Profile**

User Profile Name\*

Connect to VLAN\*  +

**Security** | Traffic Tunneling | QoS | Availability Schedule | Client SLA | Data/Time Limit

**ON** **Firewall Rules**

**IP Firewall** | MAC Firewall

IP Firewall Name\*

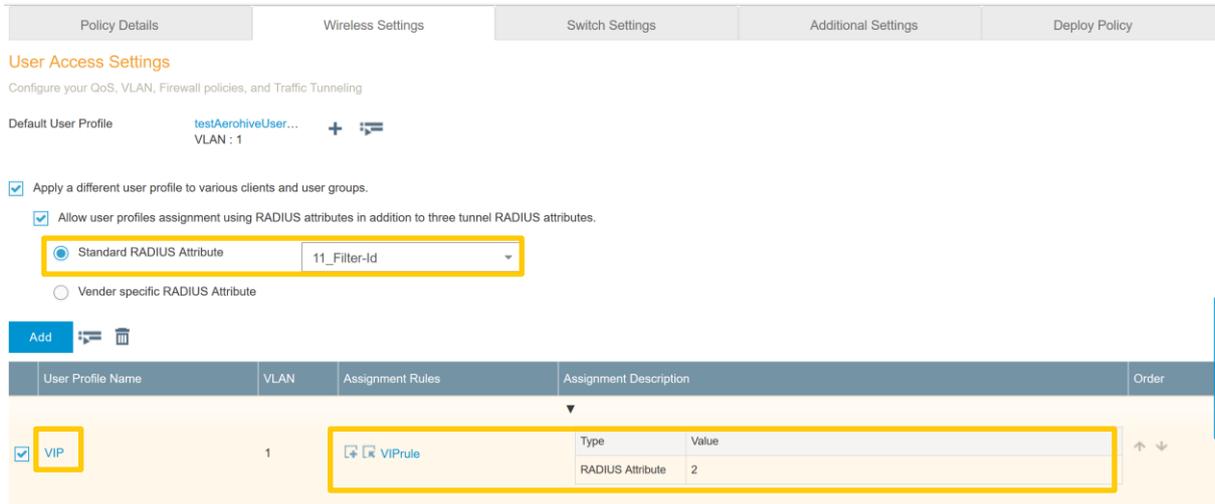
**Add**

Source IP	Destination IP	Service	Action	Logging	Order
<input type="checkbox"/> Any	Any	Any	PERMIT	Outbound Traffic	Permit
				SESSION_INITIATION	↑ ↓

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:



The screenshot shows the configuration interface for User Access Settings. The 'Policy Details' tab is selected. Under 'User Access Settings', the 'Default User Profile' is 'testAerohiveUser...' with 'VLAN : 1'. A checkbox 'Apply a different user profile to various clients and user groups.' is checked. Below it, 'Allow user profiles assignment using RADIUS attributes in addition to three tunnel RADIUS attributes.' is checked. A dropdown menu is set to 'Standard RADIUS Attribute' with '11\_Filter-Id' selected. Below that, 'Vender specific RADIUS Attribute' is unselected. A table below shows a profile named 'VIP' assigned to VLAN 1. The 'Assignment Rules' column for 'VIP' shows a rule named 'VIPRule' with a table of RADIUS attributes: Type 'RADIUS Attribute' and Value '2'.

**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

Network Policies > Consulting > Syslog Server

Policy Details | Wireless Settings | Switch Settings | Additional Settings | Deploy Policy

### Syslog Server

**Syslog Server**  ON  
*When enabled, Aerohive devices save the event log entries to Syslog servers specified below.*

**Re-use Syslog Server Settings**  
(Pick existing settings)

Name\*

Description

**Syslog Facility**  
Helps in identifying the origination of messages in Syslog server.

HiveOS Syslog Facility

Non-HiveOS Syslog Facility

Syslog servers are on the same internal network as the reporting Aerohive devices (for PCI DSS compliance)

**+ Add a new Syslog server**

Syslog Servers	Severity	Order
----------------	----------	-------

Exit | Cancel | Save | Next

Aerohive NETWORKS | DASHBOARD | MONITOR | MAPS | CONFIGURE | TROUBLESHOOT

Network Policies > Consulting > Syslog Server > New IP Address or Host Name

Policy Details | Wireless Settings | Switch Settings | Additional Settings | Deploy Policy

### New IP Address or Host Name

Name\*

IP Address\*

Figure 22 : Creation of the syslog server

**Syslog Server** ON  
*When enabled, Aerohive devices save the event log entries to Syslog servers specified below.*

**Re-use Syslog Server Settings**  
(Pick existing settings)

Name\*   
Description

**Syslog Facility**  
Helps in identifying the origination of messages in Syslog server.

HiveOS Syslog Facility   
Non-HiveOS Syslog Facility

Syslog servers are on the same internal network as the reporting Aerohive devices (for PCI DSS compliance)

+

Syslog IP Address\*  +

Severity  **Choose the level "INFO"**

<input type="checkbox"/>	Syslog Servers	Severity	Order
--------------------------	----------------	----------	-------

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.

The screenshot shows the Aerohive Networks web interface. The top navigation bar includes 'HEALTH', 'MONITOR', 'MAPS', 'CONFIGURE', 'DASHBOARD', and 'TROUBLESHOOT'. The 'CONFIGURE' tab is active, and the 'Network Policies' sub-tab is selected. The breadcrumb trail is 'Network Policies > Consulting > Deploy Policy'. Below this, there are tabs for 'Policy Details', 'Wireless Settings', 'Switch Settings', 'Additional Settings', and 'Deploy Policy'. The main content area is titled 'Apply the network policy to selected devices'. On the left, there are filter sections: 'MY FILTER CRITERIA (1)' with a 'Real Devices x' button, and 'MY SAVED FILTERS'. The main table lists two devices:

Status	Device Name	Device Model	IP Address	MAC Address	Serial Number	Last Updated On
<input type="checkbox"/>	AH-30cd00	AP120	10.0.0.41	00197730CD00	12010102800308	2017-02-08 16:17:14
<input type="checkbox"/>	AH-014a80	AP130	10.1.255.212	885BDD014A80	01301501260381	2017-02-17 13:58:25

A blue arrow points from the table to a 'Device Update' dialog box. The dialog box has a title bar with a close button (X). It contains the following options:

- Update Network Policy and Configuration
  - Delta Configuration Update  
Update device with changed configuration.
  - Complete Configuration Update  
Update device with all configurations. Used to reset device to HiveManager configuration settings.
- Upgrade HiveOS and Aerohive Switch Images

Below these options is the 'Activation Time for Aerohive Devices Running Images' section:

- Activate at next reboot (requires rebooting manually)
- Activate after  seconds

At the bottom of the dialog box are three buttons: 'Save as Defaults', 'Close', and 'Perform Update'.

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

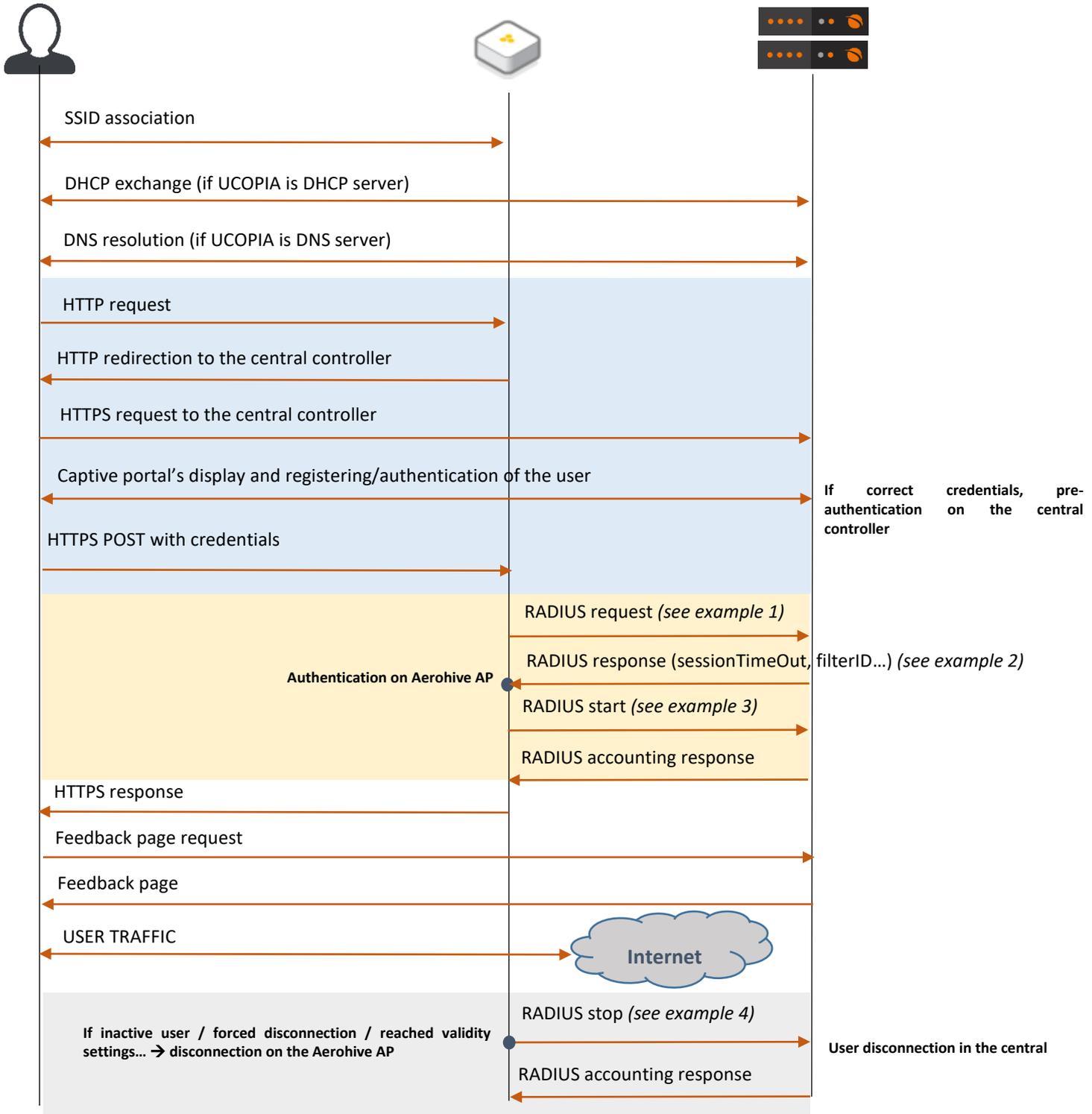


Figure 25 : Detailed flow diagram

**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	<a href="http://www.facebook.com">www.facebook.com</a>
	<a href="http://fbstatic-a.akamaihd.net">fbstatic-a.akamaihd.net</a>
	<a href="http://graph.facebook.com">graph.facebook.com</a>
	<a href="http://fbcdn-profile-a.akamaihd.net">fbcdn-profile-a.akamaihd.net</a>
	<a href="http://m.facebook.com">m.facebook.com</a>
	<a href="http://fbcdn-photos-a-a.akamaihd.net">fbcdn-photos-a-a.akamaihd.net</a>
	<a href="http://fbcdn-photos-b-a.akamaihd.net">fbcdn-photos-b-a.akamaihd.net</a>
	<a href="http://fbcdn-photos-c-a.akamaihd.net">fbcdn-photos-c-a.akamaihd.net</a>
	<a href="http://fbcdn-photos-d-a.akamaihd.net">fbcdn-photos-d-a.akamaihd.net</a>
	<a href="http://fbcdn-photos-e-a.akamaihd.net">fbcdn-photos-e-a.akamaihd.net</a>
	<a href="http://fbcdn-photos-f-a.akamaihd.net">fbcdn-photos-f-a.akamaihd.net</a>
	<a href="http://fbcdn-photos-g-a.akamaihd.net">fbcdn-photos-g-a.akamaihd.net</a>
	<a href="http://fbcdn-photos-h-a.akamaihd.net">fbcdn-photos-h-a.akamaihd.net</a>
	<a href="http://static.xx.fbcdn.net">static.xx.fbcdn.net</a>
	<a href="http://Aerohive AP-star-shv-01-cdg2.facebook.com">Aerohive AP-star-shv-01-cdg2.facebook.com</a>
<a href="http://xx-fbcdn-shv-01-cdg2.fbcdn.net">xx-fbcdn-shv-01-cdg2.fbcdn.net</a>	
Google	<a href="http://clients1.google.com">http://clients1.google.com</a>
	<a href="http://accounts.google.com">accounts.google.com</a>
	<a href="http://accounts.google.fr">accounts.google.fr</a>
	<a href="http://accounts.youtube.com">accounts.youtube.com</a>
	<a href="http://ssl.gstatic.com">ssl.gstatic.com</a>
	<a href="http://fonts.googleapis.com">fonts.googleapis.com</a>
	<a href="http://themes.googleusercontent.com">themes.googleusercontent.com</a>
	<a href="http://sb-ssl.google.com">sb-ssl.google.com</a>
LinkedIn	<a href="http://api.linkedin.com">api.linkedin.com</a>
	<a href="http://static.licdn.com">static.licdn.com</a>
	<a href="http://www.linkedin.com">www.linkedin.com</a>
Twitter	<a href="http://api.twitter.com">api.twitter.com</a>
	<a href="http://abs.twimg.com">abs.twimg.com</a>
	<a href="http://abs-0.twimg.com">abs-0.twimg.com</a>
	<a href="http://pbs.twimg.com">pbs.twimg.com</a>
	<a href="http://api.twitter.com">api.twitter.com</a>

## 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
<b>SECURITY</b>		
<b>Authentication</b>		
- 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		
<b>Redirection on corporate web portal</b>	✓	
<b>URL/domain filtering (HTTP and HTTPS)</b>		Not ensured by UCOPIA controller as the traffic won't go through it
<b>Access permissions on basis of user profile</b>	✓	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.

<b>Controller's incoming VLANs/subnets</b>	✓	
<b>WPA, 802.11i compliance</b>	✓	
<b>URLs available before authentication</b>	✓	
<b>Pre-authentication charter acceptance</b>	✓	
<b>Private information charter acceptance (opt-in marketing)</b>	✓	
<b>Password policies and password recovery</b>	✓	
<b>Quarantine after N wrong password attempts</b>	✓	
<b>Connection break between two sessions</b>	✓	
<b>Connections traceability and logs</b>	✓	Sent by Aerohive AP to UCOPIA in real-time
- User sessions	✓	
- Traffic	✓	
- URL		
- Automatic logs backup via FTP(S)	✓	
- Automatic logs compression	✓	
<b>Audit logs (Syslog)</b>	✓	
<b>MOBILITY</b>		
<b>QoS (by service, by user)</b>		No BW limitation / reservation possible on UCOPIA as the traffic won't go through it
<b>Data volume quota</b>		No quota applied by UCOPIA as the traffic won't go through it
<b>Time based access control</b>		
- Configured ending validity date	✓	
- Configured ending validity date		
- Time credit	✓	
<b>Location based access control:</b> Localization on incoming and outgoing zones	✓	
<b>Multi-portal (one portal per zone)</b>	✓	
<b>Conditional profile</b>	✓	Only for the supported features of the profile
<b>Memorization and limitation of devices per user</b>	✓	
<b>Auto disconnection</b>	N/A	Disabled on the central controller as soon as an Out-Of-Band architecture is set up
<b>Possibility for the user to disconnect from the captive portal (thanks to a « Disconnection» button)</b>		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)	
<b>BILLING</b>		
Online payment (credit card, PayPal, Ingenico)	✓	
PMS connector	✓	Only one PMS can be configured and integrated with the central UCOPIA
<b>INTEGRATION</b>		
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	✓	