



Deploy a Cloudpath ES Workflow on HiveManager NG

Cloudpath as RADIUS server and as a Hotspot (WISPr) Portal

Best Practices and Deployment Guide

Table of Contents

Intent of this Document	3
Cloudpath Workflow Overview.....	4
Onboarding and Secure WLANs on HiveManager NG.....	5
1) Get the enrollment URL and the RADIUS shared secret from Cloudpath ES	5
2) Create a new network policy in HiveManager NG.....	7
3) Add the SSID for the Onboarding Portal.....	9
4) Configure the Captive Web Portal with the Cloudpath Enrollment URL	12
5) Add the Walled Garden.....	13
6) Add Cloudpath ES RADIUS Server to Portal SSID.....	14
7) Create the Secure WLAN.....	16
8) Deploy the Network Policy	20
About Ruckus	22

This table of contents can be used as a checklist in the future.

August 2017

Intent of this Document

Cloudpath Best Practices and Deployment Guides are meant to address specific subjects in Ruckus Cloudpath deployments and to tackle those subjects in bite sized chunks. Although Cloudpath is simpler and more user-friendly than competitors, there are many options within Cloudpath and network administrators will benefit from a series of targeted Best Practices and Deployment Guides.

What is Ruckus Cloudpath? Cloudpath is a self-service onboarding portal for secure networks. We are all familiar with captive portals for public access/hotspot networks. Unlike those systems, Cloudpath can support self-service secure registration for networks, combining everything necessary for:

- *Policy Management* - Is the user a student or a teacher? Is the device a phone or a laptop?
- *Device Enablement* - Is the anti-virus up-to-date? Is the firewall running and the OS patched?
- *Certificate Deployment and Management* – Certificates are deployed automatically, uniquely identifying all devices

IT gets more control and more information, while spending less time on password problems and basic access issues.

This document walks through the deployment of a Cloudpath workflow (or registration portal), on a Ruckus SmartZone WLAN controller. It supports the typical case of two WLANs (SSIDs) – one for the onboarding portal, one for secure users. The secure SSID is 802.1X certificate secured for users and is accessible only after they have registered their devices at the onboarding portal. The open SSID can serve double duty as both the secure user onboarding portal, and also as the guest WLAN with automatic MAC registration of guest devices. Configuration of both options is described below.

This document is not a installation guide for Cloudpath or for HiveManager NG.

Cloudpath ES server should already be fully deployed and accessible, locally or as a cloud system. An external database of users should be available.* A workflow should already be configured on Cloudpath ES. If necessary, consult the Cloudpath Best Practices and Deployment Guide “Basic Cloudpath Workflow - secure users and MAC auth guests”.

Similarly, an Aerohive HiveManager NG Public Cloud account should be available, with at least one AP connected to it. To test, Wi-Fi client devices such as tablets, smart phones, or laptops will be needed.

*There is a limited onboard database in Cloudpath that can be used in a lab environment, but it is not recommended for a production environment

August 2017

Cloudpath Workflow Overview

A workflow is a tree of network access policy/classification steps contained in a series of web pages. A policy is built in a series of steps, and then published as an Onboarding Portal (web pages) on the Cloudpath web server. Adding a step usually involves adding a web page, but it could be a filter or other classification step that automatically flows through to the next step/page. A workflow generally ends in downloading a *Device Configuration* onto a secure client. A Cloudpath *Device Configuration* is typically a WLAN/SSID profile, including security settings and an 802.1X certificate. However, it may end in some alternative grant of network access, such as a PSK, a Ruckus Dynamic PSK, or display of a voucher code for a guest user.

Hotspot Portal SSID and RADIUS Secured SSID

This document describes deployment of a Cloudpath workflow for an environment with two WLANs/SSIDs. The first WLAN is a secure/employee SSID that uses 802.1X certificate authentication (supported by the Cloudpath RADIUS server). Take special note – the Cloudpath ES RADIUS server authenticates the certificates for access to the secure network. At registration, there will need to be an authentication server (database) of employees (secure users) that Cloudpath can check before distributing profiles and certificates.

The second SSID is an open WLAN redirected as a Hotspot/WISPr portal. It serves both as employee registration and as a Guest Access portal. Secure users (employees) initially register their devices and download a certificate on the open SSID. It is a one-time process for each employee device, and once a device is registered and has a unique certificate, it immediately, and always thereafter, connects to the secure network.

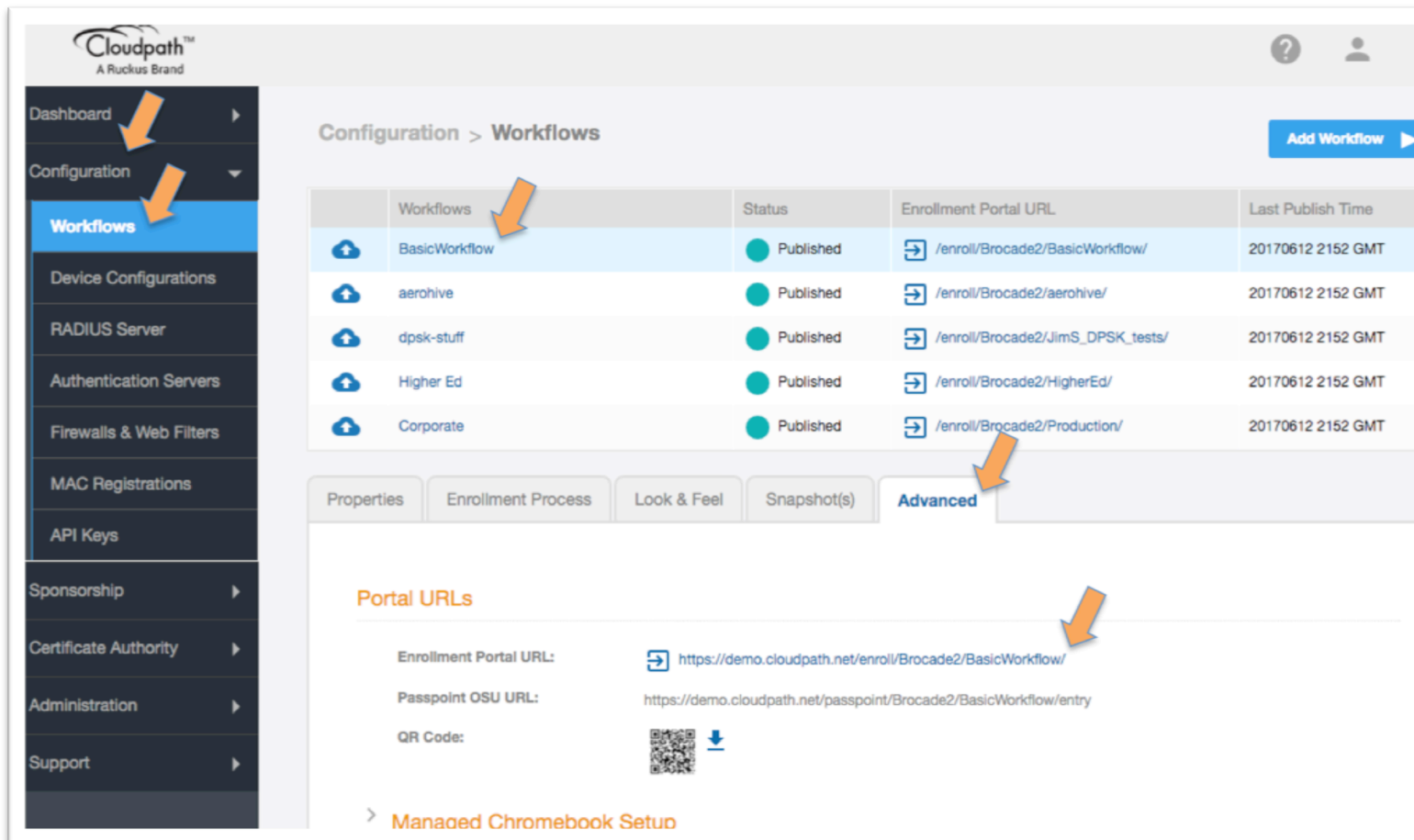
Guest users can connect to the open SSID, choose to register as a guest, and their device will be uniquely registered by its MAC address. The portal will open up (the walled garden will open) and they will be granted Internet access.

This is designed to be a simple but effective workflow that can be built on, and necessary configuration of Cloudpath is described in the Cloudpath Best Practices and Deployment Guide “Basic Cloudpath Workflow - Secure Users and MAC-auth Guests”.

Onboarding and Secure WLANs on HiveManager NG

1) Get the enrollment URL and the RADIUS shared secret from Cloudpath ES

- Configuration of a basic workflow in Cloudpath ES should have been completed. However, before moving on to a WLAN controller, there are two pieces of information that will be needed.
 - The Enrollment Portal URL
 - The Cloudpath ES RADIUS settings




The screenshot displays the Cloudpath ES interface. On the left is a navigation sidebar with 'Workflows' selected. The main area shows 'Configuration > Workflows' with a table of workflows. The 'BasicWorkflow' row is selected, and its 'Advanced' tab is active. The 'Advanced' tab shows 'Portal URLs' with the 'Enrollment Portal URL' field highlighted.

Workflows	Status	Enrollment Portal URL	Last Publish Time
BasicWorkflow	Published	/enroll/Brocade2/BasicWorkflow/	20170612 2152 GMT
aerohive	Published	/enroll/Brocade2/aerohive/	20170612 2152 GMT
dpsk-stuff	Published	/enroll/Brocade2/JimS_DPSK_tests/	20170612 2152 GMT
Higher Ed	Published	/enroll/Brocade2/HigherEd/	20170612 2152 GMT
Corporate	Published	/enroll/Brocade2/Production/	20170612 2152 GMT

Portal URLs

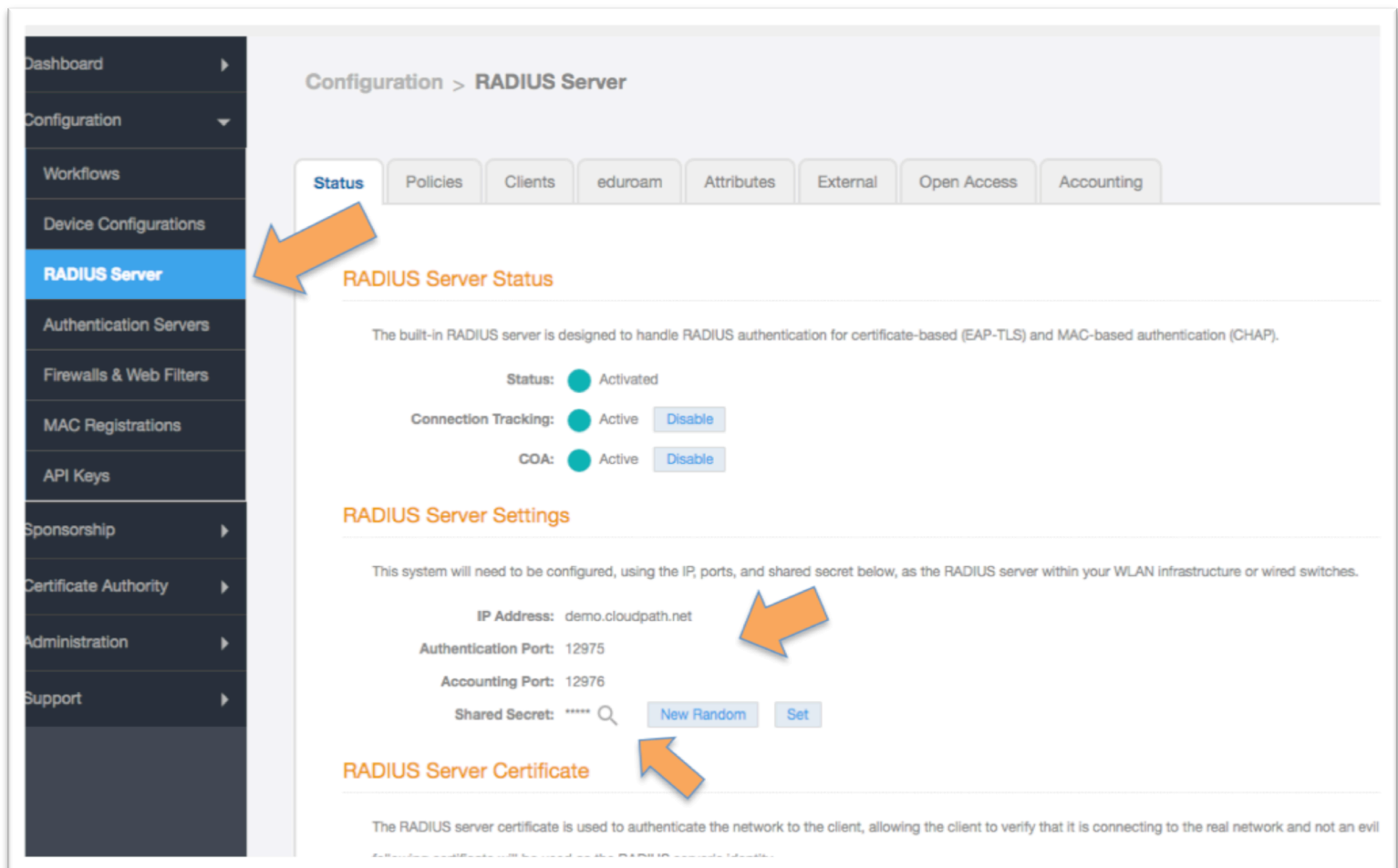
Enrollment Portal URL: <https://demo.cloudpath.net/enroll/Brocade2/BasicWorkflow/>

Passpoint OSU URL: <https://demo.cloudpath.net/passpoint/Brocade2/BasicWorkflow/entry>

QR Code: 

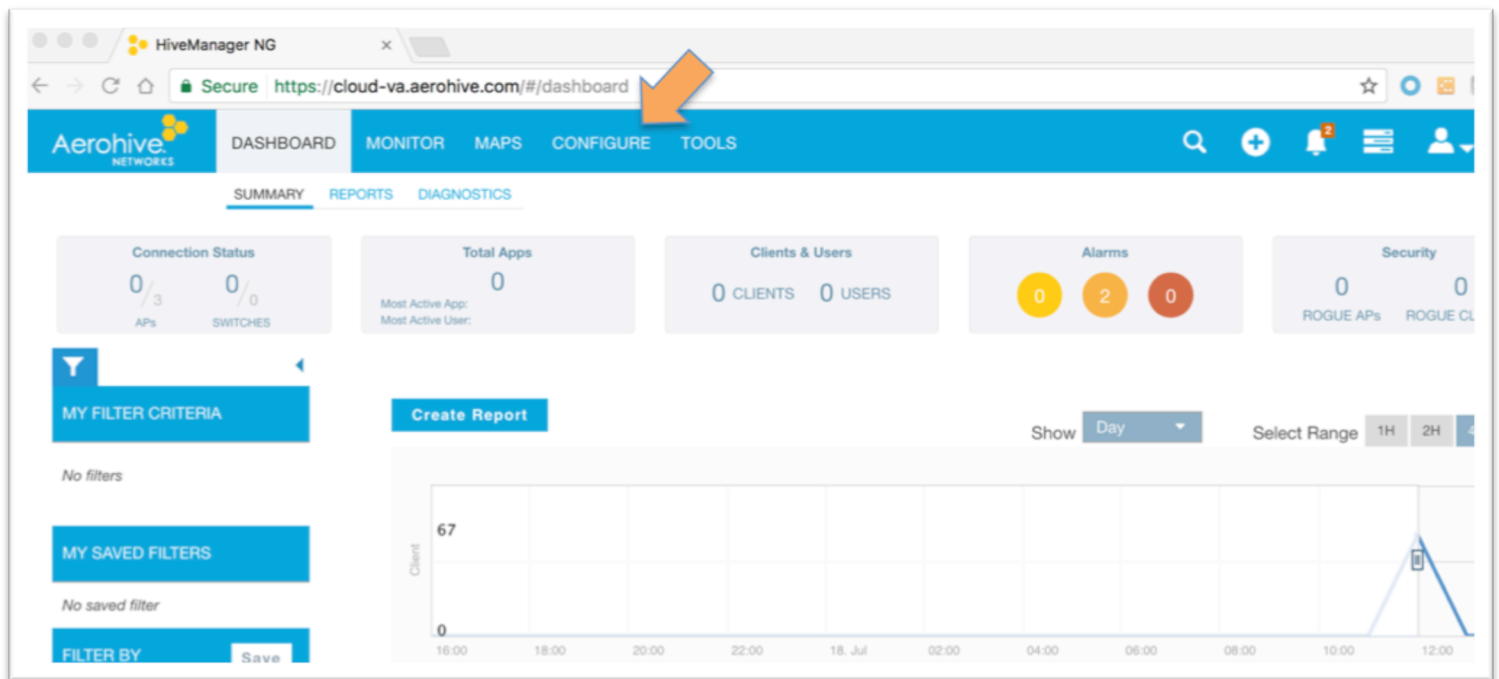
> [Managed Chromebook Setup](#)

- Login to Cloudpath ES and navigate to:
 - Configuration
 - Workflow
 - Click on the workflow to be deployed
 - Click on the workflow's **Advanced** tab
 - Go to the Enrollment Portal URL.
 - Copy this URL to a text editor for later (or be prepare to return to this window).
 - This URL will be added to HiveManager NG as an external portal

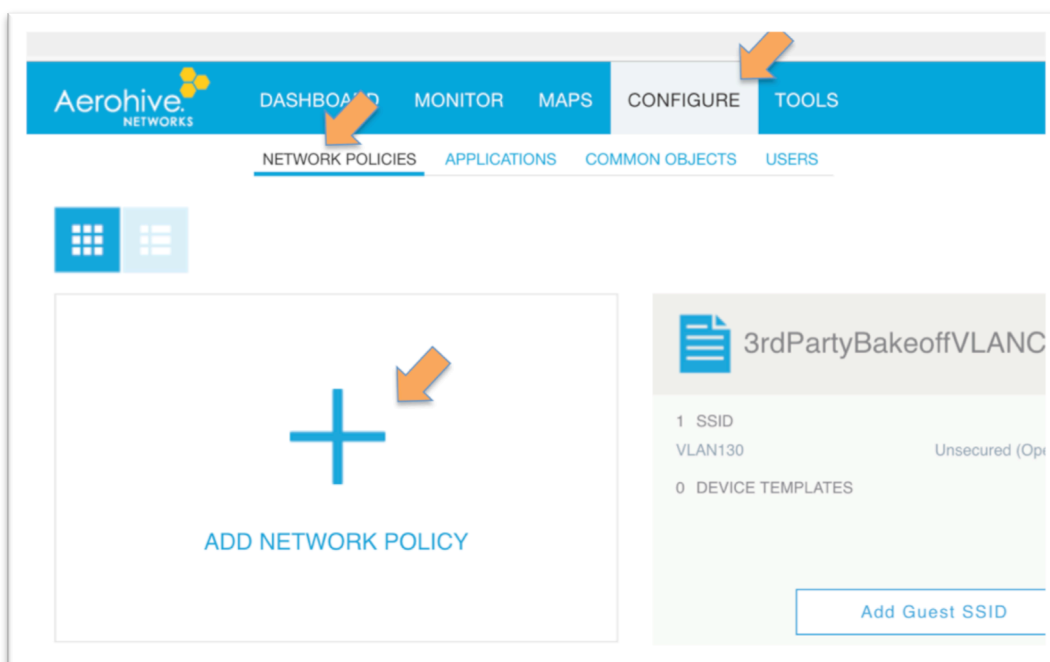


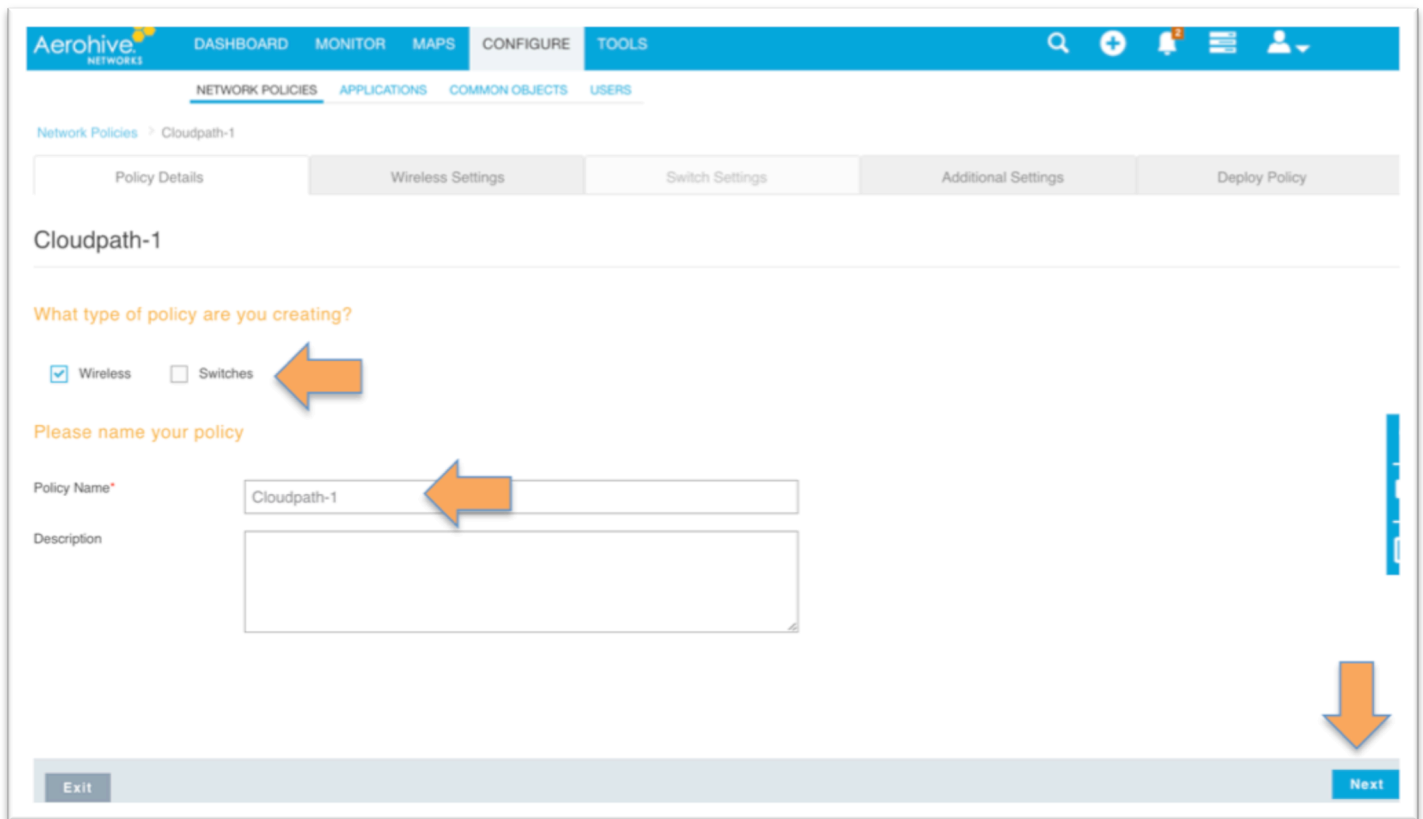
- HiveManager NG will need the RADIUS server settings. On the main menu bar, navigate to **Configuration -> RADIUS Server**. Copy the following information for later
 - The **IP address**
 - *NB - must be an IP address. If necessary, a CLI ping will determine the IP from the FQDN*
 - **Authentication port**
 - The Accounting port (optional)
 - The **Shared Secret**
 - which can be revealed by clicking on the magnifying glass

2) Create a new network policy in HiveManager NG



- Login to Hive Manager NG
 - Navigate to **Configure ->Network Policies**
 - Click on **Add Network Policy**





Aerohive NETWORKS

DASHBOARD MONITOR MAPS CONFIGURE TOOLS

NETWORK POLICIES APPLICATIONS COMMON OBJECTS USERS

Network Policies > Cloudpath-1

Policy Details Wireless Settings Switch Settings Additional Settings Deploy Policy

Cloudpath-1

What type of policy are you creating?

Wireless Switches

Please name your policy

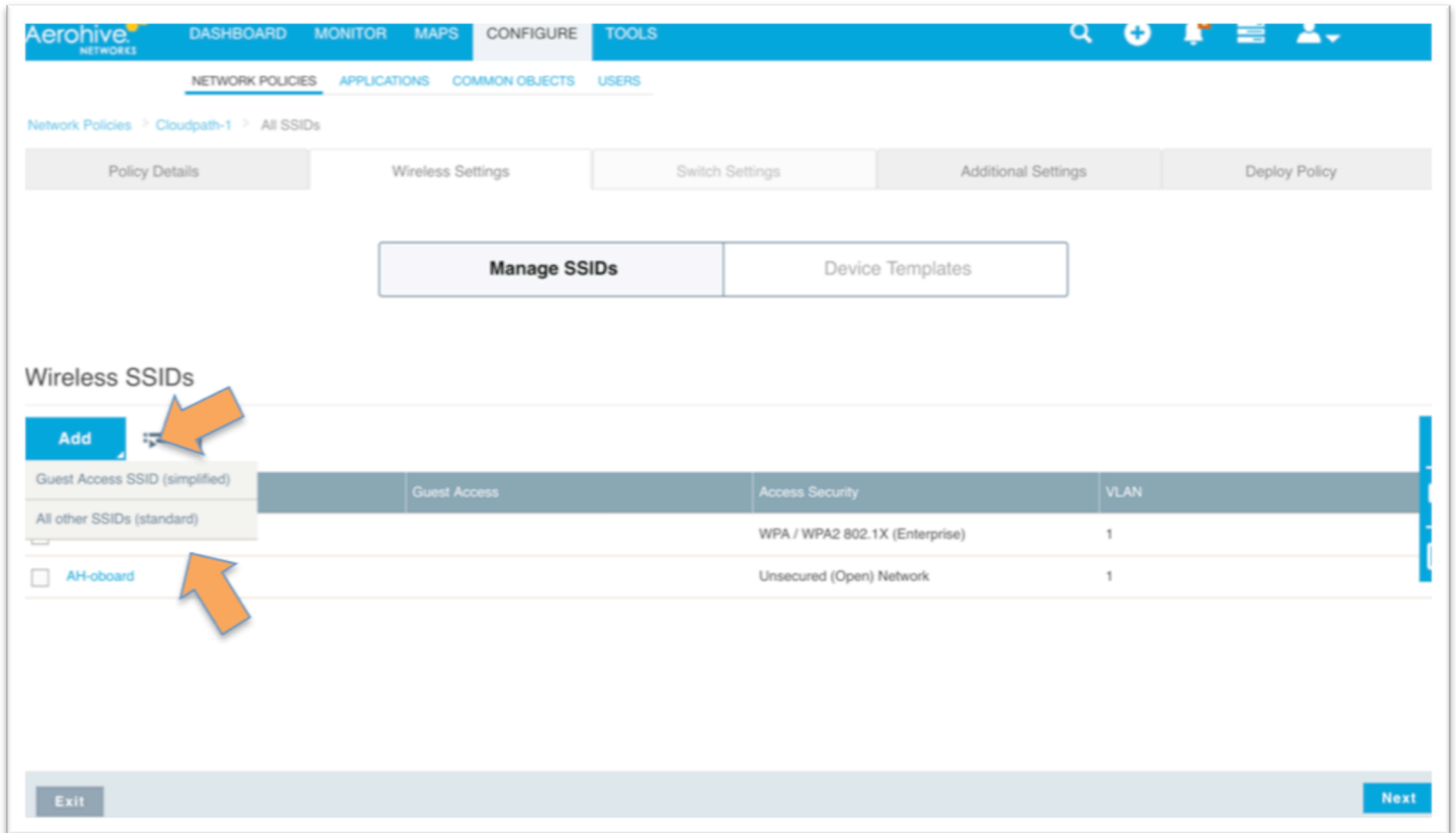
Policy Name* Cloudpath-1

Description

Exit Next

- Check **Wireless** and/or uncheck **Switches**
- Fill in **Policy Name**
- Optionally, add a **Description**
- Click **Next** to save the policy and go on to **Wireless Settings**

3) Add the SSID for the Onboarding Portal

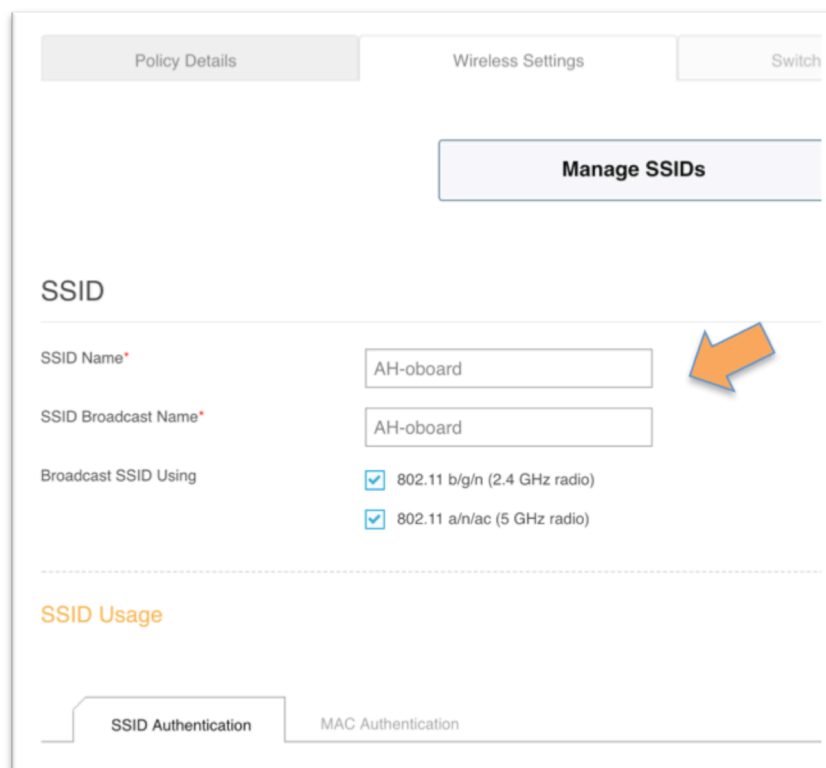


The screenshot shows the Aerohive Networks configuration interface. The top navigation bar includes DASHBOARD, MONITOR, MAPS, CONFIGURE, and TOOLS. Below this, there are tabs for NETWORK POLICIES, APPLICATIONS, COMMON OBJECTS, and USERS. The current view is 'Network Policies > Cloudpath-1 > All SSIDs'. There are several tabs: Policy Details, Wireless Settings, Switch Settings, Additional Settings, and Deploy Policy. A 'Manage SSIDs' button is visible. The 'Wireless SSIDs' section has an 'Add' button (highlighted with an orange arrow) and a dropdown menu with 'All other SSIDs (standard)' selected. Below this is a table of existing SSIDs:

SSID Name	Guest Access	Access Security	VLAN
Guest Access SSID (simplified)	Guest Access	WPA / WPA2 802.1X (Enterprise)	1
<input type="checkbox"/> AH-board		Unsecured (Open) Network	1

At the bottom, there are 'Exit' and 'Next' buttons.

- Under the **Wireless Settings** Tab
- Under **Wireless SSIDs**
- Click **Add**
- Click on **All other SSIDs (standard)**



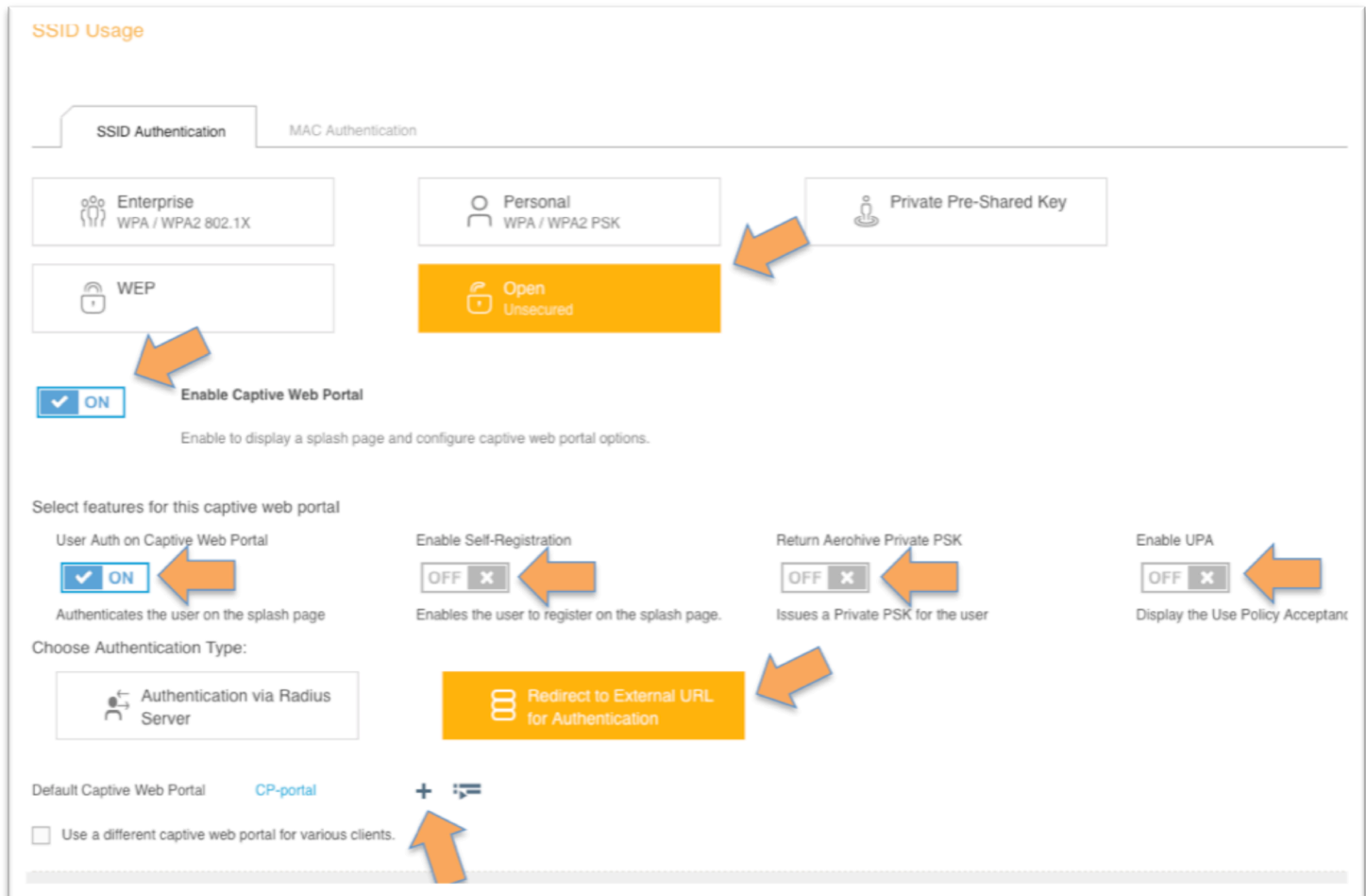
The screenshot shows a web interface for configuring wireless settings. At the top, there are three tabs: "Policy Details", "Wireless Settings", and "Switch". Below the tabs is a "Manage SSIDs" button. The main section is titled "SSID" and contains the following fields and options:

- SSID Name***: A text input field containing "AH-oboard". An orange arrow points to this field.
- SSID Broadcast Name***: A text input field containing "AH-oboard".
- Broadcast SSID Using**: Two checked checkboxes:
 - 802.11 b/g/n (2.4 GHz radio)
 - 802.11 a/n/ac (5 GHz radio)

Below the SSID configuration is a section titled "SSID Usage" with two radio buttons: "SSID Authentication" (selected) and "MAC Authentication".

- Fill in **SSID Name** (internal name)
- Fill in the **SSID Broadcast Name**
- Scroll down to **SSID Usage**

Note: because Cloudpath ES will provide the Web Portal, native Aerohive features will not be enabled



SSID Usage

SSID Authentication | MAC Authentication

Enterprise WPA / WPA2 802.1X

Personal WPA / WPA2 PSK

Private Pre-Shared Key

WEP

Open Unsecured

ON Enable Captive Web Portal
Enable to display a splash page and configure captive web portal options.

Select features for this captive web portal

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

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

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

Enable UPA OFF
Display the Use Policy Acceptant

Choose Authentication Type:

Authentication via Radius Server

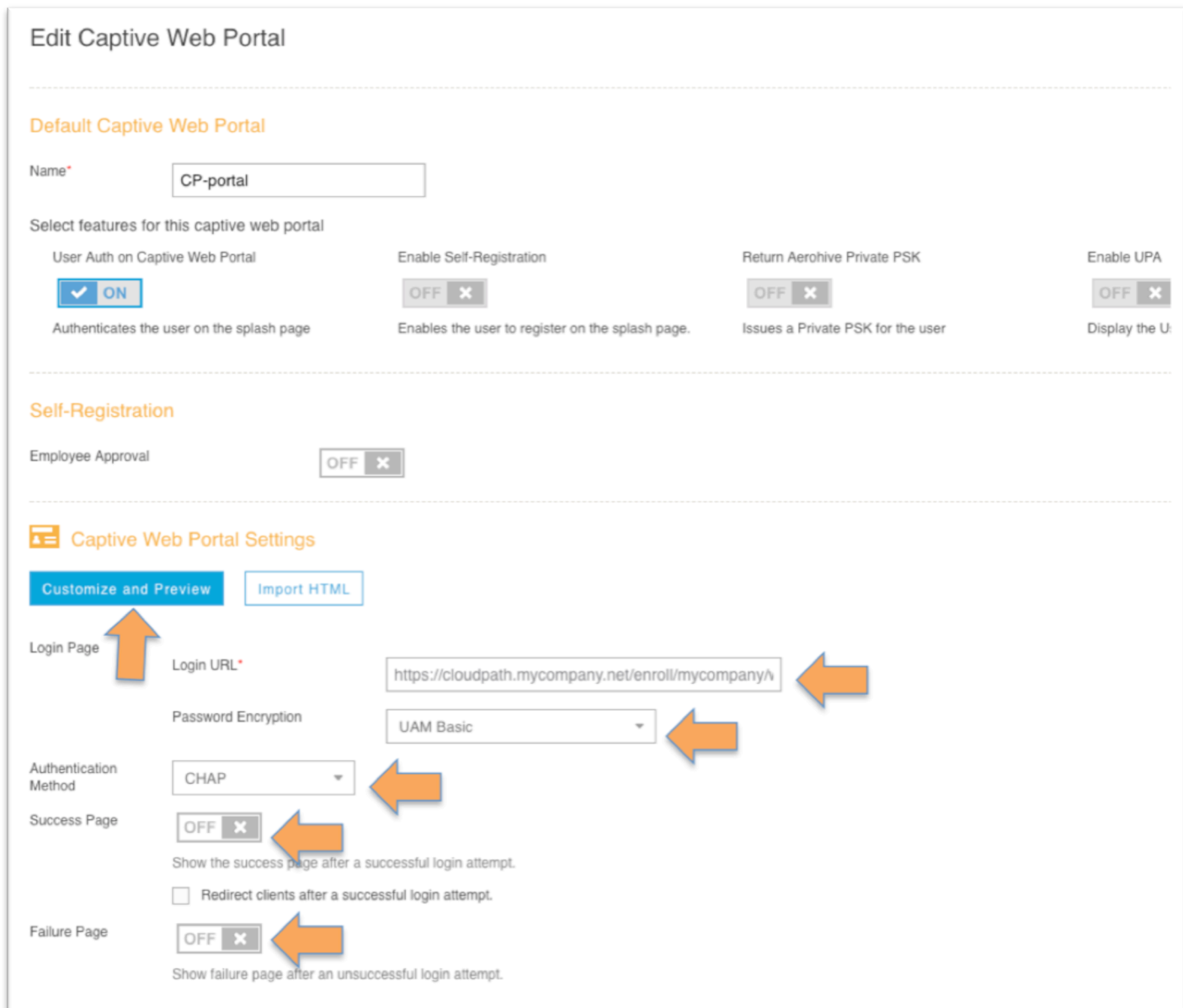
Redirect to External URL for Authentication

Default Captive Web Portal CP-portal

Use a different captive web portal for various clients.

- Under SSID authentication configure the following settings. Note that some settings only appear after the ones above them are changed
 - Click on **Open Unsecured**
 - **Enable Captive Web Portal -> ON**
 - **User Auth on Captive Web Portal -> ON**
 - **Enable Self-Registration - > OFF**
 - **Return Aerohive Private PSK -> OFF**
 - **Enable UPA - > OFF**
 - Click on **Redirect to External URL for Authentication**
- At **Default Captive Web Portal** Click the **+** to add the *Cloudpath ES enrollment URL*

4) Configure the Captive Web Portal with the Cloudpath Enrollment URL



Edit Captive Web Portal

Default Captive Web Portal

Name*

Select features for this captive web portal

User Auth on Captive Web Portal <input checked="" type="checkbox"/> ON Authenticates the user on the splash page	Enable Self-Registration <input type="checkbox"/> OFF X Enables the user to register on the splash page.	Return Aerohive Private PSK <input type="checkbox"/> OFF X Issues a Private PSK for the user	Enable UPA <input type="checkbox"/> OFF X Display the U
--	--	--	---

Self-Registration

Employee Approval OFF X

Captive Web Portal Settings

Login Page

Login URL*

Password Encryption

Authentication Method

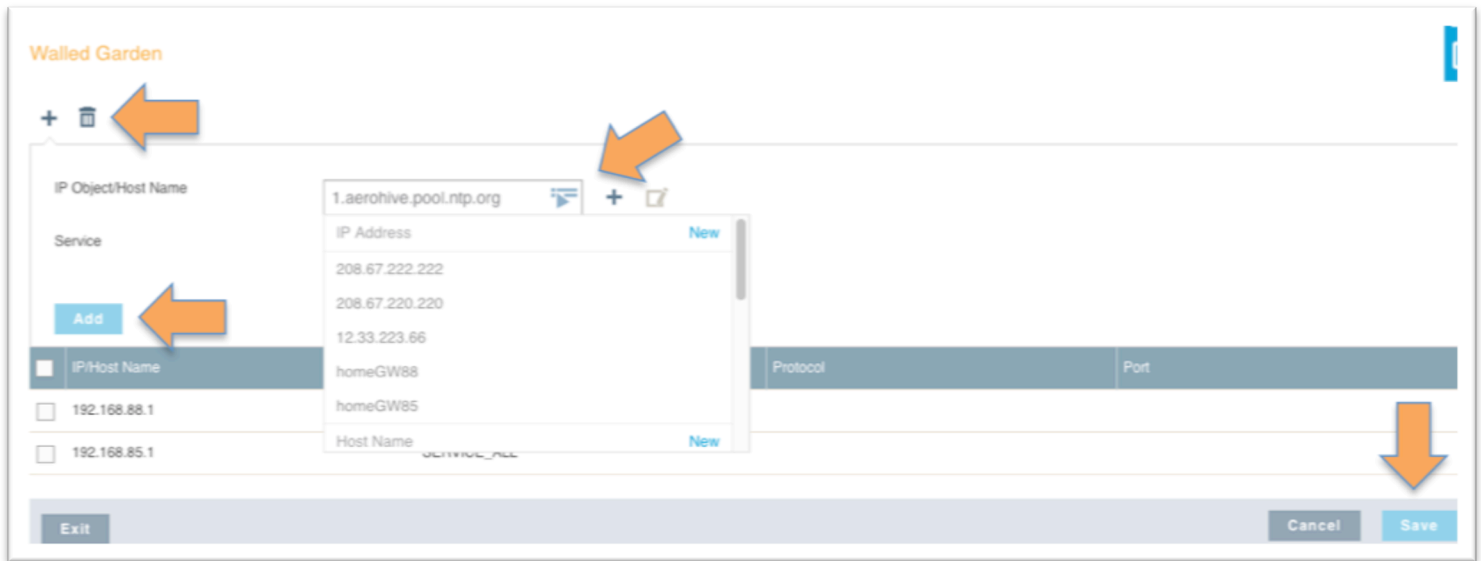
Success Page OFF X
Show the success page after a successful login attempt.
 Redirect clients after a successful login attempt.

Failure Page OFF X
Show failure page after an unsuccessful login attempt.

- **Name** the Portal
- Click **Customize and Preview**
- For **Login URL**, insert the **Cloudpath ES enrollment URL** from the appropriate workflow as shown in section 1
- Other settings
 - **Password Encryption** - > choose **UAM Basic**
 - **Authentication Method** - > choose **CHAP**
 - **Success Page** - > **OFF**
 - **Failure Page** -> **OFF**

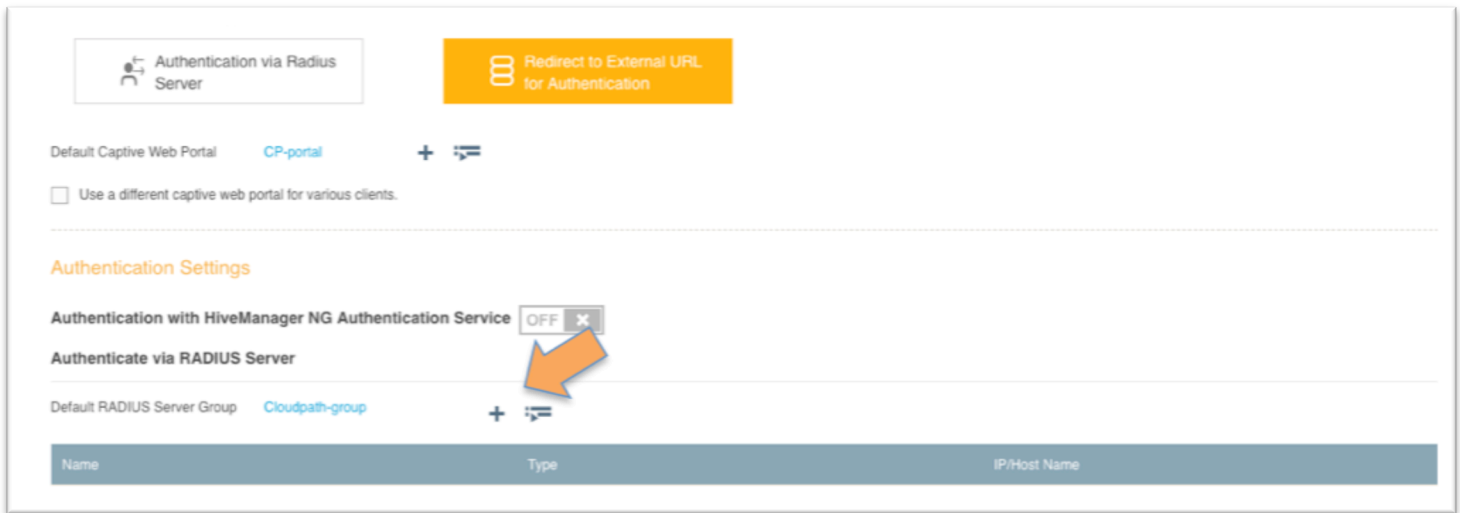
5) Add the Walled Garden

Scroll to the bottom of the **New/Edit Captive Web Portal** page

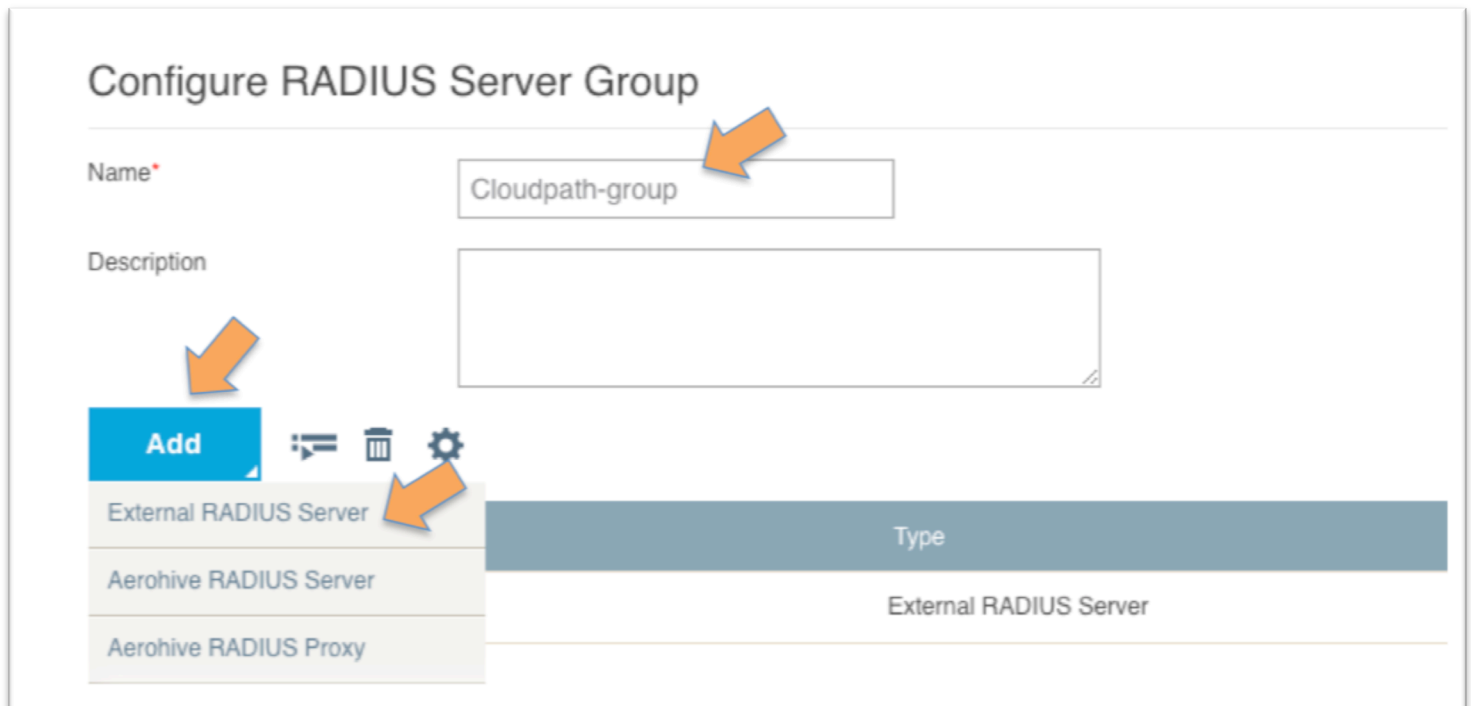


- **Walled Garden:** In order to function, specific network traffic must be allowed before the user is authenticated in order to support the authentication process. The exact entries depend on the local network. The following are generally required
 - DHCP server – the client generally needs an IP address
 - DNS server
 - Gateway (in many case, all three are the same)
 - Cloudpath server, including subdomains of the enrollment URL
- Use the **+** to open the **IP Object/Host Name** section
 - Objects must be created first, using the **+** button, then selected in the drop down. Once selected, they can be added to the **Walled Garden** list with the blue **Add** button
- Create objects as necessary, and **Add** to the **Walled Garden**
- Click **Save**

6) Add Cloudpath ES RADIUS Server to Portal SSID



- Continuing under the main SSID configuration page
- Scroll to **Authentication Settings** and use the + to add a **RADIUS server group**



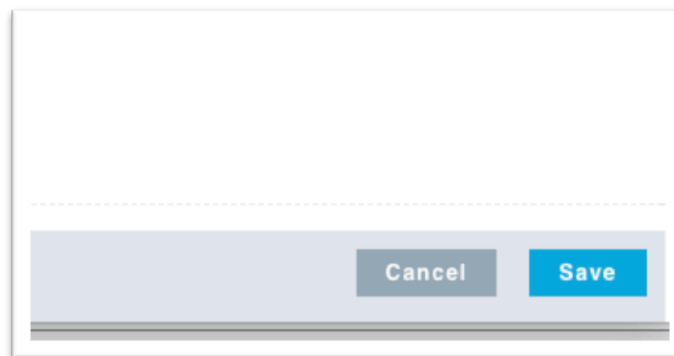
- Give the group a **Name**

August 2017

- Click **Add**
- Choose **External RADIUS Server**



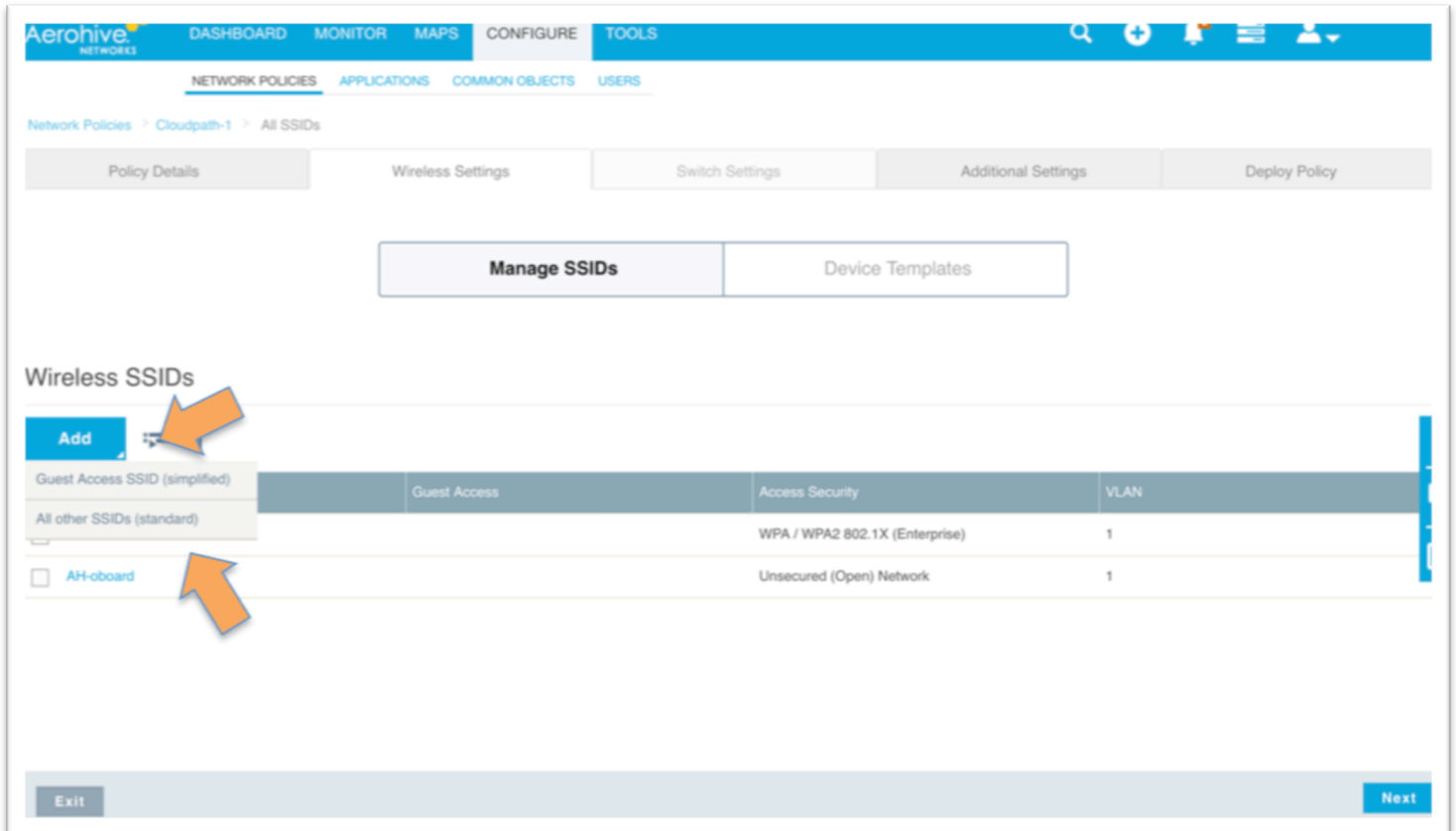
- In the **External RADIUS Server** window, enter the values for the Cloudpath RADIUS server from section 1
 - Give it a **Name**
 - At **IP Address/Hostname** use the **+** to add the **IP address**
 - At **Server Type**, assign the Authentication and Accounting **ports**
 - Enter the **Shared Secret**
 - **Save**



- **Save** - Under the main SSID configuration page, use the lower right side **Save** button to save all the SSID settings

7) Create the Secure WLAN

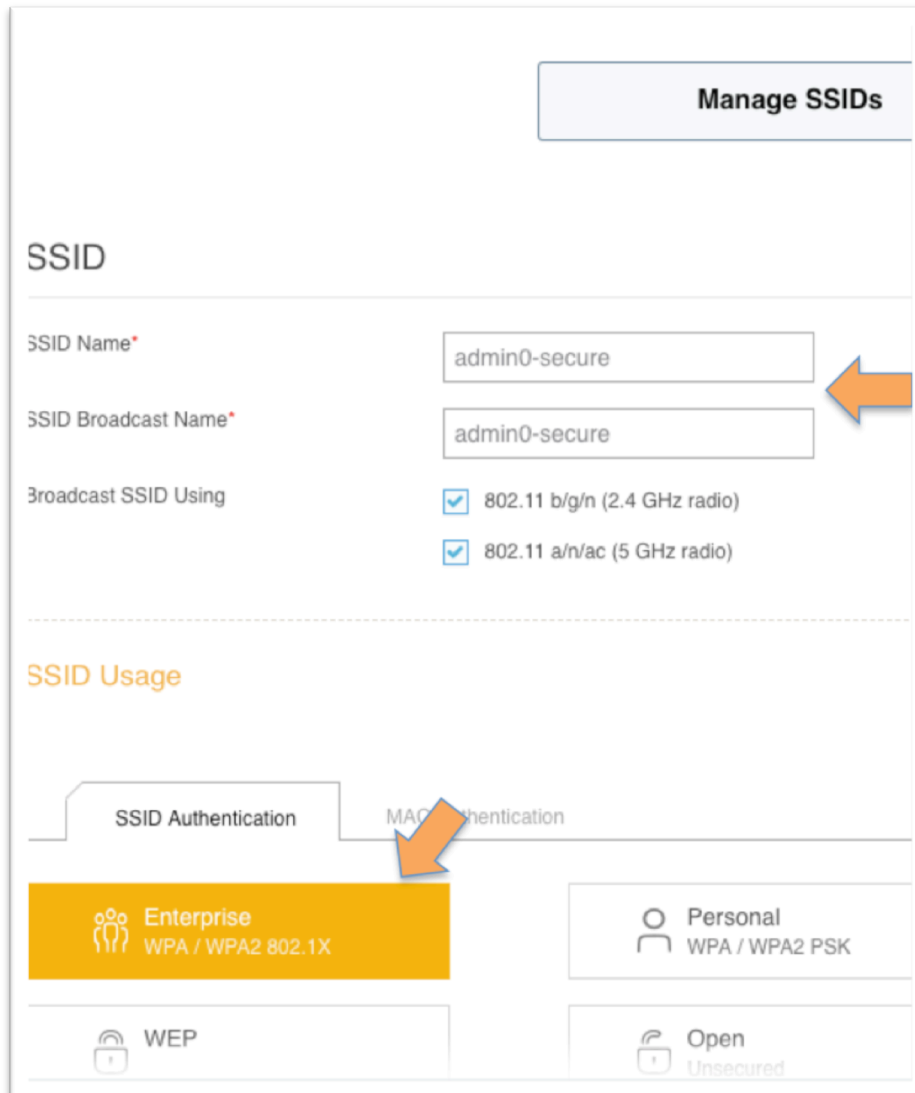
This is the secure SSID for registered users and their devices



Guest Access	Access Security	VLAN
Guest Access	WPA / WPA2 802.1X (Enterprise)	1
	Unsecured (Open) Network	1

- Create another SSID in **Wireless Settings** -> **Wireless SSIDs**
 - Click the **Add** button
 - Choose **All Other SSIDs (standard)**

August 2017



Manage SSIDs

SSID

SSID Name*

SSID Broadcast Name*

Broadcast SSID Using

- 802.11 b/g/n (2.4 GHz radio)
- 802.11 a/n/ac (5 GHz radio)

SSID Usage

SSID Authentication | MAC Authentication

Enterprise
WPA / WPA2 802.1X

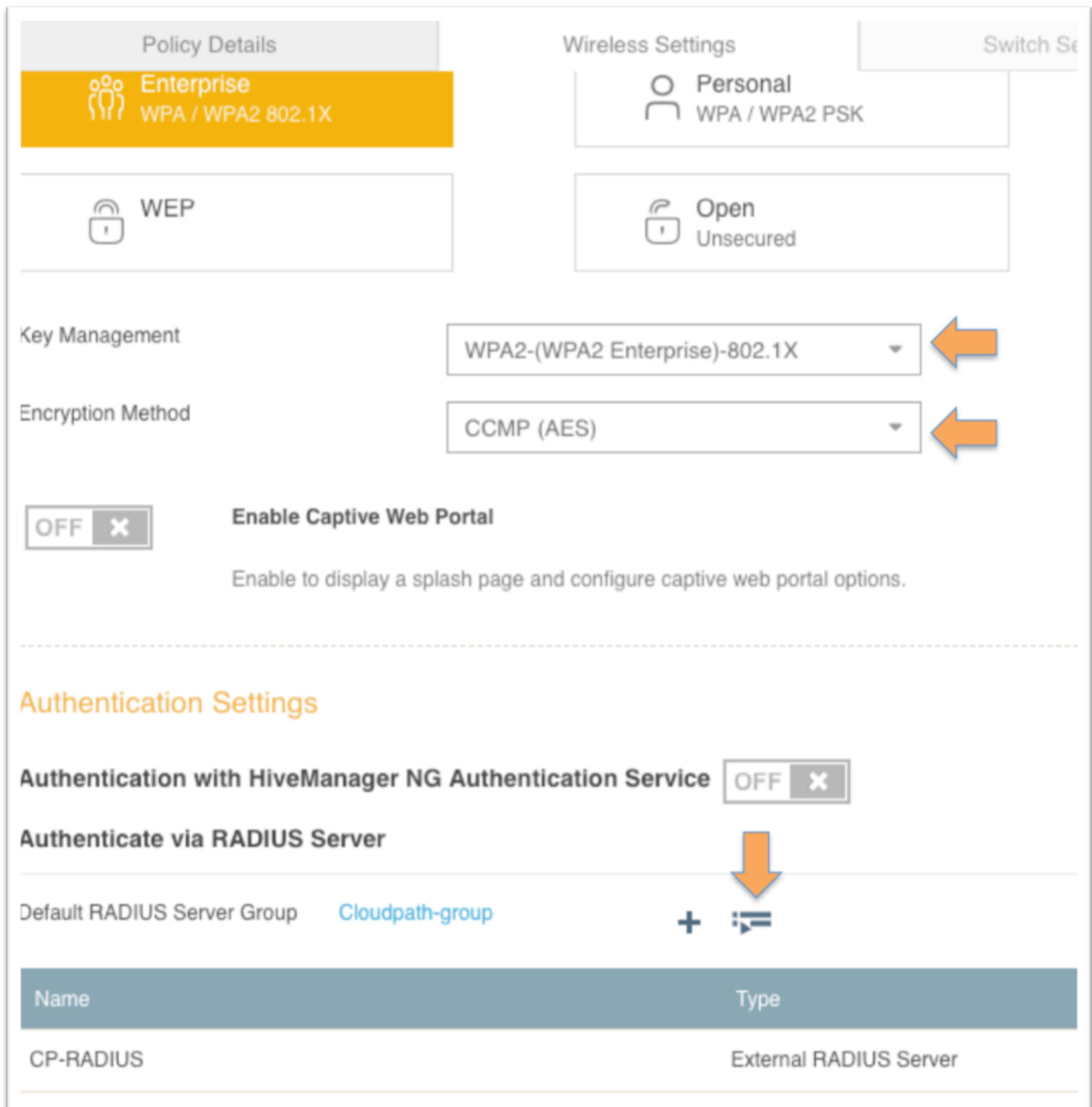
Personal
WPA / WPA2 PSK

WEP

Open
Unsecured

- **Name** the SSID and give it a **Broadcast Name**
- Under **SSID Usage**, click **Enterprise WPA/WPA2 802.1X**
- For **Key Management** choose **WPA2-(WPS2 Enterprise)-802.1X**
- For **Encryption Method** choose **CCMP(AES)**

August 2017



Policy Details

Enterprise
WPA / WPA2 802.1X

WEP

Wireless Settings

Personal
WPA / WPA2 PSK

Open
Unsecured

Key Management

WPA2-(WPA2 Enterprise)-802.1X

Encryption Method

CCMP (AES)

OFF

Enable Captive Web Portal

Enable to display a splash page and configure captive web portal options.

Authentication Settings

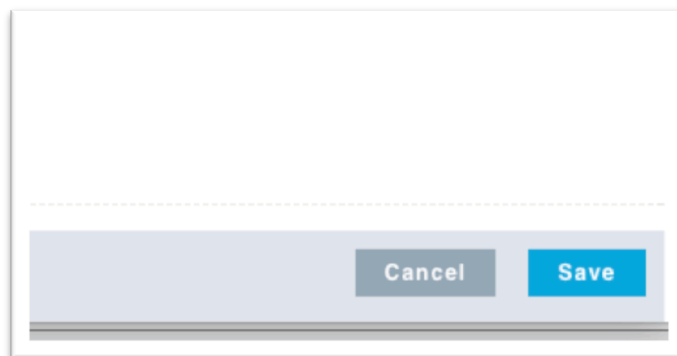
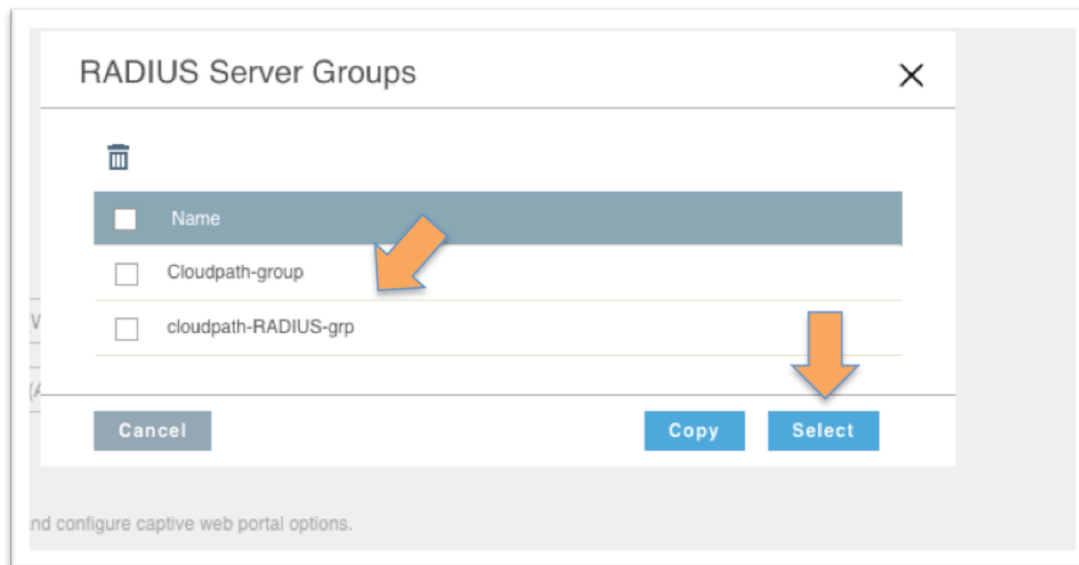
Authentication with HiveManager NG Authentication Service OFF

Authenticate via RADIUS Server

Default RADIUS Server Group **Cloudpath-group**

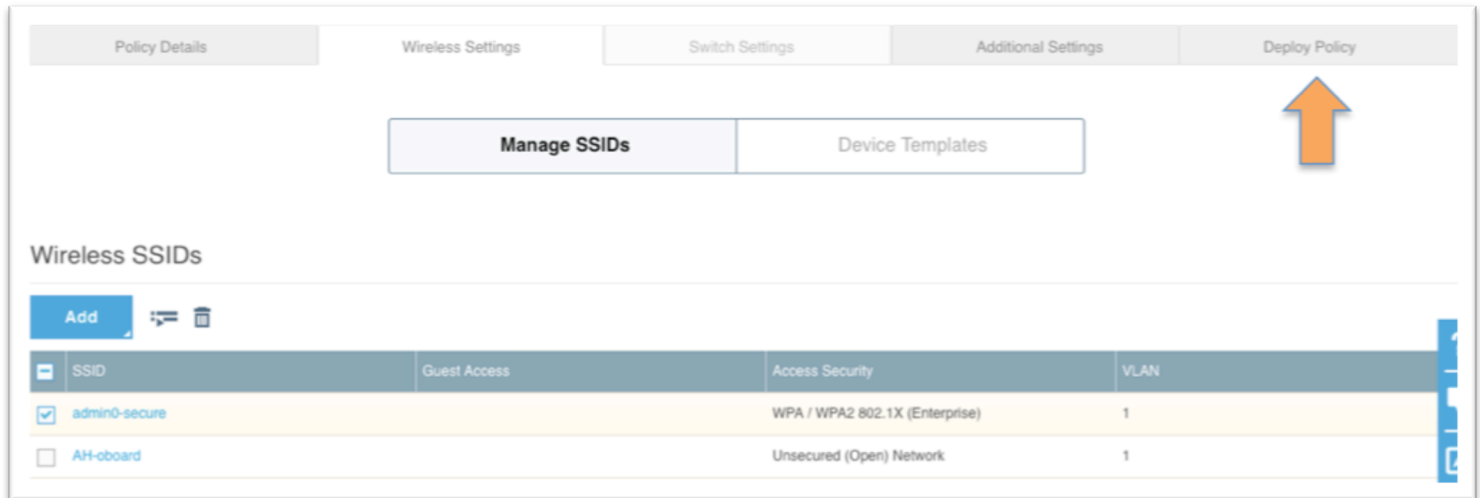
Name	Type
CP-RADIUS	External RADIUS Server

- Under **Authentication Settings** -> **Authenticate via RADIUS server**,
 - use the **selection box** to choose the previously defined **RADIUS Server Group** that matches the *Cloudpath ES RADIUS Server*



- Use the lower right side **Save** button to save all the SSID settings

8) Deploy the Network Policy



Policy Details Wireless Settings Switch Settings Additional Settings **Deploy Policy**

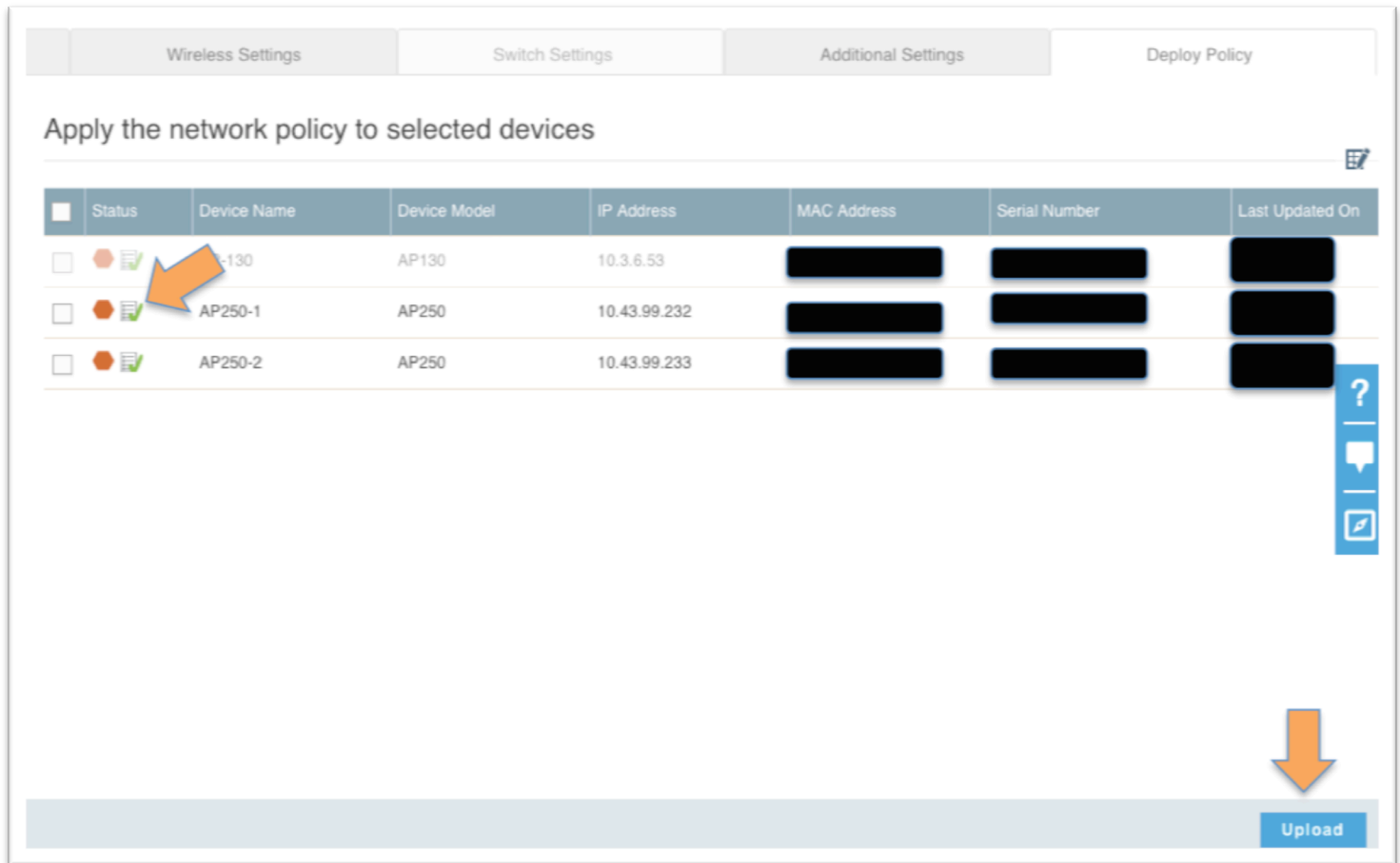
Manage SSIDs Device Templates

Wireless SSIDs

Add

SSID	Guest Access	Access Security	VLAN
<input checked="" type="checkbox"/> admin0-secure		WPA / WPA2 802.1X (Enterprise)	1
<input type="checkbox"/> AH-o-board		Unsecured (Open) Network	1

- Click on the **Deploy Policy** tab in the upper right
 - Or the **Next** button will take you through all the tabs in order



The screenshot shows the 'Deploy Policy' tab in the Aerohive Cloud Controller interface. The main heading is 'Apply the network policy to selected devices'. Below this is a table with the following columns: Status, Device Name, Device Model, IP Address, MAC Address, Serial Number, and Last Updated On. Three devices are listed: AP130, AP250-1, and AP250-2. An orange arrow points to the status icon of the first device. At the bottom right, there is a blue 'Upload' button with a large orange arrow pointing down towards it.

Status	Device Name	Device Model	IP Address	MAC Address	Serial Number	Last Updated On
<input type="checkbox"/>	AP130	AP130	10.3.6.53	[REDACTED]	[REDACTED]	[REDACTED]
<input type="checkbox"/>	AP250-1	AP250	10.43.99.232	[REDACTED]	[REDACTED]	[REDACTED]
<input type="checkbox"/>	AP250-2	AP250	10.43.99.233	[REDACTED]	[REDACTED]	[REDACTED]

- **Select the APs** to deploy the **Network Policy** to
- Click **Upload**

Configuration is done and ready to test.

August 2017

About Ruckus

Headquartered in Sunnyvale, CA, Ruckus Wireless, Inc. is a global supplier of advanced wireless systems for the rapidly expanding mobile Internet infrastructure market. The company offers a wide range of indoor and outdoor “Smart Wi-Fi” products to mobile carriers, broadband service providers, and corporate enterprises, and has over 36,000 end-customers worldwide. Ruckus technology addresses Wi-Fi capacity and coverage challenges caused by the ever-increasing amount of traffic on wireless networks due to accelerated adoption of mobile devices such as smartphones and tablets. Ruckus invented and has patented state-of-the-art wireless voice, video, and data technology innovations, such as adaptive antenna arrays that extend signal range, increase client data rates, and avoid interference, providing consistent and reliable distribution of delay-sensitive multimedia content and services over standard 802.11 Wi-Fi. For more information, visit <http://www.ruckuswireless.com>.

Ruckus and Ruckus Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries.

Copyright 2017 Ruckus Wireless, Inc. All Rights Reserved.

Copyright Notice and Proprietary Information No part of this documentation may be reproduced, transmitted, or translated, in any form or by any means without prior written permission of Ruckus Wireless, Inc. ("Ruckus"), or as expressly provided by under license from Ruckus

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL