
Deploy a Cloudpath ES Workflow on HiveManager NG

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

Best Practices and Deployment Guide

Cloudpath On Aerohive

Deploying a Cloudpath workflow on an Aerohive Cloud Controller

August 2017

Table of Contents

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

Cloudpath On Aerohive

Deploying a Cloudpath workflow on an Aerohive Cloud Controller

August 2017

Intent of this Document

Cloudpath Best Practices and Deloyment 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

Cloudpath On Aerohive

Deploying a Cloudpath workflow on an Aerohive Cloud Controller

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.

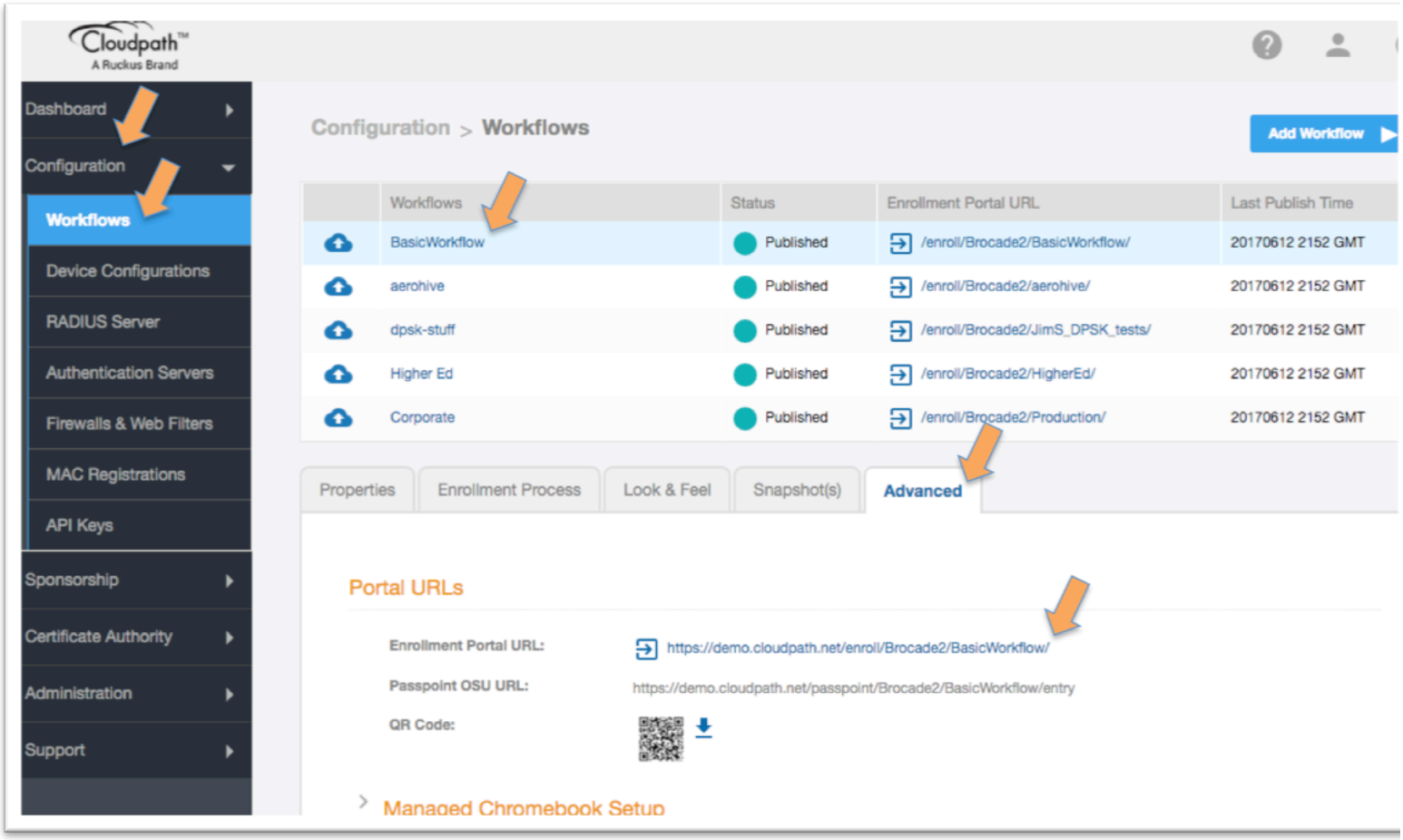
Guest users can connect to the open SSID, choose to register as a guest, and their device will be uniquely registered by its MAC address. The portal will open up (the walled garden will open) and they will be granted Internet access.

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”.

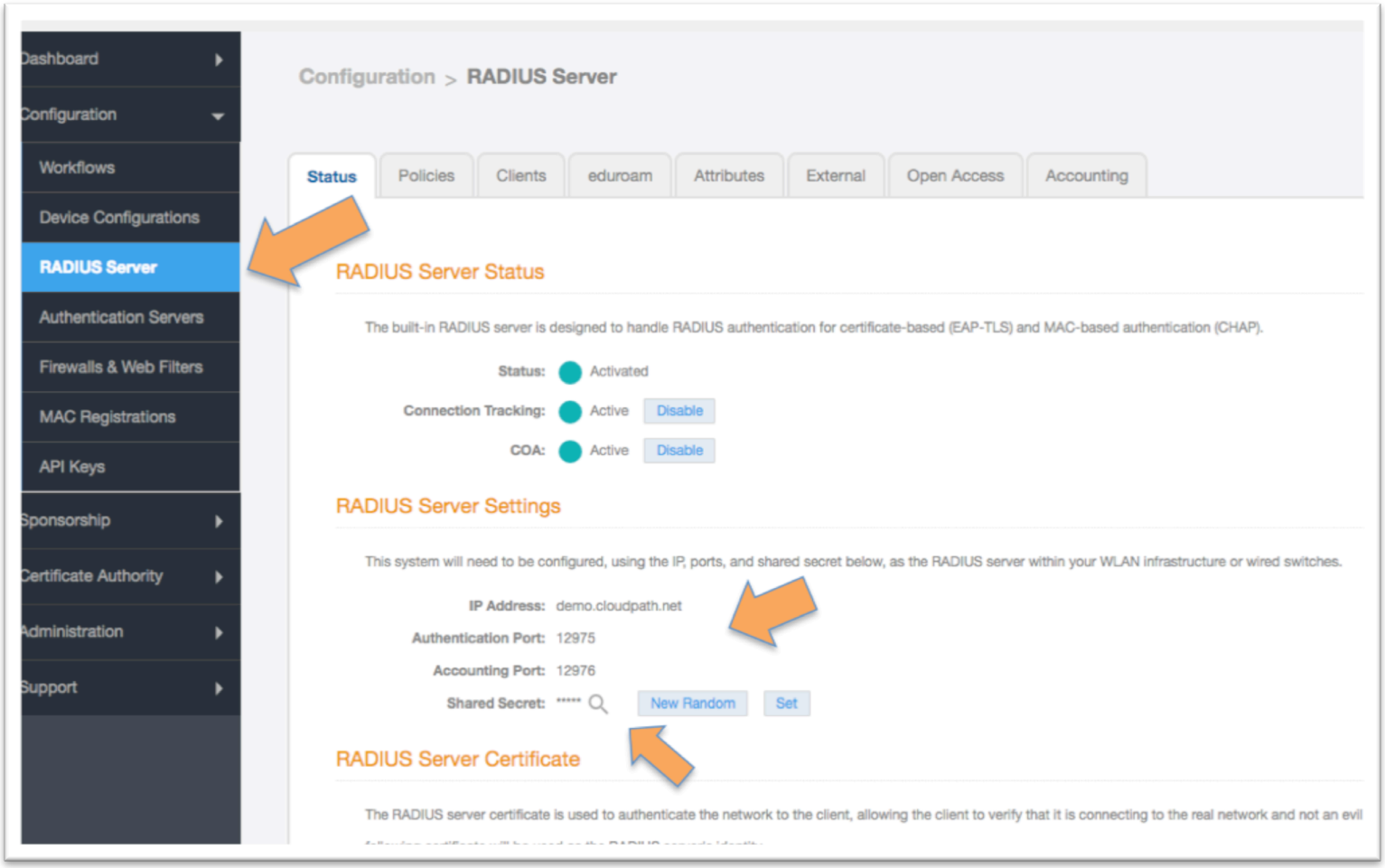
Onboarding and Secure WLANs on HiveManager NG

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

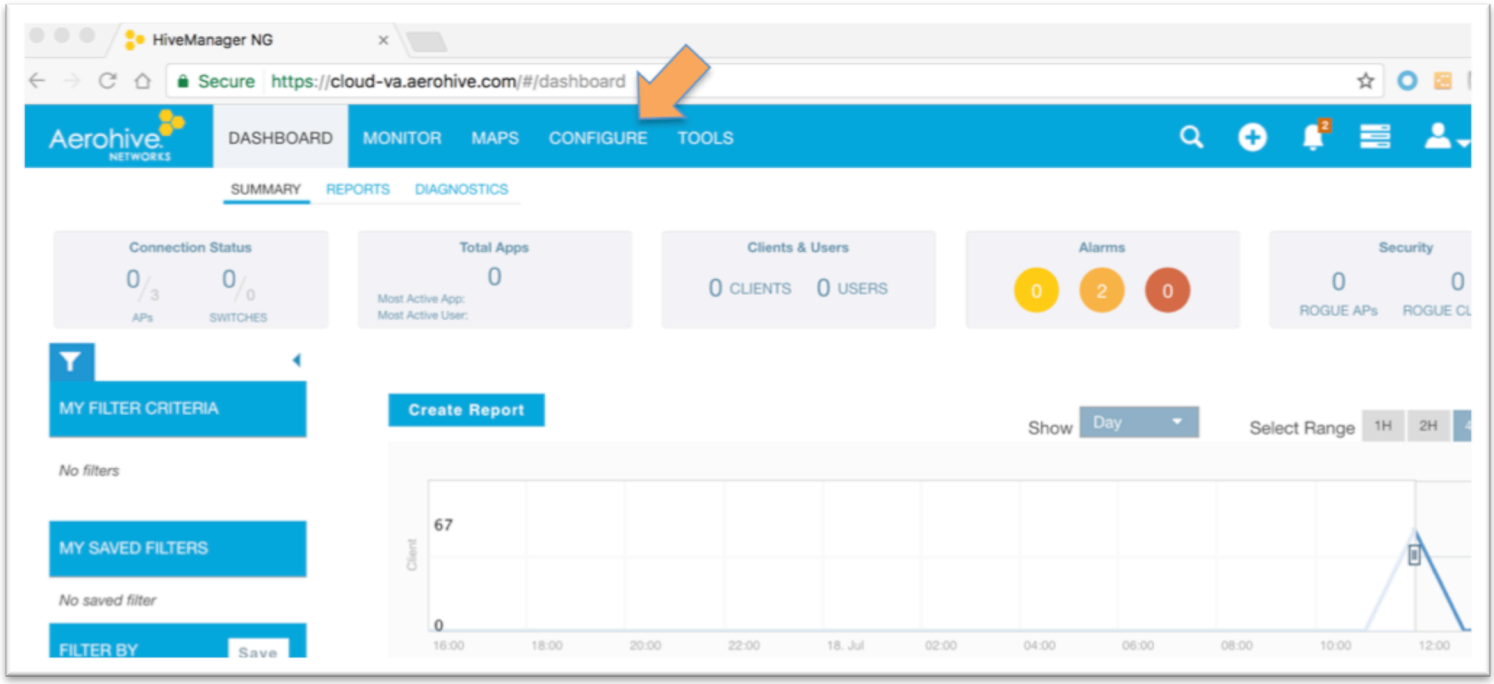


- Login to Cloudpath ES and navigate to:
    - Configuration
    - Workflow
    - Click on the workflow to be deployed
    - Click on the workflow's **Advanced** tab
    - Go to the Enrollment Portal URL.
    - Copy this URL to a text editor for later (or be prepare to return to this window).
      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

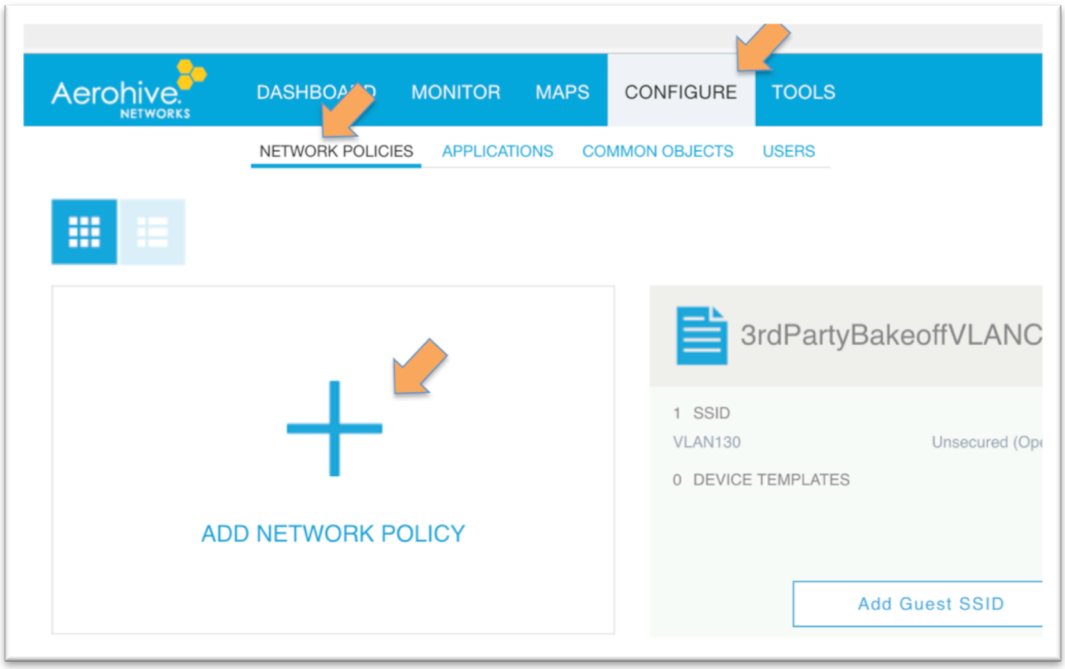


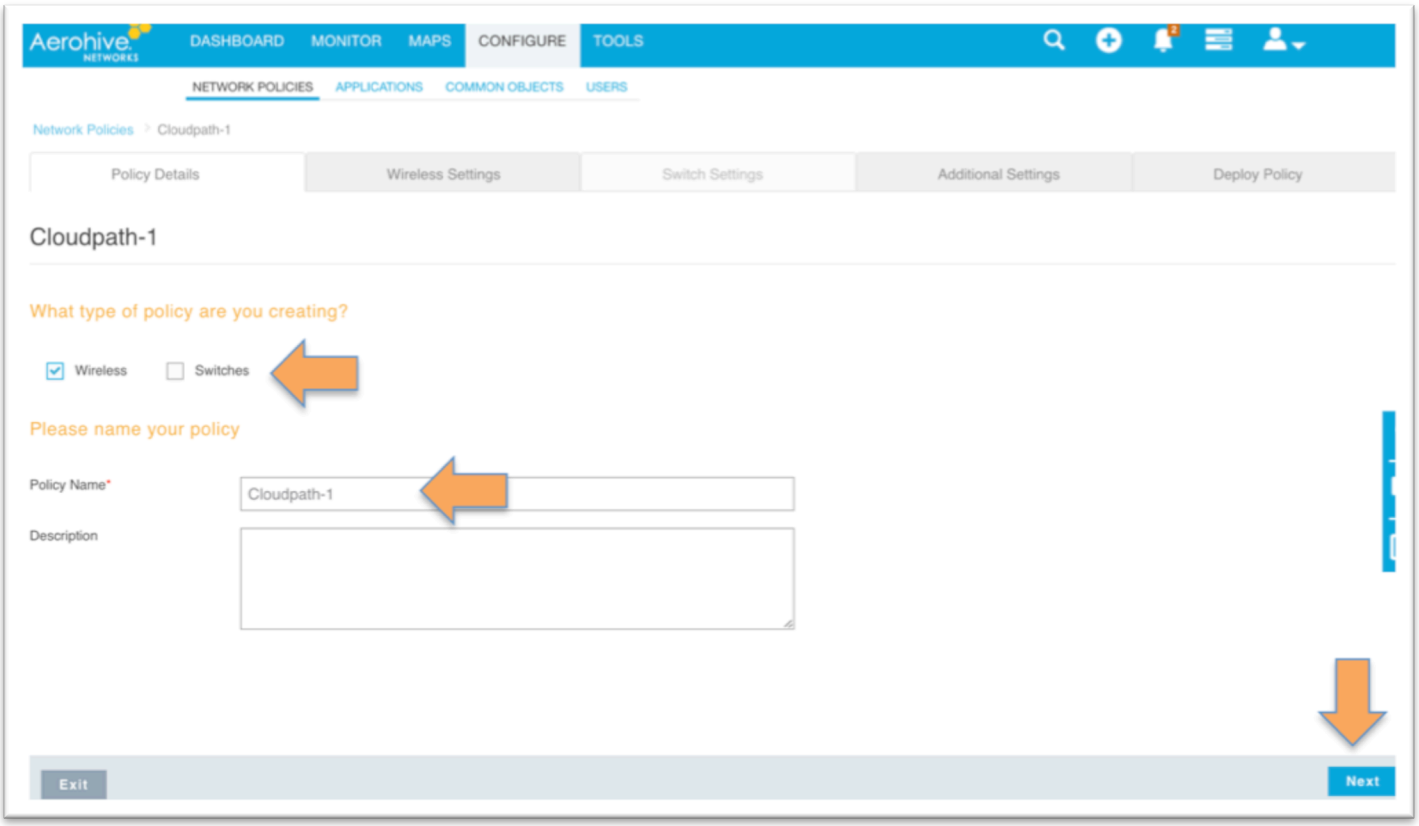
- HiveManager NG will need the RADIUS server settings. On the main menu bar, navigate to **Configuration -> RADIUS Server**. Copy the following information for later
  - The **IP address**
    - *NB - must be an IP address. If necessary, a CLI ping will determine the IP from the FQDN*
  - **Authentication 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



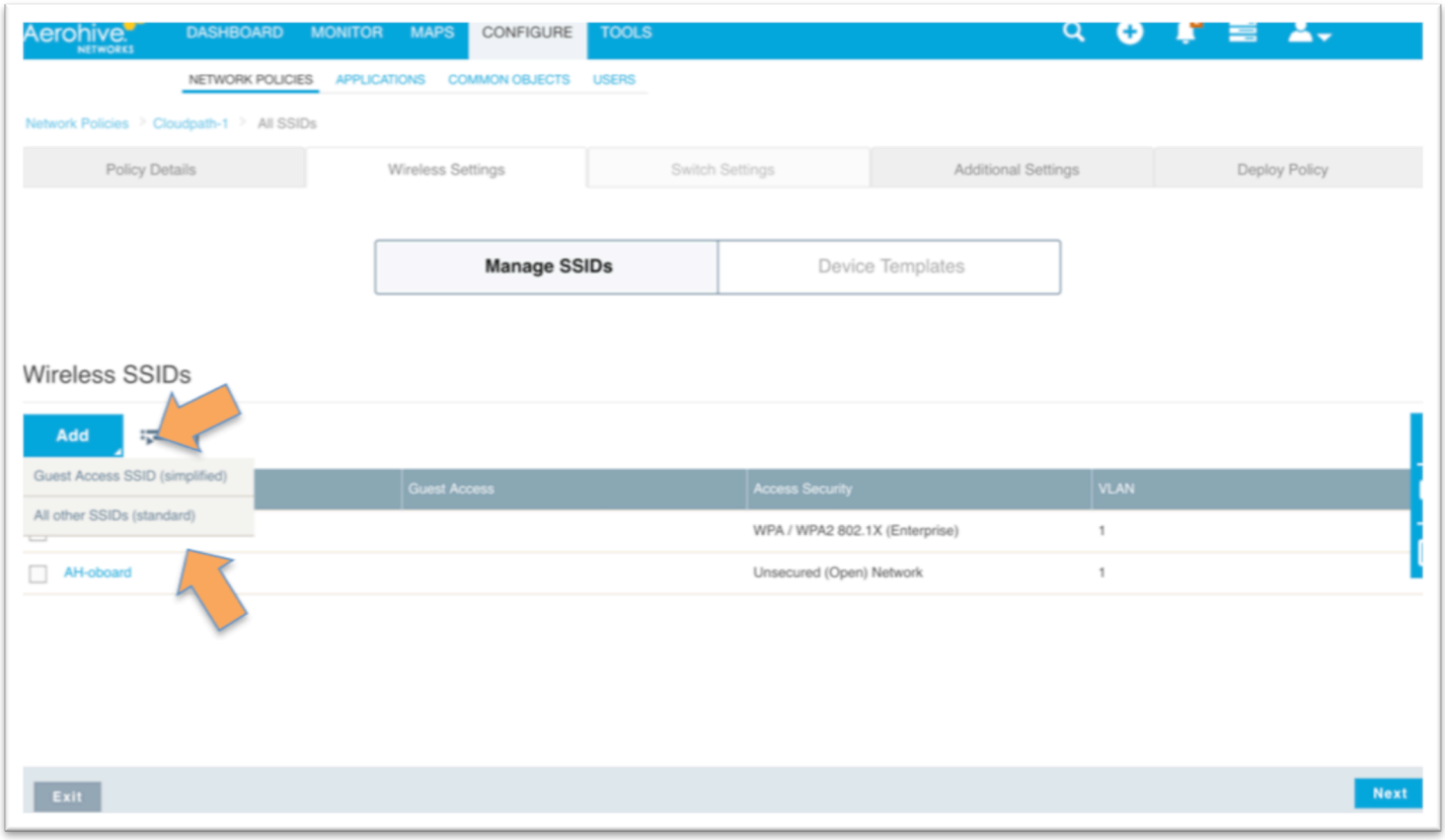
- Login to Hive Manager NG
  - Navigate to **Configure ->Network Policies**
  - Click on **Add Network Policy**



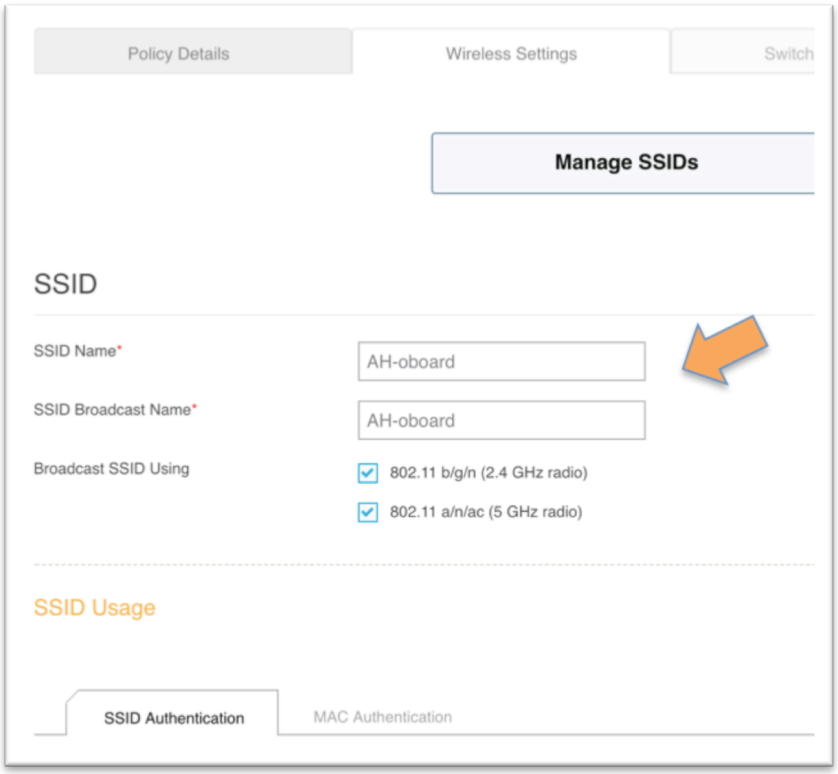


- Check **Wireless** and/or uncheck **Switches**
- Fill in **Policy Name**
- Optionally, add a **Description**
- Click **Next** to save the policy and go on to **Wireless Settings**

3) Add the SSID for the Onboarding Portal

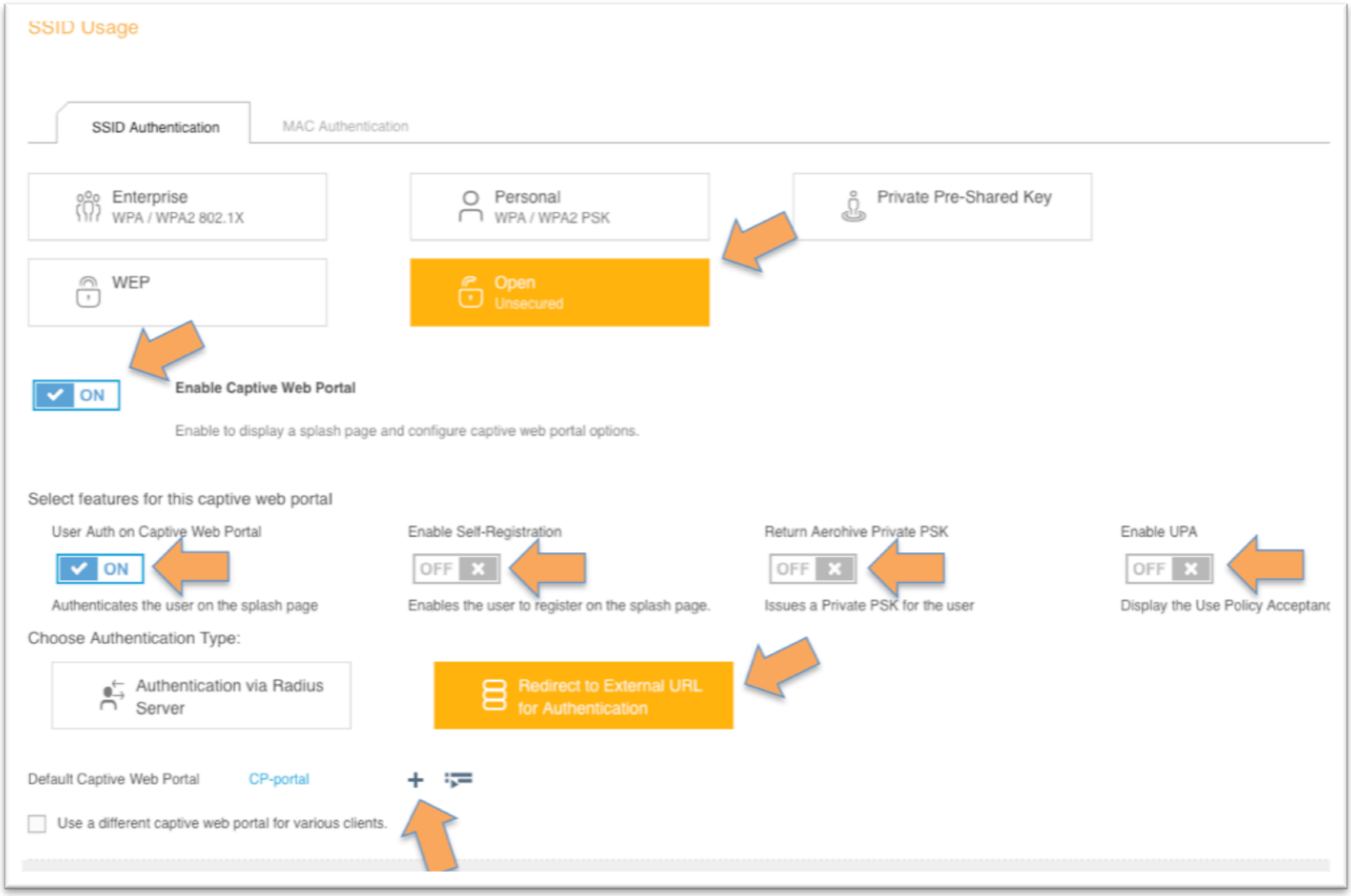


- Under the **Wireless Settings** Tab
- Under **Wireless SSIDs**
- Click **Add**
- Click on **All other SSIDs (standard)**



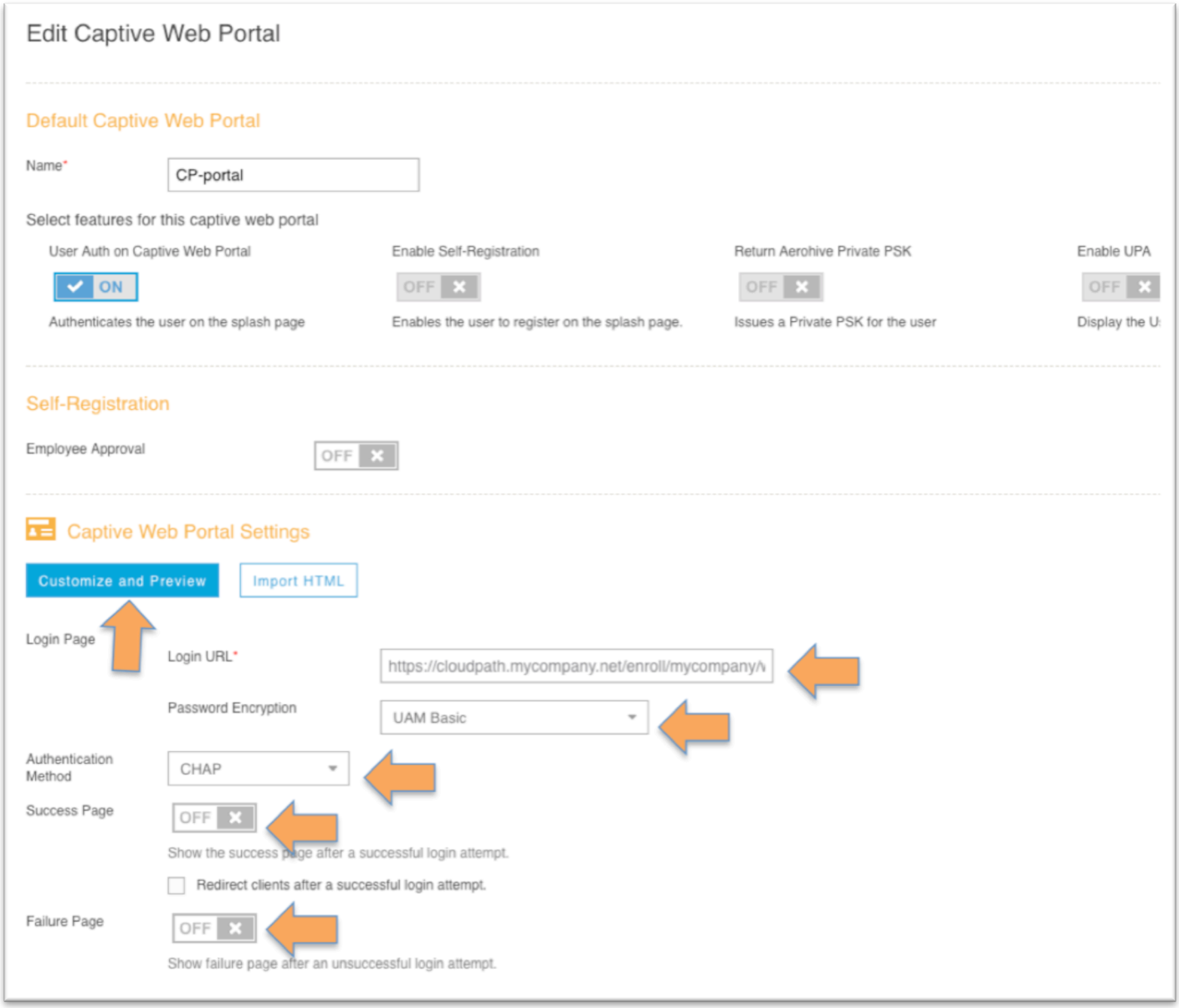
- Fill in **SSID Name** (internal name)
- Fill in the **SSID Broadcast Name**
- Scroll down to **SSID Usage**

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



- 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*

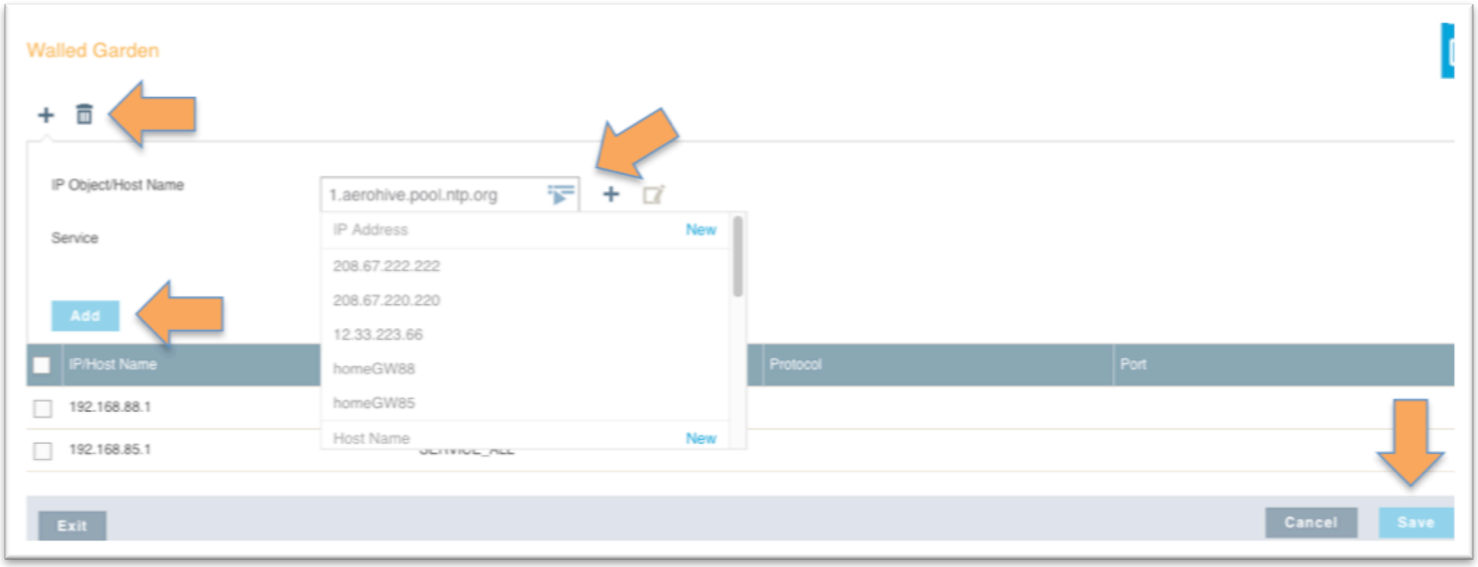
4) Configure the Captive Web Portal with the Cloudpath Enrollment URL



- **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

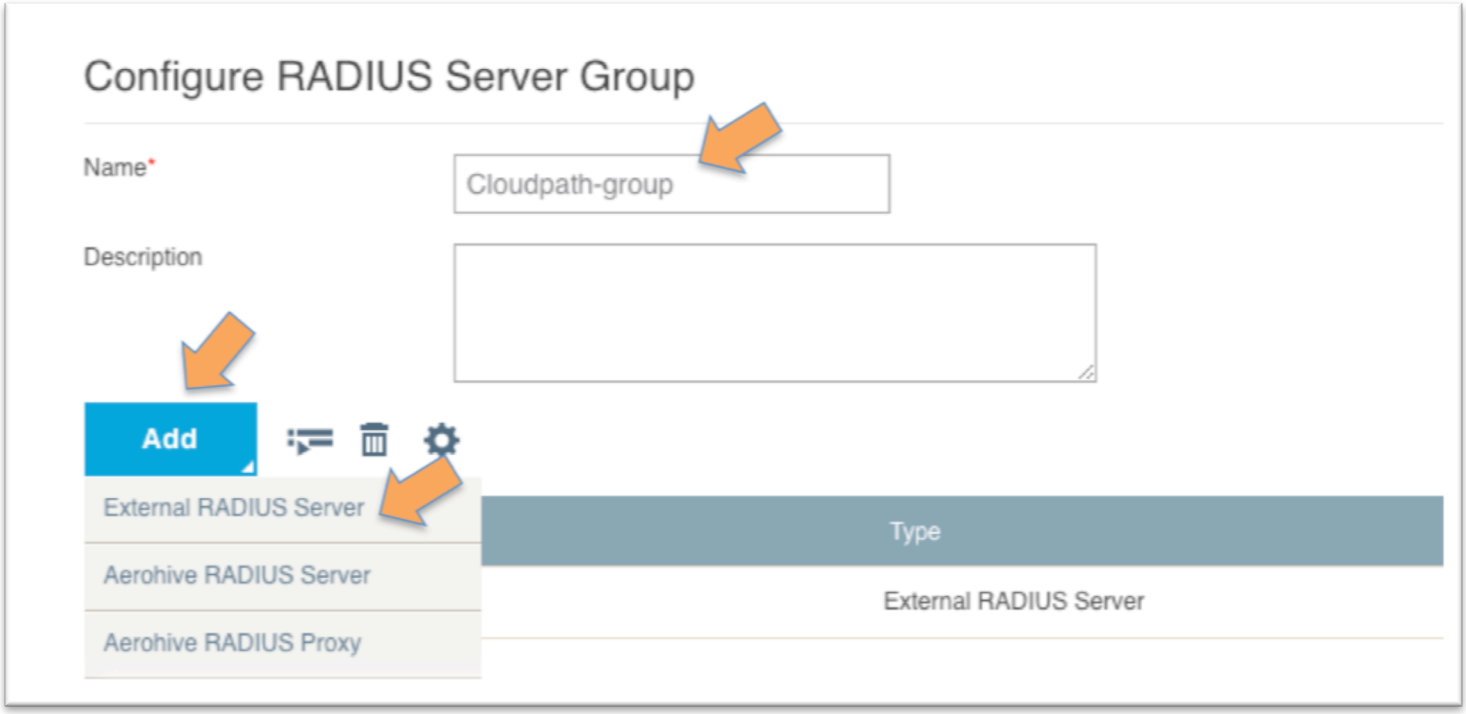
Scroll to the bottom of the **New/Edit Captive Web Portal** page



- **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

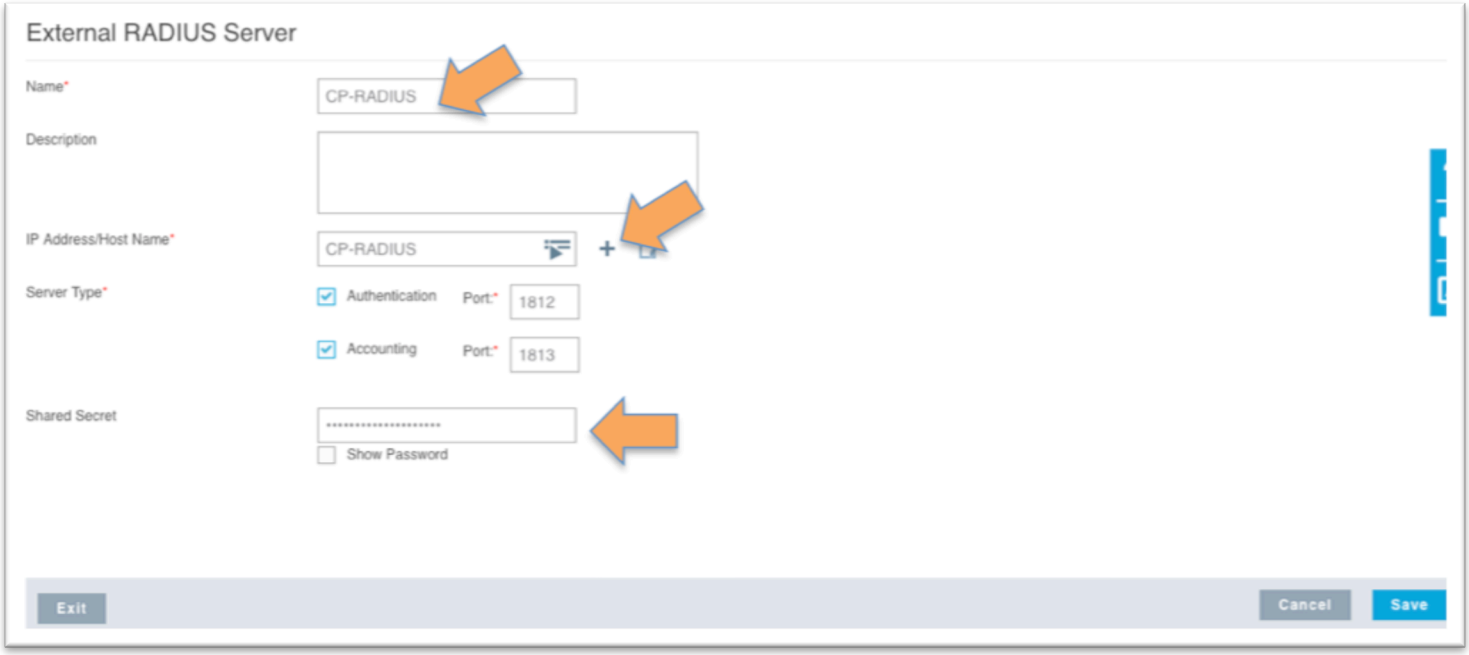
6) Add Cloudpath ES RADIUS Server to Portal SSID

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

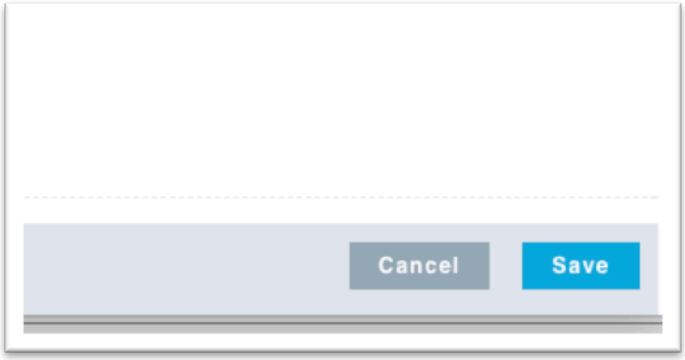


- Give the group a **Name**

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



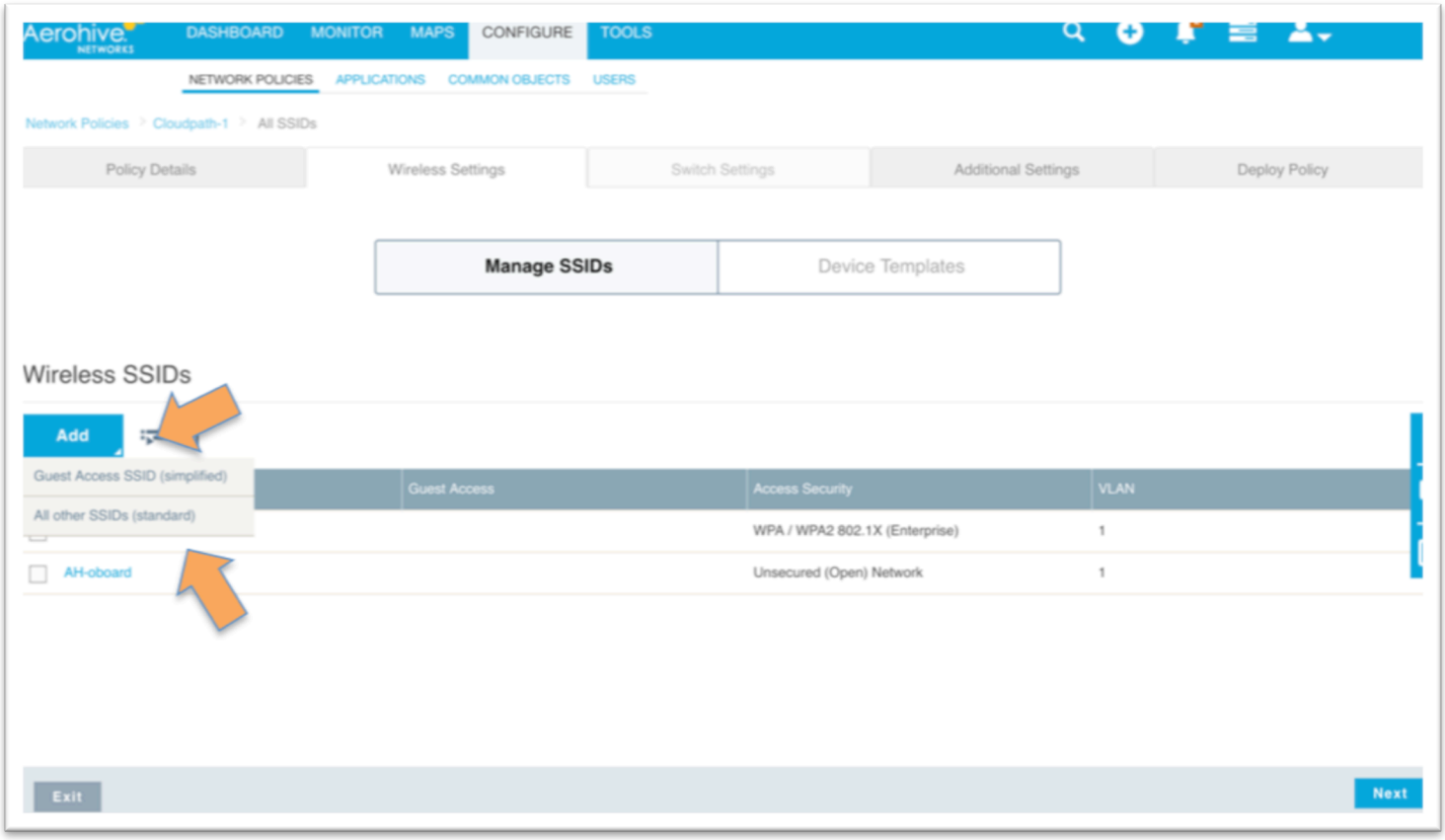
- In the **External RADIUS Server** window, enter the values for the Cloudpath RADIUS server from section 1
  - Give it a **Name**
  - At **IP Address/Hostname** use the **+** to add the **IP address**
  - At **Server Type**, assign the Authentication and Accounting **ports**
  - Enter the **Shared Secret**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



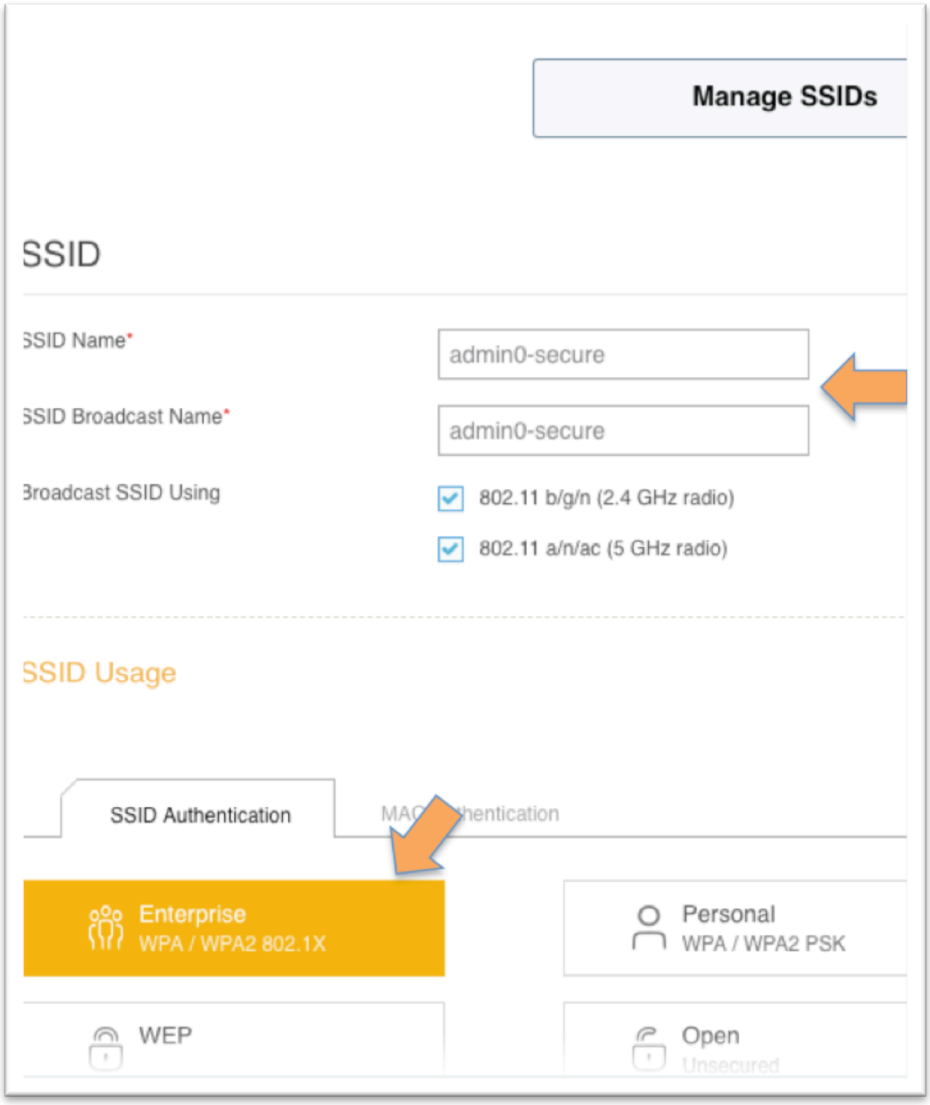
- **Save** - Under the main SSID configuration page, use the lower right side **Save** button to save all the SSID settings

7) Create the Secure WLAN

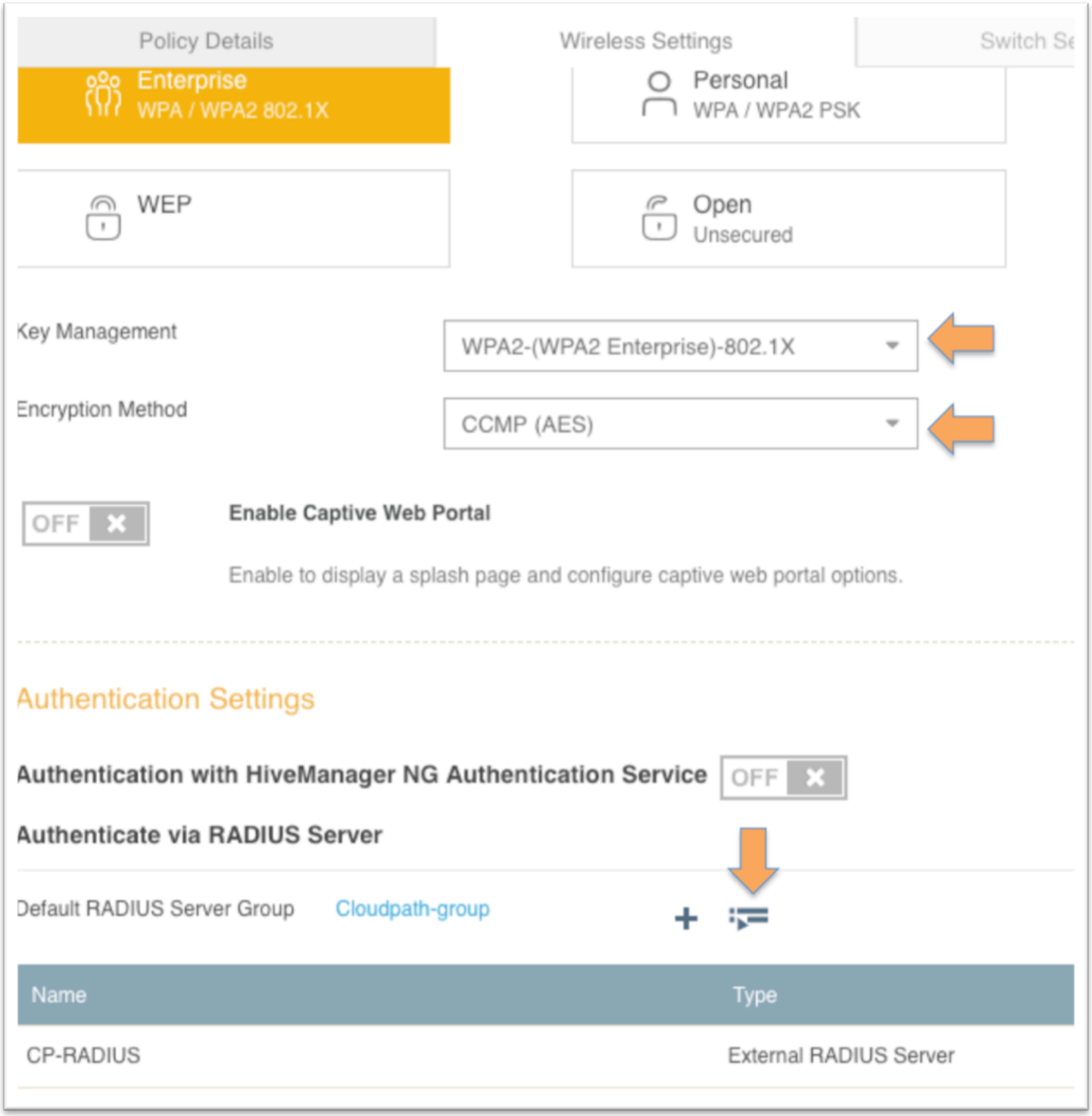
This is the secure SSID for registered users and their devices



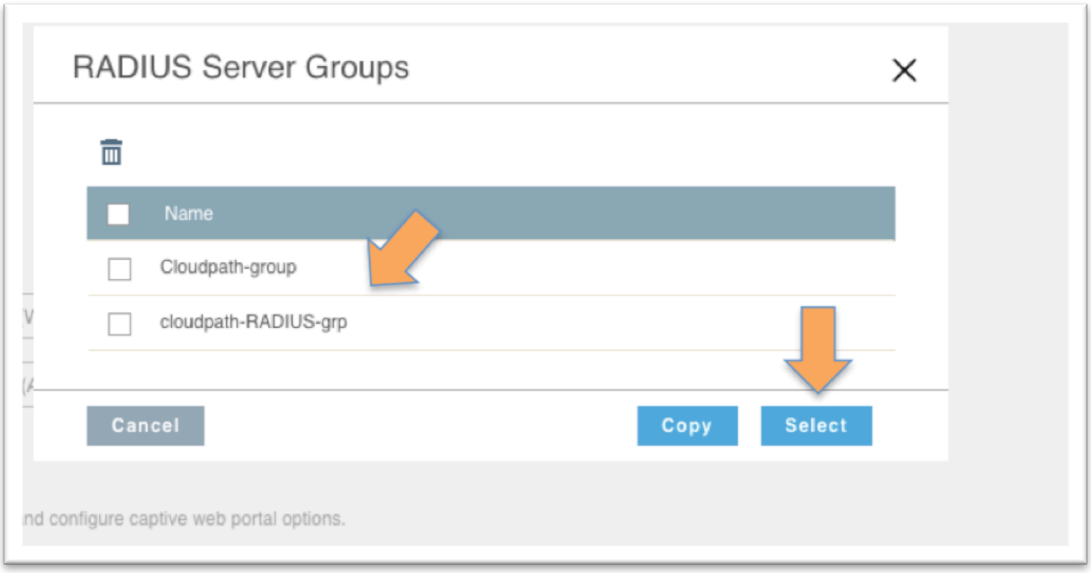
- Create onother SSID in **Wireless Settings** -> **Wireless SSIDs**
  - Click the **Add** button
  - Choose **All Other SSIDs (standard)**

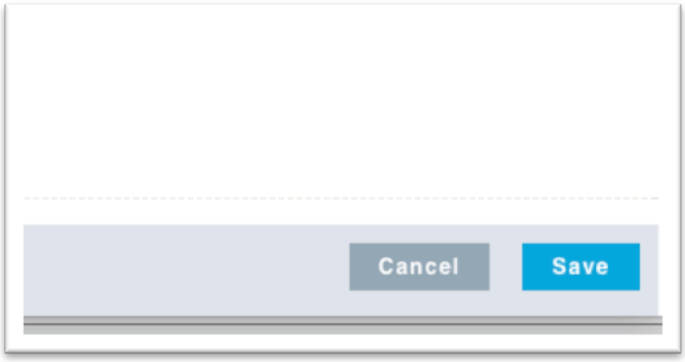


- **Name** the SSID and give it a **Broadcast Name**
- Under **SSID Usage**, click **Enterprise WPA/WPA2 802.1X**
- For **Key Management** choose **WPA2-(WPS2 Enterprise)-802.1X**
- For **Encryption Method** choose **CCMP(AES)**



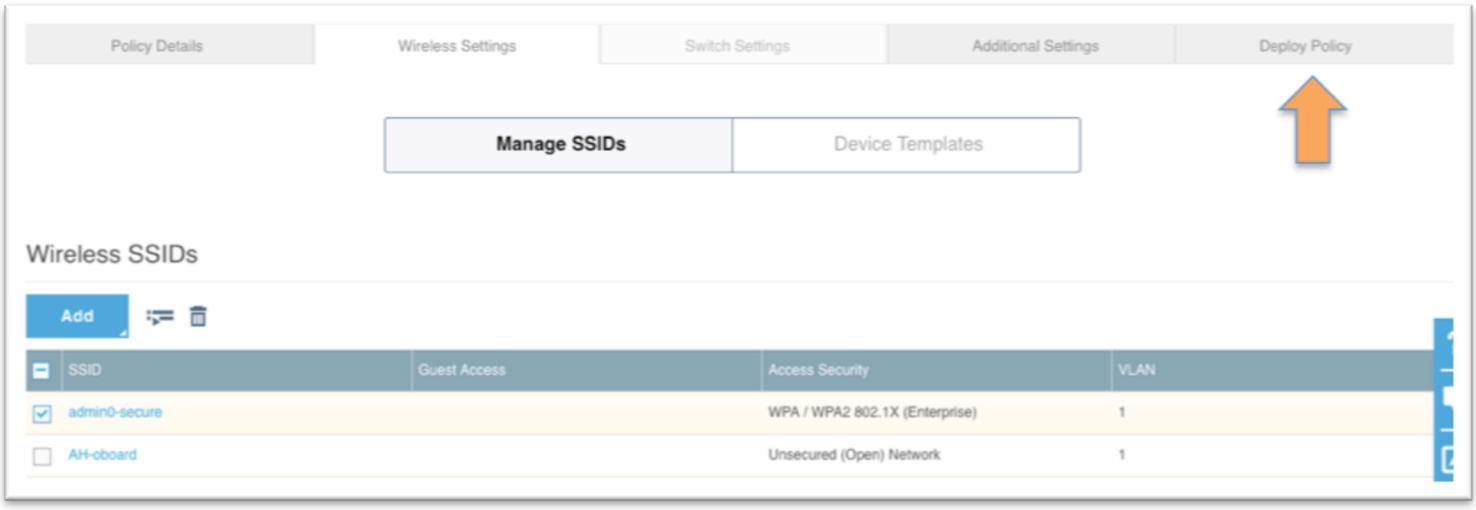
- Under **Authentication Settings** -> Au**thenticate via RADIUS server**,
  - use the **selection box** to choose the previously defined **RADIUS Server Group** that matches the *Cloudpath ES RADIUS Server*



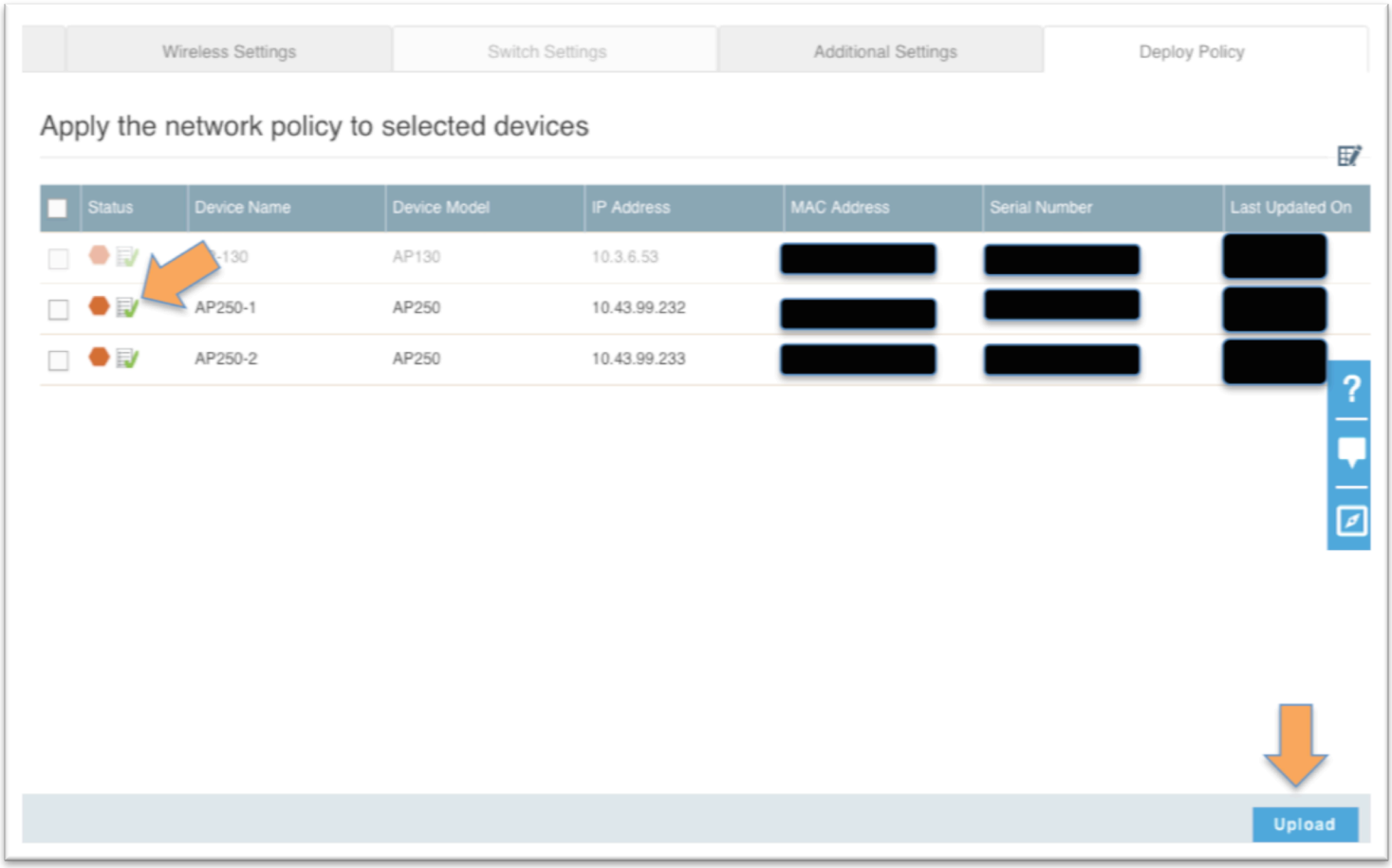


- Use the lower right side **Save** button to save all the SSID settings

8) Deploy the Network Policy



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



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

Configuration is done and ready to test.

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.

Cloudpath On Aerohive

Deploying a Cloudpath workflow on an Aerohive Cloud Controller

August 2017