
Simply Better Connections

Building a Basic Workflow in Cloudpath ES

Onboarding of secure users with MAC authentication passthrough for guests

Best Practices and Deployment Guide

Cloudpath Basic Workflow

Onboarding secure users with MAC authentication of guests

August 2017

Table of Contents

This table of contents can be used as a checklist.

Cloudpath Basic Workflow

Onboarding secure users with MAC authentication of guests

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 configuration of a Cloudpath workflow (or registration portal), for deployment on a 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 an installation guide for Cloudpath ES or for WLAN controllers.

Cloudpath ES server should already be fully deployed and accessible, locally or as a cloud system. An external database of users should be available.* After configuring the Cloudpath ES workflow, this workflow can be deployed on a WLAN controller. Use the vendor's documentation to deploy the specific WLAN controller you will use. Once the controller is deployed with at least one AP connected to it, see the appropriate Best Practices and Deployment Guide to configure it to use the Cloudpath workflow(s) 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

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.

The Basic Workflow (this document)

This document outlines a 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 portal and does double duty as employee registration and as guest access. Secure users (e.g. employees) initially register their devices and download a certificate on the open SSID. This is a one-time process for each employee device. 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/walled garden will open up and they will be granted Internet access.

This document is designed to create a simple but effective workflow that can be built on for many other use cases. Look for this documents for a complete configuration solution guide.

After completing this document, Cloudpath should be deployed on a WLAN controller. The two WLANs must be defined on the AP controller. The 802.1X secured SSID must refer to the Cloudpath RADIUS server, while the open SSID must point at the Cloudpath workflow URL as a WISPr portal.

See the corresponding cookbook for deploying a workflow on a WLAN controller by vendor.

Cloudpath Basic Workflow

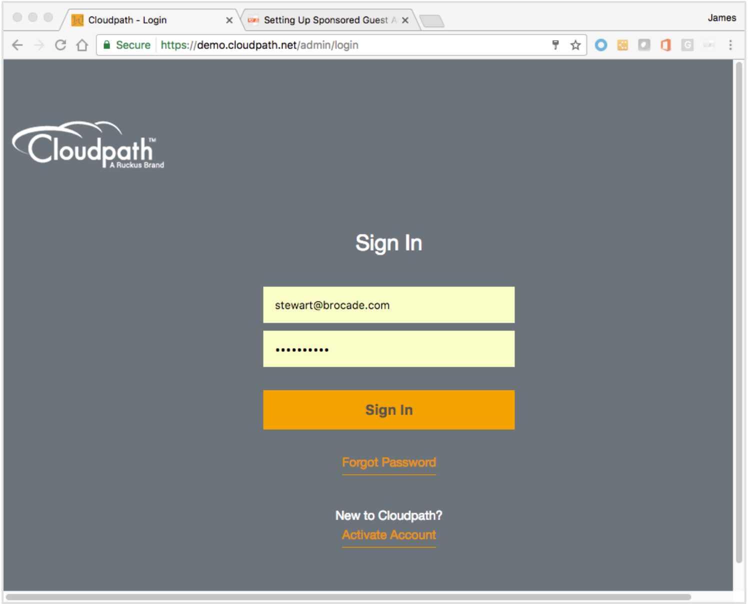
Onboarding secure users with MAC authentication of guests

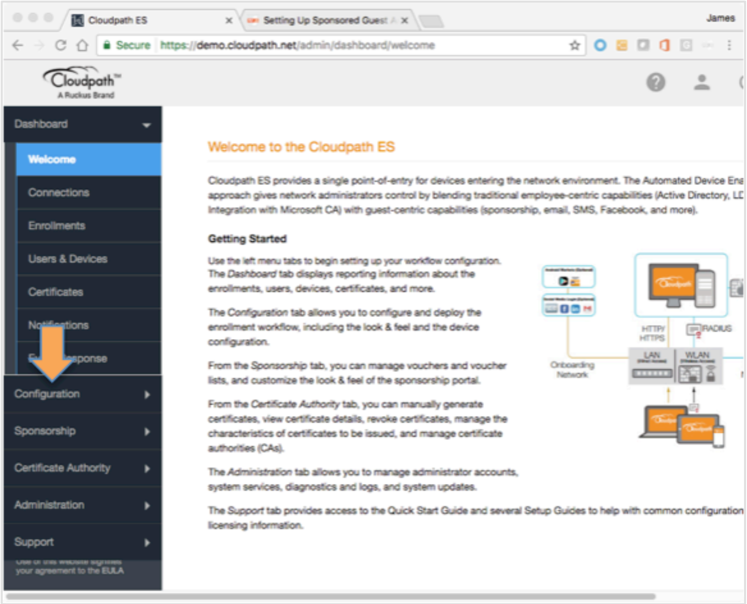
August 2017

Secure User Registration and Guest MAC-Auth Pass Through

1) Login to Cloudpath ES

It should present a welcome screen. If instead it presents a certificate signe request, it should be fine to skip it for now. However, you will want to double check your deployment for a signed public certificate. See the deployment guides.





Welcome to the Cloudpath ES

Cloudpath ES provides a single point-of-entry for devices entering the network environment. The Automated Device Ena approach gives network administrators control by blending traditional employee-centric capabilities (Active Directory, LD Integration with Microsoft CA) with guest-centric capabilities (sponsorship, email, SMS, Facebook, and more).

Getting Started

Use the left menu tabs to begin setting up your workflow configuration. The *Dashboard* tab displays reporting information about the enrollments, users, devices, certificates, and more.

The *Configuration* tab allows you to configure and deploy the enrollment workflow, including the look & feel and the device configuration.

From the *Sponsorship* tab, you can manage vouchers and voucher lists, and customize the look & feel of the sponsorship portal.

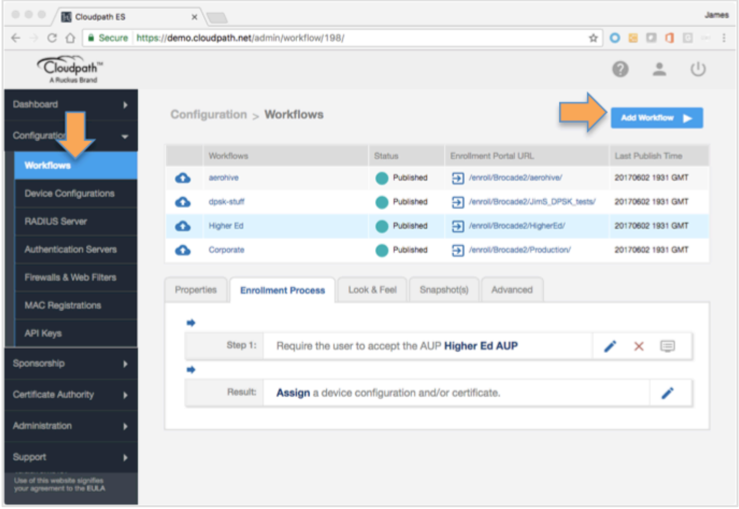
From the *Certificate Authority* tab, you can manually generate certificates, view certificate details, revoke certificates, manage the characteristics of certificates to be issued, and manage certificate authorities (CAs).

The *Administration* tab allows you to manage administrator accounts, system services, diagnostics and logs, and system updates.

The *Support* tab provides access to the Quick Start Guide and several Setup Guides to help with common configuration licensing information.

2) Add a New Workflow

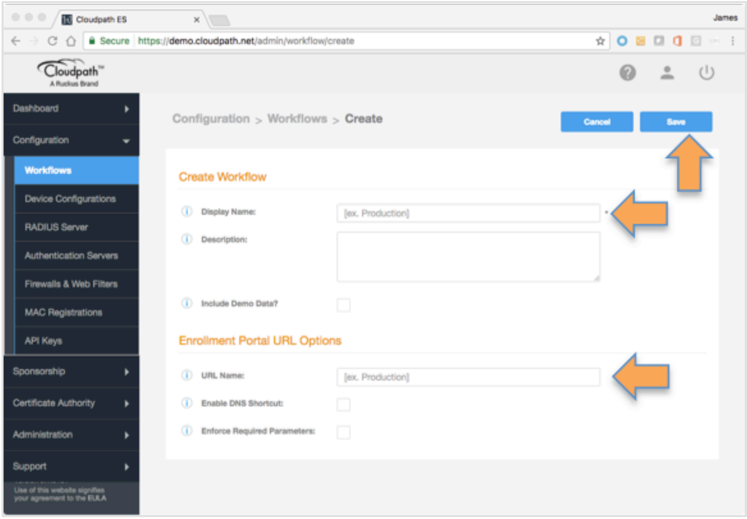
On the left menu, click on "Configuration" to expand the menu, click on "Workflows" then in the upper right, click the "add workflow" button



Workflows	Status	Enrollment Portal URL	Last Publish Time
aerohive	Published	/enroll/Brocade2/aerohive/	20170602 1931 GMT
dpsk-stuff	Published	/enroll/Brocade2/JimS_DPSK_tests/	20170602 1931 GMT
Higher Ed	Published	/enroll/Brocade2/HigherEd/	20170602 1931 GMT
Corporate	Published	/enroll/Brocade2/Production/	20170602 1931 GMT

Step 1: Require the user to accept the AUP **Higher Ed AUP**

Result: **Assign** a device configuration and/or certificate.



Create Workflow

Display Name: [ex. Production] *

Description:

Include Demo Data? □

Enrollment Portal URL Options

URL Name: [ex. Production]

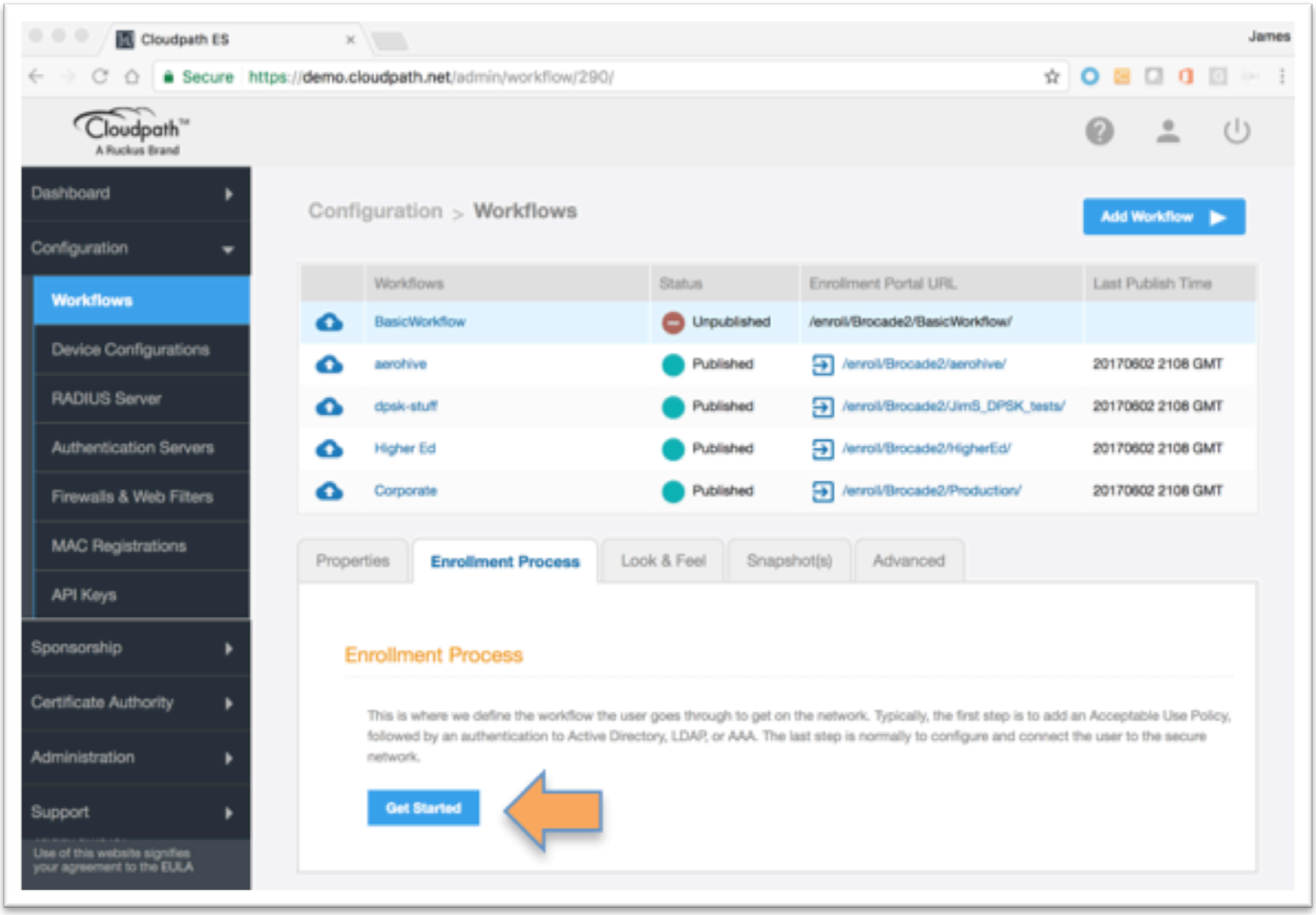
Enable DNS Shortcut: □

Enforce Required Parameters: □

3) Workflow name and URL

Give the workflow an internal name, and a URL name

- Fill in the display name. This is an internal name in Cloudpath
- Fill in the URL name. This name will become part of the URL for the registration portal and so needs to be URL friendly. Both names can match.
- For instance "BasicWorkFlow" will yield a URL something like: https://demo.cloudpath.net/enroll/Brocade2/BasicWorkflow/
- This is the URL of the eventual enrollment portal. Cloudpath ES includes an apache webserver and will host the html pages that will be created when the workflow is published.
- Click "Save" in the upper right



	Workflows	Status	Enrollment Portal URL	Last Publish Time
	BasicWorkflow	Unpublished	/enroll/Brocade2/BasicWorkflow/	
	aerohive	Published	/enroll/Brocade2/aerohive/	20170602 2108 GMT
	dpsk-stuff	Published	/enroll/Brocade2/JimS_DPSK_tests/	20170602 2108 GMT
	Higher Ed	Published	/enroll/Brocade2/HigherEd/	20170602 2108 GMT
	Corporate	Published	/enroll/Brocade2/Production/	20170602 2108 GMT

Enrollment Process

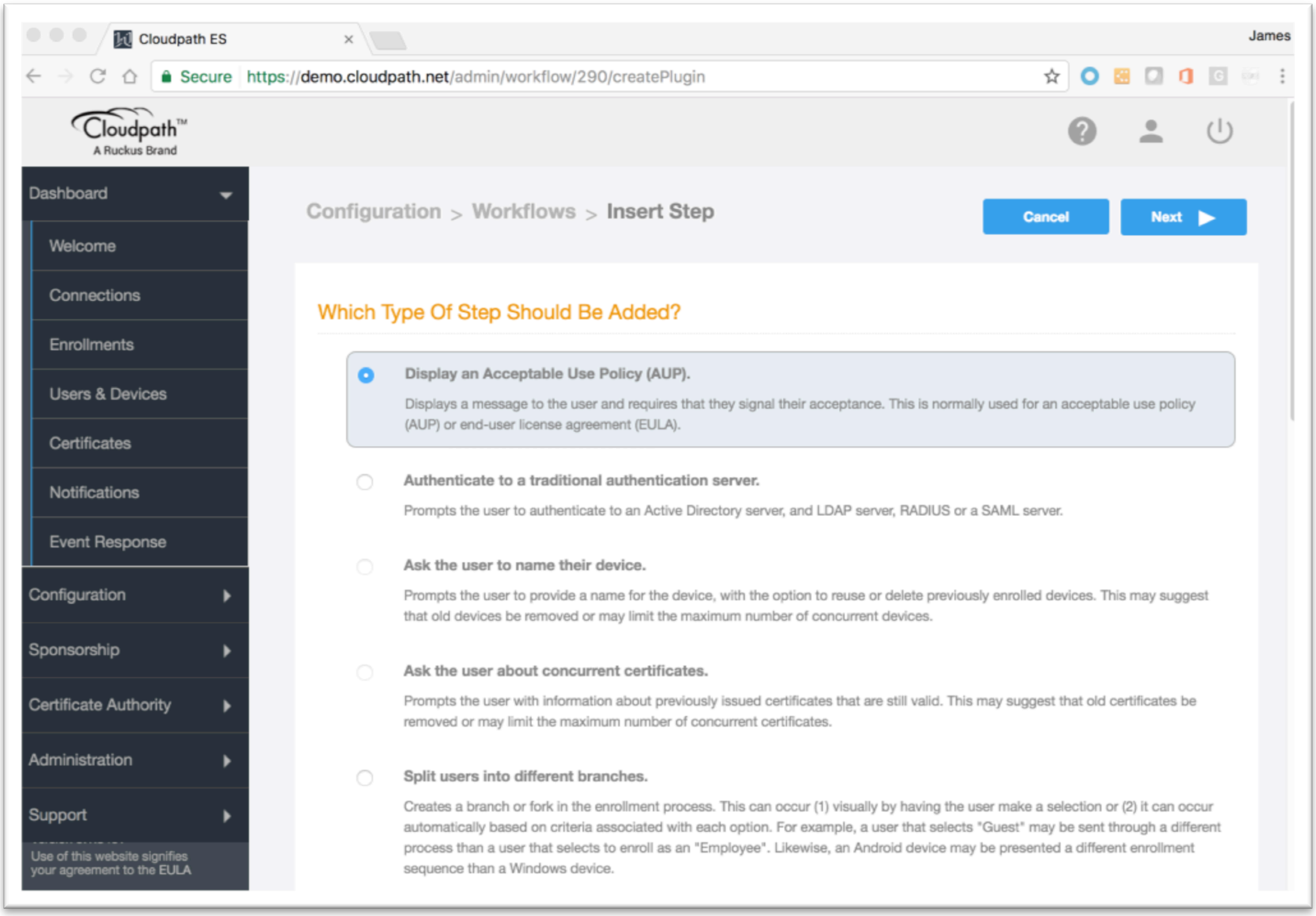
This is where we define the workflow the user goes through to get on the network. Typically, the first step is to add an Acceptable Use Policy, followed by an authentication to Active Directory, LDAP, or AAA. The last step is normally to configure and connect the user to the secure network.

4) Enrollment Process -> Get started

- The new workflow is highlighted in the list of workflows, and open to the enrollment process tab.
- The other tabs:
    - *Properties* holds the "create" information – internal name and URL identifier
    - *Look and Feel*: options for customizing the resulting web pages
    - *Snapshot(s):* as you modify and republish the workflow, snapshots enable you to fall back to earlier versions
    - *Advanced:* Specialized URL variations, QR code, and workflow cleanup/deletion
- On the Enrollment Process tab, click "Get Started"

5) Add an Acceptable Use Policy (AUP)

The first step – add an Acceptable Use Policy (AUP)


Cloudpath ES
James
Secure https://demo.cloudpath.net/admin/workflow/290/createPlugin
Cloudpath™ A Ruckus Brand
Dashboard
Welcome
Connections
Enrollments
Users & Devices
Certificates
Notifications
Event Response
Configuration
Sponsorship
Certificate Authority
Administration
Support
Use of this website signifies your agreement to the EULA
Configuration > Workflows > Insert Step
Cancel
Next

Which Type Of Step Should Be Added?

● **Display an Acceptable Use Policy (AUP).**
Displays a message to the user and requires that they signal their acceptance. This is normally used for an acceptable use policy (AUP) or end-user license agreement (EULA).

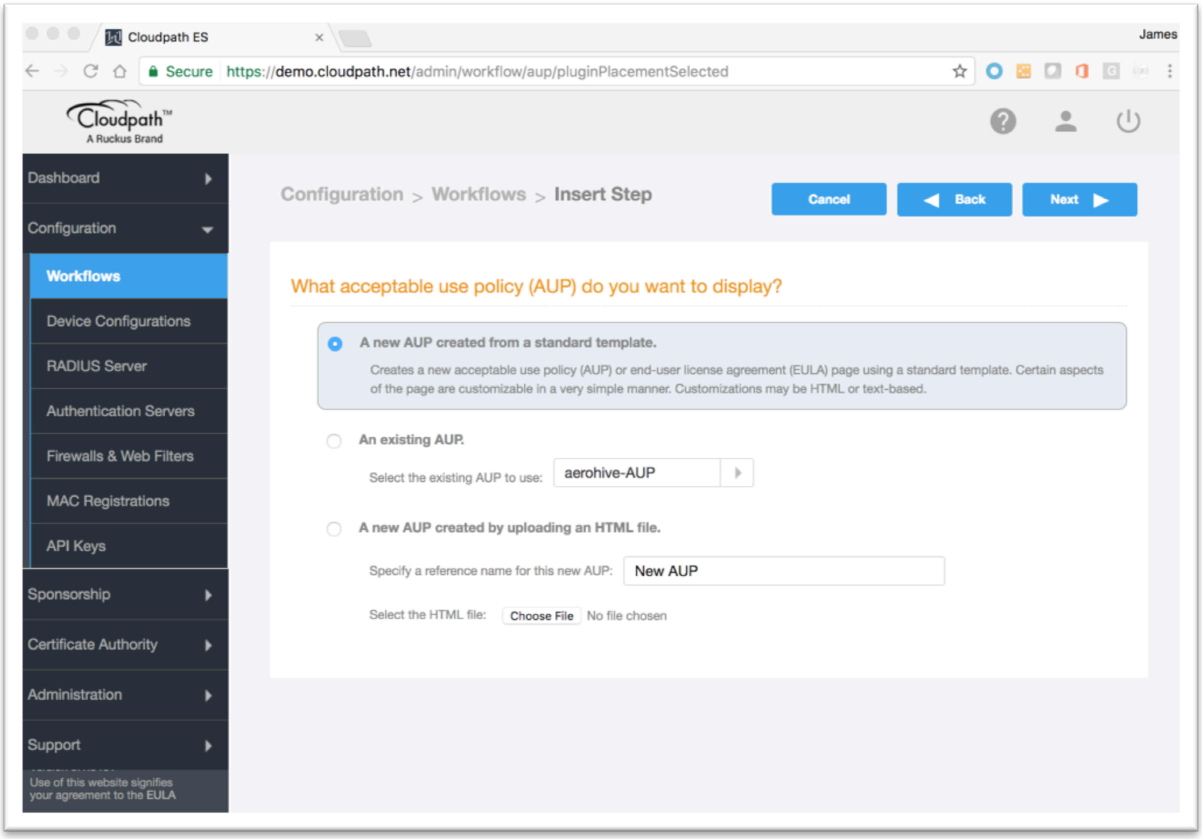
○ **Authenticate to a traditional authentication server.**
Prompts the user to authenticate to an Active Directory server, and LDAP server, RADIUS or a SAML server.

○ **Ask the user to name their device.**
Prompts the user to provide a name for the device, with the option to reuse or delete previously enrolled devices. This may suggest that old devices be removed or may limit the maximum number of concurrent devices.

○ **Ask the user about concurrent certificates.**
Prompts the user with information about previously issued certificates that are still valid. This may suggest that old certificates be removed or may limit the maximum number of concurrent certificates.

○ **Split users into different branches.**
Creates a branch or fork in the enrollment process. This can occur (1) visually by having the user make a selection or (2) it can occur automatically based on criteria associated with each option. For example, a user that selects "Guest" may be sent through a different process than a user that selects to enroll as an "Employee". Likewise, an Android device may be presented a different enrollment sequence than a Windows device.

- The Insert Step screen has over a dozen possible steps. Only a few will be used in this workflow.
- Choose the top/default option: "Display an Acceptable Use Policy (AUP)" and click Next".



What acceptable use policy (AUP) do you want to display?

● A new AUP created from a standard template.

Creates a new acceptable use policy (AUP) or end-user license agreement (EULA) page using a standard template. Certain aspects of the page are customizable in a very simple manner. Customizations may be HTML or text-based.

○ An existing AUP.

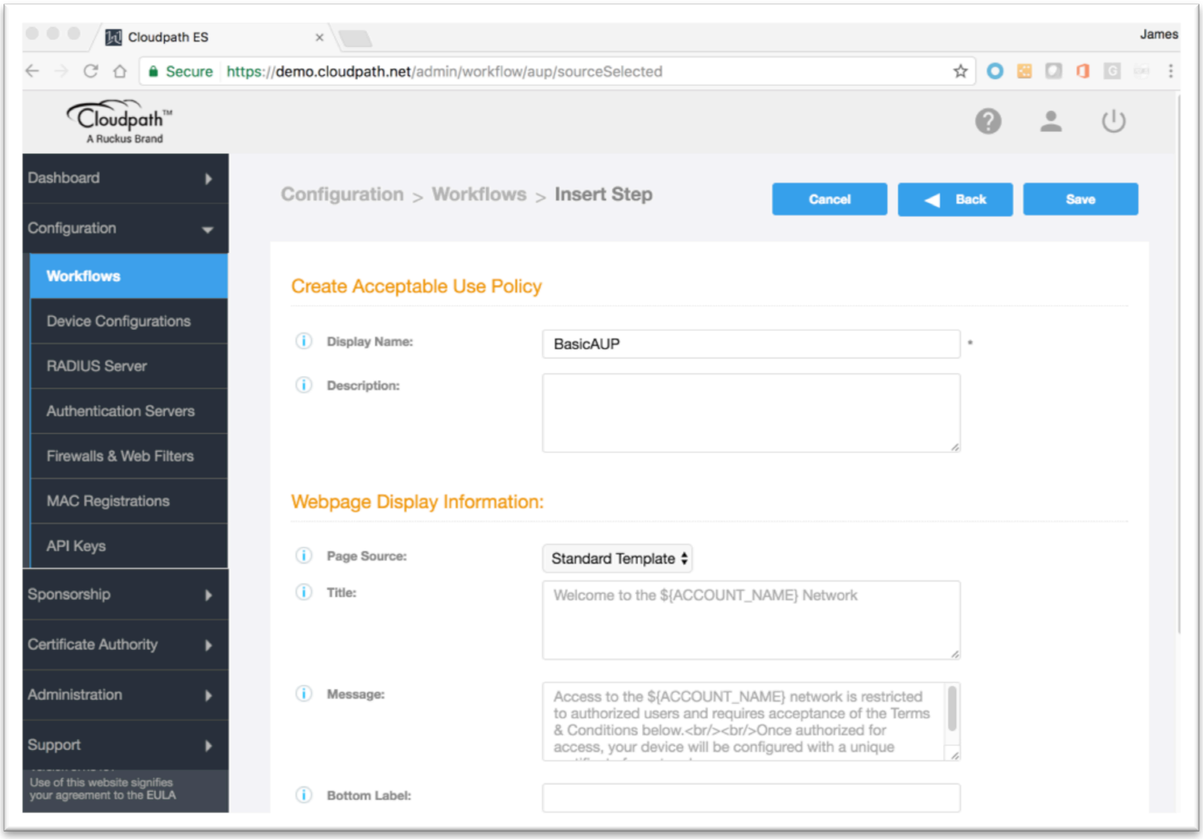
Select the existing AUP to use: aerohive-AUP

○ A new AUP created by uploading an HTML file.

Specify a reference name for this new AUP: New AUP

Select the HTML file: Choose File No file chosen

- On the next screen, choose "A new AUP created from a standard template" and click "Next".
- There are options to reuse or customize the HTML of the AUP. Leave these for a later time.



Create Acceptable Use Policy

Display Name: BasicAUP *

Description:

Webpage Display Information:

Page Source: Standard Template

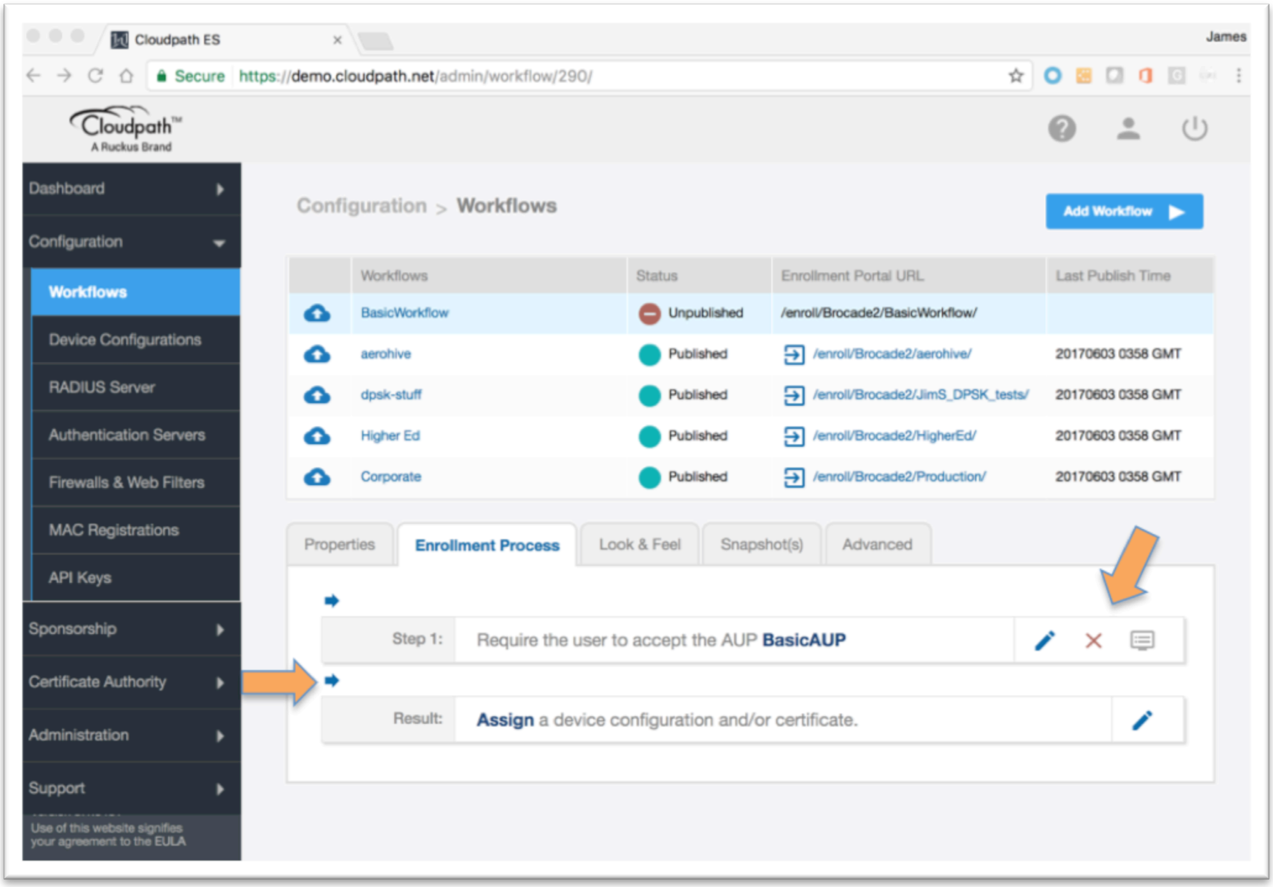
Title: Welcome to the ${ACCOUNT_NAME} Network

Message: Access to the ${ACCOUNT_NAME} network is restricted to authorized users and requires acceptance of the Terms & Conditions below.<br/><br/>Once authorized for access, your device will be configured with a unique

Bottom Label:

- Notice there are multiple customization options available on this page. For now, only give it a unique display name and accept the defaults. Click "Save".

6) Editing a workflow



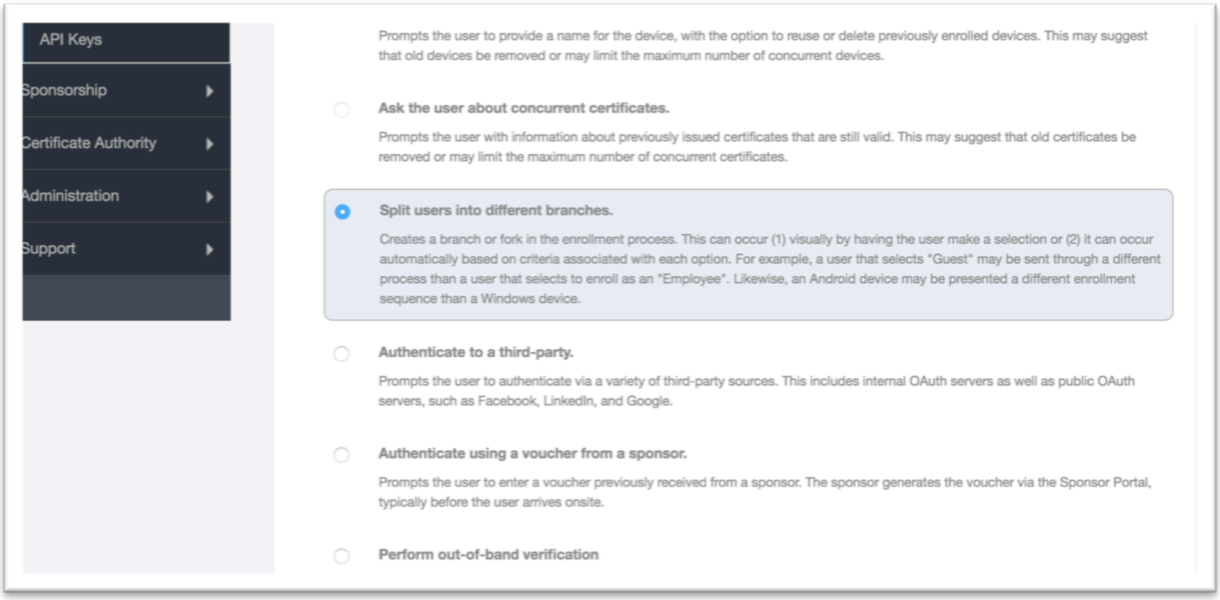
	Workflows	Status	Enrollment Portal URL	Last Publish Time
	BasicWorkflow	Unpublished	/enroll/Brocade2/BasicWorkflow/	
	aerohive	Published	/enroll/Brocade2/aerohive/	20170603 0358 GMT
	dpsk-stuff	Published	/enroll/Brocade2/JimS_DPSK_tests/	20170603 0358 GMT
	Higher Ed	Published	/enroll/Brocade2/HigherEd/	20170603 0358 GMT
	Corporate	Published	/enroll/Brocade2/Production/	20170603 0358 GMT

Step 1: Require the user to accept the AUP **BasicAUP**

Result: **Assign** a device configuration and/or certificate.

- We are back to the workflow screen with a single step enrollment process.
- Steps have 3 editing options on the right of the step
- The pencil will let you edit the step. For an AUP step, you could change the display, text, etc.
- The red **X** will delete the step – but not the AUP, which can be reused.
- The screen icon will display the web page for the step. Use the browser back button to return to the Workflows screen
- The blue arrows on the left of the workflow are used to insert steps. Insert a step between Step 1 and the Result.

7) Split users into different branches – Employees and Guests



Prompts the user to provide a name for the device, with the option to reuse or delete previously enrolled devices. This may suggest that old devices be removed or may limit the maximum number of concurrent devices.

○ **Ask the user about concurrent certificates.**

Prompts the user with information about previously issued certificates that are still valid. This may suggest that old certificates be removed or may limit the maximum number of concurrent certificates.

● **Split users into different branches.**

Creates a branch or fork in the enrollment process. This can occur (1) visually by having the user make a selection or (2) it can occur automatically based on criteria associated with each option. For example, a user that selects "Guest" may be sent through a different process than a user that selects to enroll as an "Employee". Likewise, an Android device may be presented a different enrollment sequence than a Windows device.

○ **Authenticate to a third-party.**

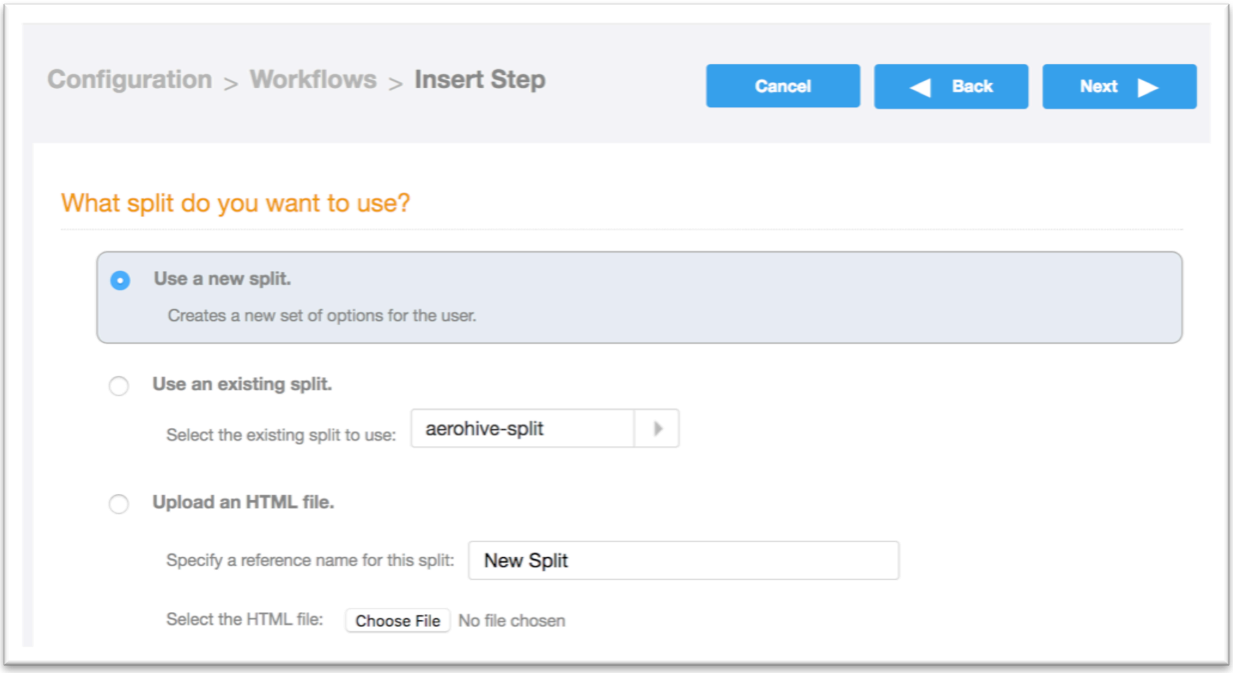
Prompts the user to authenticate via a variety of third-party sources. This includes internal OAuth servers as well as public OAuth servers, such as Facebook, LinkedIn, and Google.

○ **Authenticate using a voucher from a sponsor.**

Prompts the user to enter a voucher previously received from a sponsor. The sponsor generates the voucher via the Sponsor Portal, typically before the user arrives onsite.

○ **Perform out-of-band verification**

- For this step, choose “Split users into different branches and click “Next”.



What split do you want to use?

● **Use a new split.**

Creates a new set of options for the user.

○ **Use an existing split.**

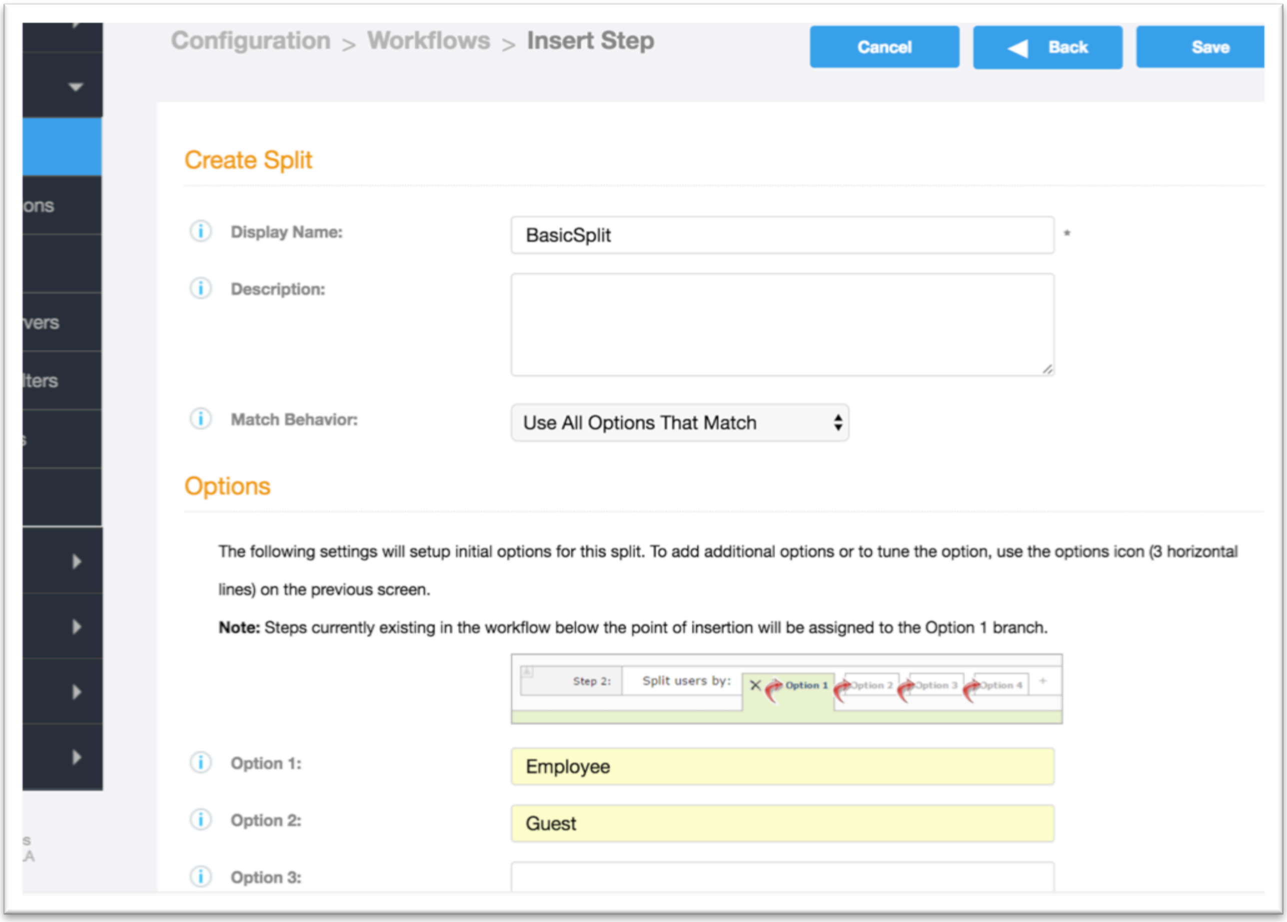
Select the existing split to use: aerohive-split

○ **Upload an HTML file.**

Specify a reference name for this split: New Split

Select the HTML file: Choose File No file chosen

- On the next screen, choose “Use a new split” and click “Next”.
- There are options to reuse or customize the HTML of the split. Leave these for a later time.



Create Split

Display Name: BasicSplit *

Description:

Match Behavior: Use All Options That Match

Options

The following settings will setup initial options for this split. To add additional options or to tune the option, use the options icon (3 horizontal lines) on the previous screen.

Note: Steps currently existing in the workflow below the point of insertion will be assigned to the Option 1 branch.

Option 1: Employee

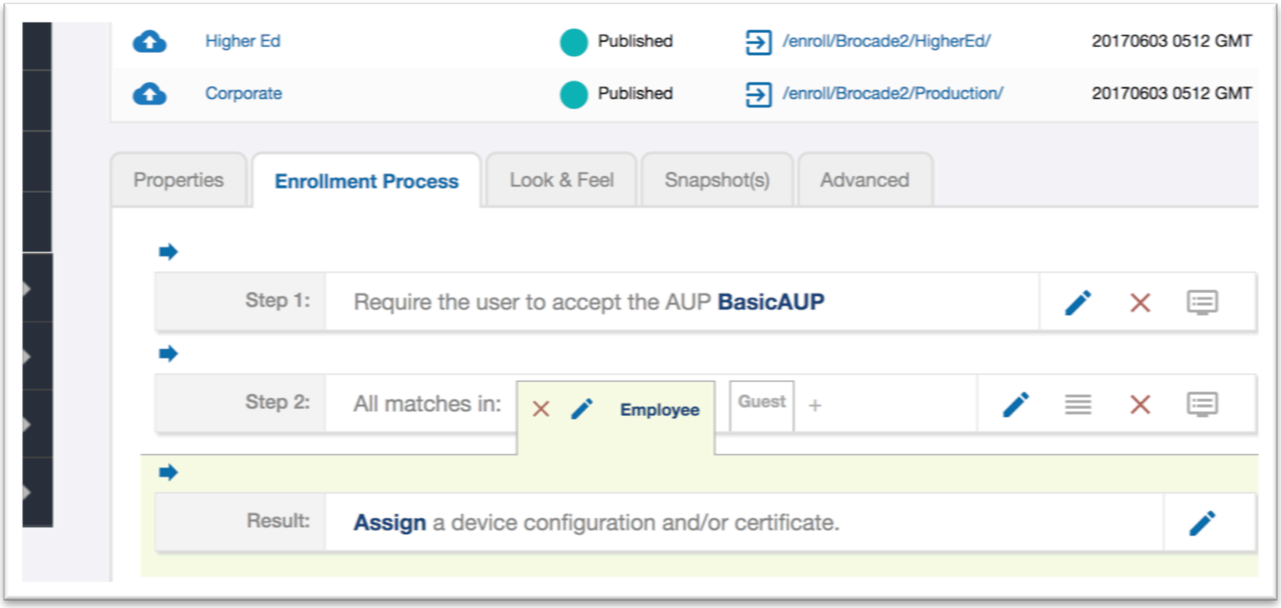
Option 2: Guest

Option 3:

- Keeping things simple, name the split and add two options: Employee and Guest
- After a split is created, there are many available options available in editing. The split can be much more than 4, and filters can be added for each option based on user, device, certificate, etc. For this document, we will stay with simple.
- Notice that step 2 (the split) adds additional editing icons for expanding the options
- Notice that you can switch between employee and guest branches. They are different branches and additional steps need to be added independently to each branch until it is completed.

8) Authenticate to a traditional authentication server

Important – Cloudpath ES is a RADIUS server for certificates and network access. It is not a replacement for your existing user database. The onboarding portal will authenticate users to the user database via password in order to validate them and apply policy, including installing a certificate. Thereafter, network access will be authenticated via certificate and the Cloudpath RADIUS server. This step is necessary to connect Cloudpath to the user database



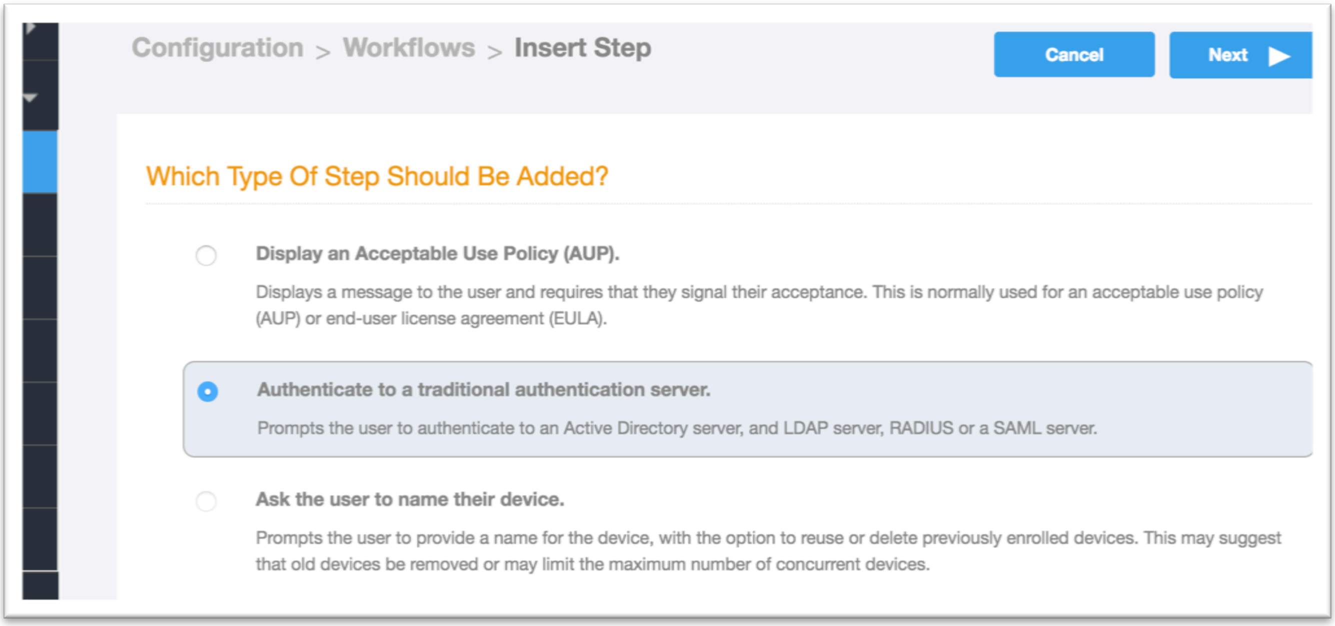
Higher Ed	Published	/enroll/Brocade2/HigherEd/	20170603 0512 GMT
Corporate	Published	/enroll/Brocade2/Production/	20170603 0512 GMT

Step 1: Require the user to accept the AUP **BasicAUP**

Step 2: All matches in: **Employee** | Guest | +

Result: **Assign** a device configuration and/or certificate.

- Go to the employee tab and insert a step before the “Result”.



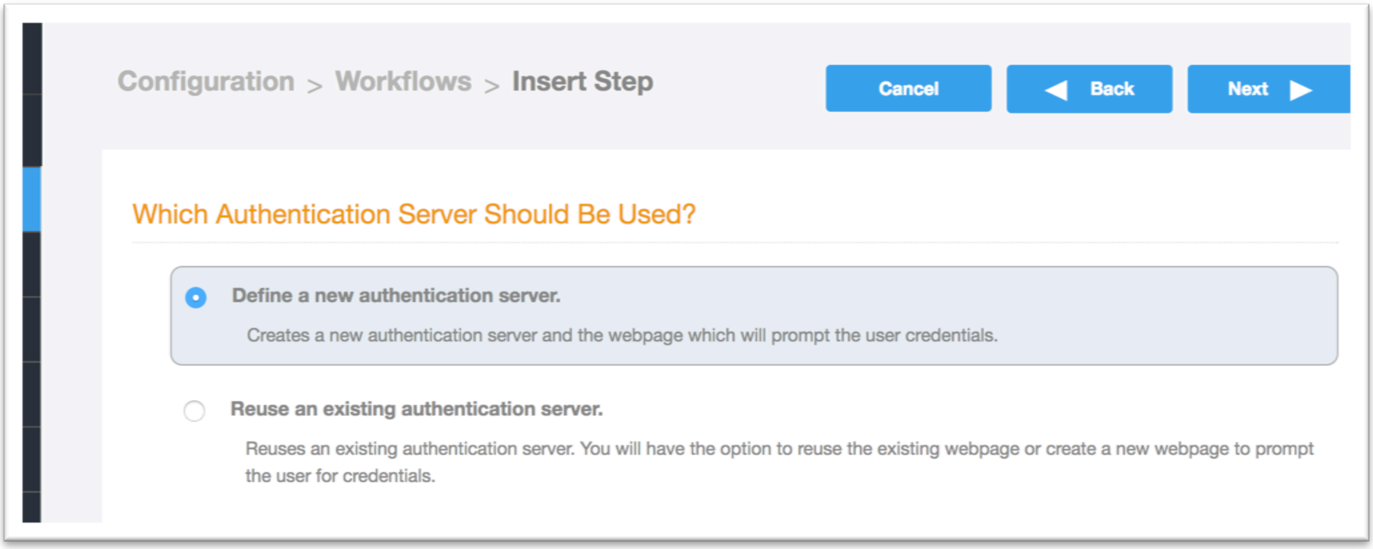
Which Type Of Step Should Be Added?

○ **Display an Acceptable Use Policy (AUP).**
Displays a message to the user and requires that they signal their acceptance. This is normally used for an acceptable use policy (AUP) or end-user license agreement (EULA).

● **Authenticate to a traditional authentication server.**
Prompts the user to authenticate to an Active Directory server, and LDAP server, RADIUS or a SAML server.

○ **Ask the user to name their device.**
Prompts the user to provide a name for the device, with the option to reuse or delete previously enrolled devices. This may suggest that old devices be removed or may limit the maximum number of concurrent devices.

- Insert a step by choosing "Authenticate to a traditional authentication server" and click "Next"

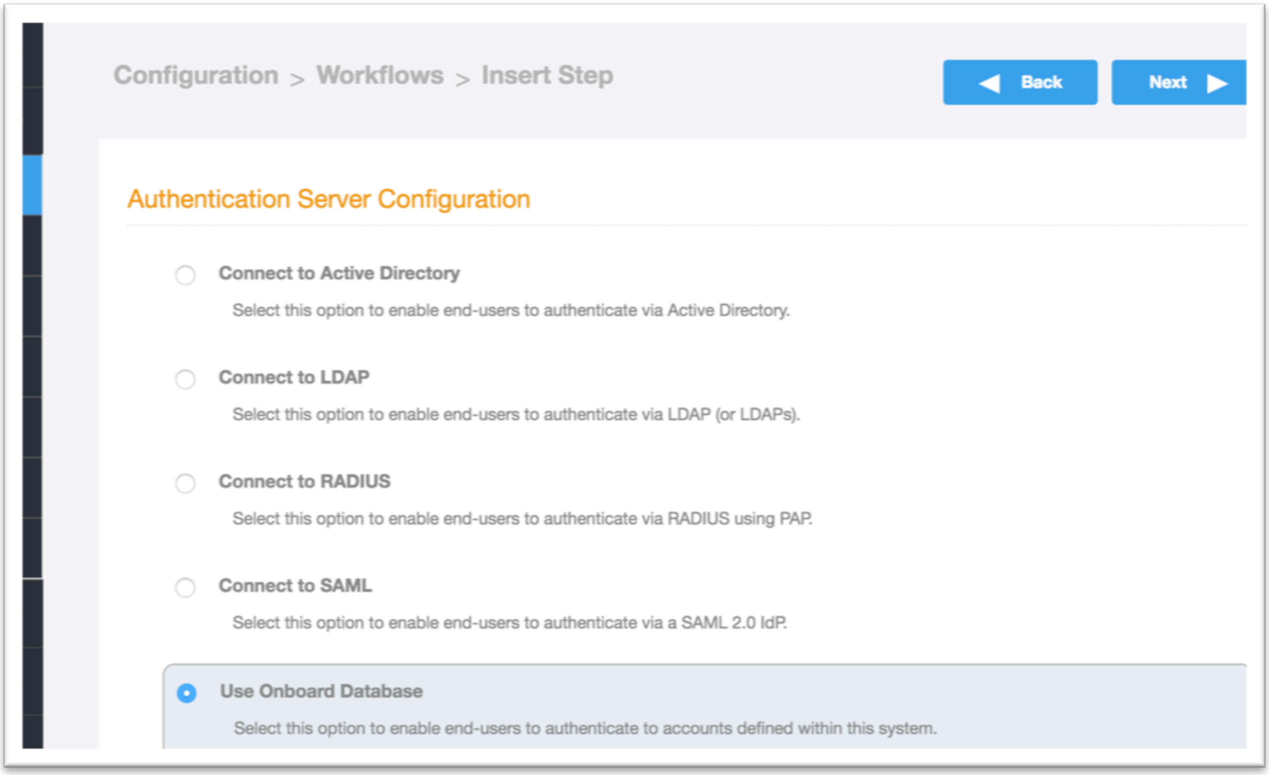


Which Authentication Server Should Be Used?

● **Define a new authentication server.**
Creates a new authentication server and the webpage which will prompt the user credentials.

○ **Reuse an existing authentication server.**
Reuses an existing authentication server. You will have the option to reuse the existing webpage or create a new webpage to prompt the user for credentials.

- Choose "Define a new authentication server" and click "Next".
- Details at this point depend on your existing user database



Authentication Server Configuration

○ Connect to Active Directory
Select this option to enable end-users to authenticate via Active Directory.

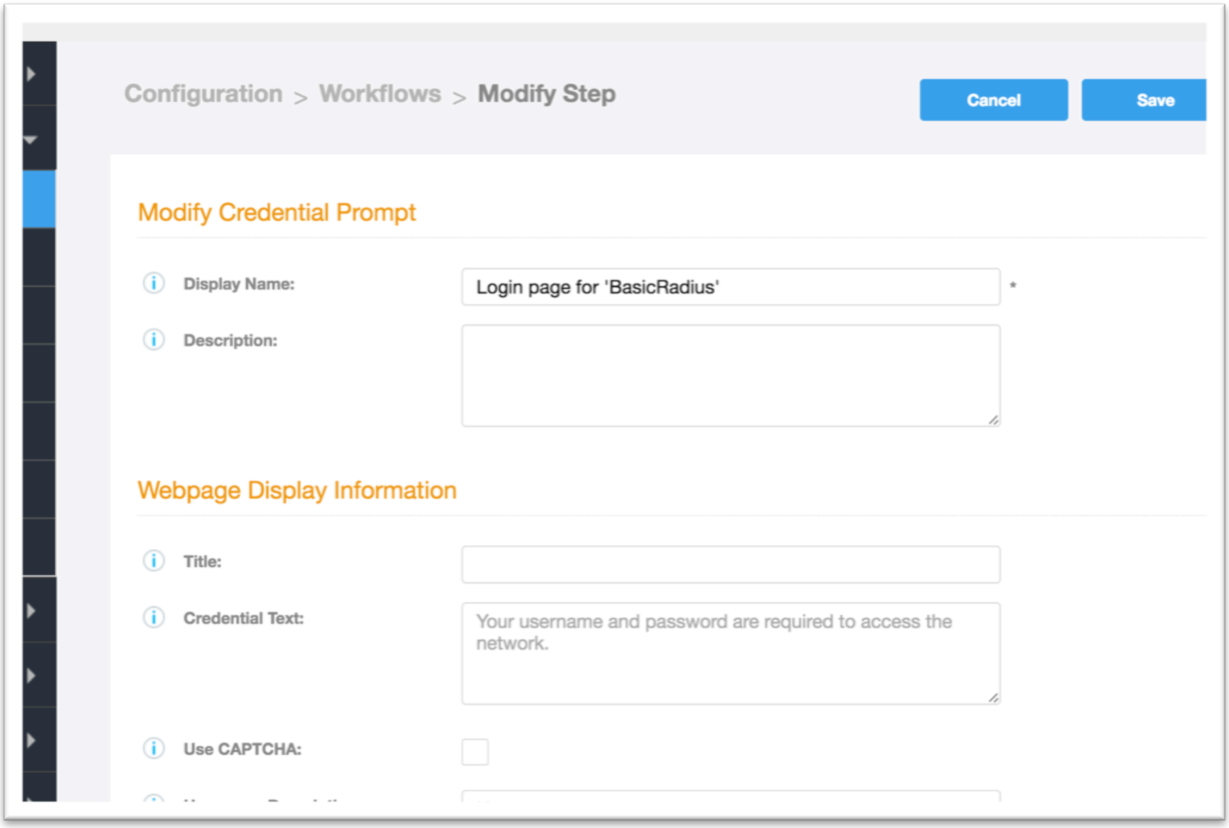
○ Connect to LDAP
Select this option to enable end-users to authenticate via LDAP (or LDAPs).

○ Connect to RADIUS
Select this option to enable end-users to authenticate via RADIUS using PAP.

○ Connect to SAML
Select this option to enable end-users to authenticate via a SAML 2.0 IdP.

● Use Onboard Database
Select this option to enable end-users to authenticate to accounts defined within this system.

- Cloudpath ES supports the following authentication types:
  - Active Directory
  - LDAP
  - RADIUS
  - SAML
- Cloudpath ES also includes a limited functionality onboard database, but that is for test purposes and should not be utilized in a production environment.
- Choose the correct server type for your environment and fill in the details. Your DB administrator should be able to provide the necessary information. – Click “Next”.
- Once the Authentication Server is defined, the final page has detailed options for how to prompt the user in the browser window. In this case, accept the defaults and click “Save”.



Modify Credential Prompt

Display Name: Login page for 'BasicRadius' *

Description:

Webpage Display Information

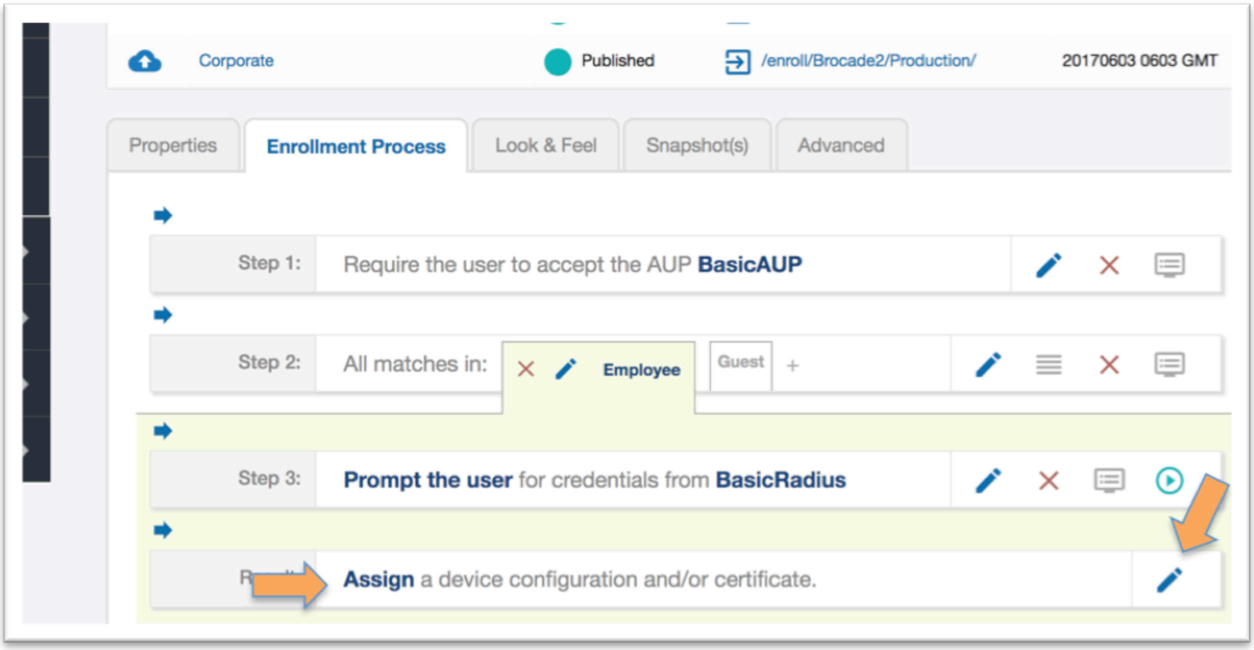
Title:

Credential Text: Your username and password are required to access the network.

Use CAPTCHA: □

9) Assign a *Device Configuration* to authenticated employees

This is a complex section, with a lot of options. This is where specific policies are applied to the onboarding devices. Once again, keeping things simple, in this case we will only configure the critical items and other wise accept the defaults.



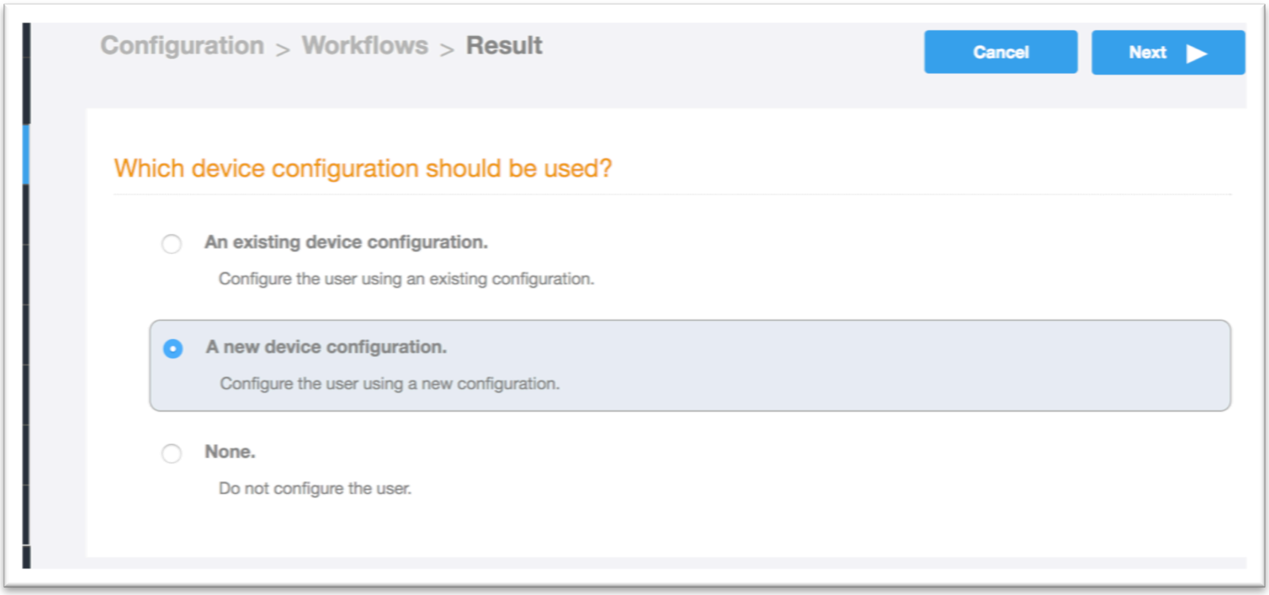
Step 1: Require the user to accept the AUP **BasicAUP**

Step 2: All matches in: Employee Guest +

Step 3: **Prompt the user** for credentials from **BasicRadius**

R... **Assign** a device configuration and/or certificate.

- Click on either the word "Assign" or the pencil icon in the final "Result" step.
- Choose "A new device configuration." Click "Next".

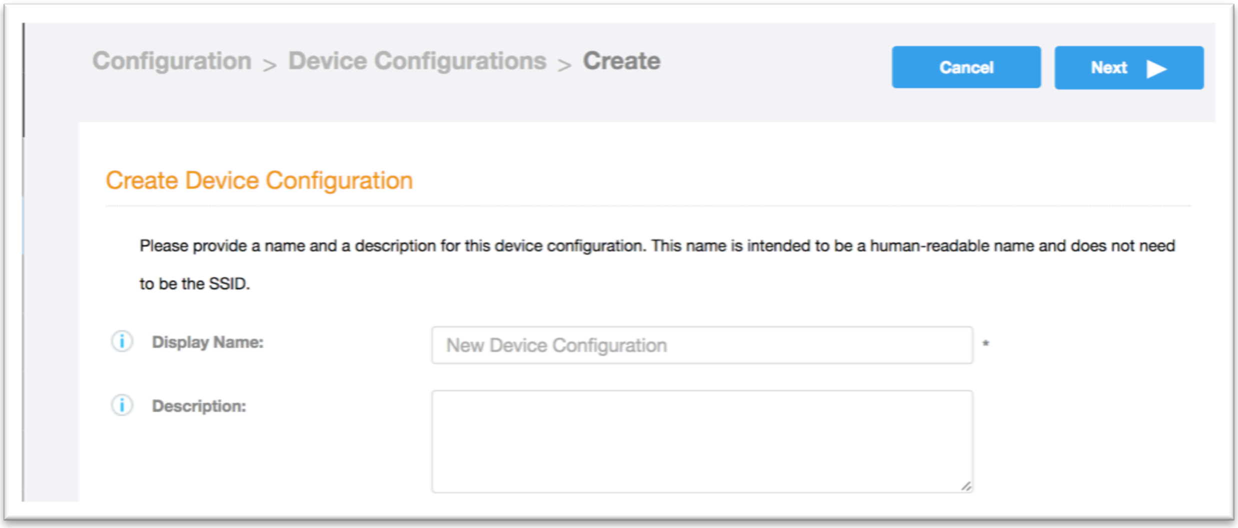


Which device configuration should be used?

○ **An existing device configuration.**
Configure the user using an existing configuration.

● **A new device configuration.**
Configure the user using a new configuration.

○ **None.**
Do not configure the user.



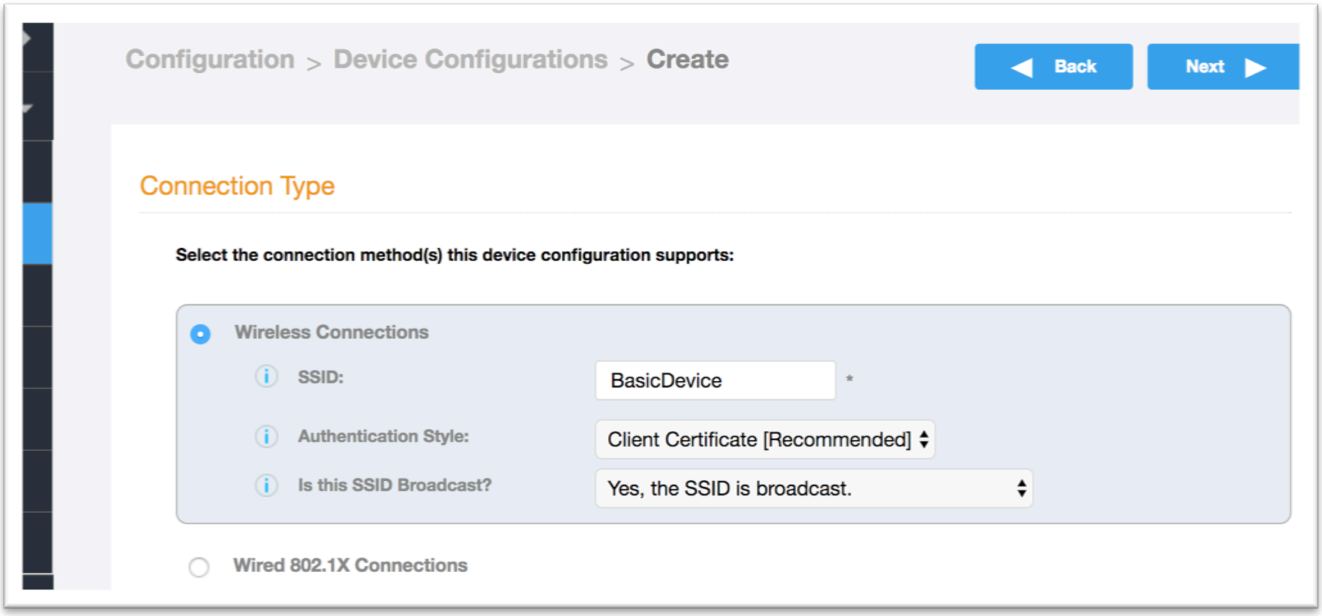
Create Device Configuration

Please provide a name and a description for this device configuration. This name is intended to be a human-readable name and does not need to be the SSID.

Display Name: New Device Configuration *

Description:

- Name the configuration. Click "Next".



Connection Type

Select the connection method(s) this device configuration supports:

● Wireless Connections

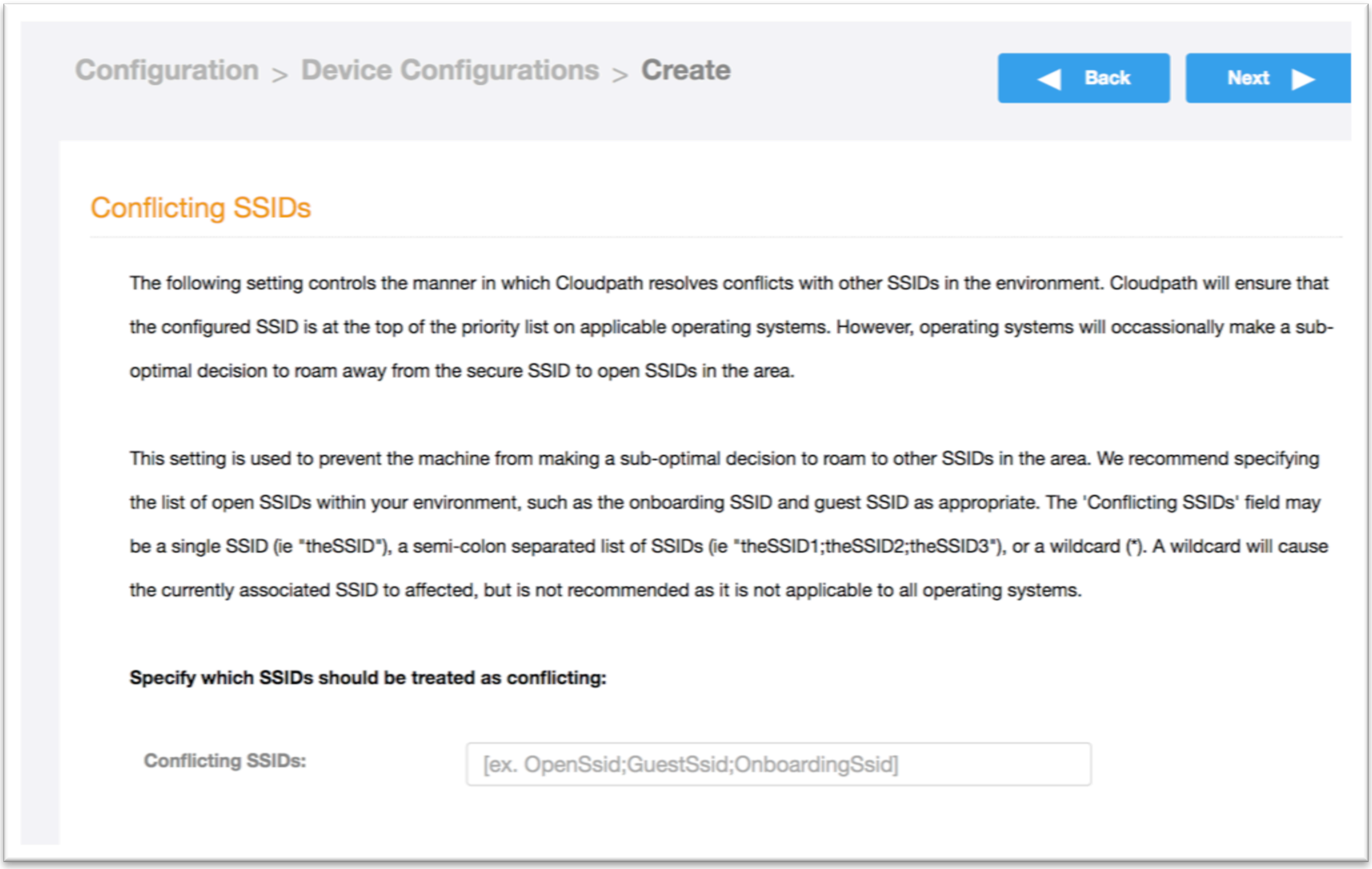
SSID: BasicDevice *

Authentication Style: Client Certificate [Recommended]

Is this SSID Broadcast? Yes, the SSID is broadcast.

○ Wired 802.1X Connections

- Connection Type is the WLAN profile.
- The SSID must match the secure WLAN.
- The Authentication type should be client certificate
- Notice that password, PSK, and Ruckus DPSK are also options
- SSID is broadcast
- Click "Next".



Conflicting SSIDs

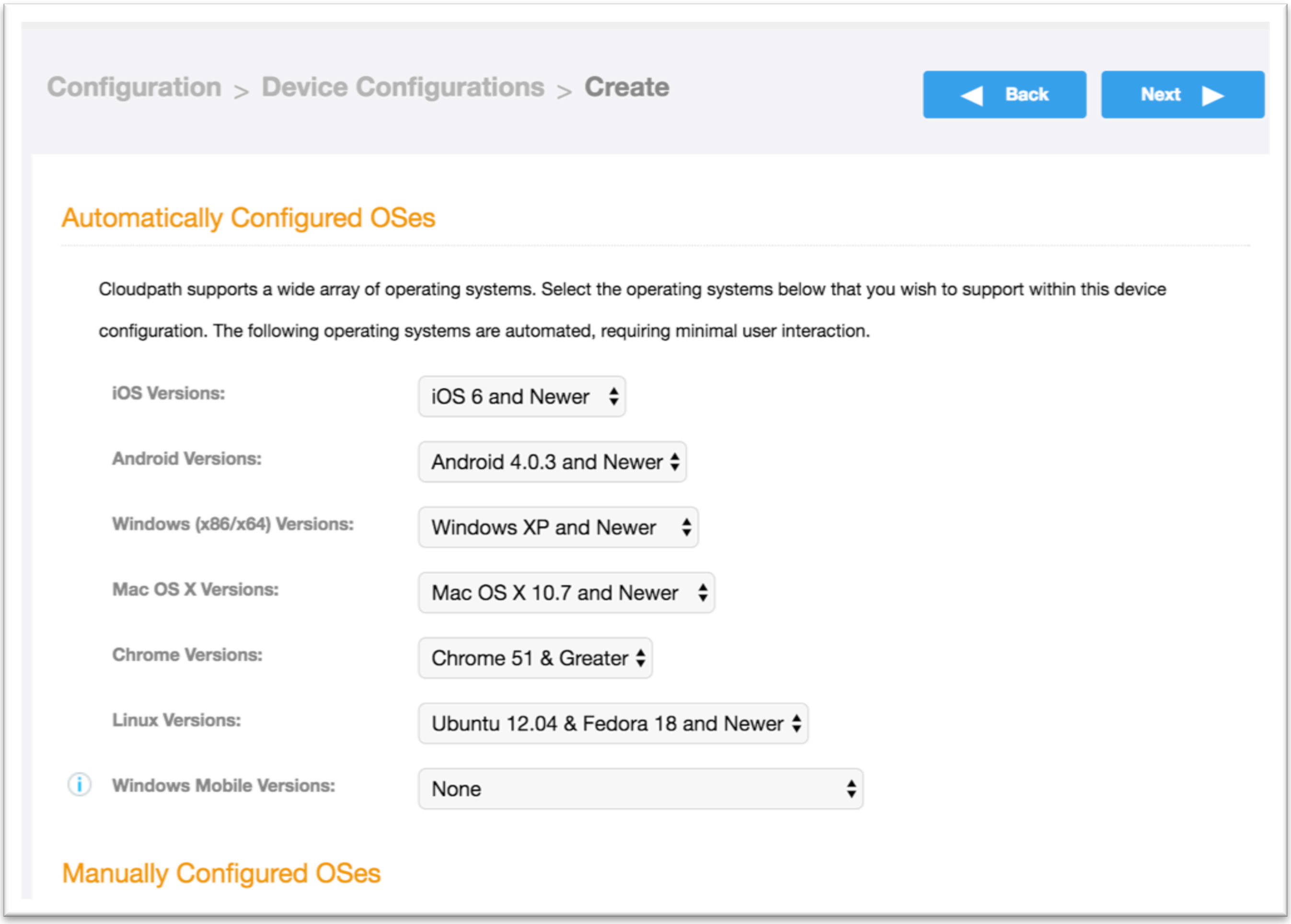
The following setting controls the manner in which Cloudpath resolves conflicts with other SSIDs in the environment. Cloudpath will ensure that the configured SSID is at the top of the priority list on applicable operating systems. However, operating systems will occassionally make a sub-optimal decision to roam away from the secure SSID to open SSIDs in the area.

This setting is used to prevent the machine from making a sub-optimal decision to roam to other SSIDs in the area. We recommend specifying the list of open SSIDs within your environment, such as the onboarding SSID and guest SSID as appropriate. The 'Conflicting SSIDs' field may be a single SSID (ie "theSSID"), a semi-colon separated list of SSIDs (ie "theSSID1;theSSID2;theSSID3"), or a wildcard (*). A wildcard will cause the currently associated SSID to affected, but is not recommended as it is not applicable to all operating systems.

Specify which SSIDs should be treated as conflicting:

Conflicting SSIDs: [ex. OpenSsid;GuestSsid;OnboardingSsid]

- This item is typically configured to ensure the device does NOT return to the onboarding SSID. It could also be used to drop the priority of nearby hotspots.
- Click “Next”.



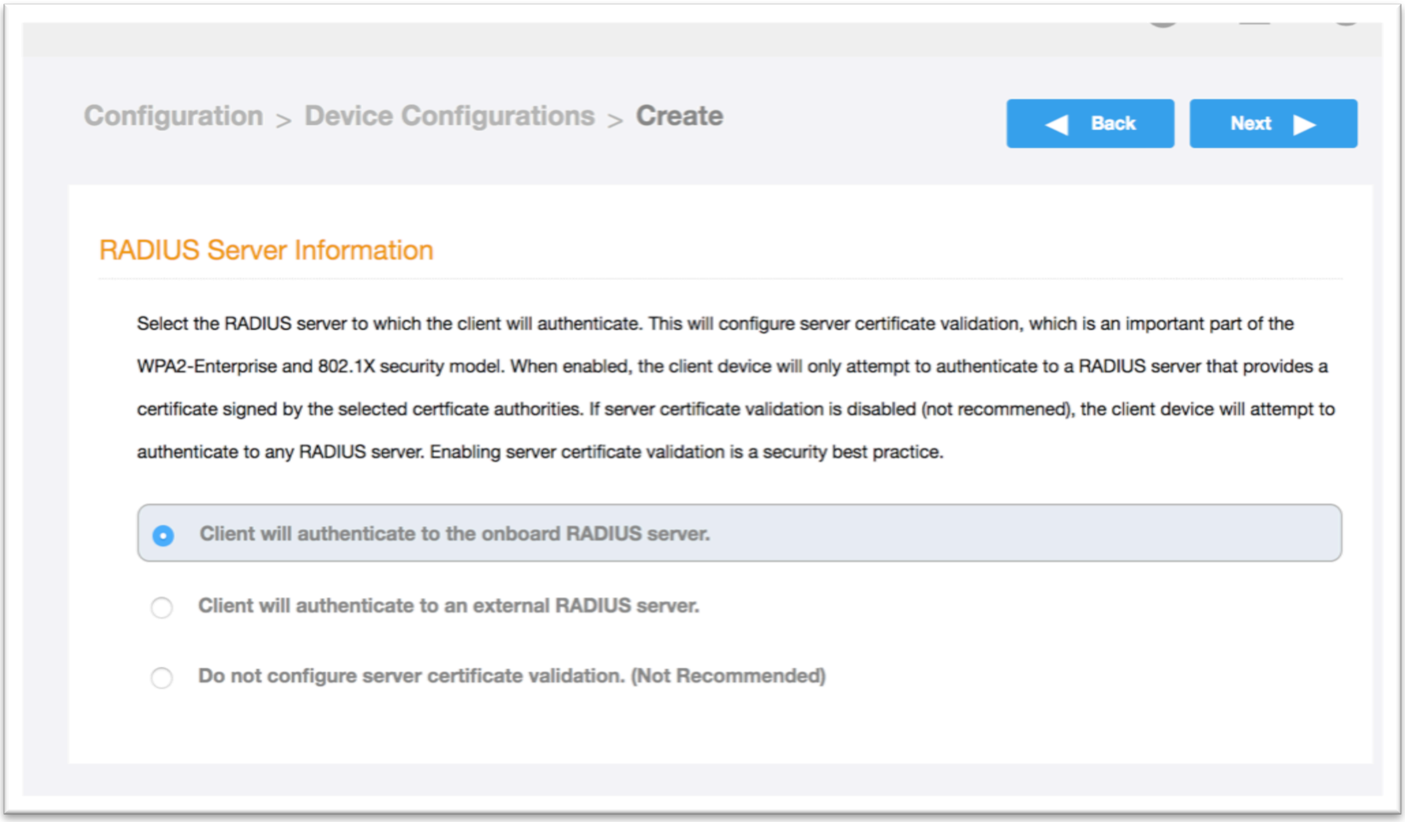
Automatically Configured OSes

Cloudpath supports a wide array of operating systems. Select the operating systems below that you wish to support within this device configuration. The following operating systems are automated, requiring minimal user interaction.

iOS Versions:	iOS 6 and Newer
Android Versions:	Android 4.0.3 and Newer
Windows (x86/x64) Versions:	Windows XP and Newer
Mac OS X Versions:	Mac OS X 10.7 and Newer
Chrome Versions:	Chrome 51 & Greater
Linux Versions:	Ubuntu 12.04 & Fedora 18 and Newer
Windows Mobile Versions:	None

Manually Configured OSes

- This option can limit the operating systems that are accepted. For now, accept the defaults and click “Next”.



RADIUS Server Information

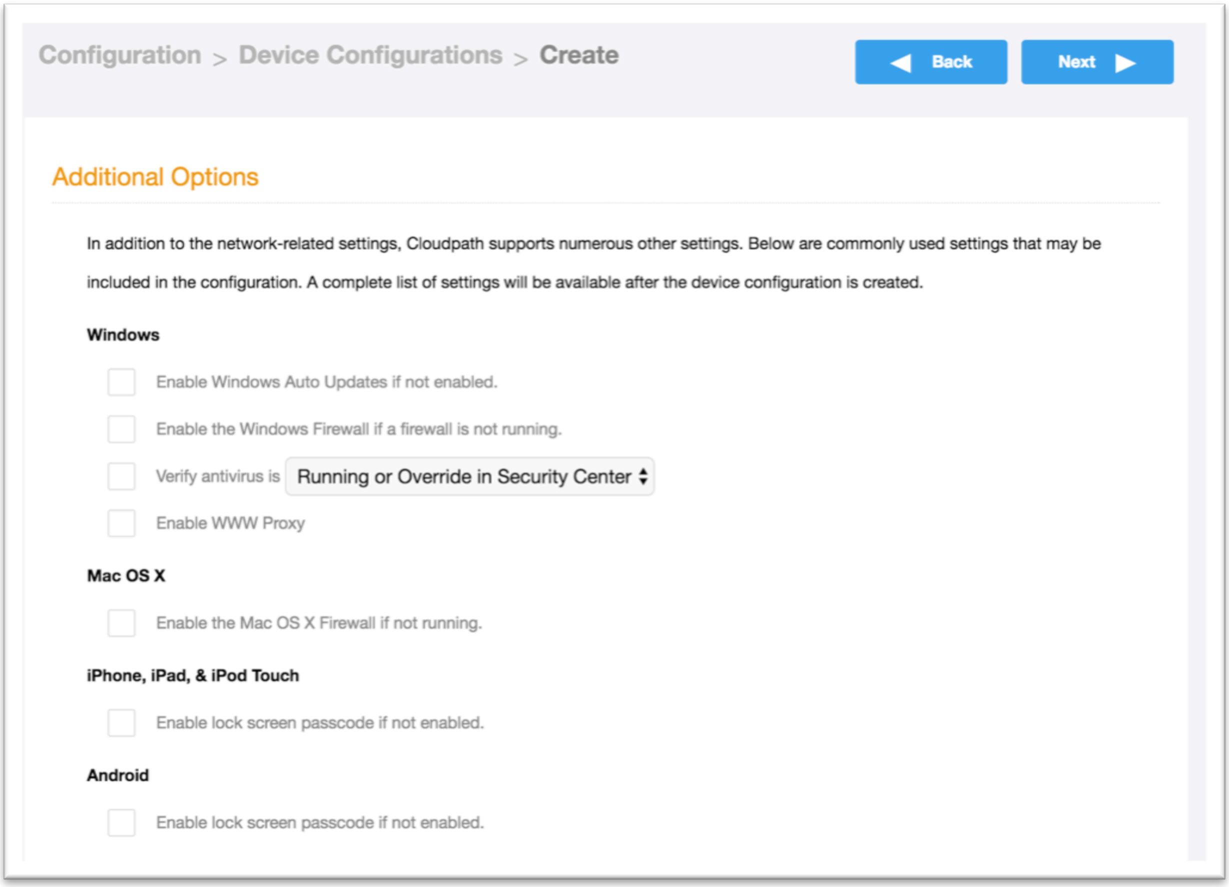
Select the RADIUS server to which the client will authenticate. This will configure server certificate validation, which is an important part of the WPA2-Enterprise and 802.1X security model. When enabled, the client device will only attempt to authenticate to a RADIUS server that provides a certificate signed by the selected certficate authorities. If server certificate validation is disabled (not recommened), the client device will attempt to authenticate to any RADIUS server. Enabling server certificate validation is a security best practice.

● Client will authenticate to the onboard RADIUS server.

○ Client will authenticate to an external RADIUS server.

○ Do not configure server certificate validation. (Not Recommended)

- Choose "Client will authenticate to the onboard RADIUS server".
- This is the integrated Cloudpath ES RADIUS server, which authenticates based on certificates. To be clear, in the onboarding portal, the user authenticates to a different database, possibly a RADIUS fronted DB, using user name and password to obtain a certificate. Thereafter, the client device uses the certificate to authenticate to the WALN via the Cloudpath RADIUS.
- Click "Next".



Additional Options

In addition to the network-related settings, Cloudpath supports numerous other settings. Below are commonly used settings that may be included in the configuration. A complete list of settings will be available after the device configuration is created.

Windows

□ Enable Windows Auto Updates if not enabled.

□ Enable the Windows Firewall if a firewall is not running.

□ Verify antivirus is Running or Override in Security Center

□ Enable WWW Proxy

Mac OS X

□ Enable the Mac OS X Firewall if not running.

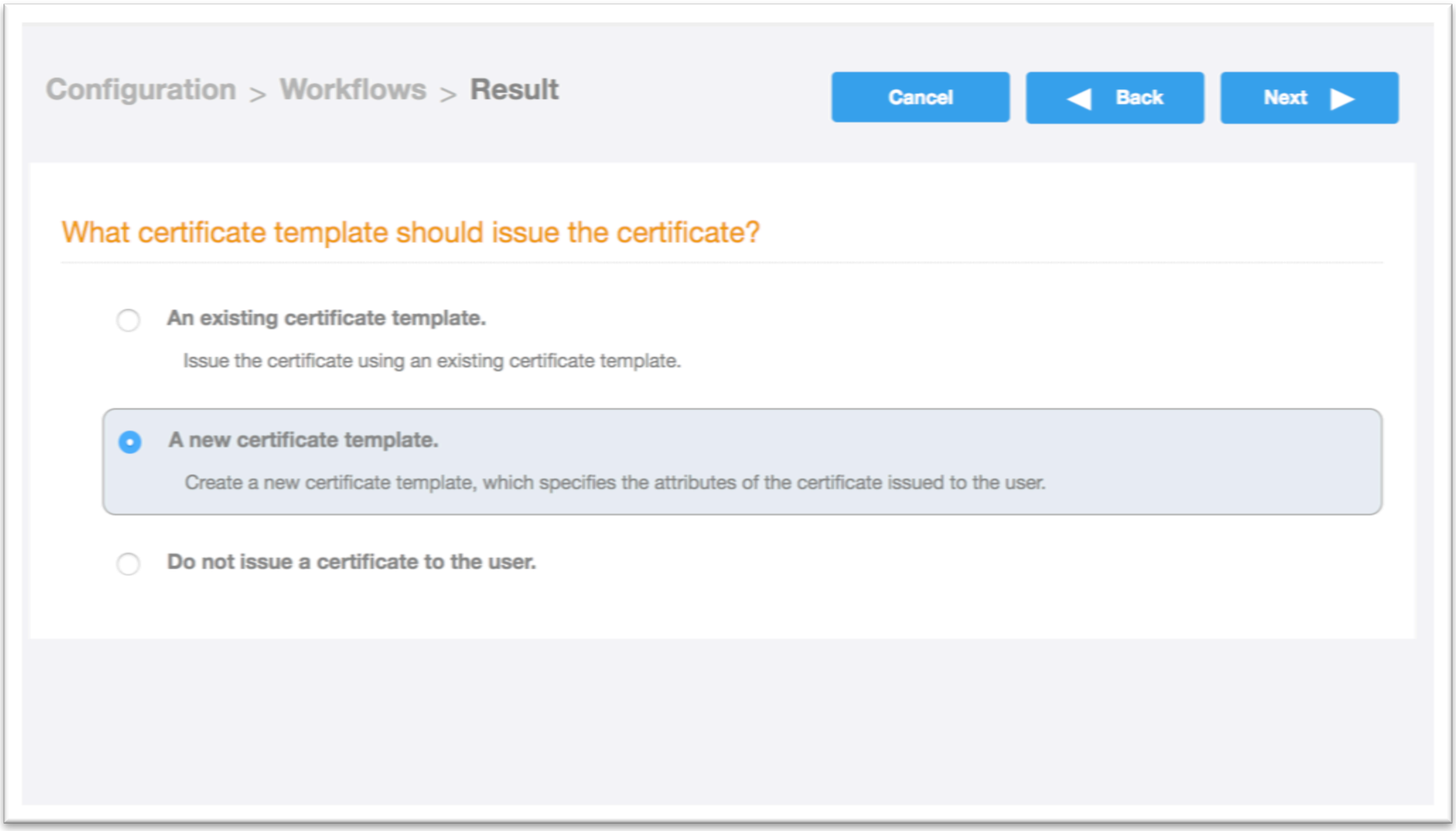
iPhone, iPad, & iPod Touch

□ Enable lock screen passcode if not enabled.

Android

□ Enable lock screen passcode if not enabled.

- Here are some of the “NAC” light functions Cloudpath can perform. Another Cookbook will cover these in depth.
- For now, Click “Next”.



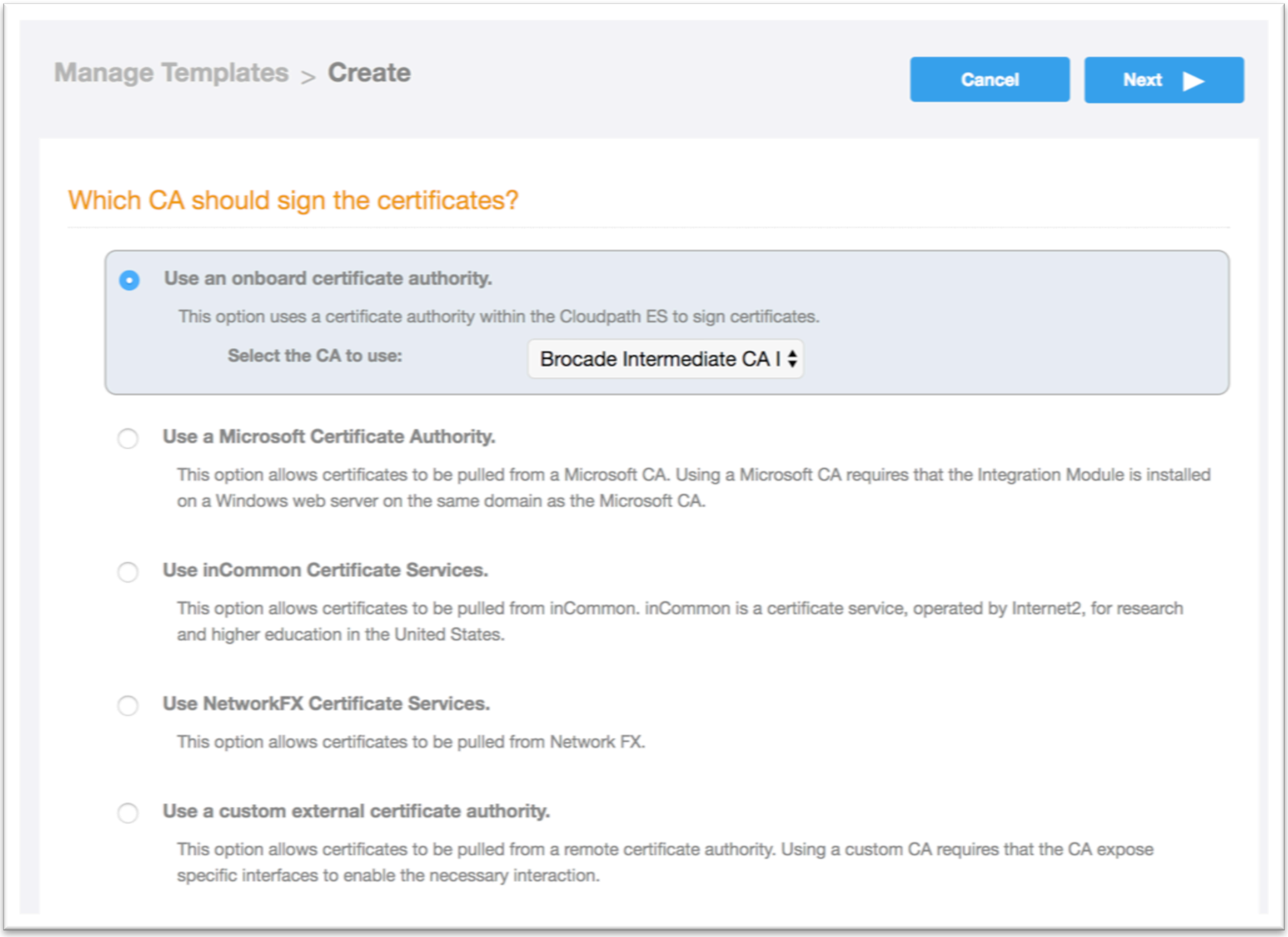
What certificate template should issue the certificate?

○ **An existing certificate template.**
Issue the certificate using an existing certificate template.

● **A new certificate template.**
Create a new certificate template, which specifies the attributes of the certificate issued to the user.

○ **Do not issue a certificate to the user.**

- Choose "A new certificate template."
- Click "Next".



Which CA should sign the certificates?

● **Use an onboard certificate authority.**

This option uses a certificate authority within the Cloudpath ES to sign certificates.

Select the CA to use: Brocade Intermediate CA I

○ **Use a Microsoft Certificate Authority.**

This option allows certificates to be pulled from a Microsoft CA. Using a Microsoft CA requires that the Integration Module is installed on a Windows web server on the same domain as the Microsoft CA.

○ **Use inCommon Certificate Services.**

This option allows certificates to be pulled from inCommon. inCommon is a certificate service, operated by Internet2, for research and higher education in the United States.

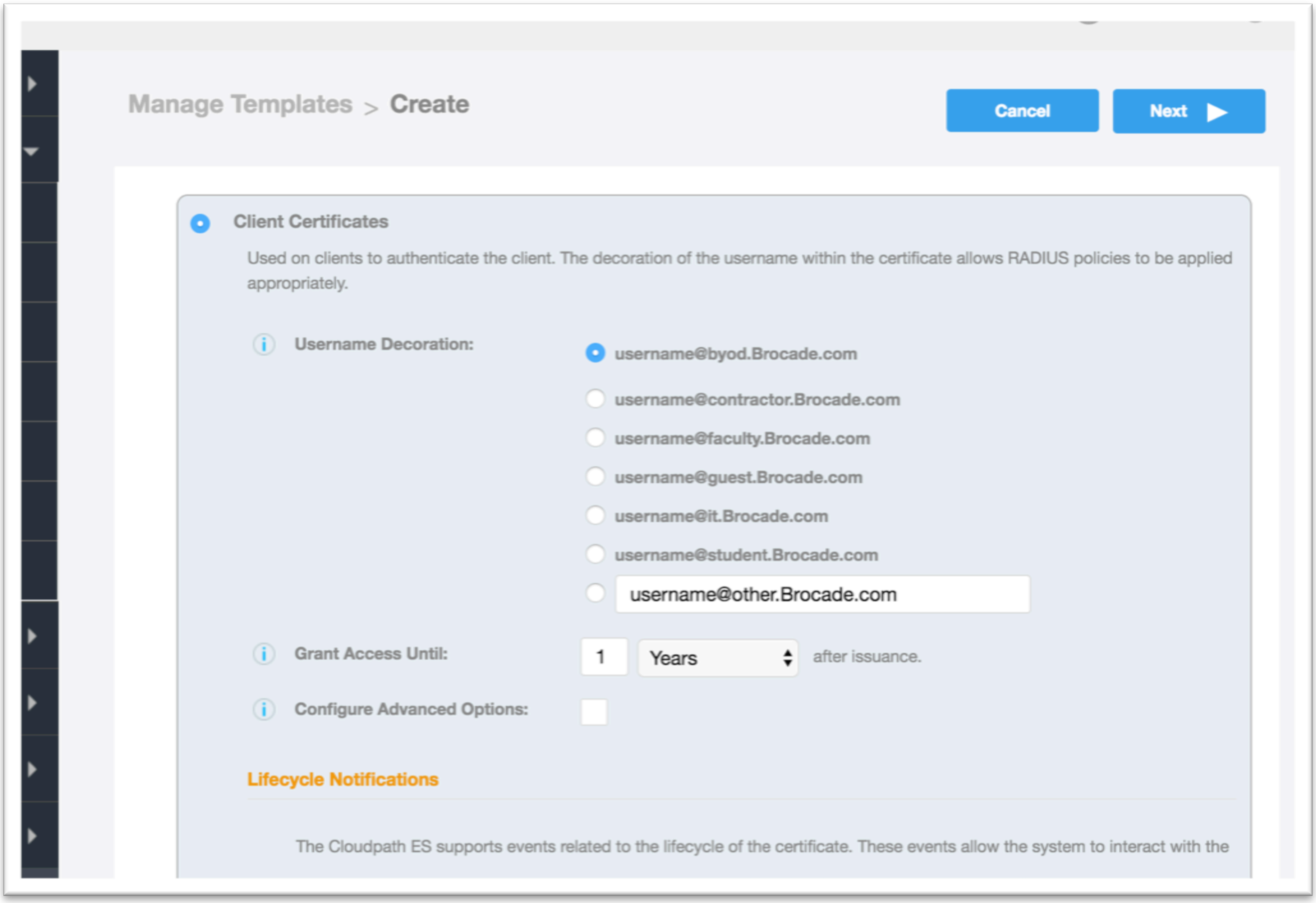
○ **Use NetworkFX Certificate Services.**

This option allows certificates to be pulled from Network FX.

○ **Use a custom external certificate authority.**

This option allows certificates to be pulled from a remote certificate authority. Using a custom CA requires that the CA expose specific interfaces to enable the necessary interaction.

- Choose to use an onboard certificate authority
- Click “Next”.



● Client Certificates

Used on clients to authenticate the client. The decoration of the username within the certificate allows RADIUS policies to be applied appropriately.

Username Decoration:
● username@byod.Brocade.com
○ username@contractor.Brocade.com
○ username@faculty.Brocade.com
○ username@guest.Brocade.com
○ username@it.Brocade.com
○ username@student.Brocade.com
○ username@other.Brocade.com

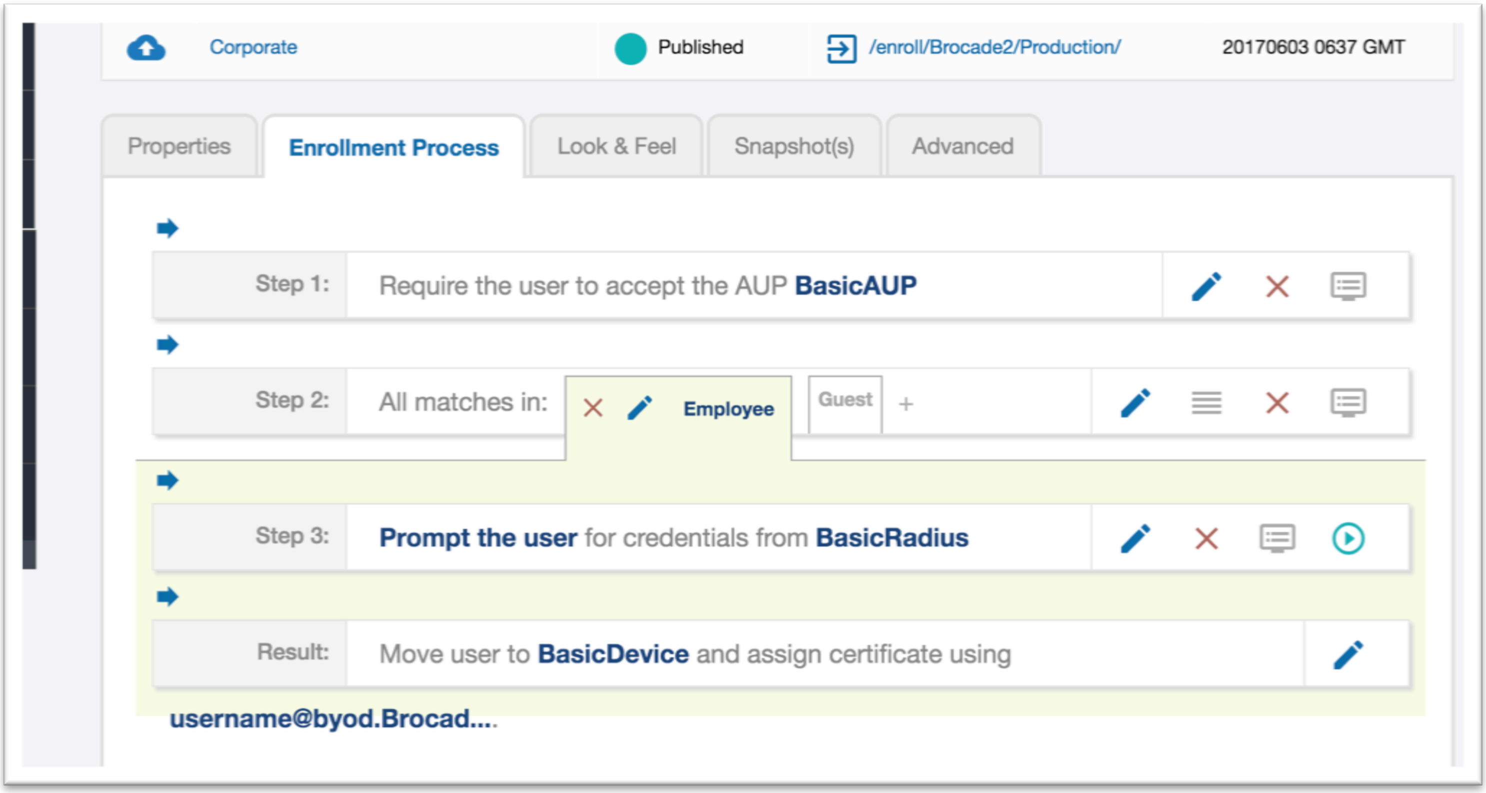
Grant Access Until: 1 Years after issuance.

Configure Advanced Options: □

Lifecycle Notifications

The Cloudpath ES supports events related to the lifecycle of the certificate. These events allow the system to interact with the

- Once again, there are a number of options here. They can be explored in more depth in the Cloudpath Administrator's Guide or other Best Practices Guides. For now, accept the defaults and click "Next".



Step 1: Require the user to accept the AUP **BasicAUP**

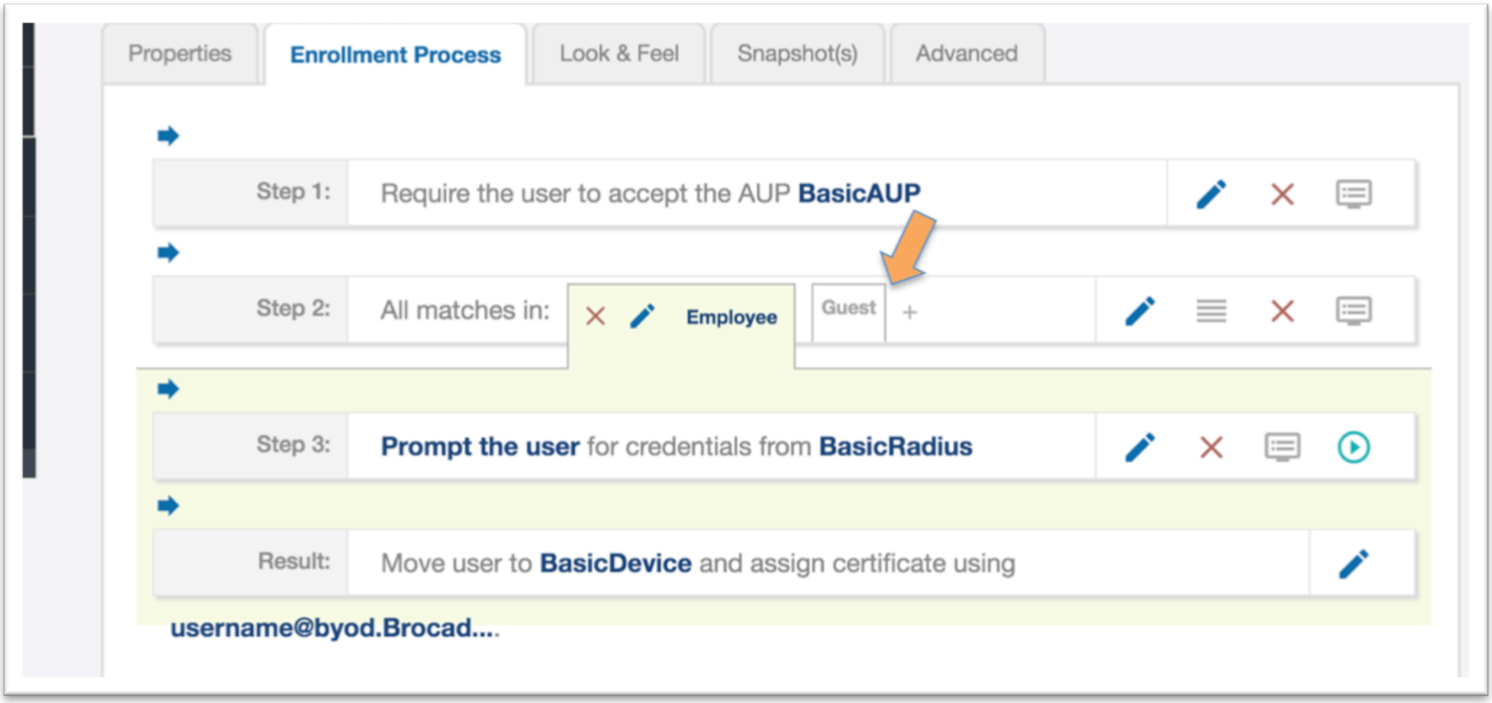
Step 2: All matches in: **Employee** Guest +

Step 3: **Prompt the user** for credentials from **BasicRadius**

Result: Move user to **BasicDevice** and assign certificate using **username@byod.Brocad...**

- The Employee branch of the basic workflow is now complete!

10) Guest Branch – Insert MAC authentication



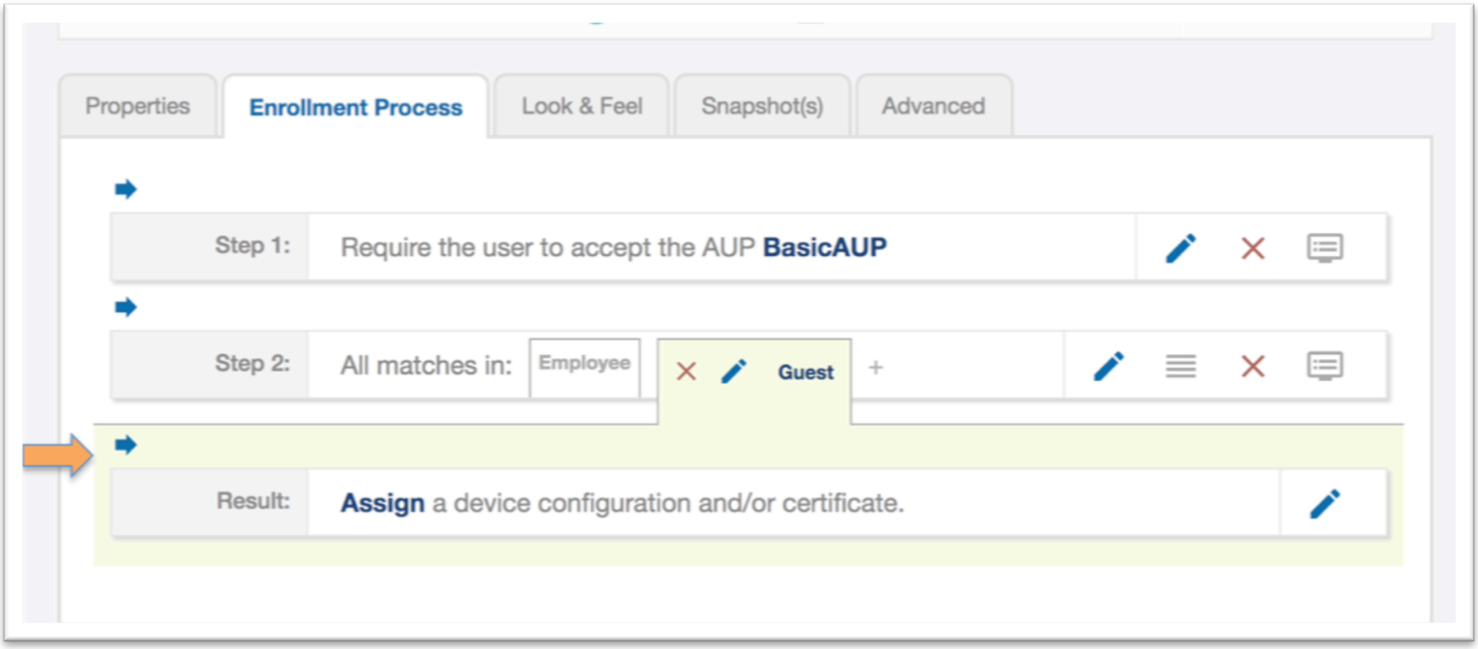
Step 1: Require the user to accept the AUP **BasicAUP**

Step 2: All matches in: **Employee** Guest +

Step 3: **Prompt the user** for credentials from **BasicRadius**

Result: Move user to **BasicDevice** and assign certificate using **username@byod.Brocad...**

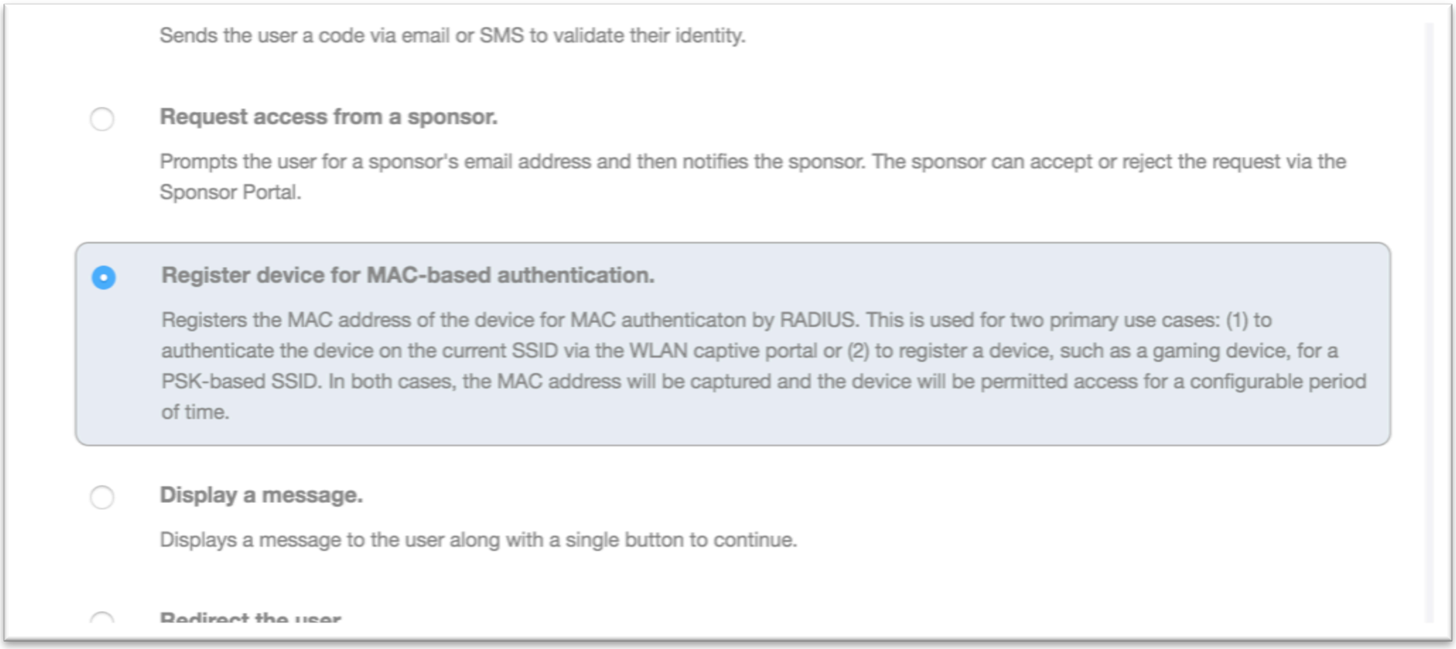
- Click on the guest tab (see above)
- Click on the arrow to insert a step above the guest "Result" step (see below)



Step 1: Require the user to accept the AUP **BasicAUP**

Step 2: All matches in: Employee | Guest

Result: **Assign** a device configuration and/or certificate.


Sends the user a code via email or SMS to validate their identity.

○ **Request access from a sponsor.**

Prompts the user for a sponsor's email address and then notifies the sponsor. The sponsor can accept or reject the request via the Sponsor Portal.

● **Register device for MAC-based authentication.**

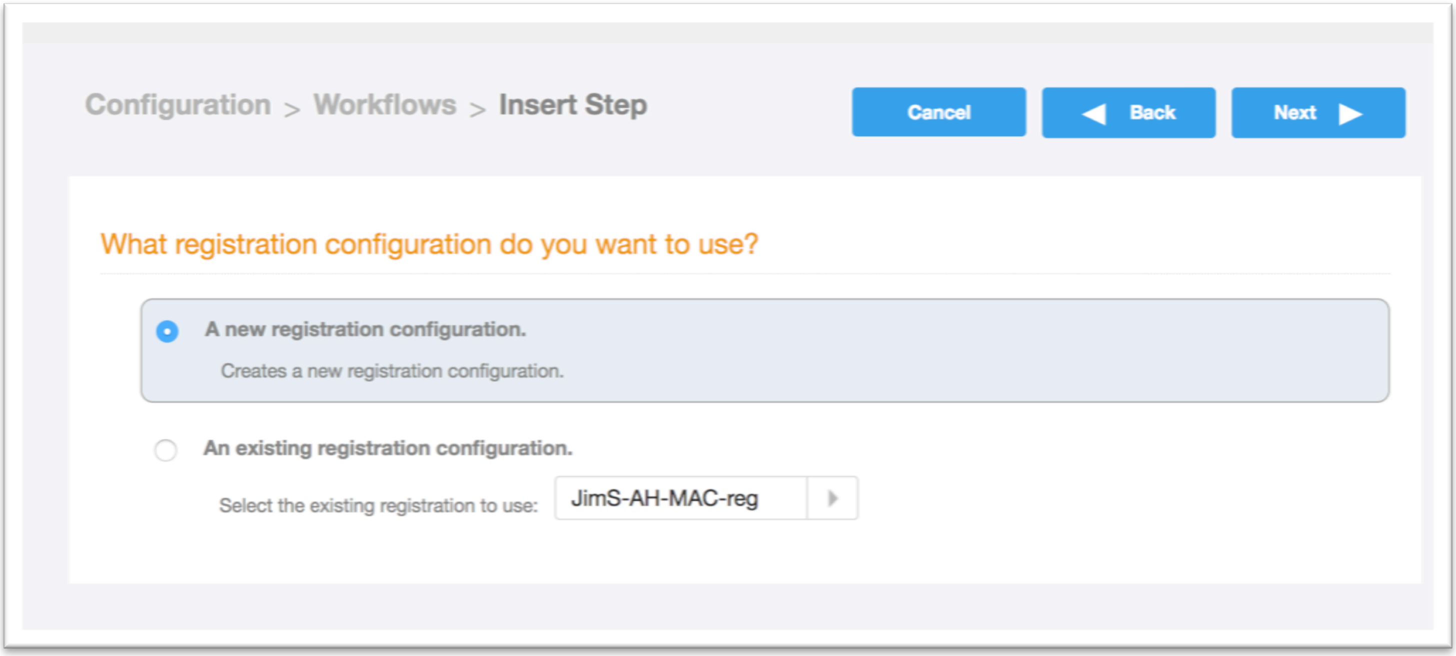
Registers the MAC address of the device for MAC authenticaton by RADIUS. This is used for two primary use cases: (1) to authenticate the device on the current SSID via the WLAN captive portal or (2) to register a device, such as a gaming device, for a PSK-based SSID. In both cases, the MAC address will be captured and the device will be permitted access for a configurable period of time.

○ **Display a message.**

Displays a message to the user along with a single button to continue.

○ **Redirect the user**

- About midway down the page, choose the step “Register device for MAC-based authentication

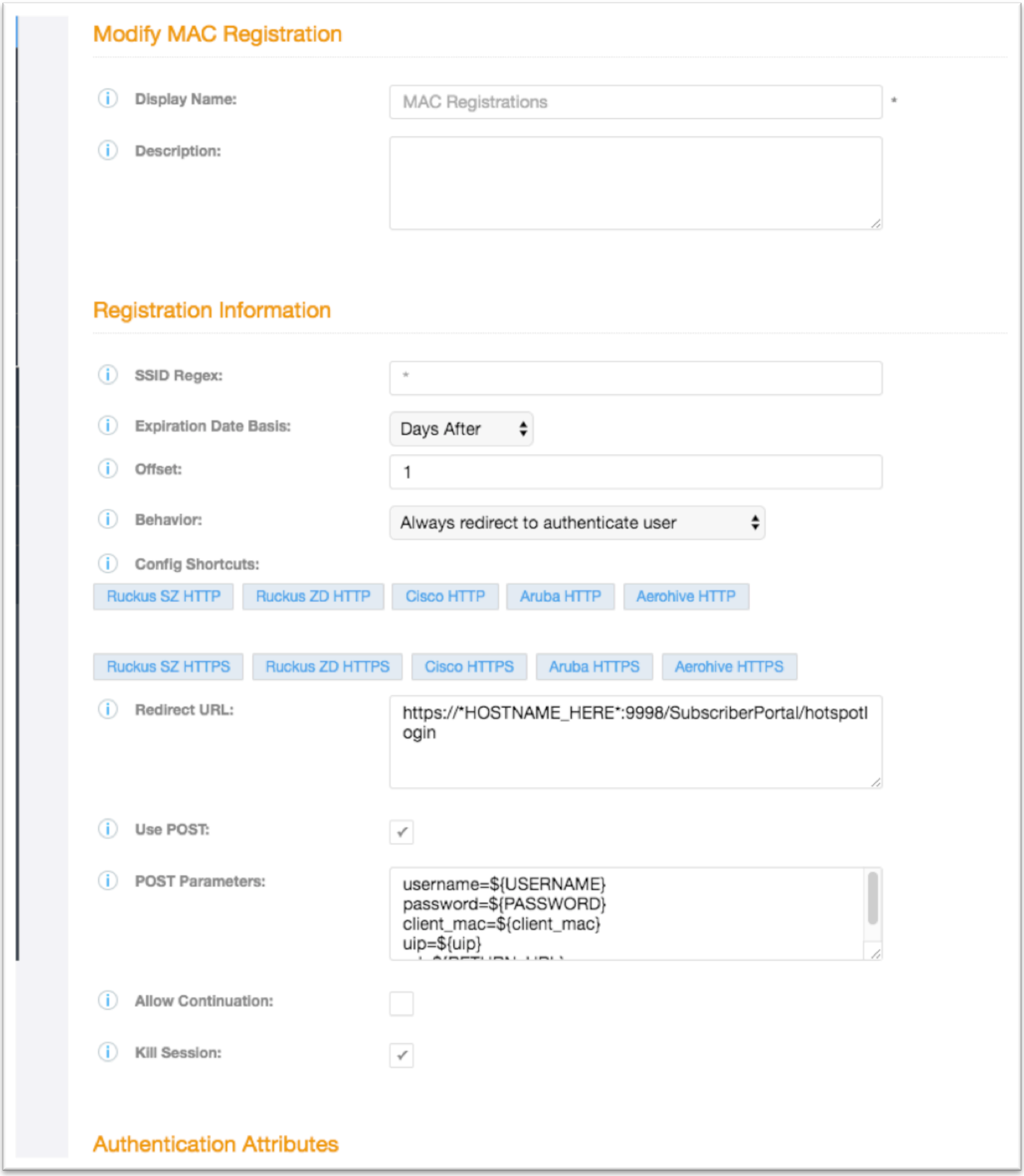


What registration configuration do you want to use?

● A new registration configuration.
Creates a new registration configuration.

○ An existing registration configuration.
Select the existing registration to use: JimS-AH-MAC-reg

- Choose " A new registration configuration and click "Next".



Modify MAC Registration

Display Name: MAC Registrations *

Description:

Registration Information

SSID Regex: *

Expiration Date Basis: Days After

Offset: 1

Behavior: Always redirect to authenticate user

Config Shortcuts:

Redirect URL: https://*HOSTNAME_HERE*:9998/SubscriberPortal/hotspotlogin

Use POST: ☑

POST Parameters:

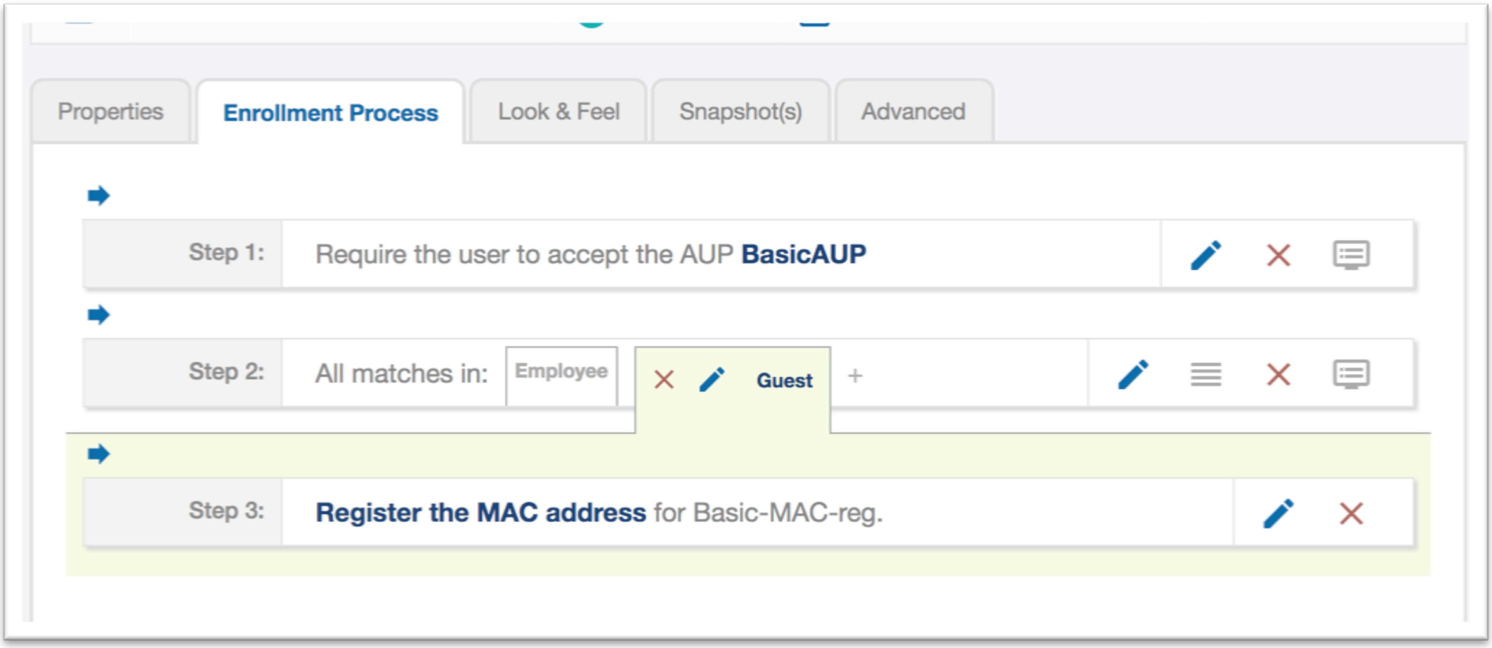
```
username=${USERNAME}
password=${PASSWORD}
client_mac=${client_mac}
uip=${uip}
```

Allow Continuation: ☐

Kill Session: ☑

Authentication Attributes

- As is typical for this exercise, configure the basics and leave the other options for later exercises.
- Add a display name
- SSID Regex can be left blank or be the Onboarding SSID
- Behavior: choose "Always redirect to authenticate user"
- Config Shortcuts: Click on the one appropriate for the WLAN controller in question.
- The example is a Ruckus SZ HTTPS
- The redirect URL is filled in by the shortcut config button –*BUT the hostname has to be edited for the WLAN controller!*
    - *Be conscious of firewalls between Cloudpath and the WLAN controller!*
- Check "Use POST"
- Leave post parameters
- Uncheck "Allow Continuation"
- Check "Kill Session"
- Click "Save" in the upper right (not shown here)



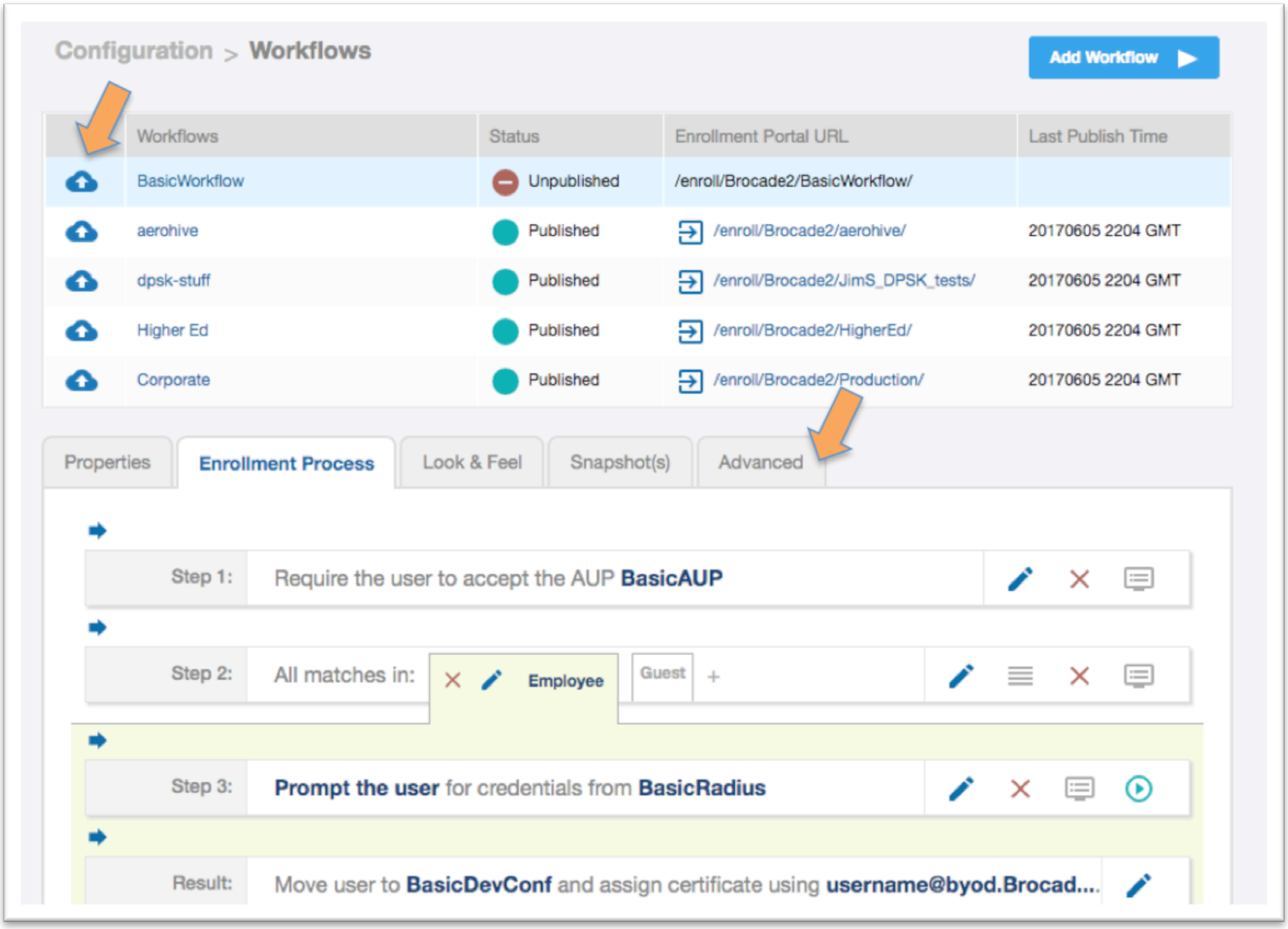
Step 1: Require the user to accept the AUP **BasicAUP**

Step 2: All matches in: Employee | **Guest**

Step 3: **Register the MAC address** for Basic-MAC-reg.

- Configuration of the Guest Branch is complete!
- Note that the "Result" step is gone. No configuration is pushed to the client device when using MAC registration

11) Publish the workflow



	Workflows	Status	Enrollment Portal URL	Last Publish Time
☁	BasicWorkflow	⊖ Unpublished	/enroll/Brocade2/BasicWorkflow/	
☁	aerohive	● Published	/enroll/Brocade2/aerohive/	20170605 2204 GMT
☁	dpsk-stuff	● Published	/enroll/Brocade2/JimS_DPSK_tests/	20170605 2204 GMT
☁	Higher Ed	● Published	/enroll/Brocade2/HigherEd/	20170605 2204 GMT
☁	Corporate	● Published	/enroll/Brocade2/Production/	20170605 2204 GMT

Step 1: Require the user to accept the AUP **BasicAUP**

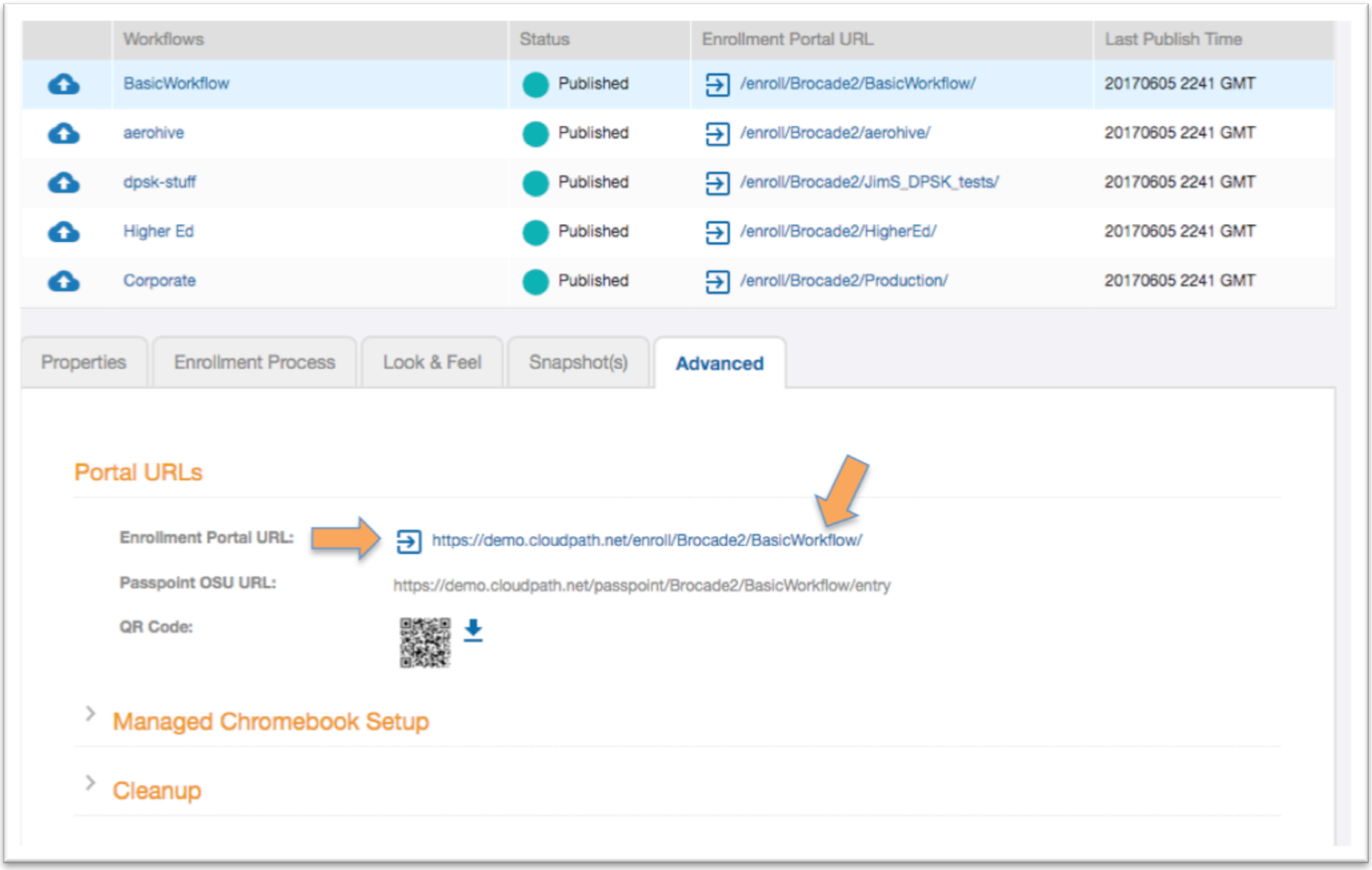
Step 2: All matches in: **Employee** Guest +

Step 3: **Prompt the user** for credentials from **BasicRadius**

Result: Move user to **BasicDevConf** and assign certificate using **username@byod.Brocad...**

- Notice on the workflow list, the status of the workflow is “Unpublished”. The workflow has to be converted to HTML and published to the Cloudpath web server. Click on the cloud/upload icon to the left of the workflow on the workflow list. This may take a couple minuttes
- This may take a few minutes
- Once publishing is completed, click on the advanced tab of the workflow

12) Get the enrollment URL and the RADIUS shared secret for the WLAN configuration



Workflows	Status	Enrollment Portal URL	Last Publish Time
BasicWorkflow	● Published	/enroll/Brocade2/BasicWorkflow/	20170605 2241 GMT
aerohive	● Published	/enroll/Brocade2/aerohive/	20170605 2241 GMT
dpsk-stuff	● Published	/enroll/Brocade2/JimS_DPSK_tests/	20170605 2241 GMT
Higher Ed	● Published	/enroll/Brocade2/HigherEd/	20170605 2241 GMT
Corporate	● Published	/enroll/Brocade2/Production/	20170605 2241 GMT

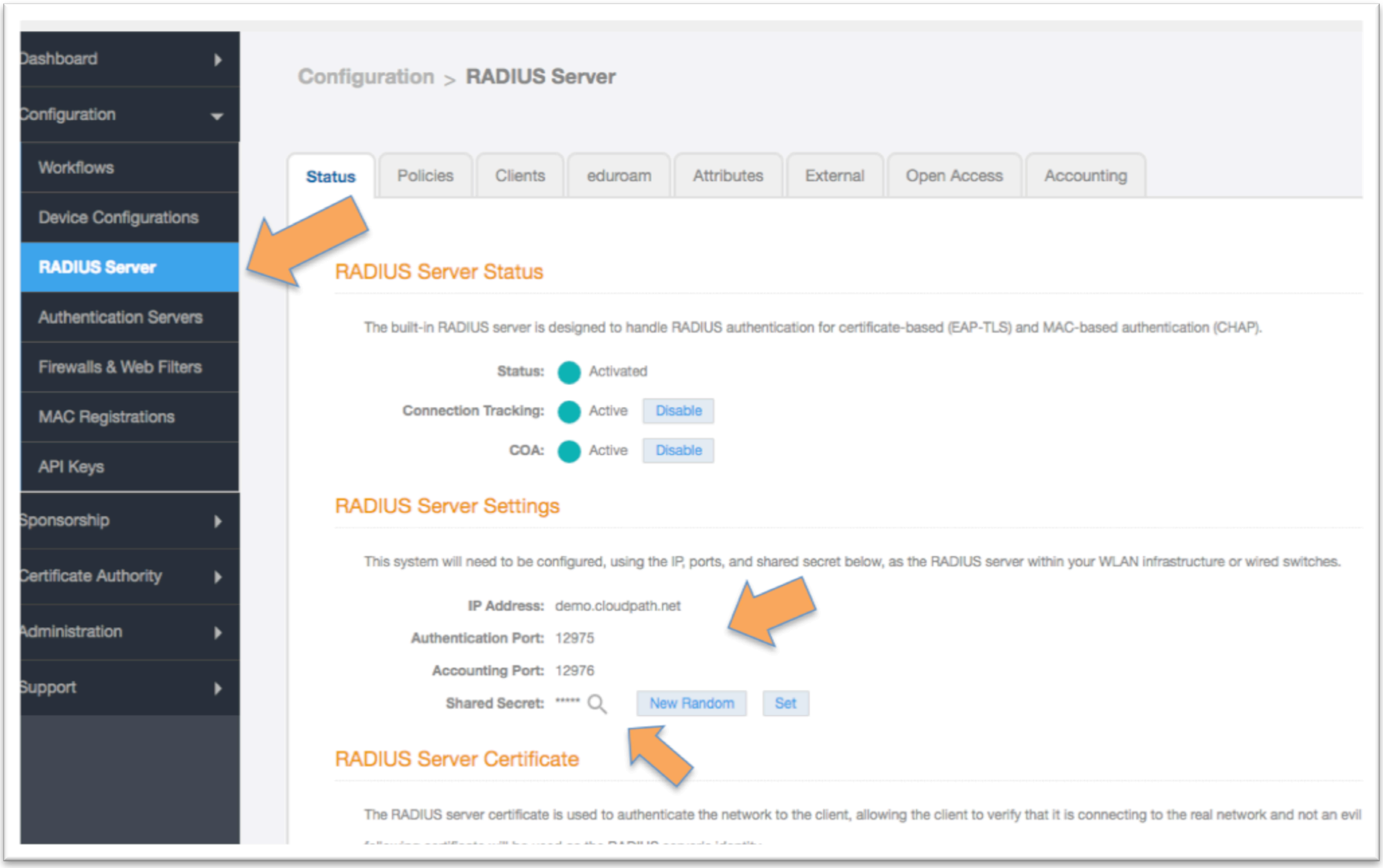
Portal URLs

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

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

QR Code:

- Configuration of a basic workflow in Cloudpath ES is now complete. 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 enrollment URL is found in the advanced tab. In fact, it can be used locally from here.
- Copy this URL to a text editor for later (or be prepare to return to this window).
- This URL will be added to a WLAN controller as a WISPr or external portal



Configuration > RADIUS Server

RADIUS Server Status

The built-in RADIUS server is designed to handle RADIUS authentication for certificate-based (EAP-TLS) and MAC-based authentication (CHAP).

Status: Activated
Connection Tracking: Active
COA: Active

RADIUS Server Settings

This system will need to be configured, using the IP, ports, and shared secret below, as the RADIUS server within your WLAN infrastructure or wired switches.

IP Address: demo.cloudpath.net
Authentication Port: 12975
Accounting Port: 12976
Shared Secret: *****

RADIUS Server Certificate

The RADIUS server certificate is used to authenticate the network to the client, allowing the client to verify that it is connecting to the real network and not an evil

- The WLAN controller will need the RADIUS server settings
- On the main menu on the left, go to “Configuration” and then “RADIUS Server”
- The WLAN controller will need the RADIUS Server Settings
- The IP address or FQDN
- Authentication port
- The Accounting port may be optional
- The Shared Secret – which can be revealed by clicking on the magnifying glass

Please refer to the WLAN controller Best Practices and Deployment Guide appropriate to your environment for further configuration details.

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 Basic Workflow

Onboarding secure users with MAC authentication of guests

August 2017

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