DEPLOYMENT GUIDE

Cloudpath Deployment Guide

Supporting Software Release 5.2

Part Number: 800-71663-001 Rev B
Publication Date: 03 October 2018

Copyright Notice and Proprietary Information

Copyright © 2018 Ruckus Networks, an ARRIS company. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Ruckus Networks (“Ruckus”). Ruckus reserves the right to revise or change this content from time to time without obligation on the part of Ruckus to provide notification of such revision or change.

Destination Control Statement

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, RUCKUS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. Ruckus does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. Ruckus does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to Ruckus that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL RUCKUS, ARRIS, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIES, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF RUCKUS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS.

If you are dissatisfied with the Materials or with the associated terms of use, your sole and exclusive remedy is to discontinue their use.

Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

The Ruckus, Ruckus Wireless, Ruckus logo, Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, Xclaim, and ZoneFlex and trademarks are registered in the U.S. and other countries. Ruckus Networks, Dynamic PSK, MediaFlex, FlexMaster, Simply Better Wireless, SmartCast, SmartCell, SmartMesh, SpeedFlex, Unleashed, ZoneDirector and ZoneFlex are Ruckus trademarks worldwide. Other names and brands mentioned in these materials may be claimed as the property of others.

Wi-Fi Alliance®, Wi-Fi®, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access® (WPA), the Wi-Fi Protected Setup logo, and WMM® are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance.

Contents

Cloudpath Security and Management Platform 7
- Cloudpath Security and Management Platform 7
- What is Cloudpath 8
- Why You Need Cloudpath 8
- Guest Users 9

Workflow Engine 11
- Workflow Building Blocks 11
- Available Workflow Plug-Ins 12
  - Display an Acceptable Use Policy 12
  - Authenticate to a Local Server 13
  - Ask the User to Name the Device 13
  - Ask the User About Concurrent Certificates 13
  - Split Users Into Different Workflow Branches 13
  - Authenticate to a Third-Party 13
  - Authenticate Using a Voucher From a Sponsor 13
  - Perform Out-of-Band Verification Using Email or SMS 13
  - Request Access From a Sponsor 13
  - Register a Device for MAC-Based Authentication 14
  - Display a Message To Users 14
  - Redirect Users to an External URL 14
  - Prompt User For Information 14
  - Authenticate Using a Shared PassPhrase 14
  - Generate a Ruckus DPSK 14
  - Send a Notification 14
- Example Workflow with Two Branches 14
- Example Complex Workflow 16

Enrollment Workflow Use Cases 17
- Overview 17
- Employee With IT Asset Authenticated to AD Group 17
- Employee With Personal Device Authenticated to AD Group 18
- Employee With Personal Device on Internet-Only VLAN 18
- Sponsored Guest on Internet-Only VLAN 19
- Contractor With IT Asset on Internal Network With Limited Access 20

Planning the Local Network Configuration 23
- Overview 23
- WPA2-Enterprise Infrastructure 23
- Setting Up SSIDs 24
  - Guest SSID 24
  - Conflicting SSIDs 24
- Setting Up Captive Portal Redirect 24
- Certificate Authority 25
  - Onboard CA 25
- RADIUS Servers 25
  - Onboard RADIUS Server 25
  - Microsoft NPS Acting as a RADIUS Server 25

External RADIUS Server....26
RADIUS Proxy....26
Additional Radius Configuration Options....26
Supported Authentication Servers....27
Active Directory....27
LDAP or LDAPS....27
Third-Party Authentication....27
RADIUS Using PAP....28
SAML 2.0 IdP....28
Cloudpath Onboard Database....28
DNS....28
Firewall Configuration....28
Use Cases....29

Deployment Scenarios....31
Prerequisites for Configuring Cloudpath....31
Deploying the Virtual Image File....31
Setting up the Initial Account....31
Configuring the Workflow....31
Deploying the Virtual Appliance to a VMware Server....32
Retrieve OVA File....32
Deploying the Virtual Appliance Using a VMware vCenter Client....32
Deploying the Virtual Appliance to a Hyper-V Server....37
Retrieve VHDX Image File....37
Replication With Hyper-V Systems....37
Deploying the Virtual Appliance Using Hyper-V Manager....37
Configure Virtual Processors....38
Deploying the Virtual Appliance Using a Console-Based Client....40
Test Network Connectivity....41
How to Install VMware Tools....41
How to Increase the Virtual Appliance Memory on VMware....42
How to Expand the MySQL Partition Size....42

Activate Account or Log In....45
Overview....45
Activate Account by Activation Code....45
Set a Password for Account....46
Activate Account by Credentials....47

Initial System Setup....49
Overview....49
System Setup Wizard....50
Publishing Tasks....57
ToDo Items....59

Enrollment Workflow....61
Overview....61
Workflow Basics....61
Modifying a Workflow Template....62
Creating a Workflow From a Blank Slate....64
Acceptable Use Policy....66
User Type Split....67

Authentication to a Local Server 67
Device Type Split 69
Prompt for Voucher 71
Device Configuration and Client Certificate 74
Publishing the Enrollment Workflow 77
How to Test a Published Workflow 79

Ruckus Controller Integration for Cloudpath 81
Overview 81
Setting up Cloudpath as an AAA Authentication Server 81
Creating AAA Accounting Server (Optional) 84
Running Authentication Test 85
ZoneDirector 85
SmartZone 85
Unleashed 86
Possible Results from Authentication Test 86
Creating Hotspot Services 87
Setting Up the Walled Garden 92
Creating the Onboarding SSID 94
Enabling Bypass CNA on ZoneDirector 98
Enabling Bypass CNA on Unleashed 99
Creating the Secure SSID 100

Troubleshooting Your Deployment 105
Overview 105
Connectivity Issues 105
Cloudpath License Server 105
RADIUS Server 105
Firewall Requirements 105
Issues with User Credentials 106
Active Directory 106
Credentials Mismatch 106
LDAP 107
DNS Issues 107
Verify that DNS is Working 107
Verify that DNS is Working 107
OSCP Issues 107
OSCP Validation 107
OSCP Server in the DNS 108
Certificate Issues 108
Certificate Chain Not Trusted 108
Common Name in Template 108
SAN Other Name in Certificate Template 108
Missing EKU in the RADIUS Server Certificate 108
NPS-Specific Troubleshooting 108
Register the NPS With the Domain 108
RADIUS Server Certificate Missing Private Key 109
Cloudpath Captive Portal Setup for Cisco Controller 109
Define an ACL that allows access to the Cloudpath webpage 109
Enable Portal Page on the Open SSID and Enforces the Preauthentication ACL 109
Configure the Portal Page 110

Cloudpath Security and Management Platform

- Cloudpath Security and Management Platform..... 7
- What is Cloudpath..... 8
- Why You Need Cloudpath..... 8
- Guest Users..... 9

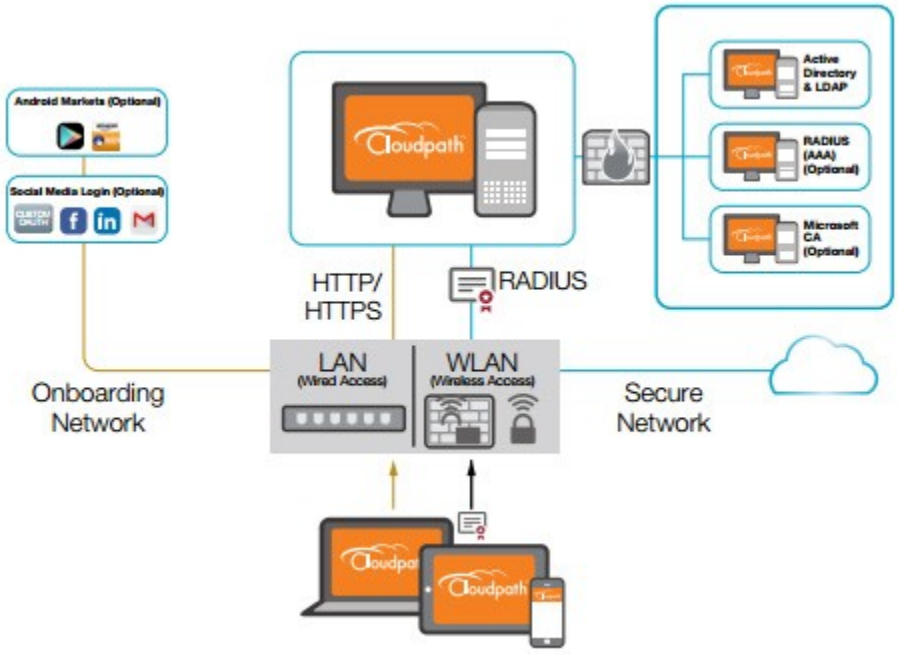
Cloudpath Security and Management Platform

Cloudpath Enrollment System (ES) software is a security and policy management platform that enables any IT organization to protect the network by easily and definitively securing users and their wired and wireless devices—while freeing those users and IT itself from the tyranny of passwords.

Available cloud-managed or as a virtual instance and priced per user, Cloudpath software lets IT do with one system what usually requires many, while easily and automatically integrating with existing access and network security infrastructure.

Cloudpath software consolidates and simplifies the deployment of multiple services that are typically disparate and complex to manage: Certificate Management, Policy Management and Device Enablement.

FIGURE 1 Cloudpath Security and Policy Management Platform



What is Cloudpath

There are two main components that make up Cloudpath: *Secure Onboarding* and *Advanced Certificate Management*. The combination of these two capabilities enable a powerful new way to secure and manage any and every device connecting to the network, while also making it extremely usable for the end user and the administrator. This combination delivers the industry's first *Automated Device Enablement* (ADE) solution.

Secure onboarding capabilities include:

- Self-service automated onboarding for a wide array of devices
- BYOD, partner, and guest access
- Automated configuration
- Secure WPA2-Enterprise encryption with PEAP or EAP-TLS
- Flexible enrollment options - AD, LDAP, OAuth, Social Networks
- Guest sponsorship, email, SMS, and voucher options
- Built-in certificate authorities and Microsoft CA integration
- Works with existing Wi-Fi infrastructure
- Automated system health compliance, including AV, firewalls, NAC, proxies, and software installation

Advanced Certificate Management capabilities include:

- Unique per-device certificate management
- Automated certificate distribution
- Self-service certificate enrollment and installation.
- Dynamic policies based on user, device, ownership (BYOD or IT-owned), access needs
- Manage access activation and termination based on employee status
- Visibility into every device connected to the network, enrollment options, form factor and expiring certificates using automated reports on the dashboard
- Per-device policy control, visibility, and utilization tracking

Why You Need Cloudpath

Cloudpath provides one portal for automatically onboarding authorized devices on the secure network. The process is simple enough to be self-service, unobtrusive in that the application is dissolvable, automated so that the migration to the secure network can be managed without contacting the help desk. Cloudpath makes for a better Wi-Fi experience by simplifying the network, and it can be implemented in your existing WLAN infrastructure because it uses standards-based WPA2-Enterprise.

By using Cloudpath, you keep unauthorized devices off the secure network. With user and device authorization, issues with sniffers, snoopers and evil twins are prevented. The reporting capabilities allow user and device visibility and control, so that a network administrator has a view of what is happening on the network.

Guest Users

Cloudpath works entirely in the background as it delivers the most secure method of WPA2- Enterprise, EAP-TLS to mobile devices, including guest users. Through the use of non-intrusive native supplicant configuration, Cloudpath allows guest users to use the same entry point as employee or student users then automatically moves them to encrypted WPA2-Enterprise wireless networks. Guests can also sign in using third-party authentication, such as Facebook, LinkedIn or Gmail.

Workflow Engine

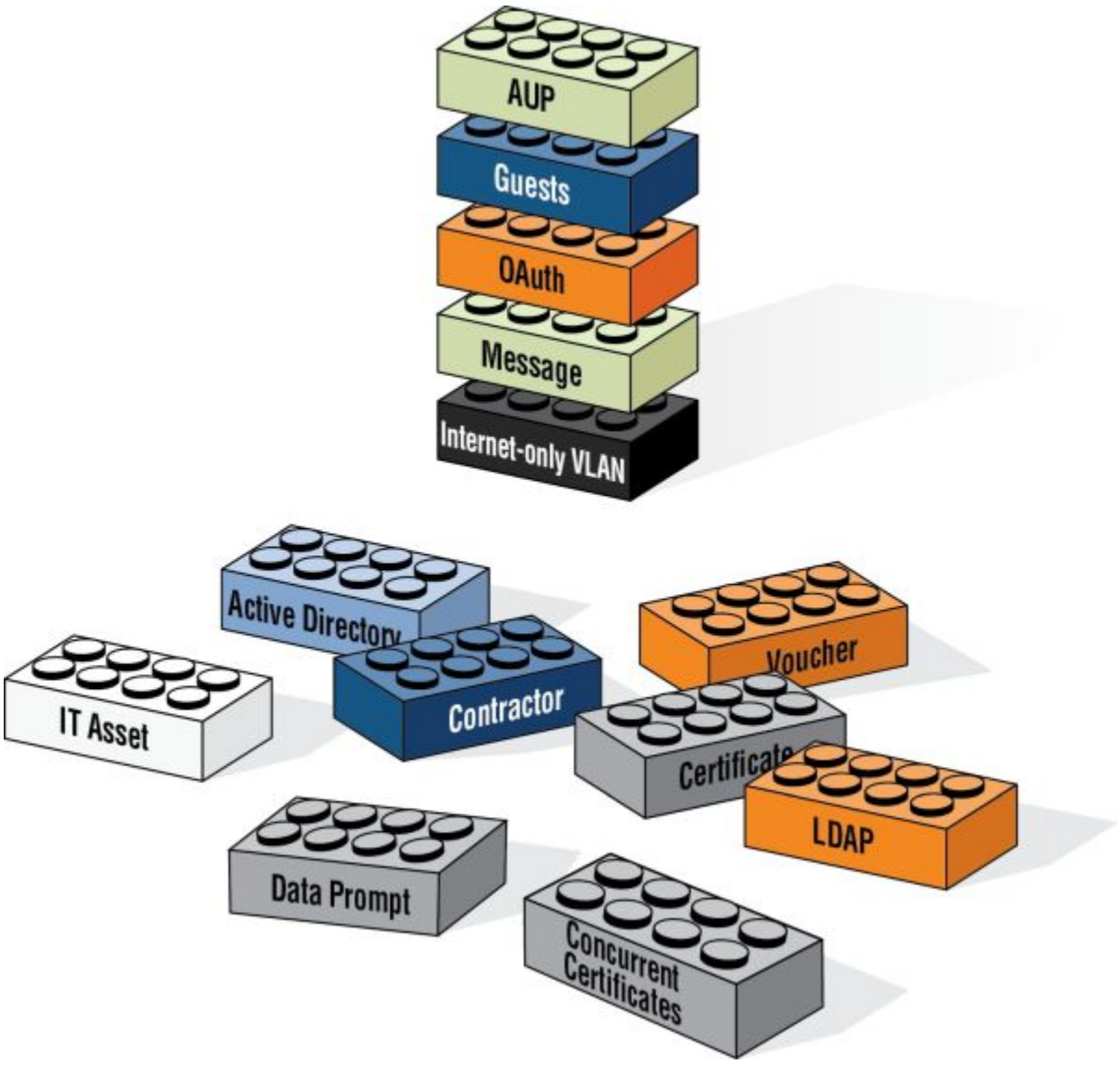
- Workflow Building Blocks..... 11
- Available Workflow Plug-Ins..... 12
- Example Workflow with Two Branches..... 14
- Example Complex Workflow..... 16

Workflow Building Blocks

The Cloudpath workflow engine is a customizable enrollment process that provides more control over who is granted network access and how they should be provisioned.

The enrollment workflow is built using a series of blocks, with each building block representing a step in the onboarding process. A workflow step might be an acceptable use policy, a display message, or an authentication hurdle. These steps, combined in a variety of different sequences, create an enrollment workflow for every device type and every user type on your network. The end result is a lot of flexibility for different use cases.

FIGURE 2 Basic Workflow



Available Workflow Plug-Ins

Cloudpath provides the following building blocks, called workflow plug-ins, which can be added to the enrollment workflow.

Display an Acceptable Use Policy

An acceptable use policy (AUP) prompt displays a message to the user and requires that they signal their acceptance. This is typically used for network policies or end-user license agreements (EULAs).

Authenticate to a Local Server

If you authenticate users to a local server, Cloudpath supports authentication using an Active Directory, LDAP (or LDAPS), or via a RADIUS server using PAP.

Ask the User to Name the Device

The **Cleanup Devices** plug-in 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

The **Cleanup Certificates** plug-in provides a method for allowing users to maintain the number of certificates registered to their devices. You can configure a certificate limit, and during the enrollment process, prompt the user to review information about previously distributed certificates.

Split Users Into Different Workflow 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

When you combine third-party authentication with traditional authorization methods, the social media provides additional identity information during the onboarding process to deliver automated, self- service access to the WPA2-Enterprise wireless network. Cloudpath supports third-party integration using Facebook, LinkedIn, Google, or you can specify a custom OAuth 2.0 server.

Authenticate Using a Voucher From a Sponsor

When you use a voucher for authorization, the user is provided with a one-time password (OTP) and is prompted for this password during the enrollment process. Vouchers can be used to control access separate from, or in addition to, user credentials. For example, use vouchers for self-service registration of IT assets, or for authenticating network access for partners.

Perform Out-of-Band Verification Using Email or SMS

Out of band verification allows the user to enter an email address or phone number and have the verification code, or one-time password, sent to them. The out of band prompt is tied to a voucher list, which controls the characteristics of the one-time password (OTP). You can create a new voucher list specifically for out of bound verification or use an existing list.

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 a Device for MAC-Based Authentication

Registers the MAC address of the device for MAC authentication by RADIUS. This is used for two primary use cases:

- To authenticate the device on the current SSID via the WLAN captive portal.
- To register a device, such as a gaming device, for a PSK-based SSID.

In both cases, the MAC address is captured and the device is permitted access for a configurable period of time.

Display a Message To Users

The message plug-in provides information to the end-user. The message is displayed, along with a single button to **Continue**. Use the message plug-in to welcome partners or guest users to your network and provide links for where to get additional information.

Redirect Users to an External URL

Redirects the user to a specified external URL. This may be used to authenticate the user to the captive portal of the onboarding SSID.

Prompt User For Information

The data prompt plug-in provides a means for gathering information about a user. This user data can be used for informational purposes only, or for configuration purposes, such as personalizing certificates.

Authenticate Using a Shared PassPhrase

This authentication method prompts the user for a shared passphrase and verifies that it is correct. A shared passphrase is useful for controlling access to an enrollment process separate from, or in addition to, user credentials.

Generate a Ruckus DPSK

Generates a a Dynamic Pre-shared Key (DPSK) via a Ruckus WLAN controller. This allows, for example, a gaming system to be registered and issued a unique PSK.

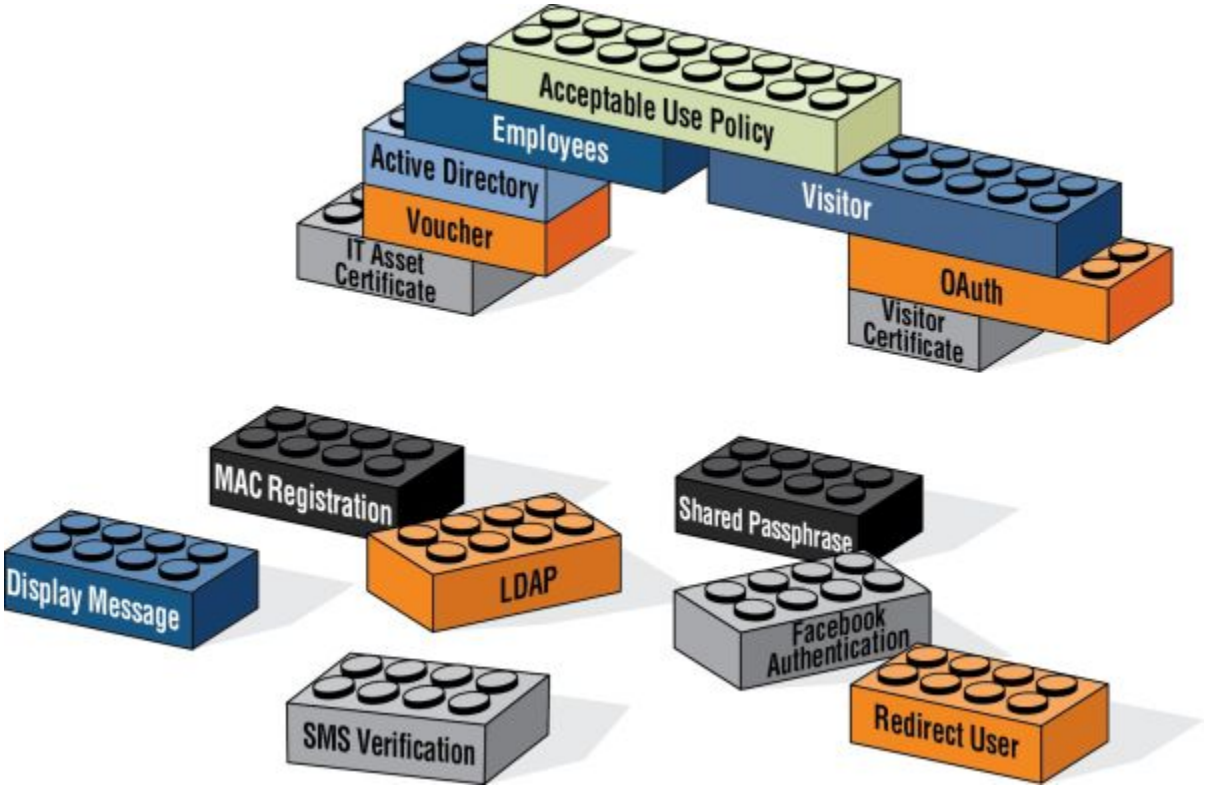
Send a Notification

Generates a notification about the enrollment, and can be added anywhere in the workflow. Notification types include email, SMS, REST API, syslog and more. This step is invisible to the end- user. All enrollment-related data is available for use in the notification via variables.

Example Workflow with Two Branches

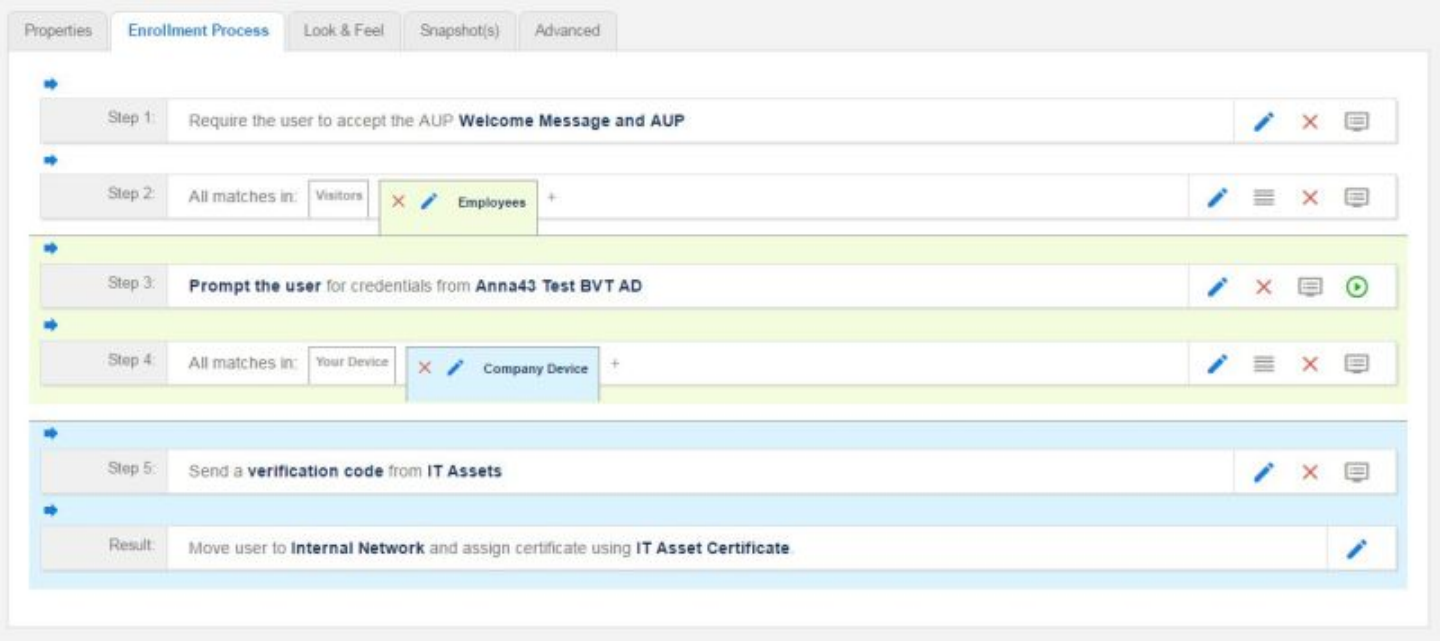
The following image represents a workflow that is split into two branches, with one sequence of steps for employees, and another for guest users. Each branch in the workflow specifies a different authentication method and assigns different certificates to the user.

FIGURE 3 Workflow With 2 Branches



The model workflow above translates to the following example workflow in Cloudpath.

FIGURE 4 Cloudpath Simple Workflow

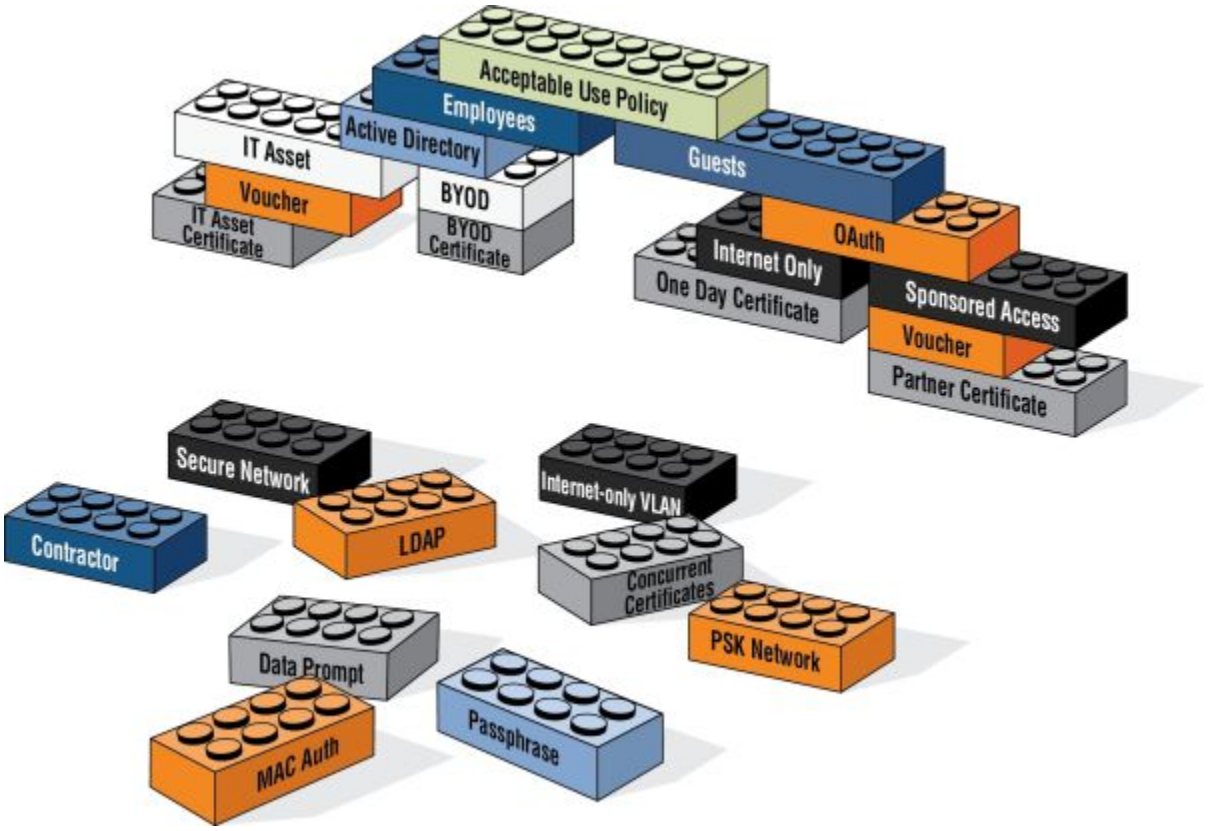


After the workflow is in place, you can fine-tune settings for specific OS versions, updates, and features, including customizations to the user experience. See Device Configuration and Client Certificate.

Example Complex Workflow

The following image represents a more complex, yet easy to configure workflow with multiple branches. The first split in the workflow accommodates different user types, and the other splits provide a different sequence of events for device types, internal and external network access, and provide client certificates with the appropriate validity period.

FIGURE 5 Complex Workflow



Enrollment Workflow Use Cases

- Overview....17
- Employee With IT Asset Authenticated to AD Group....17
- Employee With Personal Device Authenticated to AD Group....18
- Employee With Personal Device on Internet-Only VLAN....18
- Sponsored Guest on Internet-Only VLAN....19
- Contractor With IT Asset on Internal Network With Limited Access....20

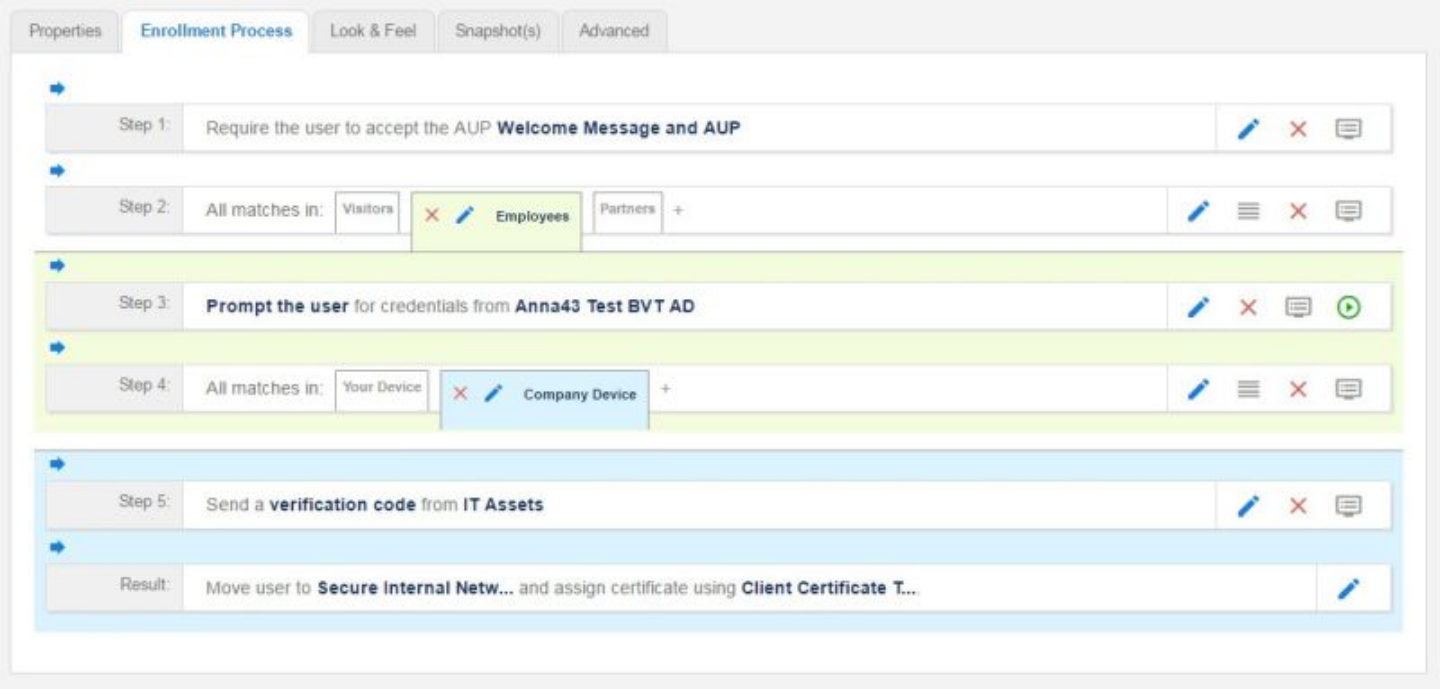
Overview

This section provides some enrollment workflow examples to help you get familiar with the different types of steps that can be configured with Cloudpath.

Employee With IT Asset Authenticated to AD Group

This is an example workflow for an employee using an IT-assigned device to access the secure network. The employee is authenticated to an Active Directory group, and the device type split is managed with a filter, which moves the user to the Company Device workflow branch if they are a member of a specified AD group. They are prompted to enter a previously sent/assigned voucher and moved to a secure internal network.

FIGURE 6 Example Workflow for Employees with IT Assets

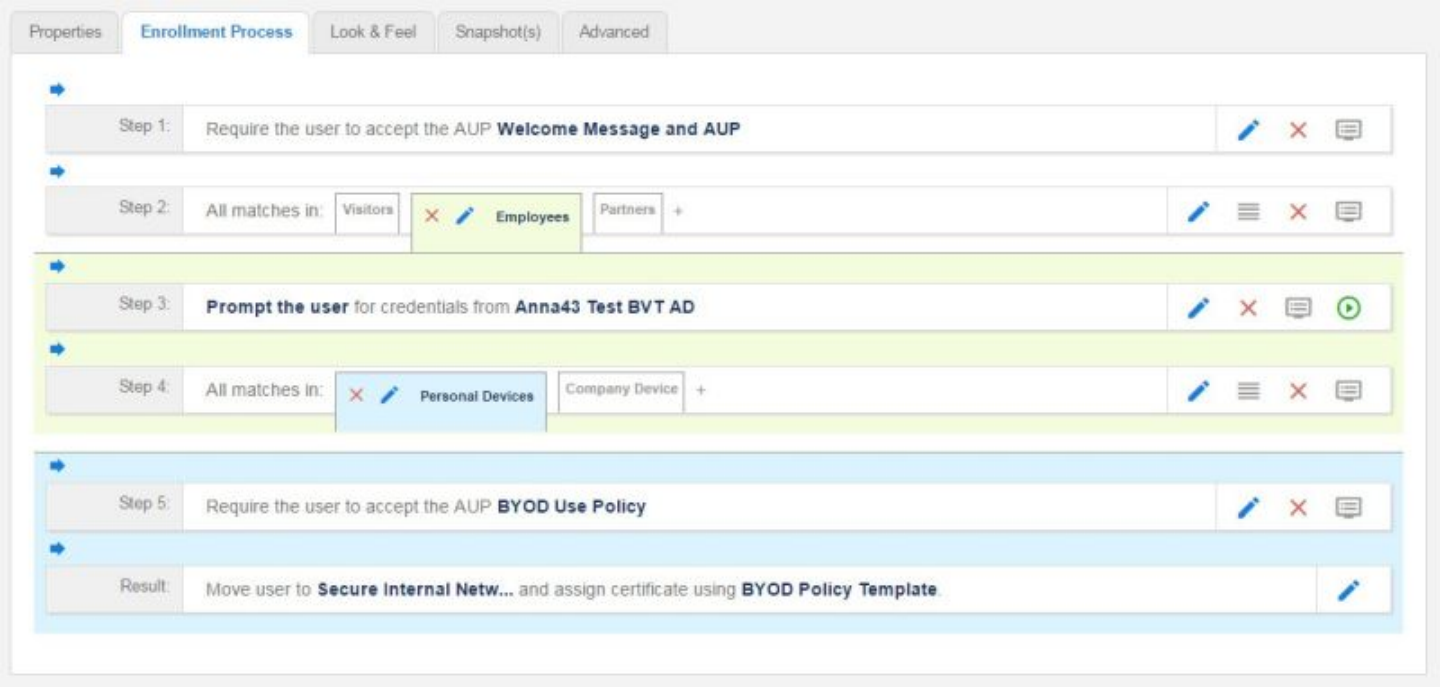


Your workflow does not have to be in the same order as the example. For example, you can move the authentication to LDAP step to immediately after the AUP step and then have the split for different workflow branches be immediately following. If you set up a filter on the LDAP group name, users can be moved to the appropriate workflow branch.

Employee With Personal Device Authenticated to AD Group

This is an example workflow for an employee using a personal device to access the secure network. The employee authenticates to an Active Directory group, and the device type split is managed with a filter, which displays the Personal Device workflow branch only if they are a member of a specified AD group. The user is asked to acknowledge a BYOD use policy before being moved to a secure internal network.

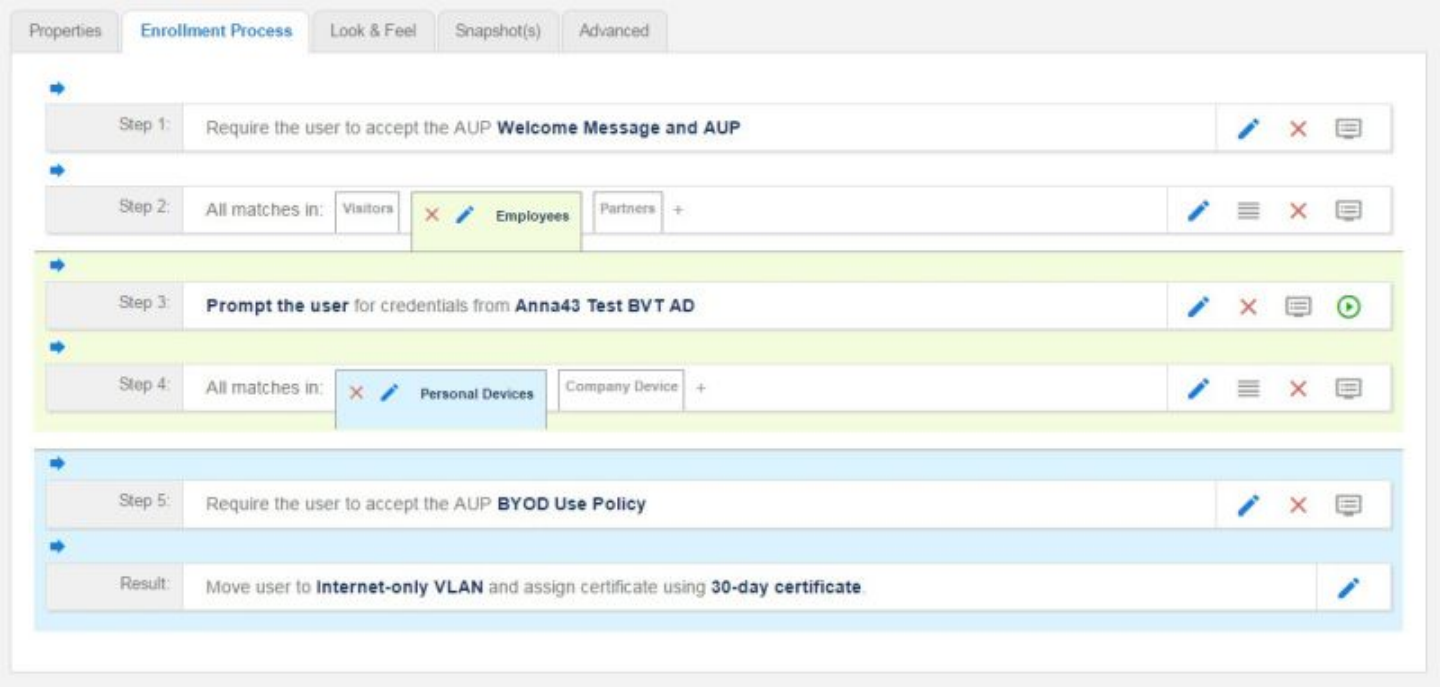
FIGURE 7 Example Workflow for Employees with Personal Devices (BYOD)



Employee With Personal Device on Internet-Only VLAN

This is an example workflow for an employee using a personal device on the secure network, but is limited to an Internet-only VLAN. The employee authenticates to an Active Directory group, and the device type split is managed with a filter, which moves the user to the Personal Device workflow branch if they are a member of a specified AD group. The user is asked to acknowledge a BYOD use policy before being moved to an Internet-only VLAN with a certificate that is limited to 30 days access.

FIGURE 8 Example Workflow for Employees with Personal Devices on Internet-only VLAN

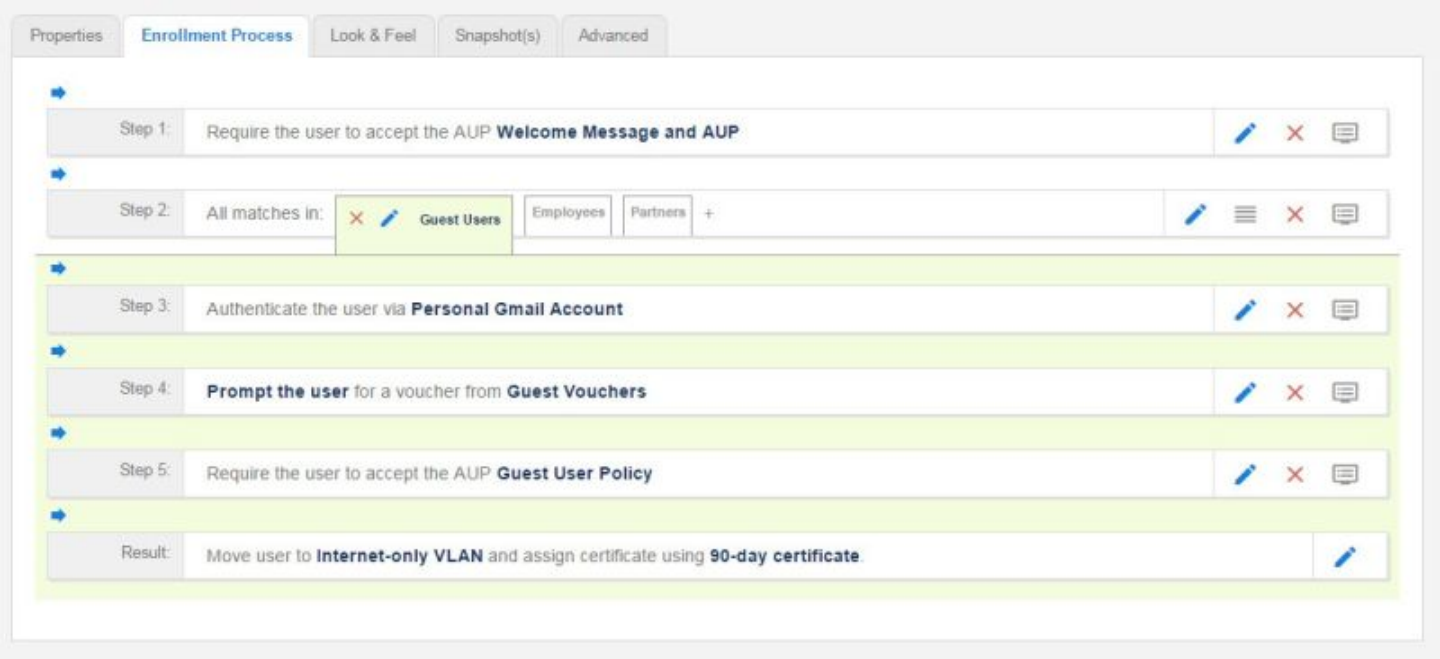


Sponsored Guest on Internet-Only VLAN

This is an example workflow for a sponsored guest to onboard to the secure network but is limited to an Internet-only VLAN. The guest authenticates using a personal Gmail account, and is verified using a voucher distributed from the employee sponsor. The user is asked to acknowledge a guest user policy before being moved to an Internet-only VLAN with a certificate that is limited to 90 days access.

For details on the sponsored guest access feature, see the *Setting Up Sponsored Guest Access Within Cloudpath* document on the Cloudpath Admin UI **Support** tab.

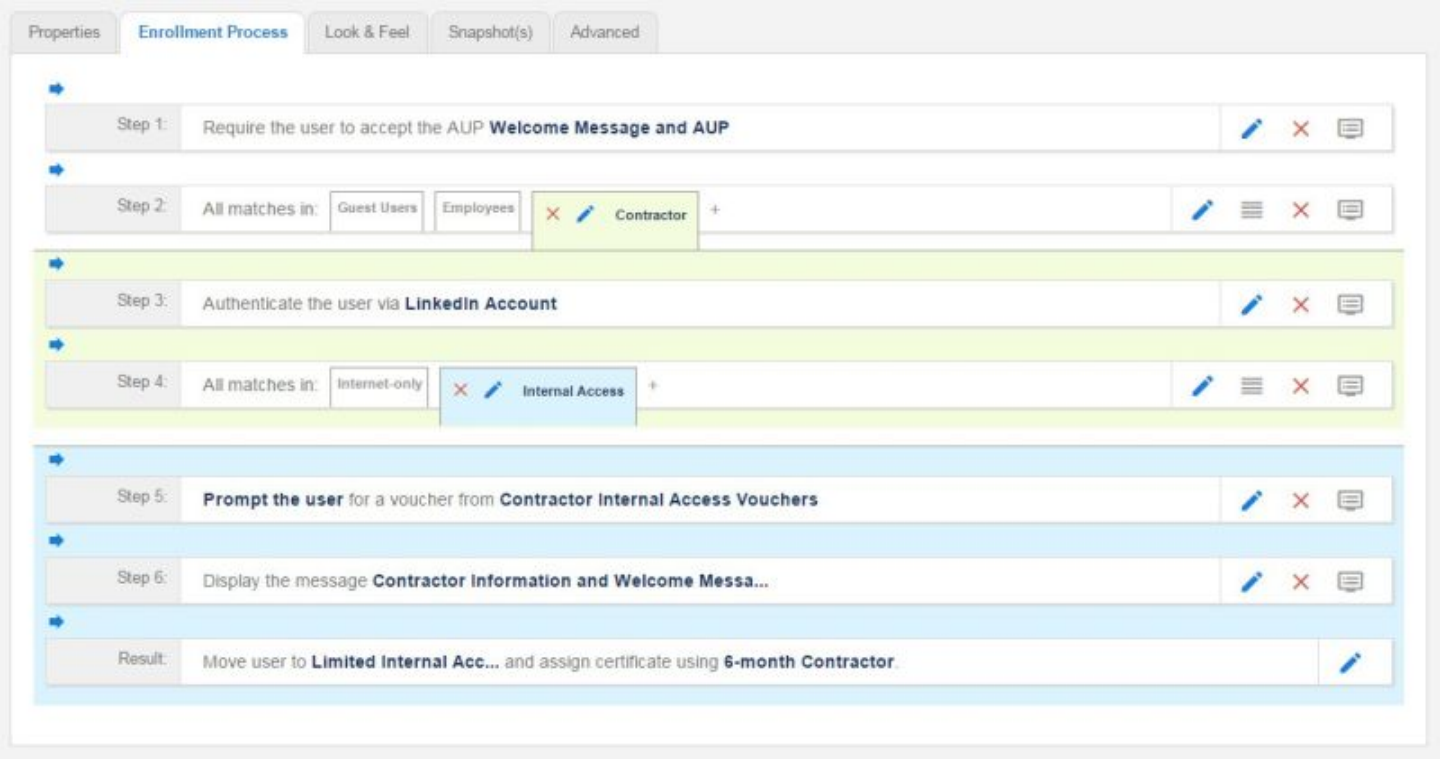
FIGURE 9 Example Workflow for Sponsored Guests on Internet-only VLAN



Contractor With IT Asset on Internal Network With Limited Access

This is an example workflow for a sponsored contractor to onboard to the secure network for a specified amount of time with limited access. The contractor authenticates using an OAuth account (Facebook, LinkedIn, or Google), and is verified using a voucher distributed from the employee sponsor. A Contractor Information message is displayed before moving them to a VLAN with limited internal access and a certificate that limits access to 6 months.

FIGURE 10 Example Workflow for Contractors with IT Assets



Planning the Local Network Configuration

- Overview....23
- WPA2-Enterprise Infrastructure....23
- Setting Up SSIDs....24
- Setting Up Captive Portal Redirect....24
- Certificate Authority....25
- RADIUS Servers....25
- Supported Authentication Servers....27
- DNS....28
- Firewall Configuration....28
- Use Cases....29

Overview

The process of configuring and connecting a device to the secure network requires the integration of many components of your network. The wireless LAN controller redirects to Cloudpath. Cloudpath issues a user certificate based on user store credentials. The client is authenticated by a RADIUS server, which verifies the certificate. The network Wizard installs the certificate in the local certificate store and migrates the user to the secure network.

Before you implement Cloudpath in your network, consider the following components of your network.

- WPA2-Enterprise Infrastructure
- Setting Up SSIDs
- Setting Up Captive Portal Redirect
- Certificate Authority
- RADIUS Servers
- Supported Authentication Servers
- DNS
- Firewall Configuration
- Use Cases

WPA2-Enterprise Infrastructure

Cloudpath works in your existing WLAN infrastructure using standards-based WPA2-Enterprise.

The following basic components are required for setting up a WPA2-Enterprise network. These components most likely exist in your network and can easily be configured to work with Cloudpath to complete the secure Wi-Fi configuration in your network.

- WPA2-Enterprise requires an external authentication server (RADIUS or NPS) to handle 802.1X user authentication.
- WPA2-Enterprise requires a CA to issue and install certificate on the RADIUS server
- The external authentication server (RADIUS or NPS) client database should be populated with the IP address and shared secret for each access point and user data with usernames and passwords for each end-user.

- On each AP, configure WPA2-Enterprise and add the authentication server (RADIUS or NPS) IP address and shared secret.

Setting Up SSIDs

Cloudpath requires an open SSID for onboarding, and one or more secure SSIDs, depending on your deployment scheme. The open SSID terminates to a captive portal that points to Cloudpath, and the secure SSID is the network to which your users migrate. We recommend creating an SSID specifically for Cloudpath.

Configure the secure SSID to use TLS, and point the RADIUS authentication requests to the RADIUS sever, whether that is the Cloudpath onboard RADIUS server, a Microsoft NPS, or other external RADIUS server.

Guest SSID

If your security policy provides a guest SSID for Internet-only or limited network access, you can set up an open SSID specifically for guests. The guest SSID redirects guest users to the Cloudpath captive portal, where they can onboard to a limited access network. The limited access is managed using VLAN assignment, which is configured in the wireless LAN controller, where you can also filter, shape or throttle the guest VLAN.

Conflicting SSIDs

Cloudpath provides a method for managing conflicting SSIDs to prevent a device from roaming away from the secure network. When setting up the device configuration, in the conflicting SSID section, you can set it up to either delete the open SSID or set it to connect manually. See Device Configuration and Client Certificate.

Setting Up Captive Portal Redirect

After the SSIDs are set up, configure a captive portal page on your wireless controller so that it redirects users from the open SSID to the Cloudpath web page to begin the enrollment process.

- On the Wireless LAN Controller (WLC), configure the open SSID pre-authentication ACLs to permit access to the IP address of the Cloudpath server. Configure the WLC to point to Cloudpath as an **External** captive portal.
- Set up the secure WPA2-Enterprise SSID to delegate authentication to the Cloudpath onboard RADIUS server, the NPS, or an external RADIUS server.

  NOTE
  If using an external RADIUS server, you must configure layer 3 access to the Cloudpath virtual appliance to allow certificate status verification.

For more information, see the following sections in this guide:

- Ruckus Controller Integration for Cloudpath
- Cloudpath Captive Portal Setup for Cisco Controller

Certificate Authority

A WPA2-Enterprise network requires a certificate authority (CA) to issue and verify certificates on the RADIUS server. Cloudpath supports many different CA configurations, including an onboard CA to act as your own private CA, certificates issued from an external CA, or Cloudpath acting as a proxy for an existing CA.

If you are using a Microsoft CA, the Cloudpath onboard CA can be configured as your intermediate CA, leaving the your Microsoft CA as your root CA.

Onboard CA

The Cloudpath onboard CA can issue a server certificate to the onboard RADIUS server and it can issue client certificates. After the client certificate issued, all authentications take place using the certificate.

The onboard CA is a full X.509 public key infrastructure (PKI), which can issue client and server certificates binding a public key to a particular common name.

RADIUS Servers

WPA2-Enterprise requires an authentication server for issuing client certificates for the wireless authentication. Cloudpath provides an onboard RADIUS server, supports integration with your existing RADIUS server, or integration with a Microsoft Network Policy Server acting as a RADIUS server.

For all configurations:

- The wireless controller requires the port number and shared secret from the RADIUS server.

  NOTE
  If using the onboard RADIUS server, the shared secret and port number can be found on the **Administration** > **System Services** > **RADIUS** component page.

- Apply the RADIUS authentication server to the secure SSID.
- Populate the client database for an external authentication server with the IP address and shared secret for each access point and the user data with usernames and passwords for each end- user.

Onboard RADIUS Server

The onboard RADIUS server, which is a a FreeRADIUS server that has been optimized for TLS, is configured as part of the initial system setup. The RADIUS server issues client certificates and the client validates the RADIUS server by hostname.The onboard RADIUS server supports all vendor- specific attributes in the FreeRADIUS dictionary.

If you are using the onboard RADIUS server, Cloudpath can generate a RADIUS server certificate using the onboard CA and server certificate template. This certificate can be installed on the onboard RADIUS server as part of the initial system setup.

Microsoft NPS Acting as a RADIUS Server

If you are using the NPS acting as a RADIUS server, you must set up the NPS server role and a RADIUS server.

These steps are required when configuring Cloudpath to integrate with the NPS:

- Create a server certificate template for the NPS.

- Generate a server certificate for the NPS. Use the FQDN of the NPS server as the **ServerName**
- when you generate the certificate using the onboard CA.
- Download the Private Key of the Root CA.
- Import the private key of RADIUS server certificate for NPS into the **Personal Trust** store. The private key must be in *.key format.
- Import the Public Key of the Root CA in to the **Enterprise Trust** store. The public key must be in *.cer format.

NOTE
See the *Cloudpath Integration with Microsoft NPS Configuration Guide* for configuration details.

External RADIUS Server

If you prefer to use an existing RADIUS server in your network, you must add the IP address of the RADIUS server to Cloudpath to allow signed certificates to be uploaded to Cloudpath and the public certificate of the CA (onboard or external).

Alternately, a CSR can be used within Cloudpath to create a usable RADIUS certificate.

RADIUS Proxy

Cloudpath supports RADIUS proxy from an external RADIUS servers. For example, you can set up a configuration so that a certificate from a specific domain (@guest) is proxied to Cloudpath for authentication. When the external RADIUS server receives a RADIUS request from user@guest, the request is forwarded to the onboard RADIUS server.

This proxy configuration is set up on the external server.

To set up RADIUS Proxy on a Network Policy Server (NPS):

1. Go to **RADIUS Clients and Servers** and add a Remote RADIUS Server Group. The group will have one member, the Cloudpath server. Enter the IP address and shared secret from NPS.
2. Go to **Connection Request Policies**, add a policy for the RADIUS proxy. Add a Condition so that the NPS looks for the @guest in the username and, if found, forwards the request to the “remote radius group”, which is the Cloudpath server.

Cloudpath receives the request (similar to it coming straight from the access point) and responds.

Additional Radius Configuration Options

RADIUS Accounting

RADIUS Accounting, which provides start/stop information and byte counts on the connection, is supported on port 1813.

RADIUS Server VLAN Attributes

When setting up SSIDs in the WLC, you can use VLANS to apply policies for different groups by combining the VLAN in the RADIUS Request as a RADIUS attribute. RADIUS attributes are configured on the certificate template.

VLAN Tagging

The onboard RADIUS server can assign policy information for devices by defining VLAN tags in the certificate template.

If you are using the Microsoft NPS as a RADIUS server, VLAN tags are managed from the NPS.

Certificate Revocation

You can disable network access in Cloudpath by revoking the user or device certificates.

- When using the NPS acting as your RADIUS server, you can disable the AD account, and because the AD and RADIUS server are tied together, the disabled account status is registered by the RADIUS server.
- When using the onboard RADIUS server:
  - To disable access for a user, locate the certificates associated with the user account and revoke these certificates in Cloudpath.
  - To disable access for a device, revoke only the certificate associated with the device.

Supported Authentication Servers

Cloudpath supports Active Directory, LDAP and a variety of third-party authentication servers, such as Facebook, LinkedIn, or Google.

Active Directory

When using Active Directory with Cloudpath, the initial user authorization is established using AD credentials, and subsequent authentications are based on the client certificate.

Consider the following information when using Active Directory in your network.

- You need AD domain information (plus any sub domains) and the IP address of the AD server.
- Set up your AD groups for use with wireless BYOD access or Sponsorship Grounds (if needed).
  - Cloudpath must have layer 3 access to the AD server.
- The AD host is an LDAP call and must be an IP routable address.
- During authentication, the username is compared to the AD SAM attribute.
- The FQDN of your AD server or IP address maps to the internal AD server IP address.
- If you are using one of the hosted Cloudpath systems (onboard.cloudpath.net, onboard2.cloudpath.net, etc.), check the Firewall Requirements page for the DNS IP address.
- Cloudpath communicates to the AD server using TCP Port 389, LDAPS TCP/UDP 636.

LDAP or LDAPS

To use LDAP with Cloudpath, you need:

- DNS/IP of the active directory server
- DN of the domain
- Username and password to bind to the LDAP server
- Cloudpath communicates to the LDAP server using TCP Port 389.

Third-Party Authentication

When you combine third-party authentication with traditional authorization methods, the social media provides additional identity information during the onboarding process to deliver automated, self- service access to the WPA2-Enterprise wireless

network. Cloudpath supports third-party integration using Facebook, LinkedIn, Google, or you can specify a custom OAuth 2.0 server.

To use third-party authentication, you need the following application information.

- Facebook - App ID and Secret
- LinkedIn - API Key and Secret Key
- Google - Client ID and Client Secret.

  NOTE
  For details on configuring Facebook, LinkedIn, or Google applications, see the appropriate configuration guide on the Cloudpath Admin UI **Support** tab.

RADIUS Using PAP

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

SAML 2.0 IdP

Cloudpath allows a Security Assertion Markup Language (SAML) Identity Provider (IdP) to be configured as an Authentication Server. With traditional authentication server types (LDAP, AD, etc) Cloudpath prompts for username/password, and the authentication server verifies the credentials. With SAML, Cloudpath delegates the IdP to prompt the user for credentials and verify the authentication.

Cloudpath Onboard Database

Select this option to enable end-users to authenticate to accounts defined within this system. This option is not meant to replace AD or LDAP system, but is useful for trial and demo accounts. It also allows you to create policies based on group information.

DNS

DNS should be configured for Cloudpath and other components in your network. Consider the following information when setting up DNS in your network.

- Configure DNS for use with Active Directory.
- The host name of Cloudpath is the FQDN hostname you assign for DNS.

See DNS Issues in the Troubleshooting section of this document.

Firewall Configuration

This section describes the firewall ports that may need to be configured to use Cloudpath and Wizard. Cloudpath must be able to communicate with:

- xpc.cloudpath.net (TCP 80/443-HTTP/HTTPS)
- dist2.cloudpath.net (used for Cloudpath updates TCP 80/443-HTTP/HTTPS)
- NTP server, 0.centos.pool.ntp.org on the standard NTP port (123). This can be configured to point to a local server during system setup, if you prefer.

Depending on your network configuration, you might be required to configure other firewall ports. See the following table.

TABLE 1 Firewall Ports for Use with Cloudpath

Port	Protocol	Notes
80	TCP and UDP	Android Communications
443	TCP and UDP	Android communications with Google Play and Amazon Market.
5228	TCP and UDP	Android APK
389	TCP	Active Directory, LDAP queries
80	TCP	NPS query to Cloudpath for OCSP
1812	UDP	RADIUS Authentication
1813	UDP	RADIUS Accounting
8022		SSH. This is the default port for SSH.
22		SSH. This port can be configured for SSH.
3268	TCP	LDAP recursive domains
	Windows RPC	I f you are using the Integration Module for Microsoft CA, the web server communicates with the Microsoft CA using Windows RPC.
3799	UDP	RADIUS Change of Authorization (CoA)
pool.ntp.org: 123		Perform NTP synchronization.

After Cloudpath is configured, a Firewall Requirements page is provided to help you understand the traffic to and from the system. Navigate to **Administration** > **Firewall Requirements** or see the Troubleshooting Your Deployment section for more information.

Use Cases

Before configuring your network for use with Cloudpath, you should have some idea about your deployment scheme for the different users in your network.

Use these questions to help you determine a deployment scheme.

- Will employees be allowed to access the secure network with personal devices?
- Do you want employees to sponsor guest user?
- How will guest users be authenticated? or do you want them to use a third-party authentication? or will you place them in an Internet-only VLAN?
- Should contractors have limited access? How long should we allow them on the secure network?
- How long do you want the different user types have access to the secure network?

The Enrollment Workflow Use Cases section provides common use cases that you can use as workflow templates when planning your own deployment scheme.

Deployment Scenarios

- Prerequisites for Configuring Cloudpath.....31
- Deploying the Virtual Appliance to a Hyper-V Server..... 37

Prerequisites for Configuring Cloudpath

Before you set up Cloudpath in your network, you need the following information:

Deploying the Virtual Image File

- VMware server or Microsoft Hyper-V Manager on which you'll install the Cloudpath virtual appliance.
- The URL where the image file resides. A Cloudpath representative provides this information.
- Hostname of the virtual appliance
- IP address (and netmask) being assigned to Cloudpath on the VMware server. Not needed if using DHCP.
- IP address to restrict administrator access
- IP address of the DNS server(s).
- Gateway IP address

Setting up the Initial Account

- Login credentials for the Cloudpath License Server
- License Server URL
- HTTPS server certificate
- Company Information (Domain, URL)
- DNS hostname
- Active Directory domain, DNS/IP address of AD server, and DN of AD domain or LDAP server.
- WWW certificate (public-signed)

If you are not using the Cloudpath onboard CA, you also need:

- Public and Private key of existing CA
- RADIUS server certificate (if not using onboard RADIUS server)

Configuring the Workflow

This section lists items to consider when you configure the workflow:

- An idea about the types of access and policies you want to offer different users.
- Images and color schemes if you plan to customize the webpage display.
- AD group names for creating filters in the workflow.
- An idea about the security policy for passwords, vouchers, and certificates.
  - Vouchers have configurable format and validity periods.

  - Certificates have configurable key lengths, algorithm types, and validity periods.
- The SSID for the secure network.
- A list of conflicting SSIDs (open SSIDs, to prevent roaming)
- An idea about which OS families and versions to support.
- Additional requirements for device configurations (for example, enable firewall, proxy, verify antivirus, enable screen lock passcode).

Deploying the Virtual Appliance to a VMware Server

NOTE
If using a Microsoft Hyper-V deployment, see Deploying the Virtual Appliance to a Hyper-V Server.

The deployment process consists of the following steps:

- Retrieve OVA File
- Deploying the Virtual Appliance Using a VMware vCenter Client

or

- Deploying the Virtual Appliance Using a Console-Based Client Test Network Connectivity
- Test Network Connectivity

Retrieve OVA File

If you are setting up a Cloudpath account for the first time, you will be sent an activation code in an email notification. For an on-premise deployment, the activation code link allows you to download the Cloudpath OVA, binding your OVA file to the activation code.

When the download is complete, deploy the OVA file using a VMware client.

Deploying the Virtual Appliance Using a VMware vCenter Client

1. Open the VMware client.
2. Select **File** > **Deploy OVF Template**.
3. Enter the file path or URL where the OVA file resides.
4. Accept the EULA.
5. Enter a unique name for the virtual appliance.

6. Select a deployment configuration:
   - Non-Production POC - Deploys using 6GB RAM and 2 vCPUs x 1 Core. Recommended for software trials, feature testing, and other non-production systems.
   - 4,000 or Fewer Users - Deploys using 8GB RAM and 2 vCPUS x 2 Cores. Recommended for production systems with fewer than 4,000 users.
   - 8,000 or Fewer Users - Deploys using 12GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with fewer than 8,000 users.
   - More than 8,000 Users - Deploys using 16GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with more than 8,000 users.
   - More than 20,000 Users - Deploys using 20GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with more than 20,000 users.
7. If you are using VMware vCenter™ Server to manage your virtual environment, select the appropriate data center, cluster, host, and destination storage, as needed.
   - Use **Thick** provisioning for a production environment. For a thick provision, the total space required for the virtual disk is allocated during creation.

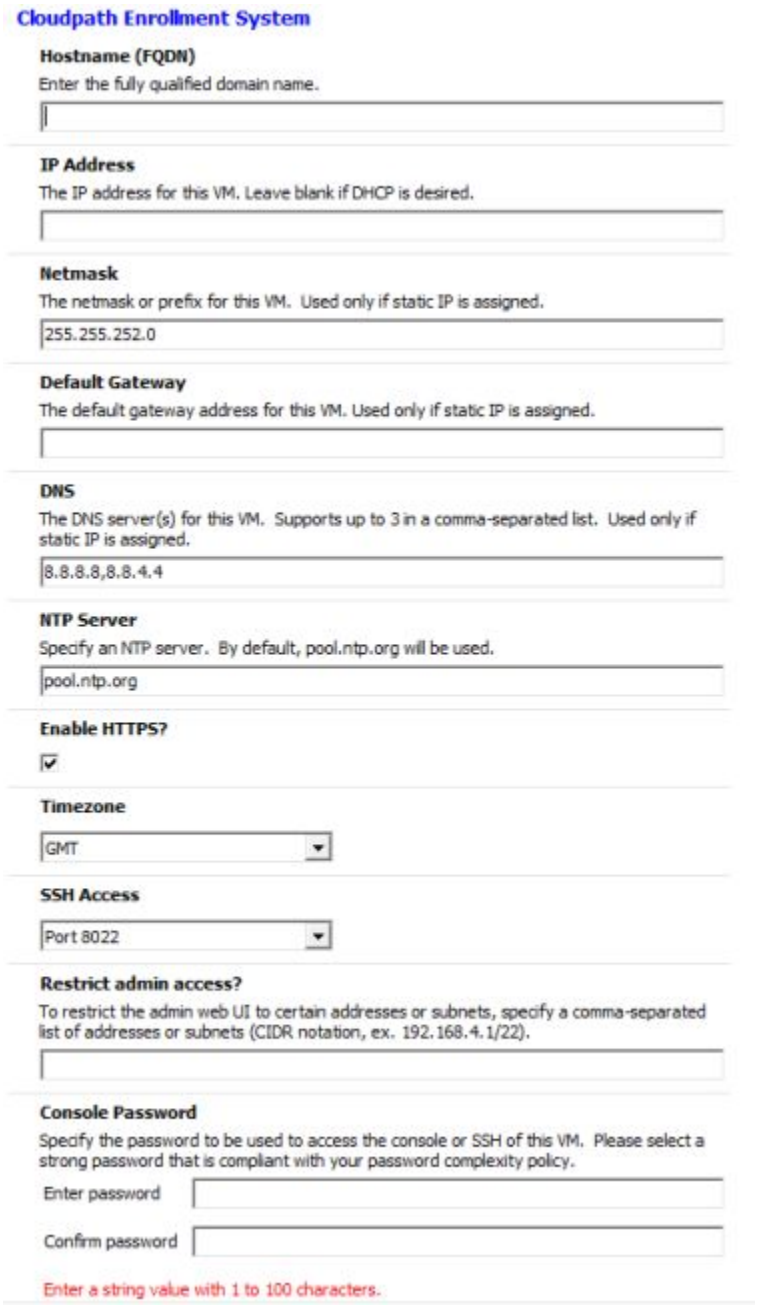
     NOTE
     If you are using Fault Tolerance, you must select **Thick** provisioning.

   - Use **Thin** provisioning for testing, or if disk space is an issue. A thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.
8. Select a disk format.
9. Continue the configuration with vCenter, or a non-vCenter console.
   - If you are using the vCenter to configure application and network properties, continue to the next section.
   - If you are using the console to configure application and network properties, review the initial settings and click **Finish**. See Deploying the Virtual Appliance Using a Console-Based Client to complete the deployment process.

Application Properties (vCenter)

Customize the application properties for the deployment.

FIGURE 11 Application Properties



1. Enter the **Hostname(FQDN)** for the virtual appliance.

   NOTE
   The Cloudpath **Hostname** is used as the default **OCSP Hostname**, which is embedded into certificates issued by the onboard root CA as part of the URL for the Online Certificate Status Protocol (OCSP).

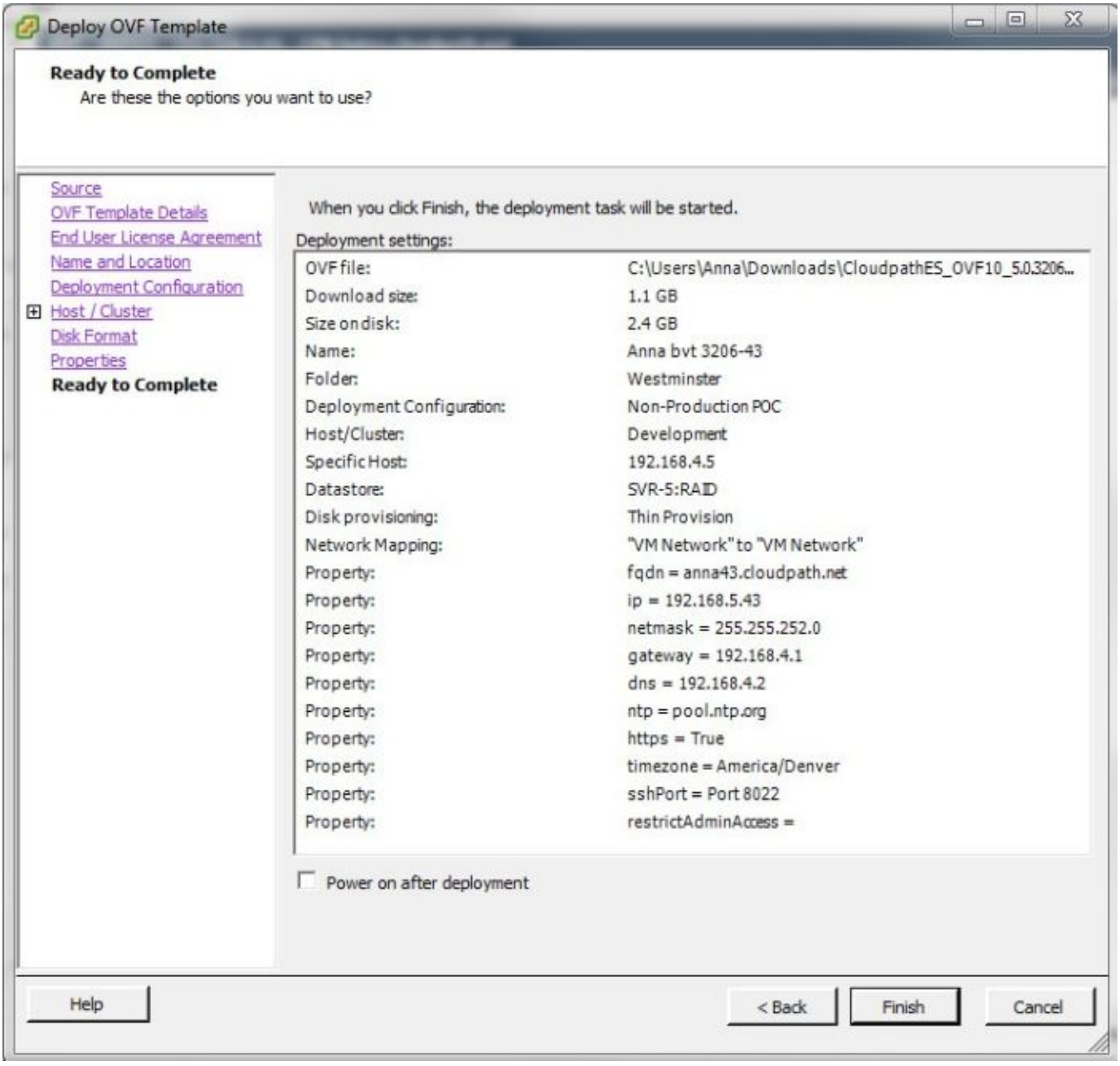
2. Enter the IP Address, Netmask, Default Gateway, and the DNS Servers for this VM. Leave blank for DHCP.
3. Specify an NTP Server or leave the default.

4. HTTPS is enabled by default. Leave unchecked only if Cloudpath is behind another web server using SSL.
5. Select the **Timezone**.
6. Select SSH port, or disable SSH access.
7. Enter the IP address(es) that can access the Cloudpath Admin UI. Leave this field blank if you do not want to limit administrative access.
8. Enter and confirm a **service user** password. The **service user** account is used by your support team for access to this system using SSH. The **service** account is not available if SSH access in not permitted.

Confirm Deployment Settings (vCenter)

1. Verify these properties before you begin the deployment.
   If you are using DHCP, the networking properties will be blank.

   FIGURE 12 Deployment Settings



2. Click **Finish**

   Deployment takes approximately 2 minutes.

Deploying the Virtual Appliance to a Hyper-V Server

NOTE
If using a VMware deployment, see Deploying the Virtual Appliance to a VMware Server.

The deployment process consists of the following steps:

- Retrieve OVA File
- Deploying the Virtual Appliance Using a VMware vCenter Client
- Test Network Connectivity

Retrieve VHDX Image File

Retrieve With Activation Link

If you are setting up a Cloudpath account for the first time, you will be sent an activation code in an email notification. For an on-premise deployment, the activation code link allows you to download the Cloudpath VHDX image file, binding your VHDX file with the activation code.

When the download is complete, deploy the OVA file using the Hyper-V Manager.

Replication With Hyper-V Systems

The VHDX files and their associated snapshots are stored in the same directory. If you plan to set up two systems in replication, be sure to keep the VHDX file for each server in a separate folder so that snapshots and other changes are kept together with the appropriate server.

Deploying the Virtual Appliance Using Hyper-V Manager

1. Open the Hyper-V Manager.
2. From the Action menu, select **New** > **Virtual Machine.**. This opens the **New Virtual Machine Wizard**.
3. Read the **Before You Begin** screen.
4. Enter a Name for the new VM and click **Next**.
5. Select **Generation 1** and click **Next**.

6. Assign **Startup memory**.

   NOTE
   When using the **New Virtual Machine Wizard**, RAM is specified, but the system assigns only one virtual processor, by default. This value can be increased after the initial setup.

   - For software trials, feature testing, and other non-production systems, we recommend using 6GB (6144MB) RAM and 2 virtual processors.
   - For production systems with 4,000 or fewer users, we recommend using 8GB (8192MB) RAM and 4 virtual processors.
   - For production systems with 8,000 or fewer users, we recommend using 12GB (12288MB) RAM and 8 virtual processors.
   - For production systems with more than 8,000 users, we recommend using 16GB (16384MB) RAM and 8 virtual processors.
   - For production system with more than 20,000 users, we recommend using 20GB (20480) RAM and 8 virtual processors.

7. Leave **Use Dynamic Memory** selected (the default) and click **Next**.
8. On the **Configure Networking** screen, select the appropriate virtual switch in the **Connections** field. Click **Next**.
9. On the **Connect Virtual Hard Disk** screen, select **Use an existing virtual hard disk**, and browse to the location where the vhdx file exists. Click **Next**.
10. Verify the setup summary and click **Finish**.

The system creates the new virtual machine.

Configure Virtual Processors

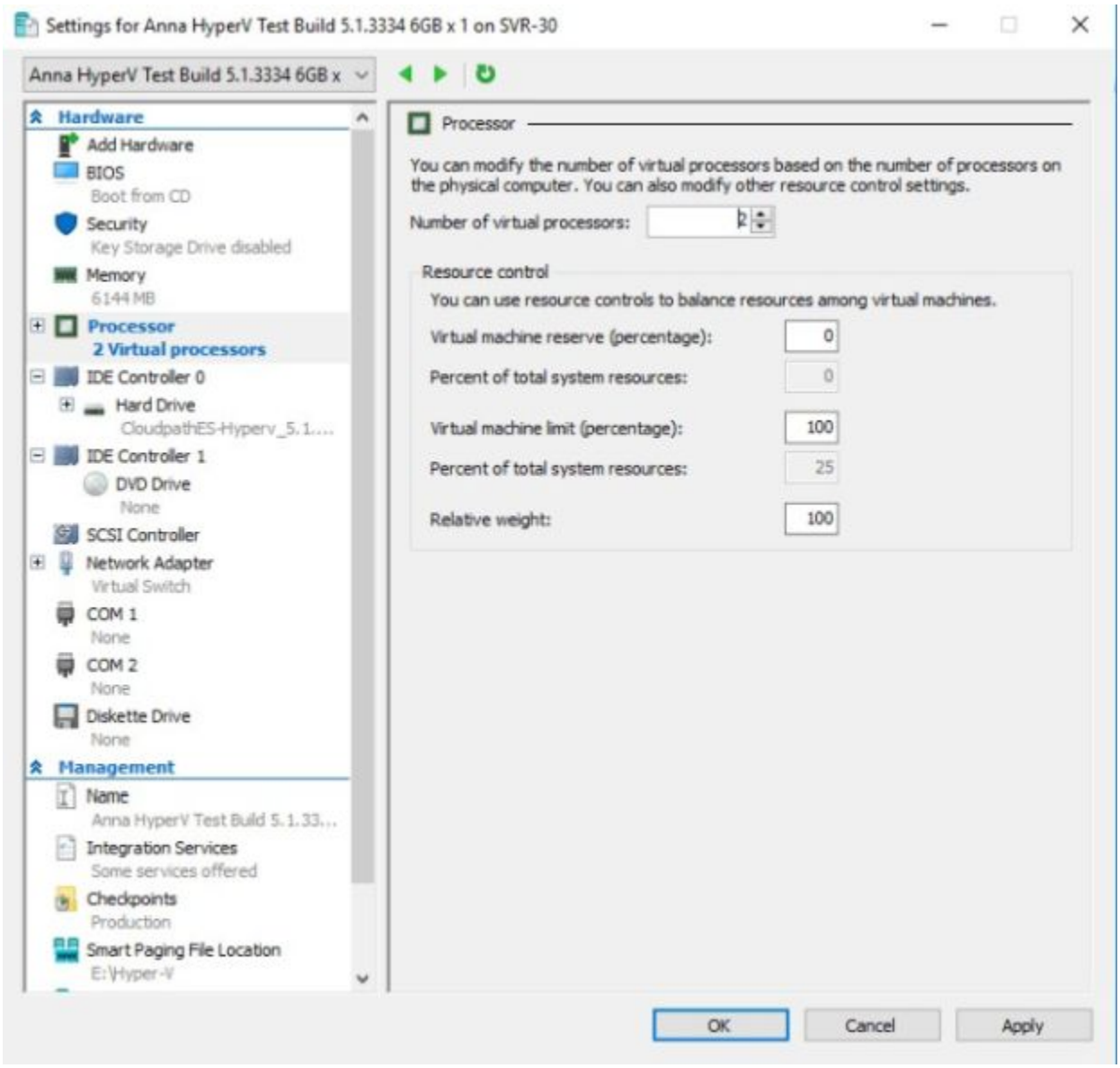
By default, the new VM wizard assigns one virtual processor to a new VM. You can increase the number of virtual processors in the VM settings.

NOTE
The VM must be powered off to change **Settings**.

1. With the VM selected, navigate to the **Action** menu, and select **Settings**. Alternately, you can right- click the selected VM.

2. Select **Processor**.

FIGURE 13 VM Settings



3. In the left pane, select **Processor**.
4. In the right pane, increase the value for **Number of virtual processors**.
5. Click **Apply**, then **OK**.

Power on the virtual machine to continue with the configuration.

Deploying the Virtual Appliance Using a Console-Based Client

Before you begin, read the list of information required to setup the system.

1. Open the console on the VMware or Hyper-V Server.
2. Enter **yes** (or **y**) to accept all license agreements.
3. Enter the time zone. For example, enter **America/Denver**.
4. Enter the **FQDN hostname** for the virtual appliance (ex., **onboard.company.com**).
5. Do you want to enable HTTPS? **Enter** for yes (default) or **n**.
6. Do you want to use a STATIC IP (rather than DHCP)? **Enter** for yes (default) or **n**.
   - If you enter yes (recommended), you assign the IP address of the virtual appliance, subnet mask, and gateway and DNS server IP addresses for your network.
   - If you enter no, DHCP is used to assign IP address of the virtual appliance interface (ens for VMware, eth0 for Hyper-V), subnet mask, gateway, and DNS server IP addresses for your network. If you are not using DHCP, enter the IP address of the virtual appliance interface.
7. Enter the IP address of the virtual appliance.
8. Enter a subnet mask in the format 255.255.252.0.
9. Enter the gateway IP address for your network.
10. Enter the DNS server IP address.
11. Do you want to permit SSH access? **Enter** for yes (default) or **n**.
12. Enter and confirm a **service** password.

    The **service** password is used by your support team for access to this system using SSH. Refer to the *Cloudpath Command Reference* on the **Support** tab for details.

    NOTE
    The service account is not available if SSH access in not permitted.

13. Do you want to us an NTP server other than pool.net.org? **Enter** for no (default) or **y** to specify an NTP server.

    The setup is complete.

14. Press **Enter** to reboot the system.

    After the reboot you are presented with the **shelluser** login prompt.

    NOTE
    The **shelluser** is only available during the initial system configuration. After the initial boot, you must use the **service** password to access the system.

Service Account

When the deployment is finished, you are presented with the service account login prompt.

To use the service account:

1. Enter **cpn_service** at the login prompt, and then the service user password.
2. Enter the **show config** command to verify your configuration. You may be prompted to re-enter the password.

   See the *Cloudpath Command Reference* on the left menu **Support** tab.

Test Network Connectivity

To verify that the virtual appliance is correctly deployed, perform the following operations from the VMware server console:

1. Ping the gateway of your system.
2. Ping the URL where the Cloudpath Licensing Server is hosted.
3. Verify that the virtual appliance can resolve DNS.

How to Install VMware Tools

VMware Tools is a suite of utilities that you install in the operating system of a virtual machine. VMware Tools enhances the performance of a virtual machine and makes possible many of the ease- of-use features for managing your virtual appliance with the vCenter Client.

Use these instructions if you wish to install VMware Tools on the Cloudpath virtual appliance.

> **NOTE**
> We recommend that you take a VM snapshot before adding tools or making changes to the configuration.

From the vCenter Client

1. From the powered-off state, select the VM, and right-click to **Edit Settings**.
2. With the **Hardware** tab selected, click the **Add** button to open the **Add Hardware** page.
3. Select **CD/DVD Drive** (or browse to locate the ISO for the media) and click **Next**.
4. Continue with the configuration using the default settings. When finished, click **OK**.
5. Power on the VM.
6. Select the VM and right-click to select **Guest** > **Install/Upgrade VMware Tools**.
7. Select **Interactive Tools Upgrade** and click **OK**.

   This popup does not occur on some systems.

From the Console

1. Log in to the **cpn_service** account.
2. Enter the following commands:

```
sudo mount -t iso9660 /dev/cdrom /media
cp /media/VMwareTools-XXXXX.tar.gz .
sudo umount /media
tar xvfzp VMwareTools-XXXXX.tar.gz
cd vmware-tools-distrib
sudo ./vmware-install.pl
```

> **NOTE**
> The VMware Tools version can vary within the same vCenter. Use the **Tab** button to auto-complete the VMwareTools-XXX.tar.gz commands to be sure you get the correct version.

3. Select the default answers to the configuration questions.

   When finished, exit the `vmware-tools-distrib` directory.

When complete, select the **Summary** tab on the vSphere Client. The **General** section shows VMware Tools is **Running (Current)**. The **IP address** should match the IP address assigned to the Cloudpath virtual appliance.

How to Increase the Virtual Appliance Memory on VMware

NOTE
For Hyper-V deployments, refer to the *Deploying Cloudpath as a Virtual Appliance Using Microsoft™ Hyper-V Manager* configuration guide.
We recommend that your VMware server have 12-16GB RAM, which is sufficient for most production environments. However, there may be circumstances (replication, performance, larger deployments) that require adjustments to the memory allocation for Cloudpath.
Use these instructions if you want to change the memory configuration of a virtual machine's hardware.

1. From the vCenter client, power off the virtual appliance.
2. Select the VM, and right-click to **Edit Settings**.
3. With the **Hardware** tab selected, select **Memory**.
4. On the right window pane, increase the **Memory Size**.
5. Click **OK**.
6. Power on and reboot the VM.

How to Expand the MySQL Partition Size

The database partition is designed to maximize performance of the Cloudpath operations. If needed, you can expand the size of the partition used for MySQL database operations.

From the vCenter Client

1. With the VM running, select the VM and right-click to **Edit Settings**.
2. With the **Hardware** tab selected, select **Hard disk 2**.
3. On the right pane, in the **Disk Provisioning** section, increase the **Provisioned Size** to the desired size and click **OK**.

NOTE
If the Provisioned Size cannot be selected, try restarting the server using the **sudo halt** command.

From the Console

Enter the following commands as `root`.

1. (Optional) View the amount of free disk space available.

```
[root@localhost cpn_service]# df -h
```

2. Signal to the OS that there has been a hardware change to the disk.

```
[root@localhost cpn_service]# echo '1' > /sys/class/scsi_disk/2\:0\:1\:0/device/ rescan
```

3. Expand the physical volume.

```
[root@localhost cpn_service]# pvresize /dev/sdb -v
```

4. Extend the size of the logical volume for MySQL operations.

   This example shows that we are extending the size of the logical volume by adding 25GB.

   ```
   [root@localhost cpn_service]# lvextend -L +25G /dev/mapper/application_vg-mysql
   ```

5. Resize the file system.

   ```
   [root@localhost cpn_service]# resize2fs /dev/mapper/application_vg-mysql
   ```

   This writes your changes to disk and completes the partition expansion process.

6. Verify the amount of free disk space available.

   ```
   [root@localhost cpn_service]# df -h
   ```

   The output should indicate the increased partition size.

Activate Account or Log In

- Overview....45
- Activate Account by Activation Code....45
- Set a Password for Account....46
- Activate Account by Credentials....47

Overview

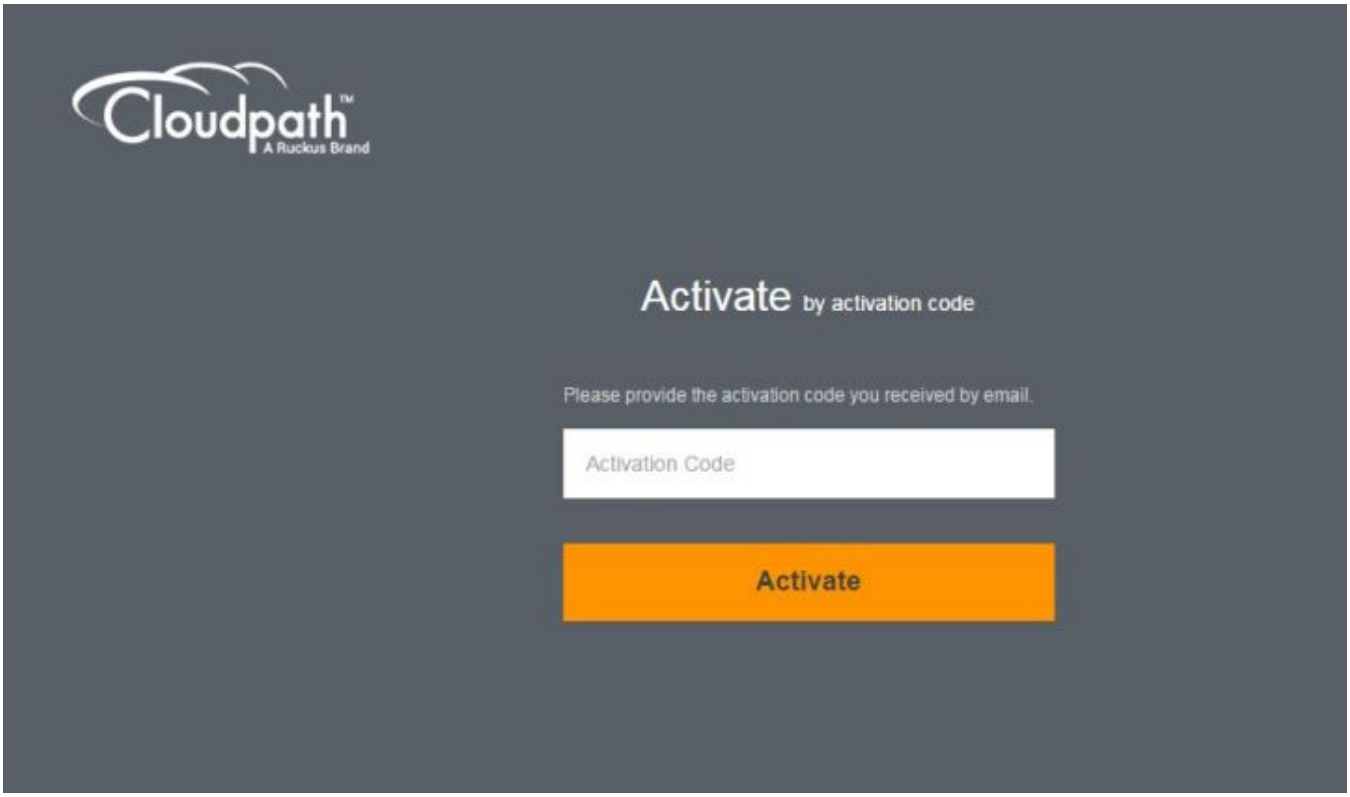
If you are setting up a Cloudpath account for the first time, you will be sent an activation code. If you have existing Cloudpath License server credentials, you can activate an account using those credentials.

Whether you create a new account with an activation code or with legacy Cloudpath credentials, the system binds the Cloudpath instance to your License Server credentials.

Activate Account by Activation Code

If you have been sent an activation account, enter it on this activation page.

FIGURE 14 Activate Cloudpath Account

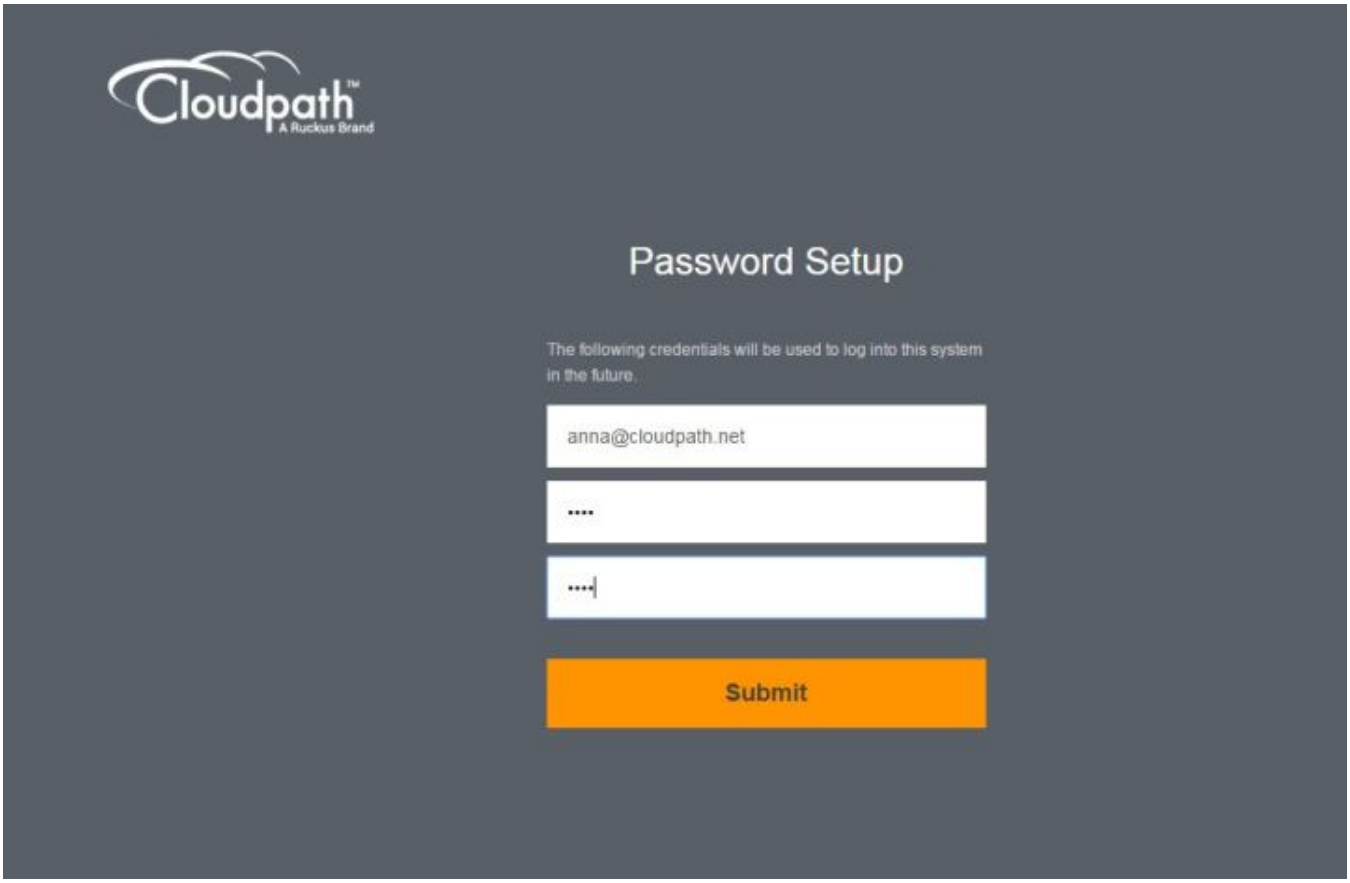


Set a Password for Account

If you have logged in with an activation code, you are prompted to set a password for this account.

1. Your email address should display. If it does not, enter it on this page.

FIGURE 15 Set Password



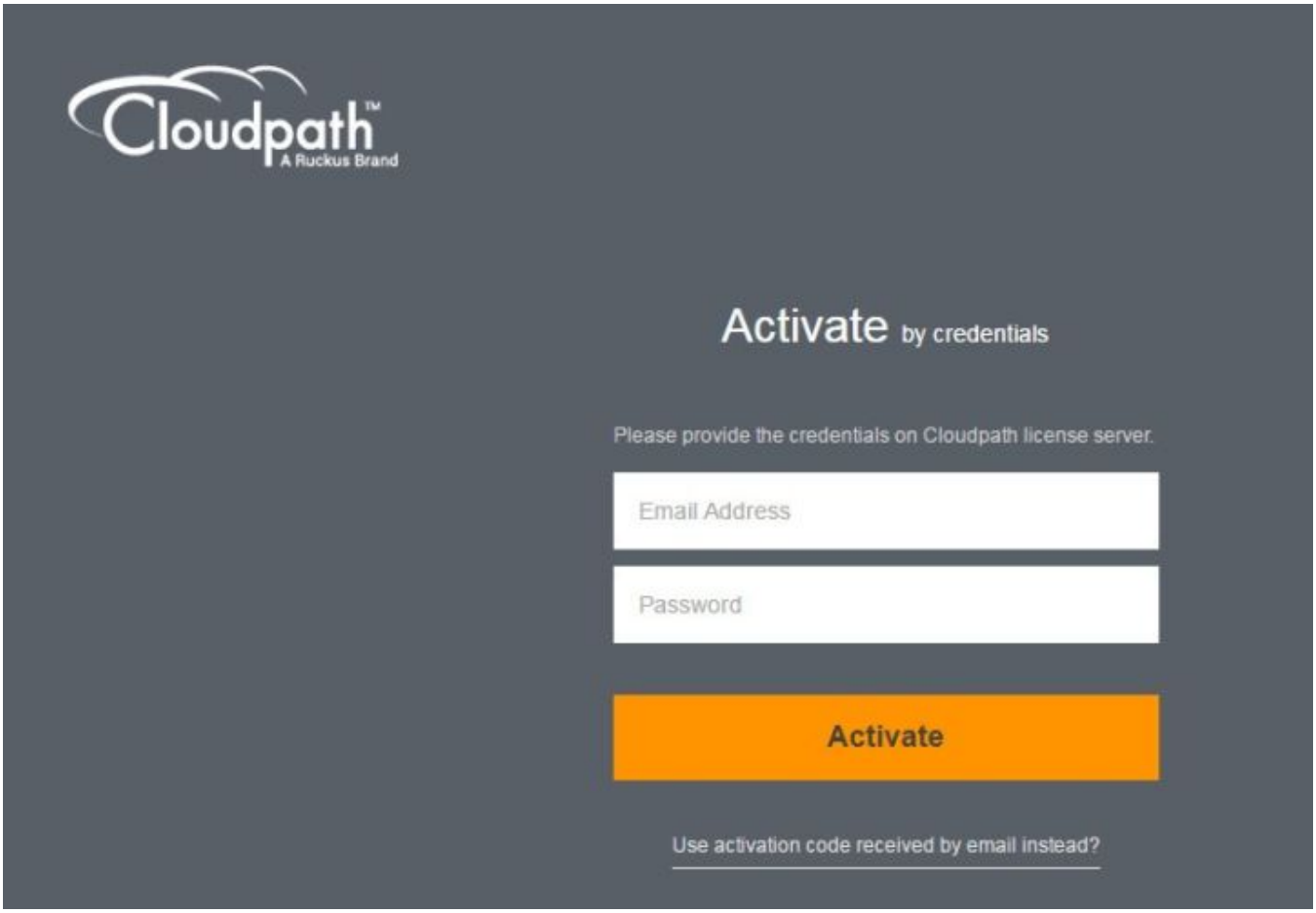
2. Enter and confirm a password.

These are the credentials to use for this Cloudpath account.

Activate Account by Credentials

If you already have a Cloudpath License Server account, you can activate a new Cloudpath account or log in to an existing account using those credentials.

FIGURE 16 Activate Account With Existing Credentials



Initial System Setup

- Overview....49
- System Setup Wizard....50
- Publishing Tasks....57
- ToDo Items....59

Overview

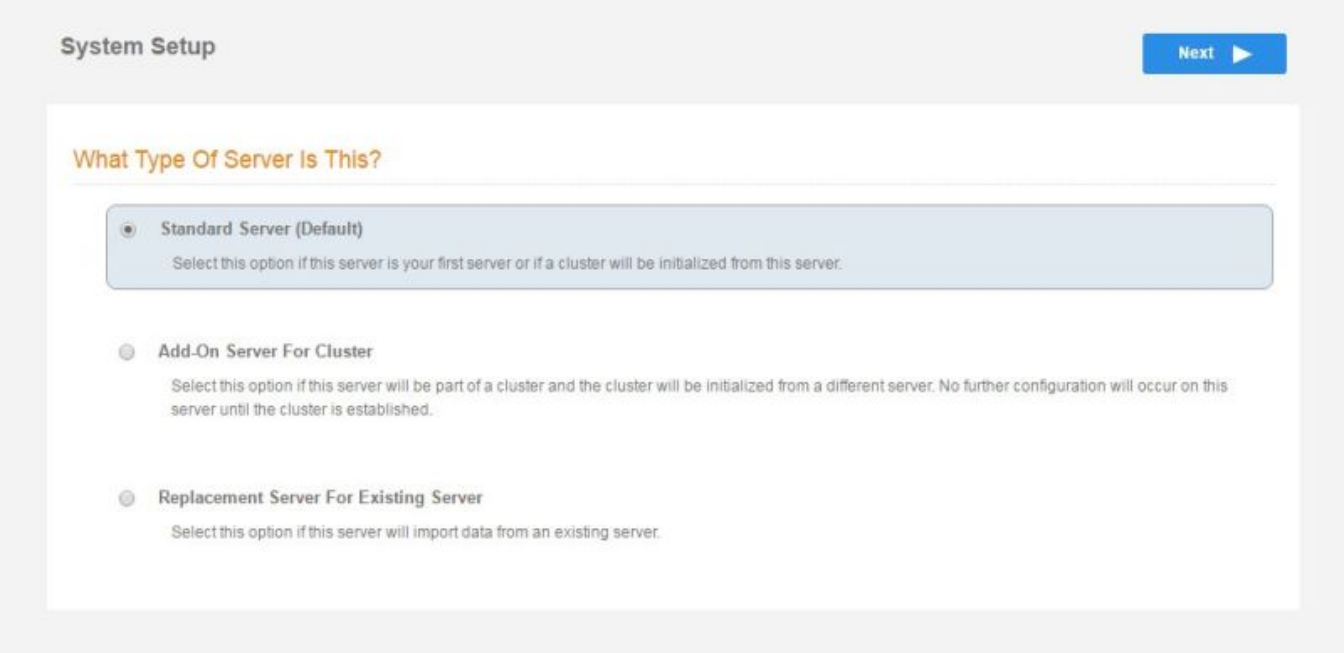
Cloudpath provides you with a single administrator login for the Cloudpath Admin UI. Additional administrators can be added from the left menu **Administration** tab, or you can enable Administrator logins from your authentication servers.

System Setup Wizard

After a successful deployment and activation (or login), the **system setup wizard** takes you through a few steps.

1. Select Server Type.

FIGURE 17 Select Server Type



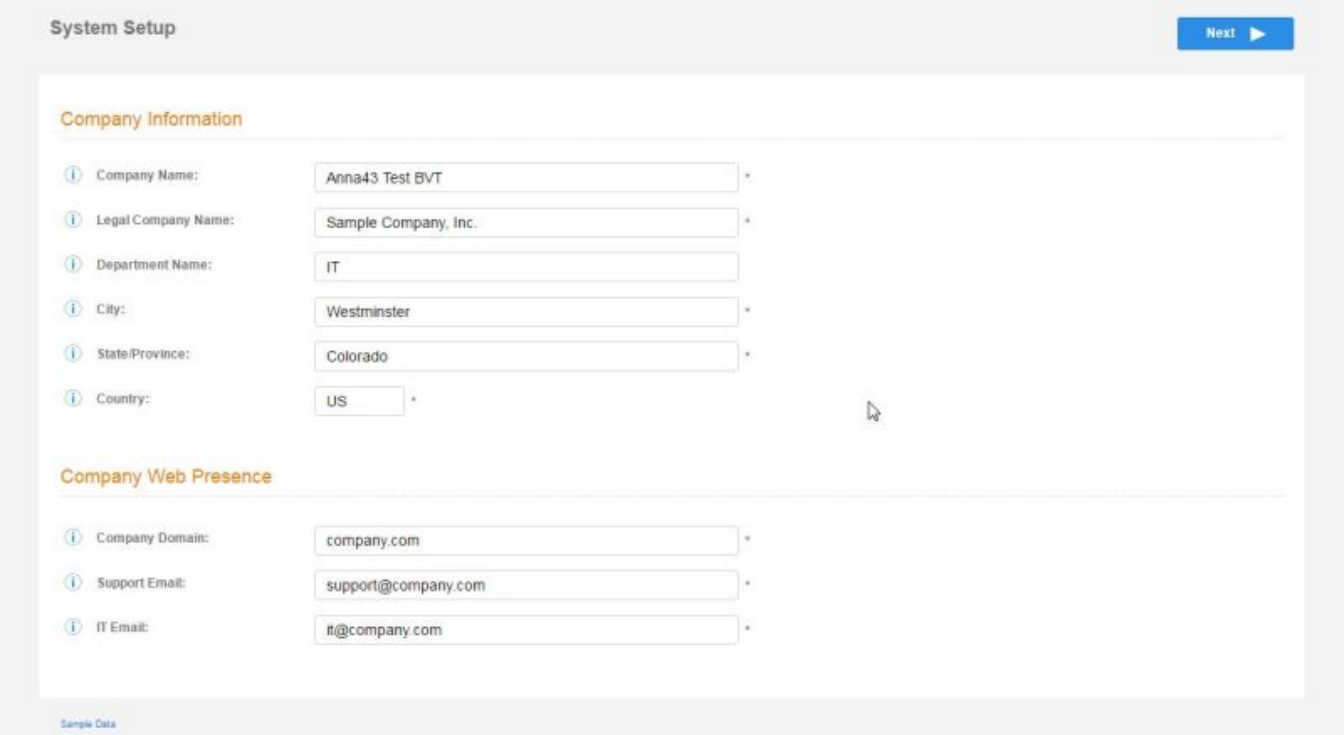
In most cases, select **Standard Server**, the default. This selection takes you through a setup wizard, which prompts you for the basic information required for an Cloudpath server.

- If you are setting up this server for replication, you can choose to set the server as an **Add-On** or **Replacement** server. These selections provide an alternate set up process, requiring less information for the initial setup. **Add-On** and **Replacement** servers receive most of their configuration from the Master server in the cluster.
- If you are setting up this server to replace an existing server, and you are importing the database from the existing server, select **Replacement Server for Existing Server**.

NOTE
For **Add-on** or **Replacement** servers, you will not be required to go through the full system setup.

2. Enter **Company Information**.
   This information is embedded in the onboard root CA certificate.

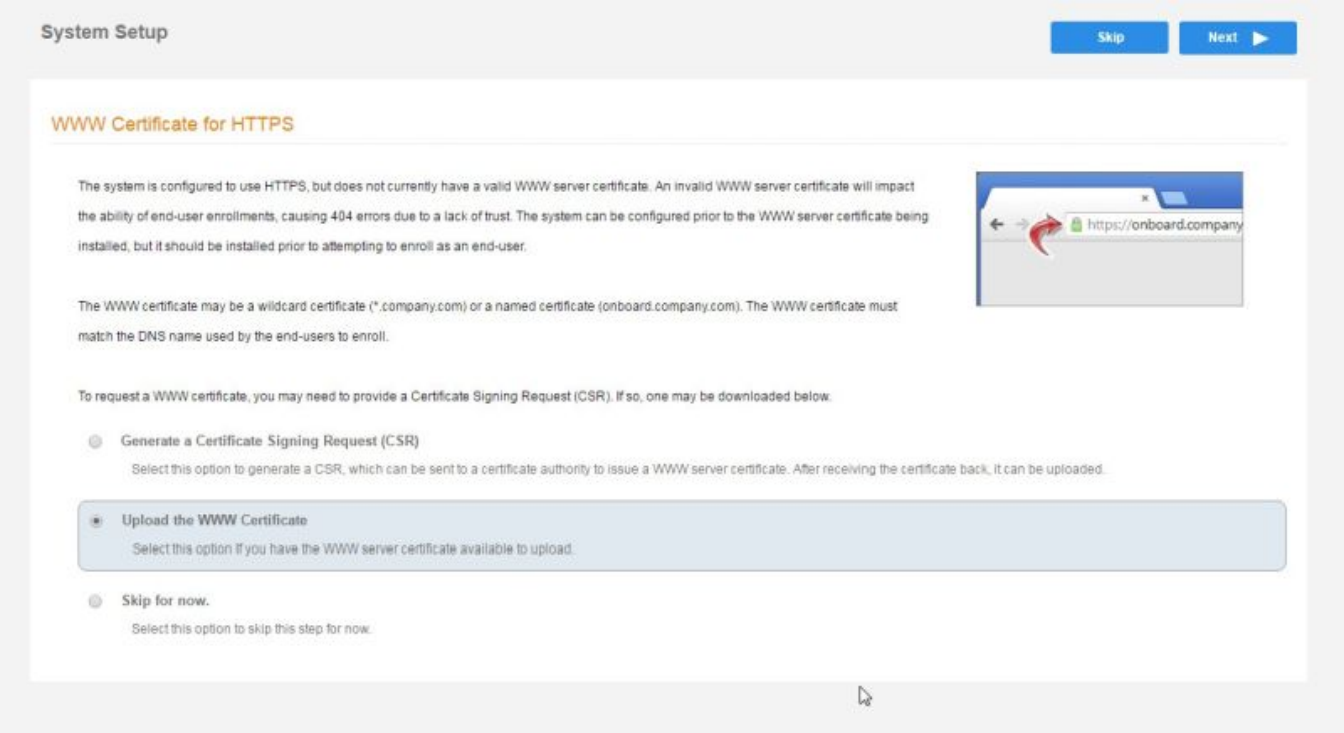
FIGURE 18 Company Information



3. Configure the WWW Certificate.

   The system is configured to use HTTPS, but does not currently have a valid WWW server certificate. An invalid WWW server certificate can impact the ability of end-user enrollments, causing 404 errors due to a lack of trust.

FIGURE 19 WWW Certificate for HTTPS

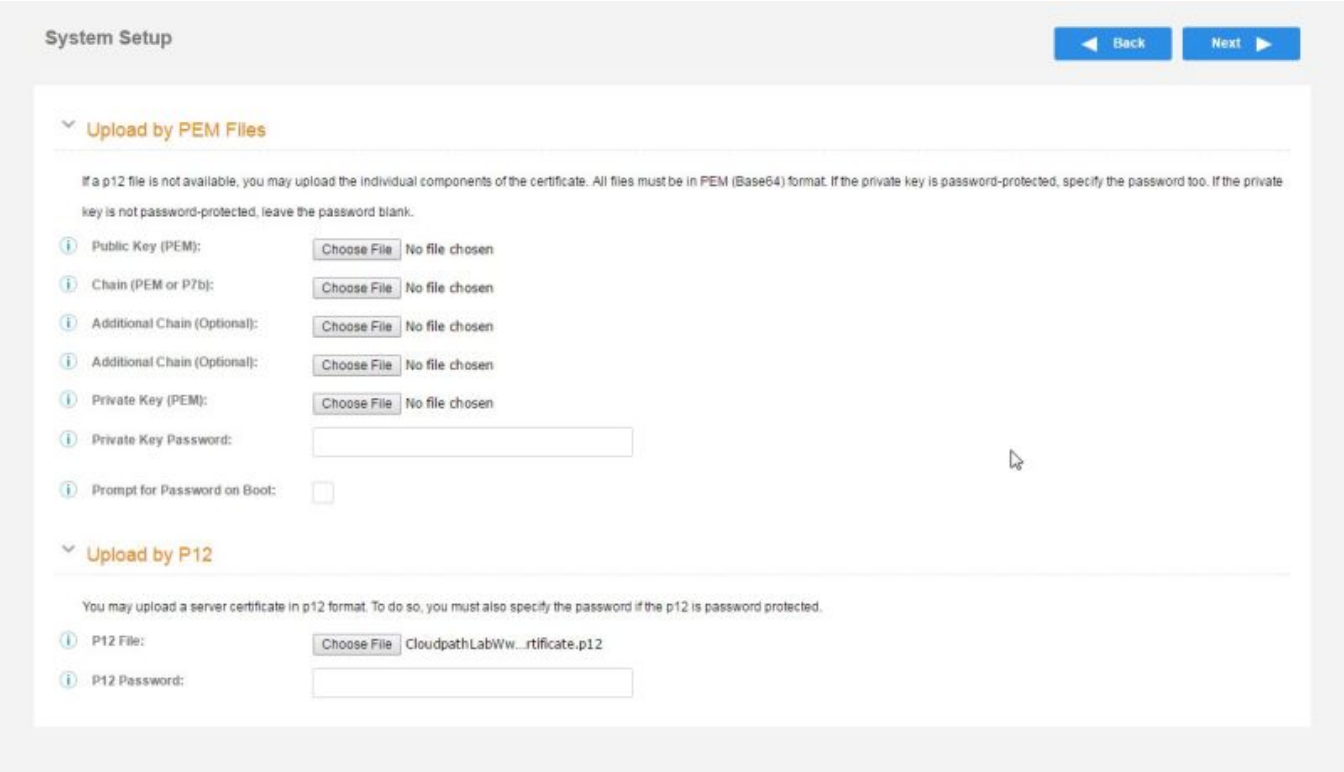


You can skip this step for the initial configuration. However, it should be installed prior to attempting to enroll as an end-user. You can configure the WWW server certificate from **Administration** > **System Services** > **Web Server service**.

Cloudpath supports web server certificates in P12 format, password protected P12, or you can upload the individual certificate components; the public key, chain, and private key or password protected private key.

4. Upload the WWW certificate.

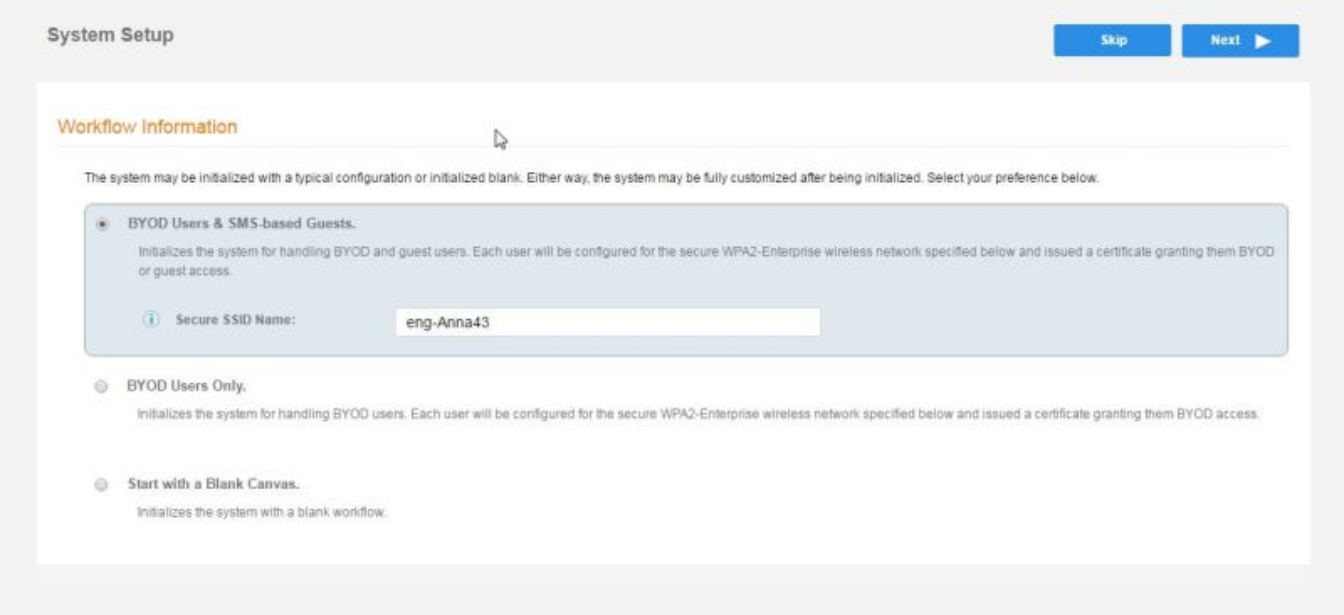
FIGURE 20 Upload WWW Certificate



Browse to locate and upload the web server certificate and click **Next** to continue with the system setup.

5. Select the Default Workflow.
   - To initialize the system with a sample configuration, select **BYOD Users & SMS Guests**, or **BYOD Users Only**. This creates an initial workflow for BYOD users and sponsored guests (or BYOD users only) that you can use as a template, or simply add a device configuration and use immediately.
   - To create your own workflow, select **Start with Blank Canvas**.

FIGURE 21 Select Default Workflow



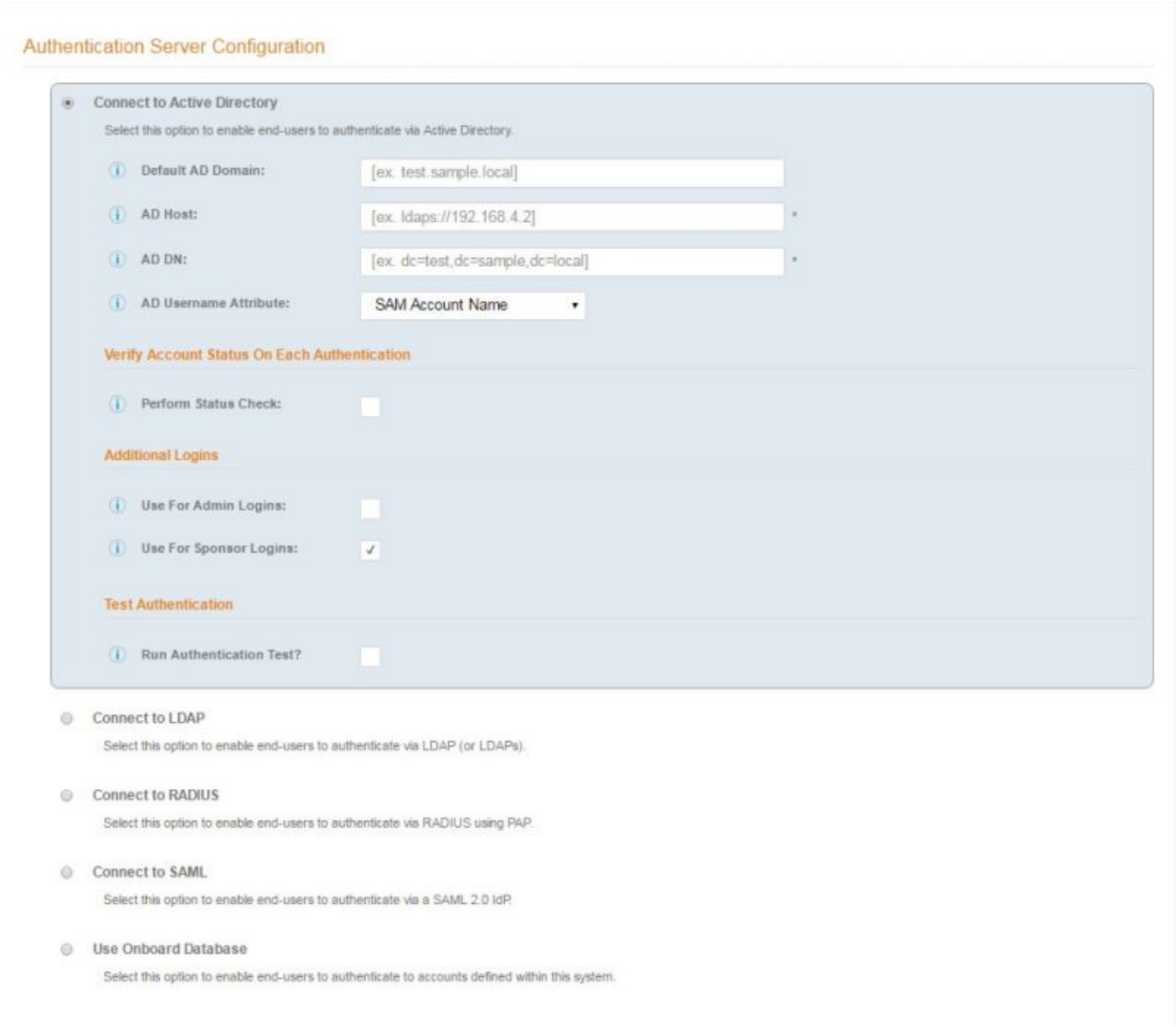
6. Configure the Authentication Server.

   NOTE
   If you selected a Blank Canvas for the default workflow, you are not prompted to set up an authentication server during the initial system setup.

   If you plan to use an authentication server to authenticate end-users or sponsors, we recommend populating the authentication server information page.

   If using multiple authentication servers, additional authentication servers may be added through the workflow or from the **Configuration** > **Authentication** Servers page.

   FIGURE 22 Authentication Server Setup



   a) To setup the initial configuration of the Authentication Server, select and enter the required fields.

NOTE
See the *Cloudpath Quick Start Guide* for information about the full list of authentication server supported by Cloudpath.

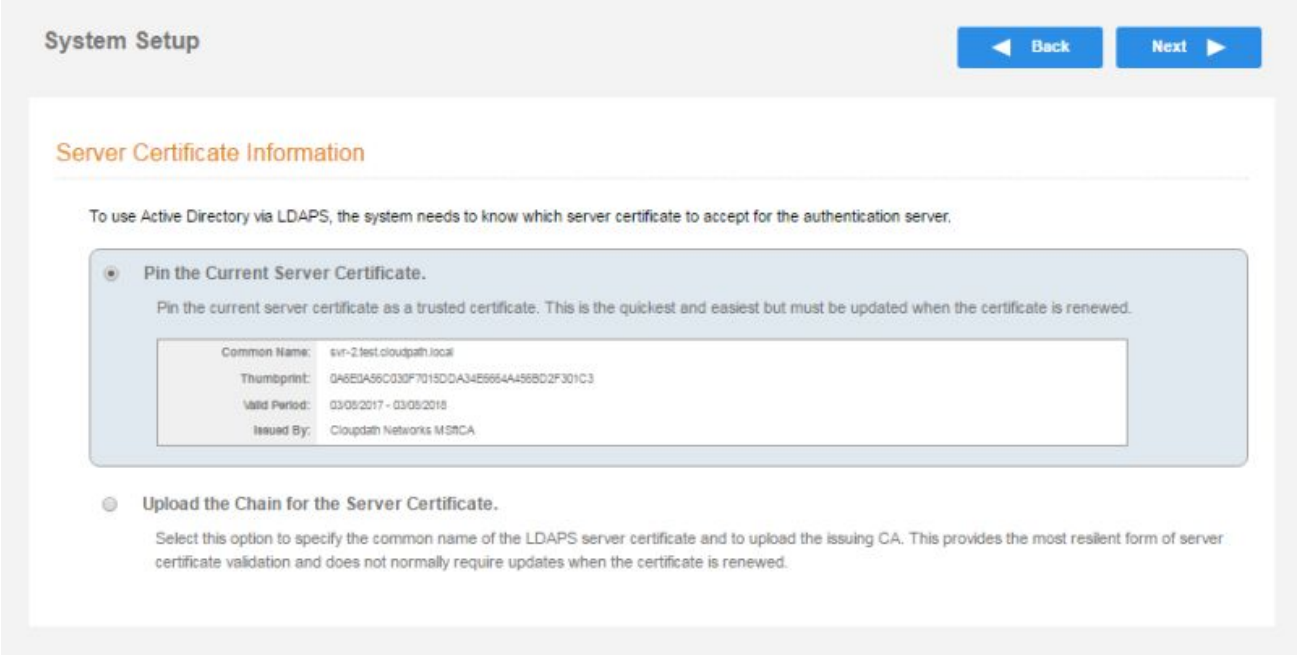
b) Consider these optional settings for the authentication server:

- **Verify Account Status on Each Authentication** - If selected, Active Directory is queried during subsequent uses of the certificate to verify the user account is still enabled. You must provide the bind username and password for an authentication server administrator account.
- **Additional Logins** - If **Use for Admin Logins** is selected, administrators can log into the Cloudpath Admin UI using credentials associated with this authentication server. If **Use for Sponsor Logins** is selected, sponsors can log into the Cloudpath Admin UI using credentials associated with this authentication server.
- **Test Authentication** - If selected, an authentication will be attempted using the username and password provided to test connectivity to the authentication server. This test can also be run from the workflow.

7. Set up the Authentication Server Certificate

a) To use LDAP over SSL (LDAPS), the system must know which server certificate to accept for the authentication server.

FIGURE 23 Authentication Server Certificate



b) Select **Upload the Chain for the Server Certificate** to upload a certificate chain from an issuing CA. You must specify the common name for the LDAPS server certificate. This certificate does not need to be updated when the certificate is renewed.

c) Select **Pin the Current Server Certificate** to use the current server certificate as the trusted certificate. This setting must be updated if the certificate is renewed.

Publishing Tasks

After the initial setup tasks, the system finishes the initialization process. When the publishing tasks are complete, the system is ready to use. The setup information is also emailed to the system administrator for this account.

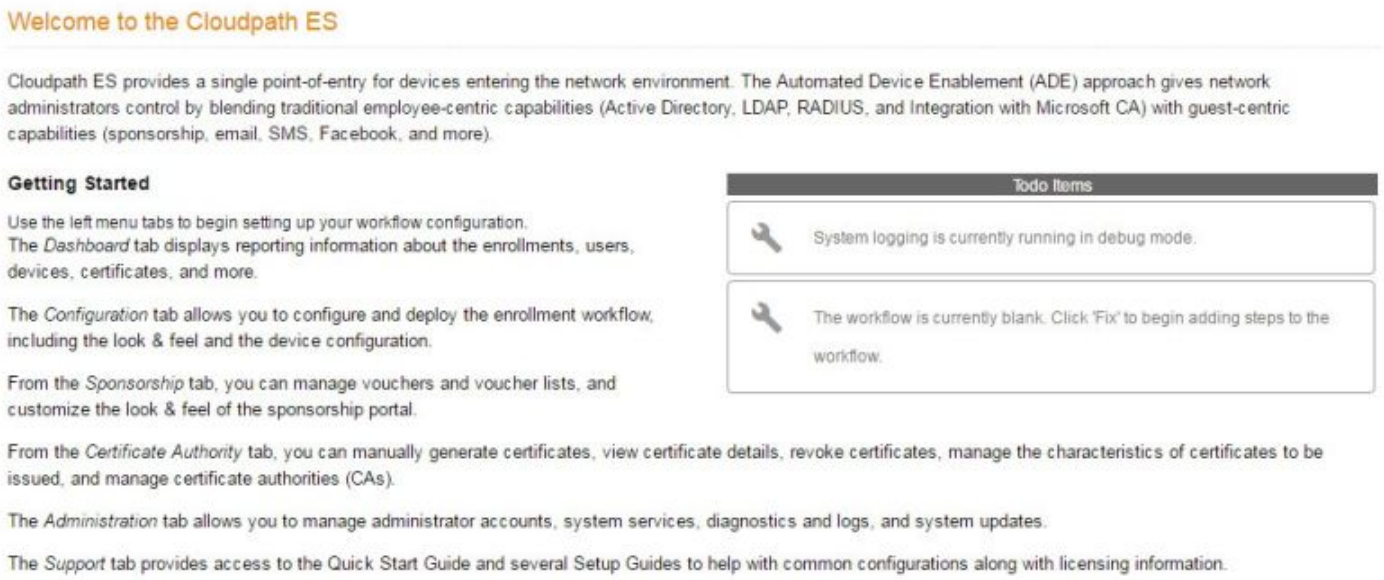
FIGURE 24 System Initialization Status

Initialization Task	Status
Create Certificate Authorities:	Completed.
Create Certificate Templates:	Completed.
Create Device Configurations:	Completed.
Configure Workflow:	Completed.
Activate Sponsor Portal:	Completed.
Publish Enrollment Portal:	Completed.
	System is ready to handle enrollments.
Access Point Setup:	
	The following information will be necessary to configure the access point with the appropriate secure SSID configuration.
SSID:	eng-Anna248 (WPA2-Enterprise, AES (CCMP), Broadcast)
RADIUS IP:	anna248.cloudpath.net
RADIUS Authentication Port:	1812
RADIUS Accounting Port:	1813
RADIUS Shared Secret:	nhu6vjjwqedwpptn7vuw
RADIUS Attributes:	BYOD Policy Template - VLAN: '1'
	Guest Policy Template - VLAN: '1'
User Experience:	
	End-users will use the enrollment portal to activate devices.
End-User Portal:	https://anna248.cloudpath.net/enroll/Anna248HyperVxpc/Production/
BYOD:	For BYOD, the authentication server is configured.
	BYOD users will be moved onto the secure SSID with VLAN '1' assigned.
Guests:	Guests will be required to provide a voucher via SMS or email.
	SMS is one of several mechanisms for handling guests.
	Guest users will be moved onto the secure SSID with VLAN '1' assigned.
Administrator Experience:	
Administrator UI:	https://anna248.cloudpath.net/admin/
Credentials:	The following email addresses have been sent a one-time password along with this information:

ToDo Items

On subsequent logins, the Cloudpath **Welcome** page is displayed. The **ToDo Items** lists the configuration items needed to complete the account setup.

FIGURE 25 Cloudpath Welcome Page



To configure Cloudpath, see the *Cloudpath Quick Start Guide*, and other Cloudpath configuration guides, which can be found on the Cloudpath **Support** tab.

Enrollment Workflow

- Overview....61
- Workflow Basics....61
- Modifying a Workflow Template....62
- Creating a Workflow From a Blank Slate....64
- Publishing the Enrollment Workflow....77
- How to Test a Published Workflow....79

Overview

The Cloudpath workflow engine is a customizable enrollment process that provides more control over who is granted network access and how they should be provisioned.

When you plan your workflow, you can have a different enrollment sequence for employees and visitors, for personal and IT-owned devices; adding custom authentication and policy prompts, to allow a separate workflow for each type of user and device in your network environment.

See Enrollment Workflow Use Cases for an example of the most commonly used workflows.

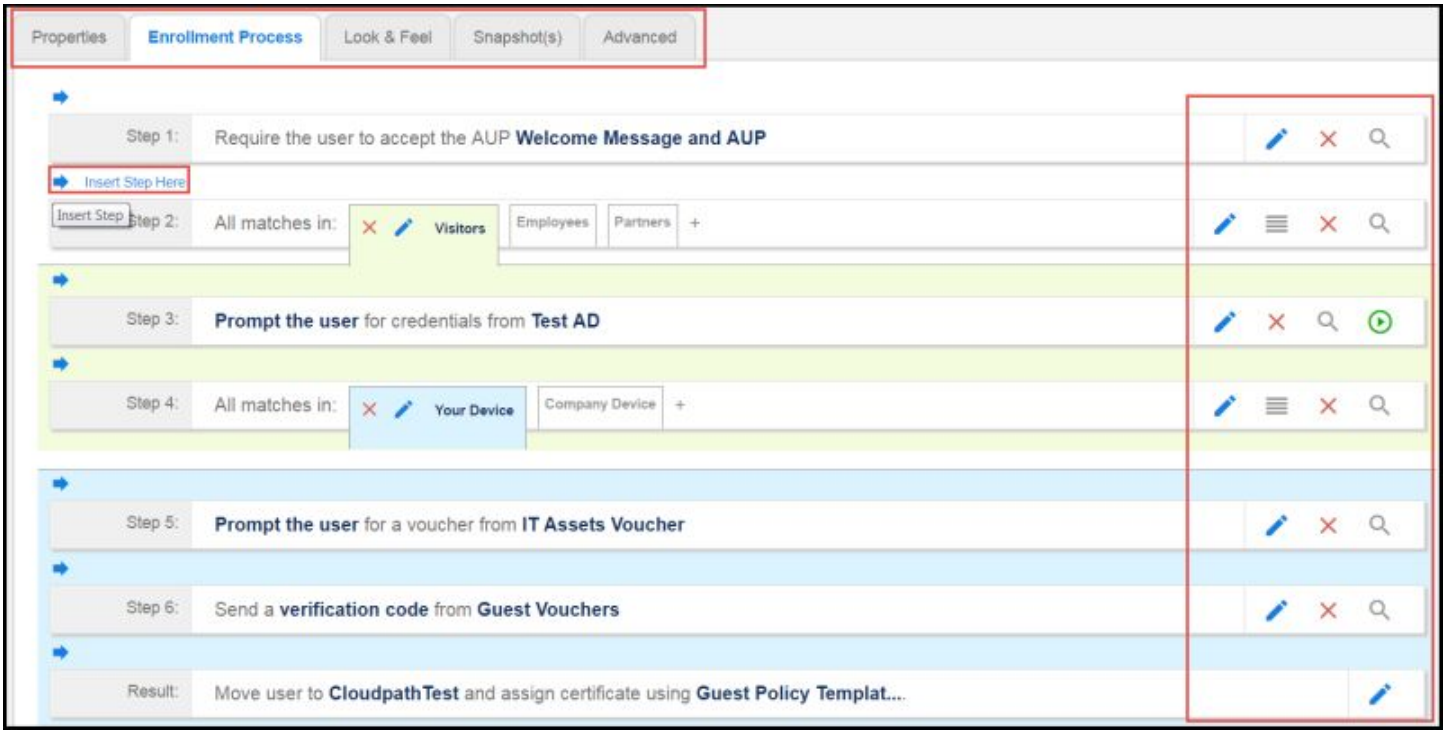
Workflow Basics

Navigate to **Configuration** > **Workflows**.

The **Workflow** page has 5 tabs across the top.

- Use the **Properties** tab to update the workflow properties and the **Enrollment Portal URL Options**.
- Use the **Enrollment Process** tab to configure the steps presented to a user to create the workflow.
- Use the **Look & Feel** tab to configure the Cloudpath skin, and to customize the logos, colors, buttons, and images for the Cloudpath server, the Cloudpath Wizard, and the Download page.
- Use the **Snapshot(s)** tab to view the latest snapshot, the version, timestamp and the notes added to a particular workflow.
- Use the **Advanced** tab to view the **Enrollment Portal URL**, **Passpoint OSU URL**, and the **QR code**. You can also use it to **Manage Chromebook Setup and for Cleanup**.

FIGURE 26 Workflow Configuration Page



Use the icons along the side to make changes to the enrollment workflow:

- Use the icons on the right side of each step to edit, modify, delete, view the enrollment steps.
- Use the **Test Server** icon to verify interaction with an authentication server.
- Use the **Edit List** icon to label options, to change the order of the selection options in a split, add more options, or add filters and restrictions.
- Use the icons on the split tabs to modify or delete a specific option.

Modifying a Workflow Template

You can modify a standard enrollment workflow template provided by Cloudpath, or create your own workflow one step at a time from a blank slate.

To create a workflow from a template using sample data:

1. Go to **Configuration** > **Workflows**.
2. On the right hand side of the **Workflow** page select **Add New Workflow**.

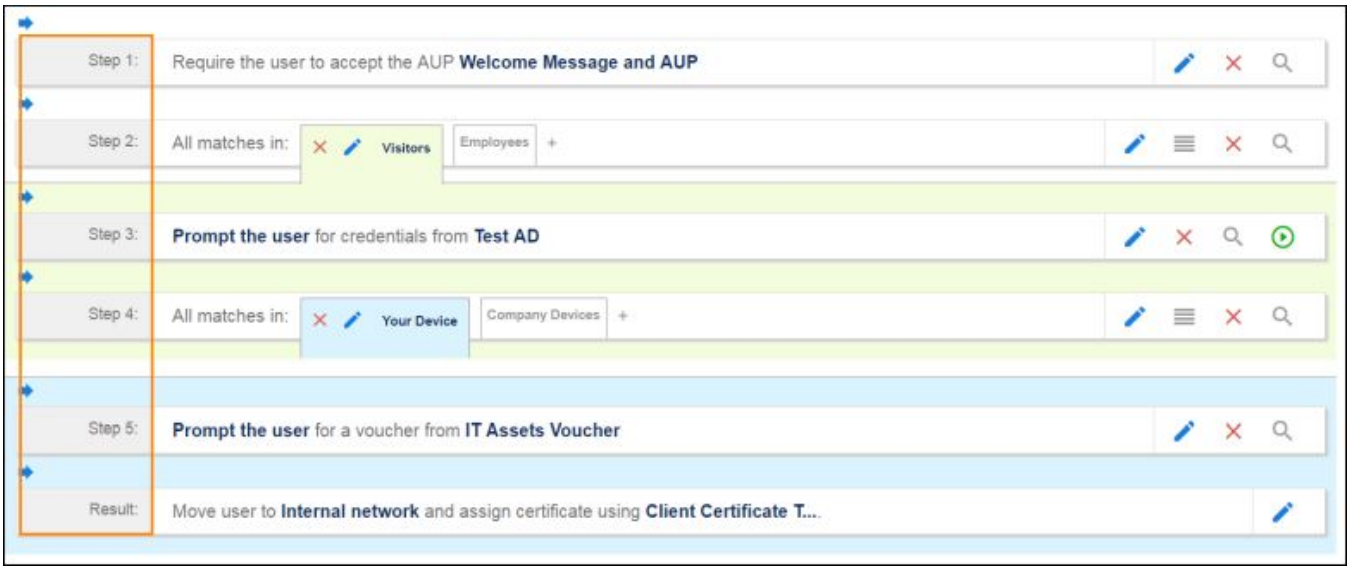
3. On the **Create Workflow** page, enter a **Name** and **Description**.

FIGURE 27 Create Workflow Using Demo Data



4. Select the check box for **Include Demo Data** and **Save**. A workflow template, which contains a typical workflow sequence, is displayed. The step numbers are shown on the left side of the workflow.

FIGURE 28 Workflow Template



The workflow template contains basic workflow steps with sample data that can be modified to fit your network plan.

TABLE 2 Example Workflow Template

Step 1	Acceptable Use Policy.
Step 2	Split in the workflow to provide a different sequence of enrollment steps for Visitors, Employees, and Partners. Splits can be modified for other industries (for example, Students, Faculty, and Guests).
Step 3	An authentication step for domain users, using Active Directory or LDAP.
Step 4	Another split in the workflow to provide a different sequence of enrollment steps for users with an IT device or a personal device.
Step 5	A prompt for a verification voucher.

TABLE 2 Example Workflow Template (continued)

Step 6	The final step, which migrates the user to the secure network and assigns a client certificate, is not pre-populated as this information is specific to your network.

Modify the existing workflow template as needed using the icons on the right side of each step. You can add or remove steps, change the labeling, create filters on the splits, or modify the authentication server.

Creating a Workflow From a Blank Slate

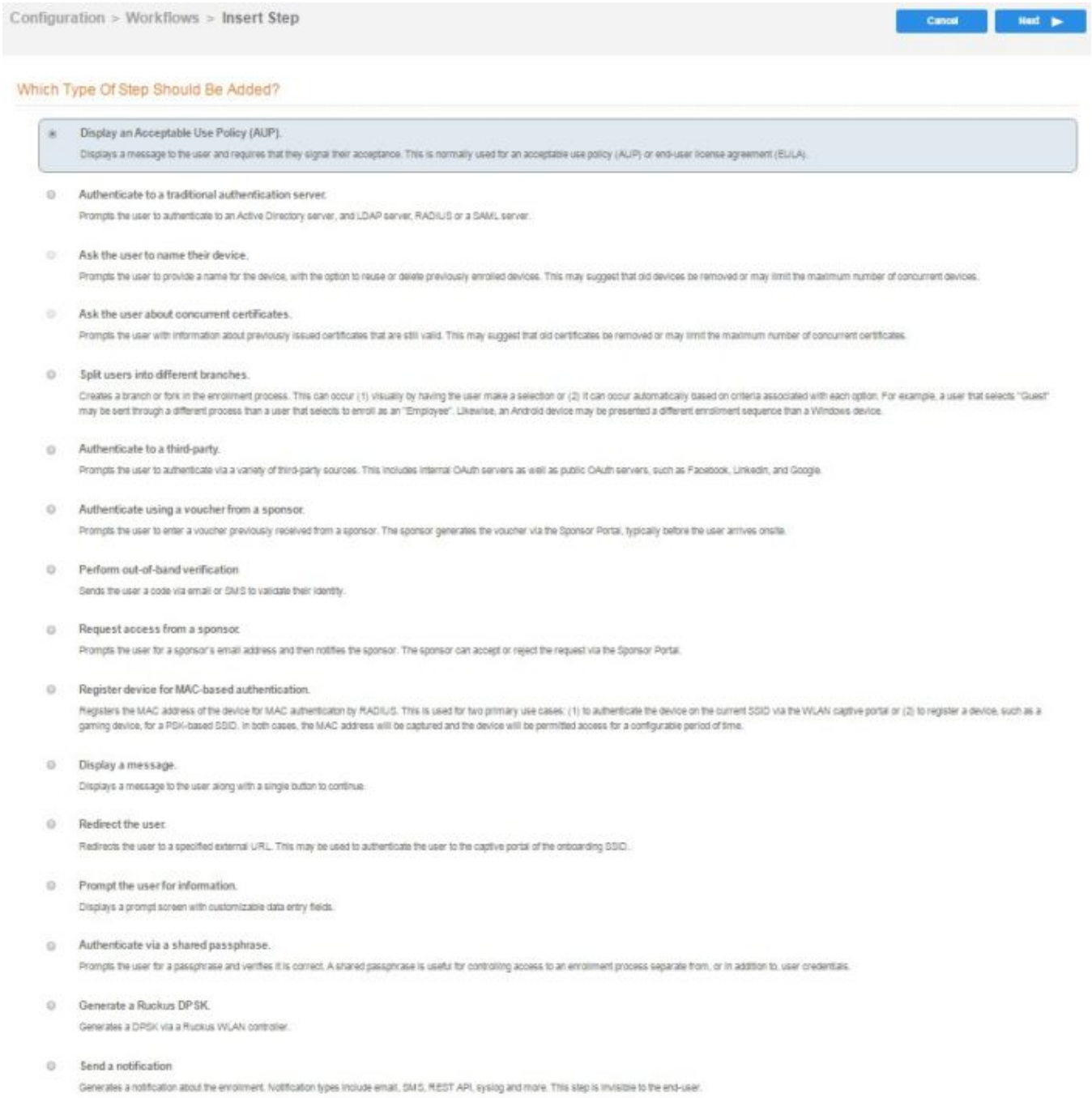
This section describes how to create a typical workflow from a blank slate. This sample workflow follows the steps provided in the workflow template.

1. Go to **Configuration** > **Workflows**.
2. On the right hand side of the Workflow page, select **Add New Workflow**.
3. On the **Create Workflow** page, enter a **Name** and **Description**. Leave **Include Demo Data** unchecked, and **Save**.

4. On the blank workflow page, click **Get Started** to add your first workflow step.

   A selection page opens that allows you to choose which type of step (workflow plug-in) to add to the enrollment workflow. Every time you add a step, the **Step Selection** page appears.

FIGURE 29 Enrollment Step Selection

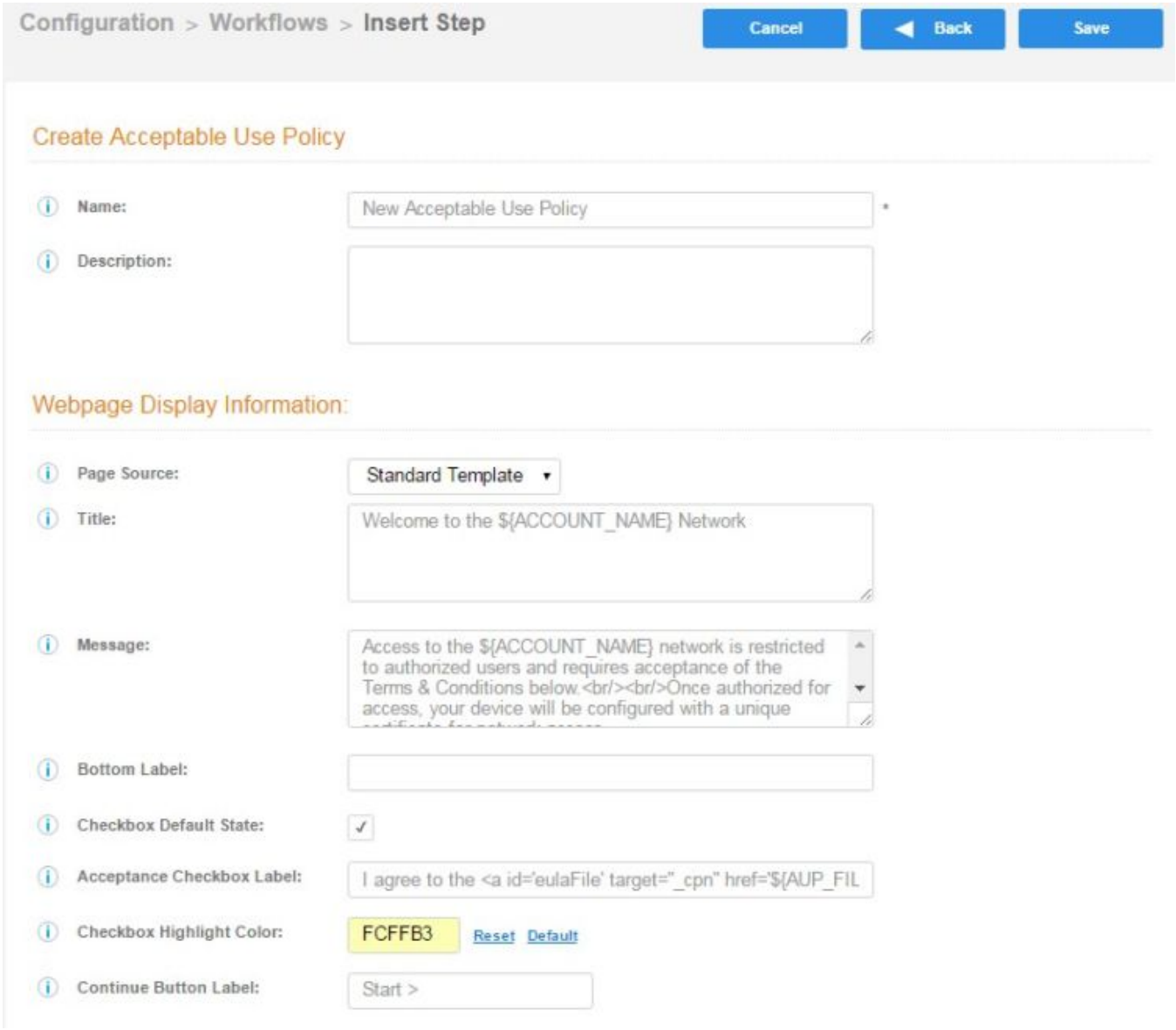


Acceptable Use Policy

Step 1 in the workflow requires the user to agree to an Acceptable Use Policy (AUP).

1. Select the button for **Display an Acceptable Use Policy (AUP)**.
2. Select **A new AUP created from a standard template**.
3. On the **Add Acceptable Use Policy** page, enter the **Reference Information** and **Webpage Display Information**.
   The **Webpage Display Information** is the what the user sees during the enrollment process.

   FIGURE 30 Add Acceptable Use Policy



4. Choose **Standard Template** as the page source and check the **Checkbox Default State** box to specify that the default setting is the acceptance of the AUP. Click **Save**.

The Workflow page displays the enrollment workflow with the AUP acceptance as the first step.

User Type Split

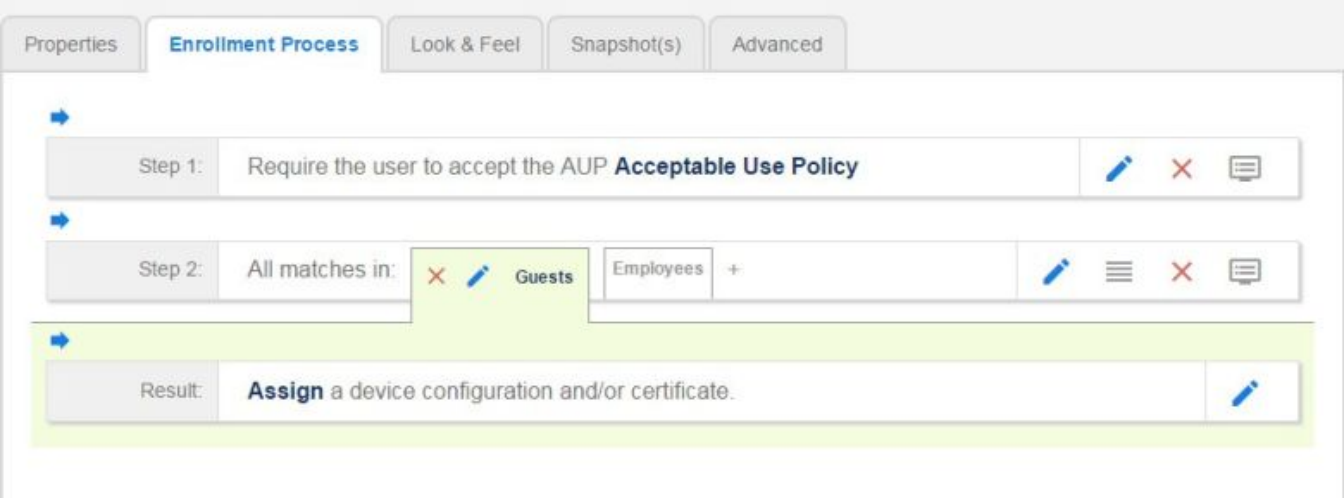
Step 2 in the workflow prompts for the type of user access.

To create a **User Type** prompt:

1. **Insert** a step above the **Result**: step in the enrollment workflow.
2. Select **Split users into different processes**.
3. Select **Use an existing split** and choose **User Type** (a pre-existing split). The **User Type** split creates a prompt to select either the **Employee** User Type or the **Visitor** User Type. These labels can be modified.

   The Workflow page displays the enrollment workflow with the **User Type** option after the **AUP step**.

   FIGURE 31 Workflow with User Type Split



Authentication to a Local Server

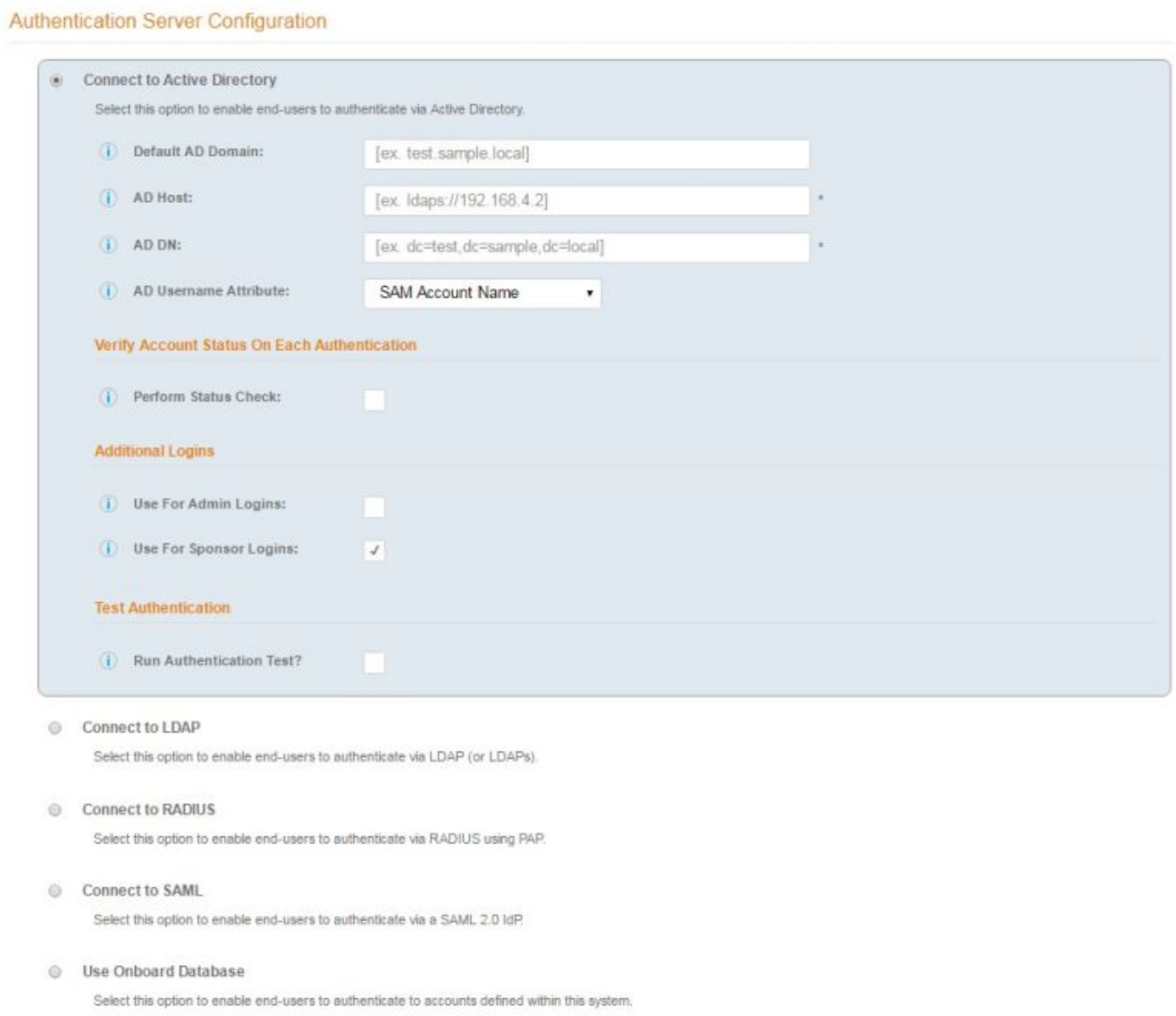
Step 3 in the workflow authenticates a user against a Corporate AD server.

You can run the authentication test at any time from the workflow, or from the **Administration** > **Advanced** > **Authentication Servers** page.

1. Select the **Employee** tab in Step 2 of the example enrollment workflow.
2. **Insert** a step above the **Result**: step in the enrollment workflow.
3. Select **Authenticate to a local server**.

4. Select **Define a new authentication server**. The **Add Authentication Server** page opens.

   FIGURE 32 Add Authentication Server



5. Enter the **Reference** and **Active Directory Information** .
6. (Optional) To test connectivity to the authentication server, select the **Run Authentication Test** box, and enter a Test **Username** and **Password**.
7. (Optional) To allow users from a specific group to log in to the Cloudpath Admin UI as administrators, check the **Use for Login Admin** box and enter the **Admin Group Regex** for the authentication server group.
8. Click **Next**.
9. Select **Use a new webpage created from a standard template**.

   The **Create Credential Prompt** page opens.

Device Type Split

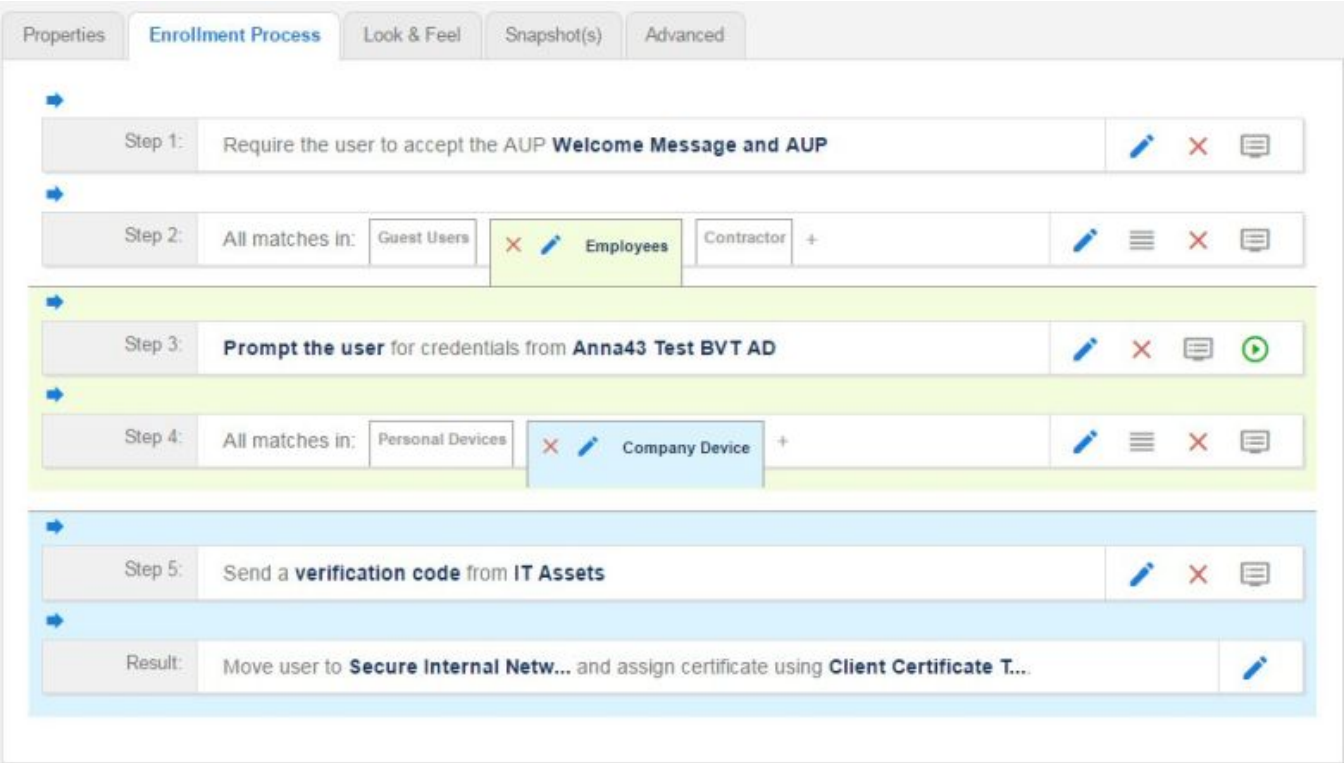
Step 4 adds an enrollment step prompts the user to select a personal device or a company-owned (IT- asset) device.

1. **Insert** a step above the **Result:** step in the enrollment workflow.
2. Select **Split users into different processes**.
3. Select **Use an existing split** and choose **Device Ownership**. The **Device Ownership** option prompts the user to select either **Your Device** or **Company Device**. These labels can be modified.

   NOTE

   Use the **Edit List** icon to customize the split option labels.
   The Workflow page displays your enrollment workflow with the Device Ownership option after the user authentication step.

FIGURE 33 Workflow with Device Ownership Split



Create a Filter in the Device Type Split

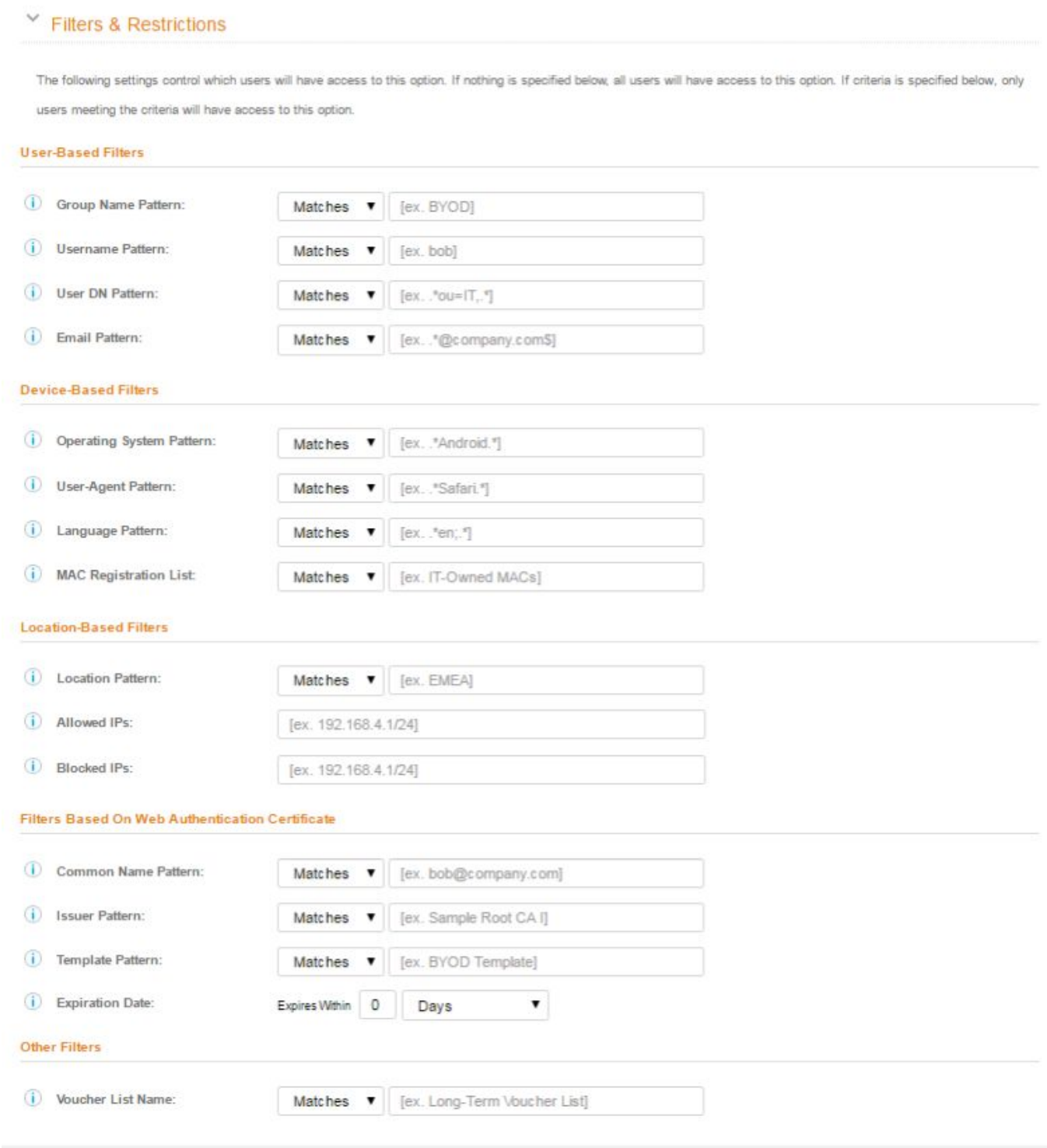
When creating splits in the workflow, you can set up a filter so that only certain users see this enrollment step.

For example, create a filter in the Device Type split that allows only users in a specified Active Directory group (ex. **BYOD App**) to receive the option for personal devices. Users that are not in the **BYOD App** AD group do not have the option to enroll personal devices and do not receive the **Device Type** prompt during enrollment.

1. On the **Enrollment Workflow** page, locate the step with the **Device Type** prompt. In this example, it is Step 4.

2. On the right side of the step, click the **Edit List** icon to open the **Selection Options** page and edit the **Your Device** option. This opens the **Modify Step** page, which allows you set up filters for this split in the workflow.

FIGURE 34 Modify Step - Filters and Restrictions



3. In the **Filters & Restrictions** section, in **User-based Filters**, enter a regex to matches the **BOYD APP** in the **Group Name Pattern** field. Cloudpath also supports Device-based, Location-based, Web authentication, and Voucher List filters.

   This filter only allows users that match the **BYOD APP** AD group name pattern to view the **Personal Device** user prompt. Users that are not in the **BYOD APP** AD group cannot enroll personal devices on the network.

   NOTE
   To see a list of available group names, return to the workflow and run a test on the Authentication Server. The test results show all of the different username patterns for the user.

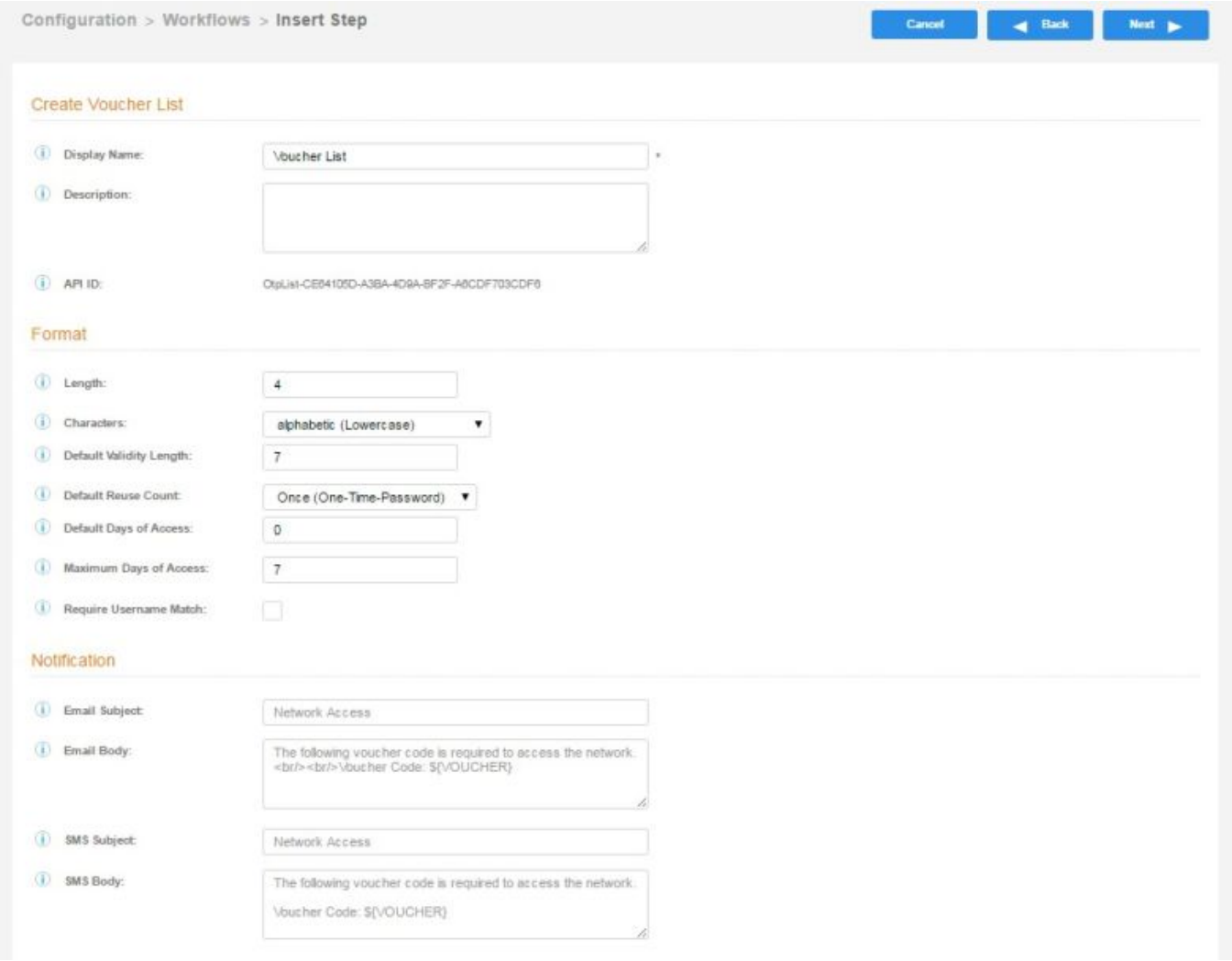
Prompt for Voucher

Step 5 adds a voucher verification step for authenticated employees with IT-assets. To create this authorization prompt:

1. Select the **Employees** tab in Step 2 and the **Company Device** tab in Step 4 of the workflow.
2. **Insert** a step above the **Result:** step in the enrollment workflow.

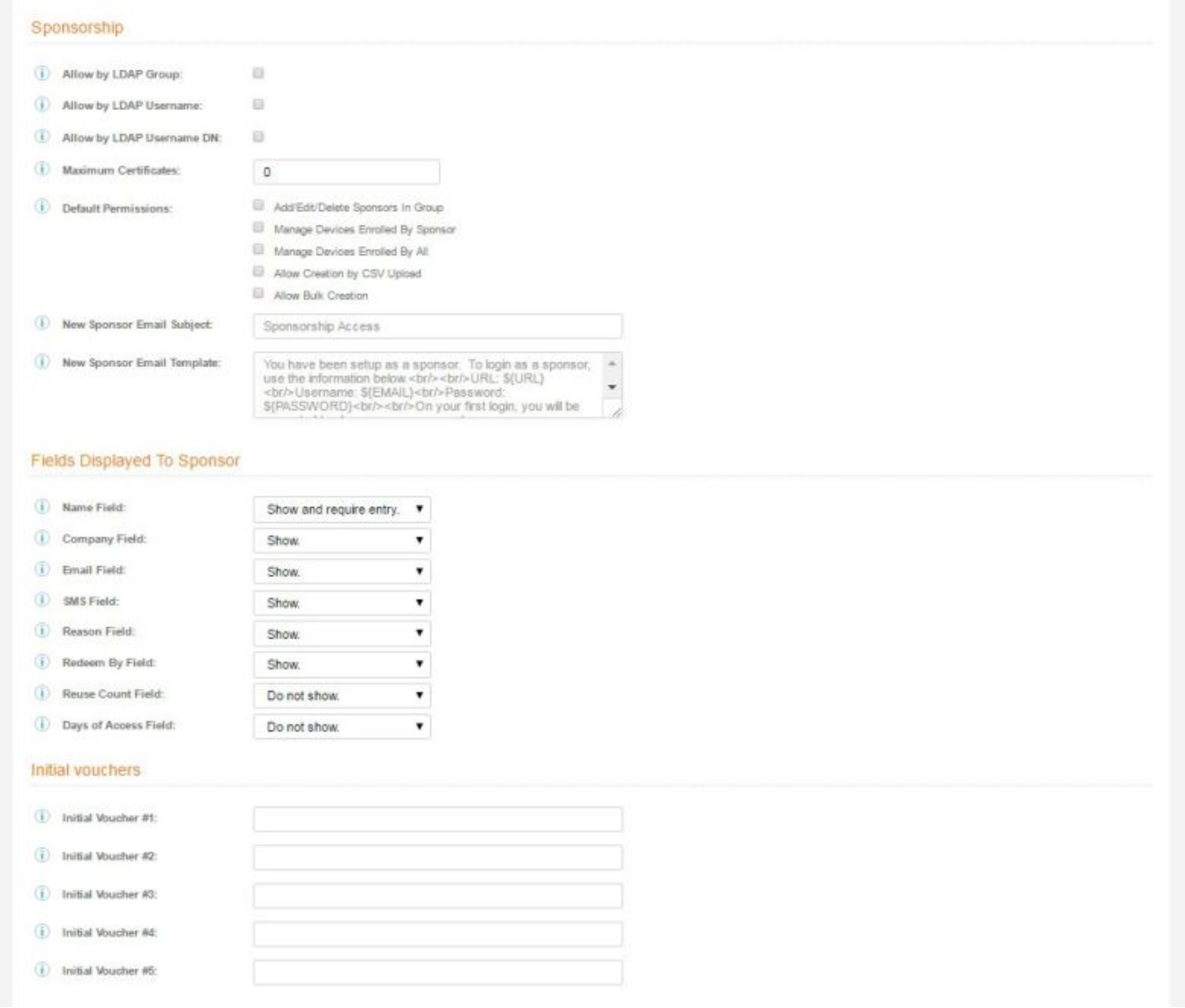
3. Select **Authenticate via voucher** and **Create a new Voucher list**.

FIGURE 35 Create Voucher List - Format and Notification Fields



4. On the **Create Voucher List** page, enter the voucher specifications for the Employees with Company Devices workflow.
   - **Format** - Describes voucher characteristics and validity.
   - **Notification** - Set up the template for emailing the voucher or sending as an SMS message.
   - **Sponsorship** - Use this section to configure the Sponsored Guest Access feature.
   - **Initial vouchers** - Create one or more initial vouchers.

FIGURE 36 Create Voucher List - Sponsorship, Fields Displayed, and Initial Vouchers



5. For the voucher prompt, select **Create a new webpage from a standard template**.
6. On the **Create Voucher Prompt** page, enter the data for the voucher prompt and **Save**.

The Workflow page displays your enrollment workflow with the **Device Ownership** option after the user authentication step.

Device Configuration and Client Certificate

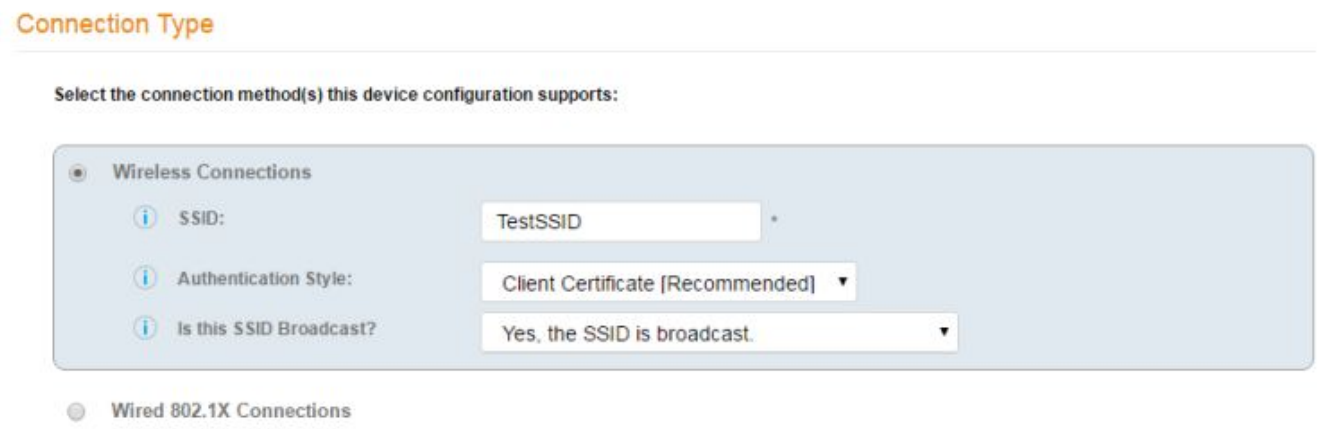
A device configuration is a group of settings containing a single configuration per operating system. This configuration determines the settings and behavior required to move the device from the onboarding SSID to the secure network.

The last step in the workflow is to migrate the user to the secure network and assign a client certificate.

Device Configuration

1. On the right side of the **Result** step, click the **Edit** icon.
2. Select **A new device configuration**.
3. On the **Add Device Configuration** page, provide a name for the device configuration. This is the name a user sees in the device Wi-Fi networks list.
4. Select **Wireless Connections** (the default) and enter the SSID of the secure wireless network.

   FIGURE 37 Configure SSID

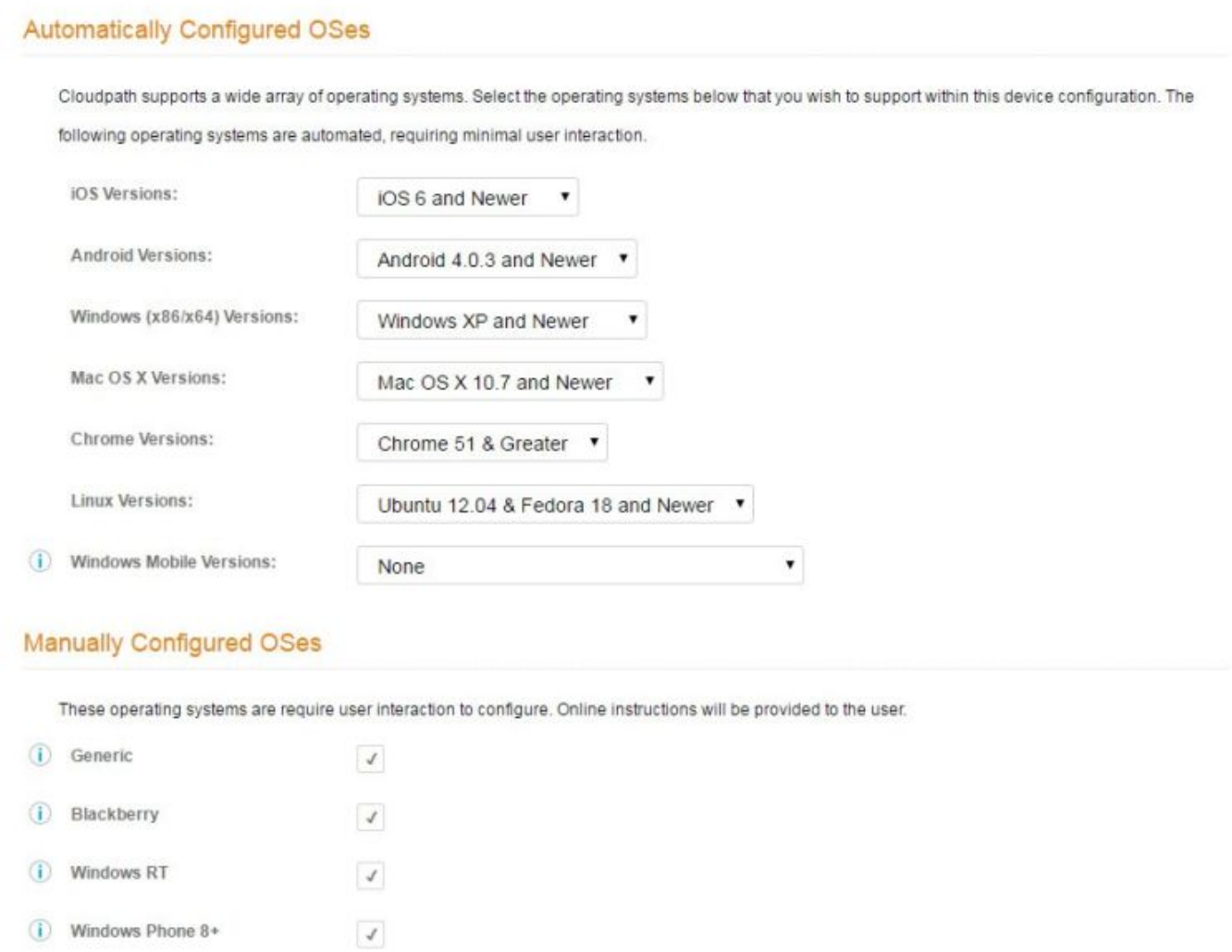


5. Set the **Authentication Style**:
   - Select **Client Certificate** for TLS network configurations
   - Select **PEAP** for PEAP/MS-CHAPv2 network configurations
   - Select **Static Pre-Shared Key** for PSK network configurations
   - Select **Ruckus DPSK** for a Dynamic Pre-Shared Key network configuration on a Ruckus controller
6. Leave the default **Broadcast** setting and click **Next**.
7. Specify **Conflicting SSIDs**.

   This setting prevents the device from roaming away from the secure SSID to any open SSID in the area.

8. Select the operating system families and versions that to support within this device configuration.
   You can restrict a particular version or service pack level after the device configuration is created.

   FIGURE 38 Select OS Versions



9. Select **Client will authenticate to the onboard RADIUS server**.
10. Configure additional settings for the device configuration.
    A more comprehensive list of additional settings is available after the device configuration is created.

Continue to the next section to select the client certificate template with the appropriate user policy.

Client Certificates

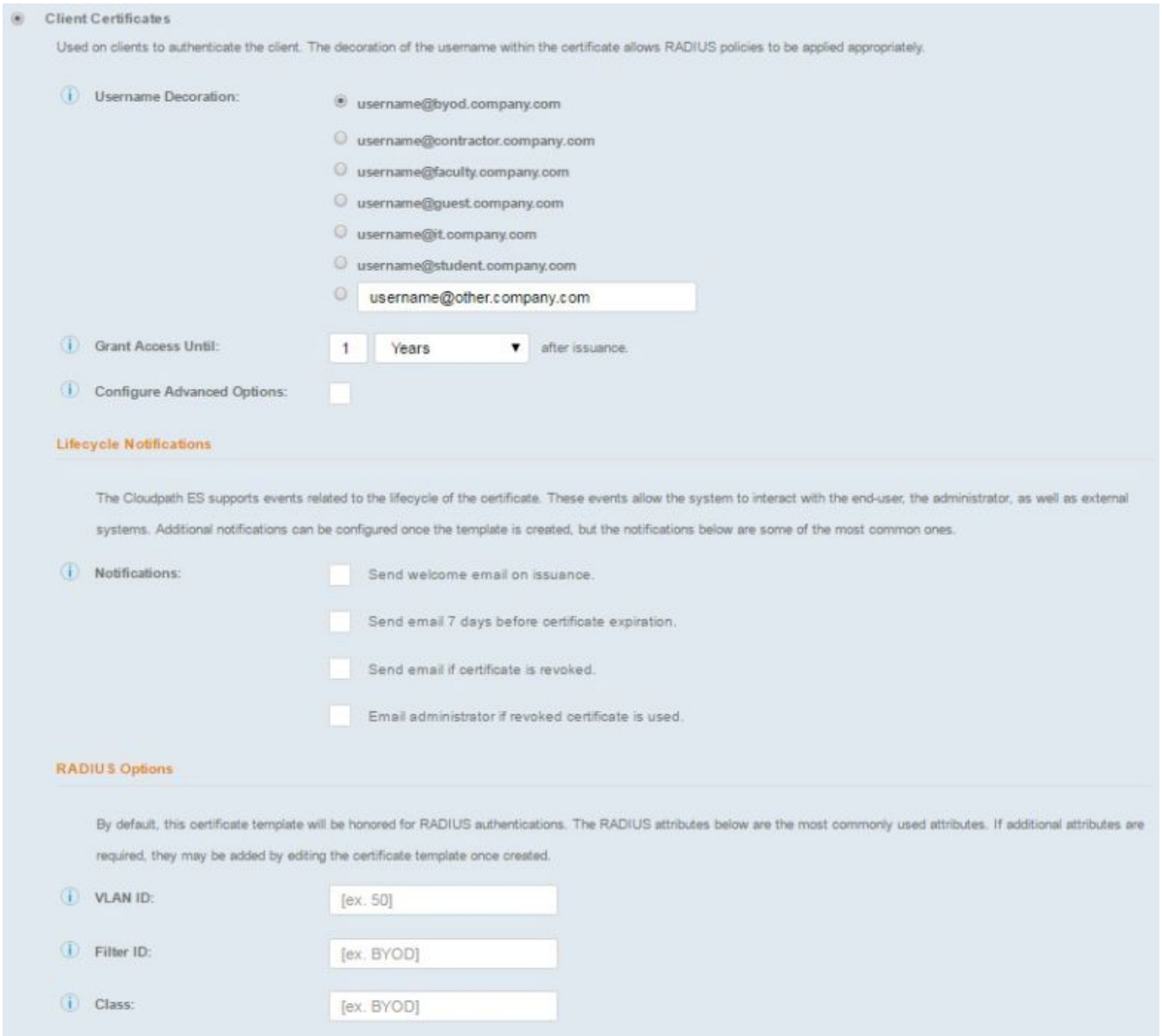
The final step in the enrollment workflow is to migrate the user to the secure network and assign a certificate to the user device. This section describes how to specify which certificate template to use when assigning a client certificate to the user device.

You can set up different certificate templates for different user types. An employee or staff certificate template might be valid for 120 days, and a guest template might be valid for 1 day or until the end of the week.

After you set up a device configuration for the workflow, you configured and assign a new certificate template.

1. Select **A new certificate template**.
2. Select **Use an onboard certificate authority**.
3. Select **Use an existing CA**. Choose the default Root CA that was created during the initial system setup.
4. Set up the **Client** certificate template. This template is used to issue a certificate to the client device.

FIGURE 39 Client Certificate Template



5. Select or enter a **Username Decoration**. The decoration of the username within the certificate allows RADIUS policies to be applied appropriately.

   The domain for the **Username Decoration** fields is taken from the **Company Information** that was entered during the initial account setup. Go to **Administration** > **Company Information** to change the default domain.

6. Grant access for the appropriate amount of time.

   For example, you might have a client certificate template for a guest user that is valid for one, or a few days, another for a contractor that is valid for 6 months, and one for employees that is good for a year.

   NOTE
   To configure pattern attributes, certificate strength, and EKUs, check the **Configure Advanced Options** box before you click **Next**.

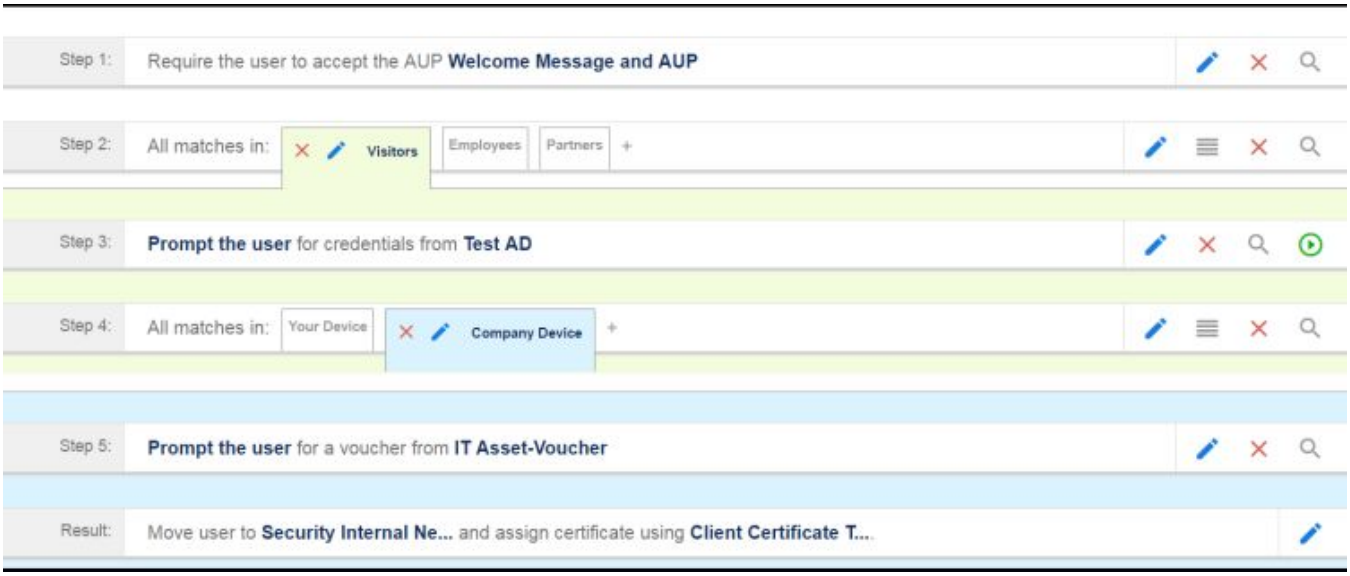
7. Select any email notifications to be sent to the user related to the life-cycle of the certificate.

   Additional certificate notifications can be configured after the template is created.

8. Optional. Enter **RADIUS Options** to assign a VLAN ID or Filter ID to certificates that use this template. These settings only applies if you are using the Cloudpath onboard RADIUS server.

9. Click **Next**. The completed workflow shows all enrollment paths. The last step shows the device configuration which is applied to the user device and the certificate template being used to assign a certificate to the user device.

FIGURE 40 Completed Workflow



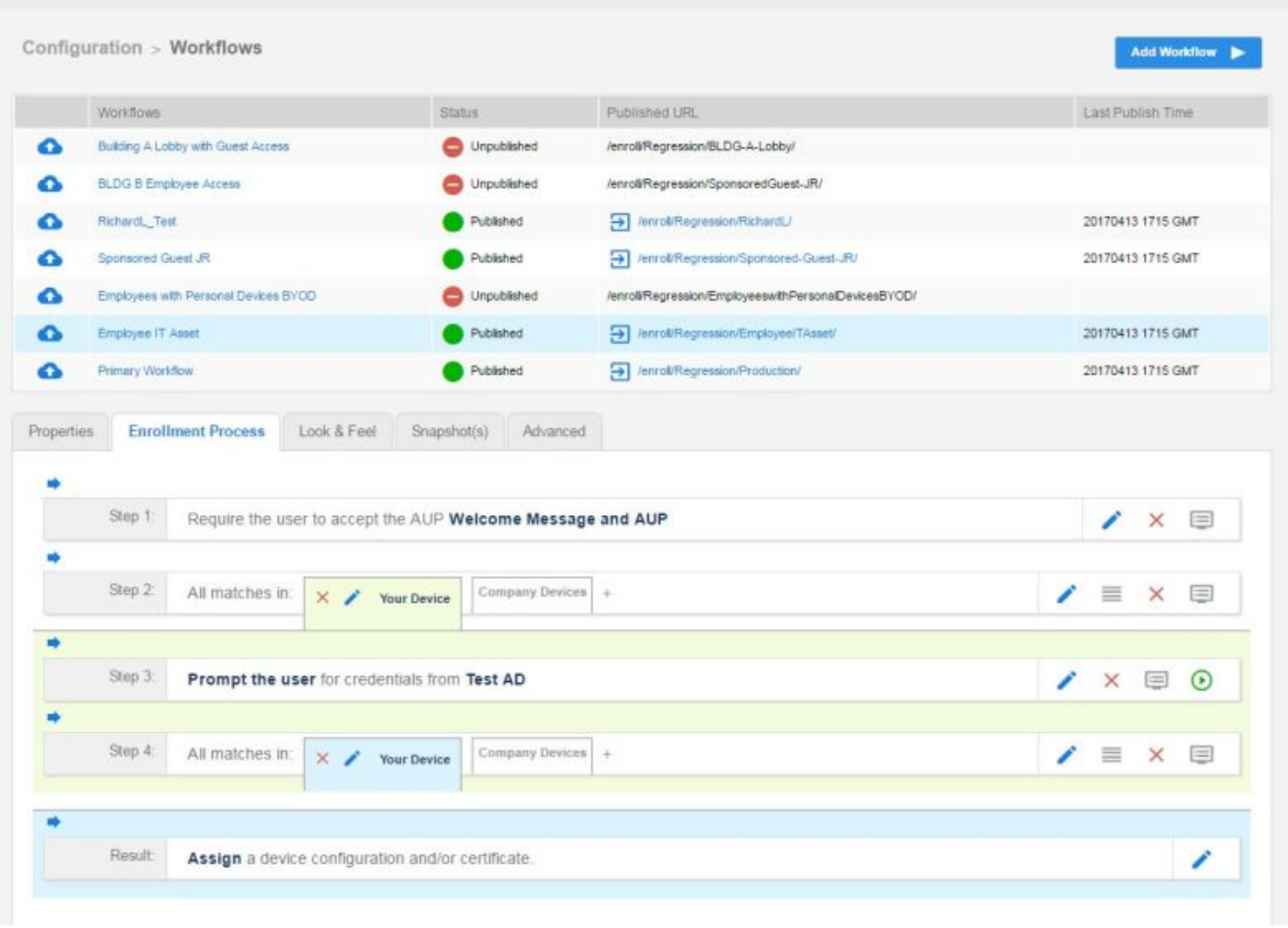
After you have finished configuring a enrollment workflow, create and deploy a snapshot of the workflow configuration to test before deploying to users.

Publishing the Enrollment Workflow

A workflow is published using Snapshots. A snapshot is a version of a workflow configuration. You can create and maintain multiple versions of each configuration. However, only one snapshot can be active at a time for each workflow.

The Workflow list contains status of the workflow (published or unpublished), the **Enrollment Portal URL** where a configuration is deployed, and the last published time for each workflow configuration.

FIGURE 41 Publish Workflows

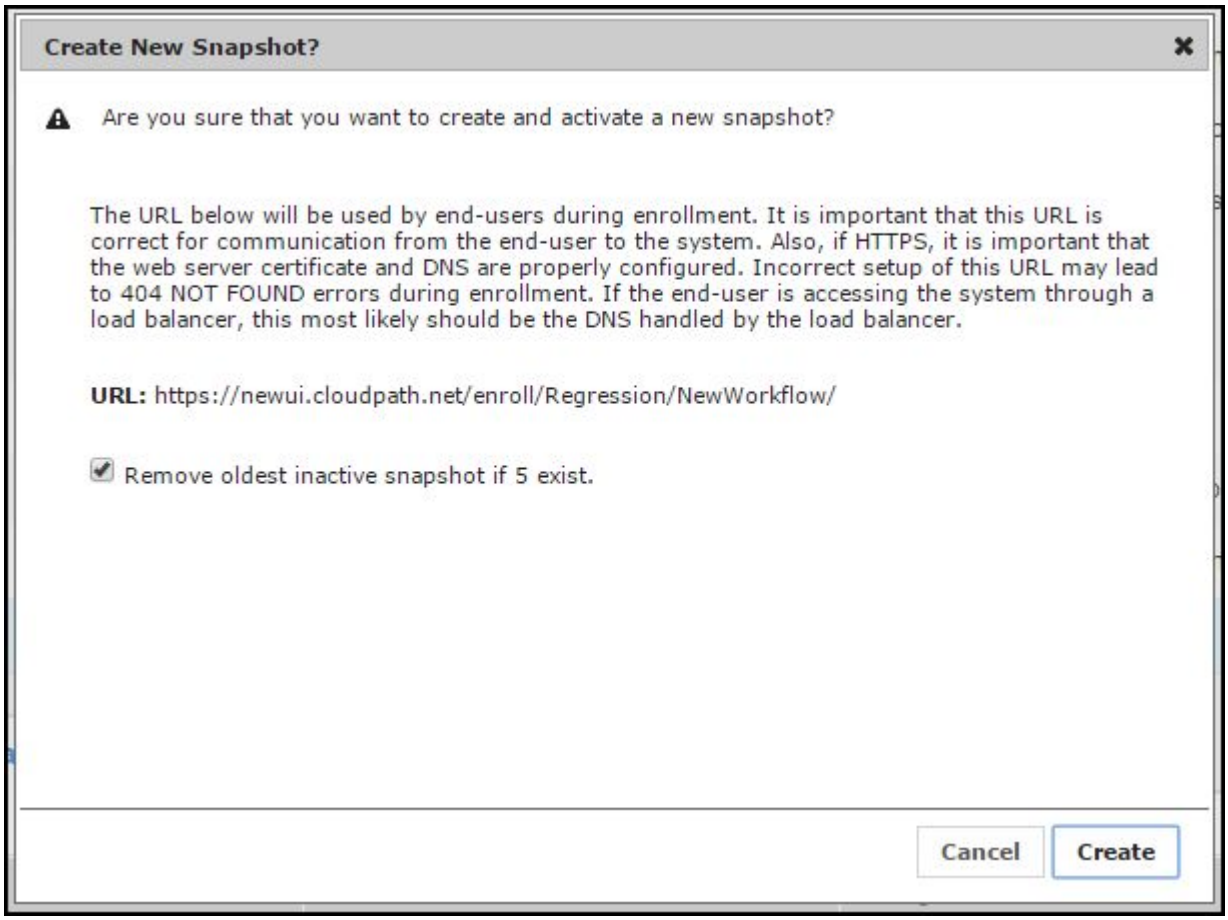


When you publish a workflow, this creates a snapshot of the workflow configuration. To publish the workflow:

1. Navigate to **Configuration** > **Workflows** tab.

2. On the Workflow configuration page, click the **Publish** icon next to the workflow to publish.

FIGURE 42 Create New Snapshot



3. Select the Wizard version to use for the new snapshot. The **Cloudpath Wizard** is the application provided to users to automate the enrollment process.
4. Verify the Enrollment Portal URL for the snapshot.
5. Click **Create**.

It takes a few minutes to build the deployment package. During this process, all Cloudpath workflow branches are pulled in by the Cloudpath system and bundled as one configuration.

How to Test a Published Workflow

Test the enrollment process for the active workflow snapshot using the Enrollment Portal URL. The Enrollment Portal URL provides access to the user enrollment process, which contains the workflow and if applicable, the Cloudpath Wizard.

1. Navigate to the **Configuration** > **Workflows** page.
2. On the workflow list, select the workflow to test.
3. Click the Enrollment Portal URL. Be sure that the snapshot you want to test is the **active** snapshot (green icon).

Ruckus Controller Integration for Cloudpath

- Overview....81
- Setting up Cloudpath as an AAA Authentication Server....81
- Creating AAA Accounting Server (Optional)....84
- Running Authentication Test....85
- Creating Hotspot Services....87
- Setting Up the Walled Garden....92
- Creating the Onboarding SSID....94
- Creating the Secure SSID....100

Overview

This section describes how to configure the Ruckus Zone Director, SmartZone, and Unleashed controllers to integrate with the Cloudpath system.

The screen shots and corresponding instructions in this manual are based on the following Ruckus Controller versions:

- ZoneDirector 10.1.1
- Virtual SmartZone 3.6.0 (High Scale)
- Unleashed 200.6

If you are using different versions of any controller, please consult your controller documentation because you may encounter some differences in the user interface.

Setting up Cloudpath as an AAA Authentication Server

Create an AAA authentication server for the Cloudpath onboard RADIUS server. The following images show this configuration on the Ruckus ZoneDirector, SmartZone, and Unleashed controllers.

On ZoneDirector, go to **Services & Profiles > AAA Servers**. On SmartZone, go to **Services & Profiles > Authentication**. On Unleashed, go to **Admin & Services > Services > AAA Servers > Authentication Servers**.

FIGURE 43 Create AAA Authentication Server on ZoneDirector

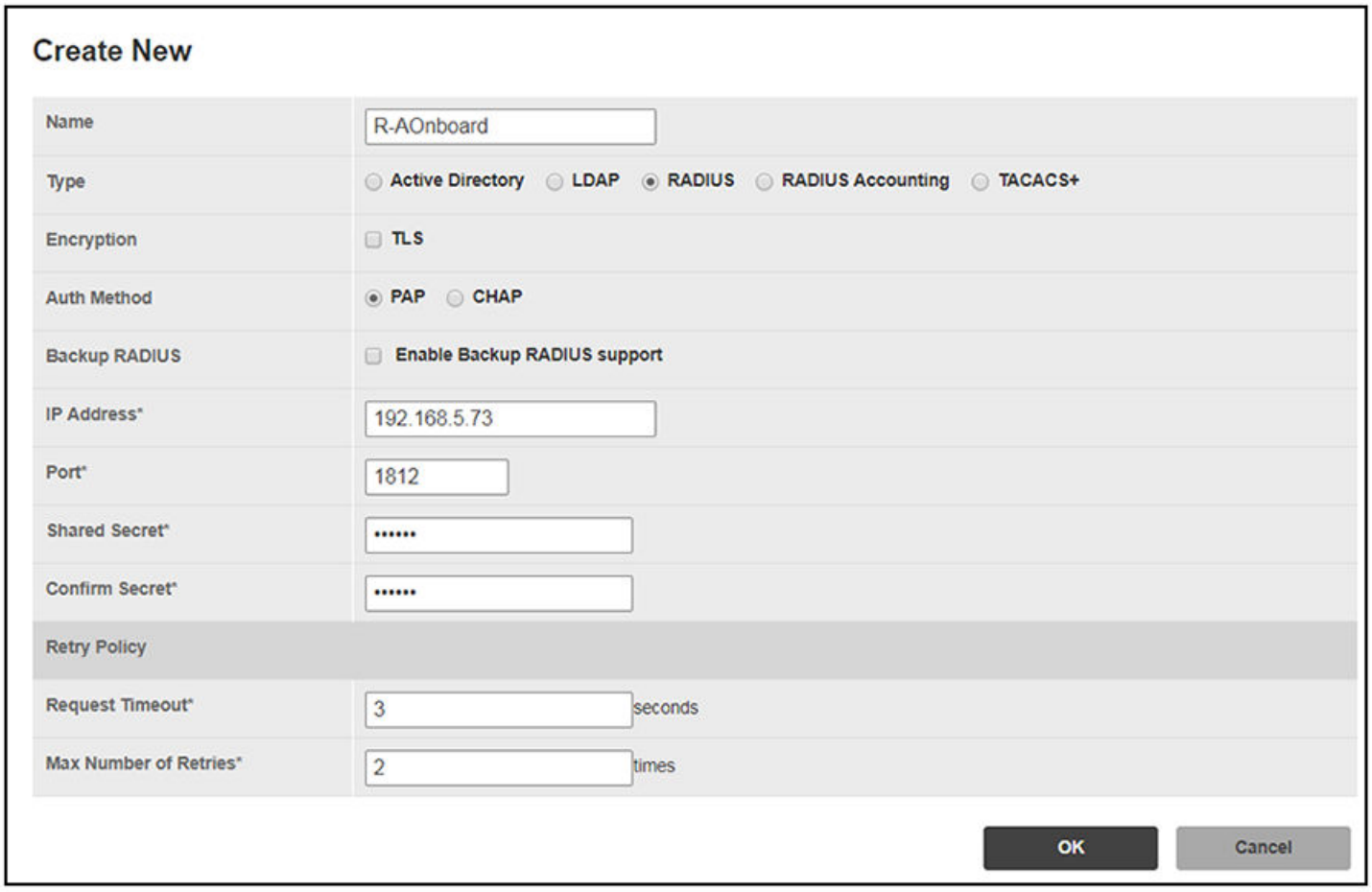


FIGURE 44 Create AAA Authentication Server on SmartZone

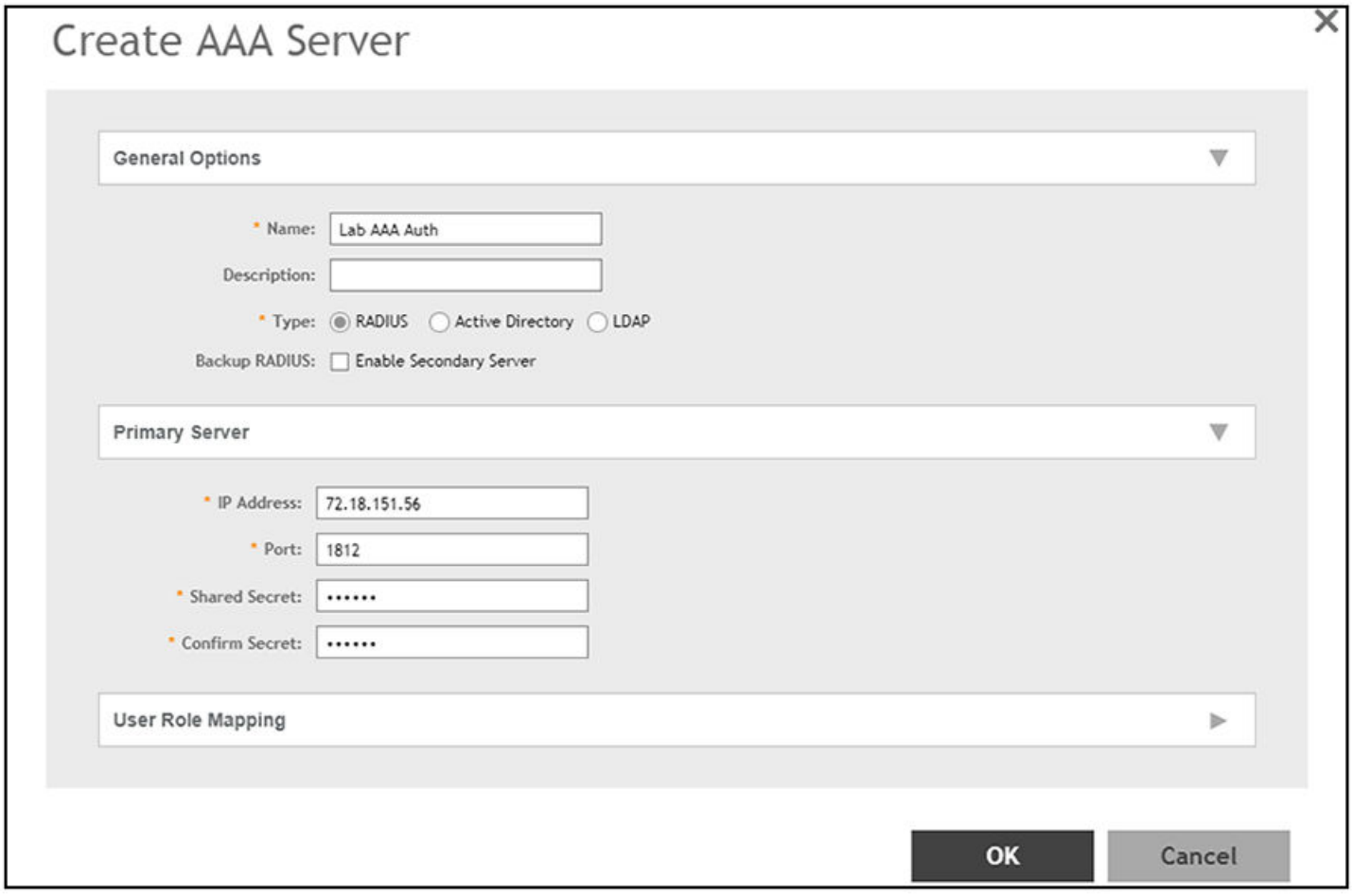
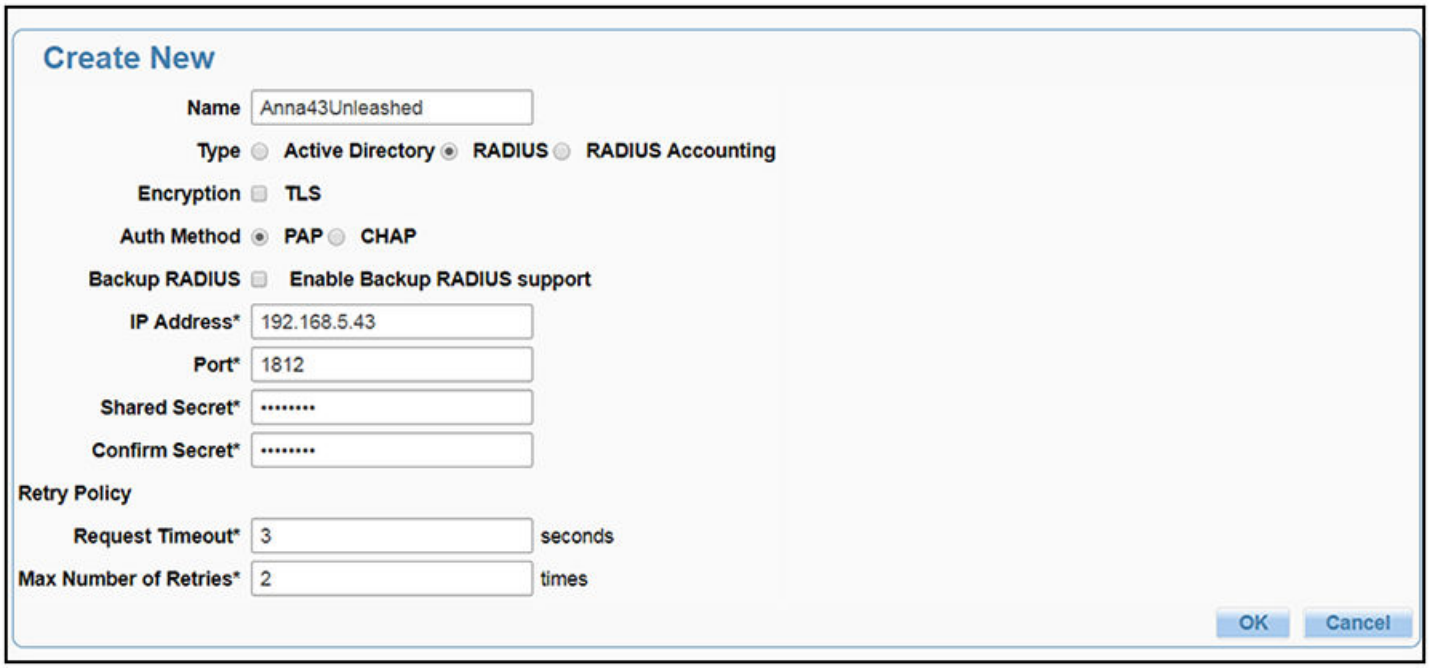


FIGURE 45 Create AAA Authentication Server on Unleashed



Enter the following values for the **Authentication** Server:

1. Name
2. Type = RADIUS
3. Auth Method (not applicable for SmartZone) = PAP
4. IP address = The IP address of the Cloudpath ES.
5. Port = 1812
6. Shared Secret = This must match the shared secret for the Cloudpath ES onboard RADIUS server. (**Configuration** > **RADIUS Server**).
7. Leave the default values for the remaining fields.

Creating AAA Accounting Server (Optional)

Use the same process to create the AAA Accounting Server.

> **NOTE**
> To navigate to the correct screen on Ruckus SmartZone, go to **Services & Profiles > Accounting**.

Enter the following values for the **Accounting** Server:

1. Name
2. Type = RADIUS ACCOUNTING.
3. IP address = The IP address of the Cloudpath ES.

4. Port = 1813

   NOTE
   The Authentication server uses port 1812. The Accounting server uses port 1813.

5. Shared Secret = This must match the shared secret for the Cloudpath ES onboard RADIUS server. (**Configuration > RADIUS Server**)
6. Leave the default values for the remaining fields.

Running Authentication Test

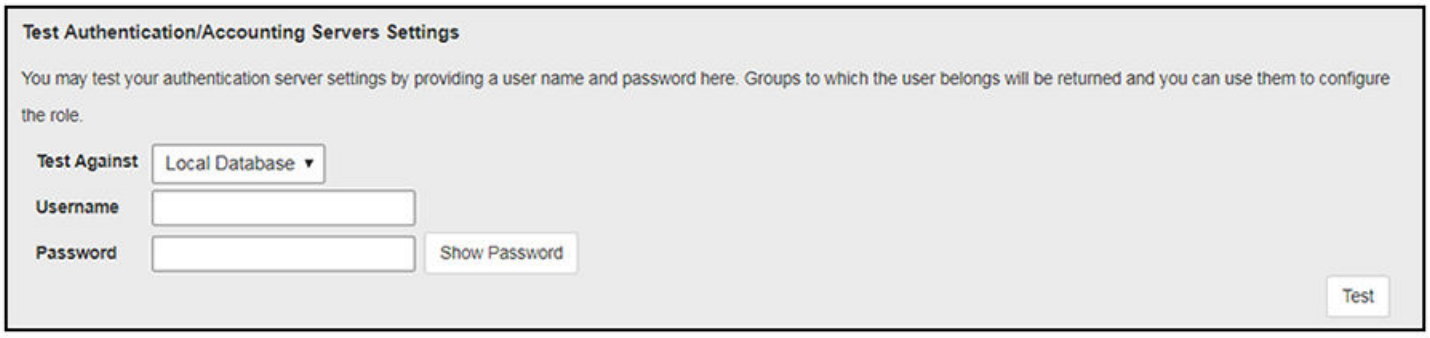
You can test the connection between the controller and the Cloudpath ES RADIUS server.

Follow the instructions for the applicable controller. For the possible results, see Possible Results from Authentication Test.

ZoneDirector

At the bottom of the AAA server page, there is a section called "Test Authentication/Accounting Servers Settings." The Test Against field should be Local Database, as shown below. Enter a test User Name and Password, then click the **Test** button.

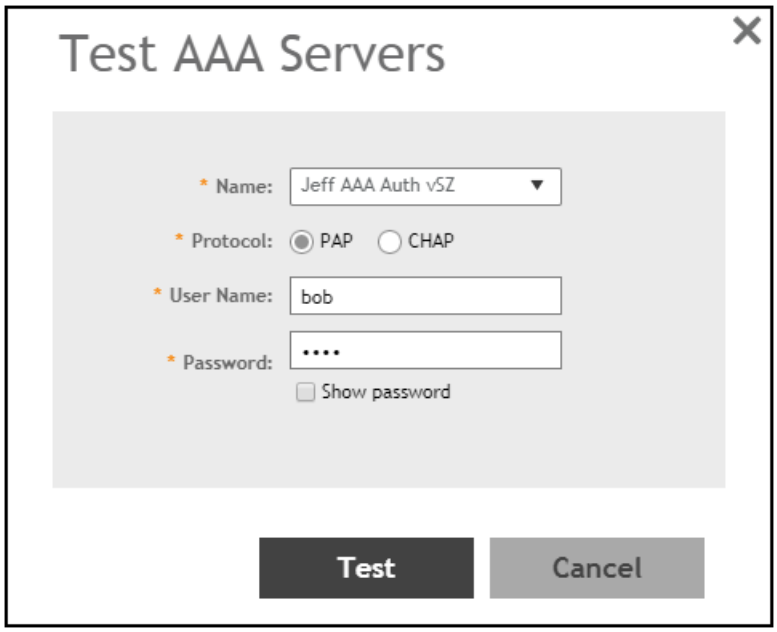
FIGURE 46 Authentication Test on ZoneDirector



SmartZone

When you save a configuration for an AAA Authentication server in SmartZone, you can click the **Test AAA** tab at the top of the screen, select the server from the drop-down list, enter your credentials, then click the **Test** button.

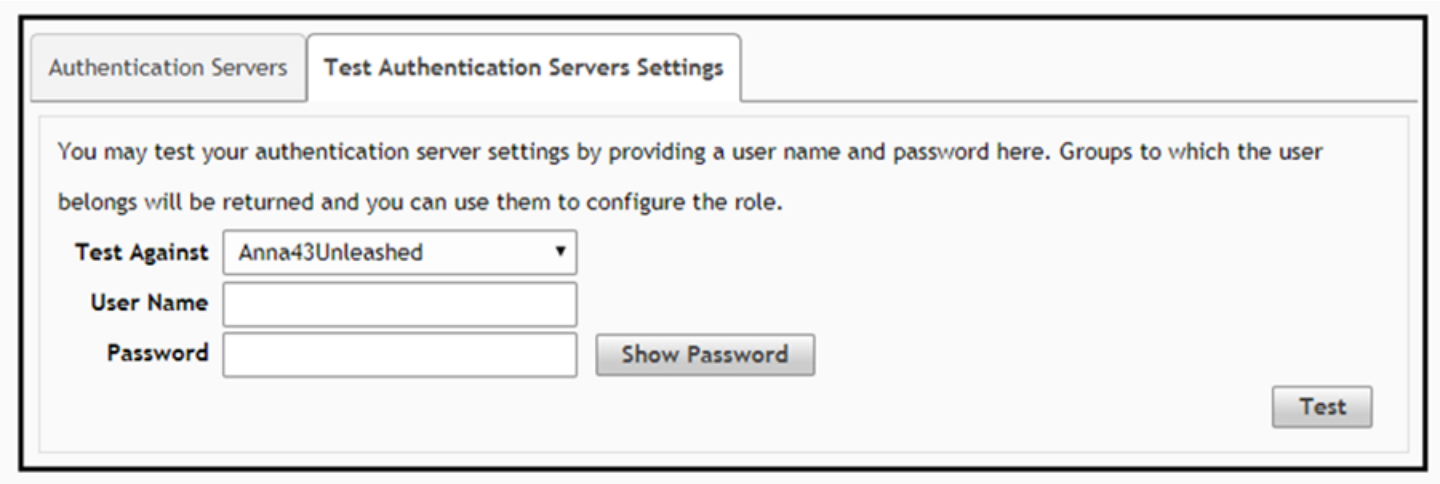
FIGURE 47 Authentication Test on SmartZone



Unleashed

Enter the test credentials on the Test Authentication Servers Settings tab, then click the **Test** button.

FIGURE 48 Authentication Test on Unleashed



Possible Results from Authentication Test

If you run the authentication test, you receive one of these responses:

- `Failed! Connection timed out`
- `Failed! Invalid username and password`

- `Authentication Failed`

The only one of these responses that means that connectivity was established is:

`Failed! Invalid username or password`

Creating Hotspot Services

You can configure the Hotspot Service on the ZoneDirector, SmartZone, or Unleashed controllers.

1. Navigate to: For ZoneDirector, go to **Services & Profiles > Hotspot Services**. For SmartZone, go to **Services & Profiles > Hotspots & Portals > Hotspot WISPr**. For Unleashed, go to **Admin & Services > Services > Hotspot Services**, then use both the **General** tab and the **Authentication** tab, as instructed later in this section.

2. Name the Hotspot Service.

FIGURE 49 Create Hotspot Service on ZoneDirector

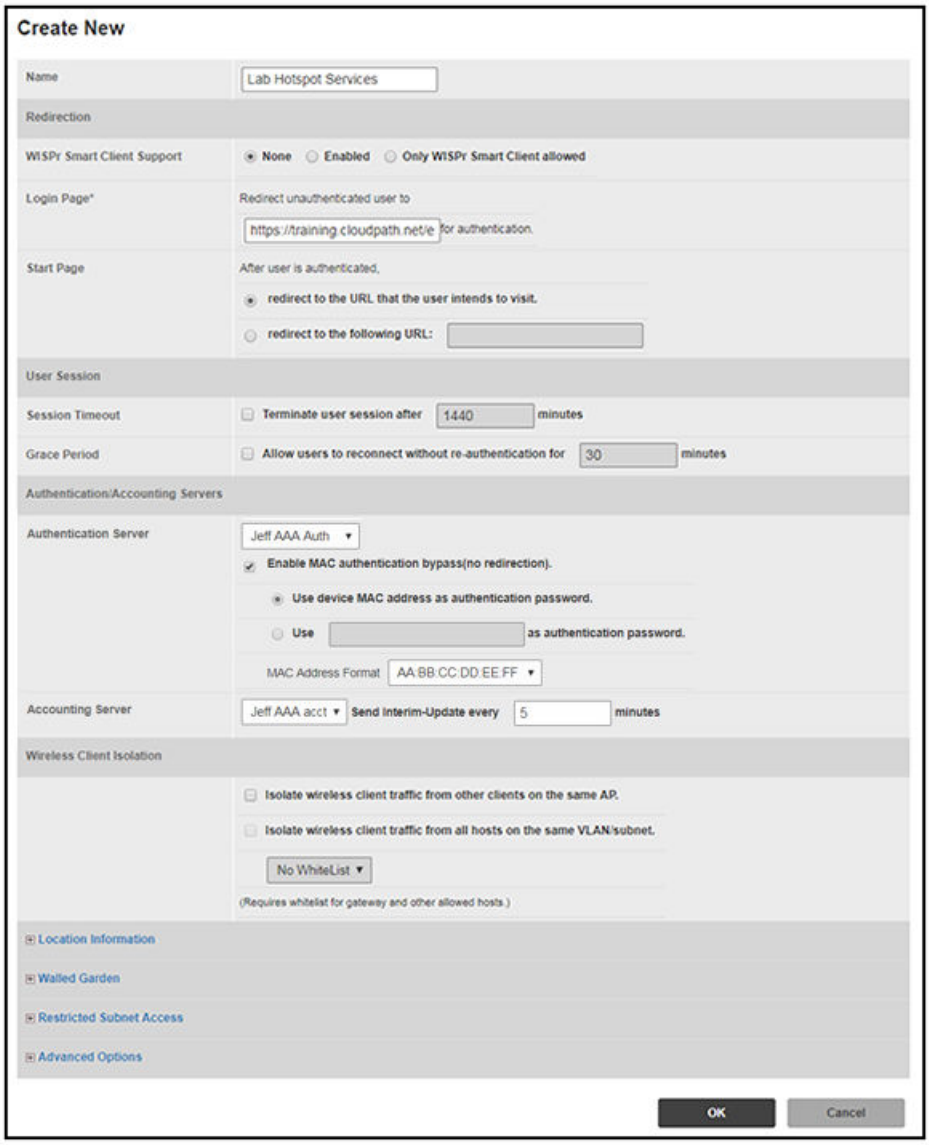


FIGURE 50 Create Hotspot WISPr on SmartZone

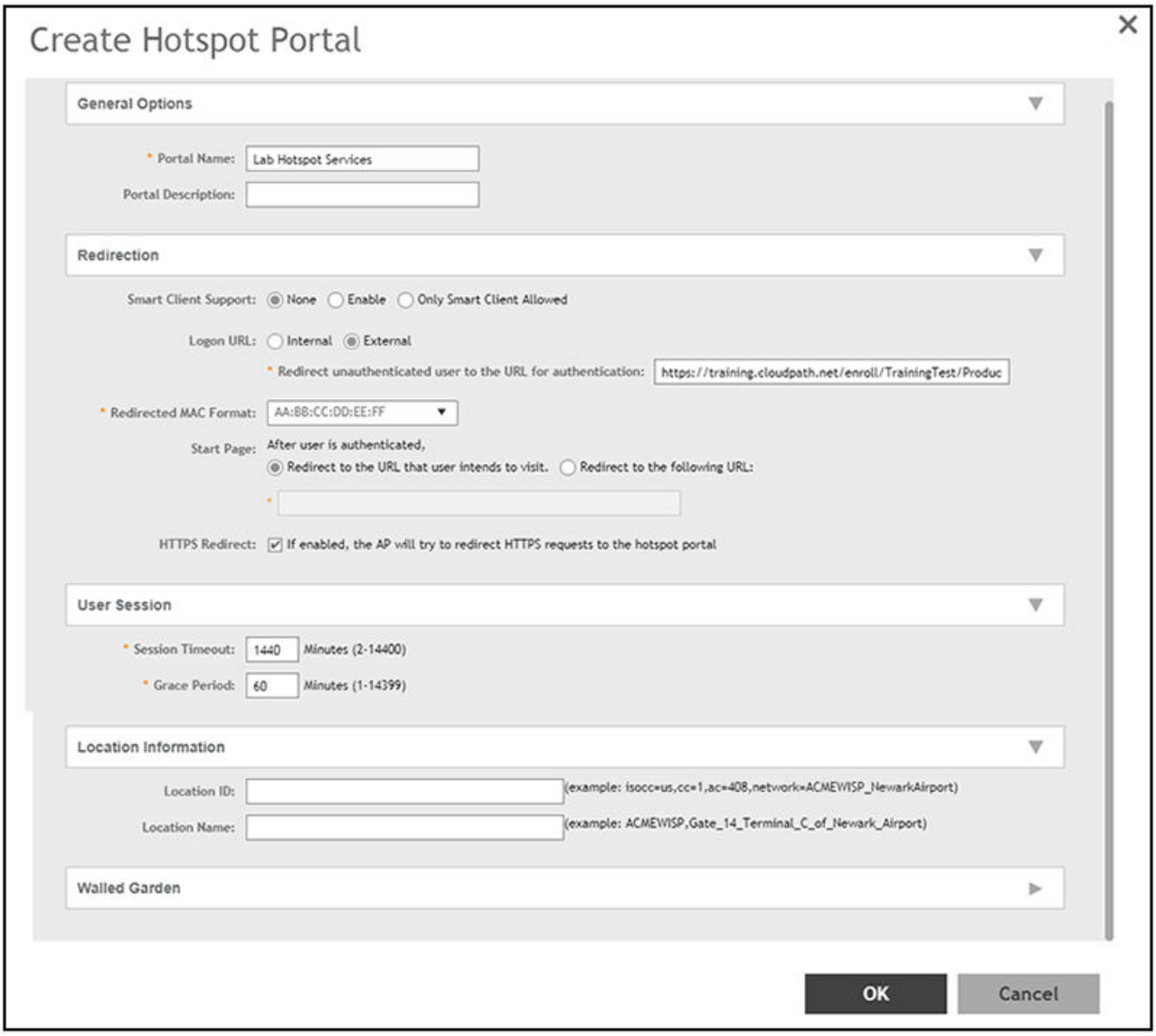


FIGURE 51 Create Hotspot Service on Unleashed - General Tab

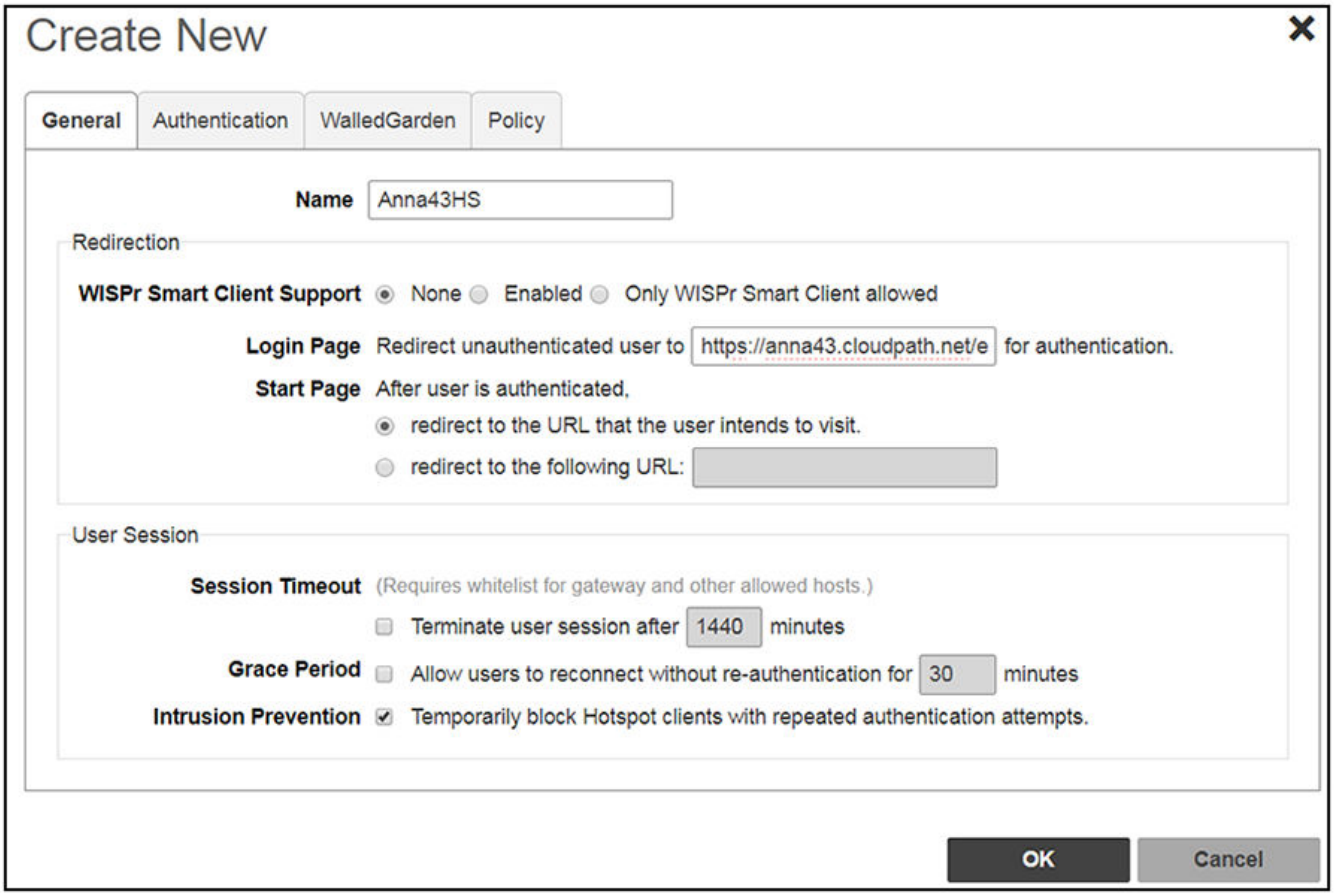
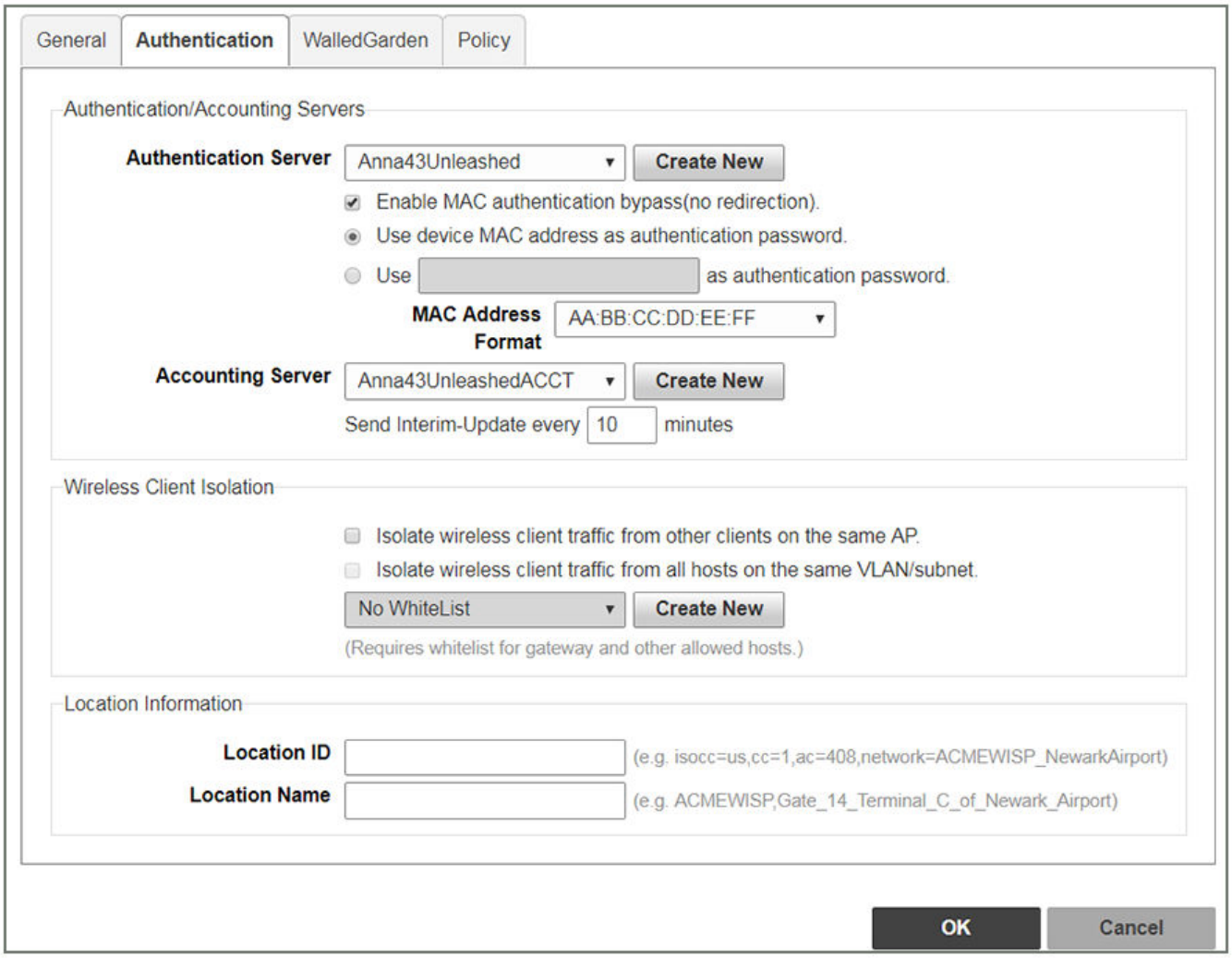


FIGURE 52 Create Hotspot Service on Unleashed - Authentication Tab



3. Point the unauthenticated user to the **Cloudpath Enrollment Portal URL**, which can be found on the **Cloudpath Admin UI Configuration** > **Workflows** page, in the **Workflows** table.
4. Check **Redirect to the URL that the user intends to visit**.
5. Select the **Cloudpath RADIUS Authentication Server**. Applicable only for ZoneDirector and Unleashed (**Authentication** tab) in this screen.
6. Select **Enable MAC authentication bypass (no redirection)**. Applicable only for ZoneDirector and Unleashed (**Authentication** tab) in this screen. Selecting this field allows users with registered MAC addresses to be transparently authorized without having to log in.
7. For MAC Address Format (which appears when you select **Enable MAC authentication bypass (no redirection)** in the preceding step, it is recommended that you select the following option from the drop-down list: AA:BB:CC:DD:EE:FF
8. Select the **Cloudpath RADIUS Accounting Server**. Applicable only for ZoneDirector and Unleashed (**Authentication** tab).
9. Leave the defaults for the remaining settings. Click **OK**.

Setting Up the Walled Garden

Perform the following steps to add a walled garden configuration to your existing Hotspot Services configuration:

1. Navigate to: For ZoneDirector, go to **Services & Profiles > Hotspot Services**. For SmartZone, go to **Services & Profiles > Hotspots & Portals > Hotspot WISPr**. For Unleashed, go to **Admin & Services > Services > Hotspot Services**.

2. For ZoneDirector and SmartZone, use the **edit** function on the existing Hotspot Services configuration, then scroll to the **Walled Garden** section and expand this section. For Unleashed, click the **WalledGarden** on the existing Hotspot Services configuration.

FIGURE 53 Walled Garden Configuration for ZoneDirector

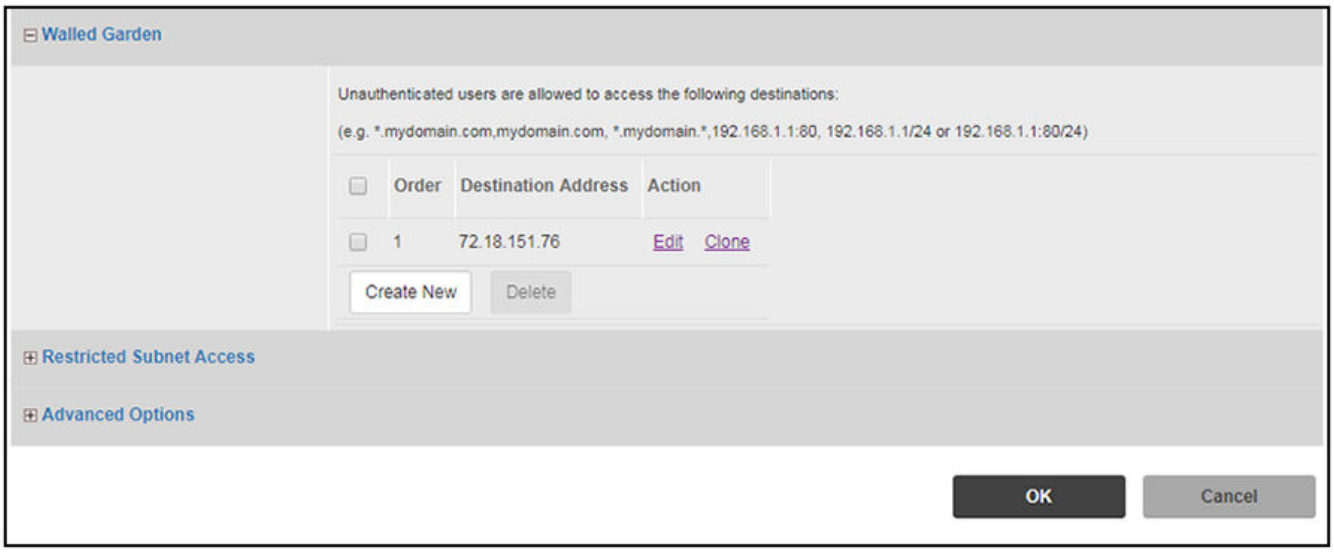


FIGURE 54 Walled Garden Configuration for SmartZone

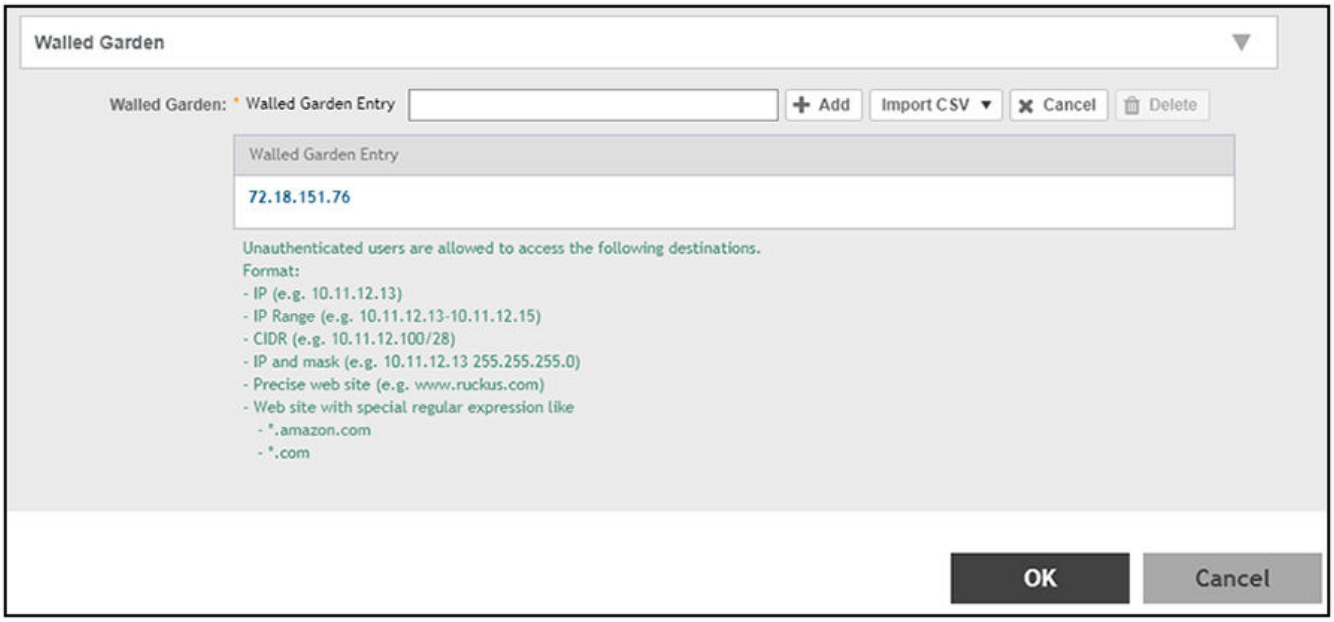
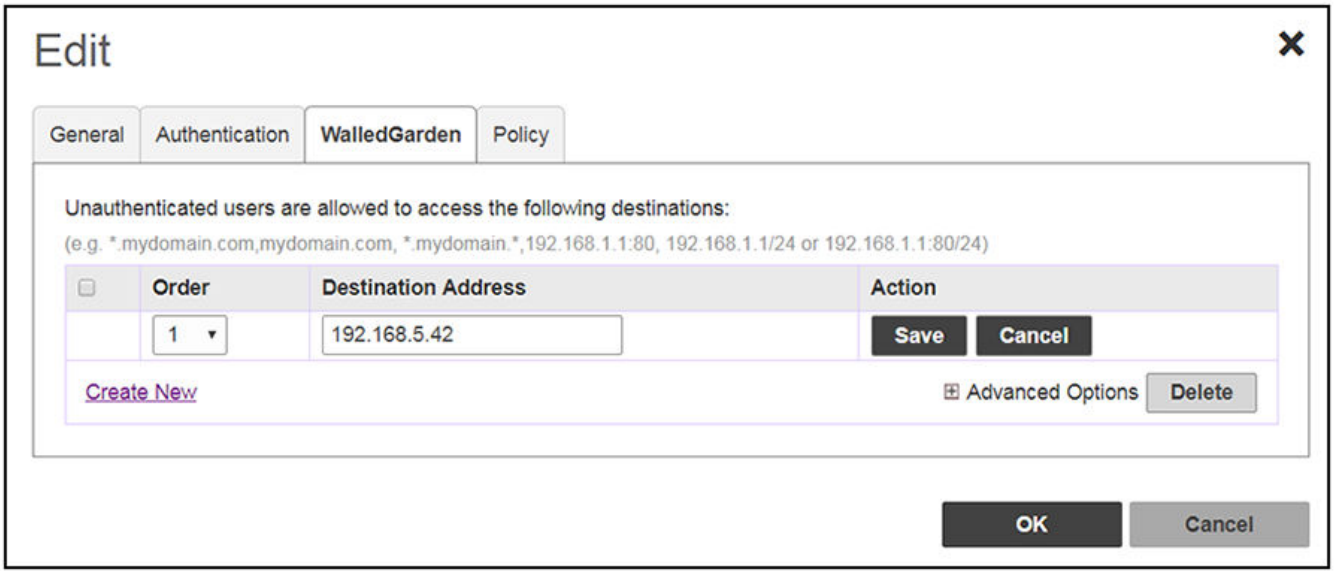


FIGURE 55 Walled Garden Configuration for Unleashed



3. Include the DNS or IP address of the Cloudpath system, then click **OK**.
4. Optionally, there are some domains that you can add to the walled garden on all controllers to:
   - Prevent the Apple CNA mini-browser from appearing on Apple devices.
   - Avoid being blocked or slowed when attempting to download the Cloudpath wizard.

   These recommended destinations for the walled garden are:

```
*.ggpht.com
*.play.googleapis.com
*.play.google.com
*.android.clients.google.com
*.www.googleapis.com
*.gvt1.com
*.connectivitycheck.android.com
*.gstatic.com
*.clients3.google.com
```

Creating the Onboarding SSID

To configure the onboarding SSID, navigate to: For ZoneDirector and SmartZone, go to the Wireless LANS section of the controller UI; for Unleashed, go to **Wifi Networks** to create the WLAN.

1. Name the SSID.

2. Type=Hotspot Service (WISPr).

FIGURE 56 Onboarding SSID Configuration on ZoneDirector

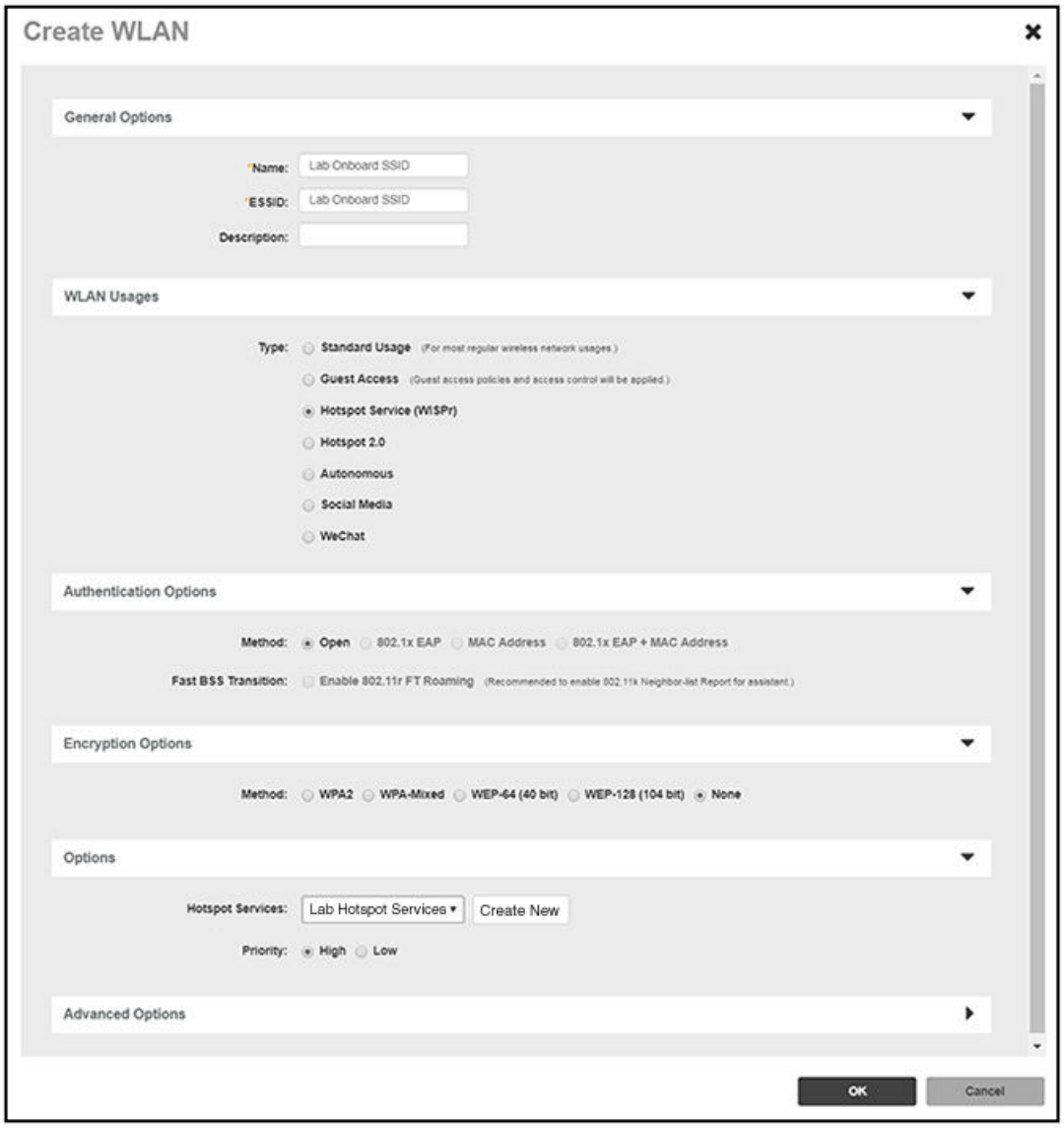


FIGURE 57 Onboarding SSID Configuration on SmartZone

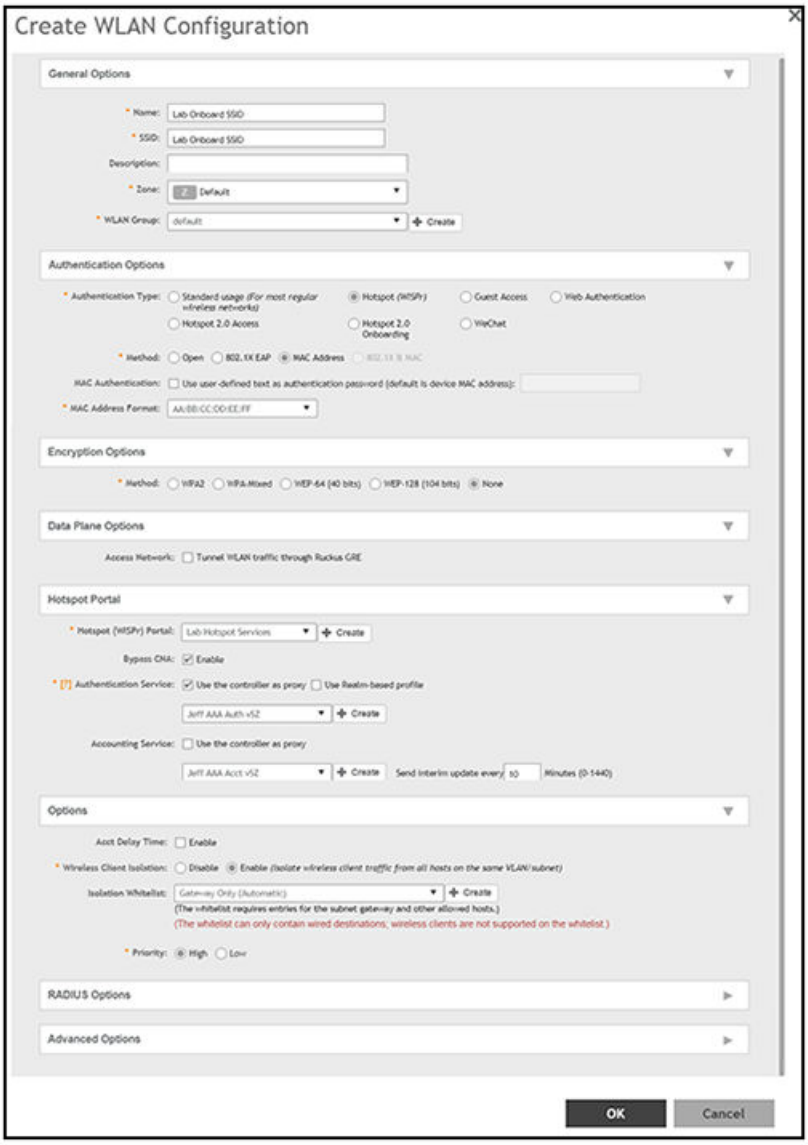
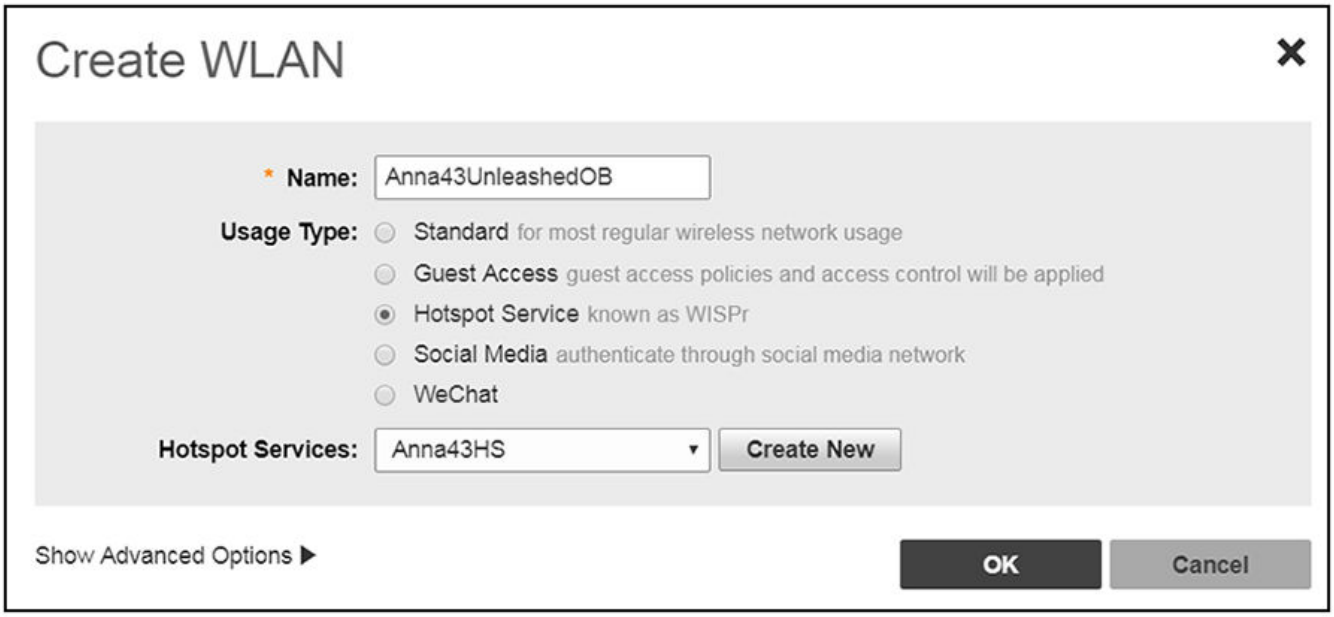


FIGURE 58 Onboarding SSID Configuration for Unleashed



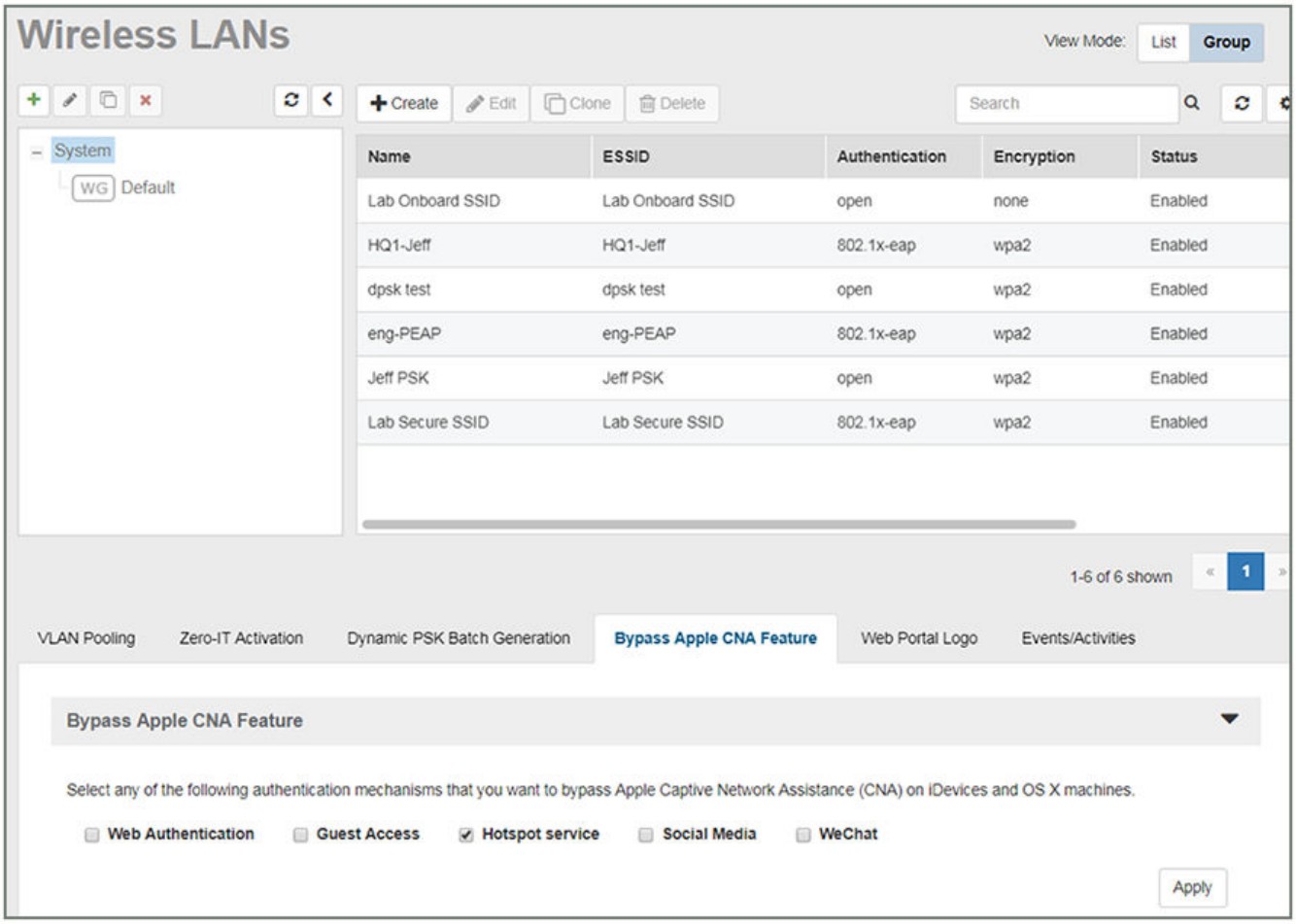
3. Authentication Options Method=Open for ZoneDirector, MAC Address for SmartZone. (Not applicable for Unleashed.)
4. The checkbox next to MAC Authentication (SmartZone only) called "Use user defined text as authentication password (default is device MAC address):" can be left unchecked.
5. The MAC Address Format (SmartZone only) recommended selection is: AA:BB:CC:DD:EE:FF. This is the default for most RADIUS servers.
6. Encryption Options Method=None (ZoneDirector and SmartZone).
7. Select the Hotspot Service from the drop-down list that you should already have created in a previous step procedure.
8. Enable the **Bypass CNA** feature as follows, depending on the controller:
   - For SmartZone: Check the box to enable "Bypass CNA," as shown in Figure 57.
   - For ZoneDirector, after you finish configuring the onboarding SSID, refer to Figure 59 on page 98.
   - For Unleashed, after you finish configuring the onboarding SSID, refer to Figure 61 on page 99.
9. Select the Cloudpath RADIUS Authentication Server (SmartZone only).
10. Select the Cloudpath RADIUS Accounting Server (SmartZone only).
11. Leave the defaults for the remaining settings and click **OK** (or **Apply**).

Enabling Bypass CNA on ZoneDirector

It is recommended to enable the "Bypass Apple CNA Feature," which you can do globally for wireless LANs in ZoneDirector.

1. In the Wireless LANs main screen, click on **Bypass Apple CNA Feature**, as shown in the following figure:

FIGURE 59 Enabling the Bypass Apple CNA Feature Globally on ZoneDirector



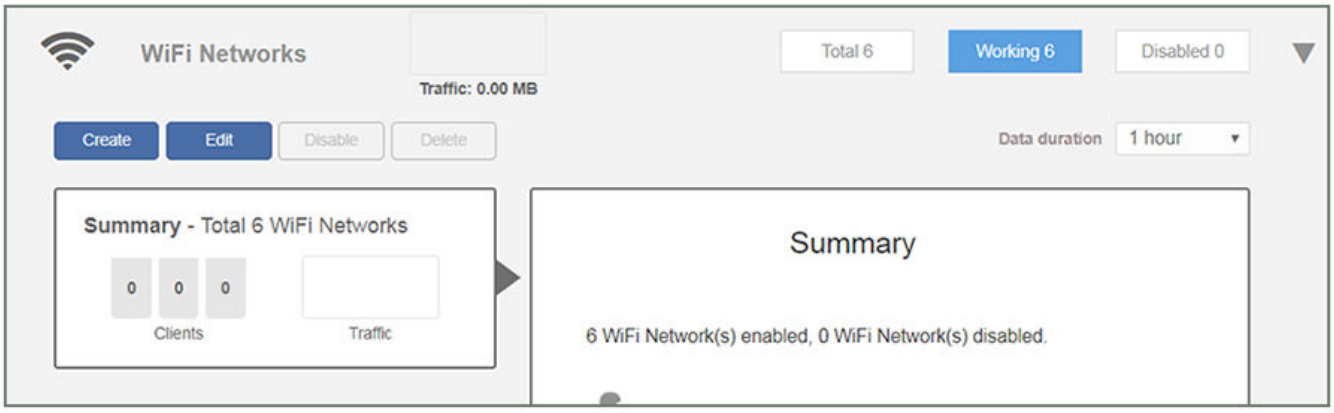
2. In the "Bypass Apple CNA Feature" area of the screen, check the "Hotspot service" box.
3. Click **Apply** to enable the "Bypass Apple CNA Feature" globally on all Wireless LANs that are configured as type "Hotspot Service (WISPr)."

Enabling Bypass CNA on Unleashed

It is recommended to enable the "Bypass Apple CNA Feature," which you can do globally for wireless LANs in Unleashed.

1. In the WiFi Networks main screen (see figure below), click **Edit**.

FIGURE 60 Clicking the Edit Button Brings you to Global Configuration



2. In the Global Configuration screen that pops up, click **Bypass Apple CNA Feature**.

FIGURE 61 Enabling the Bypass Apple CNA Feature Globally on Unleashed



3. In the "Bypass Apple CNA Feature" area of the screen, check the "Hotspot service" box.
4. Click **Apply** to enable the "Bypass Apple CNA Feature" globally on all Wireless LANs that are configured as type "Hotspot Service (WISPr)."

Creating the Secure SSID

To configure the onboarding SSID, navigate to: For ZoneDirector and SmartZone, go to the Wireless LANS section of the controller UI; for Unleashed, go to **Wifi Networks** to create the WLAN.

1. Name the SSID.
2. Type=Standard Usage.
3. Authentication Option Method=802.1x EAP.
4. Encryption Option Method=WPA2 (not applicable for Unleashed once the 802.1x EAP authentication option method is selected).
5. Encryption Option Algorithm=AES (not applicable for Unleashed once the 802.1x EAP authentication option method is selected).
6. Select the Cloudpath RADIUS authentication server.
7. Select the Cloudpath RADIUS accounting server (required only if you are using Cloudpath onboard RADIUS Accounting and Connection Tracking). **Note**: For ZoneDirector, you need to expand the Advanced Options section of the screen to locate the drop-down selection for the accounting server.

8. Leave the defaults for the remaining settings and click **OK**.

FIGURE 62 Configure Secure SSID on the ZoneDirector controller

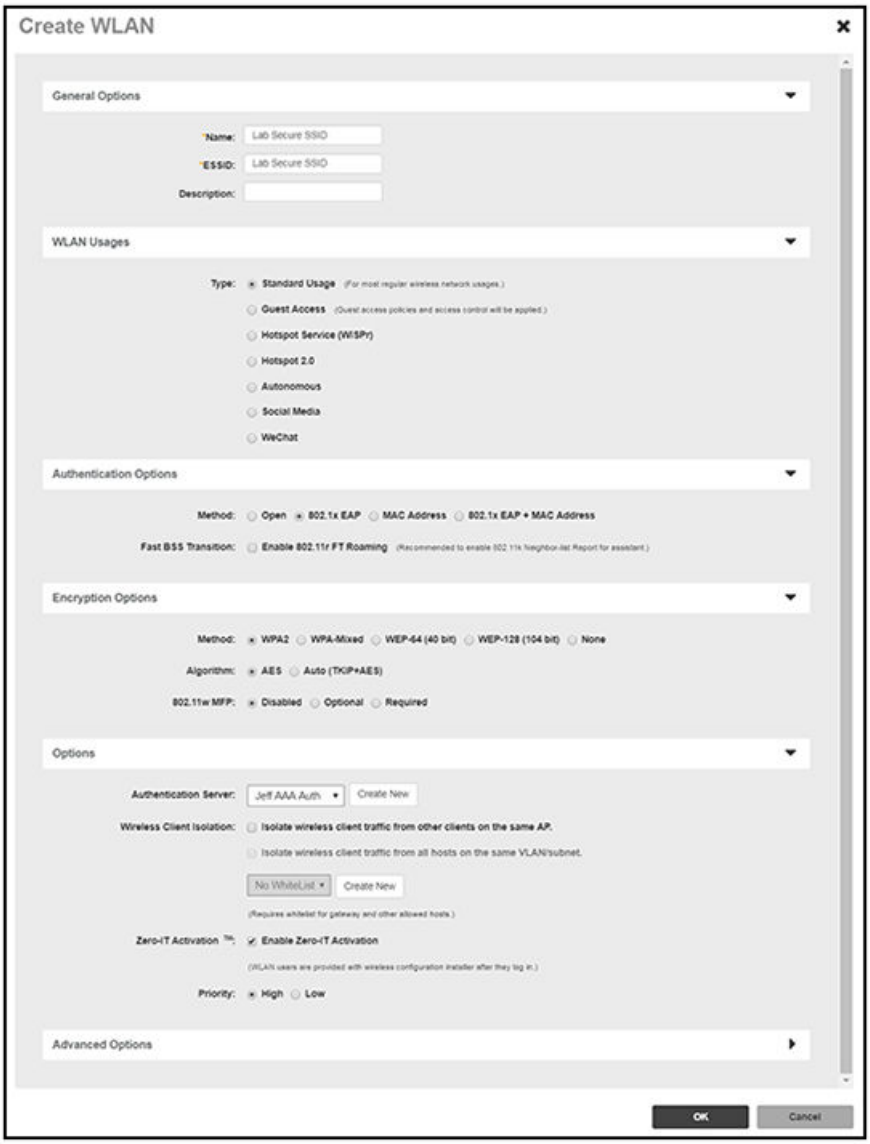


FIGURE 63 Select RADIUS Accounting Server on ZoneDirector

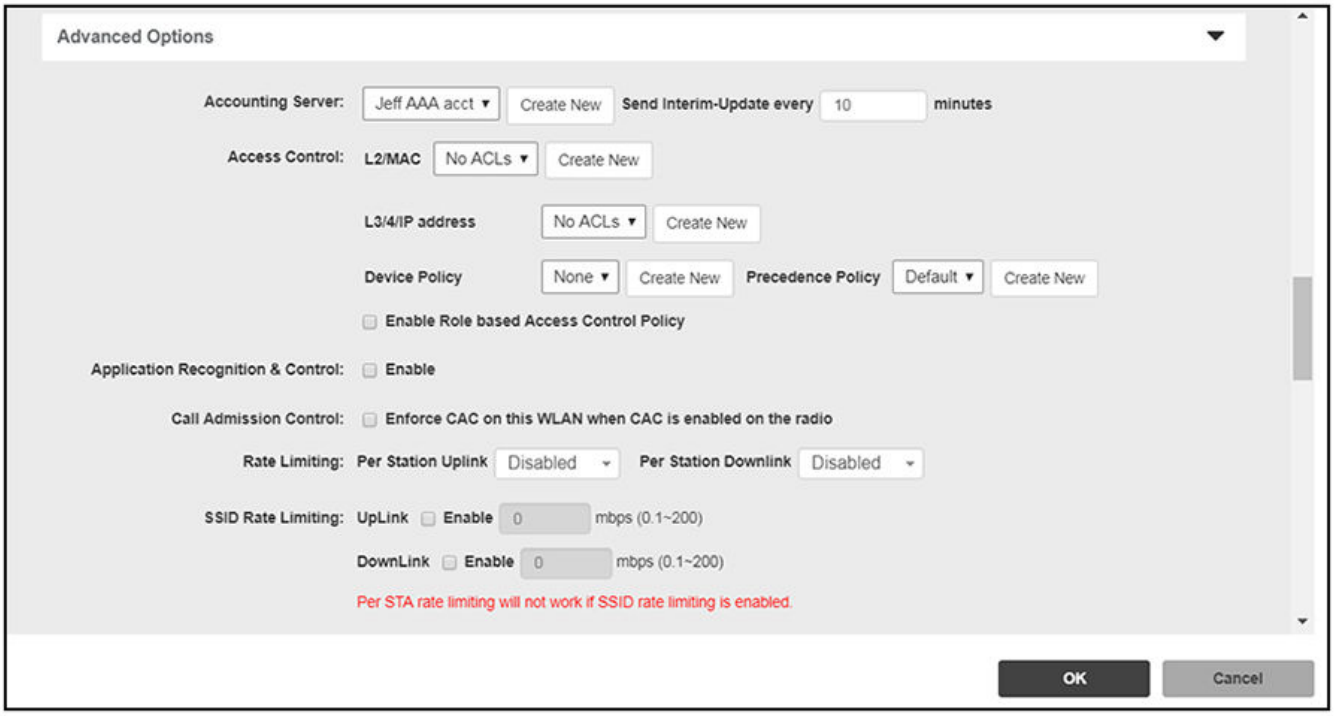


FIGURE 64 Configure Secure SSID on the SmartZone controller

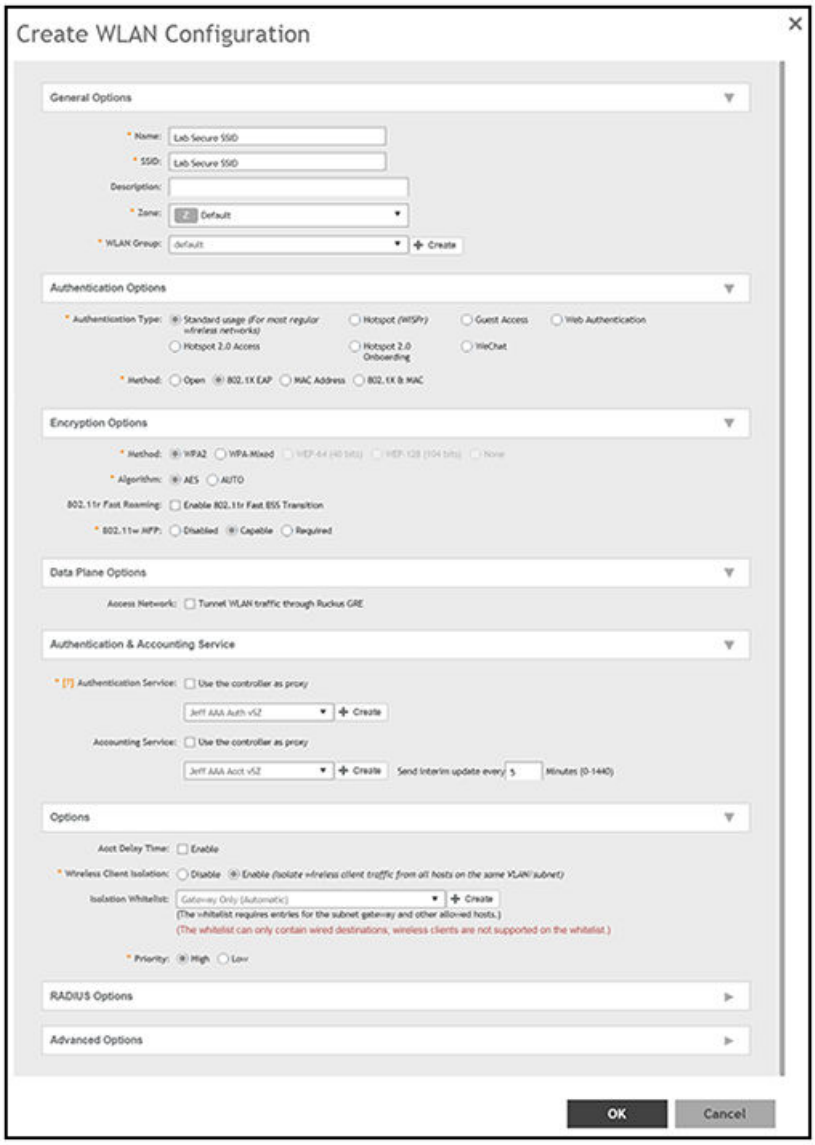
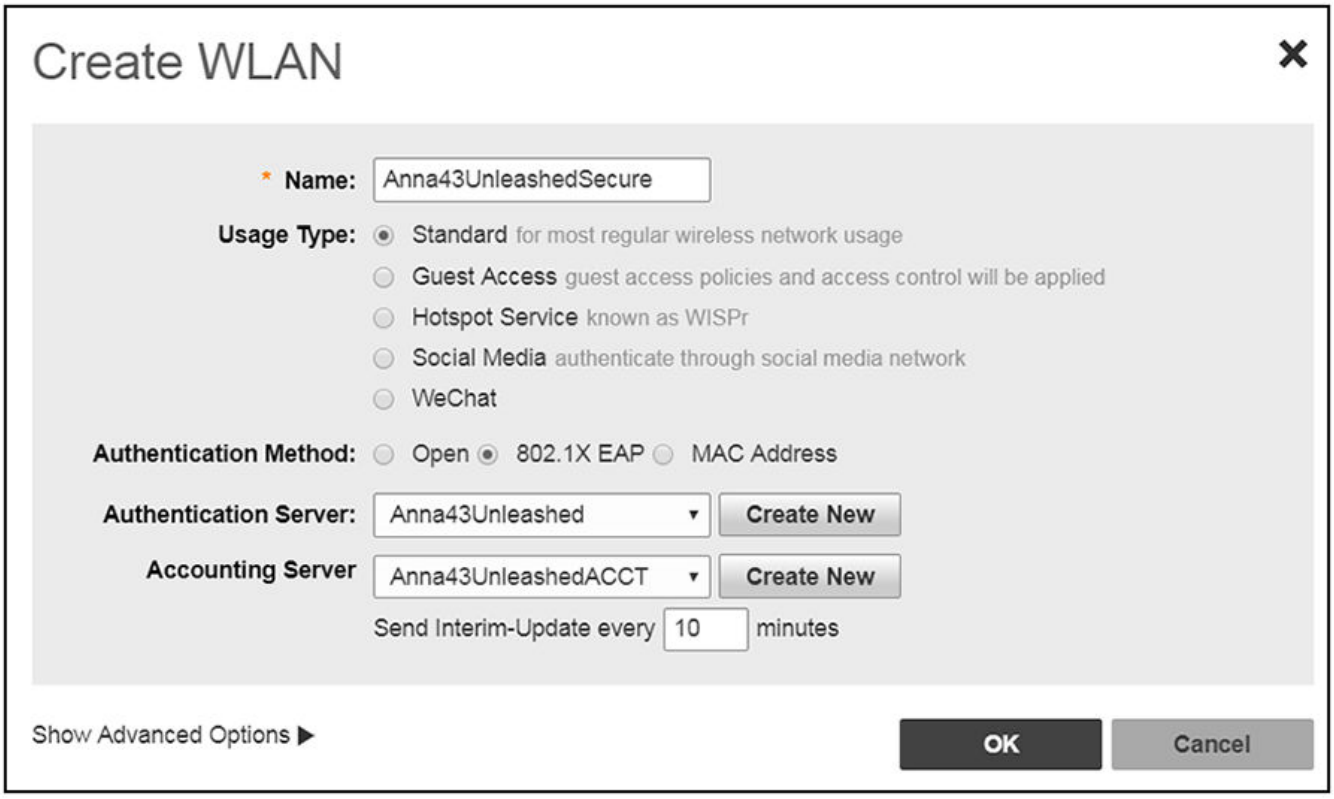


FIGURE 65 Configure Secure SSID on the Unleashed controller



The SSIDs are now configured on the wireless LAN controller. When the user connects to the onboarding (open) SSID they are redirected to the Cloudpath web page. When the user successfully completes the enrollment process, they are migrated to the secure SSID.

Troubleshooting Your Deployment

- Overview....105
- Connectivity Issues....105
- Issues with User Credentials....106
- DNS Issues....107
- OSCP Issues....107
- Certificate Issues....108
- NPS-Specific Troubleshooting....108
- Cloudpath Captive Portal Setup for Cisco Controller....109

Overview

For general Cloudpath operations information, refer to the *Cloudpath Operations Manual*, which can be found on the **Support** > **Documentation** tab.

This section describes solutions to common troubleshooting issues with the Cloudpath deployment.

Connectivity Issues

Cloudpath License Server

Cloudpath communicates with the Cloudpath License Server for network and licensing information. Cloudpath must be able to communicate to xpc.cloudpath.net (72.181.151.75) over TCP ports 80/443 for HTTP/HTTPS.

RADIUS Server

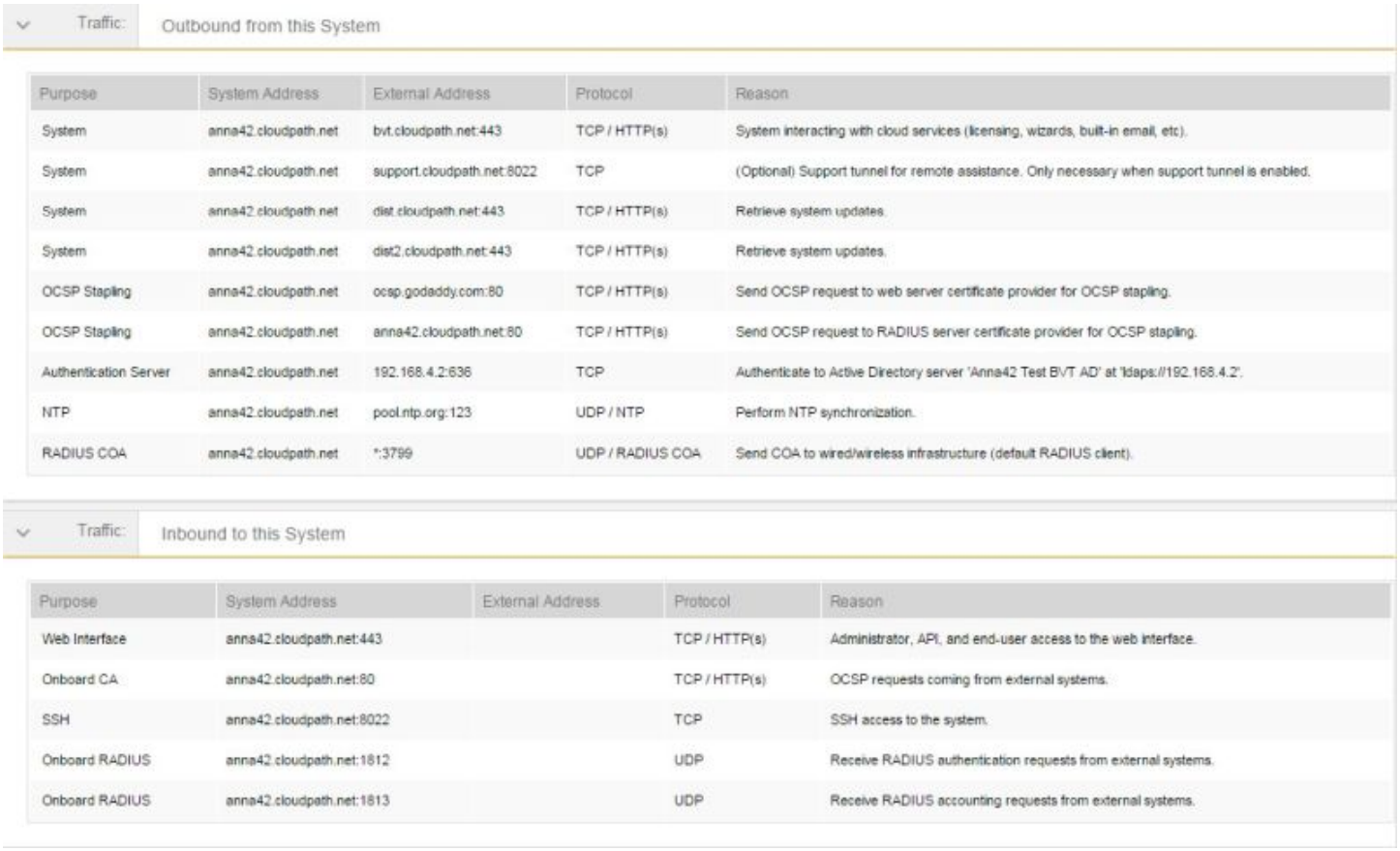
The wireless controller must be able to communicate with the Cloudpath onboard RADIUS server on port 14650.

Firewall Requirements

The Firewall Requirements table is designed to help you understanding the inbound and outbound traffic of the Cloudpath server. The table is dynamically generated based on your system configuration and can change as the system configuration is modified.

To view this information, go to **Administration** > **Firewall Requirements**.

FIGURE 66 Firewall Configuration



Traffic: Outbound from this System

Purpose	System Address	External Address	Protocol	Reason
System	anna42.cloudpath.net	bvt.cloudpath.net:443	TCP / HTTP(s)	System interacting with cloud services (licensing, wizards, built-in email, etc).
System	anna42.cloudpath.net	support.cloudpath.net:8022	TCP	(Optional) Support tunnel for remote assistance. Only necessary when support tunnel is enabled.
System	anna42.cloudpath.net	dist.cloudpath.net:443	TCP / HTTP(s)	Retrieve system updates.
System	anna42.cloudpath.net	dist2.cloudpath.net:443	TCP / HTTP(s)	Retrieve system updates.
OCSP Stapling	anna42.cloudpath.net	ocsp.godaddy.com:80	TCP / HTTP(s)	Send OCSP request to web server certificate provider for OCSP stapling.
OCSP Stapling	anna42.cloudpath.net	anna42.cloudpath.net:80	TCP / HTTP(s)	Send OCSP request to RADIUS server certificate provider for OCSP stapling.
Authentication Server	anna42.cloudpath.net	192.168.4.2:636	TCP	Authenticate to Active Directory server 'Anna42 Test BVT AD' at 'ldaps://192.168.4.2'.
NTP	anna42.cloudpath.net	pool.ntp.org:123	UDP / NTP	Perform NTP synchronization.
RADIUS COA	anna42.cloudpath.net	*:3799	UDP / RADIUS COA	Send COA to wired/wireless infrastructure (default RADIUS client).

Traffic: Inbound to this System

Purpose	System Address	External Address	Protocol	Reason
Web Interface	anna42.cloudpath.net:443		TCP / HTTP(s)	Administrator, API, and end-user access to the web interface.
Onboard CA	anna42.cloudpath.net:80		TCP / HTTP(s)	OCSP requests coming from external systems.
SSH	anna42.cloudpath.net:8022		TCP	SSH access to the system.
Onboard RADIUS	anna42.cloudpath.net:1812		UDP	Receive RADIUS authentication requests from external systems.
Onboard RADIUS	anna42.cloudpath.net:1813		UDP	Receive RADIUS accounting requests from external systems.

Issues with User Credentials

Active Directory

If users receive errors about bad credentials, check the following:

- Make sure that RADIUS requests are going outbound from the AD server.
- Ping the AD server using the FQDN to verify that DNS is working.
- Verify that the RADIUS IP address and shared secret specified on the WLC matches what is on Cloudpath.

Credentials Mismatch

If you receive an error that an authentication failed due to a user credentials mismatch, either the user name provided does not map to an existing user account, or the password was incorrect.

LDAP

Using LDAP's default port (TCP-389) with a Base DN of the parent Active Directory domain only shows objects from the parent domain. Changing the port to 3268, but keeping the same Base DN allows LDAP access to users from the child AD domain (Reference http://technet.microsoft.com/en-us/ library/cc978012.aspx).

Global Catalog queries are directed to port 3268, which indicates that Global Catalog semantics are required. By default, ordinary LDAP searches are received through port 389. If you bind to port 389, even if you bind to a Global Catalog server, your search includes a single domain directory partition. If you bind to port 3268, your search includes all directory partitions in the forest. If the server you attempt to bind to over port 3268 is not a Global Catalog server, the server refuses the bind.

DNS Issues

Verify that DNS is Working

Open a Command Prompt and enter the command: **nslookup**. The result should display the eth0 IP address of the Cloudpath virtual appliance.

Verify that DNS is Working

1. Open a Command Prompt.
2. Enter the command: **nslookup**
3. At the nslookup prompt (">"), enter the command: **set q=rr_type**
4. After the previous command completes, enter:

```
_ldap._tcp.dc._msdcs.Active_Directory_domain_name
```

Review the output of the SRV query to determine if the query succeeded or failed:

- If the query succeeds, review the registered Service Location (SRV) resource record (RR)s returned in the query to determine if all domain controllers for your Active Directory domain are included and registered using valid IP addresses.
- If the query fails, continue troubleshooting dynamic update or DNS server related issues to determine the exact cause of the problem.

OSCP Issues

OSCP Validation

The RADIUS or NPS server first attempts to validate a client certificate using the Online Certificate Status Protocol (OSCP). If the OSCP validation is successful, the validation verification is satisfied; otherwise, it attempts to perform a CRL validation of the user or computer certificate.

OCSP provides the ability to revoke certificates. However, if using OCSP affects the performance of your system, you might disable OCSP and use CRL only.

OSCP Server in the DNS

When the client fetches the OCSP response from the CA, it looks up the domain name of the CA's OCSP server in the DNS, as well as establishing a connection to the OCSP server.
If you receive a message that indicates the server cannot resolve the OSCP URL, check the hostname listed in the OSCP URL for the onboard Root CA you created in Cloudpath. You might need to add this hostname to the DNS of the domain.

Certificate Issues

Certificate Chain Not Trusted

If you receive an error that indicates the certificate chain is not trusted, verify that you have the public certificate and any intermediate certificates for the root CA.

Common Name in Template

The CN in the certificate template may need to include domain information. This can be specified as ${USERNAME}@domain within Cloudpath on the specific certificate template.

SAN Other Name in Certificate Template

If the RADIUS or NPS logs show an issue with credentials, check the **SAN Other Name Pattern** in the certificate template. The variable listed in the **SAN Other Name Pattern** field should match the variable used in the **Common Name Pattern** field.

Missing EKU in the RADIUS Server Certificate

RADIUS certificates must contain Microsoft Server EKU-1.3.6.1.5.5.7.3.1. When you create the server certificate template in Cloudpath, you must check the box for the Microsoft Server EKU.

NPS-Specific Troubleshooting

For configuration details, see the *Cloudpath Integration with Microsoft NPS Configuration Guide* on the **Cloudpath Admin UI Support** tab.

If you are receiving a message that the EAP message is not available on the server, check the following configuration issues.

Register the NPS With the Domain

If the NPS is not registered to the domain, you might receive an error message that the EAP method is not available on the server.

To see if the NPS is registered with the domain, right-click the NPS server. If the server is registered, the **Register with domain** option is not available.

If there is a problem with your working registration, try deleting and re-adding the registration using the NPS **Administrator** prompt and the commands in this example:

```
net stop ias
netsh ras delete registeredserver domain=x server=y net start ias
net stop ias
netsh ras add registeredserver domain=samplecorp.local server=SAMPLE-NPS-Server net start ias
```

RADIUS Server Certificate Missing Private Key

If the RADIUS server certificate is missing the private key, you might receive an error message that the EAP Method is not available on the server, you might be missing the private key for the RADIUS server certificate.

Be sure that the RADIUS server certificate in the Local Computer Personal Certificate Store shows the 'certificate with key' icon  next to it. This indicates that the certificate is signed with the private key. If it does not show the icon, you do not have the private key for the RADIUS certificate. Try downloading the RADIUS certificate and private key in P12 format.

Use the following command examples from the NPS **Administrator** prompt:

```
certutil -dspublish -f root.cer NTAuthCA
certutil -dspublish -f root.cer NTAuthCA certutil -enterprise -addstore NTAuth root.cer
```

Cloudpath Captive Portal Setup for Cisco Controller

The following example provides information about setting up a captive portal on a Cisco controller so that it automatically redirects the user to the Cloudpath webpage.

Define an ACL that allows access to the Cloudpath webpage

1. On the WLC, go to **Security** > **Access Control Lists**.
2. Add an ACL named **Unauthenticated**.
3. Add the following rules to the **Unauthenticated** ACL:
   - Sequence 1, Destination [Cloudpath IP Address], Protocol TCP, Destination Port HTTP, Action Permit
   - Sequence 2, Source [Cloudpath IP Address], Protocol TCP, Source Port HTTP, Action Permit
   - Sequence 3, Protocol UDP, Source Port DHCP Server, Action Permit
   - Sequence 4, Protocol UDP, Source Port DHCP Client, Action Permit
   - Sequence 5, Protocol UDP, Source Port DNS, Action Permit

     NOTE
     If using HTTPS, repeat sequence 1 and 2 for HTTPS.

Enable Portal Page on the Open SSID and Enforces the Preauthentication ACL

1. On the WLC, go to **WLANs** and **Edit** the open SSID.

2. Open the **Security** > **Layer 3** tabs.
3. Check the **Web Policy** box.
4. Select the **Authentication** option.
5. In the **Preauthentication ACL** field, select the open SSID.

Configure the Portal Page

1. On the WLC, go to the Security tab.
2. Open the **Web Auth** > **Web Login** Page.
3. Set **Web Authentication Type** to **Internal**.
4. Set **Cisco Logo** to **Hide**.
5. Add the following HTML to the **Message** field:

```
<SCRIPT language="JavaScript"> window.location="[Cloudpath URL]";
</SCRIPT>
If you are not automatically redirected,
<a href="[Cloudpath URL]">click here</a> to go to Cloudpath.
```

   NOTE
   The URL of the Cloudpath webpage must be populated into the HTML in the **Message** field.

6. Click **Apply** to save the changes.
7. Click **Preview** to preview the portal page. The browser should be redirected to the Cloudpath webpage.
8. Click **Save Configuration** at the top of the page.



© 2018 ARRIS Enterprises, LLC. All rights reserved.
350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com