Cloudpath

Cloudpath
Enrollment System

Cloudpath ES Deployment Guide

Software Release 4.3

June 2016

Summary: This document describes what the Cloudpath ES does, items to consider when integrating with the other systems in your local network, and the different configuration options for deploying the Cloudpath ES. This guide also provides instructions for getting the system up in running with a basic workflow configuration, as well as use cases to help you configure more customized enrollment workflow.
Document Type: Planning
Audience: Network Administrator

Cloudpath

Cloudpath ES Deployment Guide

Software Release 4.3

June 2016

Cloudpath ES Deployment Guide

This document contains the following sections:

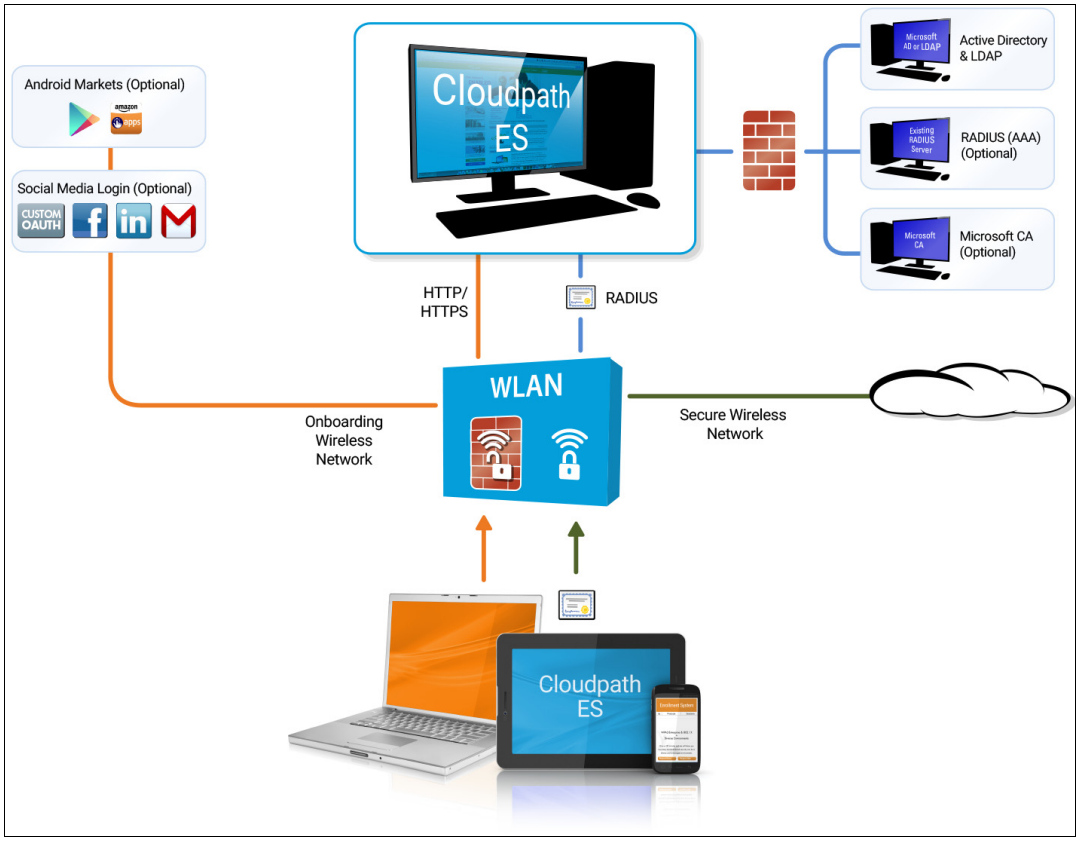
- Workflow Engine
- Enrollment Workflow Use Cases
- Planning the Local Network Configuration
- Prerequisites for Configuring the Cloudpath ES
- Deploying the ES Virtual Appliance to a VMware Server
- Enabling Multi-Tenant (optional)
- Activate Account or Log In
- Initial System Setup
- About the Enrollment Workflow
- Creating a Workflow From a Blank Slate
- Deploying the Enrollment Workflow
- Ruckus Controller Integration for Cloudpath
- Troubleshooting Your Deployment

Overview

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

The Cloudpath ES can differentiate the devices on your network by ownership, not just device type, offering the worlds first solution to extend secure Set-It-And-Forget-It-Wi-Fi™ to all users, devices, and networks without IT involvement.

FIGURE 1. Cloudpath ES Deployment Example



What is the Cloudpath ES

There are two main components that make up Cloudpath ES: *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 the Cloudpath ES

The Cloudpath ES 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. The Cloudpath ES 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 the Cloudpath ES, 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

The Cloudpath ES 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, the ES 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.

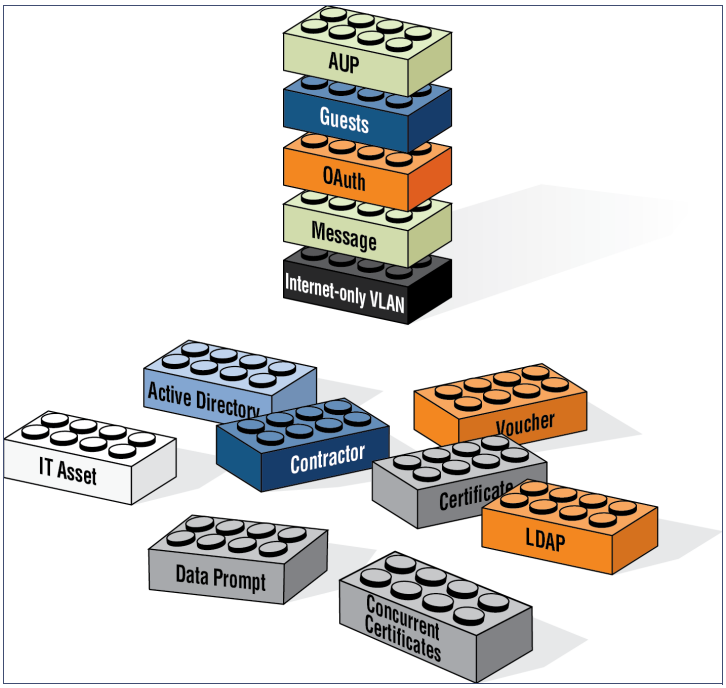
Workflow Engine

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

Workflow Building Blocks

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

The ES 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, the ES supports authentication using an Active Directory, LDAP (or LDAPS), or via a RADIUS server using PAP.

Ask the User About Concurrent Certificates

The *Cleanup* 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. The Cloudpath ES 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.

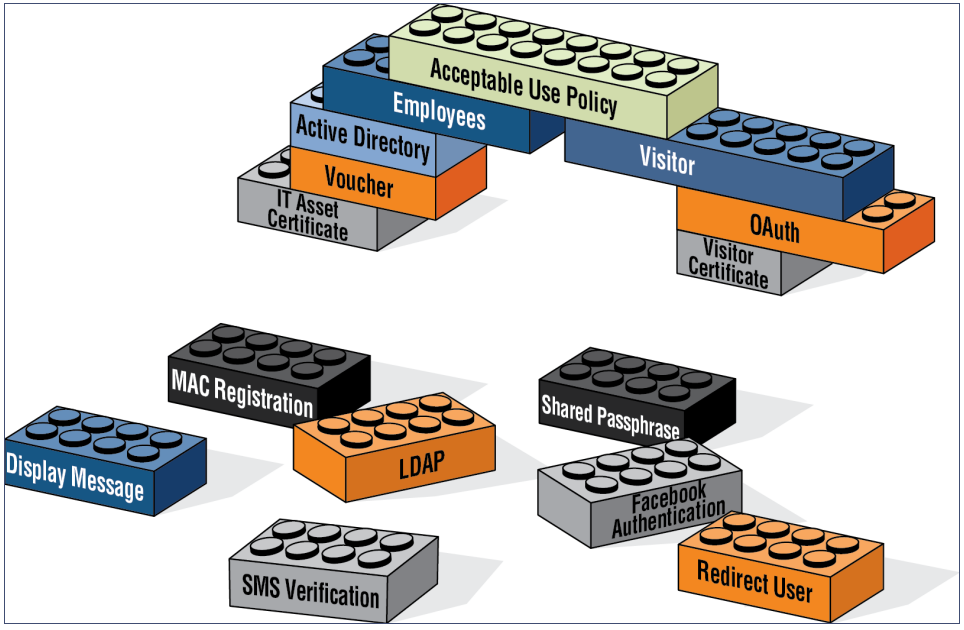
Send a Notification

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

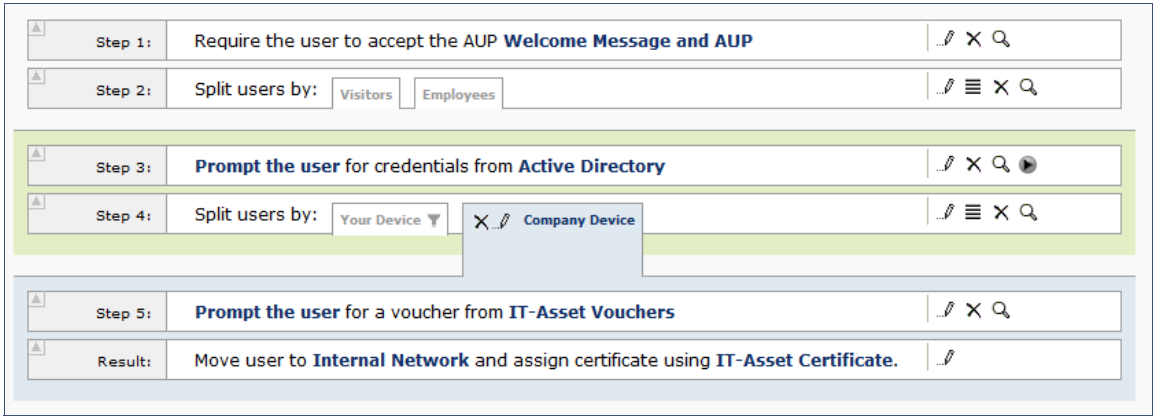
The following image represents a workflow that is split into two branches, with one sequence of steps for employees, and another for guest users. Each branch in the workflow specifies a different authentication method and assigns different certificates to the user.

FIGURE 3. Workflow With 2 Branches



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

FIGURE 4. Cloudpath ES Simple Workflow

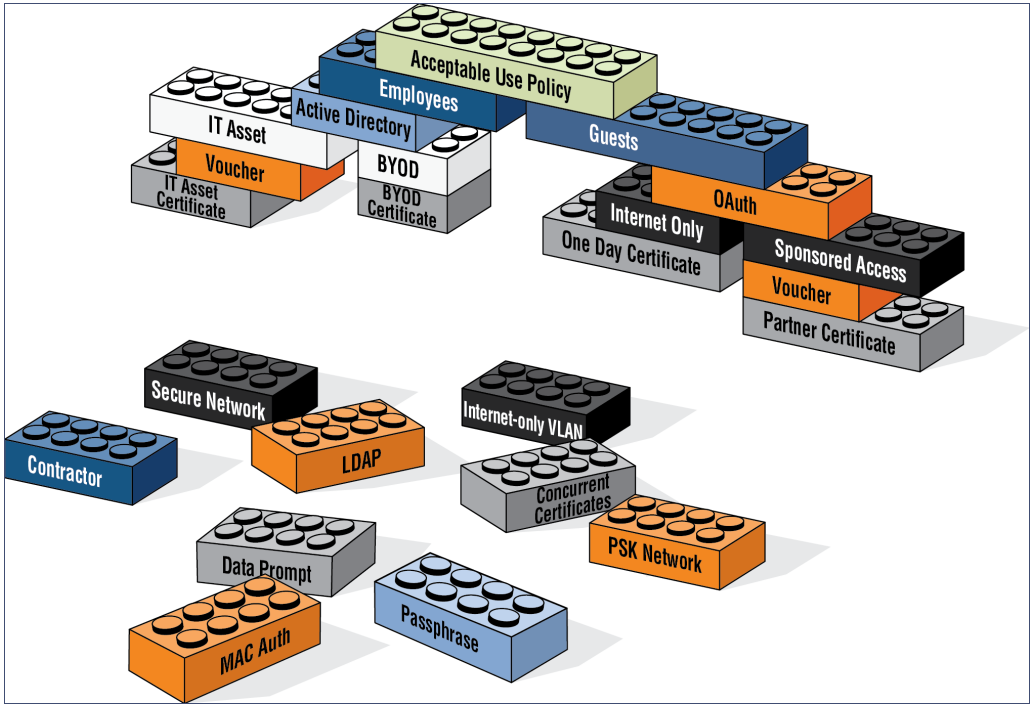


After the workflow is in place, you can fine-tune settings for specific OS versions, updates, and features, including customizations to the user experience. See Device Configuration and Client Certificate.

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



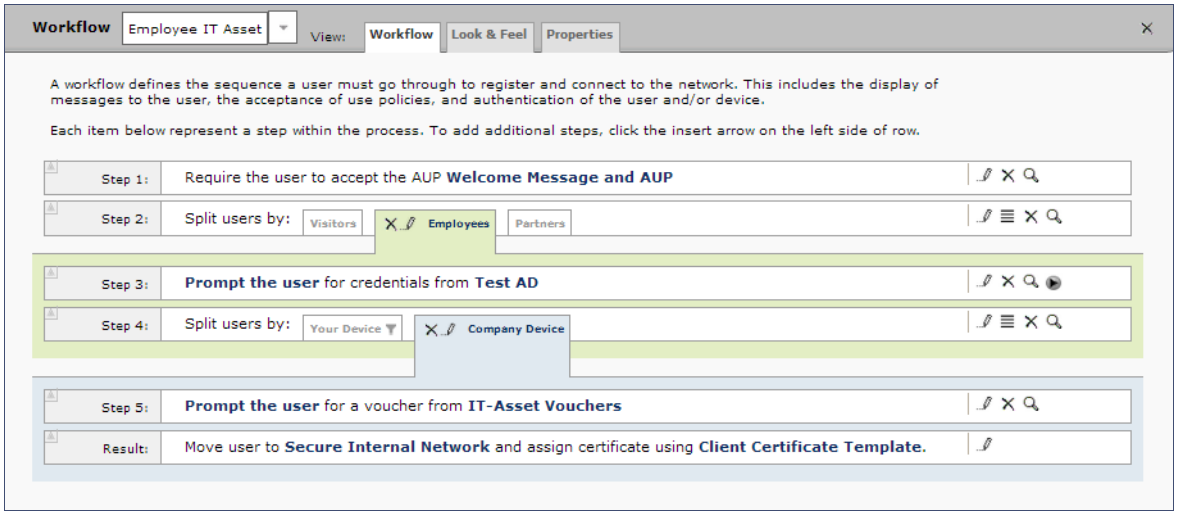
Enrollment Workflow Use Cases

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

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

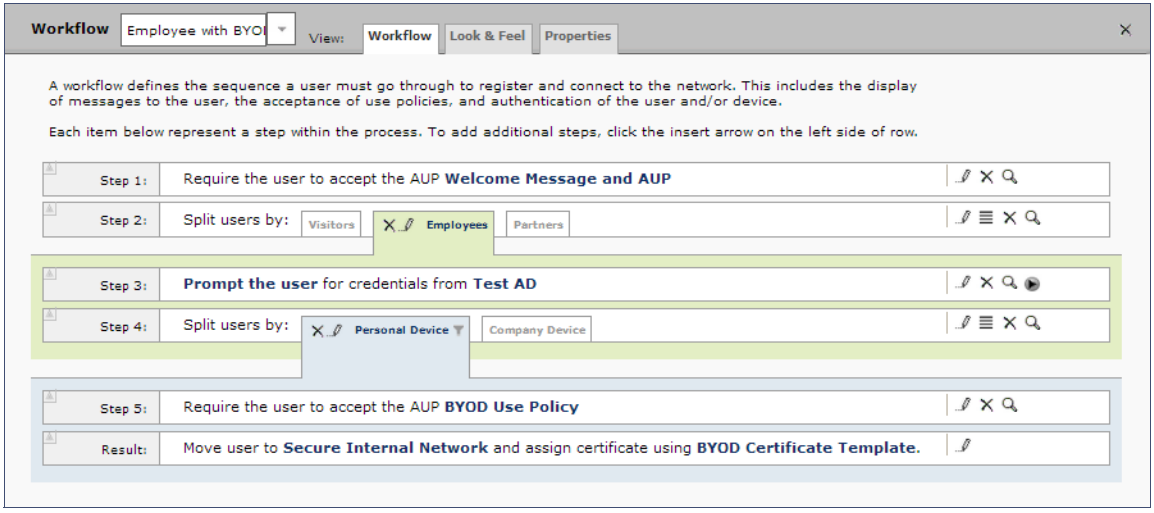


Your workflow does not have to be in the same order as the example. For example, you can move the authentication to LDAP step to immediately after the AUP step and then have the split for different workflow branches be immediately following. If you set up a filter on the LDAP group name, users can be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

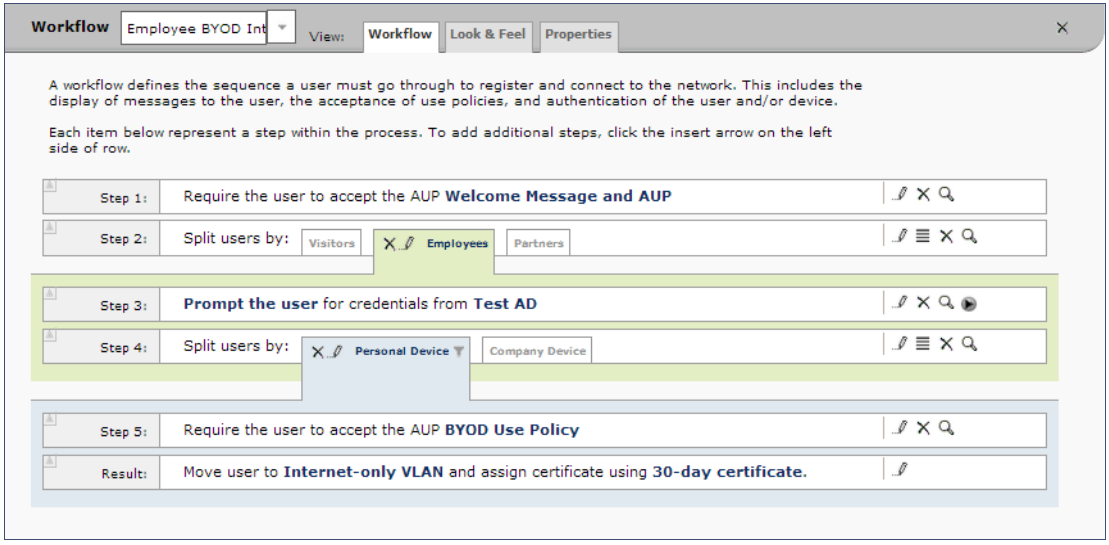
FIGURE 7. Example Workflow for Employees with Personal Devices (BYOD)



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

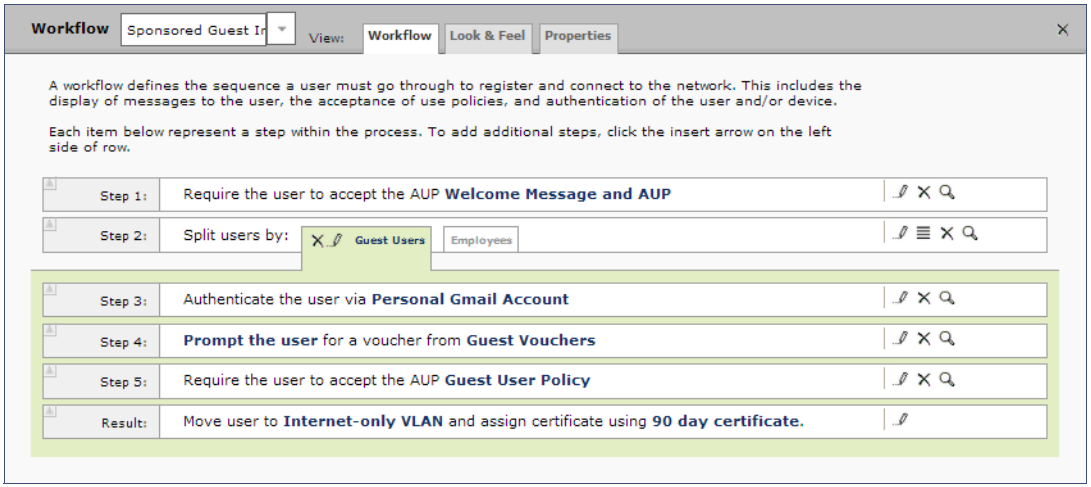


Sponsored Guest on Internet-Only VLAN

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 the Cloudpath ES* document on the ES *Support* tab.

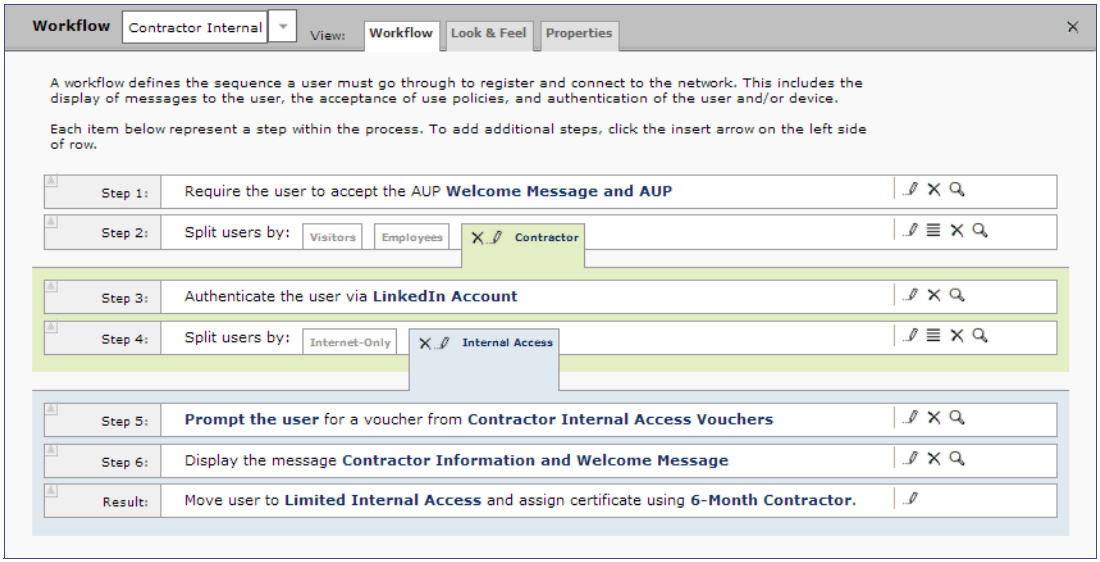
FIGURE 9. Example Workflow for Sponsored Guests on Internet-only VLAN



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

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 the Cloudpath ES. The Cloudpath ES 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 the Cloudpath ES 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

The Cloudpath ES 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 the Cloudpath ES 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

The Cloudpath ES 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 the ES, and the secure SSID is the network to which your users migrate. We recommend creating an SSID specifically for the Cloudpath ES.

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

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 ES 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

The Cloudpath ES 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 ES 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 ES. Configure the WLC to point to the ES as an *External* captive portal.
- Set up the secure WPA2-Enterprise SSID to delegate authentication to the onboard RADIUS server of the Cloudpath ES, the NPS, or an existing RADIUS server.

> **Note >>**
> If using an existing RADIUS server, you must configure layer 3 access to the Cloudpath ES virtual appliance to allow certificate status verification.

For more information, see Cloudpath ES 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. The Cloudpath ES supports many different CA configurations, including an onboard CA to act as your own private CA, certificates issued from an external CA, or the ES acting as a proxy for an existing CA.

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

Onboard CA

The ES 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. The Cloudpath ES 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 ES 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, the ES 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 the Cloudpath ES 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.

> **Tip >>**
> See the *Cloudpath ES 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 the ES to allow signed certificates to be uploaded to the ES and the public certificate of the CA (onboard or external).

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

RADIUS Proxy

The Cloudpath ES 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 the ES for authentication. When the external RADIUS server receives a RADIUS request from *user@guest*, the request is forwarded to the ES 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 ES. 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 ES.

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

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 the Cloudpath ES 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 ES onboard RADIUS server:

  -To disable access for a user, locate the certificates associated with the user account and revoke these certificates in the ES.

  -To disable access for a device, revoke only the certificate associated with the device.

Supported Authentication Servers

The Cloudpath ES 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 the Cloudpath ES, 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).

  -The Cloudpath ES 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 the hosted Cloudpath ES (onboard.cloudpath.net) DNS must resolve to onboard.cloudpath.net 72.18.151.86
- The ES communicates to the AD server using TCP Port 389, LDAPS TCP/UDP 636.

LDAP or LDAPS

To use LDAP with the Cloudpath ES, you need:

- DNS/IP of the active directory server
- DN of the domain
- Username and password to bind to the LDAP server
- The ES 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. The Cloudpath ES 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.

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

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 the Cloudpath ES 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 the Cloudpath ES 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 the Cloudpath ES and Wizard.

The Cloudpath ES must be able to communicate with:

- xpc.cloudpath.net (TCP 80/443-HTTP/HTTPS)
- dist2.cloudpath.net (used for ES 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 the Cloudpath ES

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 the ES 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	If you are using the Integration Module for Microsoft CA, the web server communicates with the Microsoft CA using Windows RPC.

After the Cloudpath ES is configured, a Firewall Requirements page is provided to help you understand the traffic to and from the ES. See the Troubleshooting Your Deployment section for more information.

Use Cases

Before configuring your network for use with Cloudpath ES, 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? For example, should employees with personal devices have

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

Prerequisites for Configuring the Cloudpath ES

This section describes the information you need before you can set up the Cloudpath ES in your Network.

What You Need

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

Deploying the OVA

- VMware server, on which you'll install the ES virtual appliance.
- The URL where the OVA file resides. A Cloudpath representative provides this information.
- Hostname of the virtual appliance
- Which server type will be implemented; single-tenant or multi-tenant?

> **Note >>**
> Multi-tenant is enabled before the initial system setup. Once enabled, the database structure cannot be reverted back to a single-tenant instance.

- IP address (and netmask) being assigned to the ES on 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 ES 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 ES Virtual Appliance to a VMware Server

The Cloudpath ES can be deployed to a cloud-hosted environment (multi-tenant), or as a virtual appliance on a locally-deployed VMware ESXi server (single tenant).

> **Note >>**
> For Multi-tenant deployments, see “Enabling Multi-Tenant (optional)” on page 31.

Specifications for Locally-Deployed VMware Servers

The Cloudpath ES virtual appliance is deployed as an open virtualization archive (OVA) file, which is a TAR file with the OVF directory inside. The OVA file can be deployed on any VMware ESXi server (ESX or ESXi architecture 4.x and 5.x).

For a production environment, we recommend that your VMware server have 12-16GB RAM, 2 vCPUs (with 4 vCores each), and 80-100GB disk space to run the Cloudpath ES.

Note >>
For test environments, the VMware server should have a minimum of 8GB RAM, 2 vCPUs (with 2 vCores each) and 40GB disk space to run the ES.

Retrieve OVA File

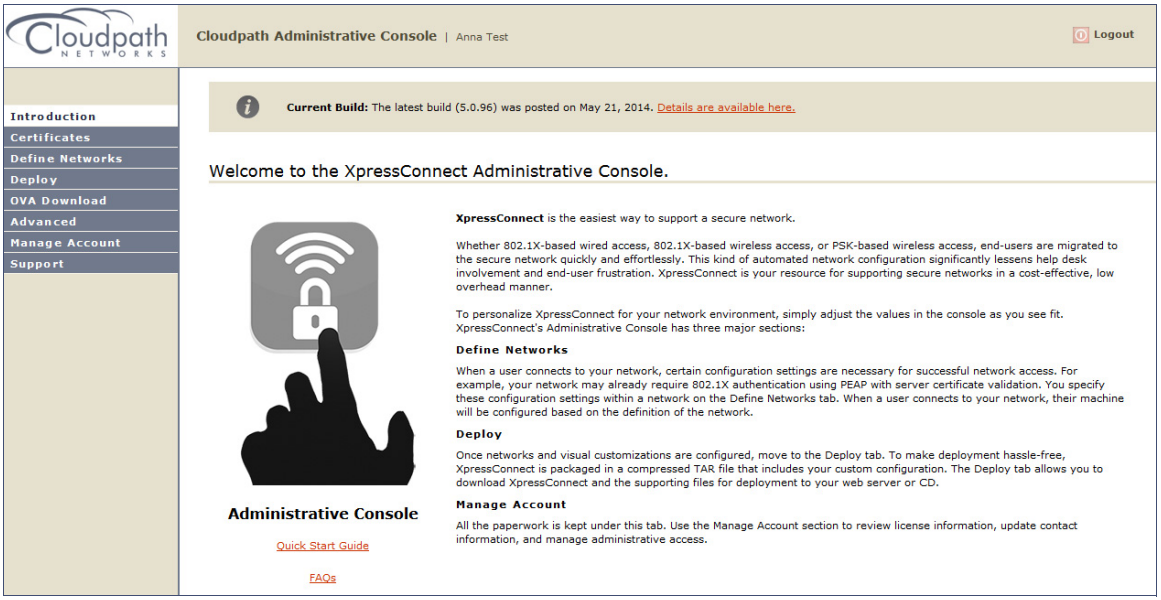
Retrieve the Cloudpath ES OVA file from the License Server *OVA Download* tab, from a direct download link, or from a Cloudpath representative.

To retrieve the OVA file using the Cloudpath License Server:

1. Log in to the Cloudpath license server using the link and credentials provided in the license activation email. The Cloudpath Welcome page is displayed.

The Cloudpath License Server is the management application where Accounts and Licenses are managed.

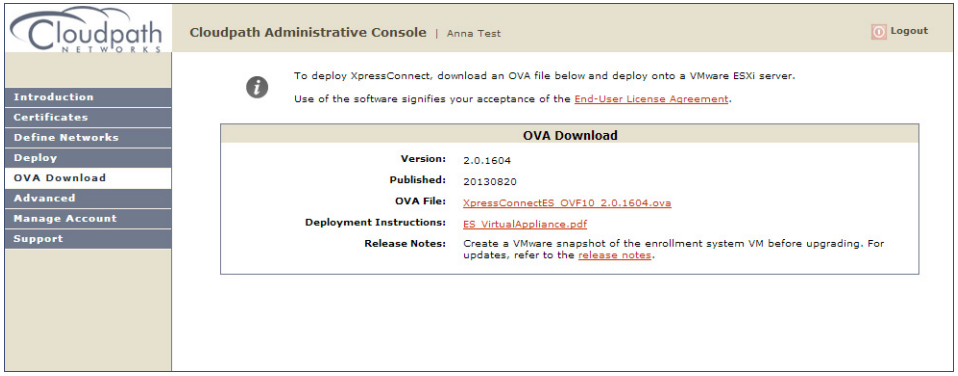
FIGURE 11. License Server Welcome Page



2. Go to the *OVA Download page*. This page provides a link to the OVA file, documentation providing instructions for setting up the Cloudpath ES virtual appliance, and the release notes for the most current GA release.

Note >>
We recommend that you download and read the release notes before you download the OVA file.

FIGURE 12. OVA Download Page



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

Deploy Virtual Appliance to a VMware Server

Set Up Virtual Appliance

1. Open the VMware client.
2. Select *File > Deploy OVF Template*.
3. Enter the file path or URL where the OVA file resides.
4. Enter a unique name for the virtual appliance. The default is *Cloudpath ES*.
5. If you are using VMware vCenter™ Server to manage your virtual environment, select the appropriate data center, cluster, host, and destination storage, as needed.
6. Select a disk format.
   - Use a thick provision for a production environment. For a thick provision, the total space required for the virtual disk is allocated during creation.

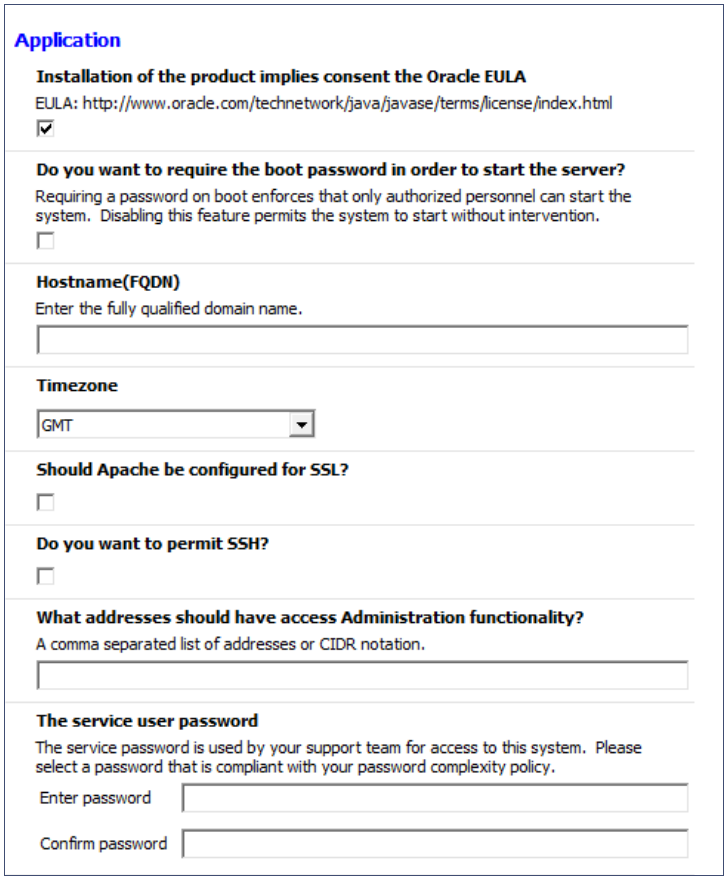
Note >>
If you are using Fault Tolerance, you must select *Thick* provisioning.

- Use a thin provision 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.

Application Properties

Customize the application properties for the deployment.

FIGURE 13. Application Properties



- Installation of the application implies that you accept the EULA. The link to the EULA is provided for reference.
- Do you want to require a boot password to start the server?

  -If checked, you must supply the boot password on the initial boot and all system reboots. This is the default.

-If unchecked, a boot password required only on the initial system boot.

> **Note >>**
> Contact a support representative to receive the boot password.

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

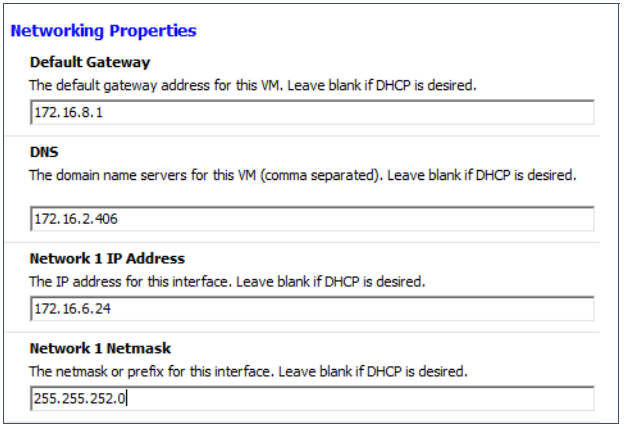
> **Note >>**
> The Cloudpath ES *Hostname* is used as the default *OCSP Hostname*, which is embedded into certificates issued by the onboard root CA as part of the URL for the Online Certificate Status Protocol (OCSP).

- Select the *Timezone*.
- Should Apache use SSL? Leave unchecked only if the Cloudpath ES is behind another web server using SSL.
- Do you want to permit SSH?
- Enter the IP addresses that can access the ES Admin UI. If you do not want to limit administrative access, leave this field blank.
- 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.

Networking Properties

Customize the network properties for deployment. To use static IP addresses, complete the *Networking Properties* fields. To use DHCP, you can skip this section and click *Next*.

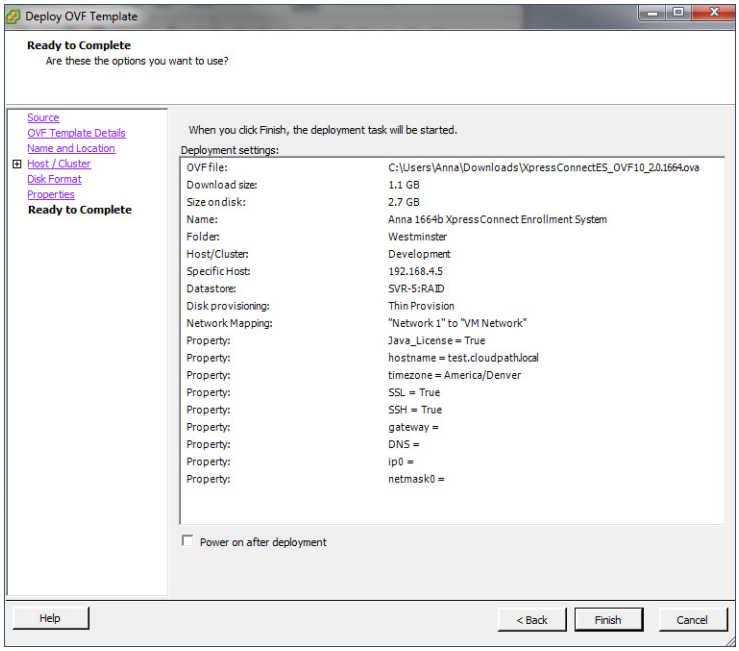
FIGURE 14. Networking Properties



Confirm Deployment Settings

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

FIGURE 15. Deployment Settings



Click *Finish*. Deployment takes approximately 2 minutes.

Service Account

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

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 ES 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:

- Ping the gateway of your system

- Ping the URL where the Cloudpath ES Licensing Server is hosted
- 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 ES 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
```

Tip >>
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.

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 ES virtual appliance.

How to Increase the Virtual Appliance Memory

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 the Cloudpath ES.

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

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

6. Verify the amount of free disk space available.

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

The output should indicate the increased partition size.

Enabling Multi-Tenant (optional)

A multi-tenant instance allows you to host multiple customer accounts on your Cloudpath ES system.

Note >>
Multi-tenant is enabled before the initial system setup. Once enabled, the database structure cannot be converted back to a single-tenant instance.

How to Enable a Multi-Tenant System

We recommend that you enable multi-tenant on a new system. If you attempt to enable multi-tenant on a Cloudpath ES system that has gone through the initial system setup process, the workflow configuration will be lost.

> **Note >>**
> Before enabling multi-tenant on your Cloudpath ES instance, we recommend that you create a VMware snapshot.

1. Log in to the Cloudpath command-line utility via SSH.
2. Enter the *console* command and access the Linux shell root account.

```
# console
[cpn_service@test220 ~]$ sudo su
[sudo] password for cpn_service: *********
```

3. From the root account, change to the scripts directory.

```
[root@test220scripts]# cd /opt/cloudpath/scripts/
```

4. Run the enableMuititenant script.

```
[root@test220scripts]# . ./enableMultitenant.sh
```

5. You are prompted to enter the IP addresses for restricted root account access.

```
Multitenant Setup

Full root capabilities is restricted to permitted IPs.
Multiple IPs can be specified in a semi-colon separated
list.

What IPs should be granted full root access?
[ex. 192.168.4/22;192.168.92.1]
```

6. Enter the restricted IP addresses in the format shown in the example.

```
192.168.4/22;192.168.92.1
```

7. A warning is displayed that this action cannot be undone. Confirm your request.

```
This will modify the system to be multi-tenant.
The existing account on the system will no longer
be functional.
```

```
** IMPORTANT:  This is not undoable.

Full root permissions will be restricted to: 192.168.4/22;192.168.92.1

Do you wish to continue with the conversion? [no] yes
```

8. The system indicates that the setup is complete.

```
Multitenant setup complete.  Please reboot the system.
```

9. Drop into the Cloudpath configuration console and reboot the system.

```
[root@test220 cpn_service]#config

#system reboot
```

After the system has rebooted, continue with account login and system setup. The bind account becomes the multi-tenant administrator account.

Activate Account or Log In

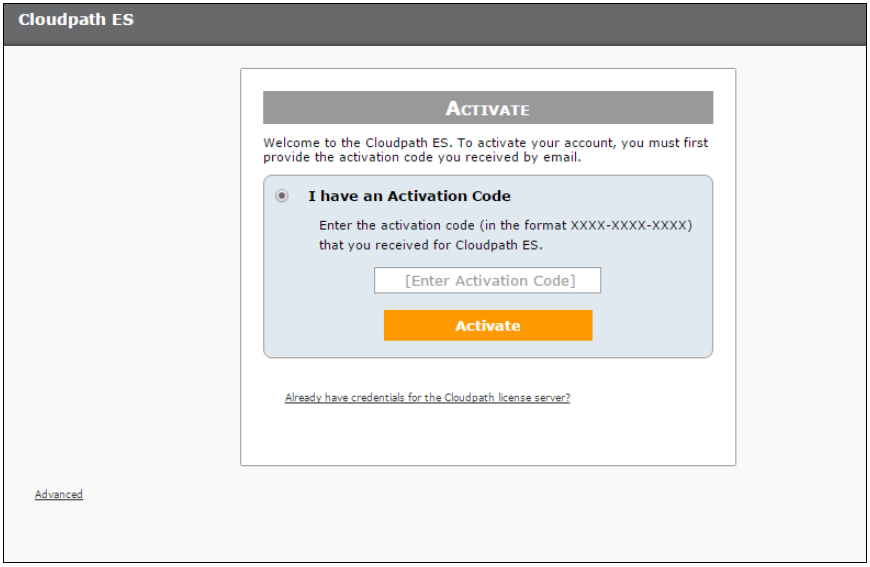
If you are setting up a Cloudpath account for the first time, you will be sent an activation code. If you have existing Cloudpath License server credentials, you can activate an account using those credentials.

When you create a new account with an activation code or existing Cloudpath credentials, the system binds this Cloudpath ES instance to your License Server credentials.

Activate Account

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

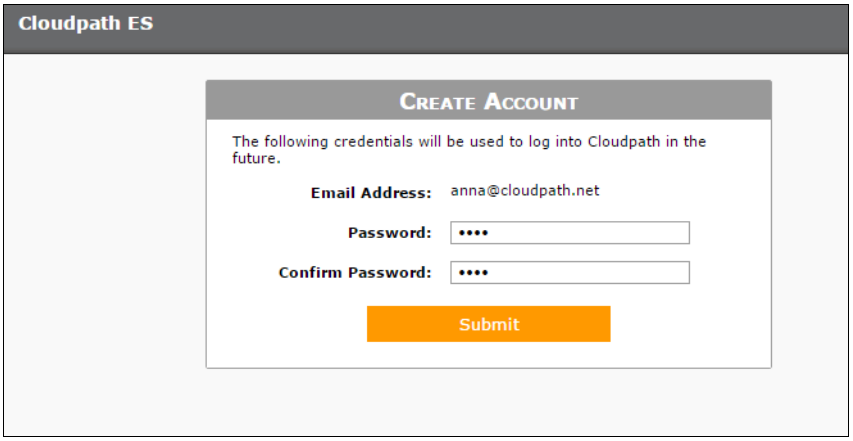
FIGURE 16. Activate Cloudpath ES Account



Set a Password for Account

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

FIGURE 17. Set Password



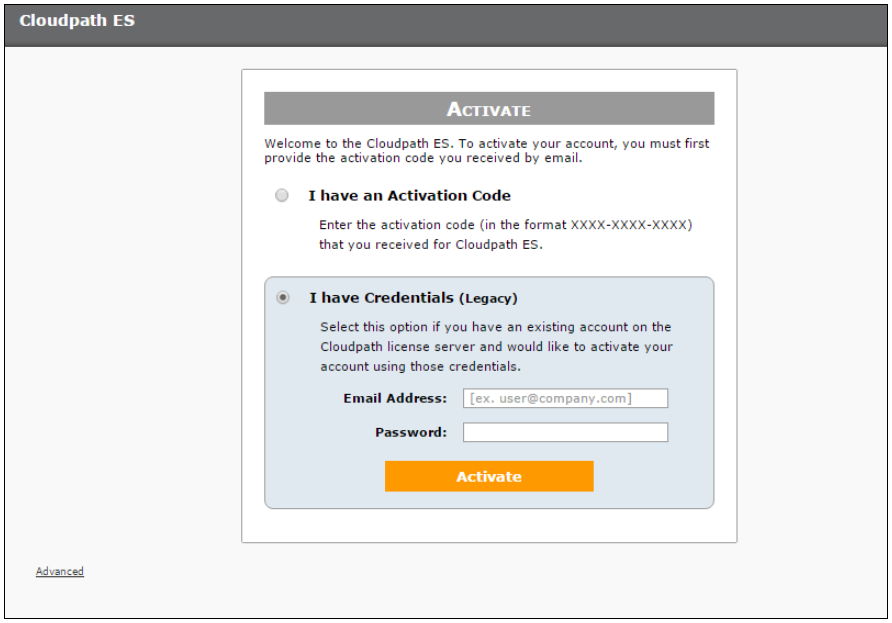
1. Your email address should display. If it does not, enter it on this page.
2. Enter and confirm a password.

These are the credentials to use for this Cloudpath ES account.

Login with Existing Credentials

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

FIGURE 18. Activate Account With Existing Credentials



Initial System Setup

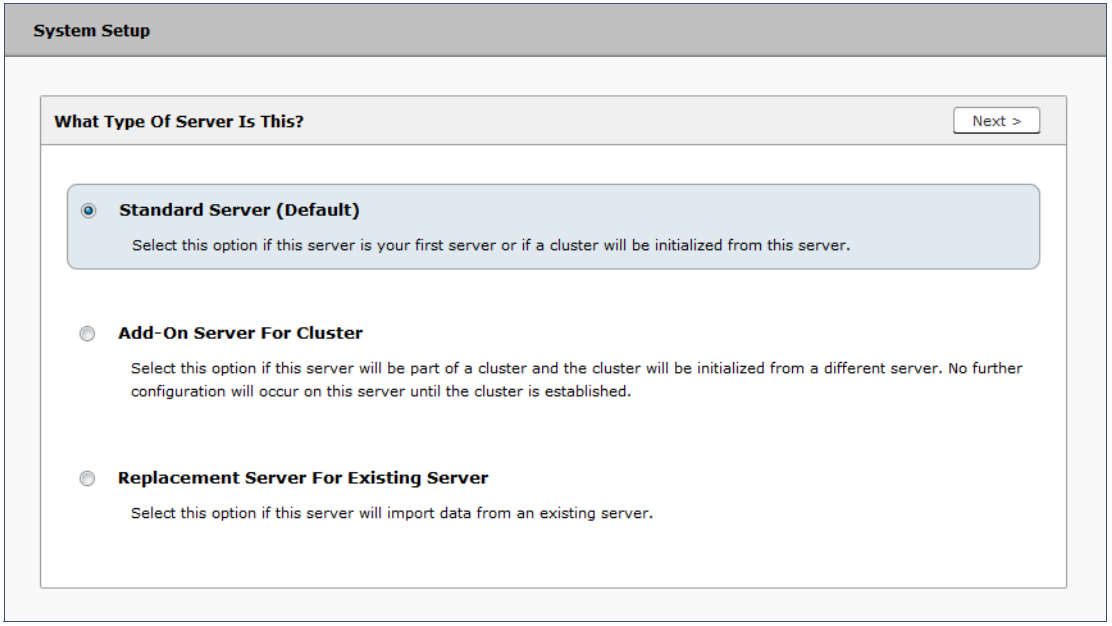
Cloudpath Networks provides you with a single administrator login for the Cloudpath ES. Additional administrators can be added from the left menu *Administration* tab, or you can enable Administrator logins from your authentication servers.

System Setup Wizard

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

1. Select Server Type.

FIGURE 19. 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 ES server.

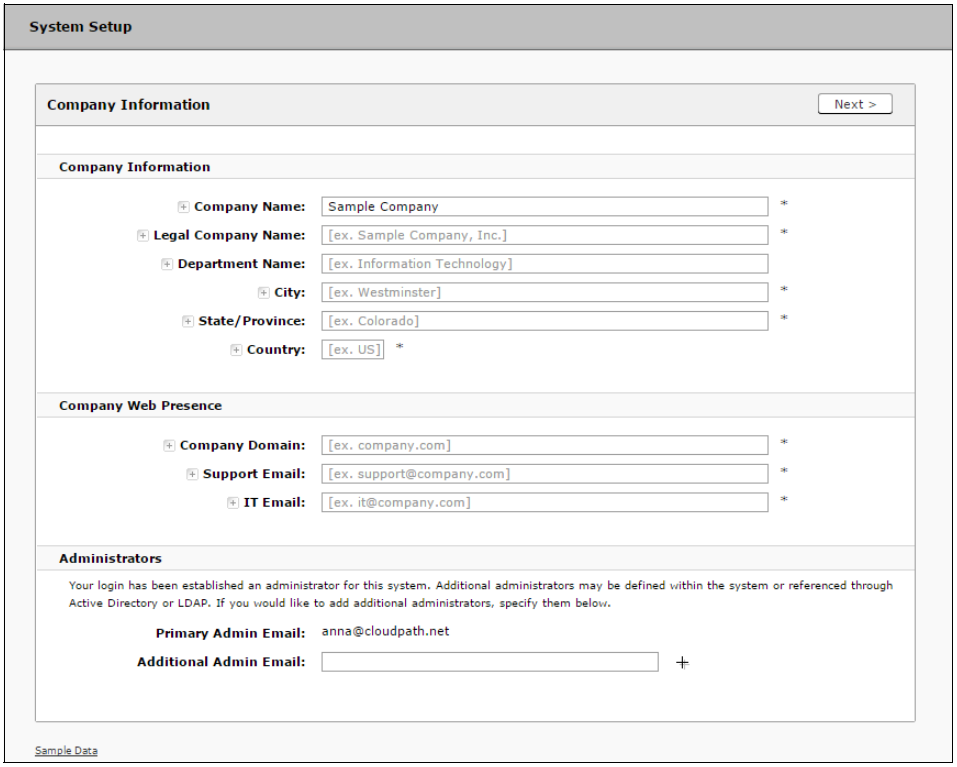
- If you are setting up this server to replace an existing server, and you are importing the database from the existing server, select *Replacement Server for Existing Server*.
- If you are setting up this server for replication, you can choose to set the server as an *Add-On* or *Replacement* server. 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.

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.

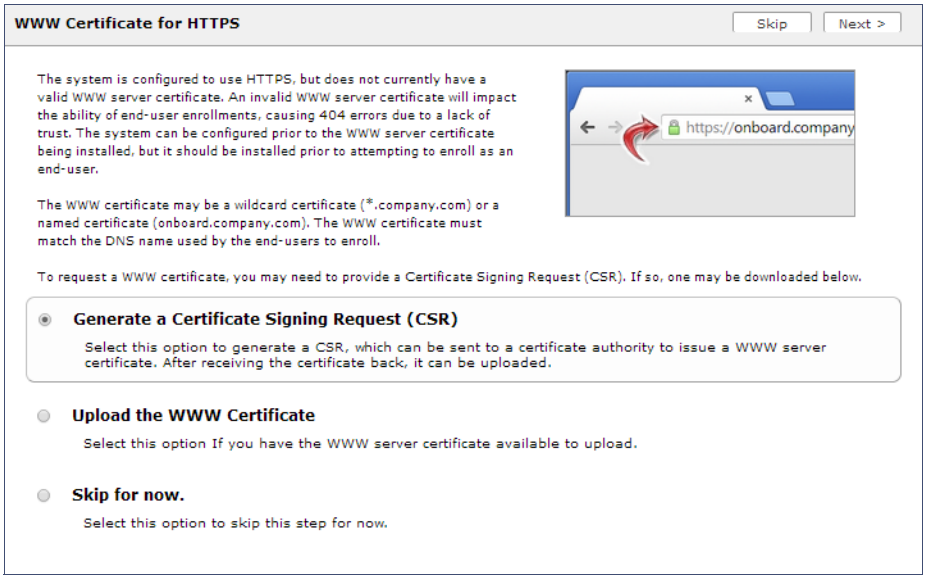
FIGURE 20. Company Information



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 21. WWW Certificate for HTTPS

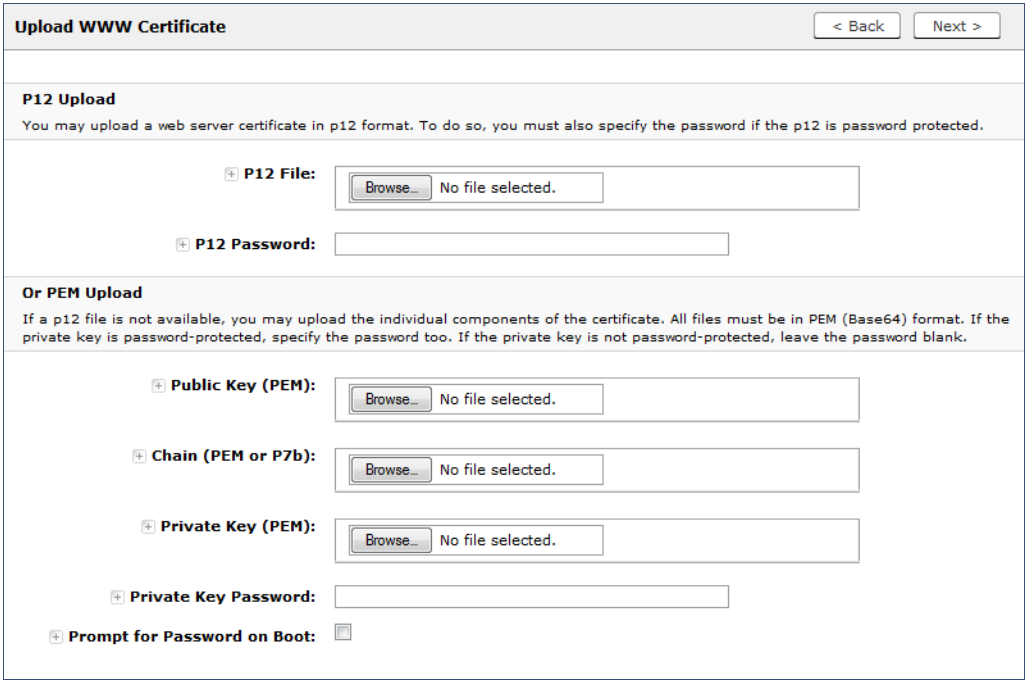


You can skip this step for the initial configuration. However, it should be installed prior to attempting to enroll as an end-user. You can configure the WWW server certificate from *Administration > System > System Services > Web Server Component*.

The Cloudpath ES 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 22. Upload WWW Certificate



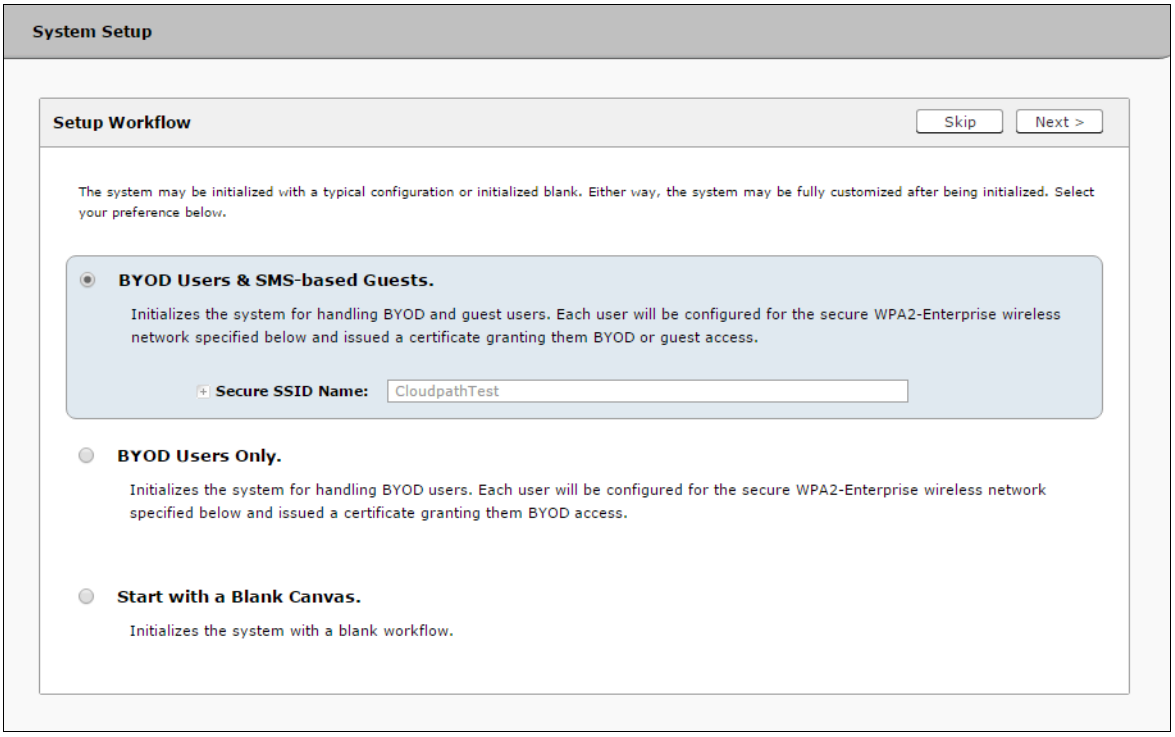
Browse to locate and upload the web server certificate and click *Next* to continue with the system setup.

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 23. Select Default Workflow



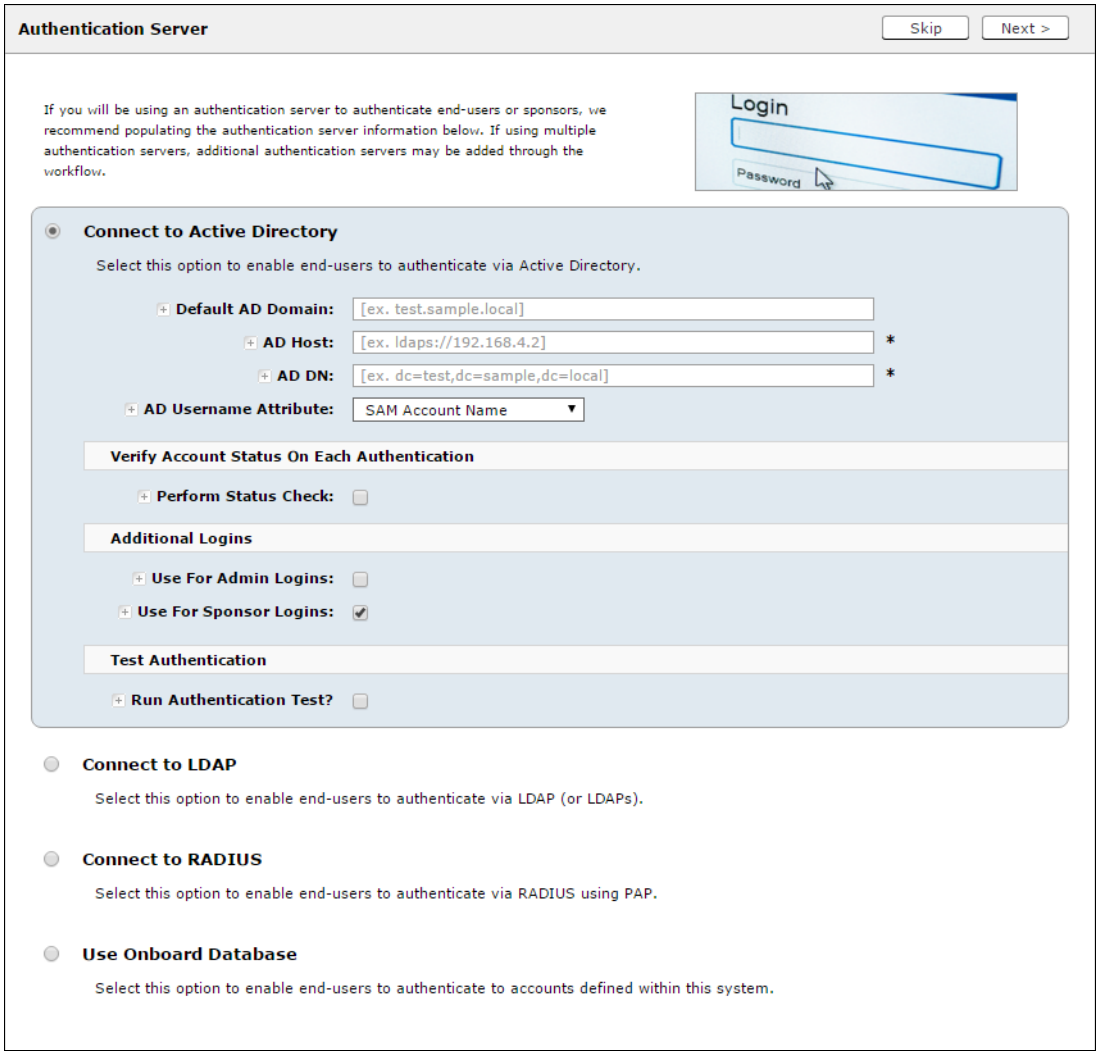
6. Configure the Authentication Server.

> **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 > Advanced > Authentication Servers* page.

FIGURE 24. Authentication Server Setup



To setup the initial configuration of the Authentication Server, select one of the following options:

- Connect to Active Directory - Authenticate end-users with AD credentials.
- Connect to LDAP - Authenticate end-users with LDAP or LDAPs credentials.
- Connect to RADIUS - Authenticate end-users with RADIUS via PAP.
- Use Onboard Database - Authenticate end-users with accounts that have been defined in the Cloudpath ES system.

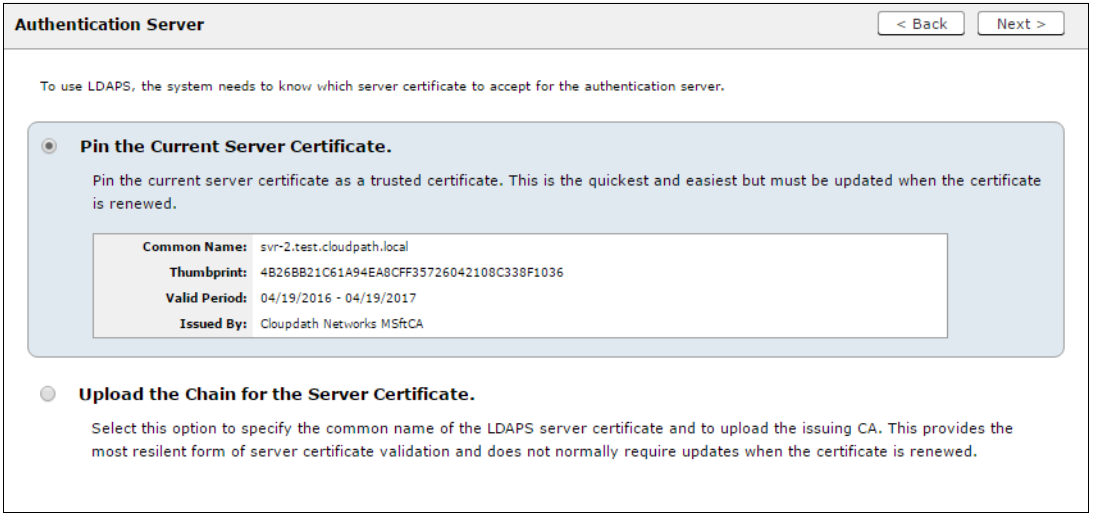
Consider these optional settings for the authentication server:

- 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 ES Admin UI using credentials associated with this authentication server. If *Use for Sponsor Logins* is selected, sponsors can log into the ES 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

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

FIGURE 25. Authentication Server Certificate



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.

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.

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.

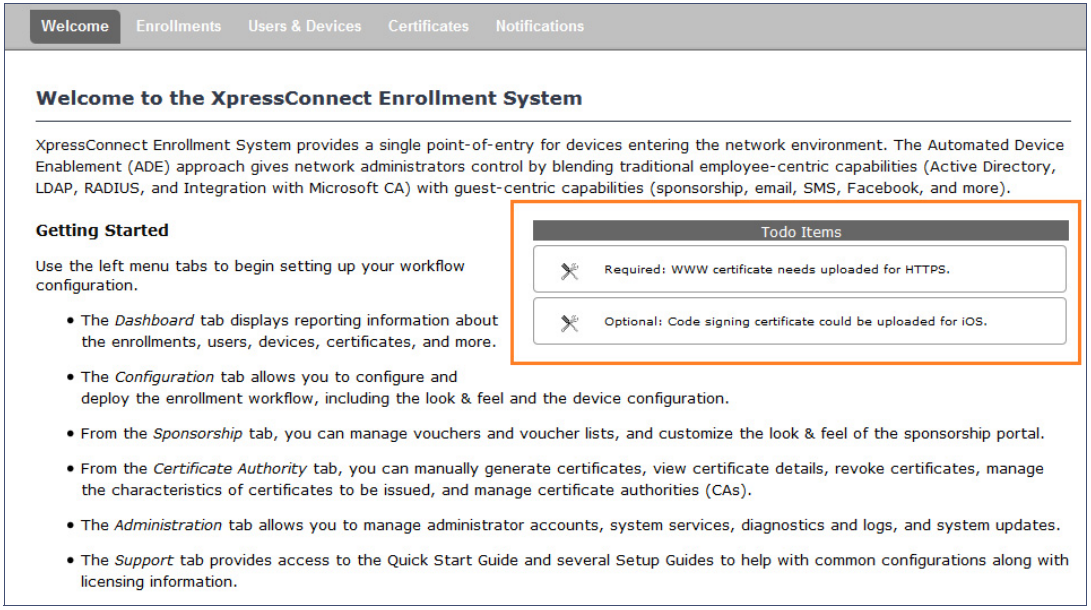
FIGURE 26. System Initialization Task

Initialization Status:	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:	CloudpathTest (WPA2-Enterprise, AES (CCMP), Broadcast)
RADIUS IP:	anna39.cloudpath.net
RADIUS Authentication Port:	1812
RADIUS Accounting Port:	1813
RADIUS Shared Secret:	hjw7mnbs3d6qvmzgfh8s
RADIUS Attributes:	BYOD Policy Template - VLAN: 'byod'
	Guest Policy Template - VLAN: 'guest'
User Experience:	
	End-users will use the enrollment portal to activate devices.
End-User Portal:	https://anna39.cloudpath.net/enroll/AnnaTest/Production/
BYOD:	For BYOD, the authentication is initially configured for a demo Active Directory server. Demo users include 'bob' (password bob1) and 'bill' (password bill1).
	The authentication configuration may be changed to point at your AD/LDAP server.
	BYOD users will be moved onto the secure SSID with VLAN 'byod' assigned.
Guests:	Guests will be required to provide a voucher from a sponsor. See the sponsor section below for currently available vouchers and instructions on creating additional vouchers.
	Sponsorship is one of several mechanisms for handling guests.
	Guest users will be moved onto the secure SSID with VLAN 'guest' assigned.
Sponsor Experience:	
	The default workflow utilizes sponsorship to authorize guests.
	To create vouchers for guests, sponsors can login to the sponsor portal below.
Sponsor Portal:	https://anna39.cloudpath.net/portal/sponsor/AnnaTest/
	The system is initially configured to allow any AD user to sponsor, so 'bob' and 'bill' will work here too.
Available Vouchers:	The following vouchers are currently available for use.
	Guest Vouchers - zjjh, bwqd, nvgv, nsic, kblw
Administrator Experience:	
Administrator UI:	https://anna39.cloudpath.net/admin/
Credentials:	The following email addresses have been sent a one-time password along with this information:
	If you ever forget your password, you can reset it from the login screen.
Key Pages:	View Enrollments - View information about enrolled devices, users, and policies.
	Configure Workflow - Modify the workflow that an end-user passes through to get on the network. This page also contains links for modifying the configuration of the authentication server, wireless netw
	Add/Manage Administrators - This page allows additional administrator logins to be setup.
	Deploy Snapshots - After making changes to the workflow, go to Configuration -> Deploy and click **Create New Snapshot** to publish the changes to the enrollment portal. After the new snapshot is do
	force it to pull in the new snapshot.
	Look & Feel - To modify the look & feel, go to Configure Workflow link above and select the **Look & Feel** tab along the top.

ToDo Items

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

FIGURE 27. ES Welcome Page



About the Enrollment Workflow

The Cloudpath ES 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.

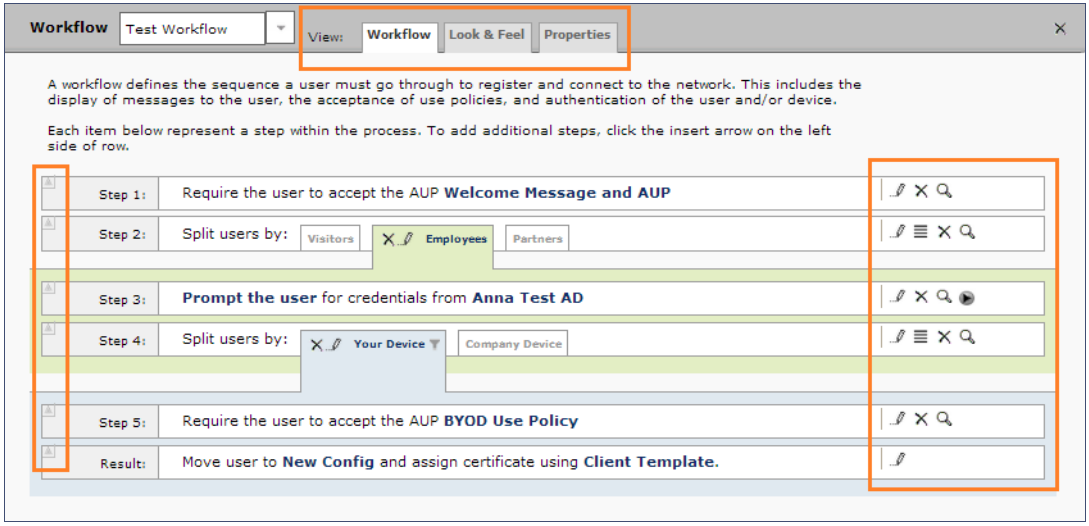
Workflow Basics

The *Workflow* page has three view tabs.

- Use the *Workflow* tab to configure the steps presented to a user during the enrollment process.
- Use the *Look & Feel* tab to configure the Cloudpath ES skin, and to customize the logos, colors, buttons, and images for the ES, the Wizard, the Download page.

- Use the *Properties* tab to enable/disable a configuration, or to modify the configuration Name and Description.

FIGURE 28. Enrollment Workflow 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.

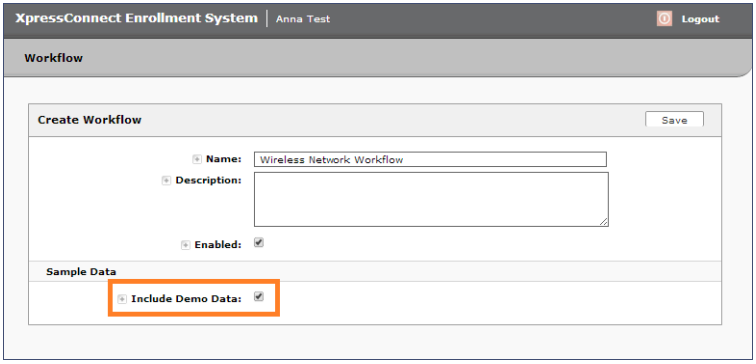
Modifying a Workflow Template

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

To create a workflow from a template using sample data:

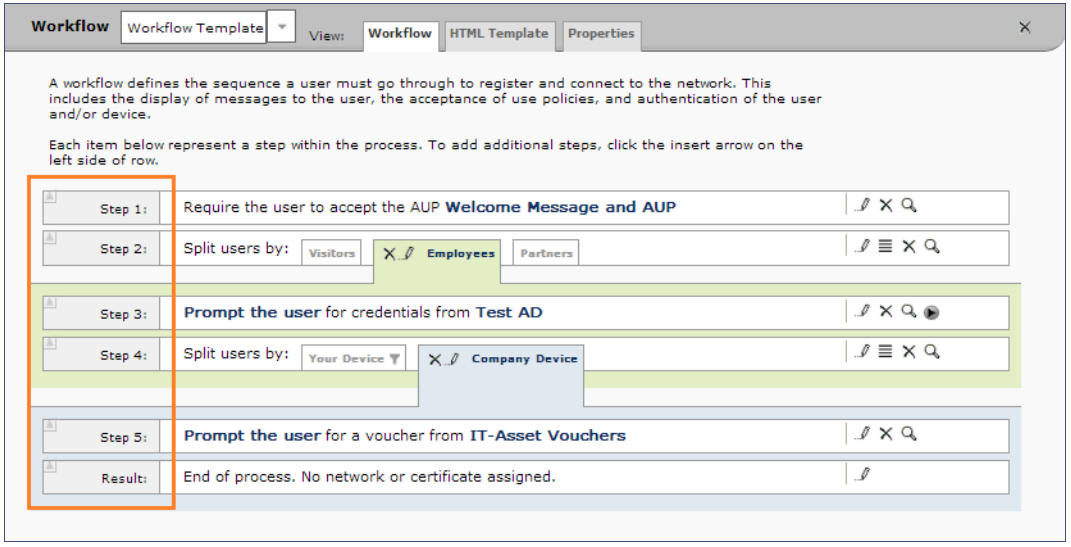
1. Go to *Configuration* > *Workflow*.
2. From the *Workflow* drop-down menu, select *Add New Workflow*.
3. On the *Create Workflow* page, enter a *Name* and *Description.* Select the check box for *Include Demo Data* and *Save*.

FIGURE 29. Create Workflow Using Demo Data



A workflow template, which contains a typical workflow sequence, is displayed. The step numbers are shown on the left side of the workflow.

FIGURE 30. Workflow Template



The workflow template contains basic workflow steps with sample data that can be modified to fit your network plan, such as:

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.

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.

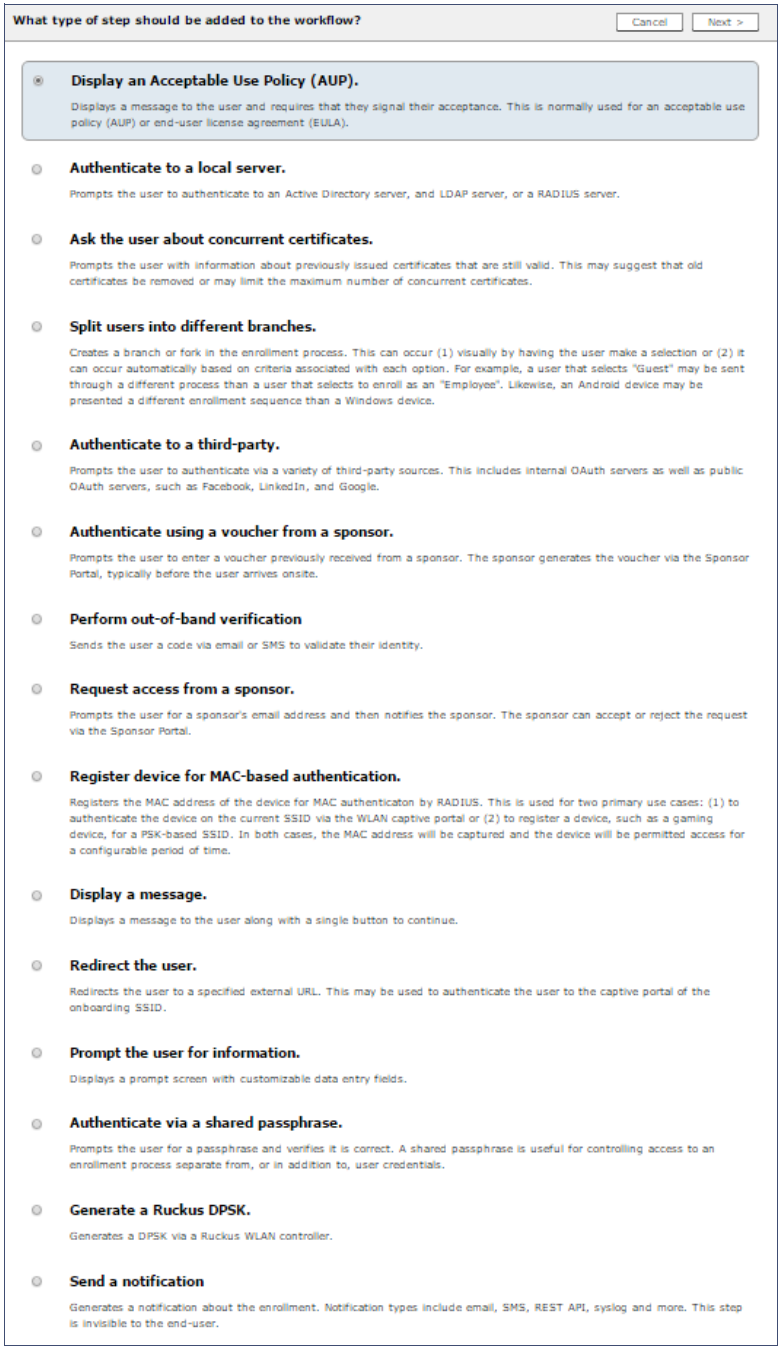
Creating a Workflow From a Blank Slate

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 > Workflow*.
2. From the *Workflow* drop-down menu, 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. Each time you add a step, this *Step Selection* page appears.

FIGURE 31. Enrollment Step Selection

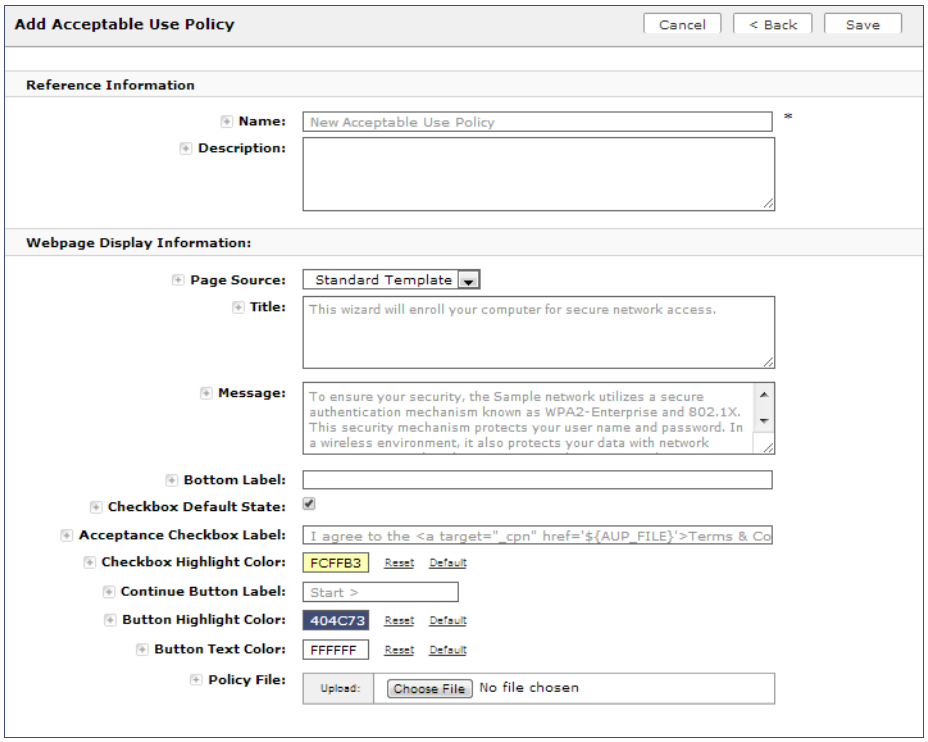


Acceptable Use Policy

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 32. 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

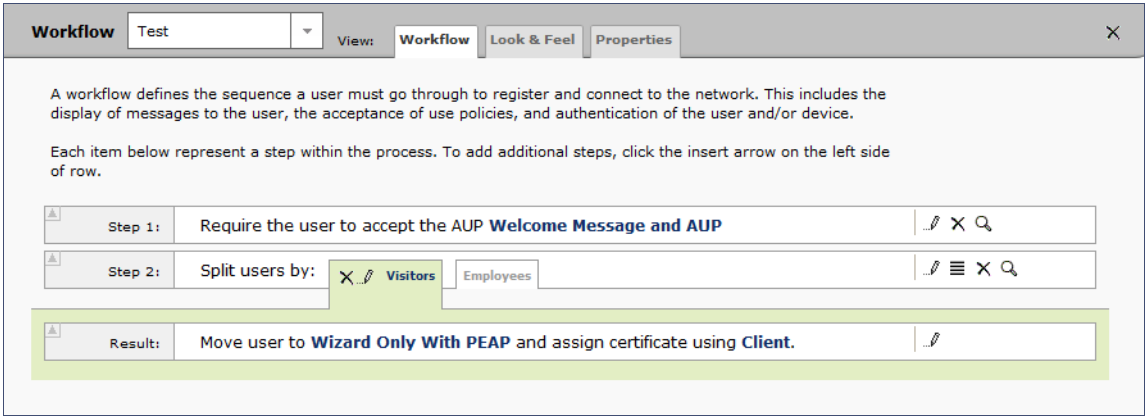
Step 2 in the workflow prompts for the type of user access.

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 33. Workflow with User Type Split

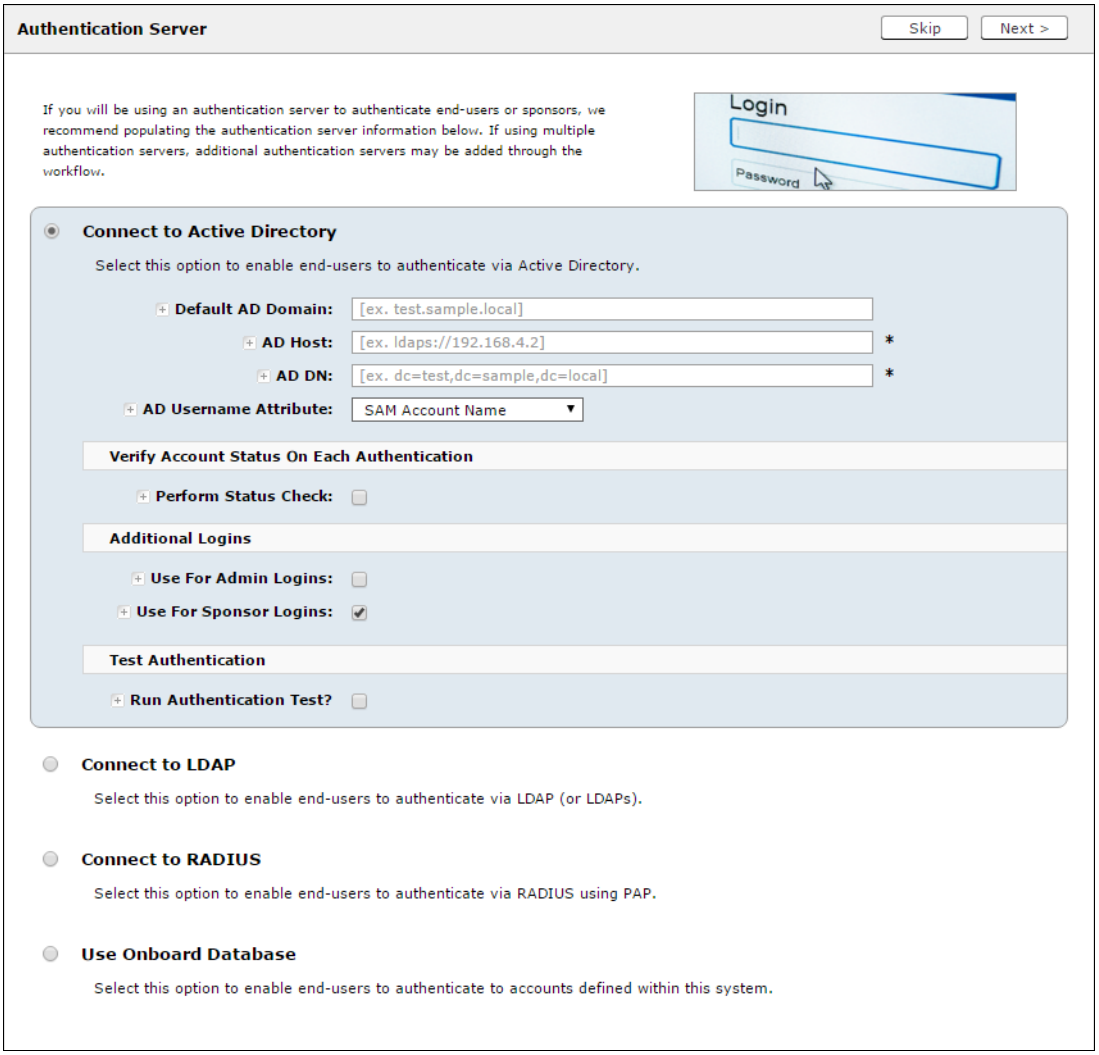


Authentication to a Local Server

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

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 34. Add Authentication Server



5. Enter the *Reference* and *Active Directory Information* and click Next.
6. Select *Use a new webpage created from a standard template.* The *Create Credential Prompt* page opens.

To test connectivity to the authentication server, select the *Run Authentication Test* box, and enter a Test *Username* and *Password* before you click *Next*.

To allow users from a specific group to log in to the ES Admin UI as administrators, check the *Use for Login Admin* box and enter the *Admin Group Regex* for the authentication server group.

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

Device Type Split

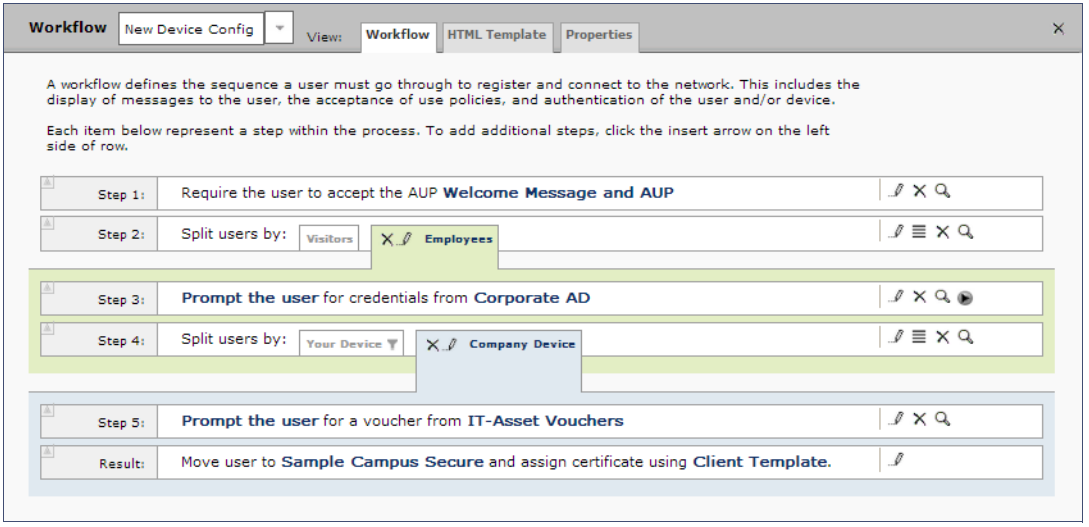
Step 4 adds an enrollment step prompts the user to select a personal device or a company-owned (IT-asset) device.

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.

> **Tip >>**
>
> 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 35. Workflow with Device Ownership Split



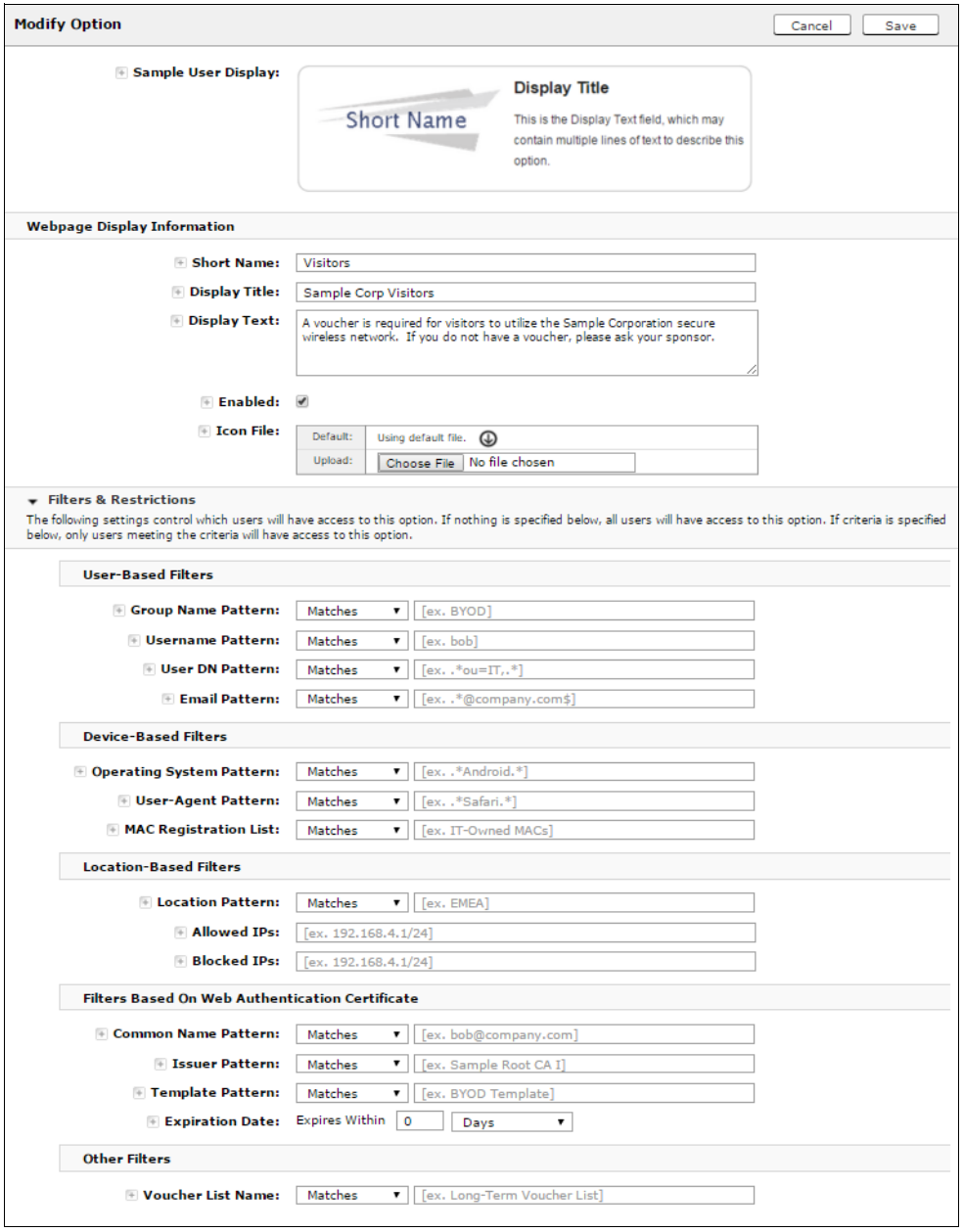
Create a Filter in the Device Type Split

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 Options* page, which allows you set up filters for this split in the workflow.

FIGURE 36. Modify Selection Option



3. In the *Filters & Restrictions* section, in *User-based Filters*, enter a regex to matches the *BOYD APP* in the *Group Name Pattern* field. The ES 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.

> **Tip >>**
> 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.

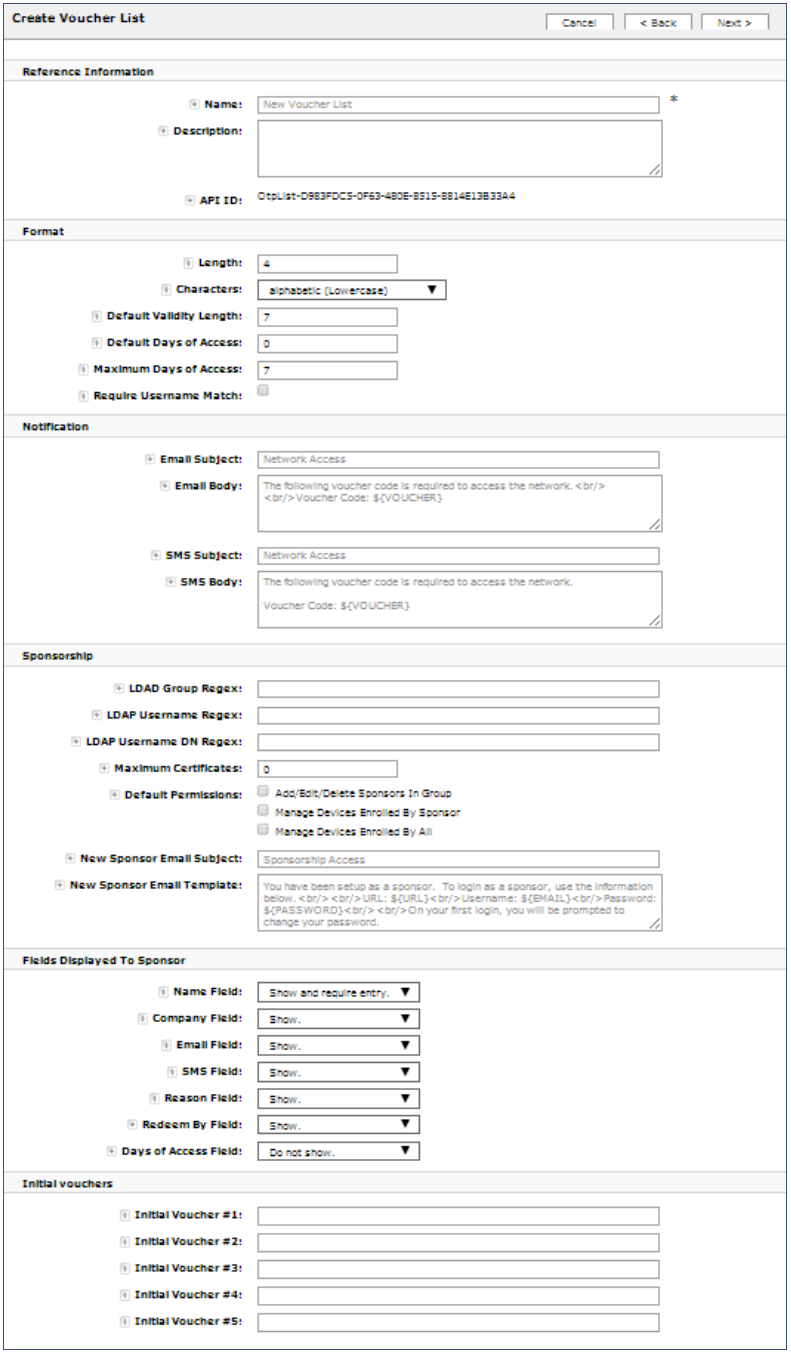
Prompt for Voucher

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 37. Create Voucher List



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.
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

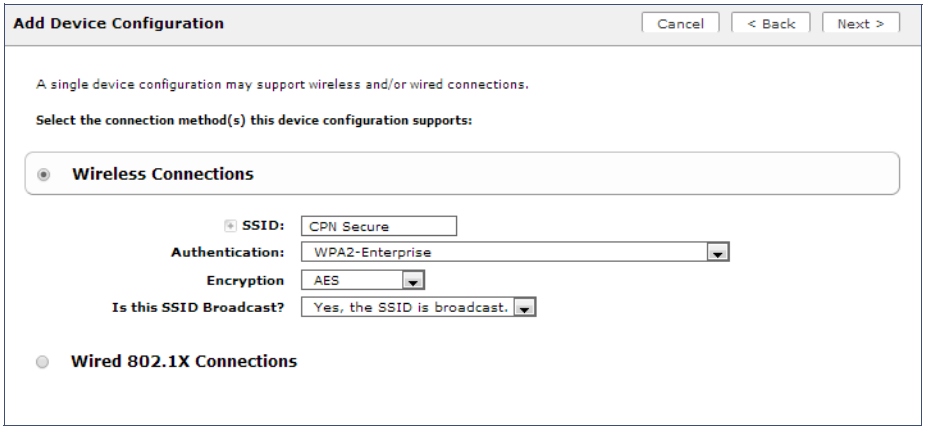
A device configuration is a group of settings containing a single configuration per operating system. This configuration determines the settings and behavior required to move the device from the onboarding SSID to the secure network.

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

Device Configuration

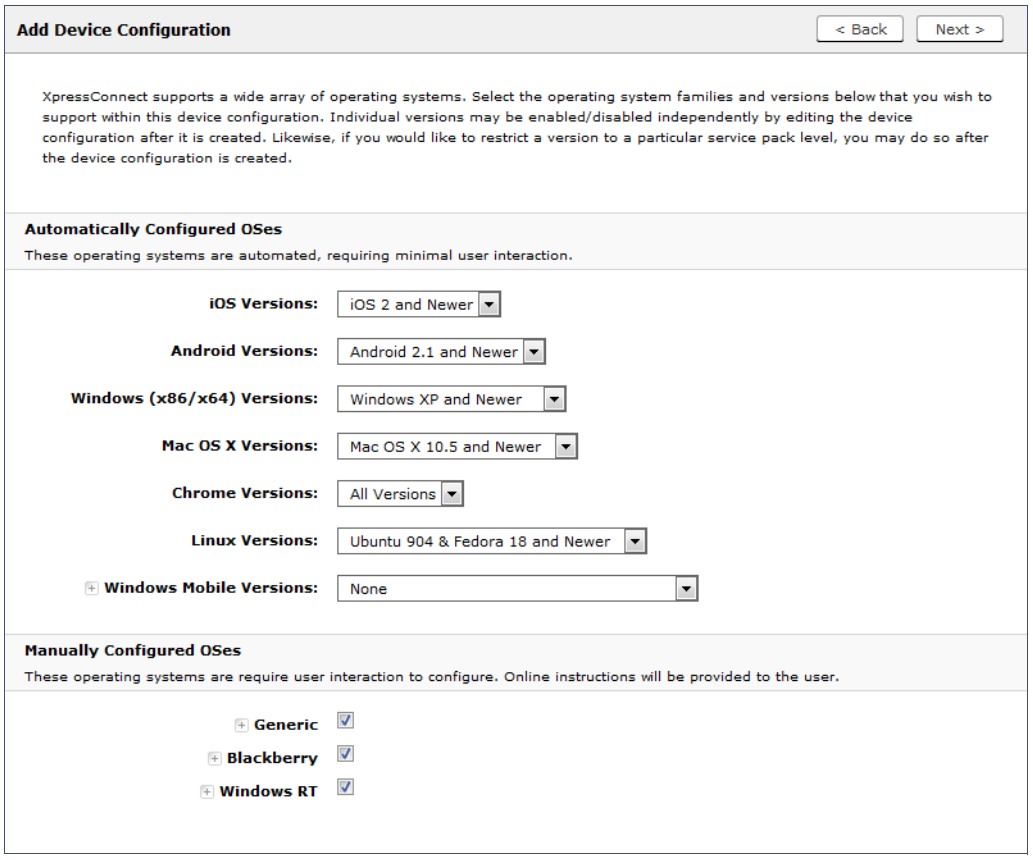
1. On the right side of the *Result* step, click the edit icon.
2. Select *A new device configuration.*
3. On the Add Device Configuration page, provide a name for the device configuration. This is the name a user sees in the device Wi-Fi networks list.
4. Select *Wireless Connections* (the default)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

FIGURE 38. 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 39. 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.

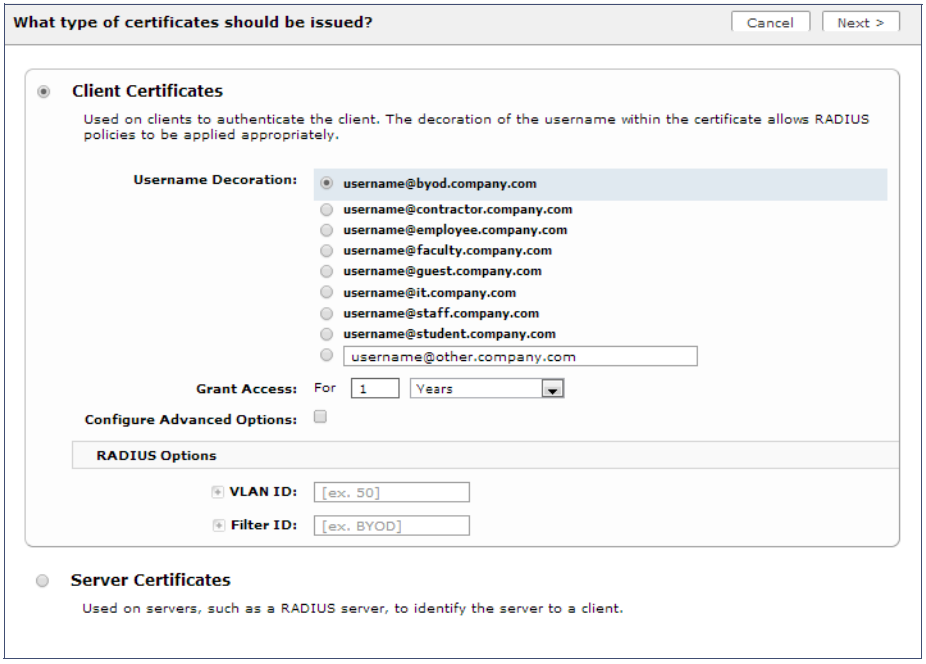
You can set up different certificate templates for different user types. An employee or staff certificate template might be valid for 120 days, and a guest template might be valid for 1 day or until the end of the week.

How to Set Up Client Certificate Templates

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 40. 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 > Advanced > Company Information* to change the default domain.

6. Grant access for the appropriate amount of time.

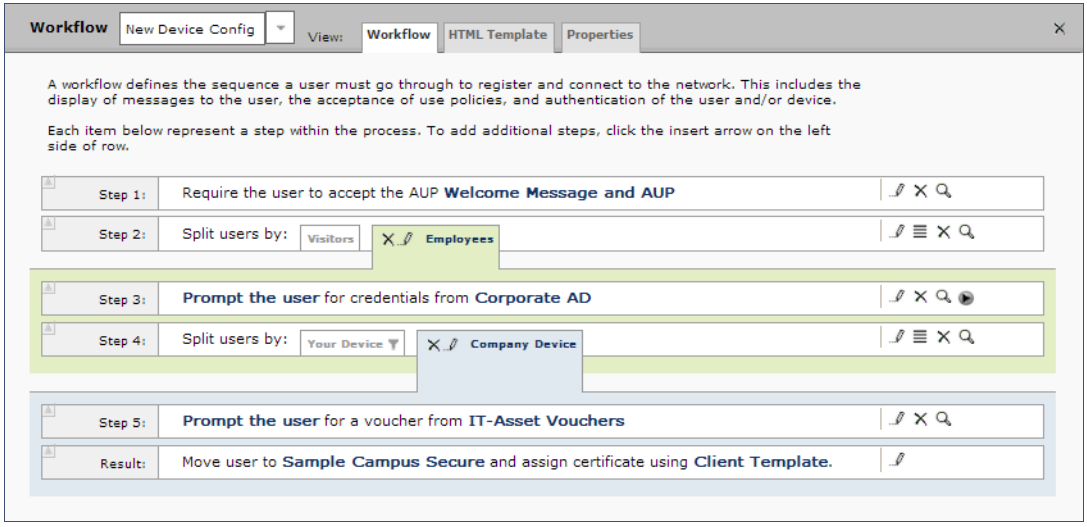
For example, you might have a client certificate template for a guest user that is valid for one, or a few days, another for a contractor that is valid for 6 months, and one for employees that is good for a year.

> **Tip >>**
> 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 ES 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 41. 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.

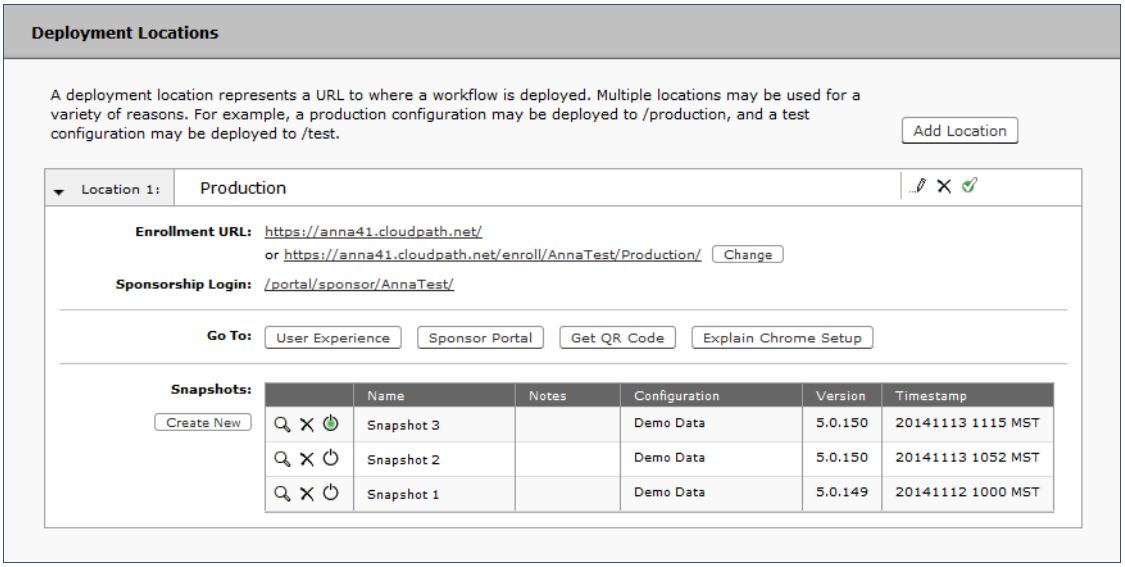
Deploying the Enrollment Workflow

Deploy the workflow from the *Configuration > Deploy* tab.

The deployment Locations page contains the URL where a configuration is deployed, and snapshots, which are build packages for each workflow configuration.

The default deployment location is *enroll/<network name>/Production,* but this can be modified.

FIGURE 42. Deployment Locations



Deployment Locations

A deployment location represents a URL to where a configuration is deployed. The Cloudpath ES supports multiple locations. For example, a test configuration might be deployed to */test* URL, and a production configuration may be deployed to */production* URL.

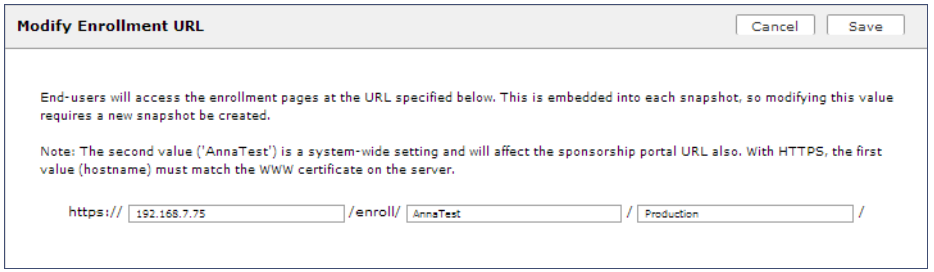
Administrators can add, edit, delete, view, and choose a default deployment location.

How to Add a Deployment Location

A deployment location is the URL where end-users access the enrollment wizard.

1. On the left menu, select *Configuration > Deploy*.
2. Click *Add Location*.

FIGURE 43. Modify Deployment Location



3. Enter the URL through which the end-users will enroll and *Save*.

The first two values, *Hostname* and *URL-Safe Company Name,* are pre-populated using the information provided in the initial system setup.

Configuration Snapshots

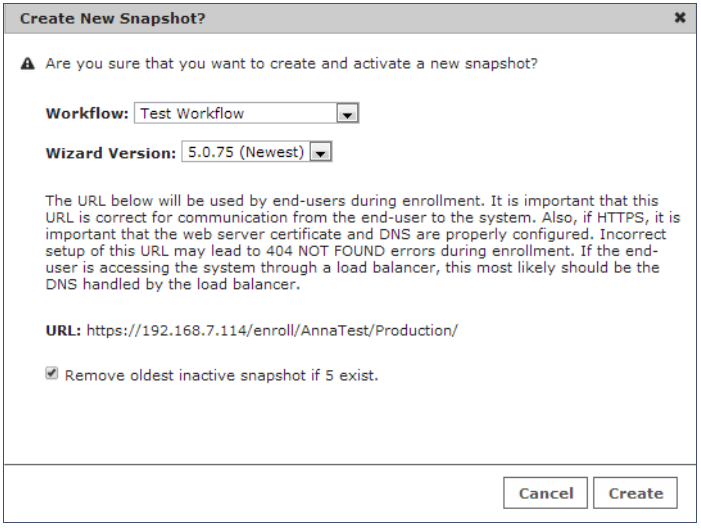
A snapshot is a version of a workflow configuration. You can create and maintain multiple versions of each configuration. However, only one snapshot can be active at a time for each deployment location.

Use the following steps to deploy a configuration snapshot to a deployment location.

How to Deploy a Snapshot of the Workflow Configuration

1. Go to *Configuration > Deploy*.
2. On the *Deployment Locations* page, in the *Snapshot* section, select *Create New*.

FIGURE 44. Create New Snapshot



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

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

When the snapshot is created and activated, expand the appropriate deployment location to test the network enrollment process.

How to Test a Configuration Snapshot

Test the enrollment process for the active configuration snapshot.

1. On the left menu, select *Configuration > Deploy*.
2. On the *Deployment Locations* page, in the Snapshot section, select the configuration you want to test.
3. Be sure that the snapshot you want to test is the *active* snapshot (green icon).

The *User Experience* button provides access to the user enrollment process, which contains the workflow and if applicable, the Cloudpath Wizard.

The *Sponsor Portal* button provides access to the Cloudpath ES *Sponsorship Portal*, which allows sponsors to invite users and create vouchers to be used during enrollment.

The *QR Code* button generates a QR code image, which when scanned, redirects the user to the deployment location. The QR code can be read on any mobile device with a camera, and QR code reading application.

The *Explain Chrome Setup* button provides instructions for setting up Managed Devices for Chromebooks. This information includes how to download and install the root CA, how to configure Wi-Fi, and how to add the Cloudpath ES extension.

See the Support tab for more information on configuring managed Chromebooks.

Ruckus Controller Integration for Cloudpath

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

Set up the Cloudpath ES as an AAA Authentication Server

Create AAA authentication and accounting servers for the Cloudpath ES onboard RADIUS server. The following images show this configuration on the Ruckus Zone Director and SmartZone controllers.

FIGURE 45. Create AAA Authentication Server on Zone Director

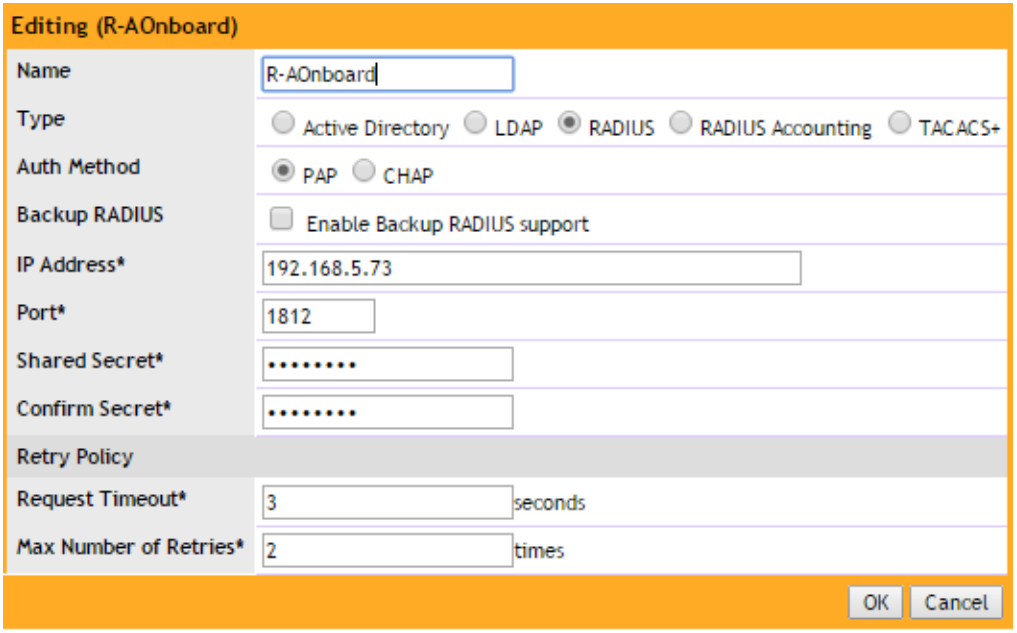
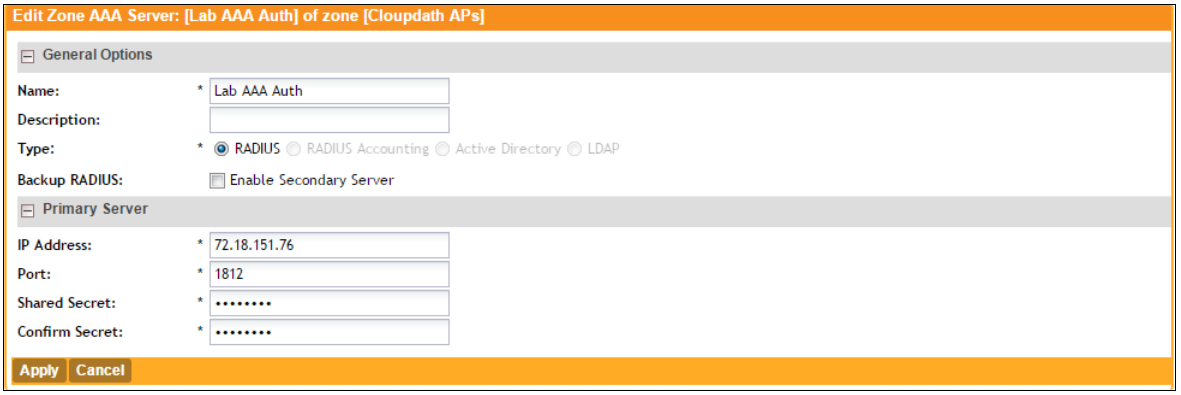


FIGURE 46. Create AAA Authentication Server SmartZone



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

1. Name
2. Type = RADIUS
3. Auth Method = 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 > Advanced > RADIUS Server*).
7. Leave the default values for the remaining fields.

Create AAA Accounting Server (Optional)

Use the same process to create the AAA Accounting Server.

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

1. Name
2. Type = RADIUS
3. Auth Method = PAP
4. IP address = The IP address of the Cloudpath ES.
5. Port = 1813

> **Note >>**
> The Authentication server uses port 1812. The Accounting server uses port 1813.

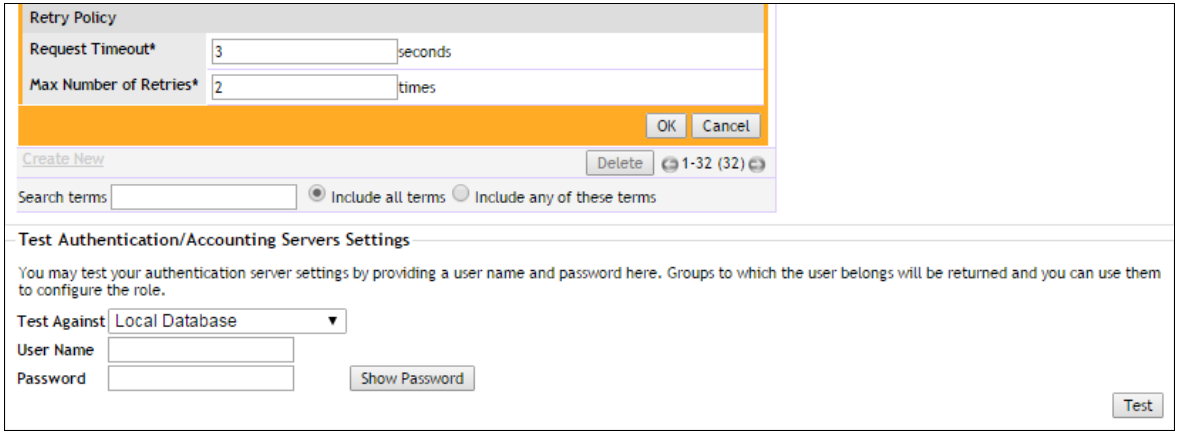
6. Shared Secret = This must match the shared secret for the Cloudpath ES onboard RADIUS server. (*Configuration > Advanced > RADIUS Server*).
7. Leave the default values for the remaining fields.

Run Authentication Test

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

At the bottom of the AAA server page, there is a section called Test Authentication/Accounting Servers Settings.

FIGURE 47. Authentication Test Zone Director



Enter a test User Name and Password and click the Test button on the bottom right of the page.

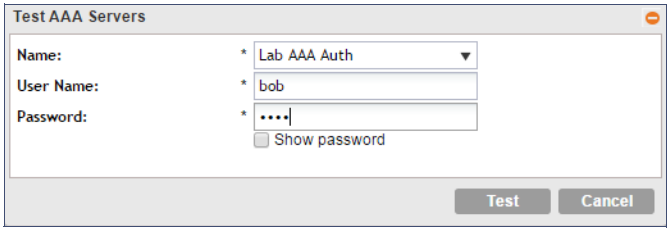
If you receive:

Failed! Invalid username or password

This means that connectivity was established.

On the SmartZone controller, you are prompted to Test Authentication when you save a configuration for an AAA Authentication server.

FIGURE 48. Authentication Test SmartZone



Create Hotspot Services

Enter the following values for the **Hotspot Service**:

1. Navigate to Hotspot Services (Hotspot WISPr on SmartZone).
2. Name the Hotspot Service.

FIGURE 49. Create Hotspot Service on Zone Director

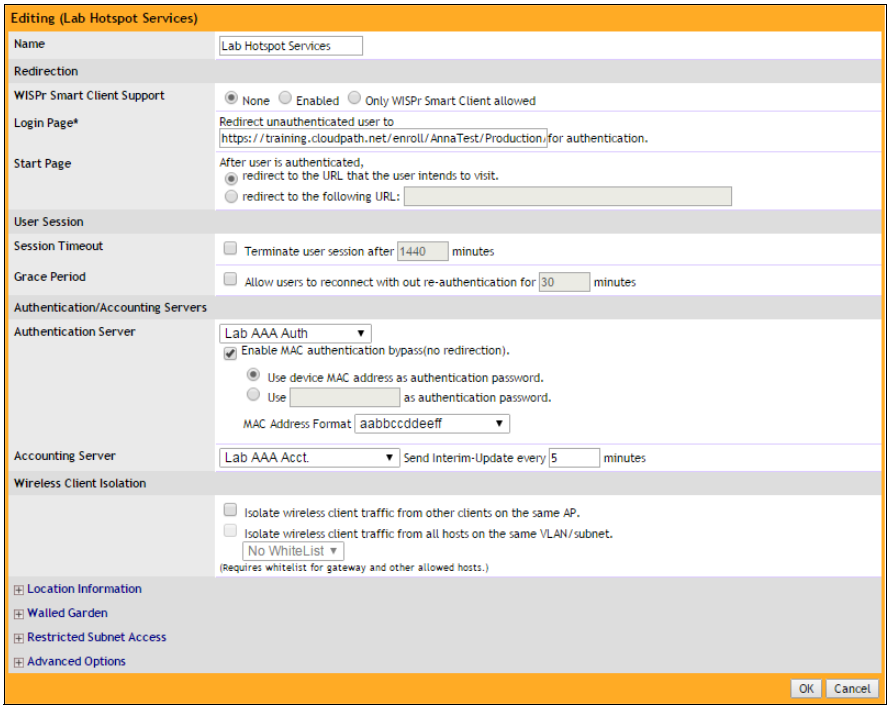
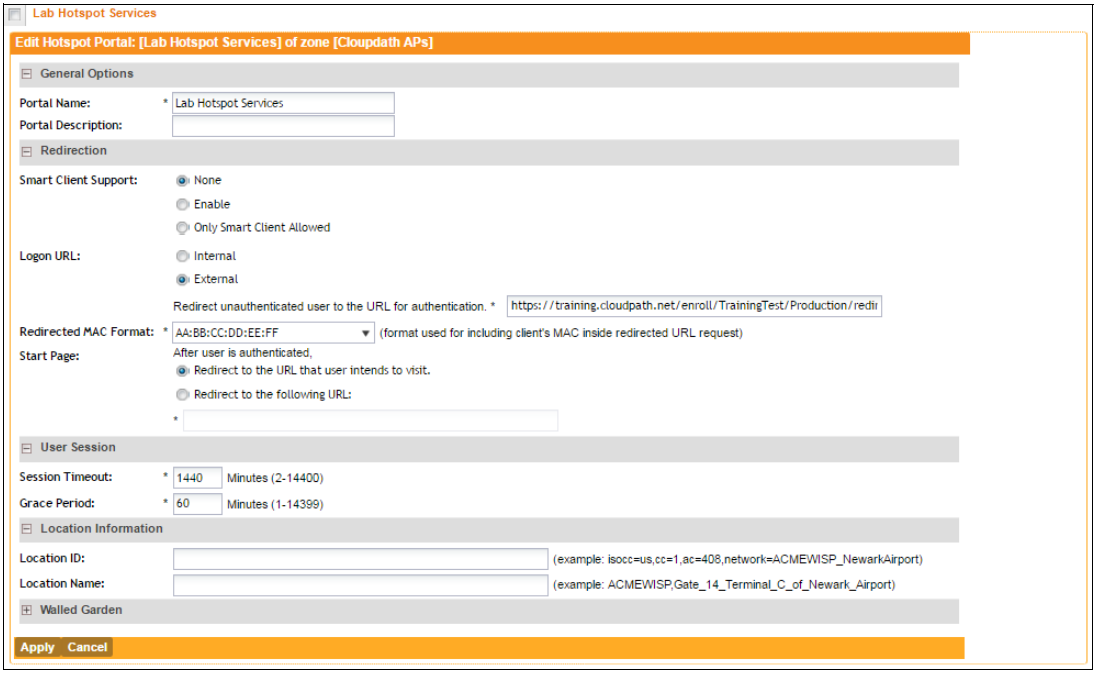


FIGURE 50. Create Hotspot WISPr on SmartZone



3. Point the unauthenticated user to the Cloudpath redirect URL. Enter the WLAN Redirect URL, which can be found on the Cloudpath Admin UI Configure > Deploy page.
4. Check Redirect to the URL that the user intends to visit.
5. Select the Cloudpath RADIUS Authentication Server (ZoneDirector only).
6. Enable MAC authentication bypass redirection (ZoneDirector only).
7. Select Use device MAC address as authentication password.
8. Select the Cloudpath RADIUS Accounting Server (ZoneDirector only).
9. Leave the defaults for the remaining settings. Click OK.

Set Up the Walled Garden

Enter the following values for the Walled Garden:

1. On the *Hotspot Service* > *Configure* page, scroll to the bottom to the **Walled Garden** section below the Hotspot Service configuration created in the previous section.

FIGURE 51. Walled Garden Configuration for Zone Director

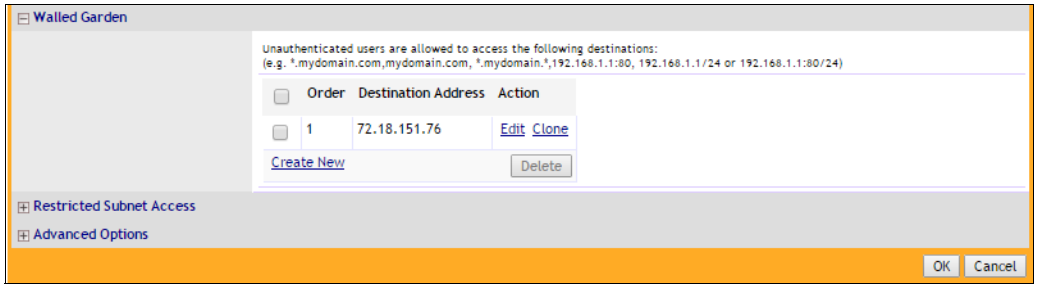
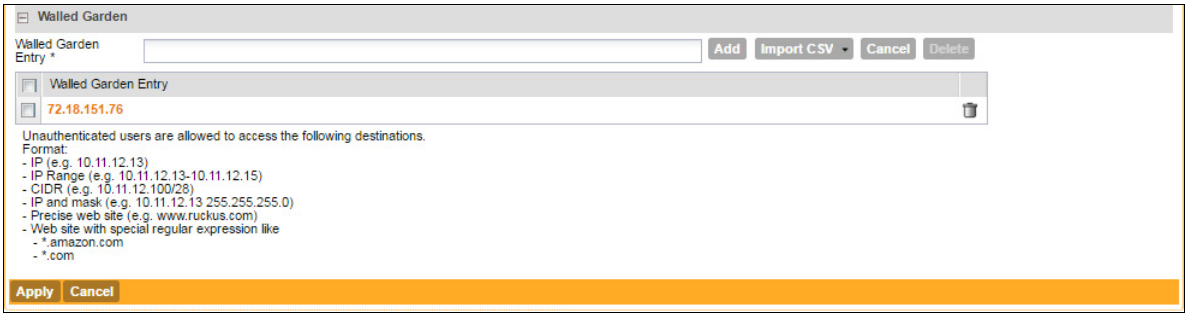


FIGURE 52. Walled Garden Configuration for SmartZone



2. Include the DNS or IP address of the Cloudpath system and **Save** (or Apply)

Create the Onboarding SSID

Enter the following values for the onboarding SSID:

1. Name the SSID.
2. Type=Hotspot Service (WISPr).

FIGURE 53. Onboarding SSID Configuration on Zone Director

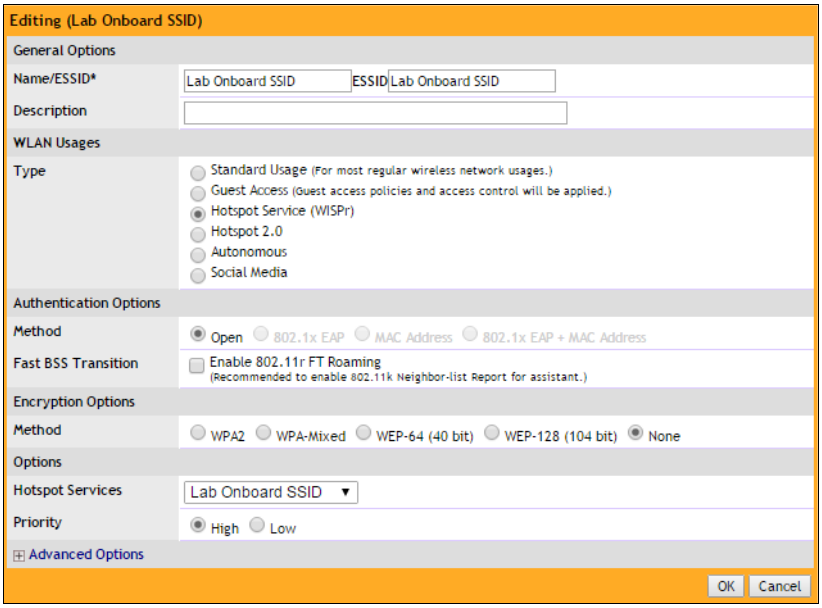
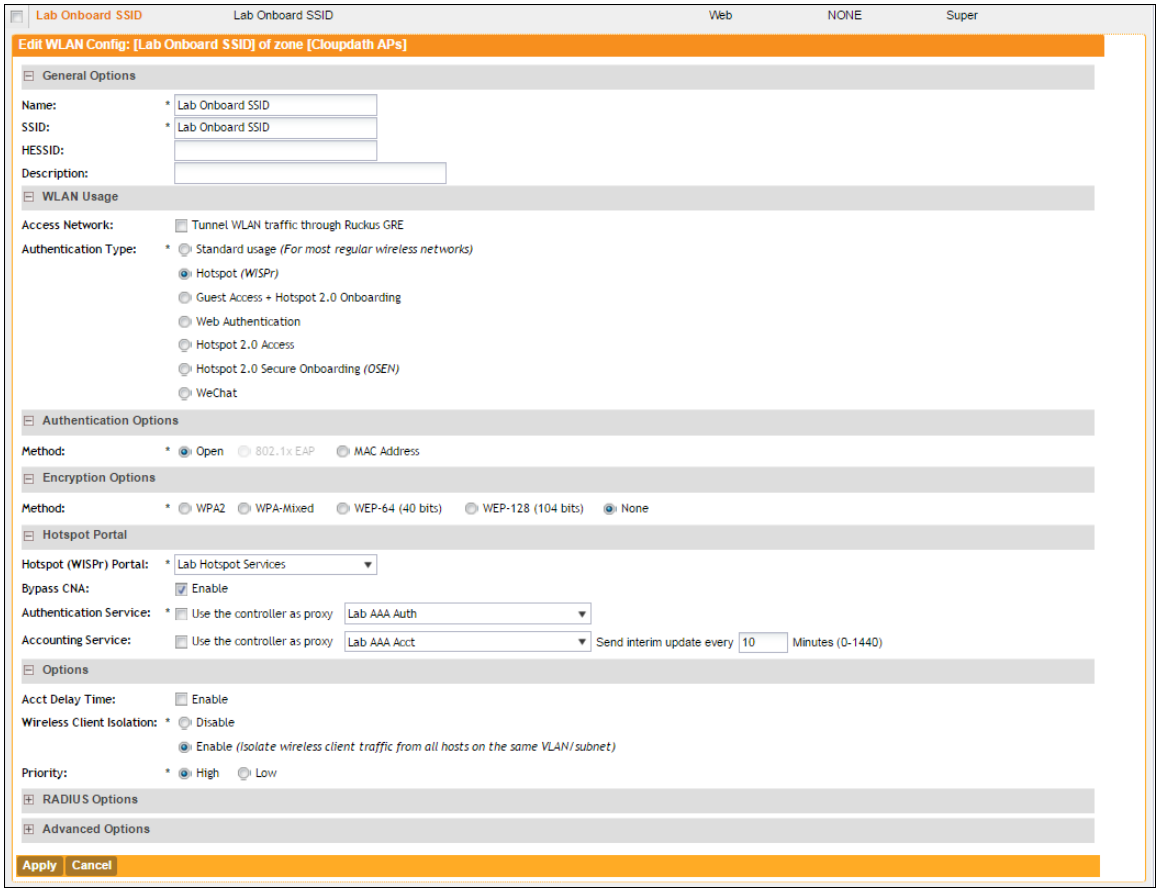


FIGURE 54. Onboarding SSID Configuration on SmartZone



3. Authentication Option Method=Open.
4. Encryption Option Method=None.
5. Select the Hotspot Service created in Task 2.
6. Enable Bypass CNA.
   - For ZoneDirector, this setting is at the bottom of the screen in the Bypass Apple CNA Feature section. Check the Hotspot service box.
   - For SmartZone, this setting is in the Hotspot Portal Section.
7. Select the Cloudpath RADIUS Authentication Server (SmartZone only).
8. Select the Cloudpath RADIUS Accounting Server (SmartZone only).

Leave the defaults for the remaining settings and click OK (or Apply).

Troubleshooting Your Deployment

Connectivity Issues

Cloudpath License Server

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

RADIUS Server

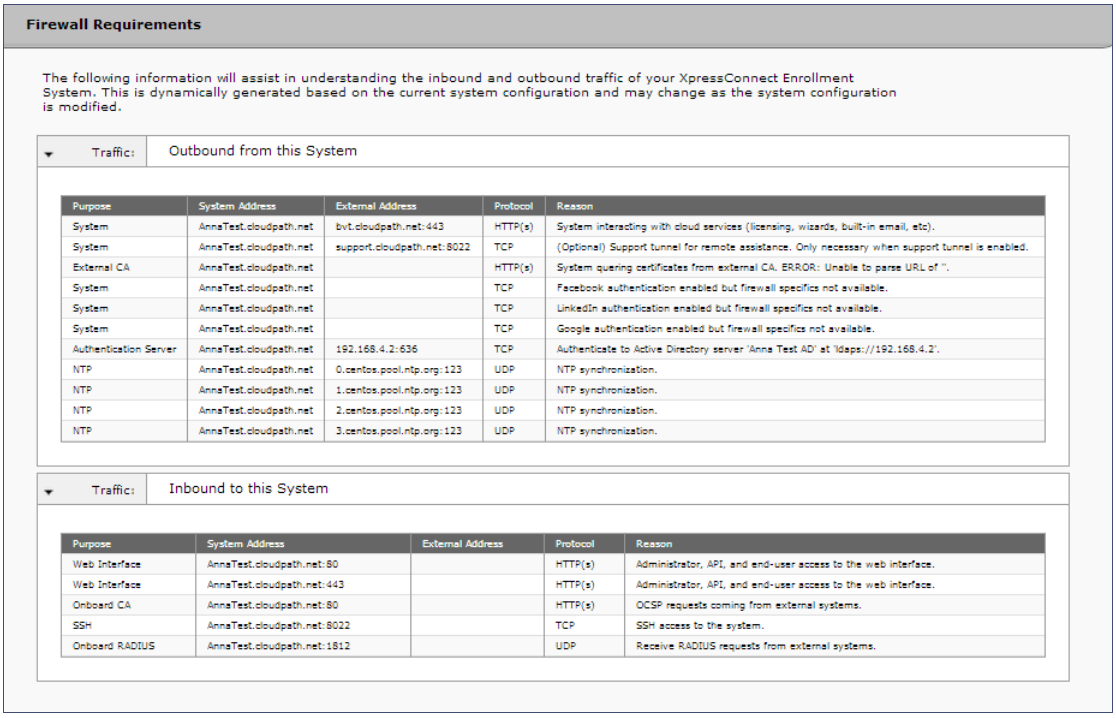
The wireless controller must be able to communicate with the ES onboard RADIUS server on port 14650.

Firewall Requirements

The Firewall Requirements table is designed to help you understanding the inbound and outbound traffic of the Cloudpath ES. 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 > Advanced > Firewall Requirements*.

FIGURE 55. Firewall Configuration



Firewall Requirements

The following information will assist in understanding the inbound and outbound traffic of your XpressConnect Enrollment System. This is dynamically generated based on the current system configuration and may change as the system configuration is modified.

Traffic: Outbound from this System

Purpose	System Address	External Address	Protocol	Reason
System	AnnaTest.cloudpath.net	bvt.cloudpath.net:443	HTTP(s)	System interacting with cloud services (licensing, wizards, built-in email, etc).
System	AnnaTest.cloudpath.net	support.cloudpath.net:8022	TCP	(Optional) Support tunnel for remote assistance. Only necessary when support tunnel is enabled.
External CA	AnnaTest.cloudpath.net		HTTP(s)	System quering certificates from external CA. ERROR: Unable to parse URL of ''.
System	AnnaTest.cloudpath.net		TCP	Facebook authentication enabled but firewall specifics not available.
System	AnnaTest.cloudpath.net		TCP	LinkedIn authentication enabled but firewall specifics not available.
System	AnnaTest.cloudpath.net		TCP	Google authentication enabled but firewall specifics not available.
Authentication Server	AnnaTest.cloudpath.net	192.168.4.2:636	TCP	Authenticate to Active Directory server 'Anna Test AD' at 'ldaps://192.168.4.2'.
NTP	AnnaTest.cloudpath.net	0.centos.pool.ntp.org:123	UDP	NTP synchronization.
NTP	AnnaTest.cloudpath.net	1.centos.pool.ntp.org:123	UDP	NTP synchronization.
NTP	AnnaTest.cloudpath.net	2.centos.pool.ntp.org:123	UDP	NTP synchronization.
NTP	AnnaTest.cloudpath.net	3.centos.pool.ntp.org:123	UDP	NTP synchronization.

Traffic: Inbound to this System

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

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 ES virtual appliance.

Verify DNS registration for domain controllers

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 the Cloudpath ES. 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 the ES 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 the Cloudpath ES, you must check the box for the Microsoft Server EKU.

NPS-Specific Troubleshooting

For configuration details, see the *Cloudpath ES Integration with Microsoft NPS Configuration Guide* on the ES 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 -enterprise -addstore NTAuth root.cer
```

Cloudpath ES 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 ES webpage.

Define an ACL that allows access to the ES 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 ES IP Address], Protocol TCP, Destination Port HTTP, Action Permit
   - Sequence 2, Source [Cloudpath ES 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 ES URL]";
</SCRIPT>
If you are not automatically redirected,
<a href="[Cloudpath ES URL]">click here</a>
to go to the Cloudpath ES.
```

> **Note >>**
> The URL of the ES 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 ES webpage.
8. Click *Save Configuration* at the top of the page.