

# XpressConnect

## Enrollment System

## Quick Start Guide

Software Release 4.2

December 2015

**Summary:** This document describes what the Enrollment System does, what you need to set up the ES, how to deploy the virtual appliance, and initial system configuration. This guide also provides instructions for getting the system up in running with a basic workflow configuration, how to create a snapshot, how to deploy it to your network, and report fundamentals.

**Document Type:** Configuration

**Audience:** Network Administrator



# **XpressConnect Enrollment System Quick Start Guide**

Software Release 4.2

December 2015

Copyright © 2015 Cloudpath Networks, Inc. All rights reserved.

**Cloudpath Networks** and **XpressConnect** are trademarks of *Cloudpath Networks, Inc.*

Other names may be trademarks of their respective owners.

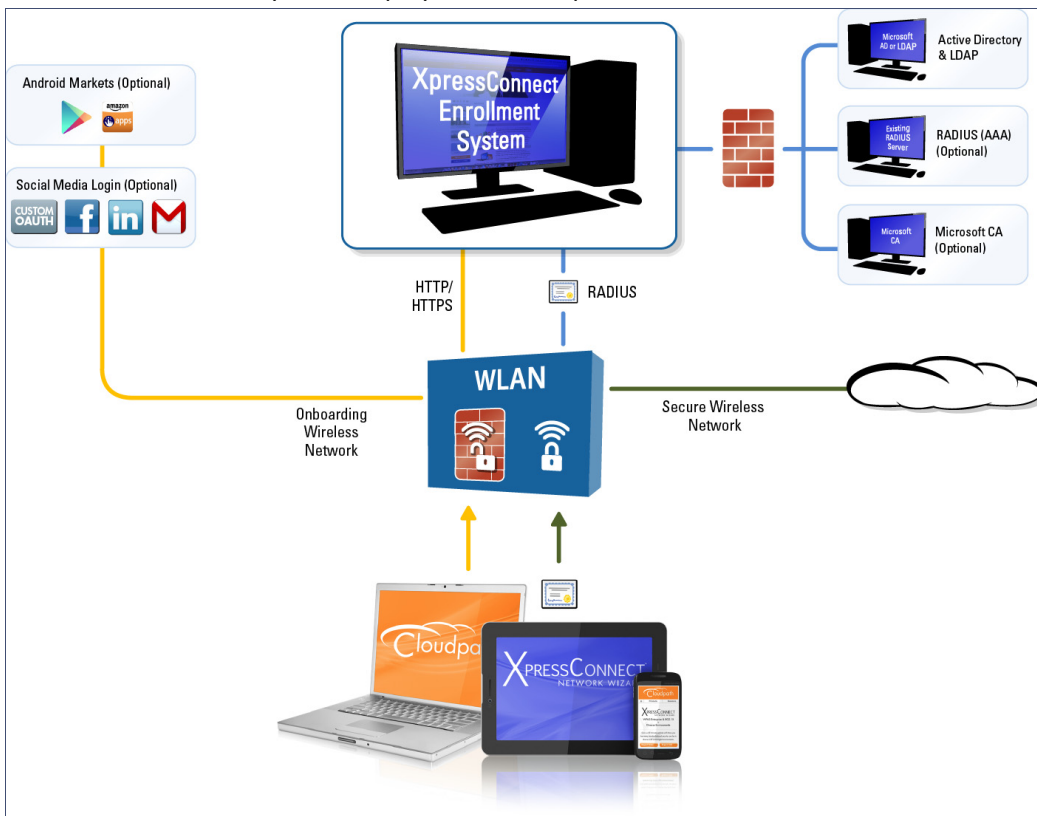
# XpressConnect Enrollment System Quick Start Guide

## Overview

XpressConnect Enrollment System 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 Enrollment System 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.** Enrollment System Deployment Example



Authorization can come from a variety of sources, including authentication using vouchers or acceptance of a use policy. Once authorized, a device can be given access along with additional policy options based on WPA2-Enterprise, such as dynamic VLAN, ACL, or bandwidth assignment.

When you plan your workflow, you can have a different enrollment sequence for employees and visitors, and 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.

During deployment, all enrollment workflow branches are bundled as one configuration in the XpressConnect system.

## Enrollment System Specifications

ES supports the following browser, operating systems, and third-party identity stores for system and user devices.

**TABLE 1. Enrollment System Specifications**

Supported Browsers for ES Admin UI	Supported OSEs for End-User Devices	Supported Third-Party Identity Stores
Internet Explorer 6.0 and greater	Windows XP SP2 and greater	Microsoft Active Directory
Firefox 1.5 and greater	Mac OS X 10.5 and greater	LDAP
Safari 2.0 and greater	Apple iOS 2.0 and greater	Facebook
Google Chrome 3.0 and greater	Ubuntu 9.04 and greater	LinkedIn
	Android 2.1 and greater	Google Gmail
	Fedora 18 and greater	Custom OAuth 2.0 Server
	Chrome OS	
	Windows Phone 8 and 8.1	
	Blackberry (assisted configuration)	
	Windows RT (assisted config)	
	Generic (assisted config)	
	Windows Mobile 5 and 6 (assisted config)	

### Note >>

The supported end-user operating systems are automated and required minimal user interaction. The assisted configuration operating systems require user interaction to configure. Online instructions are provided to the user.

---

## Information You Need

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

### Deploying the OVA (For Local Deployments)

- VMware server, on which you'll install the ES virtual appliance
- The URL where the OVA file resides
- FQDN Hostname of the virtual appliance
- IP address and subnet mask for the virtual appliance (not required if using DHCP)
- Gateway IP address for your network (not required if using DHCP)
- IP address of DNS server (not required if using DHCP)
- A list of IP addresses that are allowed Administrative access (optional)
- Service account security credentials

### Setting up the Initial Account

- Login credentials for XpressConnect Licensing Server
- Licensing 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
- Web server certificate (public-signed)
- Code-signing 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
  - If using VLANS to apply policy, you should have the VLAN IDs
- A list of conflicting SSIDs to prevent roaming (for example, open SSIDs)
- 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 pass code)

## Deploying the ES Virtual Appliance to a VMware Server

---

### Note >>

If you are setting up a hosted system, you can skip this section and continue to Initial System Setup.

---

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

### Specifications for Locally-Deployed VMware Servers

The Enrollment System 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 Enrollment System.

### 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 Enrollment System OVA file from the Licensing Server ([xpc.cloudpath.net](http://xpc.cloudpath.net)) *OVA Download* tab, from a direct download link, or from a Cloudpath representative.

To retrieve the OVA file using the XpressConnect Licensing Server:

1. Log in to the Licensing Server ([xpc.cloudpath.net](http://xpc.cloudpath.net)) using the link and credentials provided in the license activation email. The Welcome page is displayed.

The XpressConnect Licensing Server is the management application where Accounts and Licenses are managed.

FIGURE 2. Licensing Server Welcome Page

**Cloudpath** NETWORKS | Cloudpath Administrative Console | Anna Test | Logout

**Introduction**  
Certificates  
Define Networks  
Deploy  
OVA Download  
Advanced  
Manage Account  
Support

**Current Build:** The latest build (5.0.96) was posted on May 21, 2014. [Details are available here.](#)

Welcome to the XpressConnect Administrative Console.

**Administrative Console**  
[Quick Start Guide](#)  
[FAQs](#)

**XpressConnect** is the easiest way to support a secure network.

Whether 802.1X-based wired access, 802.1X-based wireless access, or PSK-based wireless access, end-users are migrated to the secure network quickly and effortlessly. This kind of automated network configuration significantly lessens help desk involvement and end-user frustration. XpressConnect is your resource for supporting secure networks in a cost-effective, low overhead manner.

To personalize XpressConnect for your network environment, simply adjust the values in the console as you see fit. XpressConnect's Administrative Console has three major sections:

**Define Networks**

When a user connects to your network, certain configuration settings are necessary for successful network access. For example, your network may already require 802.1X authentication using PEAP with server certificate validation. You specify these configuration settings within a network on the Define Networks tab. When a user connects to your network, their machine will be configured based on the definition of the network.

**Deploy**

Once networks and visual customizations are configured, move to the Deploy tab. To make deployment hassle-free, XpressConnect is packaged in a compressed TAR file that includes your custom configuration. The Deploy tab allows you to download XpressConnect and the supporting files for deployment to your web server or CD.

**Manage Account**

All the paperwork is kept under this tab. Use the Manage Account section to review license information, update contact information, and manage administrative access.

- Go to the *OVA Download page*. This page provides a link to the OVA file, documentation providing instructions for setting up the Enrollment System 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 3. OVA Download Page

**Cloudpath** NETWORKS | Cloudpath Administrative Console | Anna Test | Logout

**Introduction**  
Certificates  
Define Networks  
Deploy  
OVA Download  
Advanced  
Manage Account  
Support

To deploy XpressConnect, download an OVA file below and deploy onto a VMware ESXi server.  
Use of the software signifies your acceptance of the [End-User License Agreement](#).

**OVA Download**

<b>Version:</b>	2.0.1604
<b>Published:</b>	20130820
<b>OVA File:</b>	<a href="#">XpressConnectES_OVF10_2.0.1604.ova</a>
<b>Deployment Instructions:</b>	<a href="#">ES_VirtualAppliance.pdf</a>
<b>Release Notes:</b>	Create a VMware snapshot of the enrollment system VM before upgrading. For updates, refer to the <a href="#">release notes</a> .

3. Download and read the *Deployment Instruction* document.
4. 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 *XpressConnect Enrollment Server*.
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 4. Application Properties

**Application**

**Installation of the product implies consent the Oracle EULA**  
 EULA: <http://www.oracle.com/technetwork/java/javase/terms/license/index.html>

---

**Do you want to require the boot password in order to start the server?**  
 Requiring a password on boot enforces that only authorized personnel can start the system. Leave the checkbox unchecked if you want the system to start without intervention.

---

**Hostname(FQDN)**  
 Enter the fully qualified domain name.

---

**Timezone**

---

**Should Apache be configured for SSL?**

---

**Do you want to permit SSH?**

---

**What addresses should have access Administration functionality?**  
 A comma separated list of addresses or CIDR notation.

---

**The service user password**  
 The service password is used by your support team for access to this system. Please select a password that is compliant with your password complexity policy.

Enter password

Confirm password

---

**Enter the NTP server or leave blank to use pool.ntp.org**

- 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 a boot password for all system reboots.
  - If unchecked, a boot password is not required for system reboots.

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

**Note >>**

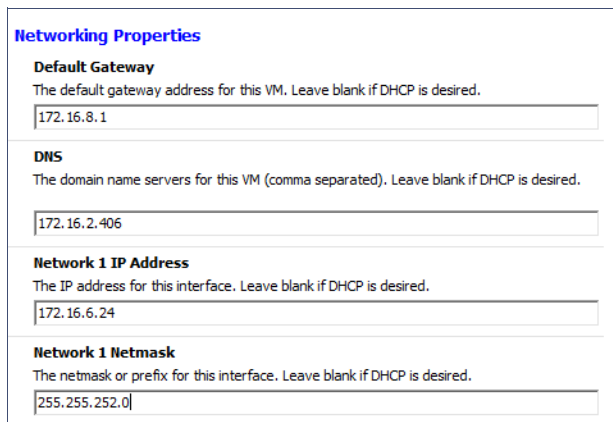
The Enrollment System *Hostname* is used as the default *OCSP Hostname*, which is embedded into certificates issued by the onboard root CA as part of the URL for the Online Certificate Status Protocol (OCSP).

- Select the *Timezone*.
- Should Apache use SSL? Leave unchecked only if the Enrollment System 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 is not permitted.
- Optional. Specify the address of an NTP server. To use pool.ntp.org, leave this field blank.

## 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 5. Networking Properties



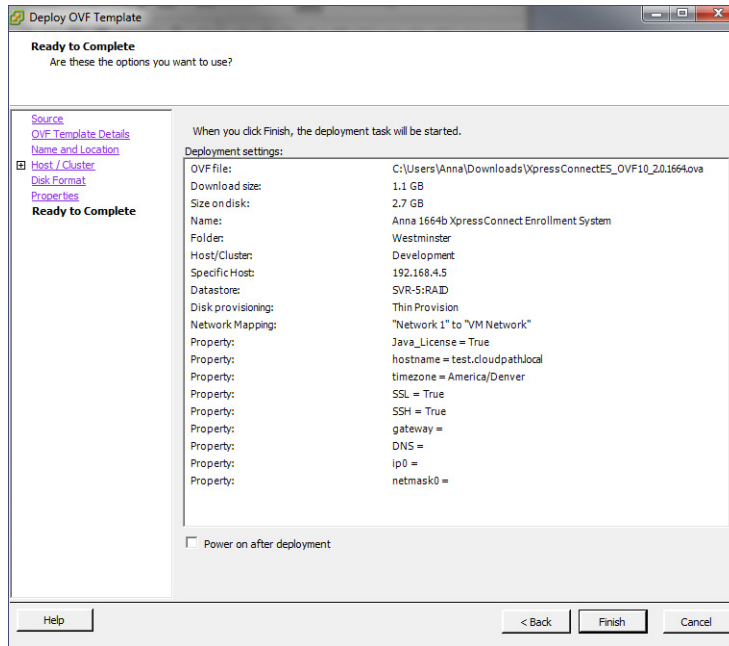
The screenshot shows a web form titled "Networking Properties" with four sections, each containing a text input field with a pre-filled value:

- Default Gateway**: The default gateway address for this VM. Leave blank if DHCP is desired. Input: 172.16.8.1
- DNS**: The domain name servers for this VM (comma separated). Leave blank if DHCP is desired. Input: 172.16.2.406
- Network 1 IP Address**: The IP address for this interface. Leave blank if DHCP is desired. Input: 172.16.6.24
- Network 1 Netmask**: The netmask or prefix for this interface. Leave blank if DHCP is desired. Input: 255.255.252.0

## Confirm Deployment Settings

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

FIGURE 6. Deployment Settings



Click *Finish*. Deployment takes approximately 2 minutes.

## Console

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

1. At the login prompt, enter `cpn_service` and then the service user password. You receive the CLI prompt (`#`) with a successful login.
2. Enter `?` to display the list of available commands on the console.
3. Enter the **show config** command to verify your configuration. You may be prompted to re-enter the password.

See the *XpressConnect Enrollment System 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 your Licensing Server is hosted
- Verify that the virtual appliance can resolve DNS

## Initial System Setup

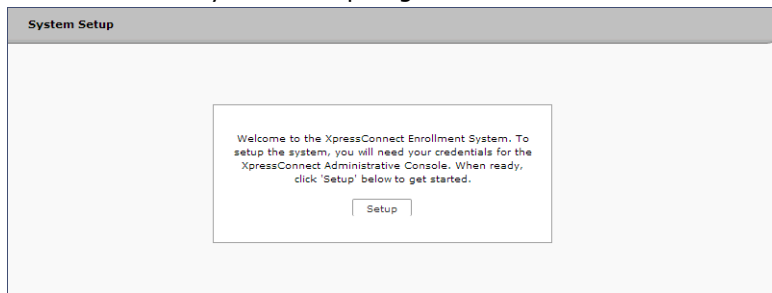
Cloudpath Networks provides you with a single administrator login for the XpressConnect Enrollment System. Additional administrators can be added from the left menu *Administration* tab, or you can enable Administrator logins from your authentication servers.

You can access the Enrollment System from a cloud-hosted network (multi-tenant), or as a virtual appliance on a locally-deployed VMware server (single-tenant).

## Account Setup

1. After a successful deployment, enter the IP address or hostname of the Enrollment System. The *System Setup* page opens.

FIGURE 7. Initial System Setup Page



2. When you have the information you need, click *Setup*.
3. Enter your XpressConnect Licensing Server login credentials. This step binds the Enrollment System to the Licensing Server.

FIGURE 8. Licensing Server Credentials

**System Setup**

**Setup Account** Next >

To setup the system, you must first authenticate using your credentials for the XpressConnect Administrative Console. Specify your username and password for <https://xpc.cloudpath.net> below and click 'Next >'.

Administrative Console URL:  \*

Email Address:  \*

    Password:  \*

4. Select the type of server to set up.

FIGURE 9. Select Server Type

**System Setup**

**What Type Of Server Is This?** Next >

**Standard Server (Default)**  
Select this option if this server is your first server or if a cluster will be initialized from this server.

**Add-On Server For Cluster**  
Select this option if this server will be part of a cluster and the cluster will be initialized from a different server. No further configuration will occur on this server until the cluster is established.

**Replacement Server For Existing Server**  
Select this option if this server will import data from an existing server.

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 Enrollment System 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

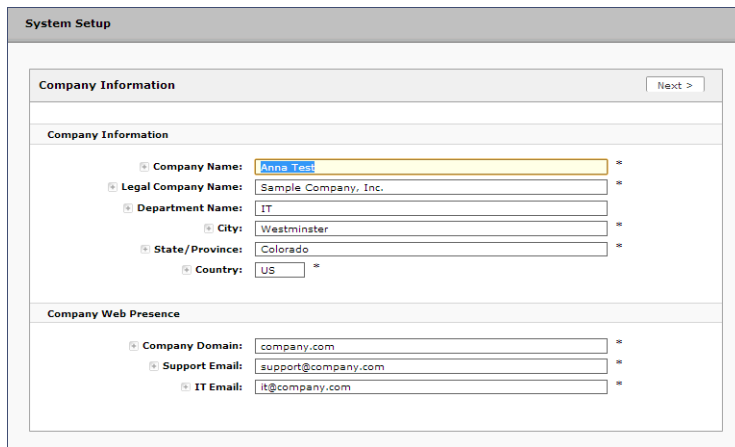
information for the initial setup. *Add-On* and *Replacement* servers receive most of their configuration from the Master server in the cluster.

### Note >>

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

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

FIGURE 10. Company Information



The screenshot shows the 'System Setup' window with the 'Company Information' section active. The 'Next >' button is in the top right. The 'Company Information' section contains the following fields:

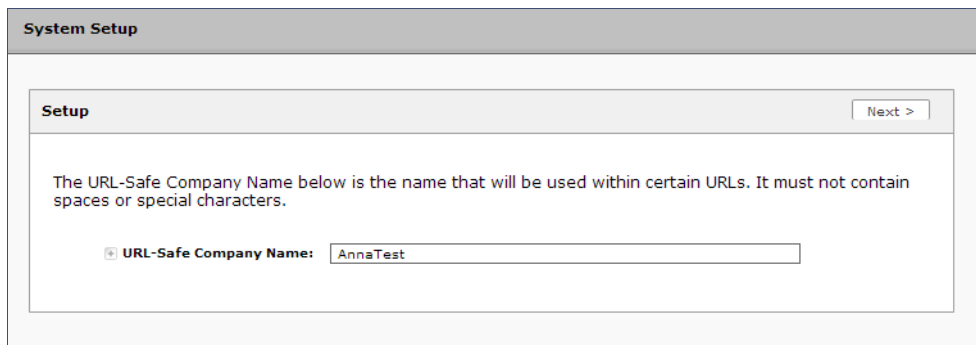
- Company Name: Anna Test
- Legal Company Name: Sample Company, Inc.
- Department Name: IT
- City: Westminster
- State/Province: Colorado
- Country: US

The 'Company Web Presence' section contains the following fields:

- Company Domain: company.com
- Support Email: support@company.com
- IT Email: it@company.com

6. Enter the *URL-Safe Company Name*. For example, enter *MyCompany* for the URL `https://xpces.cloudpath.net/enroll/MyCompany/`. The *URL-Safe Company Name* cannot contain spaces or special characters.

FIGURE 11. System Setup URL-Safe Company Name



The screenshot shows the 'System Setup' window with the 'Setup' section active. The 'Next >' button is in the top right. The 'Setup' section contains the following text and field:

The URL-Safe Company Name below is the name that will be used within certain URLs. It must not contain spaces or special characters.

URL-Safe Company Name: AnnaTest

## Authentication Server


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 12. Authentication Server Setup

**Authentication Server** Skip Next >

If you will be using an authentication server to authenticate end-users or sponsors, we recommend populating the authentication server information below. If using multiple authentication servers, additional authentication servers may be added through the workflow.



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

**Default AD Domain:** [ex. test.sample.local]

**AD Host:** [ex. ldaps://192.168.4.2] \*

**AD DN:** [ex. dc=test,dc=sample,dc=local] \*

**AD Username Attribute:** SAM Account Name

**Verify Account Status On Each Authentication**

**Perform Status Check:**

**Additional Logins**

**Use For Admin Logins:**

**Use For Sponsor Logins:**

**Test Authentication**

**Run Authentication Test?**

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

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

**Skip for now.**  
Select this option to skip this step for now. Authentication servers may be added anytime via the workflow.

To setup the initial configuration of the Authentication Server, select *Connect to Active Directory* or *Connect to LDAP* and enter the required fields.

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.

## Authentication Server Certificate

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

**FIGURE 13.** Authentication Server Certificate

**Authentication Server**
< Back    Next >

To use LDAPS, the system needs to know which server certificate to accept for the authentication server.

**Upload the Chain for the Server Certificate.**

Select this option to specify the common name of the LDAPS server certificate and to upload the issuing CA. This provides the most resilient form of server certificate validation and does not normally require updates when the certificate is renewed.

\*

**Pin the Current Server Certificate.**

Pin the current server certificate as a trusted certificate. This is the quickest and easiest but must be updated when the certificate is renewed.

<b>Common Name:</b>	svr-2.test.cloudpath.local
<b>Thumbprint:</b>	3178232065328996CBC16D5AF625D132AB5735C2
<b>Valid Period:</b>	07/11/2014 - 07/11/2015
<b>Issued By:</b>	Cloudpath Networks MSftCA



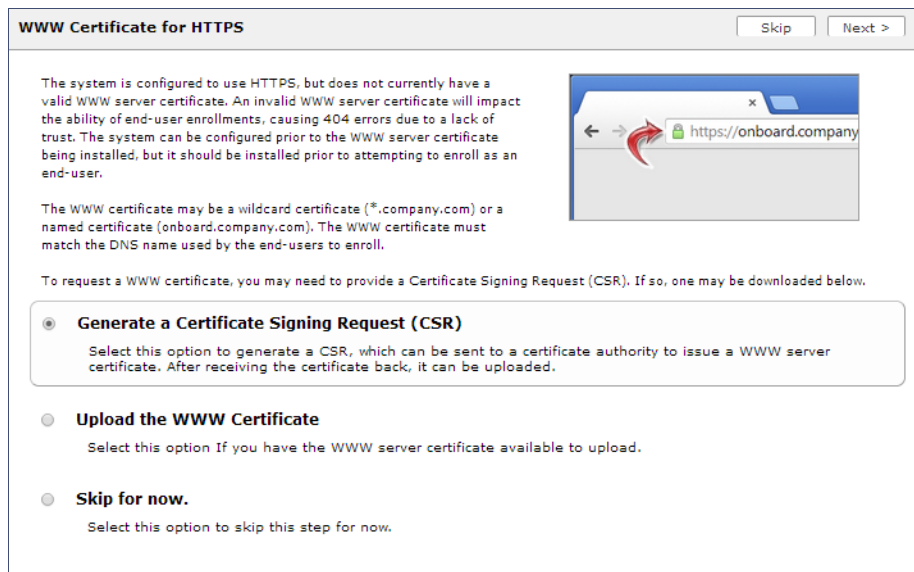
Select *Upload the Chain for the Server Certificate* to upload a certificate chain from an issuing CA. You must specify the common name for the LDAPS server certificate. This certificate does not need to be updated when the certificate is renewed.

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.

## WWW Certificate HTTPS

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 14. WWW Certificate for HTTPS



**WWW Certificate for HTTPS** Skip Next >

The system is configured to use HTTPS, but does not currently have a valid WWW server certificate. An invalid WWW server certificate will impact the ability of end-user enrollments, causing 404 errors due to a lack of trust. The system can be configured prior to the WWW server certificate being installed, but it should be installed prior to attempting to enroll as an end-user.

The WWW certificate may be a wildcard certificate (\*.company.com) or a named certificate (onboard.company.com). The WWW certificate must match the DNS name used by the end-users to enroll.

To request a WWW certificate, you may need to provide a Certificate Signing Request (CSR). If so, one may be downloaded below.

- Generate a Certificate Signing Request (CSR)**  
Select this option to generate a CSR, which can be sent to a certificate authority to issue a WWW server certificate. After receiving the certificate back, it can be uploaded.
- Upload the WWW Certificate**  
Select this option if you have the WWW server certificate available to upload.
- Skip for now.**  
Select this option to skip this step for now.

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*.

## Upload the WWW Certificate

The Enrollment System 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.

FIGURE 15. Upload WWW Certificate

**Upload WWW Certificate**

---

**P12 Upload**  
You may upload a web server certificate in p12 format. To do so, you must also specify the password if the p12 is password protected.

**P12 File:**

**P12 Password:**

---

**Or PEM Upload**  
If a p12 file is not available, you may upload the individual components of the certificate. All files must be in PEM (Base64) format. If the private key is password-protected, specify the password too. If the private key is not password-protected, leave the password blank.

**Public Key (PEM):**

**Chain (PEM or P7b):**

**Private Key (PEM):**

**Private Key Password:**

**Prompt for Password on Boot:**

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

## Certificate Authority

Select *Create Certificate Authority* to set up the onboard Certificate Authority. The entry fields are pre-populated based on the Company Information that was entered during Account Setup, but can be modified.

FIGURE 16. Create Certificate Authority

**Setup Certificate Authority** Skip Next >

**Create Certificate Authority**  
Select this option to initialize a root and intermediate CA using the information below.

**CA Naming**

**Root CA Name:**  \*

**Intermediate CA Name:**  \*

**Organization Info**

**Organization:**

**Organizational Unit:**

**Email:**

**Title:**

**Locality:**

**State:**

**Country:**

**Advanced Details**

**Years Valid:**

**Algorithm:**  ▼

**Key Length:**

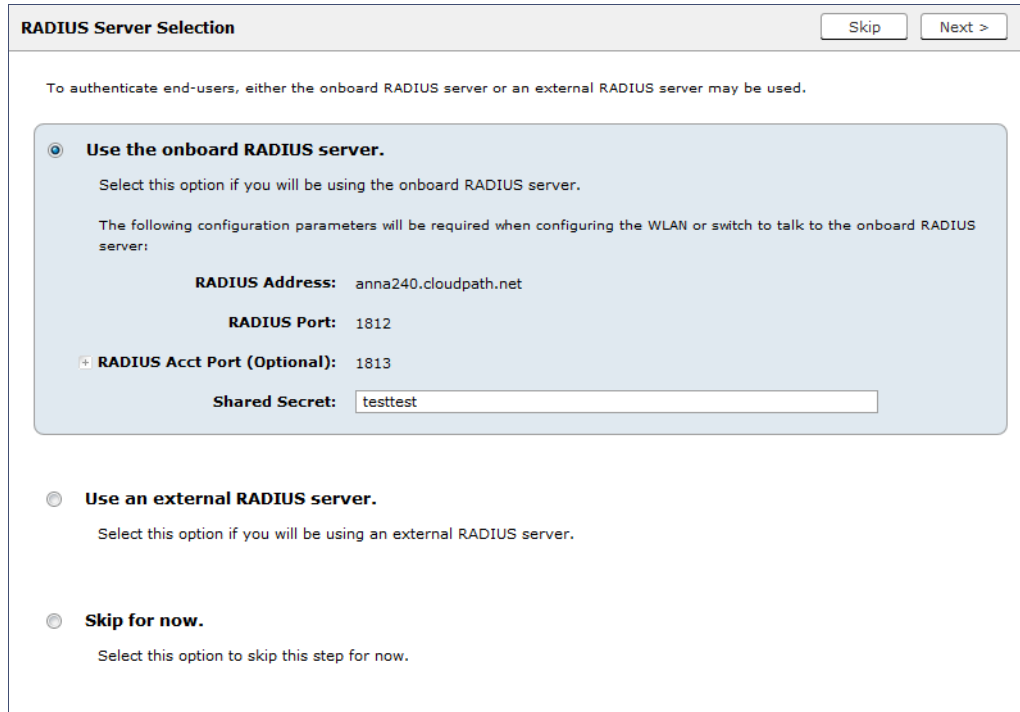
**Skip for now.**  
Select this option to skip this step for now, to manually setup the certificate authority, or to use external certificate authorities.

If you skip this step, you can create an onboard or external CA from the *Certificate Authority > Manage CA* page.

## RADIUS Server

To authenticate end-users, you must select a RADIUS server to sign client certificates. The Enrollment System provides an onboard RADIUS server, or you can use an external RADIUS.

FIGURE 17. RADIUS Server Selection



**RADIUS Server Selection** Skip Next >

To authenticate end-users, either the onboard RADIUS server or an external RADIUS server may be used.

- Use the onboard RADIUS server.**  
Select this option if you will be using the onboard RADIUS server.  
The following configuration parameters will be required when configuring the WLAN or switch to talk to the onboard RADIUS server:
  - RADIUS Address:** anna240.cloudpath.net
  - RADIUS Port:** 1812
  - RADIUS Acct Port (Optional):** 1813
  - Shared Secret:**
- Use an external RADIUS server.**  
Select this option if you will be using an external RADIUS server.
- Skip for now.**  
Select this option to skip this step for now.

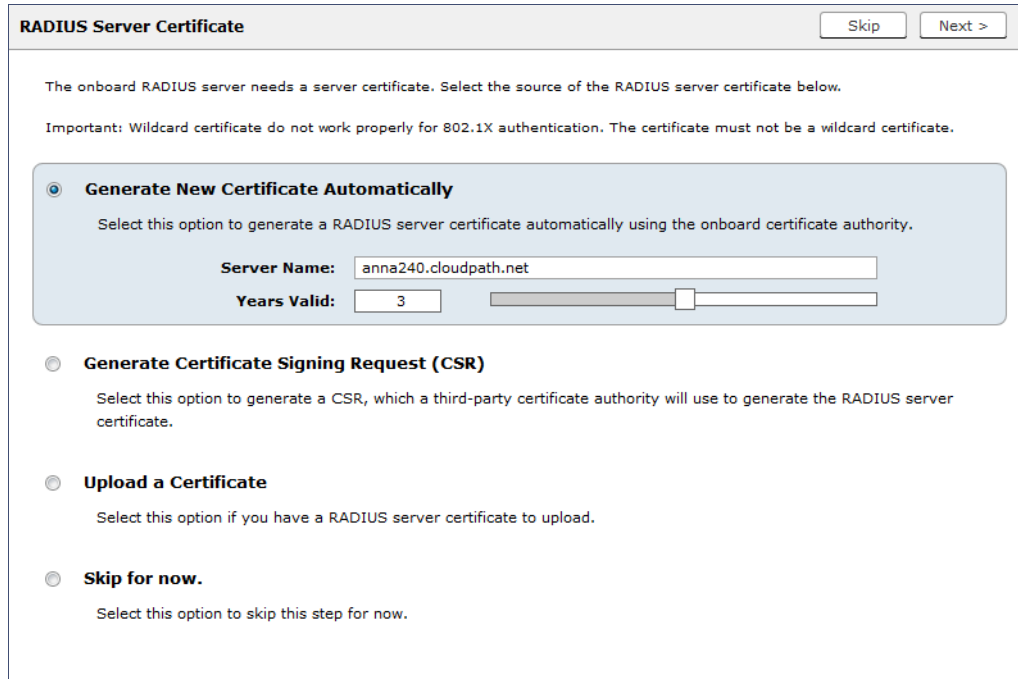
If you skip this step, you can set up a RADIUS server in the workflow.

## RADIUS Server Certificate

The Enrollment System onboard RADIUS server requires a server certificate. You can generate a RADIUS server certificate automatically using the ES onboard CA, generate a certificate signing request (CSR), which can be used by a third-party to generate the certificate, or upload an existing RADIUS server certificate.

If you choose to generate a certificate automatically using the onboard CA, the Server Name is pre-populated from the DNS Hostname, but can be modified. The RADIUS server certificate can be valid from 1 to 5 years.

FIGURE 18. RADIUS Server Certificate



**RADIUS Server Certificate** Skip Next >

The onboard RADIUS server needs a server certificate. Select the source of the RADIUS server certificate below.

Important: Wildcard certificate do not work properly for 802.1X authentication. The certificate must not be a wildcard certificate.

- Generate New Certificate Automatically**  
Select this option to generate a RADIUS server certificate automatically using the onboard certificate authority.  
**Server Name:**   
**Years Valid:**
- Generate Certificate Signing Request (CSR)**  
Select this option to generate a CSR, which a third-party certificate authority will use to generate the RADIUS server certificate.
- Upload a Certificate**  
Select this option if you have a RADIUS server certificate to upload.
- Skip for now.**  
Select this option to skip this step for now.

If you skip this step, you can upload the certificate from *Configuration > Advanced > RADIUS Server Component*.

## Set Up Workflow

To initialize the system with a sample configuration, select *Initialize for BYOD & Sponsored Guests*. This creates an initial workflow for BYOD users and sponsored guests 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 19. Setup Workflow

**System Setup**

**Setup Workflow** Skip Next >

The workflow may be initialized with a sample configuration or initialized blank. Select your preference below.

- Initialize for BYOD & Sponsored Guests.**  
Creates an initial workflow handling BYOD users and sponsored guests. Each user will be configured for the secure WPA2-Enterprise wireless network specified below and issued a certificate granting them guest or BYOD access.
- Start with Blank Canvas.**  
Creates a blank workflow.

## Publishing Tasks

After the code-signing step, 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.

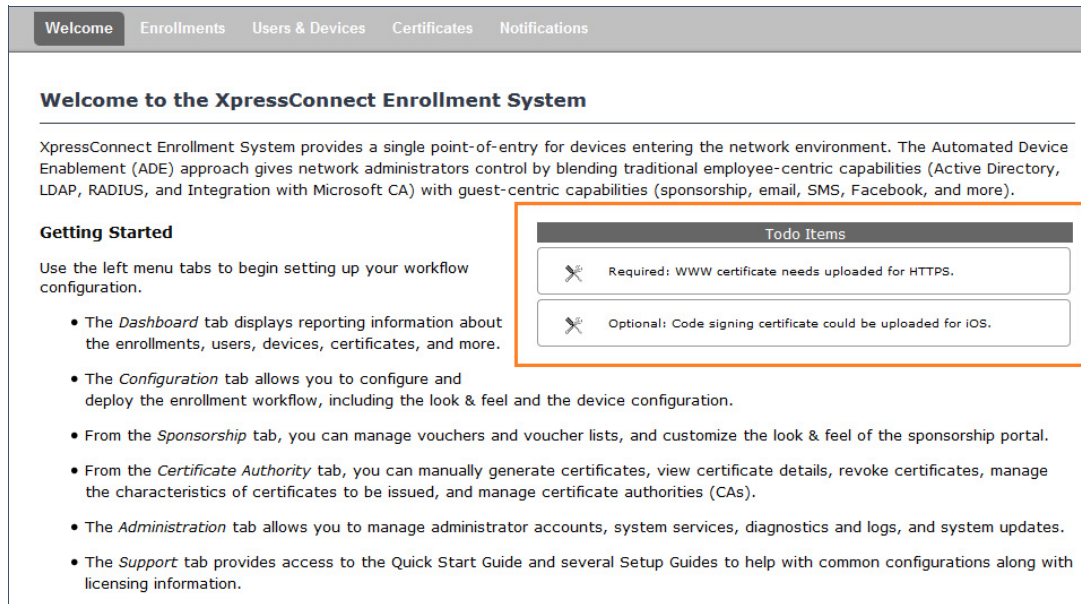
FIGURE 20. System Initialization Task

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.
<b>Access Point Setup:</b>	
	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:	h7w7mnb306qvmzgh3s
RADIUS Attributes:	BYOD Policy Template - VLAN: 'byod' Guest Policy Template - VLAN: 'guest'
<b>User Experience:</b>	
	End-users will use the enrollment portal to activate devices.
End-User Portal:	<a href="https://anna39.cloudpath.net/enroll/AnnaTest/Production/">https://anna39.cloudpath.net/enroll/AnnaTest/Production/</a>
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.
<b>Sponsor Experience:</b>	
	The default workflow utilizes sponsorship to authorize guests. To create vouchers for guests, sponsors can login to the sponsor portal below.
Sponsor Portal:	<a href="https://anna39.cloudpath.net/portal/sponsor/AnnaTest/">https://anna39.cloudpath.net/portal/sponsor/AnnaTest/</a>
Available Vouchers:	The following vouchers are currently available for use. Guest Vouchers - zjh, bvod, nvgv, nsic, kbllw
<b>Administrator Experience:</b>	
Administrator UI:	<a href="https://anna39.cloudpath.net/admin/">https://anna39.cloudpath.net/admin/</a>
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:	<a href="#">View Enrollments</a> - View information about enrolled devices, users, and policies. <a href="#">Configure Workflow</a> - 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 <a href="#">Add/Manage Administrators</a> - This page allows additional administrator logins to be setup. <a href="#">Deploy Snapshots</a> - After making changes to the workflow, go to Configuration -> Deploy and click <b>Create New Snapshot</b> to publish the changes to the enrollment portal. After the new snapshot is do force it to pull in the new snapshot. <a href="#">Look &amp; Feel</a> - To modify the look & feel, go to Configure Workflow link above and select the <b>Look &amp; Feel</b> 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 21. ES Welcome Page



**Welcome** | Enrollments | Users & Devices | Certificates | Notifications

## Welcome to the XpressConnect Enrollment System

XpressConnect Enrollment System 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).

### Getting Started

Use the left menu tabs to begin setting up your workflow configuration.

- The *Dashboard* tab displays reporting information about the enrollments, users, devices, certificates, and more.
- The *Configuration* tab allows you to configure and deploy the enrollment workflow, including the look & feel and the device configuration.
- From the *Sponsorship* tab, you can manage vouchers and voucher lists, and customize the look & feel of the sponsorship portal.
- From the *Certificate Authority* tab, you can manually generate certificates, view certificate details, revoke certificates, manage the characteristics of certificates to be issued, and manage certificate authorities (CAs).
- The *Administration* tab allows you to manage administrator accounts, system services, diagnostics and logs, and system updates.
- The *Support* tab provides access to the Quick Start Guide and several Setup Guides to help with common configurations along with licensing information.

#### Todo Items

- ✖ Required: WWW certificate needs uploaded for HTTPS.
- ✖ Optional: Code signing certificate could be uploaded for iOS.

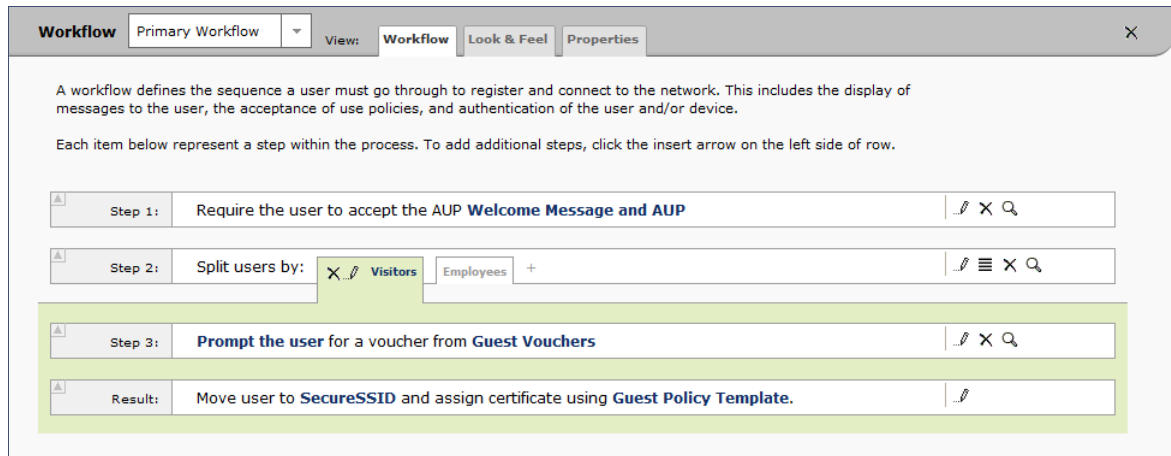
## Enrollment Workflow

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

The Enrollment System creates a basic workflow for BYOD users and sponsored guests, based on the settings entered during the initial system setup. You can use this workflow as is and start enrolling immediately, or you can modify the configuration, as needed.



FIGURE 22. Basic Workflow Configuration



To use the basic workflow, go to *Configuration > Deploy* to create a snapshot and deploy the workflow configuration. See *Deploying the Enrollment Workflow*.

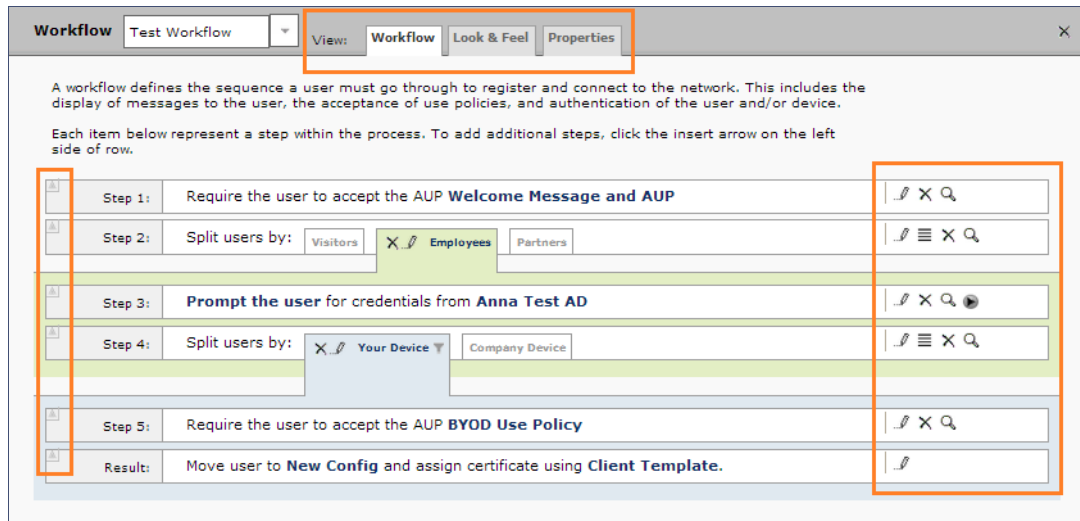
To modify the basic workflow, continue to the next section.

## 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 background and logos displayed on the XpressConnect Wizard during user enrollment.
- Use the *Properties* tab to enable/disable a configuration, or to modify the configuration Name and Description.

FIGURE 23. Enrollment Workflow Page



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

- Use the *Insert* arrows on the top left corner of each step to insert a new enrollment step. Alternately, you can click the blank space between two steps to insert a step.
- 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.

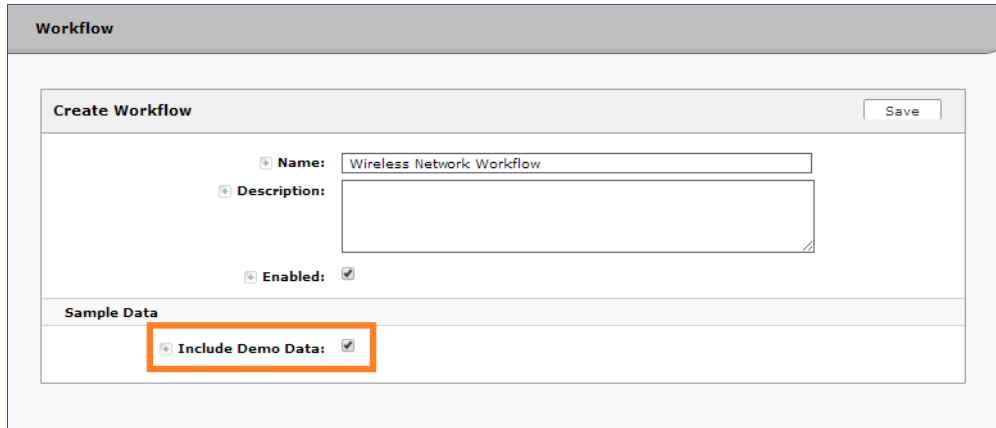
## Modifying a Workflow Template

You can modify a standard enrollment workflow template included in the application, or create a customized workflow one step at a time from a blank slate.

To create a workflow from a template:

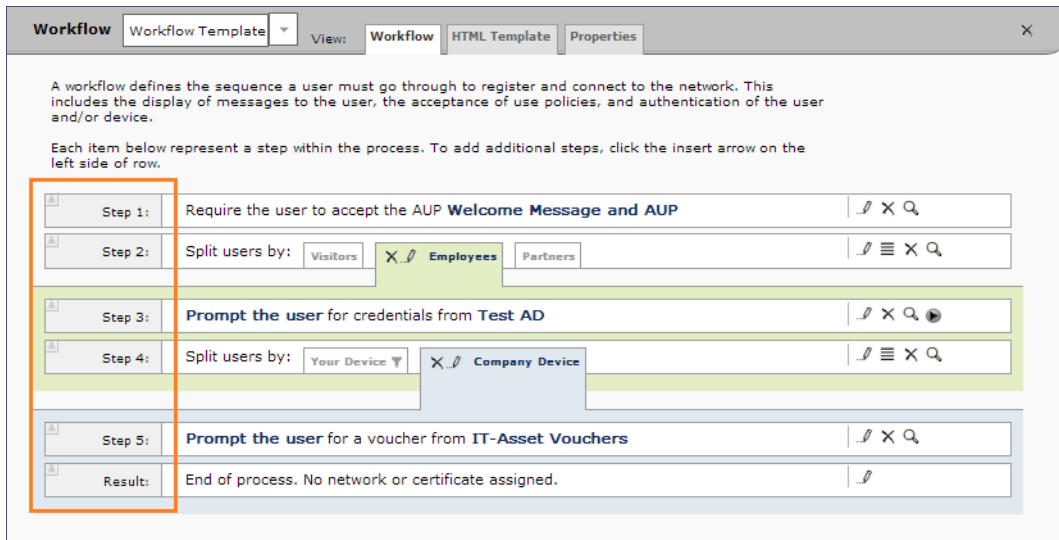
1. Go to *Configuration > Workflow*.
2. From the *Workflow* drop-down menu, select *Add New Workflow*.
3. On the *Create Workflow* page, enter a *Name* and *Description*. Select the check box for *Include Demo Data* and *Save*.

FIGURE 24. 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 25. Workflow Template



The workflow template contains basic workflow building blocks 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 Visitors, Employees, and Partners a different sequence of enrollment steps. 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 workflow contains the same steps as 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 to add to the enrollment workflow. Each time you add a step, this Step Selection page appears.

FIGURE 26. Enrollment Plug-in Selections

What type of step should be added to the workflow? Cancel Next >

- Display an Acceptable Use Policy (AUP).**  
 Displays a message to the user and requires that they signal their acceptance. This is normally used for an acceptable use policy (AUP) or end-user license agreement (EULA).
- Authenticate to a local server.**  
 Prompts the user to authenticate to an Active Directory server, and LDAP server, or a RADIUS server.
- Ask the user about concurrent certificates.**  
 Prompts the user with information about previously issued certificates that are still valid. This may suggest that old certificates be removed or may limit the maximum number of concurrent certificates.
- Split users into different branches.**  
 Creates a branch or fork in the enrollment process. This can occur (1) visually by having the user make a selection or (2) it can occur automatically based on criteria associated with each option. For example, a user that selects "Guest" may be sent through a different process than a user that selects to enroll as an "Employee". Likewise, an Android device may be presented a different enrollment sequence than a Windows device.
- Authenticate to a third-party.**  
 Prompts the user to authenticate via a variety of third-party sources. This includes internal OAuth servers as well as public OAuth servers, such as Facebook, LinkedIn, and Google.
- Authenticate using a voucher from a sponsor.**  
 Prompts the user to enter a voucher previously received from a sponsor. The sponsor generates the voucher via the Sponsor Portal, typically before the user arrives onsite.
- Perform out-of-band verification**  
 Sends the user a code via email or SMS to validate their identity.
- Request access from a sponsor.**  
 Prompts the user for a sponsor's email address and then notifies the sponsor. The sponsor can accept or reject the request via the Sponsor Portal.
- Register device for MAC-based authentication.**  
 Registers the MAC address of the device for MAC authentication by RADIUS. This is used for two primary use cases: (1) to authenticate the device on the current SSID via the WLAN captive portal or (2) to register a device, such as a gaming device, for a PSK-based SSID. In both cases, the MAC address will be captured and the device will be permitted access for a configurable period of time.
- Display a message.**  
 Displays a message to the user along with a single button to continue.
- Redirect the user.**  
 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 the user for information.**  
 Displays a prompt screen with customizable data entry fields.
- Authenticate via a shared passphrase.**  
 Prompts the user for a passphrase and verifies 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 DPSK via a Ruckus WLAN controller.
- Send a notification**  
 Generates a notification about the enrollment. Notification types include email, SMS, REST API, syslog and more. This step is invisible to the end-user.

## Acceptable Use Policy

Step 1 in the workflow requires a user 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 27. 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

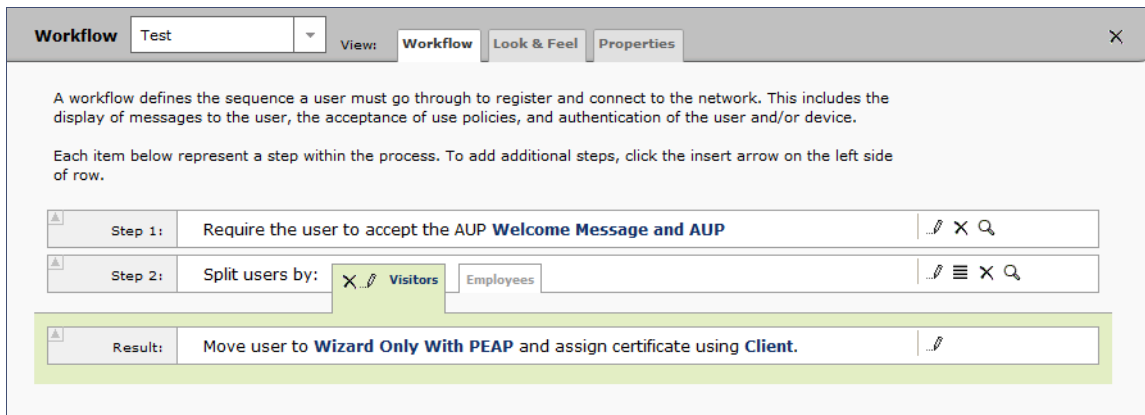
Step 2 in the workflow prompts for the type of user access.

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 28.** Workflow with User Type Split

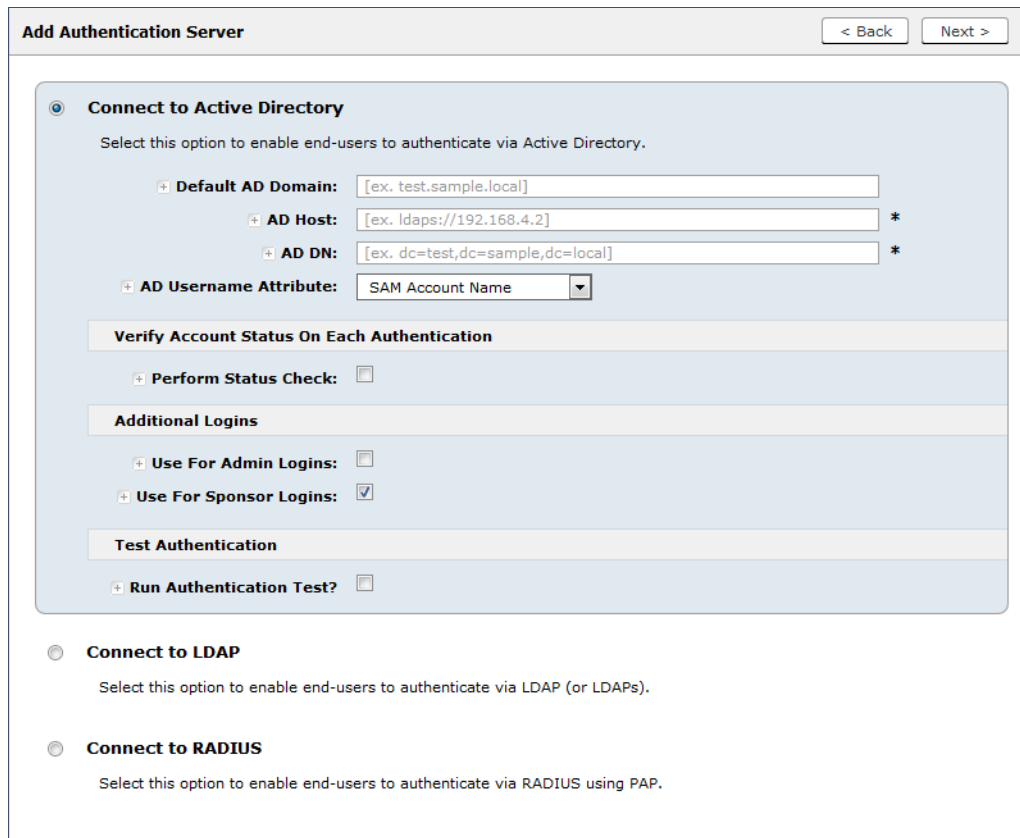


## Authentication to a Local Server

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 29. Add Authentication Server



**Add Authentication Server** < Back Next >

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

+ Default AD Domain: [ex. test.sample.local]

+ AD Host: [ex. ldaps://192.168.4.2] \*

+ AD DN: [ex. dc=test,dc=sample,dc=local] \*

+ AD Username Attribute: SAM Account Name

**Verify Account Status On Each Authentication**

+ Perform Status Check:

**Additional Logins**

+ Use For Admin Logins:

+ Use For Sponsor Logins:

**Test Authentication**

+ Run Authentication Test?

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

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

5. Select *Connect to Active Directory*, enter the appropriate data, and click *Next*.
6. Upload the server certificate (or pin the current server certificate).
7. Create a credential prompt for the authentication server, and Save.

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

You can run the authentication test at any time from the workflow, or from the *Configuration > 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*.



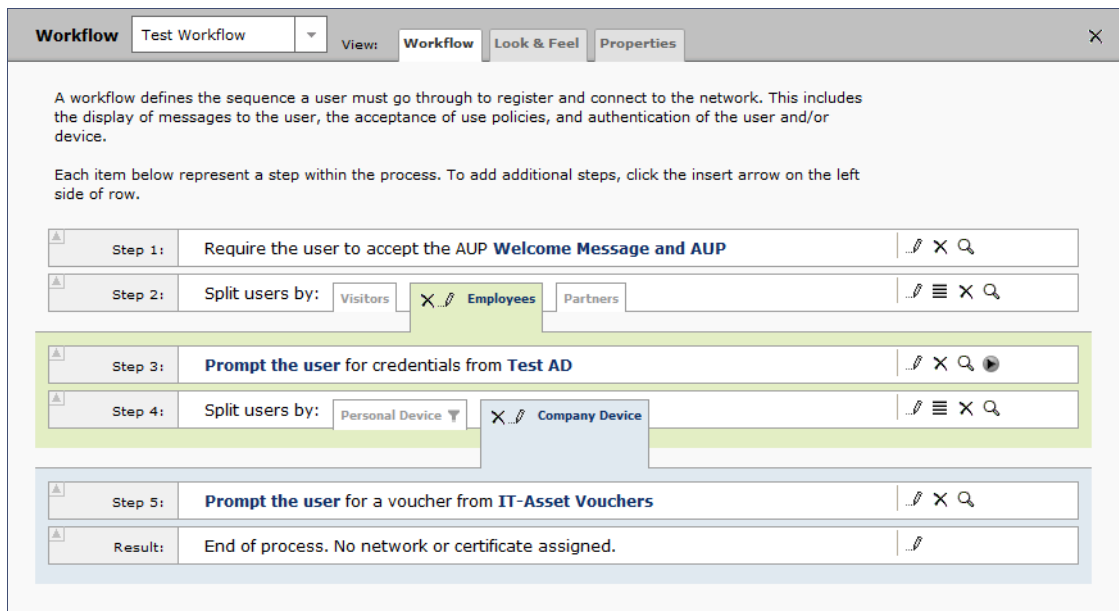
3. Select *Use an existing split* and choose *Device Ownership*. The *Device Ownership* option prompts the user to select either *Your Device* or *Company Device*. These labels can be modified.

### 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 30.** 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.

- On the right side of the step, click the *Edit List* icon to open the *Modify Options* page and configure the *Your Device* split. From this page, you can also set up filters for this split in the workflow.

FIGURE 31. Modify Selection Option

**Modify Option**
Cancel Save

**Sample User Display:**

**Display Title**

This is the Display Text field, which may contain multiple lines of text to describe this option.

---

**Webpage Display Information**

**Short Name:**

**Display Title:**

**Display Text:**

**Enabled:**

**Icon File:**

Default:	Using default file.
Upload:	<input type="button" value="Choose File"/> No file chosen

---

**Filters & Restrictions**

The following settings control which users will have access to this option. If nothing is specified below, all users will have access to this option. If criteria is specified below, only users meeting the criteria will have access to this option.

**User-Based Filters**

**Group Name Pattern:**

**Username Pattern:**

**User DN Pattern:**

**Email Pattern:**

**Device-Based Filters**

**Operating System Pattern:**

**User-Agent Pattern:**

**Location-Based Filters**

**Location Pattern:**

**Allowed IPs:**

**Blocked IPs:**

**Filters Based On Web Authentication Certificate**

**Common Name Pattern:**

**Issuer Pattern:**

**Template Pattern:**

**Expiration Date:** Expires Within

**Other Filters**

**Voucher List Name:**

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

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

---

**Note >>**

The settings in the *Filters & Restrictions* section control which users have access to a split option. If nothing is specified, all users have access to the split option. If criteria is specified, only users meeting the criteria have access to the split option.

---

## 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 32. Create Voucher List

Cancel < Back Next >

**Create Voucher List**

**Reference Information**

**Name:**  \*

**Description:**

**API ID:**

**Format**

**Length:**

**Characters:**

**Default Validity Length:**

**Default Days of Access:**

**Maximum Days of Access:**

**Require Username Match:**

**Notification**

**Email Subject:**

**Email Body:**

**SMS Subject:**

**SMS Body:**

**Sponsorship**

**Allow by LDAP Group:**  Matching

**Allow by LDAP Username:**  Matching

**Allow by LDAP Username DN:**  Matching

**Maximum Certificates:**

**Default Permissions:**

- Add/Edit/Delete Sponsors In Group
- Manage Devices Enrolled By Sponsor
- Manage Devices Enrolled By All
- Allow Bulk Creation

**New Sponsor Email Subject:**

**New Sponsor Email Template:**

**Fields Displayed To Sponsor**

**Name Field:**

**Company Field:**

**Email Field:**

**SMS Field:**

**Reason Field:**

**Redeem By Field:**

**Days of Access Field:**

**Initial vouchers**

**Initial Voucher #1:**

**Initial Voucher #2:**

**Initial Voucher #3:**

**Initial Voucher #4:**

**Initial Voucher #5:**

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.
  - Fields Displayed to Sponsors - Controls whether or not each field is displayed and, if so, whether or not it requires input from the sponsor.
  - 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

The last steps in the workflow are 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. Alternately, click the *Assign* link in the last step of the workflow.
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 WiFi networks list.
4. Select *Wireless Connections* (the default) and enter the *SSID* of the secure wireless network.

FIGURE 33. Configure SSID

The screenshot shows a web-based configuration interface titled "Add Device Configuration". At the top right, there are two buttons: "< Back" and "Next >". Below the title, a message states: "A single device configuration may support wireless and/or wired connections." This is followed by the instruction: "Select the connection method(s) this device configuration supports:". There are two radio button options: "Wireless Connections" (which is selected) and "Wired 802.1X Connections". Under the "Wireless Connections" section, there are four fields: "SSID:" with a text input containing "[ex. Sample Secure]" and an asterisk; "Authentication:" with a dropdown menu set to "WPA2-Enterprise"; "Encryption" with a dropdown menu set to "AES"; and "Is this SSID Broadcast?" with a dropdown menu set to "Yes, the SSID is broadcast.".

5. Set the *Authentication*, *Encryption*, and *Broadcast* settings and click *Next*.
6. Specify *Conflicting SSIDs*. This setting prevents the device from roaming away from the secure SSID to any open SSID in the area.
7. 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 34. Select OS Versions

**Add Device Configuration**
< Back    Next >

XpressConnect supports a wide array of operating systems. Select the operating system families and versions below that you wish to support within this device configuration. Individual versions may be enabled/disabled independently by editing the device configuration after it is created. Likewise, if you would like to restrict a version to a particular service pack level, you may do so after the device configuration is created.

---

**Automatically Configured OSes**  
These operating systems are automated, requiring minimal user interaction.

**iOS Versions:**

**Android Versions:**

**Windows (x86/x64) Versions:**

**Mac OS X Versions:**

**Chrome Versions:**

**Linux Versions:**

**Windows Mobile Versions:**

---

**Manually Configured OSes**  
These operating systems are require user interaction to configure. Online instructions will be provided to the user.

**Generic**

**Blackberry**

**Windows RT**

**Windows Phone 8+**

8. Select *Client will authenticate to the onboard RADIUS server.*

---

**Note >>**

See the Advanced Configuration for additional RADIUS server settings.

---

9. 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.

After you set up a device configuration for the workflow, you specify a new certificate template.

1. Select *A new certificate template*.
2. Select *Use an onboard certificate authority*. Select the CA to sign the client certificates.

---

**Note >>**

Typically, the client certificate is signed by the Intermediate CA. However, the client certificate can also be signed by the Root CA.

---

3. In this example, choose the Root CA that was created during the Enrollment System initial configuration. See Certificate Authority, page 16.
4. Set up the *Client* certificate template. This template is used to issue a certificate to the client device.



FIGURE 35. Client Certificate Template

What type of certificates should be issued? Cancel Next >

**Client Certificates**

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

**Username Decoration:**

- username@byod.company.com
- username@contractor.company.com
- username@faculty.company.com
- username@guest.company.com
- username@it.company.com
- username@student.company.com
- 

**Grant Access Until:**  Years  after issuance.

**Configure Advanced Options:**

**Lifecycle Notifications**

The XpressConnect Enrollment System supports events related to the lifecycle of the certificate. These events allow the system to interact with the end-user, the administrator, as well as external systems. Additional notifications can be configured once the template is created, but the notifications below are some of the most common ones.

**Notifications:**

- Send welcome email on issuance.
- Send email 7 days before certificate expiration.
- Send email if certificate is revoked.
- Email administrator if revoked certificate is used.

**RADIUS Options**

**VLAN ID:**

**Filter ID:**

**Class:**

**Server Certificates**

Used on servers, such as a RADIUS server, to identify the server to a client.

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.

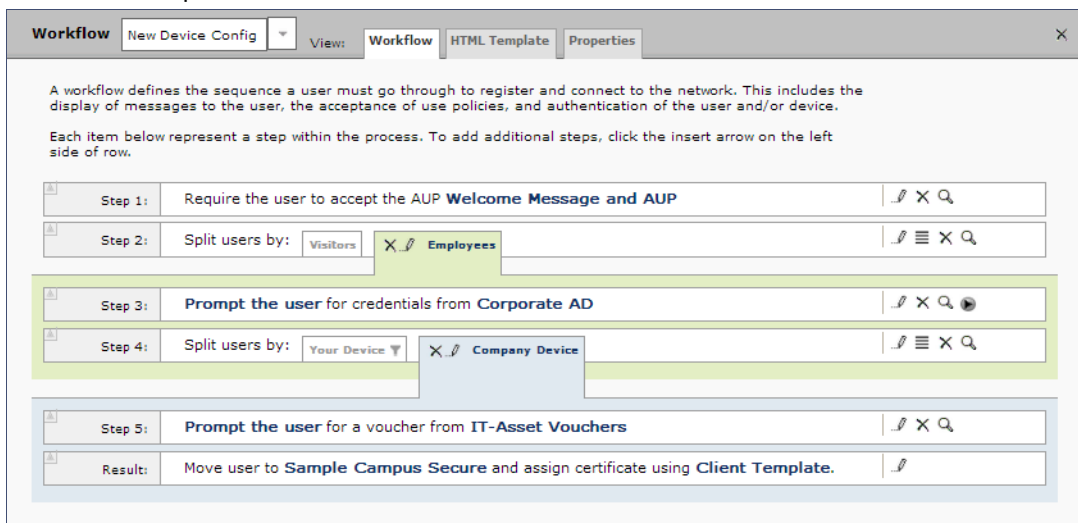
**Tip >>**

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 36.** 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 37. Deployment Locations

**Deployment Locations**

A deployment location represents a URL to where a workflow is deployed. Multiple locations may be used for a variety of reasons. For example, a production configuration may be deployed to /production, and a test configuration may be deployed to /test. Add Location

Location 1: Production ... ✕ ✓

**Enrollment URL:** <https://anna41.cloudpath.net/>  
or <https://anna41.cloudpath.net/enroll/AnnaTest/Production/> Change

**Sponsorship Login:** </portal/sponsor/AnnaTest/>

**Go To:** User Experience Sponsor Portal Get QR Code Explains Chrome Setup

**Snapshots:** Create New

	Name	Notes	Configuration	Version	Timestamp
🔍 ✕ 🟢	Snapshot 3		Demo Data	5.0.150	20141113 1115 MST
🔍 ✕ ⏻	Snapshot 2		Demo Data	5.0.150	20141113 1052 MST
🔍 ✕ ⏻	Snapshot 1		Demo Data	5.0.149	20141112 1000 MST

### Deployment Locations

A deployment location represents a URL to where a configuration is deployed. The Enrollment System 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 QR access the enrollment wizard.

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

FIGURE 38. 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 account 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 39. Create New Snapshot

3. Select the Workflow for the new snapshot.
4. Select the Wizard version to use for the new snapshot.
5. Verify the URL for the deployment.
6. Click *Create*.

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

When the snapshot is created and activated, select a deployment location to begin the network enrollment process.

### How to Test a 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).
4. Click the Go to: *User Experience* button to bring up the XpressConnect Wizard and test the enrollment process for the active configuration snapshot.

### QR Code

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. Once you have generated a QR code, it can be put on anything that a camera can see. This may include things like web sites, posters, instruction pages, and e-mail.

### Explain Chrome Setup

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 Enrollment System extension.

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

## System Administration

Access the Enrollment System *Administration* tab to manage system-related operations, using links in the following sections:

- **Administrators** - Manage administrators, group logins, restrict access to the ES Admin UI, and reset administrator passwords.
- **System** - View and manage system information, upgrade the application, and configure replication.

- **Advanced** - Manage system information, view logs (diagnostic and debug), configure SMS gateways and country codes, and clean up the database.

## Administrators

During the initial account setup, the Enrollment System sets up an administrator account using the *Company Information* provided during the setup. By default, there is also an *Administrator Group*, which allows administrative access to the Admin UI using credentials from the configured authentication server. This allows users that belong to a specific group to access the Enrollment System.

Manage administrator access to the ES Admin UI from *Administration > Administrators*.

**FIGURE 40.** Manage Administrators

The following individuals are administrators of the system. To create a new administrator, click the Add Admin button. To reset an administrators password, click the key icon. Add Admin

Admin 1: anna@cloudpath.net ⋮ ✕ 🔑

**Name:** anna@cloudpath.net  
**Username:** anna@cloudpath.net  
**Source:** Onboard  
**Role:** CA Administrator  
**Display Timezone:** Mountain Standard Time (MST7MDT)  
**Date Format:** YYYYMMDD hhmm z (20141230 2359 MST)  
**Last Login:** 20140324 1453 MDT

Admin 2: Groups in Anna Test AD ⋮

**Authentication Server:** Anna Test AD  
**State:** Administrators may login via this server.  
**Group Name Regex:** .\*

**Administrators:**

	Name	Distinguished Name	Last Login
⋮	anna	CN=Anna Eichel,CN=Users,DC=test,DC=cloudpath,DC=local	20140324
⋮	bob	CN=Bob,CN=Users,DC=test,DC=cloudpath,DC=local	20140324

## Administrator Roles

Cloudpath supports the following Administrator Roles:

- **CA Administrator** - Allows full configuration access to the Administrative UI. This administrator role can manage all administrative users.
- **Administrator** - Allows full configuration access to the Administrative UI, except for Certificate Authorities. This administrator can manage Administrator and Viewer administrative users.
- **Viewer** - Allows view-only access to Enrollment, User, and Certificate records on the Dashboard, the enrollment Workflow, and the Documentation and Licensing pages. This administrator cannot manage other administrative users.

## System








The Enrollment System provides access to all components of the system from the ES Admin UI.

Go to *Administration > System > System Services* to restart or view logs for the application server, web server, configure email or SMS servers, or start up a support tunnel. The *System* tab also allows you to upgrade the system or set up server clustering.

Access *System* operations from the following links:

- System Services - Start, stop, and restart servers, view or download log files, manage server certificates, manage SSH, open a support tunnel, and manage SMS and email services.
- System Updates - View and manage the Enrollment System build versions.
- Replication - Configure two or more servers for replication. The Enrollment System supports replication between two servers, for multiple data centers, and redundant servers.

FIGURE 41. System Services Page

Component:	Web Server	
<p><b>Web Server Status:</b> <span style="color: green;">●</span> Running (3910)</p> <p><b>Using HTTPS:</b> Yes <input type="button" value="Disable"/></p> <p><b>Version:</b> 4.2.2596</p> <p><b>Actions:</b> <input type="button" value="Restart Wwww"/> <input type="button" value="Restart App"/></p>		
<p><b>Web Server Certificate</b></p> <p><b>Common Name:</b> *.cloudpath.net <input type="button" value="Reapply"/></p> <p><b>Issuer Name:</b> Go Daddy Secure Certificate Authority - G2</p> <p><b>Validity:</b> 20150512 through 20180622</p> <p><b>Actions:</b> <input type="button" value="Upload WWW Certificate"/> <input type="button" value="Delete WWW Certificate"/></p>		
<p><b>Code Signing Certificate:</b> The web server certificate will be used. Alternately, a code signing certificate may be uploaded. <input type="button" value="Upload"/></p> <p><b>Restrict Admin UI To:</b> [Unrestricted]</p> <p><b>Enroll Session Timeout:</b> 1800 seconds.</p>		
Component:	Network	
Component:	SSH	
Component:	Support Tunnel	
Component:	Outbound Email	
Component:	Outbound SMS	
Component:	Logs	
Component:	External Reporting Server	
Component:	Virtual Machine	

- Web Server - Download the Apache Server access and error logs from the *Web Server* component. You can also Restart the web server, generate a CSR, edit administrative access

restrictions, and download or upload the web server certificate, or if needed, upload a code certificate.

- **Network** - The *Network* component displays network properties for the Enrollment System, and provides access to view or download the diagnostic logs.
- **SSH** - Use the *SSH* component to enable, disable or change the access port. SSH runs on ports 22 and 8022. You can set the port number using the command line or from the user interface. Even if you disable SSH access for both ports, SSH can continue to run.
- **Support Tunnel** - The *Support Tunnel* component allows you to open a support tunnel to help you in diagnosing issues with your application or configuration.
- **Outbound Email** - Use the onboard email provider or configure a local email server.
- **Outbound SMS** - Use the onboard SMS provider, enter a CDYNE account or route SMS message through a customer-owned account.
- **Logs** - Configure where syslog messages are sent. You can enable the syslog, select the protocol over which the syslog messages are sent, and enter a host and port number.
- **External Reporting Server** - Allows you to integrate ES enrollment data with a reporting server, such as the ELK stack (Elasticsearch, Logstash, and Kibana).
- **Virtual Machine** - Displays the system clock and system information about the virtual machine. You can also reboot or shut down the virtual machine from this page.

## Advanced Administration

The links in the *Administration > Advanced* section allow you to configure SMS gateways and country codes, and clean up the database. The ES also provides information about the system, including firewall requirements and system variables.

Advanced Operations include:

- **Company Information** - Used within the URL for enrollments and sponsorships, and included in the onboard CAs.
- **SMS Gateways** - Manage the SMS gateways available for the end-user to select for SMS messaging.
- **SMS Country Codes** - A list of the country codes available when entering the phone number for SMS messaging.
- **Variables** - A list of the enrollment-related variables available for use.
- **Data Cleanup** - Manage database cleanup thresholds for enrollment records, abandoned certificates, vouchers, notifications, manage wizard versions, and other system events.
- **Admin Console Link** - Displays the status of the link with the Licensing Server and displays legacy network configurations.
- **Firewall Requirements** - Displays inbound and outbound traffic of the Enrollment System to assist with firewall configuration.



---

## Advanced Configuration

---

The components listed in *Configuration > Advanced Configuration* are typically set up during the Initial System Setup, or during the workflow configuration, but can be modified as needed.

### Device Configurations

A device configuration is a group of configuration settings for a specified WLAN or wired network. Device Configuration settings are managed using the following tabs:

- Summary tab - An overview of the device configuration settings.
- Networks tab - WLAN settings, RADIUS server information and certificate chaining.
- OS Settings tab - User experience, network, and additional settings that are specific to an operating system or a specific version of an operating system.

### RADIUS Server

View and manage the onboard RADIUS server.

- RADIUS Server Status - View status, settings, and certificate information, generate a CSR, or upload a certificate. You can also download RADIUS server certificates and log files or export onboard CA information to be used to set up an external RADIUS server.
- Policies - View all policies for the onboard RADIUS server, including those assigned by certificate templates, eduroam configuration, and MAC registration policies.
- Clients - View all RADIUS allowed to call into the RADIUS server, including any eduroam clients.
- RADIUS Server and eduroam - Configure a eduroam federation server to interact with the onboard RADIUS server.
- Attributes - Define the RADIUS attributes that will be visible in the system. These attributes, which are included in the Access-Accept/Reject reply from the RADIUS server, can be added to the certificate template, MAC registration, and eduroam configuration.

### Authentication Servers

View and manage the servers against which users may be authenticated. This includes local servers such as Active Directory and LDAP, as well as third-party services, such as Facebook.

### MAC Registrations

View and manage MAC registrations, which allow network access to devices that do not have the 802.1X supplicant capability. The ES provides a template for importing MAC address in bulk using a .csv or .xlsx file.

### API Keys

A list of the APIs currently in use with the Enrollment System. The REST APIs allow the system to actively notify external systems and to be queried and manipulated by external systems.

## Dashboard

The Enrollment System dashboard provides detailed information about the number and status of enrollments on your network, including notifications, events, certificates, MAC registrations, and scheduled reports.

## Enrollments

The *Enrollments* table allows you to review enrollments, including the associated user, device, and certificate information. The *Enrollment Paths* tab shows a graphical depiction of the different paths taken by users during the enrollment process.

FIGURE 42. Enrollments Table

Enrollments		Enrollment Paths										
Assistance ID	Enrollment Status	Name	Timestamp	Selections	Operation System	MAC Address	Device Name	Location	Company Name	Thumbnail	Voucher List	Auth Type
9F44	Configuration Complete - Certificate Issued		20140401 1327 MDT	Mac Reg	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		@byod.company.com	6462_0101		
7973	Certificate Issued	bill	20140331 1640 MDT	Employees	Mac OS X (iPad)		Apple Inc. Mac OS X (iPad)	Corporate	destroy@other.company.com	F3E0_81AD	IT-Asset Vouchers	Active Directory
F90E	Certificate Issued		20140331 1637 MDT	Mac Reg	Mac OS X (iPad)		Apple Inc. Mac OS X (iPad)		@byod.company.com	306C_BCCB		
355A	Configuration Complete - Certificate Issued		20140331 1634 MDT	Mac Reg	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		@byod.company.com	8A59_3999		
8815	Configuration Complete - Certificate Issued	anna	20140331 1628 MDT	Employees - Your Device	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		anna@byod.company.com	2333_8A20		Active Directory
361P	Configuration Complete - Certificate Issued	anna	20140331 1627 MDT	Employees	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		destroy@other.company.com	5890_0E23	IT-Asset Vouchers	Active Directory
8720	Configuration Complete - Certificate Issued	bob	20140331 1626 MDT	Employees - Your Device	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		bob@byod.company.com	F234_7487		Active Directory
901F	Configuration Complete - Certificate Issued		20140331 1626 MDT	Mac Reg	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		@byod.company.com	6448_EBC2		
0CFC	Configuration Complete - Certificate Issued	mark	20140331 1625 MDT	Employees	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		destroy@other.company.com	EF8F_7880	IT-Asset Vouchers	Active Directory
6893	Configuration Complete - Certificate Issued	anna	20140331 1625 MDT	Employees	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		destroy@other.company.com	C103_0305	IT-Asset Vouchers	Active Directory
C642	Configuration Complete - Certificate Issued	lynn	20140331 1624 MDT	Employees	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		destroy@other.company.com	E74E_31F6	IT-Asset Vouchers	Active Directory
6826	Configuration Complete - Certificate Issued	bill	20140331 1623 MDT	Employees	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC	Corporate	destroy@other.company.com	19A3_D993	IT-Asset Vouchers	Active Directory
C6A7	Configuration Complete - Certificate Issued	mike	20140331 1622 MDT	Employees	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		destroy@other.company.com	E429_E5E9	IT-Asset Vouchers	Active Directory
0CFC	Configuration Complete - Certificate Issued	mark	20140331 1621 MDT	Employees	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		destroy@other.company.com	5899_81E4	IT-Asset Vouchers	Active Directory
379D	Configuration Complete - Certificate Issued	bob	20140331 1621 MDT	Employees - Your Device	Windows 7	E0-06-E6-C3-8A-B5	ANNA-PC		bob@byod.company.com	DF5E_659F		Active Directory

### Tip >>

Use the view icon to display further details about a specific enrollment record, to revoke a certificate, or to remove the enrollment record from the database.

## Records Export

Enrollment and User data can be downloaded, as a CSV file or Microsoft Excel spreadsheet.

Use the CSV Export icon  or XLS Export icon  located at the bottom of the table.




By default, the Enrollment data files are named *enrollments.txt* or *enrollment.xls* and the User data files are named *users.txt* or *users.xls*.

The Enrollment and User export files are designed to be a quick view of the activity since midnight. To export only certain items in the table, for a specific date and time, or to export items for a longer time period, see Scheduled Reports.

**FIGURE 43.** Download Enrollment Records

Filters:  Show unauthorized.  Show authorized but unused.  Show issued.  Show abandoned.  Show revoked.  Show expired.

Assistance ID	Enrollment Status	Name	Timestamp	Selections	Operating System	MAC Address	Device Name	Location	Common Name	Voucher List	Authentication Type
DB4F	In Progress	annae	20140311 2143	Employees - Company Device	Windows 7					IT-Asset Vouchers	Active Directory
EE34	Configuration Complete - Certificate Issued	Anna Eichel	20140311 2142	Visitors	Windows 7	E0:06:E6:C3:8A:85	ANNA-PC		Anna Eichel@byod.company.com		Google
9DA9	In Progress	annae	20140311 2142	Employees - Your Device	Windows 7						Active Directory
1615	Abandoned	annae	20140311 1654	Employees - Your Device	Windows 7						Active Directory

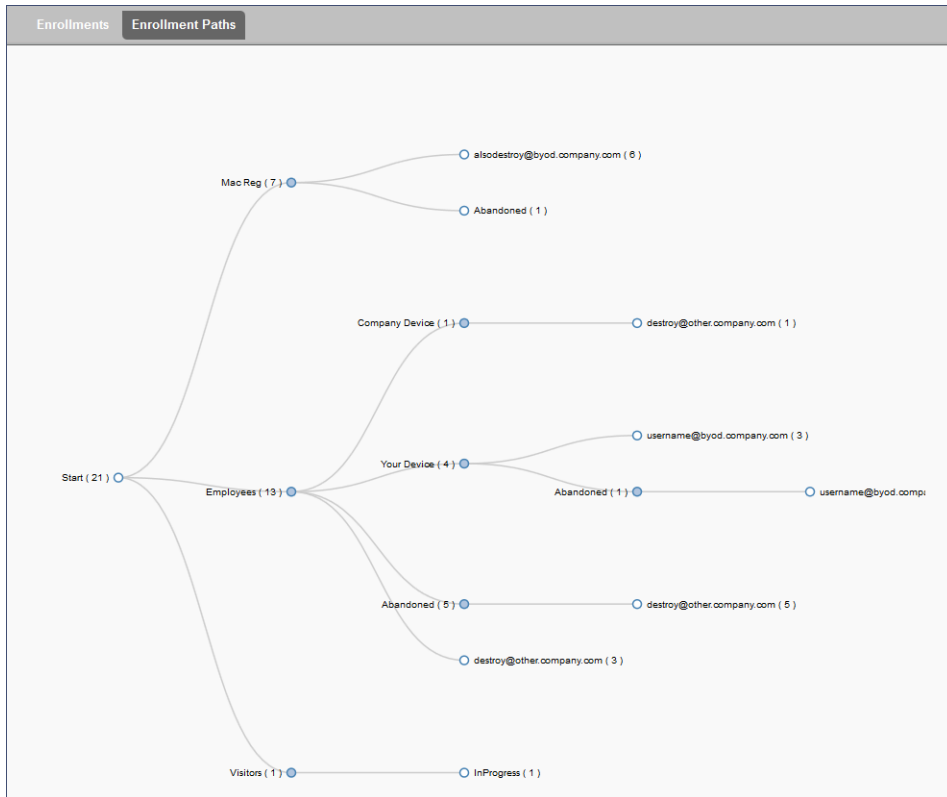
Results 1 - 4 of 4. 15   

## Enrollment Paths

During enrollment, the user is taken through a sequence of steps, called an enrollment workflow. The workflow depends on the selection chosen when the user is prompted, and on any configured filter in the workflow. For example, the user can select the Employee or Guest path, and then be moved to the IT Asset device path, because their Active Directory credentials, by way of a filter, caused them to be moved to the Personal Device path.

The Enrollment Paths tab shows a graphical depiction of the paths taken by users during the enrollment process.

FIGURE 44. Enrollment Path



## Users & Devices

The *Users* table provides a list of User records, including user devices, enrollment paths, and certificate information for each user.

FIGURE 45. User Table

Users    Device Types    Form Factors    MAC Registrations							
	Status	Photo	First Name	Last Name	Server Name	Authentication Type	Timestamp
🔍			Anna	Eichel	LinkedIn, Facebook, or Gmail	Google	20140326 1006 MDT
🔍			Anna	Eichel	Anna Test AD	Active Directory	20140326 1335 MDT
🔍			Bob	Johnson	Anna Test AD	Active Directory	20140326 1344 MDT
🔍			Bill	Smith	Anna Test AD	Active Directory	20140326 1348 MDT
🔍			Mark	Test	Anna Test AD	Active Directory	20140326 1415 MDT
🔍			Lynn	Test	Anna Test AD	Active Directory	20140326 1415 MDT
🔍			Mike	Test	Anna Test AD	Active Directory	20140331 1622 MDT
🔍			Anna	Test	Anna Test AD	Active Directory	20140331 1625 MDT
🔍			Anna	Eichel	LinkedIn, Facebook, or Gmail	Google	20140331 1638 MDT

Results 1 - 9 of 9. 15

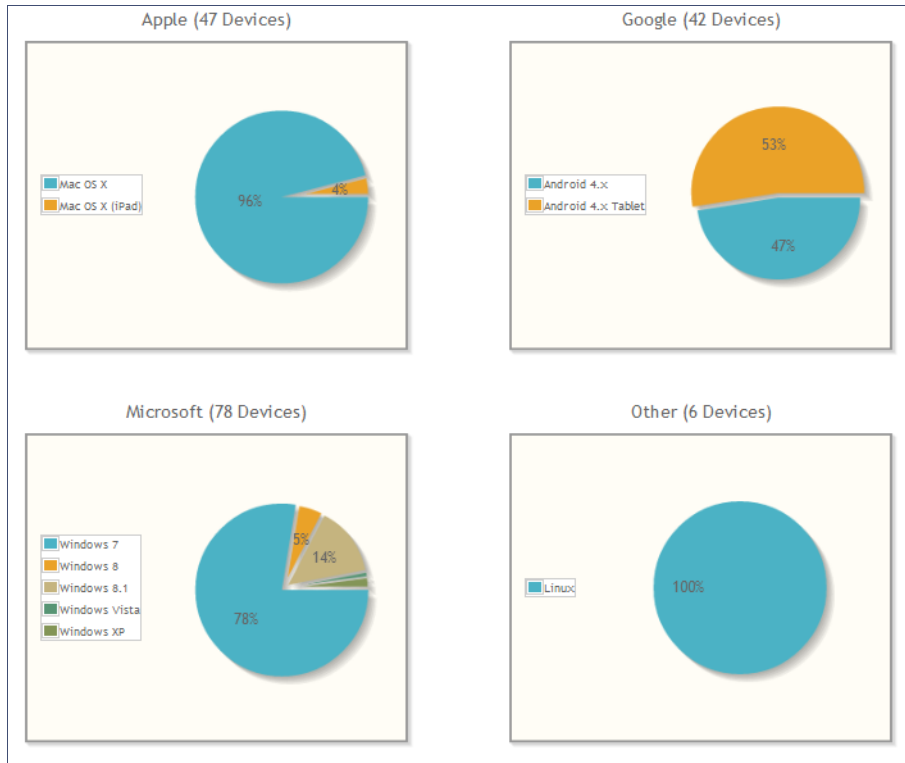
**Tip >>**

Use the view icon to display further details about a specific user record, to block the user, or to remove the user record from the database.

**Device Types**

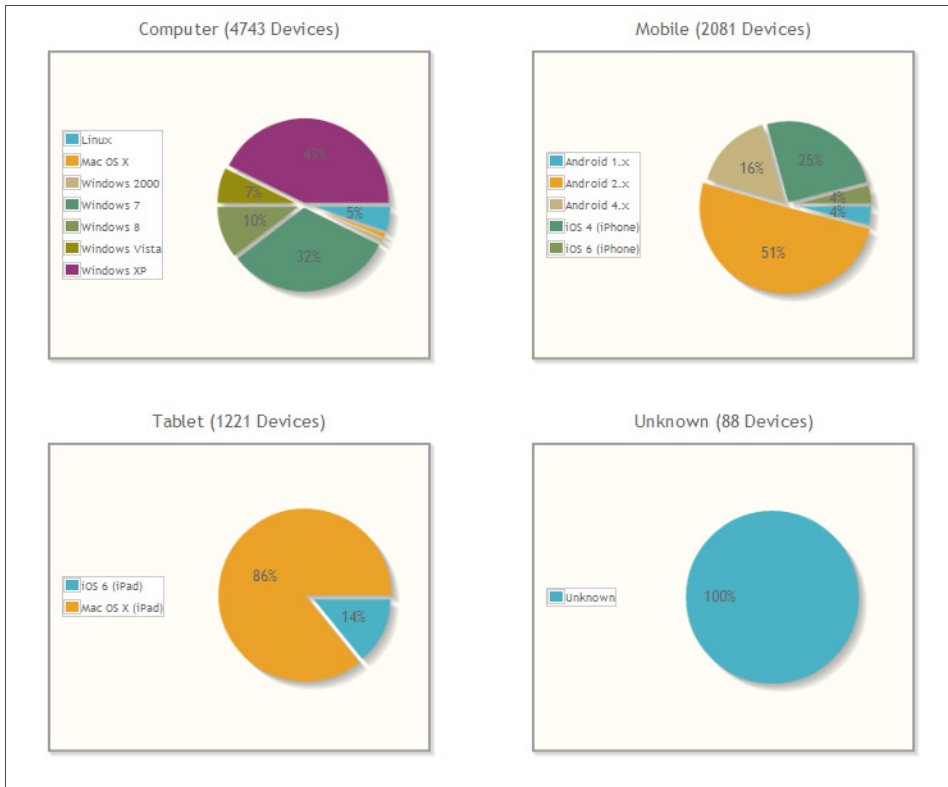
The device type information is obtained from user-agent during the initial enrollment attempt. The device types graphs show the enrollments by operating system.

FIGURE 46. Device Types



### Form Factors

The form factor is obtained from device user-agent during the initial enrollment attempt. The form factor graph displays the device type, such as computer, tablet, or mobile phone.

**FIGURE 47. Device Form Factors**

## MAC Registrations

The *MAC Registration* table displays all devices that have been registered using the MAC address instead being enrolled using a certificate.

## Certificates

The Enrollment System issues client certificates to users based on the templates set up for specific users and devices. Server certificates can be issued for the RADIUS server, web server, or other external server in your network. The active certificates graph displays, by date, the number of active (not expired) client and server certificates, and from which template they were issued.

## Certificates Table

The *Certificates* table lists all server and client certificates issued by the onboard CA. Use the *Active*, *Revoked*, *Expired*, and *All* tabs to filter the data in the table.

## Certificates Table

Active Certificates										
Revoked Expired All Active Trends Expiring Trends										
Status	Common Name	Timestamp	Expiration Date	CA Name	Template	Email	Revocation Date	Thumbprint	Last OCSP Date	
Q X	mark@byod.company.com	20140402 1056 MDT	20150402	Anna Test Intermediate CA 1	username@byod.company.com			52CD...C610	20140402 1056 MDT	
Q X	anna@byod.company.com	20140402 1054 MDT	20150402	Anna Test Intermediate CA 1	username@byod.company.com			1BCC...1B27	20140402 1054 MDT	
Q X	anna@byod.company.com	20140401 1415 MDT	20150401	Anna Test Intermediate CA 1	username@byod.company.com			AA51...E2DA	20140401 1415 MDT	
Q X	lynn@byod.company.com	20140401 1402 MDT	20150401	Anna Test Intermediate CA 1	username@byod.company.com			D472...768D	20140401 1402 MDT	
Q X	bob@byod.company.com	20140401 1351 MDT	20150401	Anna Test Intermediate CA 1	username@byod.company.com			EC1A...1554	20140401 1351 MDT	
Q X	AnnaTest.cloudpath.net	20140401 1342 MDT	20170401	Anna Test Root CA 1	Server Template	it@company.com		B2D4...45E1	20140401 1342 MDT	

Results 1 - 6 of 6. 15

### Tip >>

Use the view icon to display further details about a specific certificate record, to disable or revoke the certificate, to download the certificate, or to remove the user record from the database.

## Active Trends

The *Active Certificates* graph displays, by date, the number of active (not expired) client and server certificates, and from which template they were issued.



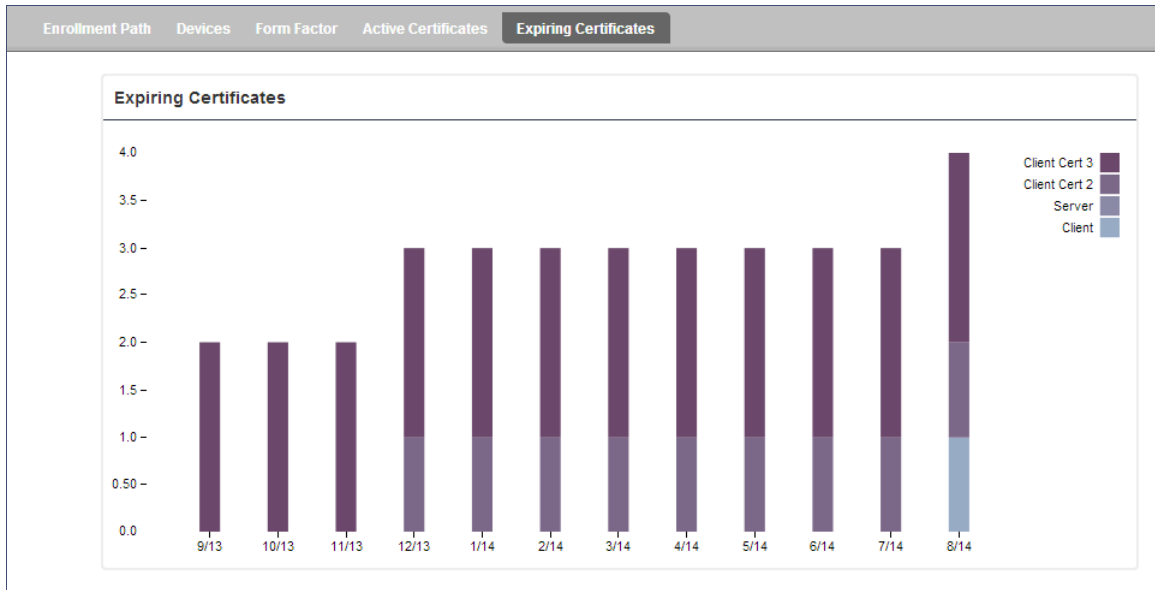
FIGURE 48. Active Certificates



### Expiring Trends

The validity period of certificates issued by the Enrollment System is derived from the certificate template used when the certificate was issued. The *Expiring Certificates* graph displays, by date, the number of client and server certificates that are about to expire, and from which template they were issued.

**FIGURE 49.** Expiring Certificates



## Notifications

The *Notifications* tab allows you to review emails and SMS messages, event logs, and schedule reports.

### Notification Records

The *Notifications* table displays email and SMS notifications that have been sent by the system. The system logs email and SMS notifications sent for sponsors, messages for vouchers, network access, and certificate issuance or revocation.

**FIGURE 50.** Notifications Table

Notifications					
Events Schedule Reports					
Type	Address	Last Known Status	Timestamp	Email Subject	
🔍	anna@cloudpath.net	Email sent.	20140401 0913 MDT	Verification Code for Network Access	
🔍	anna@cloudpath.net	Email sent.	20140401 0841 MDT	test notification	

Results 1 - 2 of 2. 15

## Events

The *Events* log displays all system events, such as account logins, enrollments, acceptance of AUPs, registrations, certificate issuance, errors, account updates, and snapshot creation.

## Scheduled Reports

The scheduled report feature allows you to schedule a task to export enrollment record data, by date, or schedule a recurring export. For example, you might schedule an enrollment data report to occur on a weekly, or daily basis. This report can be emailed to one or multiple email addresses.

You can schedule multiple reports. For example, you can create a report that emails an enrollment record report based on enrollments with revoked certificates, and another based on issued certificates.

To schedule a task:

1. Go to *Dashboard > Notifications > Scheduled Reports*.
2. On the *Scheduled Reports* page, click *Add Scheduled Report*.

**FIGURE 51.** Schedule Enrollment Records Export

**Modify Scheduled Report** Cancel Save

**Name:**

**Description:**

**Enabled:**

**Email**

**Email Addresses:**

**Email Subject:**

**Schedule**

**Frequency:**  ▼

**Time:**  MDT

**Enrollment Status To Include**

**Include Abandoned?**

**Include Authorized?**

**Include Expired?**

**Include Initiated?**

**Include Certificate Issued?**

**Include Rejected?**

**Include Revoked?**

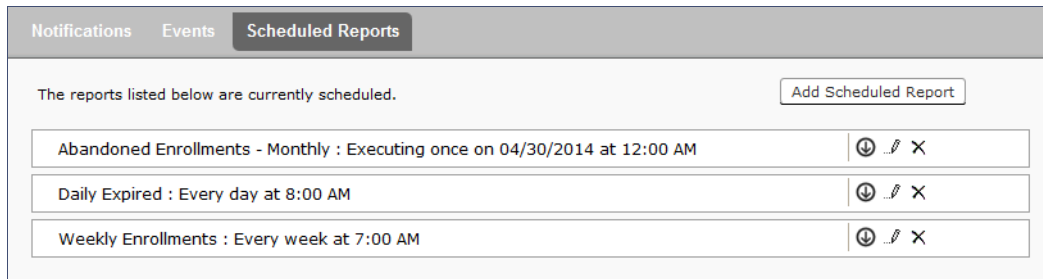
**Include In Progress?**

**Report Content**

**Columns To Include:**  ▼

3. On the *Modify Scheduled Report* page, enter the *Name*, *Description*, *Email Address* and *Subject* for the recipient of the enrollment records report. You can enter multiple email addresses, separated by commas.
4. Specify when task is to be run. The execution period can be a specific date or you can set up a recurring report to be emailed daily, weekly, or monthly.
5. In the *Enrollment Status To Include* section, check the information to be included in the report. For example, select *Certificate Issued* and *Enrollment Complete* to create a report that shows the number of devices that have successfully onboard to the network.
6. Specify the *Report Content*, which determines the data columns that will be included in the report.
7. Save the scheduled task.

**FIGURE 52.** Scheduled Reports



The enrollment record data is emailed, as a CSV file, to the specified address, at the scheduled frequency. You can also download an interim report from this page.

## Event Response

Use the *Event Response* page to block a large number of enrollments or users, or revoke certificates in bulk using information in an uploaded Excel (xls or xlsx) spreadsheet.

FIGURE 53. Event Response

Event Response
<p>This page allows items to be revoked or unrevoked in bulk via an uploaded Excel (xls, xlsx, or csv) spreadsheet. The spreadsheet can be filtered and downloaded from the respective View-All page (with additional filtering possible within Excel) or generated separate from the system.</p>
<p><b>Block Enrollments By Upload</b></p> <p>This option allows enrollments (and their related certificates) to be blocked or unblocked via an uploaded Excel file. Each row is processed using the following column headers, in order of preferences and case insensitive: Pk, GUID, Name, Enrollment Email, MAC Address.</p> <p><b>Upload File To:</b> <input type="button" value="Block Enrollments"/> <input type="button" value="Unblock Enrollments"/></p>
<p><b>Revoke Certificates By Upload</b></p> <p>This option allows certificates to be revoked or unrevoked via an uploaded Excel file. Each row is processed using the following column headers, in order of preferences and case insensitive: Certificate Pk, Full Serial Number, Serial Number, Common Name</p> <p><b>Upload File To:</b> <input type="button" value="Revoke Certificates"/> <input type="button" value="Unrevoke Certificates"/></p>
<p><b>Block Users By Upload</b></p> <p>This option allows users (and their related devices) to be blocked or unblocked via an uploaded Excel file. Each row is processed using the following column headers, in order of preferences and case insensitive: DN, CN, Username, Email</p> <p><b>Upload File To:</b> <input type="button" value="Block Users"/> <input type="button" value="Unblock Users"/></p>

The Excel spreadsheet, which is a file of enrollment records, can be filtered and downloaded from the *Dashboard > Enrollments (or Certificates)* page, allows you block/unblock users or enrollments, or revoke/unrevoke certificates.

## About Cloudpath

Cloudpath Networks, Inc. provides Automated Device Enablement (ADE) solutions that simplify the adoption of standards-based Wi-Fi security, including WPA2-Enterprise, 802.1X, and X.509, in diverse BYOD environments. Founded in 2006, Cloudpath Networks invented the modern onboarding model for personal devices and continues to drive the industry's adoption of standards-based security en masse. The Cloudpath XpressConnect solutions are proven worldwide to bring simplicity to secure networks through automated and easy-to-use form and function. To learn more, visit ([www.cloudpath.net](http://www.cloudpath.net)).

## Contact Information

**General Inquiries:** [info@cloudpath.net](mailto:info@cloudpath.net)

**Support:** [support@cloudpath.net](mailto:support@cloudpath.net)

**Sales:** [sales@cloudpath.net](mailto:sales@cloudpath.net)

**Media:** [media@cloudpath.net](mailto:media@cloudpath.net)

**Marketing:** [marketing@cloudpath.net](mailto:marketing@cloudpath.net)

**Phone:** +1 303.647.1495 (US)

+1 866.472.6053 (US)

+44 (01) 161.261.1400 (UK)

**Fax:** +1 760.462.4569

**Address:** 1120 W 122nd Ave, Suite 302

Westminster, CO 80234 USA