

XpressConnect Enrollment System

Deployment Guide

Software Release 4.2

December 2015

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

Document Type: Planning

Audience: Network Administrator



XpressConnect Enrollment System Deployment 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.

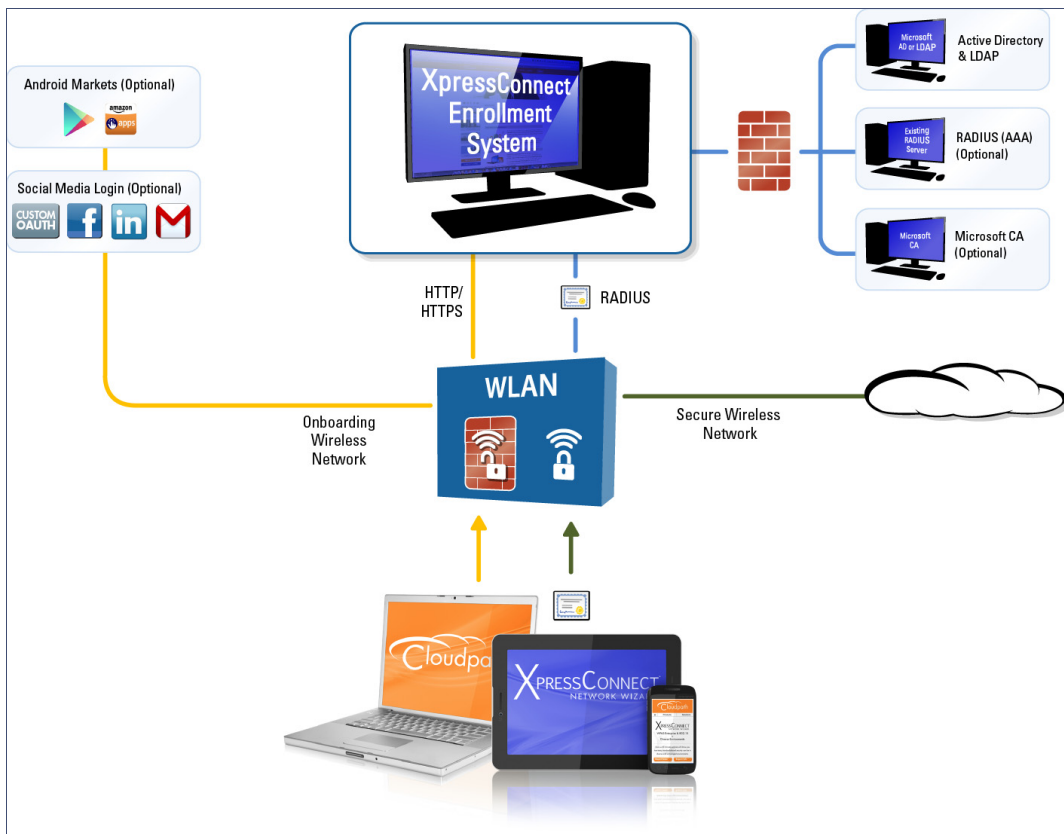
XpressConnect Enrollment System Deployment Guide

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



What is the Enrollment System

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

Secure onboarding capabilities include:

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

Advanced Certificate Management capabilities include:

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

Why You Need the Enrollment System

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

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

Guest Users

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

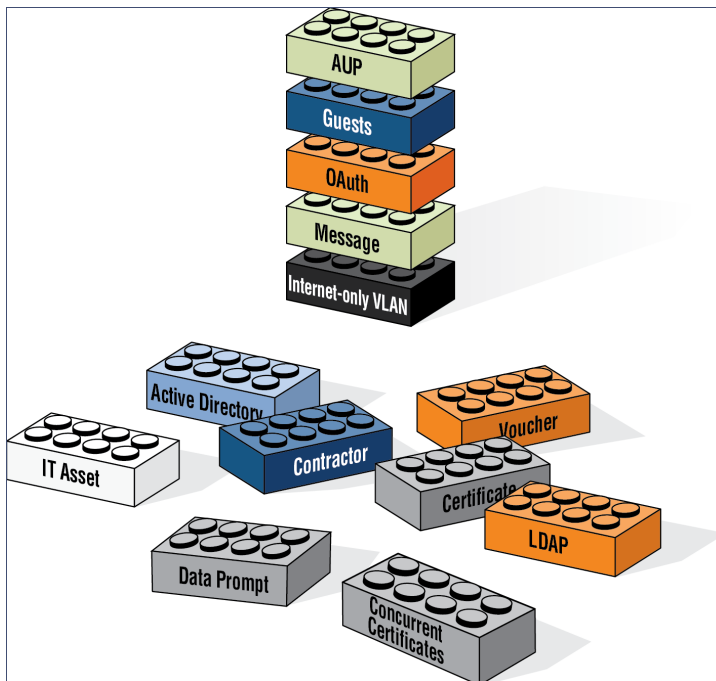
Workflow Engine

The 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.

Workflow Building Blocks

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

FIGURE 2. Basic Workflow



Available Workflow Plug-Ins

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

Display an Acceptable Use Policy

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

Authenticate to a Local Server

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

Ask the User About Concurrent Certificates

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

Split Users Into Different Workflow Branches

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

Authenticate to a Third-Party

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

Authenticate Using a Voucher From a Sponsor

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

Perform Out-of-Band Verification Using Email or SMS

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

Request Access From a Sponsor

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

Register a Device for MAC-Based Authentication

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

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

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

Display a Message To Users

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

Redirect Users to an External URL

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

Prompt User For Information

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

Authenticate Using a Shared PassPhrase

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

Generate a Ruckus DPSK

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

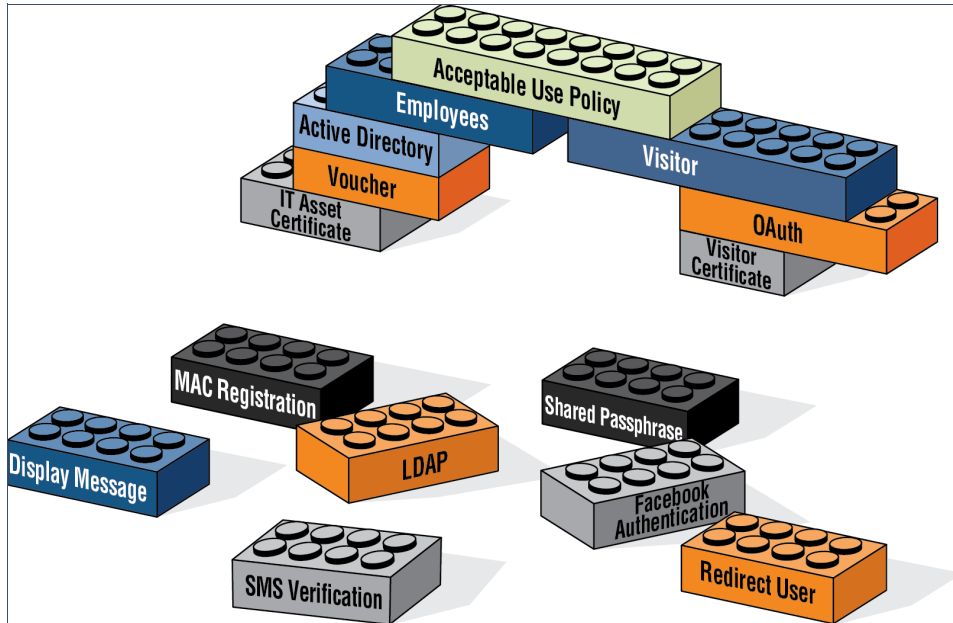
Send a Notification

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

Example Workflow with Two Branches

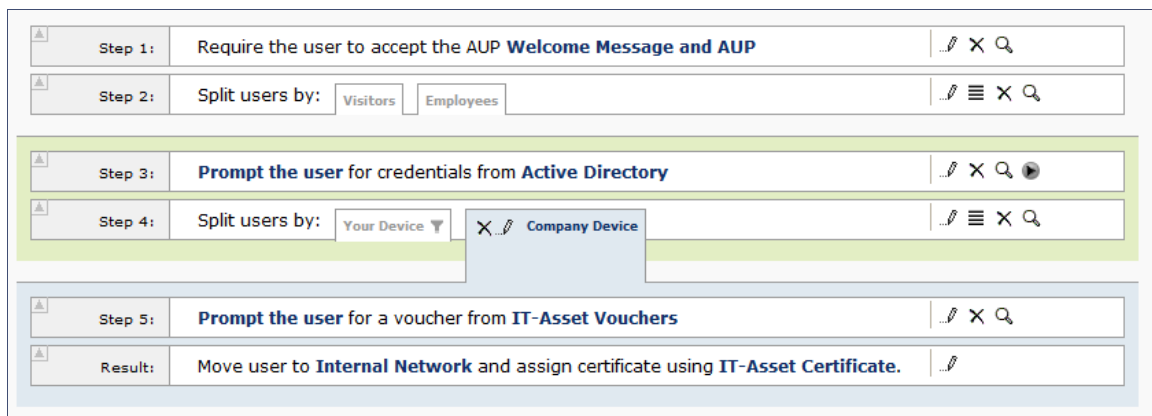
The following image represents a workflow that is split into two branches, with one sequence of steps for employees, and another for guest users. Each branch in the workflow specifies a different authentication method and assigns different certificates to the user.

FIGURE 3. Workflow With 2 Branches



The model workflow above translates to the following example workflow in the Enrollment System.

FIGURE 4. Enrollment System Simple Workflow

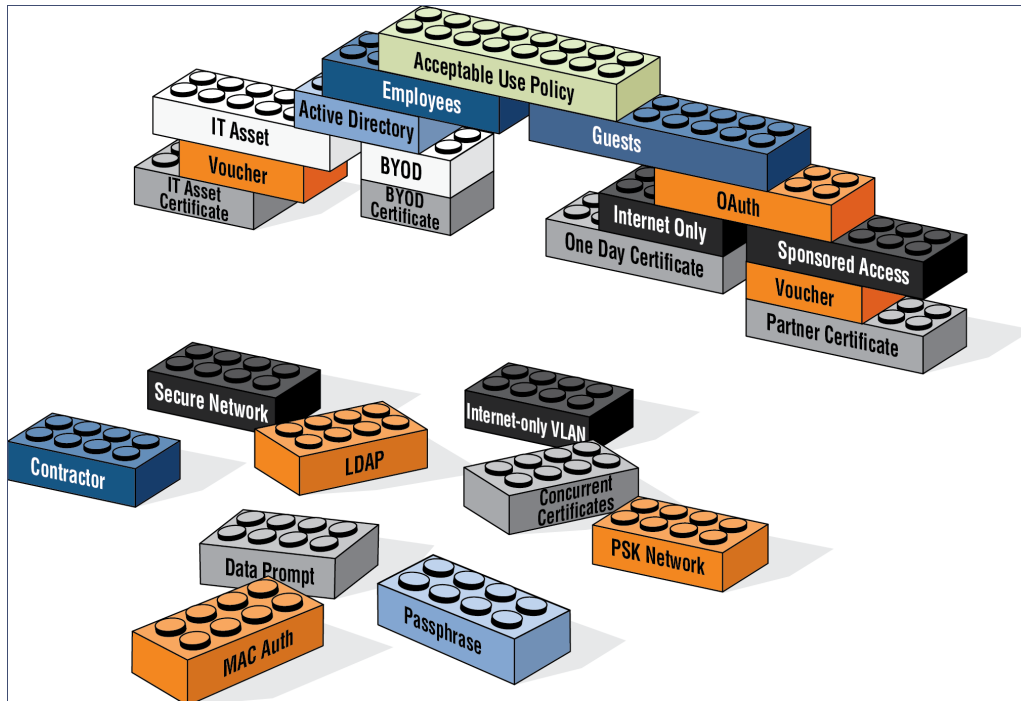


After the workflow is in place, you can fine-tune settings for specific OS versions, updates, and features, including customizations to the user experience. See Device Configuration and Client Certificate.

Example Complex Workflow

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

FIGURE 5. Complex Workflow



Enrollment Workflow Use Cases

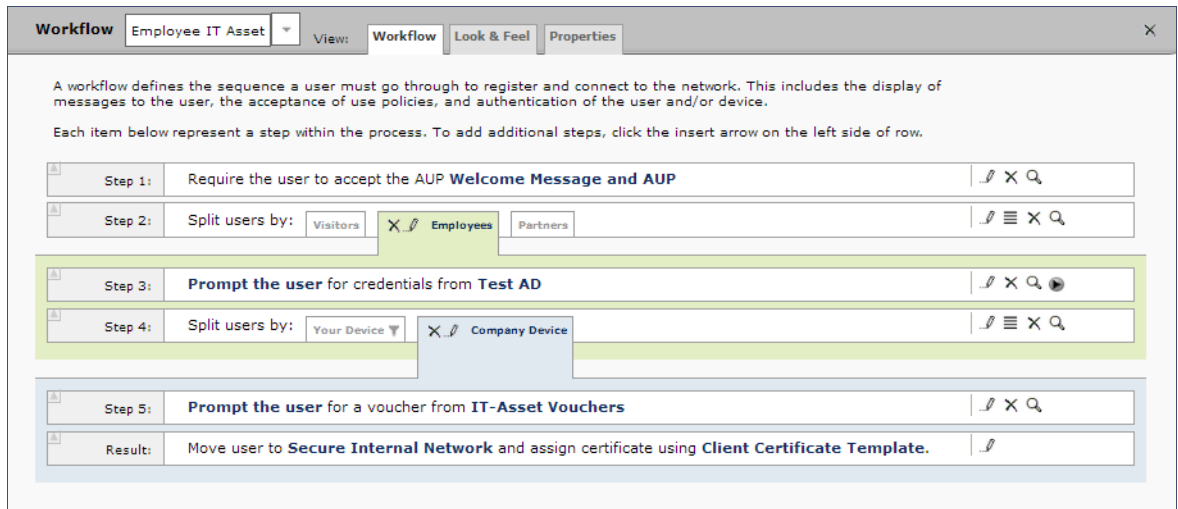
This section provides some enrollment workflow examples to help you get familiar with the different types of steps that can be configured with the Enrollment System.

Employee With IT Asset Authenticated to AD Group

This is an example workflow for an employee using an IT-assigned device to access the secure network. The employee is authenticated to an Active Directory group, and the device type split is managed with a filter, which moves the user to the Company Device workflow branch if they are a

member of a specified AD group. They are prompted to enter a previously sent/assigned voucher and moved to a secure internal network.

FIGURE 6. Example Workflow for Employees with IT Assets



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

Employee With Personal Device Authenticated to AD Group

This is an example workflow for an employee using a personal device to access the secure network. The employee authenticates to an Active Directory group, and the device type split is managed with a filter, which displays the Personal Device workflow branch only if they are a member of a

specified AD group. The user is asked to acknowledge a BYOD use policy before being moved to a secure internal network.

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

The screenshot shows a workflow configuration window titled "Workflow" for the "Employee with BYOD" process. The interface includes a "View" menu with options for "Workflow", "Look & Feel", and "Properties". A descriptive text explains that a workflow defines the sequence of user registration and connection steps, including message display, policy acceptance, and authentication. Below this, a list of steps is shown, each with an insert arrow on the left and edit/delete/search icons on the right. Step 1 is "Require the user to accept the AUP Welcome Message and AUP". Step 2 is "Split users by:" with buttons for "Visitors", "Employees" (selected), and "Partners". Step 3 is "Prompt the user for credentials from Test AD". Step 4 is "Split users by:" with buttons for "Personal Device" (selected) and "Company Device". Step 5 is "Require the user to accept the AUP BYOD Use Policy". The final "Result" is "Move user to Secure Internal Network and assign certificate using BYOD Certificate Template.".

Step	Description	Options
Step 1:	Require the user to accept the AUP Welcome Message and AUP	[Edit] [X] [Q]
Step 2:	Split users by: <input type="button" value="Visitors"/> <input checked="" type="button" value="Employees"/> <input type="button" value="Partners"/>	[Edit] [Menu] [X] [Q]
Step 3:	Prompt the user for credentials from Test AD	[Edit] [X] [Q] [Play]
Step 4:	Split users by: <input checked="" type="button" value="Personal Device"/> <input type="button" value="Company Device"/>	[Edit] [Menu] [X] [Q]
Step 5:	Require the user to accept the AUP BYOD Use Policy	[Edit] [X] [Q]
Result:	Move user to Secure Internal Network and assign certificate using BYOD Certificate Template .	[Edit]

Employee With Personal Device on Internet-Only VLAN

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

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

The screenshot displays the 'Workflow' editor for 'Employee BYOD Int'. The interface includes a 'View' menu with options for 'Workflow', 'Look & Feel', and 'Properties'. A descriptive text explains that a workflow defines the sequence of user registration and connection, including message display, policy acceptance, and authentication. It notes that each row represents a step and provides instructions on how to add steps using an insert arrow.

The workflow consists of the following steps:

- Step 1:** Require the user to accept the AUP **Welcome Message and AUP**.
- Step 2:** Split users by: Visitors, **Employees**, Partners.
- Step 3:** **Prompt the user** for credentials from **Test AD**.
- Step 4:** Split users by: **Personal Device**, Company Device.
- Step 5:** Require the user to accept the AUP **BYOD Use Policy**.
- Result:** Move user to **Internet-only VLAN** and assign certificate using **30-day certificate**.

Sponsored Guest on Internet-Only VLAN

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

For details on the sponsored guest access feature, see the *Setting Up Sponsored Guest Access Within the XpressConnect Enrollment System* document on the ES Support tab.

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

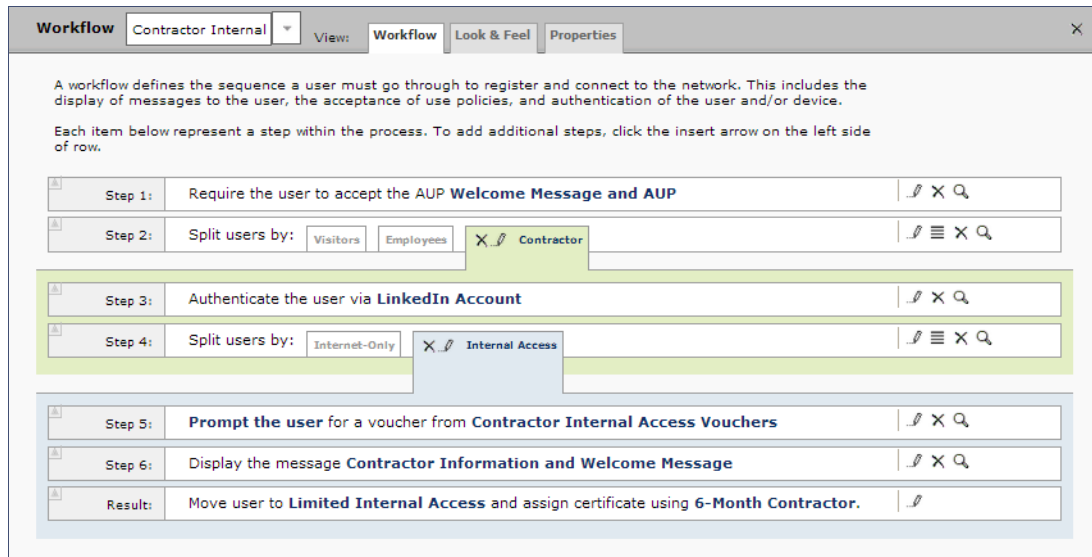
The screenshot shows a workflow configuration window titled "Workflow" for "Sponsored Guest Internet-Only VLAN". The window has tabs for "Workflow", "Look & Feel", and "Properties". Below the tabs, there is a description: "A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device. Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row." The workflow consists of the following steps:

Step	Description	Actions
Step 1:	Require the user to accept the AUP Welcome Message and AUP	✎ ✕ 🔍
Step 2:	Split users by: Guest Users (selected) Employees	✎ ☰ ✕ 🔍
Step 3:	Authenticate the user via Personal Gmail Account	✎ ✕ 🔍
Step 4:	Prompt the user for a voucher from Guest Vouchers	✎ ✕ 🔍
Step 5:	Require the user to accept the AUP Guest User Policy	✎ ✕ 🔍
Result:	Move user to Internet-only VLAN and assign certificate using 90 day certificate .	✎

Contractor With IT Asset on Internal Network With Limited Access

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

FIGURE 10. Example Workflow for Contractors with IT Assets



Planning the Local Network Configuration

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

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

- WPA2-Enterprise Infrastructure
- Setting Up SSIDs
- Setting Up Captive Portal Redirect
- Certificate Authority
- RADIUS Servers
- Supported Authentication Servers

- DNS
- Firewall Configuration
- Use Cases

WPA2-Enterprise Infrastructure

The Enrollment System works in your existing WLAN infrastructure using standards-based WPA2-Enterprise.

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

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

Setting Up SSIDs

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

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

Guest SSID

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

Conflicting SSIDs

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

Setting Up Captive Portal Redirect

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

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

Note >>

If using an existing RADIUS server, you must configure layer 3 access to the Enrollment System virtual appliance to allow certificate status verification.

For more information, see Enrollment System Captive Portal Setup.

Certificate Authority

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

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

Onboard CA

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

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

RADIUS Servers

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

For all configurations:

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

Note >>

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

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

Onboard RADIUS Server

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

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

Microsoft NPS Acting as a RADIUS Server

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

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

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

Tip >>

See the *XpressConnect Enrollment System Integration with Microsoft NPS Configuration Guide* for configuration details.

External RADIUS Server

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

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

RADIUS Proxy

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

This proxy configuration is set up on the external server.

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

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

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

RADIUS Accounting

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

RADIUS Server VLAN Attributes

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

VLAN Tagging

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

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

Certificate Revocation

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

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

Supported Authentication Servers

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

Active Directory

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

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

- You need AD domain information (plus any sub domains) and the IP address of the AD server.
- Set up your AD groups for use with wireless BYOD access or Sponsorship Grounds (if needed).
 - The Enrollment System must have layer 3 access to the AD server.
- The AD host is an LDAP call and must be an IP routable address.
- During authentication, the username is compared to the AD SAM attribute.
- The FQDN of your AD server or IP address maps to the internal AD server IP address.
- If you are using the hosted Enrollment System (onboard.cloudpath.net) DNS must resolve to onboard.cloudpath.net 72.18.151.86
- The ES communicates to the AD server using TCP Port 389, LDAPS TCP/UDP 636.

LDAP or LDAPS

To use LDAP with the Enrollment System, you need:

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

Third-Party Authentication

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

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

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

Tip >>

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

DNS

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

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

See DNS Issues in the *Troubleshooting* section of this document.

Firewall Configuration

This section describes the firewall ports that may need to be configured to use the XpressConnect Enrollment System and Wizard.

The Enrollment System must be able to communicate with:

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

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

TABLE 1. Firewall Ports for Use with the Enrollment System

Port	Protocol	Notes
80	TCP and UDP	Android Communications
443	TCP and UDP	Android communications with Google Play and Amazon Market.
5228	TCP and UDP	Android APK
389	TCP	Active Directory, LDAP queries
80	TCP	NPS query to the ES for OCSP
1812	UDP	RADIUS Authentication
1813	UDP	RADIUS Accounting
8022		SSH. This is the default port for SSH.
22		SSH. This port can be configured for SSH.

TABLE 1. Firewall Ports for Use with the Enrollment System

Port	Protocol	Notes
3268	TCP	LDAP recursive domains
	Windows RPC	If you are using the Integration Module for Microsoft CA, the web server communicates with the Microsoft CA using Windows RPC.

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

Use Cases

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

Use these questions to help you determine a deployment scheme.

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

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

Prerequisites for Configuring the Enrollment System

This section describes the information you need before you can set up the XpressConnect Enrollment System in your Network.

What You Need

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

Deploying the OVA

- VMware server, on which you'll install the ES virtual appliance.
- The URL where the OVA file resides. A Cloudpath representative provides this information.
- Hostname of the virtual appliance
- IP address (and netmask) being assigned to the ES on VMware server. Not needed if using DHCP.

- IP address to restrict administrator access
- IP address of the DNS server(s).
- Gateway IP address

Setting up the Initial Account

- Login credentials for XpressConnect License Server
- License Server URL
- HTTPS server certificate
- Company Information (Domain, URL)
- DNS hostname
- Active Directory domain, DNS/IP address of AD server, and DN of AD domain or LDAP server.
- WWW certificate (public-signed)
- 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.
- A list of conflicting SSIDs (open SSIDs, to prevent roaming)
- An idea about which OS families and versions to support.
- Additional requirements for device configurations (for example, enable firewall, proxy, verify antivirus, enable screen lock passcode).

Deploying the ES Virtual Appliance to a VMware Server

The 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 License Server *OVA Download* tab, from a direct download link, or from a Cloudpath representative.

To retrieve the OVA file using the XpressConnect License Server:

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

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

FIGURE 11. License 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 12. OVA Download Page

Cloudpath NETWORKS | Cloudpath Administrative Console | Anna Test | Logout

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	
Version:	2.0.1604
Published:	20130820
OVA File:	XpressConnectES_OVF10_2.0.i604.ova
Deployment Instructions:	ES_VirtualAppliance.pdf
Release Notes:	Create a VMware snapshot of the enrollment system VM before upgrading. For updates, refer to the release notes .

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

Deploy Virtual Appliance to a VMware Server

Set Up Virtual Appliance

1. Open the VMware client.
2. Select *File > Deploy OVF Template*.
3. Enter the file path or URL where the OVA file resides.
4. Enter a unique name for the virtual appliance. The default is *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 13. 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. Disabling this feature permits 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

- Installation of the application implies that you accept the EULA. The link to the EULA is provided for reference.
- Do you want to require a boot password to start the server?
 - If checked, you must supply the boot password on the initial boot and all system reboots. This is the default.
 - If unchecked, a boot password required only on the initial system boot.

Note >>

Contact a support representative to receive the boot password.

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

Note >>

The 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.

Networking Properties

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

FIGURE 14. Networking Properties

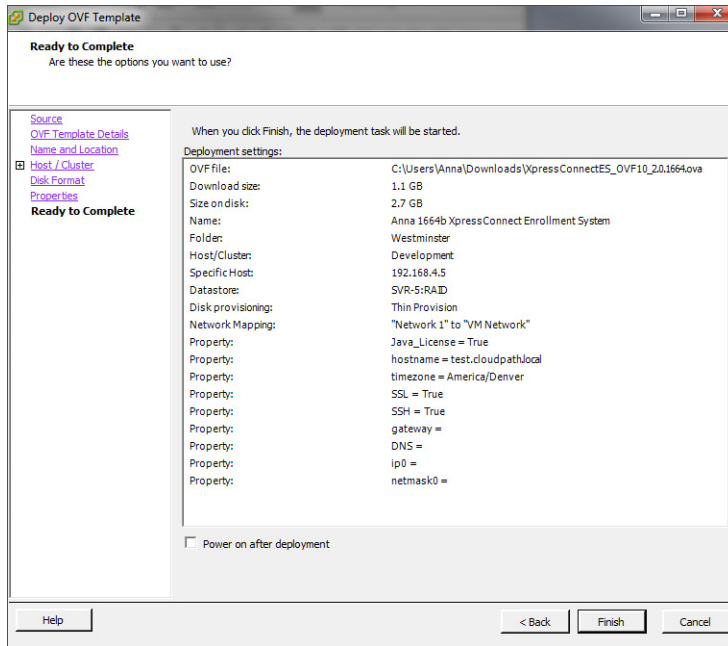
The screenshot shows a form titled "Networking Properties" with four sections, each with a text input field:

- 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 15. Deployment Settings



Click *Finish*. Deployment takes approximately 2 minutes.

Service Account

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

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

See the *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 the XpressConnect Licensing Server is hosted

- Verify that the virtual appliance can resolve DNS

How to Install VMware Tools

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

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

Note >>

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

From the vCenter Client

1. From the powered-off state, select the VM, and right-click to *Edit Settings*.
2. With the *Hardware* tab selected, click the *Add* button to open the *Add Hardware* page.
3. Select *CD/DVD Drive* (or browse to locate the ISO for the media) and click *Next*.
4. Continue with the configuration using the default settings. When finished, click *OK*.
5. Power on the VM.
6. Select the VM and right-click to select *Guest > Install/Upgrade VMware Tools*.
7. Select *Interactive Tools Upgrade* and click *OK*. This popup does not occur on some systems.

From the Console

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

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

Tip >>

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

Select the default answers to the configuration questions. When finished, exit the **vmware-tools-distrib** directory.

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

How to Increase the Virtual Appliance Memory

We recommend that your VMware server have 12-16GB RAM, which is sufficient for most production environments. However, there may be circumstances (replication, performance, larger deployments) that require adjustments to the memory allocation for the Enrollment System.

Use these instructions if you want to change the memory configuration of a virtual machine's hardware.

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

How to Expand the MySQL Partition Size

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

From the vCenter Client

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

Note >>

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

From the Console

Enter the following commands as root.

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

```
[root@localhost cpn_service]# df -h
```
2. Signal to the OS that there has been a hardware change to the disk.

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

3. Expand the physical volume.

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

4. Extend the size of the logical volume for MySQL operations. This example shows that we are extending the size of the logical volume by adding 25GB.

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

5. Resize the file system. This writes your changes to disk and completes the partition expansion process.

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

6. Verify the amount of free disk space available.

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

The output should indicate the increased partition size.

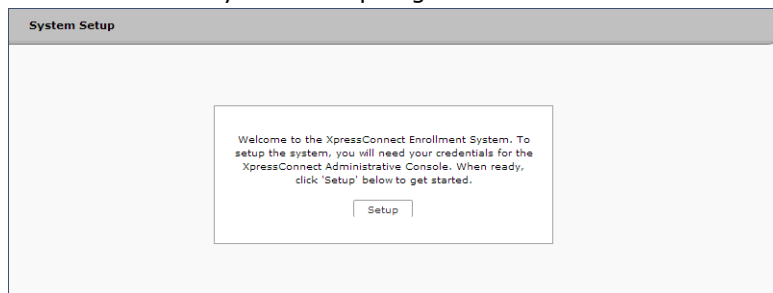
Initial System Setup

A setup wizard guides you through the system setup process and automates the initial configuration of the virtual appliance to get you up and running quickly. During the setup process, you can configure account information, onboard RADIUS server, onboard CA, and server and client certificates. If you are unsure about a particular piece of the configuration, you can skip it during the initial setup and configure it later.

Account Setup

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

FIGURE 16. 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 17. 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 18. 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

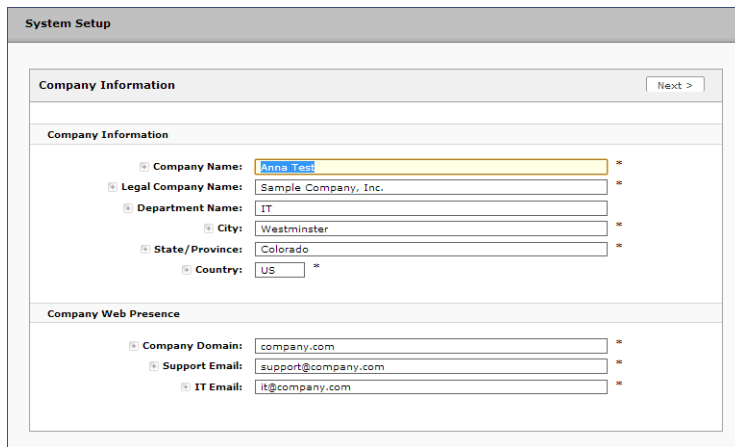
information for the initial setup. *Add-On* and *Replacement* servers receive most of their configuration from the Master server in the cluster.

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 19. Company Information



The screenshot shows the 'System Setup' window with the 'Company Information' section active. 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

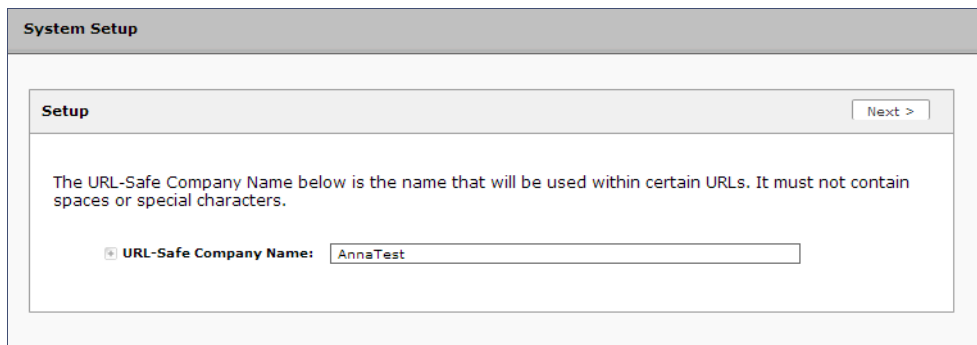
The 'Company Web Presence' section contains the following fields:

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

A 'Next >' button is visible in the top right corner of the 'Company Information' section.

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 20. System Setup URL-Safe Company Name



The screenshot shows the 'System Setup' window with the 'Setup' section active. 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

A 'Next >' button is visible in the top right corner of the 'Setup' section.

Authentication Server

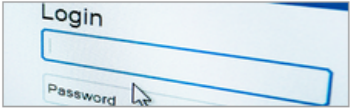
If you plan to use an authentication server to authenticate end-users or sponsors, we recommend populating the authentication server information page.

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

FIGURE 21. 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 22. Authentication Server Certificate

The screenshot shows the 'Authentication Server' configuration window. At the top, there are '< Back' and 'Next >' buttons. Below the title bar, a message states: 'To use LDAPS, the system needs to know which server certificate to accept for the authentication server.' There are two radio button options:

- Upload the Chain for the Server Certificate.** (Selected)

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.

Common Name: *

Certificate Chain: No file chosen
- 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.

Common Name: svr-2.test.cloudpath.local

Thumbprint: AC247858885FD6531C284889D7CF4897036ED849

Valid Period: 08/22/2013 - 08/22/2014

Issued By: Cloudpath Networks MS/CA

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 23. WWW Certificate for HTTPS

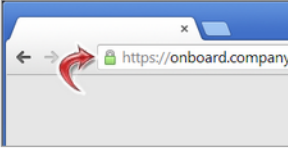
WWW Certificate for HTTPS Skip Next >

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 24. Upload WWW Certificate

Upload WWW Certificate < Back Next >

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 25. 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:

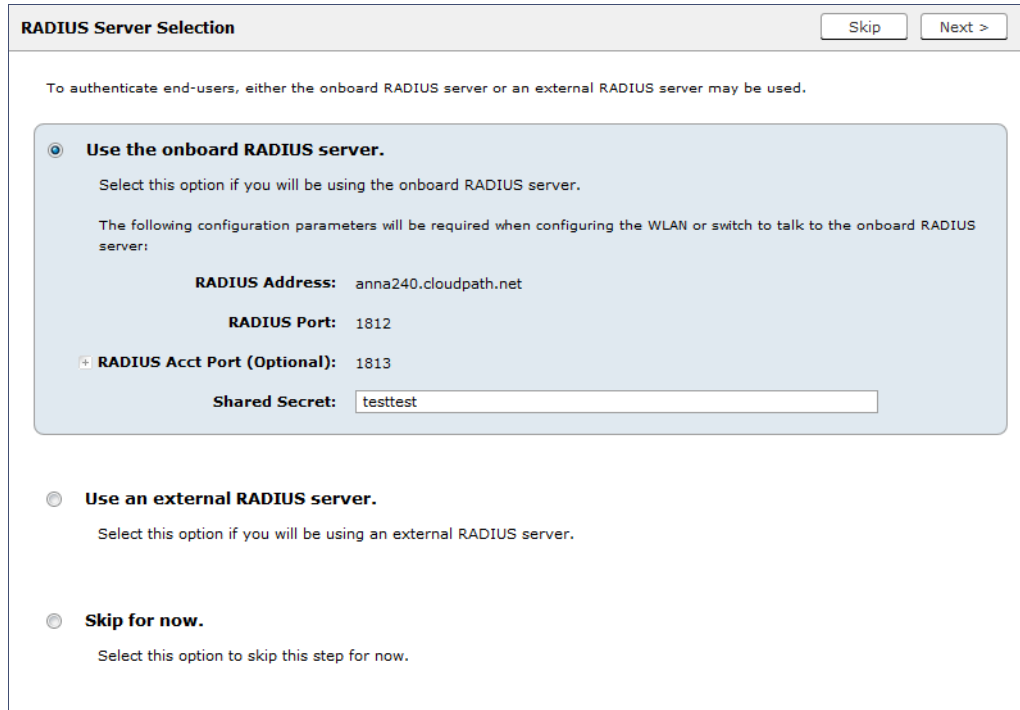
Skip for now.
Select this option to skip this step for now, to manually setup the certificate authority, or to use external certificate authorities.

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 26. 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.

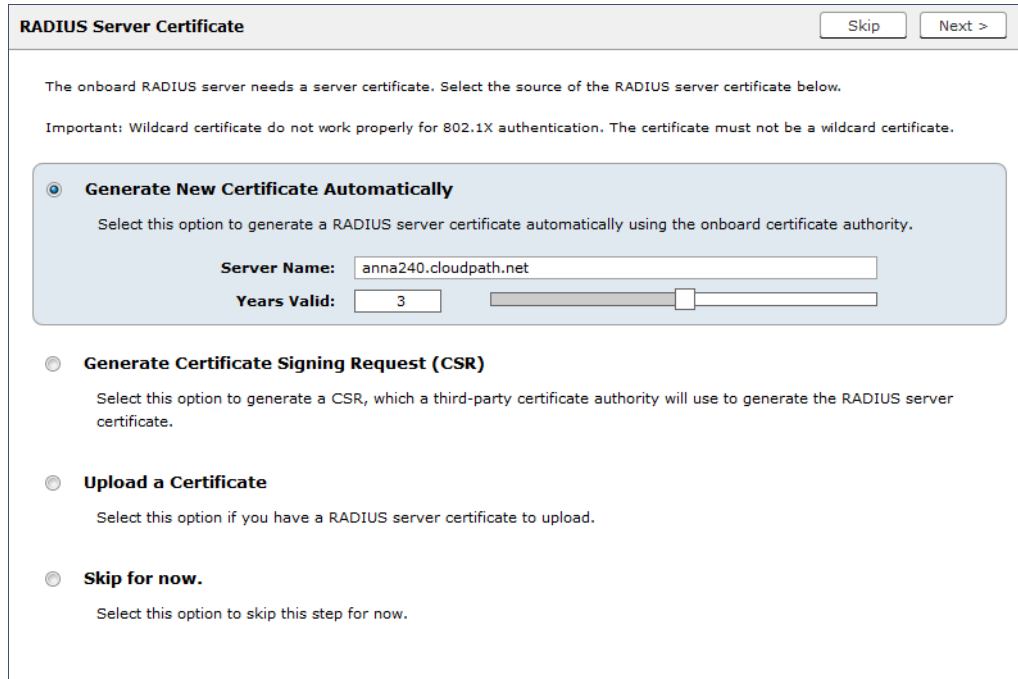
If you skip this step, you can set up a RADIUS server in the workflow.

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 27. 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 to modify, or simply add a device configuration and use immediately.

To create your own workflow, select *Start with Blank Canvas*.

FIGURE 28. 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.
Secure SSID Name:
- 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 29. System Initialization Task

Initialization Status:	Status
Create Certificate Authorities:	✔ Completed.
Create Certificate Templates:	✔ Completed.
Create Device Configurations:	✔ Completed.
Configure Workflow:	✔ Completed.
Activate Sponsor Portal:	✔ Completed.
Publish Enrollment Portal:	✔ Completed.
	✔ System is ready to handle enrollments.
Access Point Setup:	
	The following information will be necessary to configure the access point with the appropriate secure SSID configuration.
SSID:	CloudpathTest (WPA2-Enterprise, AES (CCMP), Broadcast)
RADIUS IP:	anna39.cloudpath.net
RADIUS Authentication Port:	1812
RADIUS Accounting Port:	1813
RADIUS Shared Secret:	h7w7mnb336qvmzgh3s
RADIUS Attributes:	BYOD Policy Template - VLAN: 'byod' Guest Policy Template - VLAN: 'guest'
User Experience:	
	End-users will use the enrollment portal to activate devices.
End-User Portal:	https://anna39.cloudpath.net/enroll/AnnaTest/Production/
BYOD:	For BYOD, the authentication is initially configured for a demo Active Directory server. Demo users include 'bob' (password bob1) and 'bill' (password bill1). The authentication configuration may be changed to point at your AD/LDAP server. BYOD users will be moved onto the secure SSID with VLAN 'byod' assigned.
Guests:	Guests will be required to provide a voucher from a sponsor. See the sponsor section below for currently available vouchers and instructions on creating additional vouchers. Sponsorship is one of several mechanisms for handling guests. Guest users will be moved onto the secure SSID with VLAN 'guest' assigned.
Sponsor Experience:	
	The default workflow utilizes sponsorship to authorize guests. To create vouchers for guests, sponsors can login to the sponsor portal below.
Sponsor Portal:	https://anna39.cloudpath.net/portal/sponsor/AnnaTest/
Available Vouchers:	The following vouchers are currently available for use. Guest Vouchers - zjh, bwod, nvgv, nsic, kbhw
Administrator Experience:	
Administrator UI:	https://anna39.cloudpath.net/admin/
Credentials:	The following email addresses have been sent a one-time password along with this information: If you ever forget your password, you can reset it from the login screen.
Key Pages:	View Enrollments - View information about enrolled devices, users, and policies. Configure Workflow - Modify the workflow that an end-user passes through to get on the network. This page also contains links for modifying the configuration of the authentication server, wireless netw Add/Manage Administrators - This page allows additional administrator logins to be setup. Deploy Snapshots - After making changes to the workflow, go to Configuration -> Deploy and click Create New Snapshot to publish the changes to the enrollment portal. After the new snapshot is do force it to pull in the new snapshot. Look & Feel - To modify the look & feel, go to Configure Workflow link above and select the Look & Feel tab along the top.

ToDo Items

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

FIGURE 30. 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.

About the 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.

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

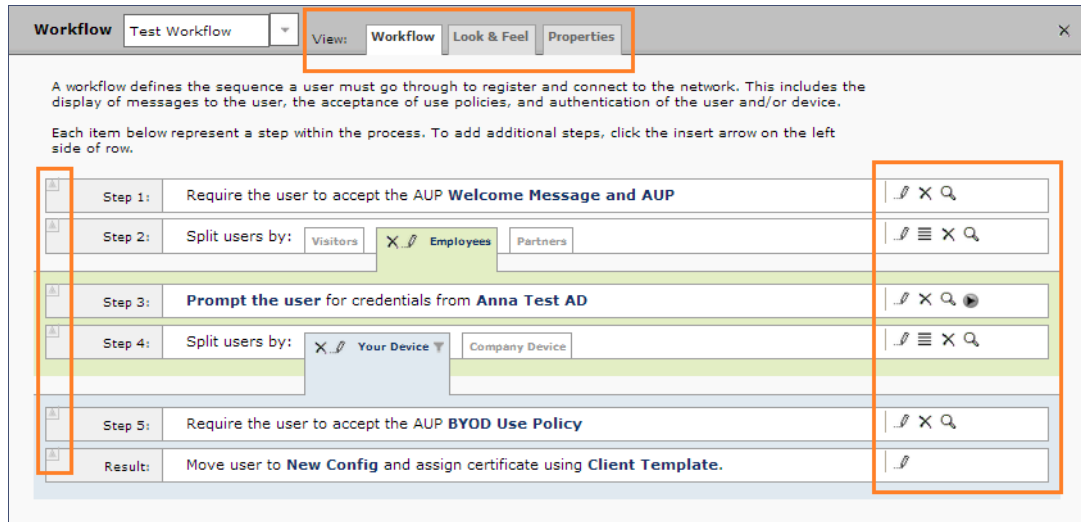
See Enrollment Workflow Use Cases for an example of the most commonly used workflows.

Workflow Basics



The *Workflow* page has three view tabs.

- Use the *Workflow* tab to configure the steps presented to a user during the enrollment process.
- Use the *Look & Feel* tab to configure the Enrollment System skin, and to customize the logos, colors, buttons, and images for the ES, the Wizard, the Download page.
- Use the *Properties* tab to enable/disable a configuration, or to modify the configuration Name and Description.

FIGURE 31. Enrollment Workflow Page



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

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

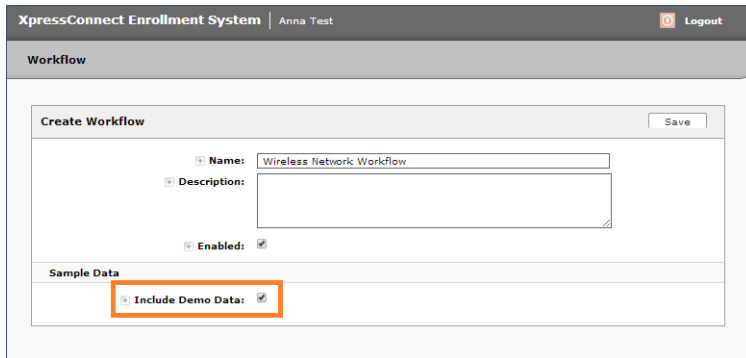
Modifying a Workflow Template

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

To create a workflow from a template using sample data:

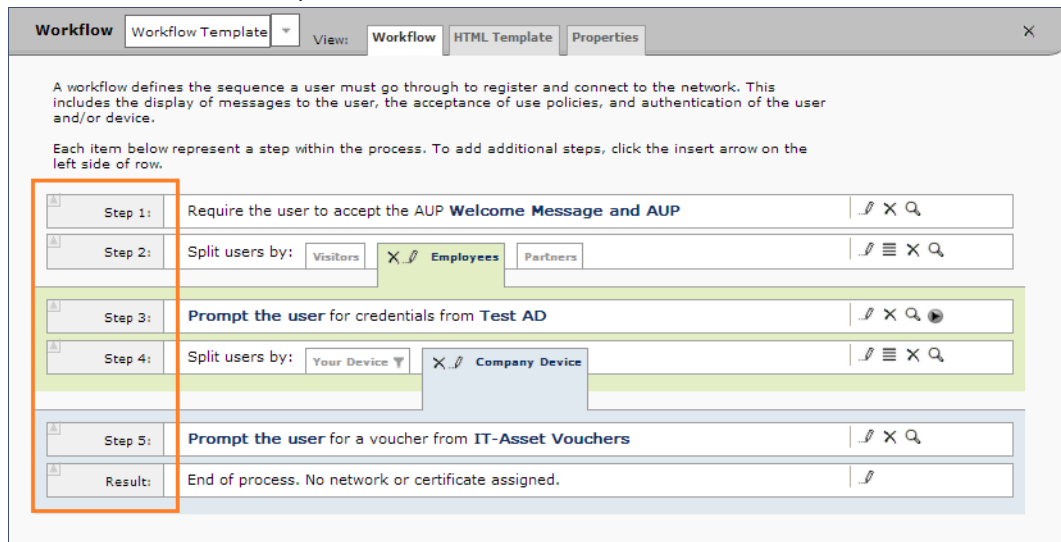
1. Go to *Configuration > Workflow*.
2. From the *Workflow* drop-down menu, select *Add New Workflow*.
3. On the *Create Workflow* page, enter a *Name* and *Description*. Select the check box for *Include Demo Data* and *Save*.

FIGURE 32. 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 33. Workflow Template



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

Step 1: Acceptable Use Policy.

Step 2: Split in the workflow to provide a different sequence of enrollment steps for Visitors, Employees, and Partners. Splits can be modified for other industries (for example, *Students, Faculty, and Guests*).

Step 3: An authentication step for domain users, using Active Directory or LDAP.

Step 4: Another split in the workflow to provide a different sequence of enrollment steps for users with an IT device or a personal device.

Step 5: A prompt for a verification voucher.

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

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

Creating a Workflow From a Blank Slate

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

1. Go to *Configuration > Workflow*.
2. From the *Workflow* drop-down menu, select *Add New Workflow*.
3. On the *Create Workflow* page, enter a *Name* and *Description*. Leave *Include Demo Data* unchecked, and *Save*.
4. On the blank workflow page, click *Get Started* to add your first workflow step.

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

FIGURE 34. Enrollment Step Selection

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

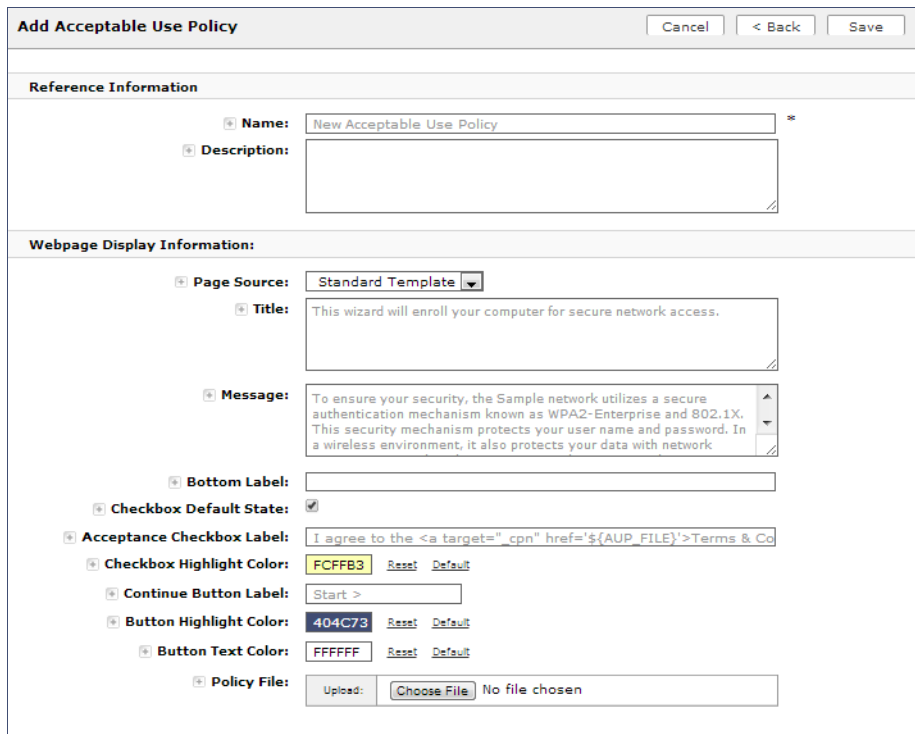
- Display an Acceptable Use Policy (AUP).**
Displays a message to the user and requires that they signal their acceptance. This is normally used for an acceptable use policy (AUP) or end-user license agreement (EULA).
- Authenticate to a local server.**
Prompts the user to authenticate to an Active Directory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

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

FIGURE 35. 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.

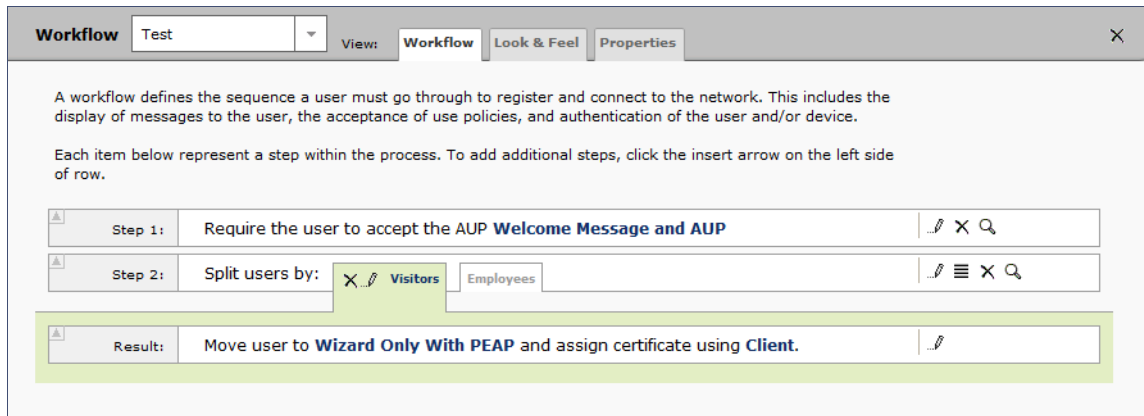
To create a *User Type* prompt:

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 36. 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 37. Add Authentication Server

Add Authentication Server < Back Next >

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

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

Administrator Login

Use For Admin Logins:

Admin Group Regexp: [ex. IT_ADMINS] *

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

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

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

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

Device Type Split

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

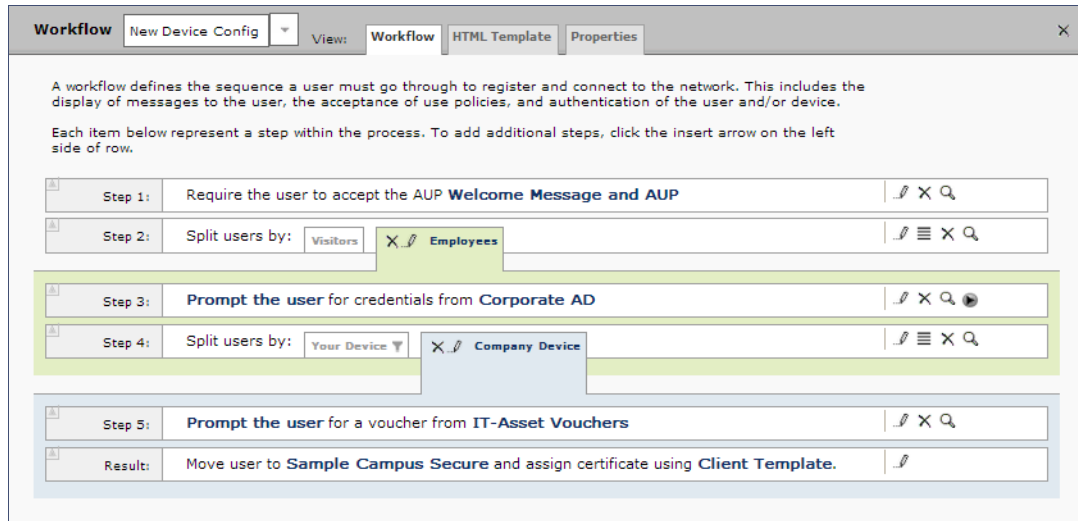
1. *Insert* a step above the *Result:* step in the enrollment workflow.
2. Select *Split users into different processes*.
3. Select *Use an existing split* and choose *Device Ownership*. The *Device Ownership* option prompts the user to select either *Your Device* or *Company Device*. These labels can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

Tip >>

Use the *Edit List* icon  to customize the *split option* labels.

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

FIGURE 38. Workflow with Device Ownership Split



Create a Filter in the Device Type Split

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

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

1. On the Enrollment Workflow page, locate the step with the *Device Type* prompt. In this example, it is Step 4.
2. On the right side of the step, click the *Edit List* icon to open the *Selection Options* page and edit the *Your Device* option. This opens the *Modify Options* page, which allows you set up filters for this split in the workflow.

FIGURE 39. 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: Upload:

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: Matches

Username Pattern: Matches

User DN Pattern: Matches

Email Pattern: Matches

Device-Based Filters

Operating System Pattern: Matches

User-Agent Pattern: Matches

Location-Based Filters

Location Pattern: Matches

Allowed IPs:

Blocked IPs:

Filters Based On Web Authentication Certificate

Common Name Pattern: Matches

Issuer Pattern: Matches

Template Pattern: Matches

Expiration Date: Expires Within

Other Filters

Voucher List Name: Matches

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

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

Tip >>

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

Prompt for Voucher

Step 5 adds a voucher verification step for authenticated employees with IT-assets.

To create this authorization prompt:

1. Select the *Employees* tab in Step 2 and the *Company Device* tab in Step 4 of the workflow.
2. *Insert* a step above the *Result:* step in the enrollment workflow.
3. Select *Authenticate via voucher* and *Create a new Voucher list*.

FIGURE 40. Create Voucher List

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

LDAP Group Regex:

LDAP Username Regex:

LDAP Username DN Regex:

Maximum Certificates:

Default Permissions:

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

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.
 - Initial vouchers - Create one or more initial vouchers.
5. For the voucher prompt, select *Create a new webpage from a standard template*.
6. On the *Create Voucher Prompt* page, enter the data for the voucher prompt and *Save*.

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

Device Configuration and Client Certificate

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

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

Device Configuration

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

FIGURE 41. Configure SSID

The screenshot shows the 'Add Device Configuration' form. At the top right, there are buttons for 'Cancel', '< Back', and 'Next >'. Below the title, a note states: 'A single device configuration may support wireless and/or wired connections.' The main instruction is 'Select the connection method(s) this device configuration supports:'. There are two radio buttons: 'Wireless Connections' (which is selected) and 'Wired 802.1X Connections'. Under 'Wireless Connections', there are four fields: 'SSID' with the value 'CPN Secure', 'Authentication' with a dropdown menu showing 'WPA2-Enterprise', 'Encryption' with a dropdown menu showing 'AES', and 'Is this SSID Broadcast?' with a dropdown menu showing 'Yes, the SSID is broadcast.'

5. Set the *Authentication, Encryption, and Broadcast* settings.
6. Specify *Conflicting SSIDs*. This setting prevents the device from roaming away from the secure SSID to any open SSID within range.
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 42. 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

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

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

How to Set Up Client Certificate Templates

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

1. Select *A new certificate template*.
2. Select *Use an onboard certificate authority*.
3. Select *Use an existing CA*. Choose the Root CA that was created during the Enrollment System initial configuration. See *Certificate Authority*, page 35.
4. Set up the *Client* certificate template. This template is used to issue a certificate to the client device.

FIGURE 43. Client Certificate Template

The screenshot shows a configuration window titled "What type of certificates should be issued?". It has "Cancel" and "Next >" buttons at the top right. There are two main sections: "Client Certificates" and "Server Certificates".

- Client Certificates:**
 - Description: "Used on clients to authenticate the client. The decoration of the username within the certificate allows RADIUS policies to be applied appropriately."
 - Username Decoration:** A list of radio buttons with the following options:
 - username@byod.company.com
 - username@contractor.company.com
 - username@employee.company.com
 - username@faculty.company.com
 - username@guest.company.com
 - username@it.company.com
 - username@staff.company.com
 - username@student.company.com
 - username@other.company.com
 - Grant Access:** For
 - Configure Advanced Options:**
 - RADIUS Options:**
 - VLAN ID:**
 - Filter ID:**
- Server Certificates:**
 - Description: "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 44. Completed Workflow

The screenshot displays a workflow configuration window with the following steps:

- Step 1:** Require the user to accept the AUP **Welcome Message and AUP**
- Step 2:** Split users by: **Visitors**, **Employees**
- Step 3:** **Prompt the user** for credentials from **Corporate AD**
- Step 4:** Split users by: **Your Device**, **Company Device**
- Step 5:** **Prompt the user** for a voucher from **IT-Asset Vouchers**
- Result:** Move user to **Sample Campus Secure** and assign certificate using **Client Template**.

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 45. 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
Q ✕ ⏻	Snapshot 3		Demo Data	5.0.150	20141113 1115 MST
Q ✕ ⏻	Snapshot 2		Demo Data	5.0.150	20141113 1052 MST
Q ✕ ⏻	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 access the enrollment wizard.

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

FIGURE 46. Modify Deployment Location

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

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

Configuration Snapshots

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

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

How to Deploy a Snapshot of the Workflow Configuration

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

FIGURE 47. Create New Snapshot

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

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

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

How to Test a Configuration Snapshot

Test the enrollment process for the active configuration snapshot.

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

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

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

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

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

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

Troubleshooting Your Deployment

Connectivity Issues

XpressConnect License Server

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

RADIUS Server

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

Firewall Requirements

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

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

FIGURE 48. Firewall Configuration

Firewall Requirements				
The following information will assist in understanding the inbound and outbound traffic of your XpressConnect Enrollment System. This is dynamically generated based on the current system configuration and may change as the system configuration is modified.				
Traffic: Outbound from this System				
Purpose	System Address	External Address	Protocol	Reason
System	AnnaTest.cloudpath.net	bvt.cloudpath.net:443	HTTP(s)	System interacting with cloud services (licensing, wizards, built-in email, etc).
System	AnnaTest.cloudpath.net	support.cloudpath.net:8022	TCP	(Optional) Support tunnel for remote assistance. Only necessary when support tunnel is enabled.
External CA	AnnaTest.cloudpath.net		HTTP(s)	System querying certificates from external CA. ERROR: Unable to parse URL of ".
System	AnnaTest.cloudpath.net		TCP	Facebook authentication enabled but firewall specifics not available.
System	AnnaTest.cloudpath.net		TCP	LinkedIn authentication enabled but firewall specifics not available.
System	AnnaTest.cloudpath.net		TCP	Google authentication enabled but firewall specifics not available.
Authentication Server	AnnaTest.cloudpath.net	192.168.4.2:636	TCP	Authenticate to Active Directory server 'Anna Test AD' at 'ldaps://192.168.4.2'.
NTP	AnnaTest.cloudpath.net	0.centos.pool.ntp.org:123	UDP	NTP synchronization.
NTP	AnnaTest.cloudpath.net	1.centos.pool.ntp.org:123	UDP	NTP synchronization.
NTP	AnnaTest.cloudpath.net	2.centos.pool.ntp.org:123	UDP	NTP synchronization.
NTP	AnnaTest.cloudpath.net	3.centos.pool.ntp.org:123	UDP	NTP synchronization.
Traffic: Inbound to this System				
Purpose	System Address	External Address	Protocol	Reason
Web Interface	AnnaTest.cloudpath.net:80		HTTP(s)	Administrator, API, and end-user access to the web interface.
Web Interface	AnnaTest.cloudpath.net:443		HTTP(s)	Administrator, API, and end-user access to the web interface.
Onboard CA	AnnaTest.cloudpath.net:80		HTTP(s)	OCSF requests coming from external systems.
SSH	AnnaTest.cloudpath.net:8022		TCP	SSH access to the system.
Onboard RADIUS	AnnaTest.cloudpath.net:1812		UDP	Receive RADIUS requests from external systems.

Issues with User Credentials

Active Directory

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

- Make sure that RADIUS requests are going outbound from the AD server.
- Ping the AD server using the FQDN to verify that DNS is working.

- Verify that the RADIUS IP address and shared secret specified on the WLC matches what is on the ES.

Credentials Mismatch

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

LDAP

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

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

DNS Issues

Verify that DNS is Working

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

Verify DNS registration for domain controllers

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

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

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

OSCP Issues

OSCP Validation

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

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

OSCP Server in the DNS

When the client fetches the OCSP response from the CA, it looks up the domain name of the CA's OCSP server in the DNS, as well as establishing a connection to the OCSP server.

If you receive a message that indicates the server cannot resolve the OSCP URL, check the hostname listed in the OSCP URL for the onboard Root CA you created in the Enrollment System. You might need to add this hostname to the DNS of the domain.

Certificate Issues

Certificate Chain Not Trusted

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

Common Name in Template

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

SAN Other Name in Certificate Template

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

Missing EKU in the RADIUS Server Certificate

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

Enrollment System Captive Portal Setup

The following steps configure the portal page on the open SSID so that it automatically redirects the user to the Enrollment System webpage.

Note >>

This example shows configuration steps for a Cisco WLC. WLAN controllers might differ between models and versions.

Define an ACL that allows access to the ES webpage

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

Note >>

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

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

1. On the WLC, go to *WLANS* and *Edit* the open SSID.
2. Open the *Security > Layer 3* tabs
3. Check the *Web Policy* box.
4. Select the *Authentication* option.
5. In the *Preauthentication ACL* field, select the open SSID.

Configure the Portal Page

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

```
<SCRIPT language="JavaScript">
    window.location="[Enrollment System URL]";
</SCRIPT>
```

If you are not automatically redirected,
click here
to go to the Enrollment System.

Note >>

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

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

NPS-Specific Troubleshooting

For configuration details, see the *XpressConnect Enrollment System Integration with Microsoft NPS Configuration Guide* on the ES Admin UI Support tab.

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

Register the NPS With the Domain

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

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


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

```
net stop ias
netsh ras delete registeredserver domain=x server=y
net start ias
```

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

RADIUS Server Certificate Missing Private Key

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

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

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

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

Support

The Cloudpath Support team is your point of contact for issues relating to the XpressConnect Enrollment System and XpressConnect Wizard. If you need assistance, discover a bug, or have other questions, you can email support at **support@cloudpath.net**.

Customers with an active *Subscription* or *Trial* license can contact Cloudpath Support. End-users should go through the local help desk. Network administrators may contact support on behalf of an end-user.

See the *XpressConnect Enrollment System Technical Support Information Guide* for more information about the process for contacting support.

Additional Documentation

Detailed information is provided in the Enrollment System *Quicks Start Guide*, *Administrator Guide*, and other configuration guides, located on the left-menu *Support* tab of the ES Admin UI.

About Cloudpath

Cloudpath Networks, Inc. provides software solutions and services that simplify the adoption of standards-based security, including WPA2-Enterprise and 802.1X, in diverse BYOD environments. Our goal is to make secure as simple as insecure; simple for network administrators to deploy and simple for users to access.

To learn more about the XpressConnect Enrollment System and how it can simplify your wireless environment, visit www.cloudpath.net or contact a Cloudpath representative.

Contact Information

General Inquiries: info@cloudpath.net

Support: support@cloudpath.net

Sales: sales@cloudpath.net

Media: media@cloudpath.net

Marketing: 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