

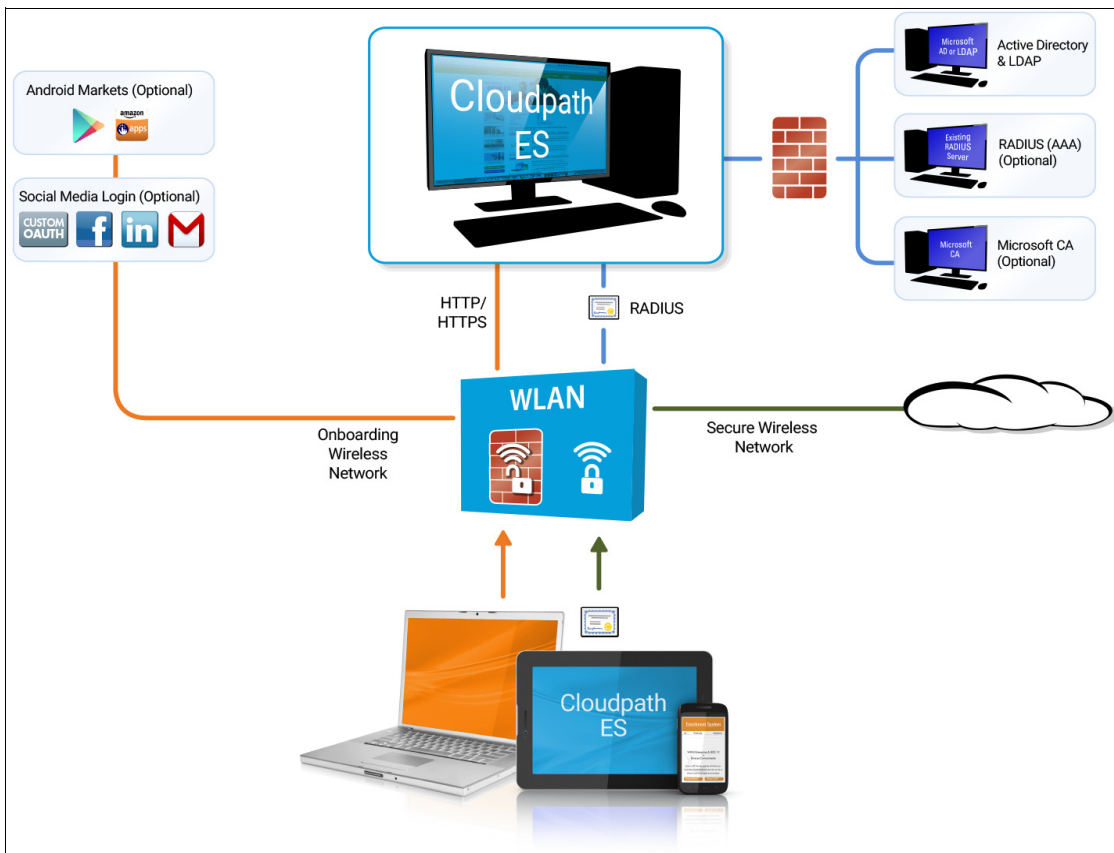
ZeroIT to Cloudpath ES Migration Guide for SmartZone 3.4

Overview

The Cloudpath Enrollment System provides a scalable, standards-based security solution that greatly reduces management demands even in the face of the skyrocketing growth in the numbers and diversity of devices requiring varied levels of access to the network. Cloudpath ES also serves as an integral piece in protecting an organization from the increasing sophistication of cyber attacks attempting unauthorized access and data theft, destruction or corruption.

Unprecedented levels of automation and flexibility make Cloudpath ES easy and simple. Cloudpath ES automates configuration for all major operating systems and segregates personal devices from IT-owned while maintaining device-by-device visibility and control.

FIGURE 1. Cloudpath ES Deployment Example



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

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

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

Cloudpath ES Specifications

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

TABLE 1. Cloudpath ES System Specifications

Supported Browsers for ES Admin UI	Supported OSES for End-User Devices	Supported Third-Party Identity Stores
Internet Explorer 6.0 and greater	Windows XP SP2 and greater	Microsoft Active Directory
Firefox 1.5 and greater	Mac OS X 10.5 and greater	LDAP
Safari 2.0 and greater	Apple iOS 2.0 and greater	Facebook
Google Chrome 3.0 and greater	Ubuntu 9.04 and greater	LinkedIn
	Android 2.2 and greater	Google Gmail
	Fedora 18 and greater	Custom OAuth 2.0 Server
	Chrome OS	
	Windows Phone 8 and 8.1	
	Blackberry (assisted configuration)	
	Windows RT (assisted config)	
	Generic (assisted config)	
	Windows Mobile 5 and 6 (assisted config)	

Note >>

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

Cloudpath ES Highlights

- Automated onboarding for all users, including employees, guests, and contractors
- Intuitive workflow engine for comprehensive policy-driven access
- Distributes unique certificate per device based on policies
- Built-in certificate infrastructure and RADIUS server
- Automates EAP-TLS, the WPA2-Enterprise gold standard
- Supports guest use cases, including sponsorship
- Differentiates between IT-owned and personal devices
- Provides visibility into users, devices, and policies
- Integrates with Microsoft Active Directory and Certificate Services
- Integrates with external LDAP and RADIUS servers
- Integrates with your existing WLAN

Cloudpath ES is deployable on-premise as a VMware server(s) or is available as a cloud service to make a powerful addition to existing ZoneDirector and SmartZone platforms.

Why You Need the Cloudpath ES

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

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

Additional features Cloudpath provides (as opposed to ZeroIT)

- Support for EAP-TLS, EAP-SIM and PEAP authentication methods
- Integrated with DPSK
- Cloudpath is a vendor neutral product and supports any standards based WLAN network
- Large deployments that have multiple controllers can aggregate to a single Cloudpath instance instead of config on every controller
- Highly customizable UI for end users
- Enhanced workflows for single or multi-factor authentication
- Integration with AD, LDAP, Oauth and Social networks for user authentication
- Updated client packages

- No longer dependent on new controller versions when new Client OS is released
- Support for newer OSES are available faster
- Minimal downtime when new OS patches are released
- Support for API integration for third party portals or mobile apps
- Integration with Microsoft and other Certificate Authorities
- Unified wired and wireless access with support for wired 802.1x
- Sophisticated policy engine
 - Issue vlans, VSAs and more
- Client Management capabilities
 - Enforcing Firewall on clients
 - Enabling pin locks
 - Enforcing system updates and Antivirus updates
 - Enforcing application install
- Integration with Google Console for Chromebooks
- Feature rich CA and certificate management platform
 - User or Device based certificates
 - Multiple certificate templates
 - Policy driven certificates
 - Secure guest access

Pre-Deployment Checklist

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

Deploying the OVA (For on-premise deployments)

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

Setting up the Initial Account.

- Login credentials for Cloudpath Licensing Server

Note >>

To obtain a Cloudpath license contact your Ruckus representative.

- Licensing Server URL
- HTTPS server certificate
- Company Information (Domain, URL)
- DNS hostname
- Active Directory domain, DNS/IP address of AD server, and DN of AD domain or LDAP server
- Web server certificate (public-signed)
- If you are not using the ES onboard CA, you also need:
 - Public and Private key of existing CA
 - RADIUS server certificate (if not using onboard RADIUS server)

Configuring the Workflow.

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

- An idea about the types of access and policies you want to offer different users
- Images and color schemes if you plan to customize the webpage display
- AD group names for creating filters in the workflow
- An idea about the security policy for passwords, vouchers, and certificates
 - Vouchers have configurable format and validity periods
 - Certificates have configurable key lengths, algorithm types, and validity periods
- The SSID for the secure network
 - If using VLANs to apply policy, you should have the VLAN IDs
- A list of conflicting SSIDs to prevent roaming (for example, open SSIDs)
- An idea about which OS families and versions to support

Additional requirements for device configurations (for example, enable firewall, proxy, verify antivirus, enable screen lock pass code)

Information Required From Customer

For on-premise deployments, Cloudpath requires the following information from the customer:

- Which brand of AP/Controller are you using?
- Do you plan to use the onboard PKI or an external certificate store?

- Do you plan to use the onboard RADIUS server or an external RADIUS server (NPS)?
- Are you using NAC in your network?
- Do you plan to use replication in your network?
- If yes, which configuration do you expect to use?
 - Master-Master
 - Hub and spoke
- Do you have a load balancer? If yes, which vendor?

Information the Customer Should Consider

Before we implement the Cloudpath ES in your network, you should consider the following network configurations:

- Your secure network must be set up for WPA2-Enterprise.
- Set up both the open and secure SSID on the Controller before the implementation call. Note: If your network is set up for PEAP, we can change it to TLS when we implement the Cloudpath ES.
- You should have knowledge about how to configure a captive portal on your wireless controller(s).
 - The open SSID typically has pre-authentication ACLs defined, which permit access to the VM. The LAN controller is configured to point to the Enrollment System VM as an external captive portal.
- The WPA2-Enterprise SSID should be setup to delegate authentication to the onboard AAA server or your existing AAA.
 - If using an existing AAA server, it requires layer 3 access to the Enrollment System VM to verify certificate status (optional).
- If using Active Directory, you need the AD domain information (plus any subdomains) and the IP address of the AD server. AD groups should be set up before the implementation call.
 - The ES/VM should have layer 3 access to Active Directory.
- A web server certificate is required for HTTPS. The system can be configured prior to the WWW server certificate being installed, but it should be installed before attempting to enroll end-users.
 - The WWW certificate may be a wildcard certificate (*.company.com) or a named certificate (test.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, you can download a CSR from the ES after the system is set up.
- If using NPS, set up the NPS server role and a RADIUS server.

Note >>

The new RADIUS server certificates and root CA can be uploaded after ES is configured.

- If using a pre-existing RADIUS server, you need the IP address and access to the RADIUS server-signed certificates.
- If using an existing CA, and you would like to use ES as an intermediates CA to issue client certificates, you need the public and private key of the existing CA to upload into the Enrollment System.
- If using the ES as a proxy for an existing CA (Microsoft CA or Custom External CA) you need the CA URL and CA chain for the remote CA.
- DNS should be configured for Enrollment System and other components appropriate for your network.
- The initial firewall configuration should be set up to allow Internet access for following:
 - Access from ES -> xpc.cloudpath.net (TCP 80/443-HTTP/HTTPS)
 - Access from ES -> dist2.cloudpath.net (used for ES updates TCP 80/443-HTTP/HTTPS)
 - Access from ES -> NTP (UDP 123) Note: 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.
- You should have some idea about your deployment scheme for employees, partners, contractors and guests. For example, some use cases might be:
 - Employee, IT asset, internal network, AD group
 - Employee, BYOD, internal network, AD group, BYOD use policy
 - Employee, BYOD, Internet-only, OAuth, short term
 - Sponsored Guest, BYOD, Internet-only, short term
 - Contractor, IT asset, internal network, limited access

Initial Setup Call

If you are setting up an account for a Cloud-based deployment or for a local VMware server, you can request an initial setup appointment with our implementation team. A typical implementation call lasts 1-2 hours.

Before the implementation call, you should review the Customer Checklist and Deployment Guide. If deploying to a local VMware server, be sure to download the OVA file prior to the setup call.

During the implementation call, we can help you with:

- Discussion about what you are trying to achieve
- Initial product setup
- Workflow basics
- If time permits, other configuration issues.
- Our goal is to get you up and running quickly so that you have adequate time to evaluate our product.

Who Should Be Involved in the Initial Setup Call

The ES implementation touches different aspects of your environment. Therefore, you might want to involve other members of your network team.

- The ES is installed as a virtual appliance. If you have a VM team, they should be contacted regarding the ES deployment.
- The open and secure SSIDs are set up on the wireless controller. The person/team that manages this aspect of your network should be available for making adjustments to the wireless controller.
- The ES can be set up to authenticate users to an Active Directory or LDAP server. Typically, you do not need to make adjustments to the authentication server. However, if there are issues connecting to the secure network, this person/team might be required.
- If you plan to use the onboard RADIUS server, which we recommend, you do not need the RADIUS server team. However, if you plan to use NPS or another external RADIUS server, this person/team should attend the setup meeting as user certificates are authenticated to the RADIUS server.
- After the initial setup, the Cloudpath ES provides a list of the inbound and outbound traffic of your Cloudpath ES. Firewall updates may be required for getting the ES up and running in your network.

Deployment Testing

Ideally, you should have devices on hand, for each operating system that you plan to support, for deployment testing. While the enrollment workflow behaves the same on each device, the Wizard application behaves slightly different on each operating system. With Android, this issue is compounded by the fact that each vendor can make modifications to the Android operating system, causing the application, in some cases, to behave slightly different between models.

Review the End-User Experience documentation for your supported OSes.

Deploying the ES Virtual Appliance to a VMware Server

Note >>

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

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

Specifications for On-Premise Deployed VMware Servers

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

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

Note >>

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

Retrieve OVA File

Retrieve the Cloudpath ES OVA file from the Licensing Server (xpc.cloudpath.net) *OVA Download* tab, from a direct download link, or from a Cloudpath representative.

To retrieve the OVA file using the Cloudpath Licensing Server:

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

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

FIGURE 2. Licensing Server Welcome Page

The screenshot shows the Cloudpath Administrative Console interface. At the top, it says 'Cloudpath Administrative Console | Anna Test' and has a 'Logout' button. A notification bar indicates the 'Current Build' (5.0.96) was posted on May 21, 2014. The main heading is 'Welcome to the XpressConnect Administrative Console.' Below this, there is a large icon of a hand pointing at a padlock with a Wi-Fi signal, labeled 'Administrative Console' with links to 'Quick Start Guide' and 'FAQs'. The content is organized into three main sections: 'XpressConnect' (easiest way to support a secure network), 'Define Networks' (configuration settings for network access), 'Deploy' (moving to the Deploy tab for hassle-free deployment), and 'Manage Account' (reviewing license information and managing administrative access).

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

Note >>

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

FIGURE 3. OVA Download Page

3. Download and read the *Deployment Instruction* document.
4. Download the OVA file. When the download is complete, deploy the OVA file using a VMware client.

Deploy Virtual Appliance to a VMware Server

Set Up Virtual Appliance

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

Note >>

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

- Use a thin provision for testing, or if disk space is an issue. A thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

Application Properties

Customize the application properties for the deployment.

FIGURE 4. Application Properties

Application

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

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

Hostname(FQDN)
 Enter the fully qualified domain name.

Timezone

Should Apache be configured for SSL?

Do you want to permit SSH?

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

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

Enter password

Confirm password

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

- Installation of the application implies that you accept the EULA. The link to the EULA is provided for reference.

- Do you want to require a boot password to start the server?
 - If checked, you must supply a boot password for all system reboots.
 - If unchecked, a boot password is not required for system reboots.
- Enter the *Hostname(FQDN)* for the virtual appliance.

Note >>

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

- Select the *Timezone*.
- Should Apache use SSL? Leave unchecked only if the Cloudpath ES is behind another web server using SSL.
- Do you want to permit SSH?
- Enter the IP addresses that can access the ES Admin UI. If you do not want to limit administrative access, leave this field blank.
- Enter and confirm a *service user* password. The *service user* account is used by your support team for access to this system using SSH. The *service* account is not available if SSH access is not permitted.
- Optional. Specify the address of an NTP server. To use pool.ntp.org, leave this field blank.

Networking Properties

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

FIGURE 5. Networking Properties

Networking Properties

Default Gateway
The default gateway address for this VM. Leave blank if DHCP is desired.

DNS
The domain name servers for this VM (comma separated). Leave blank if DHCP is desired.

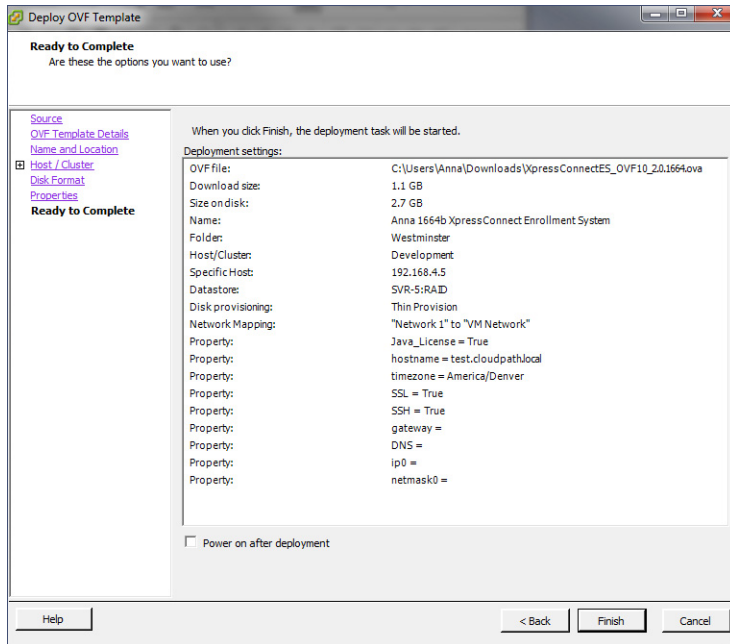
Network 1 IP Address
The IP address for this interface. Leave blank if DHCP is desired.

Network 1 Netmask
The netmask or prefix for this interface. Leave blank if DHCP is desired.

Confirm Deployment Settings

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

FIGURE 6. Deployment Settings



Click *Finish*. Deployment takes approximately 2 minutes.

Console

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

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

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

Test Network Connectivity

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

- Ping the gateway of your system
- Ping the URL where your Licensing Server is hosted
- Verify that the virtual appliance can resolve DNS

Activate Account or Log In

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

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

Activate Account

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

FIGURE 7. Activate Cloudpath ES Account

Cloudpath ES

ACTIVATE

Welcome to the Cloudpath ES. To activate your account, you must first provide the activation code you received by email.

I have an Activation Code

Enter the activation code (in the format XXXX-XXXX-XXXX) that you received for Cloudpath ES.

[Enter Activation Code]

Activate

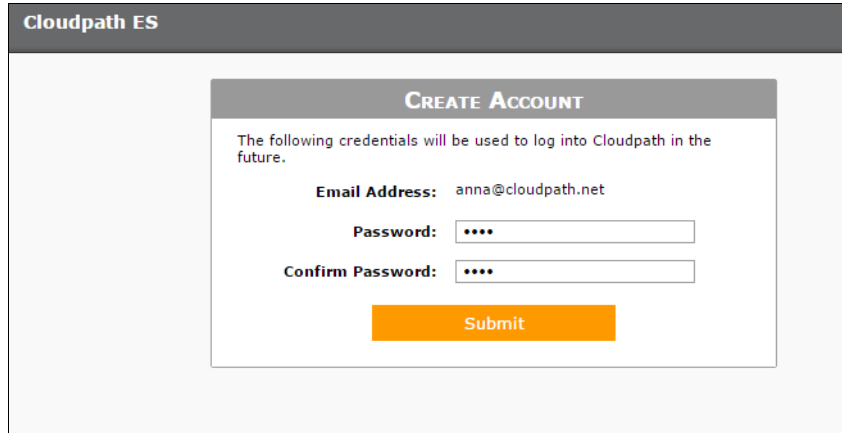
[Already have credentials for the Cloudpath license server?](#)

[Advanced](#)

Set a Password for Account

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

FIGURE 8. Set Password



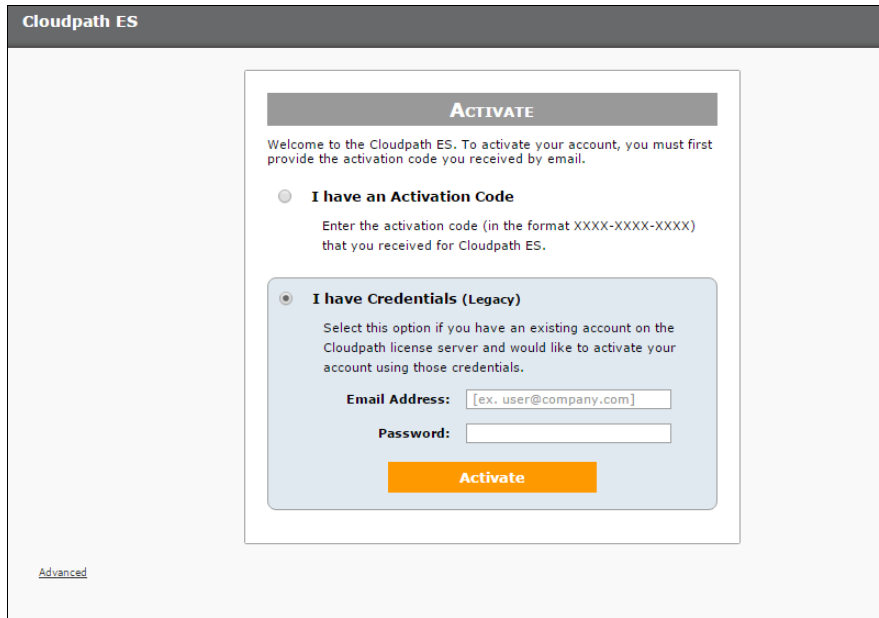
The screenshot shows a web interface for Cloudpath ES. At the top, there is a dark grey header with the text "Cloudpath ES". Below this is a white box with a grey header that says "CREATE ACCOUNT". Inside this box, there is a message: "The following credentials will be used to log into Cloudpath in the future." Below the message, there are three fields: "Email Address:" followed by the text "anna@cloudpath.net", "Password:" followed by a text input field containing four black dots, and "Confirm Password:" followed by another text input field containing four black dots. At the bottom of the form is an orange button with the text "Submit".

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

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

Login with Existing Credentials

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

FIGURE 9. Activate Account With Existing Credentials

The screenshot shows the Cloudpath ES activation page. At the top, it says "Cloudpath ES". Below that is a grey bar with the word "ACTIVATE" in white. The main content area has a light grey background and contains a white box with a grey border. Inside this box, there is a grey bar with "ACTIVATE" in white. Below this, it says "Welcome to the Cloudpath ES. To activate your account, you must first provide the activation code you received by email." There are two radio button options: "I have an Activation Code" (unselected) and "I have Credentials (Legacy)" (selected). Under "I have Credentials (Legacy)", it says "Select this option if you have an existing account on the Cloudpath license server and would like to activate your account using those credentials." Below this, there are two input fields: "Email Address:" with a placeholder "[ex. user@company.com]" and "Password:". At the bottom of the form is an orange "Activate" button. In the bottom left corner of the main page, the word "Advanced" is written in a small, light blue font.

Initial System Setup

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

System Setup Wizard

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

1. Select Server Type.

FIGURE 10. Select Server Type

The screenshot shows a 'System Setup' window with a title bar. Below the title bar is a section titled 'What Type Of Server Is This?' with a 'Next >' button in the top right corner. There are three radio button options:

- 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 Cloudpath ES server.

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

Note >>

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

2. Enter *Company Information*.

This information is embedded in the onboard root CA certificate.

FIGURE 11. Company Information

System Setup

Company Information

[Next >](#)

Company Information

Company Name: *

Legal Company Name: *

Department Name:

City: *

State/Province: *

Country: *

Company Web Presence

Company Domain: *

Support Email: *

IT Email: *

Administrators

Your login has been established an administrator for this system. Additional administrators may be defined within the system or referenced through Active Directory or LDAP. If you would like to add additional administrators, specify them below.

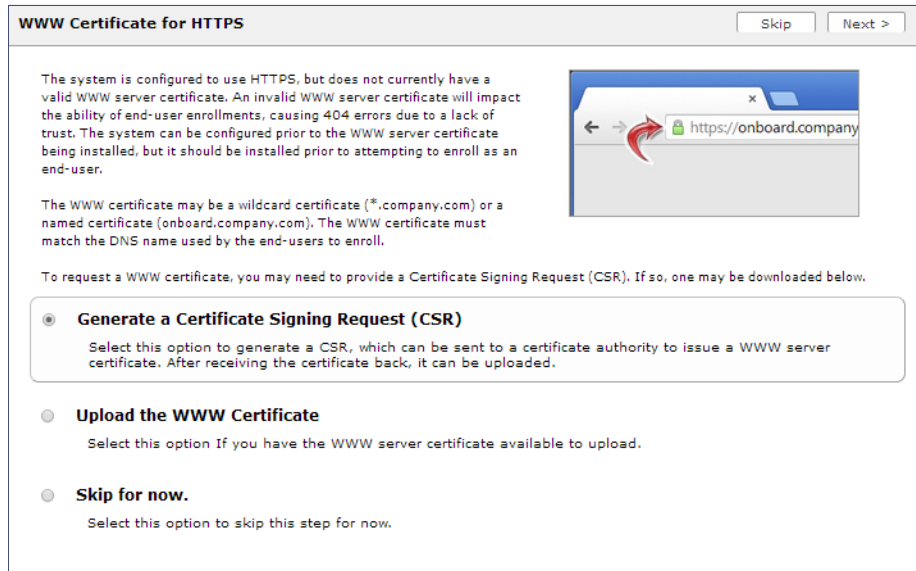
Primary Admin Email:

Additional Admin Email: +

Sample Data

3. (This step is only applicable for on-premise deployment) Configure the WWW Certificate.

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

FIGURE 12. WWW Certificate for HTTPS

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

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

4. Upload the WWW certificate.

FIGURE 13. Upload WWW Certificate

Upload WWW Certificate

P12 Upload

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

P12 File:

P12 Password:

Or PEM Upload

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

Public Key (PEM):

Chain (PEM or P7b):

Private Key (PEM):

Private Key Password:

Prompt for Password on Boot:

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

5. Select the Default Workflow

To initialize the system with a sample configuration, select *BYOD Users & SMS Guests, or BYOD Users Only*. This creates an initial workflow for BYOD users and sponsored guests (or BYOD users only) that you can use as a template, or simply add a device configuration and use immediately.

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

FIGURE 14. Select Default Workflow

System Setup

Setup Workflow Skip Next >

The system may be initialized with a typical configuration or initialized blank. Either way, the system may be fully customized after being initialized. Select your preference below.

- BYOD Users & SMS-based Guests.**
Initializes the system for handling BYOD and guest users. Each user will be configured for the secure WPA2-Enterprise wireless network specified below and issued a certificate granting them BYOD or guest access.
+ Secure SSID Name:
- BYOD Users Only.**
Initializes the system for handling BYOD users. Each user will be configured for the secure WPA2-Enterprise wireless network specified below and issued a certificate granting them BYOD access.
- Start with a Blank Canvas.**
Initializes the system with a blank workflow.

6. Configure the Authentication Server.

Note >>

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


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

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

FIGURE 15. 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.

Use Onboard Database

Select this option to enable end-users to authenticate to accounts defined within this system.

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

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

Consider these settings for the authentication server:

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

7. Set up the Authentication Server Certificate

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

FIGURE 16. Authentication Server Certificate

Authentication Server

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

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:	4B26BB21C61A94EA8CFF35726042108C338F1036
Valid Period:	04/19/2016 - 04/19/2017
Issued By:	Cloupath Networks MSrCA

Upload the Chain for the Server Certificate.

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

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

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

Publishing Tasks

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

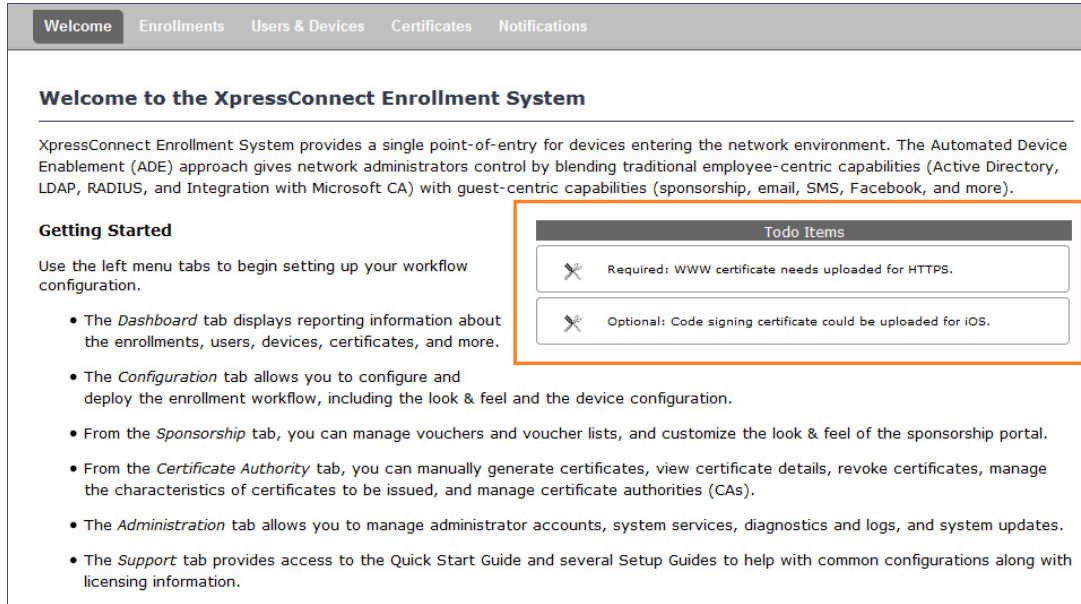
FIGURE 17. System Initialization Task

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:	hgW7mndz3o6vimgH3s
RADIUS Attributes:	BYOD Policy Template - VLAN: 'byod' Guest Policy Template - VLAN: 'guest'
User Experience:	
	End-users will use the enrollment portal to activate devices.
End-User Portal:	https://anna39.cloudpath.net/enroll/AnnaTest/Production/
BYOD:	For BYOD, the authentication is initially configured for a demo Active Directory server. Demo users include 'bob' (password bob1) and 'bill' (password bill1). The authentication configuration may be changed to point at your AD/LDAP server. BYOD users will be moved onto the secure SSID with VLAN 'byod' assigned.
Guests:	Guests will be required to provide a voucher from a sponsor. See the sponsor section below for currently available vouchers and instructions on creating additional vouchers. Sponsorship is one of several mechanisms for handling guests. Guest users will be moved onto the secure SSID with VLAN 'guest' assigned.
Sponsor Experience:	
	The default workflow utilizes sponsorship to authorize guests.
	To create vouchers for guests, sponsors can login to the sponsor portal below.
Sponsor Portal:	https://anna39.cloudpath.net/portal/sponsor/AnnaTest/
	The system is initially configured to allow any AD user to sponsor, so 'bob' and 'bill' will work here too.
Available Vouchers:	The following vouchers are currently available for use. Guest Vouchers - zjh, bwod, mgvi, nsic, kbllw
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 network, and sponsor portal. 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 done, 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.

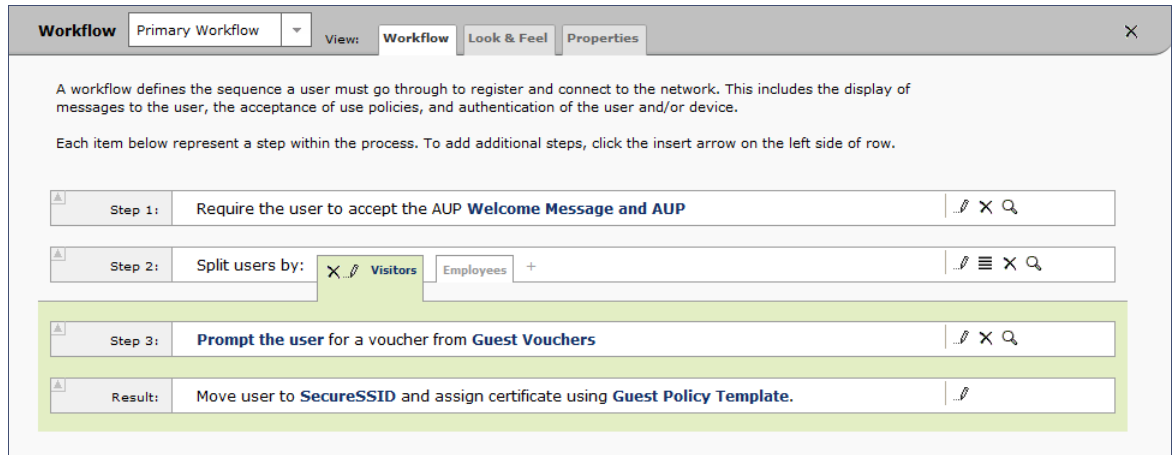
FIGURE 18. ES Welcome Page



Enrollment Workflow

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

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

FIGURE 19. Basic Workflow Configuration

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

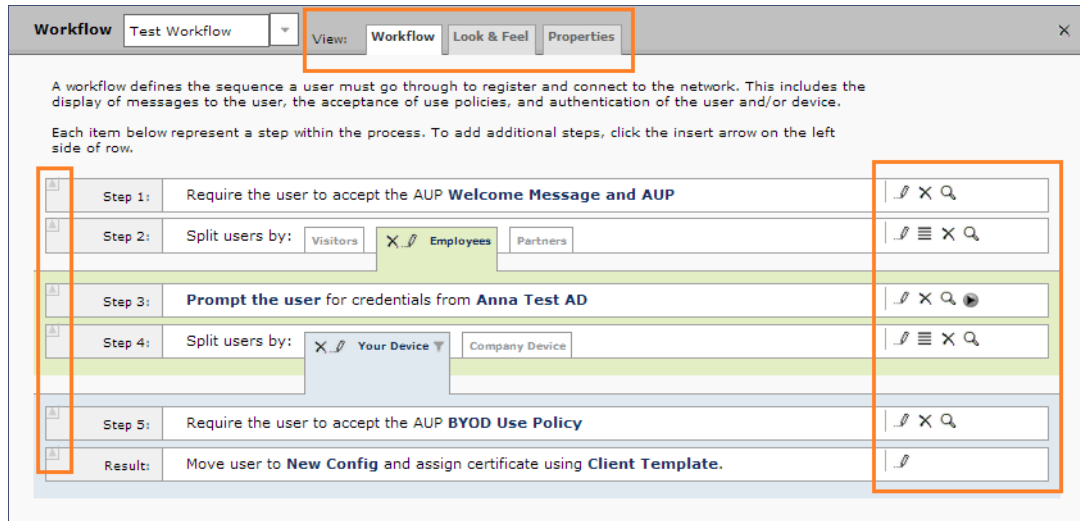
To modify the basic workflow, continue to the next section.

Workflow Basics



The *Workflow* page has three view tabs.

- Use the *Workflow* tab to configure the steps presented to a user during the enrollment process.
- Use the *Look & Feel* tab to configure background and logos displayed on the XpressConnect Wizard during user enrollment.
- Use the *Properties* tab to enable/disable a configuration, or to modify the configuration Name and Description.

FIGURE 20. Enrollment Workflow Page



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

- Use the *Insert* arrows on the top left corner of each step to insert a new enrollment step. Alternately, you can click the blank space between two steps to insert a step.
- Use the icons on the right side of each step to edit, modify, delete, view the enrollment steps.
- Use the *Test Server* icon  to verify interaction with an authentication server.
- Use the *Edit List* icon  to label options, to change the order of the selection options in a split, add more options, or add filters and restrictions.
- Use the icons on the split tabs to modify or delete a specific option.

Modifying a Workflow Template

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

To create a workflow from a template:

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

FIGURE 21. 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 22. Workflow Template

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

Step 1: Acceptable Use Policy.

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

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

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

Step 5: A prompt for a verification voucher.

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

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

Creating a Workflow From a Blank Slate

This section describes how to create a typical workflow from a blank slate. This workflow contains the same steps as the workflow template.

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

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

FIGURE 23. Enrollment Plug-in Selections

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 a user agree to an Acceptable Use Policy (AUP).

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

FIGURE 24. 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

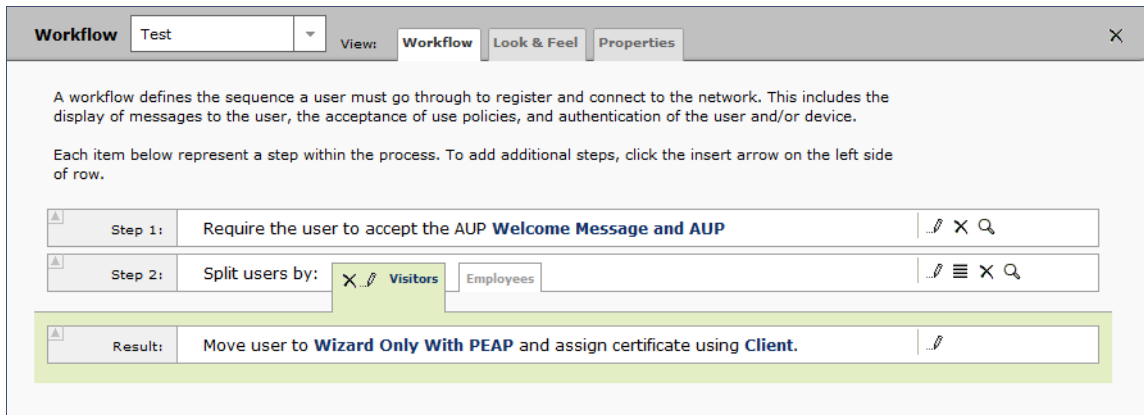
Step 2 in the workflow prompts for the type of user access.

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 25. 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 26. Add Authentication Server

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:

AD Host: *

AD DN: *

AD Username Attribute:

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.

Use Onboard Database

Select this option to enable end-users to authenticate to accounts defined within this system.

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

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


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

Device Type Split

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

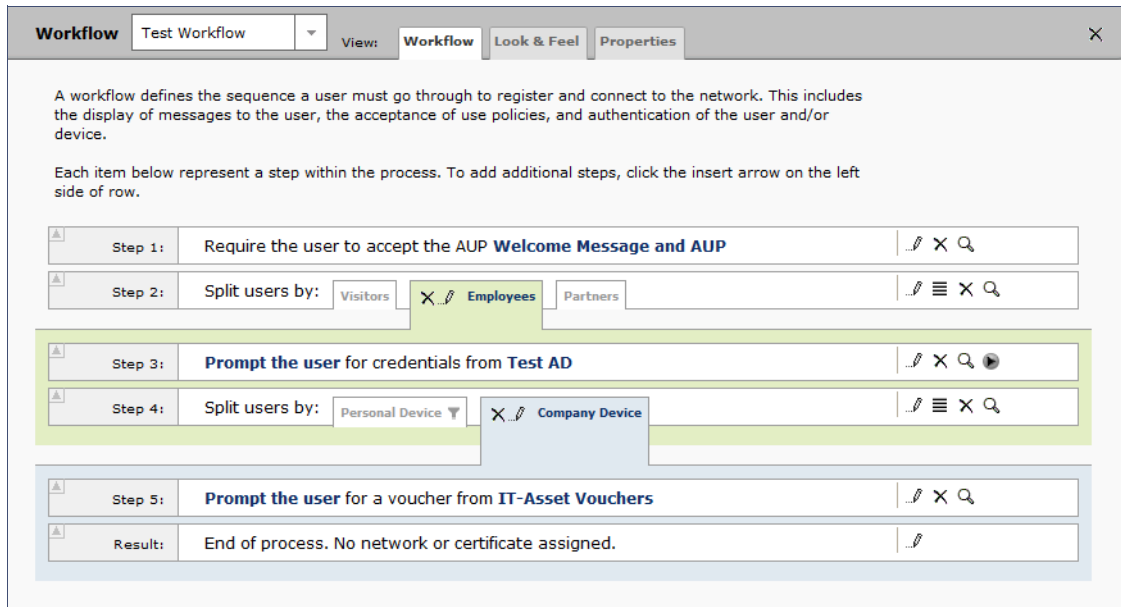
1. Insert a step above the *Result:* step in the enrollment workflow.
2. Select *Split users into different processes*.
3. Select *Use an existing split* and choose *Device Ownership*. The *Device Ownership* option prompts the user to select either *Your Device* or *Company Device*. These labels can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

Tip >>

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

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

FIGURE 27. Workflow with Device Ownership Split



The screenshot shows a workflow configuration interface with 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:** **Prompt the user** for a voucher from **IT-Asset Vouchers**
- Result:** End of process. No network or certificate assigned.

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 *Modify Options* page and configure the *Your Device* split. From this page, you can also set up filters for this split in the workflow.

FIGURE 28. 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:

Username Pattern:

User DN Pattern:

Email Pattern:

Device-Based Filters

Operating System Pattern:

User-Agent Pattern:

MAC Registration List:

Location-Based Filters

Location Pattern:

Allowed IPs:

Blocked IPs:

Filters Based On Web Authentication Certificate

Common Name Pattern:

Issuer Pattern:

Template Pattern:

Expiration Date: Expires Within

Other Filters

Voucher List Name:

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

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

Note >>

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

Prompt for Voucher

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

To create this authorization prompt:

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

FIGURE 29. Create Voucher List

Create Voucher List

Reference Information

Name: *

Description:

API ID: OtpList-729E47A4-C067-43B9-9968-394137DDFBF5

Format

Length:

Characters: ▼

Default Validity Length:

Default Days of Access:

Maximum Days of Access:

Require Username Match:

Notification

Email Subject:

Email Body:

SMS Subject:

SMS Body:

Sponsorship

Allow by LDAP Group: Matching ▼

Allow by LDAP Username: Matching ▼

Allow by LDAP Username DN: Matching ▼

Maximum Certificates:

Default Permissions:

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

New Sponsor Email Subject:

New Sponsor Email Template:

Fields Displayed To Sponsor

Name Field: ▼

Company Field: ▼

Email Field: ▼

SMS Field: ▼

Reason Field: ▼

Redeem By Field: ▼

Days of Access Field: ▼

Initial vouchers

Initial Voucher #1:

Initial Voucher #2:

Initial Voucher #3:

Initial Voucher #4:

Initial Voucher #5:

4. On the *Create Voucher List* page, enter the voucher specifications for the *Employees with Company Devices* workflow.
 - Format - Describes voucher characteristics and validity.
 - Notification - Set up the template for emailing the voucher or sending as an SMS message.
 - Sponsorship - Use this section to configure the *Sponsored Guest Access* feature.
 - Fields Displayed to Sponsors - Controls whether or not each field is displayed and, if so, whether or not it requires input from the sponsor.
 - Initial vouchers - Create one or more initial vouchers.
5. For the voucher prompt, select *Create a new webpage from a standard template*.
6. On the *Create Voucher Prompt* page, enter the data for the voucher prompt and *Save*.

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

Device Configuration and Client Certificate

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

Device Configuration

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

FIGURE 30. Configure SSID

5. Set the *Authentication Style*:
 - Select Client Certificate for TLS network configurations
 - Select PEAP for PEAP/MS-CHAPv2 network configurations
 - Select Static Pre-Shared Key for PSK network configurations
 - Select Ruckus DPSK for a Dynamic Pre-Shared Key network configuration on a Ruckus controller
6. Leave the default *Broadcast* setting and click *Next*.
7. Specify *Conflicting SSIDs*. This setting prevents the device from roaming away from the secure SSID to any open SSID in the area.
8. Select the operating system families and versions that to support within this device configuration. You can restrict a particular version or service pack level after the device configuration is created.

FIGURE 31. 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 require user interaction to configure. Online instructions will be provided to the user.

Generic

Blackberry

Windows RT

Windows Phone 8+

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

Note >>

See the Advanced Configuration for additional RADIUS server settings.

10. Configure additional settings for the device configuration. A more comprehensive list of additional settings is available after the device configuration is created.

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

Client Certificates

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

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

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

Note >>

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

3. In this example, choose the default Root CA that was created during the Cloudpath ES initial configuration.
4. Set up the *Client* certificate template. This template is used to issue a certificate to the client device.

FIGURE 32. Client Certificate Template

What type of certificates should be issued? Cancel Next >

Client Certificates

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

+ Username Decoration:

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

+ Grant Access Until: 1 Years after issuance.

+ Configure Advanced Options:

Lifecycle Notifications

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

Notifications:

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

RADIUS Options

+ VLAN ID: [ex. 50]
+ Filter ID: [ex. BYOD]
+ Class: [ex. BYOD]

Server Certificates

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

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

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

6. Grant access for the appropriate amount of time.

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

Tip >>

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

7. Select any email notifications to be sent to the user related to the life-cycle of the certificate. Additional certificate notifications can be configured after the template is created.
8. Optional. Enter *RADIUS Options* to assign a VLAN ID or Filter ID to certificates that use this template. These settings only applies if you are using the ES onboard RADIUS server.
9. Click *Next*.

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

FIGURE 33. Completed Workflow

The screenshot shows 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 an 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 34. 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** ..f X ✓

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 Explain Chrome Setup

Snapshots: Create New

	Name	Notes	Configuration	Version	Timestamp
Q X ⏻	Snapshot 3		Demo Data	5.0.150	20141113 1115 MST
Q X ⏻	Snapshot 2		Demo Data	5.0.150	20141113 1052 MST
Q X ⏻	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 Cloudpath ES supports multiple locations. For example, a test configuration might be deployed to */test* URL, and a production configuration may be deployed to */production* URL.

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

How to Add a Deployment Location

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

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

FIGURE 35. Modify Deployment Location

Modify Enrollment URL Cancel Save

End-users will access the enrollment pages at the URL specified below. This is embedded into each snapshot, so modifying this value requires a new snapshot be created.

Note: The second value ('AnnaTest') is a system-wide setting and will affect the sponsorship portal URL also. With HTTPS, the first value (hostname) must match the WWW certificate on the server.

https:// /enroll/ / /

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

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

Configuration Snapshots

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

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

How to Deploy a Snapshot of the Workflow Configuration

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

FIGURE 36. Create New Snapshot

Create New Snapshot? ✕

⚠ Are you sure that you want to create and activate a new snapshot?

Workflow: ▼

Wizard Version: ▼

The URL below will be used by end-users during enrollment. It is important that this URL is correct for communication from the end-user to the system. Also, if HTTPS, it is important that the web server certificate and DNS are properly configured. Incorrect setup of this URL may lead to 404 NOT FOUND errors during enrollment. If the end-user is accessing the system through a load balancer, this most likely should be the DNS handled by the load balancer.

URL: https://192.168.7.114/enroll/AnnaTest/Production/

Remove oldest inactive snapshot if 5 exist.

Cancel Create

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

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

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

How to Test a Configuration Snapshot

1. On the left menu, select *Configuration > Deploy*.
2. On the *Deployment Locations* page, in the *Snapshot* section, select the configuration you want to test.
3. Be sure that the snapshot you want to test is the *active* snapshot (green icon).
4. Click the *Go to: User Experience* button to bring up the XpressConnect Wizard and test the enrollment process for the active configuration snapshot.

QR Code

The *QR Code* button generates a QR code image, which when scanned, redirects the user to the deployment location.

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

Explain Chrome Setup

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

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

System Administration

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

- **Administrators** - Manage administrators, group logins, restrict access to the ES Admin UI, and reset administrator passwords.
- **System** - View and manage system information, upgrade the application, and configure replication.
- **Advanced** - Manage system information, view logs (diagnostic and debug), configure SMS gateways and country codes, and clean up the database.

Ruckus Controller Integration for Cloudpath

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

Set up the Cloudpath ES as an AAA Authentication Server

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

FIGURE 37. Create AAA Authentication Server SmartZone

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

1. Name
2. Type = RADIUS
3. Auth Method = PAP
4. IP address = The IP address of the Cloudpath ES.
5. Port = 1812
6. Shared Secret = This must match the shared secret for the Cloudpath ES onboard RADIUS server. (*Configuration > Advanced > RADIUS Server*).

Note >>

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

7. Leave the default values for the remaining fields.

Create AAA Accounting Server (Optional)

Use the same process to create the AAA Accounting Server.

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

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

Note >>

For on-premise deployments the port numbers are 1812 (RADIUS) and 1813 (RADIUS Accounting). For Cloud-based deployments the port numbers are listed on the Cloudpath Configuration > RADIUS Server page.

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

Run Authentication Test

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

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

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

If you receive:

Failed! Invalid username or password

Ignore this error message. This means that connectivity was established.

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

FIGURE 38. Authentication Test SmartZone

Create Hotspot Services

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

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

FIGURE 39. Create Hotspot WISPr on SmartZone

3. Point the unauthenticated user to the Cloudpath redirect URL. Enter the WLAN Redirect URL, which can be found on the Cloudpath Admin UI Configure > Deploy page.
4. Check Redirect to the URL that the user intends to visit. For more information on setting this URL see, *Deploying the Enrollment Workflow*.
5. Select Use device MAC address as authentication password.
6. Leave the defaults for the remaining settings. Click OK.

Set Up the Walled Garden

Enter the following values for the Walled Garden:

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

FIGURE 40. Walled Garden Configuration for SmartZone

Walled Garden

Walled Garden Entry *

Walled Garden Entry

72.18.151.76	
--------------	--

Unauthenticated users are allowed to access the following destinations.
Format:

- IP (e.g. 10.11.12.13)
- IP Range (e.g. 10.11.12.13-10.11.12.15)
- CIDR (e.g. 10.11.12.100/28)
- IP and mask (e.g. 10.11.12.13 255.255.255.0)
- Precise web site (e.g. www.ruckus.com)
- Web site with special regular expression like
 - *.amazon.com
 - *.com

Apply Cancel

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

Create the Onboarding SSID

Enter the following values for the onboarding SSID:

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

FIGURE 41. Onboarding SSID Configuration on SmartZone

The screenshot displays the configuration page for a 'Lab Onboard SSID'. The page is titled 'Edit WLAN Config: [Lab Onboard SSID] of zone [Cloudpath APs]'. It features several expandable sections:

- General Options:** Name, SSID, HESSID, and Description fields, all containing 'Lab Onboard SSID'.
- WLAN Usage:** Access Network (checkbox), Authentication Type (radio buttons: Standard usage, Hotspot (WISPr), Guest Access + Hotspot 2.0 Onboarding, Web Authentication, Hotspot 2.0 Access, Hotspot 2.0 Secure Onboarding (OSEN), WeChat). 'Hotspot (WISPr)' is selected.
- Authentication Options:** Method (radio buttons: Open, 802.1x EAP, MAC Address). 'Open' is selected.
- Encryption Options:** Method (radio buttons: WPA2, WPA-Mixed, WEP-64 (40 bits), WEP-128 (104 bits), None). 'None' is selected.
- Hotspot Portal:** Hotspot (WISPr) Portal (dropdown: Lab Hotspot Services), Bypass CNA (checkbox: Enable), Authentication Service (checkbox: Use the controller as proxy, dropdown: Lab AAA Auth), Accounting Service (checkbox: Use the controller as proxy, dropdown: Lab AAA Acct, Send interim update every 10 Minutes (0-1440)).
- Options:** Acct Delay Time (checkbox: Enable), Wireless Client Isolation (radio buttons: Disable, Enable (Isolate wireless client traffic from all hosts on the same VLAN/subnet)), Priority (radio buttons: High, Low). 'Enable' and 'High' are selected.
- RADIUS Options:** (Collapsed)
- Advanced Options:** (Collapsed)

At the bottom, there are 'Apply' and 'Cancel' buttons.

3. Authentication Option Method=Open.
 4. Encryption Option Method=None.
 5. Select the Hotspot Service created in Task 2.
 6. Enable Bypass CNA. This setting is in the Hotspot Portal section.
 7. Select the Cloudpath RADIUS Authentication Server.
 8. Select the Cloudpath RADIUS Accounting Server
- Leave the defaults for the remaining settings and click OK (or Apply).

Create the Secure SSID

Enter the following values for the secure SSID:

1. Name the SSID.
 2. Type=Standard Usage.
 3. Authentication Option Method=802.1x EAP.
 4. Encryption Option Method=WPA2
 5. Encryption Option Algorithm=AES
 6. Select the Cloudpath RADIUS Authentication Server.
 7. Select the Cloudpath RADIUS Accounting Server
- Leave the defaults for the remaining settings and click OK (or Apply).

FIGURE 42. Configure Secure SSID on the SmartZone controller.

Create New WLAN Configuration

General Options

Name: * Lab Secure SSID
 SSID: * Lab Secure SSID
 HESSID:
 Description:

WLAN Usage

Access Network: Tunnel WLAN traffic through Ruckus GRE
 Authentication Type: * Standard usage (For most regular wireless networks)
 Hotspot (WISPr)
 Guest Access + Hotspot 2.0 Onboarding
 Web Authentication
 Hotspot 2.0 Access
 Hotspot 2.0 Secure Onboarding (OSEN)
 WeChat

Authentication Options

Method: * Open 802.1x EAP MAC Address

Encryption Options

Method: * WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None
 Algorithm: * AES AUITO (TKIP+AES)
 802.11w MFP: * Disabled Capable Required

Authentication & Accounting Server

Authentication Server: * Use the Controller as Proxy Lab AAA Auth
 Accounting Server: Use the Controller as Proxy Lab AAA Acct. Send interim update every 5 Minutes (0-1440)

Options

Acct Delay Time: Enable
 Wireless Client Isolation: * Dtable
 Enable (Isolate wireless client traffic from all hosts on the same VLAN/subnet)
 Priority: * High Low
 Zero-IT Activation: Enable Zero-IT Activation (WLAN users are provided with a wireless configuration installer after they log on)

RADIUS Options

Advanced Options

OK Cancel

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

Troubleshooting Your Deployment

Connectivity Issues

Cloudpath License Server

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

RADIUS Server

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

Firewall Requirements

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

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

FIGURE 43. 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)	OCSP requests coming from external systems.
SSH	AnnaTest.cloudpath.net:8022		TCP	SSH access to the system.
Onboard RADIUS	AnnaTest.cloudpath.net:1812		UDP	Receive RADIUS requests from external systems.

Issues with User Credentials

Active Directory

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

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

Credentials Mismatch

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

LDAP

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

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

For more troubleshooting information, see *Cloudpath Enrollment System Deployment Guide* Release 4.3.

Test Deployment locally

You can test the deployment:

Note >>

This example only depicts the Windows environment. For other OS, see, <https://support.ruckuswireless.com/documents?filter=89#documents>

1. Click **User Experience** tab.

FIGURE 44. User Experience

XpressConnect Enrollment System | Ruckus QA Logout

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 Portal:** <https://bdctf.ruckuswireless.com/>
or <https://bdctf.ruckuswireless.com/enroll/RuckusBDCqa/Production/> Change
- WLAN Redirect URL:** <https://bdctf.ruckuswireless.com/enroll/RuckusBDCqa/Production/redirect>
- Sponsorship Portal:** </portal/sponsor/RuckusBDCqa/>

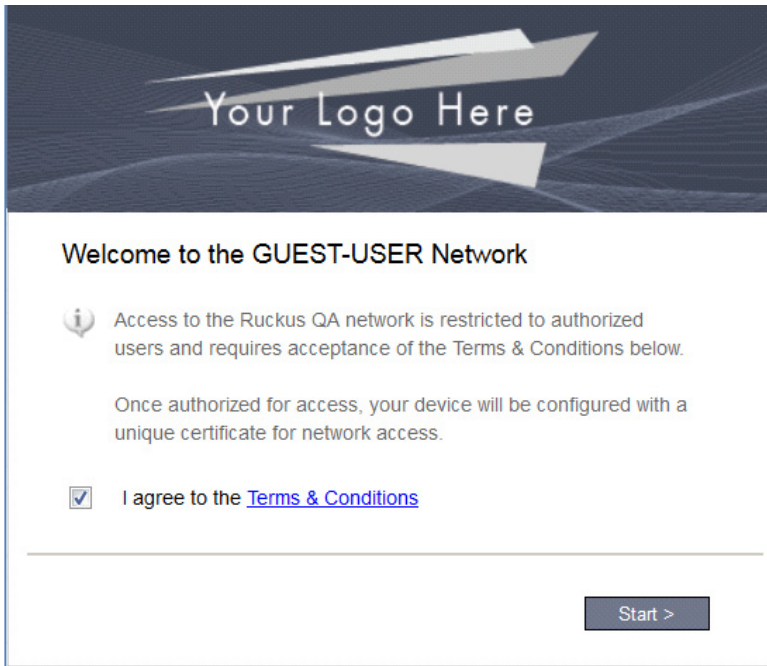
Go To: User Experience Sponsor Portal Get QR Code Explain Chrome Setup

Snapshots: Create New

	Name	Notes	Configuration	Version	Timestamp
Q X ⊕	Snapshot 3		SCG-GUEST_USER	5.0.273	20160125 1127 UTC
Q X ⊕	Snapshot 2		SCG-Test	5.0.273	20160123 1204 UTC
Q X ⊕	Snapshot 1		Primary Workflow	5.0.273	20160121 1856 UTC

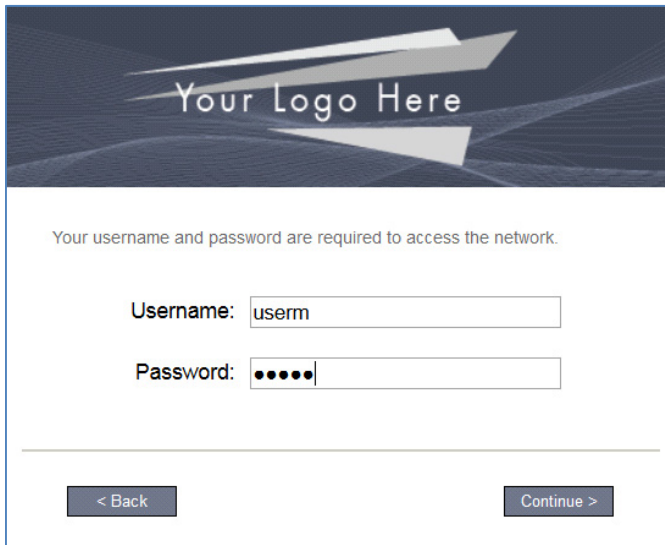
- The Network interface is displayed on the client. You are prompted to agree to **Terms and Conditions**.

FIGURE 45. Client Confirmation



- Enter your **Username** and **Password**

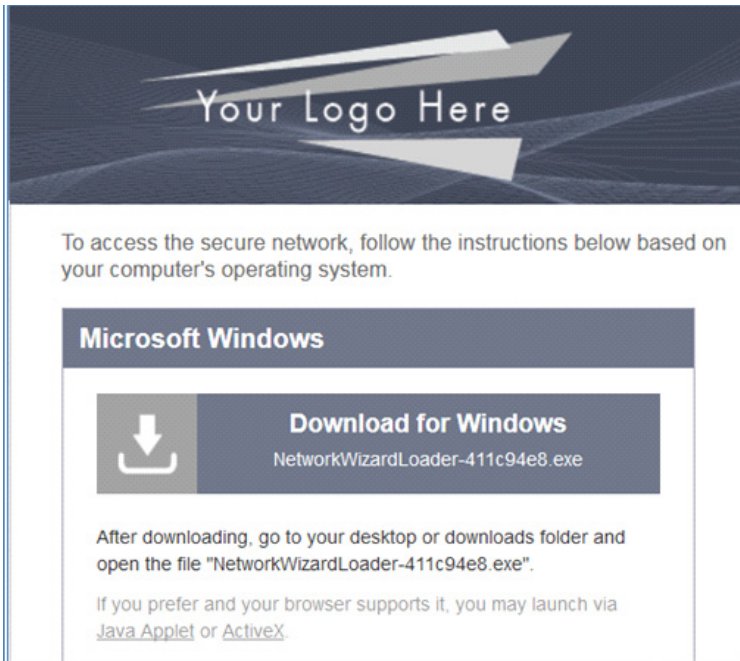
FIGURE 46. Access the Network



The image shows a network access login interface. At the top, there is a dark blue header with the text "Your Logo Here" in white. Below the header, a message states: "Your username and password are required to access the network." There are two input fields: "Username:" with the text "userm" and "Password:" with five black dots. At the bottom, there are two buttons: "< Back" on the left and "Continue >" on the right.

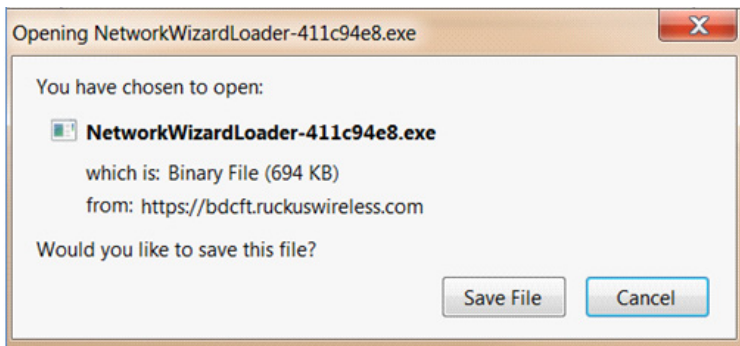
4. You are prompted to download the .exe file for installing on the device.

FIGURE 47. Download .exe File

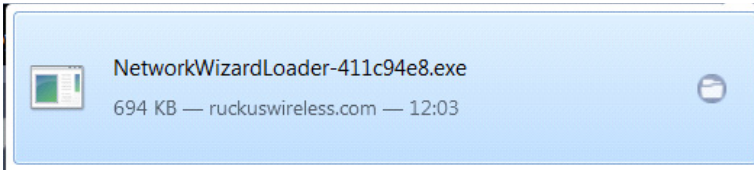
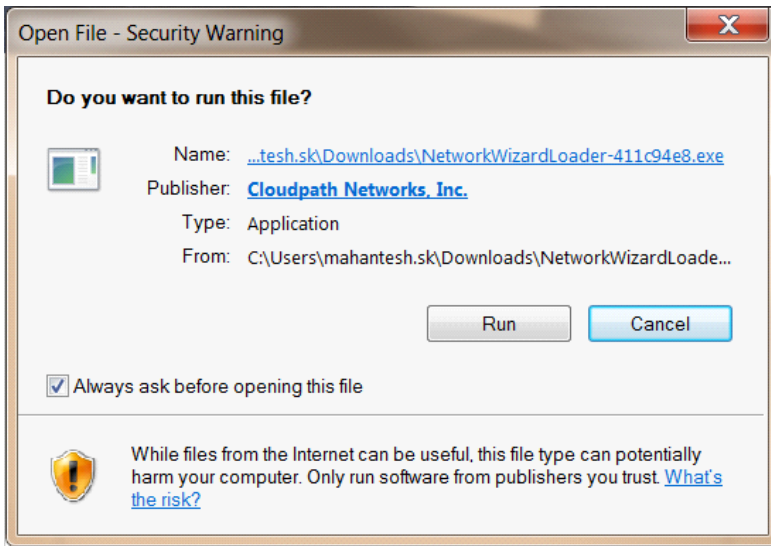


5. Save the downloaded .exe file

FIGURE 48. Save the File

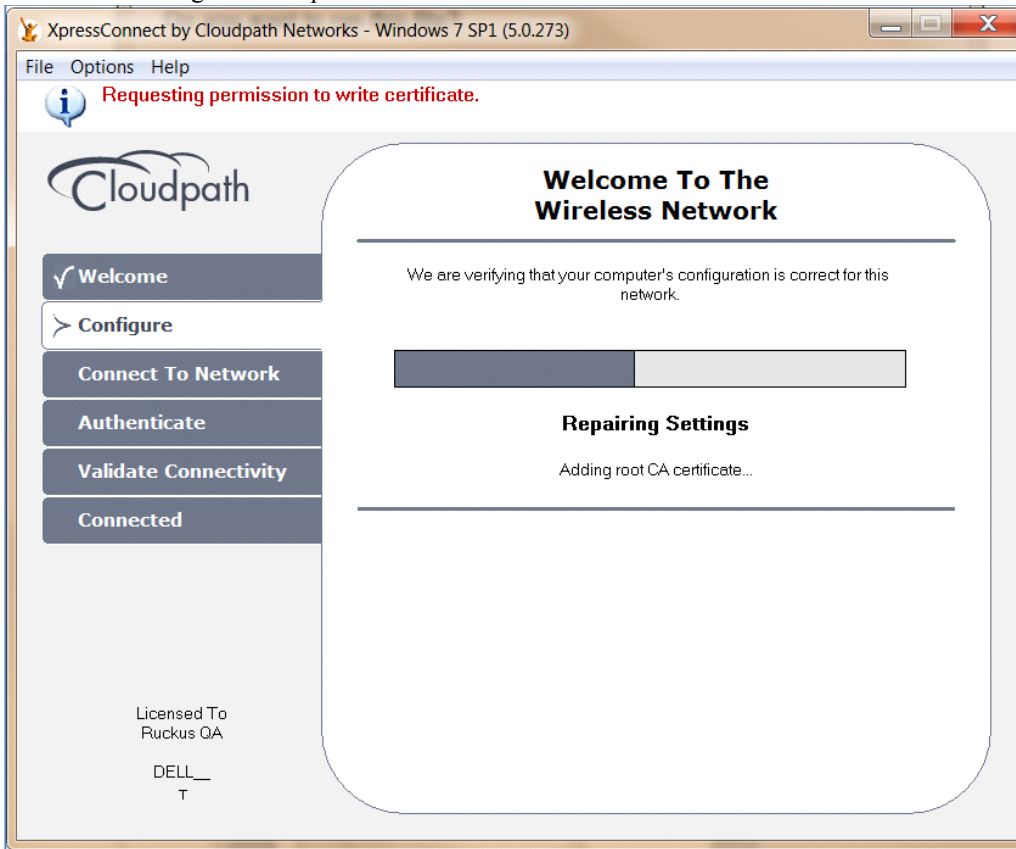


Your .exe file is displayed.

FIGURE 49. .exe Filename**6.** Run the .exe file**FIGURE 50.** Run the .exe File

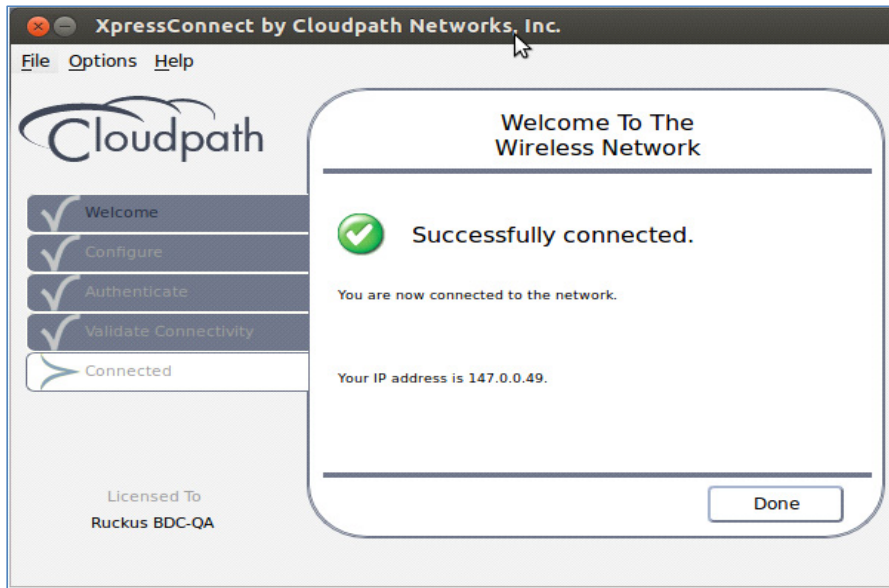
7. Cloudpath gets configured on your device

FIGURE 51. Configure Cloudpath



8. After the **Authentication** and **Connectivity** is validated, you are successfully connected.

FIGURE 52. Connection Successful Confirmation



Monitor the Client on SmartZone

1. Go to **Monitor > Clients**.

The **Associated Clients List** page appears and displays a table that lists all access points that are currently associated with the managed access points.

FIGURE 53. Monitor Client in AP Zone

Monitor >> Clients

Associated Client in AP Zone: ZONE_DBR

View all clients that are currently associated with the selected zone. To filter the client list, click **Load Criteria**, and then configure the filters that you want to apply.

Associated Clients | TTG Clients Statistics

Refresh | Export CSV

Load Criteria: Zone = 'ZONE_DBR'

STA MAC Address	IP Address	OS Type	Host Name	AP Name	WLAN (SSID)	VLAN	Channel	Status	User Name	Auth Method	Encryption Method	Actions
08:3E:8E:82:F9:0D	147.0.0.49	N/A	N/A	RuckusAP	ENG-Mahan_XpressES	1004	1	AUTHORIZED	userm@tyrod.ruckuswireless.com	Standard+802.1X	WPA2_AES	

Show 20 >>> <<< | 1 | >>>

Congratulations! You have successfully configured Cloudpath on SmartZone 3.4.