

XpressConnect Enrollment System

Deploying the Enrollment System as a Virtual Appliance on a VMware™ Server

Software Release 4.2

December 2015

Summary: This document describes the specifications for deploying the Enrollment System as a virtual appliance, how to download and deploy the package, and initial configuration and account setup. This guide also includes the Enrollment System command reference, which provides descriptions and examples for the commands that can be entered from the VMware client console or from an SSH login.

Document Type: Configuration

Audience: Network Administrator



Deploying the Enrollment System as a Virtual Appliance on a VMware Server

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.

Deploying the Enrollment System as a Virtual Appliance on a VMware™ Server

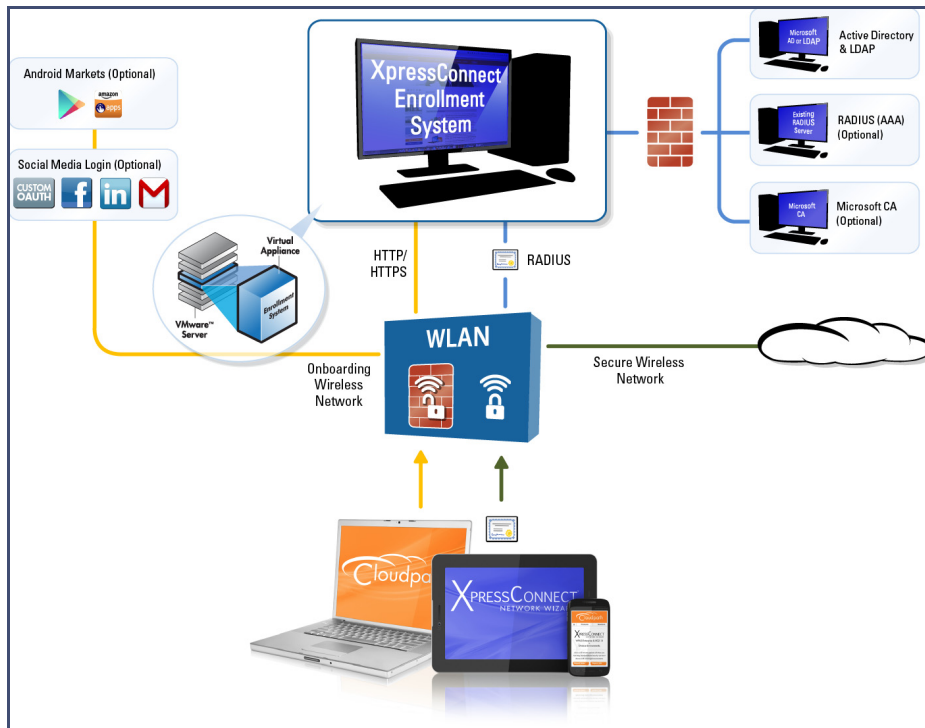
Overview

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.

The 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).

FIGURE 1. Enrollment System Deployment Example



Specifications for Locally-Deployed VMware Server

Enrollment System Virtual Appliance Specifications

The Enrollment System virtual appliance is deployed as an open virtualization archive (OVA) file, which can be deployed on any VMware ESXi server (ESX or ESXi architecture 4.x and 5.x and greater).

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.

Treating the Enrollment System as a Physical Appliance

The XpressConnect ES is delivered as a VMware virtual appliance. This provides the administrative simplicity of a traditional appliance, the resource flexibility of virtual machines, and avoids the logistical and physical constraints of physical servers. However, in some environments, physical appliances are preferred, either due to a lack of VMware infrastructure or due to administrator preference.

In these situations, the Enrollment System may be treated similar to a physical appliance by placing it on a dedicated VMware vSphere ESXi server. ESXi is VMware's bare metal hypervisor and, unlike VMware's management platform vCenter, ESXi is free. It does require a VMware account to download and a license key to install, but these are available without charge from the VMware website.

When deployed in this model, size the physical server to have at least 2-4 GB of RAM greater than the virtual appliance requires. Additional RAM may be desirable to allow multiple VMs to be running concurrently.

The ESXi 5.5 ISO is available at https://my.vmware.com/web/vmware/details?downloadGroup=ESXI55U2&productId=353#product_downloads under the *ESXi 5.5 Update 2d ISO image (Includes VMware Tools)* entry.

What You Need

For Deployment

- OVA file for the Enrollment System virtual appliance
- VMware Client

For Virtual Appliance Initial Configuration

- FQDN Hostname of the virtual appliance
- A list of IP addresses that are allowed Administrative access (optional)

- Service account security credentials
- IP address and subnet mask for the virtual appliance (not required if using DHCP)
- Gateway IP address for your network (not required if using DHCP)
- IP address of DNS server (not required if using DHCP)

For Enrollment System Account Setup

- URL for the VMware server where the Enrollment System is deployed
- URL for the XpressConnect Licensing Server
- Login credentials for the XpressConnect Licensing Server
- Web certificate for the Enrollment System virtual appliance (public-signed)

Supported Browsers

- Internet Explorer 6.0 and greater
- Firefox 1.5 and greater
- Safari 2.0 and greater
- Chrome 3.0 and greater

Supported Operating Systems

- Windows XP SP2 and greater
- Mac OS X 10.5 and greater
- Apple iOS 2.0 and greater
- Ubuntu 9.04 and greater
- Fedora 18 and greater
- Android 2.1 and greater
- Windows Phone 8.0 and 8.1
- Chromium, all Google-supported versions

Deploying the ES Virtual Appliance to a VMware Server

The deployment process consists of the following steps:

Retrieve OVA File

Deploy Virtual Appliance

Test Network Connectivity

How to Install VMware Tools

How to Increase the Virtual Appliance Memory

How to Expand the MySQL Partition Size

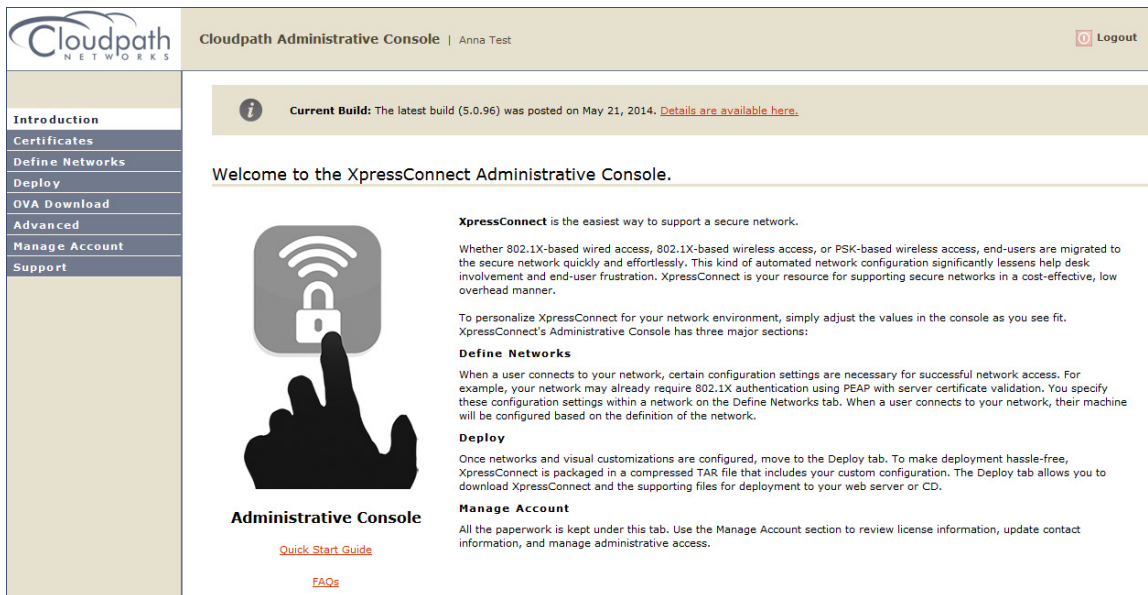
Retrieve OVA File

Retrieve the Enrollment System OVA file from the Licensing Server *OVA Download* tab, from a direct download link, or from a sales or support representative.

To retrieve the OVA file using the XpressConnect Licensing Server:

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

FIGURE 2. Licensing Server Welcome Page



The XpressConnect Licensing Server is the management application where accounts and licenses are managed.

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

Note >>

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

FIGURE 3. OVA Download Page

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

Deploy Virtual Appliance

Set Up Virtual Appliance Using the VMware Client

1. Open the VMware client.
2. Select *File > Deploy OVF Template*.
3. Enter the file path or URL where the OVA file resides.
4. 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.

7. Continue the configuration with vCenter, or a non-vCenter console.
 - If you are using the vCenter to configure application and network properties, continue to the next section.

- If you are using the console to configure application and network properties, review the initial settings and click *Finish*. See Console-Based Configuration to complete the deployment process.

Application Properties (vCenter)

Customize the application properties for the deployment.

FIGURE 4. Application Properties

Application

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

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

Hostname(FQDN)
 Enter the fully qualified domain name.

Timezone

Should Apache be configured for SSL?

Do you want to permit SSH?

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

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

Enter password

Confirm password

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

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

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

Note >>

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

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

Networking Properties (vCenter)

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*.

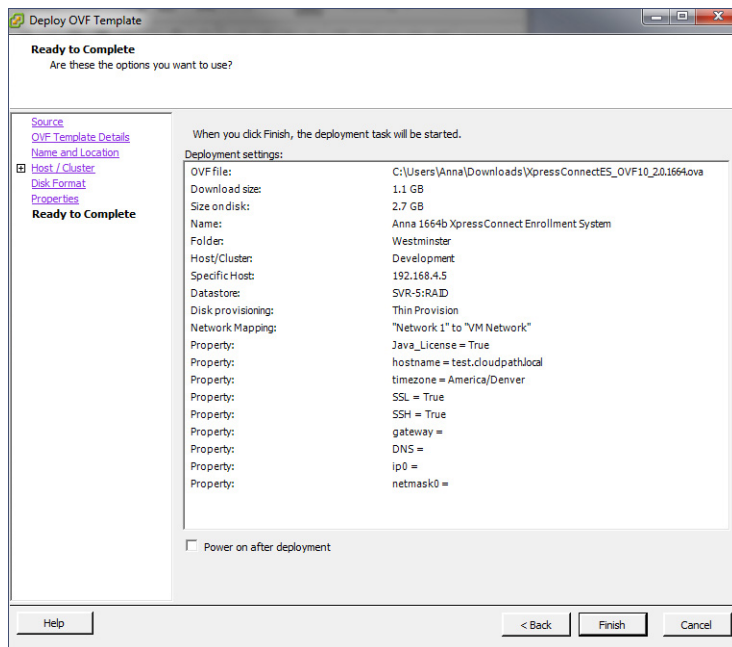
FIGURE 5. Networking Properties

Networking Properties	
Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired.
<input type="text" value="172.16.8.1"/>	
DNS	The domain name servers for this VM (comma separated). Leave blank if DHCP is desired.
<input type="text" value="172.16.2.406"/>	
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired.
<input type="text" value="172.16.6.24"/>	
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired.
<input type="text" value="255.255.252.0"/>	

Confirm Deployment Settings

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

FIGURE 6. Deployment Settings



Click *Finish*. Deployment takes approximately 2 minutes.

Tip >>

If you plan to install VMware Tools, leave the *Power on after deployment* box unchecked. The first few steps of the installation process occur with the image powered-off. See [How to Install VMware Tools](#).

Console-Based Configuration

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

1. Press *Enter* to begin setup.
2. Press *Enter* to accept the Java license agreement. Use the space bar to view *More* pages.
3. Enter *yes* (or *y*) to accept all license agreements.
4. Press *Enter* to scroll through the list of supported time zones. Enter your time zone in the format specified. For example, enter *MST*.

5. Enter the *FQDN hostname* for the virtual appliance (for example, *onboard.company.com*).
6. Do you want to enable HTTPS? Enter *y* (recommended) or *n*.
7. Do you want to use a STATIC IP (rather than DHCP)? Enter *y* or *n*.
 - If you enter yes (recommended), you assign the IP address of the virtual appliance, subnet mask, and gateway and DNS server IP addresses for your network.
 - If you enter no, DHCP is used to assign IP address of the virtual appliance eth0 interface, subnet mask, gateway, and DNS server IP addresses for your network. If you are not using DHCP, enter the IP address of the virtual appliance eth0 interface.
8. Enter the IP address of the virtual appliance.
9. Enter a subnet mask in the format 255.255.252.0.
10. Enter the gateway IP address for your network.
11. Enter the DNS server IP address.
12. Do you want to permit SSH access? Enter *y* or *n*.
13. Enter and confirm a *service* password. The *service* password is used by your support team for access to this system using SSH. Refer to the *Enrollment System Command Reference* on the *Support* tab for details.

Note >>

The *service* account is not available if SSH access is not permitted.

14. Do you want to use an NTP server other than pool.net.org? *y* or *n*.

The setup is complete. Press *Enter* to reboot the system. After the reboot you are presented with the *shelluser* login prompt.

Note >>

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

Service Account

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

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

Use these instructions if you want 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 autocomplete 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

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

Use these instructions to expand 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
```

- 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
```

- Expand the physical volume.

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

- 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
```

- 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
```

- Verify the amount of free disk space available.

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

The output should indicate the increased partition size.

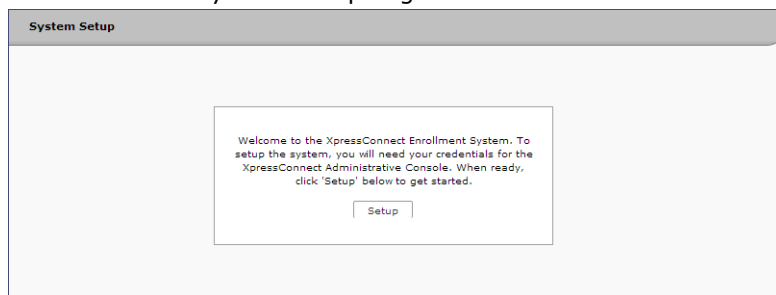
Initial System Setup

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

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

FIGURE 7. Initial System Setup Page



- When you have the information you need, click *Setup*.

3. Enter your XpressConnect Licensing Server login credentials. This step binds the Enrollment System to the Licensing Server.

FIGURE 8. Licensing Server Credentials

The screenshot shows a web-based 'System Setup' wizard. The title bar reads 'System Setup'. Below it is a section titled 'Setup Account' with a 'Next >' button in the top right. The main content area contains the following text: '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 >'. Below this text are three input fields: 'Administrative Console URL' with the value 'https://test.company.net', 'Email Address' with the value 'user@company.net', and 'Password' with four asterisks. Each input field has a small asterisk icon to its right.

4. Select the type of server to set up.

FIGURE 9. Select Server Type

The screenshot shows the 'System Setup' wizard at the 'What Type Of Server Is This?' step. The title bar reads 'System Setup'. Below it is a section titled 'What Type Of Server Is This?' with a 'Next >' button in the top right. The main content area contains three radio button options: 'Standard Server (Default)' (selected), 'Add-On Server For Cluster', and 'Replacement Server For Existing Server'. Each option has a brief description below it. The 'Standard Server (Default)' option is highlighted with a light blue background.

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

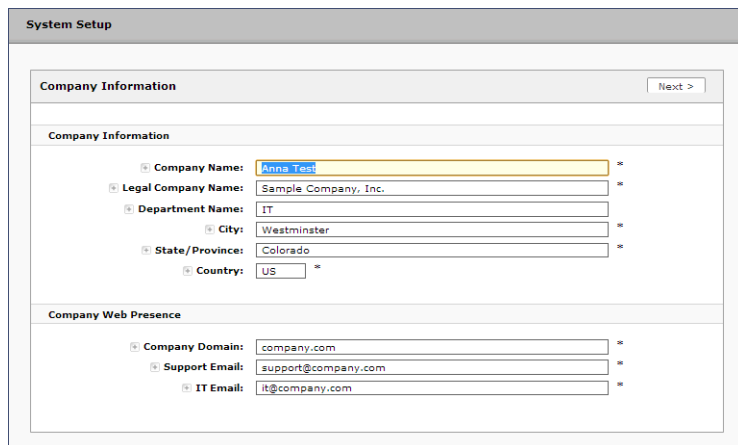
- If you are setting up this server to replace an existing server, and you are importing the database from the existing server, select *Replacement Server for Existing Server*.

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

Note >>

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

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

FIGURE 10. Company Information

The screenshot shows the 'System Setup' window with the 'Company Information' section active. The form contains the following fields:

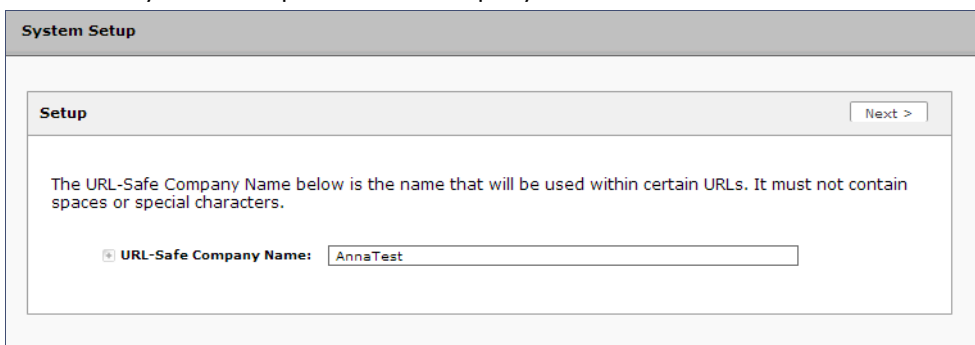
- Company Name: Anna Test *
- Legal Company Name: Sample Company, Inc. *
- Department Name: IT *
- City: Westminster *
- State/Province: Colorado *
- Country: US *

Below this is the 'Company Web Presence' section with the following fields:

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

A 'Next >' button is located in the top right corner of the form area.

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

FIGURE 11. System Setup URL-Safe Company Name

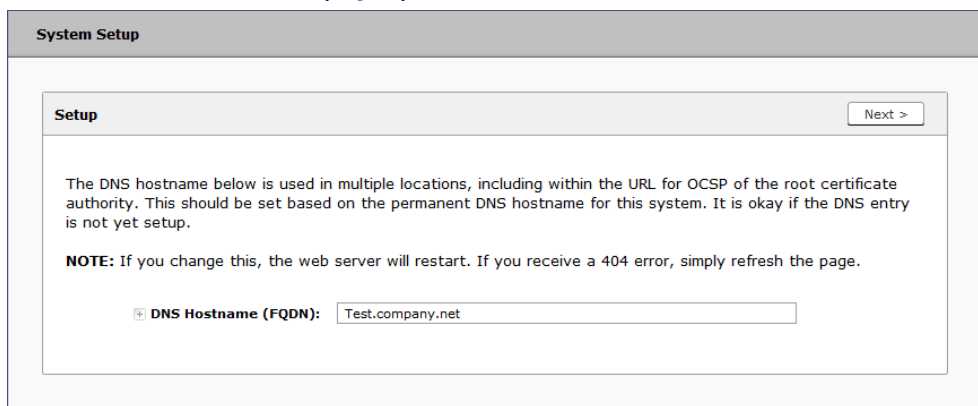
The screenshot shows the 'System Setup' window with the 'Setup' section active. The form contains the following field:

- URL-Safe Company Name: AnnaTest *

A 'Next >' button is located in the top right corner of the form area. A note above the field states: 'The URL-Safe Company Name below is the name that will be used within certain URLs. It must not contain spaces or special characters.'

7. Enter the *DNS Hostname (FQDN)*. This is pre-populated with the system DNS hostname and is in the URL for Online Certificate Status Protocol (OCSP) of the root CA.

FIGURE 12. DNS Hostname (FQDN)



The screenshot shows a web interface titled "System Setup". Inside, there is a "Setup" section with a "Next >" button. The text explains that the DNS hostname is used in multiple locations, including the OCSP URL for the root certificate authority. A note states that changing this will restart the web server and a 404 error should be refreshed. A text input field is labeled "DNS Hostname (FQDN):" and contains the value "Test.company.net".

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 13. 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 14. Authentication Server Certificate

The screenshot shows a web-based configuration window titled "Authentication Server" with navigation buttons for "< Back" and "Next >". The main content area contains the following text: "To use LDAPS, the system needs to know which server certificate to accept for the authentication server." Below this, 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: AC247E58885FD6531C284889D7CF4897036ED849

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

Issued By: Cloudpath Networks MSNCA

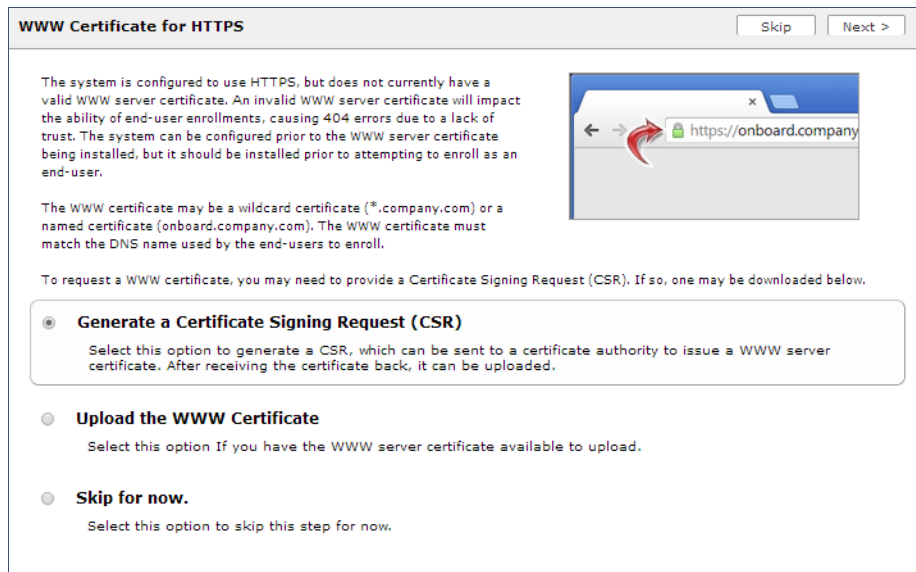
Select *Upload the Chain for the Server Certificate* to upload a certificate chain from an issuing CA. You must specify the common name for the LDAPS server certificate. This certificate does not need to be updated when the certificate is renewed.

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 15. 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*.

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 16. 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: Browse... No file selected.

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): Browse... No file selected.

Chain (PEM or P7b): Browse... No file selected.

Private Key (PEM): Browse... No file selected.

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 17. 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 18. RADIUS Server Selection

The screenshot shows a configuration window titled "RADIUS Server Selection" with "Skip" and "Next >" buttons in the top right. The main text reads: "To authenticate end-users, either the onboard RADIUS server or an external RADIUS server may be used." There are three radio button options:

- Use the onboard RADIUS server.** (Selected)
 - 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:** testtest
- 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.

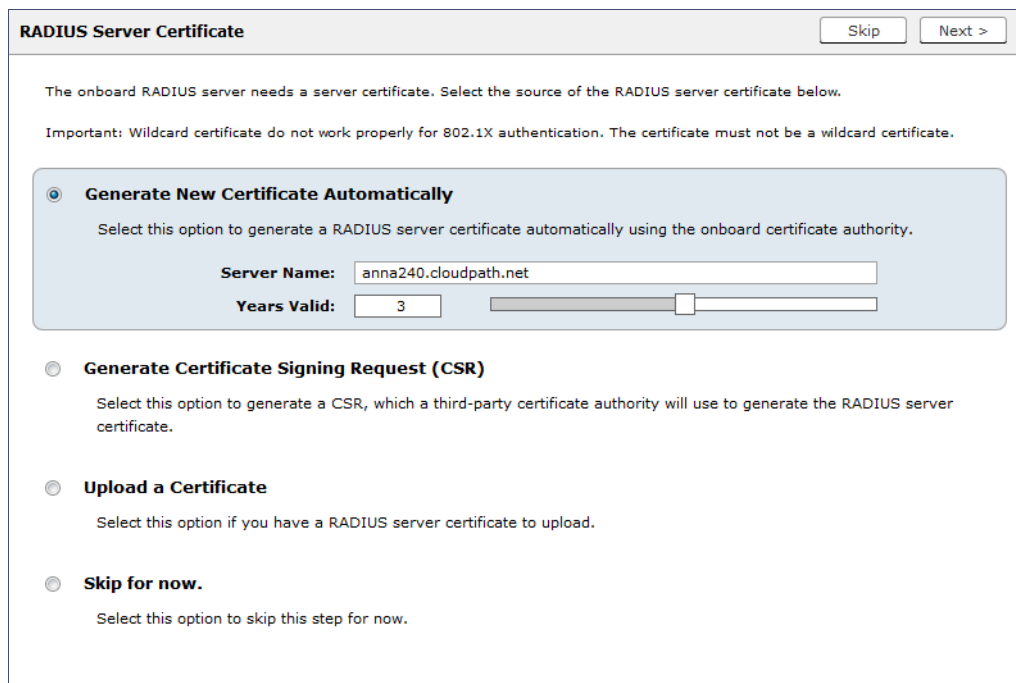
If you skip this step, you can set up a RADIUS server in the workflow.

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

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

FIGURE 20. 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.

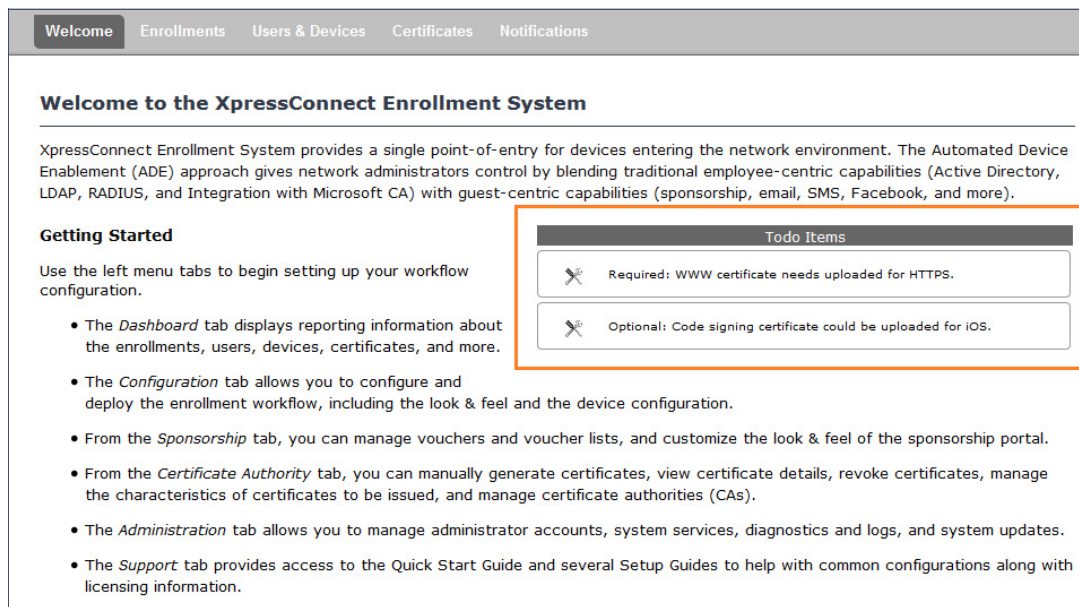
FIGURE 21. System Initialization Task

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:	hw7mnb8366vmzgh8s
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, bvoid, nvgv, nslc, kblw
Administrator Experience:	
Administrator UI:	https://anna39.cloudpath.net/admin/
Credentials:	The following email addresses have been sent a one-time password along with this information: If you ever forget your password, you can reset it from the login screen.
Key Pages:	View Enrollments - View information about enrolled devices, users, and policies. Configure Workflow - Modify the workflow that an end-user passes through to get on the network. This page also contains links for modifying the configuration of the authentication server, wireless network, and guest access. 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 22. ES Welcome Page



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

Command Reference

You can access the Enrollment System command line using the *service* account.

The *service* account is used by your support team to access the system. To use the service account, open a terminal and enter `cpn_service` at the login prompt, and enter the service password.

Tip >>

The default SSH port number is 8022, but can be changed to port 22 on the *Administration > System > System Status* page.

After a successful login to the service account, the command-line configuration utility prompt (`#`) displays. Enter `?` to view the list of available commands.

Tip >>

From the command-line configuration utility, enter the `console` command to access the Linux shell. From the Linux shell, enter the `config` command to access the command-line configuration utility.

Command List

config commands
 console command
 diag commands
 maintenance commands
 replication commands
 show commands
 support commands
 system commands

config commands

The **config** commands allow you to change the configuration of the system.

TABLE 1. **config commands**

Command	Description	Parameters and Examples
config	From the Linux shell, this command provides access to the command line configuration utility.	No parameters. <code>[<serviceacctlogin@<fqdnhostname>]\$ config</code>
config admin allow-access	Clears restrictions to the administrative functionality so that an administrator can access the ES Admin UI from any IP address.	No parameters. <code>config admin allow-access</code>
config admin restrict-access	Restricts which IP addresses have administrative access to the ES Admin UI.	[Comma separated list of IP addresses/CIDR] <code>config admin restrict-access 172.16.4.20, 172.16.5.18</code> or <code>config admin restrict-access 172.16.4.20/24</code>
config allow-apache-ssl3	Permits SSLv3 protocol on https connections.	[<i>true</i> to permit SSLv3, <i>false</i> to permit SSLv3] <code>config allow-apache-ssl3 true</code>
config bootpassword	Enables or disables the boot password upon startup.	No parameters. <code>config bootpassword enable</code> <code>config bootpassword disable</code>

TABLE 1. config commands

Command	Description	Parameters and Examples
config clear-apache-servername	Clears a changed apache server name and reverts it back to the FQDN.	No parameters. <code>config clear-apache-servername</code>
config clear-proxy	Clears the proxy server setting.	No parameters. <code>config clear-proxy</code>
config hostname	Sets the hostname.	[System's network name] <code>config hostname companyA.local</code>
config hostname-restricted	If enabled, requests that do not match the hostname receive an HTTP 404 error.	[<i>true</i> to enable, <i>false</i> to disable.] <code>config hostname-restricted true</code>
config https	Sets whether the Apache server should be run as HTTP or HTTPS.	[<i>enabled</i> to enable HTTPS, <i>disabled</i> to run HTTP] <code>config https enabled</code>
config network DHCP	Configures whether you want DHCP to assign network IP addresses.	[<i>true</i> to use DHCP, <i>false</i> to use STATIC IP addresses] <code>config network DHCP true</code> This command causes the system to toggle the eth0 and loopback interfaces.
config network restart	Restarts the network after making configuration changes to DHCP settings.	No parameters. <code>config network restart</code>
config network STATIC dns	Configures the STATIC IP addresses for the DNS server.	[IP address of the DNS server] <code>config network STATIC dns 172.16.4.202</code>
config network STATIC gateway	Configures the STATIC IP addresses for the gateway.	[IP address of the gateway] <code>config network STATIC gateway 172.16.4.1</code>
config network STATIC ip-netmask	Configures the STATIC IP addresses for the system's eth0 interface and subnet mask.	[IP address and subnet mask for the eth0 interface] <code>config network STATIC ip-netmask 172.16.6.35 255.255.252.0</code>
config ntp	Sets the NTP server	[IP address of the NTP server] <code>config ntp 172.16.2.106</code>

TABLE 1. config commands

Command	Description	Parameters and Examples
config ntp-sync-now	Forces an ntpdate to the configured NTP server.	No parameters. <code>config ntp-sync-now</code>
config proxy	Sets the HTTP proxy. Requires a reboot. The [proxy-bypass-hosts] parameter (optional) is a comma-separated list of hosts that should bypass the proxy.	[HTTP hostname] [HTTP port] [HTTPS hostname] [HTTPS port] [proxy-bypass-hosts] <code>config proxy hostA 8080 hostB 443 hostC,hostD</code>
config set-apache-servername	Set the apache server name in the httpd.conf file. This is typically used when operating behind a load balancer.	[Apache Server Name] <code>config set-apache-servername test22.company.net</code>
config ssh	Enables or disables SSH access.	[true to enable, false to disable.] <code>config ssh true</code>
config timezone	Sets the timezone to be used.	[Zone name] This command displays a list of acceptable timezones. When prompted, enter the desired timezone as shown. For example, for Mountain Standard time, enter MST , and for Mountain Daylight time, enter MST7MDT . <code>config timezone</code> Enter the timezone you would like to use: MST

console command

TABLE 2. console command

Command	Description
console	Provides access to the Linux shell (command line).

diag commands

The **diag** commands provide diagnostic tests for network connectivity.

TABLE 3. diag commands

Command	Description	Parameters and Examples
diag arp-table	Displays arp table.	No parameters. diag arp-table
diag dns-lookup	Performs a DNS lookup.	[IP address of the host to resolve] diag dns-lookup 172.16.4.64
diag interfaces	Displays network interfaces.	No parameters. diag interfaces
diag ping	Sends ICMP IPv4 messages to network hosts.	[IP address of the host] diag ping 172.16.2.1
diag routing-table	Displays routing table.	No parameters. diag routing-table
diag rpm-version	Displays the current version for the rpms.	No parameters. diag rpm-version
diag schema-version	Displays the status of database updates	No parameters. diag schema-version

maintenance commands

The **maintenance** commands import or export the Enrollment System database.

TABLE 4. **maintenance commands**

Command	Description	Parameters and Examples
maintenance export-database	Dumps the Enrollment System database in to a zipped tar.gz file and transfers it using SCP to a remote server.	[IP address or hostname of the remote server] [Port number] [Remote username] [Path to file location on the remote system] <code>maintenance export-database 172.16.4.20 22 username /home/db/file</code>
maintenance import-database	Allows you to copy the database file from a remote Enrollment System to overwrite the database on a new system. The new system must have the same network settings as the old system, from which the database was exported. The ES uses the SSH port configured in the new system to transfer the database files.	[IP address or hostname of the remote server] <code>maintenance import-database 172.16.4.20</code>
maintenance restore-backup	Copies the database backup file, using SCP, overwriting the existing database.	[IP address or hostname of the remote server] [Remote port number] [Remote username] [Path to the remote system to place the backup file] <code>maintenance restore-backup 172.16.4.20 22 username /home/db/file</code>
maintenance scheduled-backup mount remove	Removes the previously set up cron job for copying the system database to a remote server via mounted (CIFS) drive.	No parameters. <code>maintenance scheduled-backup mount remove</code>

TABLE 4. maintenance commands

Command	Description	Parameters and Examples
maintenance scheduled-backup mount setup	Sets up a cron job to copy the system database via mounted (CIFS) drive to a remote server.	[Username for the remote drive] [Password for the remote drive] [Path to mount] [Path within the mount to the backup directory] [Type of drive, like cifs] <code>maintenance scheduled-backup mount setup username password path/to/mount mount/backupdir cifs</code>
maintenance scheduled-backup scp remove	Removes the previously set up cron job for copying the system database to a remote server via SCP.	No parameters. <code>maintenance scheduled-backup scp remove</code>
maintenance scheduled-backup scp setup	Sets up a cron job to copy the system database via SCP to a remote server. The [pattern for the cron schedule] parameter uses traditional cron format, consisting of 5 fields; <Minute><Hour><Day_of_the_Month><Month_of_the_Year><Day_of_the_Week>.	[IP address or hostname of the remote server] [Remote port number] [Remote username] [Path to the remote system to place the backup file] [Pattern for the cron schedule] <code>maintenance scheduled-backup scp setup 172.16.4.20 22 username /path/to /file 00*3</code>

replication commands

The replication commands are designed for members of the support team to use for troubleshooting. Customers would typically not be required to run these commands unless requested by the support team.

Note >>

In most cases, gathering log data through the ES Admin UI, *Collect Replication Logs* button, is sufficient for troubleshooting purposes.

TABLE 5. replication commands

Command	Description	Parameters and Examples
replication force-cleanup	Forces the removal of the replication setup.	No parameters. <code>replication force-cleanup</code>
replication replicator	Perform an operation on the replication server.	[start][stop][restart][status][offline] [online] <code>replication replicator restart</code> or <code>replication replicator status</code>
replication show-cluster	Displays the state of the cluster.	No parameters. <code>replication show-cluster</code>
replication show-log	Show log.	No parameters. <code>replication show-log</code>
replication trepctl	Performs an operation on a service (ex. alpha, bravo, charlie).	[FQDN of the server node][service name][status/online/offline] <code>replication trepctl</code> <code>test23.company.net alpha status</code> or <code>replication trepctl</code> <code>test23.company.net bravo</code> <code>offline</code>
replication validate-cluster	Displays whether replication can be set up on this server. Note: This command should only be used before replication is set up.	No parameters. <code>replication validate-cluster</code>

show commands

The **show** commands display the current configuration.

TABLE 6. **show commands**

Command	Description
show config	Shows currently operating configuration.
show date	Shows current date.
show logs	Shows application and server logs.
show logs apache-access	Shows contents of Apache server access logs.
show logs apache-error	Shows contents of Apache server error logs.
show logs application	Shows contents of JBoss logs.
show logs config	Shows contents of config log.
show proxy	Shows HTTP proxy information.
show timezone	Shows currently configured timezone.

support commands

The **support** commands enable or disable the support tunnel.

TABLE 7. **support commands**

Command	Description
support activate-ui-recovery	Activates a temporary password to allow you to log into the ES Admin UI. This command requires the <i>service</i> password. The recovery user credentials are only valid for 5 minutes.
support apply-patches	Applies patches for the current version. The system will reboot.
support benchmark	Perform CPU and disk IO tests.
support clean-disk	The ES runs a clean-disk script on a schedule. This command allows an administrator to clean up the jboss.log manually.
support db	Allows you to log into the database. The password for this command is only available to support staff.
support disable-support-tunnel-access	Stops support tunnel.
support enable-support-tunnel-access	Starts support tunnel on port 8022.
support reset-schema-version	Sets the database schema version to 1.

TABLE 7. support commands

Command	Description
support restore-https-certificate	Resets HTTPS to self-signed certificate.
support shrink-database	Moves application data to the database partition.
support view-schema-version	Lists the status of the database schema version.

system commands

The **system** commands control system operations.

Note >>

If the boot password requirement has been set, you must enter a password to complete these commands.

TABLE 8. system commands

Command	Description
system reboot	Reboots system.
system restart	Restarts the JBoss and Apache servers.
system shutdown	Shuts down the system. This command requires VMware access to boot the system.

Password Recovery

How To Recover Admin UI Password

If you are locked out of the ES Admin UI, you can log in via SSH and use the **activate-ui-recovery** command from the service account. This activates a temporary password for a short time period to allow you to log into the ES Admin UI and set up a new Administrator account, or reset a password for an existing account.

How To Recover Service Password

If you are locked out of the service account, you can log in via SSH to a *Recovery* account.

Note >>

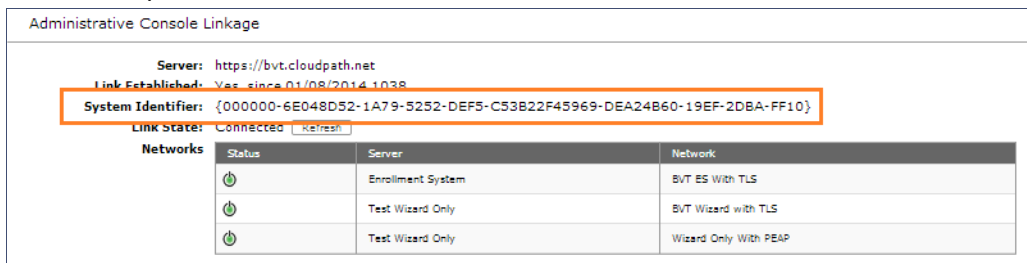
You must contact Cloudpath Networks to obtain a recovery password.

To receive a recovery password for the service account, you must provide the System Identifier and current ES version on your system.

How To Find Your System Identifier

1. Log into the ES Admin UI.
2. Go to *Administration > Advanced > Admin Console Link*.
3. The System Identifier is listed on the Administrative Console Linkage page.

FIGURE 23. System Identifier



The screenshot shows the 'Administrative Console Linkage' page. It displays the following information:

- Server: <https://bvt.cloudpath.net>
- Link Established: Yes, since 01/08/2014 10:38
- System Identifier: {000000-6E048D52-1A79-5252-DEF5-C53B22F45969-DEA24B60-19EF-2DBA-FF10}
- Link State: Connected















Below this information is a table titled 'Networks' with three columns: Status, Server, and Network.

Status	Server	Network
	Enrollment System	BVT ES With TLS
	Test Wizard Only	BVT Wizard with TLS
	Test Wizard Only	Wizard Only With PEAP

How To Find Your Current ES Version

1. Go to *Administration > System > System Services > Application* component.
2. The ES build version is listed in the *Version* field.

FIGURE 24. Current ES Version

Component:	Application	
<p>Status: Running Version: 3.0.1833</p>		
<p>iOS Certificate Public Key: Missing Private Key: Missing Chain: Missing</p>		
<p>Log Level: Normal <input type="button" value="Debug"/></p> <p>Downloads: <input type="button" value="Log"/> <input type="button" value="Backup"/></p>		
Component:	Web Server	   
Component:	RADIUS Server	
Component:	Network	
Component:	SSH	
Component:	Support Tunnel	
Component:	Outbound Email	
Component:	Outbound SMS	
Component:	Logs	 
Component:	Replication	 

See About Cloudpath for information about contacting Support.

Terminology

TABLE 9. Enrollment System Terminology

Term	Definition
Admin Console Link	The URL that the Enrollment System uses to communicate with the XpressConnect Licensing Server.
Administrator	An administrator role whose login credentials allow them to access all aspects of the Enrollment System, including permission to add, edit, delete, or reset passwords for other administrators.
Certificate signing request (CSR)	An unsigned copy of your certificate, which can be signed by a trusted CA and used to generate a certificate.
Device Configuration	A concept used with the XpressConnect Enrollment System to group configuration settings. Each network contains a single configuration per operating system. A device configuration within XpressConnect represents a physical network within your environment.
ESXi Server	An enterprise-level computer virtualization product offered by VMware, Inc.

TABLE 9. Enrollment System Terminology (continued)

Term	Definition
Fault Tolerance	Fault Tolerance (FT) provides continuous availability for applications in the event of server failures by creating a live shadow instance of a virtual machine that is in virtual lockstep with the primary instance.
HTTPS certificate	Also called an SSL certificate, or web server certificate, an HTTPS certificate allows you to host secure pages on your website.
OVA File	<p>The Enrollment System build package is deployed as an open virtualization archive (OVA) file, which is a TAR file with the OVF directory inside.</p> <ul style="list-style-type: none"> • Open Virtualization Format (OVF) is an open standard for describing a virtual machine template. • Open Virtualization Archive (OVA) is an open standard to package and distribute these templates.
OVF Template	OVF templates allow you to create virtual appliances that can be imported by other users. You can deploy an OVF template from any local file system accessible from a vSphere Client machine, or from a remote web server.
Provisioning (Thin or Thick)	<p>Provisioning is a systems management process that creates a new virtual machine (VM) on a physical host server and allocates computing resources to support the VM.</p> <ul style="list-style-type: none"> • Thin provisioning - Optimizes storage utilization by allocating storage space in a flexible on-demand manner. • Thick provisioning - Large amount of storage space is provided in advance in anticipation of future storage needs.
Virtual Appliance	A pre-configured virtual machine that includes a pre-installed guest operating system and other software.
VMware Client	An interface that allows users to connect remotely to VMware server from any PC.
VMware Server	A virtualization layer run on physical servers that abstracts processor, memory, storage, and resources into multiple virtual machines.
XpressConnect Enrollment System	The workflow configuration application for XpressConnect.
XpressConnect Wizard	The network access wizard provided to users to automate network access.

Additional Documentation

You can find detailed information in the Enrollment System 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.

If you need technical assistance, discover a bug, or have other technical questions, email support at support@cloudpath.net.

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