

Cloudpath Enrollment System VMware Server Deployment Guide, 6.0

Supporting Cloudpath Software Release 6.0

© 2024 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

What's New in this Document.....	5
Specifications for On-Premise Deployed VMware Server.....	7
Cloudpath Virtual Appliance Specifications.....	7
Cloudpath as a Physical Appliance.....	7
What You Need.....	7
For Deployment.....	7
For Virtual Appliance Initial Configuration.....	8
For Cloudpath Account Setup.....	8
Supported Browsers and Operating Systems.....	8
Deploying the Virtual Appliance to a VMware Server.....	9
Retrieve OVA File.....	9
Deploying the Virtual Appliance Using a VMware vCenter Client.....	9
Application Properties (vCenter).....	10
Confirm Deployment Settings (vCenter).....	13
Deploying the Virtual Appliance Using a Console-Based VMware Client.....	14
Service Account.....	14
Activate Account or Log In.....	17
Activate Account by Activation Code.....	17
Set a Password for Account.....	18
Activate Account by Credentials.....	19
Initial System Setup.....	21
System Setup Wizard.....	22
Publishing Tasks.....	32
ToDo Items.....	33
Command Reference.....	35
Troubleshooting.....	37
Test Network Connectivity.....	37
How to Increase the Virtual Appliance Memory.....	37
How to Expand the MySQL Partition Size.....	37
From the vCenter Client.....	37
From the Console.....	38
Password Recovery.....	38
How To Recover Admin UI Password.....	38
How To Recover Service Password.....	38
How To Find Your System Identifier.....	38
How To Find Your Current Cloudpath Version.....	40
Additional Documentation.....	41

What's New in this Document

There are no changes in this release.

Specifications for On-Premise Deployed VMware Server

- [Cloudpath Virtual Appliance Specifications.....7](#)
- [Cloudpath as a Physical Appliance..... 7](#)
- [What You Need.....7](#)

Cloudpath supports virtual appliance deployments using a VMware ESXi server or a Microsoft Hyper-V Manager. For Hyper-V deployments, refer to the *Deploying Cloudpath as a Virtual Appliance Using Microsoft™ Hyper-V Manager* configuration guide.

Cloudpath Virtual Appliance Specifications

The Cloudpath 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).

NOTE

If using version 6.5 ESXi server, you must use a SHA-256 signed OVA.

Cloudpath offers a Non-Production POC, as well as several Production configurations for deployment. See the *Deploying the Virtual Appliance Using a VMware vCenter Client* section for details.

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

Cloudpath as a Physical Appliance

Cloudpath 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, Cloudpath 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.

What You Need

For Deployment

- OVA file for the Cloudpath 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, subnet mask, and gateway for the virtual appliance (not required if using DHCP)
- IP address of DNS server (not required if using DHCP)

For Cloudpath Account Setup

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

Supported Browsers and Operating Systems

Refer to the *Cloudpath Enrollment System Administration Guide* for this information.

Deploying the Virtual Appliance to a VMware Server

- [Retrieve OVA File.....](#) 9
- [Deploying the Virtual Appliance Using a VMware vCenter Client.....](#) 9
- [Deploying the Virtual Appliance Using a Console-Based VMware Client.....](#) 14

The deployment process consists of the following steps:

- Retrieve OVA File
- Deploying the Virtual Appliance Using a VMware vCenter Client

or

- Deploying the Virtual Appliance Using a Console-Based VMware Client
- Activate Account or Log In

Retrieve OVA File

If you are setting up a Cloudpath account for the first time, you will be sent an activation code in an email notification. For an on-premise deployment, the activation code link allows you to download the Cloudpath OVA, binding your OVA file to the activation code.

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

Deploying the Virtual Appliance Using a VMware vCenter 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. Accept the EULA.
5. Enter a unique name for the virtual appliance.
6. Select a deployment configuration:
 - Non-Production POC - Deploys using 6GB RAM and 2 vCPUs x 1 Core. Recommended for software trials, feature testing, and other non-production systems.
 - 4,000 or Fewer Users - Deploys using 8GB RAM and 2 vCPUS x 2 Cores. Recommended for production systems with fewer than 4,000 users.
 - 8,000 or Fewer Users - Deploys using 12GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with fewer than 8,000 users.
 - More than 8,000 Users - Deploys using 16GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with more than 8,000 users.
 - More than 20,000 Users - Deploys using 20GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with more than 20,000 users.

Deploying the Virtual Appliance to a VMware Server

Deploying the Virtual Appliance Using a VMware vCenter Client

7. If you are using VMware vCenter™ Server to manage your virtual environment, select the appropriate data center, cluster, host, and destination storage, as needed.
8. Select a disk format.
 - Use **Thick** provisioning 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 **Thin** provisioning 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.
9. 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 Deploying the Virtual Appliance Using a Console-Based Client to complete the deployment process.

Application Properties (vCenter)

Customize the application properties for the deployment.

FIGURE 1 Application Properties

The screenshot shows the 'Cloudpath Enrollment System' configuration form. It contains the following sections and fields:

- Hostname (FQDN)**: A text input field with the instruction 'Enter the fully qualified domain name.'
- IP Address**: A text input field with the instruction 'The IP address for this VM. Leave blank if DHCP is desired.'
- Netmask**: A text input field with the instruction 'The netmask or prefix for this VM. Used only if static IP is assigned.' The value '255.255.252.0' is entered.
- Default Gateway**: A text input field with the instruction 'The default gateway address for this VM. Used only if static IP is assigned.'
- DNS**: A text input field with the instruction 'The DNS server(s) for this VM. Supports up to 3 in a comma-separated list. Used only if static IP is assigned.' The value '8.8.8.8,8.8.4.4' is entered.
- NTP Server**: A text input field with the instruction 'Specify an NTP server. By default, pool.ntp.org will be used.' The value 'pool.ntp.org' is entered.
- Enable HTTPS?**: A checkbox that is checked.
- Timezone**: A dropdown menu with 'GMT' selected.
- SSH Access**: A dropdown menu with 'Port 8022' selected.
- Restrict admin access?**: A text input field with the instruction 'To restrict the admin web UI to certain addresses or subnets, specify a comma-separated list of addresses or subnets (CIDR notation, ex. 192.168.4.1/22).'
- Console Password**: Two text input fields labeled 'Enter password' and 'Confirm password' with the instruction 'Specify the password to be used to access the console or SSH of this VM. Please select a strong password that is compliant with your password complexity policy.' Below these fields is a red error message: 'Enter a string value with 1 to 100 characters.'

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

NOTE

The Cloudpath **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).

2. Enter the IP Address, Netmask, Default Gateway, and the DNS Servers for this VM. Leave blank for DHCP.
3. Specify an NTP Server or leave the default.
4. HTTPS is enabled by default. Leave unchecked only if Cloudpath is behind another web server using SSL.
5. Select the **Timezone**.
6. Select SSH port, or disable SSH access.

Deploying the Virtual Appliance to a VMware Server

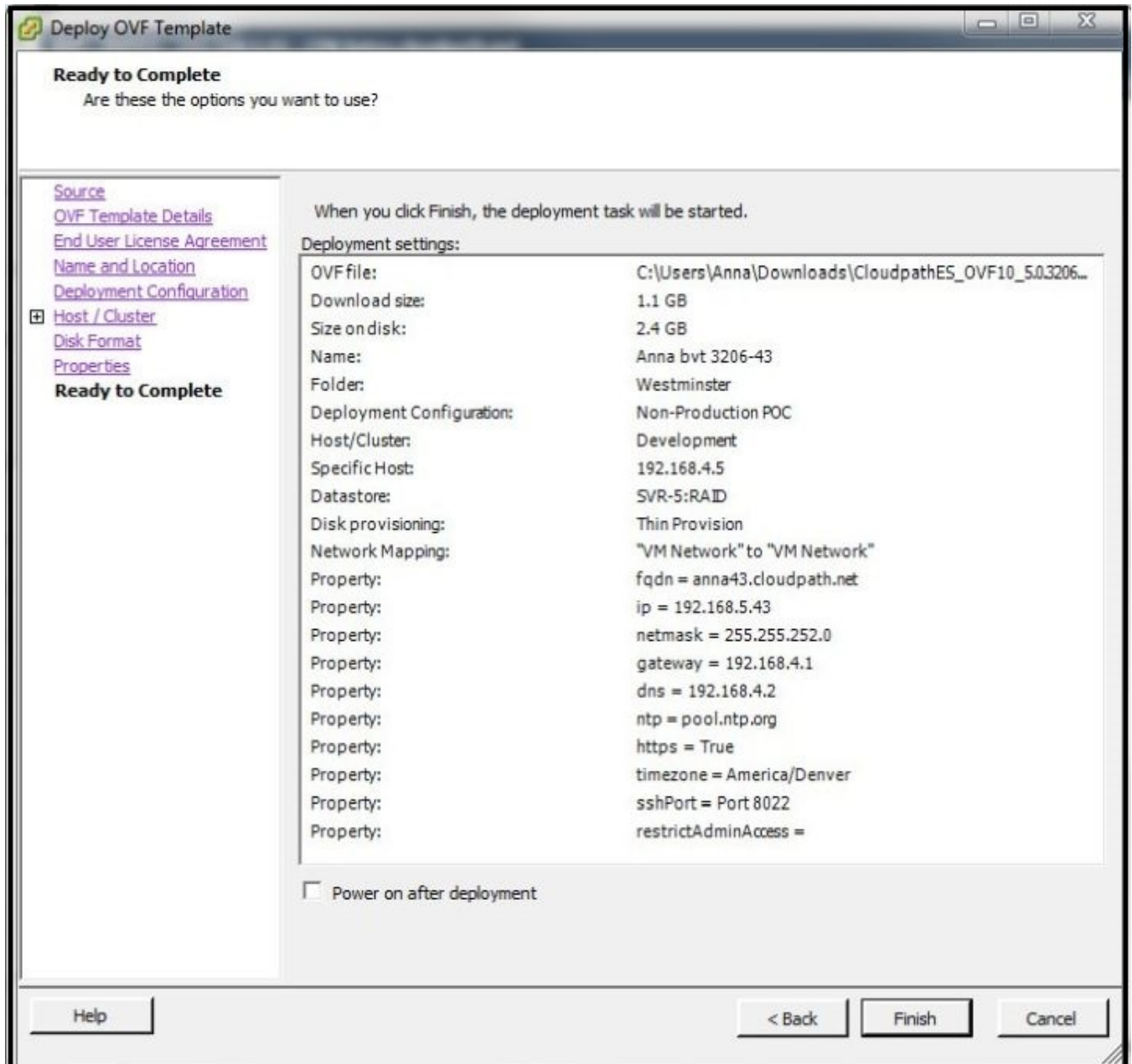
Deploying the Virtual Appliance Using a VMware vCenter Client

7. Enter the IP address(es) that can access the Cloudpath Admin UI. Leave this field blank if you do not want to limit administrative access.
8. 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.

Confirm Deployment Settings (vCenter)

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

FIGURE 2 Deployment Settings



2. Click **Finish**
Deployment takes approximately 2 minutes.

Deploying the Virtual Appliance Using a Console-Based VMware Client

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

1. Open a console for the VM.
2. Enter **yes** (or **y**) to accept all license agreements.
3. Enter the time zone. For example, enter **America/Denver**.
4. Enter the **FQDN hostname** for the virtual appliance (ex., **onboard.company.com**).
5. Do you want to enable HTTPS? Enter for yes (default) or **n**.
6. Do you want to use a STATIC IP (rather than DHCP)? Enter for yes (default) 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.
7. Enter the IP address of the virtual appliance.
8. Enter a subnet mask in the format 255.255.252.0.
9. Enter the gateway IP address for your network.
10. Enter the DNS server IP address.
11. Do you want to permit SSH access? Enter for yes (default) or **n**.
12. 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 *Cloudpath Command Reference* on the **Support** tab for details.

NOTE

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

13. Do you want to use an NTP server other than pool.net.org? Enter for no (default) or **y** to specify an NTP server.

The setup is complete.

14. 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.

To use the service account:

1. Enter **cpn_service** at the login prompt, and then the service user password.

2. Enter the **show config** command to verify your configuration. You may be prompted to re-enter the password.
See the *Cloudpath Command Reference* on the left menu **Support** tab.

Activate Account or Log In

- [Activate Account by Activation Code.....](#) 17
- [Set a Password for Account.....](#) 18
- [Activate Account by Credentials.....](#) 19

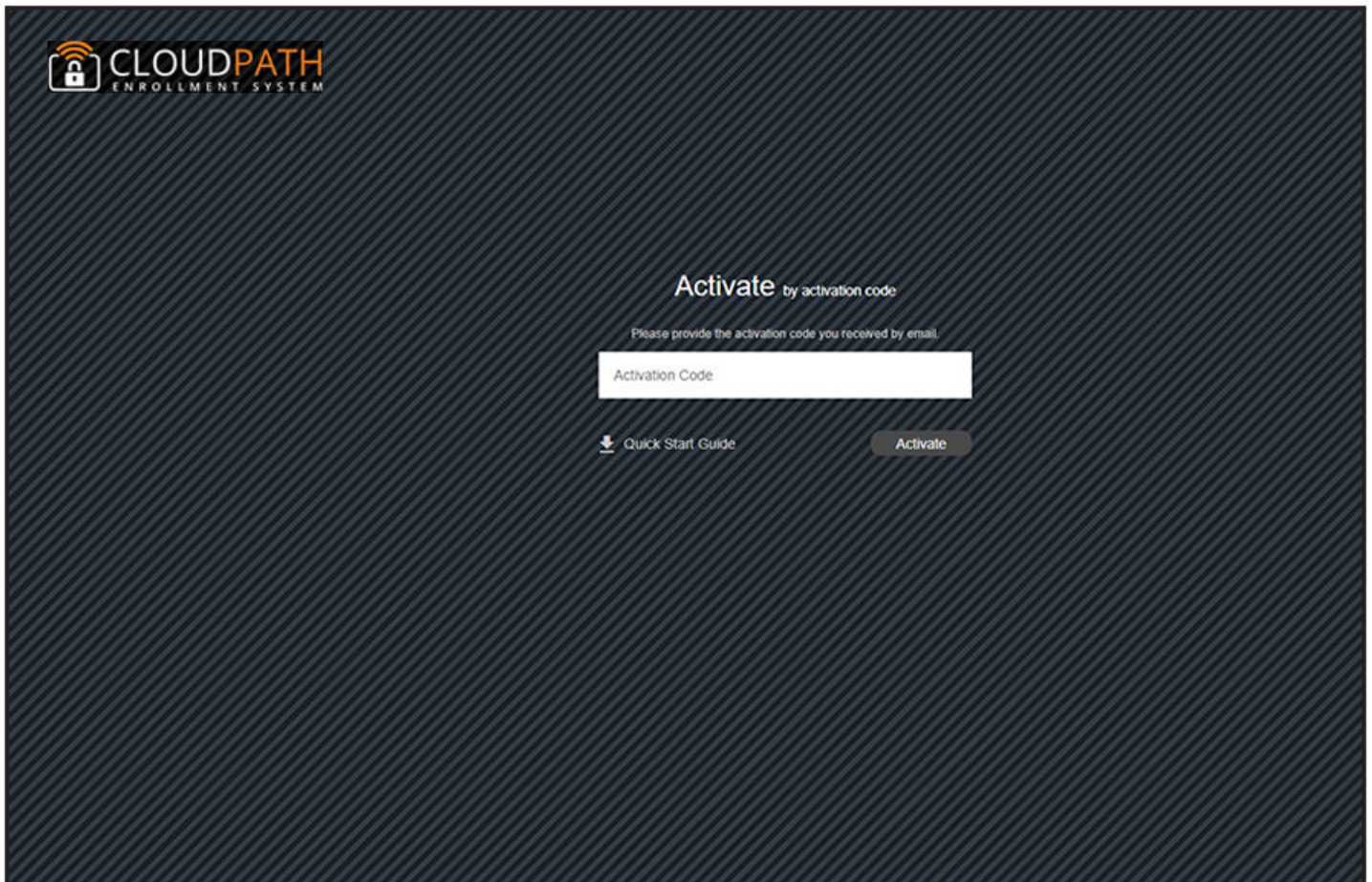
If you are setting up a Cloudpath account for the first time, you will be sent an activation code. If you have existing Cloudpath License server credentials, you can activate an account using those credentials.

Whether you create a new account with an activation code or with legacy Cloudpath credentials, the system binds the Cloudpath instance to your License Server credentials.

Activate Account by Activation Code

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

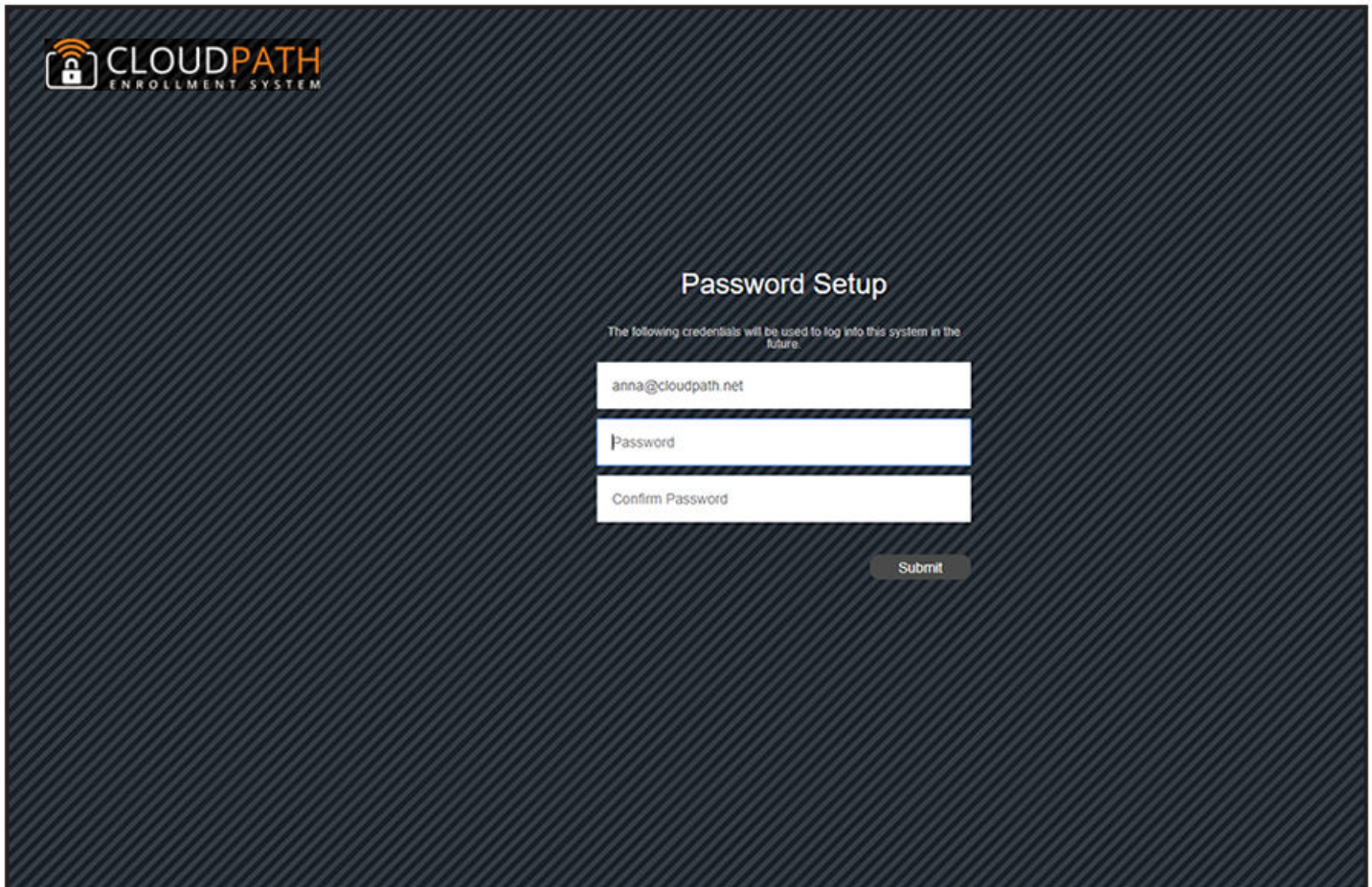
FIGURE 3 Activate Cloudpath Account



Set a Password for Account

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

FIGURE 4 Set Password



The screenshot shows the 'Password Setup' page of the Cloudpath Enrollment System. The page has a dark blue background with a diagonal line pattern. In the top left corner is the logo for 'CLOUDPATH ENROLLMENT SYSTEM'. The main heading is 'Password Setup'. Below the heading is a message: 'The following credentials will be used to log into this system in the future.' There are three input fields: the first contains 'anna@cloudpath.net', the second is labeled 'Password', and the third is labeled 'Confirm Password'. A 'Submit' button is located at the bottom right of the form area.

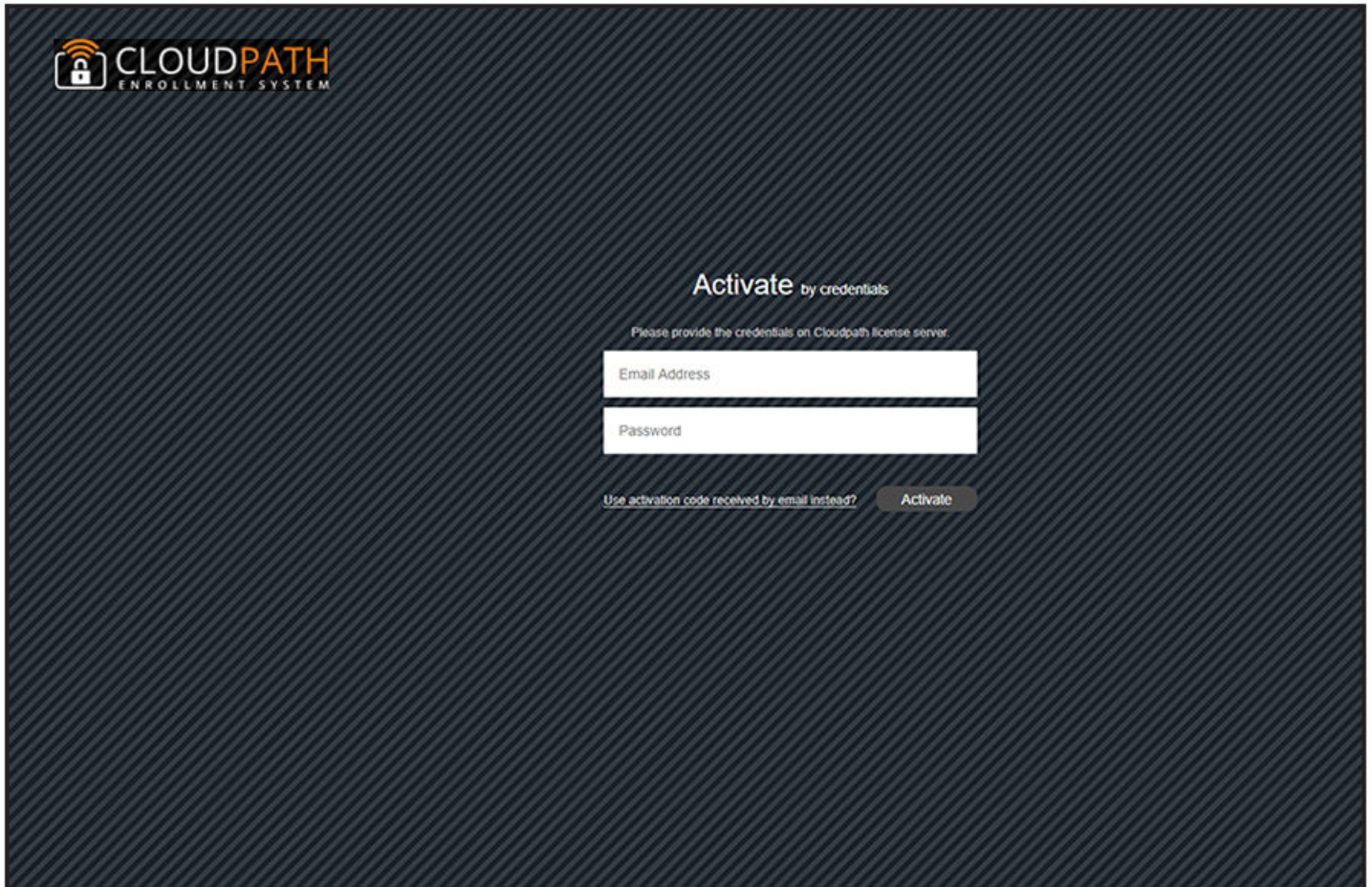
1. Your email address should display. If it does not, enter it on this page.
2. Enter and confirm a password.

These are the credentials to use for this Cloudpath account.

Activate Account by Credentials

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

FIGURE 5 Activate Account With Existing Credentials



The screenshot shows the 'Activate by credentials' page of the Cloudpath Enrollment System. The page has a dark blue background with a diagonal line pattern. In the top left corner is the logo for 'CLOUDPATH ENROLLMENT SYSTEM', which includes a padlock icon. The main heading is 'Activate by credentials'. Below this, a small instruction reads 'Please provide the credentials on Cloudpath license server.' There are two white input fields: 'Email Address' and 'Password'. At the bottom, there is a link that says 'Use activation code received by email instead?' and an 'Activate' button.

Initial System Setup

- System Setup Wizard..... 22
- Publishing Tasks..... 32
- ToDo Items..... 33

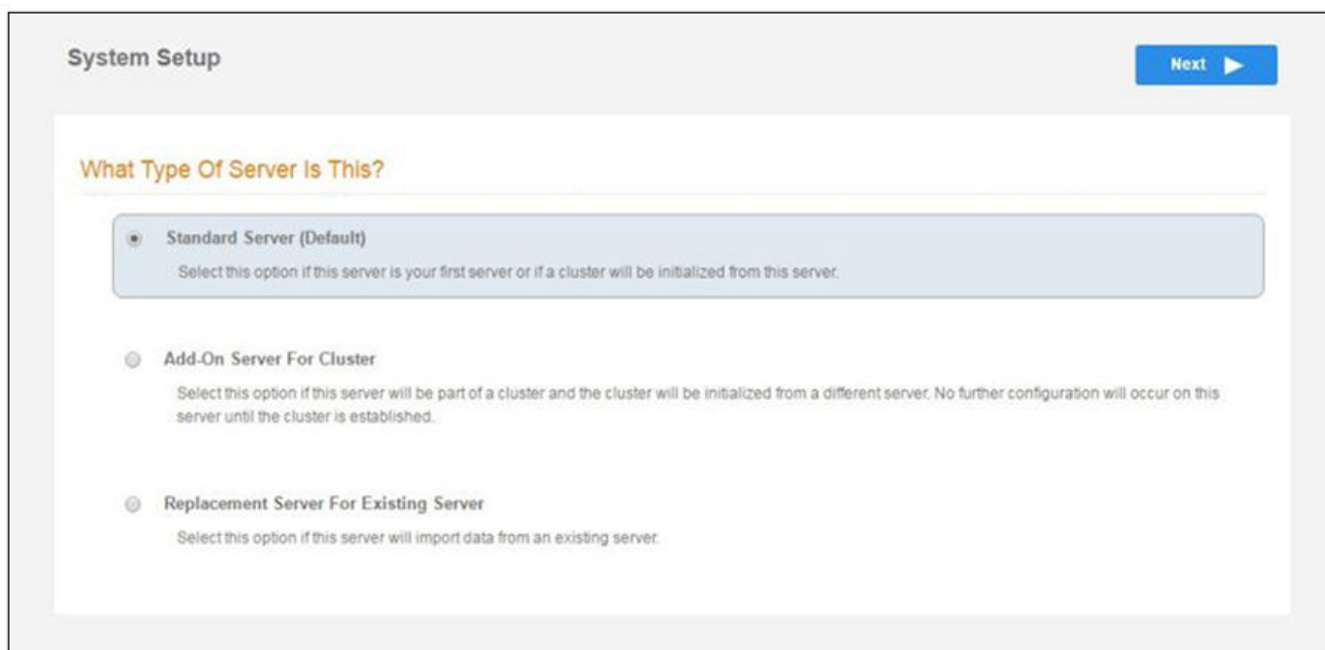
Cloudpath provides you with a single administrator login for the Cloudpath Admin UI. Additional administrators can be added from the left menu **Administration** tab, or you can enable Administrator logins from your authentication servers.

System Setup Wizard

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

1. Select Server Type.

FIGURE 6 Select Server Type



In most cases, select **Standard Server**, the default. This selection takes you through a setup wizard, which prompts you for the basic information required for an Cloudpath 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 primary server in the cluster.
- 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**.

NOTE

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

- 2. Enter **Company Information**, then click **Next**.
This information is embedded in the onboard root CA certificate.

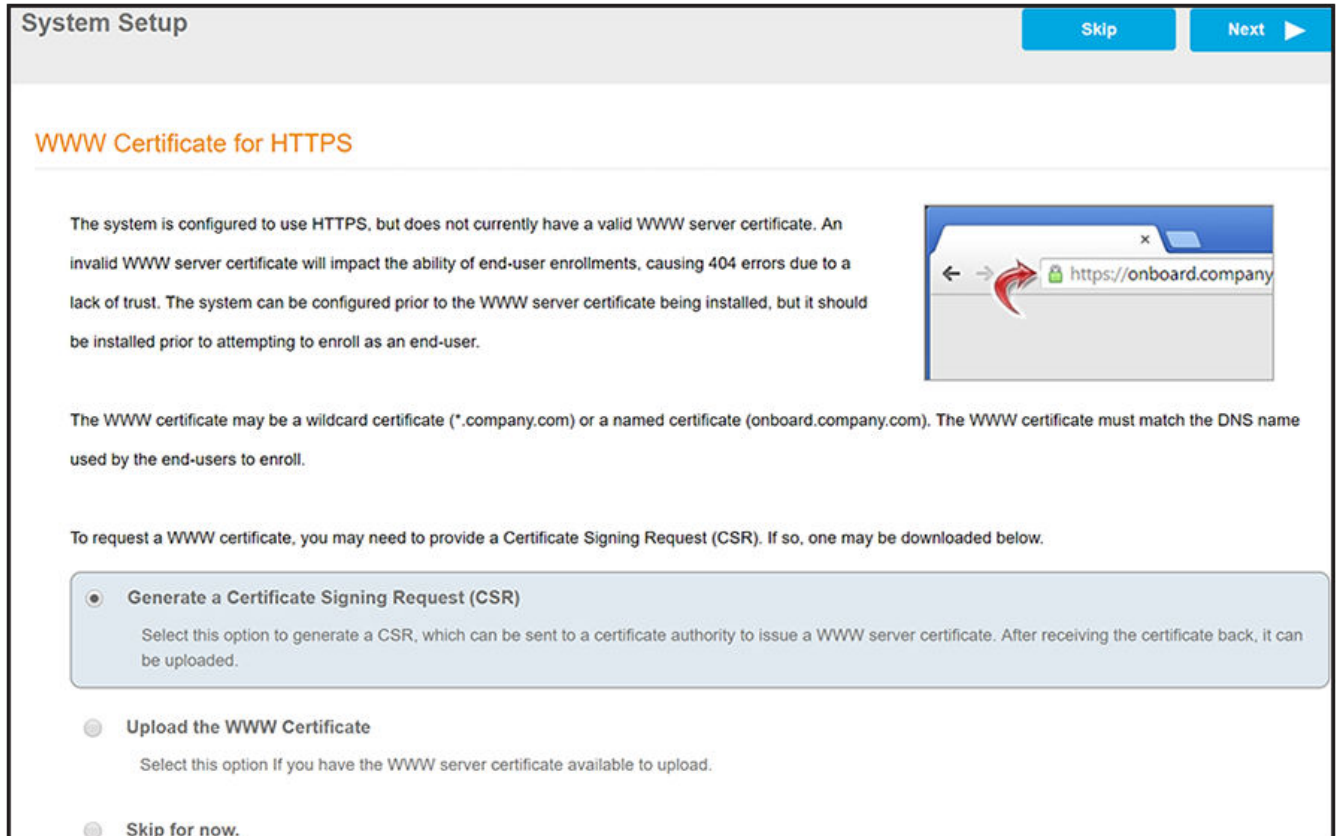
FIGURE 7 Company Information

The screenshot shows a 'System Setup' window with a 'Next' button in the top right corner. The main content area is divided into two sections: 'Company Information' and 'Company Web Presence'. Each section contains several input fields with a small information icon (i) to the left of the label. The 'Company Information' section includes fields for Company Name, Legal Company Name, Department Name, City, State/Province, and Country. The 'Company Web Presence' section includes fields for Company Domain, Support Email, and IT Email. A mouse cursor is visible over the Country field.

Section	Field Label	Value
Company Information	Company Name	Anna43 Test BVT
	Legal Company Name	Sample Company, Inc.
	Department Name	IT
	City	Westminster
	State/Province	Colorado
	Country	US
Company Web Presence	Company Domain	company.com
	Support Email	support@company.com
	IT Email	it@company.com

3. In the WWW Certificate for HTTPS screen (below), choose the applicable radio button, then click **Next**.

FIGURE 8 WWW Certificate for HTTPS Screen



NOTE

Cloudpath 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.

- If you selected the "Generate CSR" radio button, perform [Step 4](#).
- If you selected the "Upload the WWW Certificate" radio button, perform [Step 5](#).
- You can select the "Skip for now" radio button for the initial configuration. However, you should perform this step prior to attempting to enroll as an end-user. To return at a later time to the screen shown above, navigate to **Administration > System Services > Web Server** service, then click **Upload WWW Certificate**. For now, proceed to [Step 6](#)

4. (Only if you selected "Generate CSR" radio button.) You should now be at the Create CSR for HTTPS screen:

FIGURE 9 Create CSR for HTTPS Screen

- a) Enter the required information.

NOTE

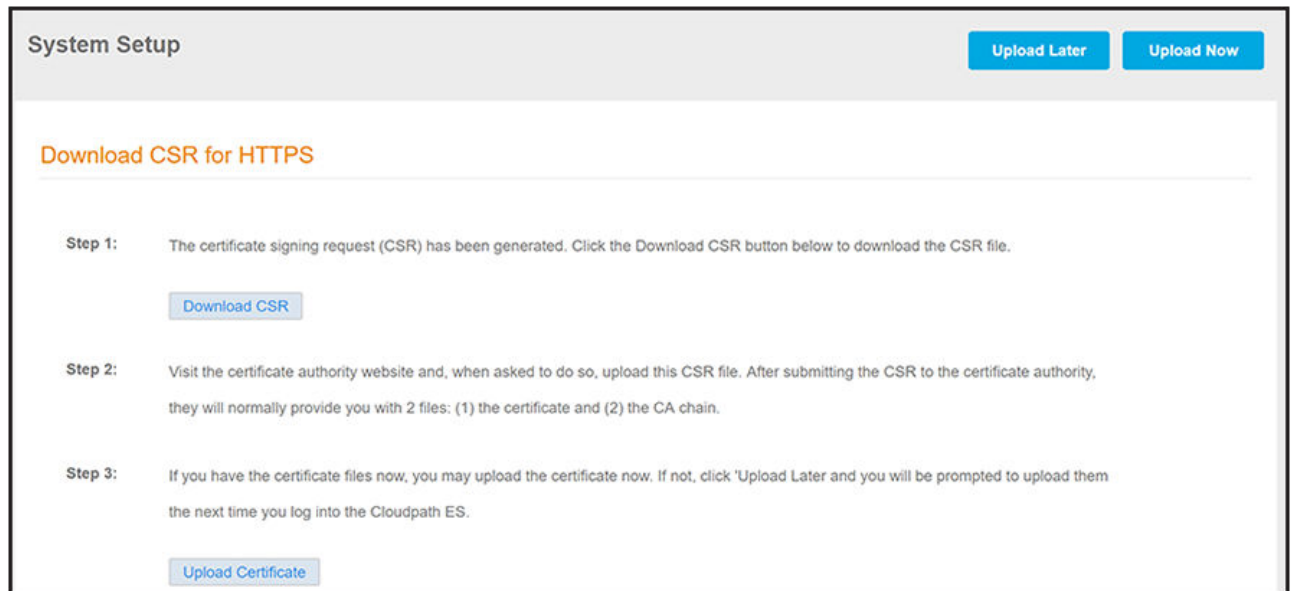
In the Common Name field:

- If you are re-issuing a wildcard certificate, make sure the hostname includes *. For example: *.domain.com.
- If using a single-domain SSL certificate, the HTTPS server name should already be populated for you.

- b) Click **Next**.

The Download CSR for HTTPS Screen is displayed:

FIGURE 10 Download CSR for HTTPS Screen



- c) Click **Download CSR** to download the .csr file, which you can then open in Notepad.
- d) Upload the CSR to any CA website to receive a certificate.
- e) Follow the instructions for the CA website to download the public key and chain.

The public key usually has a filename similar to the domain name. The chain will vary depending on the CA, but it typically contains the word "Root," "Intermediate," "Bundle," or something similar, and may have the filename extension of *.chain*.

- f) In the screen that is shown in [Figure 10](#), click **Upload Certificate**.

You are taken to the screen where you upload the files you received from the CA. The screen below shows the Private Key and the Chain already uploaded, and the Private Key Source is "Certificate is based on the downloaded CSR":

FIGURE 11 Upload WWW Certificate Based on the Downloaded CSR

The screenshot shows a 'System Setup' window with a 'Back' and 'Next' button in the top right. The main section is titled 'Upload by PEM Files' and contains the following text: '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.'

Below the text are five fields, each with an information icon (i) on the left and a 'Choose File' button on the right:

- Public Key (PEM): Choose File `anna242cloudpathnet.cer`
- Chain (PEM or P7b): Choose File `anna242cloudpathnet.chain`
- Additional Chain (Optional): Choose File No file chosen
- Additional Chain (Optional): Choose File No file chosen
- Private Key Source: Certificate is based on the downloaded CSR ▼

At the bottom of the section is a link '> Upload by P12'.

- g) Upload your certificates using the screen shown above.
- h) Click **Next** to continue with the system setup.
- i) Proceed to [Step 6](#).

5. (Only if you selected the "Upload the WWW Certificate" radio button, which you should only have done if you already have received your WWW certificate from a public CA.) You should now be at the following screen:

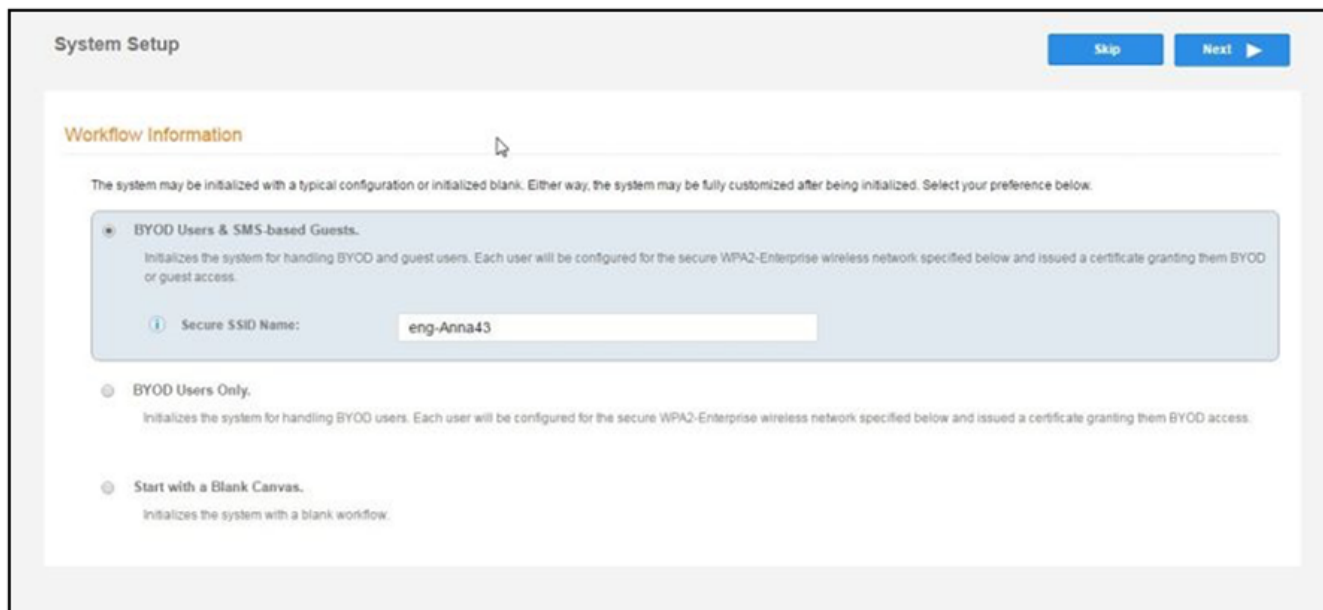
FIGURE 12 Upload Existing WWW Certificate

The screenshot shows the 'System Setup' wizard interface. At the top right, there are 'Back' and 'Next' navigation buttons. The main content area is divided into two sections: 'Upload by PEM Files' and 'Upload by P12'. The 'Upload by PEM Files' section includes a note: '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.' Below this note are six rows of input fields, each with a 'Choose File' button and a status indicator: 'Public Key (PEM):' (No file chosen), 'Chain (PEM or P7b):' (No file chosen), 'Additional Chain (Optional):' (No file chosen), 'Additional Chain (Optional):' (No file chosen), 'Private Key (PEM):' (No file chosen), and 'Private Key Password:' (empty text box). There is also a checkbox for 'Prompt for Password on Boot:'. The 'Upload by P12' section includes a note: 'You may upload a server certificate in p12 format. To do so, you must also specify the password if the p12 is password protected.' Below this note are two rows of input fields: 'P12 File:' (with a 'Choose File' button and the text 'CloudpathLabWw...rtificate.p12') and 'P12 Password:' (empty text box).

- a) Upload your certificates using the screen shown above.
You can do one of the following: 1) Upload the Public Key, the Chain, *and* the Private Key, **or** 2) Upload the P12 file. The example in the screen above shows a P12 file has been uploaded.
- b) Click **Next** to continue with the system setup.
- c) Proceed to [Step 6](#).

6. 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 13 Select Default Workflow



7. 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, Ruckus recommends populating the authentication server information page.

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

FIGURE 14 Authentication Server Setup

Authentication Server Configuration

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?

VLAN Configuration

Use VLAN Range:

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.

Connect to SAML
Select this option to enable end-users to authenticate via a SAML 2.0 IdP.

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

a) To setup the initial configuration of the Authentication Server, select and enter the required fields.

b) 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** - Authentication Server definitions of types **Connect to Active Directory**, **Connect to LDAP** and **Connect to SAML** offer additional options.

If **Use for Admin Logins** is selected, administrators can log into the Cloudpath Admin UI using credentials associated with this authentication server. Additionally, three related options become available to define which authentication server defined user groups are allowed as Cloudpath administrators. They are:

- CA Administrator Group Regex
- Administrator Group Regex
- Viewer Group Regex

Group Regex options are used to map Authentication Server defined groups to Cloudpath administrator Roles. User groups returned by the authentication server must match at least one of the Group Regex fields for the Admin login to be allowed.

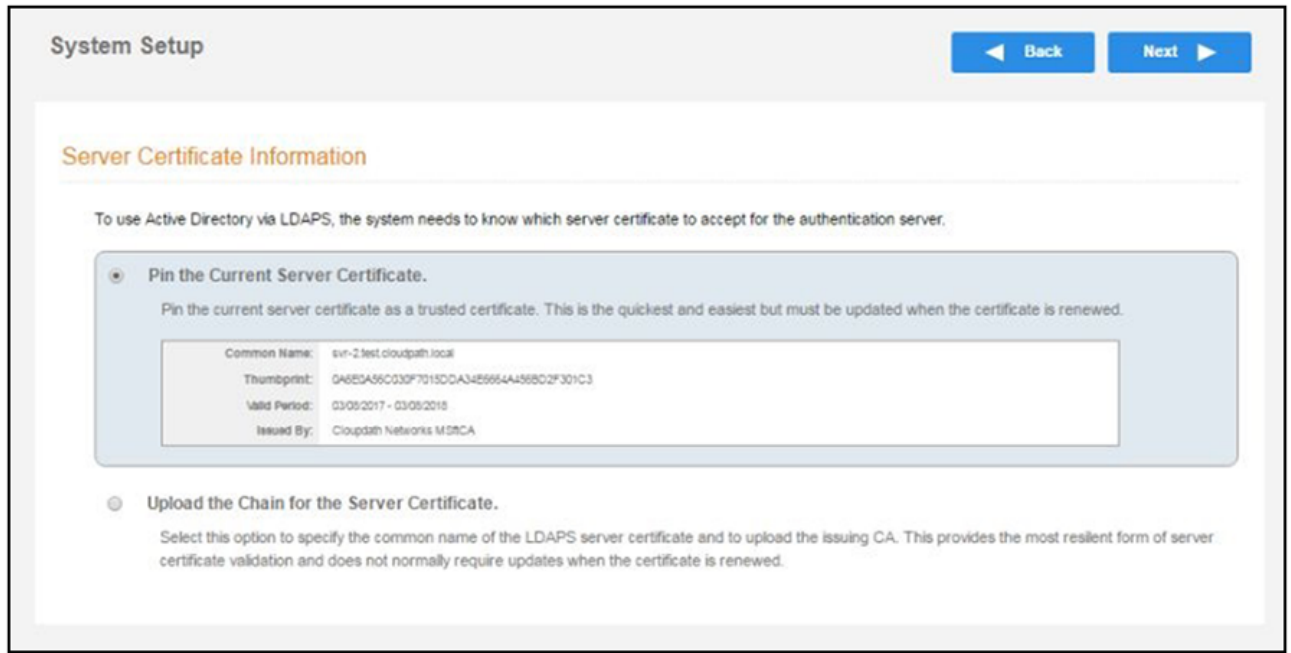
While authenticating the admin user, if multiple regexes match, the role with the highest privilege takes precedence. If none of the three regexes match, authentication is denied to the user.

If **Use for Sponsor Logins** is selected, sponsors can log into the Cloudpath Sponsorship Portal 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.

8. Set up the Authentication Server Certificate:
 - a) To use LDAP over SSL (LDAPS), the system must know which server certificate to accept for the authentication server.

FIGURE 15 Authentication Server Certificate



- b) 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.
- c) 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.

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 16 System Initialization Status

Initialization Task	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:	eng-Anna248 (WPA2-Enterprise, AES (CCMP), Broadcast)
RADIUS IP:	anna248.cloudpath.net
RADIUS Authentication Port:	1812
RADIUS Accounting Port:	1813
RADIUS Shared Secret:	nhu0vjvxedwppn7vuw
RADIUS Attributes:	BYOD Policy Template - VLAN '1' Guest Policy Template - VLAN '1'
User Experience:	
	End-users will use the enrollment portal to activate devices.
End-User Portal:	https://anna248.cloudpath.net/enroll/Anna248HyperVxpc/Production/
BYOD:	For BYOD, the authentication server is configured. BYOD users will be moved onto the secure SSID with VLAN '1' assigned.
Guests:	Guests will be required to provide a voucher via SMS or email. SMS is one of several mechanisms for handling guests. Guest users will be moved onto the secure SSID with VLAN '1' assigned.
Administrator Experience:	
Administrator UI:	https://anna248.cloudpath.net/admin/
Credentials:	The following email addresses have been sent a one-time password along with this information:

ToDo Items

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

Initial System Setup

ToDo Items

FIGURE 17 Cloudpath Welcome Page

Welcome to the Cloudpath ES

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

Getting Started

Use the left menu tabs to begin setting up your workflow configuration. The *Dashboard* tab displays reporting information about the enrollments, users, devices, certificates, and more.

The *Configuration* tab allows you to configure and deploy the enrollment workflow, including the look & feel and the device configuration.



From the *Sponsorship* tab, you can manage vouchers and voucher lists, and customize the look & feel of the sponsorship portal.

From the *Certificate Authority* tab, you can manually generate certificates, view certificate details, revoke certificates, manage the characteristics of certificates to be issued, and manage certificate authorities (CAs).

The *Administration* tab allows you to manage administrator accounts, system services, diagnostics and logs, and system updates.

The *Support* tab provides access to the Quick Start Guide and several Setup Guides to help with common configurations along with licensing information.

Todo Items

-  System logging is currently running in debug mode.
-  The workflow is currently blank. Click 'Fix' to begin adding steps to the workflow.

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

Command Reference

For all Cloudpath commands, syntax, and descriptions, see the *Cloudpath Enrollment System Command Reference*.

Troubleshooting

- Test Network Connectivity..... 37
- How to Increase the Virtual Appliance Memory..... 37
- How to Expand the MySQL Partition Size..... 37
- Password Recovery..... 38

Test Network Connectivity

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

1. Ping the gateway of your system.
2. Ping the URL where the Cloudpath Licensing Server is hosted.
3. Verify that the virtual appliance can resolve DNS.

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 the size of the partition used for MySQL database operations.

From the vCenter Client

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

NOTE

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

From the Console

Enter the following commands as `root`.

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

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

2. Signal to the OS that there has been a hardware change to the disk.

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

3. Expand the physical volume.

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

4. Extend the size of the logical volume for MySQL operations.

This example shows that we are extending the size of the logical volume by adding 25GB.

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

5. Resize the file system.

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

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

6. Verify the amount of free disk space available.

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

The output should indicate the increased partition size.

Password Recovery

How To Recover Admin UI Password

If you are locked out of the Cloudpath 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 Cloudpath 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 Support to obtain a recovery password.

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

How To Find Your System Identifier

1. Log into the Cloudpath Admin UI.

2. Go to **Support > Licensing**.
3. The System Identifier is listed on the **License Server** section.

FIGURE 18 System Identifier

The screenshot displays the 'Support > Licensing' interface. At the top right, there is a 'Check For Updates' button. The page is divided into several sections:

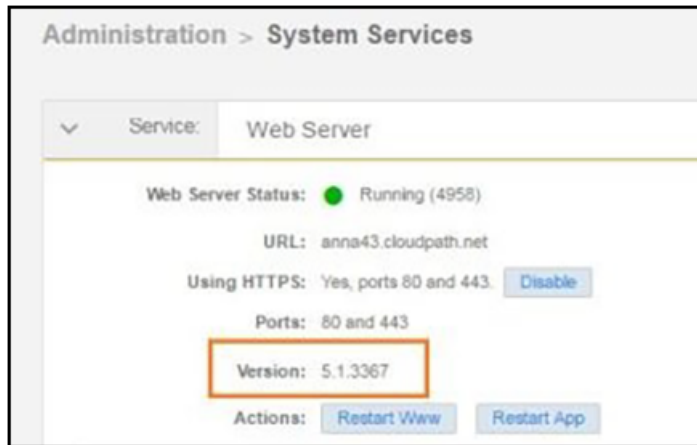
- License Information:** Shows 'License Type: Trial' with a green dot icon and 'Active trial through [Unknown]'.
- System Utilization:** Lists 'Active Certificates' (2 Currently Active, 2 Issued in Last 30 Days, 2 Issued in Last 60 Days, 2 Issued in Last 90 Days, 2 Issued in Last Year), 'AD/LDAP Users' (1 Total), 'Email Count' (2 This Year), and 'Statistics' (Users, Authentications, Certificates, MAC Registrations, Notifications).
- License Server:** Shows 'License Server: https://bvt.cloudpath.net', 'Link Established: Yes, since 20170324 1047 MDT Advanced', 'Customer GUID: (ef51219dd6993e2bb68afcd9dd019e39a9e433)', and 'System Identifier: (000000-115030E4-BF8D-389B-C7EA-4FE942A30ABC-2134023F-F668-BA8F-C237)'. The System Identifier is highlighted with a red rectangular box.
- Notices:** Includes 'Open Source Notices', 'Patent Notice', and 'Copyright Notice'.

How To Find Your Current Cloudpath Version

The Cloudpath version is displayed in two locations.

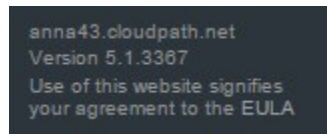
1. Go to **Administration > System Services > Web Server** service.
The current build is listed in the **Version** field.

FIGURE 19 Current Cloudpath Version System Services



2. The Cloudpath version is displayed in the lower left corner of the Admin UI, and is visible on all pages.

FIGURE 20 Current Cloudpath Version Lower Left



Additional Documentation

You can find more information in the Cloudpath configuration guides, located on the left-menu **Support** tab of the Cloudpath Admin UI.



© 2024 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>