

Cloudpath Enrollment System Microsoft Hyper-V Deployment Guide, 5.11

Supporting Cloudpath Software Release 5.11

Copyright, Trademark and Proprietary Rights Information

© 2022 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

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

| | |
|--|-----------|
| Introduction..... | 5 |
| About this document..... | 5 |
| Specifications for On-Premise Hyper-V Server..... | 5 |
| Cloudpath Virtual Appliance Specifications..... | 5 |
| Microsoft Hyper-V Specifications..... | 5 |
| What You Need..... | 5 |
| For Deployment..... | 5 |
| For Hyper-V Server Initial Configuration..... | 6 |
| For Cloudpath Account Setup..... | 6 |
| Deploying the Virtual Appliance to a Hyper-V Server..... | 7 |
| Deployment Overview..... | 7 |
| Retrieving VHDX Image File..... | 7 |
| Replication with Hyper-V Systems..... | 7 |
| Deploying the Virtual Appliance Using Hyper-V Manager..... | 7 |
| Configuring Virtual Processors..... | 8 |
| Configuring the VM Using the Hyper-V Manager Connection Console..... | 10 |
| Hyper-V Checkpoints..... | 10 |
| Activate Account or Log In..... | 11 |
| Overview..... | 11 |
| Activate Account by Activation Code..... | 12 |
| Set a Password for Account..... | 12 |
| Activate Account by Credentials..... | 14 |
| Initial System Setup..... | 15 |
| System Setup Overview..... | 15 |
| System Setup Wizard..... | 16 |
| Publishing Tasks..... | 25 |
| ToDo Items..... | 27 |
| Command Reference..... | 29 |
| Troubleshooting..... | 31 |
| Test Network Connectivity..... | 31 |
| How to Increase the Virtual Appliance Memory..... | 31 |
| How to Expand the MySQL Partition Size from the vCenter Client..... | 31 |
| How to Expand the MySQL Partition Size from the Console..... | 32 |
| Password Recovery..... | 32 |
| How to Recover Admin UI Password..... | 32 |
| How to Recover Service Password..... | 32 |
| How To Find Your System Identifier..... | 33 |
| How To Find Your Current Cloudpath Version | 34 |
| Additional Documentation..... | 35 |

Introduction

- [About this document.....](#) 5
- [Specifications for On-Premise Hyper-V Server.....](#) 5
- [What You Need.....](#) 5

About this document

This is a configuration document that is intended for network administrators.

The document describes the specifications for deploying Cloudpath as a virtual appliance using Microsoft Hyper-V, how to download and deploy the package, and how to perform initial configuration and account setup. This guide also includes the Cloudpath command reference, which provides descriptions and examples for the commands that can be entered from the Hyper-V console or from an SSH login.

Specifications for On-Premise Hyper-V Server

Cloudpath supports virtual appliance deployments using a VMware ESXI server or a Microsoft Hyper-V Manager.

NOTE

For VMware deployments, see the *Deploying Cloudpath as a Virtual Appliance on a VMware™ Server* configuration guide.

Cloudpath Virtual Appliance Specifications

The Cloudpath virtual appliance can be distributed as a Hyper-V virtual hard disk (vhdx) disk image file, which can be deployed as a virtual machine using Microsoft Hyper-V Manager

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

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

Microsoft Hyper-V Specifications

Cloudpath supports Hyper-V versions 2012, and later. This includes Hyper-V Server, Windows Server, and the Client Hyper-V client for Windows 10.

What You Need

You will need to obtain or have access to the following:

For Deployment

- Cloudpath image (vhdx file for Hyper-V)
- Hyper-V Manager

Introduction

What You Need

For Hyper-V Server 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)

Deploying the Virtual Appliance to a Hyper-V Server

- Deployment Overview..... 7
- Retrieving VHDX Image File..... 7
- Deploying the Virtual Appliance Using Hyper-V Manager..... 7
- Configuring Virtual Processors..... 8
- Configuring the VM Using the Hyper-V Manager Connection Console..... 10
- Hyper-V Checkpoints..... 10

Deployment Overview

The deployment process includes the following procedures:

- Retrieving the VHDX Image File
- Deploying the Virtual Appliance Using Hyper-V Manager
- Configuring the VM Using the Hyper-V Manager Connection Console
- Activating the Account or Logging In

Retrieving VHDX Image 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 VHDX image file, binding your VHDX file with the activation code.

When the download is complete, deploy the OVA file using the Hyper-V Manager.

Replication with Hyper-V Systems

The vhd files and their associated snapshots are stored in the same directory. If you plan to set up two systems in replication, be sure to keep the vhd file for each server in a separate folder so that snapshots and other changes are kept together with the appropriate server.

Deploying the Virtual Appliance Using Hyper-V Manager

To deploy the Virtual Appliance using Hyper-V Manager, perform the following steps:

1. Open the Hyper-V Manager.
2. From the **Action** menu, select **New > Virtual Machine**.
This opens the **New Virtual Machine Wizard**.
3. Read the **Before You Begin** screen.
4. In the **Name** field, enter a name for the new VM, and click **Next**.
5. Select **Generation 1**, and click **Next**.

6. Assign **Startup memory**.

NOTE

When using the **New Virtual Machine Wizard**, RAM is specified, but the system assigns only one virtual processor, by default. This value can be increased after the initial setup.

- For software trials, feature testing, and other non-production systems, we recommend using 6 GB (6144 MB) RAM and two virtual processors.
 - For production systems with 4,000 or fewer users, we recommend using 8 GB (8192 MB) RAM and four virtual processors.
 - For production systems with 8,000 or fewer users, we recommend using 12 GB (12,288 MB) RAM and eight virtual processors.
 - For production systems with more than 8,000 users, we recommend using 16 GB (16,384 MB) RAM and eight virtual processors.
 - For production systems with more than 20,000 users, we recommend using 20 GB (20,480 MB) RAM and eight virtual processors.
7. Leave **Use Dynamic Memory** selected (the default), and click **Next**.
 8. On the **Configure Networking** screen, select the appropriate virtual switch in the **Connections** field. Click **Next**.
 9. On the **Connect Virtual Hard Disk** screen, select **Use an existing virtual hard disk**, and browse to the location where the vhdx file exists. Click **Next**.
 10. Verify the setup summary, and click **Finish**.

The system creates the new virtual machine.

Configuring Virtual Processors

By default, the new VM wizard assigns one virtual processor to a new VM. You can increase the number of virtual processors in the VM settings.

NOTE

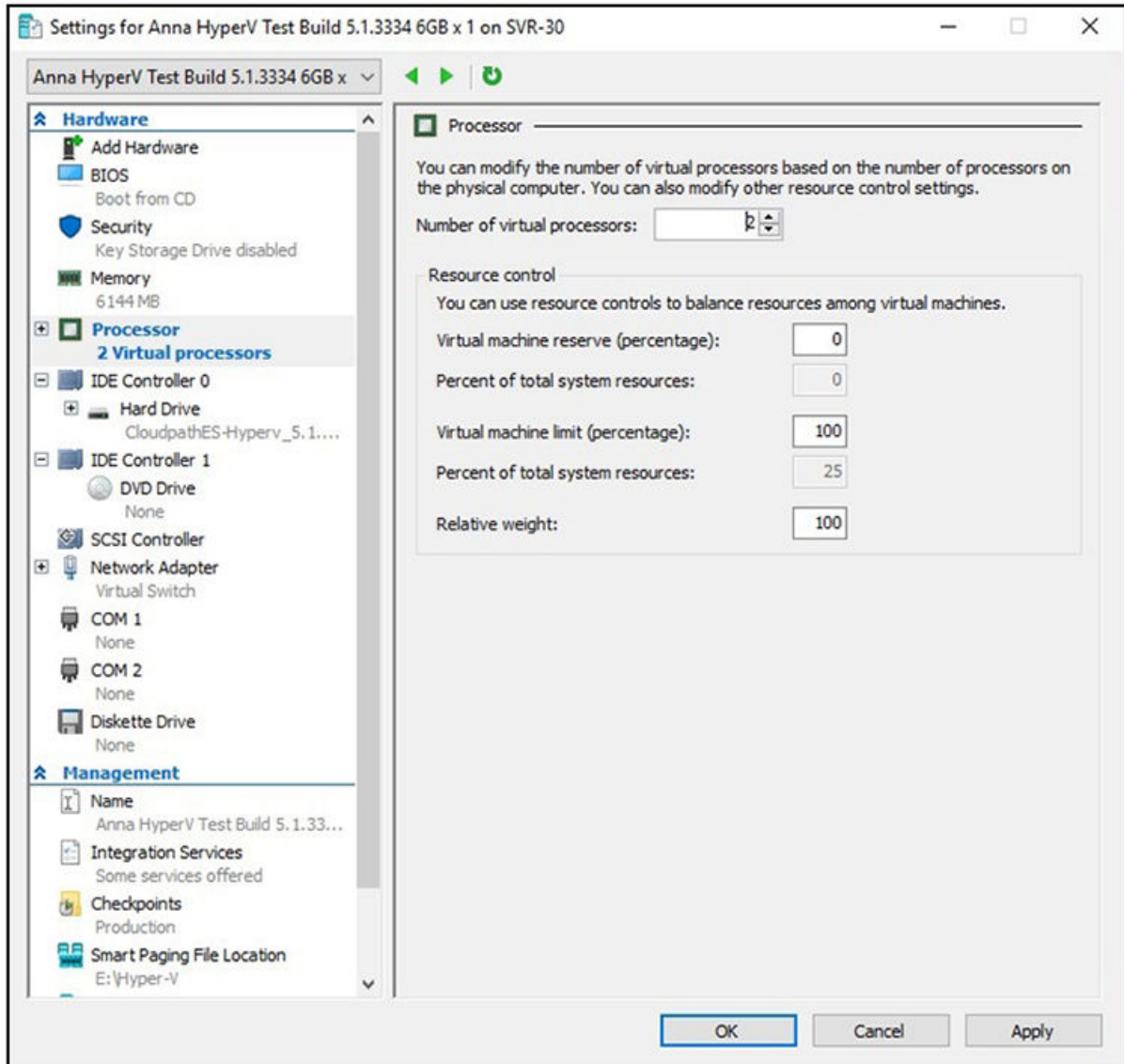
The VM must be powered off to change **Settings**.

To configure virtual processors, perform the following steps:

1. With the VM selected, navigate to the **Action** menu, and select **Settings**. Alternately, you can right-click the selected VM.

2. Select **Processor**.

FIGURE 1 VM Settings



3. In the left pan, select **Processor**.
4. In the right pane, increase the value for **Number of virtual processors**.
5. Click **Apply**, then click **OK**.
6. Power on the virtual machine to continue with the configuration.

Configuring the VM Using the Hyper-V Manager Connection Console

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

To use the Hyper-V Manager Connection console to configure the VM, perform the following steps:

1. From the Hyper-V Manager, with your VM selected, right-click and select **Connect**.
This opens the connection console.
2. Enter **yes** (or **y**) to accept all license agreements.
3. Enter the time zone. For example, enter **America/Denver**.
The default is UTC.
4. Enter the **FQDN hostname** for the virtual appliance (for example, **onboard.company.com**).
5. If you want to enable HTTPS, press **Enter** for "yes" (default), or if not, enter **n** for "no."
6. If you want to use a STATIC IP (rather than DHCP), press **Enter** for "yes" (default), or if not, enter **n** for "no."
 - If you specify "yes" (recommended), assign the IP address of the virtual appliance, subnet mask, and gateway and DNS server IP addresses for your network.
 - If you specify "no," DHCP is used to assign the 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 the 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. If you want to permit SSH access, then press **Enter** for "yes" (default), or if not, enter **n** for "no."
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. If you want to use an NTP server other than pool.net.org, then press **Enter** for "no" (default), or if not, enter **y** for "yes" to specify an NTP server.
The setup is complete.
14. Press **Enter** to reboot the system.

Hyper-V Checkpoints

Checkpoint settings should be changed to Standard, instead of the default, Production.

Activate Account or Log In

- [Overview..... 11](#)
- [Activate Account by Activation Code..... 12](#)
- [Set a Password for Account..... 12](#)
- [Activate Account by Credentials..... 14](#)

Overview

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.

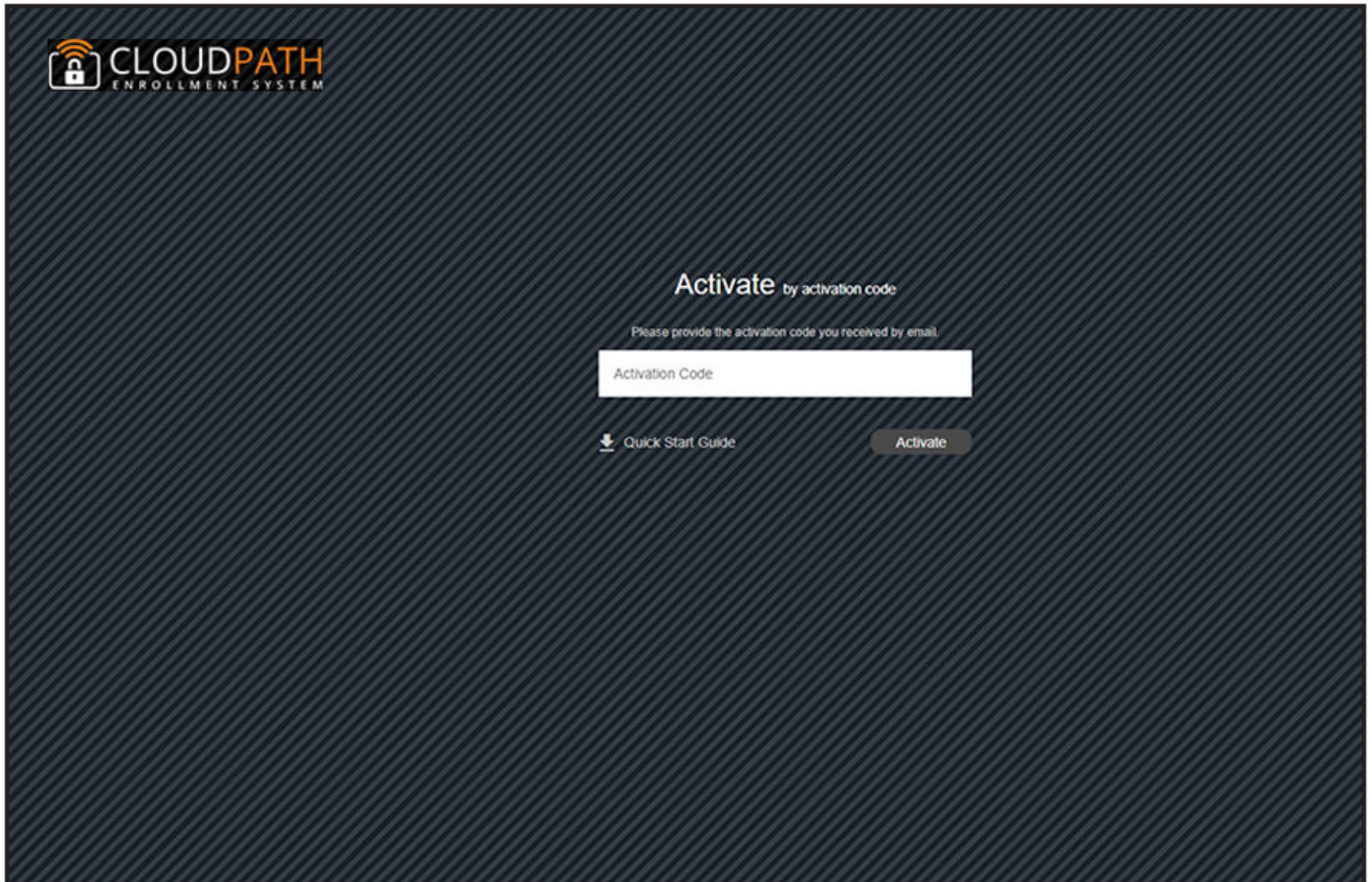
NOTE

The customer Cloudpath *Activation Code* pre-determines whether the Cloudpath application is the single tenant or multitenant version.

Activate Account by Activation Code

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

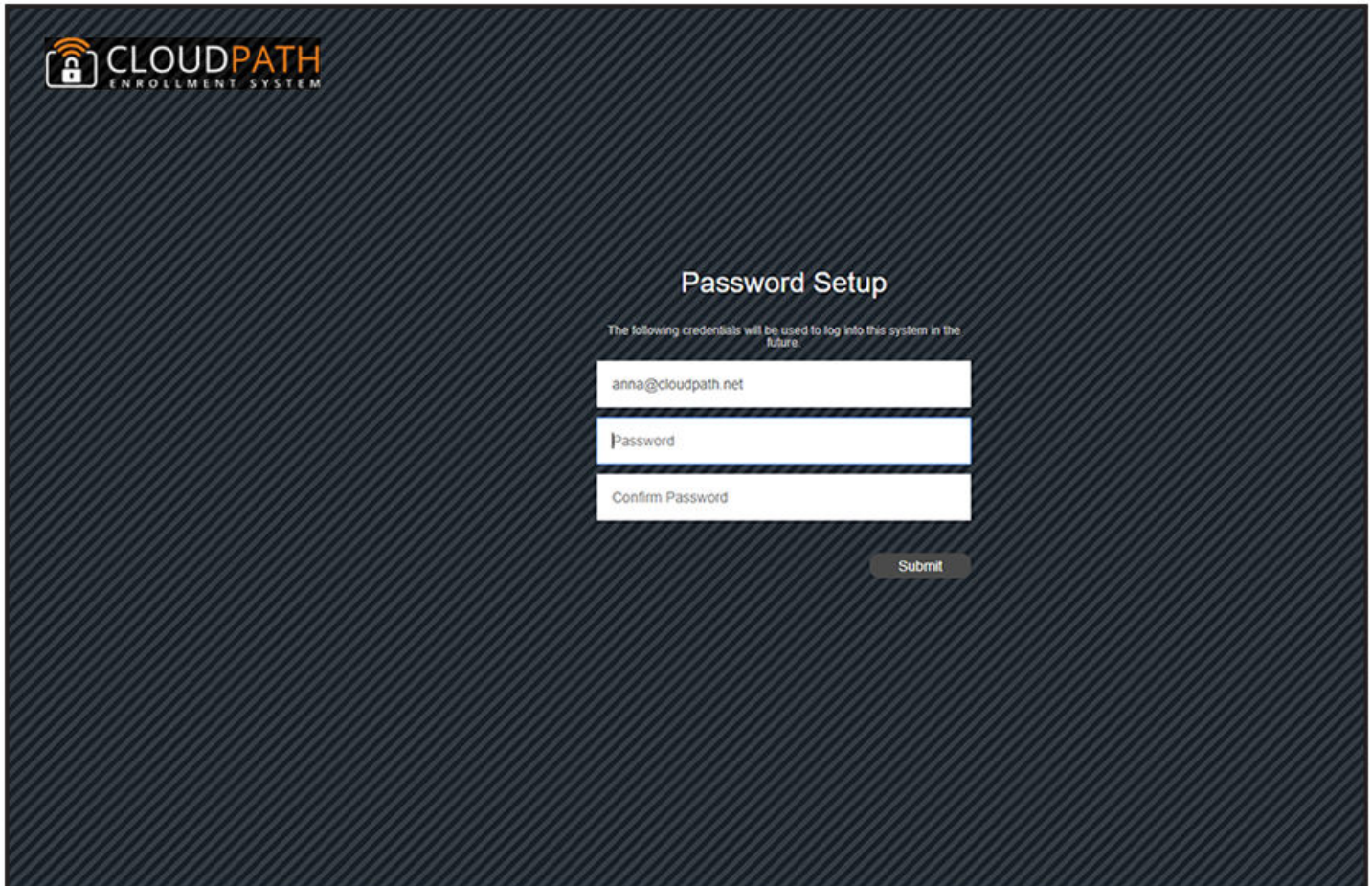
FIGURE 2 Activate Cloudpath Account



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 3 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 below the input fields.

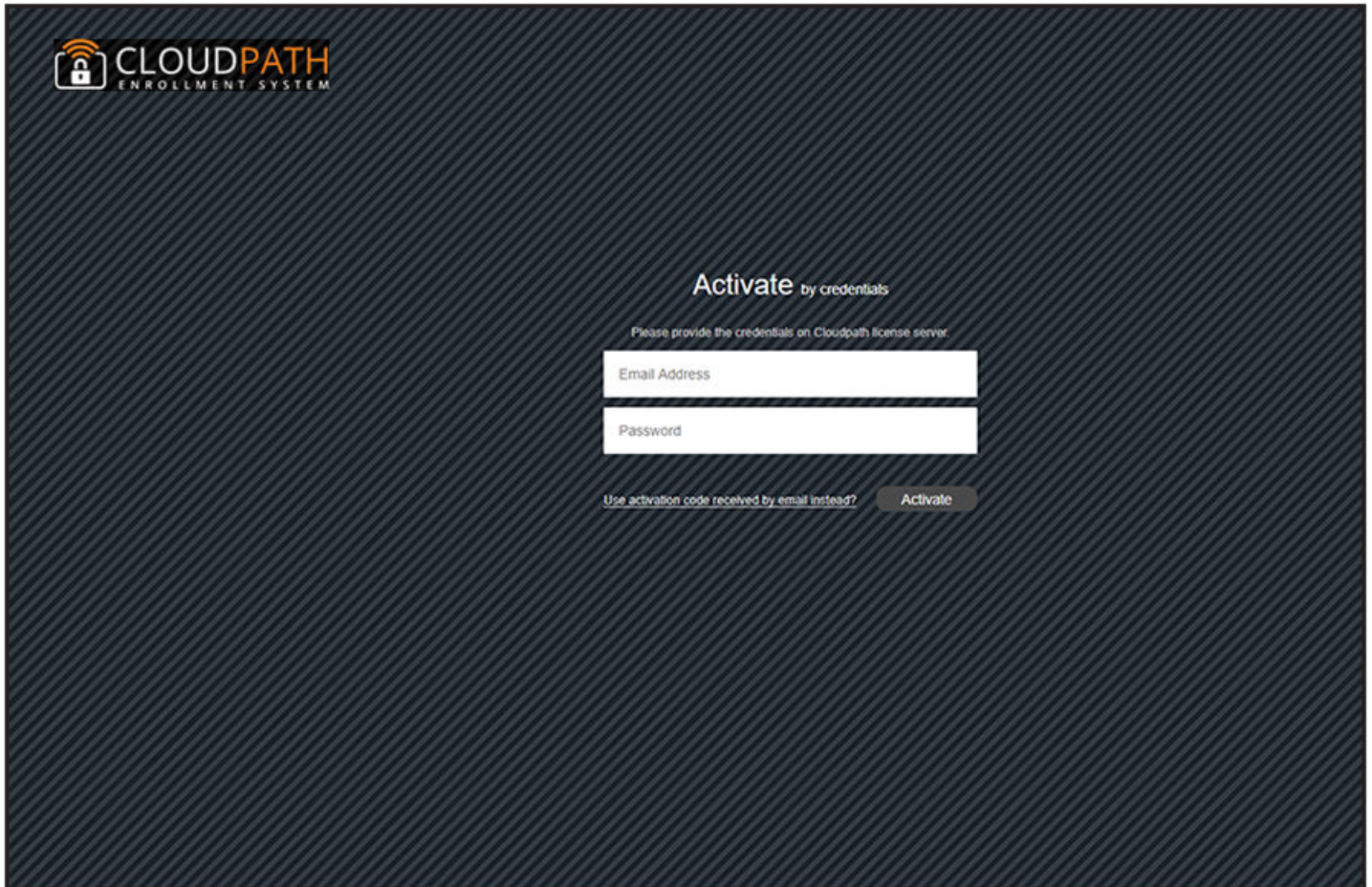
1. Your email address should display. If it does not, enter it on this page.
2. Enter and confirm a password.

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 4 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 Overview..... 15
- System Setup Wizard..... 16
- Publishing Tasks..... 25
- ToDo Items..... 27

System Setup Overview

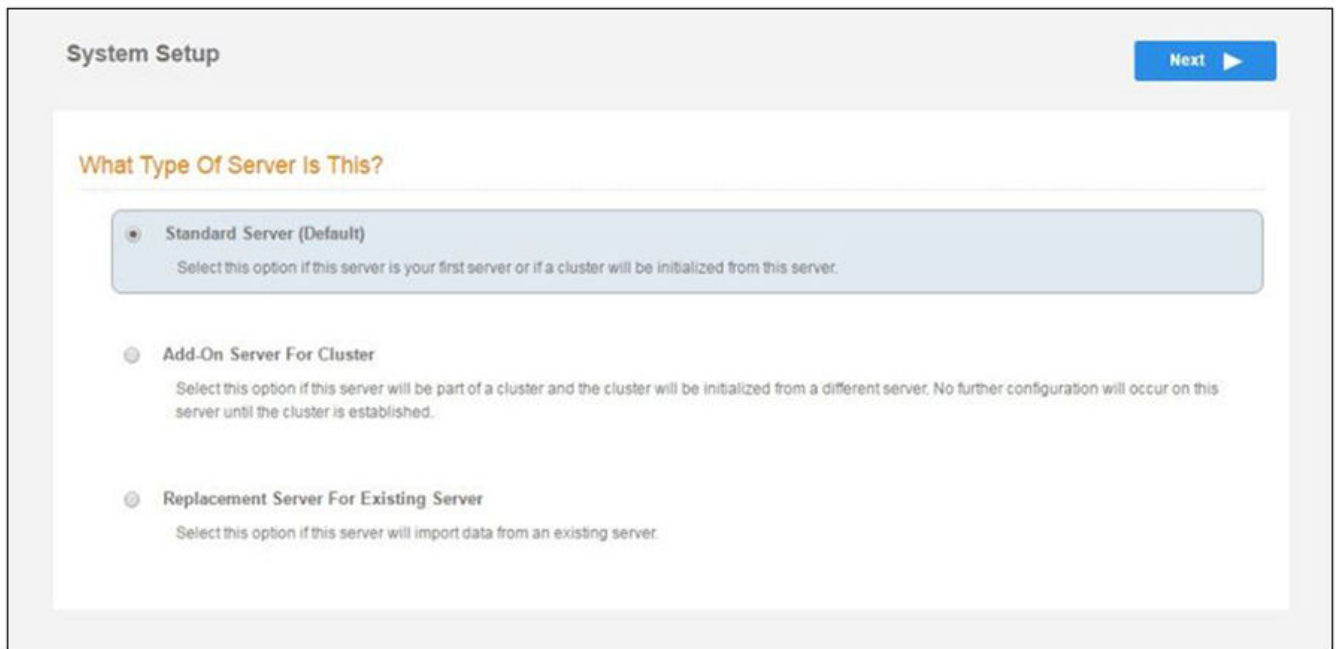
Cloudpath provides you with a single administrator login for the Cloudpath Admin user interface (UI). Additional administrators can be added from the left menu on the **Administration** tab, or you can enable Administrator logins from your authentication servers.

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 5 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 6 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 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 7 WWW Certificate for HTTPS Screen

The screenshot shows a 'System Setup' window with a 'Skip' button and a 'Next' button with a right-pointing arrow. The main heading is 'WWW Certificate for HTTPS'. Below this, there is a paragraph explaining that the system is configured for HTTPS but lacks a valid certificate, leading to 404 errors. To the right is a browser window showing a 404 error for 'https://onboard.company'. Below the text are three radio button options: 'Generate a Certificate Signing Request (CSR)' (selected), 'Upload the WWW Certificate', and 'Skip for now.'.

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 8 Create CSR for HTTPS Screen

- a) Enter the required information.

NOTE

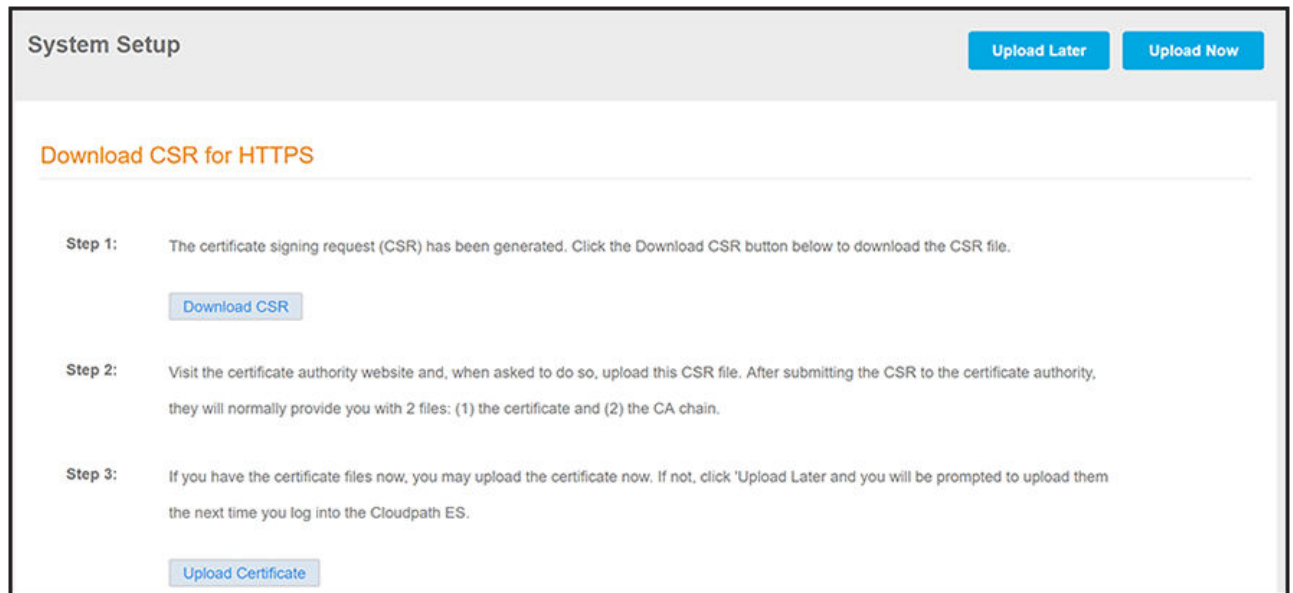
In the Common Name field:

- 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 9 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 9](#), 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 10 Upload WWW Certificate Based on the Downloaded CSR

The screenshot shows a 'System Setup' window with a 'Back' and 'Next' button at the top right. The main content area 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:

- Public Key (PEM):** A 'Choose File' button followed by the text 'anna242cloudpathnet.cer'.
- Chain (PEM or P7b):** A 'Choose File' button followed by the text 'anna242cloudpathnet.chain'.
- Additional Chain (Optional):** A 'Choose File' button followed by the text 'No file chosen'.
- Additional Chain (Optional):** A 'Choose File' button followed by the text 'No file chosen'.
- Private Key Source:** A dropdown menu with the text 'Certificate is based on the downloaded CSR' and a downward arrow.

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

- 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:

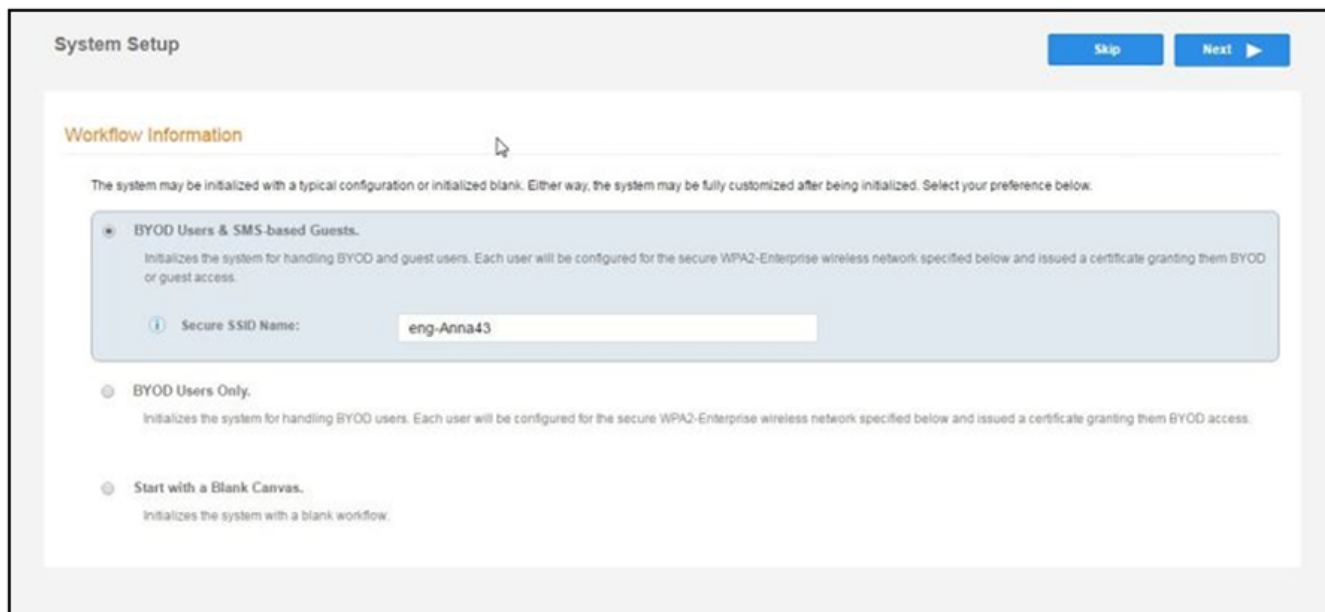
FIGURE 11 Upload Existing WWW Certificate

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 several fields: 'Public Key (PEM):', 'Chain (PEM or P7b):', two 'Additional Chain (Optional):' fields, 'Private Key (PEM):', 'Private Key Password:', and a checkbox for 'Prompt for Password on Boot:'. Each of the first five fields has a 'Choose File' button and the text 'No file chosen'. The 'Private Key Password:' field is an empty text input. 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 fields: 'P12 File:' with a 'Choose File' button and the text 'CloudpathLabWw...rtificate.p12', and 'P12 Password:' with an empty text input.

- 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 12 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 13 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.

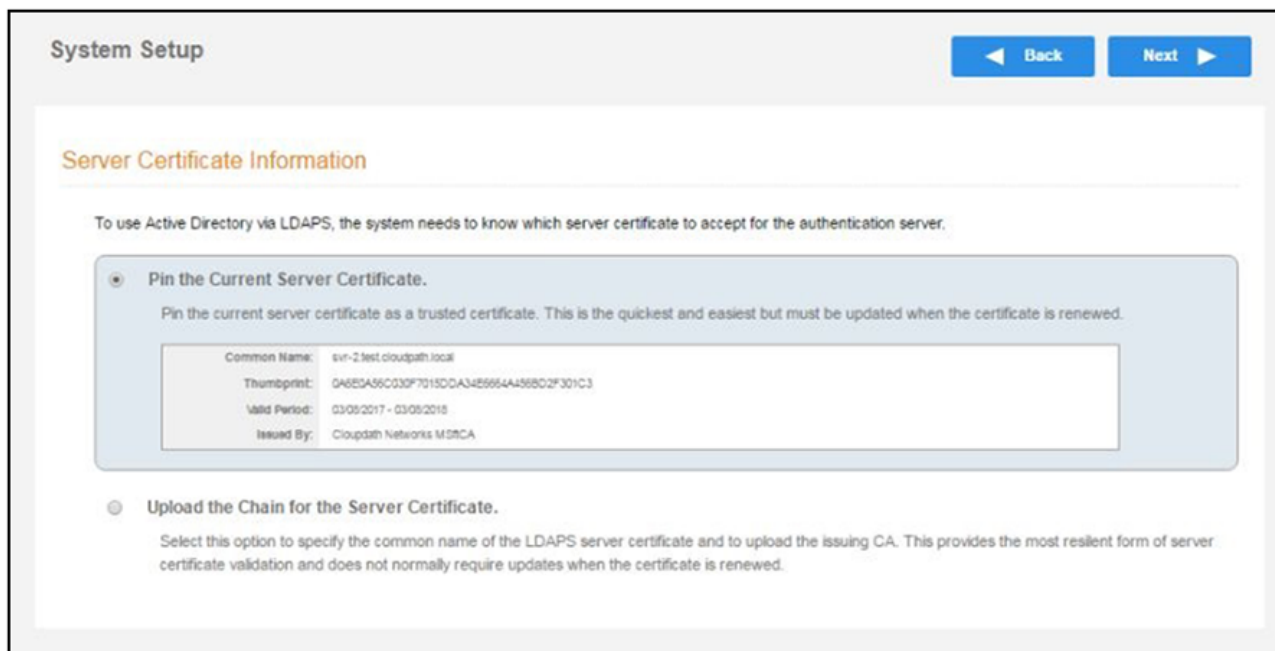
Connect to SAML
Select this option to enable end-users to authenticate via a SAML 2.0 IdP.

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** - If **Use for Admin Logins** is selected, administrators can log into the Cloudpath Admin UI using credentials associated with this authentication server. If **Use for Sponsor Logins** is selected, sponsors can log into the Cloudpath 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.
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 14 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.

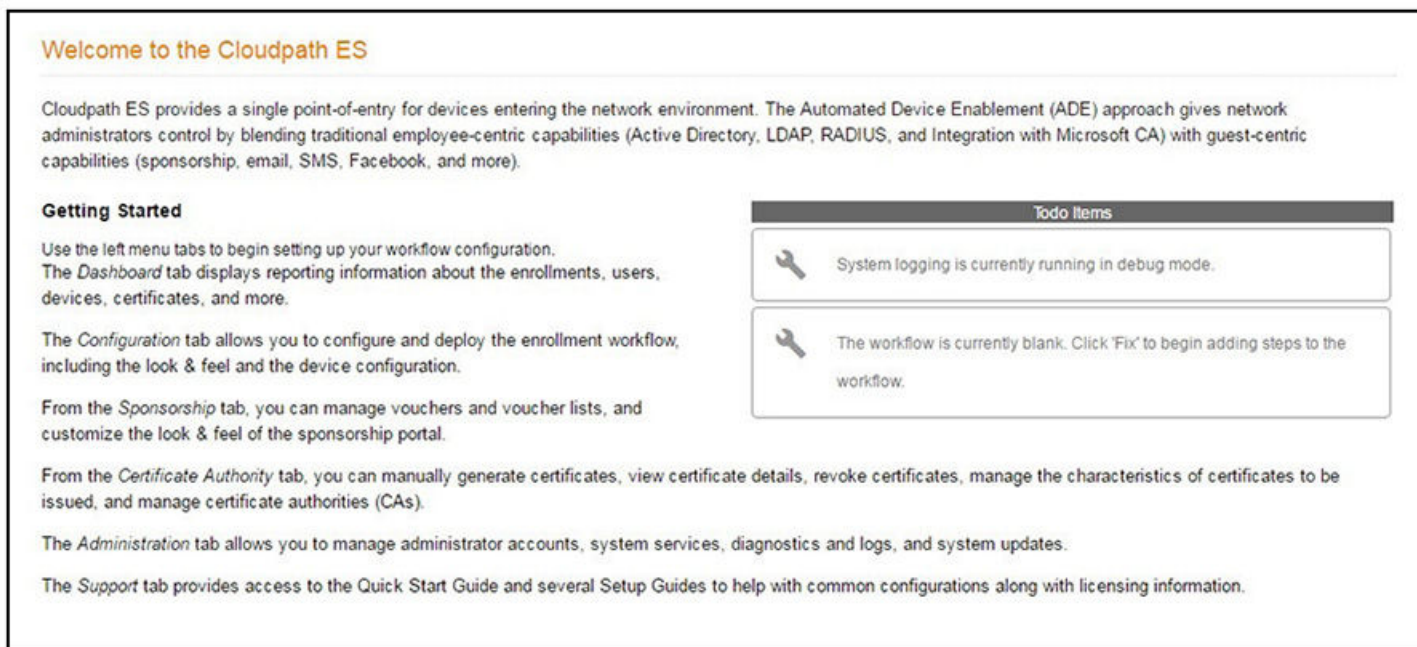
FIGURE 15 System Initialization Status

| 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: | nhu0vjwqediwppth7vw |
| 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.

FIGURE 16 Cloudpath Welcome Page



To configure Cloudpath, refer to 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..... 31
- How to Increase the Virtual Appliance Memory..... 31
- How to Expand the MySQL Partition Size from the vCenter Client..... 31
- How to Expand the MySQL Partition Size from the Console..... 32
- Password Recovery..... 32
- How To Find Your System Identifier..... 33
- How To Find Your Current Cloudpath Version 34

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

To change the memory configuration of a virtual machine's hardware, perform the following steps:

1. From the vCenter client, power off the virtual appliance.
2. Select the VM, and right-click to **Edit Settings**.
3. Select the **Hardware** tab, then 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 from the vCenter Client

To use the vCenter client to expand the size of the partition size that is used for MySQL database operations, perform the following steps:

1. With the VM running, select the VM and right-click to **Edit Settings**.
2. Select the **Hardware** tab, then 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 **Provisioned Size** cannot be selected, try restarting the server using the `sudo halt` command.

Troubleshooting

How to Expand the MySQL Partition Size from the Console

How to Expand the MySQL Partition Size from the Console

To use the console to expand the size of the partition used for MySQL operations, enter the following commands as root:

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

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

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

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

3. Expand the physical volume.

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

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

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

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

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

6. Verify the amount of free disk space available.

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

The output should indicate the increased partition size.

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-uirecovery** 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 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.

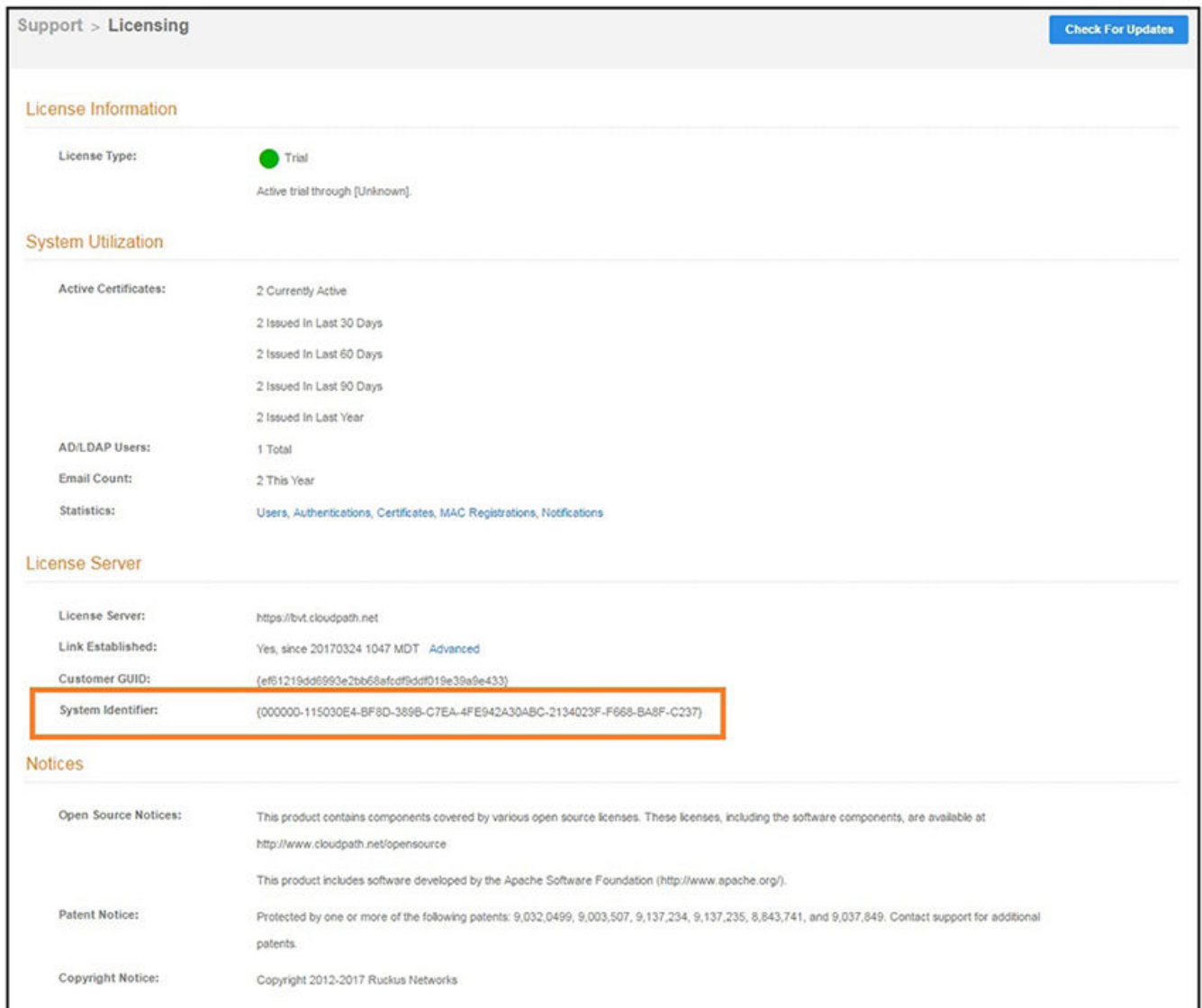
How To Find Your System Identifier

To find your system identifier, perform the following steps:

1. Log into the Cloudpath Admin UI.
2. Go to **Support > Licensing**.

The **System Identifier** is listed in the **License Server** section.

FIGURE 17 Finding the System Identifier



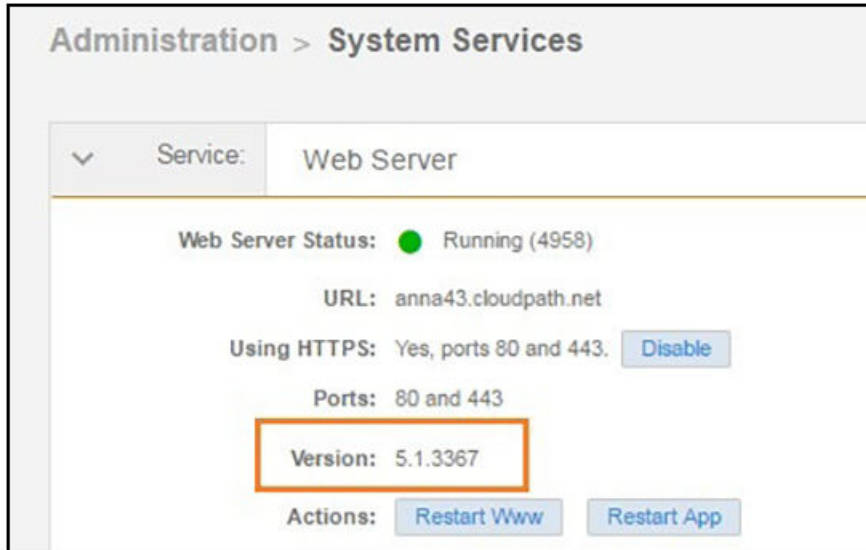
How To Find Your Current Cloudpath Version

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 18 Current Cloudpath Version System Services



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

FIGURE 19 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.



© 2022 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>