DEPLOYMENT GUIDE

Deploying Cloudpath as a Virtual Appliance on a VMware™ Server

Supporting Software Release 5.2

Part Number: 800-71682-001
Publication Date: September 2017

Copyright Notice and Proprietary Information

Copyright 2017 Brocade Communications Systems, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of or as expressly provided by under license from Brocade.

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. BROCADE and RUCKUS WIRELESS, INC. AND THEIR LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. BROCADE and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL BROCADE or RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Brocade, the B-wing symbol, MyBrocade, and ICX are trademarks of Brocade Communications Systems, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

Contents

Specifications for On-Premise Deployed VMware Server

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.

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 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

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

Supported Operating Systems

- Windows XP SP2 and later
- Mac OS X 10.7 and later
- Apple iOS 6.0 and later
- Ubuntu 12.04 and later
- Fedora 18 and later
- Android 4.0.3 and later
- Windows Phone 8.1
- Chromium, all Google-supported versions

Deploying the Virtual Appliance to a VMware Server

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.
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.

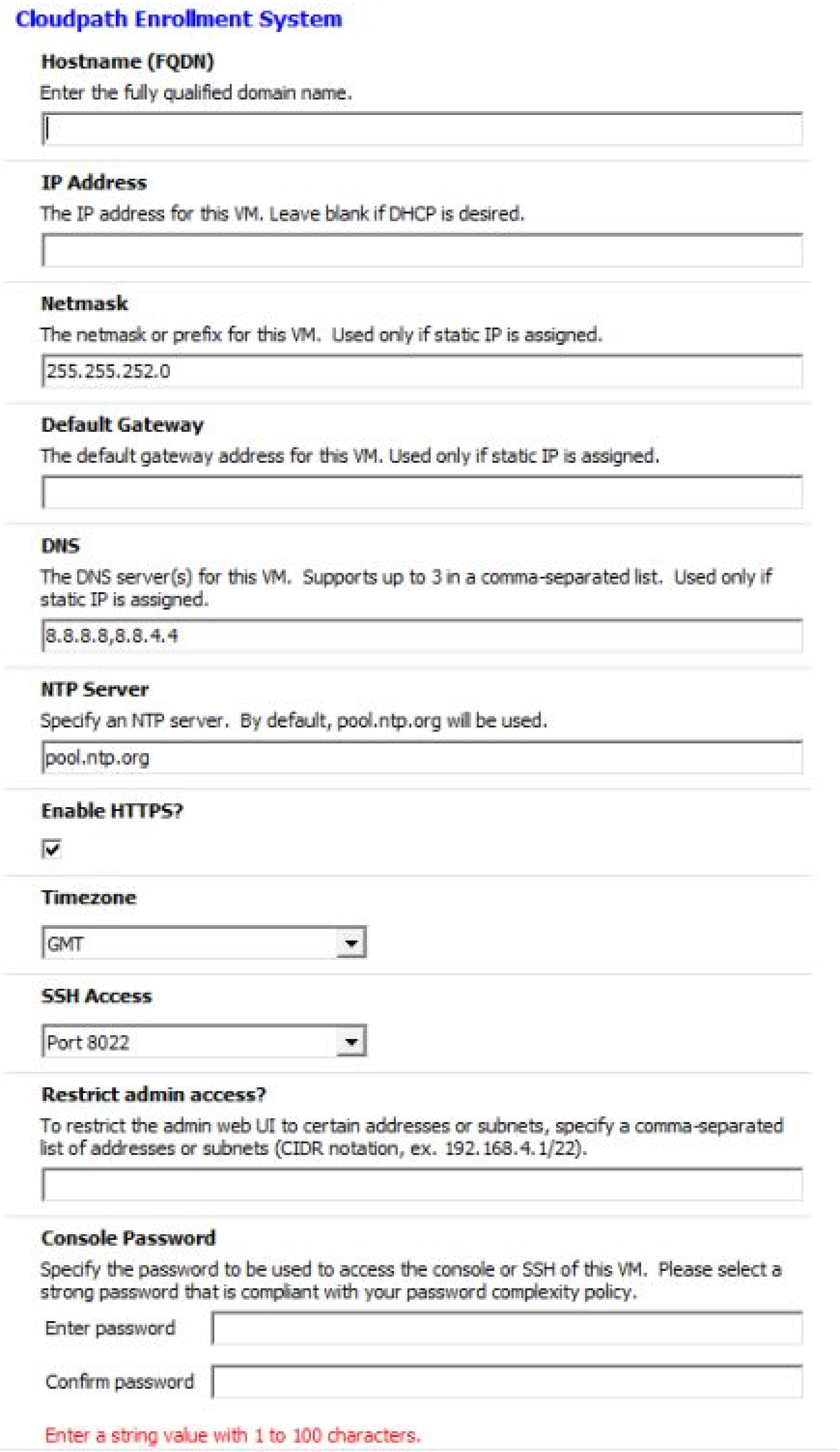
     NOTE
     If you are using Fault Tolerance, you must select Thick provisioning.

   - 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



Cloudpath Enrollment System

Hostname (FQDN)

Enter the fully qualified domain name.

IP Address

The IP address for this VM. Leave blank if DHCP is desired.

Netmask

The netmask or prefix for this VM. Used only if static IP is assigned.

255.255.252.0

Default Gateway

The default gateway address for this VM. Used only if static IP is assigned.

DNS

The DNS server(s) for this VM. Supports up to 3 in a comma-separated list. Used only if static IP is assigned.

8.8.8.8,8.8.4.4

NTP Server

Specify an NTP server. By default, pool.ntp.org will be used.

pool.ntp.org

Enable HTTPS?

☑

Timezone

GMT

SSH Access

Port 8022

Restrict admin access?

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

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.

Enter password

Confirm password

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).

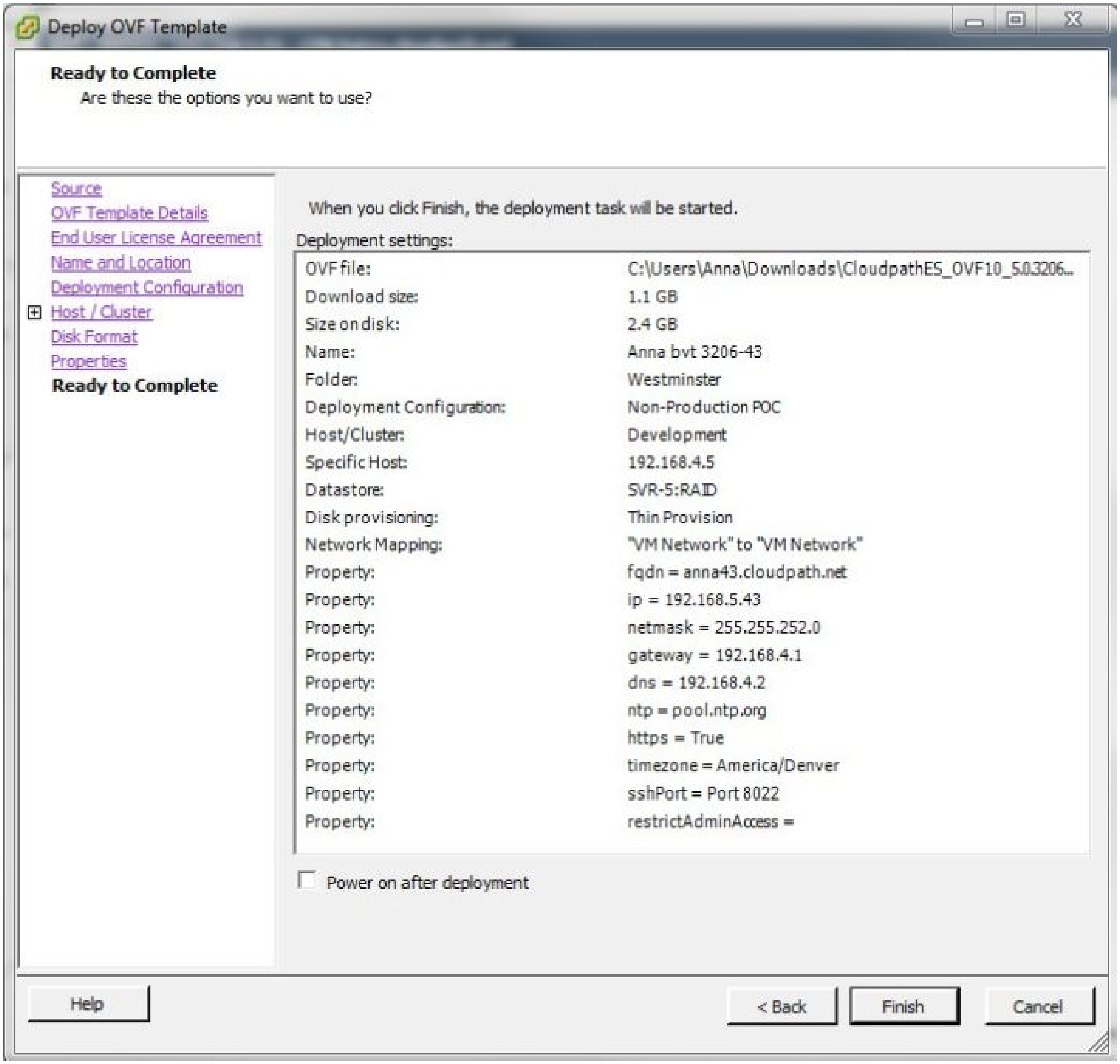
2. Enter the IP Address, Netmask, Default Gateway, and the DNS Servers for this VM. Leave blank for DHCP.
3. Specify an NTP Server or leave the default.
4. HTTPS is enabled by default. Leave unchecked only if Cloudpath is behind another web server using SSL.
5. Select the Timezone.
6. Select SSH port,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



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Users\Anna\Downloads\CloudpathES_OVF10_5.0.3206...
Download size:	1.1 GB
Size on disk:	2.4 GB
Name:	Anna bvt 3206-43
Folder:	Westminster
Deployment Configuration:	Non-Production POC
Host/Cluster:	Development
Specific Host:	192.168.4.5
Datastore:	SVR-5:RAID
Disk provisioning:	Thin Provision
Network Mapping:	"VM Network" to "VM Network"
Property:	fqdn = anna43.cloudpath.net
Property:	ip = 192.168.5.43
Property:	netmask = 255.255.252.0
Property:	gateway = 192.168.4.1
Property:	dns = 192.168.4.2
Property:	ntp = pool.ntp.org
Property:	https = True
Property:	timezone = America/Denver
Property:	sshPort = Port 8022
Property:	restrictAdminAccess =

☐ Power on after deployment

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 in 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

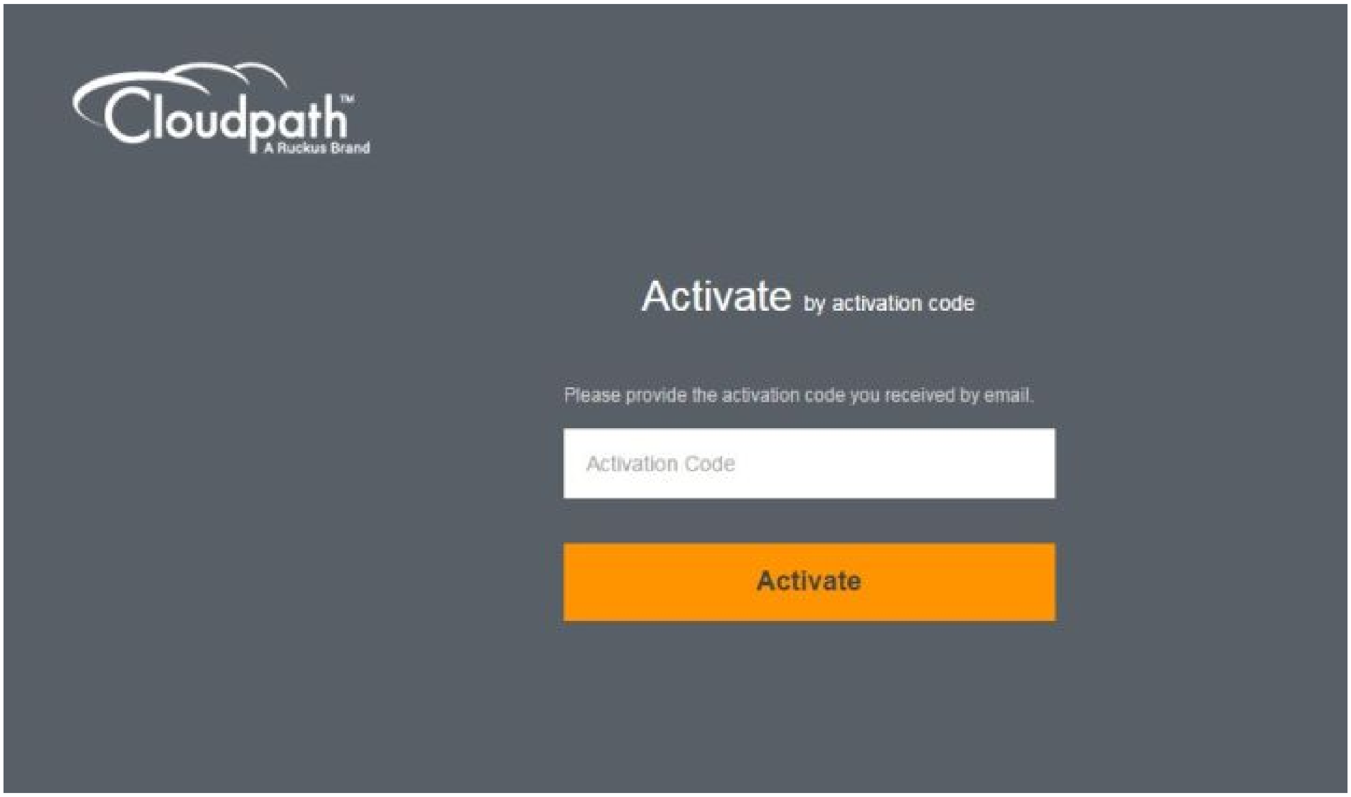
If you are setting up a Cloudpath account for the first time, you will be sent an activation code. If you have existing Cloudpath License server credentials, you can activate an account using those credentials.

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



Activate by activation code

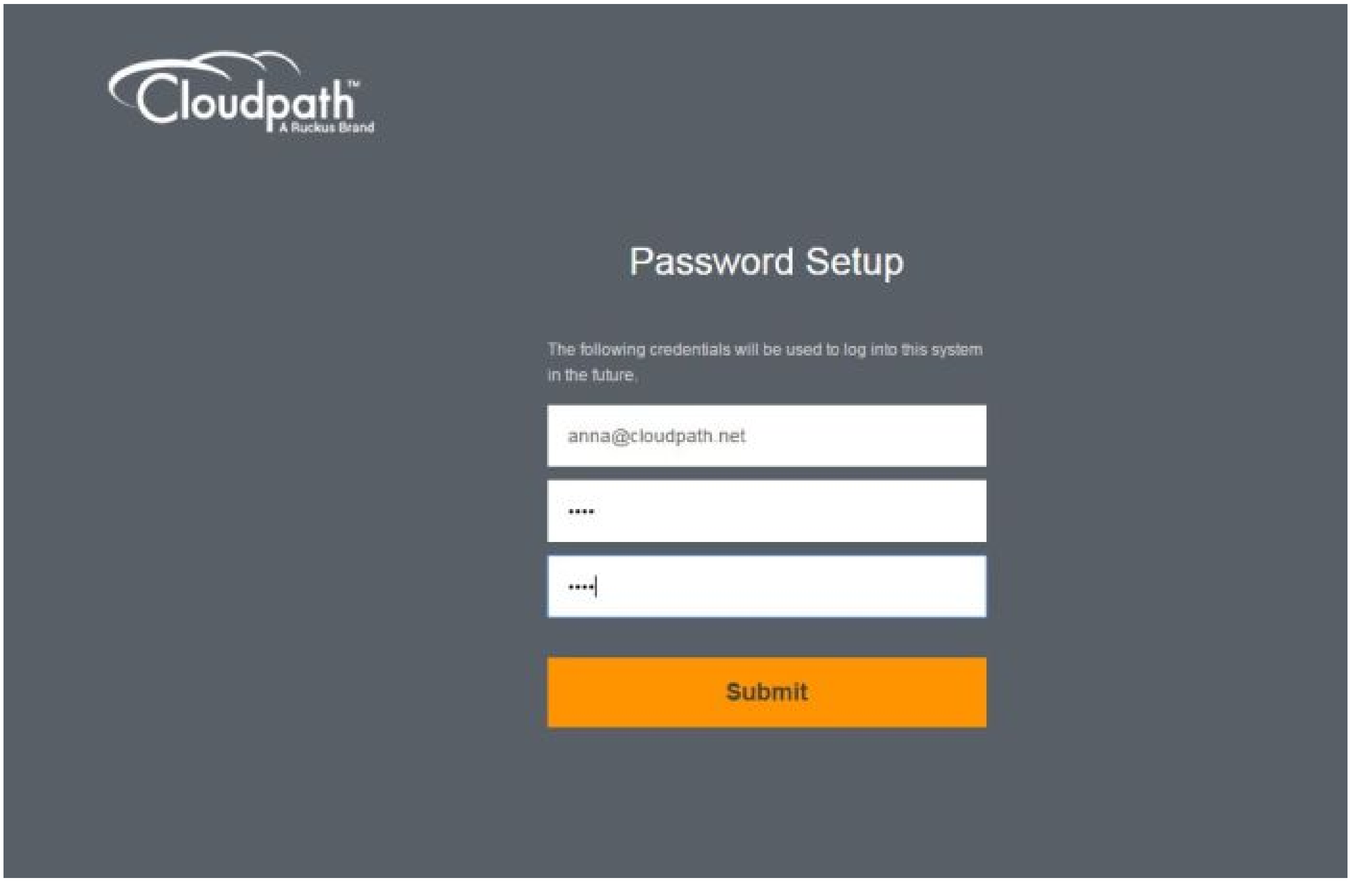
Please provide the activation code you received by email.

Set a Password for Account

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

1. Your email address should display. If it does not, enter it on this page.

FIGURE 4 Set Password



Password Setup

The following credentials will be used to log into this system in the future.

anna@cloudpath.net

••••

••••

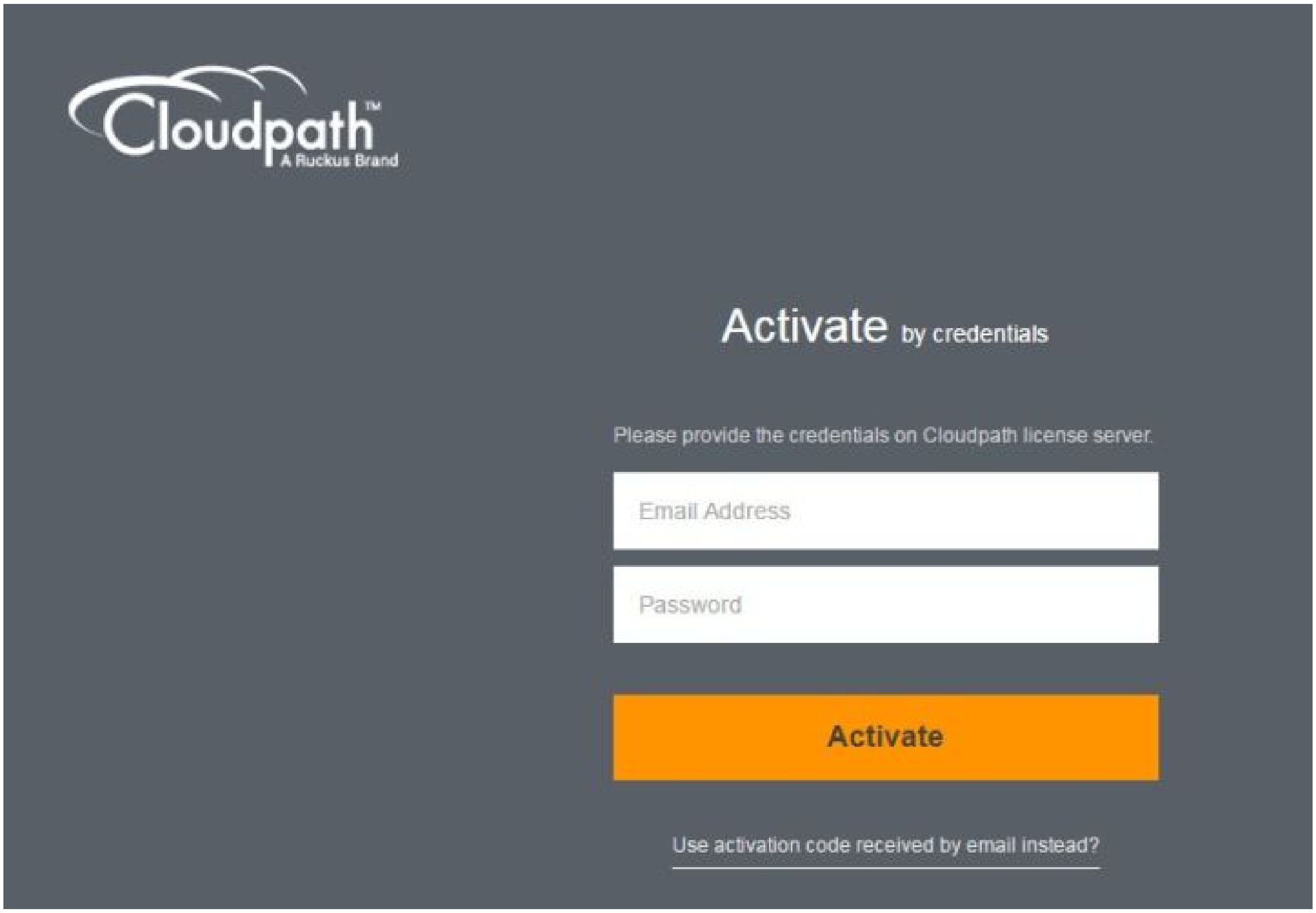
2. Enter and confirm a password.

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



Activate by credentials

Please provide the credentials on Cloudpath license server.

Email Address

Password

Initial System Setup

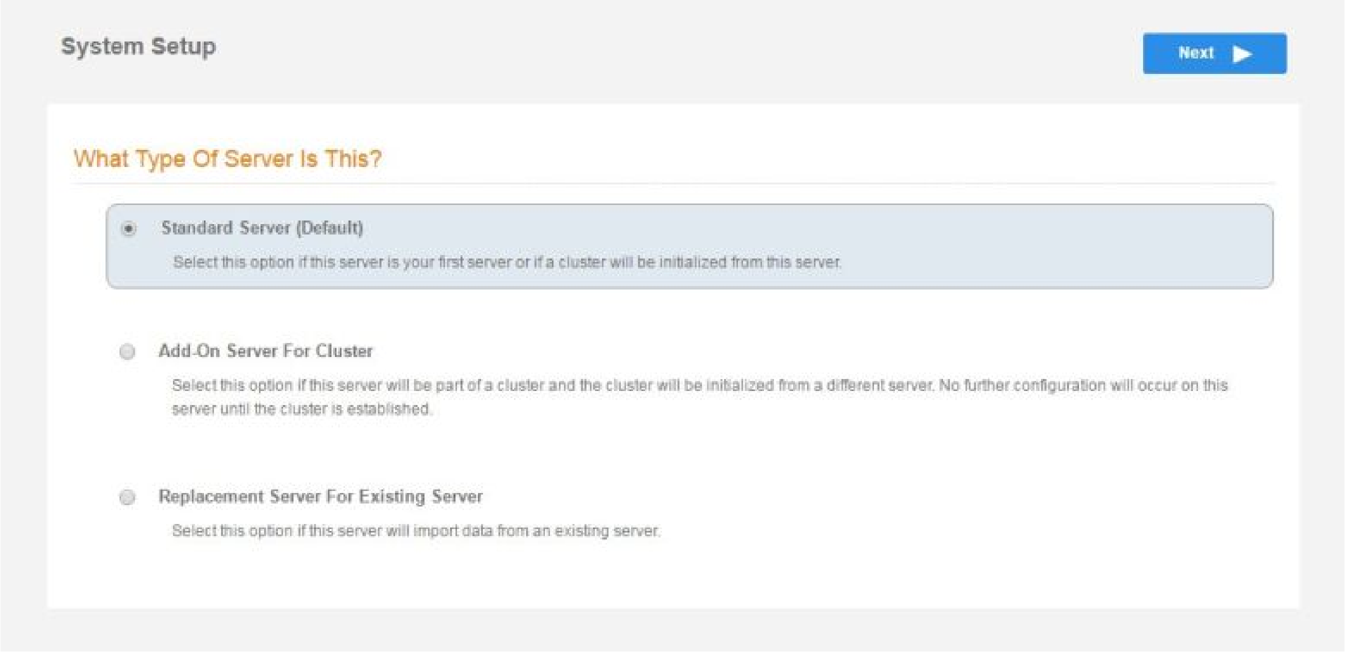
Cloudpath provides you with a single administrator login for the Cloudpath Admin UI. Additional administrators can be added from the left menu Administration tab, or you can enable Administrator logins from your authentication servers.

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



System Setup

What Type Of Server Is This?

● Standard Server (Default)

Select this option if this server is your first server or if a cluster will be initialized from this server.

○ Add-On Server For Cluster

Select this option if this server will be part of a cluster and the cluster will be initialized from a different server. No further configuration will occur on this server until the cluster is established.

○ Replacement Server For Existing Server

Select this option if this server will import data from an existing server.

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

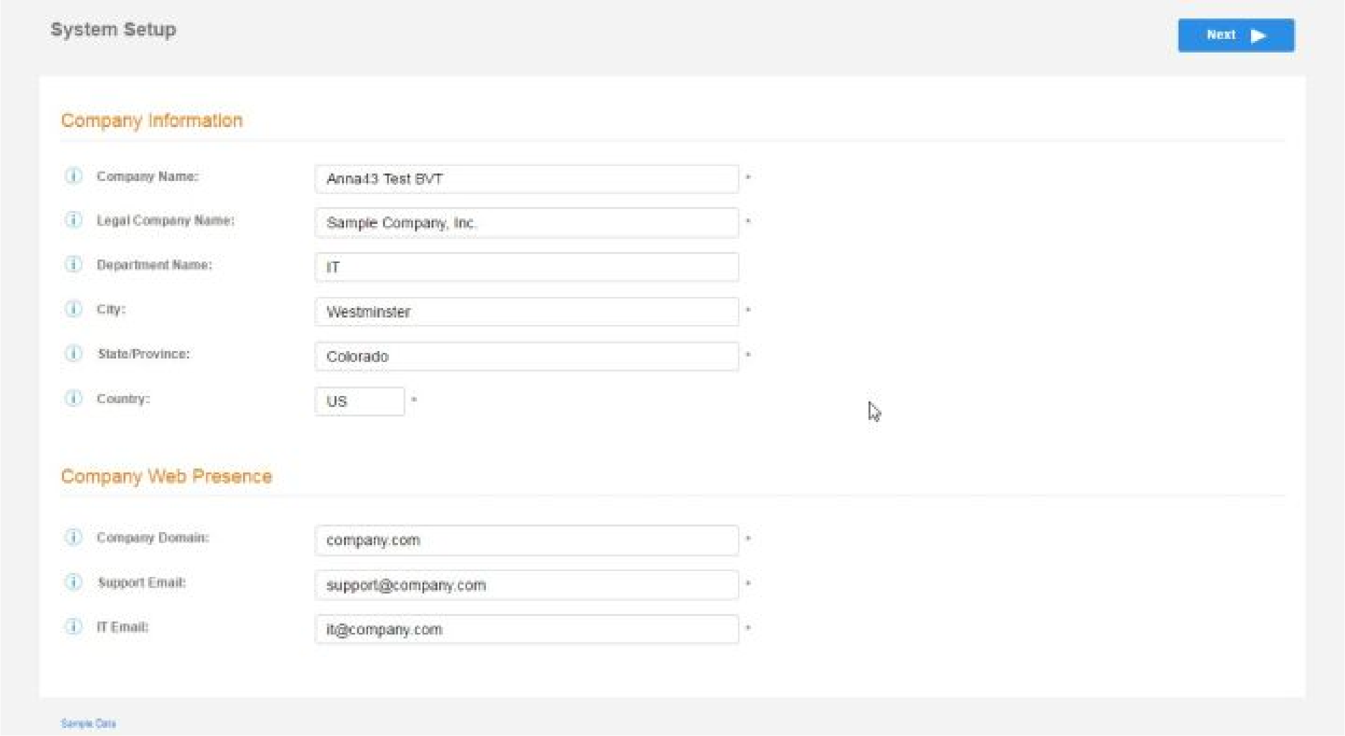
- If you are setting up this server for replication, you can choose to set the server as an Add-On or Replacement server. These selections provide an alternate set up process, requiring less information for the initial setup. Add-On and Replacement servers receive most of their configuration from the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

   This information is embedded in the onboard root CA certificate.

   FIGURE 7 Company Information



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 *

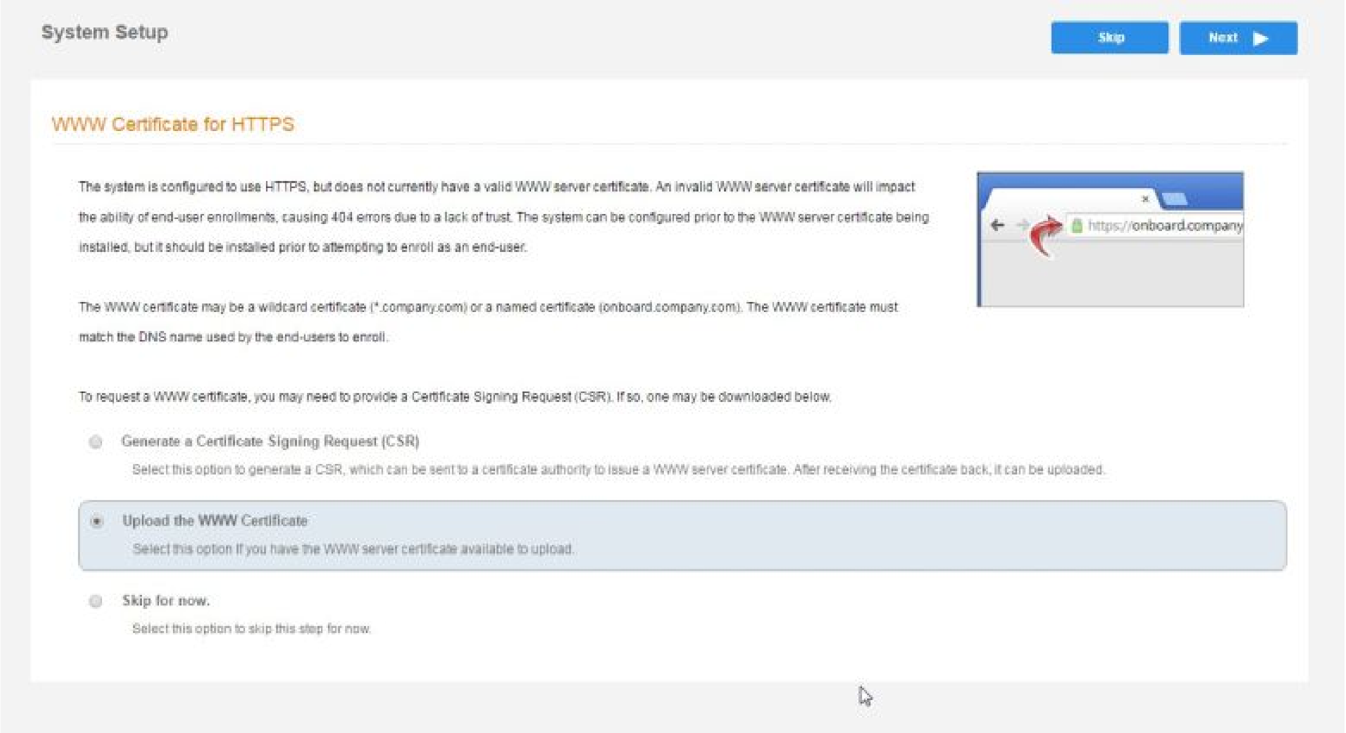
Support Email: support@company.com *

IT Email: it@company.com *

3. Configure the WWW Certificate.

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

FIGURE 8 WWW Certificate for HTTPS



WWW Certificate for HTTPS

The system is configured to use HTTPS, but does not currently have a valid WWW server certificate. An invalid WWW server certificate will impact the ability of end-user enrollments, causing 404 errors due to a lack of trust. The system can be configured prior to the WWW server certificate being installed, but it should be installed prior to attempting to enroll as an end-user.

The WWW certificate may be a wildcard certificate (*.company.com) or a named certificate (onboard.company.com). The WWW certificate must match the DNS name used by the end-users to enroll.

To request a WWW certificate, you may need to provide a Certificate Signing Request (CSR). If so, one may be downloaded below.

○ Generate a Certificate Signing Request (CSR)
Select this option to generate a CSR, which can be sent to a certificate authority to issue a WWW server certificate. After receiving the certificate back, it can be uploaded.

● Upload the WWW Certificate
Select this option if you have the WWW server certificate available to upload.

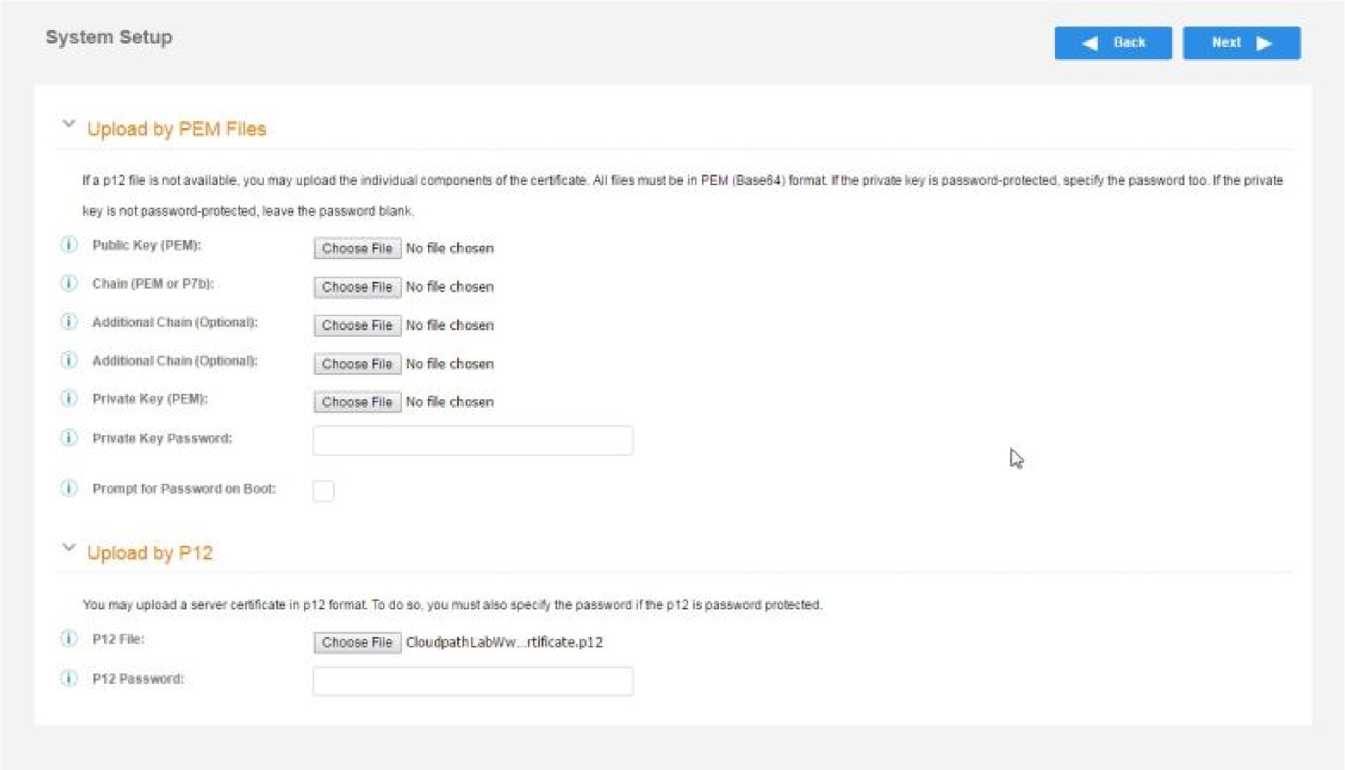
○ Skip for now.
Select this option to skip this step for now.

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

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.

4. Upload the WWW certificate.

FIGURE 9 Upload WWW Certificate



Upload by PEM Files

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):	Choose File	No file chosen
Chain (PEM or P7b):	Choose File	No file chosen
Additional Chain (Optional):	Choose File	No file chosen
Additional Chain (Optional):	Choose File	No file chosen
Private Key (PEM):	Choose File	No file chosen
Private Key Password:		
Prompt for Password on Boot:	□	

Upload by P12

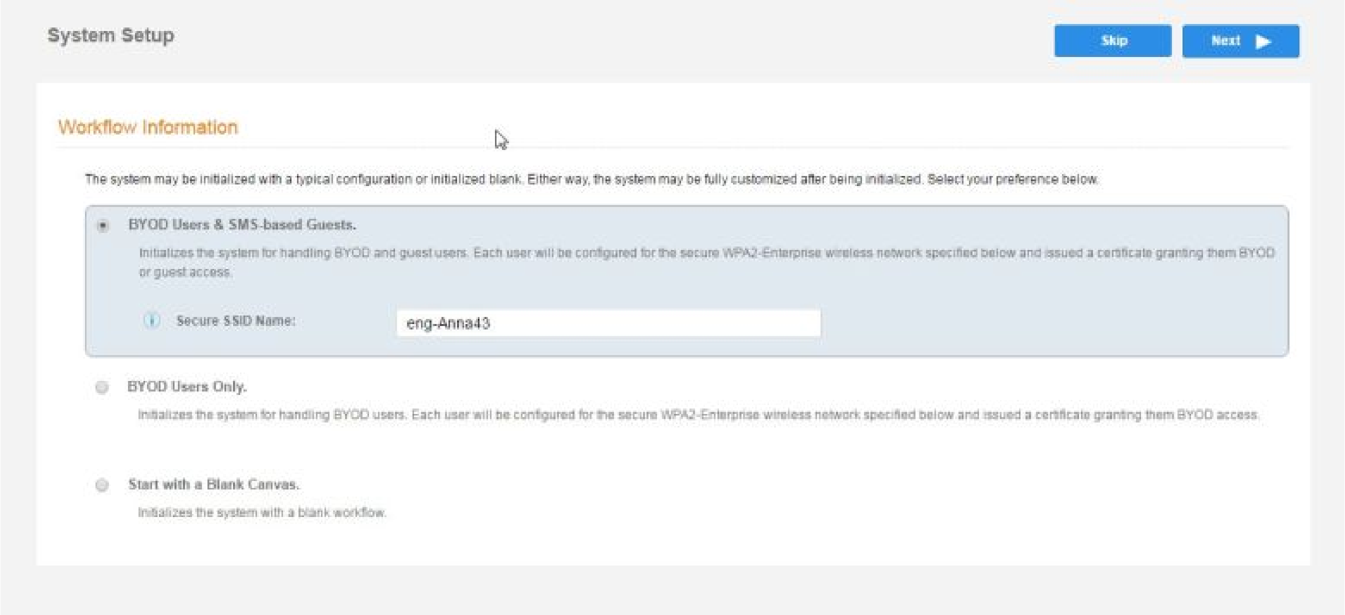
You may upload a server certificate in p12 format. To do so, you must also specify the password if the p12 is password protected.

P12 File:	Choose File	CloudpathLabWw...rtificate.p12
P12 Password:		

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

5. Select the Default Workflow.
   - To initialize the system with a sample configuration, select BYOD Users & SMS Guests, or BYOD Users Only. This creates an initial workflow for BYOD users and sponsored guests (or BYOD users only) that you can use as a template, or simply add a device configuration and use immediately.
   - To create your own workflow, select Start with Blank Canvas.

FIGURE 10 Select Default Workflow



Workflow Information

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

● BYOD Users & SMS-based Guests.
Initializes the system for handling BYOD and guest users. Each user will be configured for the secure WPA2-Enterprise wireless network specified below and issued a certificate granting them BYOD or guest access.

Secure SSID Name: eng-Anna43

○ BYOD Users Only.
Initializes the system for handling BYOD users. Each user will be configured for the secure WPA2-Enterprise wireless network specified below and issued a certificate granting them BYOD access.

○ Start with a Blank Canvas.
Initializes the system with a blank workflow.

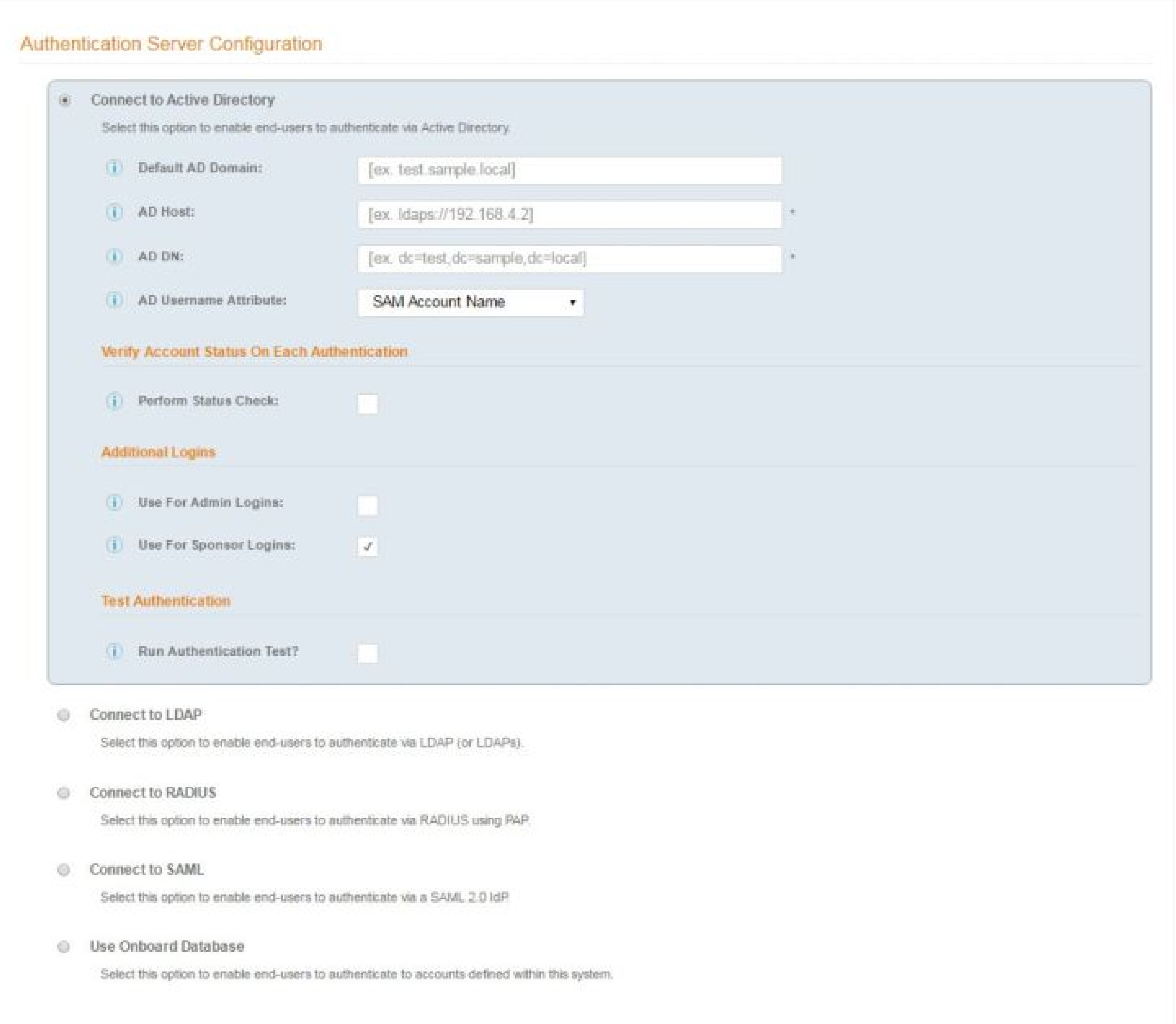
6. Configure the Authentication Server.

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

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

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

   FIGURE 11 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? □

○ 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.

NOTE
See the *Cloudpath Quick Start Guide* for information about the full list of authentication server supported by Cloudpath.

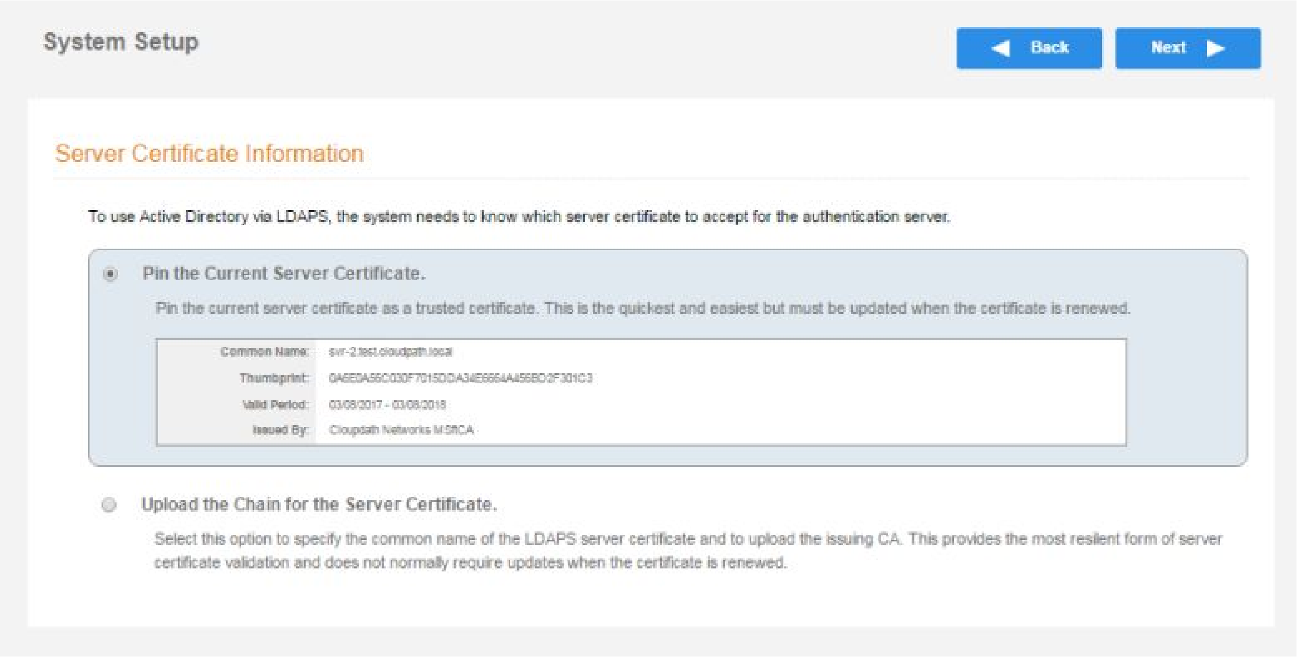
b) Consider these optional settings for the authentication server:

- 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.

7. 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 12 Authentication Server Certificate



Server Certificate Information

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

● Pin the Current Server Certificate.

Pin the current server certificate as a trusted certificate. This is the quickest and easiest but must be updated when the certificate is renewed.

Common Name:	svr-2.test.cloudpath.local
Thumbprint:	0A6E0A56C030F7015DDA34E6664A456BD2F301C3
Valid Period:	03/08/2017 - 03/08/2018
Issued By:	Cloudpath Networks MSftCA

○ Upload the Chain for the Server Certificate.

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

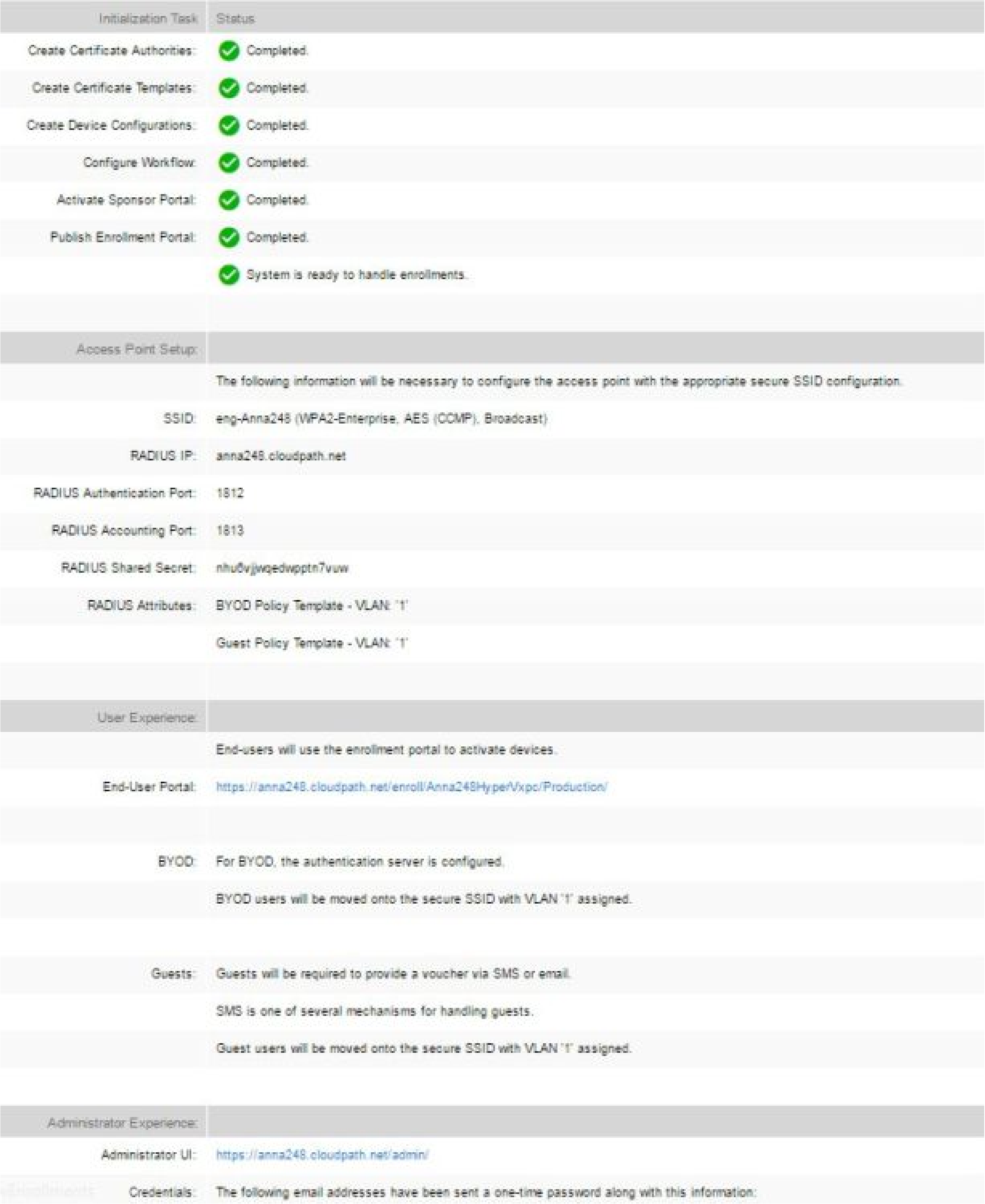
b) Select Upload the Chain for the Server Certificate to upload a certificate chain from an issuing CA. You must specify the common name for the LDAPS server certificate. This certificate does not need to be updated when the certificate is renewed.

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 13 System Initialization Status

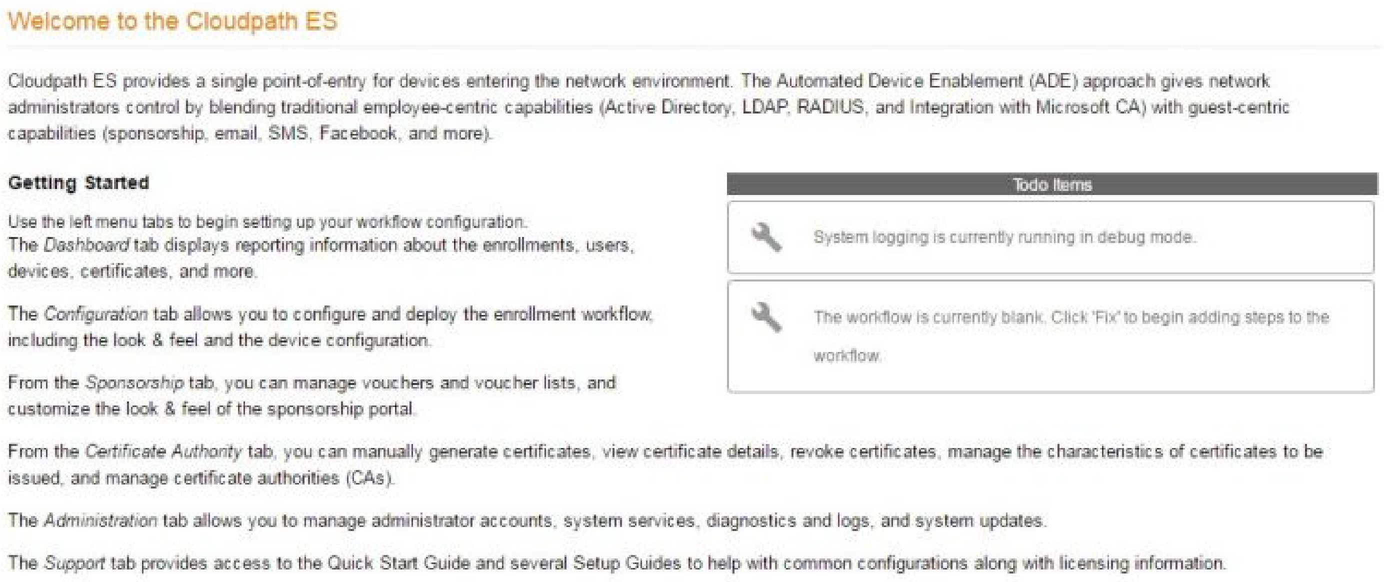


Initialization Task	Status
Create Certificate Authorities:	✓ Completed.
Create Certificate Templates:	✓ Completed.
Create Device Configurations:	✓ Completed.
Configure Workflow:	✓ Completed.
Activate Sponsor Portal:	✓ Completed.
Publish Enrollment Portal:	✓ Completed.
	✓ System is ready to handle enrollments.
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:	nhu6vjjwqedwpptn7vuw
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 14 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.

Todo Items

System logging is currently running in debug mode.

The workflow is currently blank. Click 'Fix' to begin adding steps to the workflow.

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.

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

Cloudpath Command Reference

You can access the Cloudpath command line using the service account.

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.

> NOTE
> 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.

> NOTE
> 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. `[<serviceacctlogin@<hostname>]$ config`
config admin-access allow-all	Clears restrictions to the administrative functionality so that an administrator can access the Cloudpath Admin UI from any IP address.	No parameters. `config admin-access allow-all`

config admin-access restrict	Restricts which IP addresses have administrative access to the Cloudpath Admin UI.	[Comma separated list of IP addresses/CIDR]
		`config admin-access restrict 172.16.4.20, 172.16.5.18`
		or
		`config admin-access restrict 172.16.4.20/24`

config fips-crypto	Enable or disable use of FIPS 140-2 cryptography.	[Enable or Disable] [Requires the service password]
		`# config fips-crypto enable`
		`[sudo] password for cpn_service: enterservicepwd`

config fips-crypto state	Display whether FIPS 140-2 cryptography is enabled.	No parameters. `config fips-crypto state`
config hostname	Sets the hostname.	[This system's network name (FQDN)] `config hostname test22.company.net`
config hostname-restricted allow-all	Request by IP address are not blocked.	No parameters `config hostname-restricted allow-all`
config hostname-restricted restrict	Requests that do not match the hostname are blocked.	No parameters `config hostname-restricted restrict`
config https enable	Sets whether the Apache server should be run as HTTP or HTTPS.	[The HTTPs port to use] `config https enable 55`
config https disable	Sets whether the Apache server should be run as HTTP or HTTPS.	No parameters `config https disable`
config https-servername default	Uses the system's hostname (FQDN).	No parameters `config https-servername default`
config https-servername override	Set the HTTPS server name. This is typically used when operating behind a load balancer.	[This system's network name] `config https-servername test22.company.net`

TABLE 1 config commands (continued)

Command	Description	Parameters and Examples
config network DHCP	Configures whether you want DHCP to assign network IP addresses.	[*true* to use DHCP, *false* to use STATIC IP addresses] `config network DHCP true` 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. `config network restart`
config network STATIC dns	Configures the STATIC IP addresses for the DNS server.	[IP address of the DNS server] `config network STATIC dns 172.16.4.202`
config network STATIC ip	Configures the STATIC IP addresses for the system's eth0 interface, subnet mask, and gateway.	[IP address, subnet mask, and gateway for the eth0 interface] `config network STATIC ip 172.16.6.35 255.255.252.0 172.16.4.1`
config ntp	Sets the NTP server	[IP address of the NTP server] `config ntp 172.16.2.106`
config ntp sync-now	Forces an ntpdate to the configured NTP server.	[hostname for shared db] `config ntp sync-now`
config proxy set	Sets the HTTP proxy. Requires a reboot. The HTTP port and HTTPS port must be the same. This is the port number for the HTTP proxy tunnel. The [proxy-bypass-hosts] parameter (optional) is a comma-separated list of hosts that should bypass the proxy. Use **config clear-proxy** to remove the configuration.	[HTTP hostname] [HTTP port] [HTTPS hostname] [HTTPS port] [proxy- bypass-hosts] `config proxy hostA 80 hostB 80 hostC,hostD`
config proxy remove	Removes the HTTP proxy	No parameters `config proxy remove`

config ssh enable	Enables SSH access. The default port is 8022, or you can select port 22.	[SSH port]
		`config ssh enable`
		or
		`config ssh enable 22`

config ssh disable	Disables SSH access.	[SSH port] `config ssh disable`
config sslv3 allow	Permits SSLv3 protocol on HTTPS connections.	No parameters `config sslv3 allow`
config sslv3 block	Prevents SSLv3 protocol on HTTPS connections.	No parameters `config sslv3 block`

config timezone	Sets the timezone to be used.	[Zone name]
		`config timezone`
		This command displays a list of acceptable timezones.
		When prompted, enter the desired timezone as shown.
		`America/Denver`
		Alternately, you can enter the correct timezone as part of the command.
		`config timezone America/Denver`

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 Cloudpath database.

TABLE 4 maintenance commands

Command	Description	Parameters and Examples
maintenance backup create	Create a backup file (zipped `tar.gz`) of the Cloudpath database and SCP it to a remote server.	[IP address or hostname of the remote server] [Port number] [Remote username] [Path to file location on the remote system] **`maintenance backup create 172.16.4.20 22 username / home/db/file`**
maintenance backup restore mount	Restore a backup from a locally mounted drive.	No parameters. **`maintenance backup restore mount`**
maintenance backup restore scp	Restore a backup file from a remote server via SCP.	[IP address or hostname of the remote server] [Port number] [Remote username] [Path to file location on the remote system] **`maintenance backup restore scp 172.16.4.20 22 u sername /home/db/file`**
maintenance backup schedule mount	Creates a recurring backup via a locally mounted drive. Note the different syntax examples for cifs and nfs drive types.	[Username for remote drive] [Path to mount] [Path within mount to backup directory] [Type of drive (cifs or nfs)] [true to merge changes into full backup, false to not merge] Syntax for cifs:

TABLE 4 maintenance commands (continued)

Command	Description	Parameters and Examples

		`# maintenance backup schedule mount admin \ \\\\172.128.4.20\\backu p\\test servername-cifs cifs true`
		Syntax for nfs:
		`# maintenance backup schedule mount '' 172.128.4.20:/backup/ servername-nfs nfs true`

maintenance backup schedule scp	Creates a recurring backup via SCP to a remote server	[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] `maintenance backup schedule scp 172.16.4.20 22 username /path/to /file 0 0 * * 3` (Note the space between minute, hour, day, month schedule parameters.) For more information about cron schedule parameters, refer to Linux documentation.
maintenance backup unschedule mount	Removes the previously set up cron job for copying the system database to a remote server via mounted (CIFS) drive.	No parameters. `maintenance backup unschedule mount`
maintenance backup unschedule scp	Removes the previously set up cron job for copying the system database to a remote server via SCP.	No parameters. `maintenance backup unscheduled scp`
maintenance cannibalize	Extract the configuration from a remote system and overwrite this system. The new system must have the same network settings as the old system, from which the database was exported. The Cloudpath uses the SSH port configured in the new system to transfer the database files.	[IP address or hostname of the remote server] `maintenance cannibalize 172.16.4.20`

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 Cloudpath 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. `replication force-cleanup`

replication replicator	Performs an operation on the replication server.	[start][stop][restart][status][offline][on line]
		`replication replicator restart`
		or
		`replication replicator status`

replication show-cluster	Displays the state of the cluster.	No parameters.

TABLE 5 replication commands (continued)

Command	Description	Parameters and Examples
		`replication show-cluster`
replication show-log	Show log.	No parameters. **`replication show-log`**

replication trepctl	Performs an operation on a service (for example alpha, bravo, charlie).	[FQDN of the server node][service name][status/online/offline]
		`replication trepctl test23.company.net alpha status`
		or
		`replication trepctl test23.company.net bravo offline`

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. **`replication validate-cluster`**

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, which allows you to log into the Cloudpath Admin UI with the **recovery** username. This command requires the **service** password. The recovery user credentials are only valid for 5 minutes.
support database login	Allows you to log into the database. The password for this command is only available to support staff.
support database reset-schema	Resets the status of the last database schema version.
support database schema-version	Lists the database schema version.
support database shrink	Depending on the size of the database, this operation may take some time to complete.
support database view-size	Displays the amount of data in the database.

TABLE 7 support commands (continued)

Command	Description
support https restore certificate	Resets HTTPS to self-signed certificate.
support https restore ciphers-and-protocols	Resets https to default SSL ciphers and protocol.
support support-tunnel enable	Start support tunnel on port 8022.
support support-tunnel disable	Stop support tunnel.
support system apply-patches	Applies patches for the current version. The system will reboot.
support system benchmark	Perform CPU and disk IO tests.
support system clean-disk	The Cloudpath runs a clean-disk script on a schedule. This command allows an administrator to clean up the `jboss.log` manually.

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.
system status	Lists the status of key services (web server, firewall, NTP, RADIUS, etc.)

Troubleshooting

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.

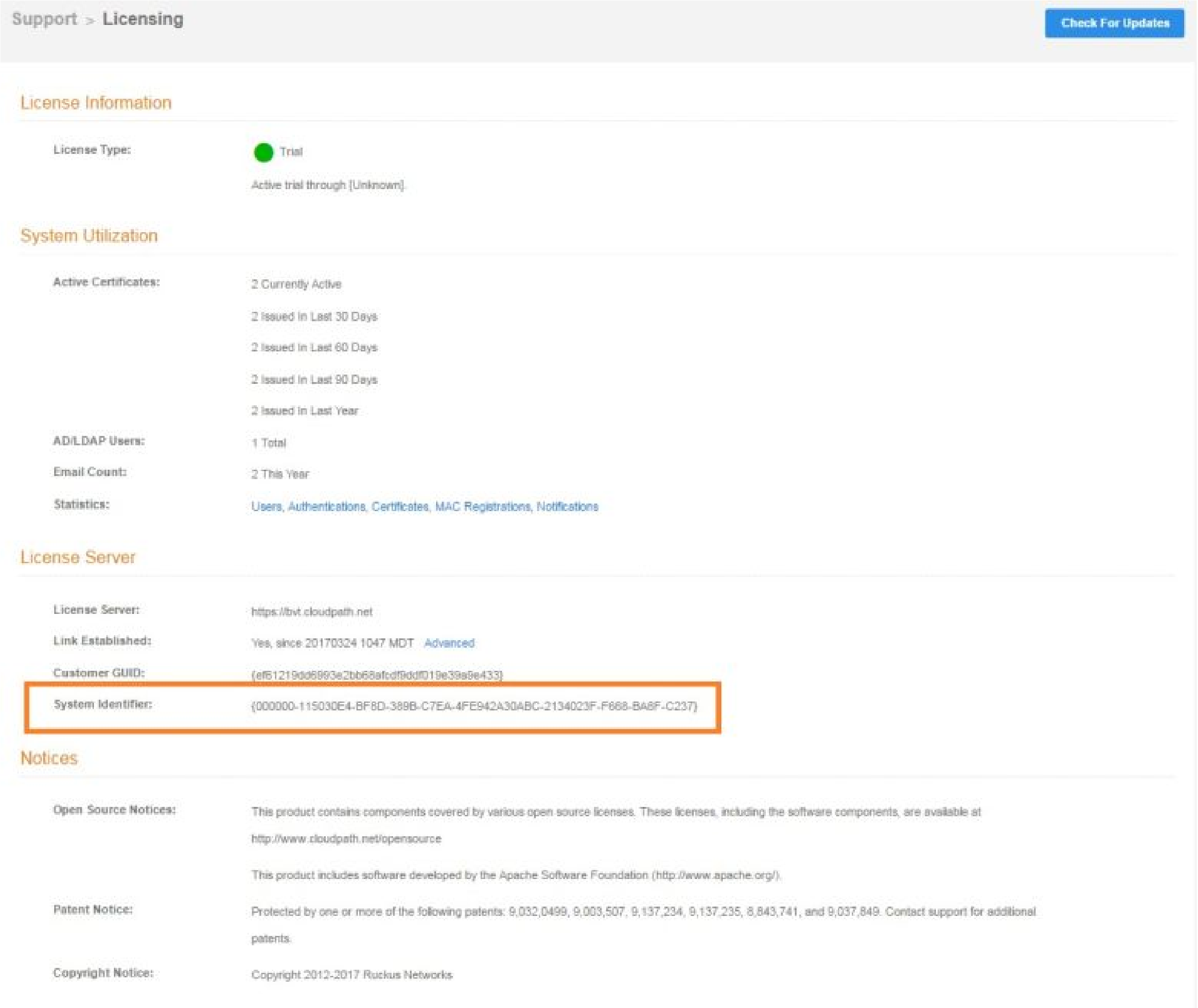
To receive a recovery password for the service account, you must provide the System Identifier and current Cloudpath version on your system.

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 15 System Identifier



Support > Licensing

License Information

License Type: ● Trial

Active trial through [Unknown].

System Utilization

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

Statistics: Users, Authentications, Certificates, MAC Registrations, Notifications

License Server

License Server: https://bvt.cloudpath.net

Link Established: Yes, since 20170324 1047 MDT Advanced

Customer GUID: {ef61219dd6993e2bb68afcdf9ddf019e39a9e433}

System Identifier: {000000-115030E4-BF8D-389B-C7EA-4FE942A30ABC-2134023F-F668-BA8F-C237}

Notices

Open Source Notices: This product contains components covered by various open source licenses. These licenses, including the software components, are available at http://www.cloudpath.net/opensource

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Patent Notice: Protected by one or more of the following patents: 9,032,0499, 9,003,507, 9,137,234, 9,137,235, 8,843,741, and 9,037,849. Contact support for additional patents.

Copyright Notice: Copyright 2012-2017 Ruckus Networks

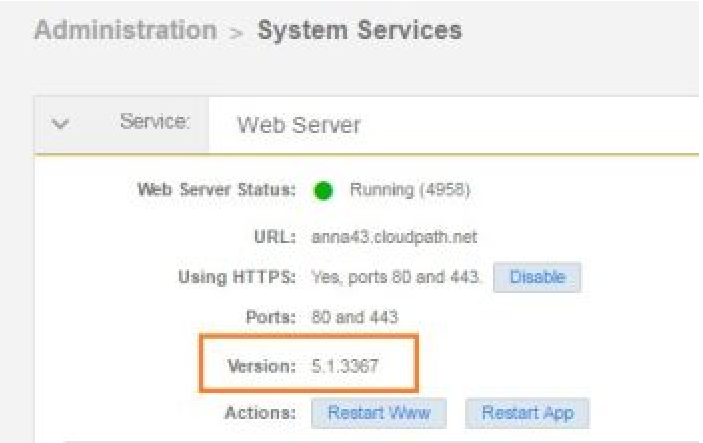
How To Find Your Current Cloudpath Version

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 16 Current Cloudpath Version System Services



Administration > System Services

Service: Web Server

Web Server Status: ● Running (4958)

URL: anna43.cloudpath.net

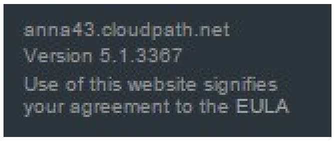
Using HTTPS: Yes, ports 80 and 443.

Ports: 80 and 443

Version: 5.1.3367

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

   FIGURE 17 Current Cloudpath Version Lower Left



anna43.cloudpath.net
Version 5.1.3367
Use of this website signifies
your agreement to the EULA

Additional Documentation

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

Copyright © 2006-2017. Ruckus Wireless, Inc.

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com