

Cloudpath Enrollment System Quick Start Guide, 5.6

Supporting Cloudpath Software Release 5.6

Copyright, Trademark and Proprietary Rights Information

© 2019 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, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex 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

Cloudpath Security and Management Platform.....	5
Overview.....	5
Cloudpath System Specifications.....	6
Prerequisites for Configuring Cloudpath.....	6
Deploying the OVA (For Local Deployments).....	6
Setting up the Initial Account.....	7
Configuring the Workflow.....	7
Deploying the Cloudpath Virtual Appliance to a VMware Server.....	9
Overview.....	9
Specifications for Locally-Deployed VMware Servers.....	9
Retrieve OVA File With Activation Link.....	9
Deploying the Virtual Appliance Using a vCenter VMware Client.....	9
Deploying the Virtual Appliance Using a VMware vCenter Client.....	10
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.....	15
Overview.....	15
Activate Account by Activation Code.....	16
Set a Password for Account.....	16
Activate Account by Credentials.....	18
Initial System Setup.....	19
Overview.....	19
System Setup Wizard.....	20
Publishing Tasks.....	29
ToDo Items.....	30
Enrollment Workflow.....	33
Overview.....	33
Workflow Basics.....	33
Modifying a Workflow Template.....	34
Creating a Workflow From a Blank Slate.....	36
Acceptable Use Policy.....	37
User Type Split.....	38
Authentication to a Traditional Authentication Server.....	39
Device Type Split.....	41
Prompt for Voucher.....	43
Device Configuration and Client Certificate.....	46
Using the Timed Access Workflow Template.....	50
Publishing the Enrollment Workflow.....	53
How to Test a Published Workflow.....	55
Administration.....	57
Administration Overview.....	57
Administrators.....	57

Company Information.....	58
System Services.....	58
System Updates.....	59
Data Cleanup.....	59
Firewall Requirements.....	59
Configuration.....	61
Overview.....	61
Device Configurations.....	61
RADIUS Server.....	61
Authentication Servers.....	63
Firewalls and Web Filter Integration.....	63
MAC Registration Lists.....	63
API Keys.....	63
Dashboard.....	65
Overview.....	65
Enrollments.....	65
Records Export.....	65
Enrollment Paths.....	66
Connections.....	67
Users & Devices.....	68
Device Types.....	68
Form Factors.....	69
MAC Registrations.....	70
Certificates.....	70
Certificates Table.....	71
Active Trends.....	71
Expiring Trends.....	71
Notifications.....	72
Notification Records.....	72
Events.....	72
Schedule Reports.....	72
Event Response.....	74
Support.....	75
Overview.....	75
Documentation.....	75
Licensing.....	75
Diagnostics.....	79
Upload Support File.....	80
Cloudpath Video Tutorials.....	81

Cloudpath Security and Management Platform

- Overview..... 5
- Cloudpath System Specifications..... 6
- Prerequisites for Configuring Cloudpath..... 6

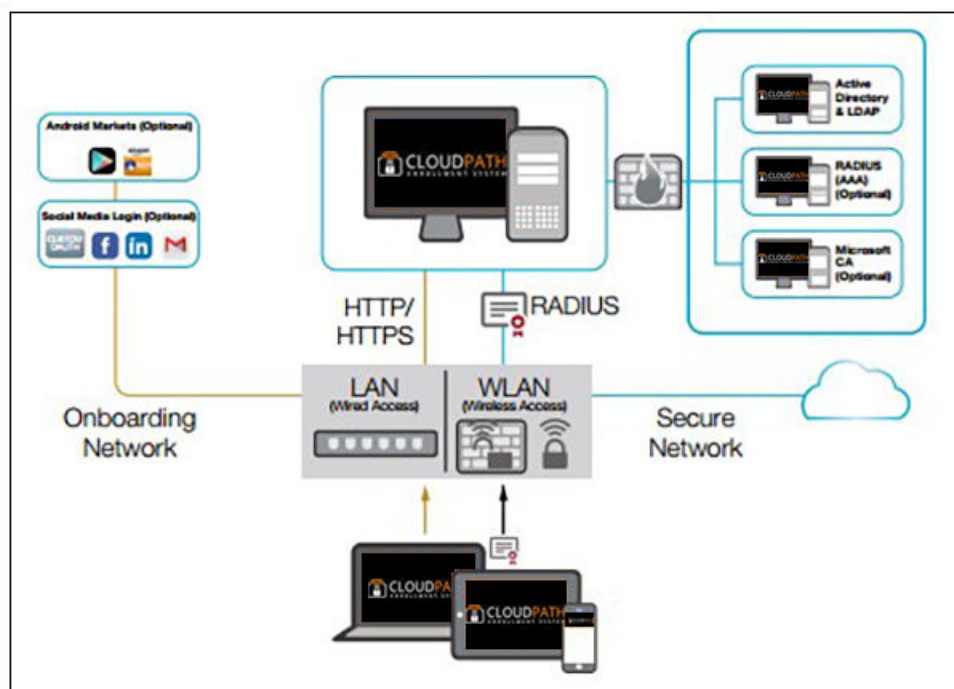
Overview

Cloudpath Enrollment System (ES) software is a security and policy management platform that enables any IT organization to protect the network by easily and definitively securing users and their wired and wireless devices—while freeing those users and IT itself from the tyranny of passwords.

Available cloud-managed or as a virtual instance and priced per user, Cloudpath software lets IT do with one system what usually requires many, while easily and automatically integrating with existing access and network security infrastructure.

Cloudpath software consolidates and simplifies the deployment of multiple services that are typically disparate and complex to manage: Certificate Management, Policy Management and Device Enablement.

FIGURE 1 Cloudpath Security and Policy Management Platform



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

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

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

Cloudpath System Specifications

Cloudpath supports the following browsers, operating systems, and third-party identity stores for system and user devices.

TABLE 1 Cloudpath System Specifications

Supported Browsers for Cloudpath Admin UI	Supported OSes for End-User Devices	Supported Third-Party Identity Stores
Internet Explorer 6.0 and later	Windows 7 and later	Microsoft Active Directory
Firefox 1.5 and later	Mac OS X 10.11 and later	LDAP
Safari 2.0 and later	Apple iOS 9.0 and later	Facebook
Google Chrome 3.0 and later	Ubuntu 15.04 and later	LinkedIn
	Android 6.0 and later	Google Gmail
	Fedora 22 and later	Custom OAuth 2.0 Server
	Chrome OS 51 and later	
	Windows Phone 8+	
	Blackberry (assisted configuration)	
	Windows RT (assisted configuration)	
	Generic (assisted configuration)	
	Windows Mobile 5 and 6 (assisted configuration)	

NOTE

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

Prerequisites for Configuring Cloudpath

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

Deploying the OVA (For Local Deployments)

- VMware server or Microsoft Hyper-V Manager on which you'll install the Cloudpath virtual appliance.
- The URL where the image file resides
- FQDN Hostname of the virtual appliance
- IP address and subnet mask for the virtual appliance (not required if using DHCP)
- Gateway IP address for your network (not required if using DHCP)
- IP address of DNS server (not required if using DHCP)
- A list of IP addresses that are allowed Administrative access (optional)
- Service account security credentials

Setting up the Initial Account

- Activation code issued from Cloudpath Licensing Server
- HTTPS server certificate
- Company Information (Domain, URL)
- DNS hostname
- Active Directory domain, DNS/IP address of AD server, and DN of AD domain or LDAP server
- Web server certificate (public-signed)

If you are not using the Cloudpath onboard CA, you also need:

- Public and Private key of existing CA
- RADIUS server certificate (if not using onboard RADIUS server)

Configuring the Workflow

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

- An idea about the types of access and policies you want to offer different users
- Images and color schemes if you plan to customize the webpage display
- AD group names for creating filters in the workflow
- An idea about the security policy for passwords, vouchers, and certificates
 - Vouchers have configurable format and validity periods
 - Certificates have configurable key lengths, algorithm types, and validity periods
- The SSID for the secure network
 - If using VLANs to apply policy, you should have the VLAN IDs

NOTE

For SSID configuration, see [Configuring Cloudpath to Integrate With a Ruckus Wireless LAN Controller](#).

- A list of conflicting SSIDs to prevent roaming (for example, open SSIDs)
- An idea about which OS families and versions to support
- Additional requirements for device configurations (for example, enable firewall, proxy, verify antivirus, enable screen lock pass code)

Deploying the Cloudpath Virtual Appliance to a VMware Server

- Overview..... 9
- Deploying the Virtual Appliance Using a vCenter VMware Client..... 9
- Deploying the Virtual Appliance Using a VMware vCenter Client..... 10
- Deploying the Virtual Appliance Using a Console-Based VMware Client..... 14

Overview

Cloudpath supports deployments using a VMware server or Hyper-V Manager. This section describes deploying to a VMware server. For Hyper-V deployments, see the configuration document, *Deploying Cloudpath as a Virtual Appliance using Microsoft Hyper-V*.

NOTE

If you are setting up a hosted system, you can skip this section and continue to [Initial System Setup](#) on page 19.

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

Specifications for Locally-Deployed VMware Servers

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 an 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 vCenter VMware Client](#) section for details.

Retrieve OVA File With Activation Link

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.

Deploying the Virtual Appliance Using a vCenter VMware Client

The deployment process consists of the following steps:

- [Deploying the Virtual Appliance Using a vCenter VMware Client](#)

or

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

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 VMware Client* to complete the deployment process.

Application Properties (vCenter)

Customize the application properties for the deployment.

FIGURE 2 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.

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.

NTP Server

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

Enable HTTPS?

Timezone

SSH Access

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

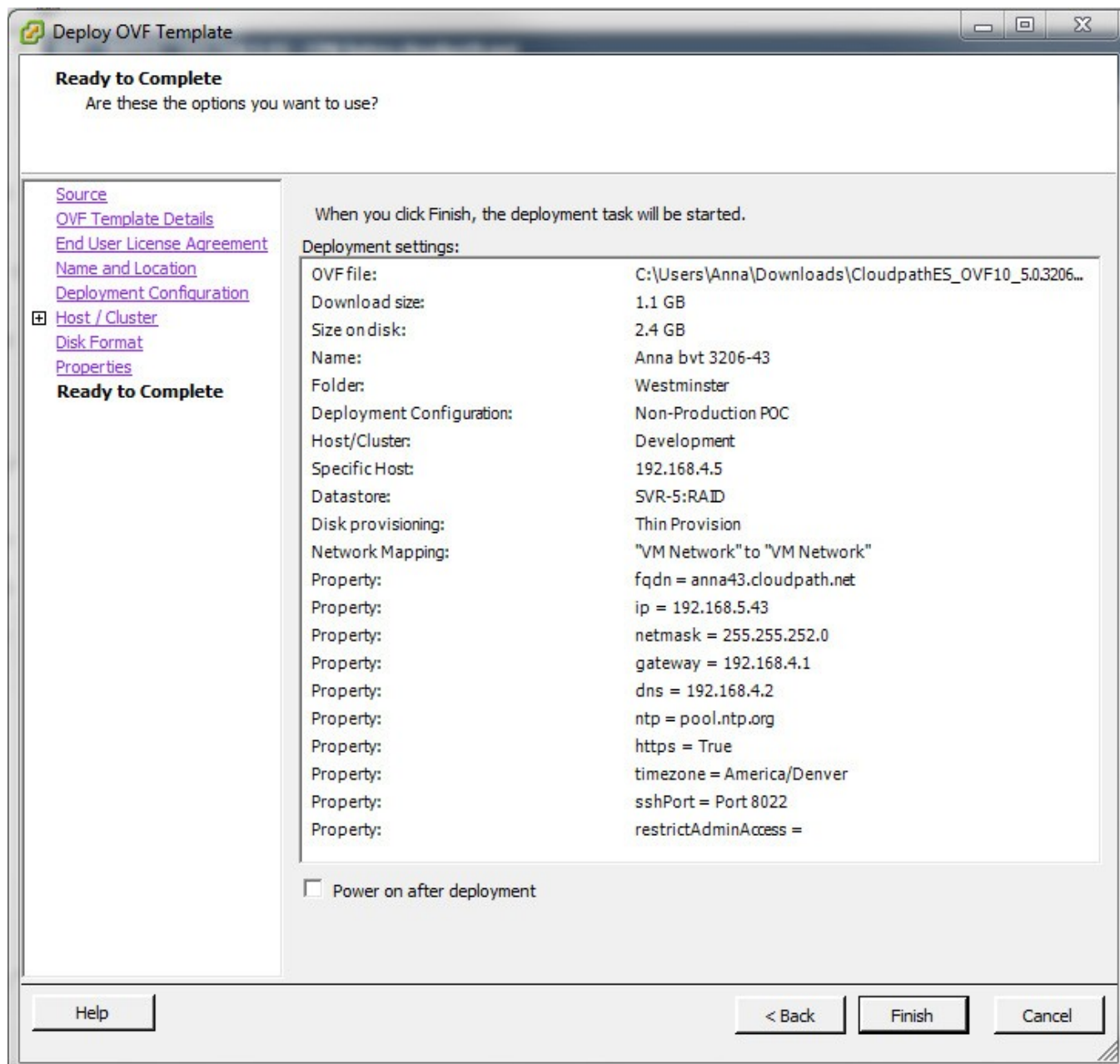
The Cloudpath Hostname is used as the default OCSP Hostname, which is embedded into certificates issued by the onboard root CA as part of the URL for the Online Certificate Status Protocol (OCSP).

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** 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 3 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 (for example, **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 interface (ens for VMware, eth0 for Hyper-V), 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 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 **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 **no** (default) or **y** to specify an NTP server. The setup is complete. Press **Enter** to reboot the system. After the reboot you are presented with the shelluser login prompt.

NOTE

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

Service Account

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

1. Enter **cpn_service** at the login prompt, and then the service user password.
2. Enter the **show config** command to verify your configuration. You may be prompted to re-enter the password. See the *Cloudpath Command Reference* on the left menu **Support** tab.

Activate Account or Log In

- Overview..... 15
- Activate Account by Activation Code..... 16
- Set a Password for Account..... 16
- Activate Account by Credentials..... 18

Overview

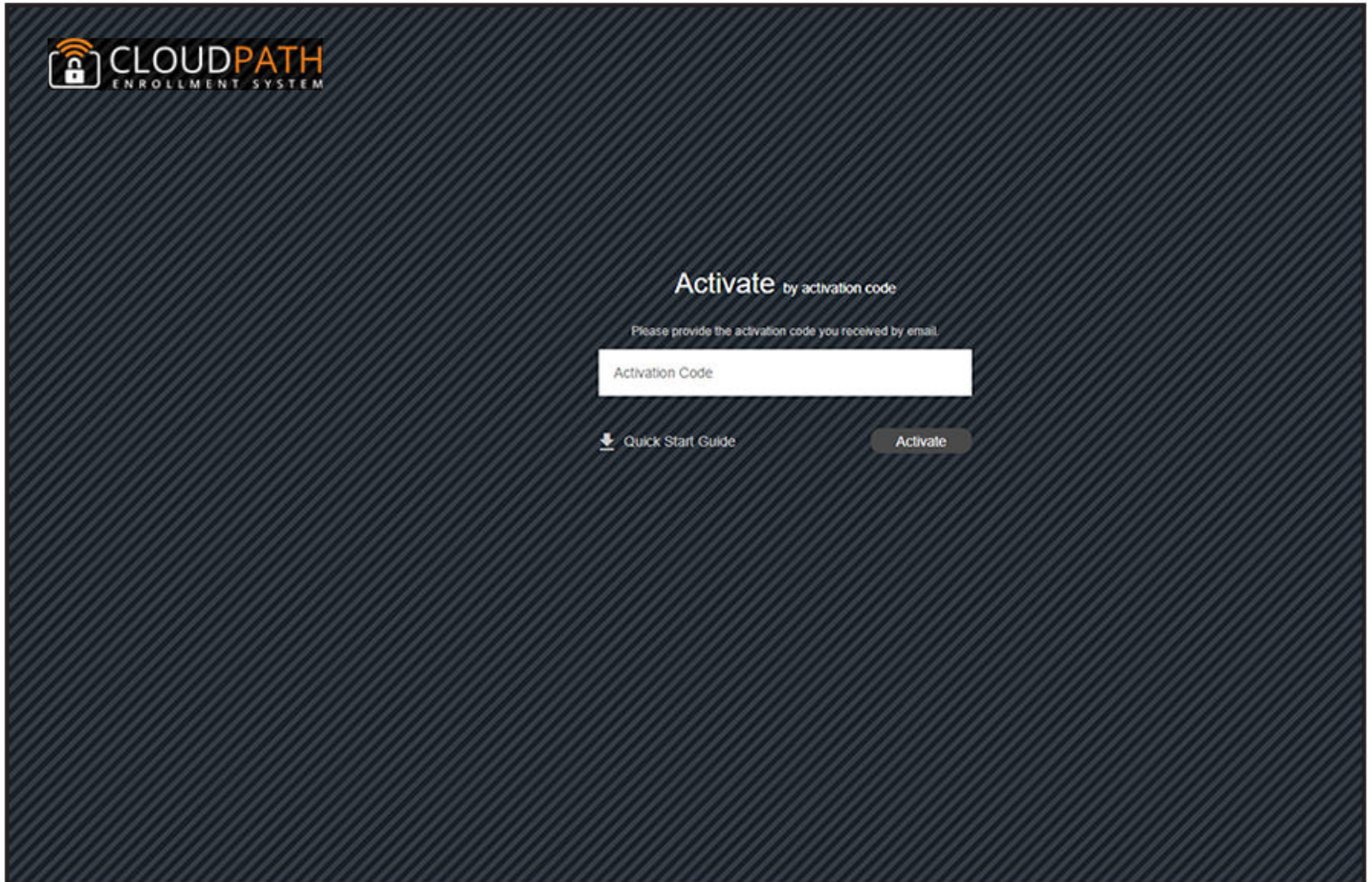
If you are setting up a Cloudpath account for the first time, you will be sent an activation code. If you have existing Cloudpath License server credentials, you can activate an account using those credentials.

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.

Activate Account by Activation Code

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

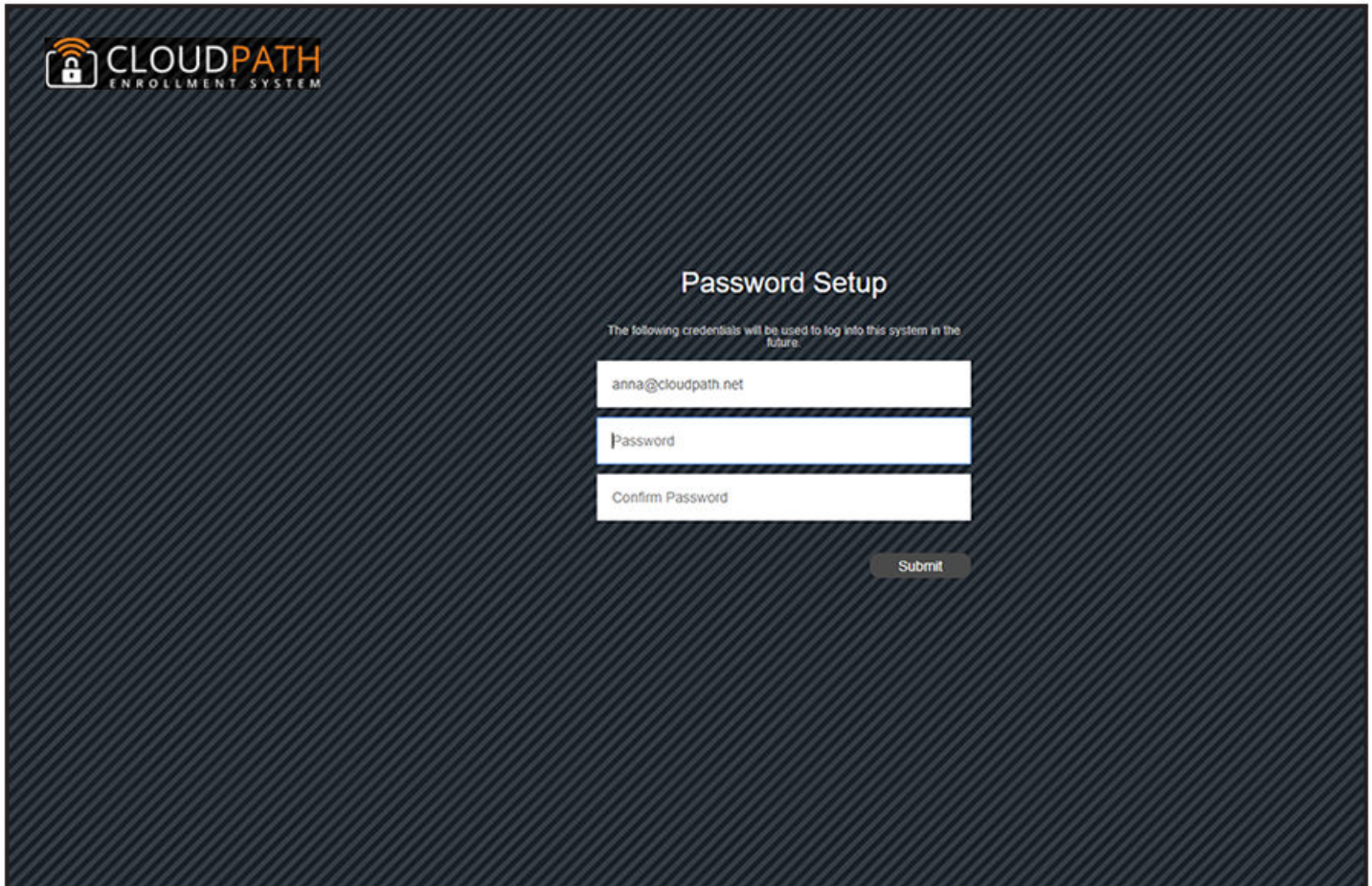
FIGURE 4 Activate Cloudpath Account



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 5 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', which includes a padlock icon. The main heading is 'Password Setup'. Below the heading, a message states: 'The following credentials will be used to log into this system in the future.' There are three input fields: the first contains the email address 'anna@cloudpath.net', the second is labeled 'Password', and the third is labeled 'Confirm Password'. A 'Submit' button is located below the input fields.

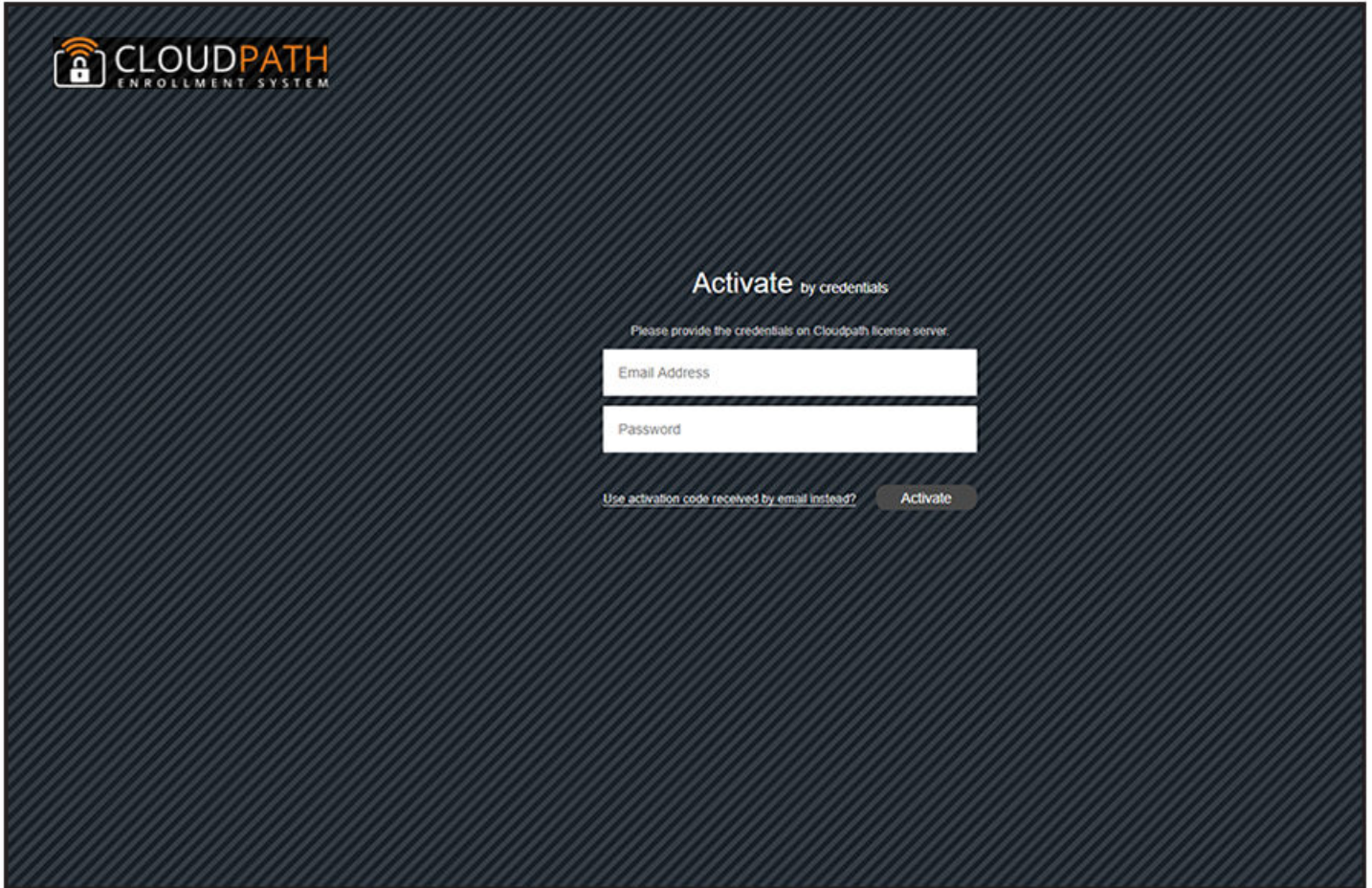
1. Your email address should display. If it does not, enter it on this page.
2. Enter and confirm a password.

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 6 Activate Account With Existing Credentials



Initial System Setup

- Overview..... 19
- System Setup Wizard..... 20
- Publishing Tasks.....29
- ToDo Items..... 30

Overview

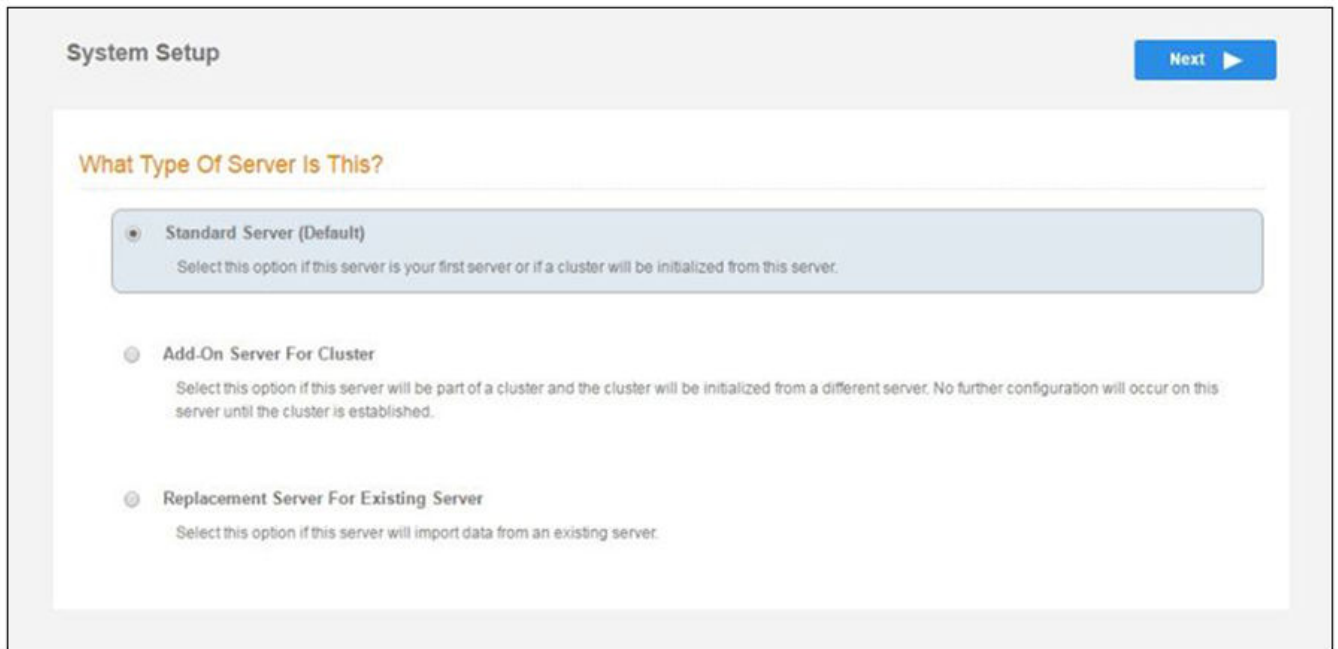
Cloudpath provides you with a single administrator login for the Cloudpath Admin UI. Additional administrators can be added from the left menu Administration tab, or you can enable Administrator logins from your authentication servers.

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 7 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 8 Company Information

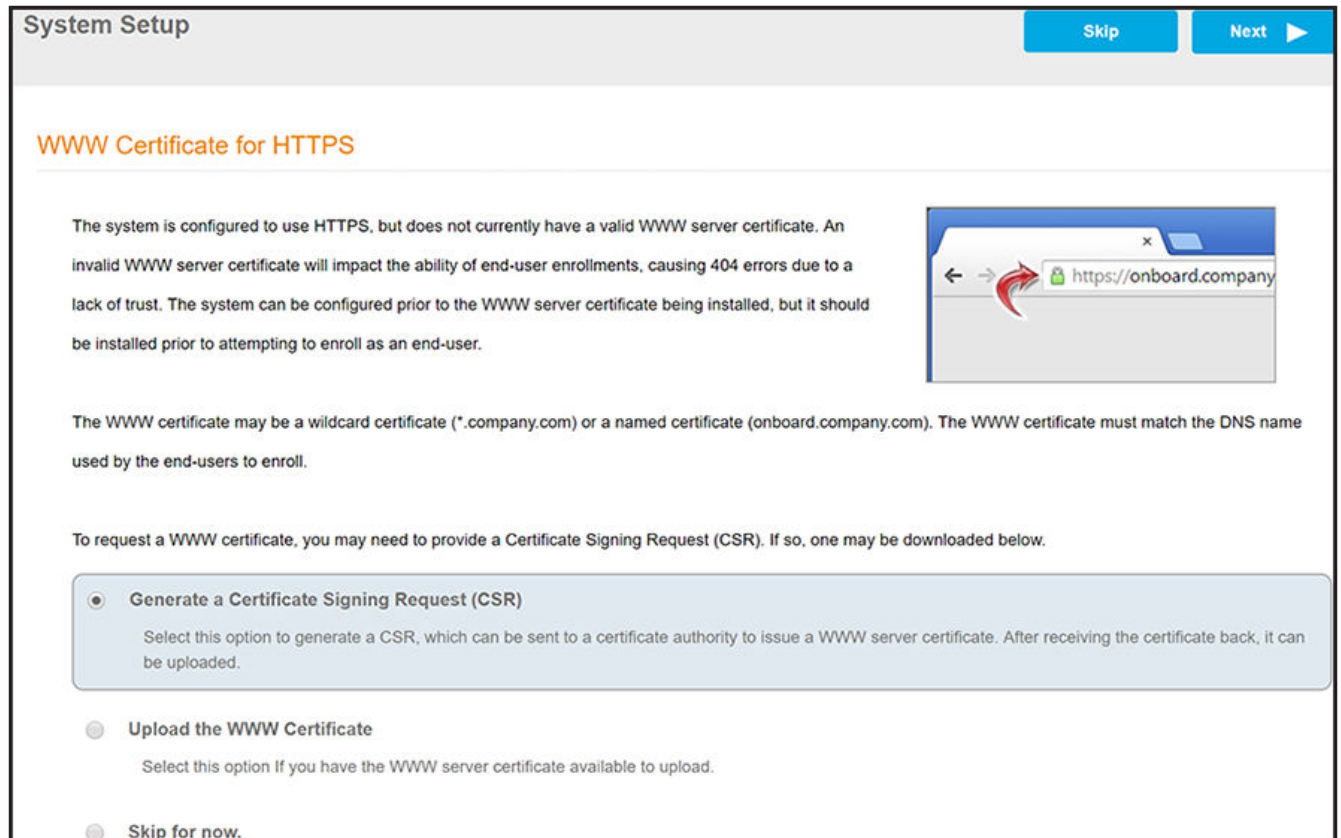
The screenshot shows a 'System Setup' window with a 'Next' button in the top right corner. The main content area is divided into two sections: 'Company Information' and 'Company Web Presence'. Each section contains several input fields with a small information icon (i) to the left of the label. The 'Company 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

Sample Data

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

FIGURE 9 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 10 Create CSR for HTTPS Screen

- a) Enter the required information.

NOTE

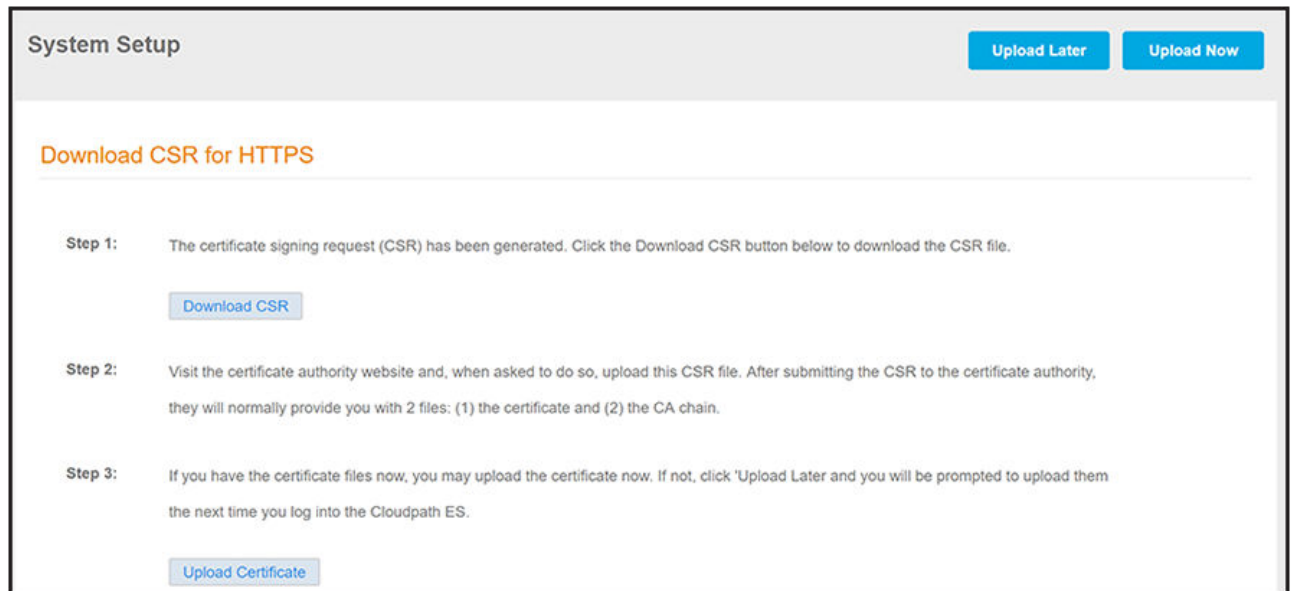
In the Common Name field:

- 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 11 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 11](#), 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 12 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 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, 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:

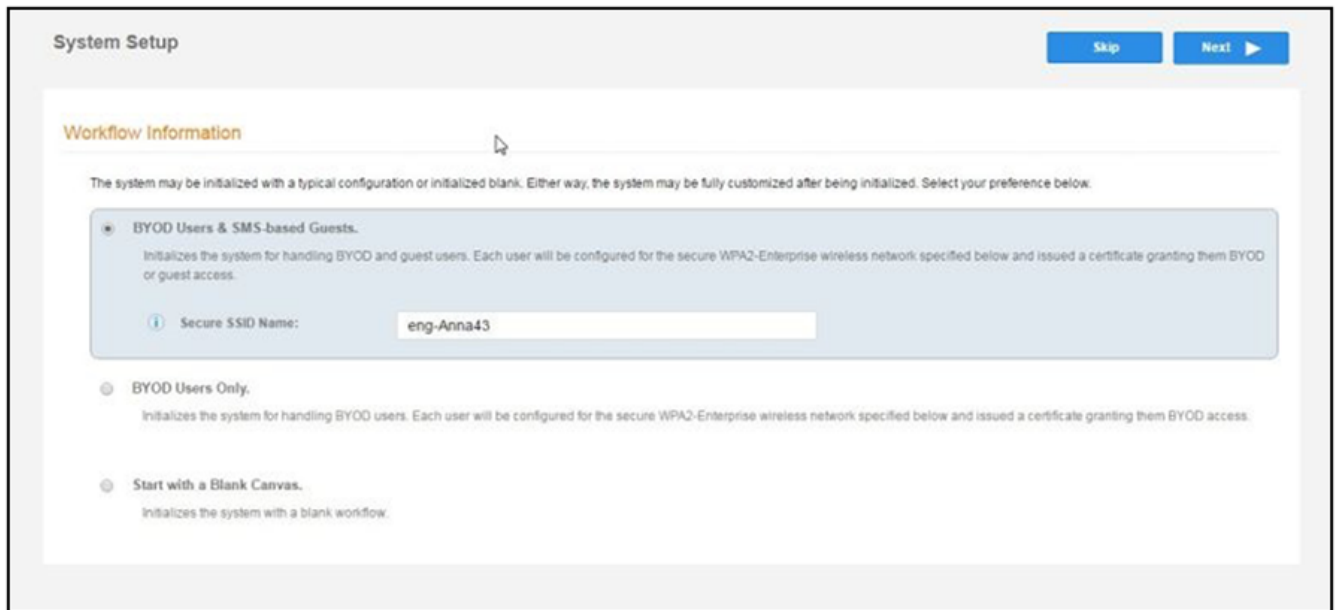
FIGURE 13 Upload Existing WWW Certificate

The screenshot shows the 'System Setup' wizard interface. At the top right, there are 'Back' and 'Next' 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 fields: 'Public Key (PEM):', 'Chain (PEM or P7b):', 'Additional Chain (Optional):', 'Additional Chain (Optional):', 'Private Key (PEM):', and 'Private Key Password:'. 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. There is also a 'Prompt for Password on Boot:' checkbox which is unchecked. 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 14 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 15 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.

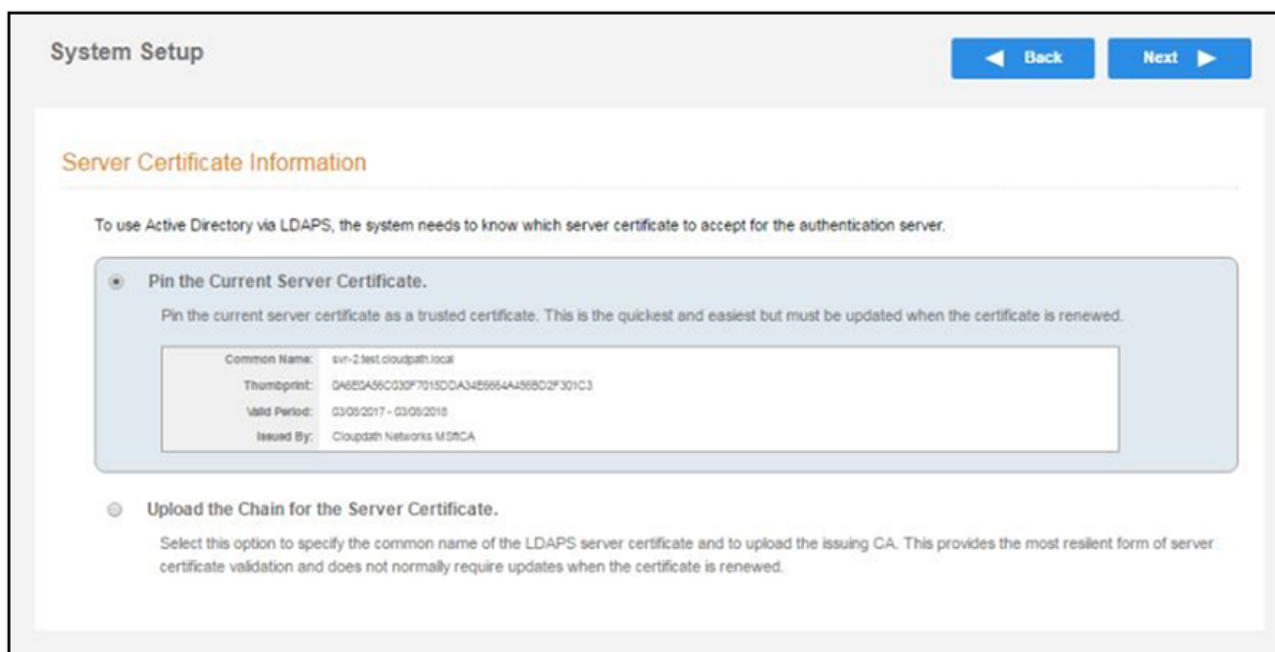
Connect to SAML
Select this option to enable end-users to authenticate via a SAML 2.0 IdP.

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 16 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 17 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:	nhu0vjwqedwopth7vaw
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 18 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.

Enrollment Workflow

- Overview..... 33
- Workflow Basics..... 33
- Modifying a Workflow Template..... 34
- Creating a Workflow From a Blank Slate..... 36
- Using the Timed Access Workflow Template..... 50
- Publishing the Enrollment Workflow..... 53
- How to Test a Published Workflow..... 55

Overview

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

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

See Enrollment Workflow Use Cases for an example of the most commonly used workflows.

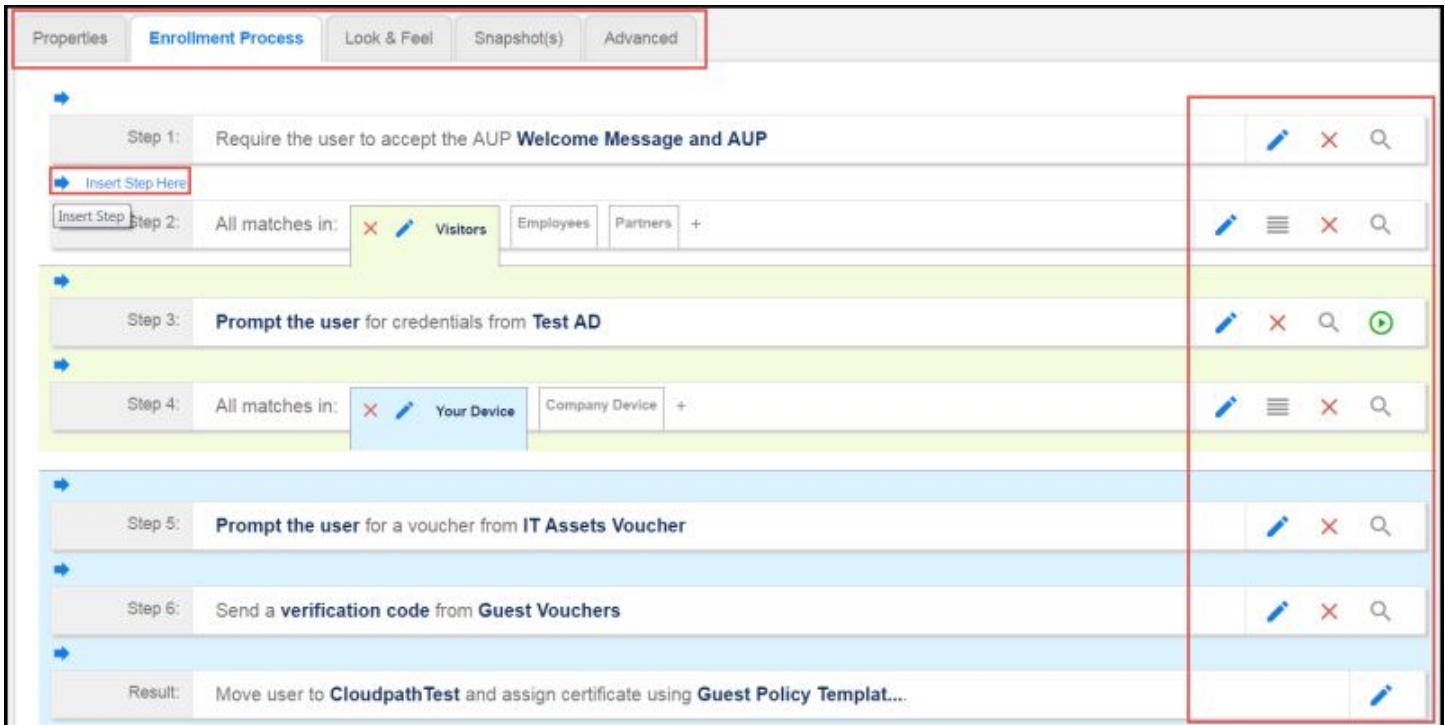
Workflow Basics

Navigate to **Configuration > Workflows**.



The **Workflow** page has 5 tabs across the top.

- Use the **Properties** tab to update the workflow properties and the **Enrollment Portal URL Options**.
- Use the **Enrollment Process** tab to configure the steps presented to a user to create the workflow.
- Use the **Look & Feel** tab to configure the Cloudpath skin, and to customize the logos, colors, buttons, and images for the Cloudpath server, the Cloudpath Wizard, and the Download page.
- Use the **Snapshot(s)** tab to view the latest snapshot, the version, timestamp and the notes added to a particular workflow.
- Use the **Advanced** tab to view the **Enrollment Portal URL**, **Passpoint OSU URL**, and the **QR code**. You can also use it to **Manage Chromebook Setup and for Cleanup**.

FIGURE 19 Workflow Configuration Page



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

- Use the icons on the right side of each step to edit, modify, delete, view the enrollment steps.
- Use the **Test Server** icon  to verify interaction with an authentication server.
- Use the **Edit List** icon  to label options, to change the order of the selection options in a split, add more options, or add filters and restrictions.
- Use the icons on the split tabs to modify or delete a specific option.

When you create a new workflow, you will choose one of three options from a drop-down list called Workflow Template Type. These options are described in detail in the following sections:

- [Modifying a Workflow Template](#) on page 34
- [Creating a Workflow From a Blank Slate](#) on page 36
- [Using the Timed Access Workflow Template](#) on page 50

Modifying a Workflow Template

You can modify a standard enrollment workflow template provided by Cloudpath.

To create a workflow from a template using sample data:

1. Go to **Configuration > Workflows**.

2. On the right hand side of the **Workflow** page select **Add Workflow**.

The Create Workflow screen is displayed:

FIGURE 20 Create Workflow Screen - Selecting "BYOD and SMS Guest" For Workflow Template Type

Configuration > Workflows > Create

Cancel Save

Create Workflow

Display Name: [ex. Production]

Description:

Workflow Template Type: BYOD and SMS Guest

Enrollment Portal URL Options

URL Name:

None

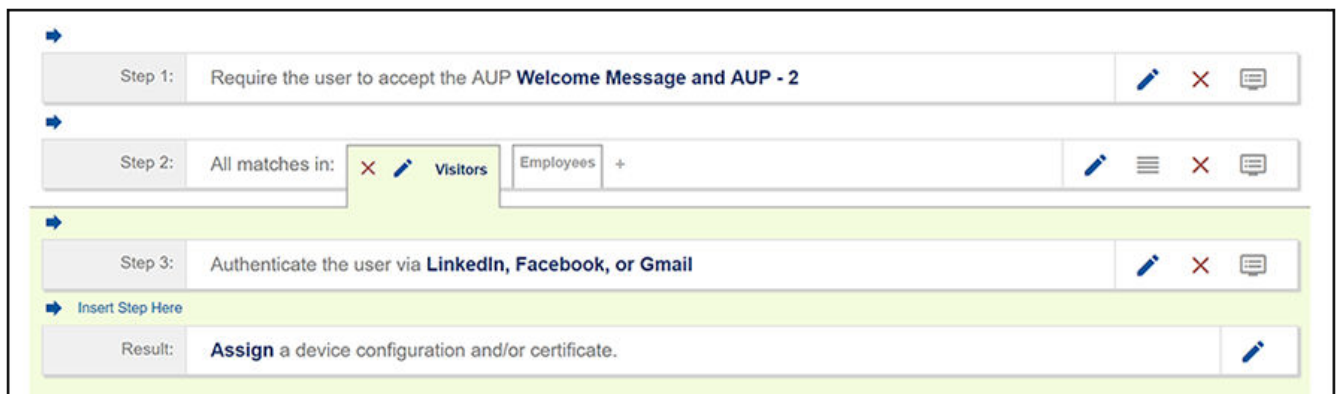
BYOD and SMS Guest

Timed Access

3. On the **Create Workflow** screen, enter a **Display Name** and **Description**.
4. From the Workflow Template Type drop-down list, select "BYOD and SMS Guest."
5. Fill out the URL Name field.
6. Click **Save**.

A workflow template, which contains a typical workflow sequence, is displayed. The step numbers are shown on the left side of the workflow.

FIGURE 21 Workflow Template



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

The workflow template contains basic workflow steps with sample data that can be modified to fit your network plan. These basic steps are described in the following table.

TABLE 2 Example Workflow Template Steps

Step 1	Acceptable Use Policy.
Step 2	Split in the workflow to provide a different sequence of enrollment steps for Visitors and Employees. Splits can be modified for other industries (for example, Students, Faculty, and Guests).
Step 3	An authentication step for users.
Result	The final step, which migrates the user to the secure network and assigns a client certificate, is not pre-populated as this information is specific to your network.

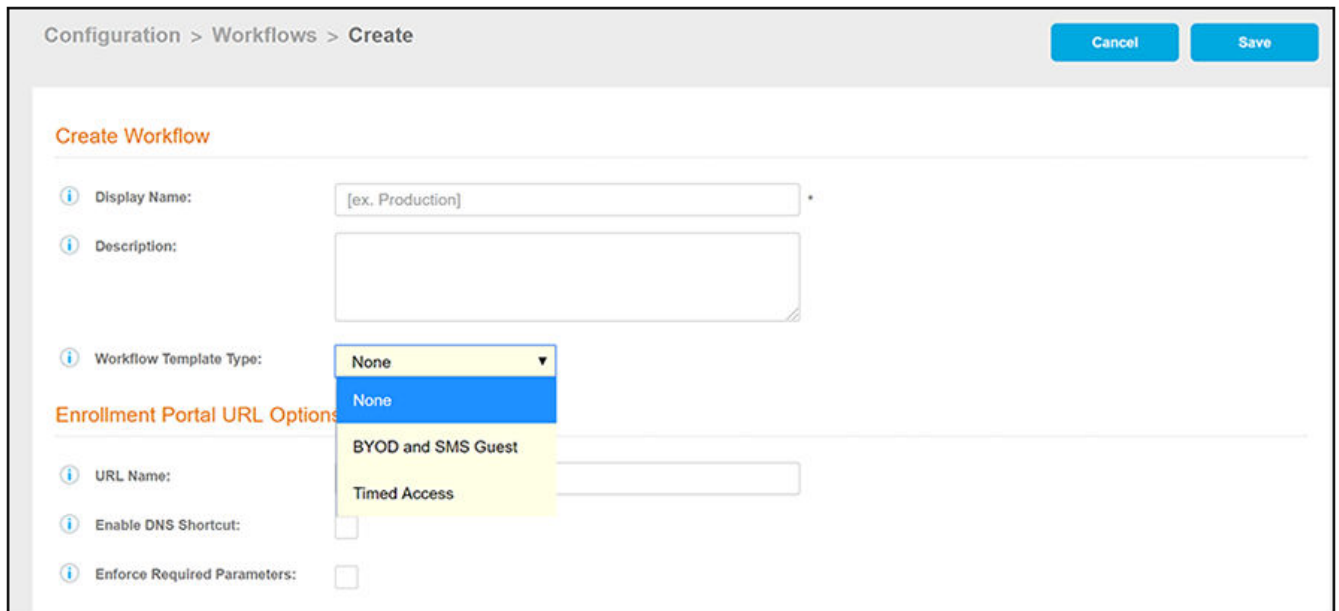
Creating a Workflow From a Blank Slate

You can create a typical workflow from a blank slate. This sample workflow follows the steps provided in the workflow template.

1. Go to **Configuration > Workflows**.
2. On the right hand side of the **Workflow** page select **Add Workflow**.

The Create Workflow screen is displayed:

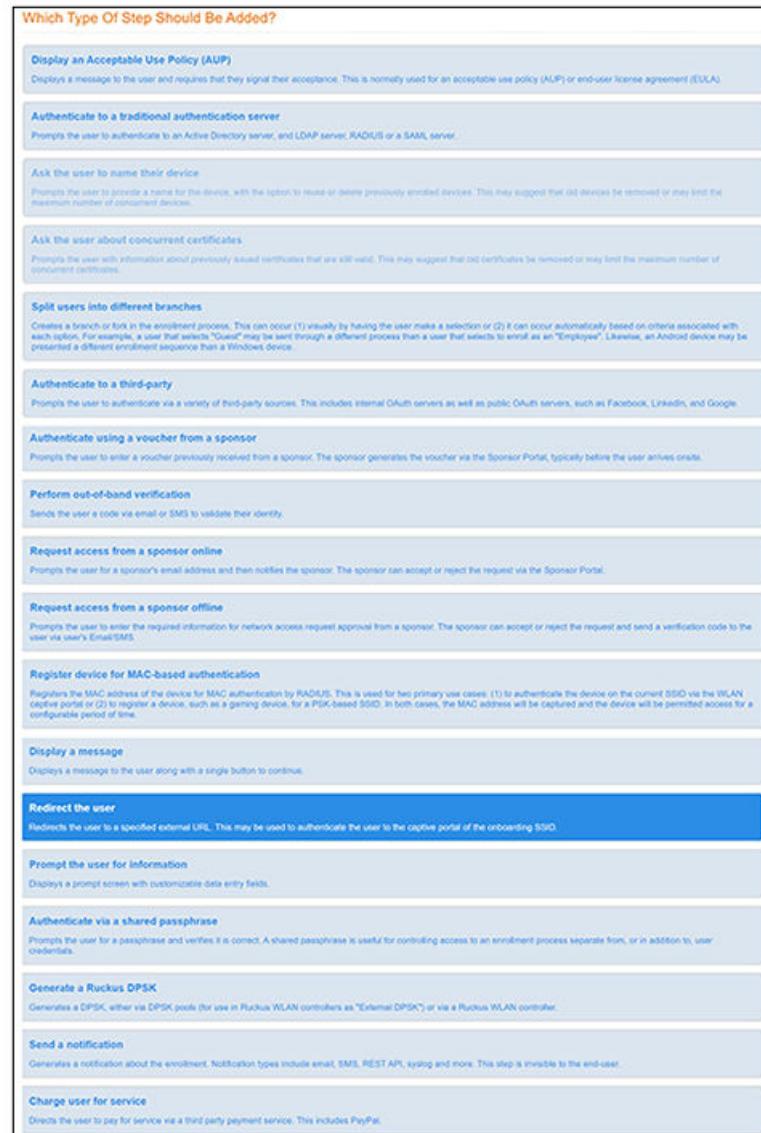
FIGURE 22 Create Workflow Screen - Selecting "None" For Workflow Template Type



3. On the **Create Workflow** screen, enter a **Display Name** and **Description**.
4. From the Workflow Template Type drop-down list, select "None."
5. Fill out the URL Name field.
6. Click **Save**, and you are returned to a blank workflow page.

- On the blank workflow page, click **Get Started** near the bottom of the page to add your first workflow step. A selection page opens that allows you to choose which type of step (workflow plug-in) to add to the enrollment workflow. Every time you add a step, the **Step Selection** page appears.

FIGURE 23 Enrollment Step Selection



Acceptable Use Policy

Step 1 in the workflow requires the user to agree to an Acceptable Use Policy (AUP).

- Select the button for **Display an Acceptable Use Policy (AUP)**.
- Select **A new AUP created from a standard template**.

3. On the **Add Acceptable Use Policy** page, enter the **Reference Information** and **Webpage Display Information**. The **Webpage Display Information** is the what the user sees during the enrollment process.

FIGURE 24 Add Acceptable Use Policy

4. Choose **Standard Template** as the page source and check the **Checkbox Default State** box to specify that the default setting is the acceptance of the AUP. Click **Save**.

The Workflow page displays the enrollment workflow with the AUP acceptance as the first step.

User Type Split

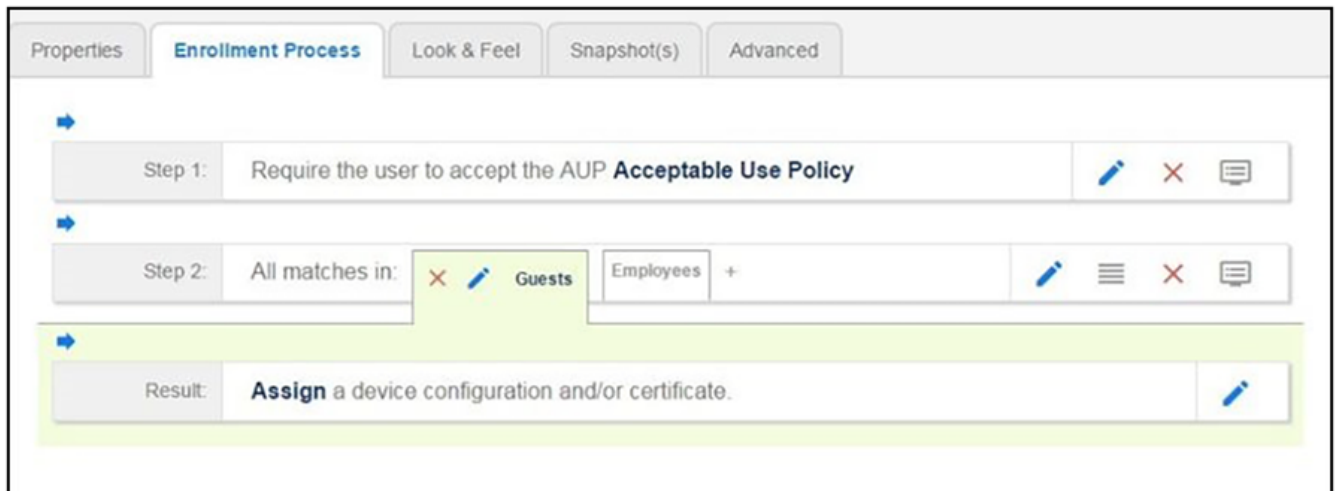
Step 2 in the workflow prompts for the type of user access.

To create a **User Type** prompt:

1. **Insert** a step above the **Result:** step in the enrollment workflow.
2. Select **Split users into different processes**.
3. Select **Use an existing split** and choose **User Type** (a pre-existing split). The **User Type** split creates a prompt to select either the **Employee** User Type or the **Visitor** User Type. These labels can be modified.

The Workflow page displays the enrollment workflow with the **User Type** option after the **AUP step**.

FIGURE 25 Workflow with User Type Split



Authentication to a Traditional Authentication Server

Step 3 in the workflow authenticates a user against a Corporate AD server.

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

1. Select the **Employee** tab in Step 2 of the example enrollment workflow.
2. **Insert** a step above the **Result:** step in the enrollment workflow.
3. Select **Authenticate to a traditional authentication server**.

4. Select **Define a new authentication server**. The **Add Authentication Server** page opens.

FIGURE 26 Add Authentication Server

The screenshot shows the 'Authentication Server Configuration' page. The 'Connect to Active Directory' section is selected and contains the following fields: 'Default AD Domain' with the value '[ex. test.sample.local]', 'AD Host' with '[ex. ldaps://192.168.4.2]', 'AD DN' with '[ex. dc=test,dc=sample,dc=local]', and 'AD Username Attribute' set to 'SAM Account Name'. Below this are sections for 'Verify Account Status On Each Authentication' (with a 'Perform Status Check' checkbox), 'Additional Logins' (with 'Use For Admin Logins' and 'Use For Sponsor Logins' checkboxes, the latter checked), 'Test Authentication' (with a 'Run Authentication Test?' checkbox), and 'VLAN Configuration' (with a 'Use VLAN Range' checkbox). At the bottom, there are radio buttons for 'Connect to LDAP', 'Connect to RADIUS', 'Connect to SAML', and 'Use Onboard Database', with 'Connect to Active Directory' being the selected option.

5. Enter the **Reference** and **Active Directory Information** .
6. (Optional) To test connectivity to the authentication server, select the **Run Authentication Test** box, and enter a Test **Username** and **Password**.
7. (Optional) To allow users from a specific group to log in to the Cloudpath Admin UI as administrators, check the **Use for Login Admin** box and enter the **Admin Group Regex** for the authentication server group.
8. Click **Next**.
9. Select **Use a new webpage created from a standard template**.

The **Create Credential Prompt** page opens.

Device Type Split

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

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

NOTE


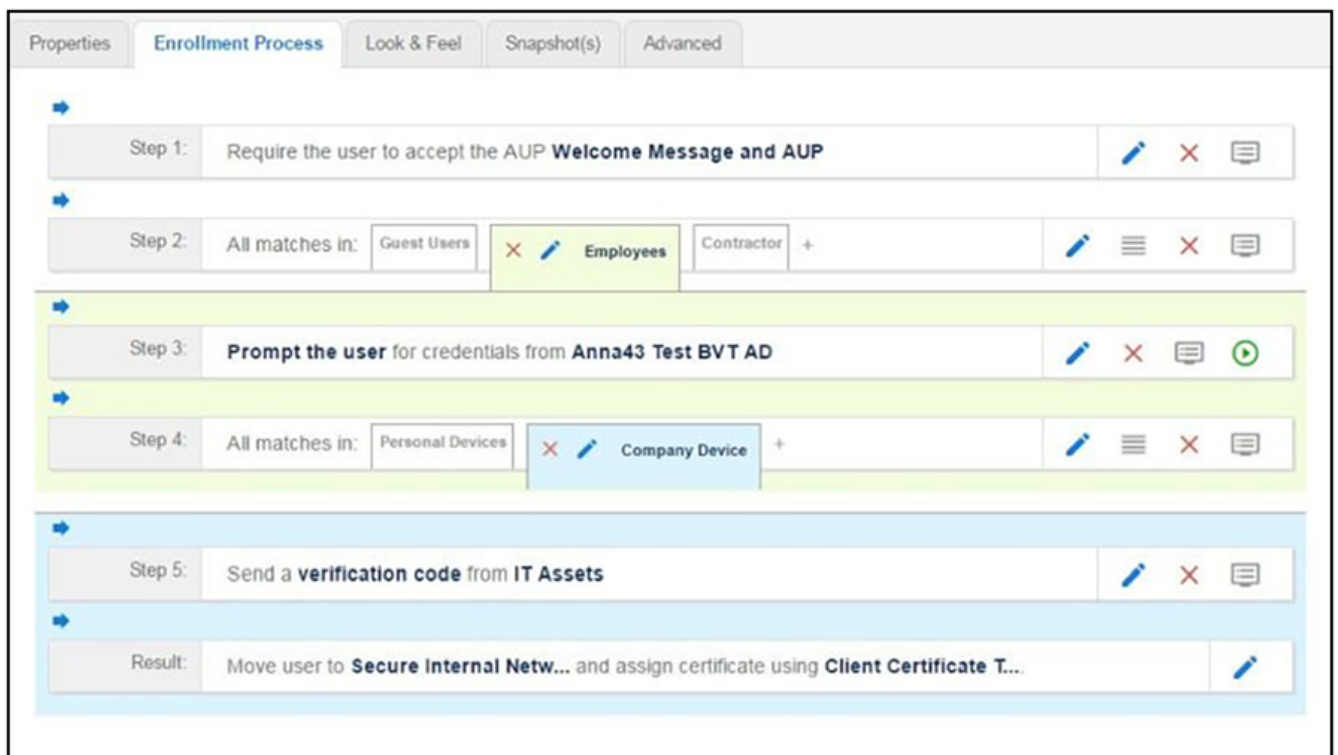
Use the **Edit List** icon  to customize the split option labels. The Workflow page displays your enrollment workflow with the Device Ownership option after the user authentication step.

FIGURE 27 Workflow with Device Ownership Split



Create a Filter in the Device Type Split

When creating splits in the workflow, you can set up a filter so that only certain users see this enrollment step.

For example, create a filter in the Device Type split that allows only users in a specified Active Directory group (ex. **BYOD App**) to receive the option for personal devices. Users that are not in the **BYOD App** AD group do not have the option to enroll personal devices and do not receive the **Device Type** prompt during enrollment.

1. On the **Enrollment Workflow** page, locate the step with the **Device Type** prompt. In this example, it is Step 4.

2. On the right side of the step, click the **Edit List** icon to open the **Selection Options** page and edit the **Your Device** option. This opens the **Modify Step** page, which allows you set up filters for this split in the workflow.

FIGURE 28 Modify Step - Filters and Restrictions

The screenshot shows the 'Filters & Restrictions' configuration page. At the top, there is a title 'Filters & Restrictions' with a dropdown arrow. Below the title is a paragraph: 'The following settings control which users will have access to this option. If nothing is specified below, all users will have access to this option. If criteria is specified below, only users meeting the criteria will have access to this option.'

The page is organized into several sections:

- User-Based Filters:** Contains four rows, each with a label, a 'Matches' dropdown, and a text input field.
 - Group Name Pattern: [Matches] [ex. BYOD]
 - Username Pattern: [Matches] [ex. bob]
 - User DN Pattern: [Matches] [ex. *ou=IT,*]
 - Email Pattern: [Matches] [ex. *@company.com\$]
- Device-Based Filters:** Contains four rows, each with a label, a 'Matches' dropdown, and a text input field.
 - Operating System Pattern: [Matches] [ex. *Android.*]
 - User-Agent Pattern: [Matches] [ex. *Safari*]
 - Language Pattern: [Matches] [ex. *en,*]
 - MAC Registration List: [Matches] [ex. IT-Owned MACs]
- Location-Based Filters:** Contains three rows.
 - Location Pattern: [Matches] [ex. EMEA]
 - Allowed IPs: [ex. 192.168.4.1/24]
 - Blocked IPs: [ex. 192.168.4.1/24]
- Filters Based On Web Authentication Certificate:** Contains four rows.
 - Common Name Pattern: [Matches] [ex. bob@company.com]
 - Issuer Pattern: [Matches] [ex. Sample Root CA I]
 - Template Pattern: [Matches] [ex. BYOD Template]
 - Expiration Date: Expires Within [0] [Days]
- Other Filters:** Contains one row: Voucher List Name: [Matches] [ex. Long-Term Voucher List]

3. In the **Filters & Restrictions** section, in **User-based Filters**, enter a regex to matches the **BOYD APP** in the **Group Name Pattern** field. Cloudpath also supports Device-based, Location-based, Web authentication, and Voucher List filters.

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

NOTE

To see a list of available group names, return to the workflow and run a test on the Authentication Server. The test results show all of the different username patterns for the user.

Prompt for Voucher

Step 5 adds a voucher verification step for authenticated employees with IT-assets. To create this authorization prompt:

1. Select the **Employees** tab in Step 2 and the **Company Device** tab in Step 4 of the workflow.
2. **Insert** a step above the **Result:** step in the enrollment workflow.

3. Select **Authenticate using a voucher from a sponsor** and **Create a new Voucher list**.

FIGURE 29 Create Voucher List - Format and Notification Fields

Configuration > Workflows > Insert Step

Cancel Back Next

Create Voucher List

Display Name: Voucher List

Description:

API ID: 0c91a1-c8d4105d-a38a-4d9a-8f2f-a6cdf703cdf8

Format

Length: 4

Characters: alphanumeric (Lowercase)

Default Validity Length: 7

Default Reuse Count: Once (One-Time-Password)

Default Days of Access: 0

Maximum Days of Access: 7

Require Username Match:

Notification

Email Subject: Network Access

Email Body: The following voucher code is required to access the network.

Voucher Code: \${VOUCHER}

SMS Subject: Network Access

SMS Body: The following voucher code is required to access the network.
Voucher Code: \${VOUCHER}

4. On the **Create Voucher List** page, enter the voucher specifications for the Employees with Company Devices workflow.
 - **Format** - Describes voucher characteristics and validity.
 - **Notification** - Set up the template for emailing the voucher or sending as an SMS message.
 - **Sponsorship** - Use this section to configure the Sponsored Guest Access feature.
 - **Initial vouchers** - Create one or more initial vouchers.

FIGURE 30 Create Voucher List - Sponsorship, Fields Displayed, and Initial Vouchers

Sponsorship

- ① Allow by LDAP Group:
- ① Allow by LDAP Username:
- ① Allow by LDAP Username DN:
- ① Maximum Certificates:
- ① Default Permissions:
 - Add/Edit/Delete Sponsors In Group
 - Manage Devices Enrolled By Sponsor
 - Manage Devices Enrolled By All
 - Allow Creation by CSV Upload
 - Allow Bulk Creation
- ① New Sponsor Email Subject:
- ① New Sponsor Email Template:

```
You have been setup as a sponsor. To login as a sponsor, use the information below:  
<br/><br/>URL: ${URL}  
<br/>Username: ${EMAIL}<br/>Password: ${PASSWORD}<br/><br/>On your first login, you will be
```

Fields Displayed To Sponsor

- ① Name Field:
- ① Company Field:
- ① Email Field:
- ① SMS Field:
- ① Reason Field:
- ① Redeem By Field:
- ① Reuse Count Field:
- ① Days of Access Field:

Initial vouchers

- ① Initial Voucher #1:
- ① Initial Voucher #2:
- ① Initial Voucher #3:
- ① Initial Voucher #4:
- ① Initial Voucher #5:

5. For the voucher prompt, select **Create a new webpage from a standard template**.
6. On the **Create Voucher Prompt** page, enter the data for the voucher prompt and **Save**.

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

Device Configuration and Client Certificate

A device configuration is a group of settings containing a single configuration per operating system. This configuration determines the settings and behavior required to move the device from the onboarding SSID to the secure network.

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

Device Configuration

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

FIGURE 31 Configure SSID

Connection Type

Select the connection method(s) this device configuration supports:

The screenshot shows a configuration interface for connection types. At the top, it says "Select the connection method(s) this device configuration supports:". Below this, there are two main sections: "Wireless Connections" and "Wired 802.1X Connections". The "Wireless Connections" section is selected with a radio button. It contains three rows of settings, each with an information icon (i) on the left and a control on the right: "SSID:" with a text input field containing "TestSSID"; "Authentication Style:" with a dropdown menu showing "Client Certificate [Recommended]"; and "Is this SSID Broadcast?" with a dropdown menu showing "Yes, the SSID is broadcast.". The "Wired 802.1X Connections" section is unselected.

5. Set the **Authentication Style**:
 - Select **Client Certificate** for TLS network configurations
 - Select **PEAP** for PEAP/MS-CHAPv2 network configurations
 - Select **Static Pre-Shared Key** for PSK network configurations
 - Select **Ruckus DPSK** for a Dynamic Pre-Shared Key network configuration on a Ruckus controller
6. Leave the default **Broadcast** setting and click **Next**.

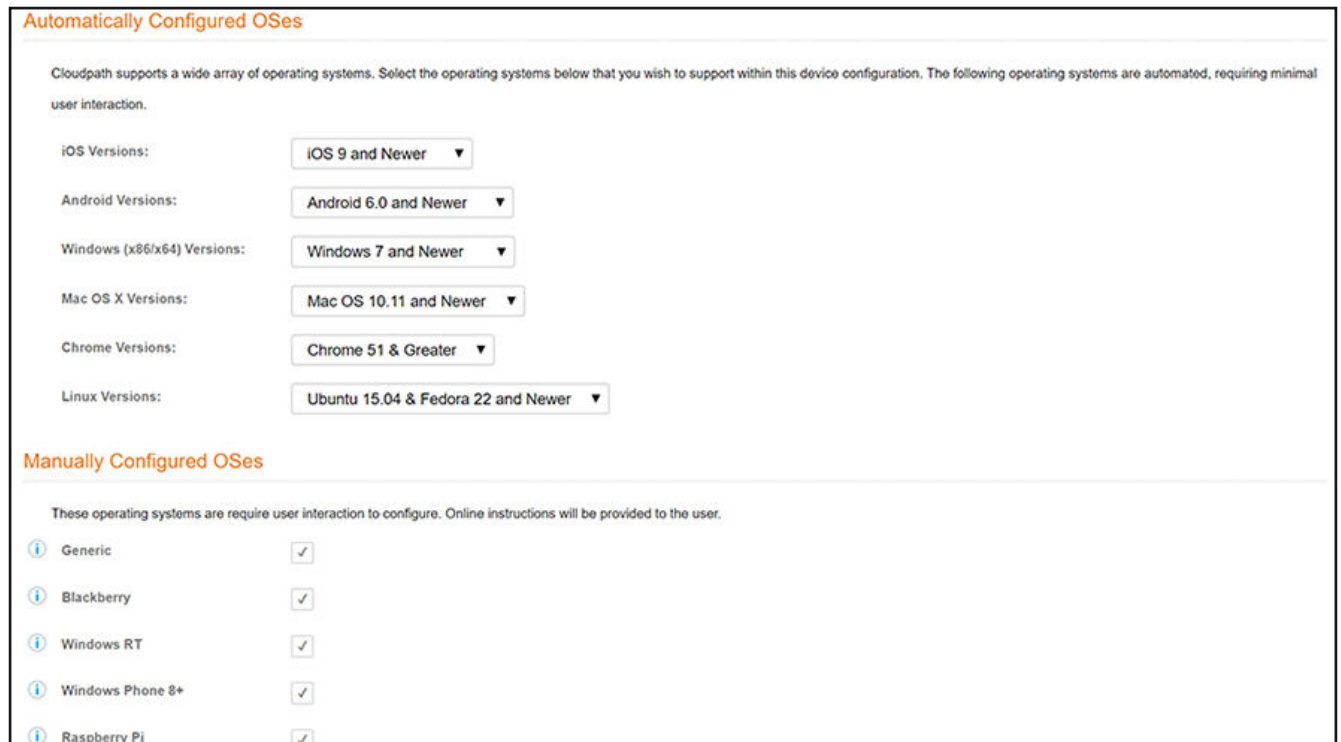
7. Specify **Conflicting SSIDs**.

This setting attempts to deter enrolled devices from joining listed SSIDs after the secure SSID is configured. It is recommended that you include the open-enrollment SSID in this list. Specifying this option is required for mobileconfig-based iOS/macOS enrollments to disconnect from the open-enrollment SSID and re-scan for the secure SSID at the time of the mobileconfig profile installation. *Note that this option is case-sensitive, and the case must match exactly the value broadcast by your wireless network infrastructure.*

For mobileconfig-based Mac OS X enrollments to be disconnected upon profile installation, the "WLAN Profile Type" must be set to "Machine." To locate this setting in the UI, go to **Configuration > Device Configurations**, then click the arrow to expand the device configuration. Next, click the **OS Settings** tab, then click the pencil icon to edit the field called "Configuration from the Network(s) and Trust tabs" under the Mac OS X Settings area. In the Advanced Settings area, see "WLAN Profile Type."

8. Select the operating system families and versions that to support within this device configuration.
You can restrict a particular version or service pack level after the device configuration is created.

FIGURE 32 Select OS Versions



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

10. Configure additional settings for the device configuration.

A more comprehensive list of additional settings is available after the device configuration is created. You can go to **Configuration > Device Configurations**, click the arrow next to the desired device configuration to expand the view, then click the **OS Settings** tab. From there, you can scroll to see your options to edit or add settings for the various operating systems.

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

Client Certificates

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

You can set up different certificate templates for different user types. An employee or staff certificate template might be valid for 120 days, and a guest template might be valid for 1 day or until the end of the week.

After you set up a device configuration for the workflow, you configured and assign a new certificate template.

1. Select **A new certificate template**.
2. Select **Use an onboard certificate authority**.
3. Select **Use an existing CA**. Choose the default Root CA that was created during the initial system setup.

4. Set up the **Client** certificate template. This template is used to issue a certificate to the client device.

FIGURE 33 Client Certificate Template

The screenshot shows the 'Client Certificates' configuration page. At the top, it states: 'Used on clients to authenticate the client. The decoration of the username within the certificate allows RADIUS policies to be applied appropriately.' Below this, there are three main sections: 'Username Decoration', 'Grant Access Until', and 'Configure Advanced Options'. The 'Username Decoration' section has a list of radio buttons for different email domains, with 'username@other.ccompany.com' selected. The 'Grant Access Until' section has a dropdown menu set to '1 Years' and a note 'after issuance.'. The 'Configure Advanced Options' section has an unchecked checkbox. Below these is the 'Lifecycle Notifications' section, which explains that the system supports events related to the certificate lifecycle and lists four notification options, all of which are unchecked: 'Send welcome email on issuance.', 'Send email 7 days before certificate expiration.', 'Send email if certificate is revoked.', and 'Email administrator if revoked certificate is used.'. The final section is 'RADIUS Options', which explains that the template will be honored for RADIUS authentications and lists three attributes: 'VLAN ID' (with a placeholder '[ex. 50]'), 'Filter ID' (with a placeholder '[ex. BYOD]'), and 'Class' (with a placeholder '[ex. BYOD]').

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

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

6. Grant access for the appropriate amount of time.

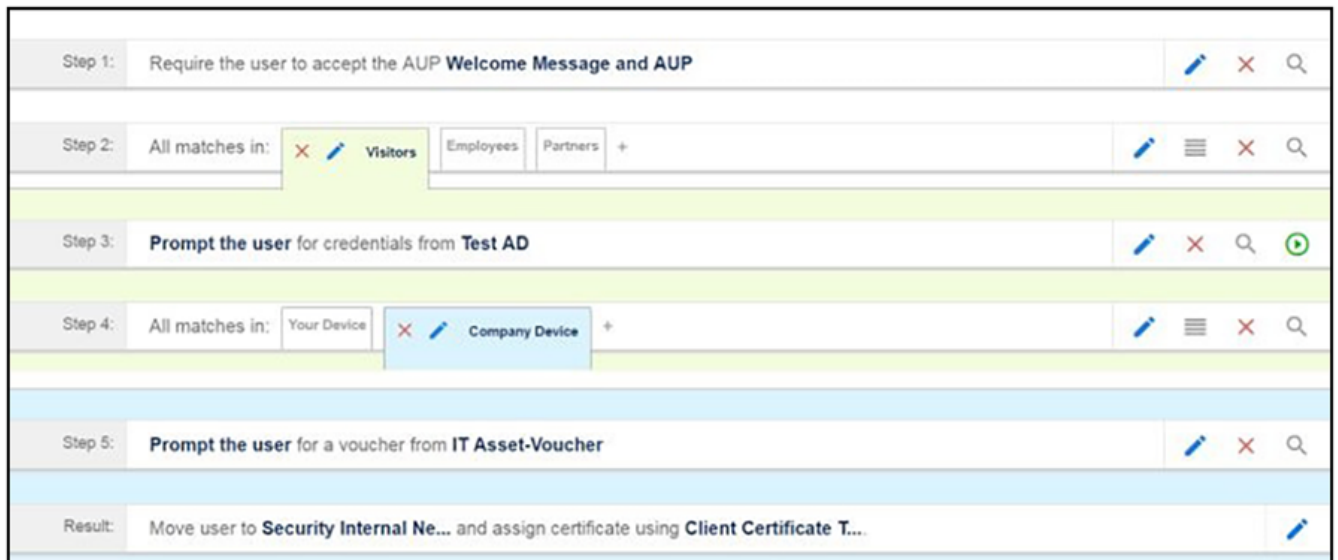
For example, you might have a client certificate template for a guest user that is valid for one, or a few days, another for a contractor that is valid for 6 months, and one for employees that is good for a year.

NOTE

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

7. Select any email notifications to be sent to the user related to the life-cycle of the certificate.
Additional certificate notifications can be configured after the template is created.
8. Optional. Enter **RADIUS Options** to assign a VLAN ID or Filter ID to certificates that use this template. These settings only applies if you are using the Cloudpath onboard RADIUS server.
9. Click **Next**. The completed workflow shows all enrollment paths. The last step shows the device configuration which is applied to the user device and the certificate template being used to assign a certificate to the user device.

FIGURE 34 Completed Workflow



After you have finished configuring a enrollment workflow, create and deploy a snapshot of the workflow configuration to test before deploying to users.

Using the Timed Access Workflow Template

You can the Timed Access workflow template to create a workflow that allows limited-time access for a user based on MAC address authentication.

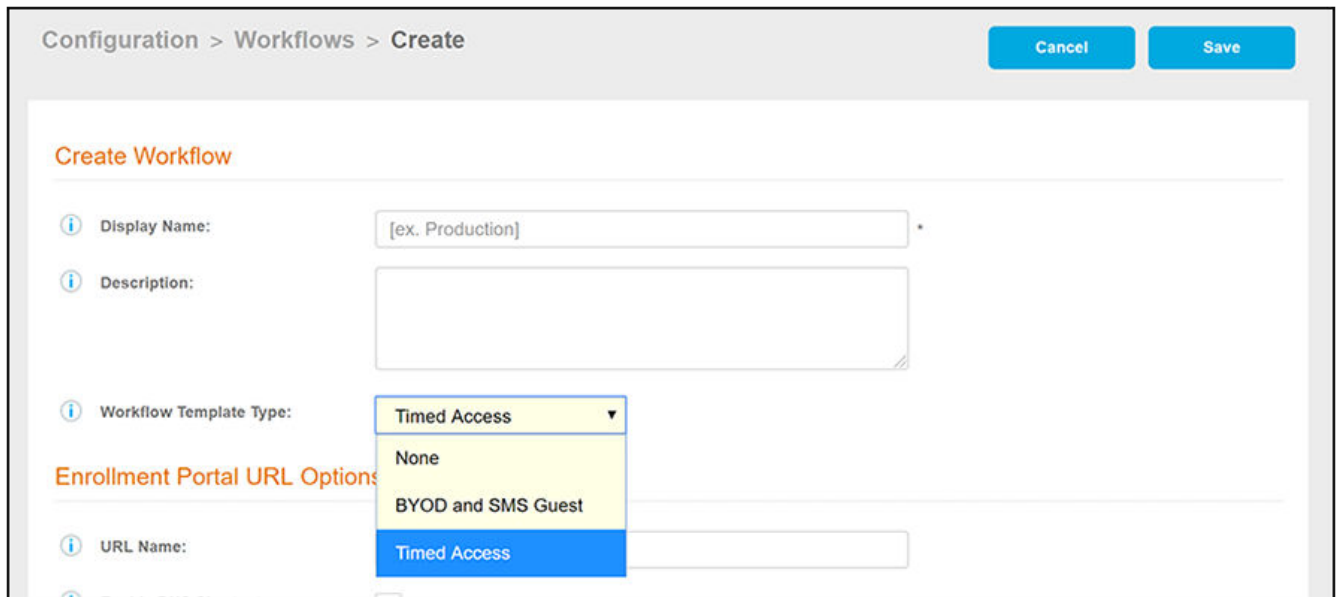
The main concept of the Timed Access workflow template is to give users free access to a network connection for a limited time period, and, when that time period expires, they can re-enroll their device to one of the a pre-configured "premium" lists. You can use other workflow plug-ins to add steps to this workflow, and in fact that is how the Timed Access template is intended to be used. An example of a useful plug-in that works well with this template is described later in this section.

The procedure below demonstrates how to create a Timed Access workflow.

1. Go to **Configuration > Workflows**.
2. On the right hand side of the **Workflow** page select **Add Workflow**.

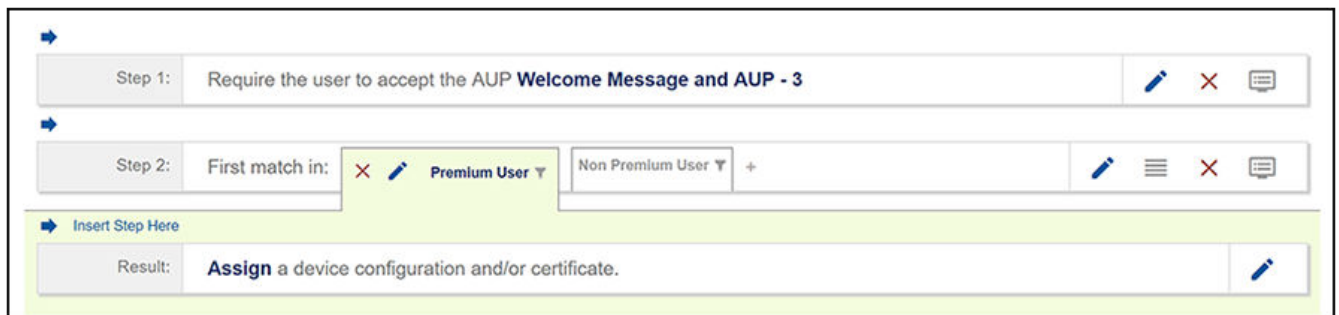
The Create Workflow screen is displayed:

FIGURE 35 Create Workflow Screen - Selecting "Timed Access" For Workflow Template Type



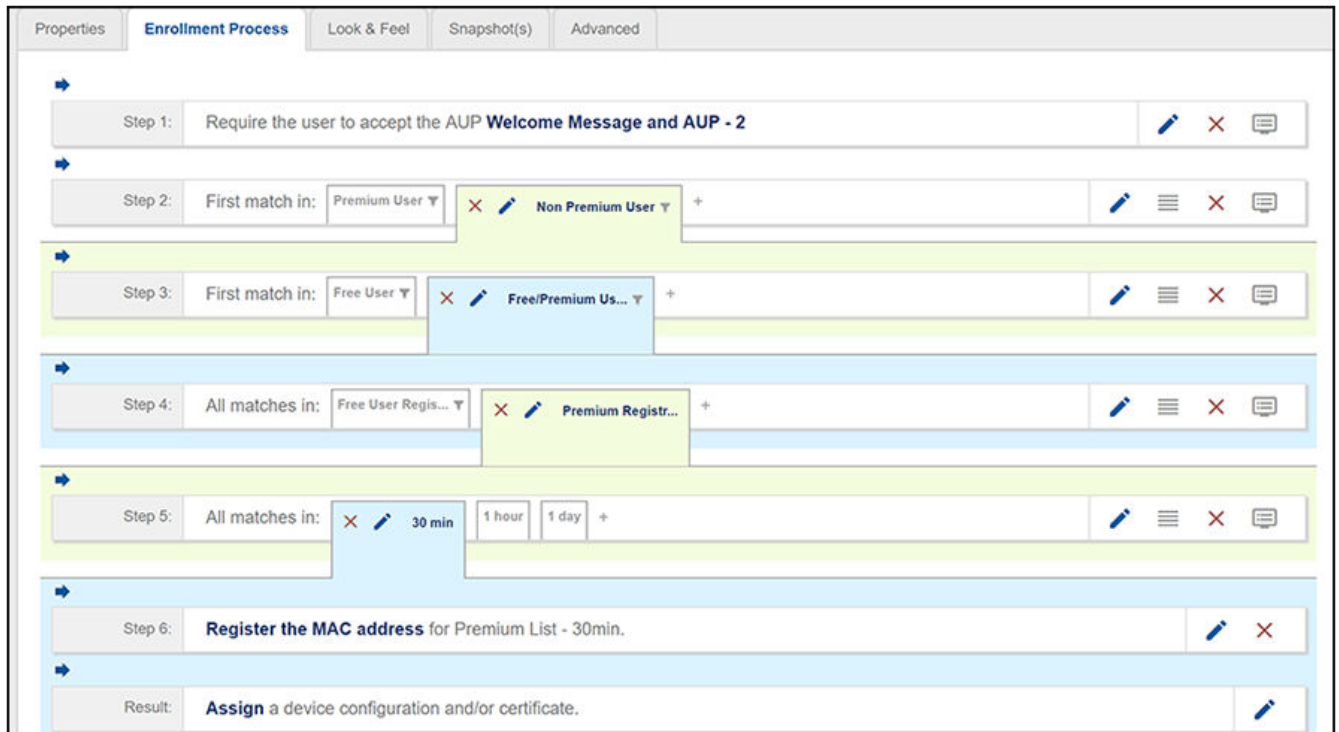
3. On the **Create Workflow** screen, enter a **Display Name** and **Description**.
4. From the Workflow Template Type drop-down list, select "Timed Access."
5. Fill out the URL Name field.
6. Click **Save**, and you are returned to the workflow page that is shown in the following figure.

FIGURE 36 Timed Access Workflow After Initial Creation



- Expand the workflow to show its complete logic by clicking **Non Premium User**, then clicking **Free/Premium User**, then clicking **Premium Registration**. The workflow appears as shown in the following figure:

FIGURE 37 Timed Access Workflow Fully Expanded



The following MAC registration lists are automatically created by this workflow template, and can be viewed in the **Configuration > MAC Registrations** portion of the UI:

- Premium List - 1 day
- Premium List - 1 hr
- Premium List - 30min
- Free List

Free User Registration

The Free User Registration branch is exposed to users only when they enroll for the first time within a 24-hour period. The Free List is pre-configured to have a 30-minute expiration; this list is automatically cleaned up every 24 hours so that users can again use the Free User Registration branch again in the next 24-hour period.

Workflow Logic:

To understand workflow logic and how the user gets presented with various steps, it is essential to know how "First match in" and "All matches in" work during user enrollment:

- "First match in:" The first branch (going from left to right in the workflow) where the criteria being evaluated matches that of the user is used automatically.
- "All matches in:" All branches are evaluated to determine if the criteria being evaluated matches that of the user. After this determination has been calculated, *all* options that are a match are offered to the user, and the user can select an option from the choices presented. If only one match occurs, the matching branch is used automatically.

The basic steps shown in this workflow are described in the following table.

NOTE

In the UI, be sure to use your cursor to hover over the text of each workflow step, and the logic of each possible option is described.

TABLE 3 Description of Steps in Timed Access Workflow Template

Step 1	Acceptable Use Policy.
Step 2	<p>First match in:</p> <ul style="list-style-type: none"> Premium User: An enrollment whose MAC address is already registered in one of the three premium lists is taken down this branch. This branch is never available to a first-time enrollment in a 24-hour period. If this option is a match, the enrollment then goes directly to the device configuration (Result step). Non Premium User: Any enrollment that does not match the "Premium User" criteria is taken down this branch. A first-time enrollment in a new 24-hour period is taken down this branch.
Step 3	<p>First match in:</p> <ul style="list-style-type: none"> Free User: An enrollment whose MAC address is already registered in the Free List (and has not yet expired) is taken down this branch. If this option is a match, the enrollment then goes directly to the device configuration (Result step). Free/Premium User: Any enrollment that does not match the "Free User" criteria is taken down this branch.
Step 4	<p>All matches in:</p> <ul style="list-style-type: none"> Free User Registration: Presented if the MAC address is <i>not</i> currently in the Free List, nor is the MAC address marked as "expired" or "revoked" in the Free List. If this branch is chosen, the MAC address is registered to the Free List and the enrollment is assigned a device configuration (Result step). Premium Registration: Available to all enrollments <p>A first-time enrollment (for a new 24-hour period) will either be presented with both options or will be taken down the Premium Registration branch.</p>
Step 5	<p>All matches in:</p> <ul style="list-style-type: none"> 30 min: Available to all enrollments 1 hour: Available to all enrollments 1 day: Available to all enrollments <p>These options are presented to all enrollments who have gone down the Premium Registration branch. The user makes a selection, and the enrollment proceeds with the MAC address getting registered.</p>
Step 6	Register the MAC address: The MAC address is registered in the selected premium MAC Registration list.

You can determine what other steps you want to include in your workflow. For example, a "Charge user for service" step would fit well within a workflow where timed access is involved. You could insert such a step before the MAC Registration step. (Refer to the "Charge User for Service" topic in the Cloudpath Enrollment System Deployment Administration Guide.)

Publishing the Enrollment Workflow

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

The Workflow list contains status of the workflow (published or unpublished), the **Enrollment Portal URL** where a configuration is deployed, and the last published time for each workflow configuration.

FIGURE 38 Publish Workflows

The screenshot displays the 'Configuration > Workflows' interface. At the top right, there is an 'Add Workflow' button. Below it is a table with the following columns: Workflows, Status, Enrollment Portal URL, and Last Publish Time.

Workflows	Status	Enrollment Portal URL	Last Publish Time
Building A Lobby with Guest Access	Unpublished	/enroll/Regression/BLDG-A-Lobby/	
BLDG B Employee Access	Unpublished	/enroll/Regression/SponsoredGuest-JR/	
Richard_Test	Published	/enroll/Regression/RichardJ/	20170413 1715 GMT
Sponsored Guest JR	Published	/enroll/Regression/Sponsored-Guest-JR/	20170413 1715 GMT
Employees with Personal Devices BYOD	Unpublished	/enroll/Regression/EmployeeswithPersonalDevicesBYOD/	
Employee IT Asset	Published	/enroll/Regression/EmployeeITAsset/	20170413 1715 GMT
Primary Workflow	Published	/enroll/Regression/Production/	20170413 1715 GMT

Below the table, there are tabs for 'Properties', 'Enrollment Process', 'Look & Feel', 'Snapshot(s)', and 'Advanced'. The 'Enrollment Process' tab is selected, showing a sequence of steps:

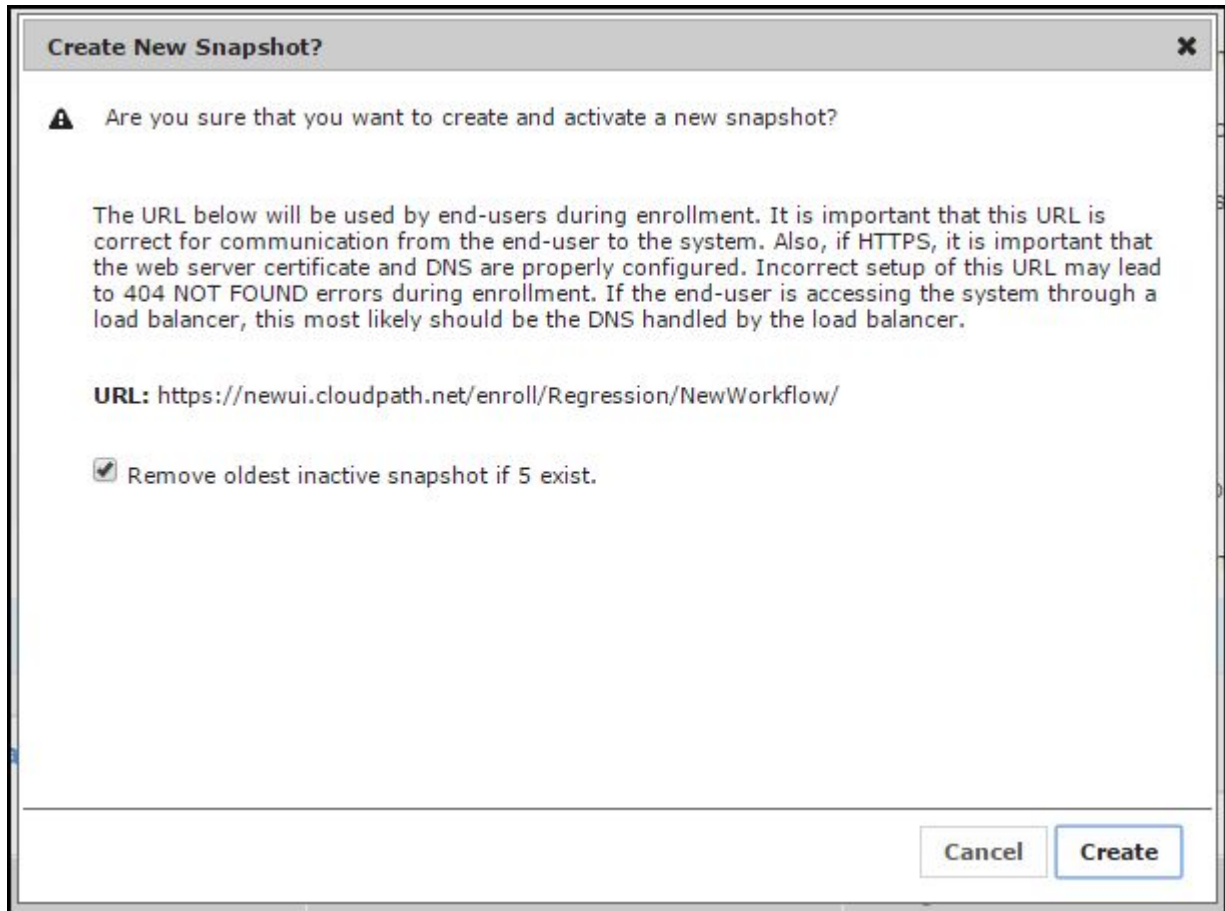
- Step 1: Require the user to accept the AUP **Welcome Message and AUP**
- Step 2: All matches in: **Your Device**, Company Devices +
- Step 3: **Prompt the user** for credentials from **Test AD**
- Step 4: All matches in: **Your Device**, Company Devices +
- Result: **Assign** a device configuration and/or certificate.

When you publish a workflow, this creates a snapshot of the workflow configuration. To publish the workflow:

1. Navigate to **Configuration > Workflows** tab.

2. On the Workflow configuration page, click the **Publish** icon next to the workflow to publish.

FIGURE 39 Create New Snapshot



3. Select the Wizard version to use for the new snapshot. The **Cloudpath Wizard** is the application provided to users to automate the enrollment process.
4. Verify the Enrollment Portal URL for the snapshot.
5. Click **Create**.

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

How to Test a Published Workflow

Test the enrollment process for the active workflow snapshot using the Enrollment Portal URL. The Enrollment Portal URL provides access to the user enrollment process, which contains the workflow and if applicable, the Cloudpath Wizard.

1. Navigate to the **Configuration > Workflows** page.
2. On the workflow list, select the workflow to test.
3. Click the Enrollment Portal URL. Be sure that the snapshot you want to test is the **active** snapshot (green icon).

Administration

- Administration Overview..... 57

Administration Overview

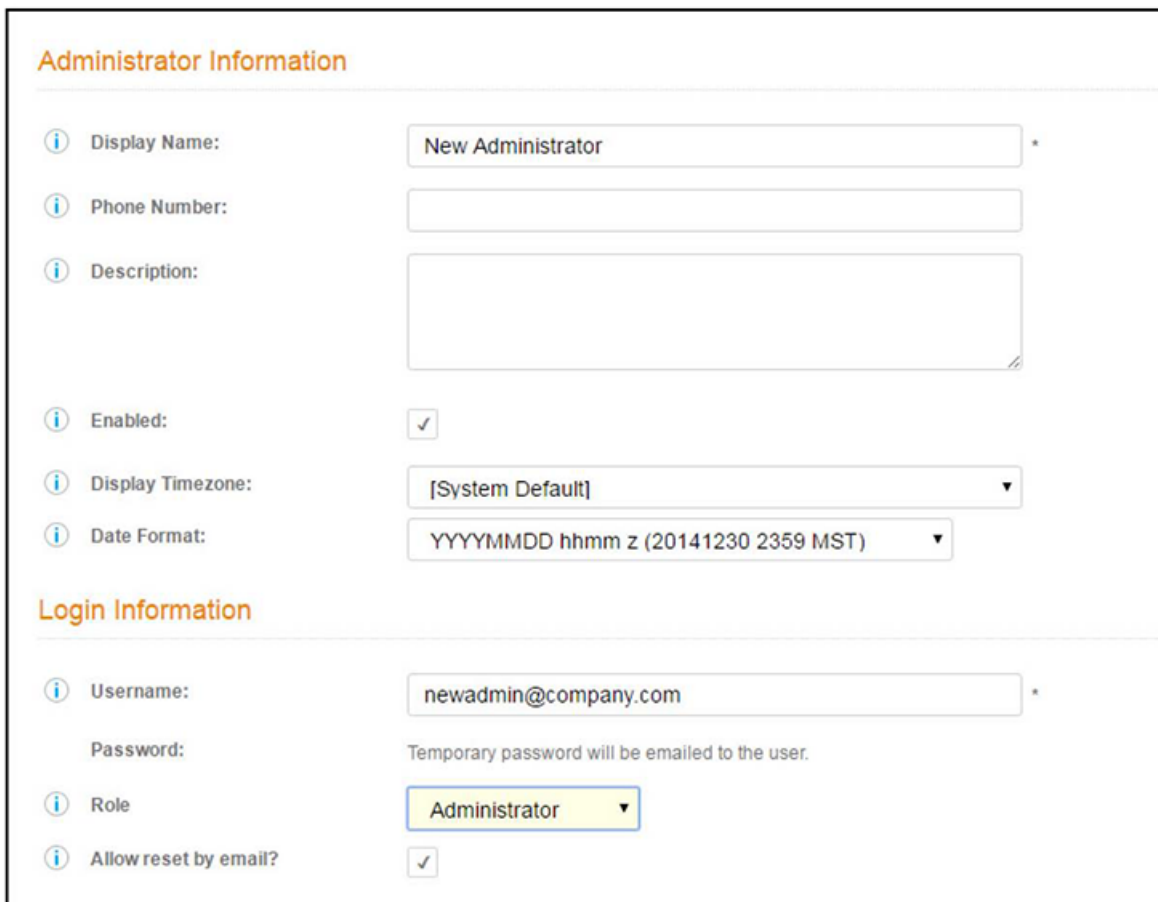
Access the **Cloudpath Administration** tab to manage system-related operations, using links in the following sections:

Administrators

During the initial account setup, Cloudpath sets up an administrator account using the company information provided during the setup. By default, there is also an Administrator Group, which allows administrative access to the Admin UI using credentials from the configured authentication server. This allows users who belong to a specific group to access Cloudpath.

Manage administrator access to the Cloudpath Admin UI from **Administration > Administrators**.

FIGURE 40 Add Administrator



Administrator Information

Display Name: New Administrator *

Phone Number:

Description:

Enabled:

Display Timezone: [System Default] ▼

Date Format: YYYYMMDD hhmm z (20141230 2359 MST) ▼

Login Information

Username: newadmin@company.com *

Password: Temporary password will be emailed to the user.

Role: Administrator ▼

Allow reset by email?:

Cloudpath supports the following Administrator Roles:

- CA Administrator - Allows full configuration access to the Administrative UI. This administrator role can manage all administrative users.
- Administrator - Allows full configuration access to the Administrative UI, except for Certificate Authorities. This administrator can manage Administrator and Viewer administrative users.
- Viewer - Allows view-only access to Enrollment, User, and Certificate records on the Dashboard, the enrollment Workflow, and the Documentation and Licensing pages. This administrator cannot manage other administrative users.

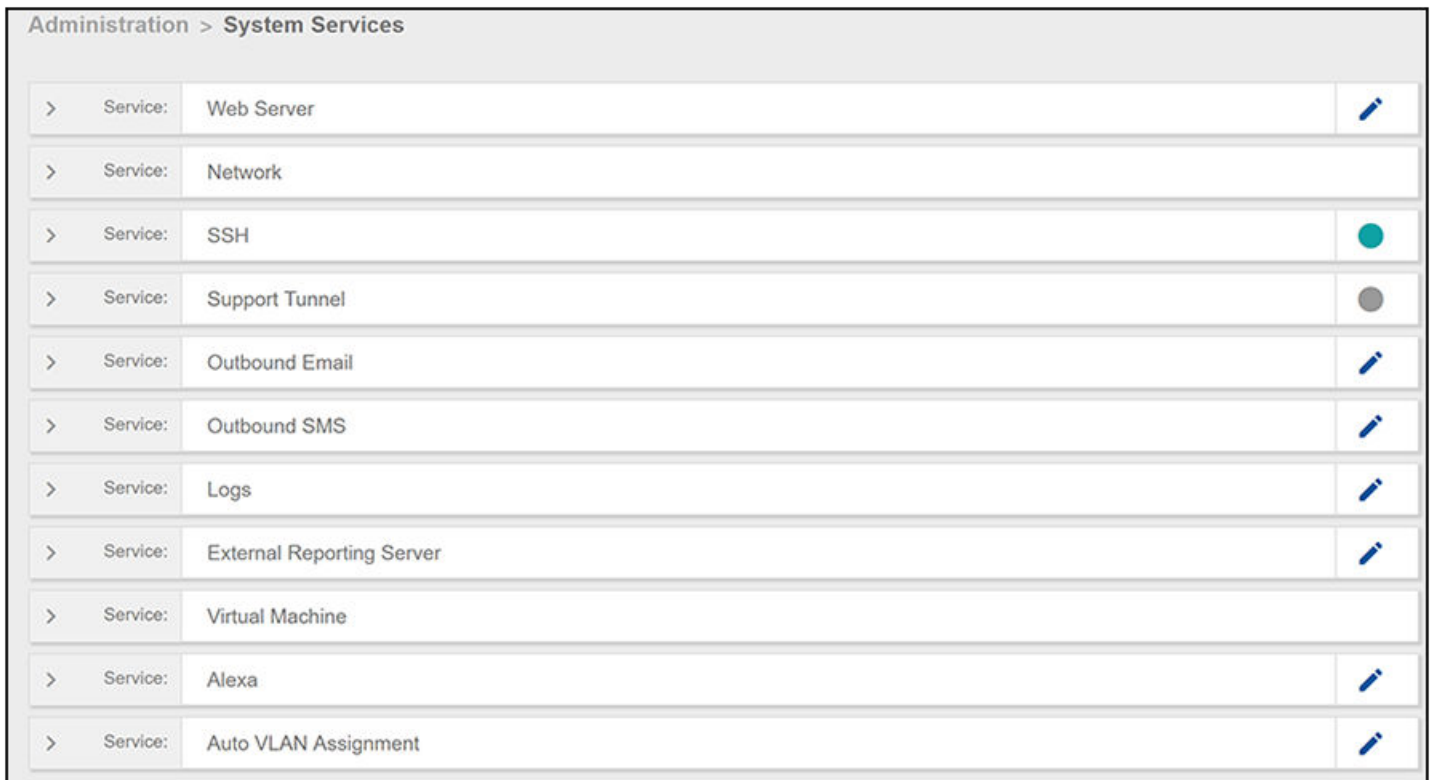
Company Information

Company Information - Used within the URL for enrollments and sponsorships, and included in the onboard CAs.

System Services

Navigate to **Administration > System Services** to restart or view logs for the application server, web server, configure email or SMS servers, or start up a support tunnel.

FIGURE 41 Cloudpath System Services



Administration > System Services		
>	Service: Web Server	
>	Service: Network	
>	Service: SSH	
>	Service: Support Tunnel	
>	Service: Outbound Email	
>	Service: Outbound SMS	
>	Service: Logs	
>	Service: External Reporting Server	
>	Service: Virtual Machine	
>	Service: Alexa	
>	Service: Auto VLAN Assignment	

- Web Server - Download the Apache Server access and error logs from the Web Server component. You can also Restart the web server, generate a CSR, edit administrative access restrictions, and download or upload the web server certificate, or if needed, upload a code certificate.

- Network - The **Network** service displays network properties for Cloudpath, and provides access to view or download the diagnostic logs.
- SSH - Use the **SSH** service to enable, disable or change the access port. SSH runs on ports 22 and 8022. You can set the port number using the command line or from the user interface. Even if you disable SSH access for both ports, SSH can continue to run.
- Support Tunnel - The **Support Tunnel** service allows you to open a support tunnel to help you in diagnosing issues with your application or configuration.
- Outbound Email - Use the onboard email provider or configure a local email server.
- Outbound SMS - Use the onboard SMS provider, enter a CDYNE account or route SMS message through a customer-owned account.
- Logs - Configure where syslog messages are sent. You can enable the syslog, select the protocol over which the syslog messages are sent, and enter a host and port number.
- External Reporting Server - Allows you to integrate Cloudpath enrollment data with a reporting server, such as the ELK stack (Elasticsearch, Logstash, and Kibana).
- Virtual Machine - Displays the system clock and system information about the virtual machine. You can also reboot or shut down the virtual machine from this page.
- Alexa - Allows you to bind or unbind Alexa, remove old binding data, or get Alexa log files.
- Auto VLAN Assignment - Allows you assign available VLAN IDs from a configured range of VLANs to users during their enrollment.

System Updates

System Updates - View and manage the Cloudpath build versions.

Data Cleanup

Data Cleanup - Manage database cleanup thresholds for enrollment records, abandoned certificates, vouchers, notifications, manage wizard versions, and other system events.

Firewall Requirements

Firewall Requirements - Displays inbound and outbound traffic from Cloudpath to assist with firewall configuration.

Configuration

- Overview..... 61
- Device Configurations..... 61
- RADIUS Server..... 61
- Authentication Servers..... 63
- Firewalls and Web Filter Integration..... 63
- MAC Registration Lists..... 63
- API Keys..... 63

Overview

The components listed in the **Configuration** tab are described in the following sections. They are typically set up during the Initial System Setup, or during the workflow configuration, but can be modified as needed.

The Workflow tab is covered in the "Enrollment Workflow" chapter.

Device Configurations

A device configuration is a group of configuration settings for a specified WLAN or wired network. Device Configuration settings are managed using the following tabs:

- Summary tab - An overview of the device configuration settings.
- Networks tab - WLAN settings.
- Trust tab - RADIUS server information and certificate chaining.
- OS Settings tab - User experience, network, and additional settings that are specific to an operating system or a specific version of an operating system.
- Passpoint tab - Passpoint settings for the device configuration, which includes certificate settings, and home service provider, subscriber, and policy settings.

Refer to the *Configuring Cloudpath to Support Hotspot 2.0 Release 2 (Passpoint)* guide on the **Admin UI Support** tab for complete details on setting up a Ruckus SmartZone controller and Cloudpath for Passpoint.

- Credentials tab - (For PEAP networks only) Settings related to password-based Wi-Fi.

RADIUS Server

View and manage the onboard RADIUS server.

- RADIUS Server Status - View status, settings, and certificate information, generate a CSR, or upload a certificate. You can also download RADIUS server certificates and log files or export onboard CA information to be used to set up an external RADIUS server.
 - Connection Tracking - Enabled by default on new systems, Connection Tracking displays the current device connections on the **Dashboard > Connections** page. RADIUS Accounting must be enabled on your wireless LAN controller. See the *Integration with Ruckus Controllers* guide on the **Support** tab for more information.

- CoA - Enable CoA to send Change of Authorization disconnect messages (DMs) from Cloudpath to the switch or wireless LAN controller. You can send disconnects from the **Dashboard > Connections** page, or via an enrollment **Revoke**. See the *Onboard RADIUS Server CoA guide* on the **Support** tab for more information.
- Policies - View all policies for the onboard RADIUS server, including those assigned by certificate templates, eduroam configuration, and MAC registration policies.
- Clients - View all RADIUS allowed to call into the RADIUS server, including any eduroam clients.
- RADIUS Server and eduroam - Configure a eduroam federation server to interact with the onboard RADIUS server.
- Attributes - Define the RADIUS attributes that will be visible in the system. These attributes, which are included in the Access-Accept/Reject reply from the RADIUS server, can be added to the certificate template, MAC registration, and eduroam configuration.
- External - Download a zip file, which provides the information and CA certificate needed for an external RADIUS server.
- Open Access - Configure open access for a specific SSID, for a specified time-period for short term usage.

NOTE

We recommend using Open Access in a limited, or test environment. SSIDs configured for Open Access are not secure.

- RADIUS Accounting - If your wireless LAN controller is configured to support RADIUS accounting, and if Connection Tracking is enabled, the Accounting tab displays RADIUS accounting packets local to the Cloudpath server. See the *Integration with Ruckus Controllers* guide on the **Support** tab for more information.

FIGURE 42 RADIUS Accounting

The screenshot shows the 'Accounting' tab in the Cloudpath interface. The title is 'Recent RADIUS Accounting Packets (Local)'. Below the title is a table with the following columns: Event Timestamp, Type, Session ID, Calling Station, Client IP, Username, NAS ID, NAS IP, and Vlan Port. The table contains 12 rows of data, each with a magnifying glass icon in the first column.

Event Timestamp	Type	Session ID	Calling Station	Client IP	Username	NAS ID	NAS IP	Vlan Port
Dec 14 2016 13:42:24 WIT	Start	999CBAD1-0000769	4C:00:78:89:1A:18	192.168.93.201	aria@tst.companys.com	38-FF:34:02:4A-7E	192.168.93.135	59
Dec 14 2016 13:43:52 WIT	Start	999CBAD1-0000769	6A:FE:9C:67:87:AD	192.168.93.201	bob@tst.companys.com	38-FF:34:02:4A-7E	192.168.93.135	59
Dec 14 2016 13:44:24 WIT	Start	999CBAD1-0000769	3d:84:a8:08:C8:F9	192.168.93.201	jack@tst.companys.com	38-FF:34:02:4A-7E	192.168.93.135	60
Dec 14 2016 13:47:04 WIT	Start	999CBAD1-0000769	4C:04:F9:8B:08:04	192.168.93.147	l-r@tst.companys.com	38-FF:34:02:4A-7E	192.168.93.135	61
Dec 14 2016 13:47:17 WIT	Start	999CBAD1-0000769	3d:0C:0F:21:8D:AD	192.168.93.138	m-h@tst.companys.com	38-FF:34:02:4A-7E	192.168.93.135	63
Dec 14 2016 13:50:14 WIT	Start	999CBAD1-0000769	3C:A9:F4:01:02:50	192.168.93.40	aria@tst.companys.com	6C:AA:8D:54:AF:8C	192.168.93.143	1
Dec 14 2016 13:52:24 WIT	Start/stop	999CBAD1-0000769	4C:00:78:89:1A:18	192.168.93.201	aria@tst.companys.com	38-FF:34:02:4A-7E	192.168.93.135	59
Dec 14 2016 13:53:02 WIT	Start/stop	999CBAD1-0000769	6A:FE:9C:67:87:AD	192.168.93.201	bob@tst.companys.com	38-FF:34:02:4A-7E	192.168.93.135	59
Dec 14 2016 13:53:49 WIT	Start	999CBAD1-0000769	8C:3A:83:13:4D:0A	192.168.93.209	bob@tst.companys.com	6C:AA:8D:54:AF:8C	192.168.93.143	1
Dec 14 2016 13:54:34 WIT	Start/stop	999CBAD1-0000769	3d:84:a8:08:C8:F9	192.168.93.135	jack@tst.companys.com	38-FF:34:02:4A-7E	192.168.93.135	60

Authentication Servers

View and manage the servers against which users may be authenticated. This includes local servers such as Active Directory and LDAP, as well as third-party services, such as Facebook, SAML (Shibboleth), RADIUS via PAP, and an onboard database.

Firewalls and Web Filter Integration

Configure Cloudpath to integrate with Palo Alto Firewalls and Web Filter applications.

Cloudpath supplements data already captured by these applications by adding mappings of the IP address to a UserId, which allows the captured traffic to be identifiable. When the user joins the network via Cloudpath, the firewall or web filter application is notified of the user's login. Similarly, when a user is known to have left the network, the application is notified of the logout.

MAC Registration Lists

View and manage MAC registration databases, which allow network access to devices that do not have the 802.1X supplicant capability.

Each database has its own policies. When a device is registered, it is assigned to one of the databases. Cloudpath provides a template for importing MAC address in bulk using a .csv or .xlsx file.

API Keys

A list of the APIs currently in use with Cloudpath.

The REST APIs allow the system to actively notify external systems and to be queried and manipulated by external systems.

Dashboard

- Overview..... 65
- Enrollments..... 65
- Connections..... 67
- Users & Devices..... 68
- Certificates..... 70
- Notifications..... 72
- Event Response..... 74

Overview

The Cloudpath dashboard provides detailed information about the number and status of enrollments on your network, including notifications, events, certificates, MAC registrations, and scheduled reports.

Enrollments

The **Enrollments** table allows you to review enrollments, including the associated user, device, and certificate information. The **Enrollment Paths** tab shows a graphical depiction of the different paths taken by users during the enrollment process.

FIGURE 43 Enrollments Table

ID	Status	Enrollment Type	User	Device	Certificate	Created	Updated	Expires	Notes
1081	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 17:58:45Z	2018-10-26 17:58:45Z	2019-10-26 17:58:45Z	None
4389	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:28:53Z	2018-10-26 18:28:53Z	2019-10-26 18:28:53Z	None
4754	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:28:53Z	2018-10-26 18:28:53Z	2019-10-26 18:28:53Z	None
4768	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:28:53Z	2018-10-26 18:28:53Z	2019-10-26 18:28:53Z	None
5887	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:40:53Z	2018-10-26 18:40:53Z	2019-10-26 18:40:53Z	None
4878	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:40:53Z	2018-10-26 18:40:53Z	2019-10-26 18:40:53Z	None
1478	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:27:45Z	2018-10-26 18:27:45Z	2019-10-26 18:27:45Z	None
8104	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:27:45Z	2018-10-26 18:27:45Z	2019-10-26 18:27:45Z	None
4428	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:27:45Z	2018-10-26 18:27:45Z	2019-10-26 18:27:45Z	None
4351	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:27:45Z	2018-10-26 18:27:45Z	2019-10-26 18:27:45Z	None
7128	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:27:45Z	2018-10-26 18:27:45Z	2019-10-26 18:27:45Z	None
4759	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:27:45Z	2018-10-26 18:27:45Z	2019-10-26 18:27:45Z	None
4888	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:27:45Z	2018-10-26 18:27:45Z	2019-10-26 18:27:45Z	None
4614	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:27:45Z	2018-10-26 18:27:45Z	2019-10-26 18:27:45Z	None
8884	Completed	Certificate Install	bob	iPhone8,2	iPhone8,2	2018-10-26 18:27:45Z	2018-10-26 18:27:45Z	2019-10-26 18:27:45Z	None

NOTE

Use the view icon to display further details about a specific enrollment record, to revoke a certificate, or to remove the enrollment record from the database.

Records Export

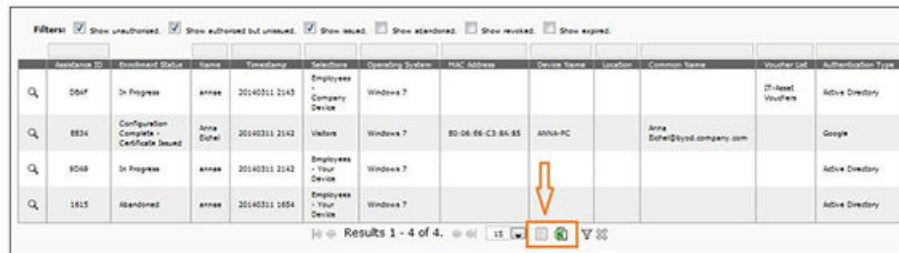
Enrollment and User data can be downloaded, as a CSV file or Microsoft Excel spreadsheet.

Use the CSV Export icon  or XLS Export icon  located at the bottom of the table.

By default, the Enrollment data files are named **enrollments.txt** or **enrollment.xls** and the User data files are named **users.txt** or **users.xls**.

The Enrollment and User export files are designed to be a quick view of the activity since midnight. To export only certain items in the table, for a specific date and time, or to export items for a longer time period, see *Scheduled Reports*.

FIGURE 44 Download Enrollment Records



The screenshot shows a table with the following columns: Instance ID, Enrollment Status, Name, Timestamp, Category, Operating System, MAC Address, Device Name, Location, Company Name, User ID, and Authentication Type. There are four rows of data. An orange arrow points to a download icon (a green circle with a white document symbol) in the bottom right corner of the table, which is also highlighted with an orange box. The table footer shows 'Results 1 - 4 of 4' and a page number '15'.

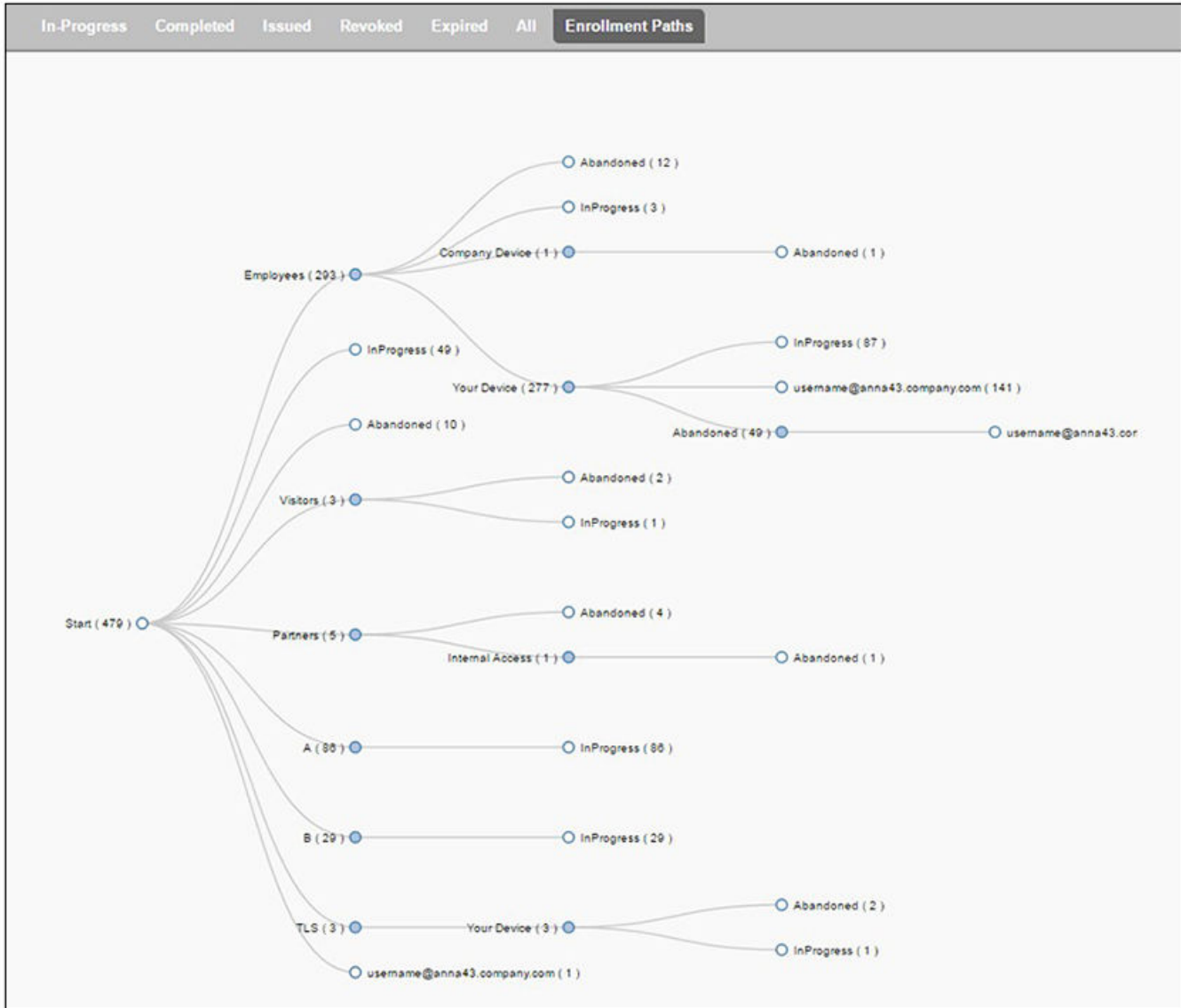
Instance ID	Enrollment Status	Name	Timestamp	Category	Operating System	MAC Address	Device Name	Location	Company Name	User ID	Authentication Type
004F	In Progress	anna	20140311 2143	Employees - Company Device	Windows 7					IT Asset You/Ann	Active Directory
8E34	Configuration Complete - Certificate Issued	Anna Eitel	20140311 2142	Victors	Windows 7	80-06-06-C3-8A-85	ANNA-PC		Anna Eitel@byond.company.com		Google
9C68	In Progress	anna	20140311 2142	Employees - Your Device	Windows 7						Active Directory
1615	Abandoned	anna	20140311 1804	Employees - Your Device	Windows 7						Active Directory

Enrollment Paths

During enrollment, the user is taken through a sequence of steps, called an enrollment workflow. The workflow depends on the selection chosen when the user is prompted, and on any configured filter in the workflow. For example, the user can select the Employee or Guest path, and then be moved to the IT Asset device path, because their Active Directory credentials, by way of a filter, caused them to be moved to the Personal Device path.

The **Enrollment Paths** tab shows a graphical depiction of the paths taken by users during the enrollment process.

FIGURE 45 Enrollment Path



Connections

The **Connections** tab displays the current device connections for the Cloudpath system. To view the connections, **RADIUS Accounting** must be enabled on your wireless LAN controller and **Connection Tracking** must be enabled for the onboard RADIUS server. See the *Cloudpath Enrollment System Integration with Ruckus WLAN Controllers Configuration Guide* for more information.

FIGURE 46 RADIUS Connections

		Status	IP Address	MAC Address	Username	SSID	Duration
Q X	+	Connected	192.168.95.136	04:0C:CE:21:8D:A0	mike@byod.company.com	eng-Anna42	10 minutes ago
Q X	+	Connected	192.168.95.40	3C:A9:F4:01:02:50	anna@byod.company.com	eng-Anna42	7 minutes ago
Q X	+	Connected	192.168.95.197	6C:94:F8:B9:DB:06	bill@byod.company.com	eng-Anna42	11 minutes ago
Q X	+	Connected	192.168.95.195	34:E6:AD:0E:CE:F5	jack@byod.company.com	eng-Anna42	13 minutes ago
Q X	+	Connected	192.168.95.251	E4:F8:9C:07:B7:4D	bob@byod.company.com	eng-Anna42	15 minutes ago
Q X	+	Connected	192.168.95.181	4C:8D:79:E9:16:18	anna@byod.company.com	eng-Anna42	16 minutes ago
Q X	+	Connected	192.168.95.209	8C:3A:E3:15:6C:C6	bob@byod.company.com	eng-Anna42	4 minutes ago

You can send Change of Authorization (CoA) disconnect messages (DMs) to the controller or switch from the **Connections** page, or via an enrollment **Revoke**. See the *Onboard RADIUS Server CoA* guide on the **Documentation** tab for more information.

Users & Devices

The **Users** table provides a list of User records, including user devices, enrollment paths, and certificate information for each user.

FIGURE 47 User Table

		Status	Photo	First Name	Last Name	Server Name	Authentication Type	Timestamp
Q				Anna	Eichel	LinkedIn, Facebook, or Gmail	Google	20140326 1006 MDT
Q				Anna	Eichel	Anna Test AD	Active Directory	20140326 1335 MDT
Q				Bob	Johanson	Anna Test AD	Active Directory	20140326 1344 MDT
Q				Bill	Smith	Anna Test AD	Active Directory	20140326 1348 MDT
Q				Mark	Test	Anna Test AD	Active Directory	20140326 1415 MDT
Q				Lynn	Test	Anna Test AD	Active Directory	20140326 1415 MDT
Q				Mike	Test	Anna Test AD	Active Directory	20140331 1622 MDT
Q				Anna	Test	Anna Test AD	Active Directory	20140331 1625 MDT
Q				Anna	Eichel	LinkedIn, Facebook, or Gmail	Google	20140331 1638 MDT

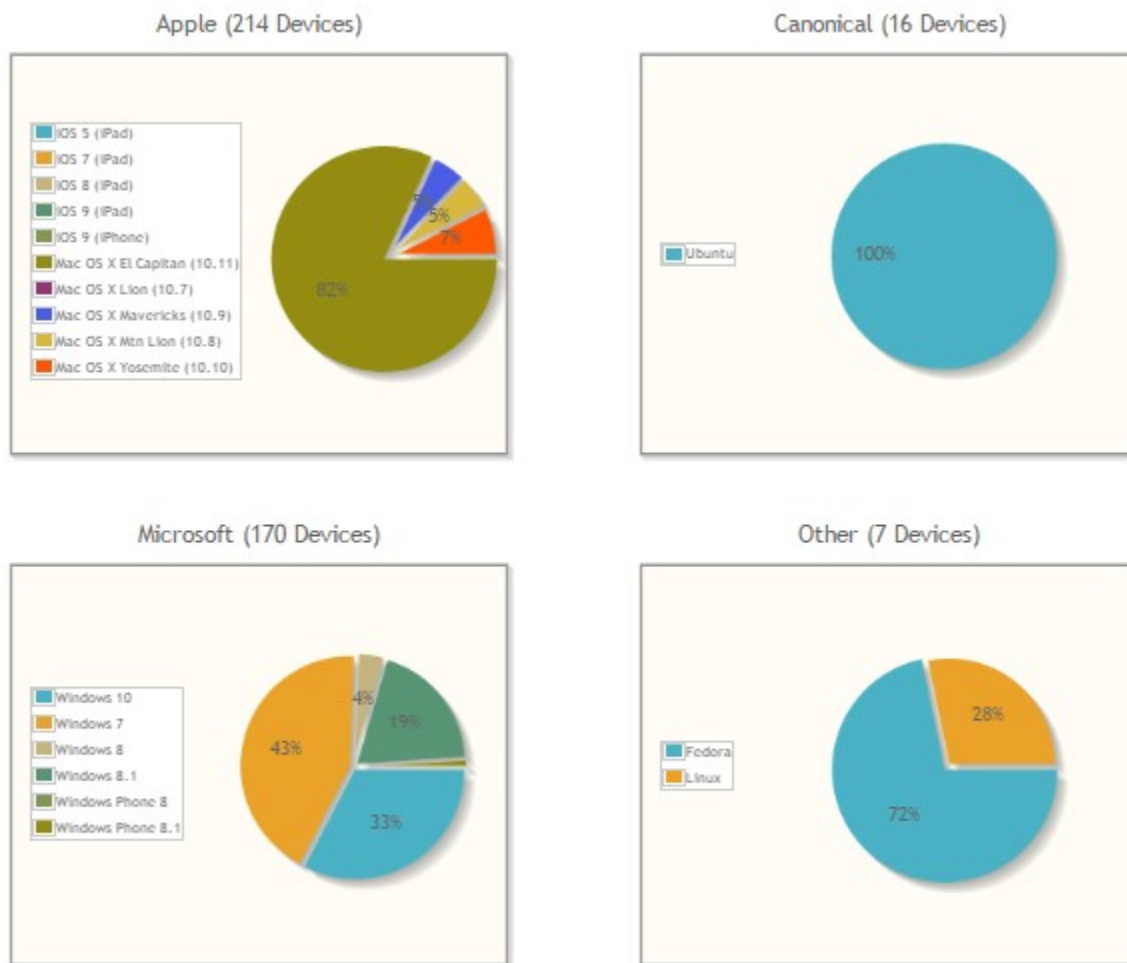
NOTE

Use the view icon to display further details about a specific user record, to block the user, or to remove the user record from the database.

Device Types

The device type information is obtained from user-agent during the initial enrollment attempt. The device types graphs show the enrollments by operating system.

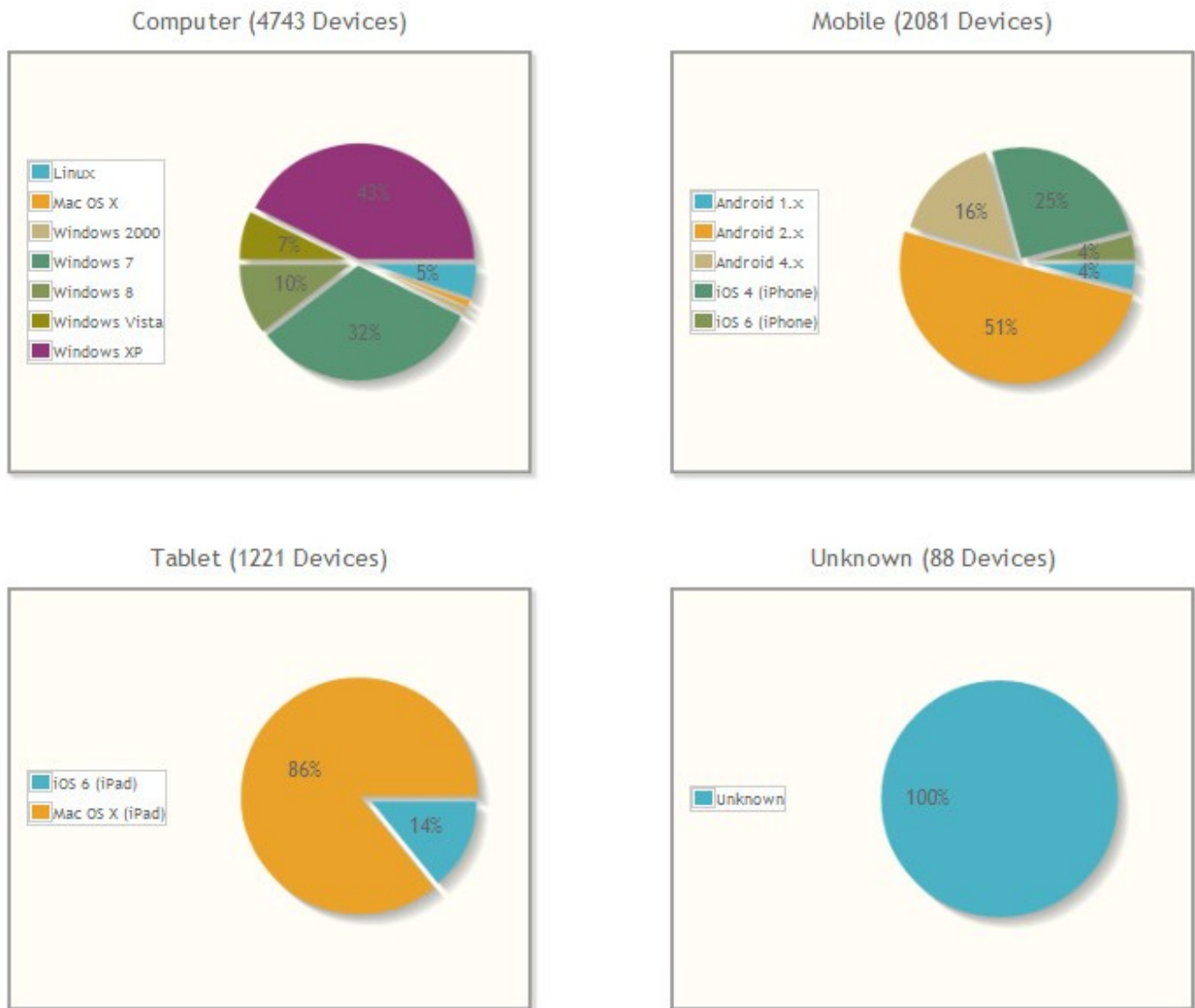
FIGURE 48 Device Types



Form Factors

The form factor is obtained from the device user-agent during the initial enrollment attempt. The form factor graph displays the device type, such as computer, tablet, or mobile phone.

FIGURE 49 Device Form Factors



MAC Registrations

The **MAC Registration** table displays all devices that have been registered using the MAC address instead of being enrolled using a certificate.

Certificates

Cloudpath issues client certificates to users based on the templates set up for specific users and devices. Server certificates can be issued for the RADIUS server, web server, or other external server in your network. The active certificates graph displays, by date, the number of active (not expired) client and server certificates, and from which template they were issued

Certificates Table

The Certificates table lists all server and client certificates issued by the onboard CA. Use the **Active**, **Revoked**, **Expired**, and **All** tabs to filter the data in the table.

FIGURE 50 Certificates Table

Search	Status	Contact Name	Issuance	Expiration Date	CA Name	Template	Email	Revocation Code	Type/Name	Exp. On/Off Date
Q X	●	mark@byod.company.com	20140402 1056 MDT	20150402	Anna Test Intermediate CA 1	username@byod.company.com			52CD...C610	20140402 1056 MDT
Q X	●	anna@byod.company.com	20140402 1054 MDT	20150403	Anna Test Intermediate CA 1	username@byod.company.com			18CC...1827	20140402 1054 MDT
Q X	●	anna@byod.company.com	20140401 1415 MDT	20150401	Anna Test Intermediate CA 1	username@byod.company.com			AAS1...E2DA	20140401 1415 MDT
Q X	●	lynn@byod.company.com	20140401 1402 MDT	20150401	Anna Test Intermediate CA 1	username@byod.company.com			D472...768D	20140401 1402 MDT
Q X	●	bill@byod.company.com	20140401 1351 MDT	20150401	Anna Test Intermediate CA 1	username@byod.company.com			EC14...1554	20140401 1351 MDT
Q X	●	AnnaTest.cloudpath.net	20140401 1342 MDT	20170401	Anna Test Root CA 1	Server-Templates	it@company.com		82D4...43E1	20140401 1342 MDT

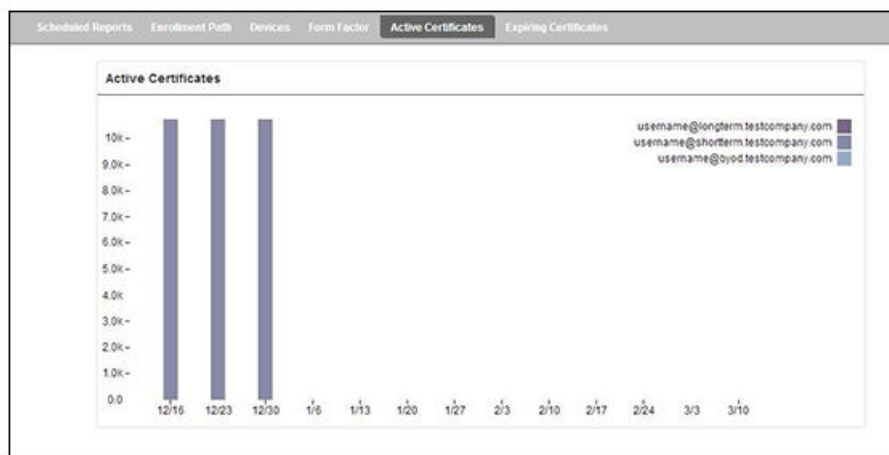
NOTE

Use the view icon to display further details about a specific certificate record, to disable or revoke the certificate, to download the certificate, or to remove the user record from the database.

Active Trends

The **Active Certificates** graph displays, by date, the number of active (not expired) client and server certificates, and from which template they were issued.

FIGURE 51 Active Certificates



Expiring Trends

The validity period of certificates issued by Cloudpath is derived from the certificate template used when the certificate was issued. The **Expiring Certificates** graph displays, by date, the number of client and server certificates that are about to expire, and from which template they were issued.

FIGURE 52 Expiring Certificates



Notifications

The **Notifications** tab allows you to review emails and SMS messages, event logs, and schedule reports.

Notification Records

The **Notifications** table displays email and SMS notifications that have been sent by the system. The system logs email and SMS notifications sent for sponsors, messages for vouchers, network access, and certificate issuance or revocation.

FIGURE 53 Notifications Table

Type	Address	Last Known Status	Timestamp	Email Subject
EMAIL	anna@cloudpath.net	Email sent.	20140401 0913 MDT	Verification Code for Network Access
EMAIL	anna@cloudpath.net	Email sent.	20140401 0841 MDT	text notification

Events

The **Events** log displays all system events, such as account logins, enrollments, acceptance of AUPs, registrations, certificate issuance, errors, account updates, and snapshot creation.

Schedule Reports

The scheduled report feature allows you to schedule a task to export enrollment record data, by date, or schedule a recurring export. For example, you might schedule an enrollment data report to occur on a weekly, or daily basis. This report can be emailed to one or multiple email addresses.

You can schedule multiple reports. For example, you can create a report that emails an enrollment record report based on enrollments with revoked certificates, and another based on issued certificates.

To schedule a task:

1. Go to **Dashboard > Notifications > Scheduled Reports**.
2. On the **Scheduled Reports** page, click **Add Scheduled Report**.

FIGURE 54 Schedule Enrollment Records Export

3. On the **Modify Scheduled Report** page, enter the **Name**, **Description**, **Email Address** and **Subject** for the recipient of the enrollment records report. You can enter multiple email addresses, separated by commas.
4. Specify when task is to be run. The execution period can be a specific date or you can set up a recurring report to be emailed daily, weekly, or monthly.
5. In the **Enrollment Status To Include** section, check the information to be included in the report. For example, select **Certificate Issued** and **Enrollment Complete** to create a report that shows the number of devices that have successfully onboard to the network.
6. Specify the **Report Content**, which determines the data columns that will be included in the report.
7. **Save** the scheduled task.

FIGURE 55 Scheduled Report

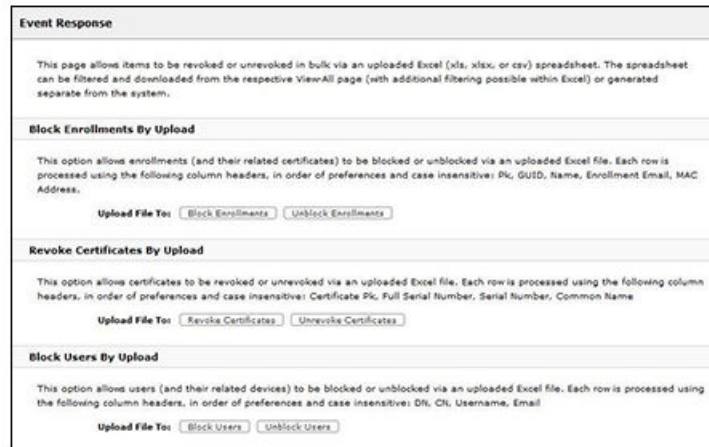
Name	Frequency	Time
Abandoned Enrollments - Monthly	Monthly	Executing once on 04/30/2014 at 12:00 AM
Daily Expired	Every day	at 8:00 AM
Weekly Enrollments	Every week	at 7:00 AM

The enrollment record data is emailed, as a CSV file, to the specified address, at the scheduled frequency. You can also download an interim report from this page.

Event Response

Use the **Event Response** page to block a large number of enrollments or users, or revoke certificates in bulk using information in an uploaded Excel (xls or xlsx) spreadsheet.

FIGURE 56 Event Response



The Excel spreadsheet, which is a file of enrollment records, can be filtered and downloaded from the **Dashboard > Enrollments** (or Certificates) page, allows you block/unblock users or enrollments, or revoke/unrevoke certificates.

Support

- [Overview.....](#) 75

Overview

The **Support** tab provides links to technical documentation, information related to product licensing and statistics, diagnostics, and a process for uploading a support file, if needed.

Documentation

The **Documentation** page contains technical documents for getting the system set up, integration with other systems, managing the system, and special configuration instructions. This page also provides links to the most commonly used pages in the Cloudpath Admin UI.

Licensing

The **Licensing** page displays information about the type and number of Cloudpath licenses, active certificates, usage statistics, and copyright notices.

FIGURE 57 Licensing Information Page

The screenshot displays a web interface for licensing information, organized into four main sections:

- License Information:** Shows licensee 'Jeff Test', license type 'Subscription' (active through 20200915), customer ID 'XPC-CPN-00114', support link 'https://support.ruckuswireless.com/', and a 'Contact Sales' button.
- System Utilization:** Shows 1 total user license and 1 consumed. Active certificates include 2 currently active, with breakdowns by issuance period (Last 30, 60, 90 days, and Last Year).
- License Server:** Shows server URL 'https://bvt.cloudpath.net', link status 'Advanced' (since 20190807 0858 MDT), and GUIDs for customer and system.
- Notices:** Includes Open Source, Patent, and Copyright notices.

What Happens If More Licenses Are Being Consumed Than Have Been Allocated?

Licenses are counted as follows:

- Each active user consumes one license, no matter how many devices are linked to a specific user account.
- Each active device where no user is linked to that device also consumes one license.

The following Licensing Information page shows an example of the number of total user licenses consumed exceeding the number of total user licenses for an existing Cloudpath system:

FIGURE 58 Example of Total User Licenses Consumed Exceeding Limit

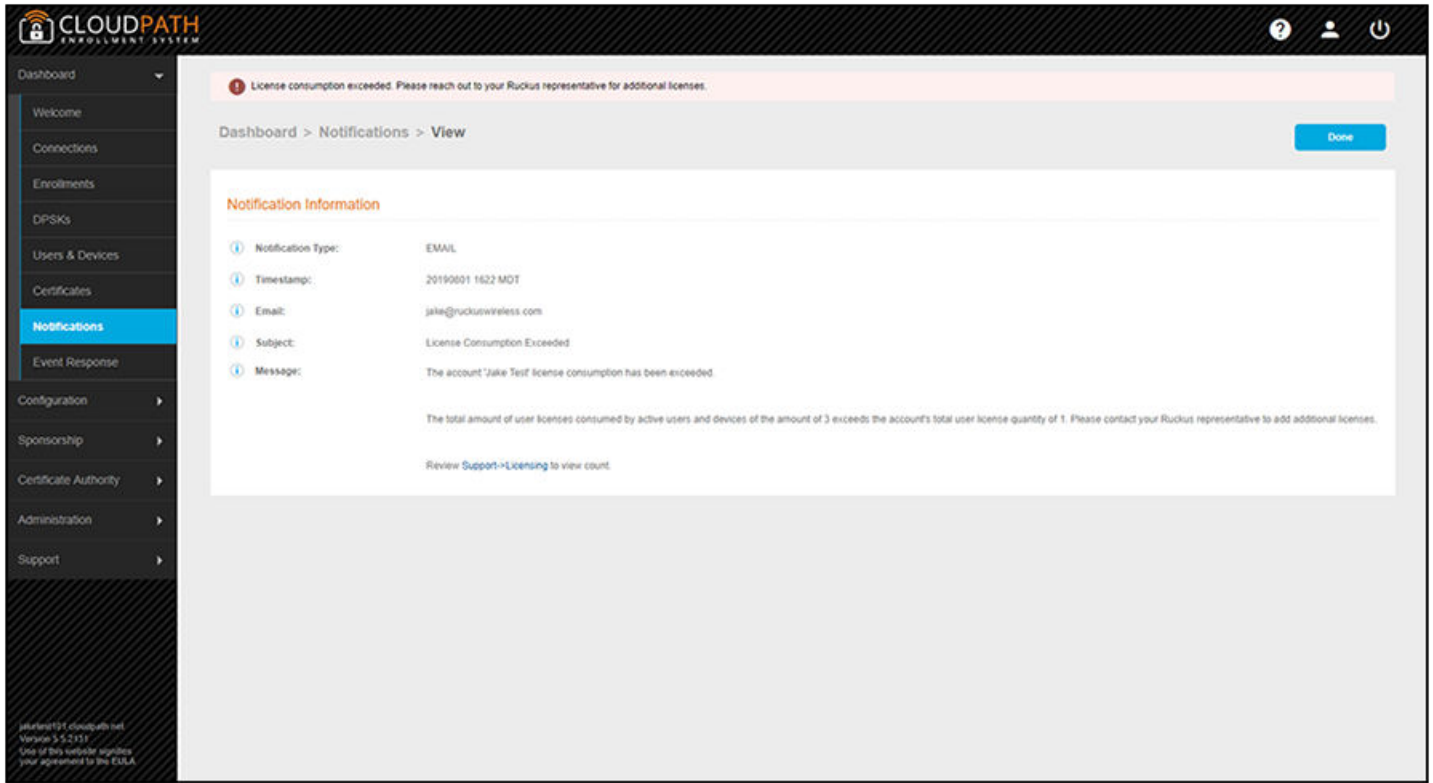
System Utilization	
Total User Licenses:	30 users
Total User Licenses Consumed:	50 users
Active Certificates:	104 Currently Active
	104 Issued In Last 30 Days
	104 Issued In Last 60 Days
	104 Issued In Last 90 Days
	104 Issued In Last Year
AD/LDAP Users:	50 Total
Email Count:	5 In Last 90 Days

When this situation occurs, the account is flagged at midnight, and you receive an email notification. The next time you log in to your Cloudpath system, a banner indicating that the license consumption has exceeded the maximum number of allowed licenses will appear, and the email that was sent will also appear in your Notifications (see the two figures below). The banner continues to appear, followed by monthly email notifications, until the situation has been resolved with your Cloudpath support representative. Once the situation has been resolved, the banner will be removed the next day, and monthly email notifications will no longer be sent.

FIGURE 59 License-Consumption Banner on Welcome Page When Consumption Exceeds Limit

The screenshot displays the Cloudpath ES web interface. At the top left is the logo for Cloudpath Enrollment System. A dark sidebar on the left contains a navigation menu with items: Dashboard, Welcome, Connections, Enrollments, DPSKs, Users & Devices, Certificates, Notifications, Event Response, Configuration, Sponsorship, Certificate Authority, Administration, and Support. The main content area features a red banner at the top with a warning icon and the text: "License consumption exceeded. Please reach out to your Ruckus representative for additional licenses." Below the banner is a "Welcome to the Cloudpath ES" section. It includes a paragraph about the Automated Device Enablement (ADE) approach, a "Getting Started" section with instructions on using the left menu, and a diagram illustrating the network architecture. The diagram shows an "Onboarding Network" connected to a "LAN (Ruckus Network)" and a "WLAN (Ruckus Network)". The LAN and WLAN are connected to a "Secure Network". A "RADIUS" server is connected to the LAN and WLAN. A "Mobile Network (3G/4G)" is connected to the WLAN. A "Cloud" icon is also shown. At the bottom left of the page, there is a footer with the text: "jakelst101.cloudpath.net", "Version 5.5.2131", and "Use of this website signifies your agreement to the EULA".

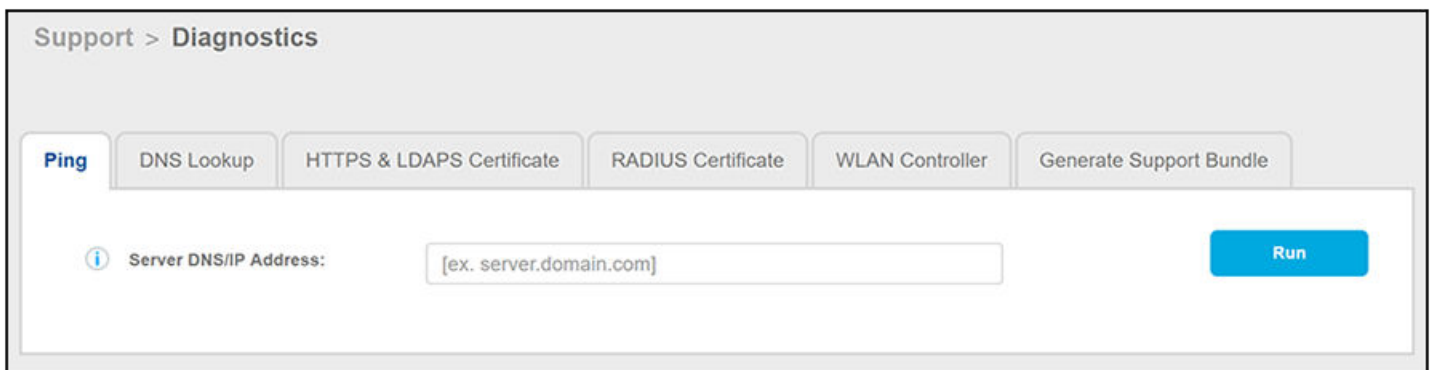
FIGURE 60 License-Consumption Banner in Notifications When Consumption Exceeds Limit



Diagnostics

The Diagnostics page provides useful tools for system troubleshooting connectivity issues and for verifying certificate information.

FIGURE 61 Cloudpath Connectivity Diagnostics



The diagnostics include:

- Ping: Ping an IP address or hostname
- DNS Lookup: Provide server information and IP address for a given hostname.

- HTTPS & LDAPS Certificate: Query the server certificate used by a secured server (such as HTTPS or LDAPS) to verify the certificate currently in use by a server.
- RADIUS Certificate: Query the RADIUS server certificate and the chain presented by the RADIUS server. This is useful to verify the certificate currently in use by a RADIUS server. For this test to work, Cloudpath must be able to reach the IP and port, the shared secret must be correct, and Cloudpath must be an approved client for the RADIUS server.
- WLAN Controller: Query the WLAN controller to check if required ports are accessible.
- Generate Support Bundle: Click **Run** from this tab to generate a zip file that contains log files and metrics information to provide to your Ruckus support representative.

Upload Support File

If Cloudpath support has provided a support file, you can upload it on this page. This will make changes to the system, so it is recommended that you first create a VMware snapshot.

NOTE

Only use a support file with the assistance of the Cloudpath Support team.

Cloudpath Video Tutorials

In addition to the complete Cloudpath documentation set located on the <https://www.support.ruckuswireless.com> website, you can also refer to a number of Cloudpath instructional videos located on youtube

The table below provides links to these videos as well as a summary of each one. You can check the summary descriptions to determine which videos would apply to your environment.

NOTE

The videos listed below do not depict the most recent version of Cloudpath (therefore you will see differences in logos and some configuration screens), but the instructional information presented in the videos is still applicable.

Title	Link	Summary
On-Premise Installation	https://www.youtube.com/watch?v=8Sla4dA4otY	On-premise installation where customers host their own Cloudpath system is the most common installation. This is done either with VMWare or Hyper-V. This video covers VMWare installation. The video goes through prerequisites, obtaining and installing the OVA file in your VMWare environment, activating the Cloudpath system, initial system setup, and basic workflow setup including active directory authentication-server configuration.
Off-Premise (Cloud) Installation	https://www.youtube.com/watch?v=pKRbyz_WxNg	This video covers an installation where Ruckus Networks hosts the Cloudpath system in the cloud for the customer. It goes through activating the Cloudpath system, initial system setup, and basic workflow setup including active directory authentication-server configuration.
Integrating Cloudpath with a SmartZone Controller	https://www.youtube.com/watch?v=ckERq_ktY14&list=PLWS1OkMTACNxNMij5ShBD_ZL5TFbloNbE&index=4	This video demonstrates the configuration on a SmartZone controller and the corresponding configuration in the Cloudpath UI for controller integration. It includes configuring an authentication server, an accounting server, a hotspot (WISPr) portal, a walled garden, an onboarding SSID, and a secure SSID.
Management Interface Overview and Setting Up an Admin Account	https://www.youtube.com/watch?v=nATdbfa9cek&list=PLWS1OkMTACNxNMij5ShBD_ZL5TFbloNbE&index=2	This video demonstrates the configuration on a SmartZone controller and the corresponding configuration in the Cloudpath UI for controller integration. It includes configuring an authentication server, an accounting server, a hotspot (WISPr) portal, a walled garden, an onboarding SSID, and a secure SSID.
Management Interface Overview and Setting Up an Admin Account	https://www.youtube.com/watch?v=nATdbfa9cek&list=PLWS1OkMTACNxNMij5ShBD_ZL5TFbloNbE&index=2	This video provides a brief tour of the Cloudpath user interface and shows how to set up administrator accounts.
Configuring a Workflow for Client Onboarding	https://www.youtube.com/watch?v=jBT8zbcIGuc&list=PLWS1OkMTACNxNMij5ShBD_ZL5TFbloNbE&index=3	This video provides details on creating a workflow from scratch. It covers adding steps for an acceptable use policy, creating workflow branches (or “splits”), using an active directory to authenticate a user,

Title	Link	Summary
		<p>customizing the web page display that is shown to an onboarding user, and configuring the “Result” step in a workflow to assign a device configuration and/or a certificate to the user’s device once the user has been authenticated and taken through the applicable workflow branch.</p> <p>This video includes a walkthrough of a device configuration where you select the secure SSID that has already been configured on the controller. Certificate template configuration is also shown because you can have a certificate issued to the onboarding user for future authentication when the user connects to the secure SSID. Publishing the workflow to put it into effect, then testing the user experience by going to the enrollment URL, close out this video. The user’s device is configured and the certificate is installed onto the user’s device.</p>
<p>Cloudpath Authentication Using MAC Addresses</p>	<p>https://www.youtube.com/watch?v=0WYfQo8n9E4&list=PLWS1OkMTACNxnMij5ShBD_ZL5TFbloNbE&index=5</p>	<p>This video walks you through setting up workflow branches using the plugin step called “Register device for MAC-based authentication.” For devices that do not have WPA-2 capabilities, or for limited-time usage, Cloudpath offers authentication using the device’s MAC address for limited and secure network access. Certificates are not used in this authentication. This video shows different ways in which you can use the same “Register device for MAC-based authentication” step, depending on configuration settings you choose within that plugin.</p> <p>Also shown is the use of the “Redirect the user” plug-in step to move the enrolled user to a specified external URL; this replaces the “Result” step because you don’t need a configuration or certificate installed onto the user’s device for MAC registration authentication.</p>
<p>Cloudpath Auto-Branching</p>	<p>https://www.youtube.com/watch?v=vq84JPIWS6Q&list=PLWS1OkMTACNxnMij5ShBD_ZL5TFbloNbE&index=8&t=0s</p>	<p>This video shows how to build a workflow branch that contains sub-branches that will be selected automatically by Cloudpath, based on filter criteria you configure for each sub-branch. This video shows you how to use the “First match in:” option in the workflow so that the first sub-branch (going from left to right in the workflow) where the criteria being evaluated matches what the user entered during an authentication step is used automatically.</p>
<p>Cloudpath Authentication Methods for Guest User Access</p>	<p>https://www.youtube.com/watch?v=2Ot5faLCRLM&list=PLWS1OkMTACNxnMij5ShBD_ZL5TFbloNbE&index=8</p>	<p>This video shows you how to build a workflow branch for providing guest user access. Three sub-branches are shown:</p> <ul style="list-style-type: none"> Using the “Authenticate using a voucher from a sponsor” plug-in step, which involves sending a voucher to the user.

Title	Link	Summary
		<ul style="list-style-type: none"> Using the “Perform out-of-band verification,” plug-in step, where the user receives a voucher code via email or text message. Using the “Request access from a sponsor” plug-in step, which notifies the sponsor in real time. The sponsor can approve the request, in which case the user’s enrollment continues. Note: Beginning with Cloudpath 5.6, this plug-in is called “Request access from a sponsor online” to differentiate it from a new plug-in in release 5.6 called “Request access from a sponsor offline.” <p>The video also shows creating voucher lists and adding sponsors for specific voucher lists.</p>
Customizing Your Cloudpath Onboarding Landing Pages	https://www.youtube.com/watch?v=R9MnH8kri90&list=PLWS1OkMTACNxNMij5ShBD_ZL5TFbloNbE&index=9	This video demonstrates using the “Look and Feel” tab in a workflow to change the appearance of the onboarding landing pages to suit the needs of your organization.
Creating Multiple Workflows with Cloudpath	https://www.youtube.com/watch?v=NDDuQpQyOHA&list=PLWS1OkMTACNxNMij5ShBD_ZL5TFbloNbE&index=10	This video provides examples of why you might need to use multiple workflows, and shows how to maintain them separately from each other. For instance, you might need separate workflows for users in different countries due to country code differences; this video informs you on how to use redirect URLs on the corresponding controllers.
Cloudpath Device Management	https://www.youtube.com/watch?v=hbsbBjkPtsc&list=PLySwoo7u9-KI5EgLR6XBjtjAGhd35mjyq&index=11&t=0s	This video shows you how to edit existing device configurations in the Configuration > Device Configurations area of the Cloudpath user interface. The video includes an example of using the “Network(s)” tab of a device configuration to add an additional network to which the user can connect.
Cloudpath Advanced Workflows	https://www.youtube.com/watch?v=CUDjXW2WB38	This video provides a demonstration of how to use the “Prompt the user for information” plug-in step in conjunction with the “Split users into different branches” plug-in step. Also shown are how to edit the branches to employ the use of filters that are based on the user input. You can use filters and the different “match” options to direct users down the desired workflow branch.
Configuring Notifications with Cloudpath Enrollment System	https://www.youtube.com/watch?v=FISYrz6bQiU	This video shows how to use a “Send a notification” plug-in step in a workflow. This plug-in generates a notification about the enrollment. Notification types include email, SMS, REST API, syslog and more. This step is invisible to the end-user. You are shown how you can use variables in the notification configuration, and how you can choose from a variety of notification methods from a drop-down list.

Cloudpath Video Tutorials

Title	Link	Summary
		Also shown is how to create a notification regarding the issuance of certificates from within the Certificate Authority > Manage Templates area of the Cloudpath UI.



© 2019 CommScope, Inc. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com