QUICK START GUIDE

Cloudpath Enrollment System Quick Start Guide, 5.11

Supporting Cloudpath Software Release 5.11

Part Number: 800-73253-001 Rev A
Publication Date: 16 September 2022

Copyright, Trademark and Proprietary Rights Information

© 2022 CommScope, Inc. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Contents

Cloudpath Security and Management Platform 5
- Overview 5
- Cloudpath System Specifications 6
- Prerequisites for Configuring Cloudpath 7
  - Deploying the OVA (For Local Deployments) 7
  - Setting up the Initial Account 7
  - Configuring the Workflow 8

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 37
  - Acceptable Use Policy 38
  - User Type Split 39
  - Authentication to a Traditional Authentication Server 40
  - Device Type Split 42
  - Prompt for Voucher 44
  - Device Configuration and Client Certificate 46
- Using the Timed Access Workflow Template 51
- Publishing the Enrollment Workflow 54
- How to Test a Published Workflow 57
- Cloning a Workflow 57

Administration 61
- Administration Overview 61

Administrators....61
Company Information....62
System Services....62
System Updates....63
Data Cleanup....63
Firewall Requirements....63

Configuration....65
Overview....65
Device Configurations....65
RADIUS Server....66
Authentication Servers....67
Firewalls and Web Filter Integration....67
MAC Registration Lists....67
API Keys....67

Dashboard....69
Overview....69
Connections....69
Enrollments....70
Records Export....70
Enrollment Paths....71
DPSKs....72
Users & Devices....72
Device Types....72
Form Factors....73
MAC Registrations....74
Certificates....74
Certificates Table....75
Active Trends....75
Expiring Trends....75
Notifications....76
Notification Records....76
Events....76
Schedule Reports....76
Event Response....78
VLAN Assignments....78
Traffic Monitor....78

Support....81
Overview....81
Documentation....81
Licensing....81
Diagnostics....86
Upload Support File....87

Cloudpath Video Tutorials....89

Cloudpath Security and Management Platform

- Overview..... 5
- Cloudpath System Specifications..... 6
- Prerequisites for Configuring Cloudpath..... 7

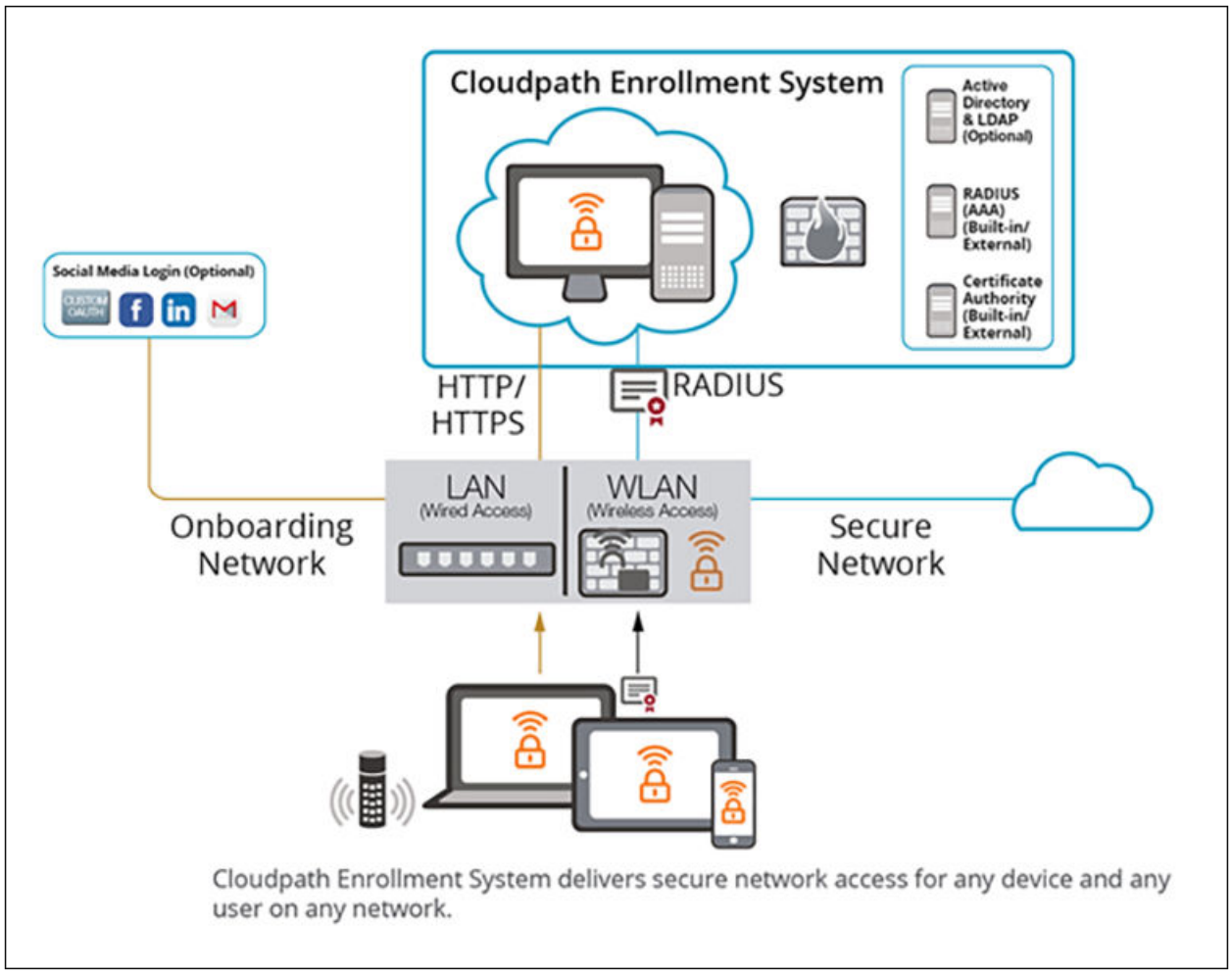
Overview

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

TABLE 1 Cloudpath System Specifications (continued)

Supported Browsers for Cloudpath Admin UI	Supported OSes for End-User Devices	Supported Third-Party Identity Stores
Safari 2.0 and later	Apple iOS 9.0 and later	Facebook
Google Chrome 3.0 and later	Ubuntu 16.04 and later	LinkedIn
	Android 6.0 and later	Google Gmail
	Fedora 24 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.

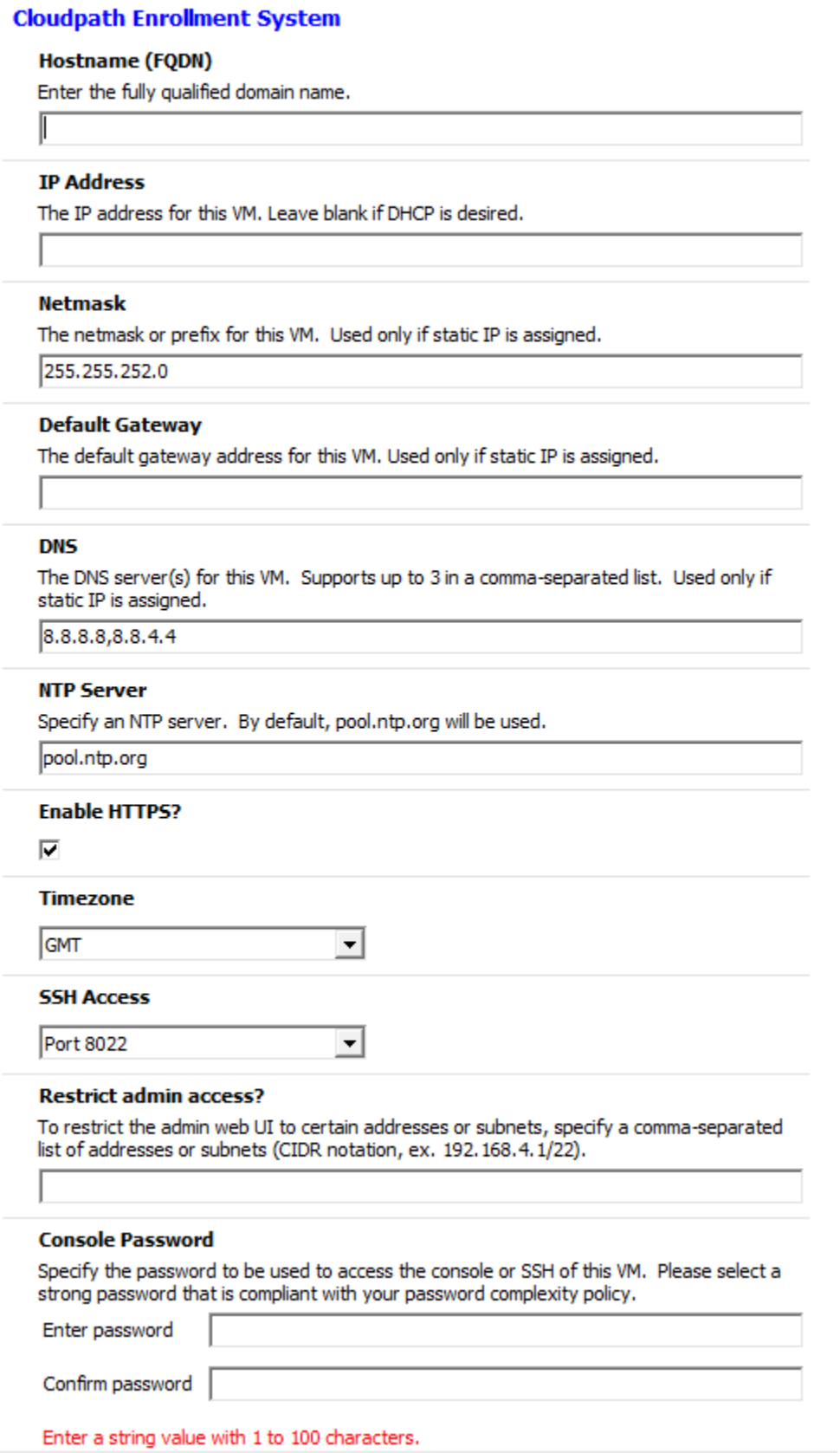
     NOTE
     If you are using Fault Tolerance, you must select **Thick** provisioning.

   - 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



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

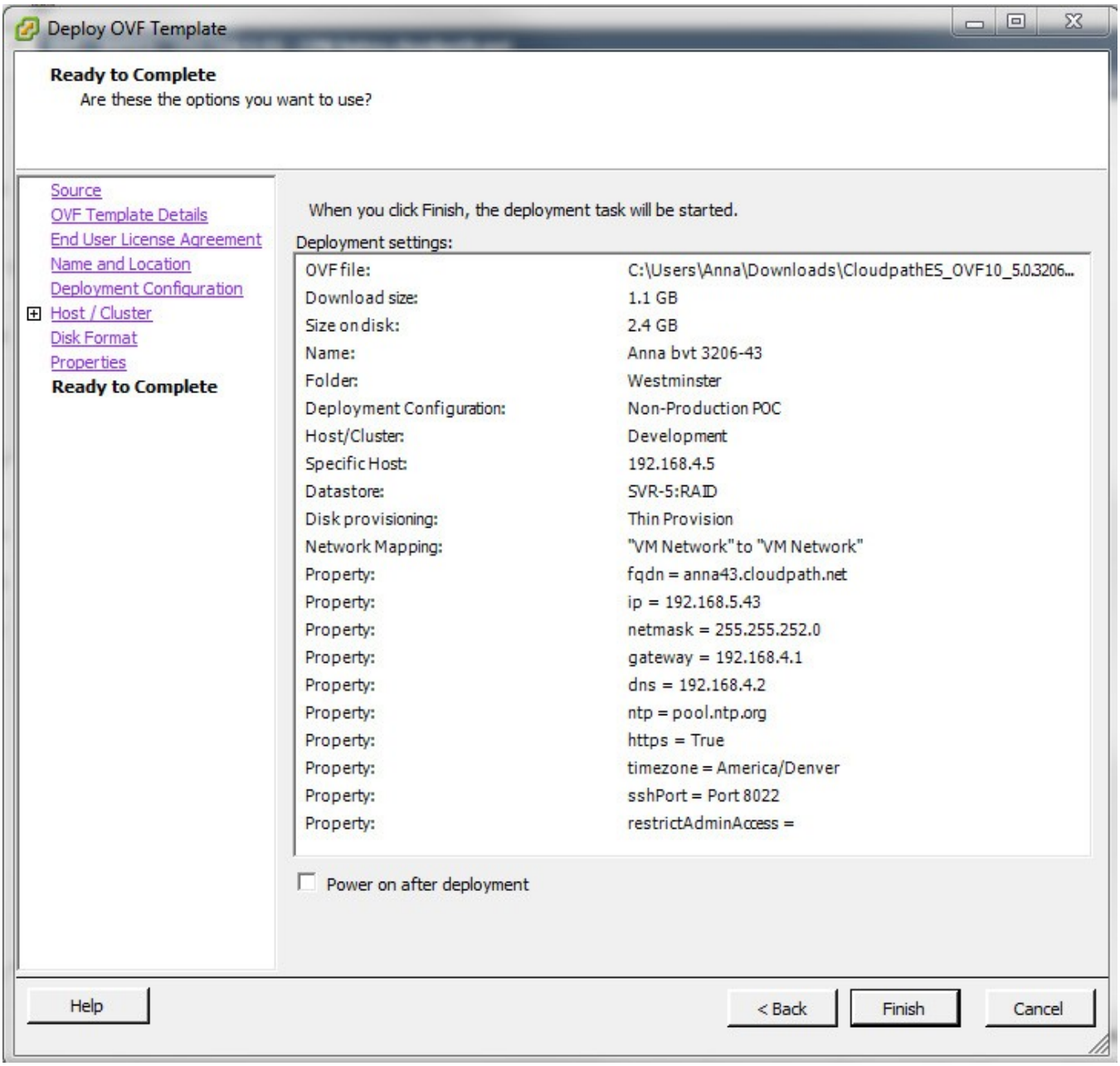
   NOTE
   The Cloudpath Hostname is used as the default OCSP Hostname, which is embedded into certificates issued by the onboard root CA as part of the URL for the Online Certificate Status Protocol (OCSP).

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* for details.

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

13. Do you want to use an NTP server other than `pool.net.org`? Enter **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* for command information.

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.

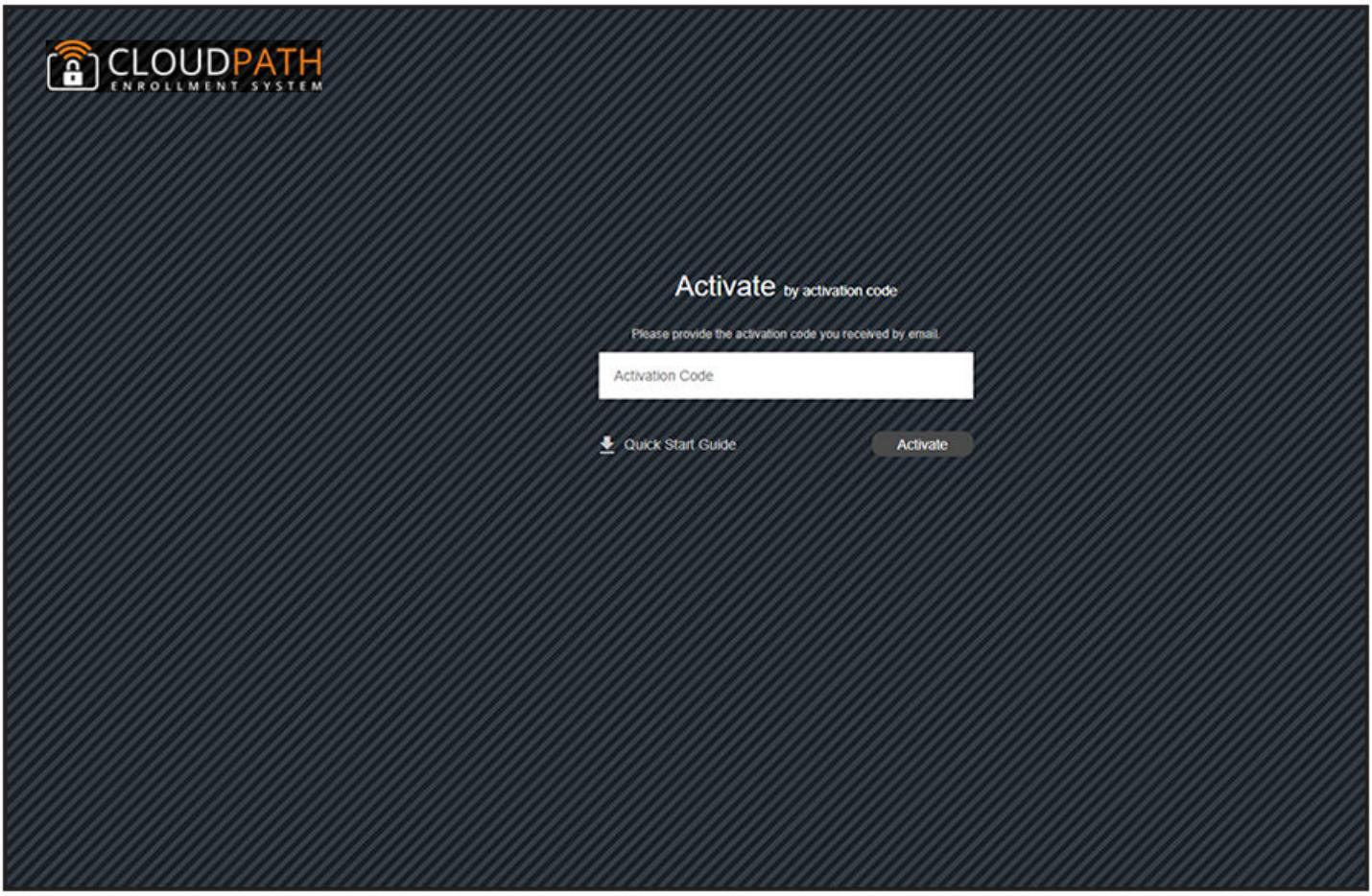
NOTE

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

Activate Account by Activation Code

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

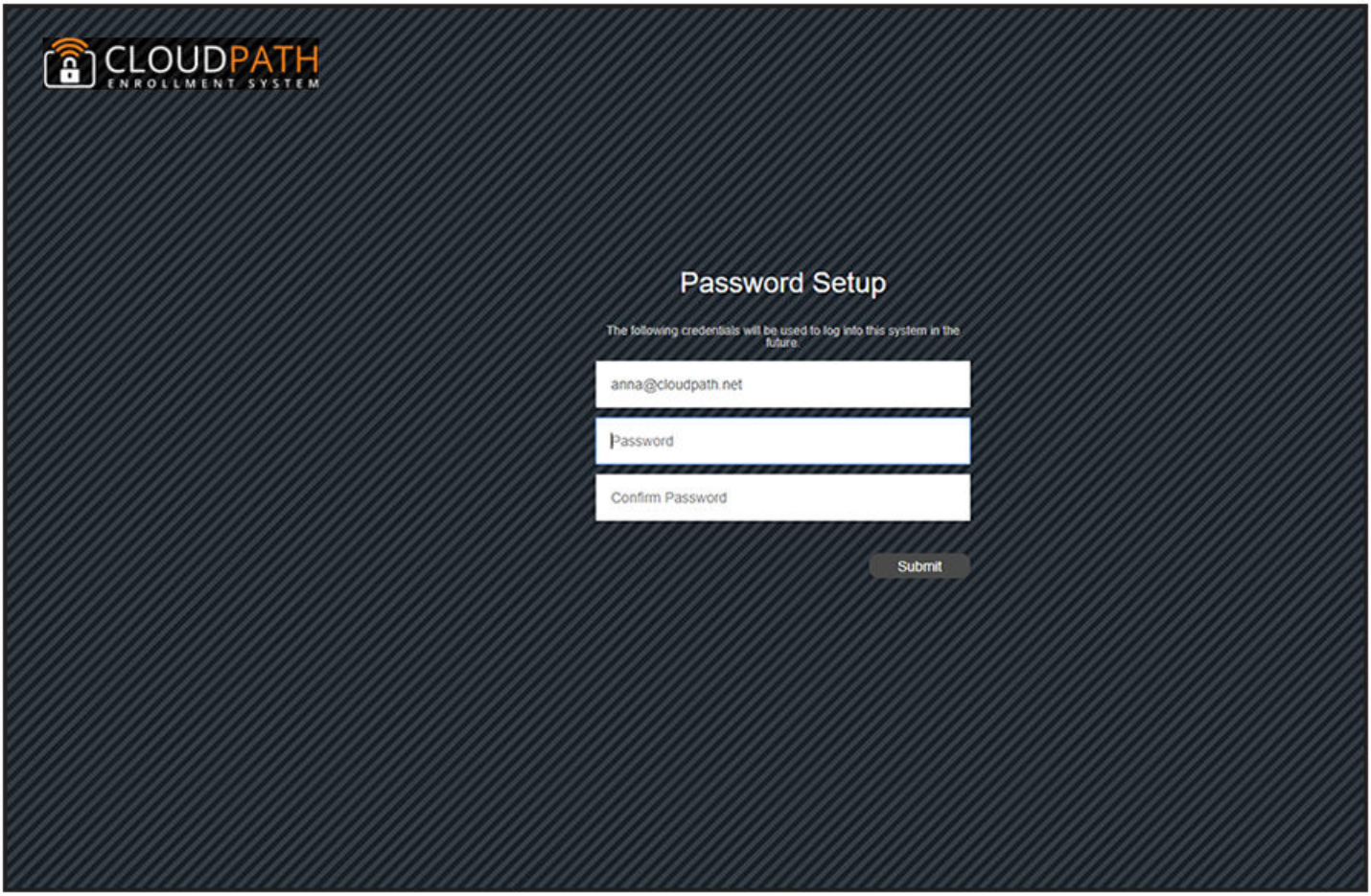
FIGURE 4 Activate Cloudpath Account



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



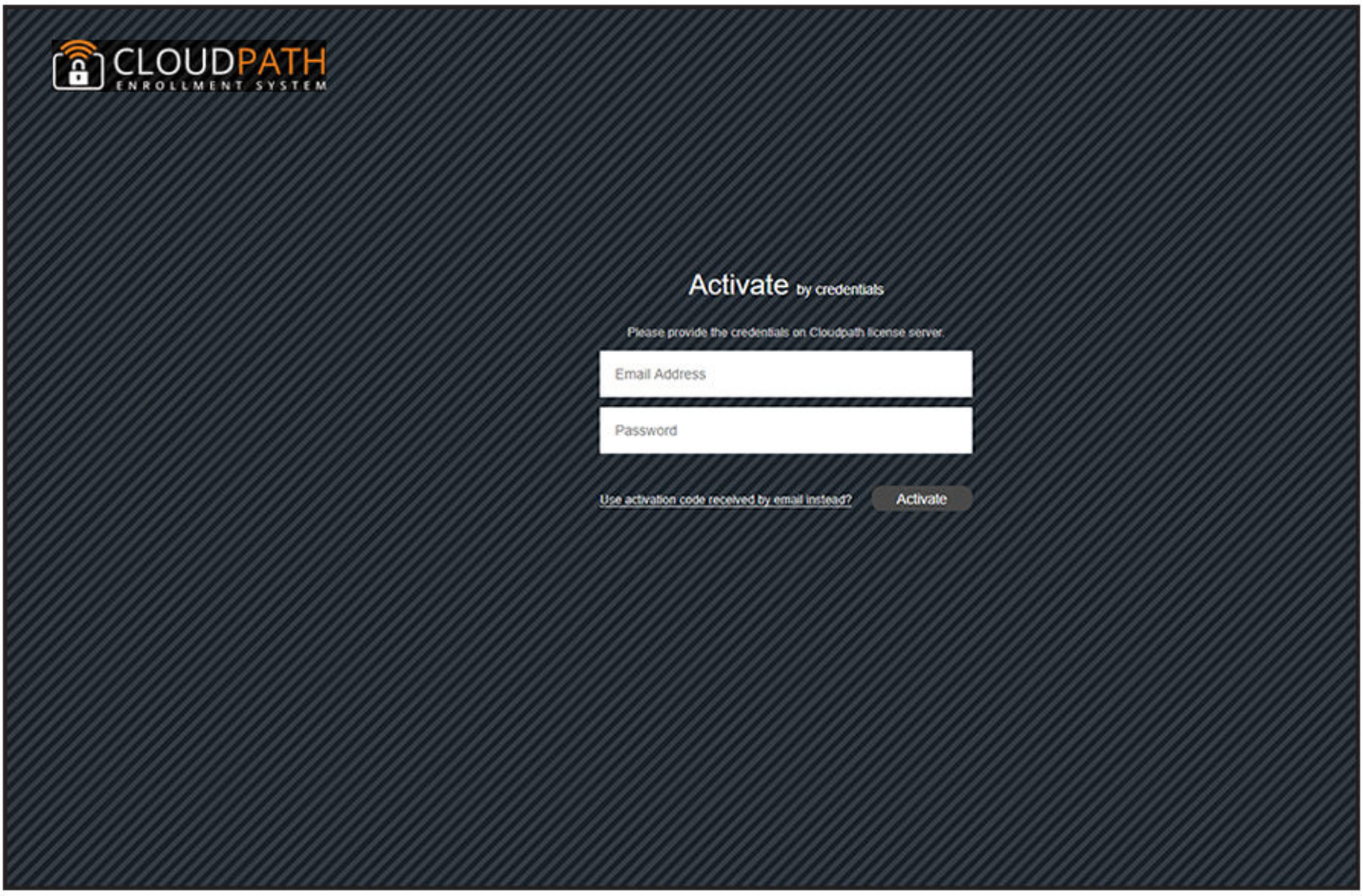
1. Your email address should display. If it does not, enter it on this page.
2. Enter and confirm a password.

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

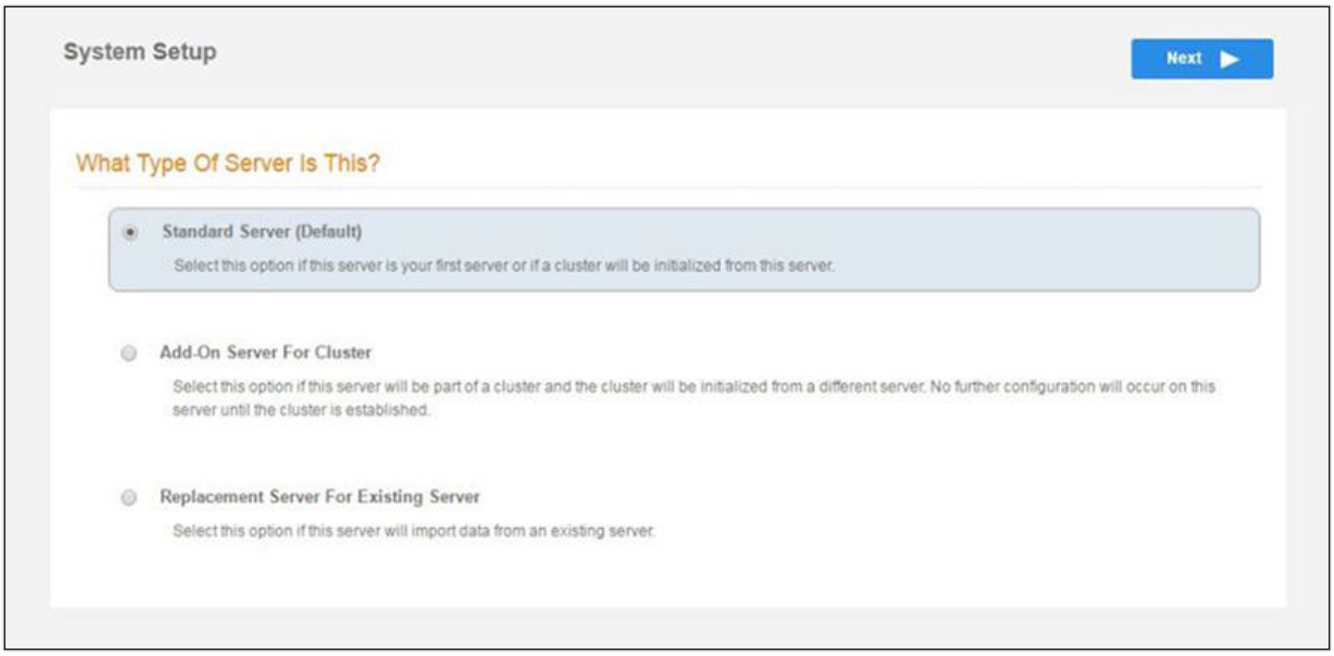
Cloudpath provides you with a single administrator login for the Cloudpath Admin UI. Additional administrators can be added from the left menu Administration tab, or you can enable Administrator logins from your authentication servers.

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.

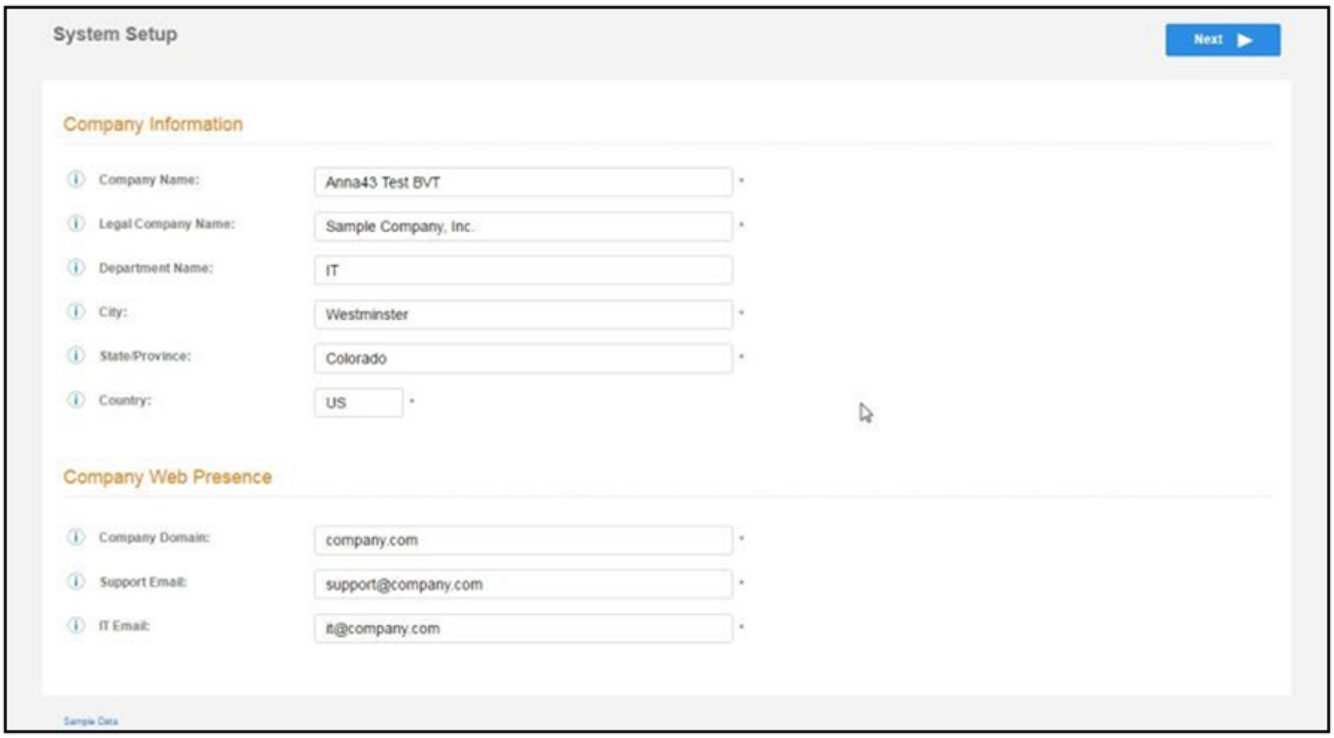
- If you are setting up this server for replication, you can choose to set the server as an **Add-On** or **Replacement** server. These selections provide an alternate set up process, requiring less information for the initial setup. **Add-On** and **Replacement** servers receive most of their configuration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

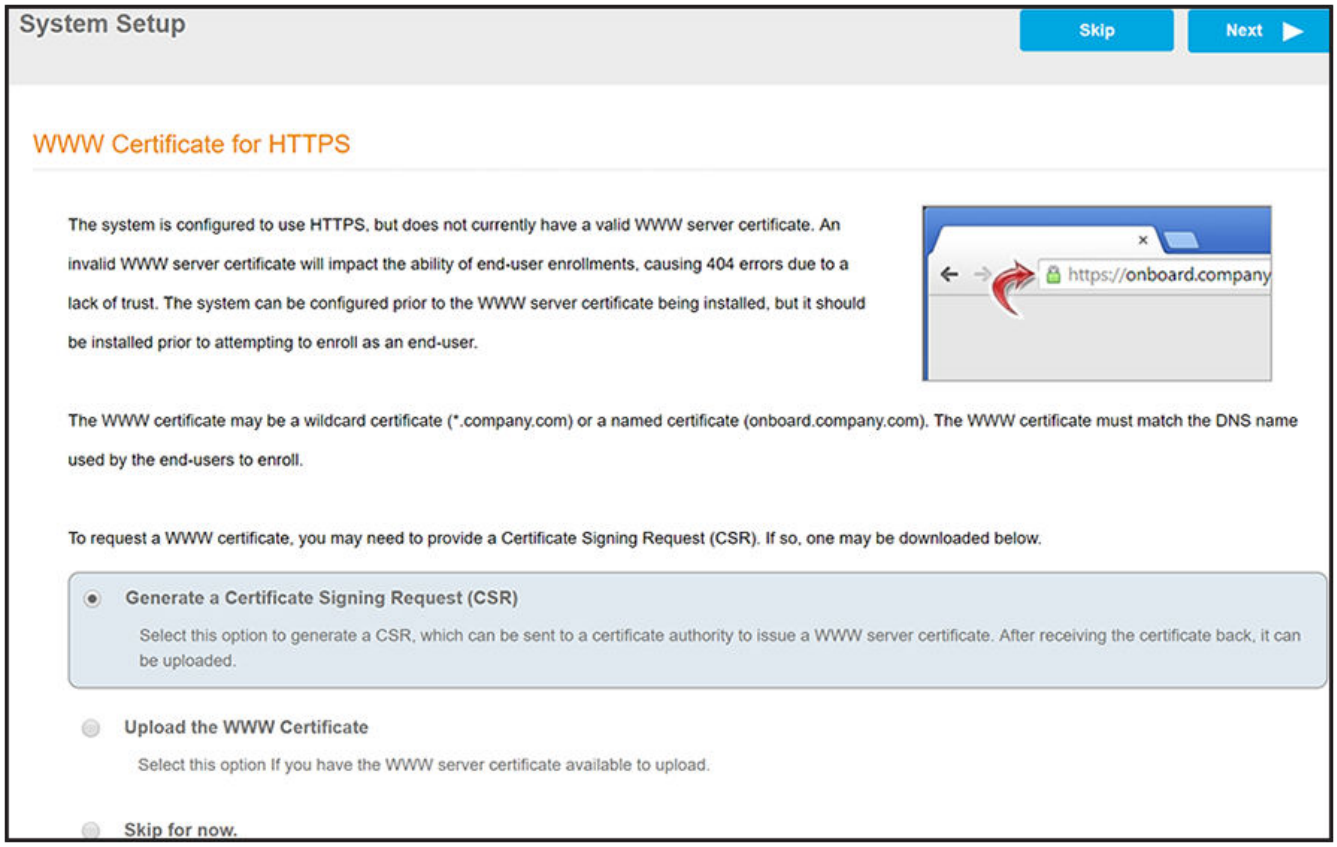
   This information is embedded in the onboard root CA certificate.

FIGURE 8 Company Information



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

FIGURE 9 WWW Certificate for HTTPS Screen

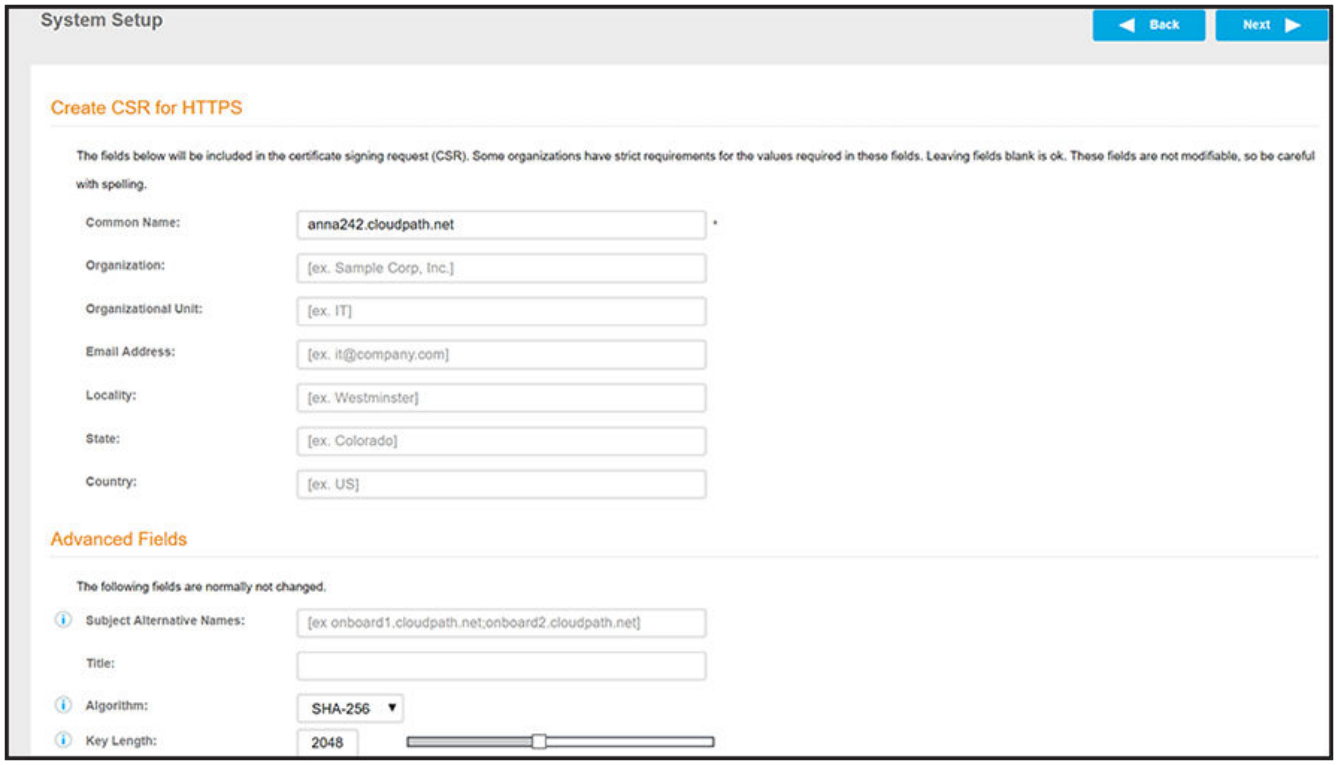


NOTE
Cloudpath supports web server certificates in P12 format, password-protected P12, or you can upload the individual certificate components: the public key, chain, and private key or password-protected private key.

- 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.

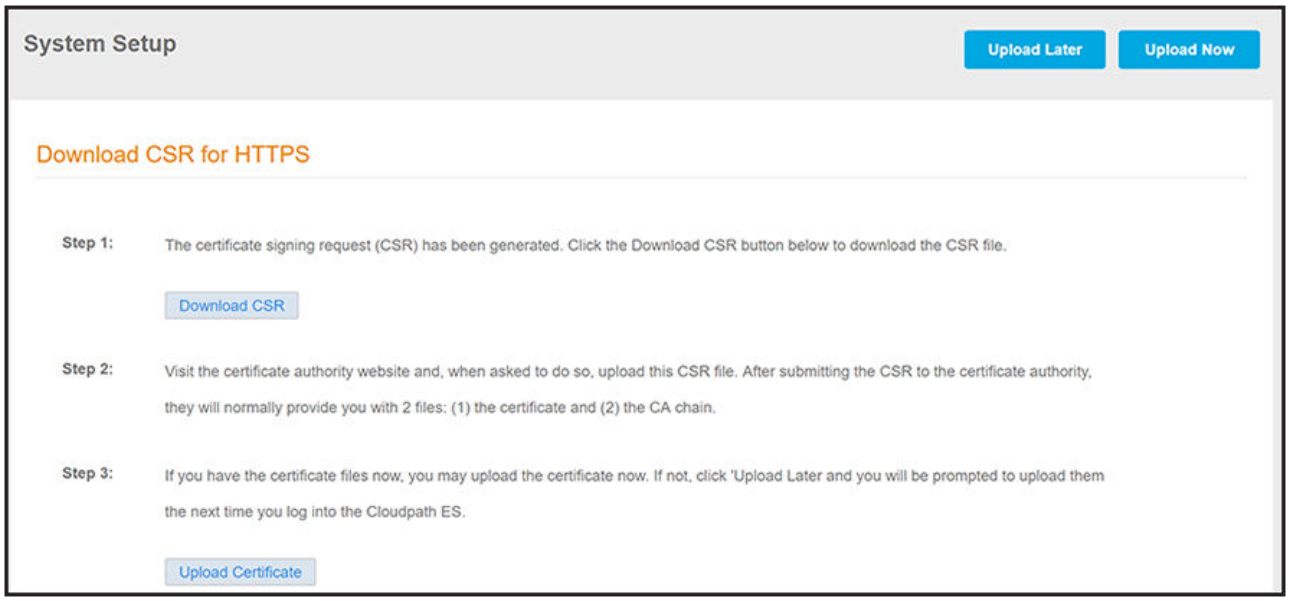
NOTE
In the Common Name field:

- 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.

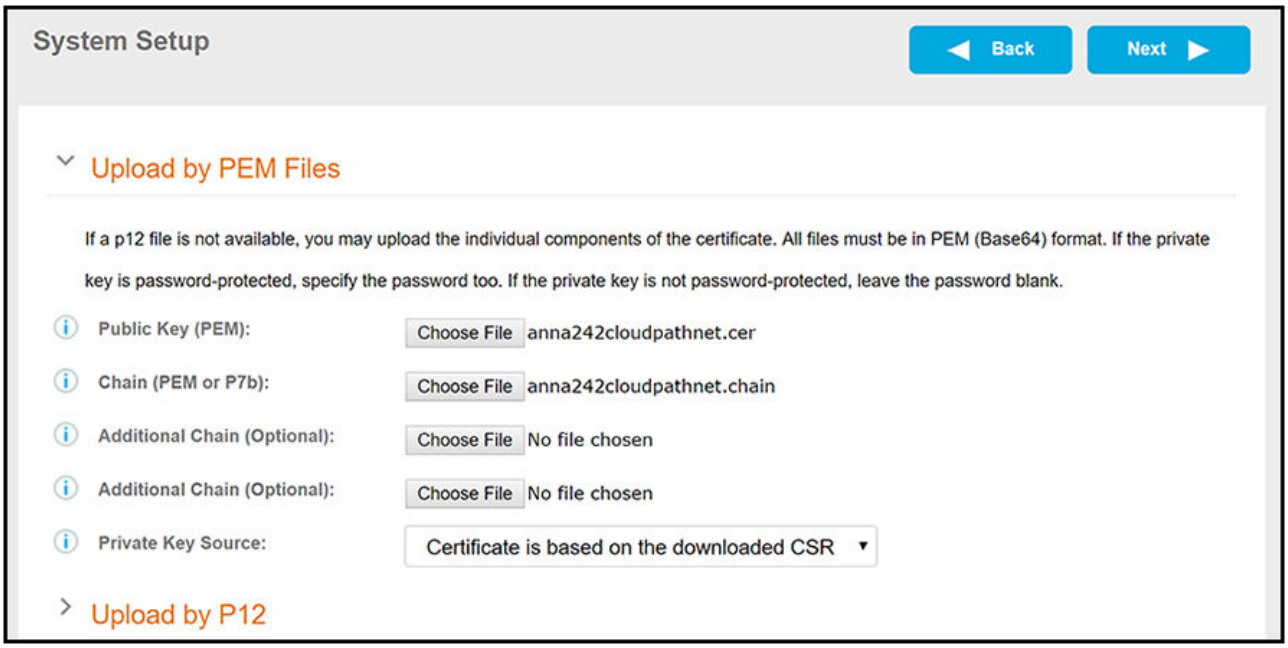
e) Follow the instructions for the CA website to download the public key and chain.

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



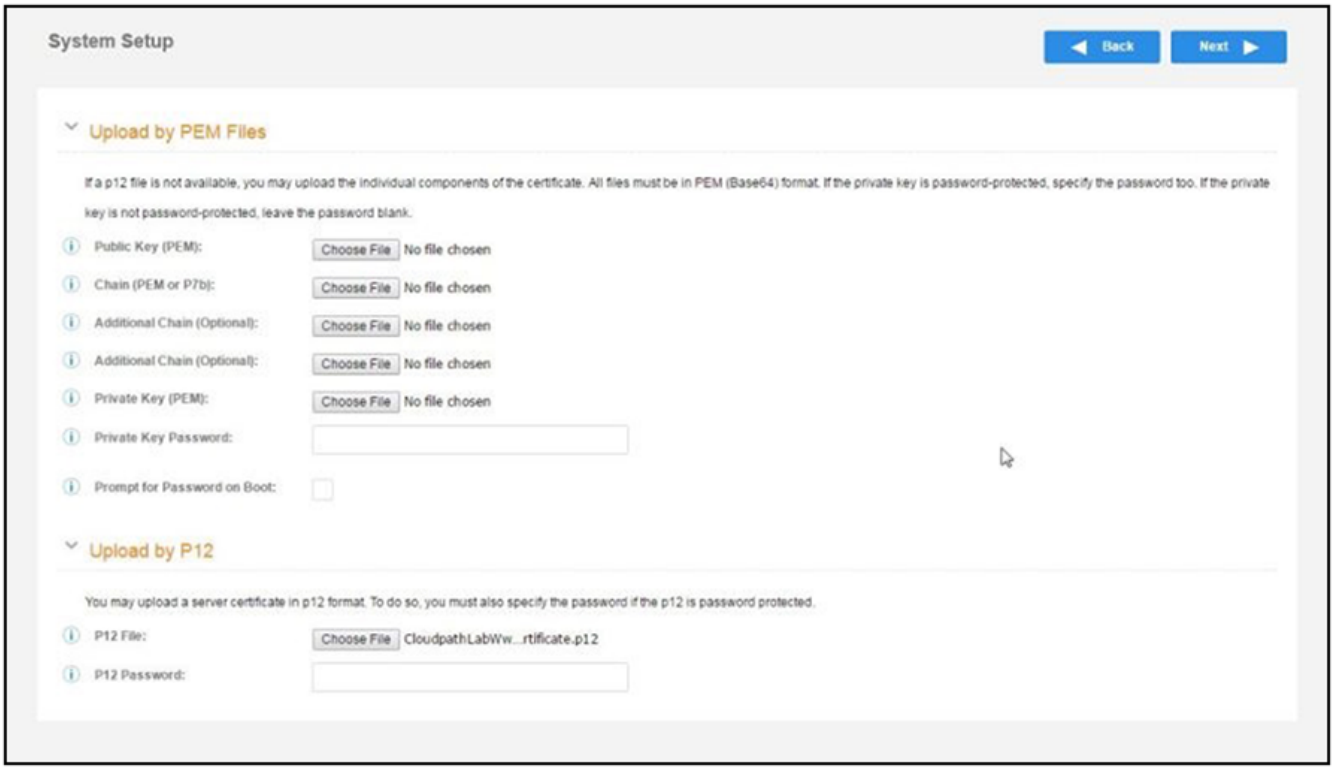
g) Upload your certificates using the screen shown above.

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



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

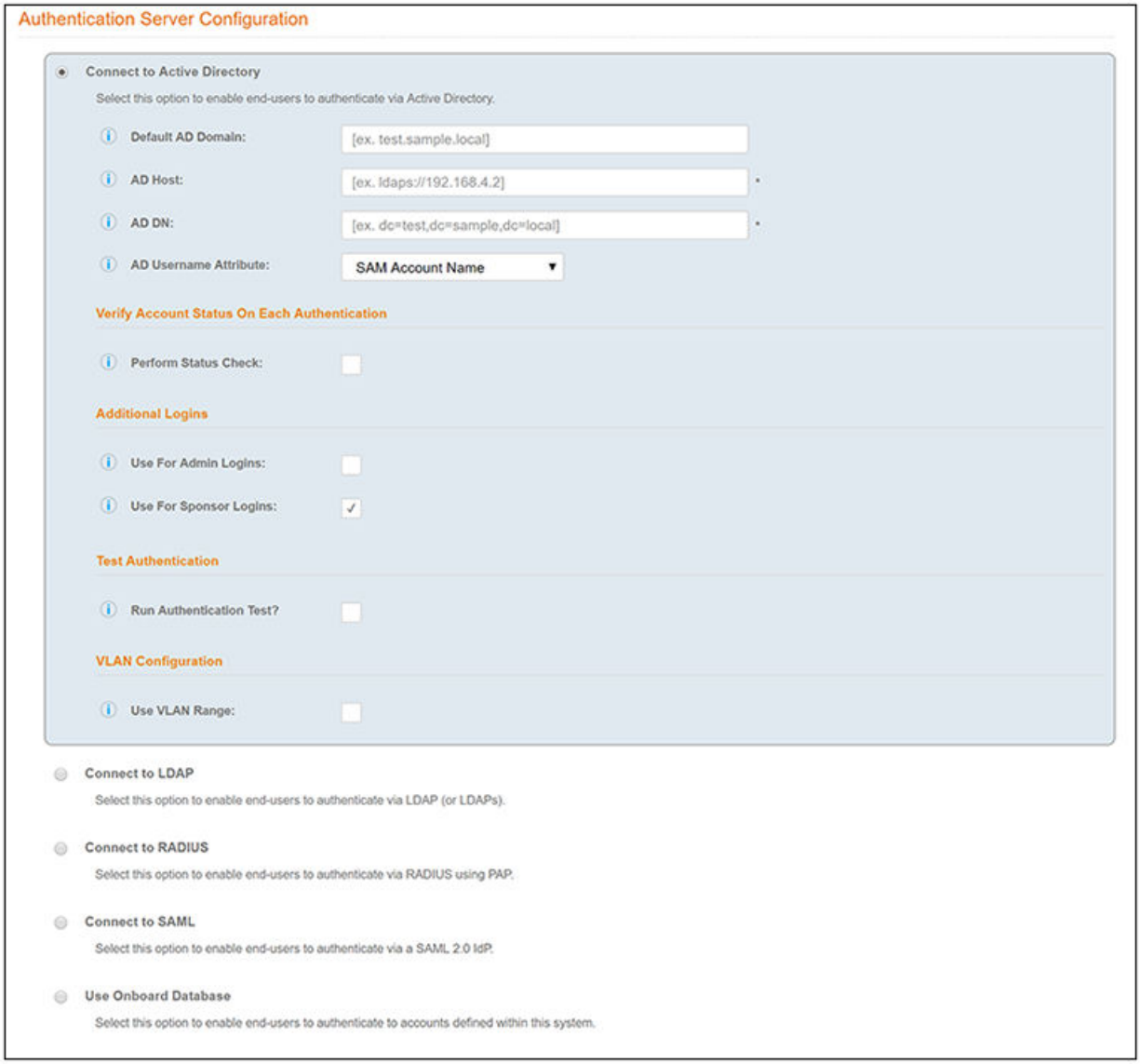
7. Configure the Authentication Server.

   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



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

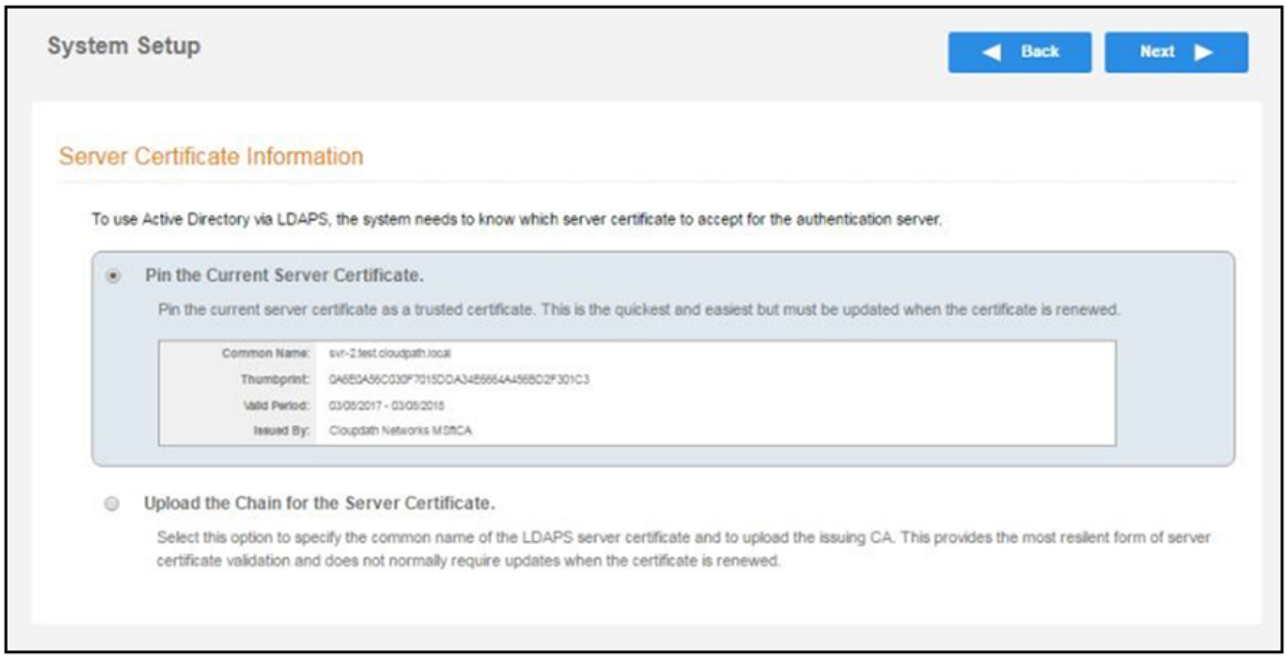
b) Consider these optional settings for the authentication server:

- **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



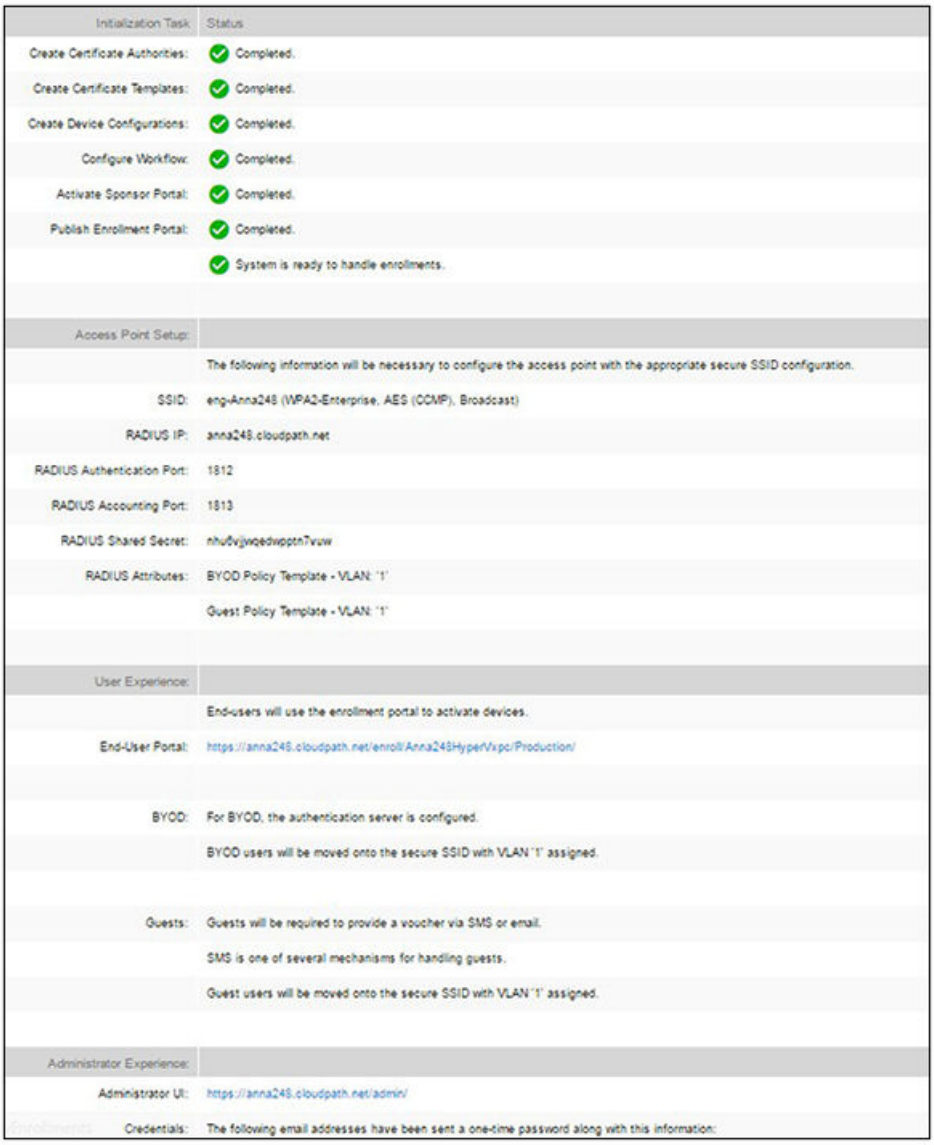
b) Select **Upload the Chain for the Server Certificate** to upload a certificate chain from an issuing CA. You must specify the common name for the LDAPS server certificate. This certificate does not need to be updated when the certificate is renewed.

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

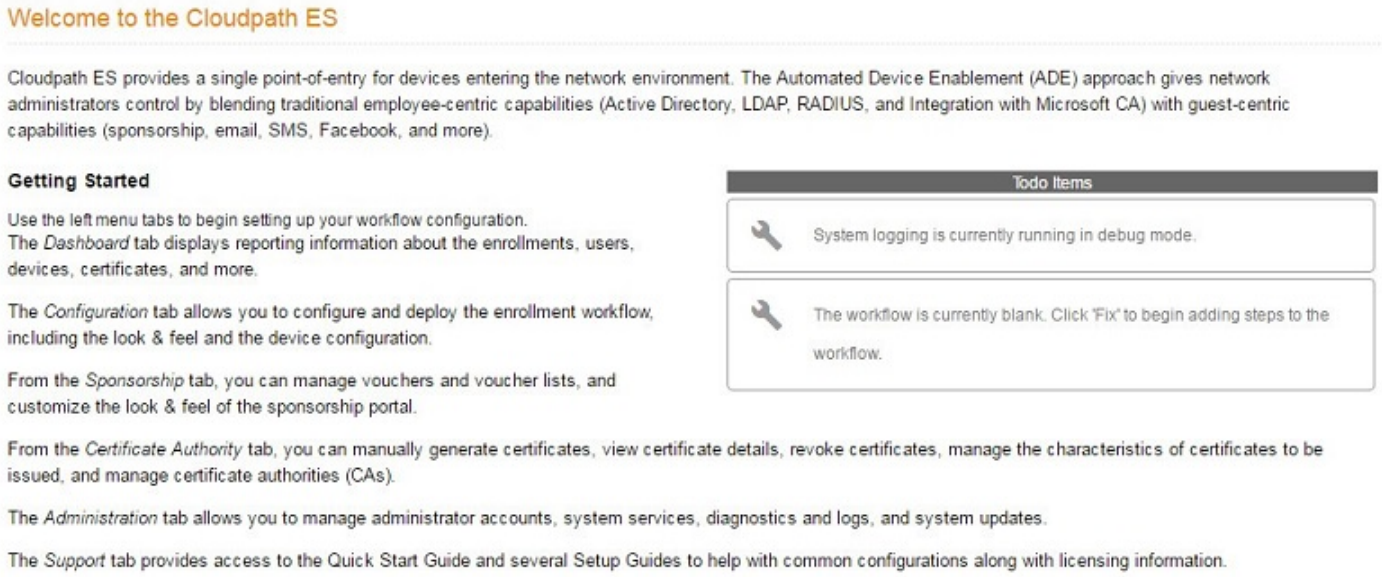


Initialization Task	Status
Create Certificate Authorities:	Completed.
Create Certificate Templates:	Completed.
Create Device Configurations:	Completed.
Configure Workflow:	Completed.
Activate Sponsor Portal:	Completed.
Publish Enrollment Portal:	Completed.
	System is ready to handle enrollments.
Access 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:	nhu6vjjwqedwpptn7vuw
RADIUS Attributes:	BYOD Policy Template - VLAN: '1'
	Guest Policy Template - VLAN: '1'
User Experience:	
	End-users will use the enrollment portal to activate devices.
End-User Portal:	https://anna248.cloudpath.net/enroll/Anna248HyperVxpc/Production/
BYOD:	For BYOD, the authentication server is configured.
	BYOD users will be moved onto the secure SSID with VLAN '1' assigned.
Guests:	Guests will be required to provide a voucher via SMS or email.
	SMS is one of several mechanisms for handling guests.
	Guest users will be moved onto the secure SSID with VLAN '1' assigned.
Administrator Experience:	
Administrator UI:	https://anna248.cloudpath.net/admin/
Credentials:	The following email addresses have been sent a one-time password along with this information:

ToDo Items

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

FIGURE 18 Cloudpath Welcome Page



Enrollment Workflow

- Overview 33
- Workflow Basics 33
- Modifying a Workflow Template 34
- Creating a Workflow From a Blank Slate 37
- Using the Timed Access Workflow Template 51
- Publishing the Enrollment Workflow 54
- How to Test a Published Workflow 57
- Cloning a Workflow 57

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.

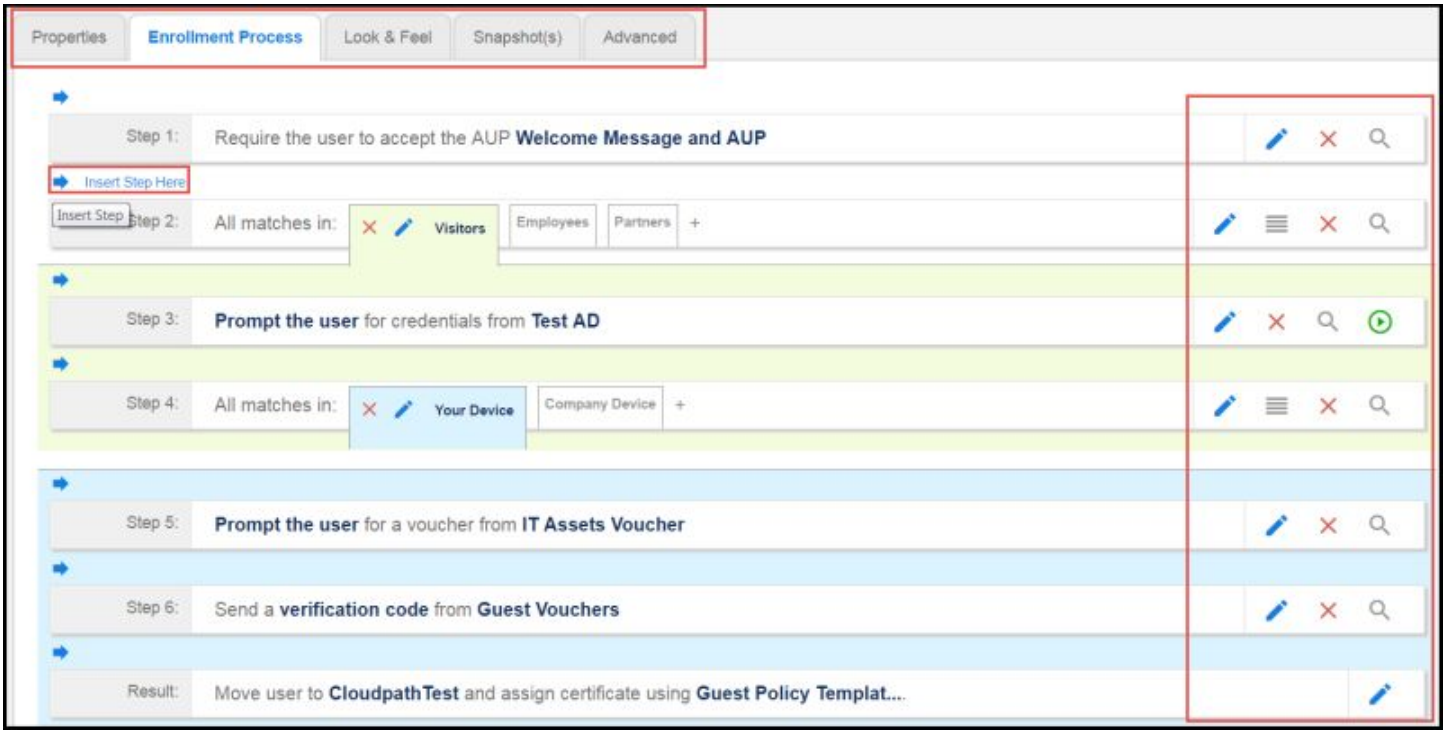
Workflow Basics

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.

  NOTE
  There are additional options available by entering Edit mode for the workflow plugin that are not available during the creation of the plugin to add to a workflow. It is recommended to go into Edit mode to at least view all the options.

- 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 37
- Using the Timed Access Workflow Template on page 51

Modifying a Workflow Template

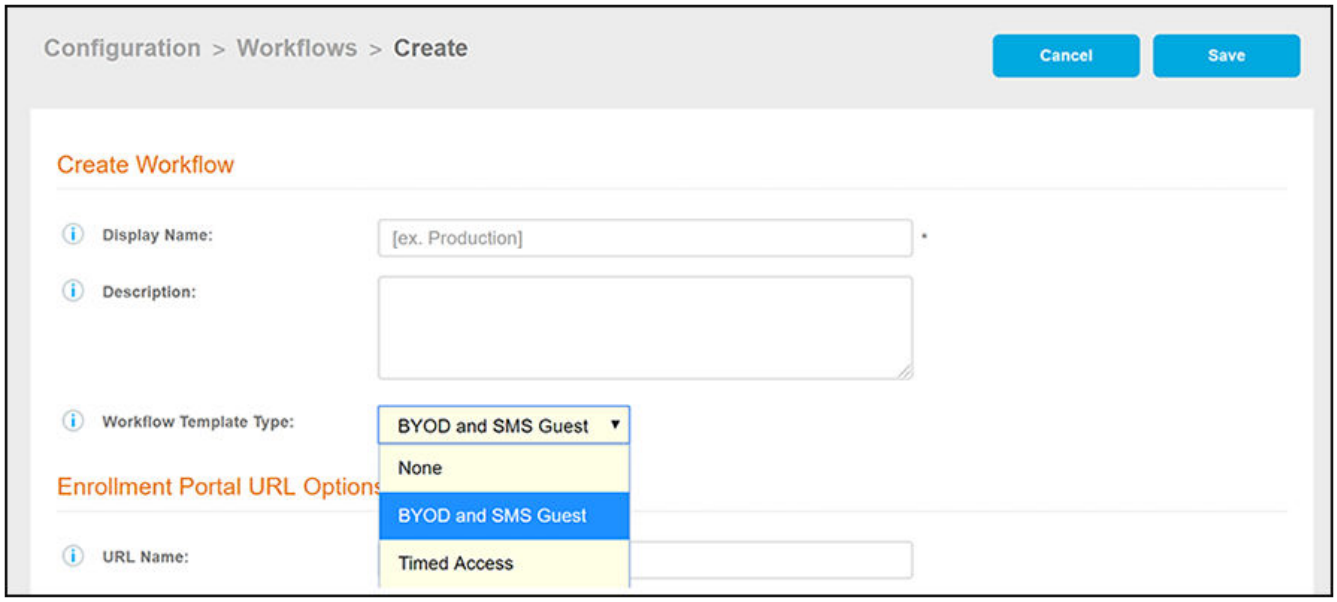
You can modify a standard enrollment workflow template provided by Cloudpath.

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, click **Add Workflow**, then, with the "Create a new Workflow" button selected, click **Next**.

   The Create Workflow screen is displayed:

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

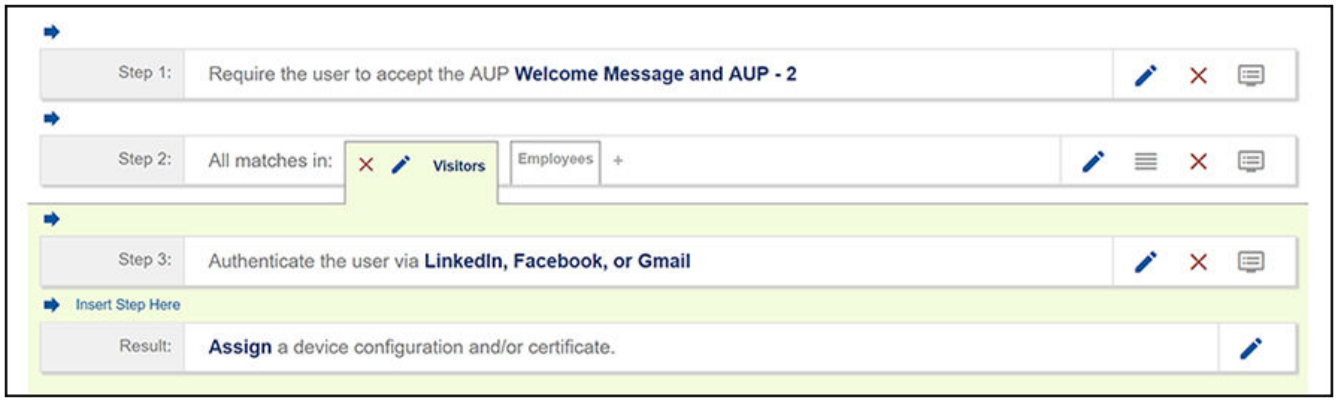


3. On the **Create Workflow** screen, enter a **Display Name** and **Description**.
4. From the Workflow Template Type drop-down list, select "BYOD and SMS Guest."
5. Fill out the URL Name field.

6. Click **Save**.

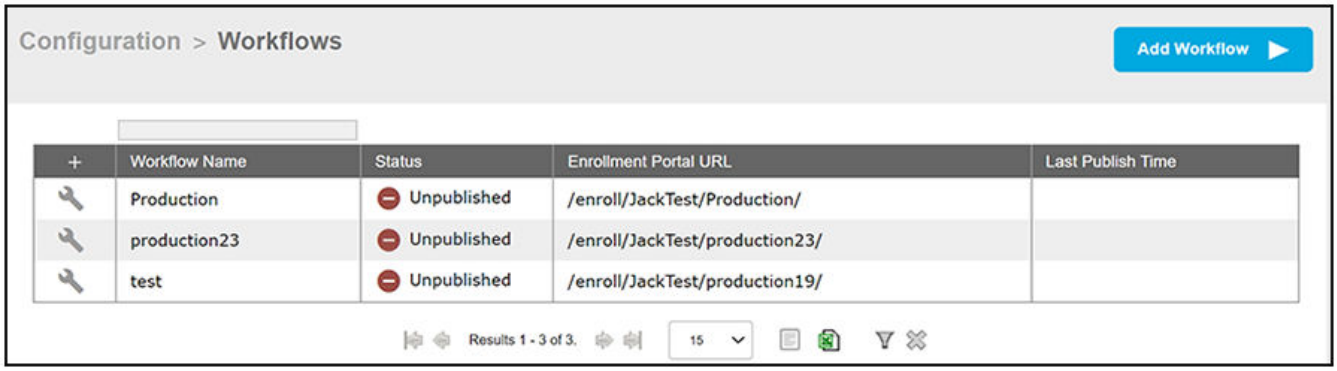
   A workflow template, which contains a typical workflow sequence, is displayed. The step numbers are shown on the left side of the workflow.

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.
8. When you are done creating a workflow, you can click **View All Workflows** to view a grid-like screen that shows all configured workflows. An example of such as screen, after three workflows have been configured, is shown below:

FIGURE 22 Grid View of Configured Workflows



   To make changes to a workflow, click the wrench icon in the screen above (**Configuration > Workflows**).

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.

TABLE 2 Example Workflow Template Steps (continued)

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.

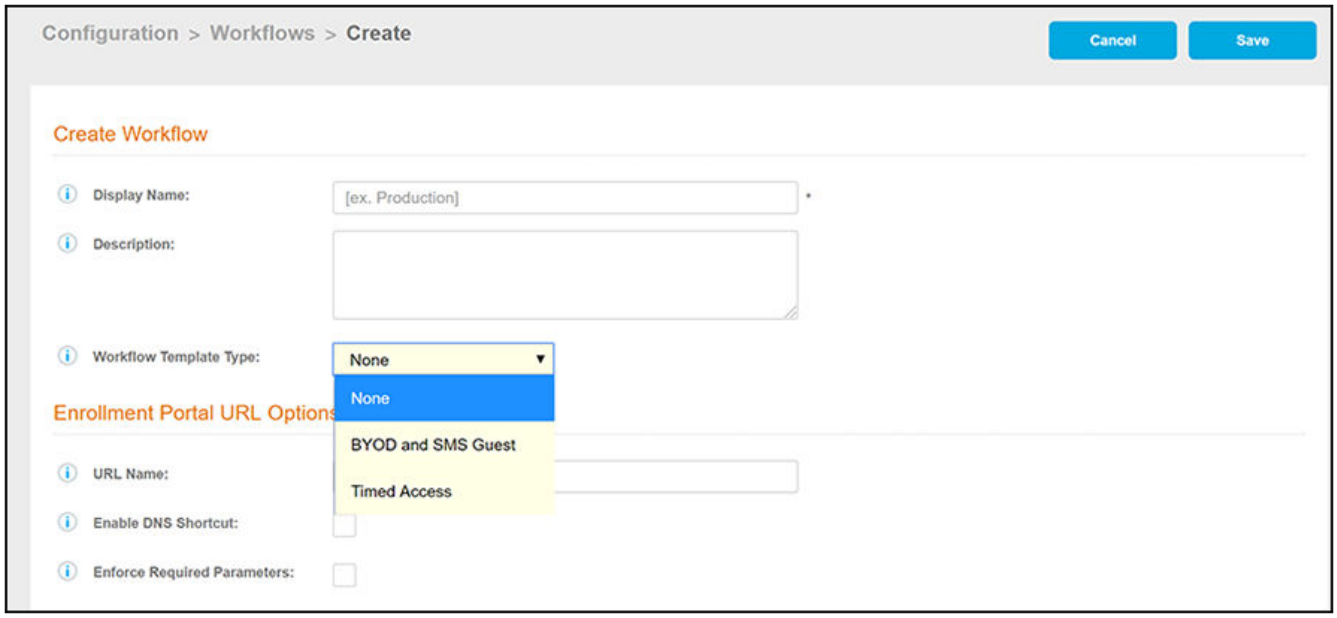
Creating a Workflow From a Blank Slate

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, click **Add Workflow**, then, with the "Create a new Workflow" button selected, click **Next**.

   The Create Workflow screen is displayed:

   FIGURE 23 Create Workflow Screen - Selecting "None" For Workflow Template Type

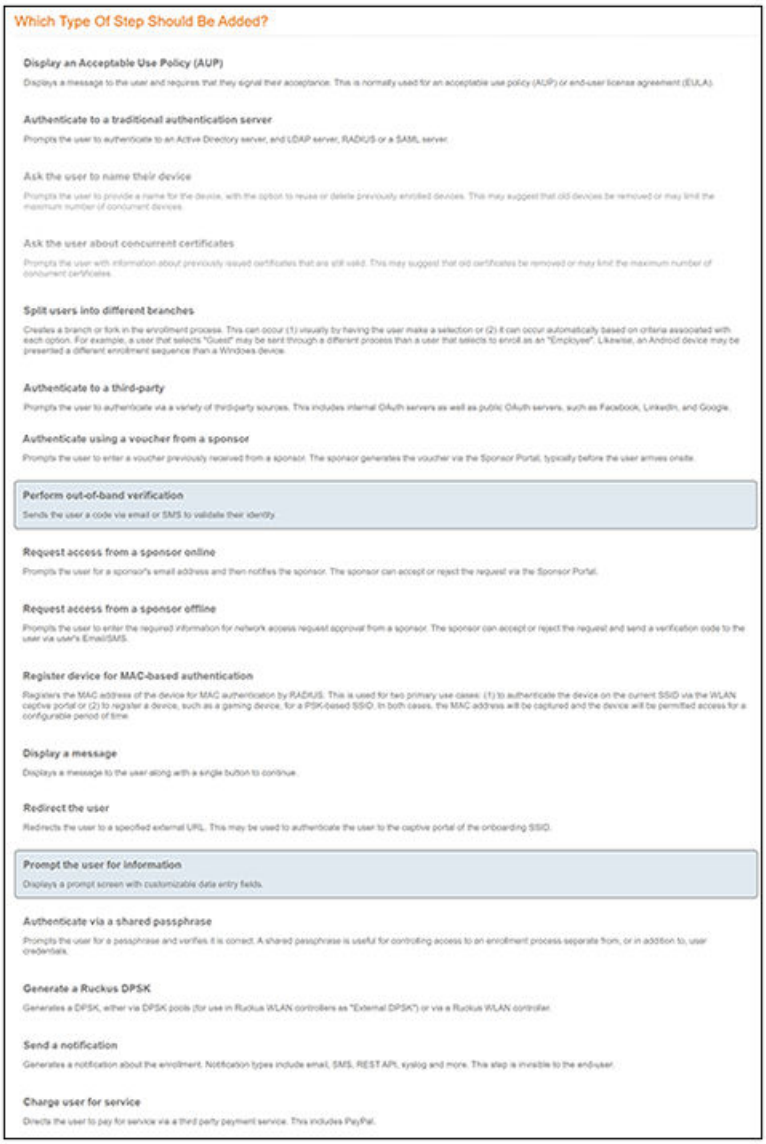


3. On the **Create Workflow** screen, enter a **Display Name** and **Description**.
4. From the Workflow Template Type drop-down list, select "None."
5. Fill out the URL Name field.
6. Click **Save**, and you are returned to a blank workflow page.

7. 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 24 Enrollment Step Selection



Acceptable Use Policy

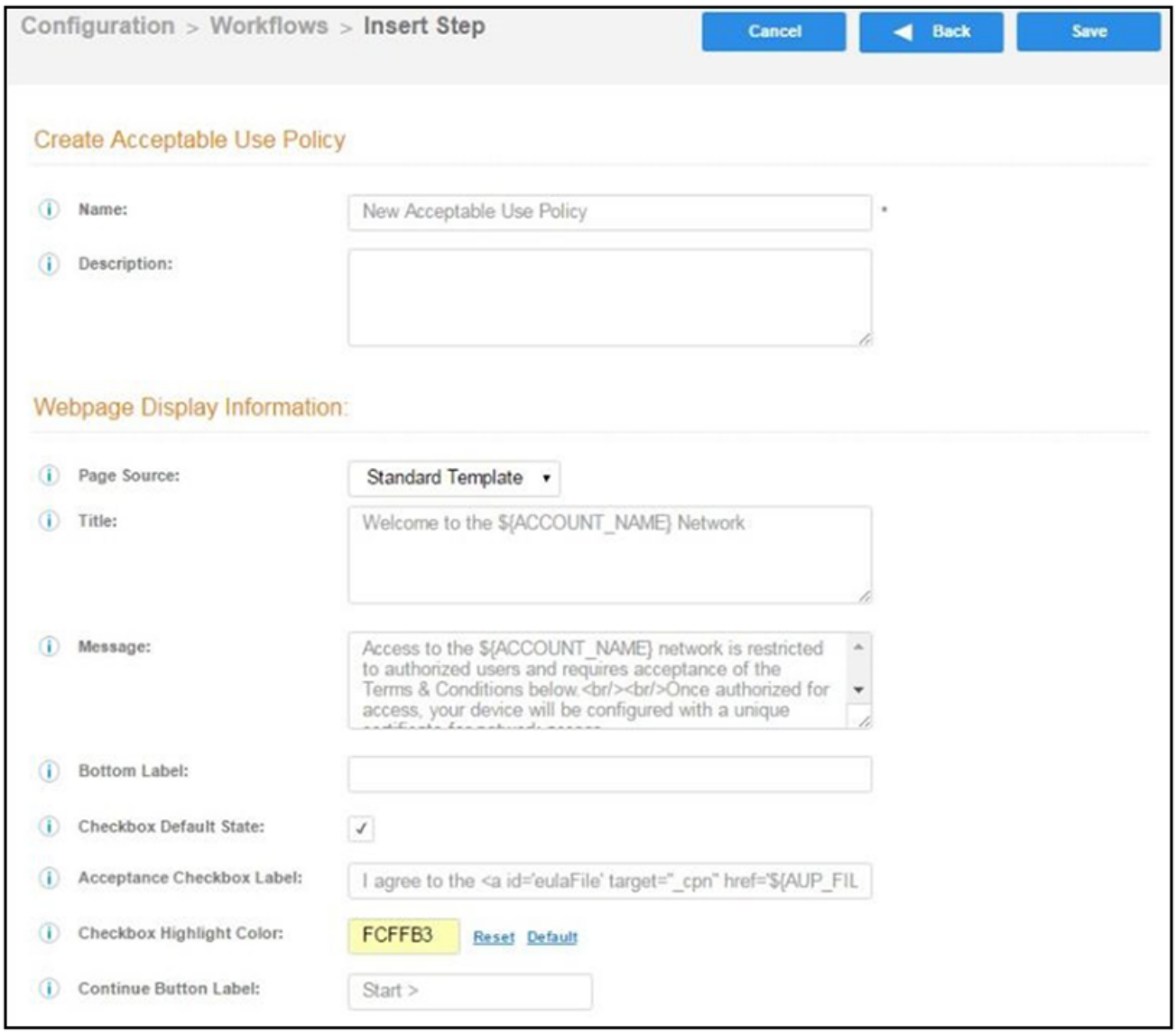
Step 1 in the workflow requires the user to agree to an Acceptable Use Policy (AUP).

1. Select the button for **Display an Acceptable Use Policy (AUP)**.
2. 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 25 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

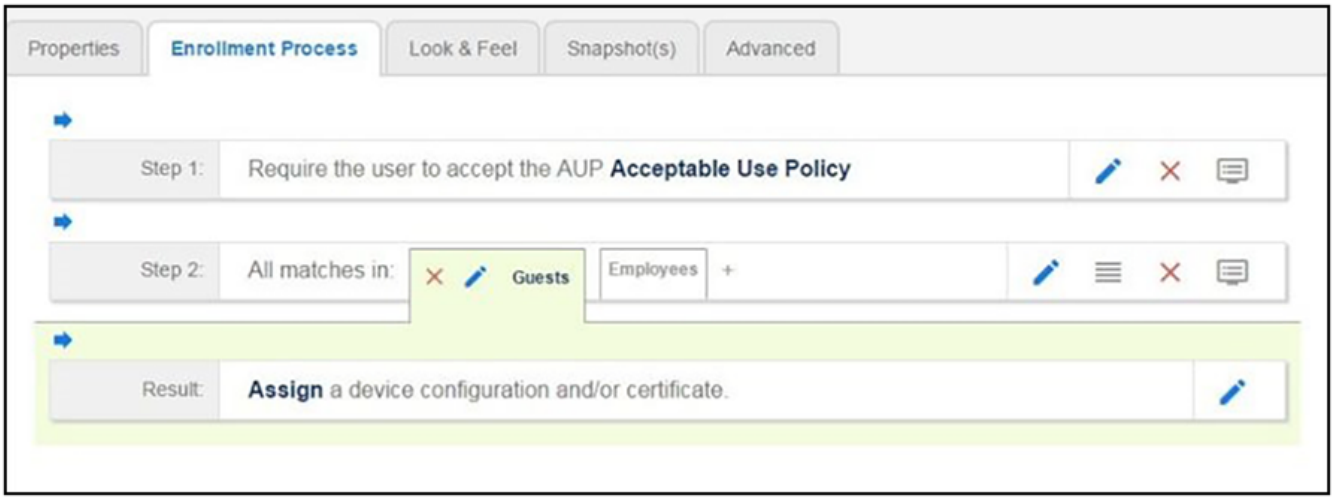
Step 2 in the workflow prompts for the type of user access.

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 26 Workflow with User Type Split



Authentication to a Traditional Authentication Server

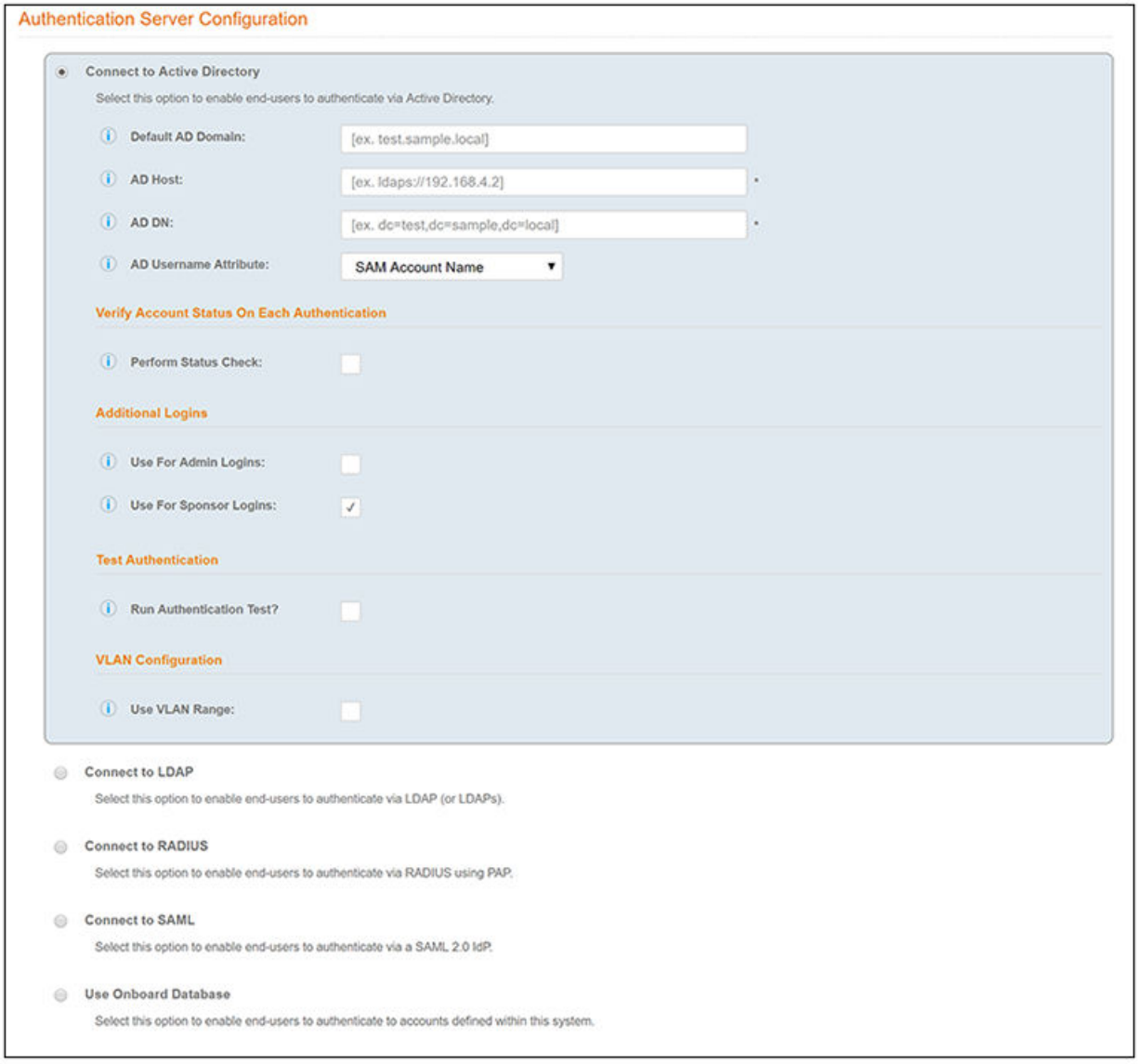
Step 3 in the workflow authenticates a user against a Corporate AD server.

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 27 Add Authentication Server



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

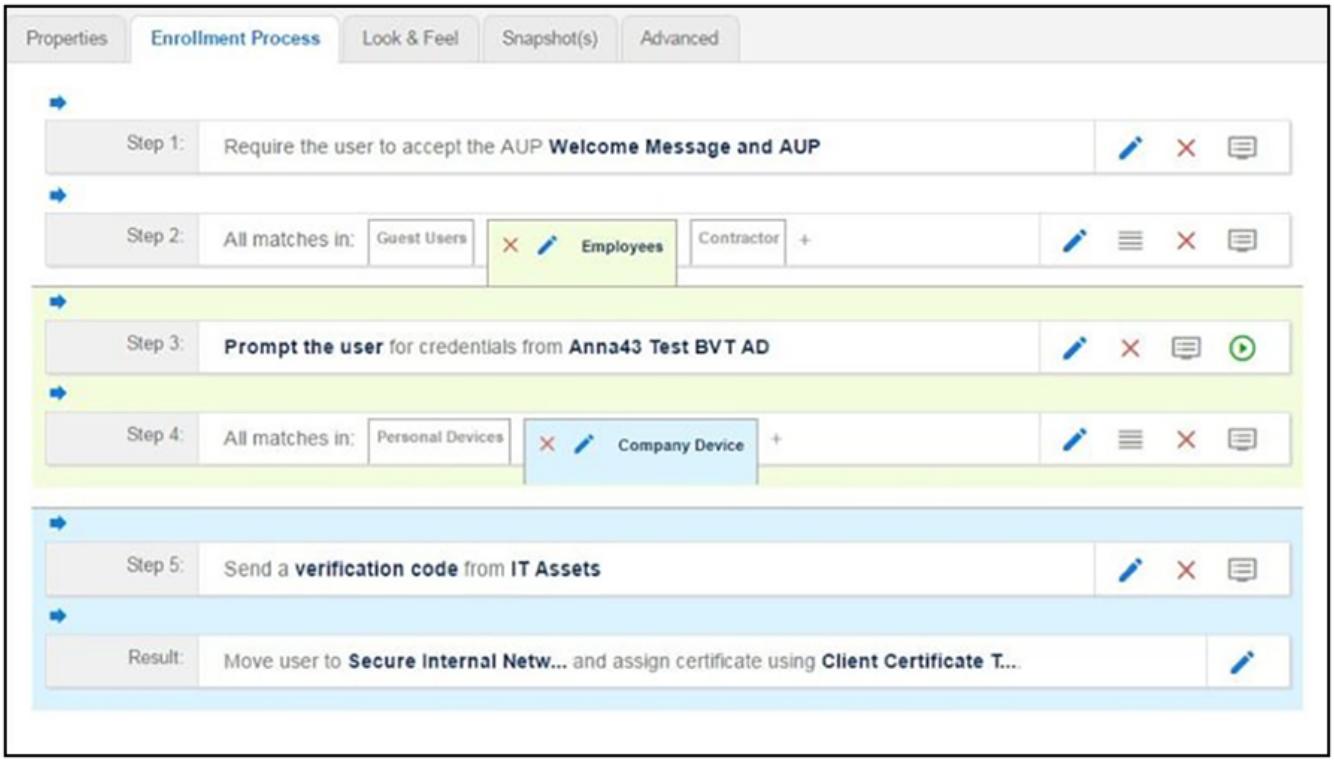
Step 4 adds an enrollment step prompts the user to select a personal device or a company-owned (IT- asset) device.

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 28 Workflow with Device Ownership Split



Create a Filter in the Device Type Split

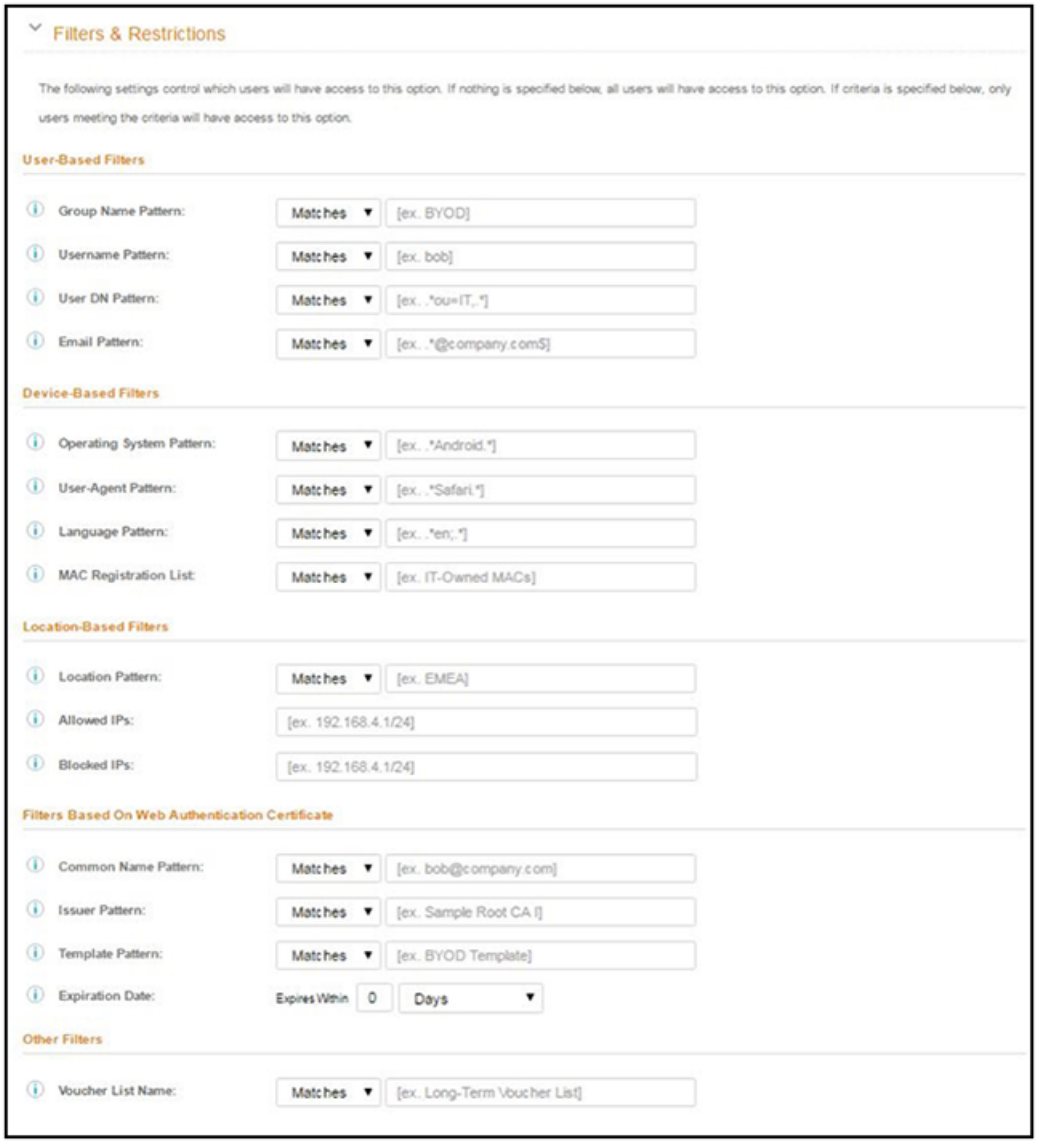
When creating splits in the workflow, you can set up a filter so that only certain users see this enrollment step.

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 29 Modify Step - Filters and Restrictions



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.

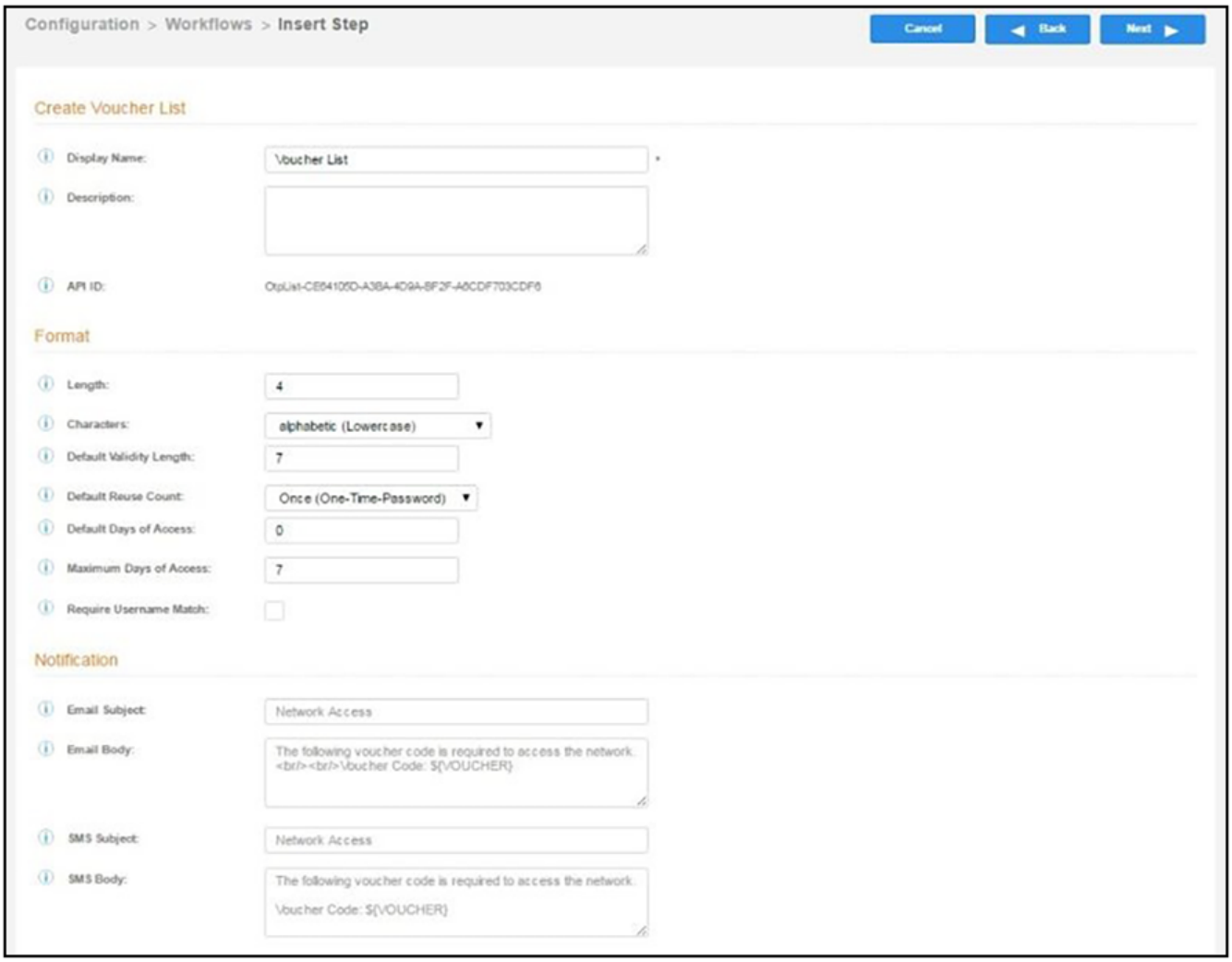
Prompt for Voucher

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**.

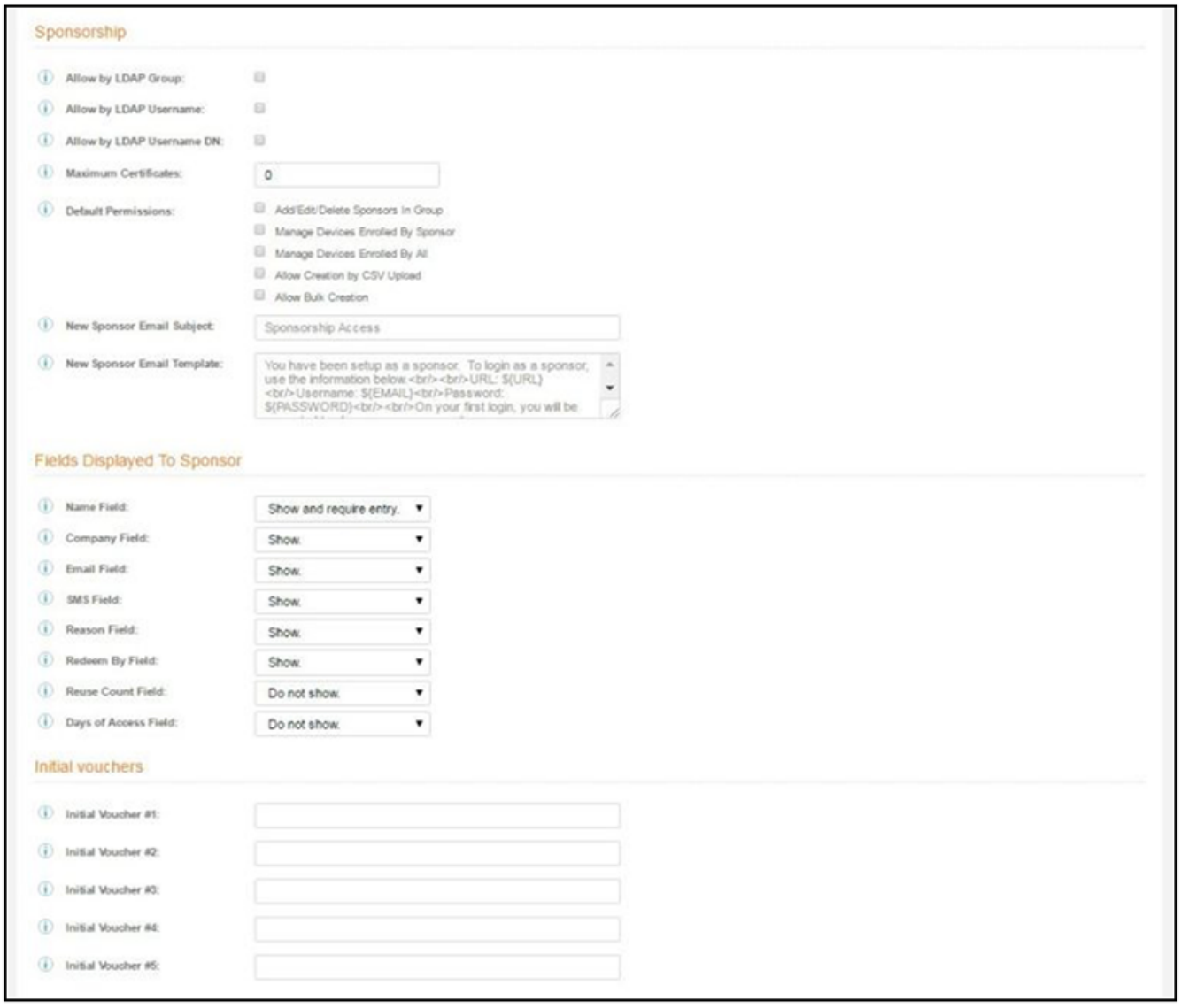
> **NOTE**
> For complete information about using the "Authenticate using a voucher from a sponsor" workflow plugin, refer to the *Cloudpath Enrollment System Sponsored Guest Access Configuration Guide*.

FIGURE 30 Create Voucher List - Format and Notification Fields



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 31 Create Voucher List - Sponsorship, Fields Displayed, and Initial Vouchers



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

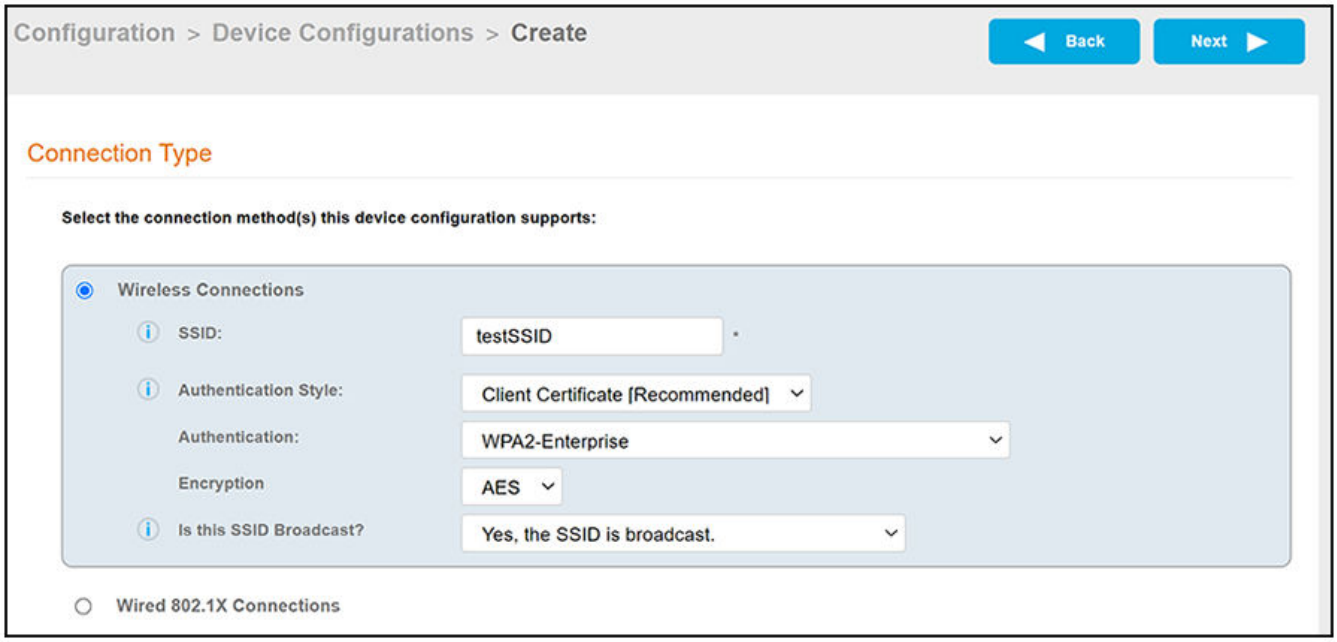
A device configuration is a group of settings containing a single configuration per operating system. This configuration determines the settings and behavior required to move the device from the onboarding SSID to the secure network.

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 and optional description for the device configuration, then click **Next**.
4. Select **Wireless Connections** (the default) and enter the SSID of the secure wireless network.

FIGURE 32 Configure SSID



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. For **Authentication Style**, use the default of "WPA2-Enterprise".
7. For **Encryption**, "AES" is the only option for the "WPA2-Enterprise" authentication style.
8. Leave the default **Broadcast** setting and click **Next**.

9. Specify **Conflicting SSIDs**.

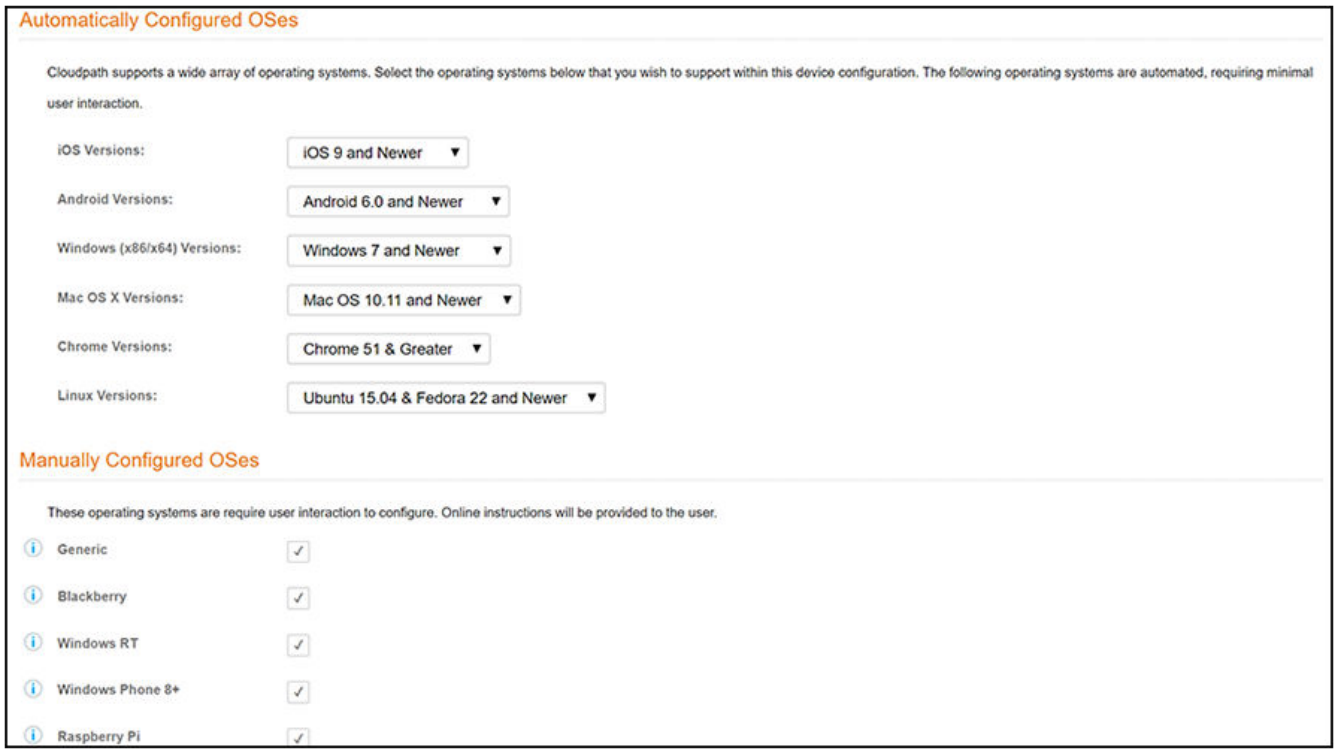
   This setting attempts to deter enrolled devices from joining listed SSIDs after the secure SSID is configured. It is recommended that you include the open-enrollment SSID in this list. Specifying this option is required for mobileconfig-based iOS/MacOS enrollments to disconnect from the open-enrollment 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.*

   NOTE
   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 for a completed device configuration, 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."

10. 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 33 Select OS Versions

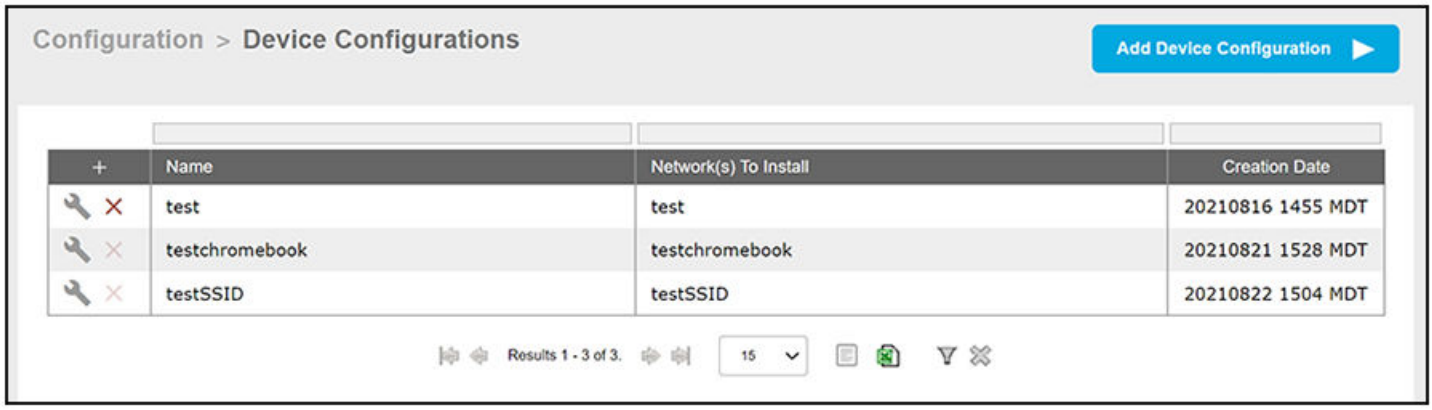


11. Select **Client will authenticate to the onboard RADIUS server**.
12. Configure additional settings for the device configuration.
13. On the screen called "What certificate template should issue the certificate?":
    - If you select **Do not issue a certificate to the user** and click **Next**, the configuration completes.
    - If you select **A new certificate template** and click **Next**, follow the instructions in the Client Certificates on page 49 to select the client certificate template with the appropriate user policy.

To make changes to a completed device configuration, as well as to view a list of additional settings, you can go to **Configuration > Device Configurations**.

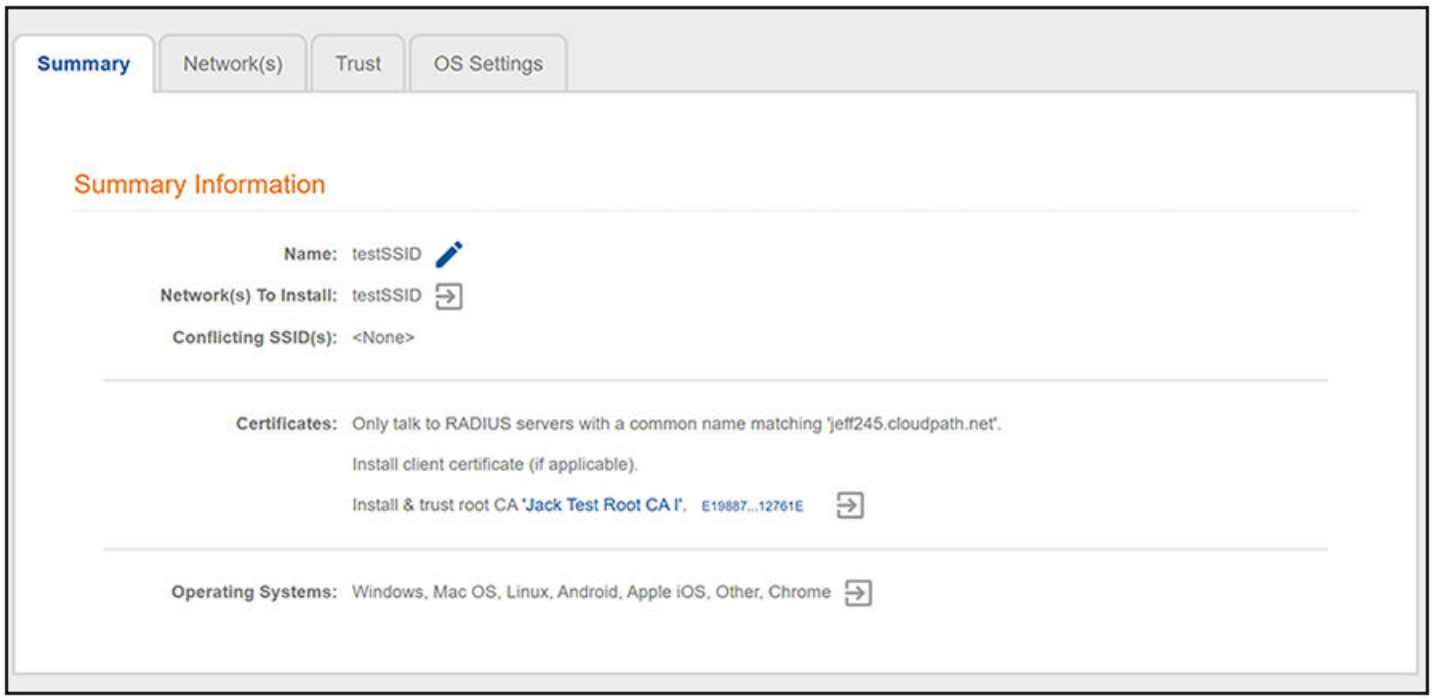
The following figure shows an example **Configuration > Device Configurations** page with the grid view and wrench icons:

FIGURE 34 Device Configurations Page Example



If you click the wrench icon, you are presented with the tabs view of the corresponding device configuration, from which you can view and make any desired changes.

FIGURE 35 Device Configuration Tabs View



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.

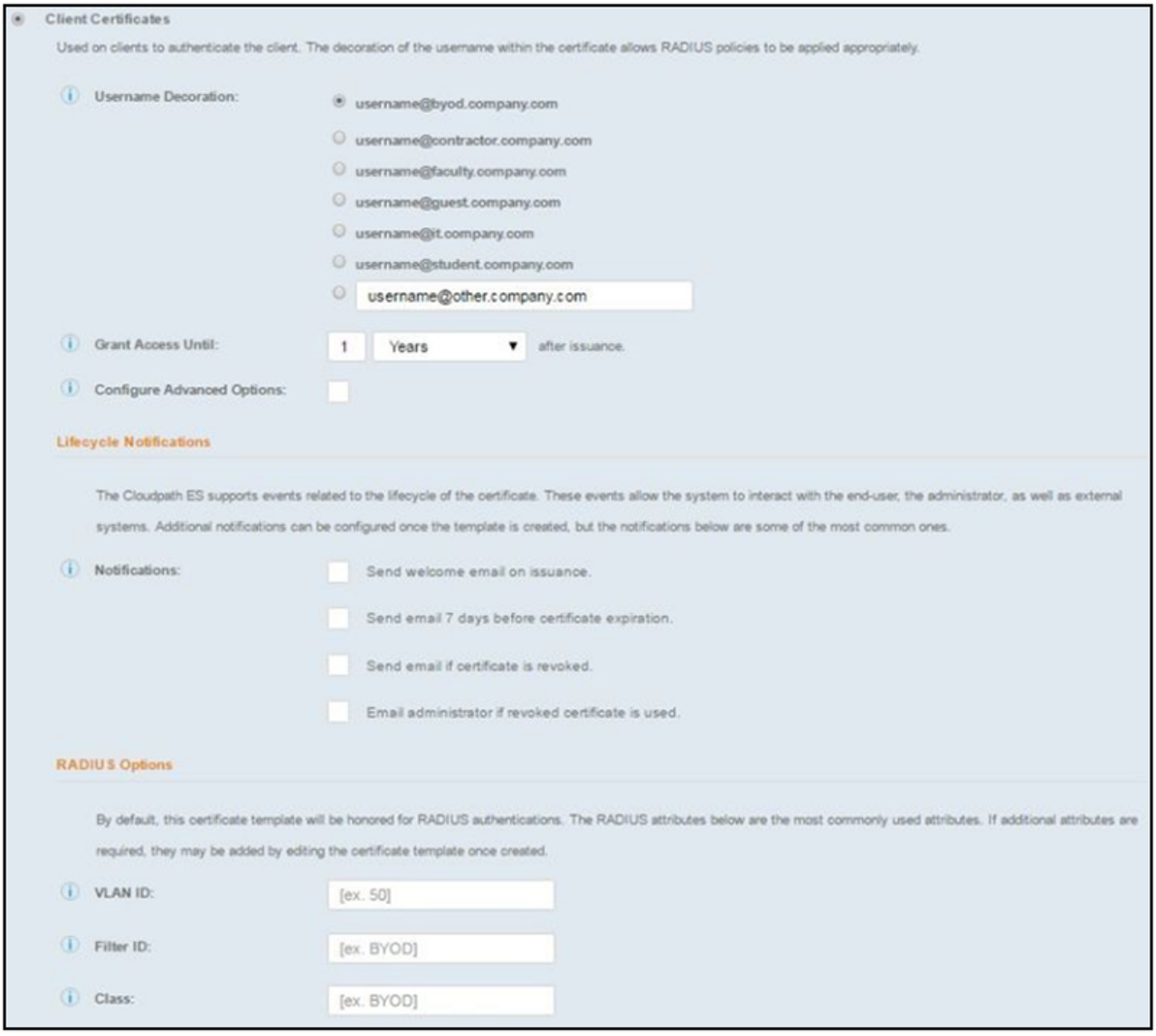
You can set up different certificate templates for different user types. An employee or staff certificate template might be valid for 120 days, and a guest template might be valid for 1 day or until the end of the week.

After you set up a device configuration for the workflow, you can configure 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 36 Client Certificate Template



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**.

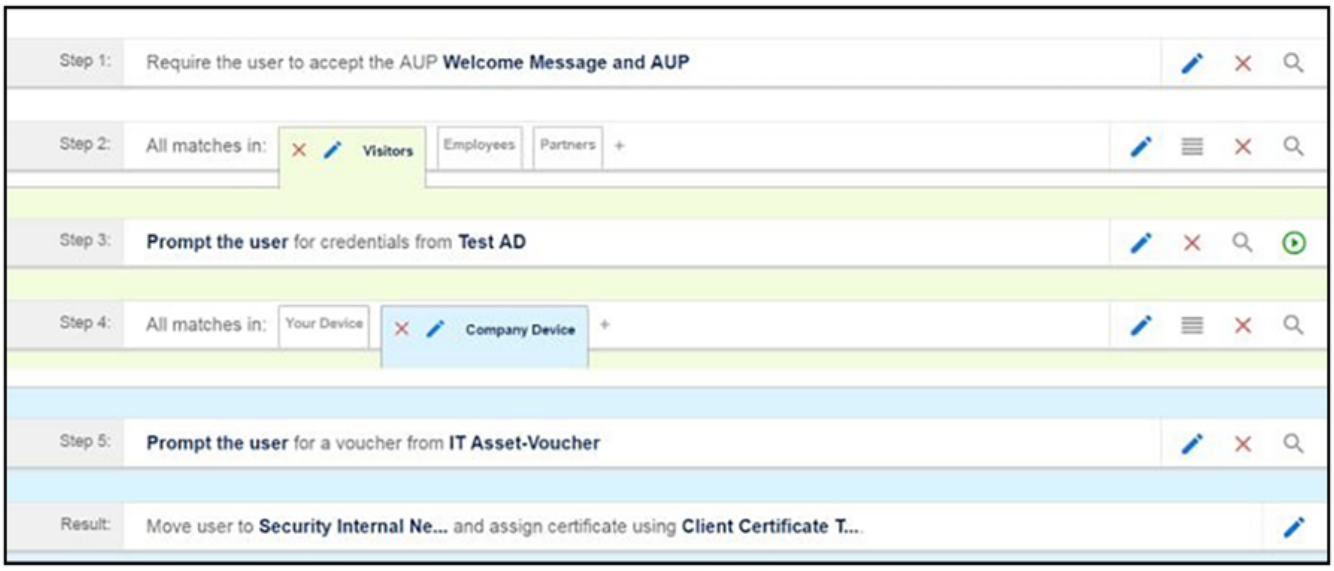
7. Select any email notifications to be sent to the user related to the life-cycle of the certificate.

   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 37 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.

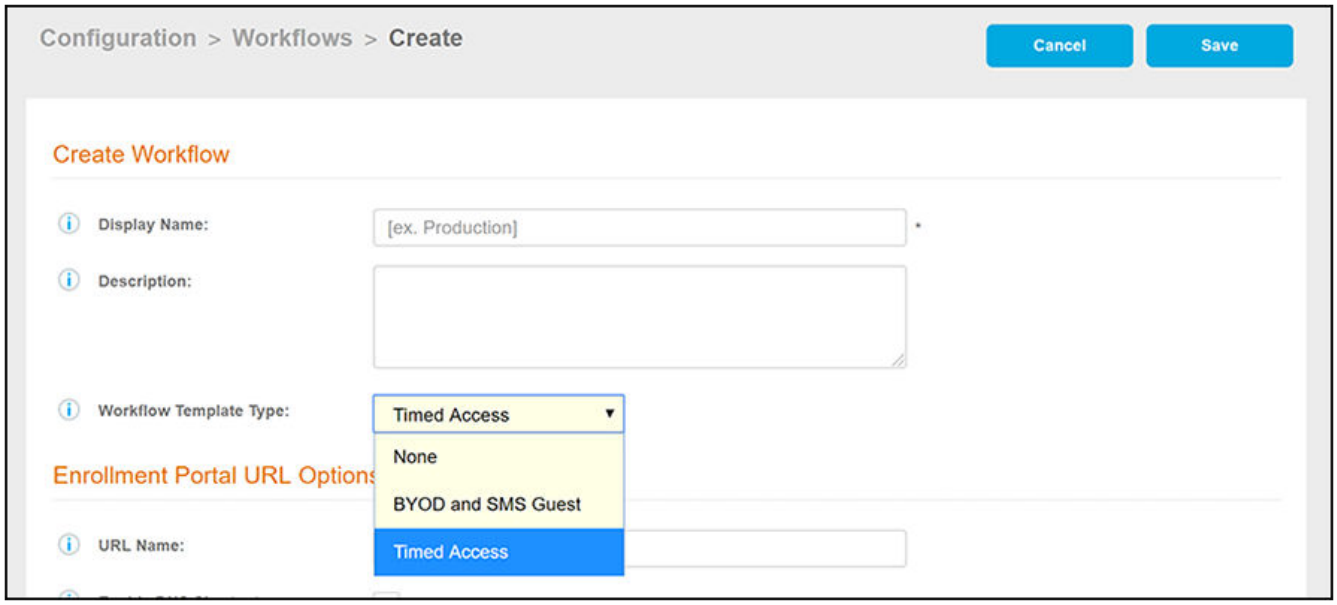
The main concept of the Timed Access workflow template is to give users free access to a network connection for a limited time period, and, when that time period expires, they can re-enroll their device to one of the a pre-configured "premium" lists. You can use other workflow plug-ins to add steps to 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, click **Add Workflow**, then, with the "Create a new Workflow" button selected, click **Next**.

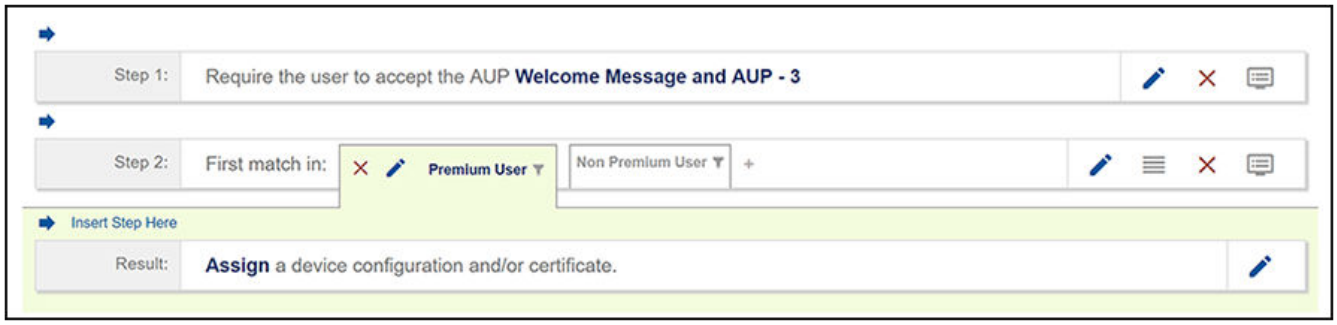
   The Create Workflow screen is displayed:

FIGURE 38 Create Workflow Screen - Selecting "Timed Access" For Workflow Template Type



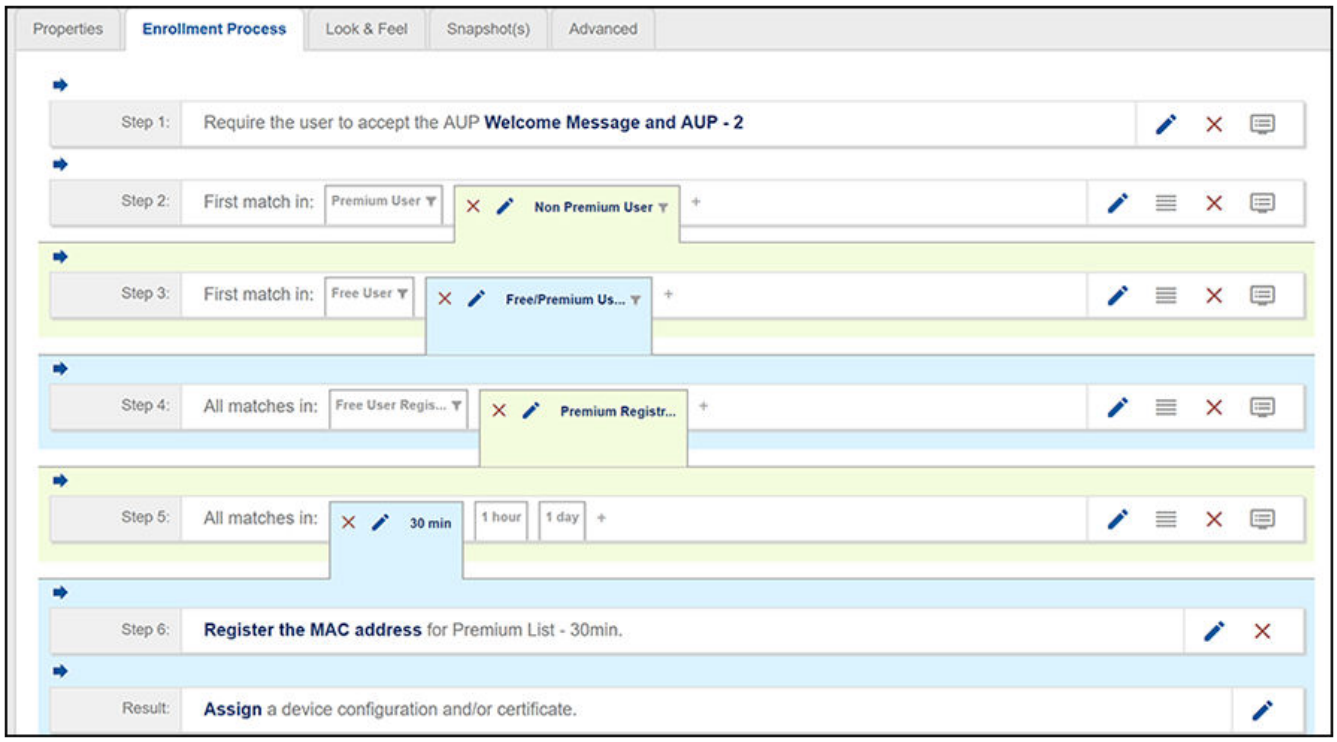
3. On the **Create Workflow** screen, enter a **Display Name** and **Description**.
4. From the Workflow Template Type drop-down list, select "Timed Access."
5. Fill out the URL Name field.
6. Click **Save**, and you are returned to the workflow page that is shown in the following figure.

FIGURE 39 Timed Access Workflow After Initial Creation



7. 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 40 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 - 1day
- Premium List - 1hr
- 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	First match in: • 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	First match in: • 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	All matches in: • Free User Registration: Presented if the MAC address is *not* 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 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.
Step 5	All matches in: • 30 min: Available to all enrollments • 1 hour: Available to all enrollments • 1 day: Available to all enrollments 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.
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

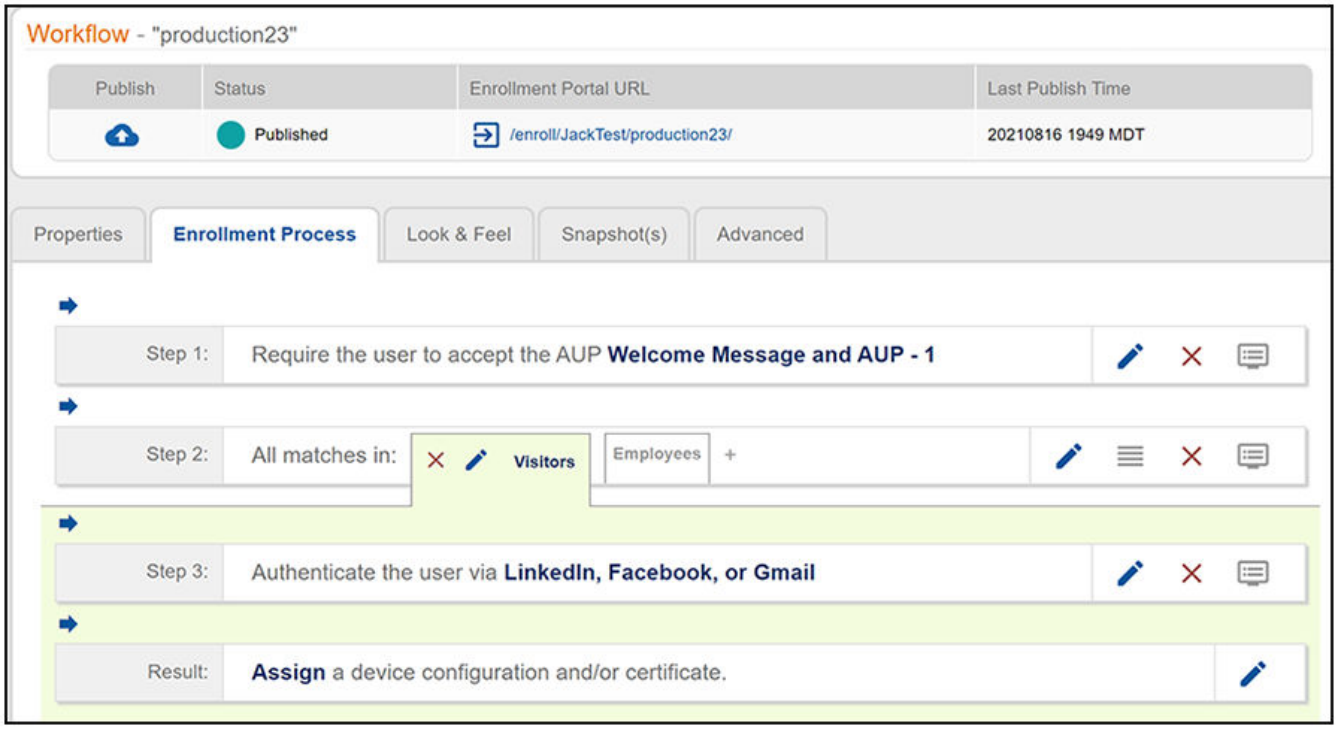
A workflow is published using Snapshots. A snapshot is a version of a workflow configuration. You can create and maintain multiple versions of each configuration. However, only one snapshot can be active at a time for each workflow.
To publish the workflow:

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

2. Click the wrench icon of the workflow you wish to publish; for example "production23" in Figure 22 on page 36.

   The following screen is displayed:

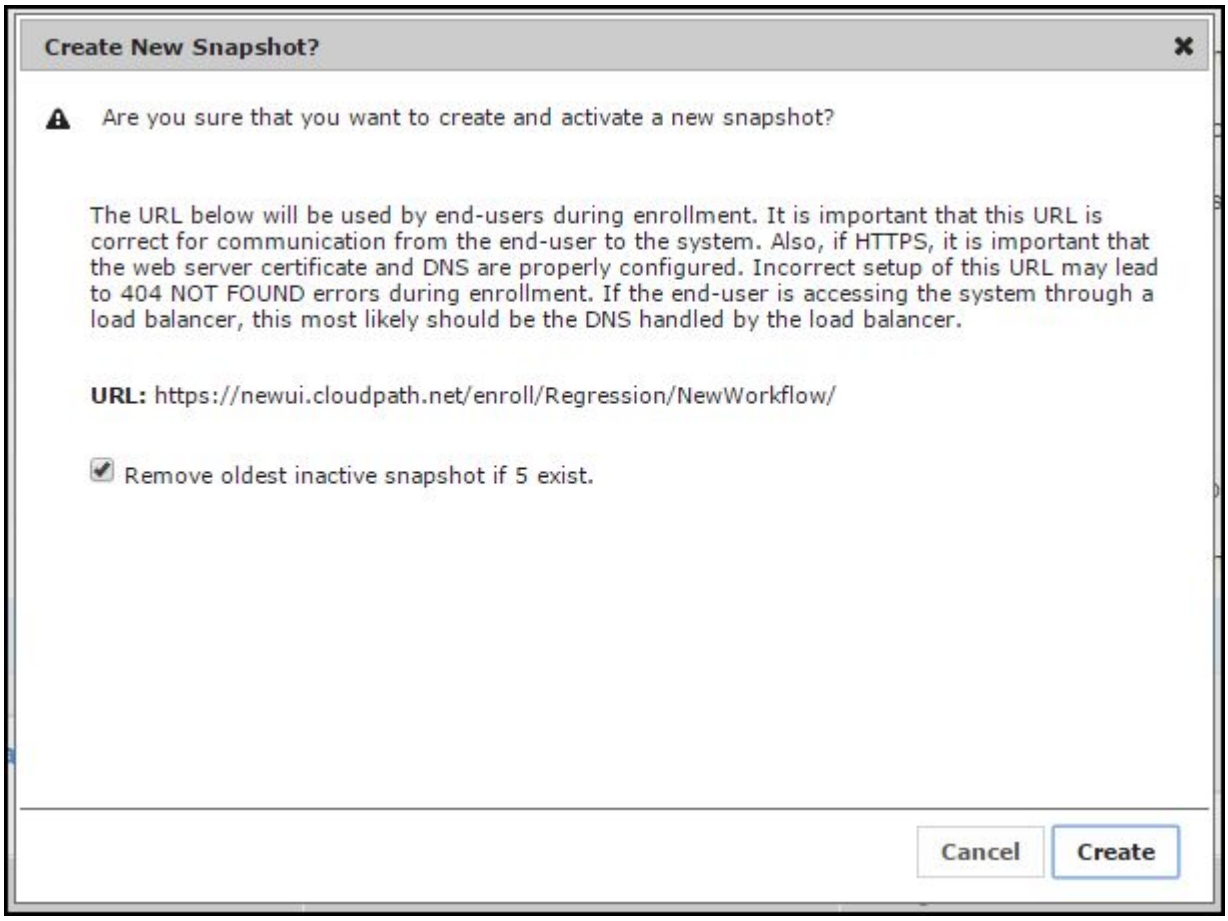
FIGURE 41 Publish Icon Under "Publish" Column



3. On the preceding screen, click the **Publish** icon to publish the workflow.

   The following screen is displayed:

FIGURE 42 Create New Snapshot

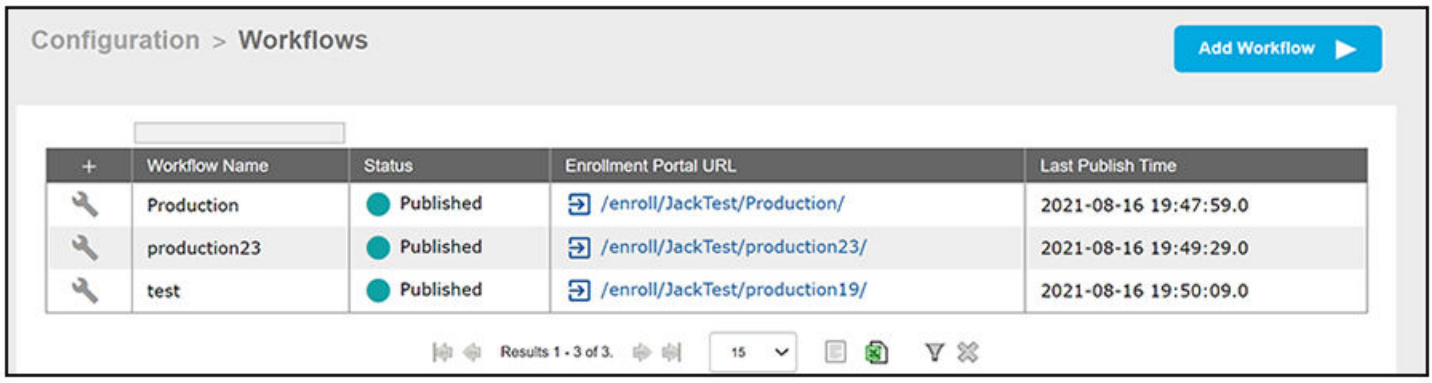


4. Select the Wizard version to use for the new snapshot. The **Cloudpath Wizard** is the application provided to users to automate the enrollment process.
5. Verify the Enrollment Portal URL for the snapshot.
6. Click **Create**.

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.

The Workflow grid view (**Configuration > Workflows**) 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 43 Workflow Grid View Showing That All Workflows Have Been Published



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).

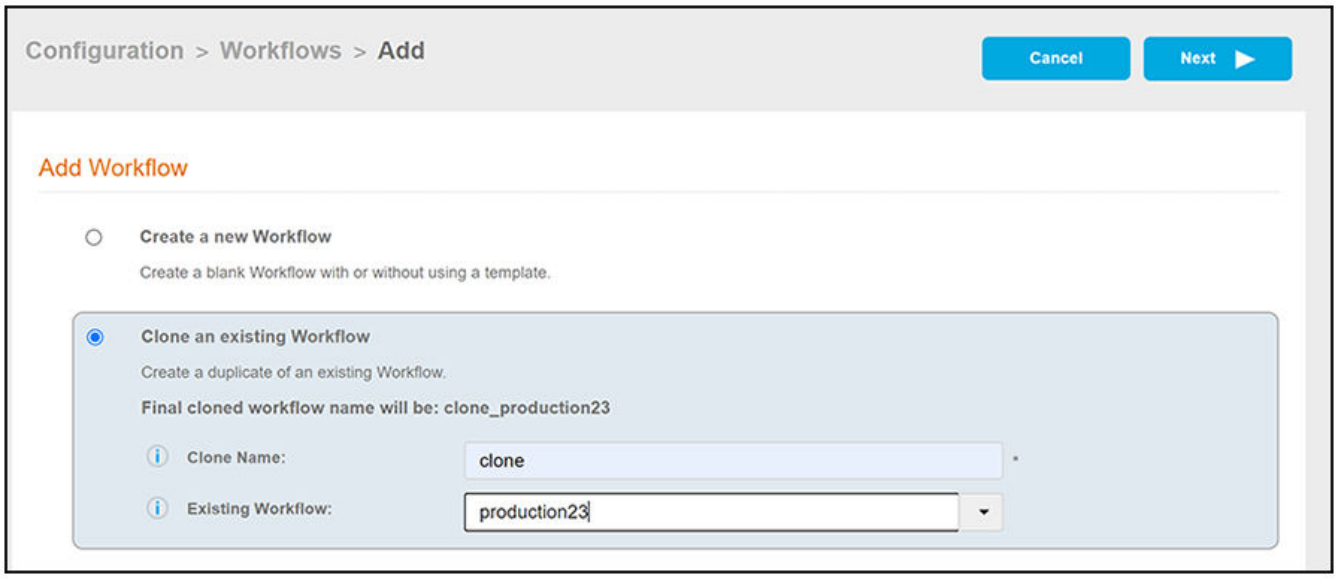
Cloning a Workflow

Cloning a workflow can be a useful tool during development because you can make exact copies of current workflows. From these copies, you can make desired updates to create new workflows without having to start every workflow from scratch.

The steps use an example to instruct you on cloning a workflow:

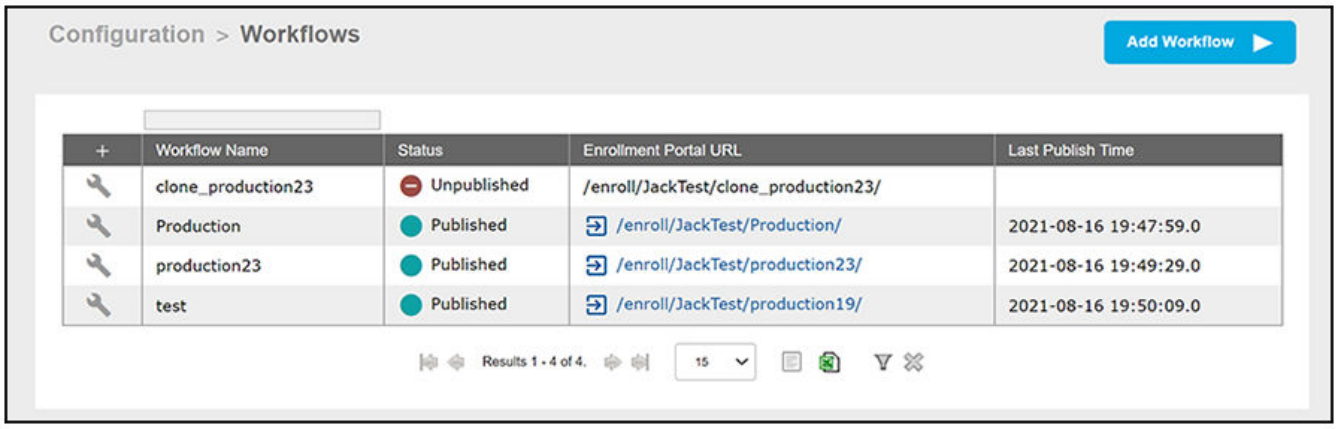
1. In the UI, go to **Configuration > Workflows** to display your current workflows. Suppose you want to clone the workflow called "Production_23" shown in the Figure 22 on page 36.
2. Click **Add Workflow**.
3. On the ensuing screen, do the following:
   a. Select the "Clone an existing Workflow" button (see screen below).
   b. In the Clone Name field, enter the name you want for the cloned workflow. The name you provide will be pre-pended with an underscore to the name of the selected existing workflow.
   c. From the Existing Workflow drop-down, select the workflow you want to clone.

FIGURE 44 Selecting the Workflow to Clone



4. Click **Next**.
5. When the cloning completes, the cloned workflow appears in your list of workflows just like any other workflow. The example below shows the new workflow: "clone_Production_23".

FIGURE 45 Cloned Workflow Added to Top of Workflow List



Basic behavior of cloning:

- A cloned workflow appears in the list of workflows.
- A cloned workflow is an identical copy of the workflow from which it was cloned.

> **NOTE**
> Items that are not part of the actual workflow will not be cloned. Examples include MAC authorization lists, approvers lists, authentication servers, and so on.

- Plug-ins that require unique names are also renamed with "clone_" prepended to their original names, as shown in the preceding illustration with the Use Policy and Notification plug-ins.

  NOTE
  After cloning is complete, you can rename a cloned workflow and plug-ins to any names you want.

- Editing a cloned workflow has no impact on the workflow from which it was cloned.
- You can also make a clone of a clone.
- A cloned workflow is not automatically published, but it can be published at any time.

Administration

- Administration Overview.....61

Administration Overview

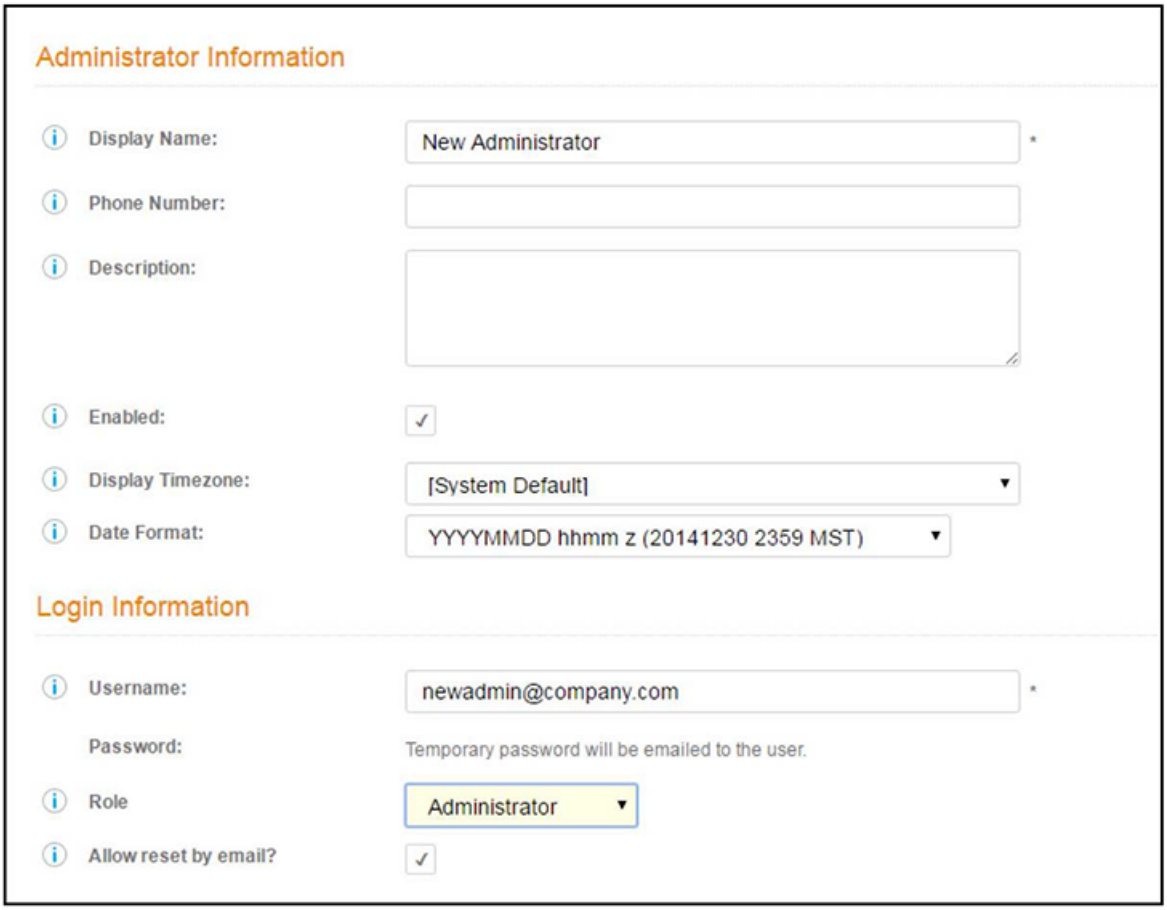
Access the **Cloudpath Administration** tab to manage system-related operations, using links in the following sections:

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 46 Add Administrator



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.

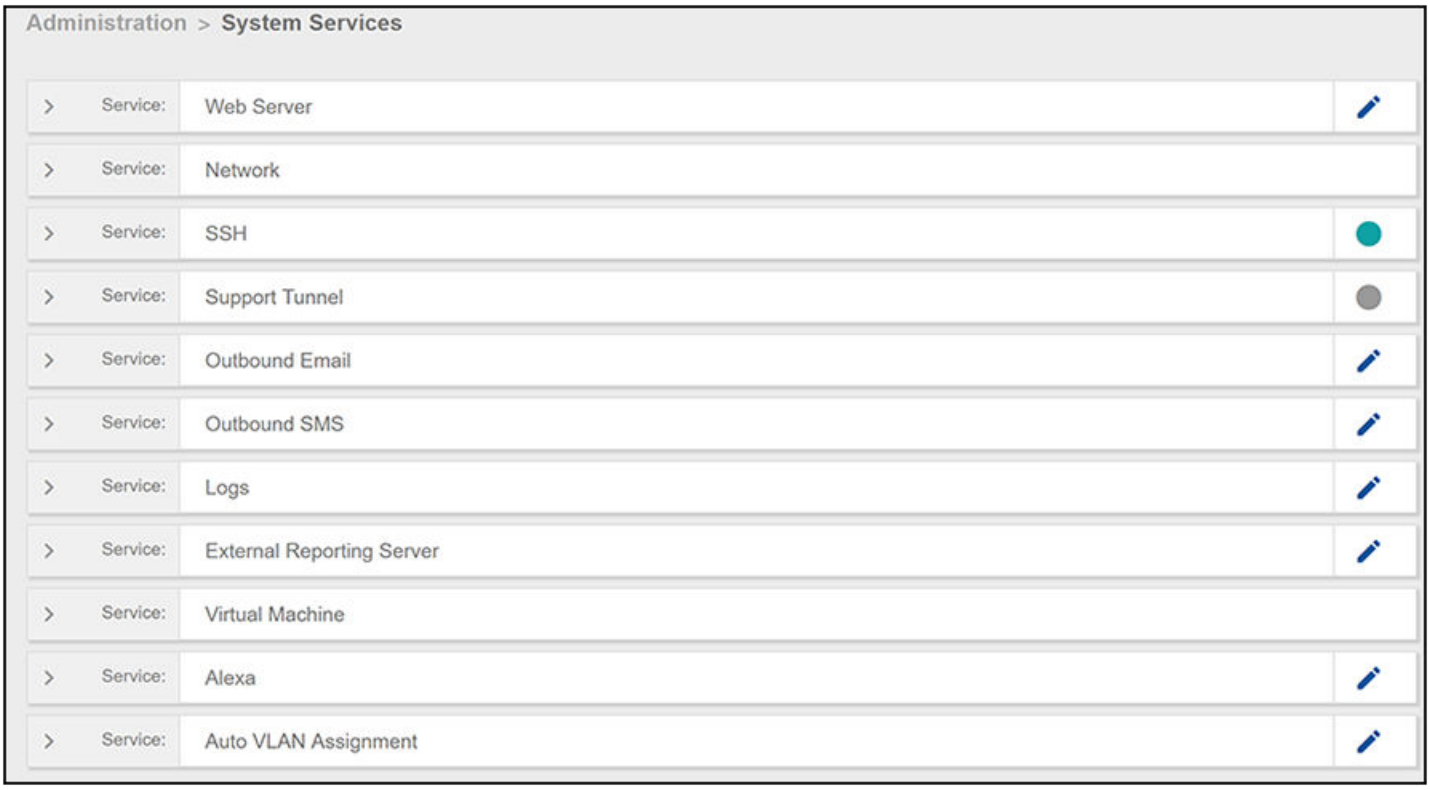
Company Information

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 47 Cloudpath System Services



- 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 65
- Device Configurations 65
- RADIUS Server 66
- Authentication Servers 67
- Firewalls and Web Filter Integration 67
- MAC Registration Lists 67
- API Keys 67

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:

> **NOTE**
> For a completed device configuration, in the **Configuration > Device Configurations** area, click the arrow next to the desired device configuration to expand the view, then use the various tabs to add or edit settings.

- Summary tab - An overview of the device configuration settings.
- Network(s) tab - WLAN settings.
- Trust tab - RADIUS server information and certificate chaining.
- OS Settings tab - User-experience settings, configuration from the "Network(s)" and "Trust" tabs, 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 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

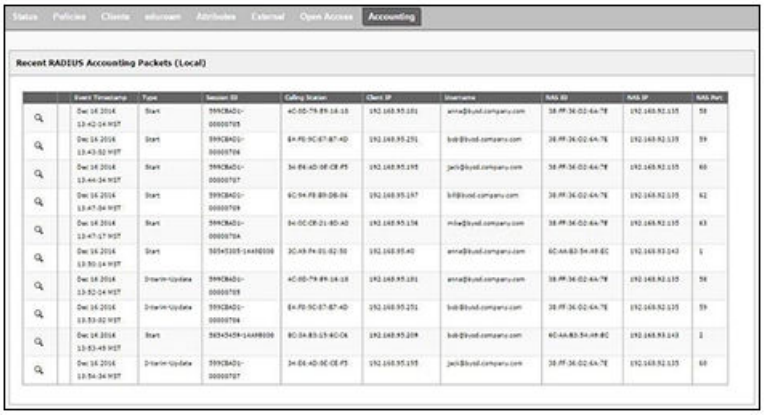
View and manage the onboard RADIUS server.

- 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* for more information.
  - CoA - Enable CoA to send Change of Authorization disconnect messages (DMs) from Cloudapth 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* 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 for more information.

FIGURE 48 RADIUS Accounting



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 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 69
- Connections 69
- Enrollments 70
- DPSKs 72
- Users & Devices 72
- Certificates 74
- Notifications 76
- Event Response 78
- VLAN Assignments 78
- Traffic Monitor 78

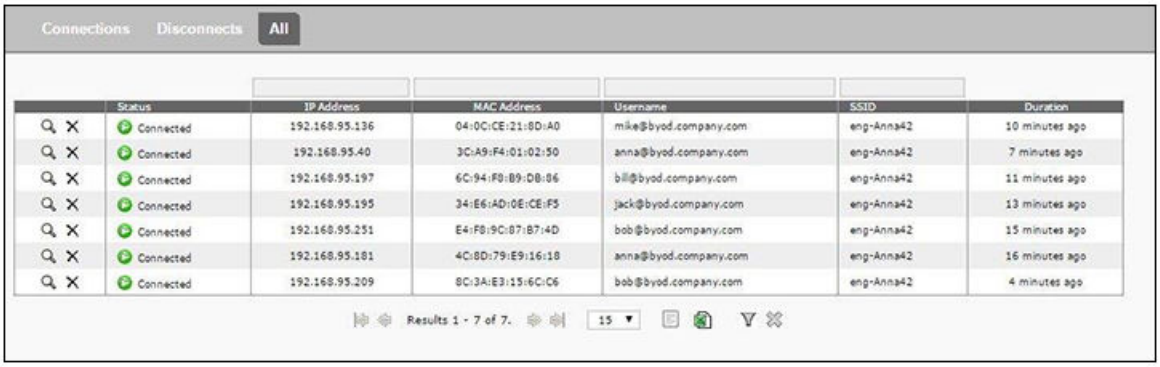
Overview

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.

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 49 RADIUS Connections

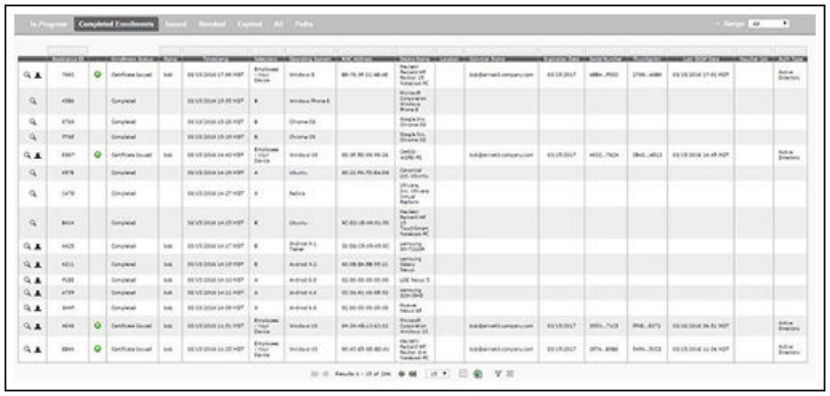


You can send Change of Authorization (CoA) disconnect messages (DMs) to the controller or switch from the **Connections** page, or via an enrollment **Revoke**. See the *Onboard RADIUS Server CoA* guide on the **Documentation** tab for more information.

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 50 Enrollments Table



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

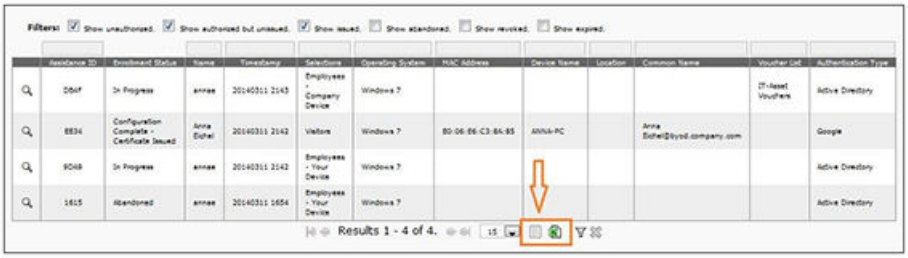
Enrollment and User data can be can be downloaded, as a CSV file or Microsoft Excel spreadsheet.

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 51 Download Enrollment Records

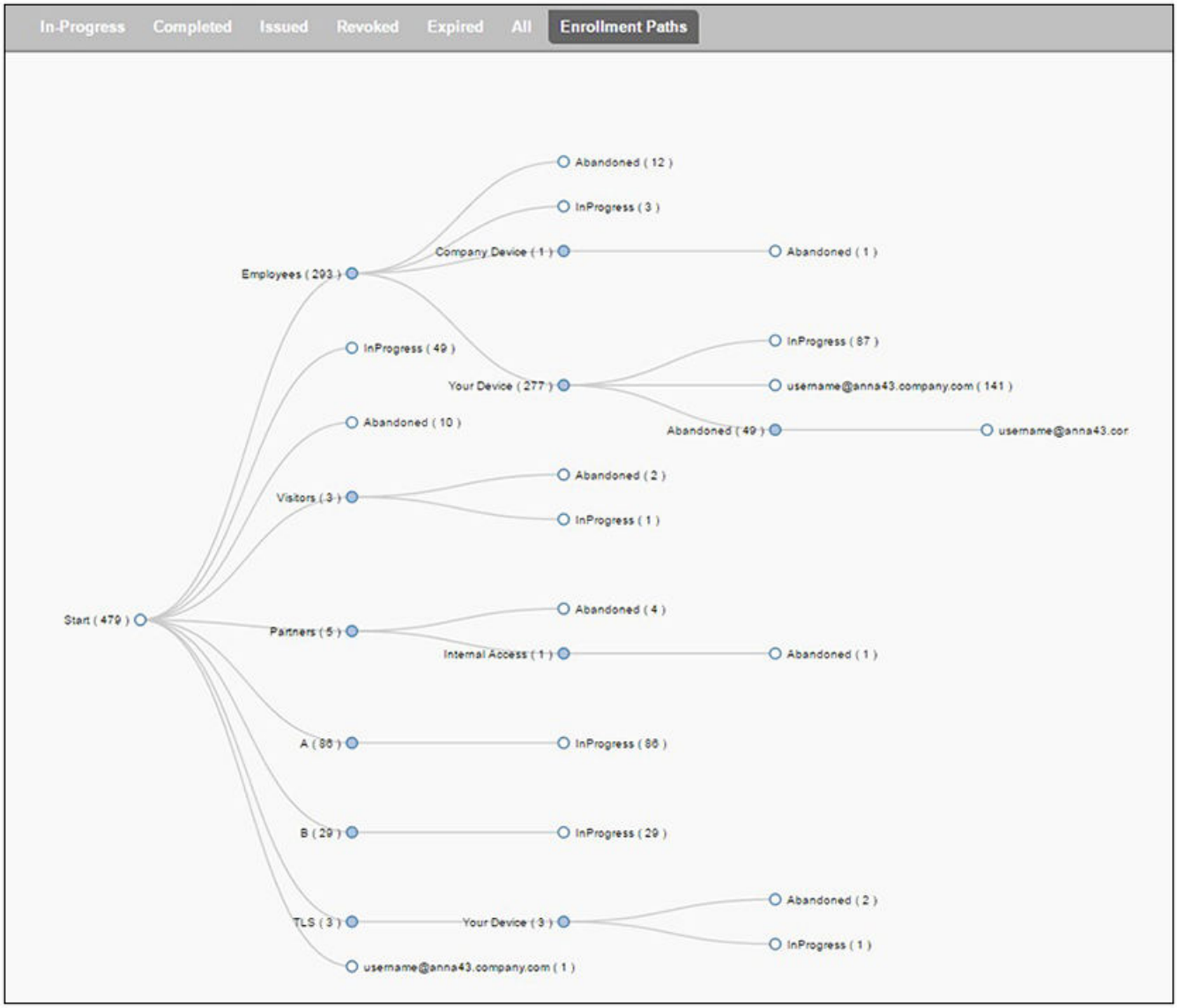


Enrollment Paths

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 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 52 Enrollment Path

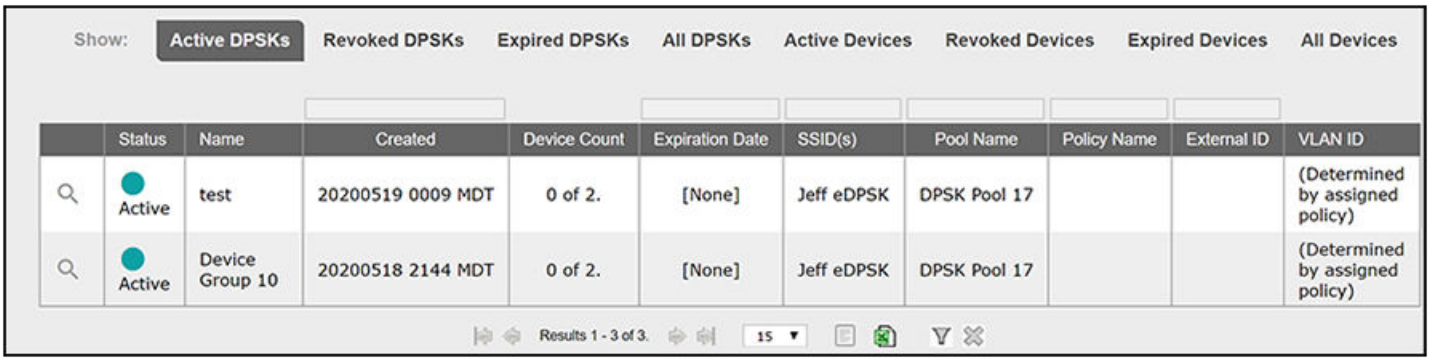


DPSKs

The DPSKs tab provides information about all the dynamic pre-shared keys (DPSKs) in the system. DPSKs are used with the external Dynamic Pre-shared Key (eDPSK) feature of Cloudpath.

The following screen is an example of the information provided from the DPSKs area of the dashboard:

FIGURE 53 DPSKs Table Example

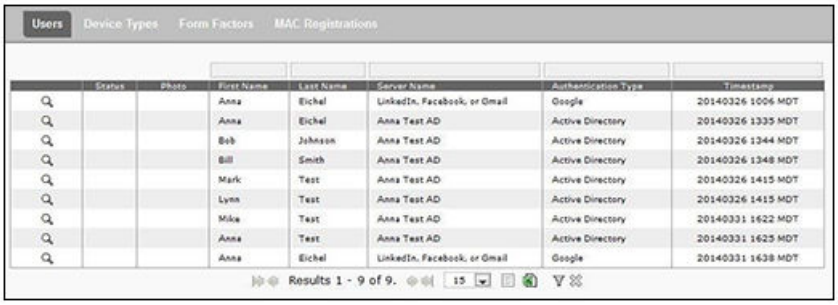


For more information, refer to the *Cloudpath Enrollment System eDPSK Configuration Guide*.

Users & Devices

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

FIGURE 54 User Table

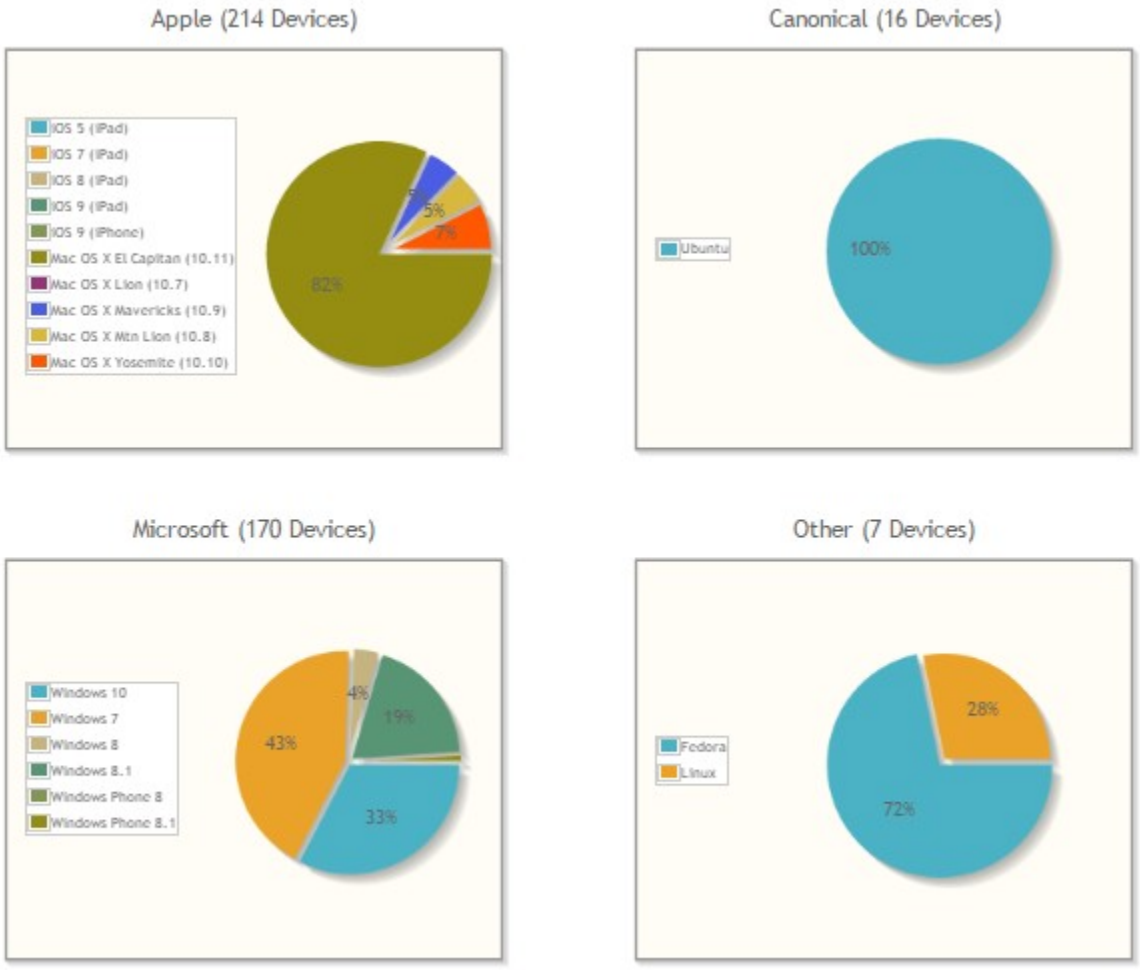


NOTE
Use the view icon to display further details about a specific user record, to block the user, or to remove the user record from the database.

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.

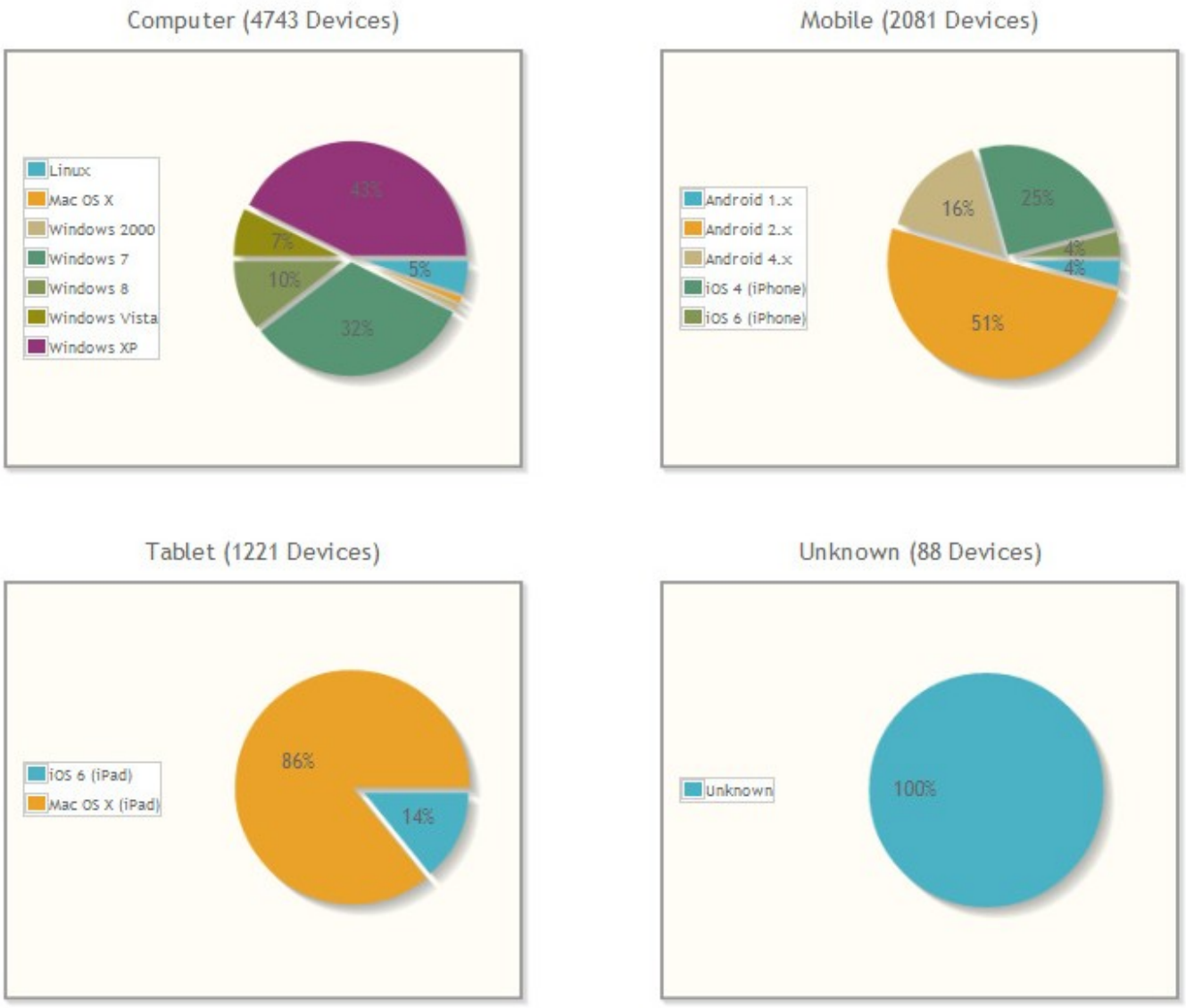
FIGURE 55 Device Types



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 56 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.

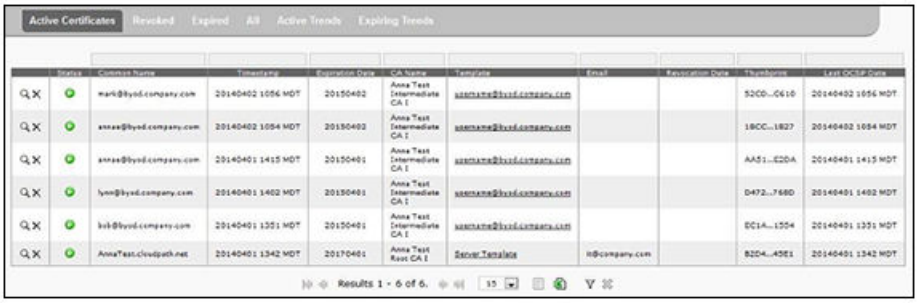
Certificates

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 57 Certificates Table

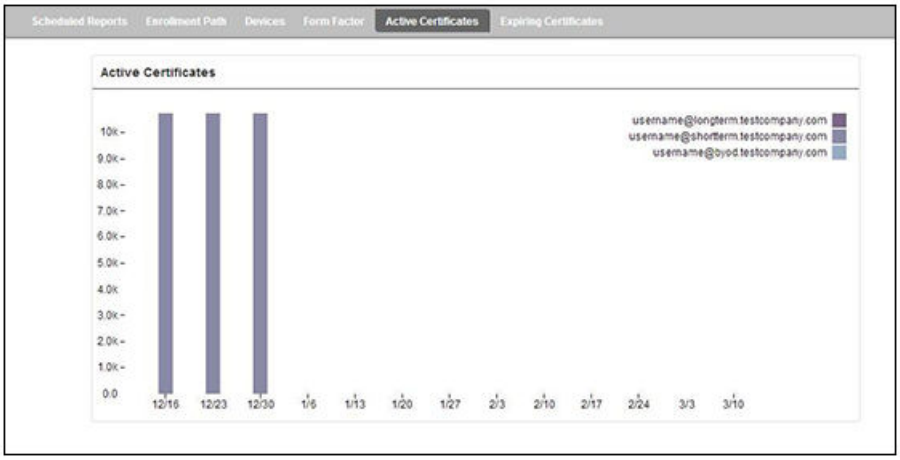


NOTE
Use the view icon to display further details about a specific certificate record, to disable or revoke the certificate, to download the certificate, or to remove the user record from the database.

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 58 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 59 Expiring Certificates

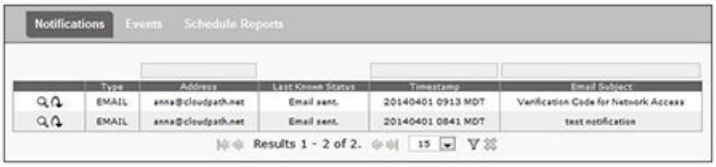
Notifications

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 60 Notifications Table



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

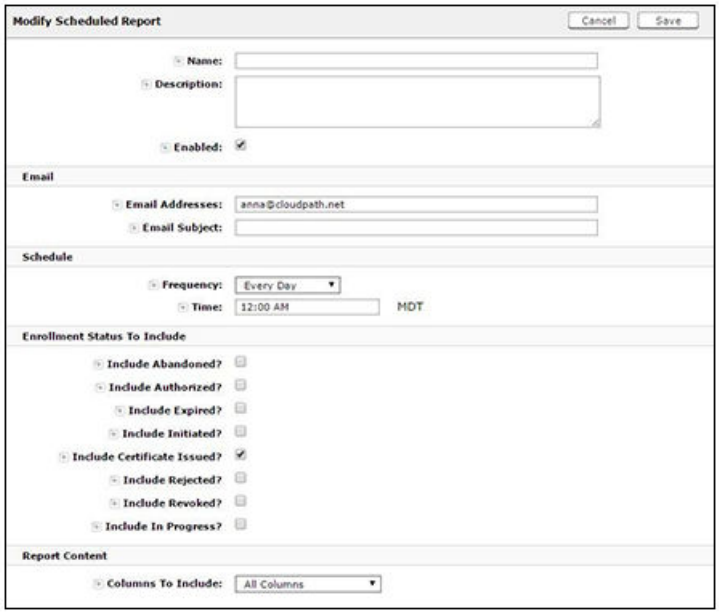
The scheduled report feature allows you to schedule a task to export enrollment record data, by date, or schedule a recurring export. For example, you might schedule an enrollment data report to occur on a weekly, or daily basis. This report can be emailed to one or multiple email addresses.

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 61 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.

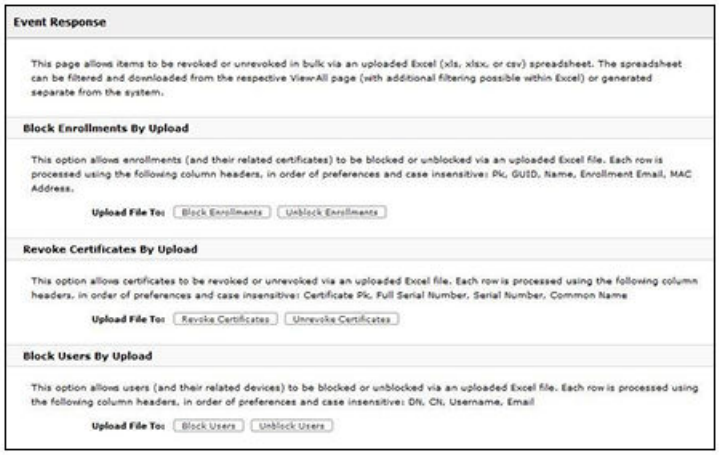
FIGURE 62 Scheduled Report

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 63 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.

VLAN Assignments

The VLAN Assignments tab provides complete information about VLANs available, assigned, users for each VLAN, and so on

For more information, refer to the *Cloudpath Enrollment System Deployment Administration Guide*, "Auto VLAN" chapter.

Traffic Monitor

The Traffic Monitor tab contains a traffic dashboard and a metric analyzer.

Use the two tabs and their respective settings to display the information you want. An example from both the traffic dashboard and metric analyzer are shown below:

FIGURE 64 Traffic Dashboard Example

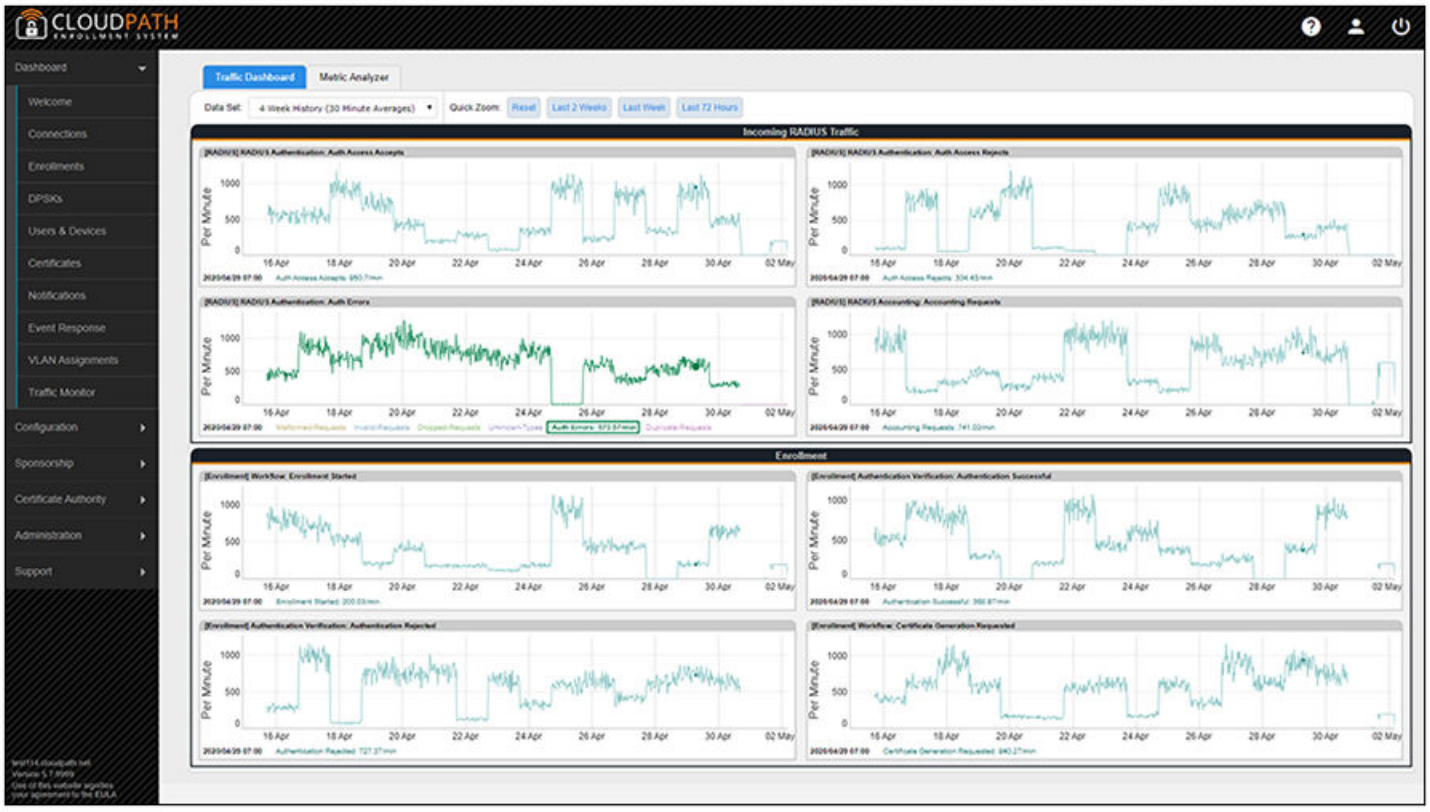
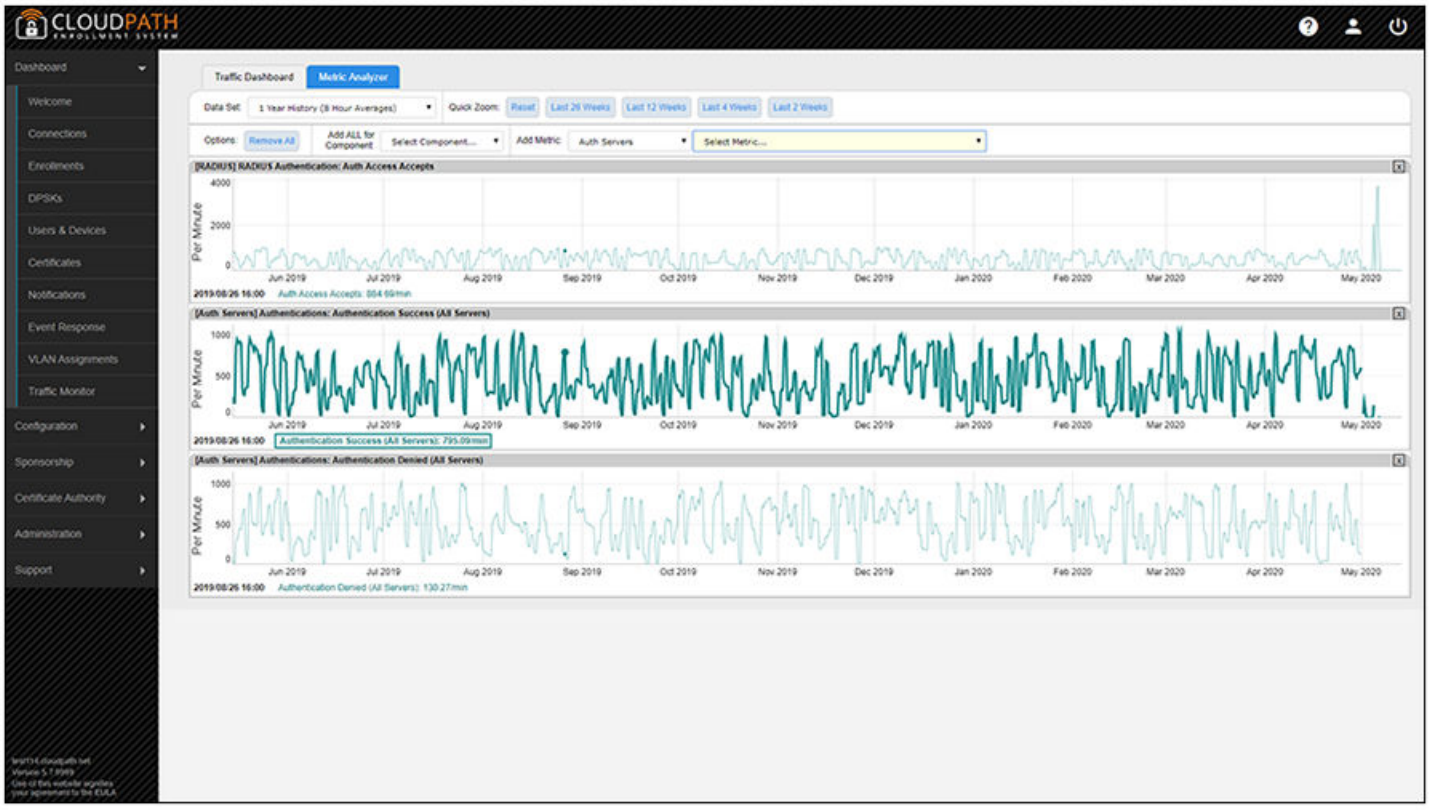


FIGURE 65 Metric Analyzer Example



Support

- Overview..... 81

Overview

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

Documentation

The **Documentation** page contains a link to the Cloudpath technical documents.

Licensing

The **Licensing** page contains two tabs ("License" and "Details") that display information about the type and number of Cloudpath licenses, active certificates, usage statistics, and copyright notices.

FIGURE 66 Licensing Information Page - License Tab Example

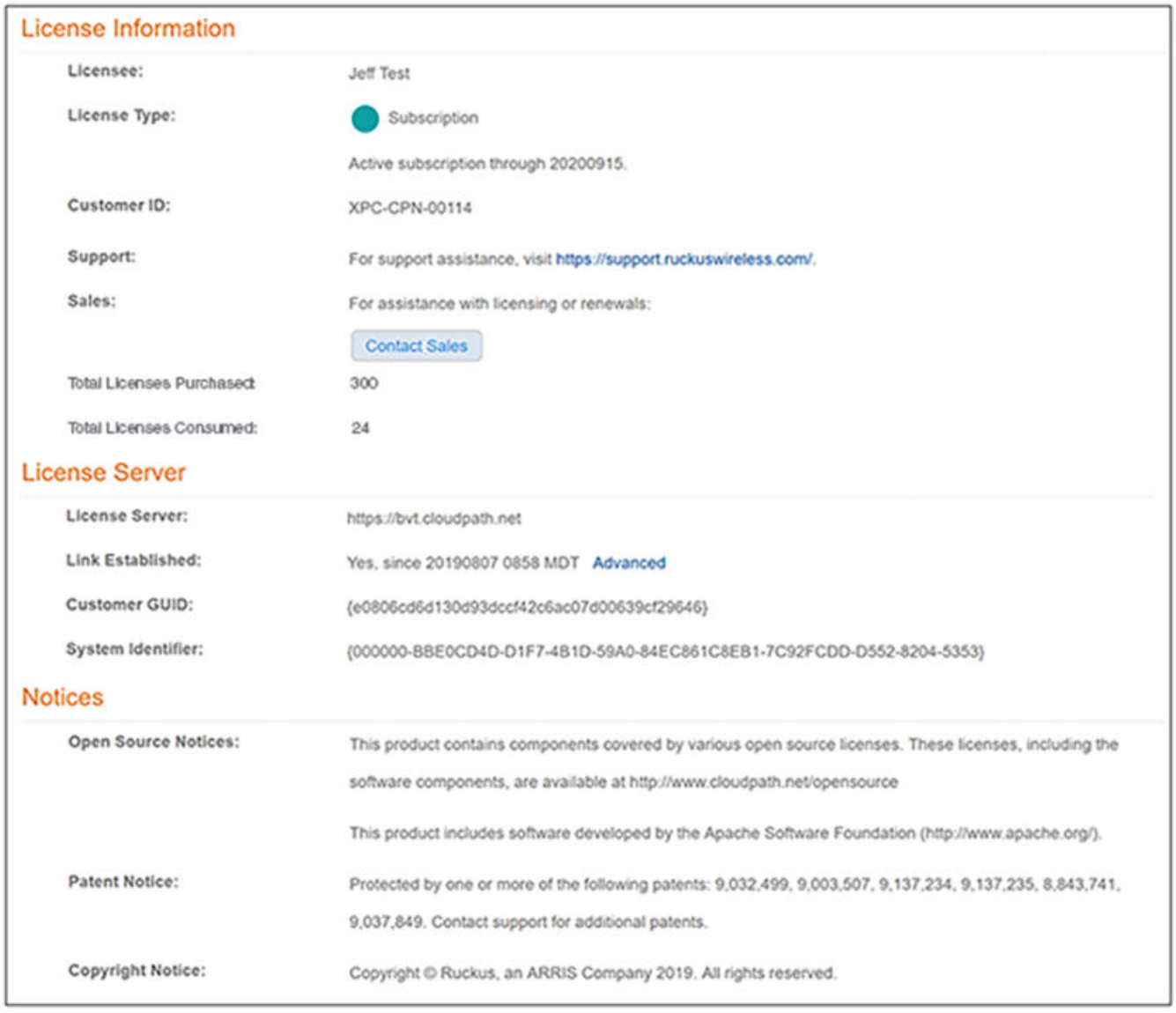


FIGURE 67 Licensing Information Page - Details Tab Example

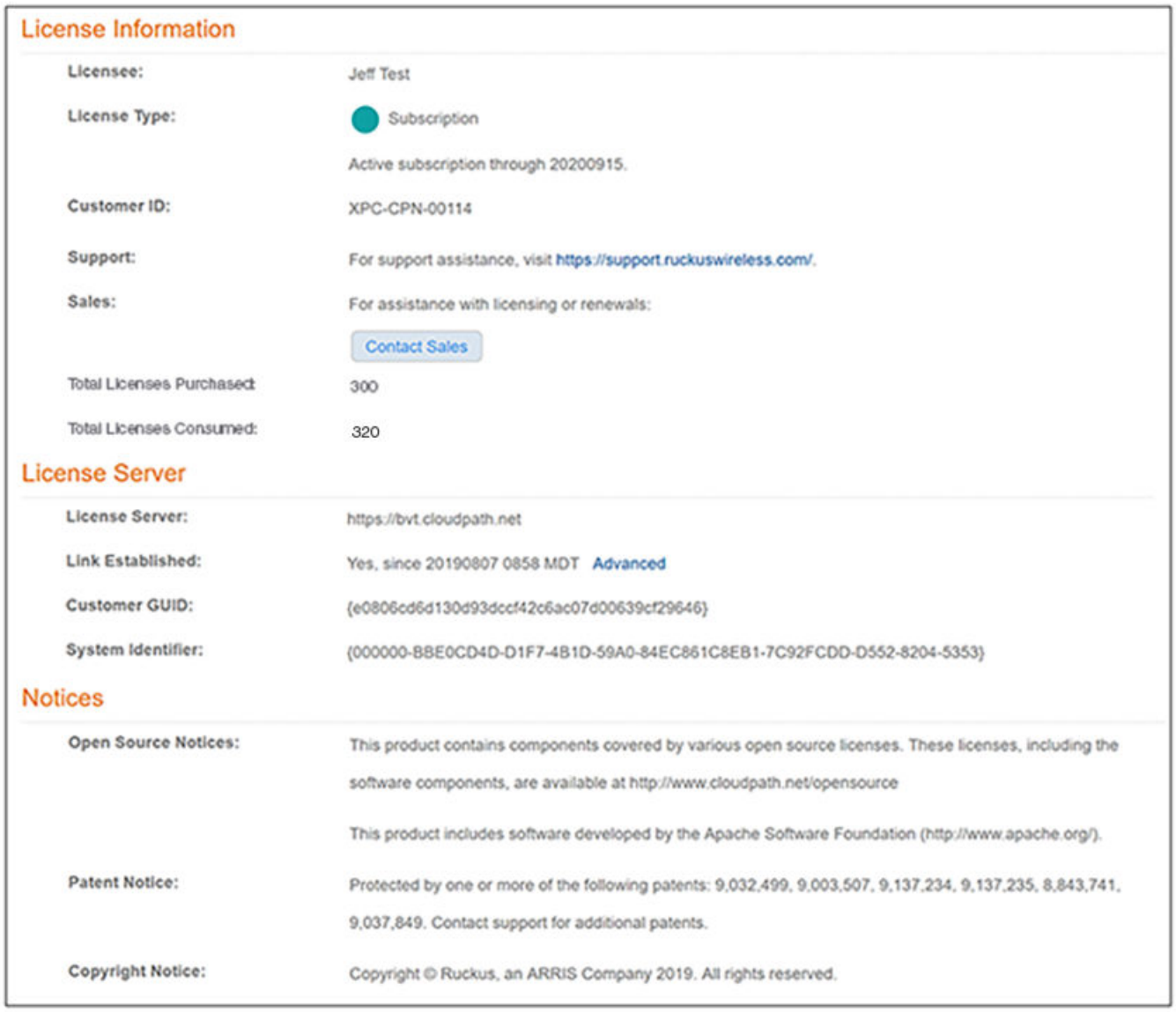
What Happens If More Licenses Are Being Consumed Than Have Been Allocated?

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 licenses consumed exceeding the number of total licenses purchased for an existing Cloudpath system:

FIGURE 68 Example of Total Licenses Consumed Exceeding Limit



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 69 License-Consumption Banner on Welcome Page When Consumption Exceeds Limit

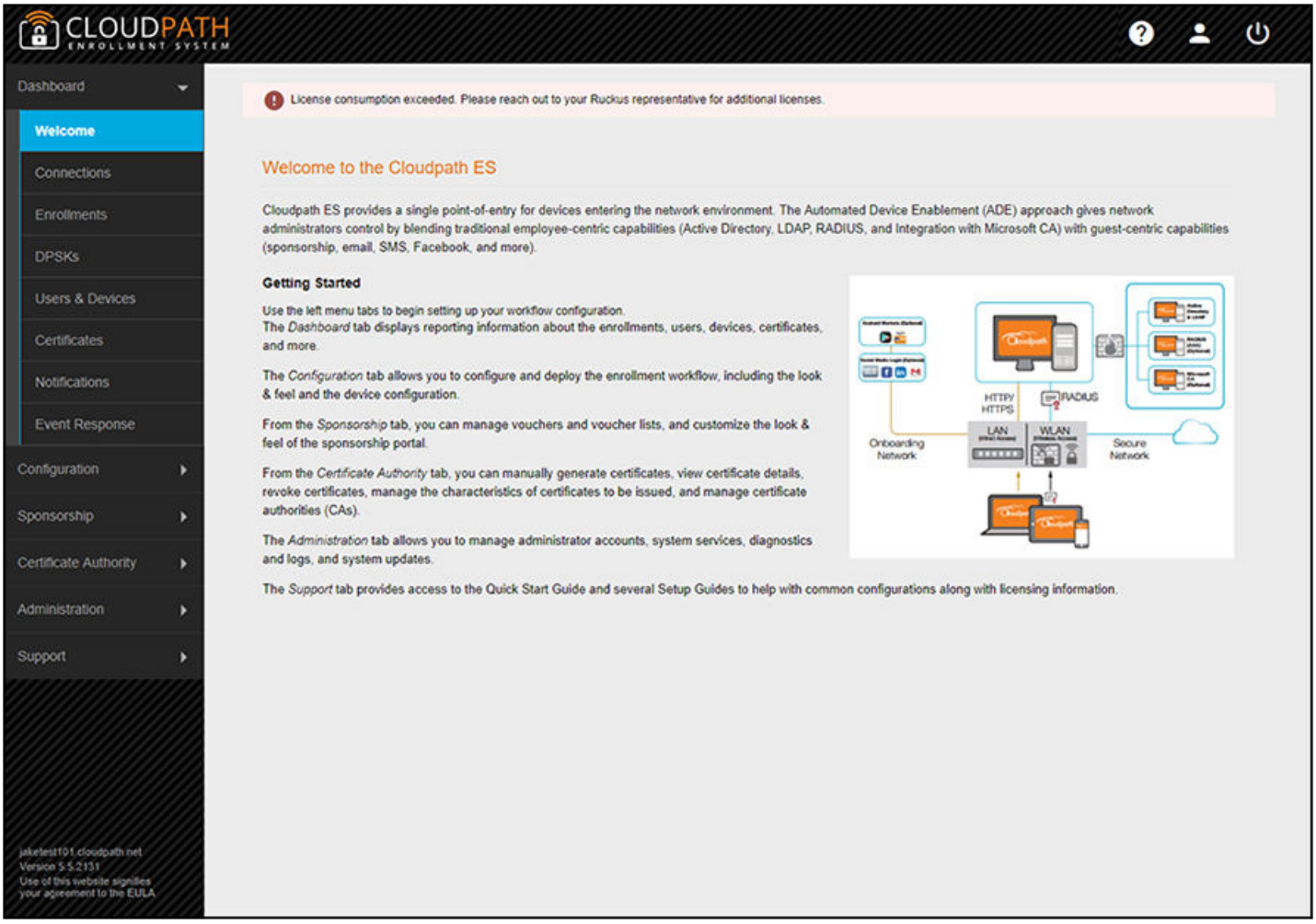
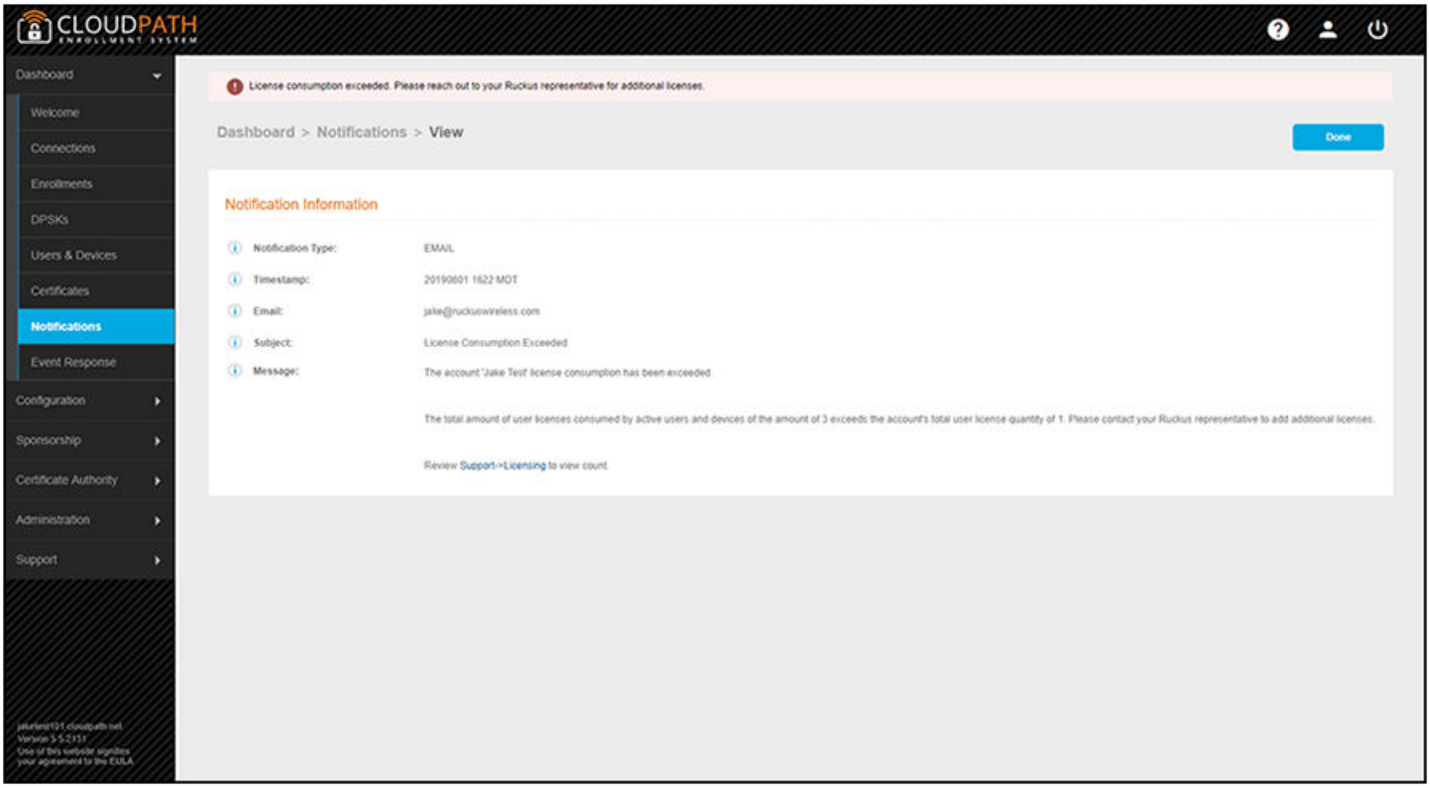


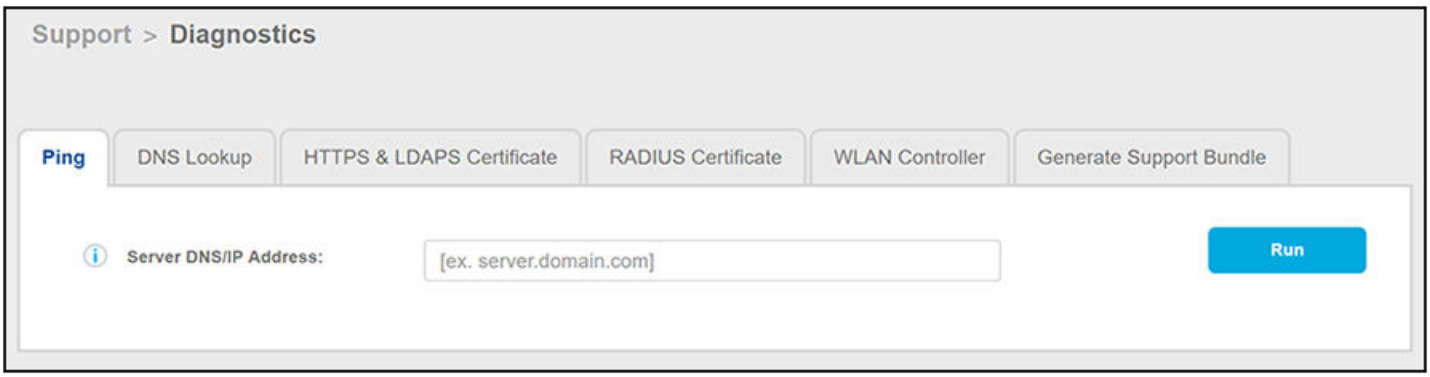
FIGURE 70 License-Consumption Banner in Notifications When Consumption Exceeds Limit



Diagnostics

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

FIGURE 71 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	Summary
On-Premise Installation	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	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	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	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	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, 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. 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.

Cloudpath Video Tutorials

Title	Summary
Cloudpath Authentication Using MAC Addresses	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. 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.
Cloudpath Auto-Branching	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.
Cloudpath Authentication Methods for Guest User Access	This video shows you how to build a workflow branch for providing guest user access. Three sub-branches are shown: • Using the “Authenticate using a voucher from a sponsor” plug-in step, which involves sending a voucher to the user. • 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." The video also shows creating voucher lists and adding sponsors for specific voucher lists.
Customizing Your Cloudpath Onboarding Landing Pages	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	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	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	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.

Title	Summary
Configuring Notifications with Cloudpath Enrollment System	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. 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.

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