

Cloudpath Quick Start Guide

Supporting Software Release 5.2

Copyright, Trademark and Proprietary Rights Information

© 2018 ARRIS Enterprises LLC. 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 ARRIS International plc and/or its affiliates ("ARRIS"). ARRIS reserves the right to revise or change this content from time to time without obligation on the part of ARRIS 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, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS 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 ARRIS 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, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgellon, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Cloudpath Security and Management Platform.....	5
Overview.....	5
Cloudpath System Specifications.....	6
Prerequisites for Configuring Cloudpath.....	6
Deploying the OVA (For Local Deployments).....	6
Setting up the Initial Account.....	7
Configuring the Workflow.....	7
Deploying the Cloudpath Virtual Appliance to a VMware Server.....	9
Overview.....	9
Specifications for Locally-Deployed VMware Servers.....	9
Retrieve OVA File With Activation Link.....	9
Deploying the Virtual Appliance Using a vCenter VMware Client.....	9
Deploying the Virtual Appliance Using a VMware vCenter Client.....	10
Application Properties (vCenter).....	10
Confirm Deployment Settings (vCenter).....	13
Deploying the Virtual Appliance Using a Console-Based VMware Client.....	14
Service Account.....	14
Activate Account or Log In.....	15
Overview.....	15
Activate Account by Activation Code.....	15
Set a Password for Account.....	16
Activate Account by Credentials.....	16
Initial System Setup.....	19
Overview.....	19
System Setup Wizard.....	20
Publishing Tasks.....	27
ToDo Items.....	29
About the Enrollment Workflow.....	31
Overview.....	31
Workflow Basics.....	31
Modifying a Workflow Template.....	32
Creating a Workflow From a Blank Slate.....	34
Acceptable Use Policy.....	36
User Type Split.....	37
Authentication to a Local Server.....	37
Device Type Split.....	39
Create a Filter in the Device Type Split.....	39
Prompt for Voucher.....	41
Device Configuration and Client Certificate.....	44
Device Configuration.....	44
Client Certificates.....	45
How to Set Up Client Certificate Templates.....	46
Publishing the Enrollment Workflow.....	49
How to Test a Published Workflow.....	50

Administration.....	51
Administration Overview.....	51
Administrators.....	51
Company Information.....	52
System Services.....	52
System Updates.....	53
Replication.....	53
Data Cleanup.....	53
Firewall Requirements.....	54
Configuration.....	55
Overview.....	55
Device Configurations.....	55
RADIUS Server.....	55
Authentication Servers.....	57
Firewall & Web Filter Integration.....	57
MAC Registration Lists.....	57
API Keys.....	57
Dashboard.....	59
Overview.....	59
Enrollments.....	59
Records Export.....	60
Enrollment Paths.....	60
Connections.....	61
Users & Devices.....	62
Device Types.....	63
Form Factors.....	63
MAC Registrations.....	64
Certificates.....	64
Certificates Table.....	65
Active Trends.....	65
Expiring Trends.....	66
DHCP Fingerprints.....	67
Notifications.....	67
Notification Records.....	67
Events.....	68
Schedule Reports.....	68
Event Response.....	70
Support.....	73
Overview.....	73
Documentation.....	73
Licensing.....	73
Diagnostics.....	74
Advanced Support.....	75

Cloudpath Security and Management Platform

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

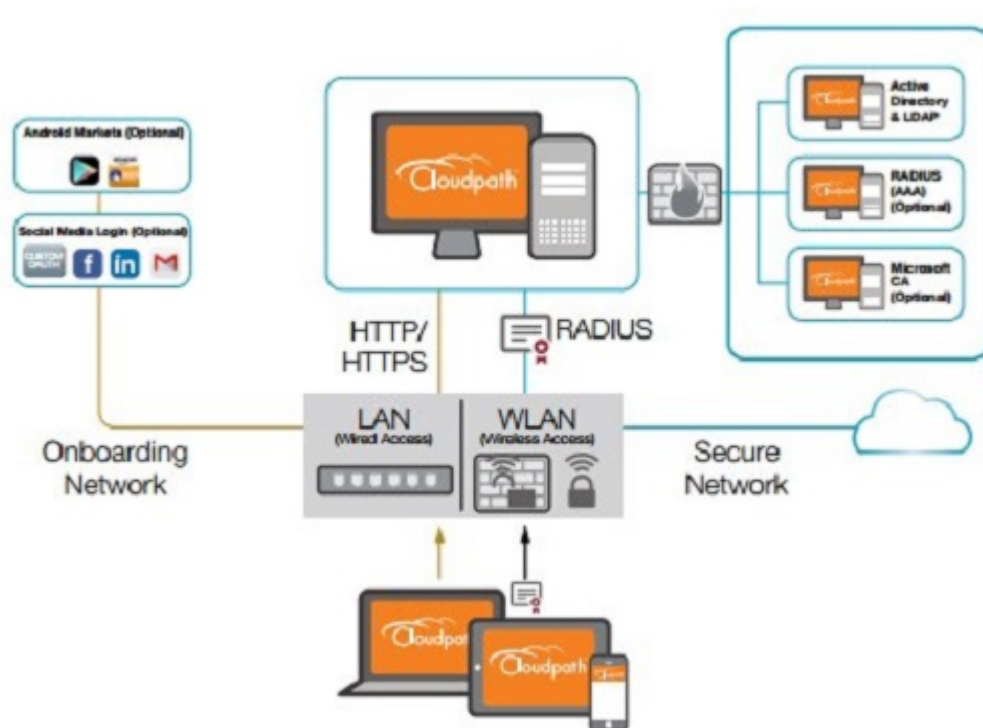
Overview

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

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

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

FIGURE 1 Cloudpath Security and Policy Management Platform



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

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

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

Cloudpath System Specifications

Cloudpath supports the following browser, operating systems, and third-party identity stores for system and user devices. Cloudpath supports the following browser, 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 XP SP2 and later	Microsoft Active Directory
Firefox 1.5 and later	Mac OS X 10.7 and later	LDAP
Safari 2.0 and later	Apple iOS 6.0 and later	Facebook
Google Chrome 3.0 and later	Ubuntu 12.04 and later	LinkedIn
	Android 4.03 and later	Google Gmail
	Fedora 18 and later	Custom OAuth 2.0 Server
	Chrome OS	
	Windows Phone 8.1	
	Blackberry (assisted configuration)	
	Windows RT (assisted configuration)	
	Generic (assisted configuration)	
	Windows Mobile 5 and 6 (assisted configuration)	

NOTE

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

Prerequisites for Configuring Cloudpath

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

Deploying the OVA (For Local Deployments)

- VMware server or Microsoft Hyper-V Manager on which you'll install the Cloudpath virtual appliance.
- The URL where the image file resides
- FQDN Hostname of the virtual appliance
- IP address and subnet mask for the virtual appliance (not required if using DHCP)

- Gateway IP address for your network (not required if using DHCP)
- IP address of DNS server (not required if using DHCP)
- A list of IP addresses that are allowed Administrative access (optional)
- Service account security credentials

Setting up the Initial Account

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

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

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

Configuring the Workflow

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

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

NOTE

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

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

Deploying the Cloudpath Virtual Appliance to a VMware Server

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

Overview

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

NOTE

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

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

Specifications for Locally-Deployed VMware Servers

The Cloudpath virtual appliance is deployed as an open virtualization archive (OVA) file, which can be deployed on any VMware ESXi server (ESX or ESXi architecture 4.x and 5.x and greater).

NOTE

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

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

Retrieve OVA File With Activation Link

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

Deploying the Virtual Appliance Using a vCenter VMware Client

The deployment process consists of the following steps:

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

or

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

Deploying the Virtual Appliance Using a VMware vCenter Client

1. Open the VMware client.
2. Select **File > Deploy OVF Template**.
3. Enter the file path or URL where the OVA file resides.
4. Accept the EULA.
5. Enter a unique name for the virtual appliance.
6. Select a deployment configuration:
 - Non-Production POC - Deploys using 6GB RAM and 2 vCPUs x 1 Core. Recommended for software trials, feature testing, and other non-production systems.
 - 4,000 or Fewer Users - Deploys using 8GB RAM and 2 vCPUS x 2 Cores. Recommended for production systems with fewer than 4,000 users.
 - 8,000 or Fewer Users - Deploys using 12GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with fewer than 8,000 users.
 - More than 8,000 Users - Deploys using 16GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with more than 8,000 users.
 - More than 20,000 Users - Deploys using 20GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with more than 20,000 users.
7. If you are using VMware vCenter™ Server to manage your virtual environment, select the appropriate data center, cluster, host, and destination storage, as needed.
8. Select a disk format.
 - Use **Thick** provisioning for a production environment. For a thick provision, the total space required for the virtual disk is allocated during creation.

NOTE

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

- Use **Thin** provisioning for testing, or if disk space is an issue. A thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.
9. Continue the configuration with vCenter, or a non-vCenter console.
 - If you are using the vCenter to configure application and network properties, continue to the next section.
 - If you are using the console to configure application and network properties, review the initial settings and click **Finish**. See *Deploying the Virtual Appliance Using a Console-Based VMware Client* to complete the deployment process.

Application Properties (vCenter)

Customize the application properties for the deployment.

FIGURE 2 Application Properties

Cloudpath Enrollment System

Hostname (FQDN)

Enter the fully qualified domain name.

IP Address

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

Netmask

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

Default Gateway

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

DNS

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

NTP Server

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

Enable HTTPS?

Timezone

SSH Access

Restrict admin access?

To restrict the admin web UI to certain addresses or subnets, specify a comma-separated list of addresses or subnets (CIDR notation, ex. 192.168.4.1/22).

Console Password

Specify the password to be used to access the console or SSH of this VM. Please select a strong password that is compliant with your password complexity policy.

Enter password

Confirm password

Enter a string value with 1 to 100 characters.

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

NOTE

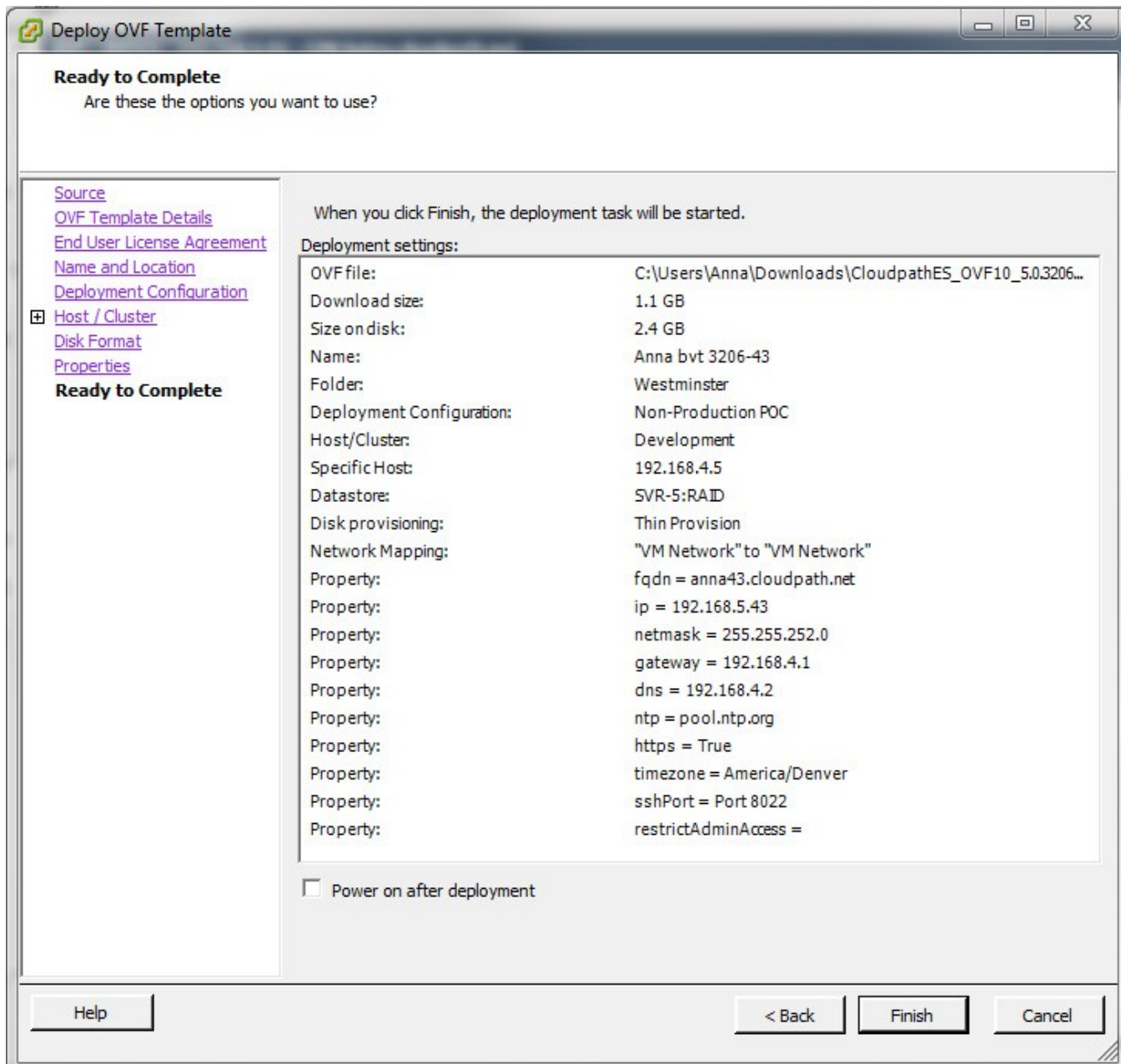
The Cloudpath Hostname is used as the default OCSP Hostname, which is embedded into certificates issued by the onboard root CA as part of the URL for the Online Certificate Status Protocol (OCSP).

2. Enter the **IP Address, Netmask, Default Gateway**, and the **DNS Servers** for this VM. Leave blank for DHCP.
3. Specify an **NTP Server** or leave the default.
4. HTTPS is enabled by default. Leave unchecked only if Cloudpath is behind another web server using SSL.
5. Select the **Timezone**.
6. Select **SSH port**, or disable **SSH Access**.
7. Enter the IP address(es) that can access the **Cloudpath Admin UI**. Leave this field blank if you do not want to limit administrative access.
8. Enter and confirm a service user password. The service user account is used by your support team for access to this system using SSH. The service account is not available if **SSH access** is not permitted.

Confirm Deployment Settings (vCenter)

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

FIGURE 3 Deployment Settings



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

Deploying the Virtual Appliance Using a Console-Based VMware Client

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

1. Open a console for the VM.
2. Enter **yes** (or **y**) to accept all license agreements.
3. Enter the time zone. For example, enter **America/Denver**.
4. Enter the **FQDN hostname** for the virtual appliance (for example, **onboard.company.com**).
5. Do you want to enable HTTPS? Enter for **yes** (default) or **n**.
6. Do you want to use a STATIC IP (rather than DHCP)? Enter for **yes** (default) or **n**.
 - If you enter **yes** (recommended), you assign the IP address of the virtual appliance, subnet mask, and gateway and DNS server IP addresses for your network.
 - If you enter **no**, DHCP is used to assign IP address of the virtual appliance interface (ens for VMware, eth0 for Hyper-V), subnet mask, gateway, and DNS server IP addresses for your network. If you are not using DHCP, enter the IP address of the virtual appliance interface.
7. Enter the IP address of the virtual appliance.
8. Enter a subnet mask in the format 255.255.252.0.
9. Enter the gateway IP address for your network.
10. Enter the DNS server IP address.
11. Do you want to permit SSH access? Enter **yes** (default) or **n**.
12. Enter and confirm a service password. The service password is used by your support team for access to this system using SSH. Refer to the *Cloudpath Command Reference* on the **Support** tab for details.

NOTE

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

13. Do you want to use an NTP server other than `pool.net.org`? Enter **no** (default) or **y** to specify an NTP server. The setup is complete. Press **Enter** to reboot the system. After the reboot you are presented with the shelluser login prompt.

NOTE

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

Service Account

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

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

Activate Account or Log In

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

Overview

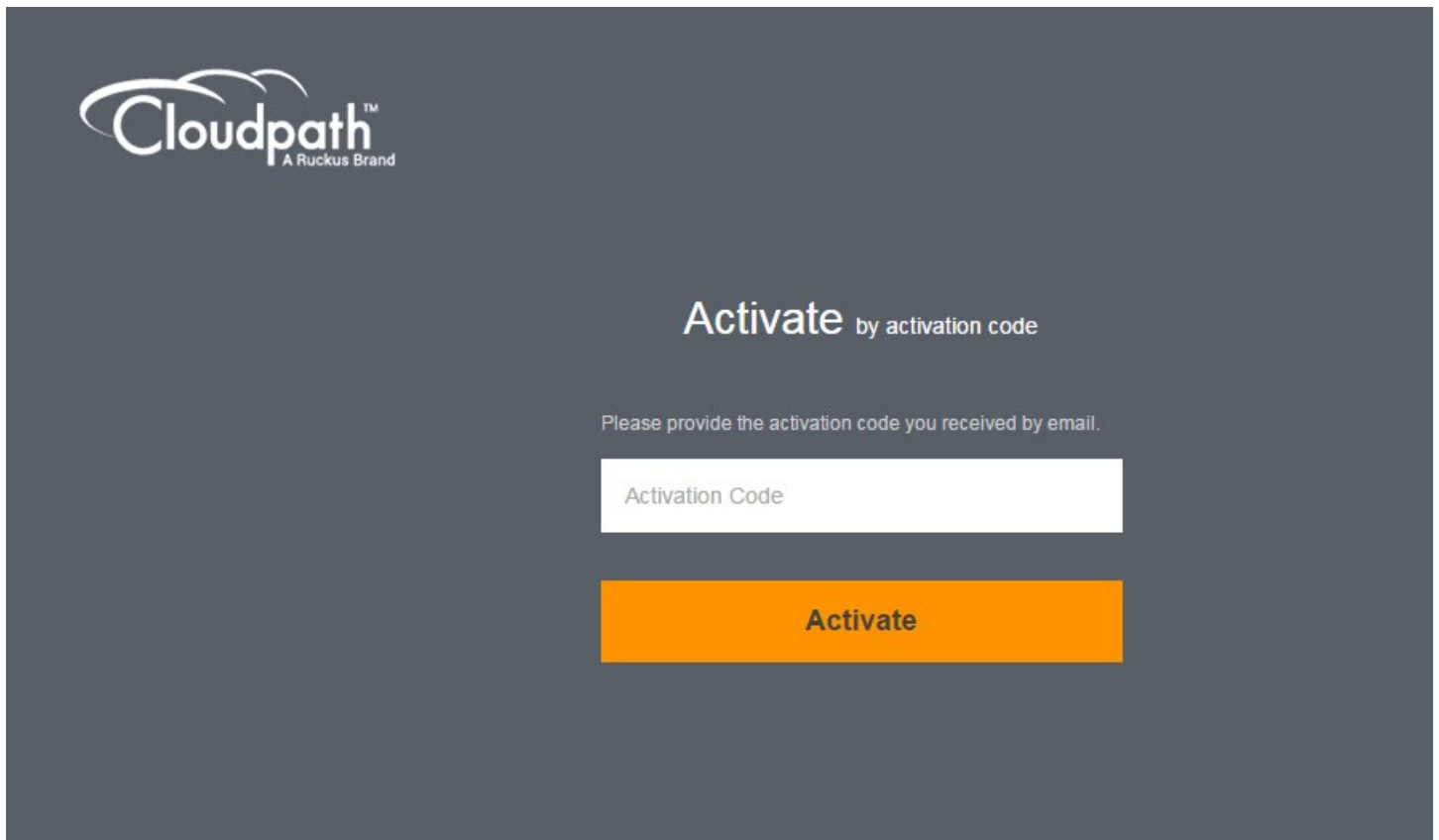
If you are setting up a Cloudpath account for the first time, you will be sent an activation code. If you have existing Cloudpath License server credentials, you can activate an account using those credentials.

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

Activate Account by Activation Code

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

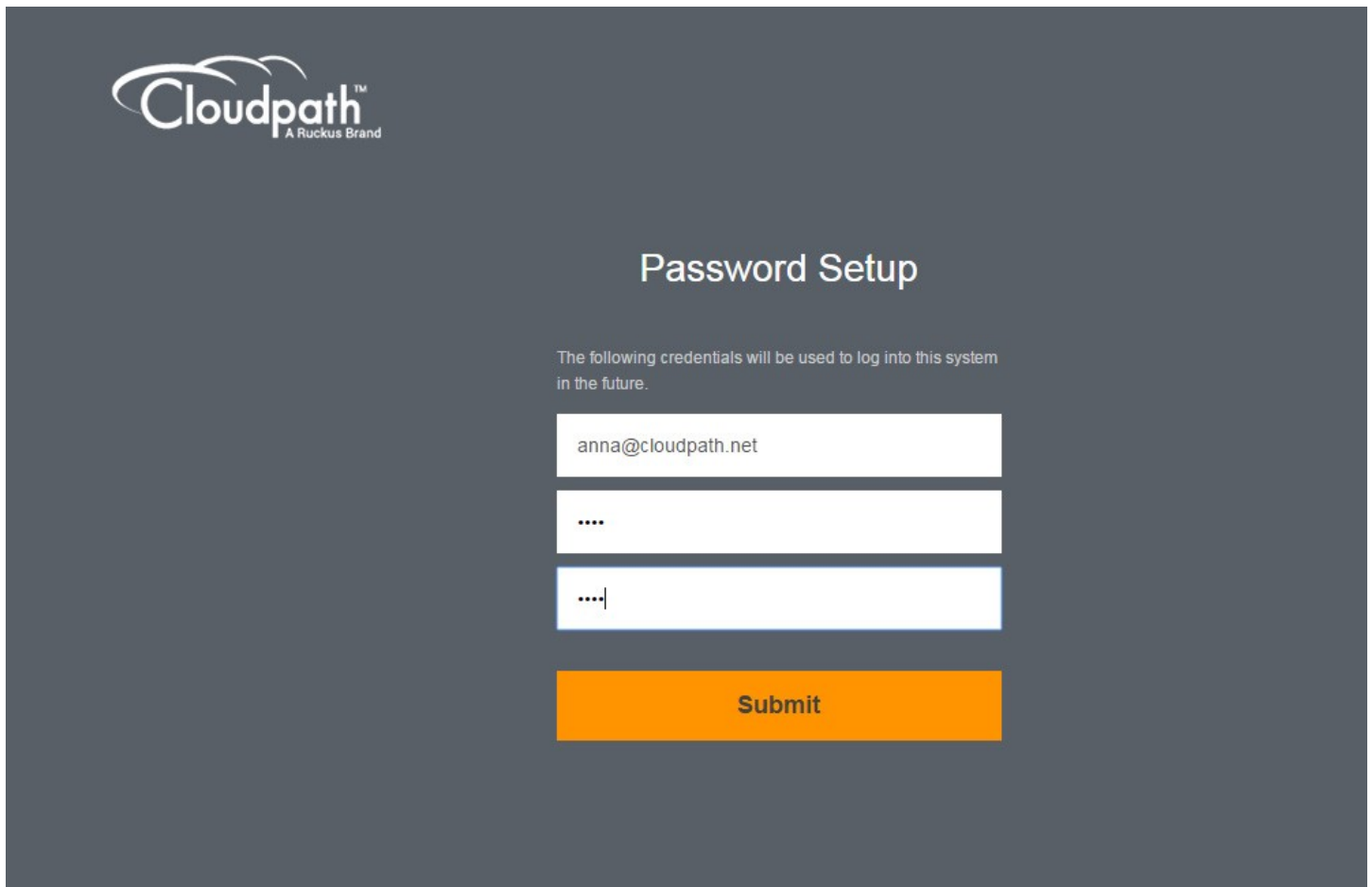
FIGURE 4 Activate Cloudpath Account



Set a Password for Account

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

FIGURE 5 Set Password



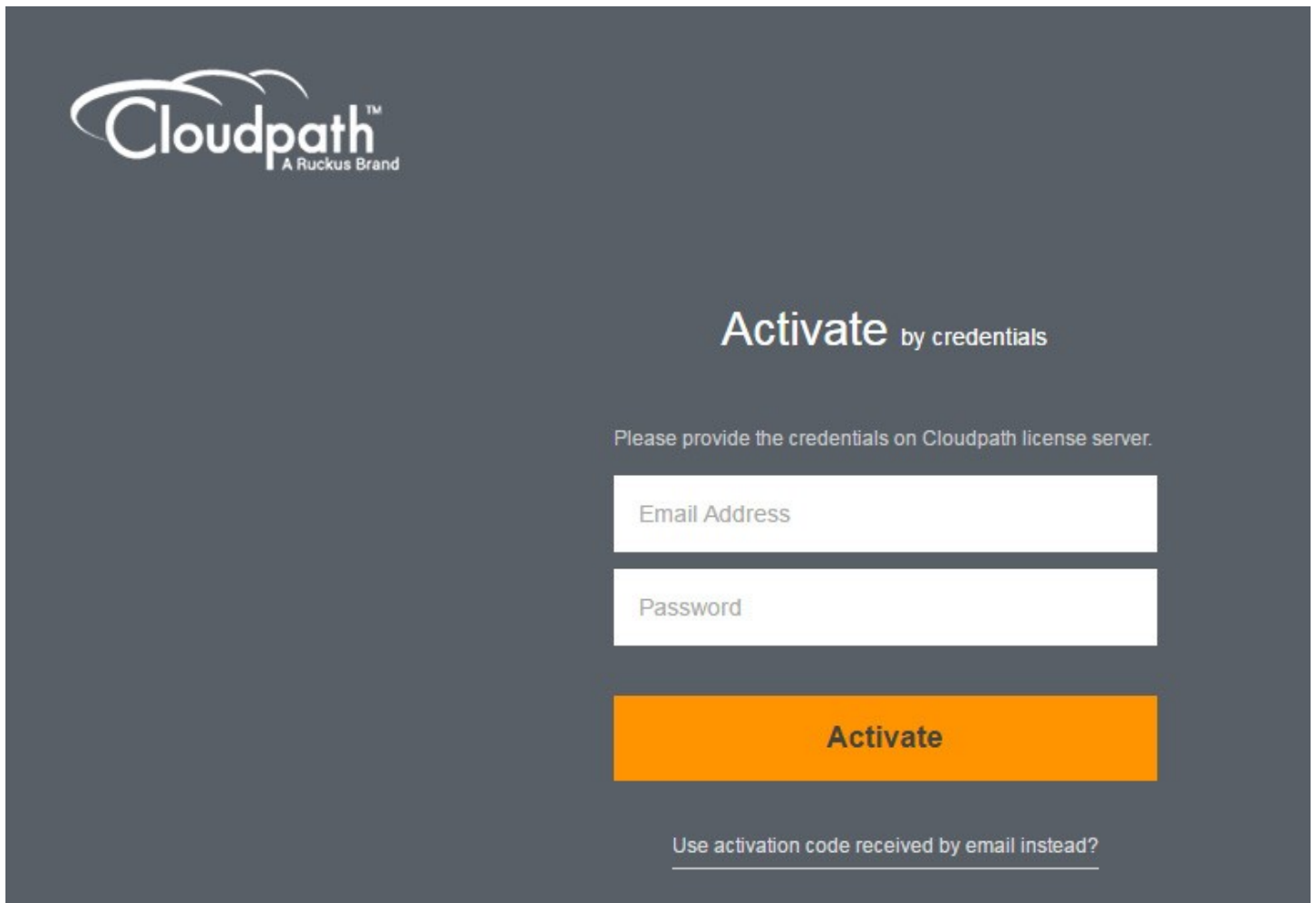
1. Your email address should display. If it does not, enter it on this page.
2. Enter and confirm a password.

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



The screenshot shows a dark gray web interface for activating a Cloudpath account. In the top left corner is the Cloudpath logo, which includes the text 'Cloudpath™' and 'A Ruckus Brand' below it. The main heading is 'Activate by credentials' in a large, white, sans-serif font. Below the heading is a line of smaller white text: 'Please provide the credentials on Cloudpath license server.' There are two white input fields: the first is labeled 'Email Address' and the second is labeled 'Password'. Below these fields is a prominent orange button with the word 'Activate' in white, bold, sans-serif font. At the bottom of the form, there is a white underlined link that reads 'Use activation code received by email instead?'.

Initial System Setup

- Overview..... 19
- System Setup Wizard..... 20
- Publishing Tasks.....27
- ToDo Items..... 29

Overview

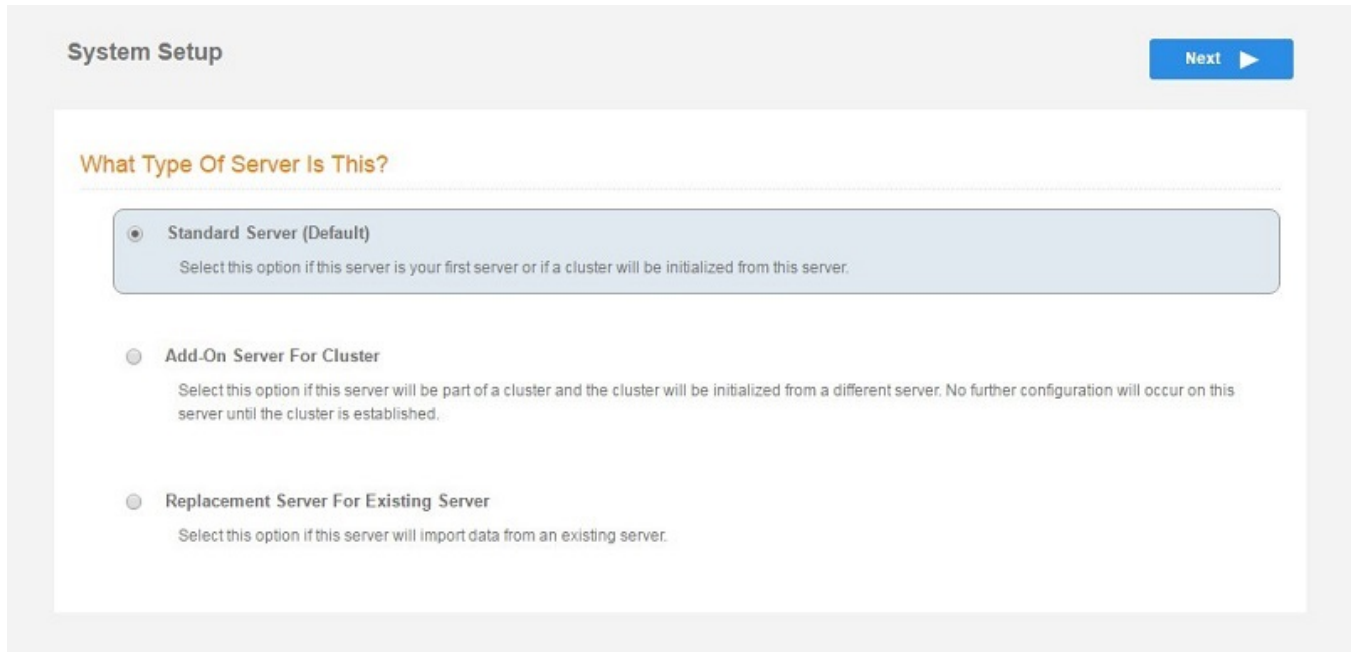
Cloudpath provides you with a single administrator login for the Cloudpath Admin UI. Additional administrators can be added from the left menu Administration tab, or you can enable Administrator logins from your authentication servers.

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 Master server in the cluster.
- If you are setting up this server to replace an existing server, and you are importing the database from the existing server, select **Replacement Server for Existing Server**.

NOTE

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

2. Enter **Company Information**.

This information is embedded in the onboard root CA certificate.

FIGURE 8 Company Information

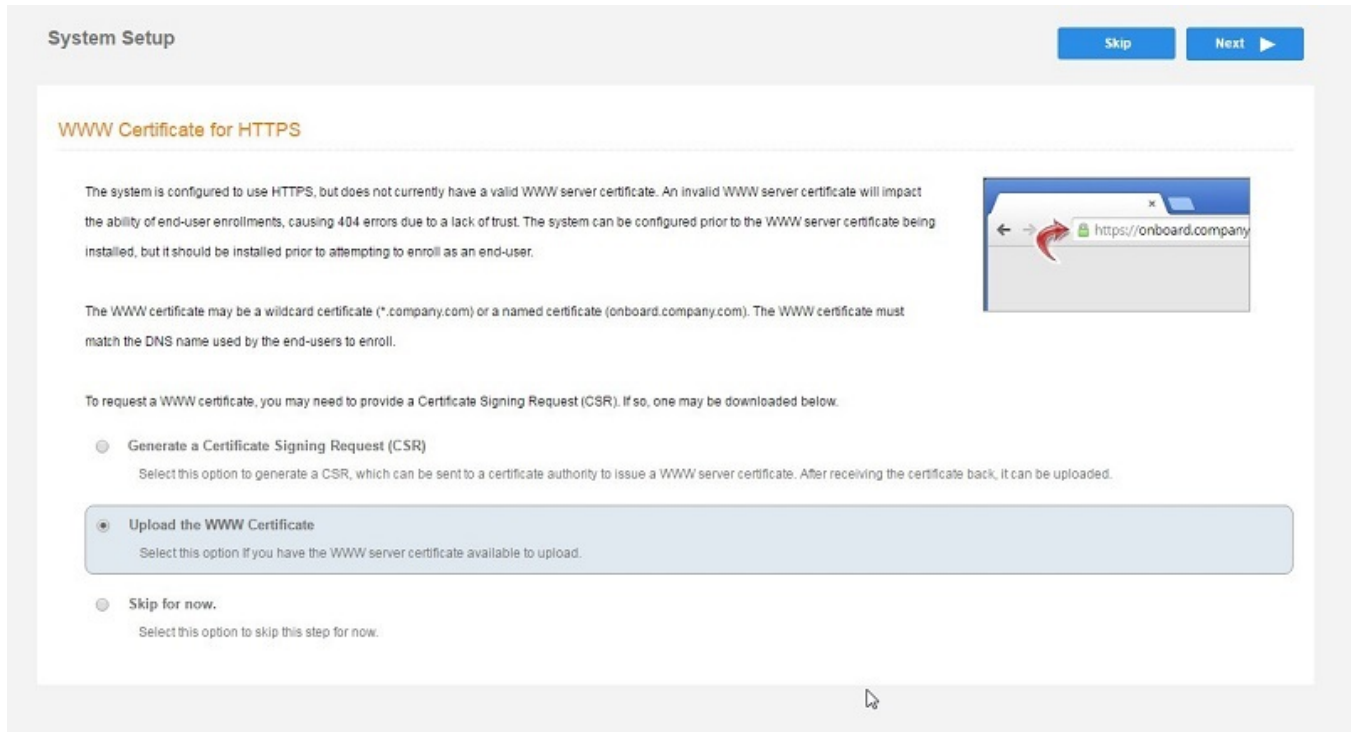
The screenshot shows a 'System Setup' wizard interface. At the top right, there is a blue 'Next' button with a right-pointing arrow. The main content area is divided into two sections: 'Company Information' and 'Company Web Presence'. Each section contains several input fields, each preceded by an information icon (i in a circle) and a dropdown arrow (▾). The 'Company Information' section includes: Company Name (Anna43 Test BVT), Legal Company Name (Sample Company, Inc.), Department Name (IT), City (Westminster), State/Province (Colorado), and Country (US). The 'Company Web Presence' section includes: Company Domain (company.com), Support Email (support@company.com), and IT Email (it@company.com). At the bottom left of the form area, the text 'Sample Data' is visible.

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

3. Configure the WWW Certificate

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

FIGURE 9 WWW Certificate for HTTPS



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

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

4. Upload the WWW certificate.

FIGURE 10 Upload WWW Certificate

The screenshot shows the 'System Setup' wizard interface. At the top right, there are 'Back' and 'Next' buttons. The main content area is titled 'Upload by PEM Files' and contains the following text: 'If a p12 file is not available, you may upload the individual components of the certificate. All files must be in PEM (Base64) format. If the private key is password-protected, specify the password too. If the private key is not password-protected, leave the password blank.'

Below the text are several fields for uploading PEM files:

- Public Key (PEM): Choose File No file chosen
- Chain (PEM or P7b): Choose File No file chosen
- Additional Chain (Optional): Choose File No file chosen
- Additional Chain (Optional): Choose File No file chosen
- Private Key (PEM): Choose File No file chosen
- Private Key Password: [Text Input Field]
- Prompt for Password on Boot:

Below these fields is the 'Upload by P12' section with the following text: 'You may upload a server certificate in p12 format. To do so, you must also specify the password if the p12 is password protected.'

Below the text are two fields for uploading a P12 file:

- P12 File: Choose File CloudpathLabWw...rtificate.p12
- P12 Password: [Text Input Field]

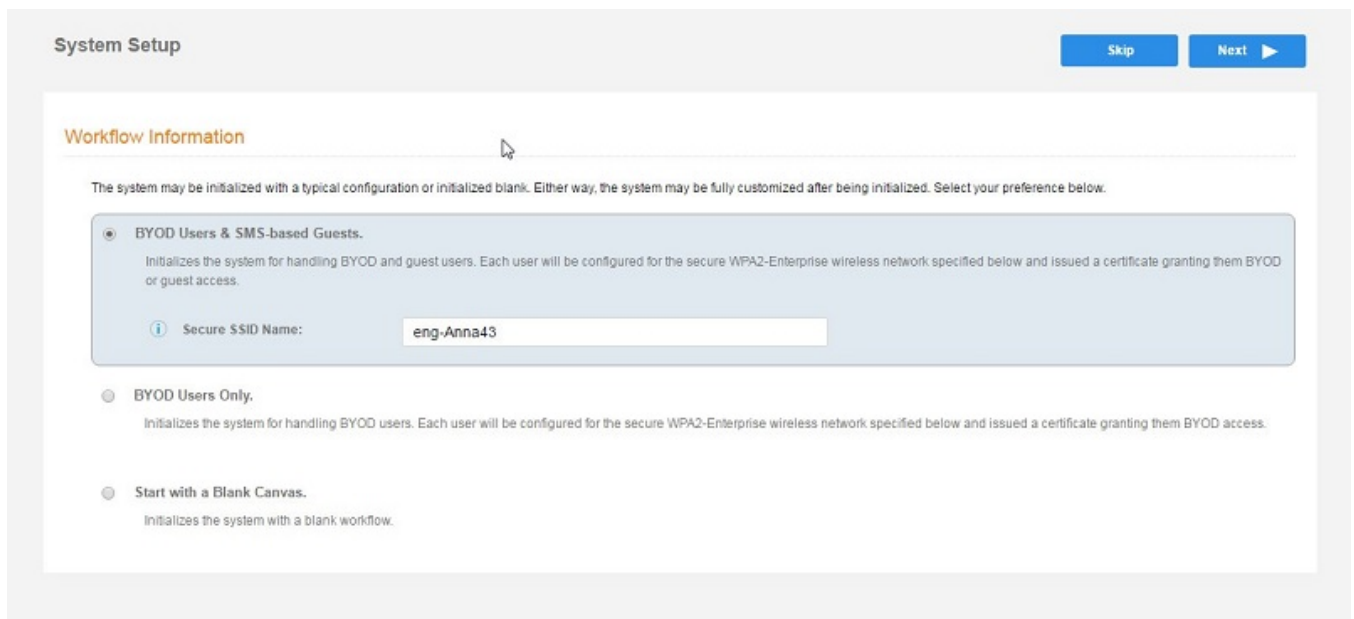
Browse to locate and upload the web server certificate and click **Next** to continue with the system setup.

5. Select the Default Workflow.

To initialize the system with a sample configuration, select **BYOD Users & SMS Guests**, or **BYOD Users Only**. This creates an initial workflow for BYOD users and sponsored guests (or BYOD users only) that you can use as a template, or simply add a device configuration and use immediately.

To create your own workflow, select **Start with a Blank Canvas**.

FIGURE 11 Select Default Workflow



6. Configure the Authentication Server.

NOTE

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

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

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

FIGURE 12 Authentication Server Setup

Authentication Server Configuration

Connect to Active Directory
Select this option to enable end-users to authenticate via Active Directory.

Default AD Domain

AD Host

AD DN

AD Username Attribute

Verify Account Status On Each Authentication

Perform Status Check

Additional Logins

Use For Admin Logins

Use For Sponsor Logins

Test Authentication

Run Authentication Test?

Connect to LDAP
Select this option to enable end-users to authenticate via LDAP (or LDAPs).

Connect to RADIUS
Select this option to enable end-users to authenticate via RADIUS using PAP.

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

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

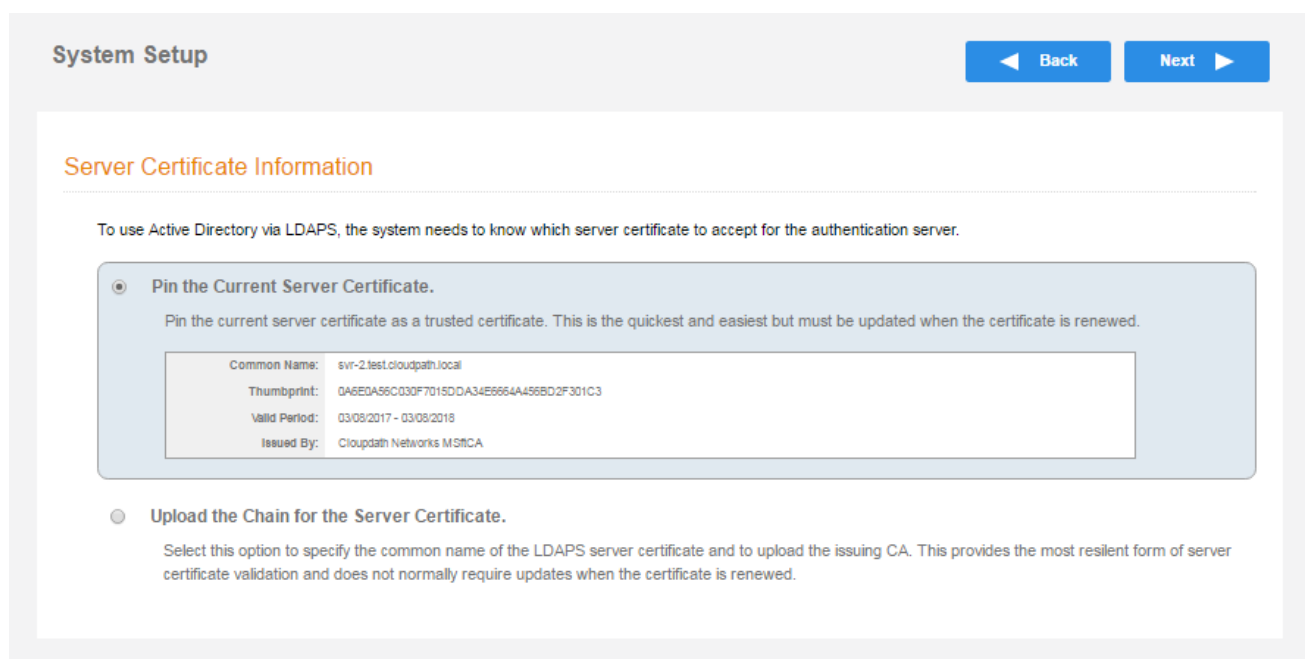
a) To setup the initial configuration of the Authentication Server, select and enter the required fields.

NOTE

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

- b) Consider these optional settings for the authentication server:
- **Verify Account Status on Each Authentication** - If selected, Active Directory is queried during subsequent uses of the certificate to verify the user account is still enabled. You must provide the bind username and password for an authentication server administrator account.
 - **Additional Logins** - If **Use for Admin Logins** is selected, administrators can log into the Cloudpath Admin UI using credentials associated with this authentication server. If **Use for Sponsor Logins** is selected, sponsors can log into the Cloudpath Admin UI using credentials associated with this authentication server.
 - **Test Authentication** - If selected, an authentication will be attempted using the username and password provided to test connectivity to the authentication server. This test can also be run from the workflow.
7. Set up the Authentication Server Certificate
- a) To use LDAP over SSL (LDAPS), the system must know which server certificate to accept for the authentication server.

FIGURE 13 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 14 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:	nhu0vjwqedwpptn7vuw
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/Anna248HyperVxpo/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/
Enrollments 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 15 Cloudpath Welcome Page

Welcome to the Cloudpath ES

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

Getting Started

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

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

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

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

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

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

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

About the Enrollment Workflow

• Overview.....	31
• Workflow Basics.....	31
• Modifying a Workflow Template.....	32
• Creating a Workflow From a Blank Slate.....	34
• Acceptable Use Policy.....	36
• User Type Split.....	37
• Authentication to a Local Server.....	37
• Device Type Split.....	39
• Prompt for Voucher.....	41
• Device Configuration and Client Certificate.....	44

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.

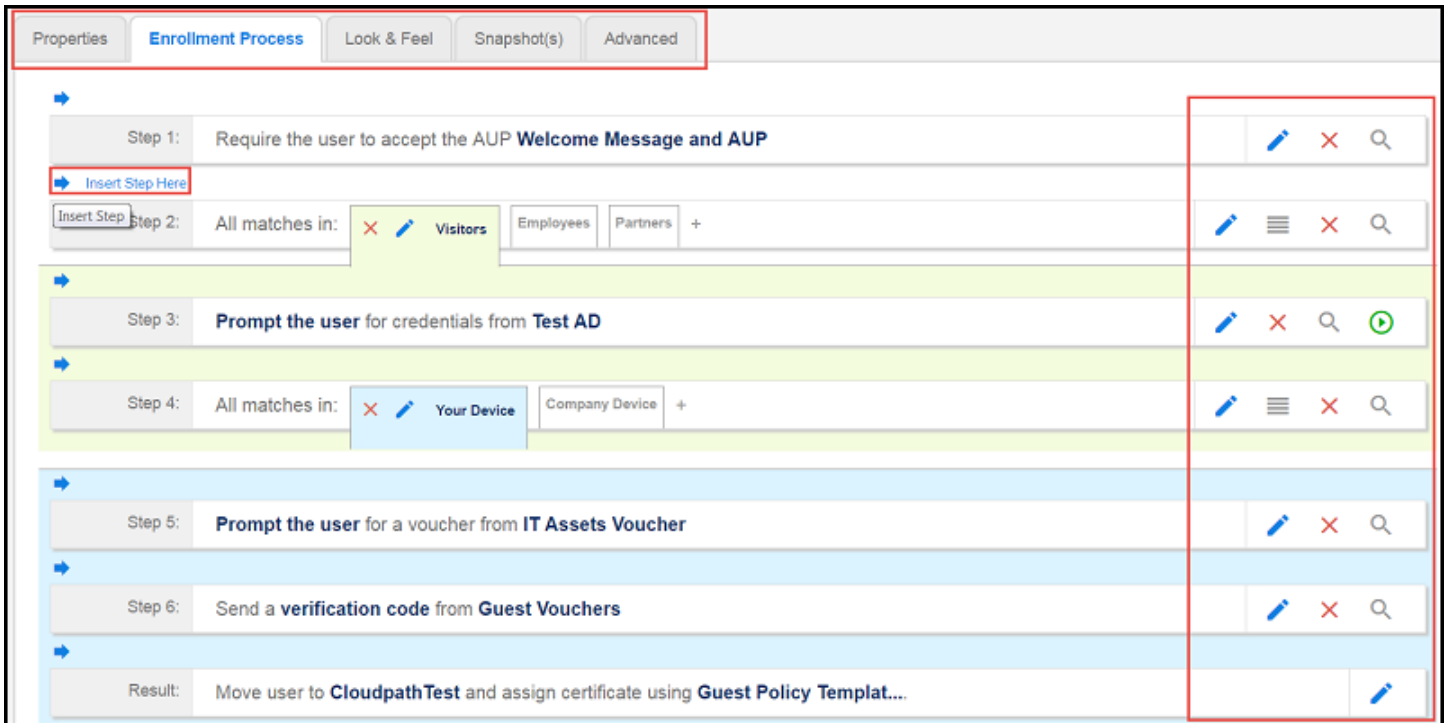
Workflow Basics

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 16 Workflow Configuration Page



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

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

Modifying a Workflow Template

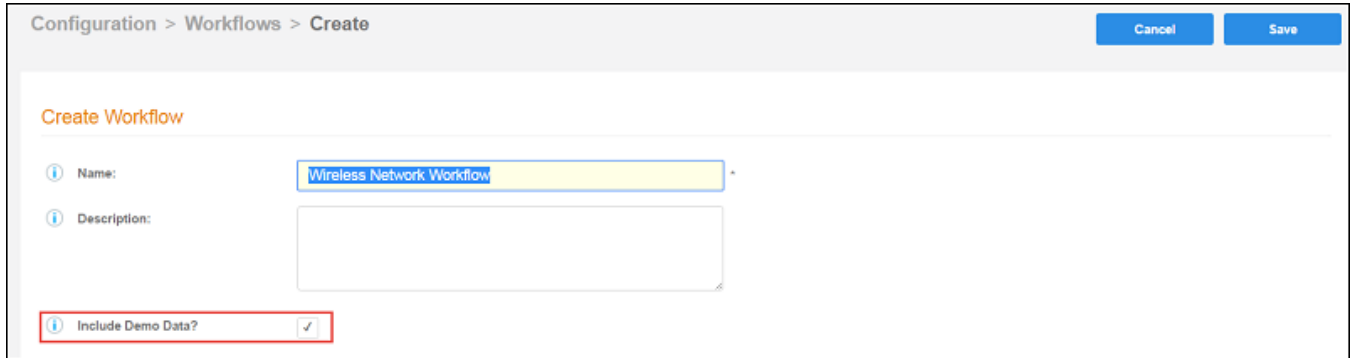
You can modify a standard enrollment workflow template provided by Cloudpath, or create your own workflow one step at a time from a blank slate.

To create a workflow from a template using sample data:

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

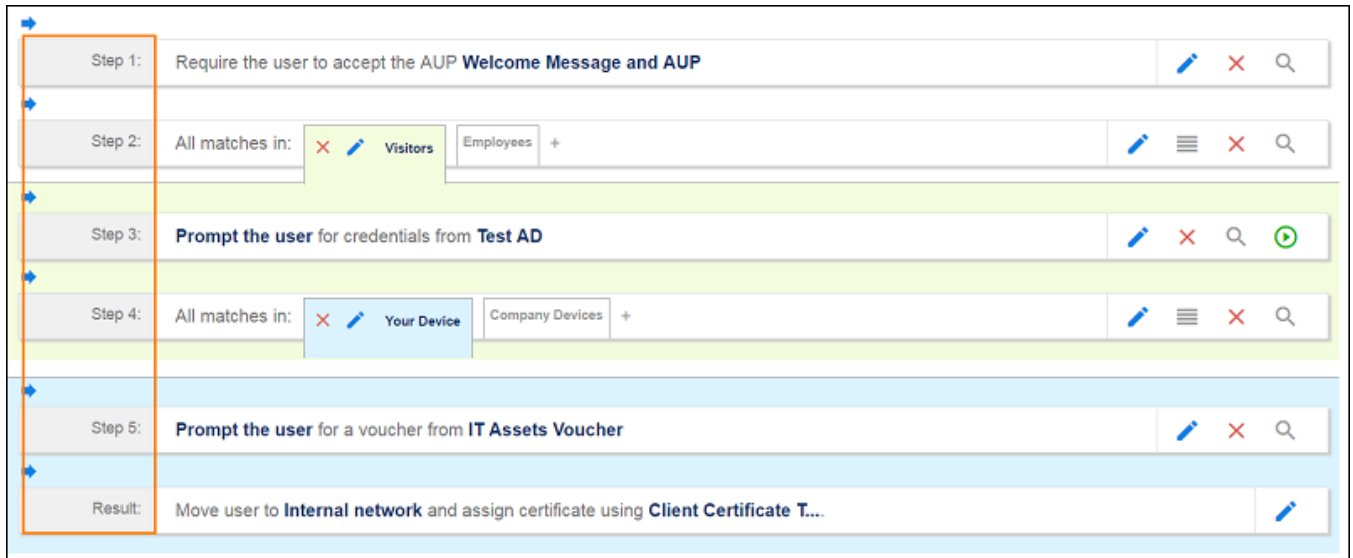
- On the **Create Workflow** page, enter a **Name** and **Description**. Select the check box for **Include Demo Data** and **Save**.

FIGURE 17 Create Workflow Using Demo Data



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

FIGURE 18 Workflow Template



The workflow template contains basic workflow steps with sample data that can be modified to fit your network plan.

TABLE 2 Example Workflow Template

Step 1	Acceptable Use Policy.
Step 2	Split in the workflow to provide a different sequence of enrollment steps for Visitors, Employees, and Partners. Splits can be modified for other industries (for example, Students, Faculty, and Guests).
Step 3	An authentication step for domain users, using Active Directory or LDAP.
Step 4	Another split in the workflow to provide a different sequence of enrollment steps for users with an IT device or a personal device.
Step 5	A prompt for a verification voucher.

TABLE 2 Example Workflow Template (continued)

Step 6	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.
---------------	---

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.

Creating a Workflow From a Blank Slate

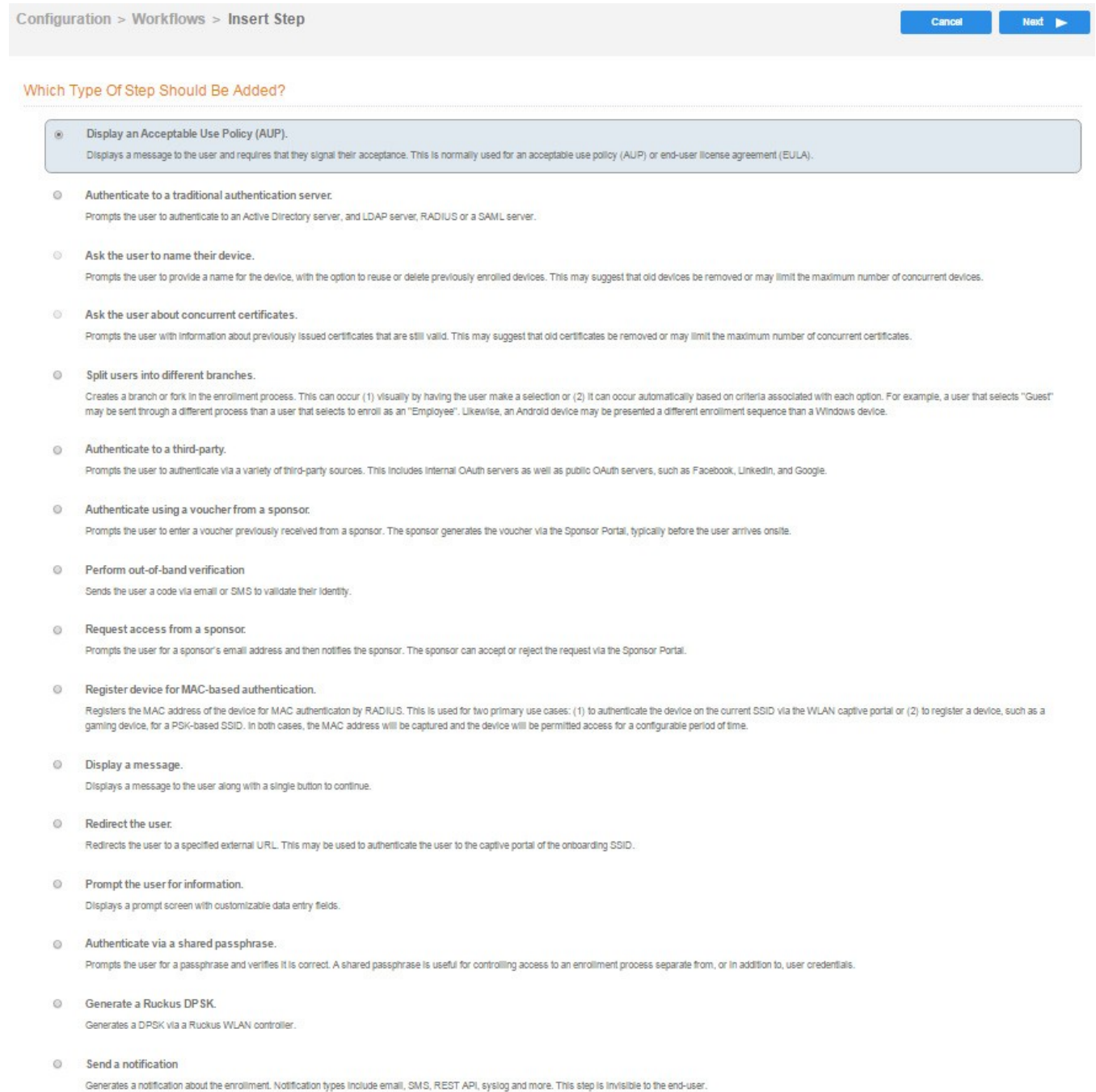
This section describes how to create a typical workflow from a blank slate. This sample workflow follows the steps provided in the workflow template.

1. Go to **Configuration > Workflows**.
2. On the right hand side of the Workflow page, select **Add New Workflow**.
3. On the Create Workflow page, enter a **Name** and **Description**. Leave **Include Demo Data** unchecked, and **Save**.

- On the blank workflow page, click **Get Started** 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 19 Enrollment Step Selection

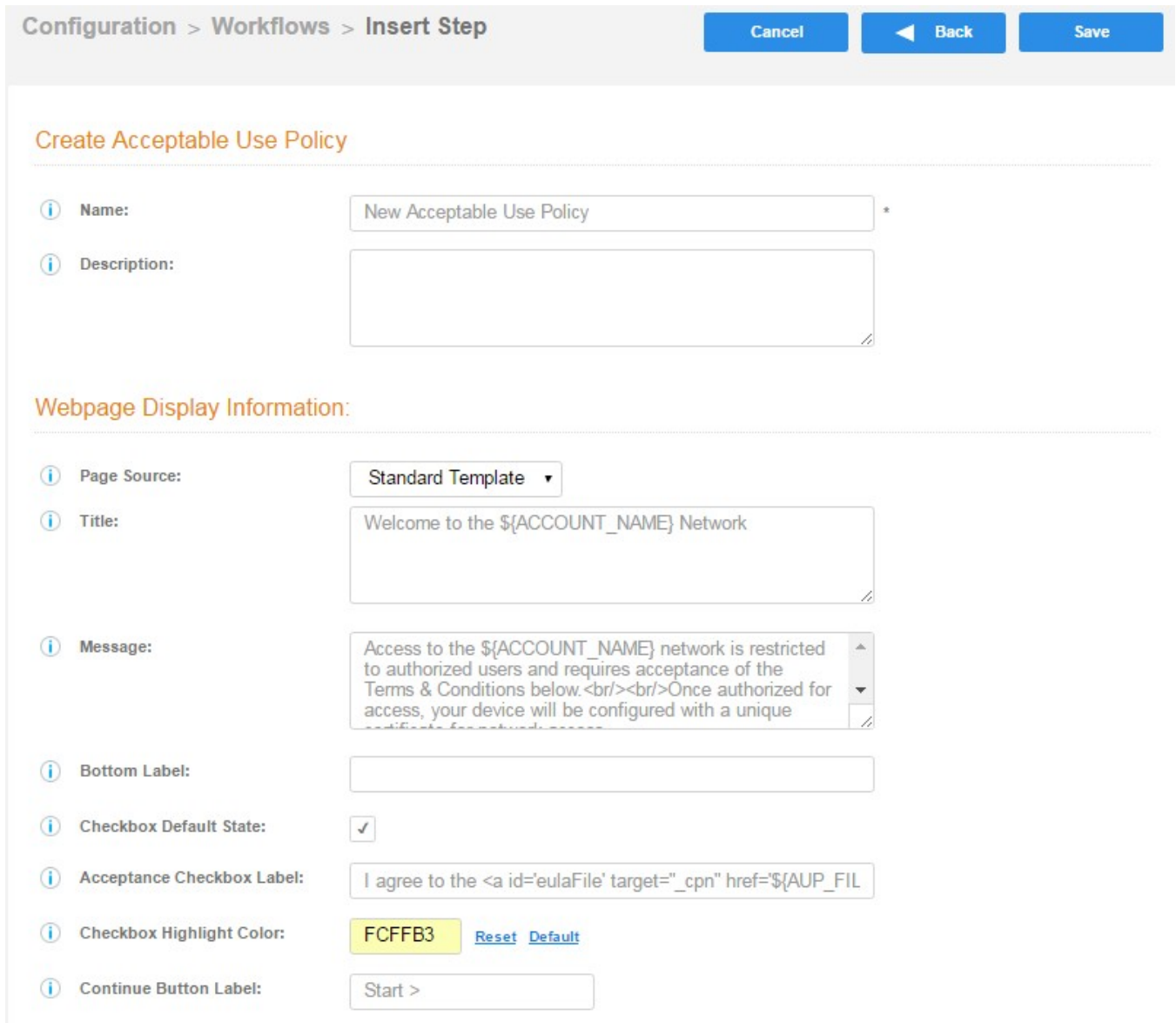


Acceptable Use Policy

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 20 Add Acceptable Use Policy



Configuration > Workflows > Insert Step Cancel Back Save

Create Acceptable Use Policy

Name: *

Description:

Webpage Display Information:

Page Source:

Title:

Message:

Bottom Label:

Checkbox Default State:

Acceptance Checkbox Label:

Checkbox Highlight Color: [Reset](#) [Default](#)

Continue Button Label:

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.

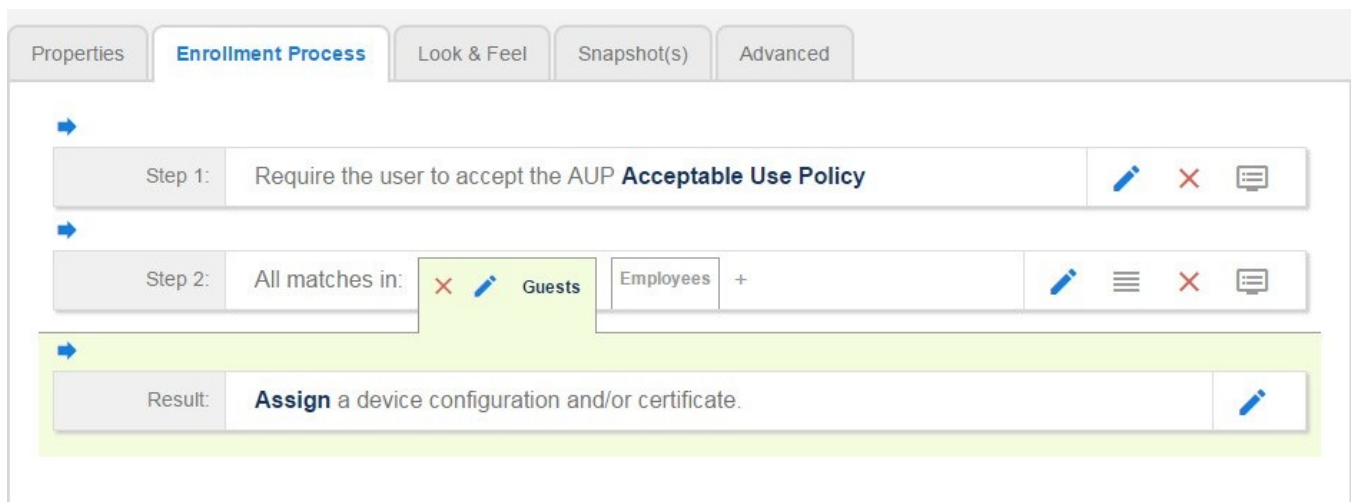
User Type Split

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 21 Workflow with User Type Split



Authentication to a Local Server

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

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 local server**.

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

FIGURE 22 Add Authentication Server

Authentication Server Configuration

Connect to Active Directory
Select this option to enable end-users to authenticate via Active Directory.

Default AD Domain: [ex. test.sample.local]

AD Host: [ex. ldaps://192.168.4.2] *

AD DN: [ex. dc=test,dc=sample,dc=local] *

AD Username Attribute: SAM Account Name

Verify Account Status On Each Authentication

Perform Status Check:

Additional Logins

Use For Admin Logins:

Use For Sponsor Logins:

Test Authentication

Run Authentication Test?

Connect to LDAP
Select this option to enable end-users to authenticate via LDAP (or LDAPs).

Connect to RADIUS
Select this option to enable end-users to authenticate via RADIUS using PAP.

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

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

5. Enter the **Reference** and **Active Directory Information** and click **Next**.
6. Select **Use a new webpage created from a standard template**. The **Create Credential Prompt** page opens.
 - To test connectivity to the authentication server, select the **Run Authentication Test** box, and enter a **Test Username** and **Password** before you click **Next**.
 - 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.

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

Device Type Split

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

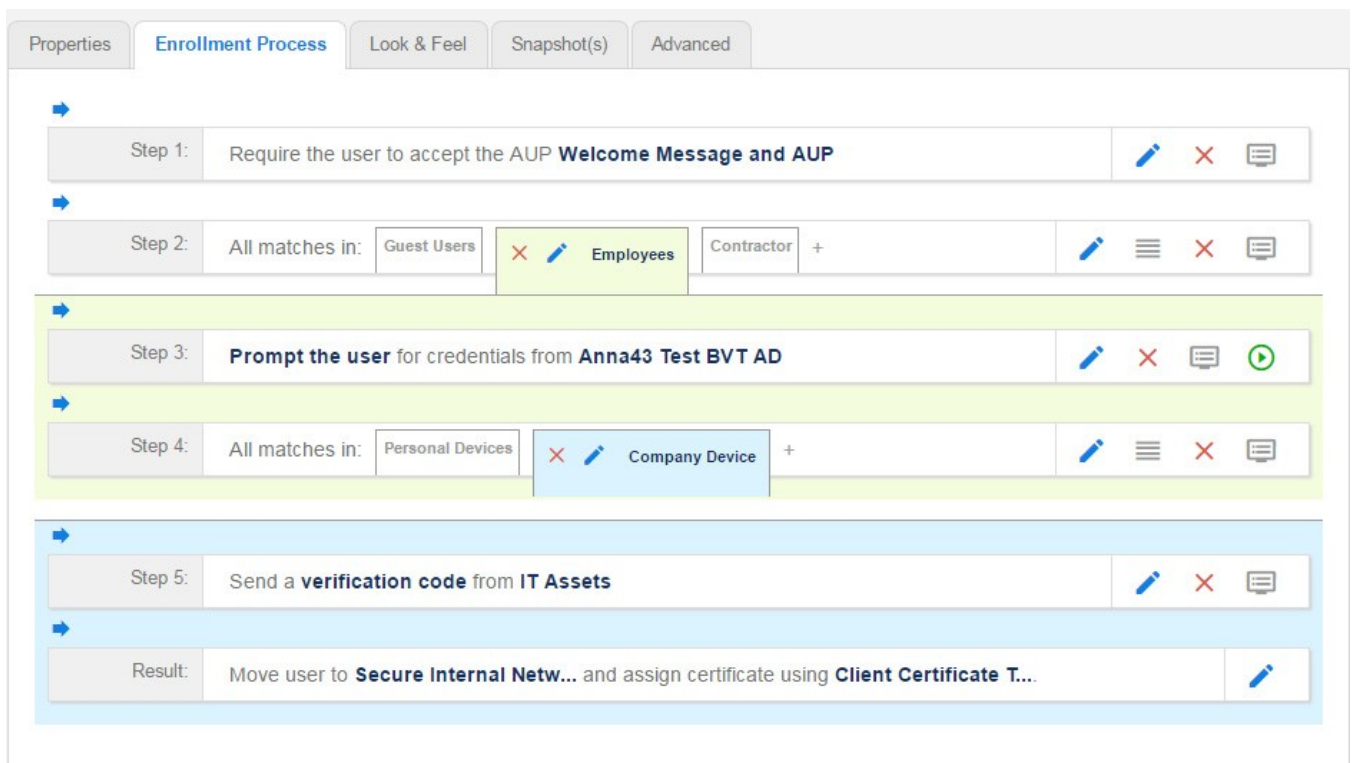
1. Insert a step above the **Result:** step in the enrollment workflow.
2. Select **Split users into different processes.**
3. Select **Use an existing split** and choose **Device Ownership**. The **Device Ownership** option prompts the user to select either **Your Device** or **Company Device**. These 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 23 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 (for example, 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 24 Modify Step - Filters and Restrictions

▼ **Filters & Restrictions**

The following settings control which users will have access to this option. If nothing is specified below, all users will have access to this option. If criteria is specified below, only users meeting the criteria will have access to this option.

User-Based Filters

Group Name Pattern:

Username Pattern:

User DN Pattern:

Email Pattern:

Device-Based Filters

Operating System Pattern:

User-Agent Pattern:

Language Pattern:

MAC Registration List:

Location-Based Filters

Location Pattern:

Allowed IPs:

Blocked IPs:

Filters Based On Web Authentication Certificate

Common Name Pattern:

Issuer Pattern:

Template Pattern:

Expiration Date: Expires Within

Other Filters

Voucher List Name:

3. In the **Filters & Restrictions** section, in **User-based Filters**, enter a regex to match 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 via voucher** and **Create a new Voucher** list.

FIGURE 25 Create Voucher List - Format and Notification Fields

The screenshot displays the 'Sponsorship' configuration interface, organized into three main sections:

- Sponsorship:** This section contains several configuration options:
 - Allow by LDAP Group:
 - Allow by LDAP Username:
 - Allow by LDAP Username DN:
 - Maximum Certificates:
 - Default Permissions: A list of checkboxes including 'Add/Edit/Delete Sponsors In Group', 'Manage Devices Enrolled By Sponsor', 'Manage Devices Enrolled By All', 'Allow Creation by CSV Upload', and 'Allow Bulk Creation'.
 - New Sponsor Email Subject:
 - New Sponsor Email Template: A text area containing a placeholder email template with variables like \$[URL], \$[EMAIL], \$[PASSWORD], and \$[PASSWORD].
- Fields Displayed To Sponsor:** This section allows for the configuration of which fields are shown to sponsors, each with a dropdown menu:
 - Name Field: Show and require entry.
 - Company Field: Show.
 - Email Field: Show.
 - SMS Field: Show.
 - Reason Field: Show.
 - Redeem By Field: Show.
 - Reuse Count Field: Do not show.
 - Days of Access Field: Do not show.
- Initial vouchers:** This section contains five empty text input fields labeled 'Initial Voucher #1' through 'Initial Voucher #5'.

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

The screenshot displays the configuration interface for the 'Create Voucher List' page, divided into three main sections:

- Sponsorship:** This section includes several configuration options:
 - Allow by LDAP Group:
 - Allow by LDAP Username:
 - Allow by LDAP Username DN:
 - Maximum Certificates:
 - Default Permissions: Add/Edit/Delete Sponsors In Group, Manage Devices Enrolled By Sponsor, Manage Devices Enrolled By All, Allow Creation by CSV Upload, Allow Bulk Creation
 - New Sponsor Email Subject:
 - New Sponsor Email Template:

```
You have been setup as a sponsor. To login as a sponsor, use the information below.<br/><br/>URL: ${URL}<br/>Username: ${EMAIL}<br/>Password: ${PASSWORD}<br/><br/>On your first login, you will be
```
- Fields Displayed To Sponsor:** This section allows configuring the visibility of various fields:
 - Name Field: ▼
 - Company Field: ▼
 - Email Field: ▼
 - SMS Field: ▼
 - Reason Field: ▼
 - Redeem By Field: ▼
 - Reuse Count Field: ▼
 - Days of Access Field: ▼
- Initial vouchers:** This section contains five empty text input fields labeled 'Initial Voucher #1' through 'Initial Voucher #5'.

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

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

Device Configuration and Client Certificate

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

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

Device Configuration

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

FIGURE 27 Configure SSID

Connection Type

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

The screenshot shows a configuration panel with two main sections: 'Wireless Connections' and 'Wired 802.1X Connections'. The 'Wireless Connections' section is active and contains three rows of settings, each with an information icon (i) on the left. The first row is 'SSID:' with a text input field containing 'TestSSID' and an asterisk. The second row is 'Authentication Style:' with a dropdown menu showing 'Client Certificate [Recommended]'. The third row is 'Is this SSID Broadcast?' with a dropdown menu showing 'Yes, the SSID is broadcast.'. The 'Wired 802.1X Connections' section is unselected.


5. Set the **Authentication Style**:
 - Select **Client Certificate for TLS** network configurations.
 - Select **PEAP** for PEAP/MS-CHAPv2 network configurations.
 - Select **Static Pre-Shared Key** for PSK network configurations.
 - Select **Ruckus DPSK for a Dynamic Pre-Shared Key** network configuration on a Ruckus controller.
6. Leave the default Broadcast setting and click **Next**.
7. Specify Conflicting SSIDs. This setting prevents the device from roaming away from the secure SSID to any open SSID in the area.

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

FIGURE 28 Select OS Versions

Automatically Configured OSes

Cloudpath supports a wide array of operating systems. Select the operating systems below that you wish to support within this device configuration. The following operating systems are automated, requiring minimal user interaction.

iOS Versions:	<input type="text" value="iOS 6 and Newer"/>
Android Versions:	<input type="text" value="Android 4.0.3 and Newer"/>
Windows (x86/x64) Versions:	<input type="text" value="Windows XP and Newer"/>
Mac OS X Versions:	<input type="text" value="Mac OS X 10.7 and Newer"/>
Chrome Versions:	<input type="text" value="Chrome 51 & Greater"/>
Linux Versions:	<input type="text" value="Ubuntu 12.04 & Fedora 18 and Newer"/>
 Windows Mobile Versions:	<input type="text" value="None"/>

Manually Configured OSes

These operating systems are require user interaction to configure. Online instructions will be provided to the user.

 Generic	<input checked="" type="checkbox"/>
 Blackberry	<input checked="" type="checkbox"/>
 Windows RT	<input checked="" type="checkbox"/>
 Windows Phone 8+	<input checked="" type="checkbox"/>

9. Select **Client will authenticate to the onboard RADIUS server.**
10. Configure additional settings for the device configuration. A more comprehensive list of additional settings is available after the device configuration is created.

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

Client Certificates

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

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

How to Set Up Client Certificate Templates

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

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

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

FIGURE 29 Client Certificate Template

Client Certificates
Used on clients to authenticate the client. The decoration of the username within the certificate allows RADIUS policies to be applied appropriately.

Username Decoration:

- username@byod.company.com
- username@contractor.company.com
- username@faculty.company.com
- username@guest.company.com
- username@it.company.com
- username@student.company.com
- username@other.company.com

Grant Access Until: 1 Years after issuance.

Configure Advanced Options:

Lifecycle Notifications

The Cloudpath ES supports events related to the lifecycle of the certificate. These events allow the system to interact with the end-user, the administrator, as well as external systems. Additional notifications can be configured once the template is created, but the notifications below are some of the most common ones.

Notifications:

- Send welcome email on issuance.
- Send email 7 days before certificate expiration.
- Send email if certificate is revoked.
- Email administrator if revoked certificate is used.

RADIUS Options

By default, this certificate template will be honored for RADIUS authentications. The RADIUS attributes below are the most commonly used attributes. If additional attributes are required, they may be added by editing the certificate template once created.

VLAN ID: [ex. 50]

Filter ID: [ex. BYOD]

Class: [ex. BYOD]

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

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

6. Grant access for the appropriate amount of time.

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

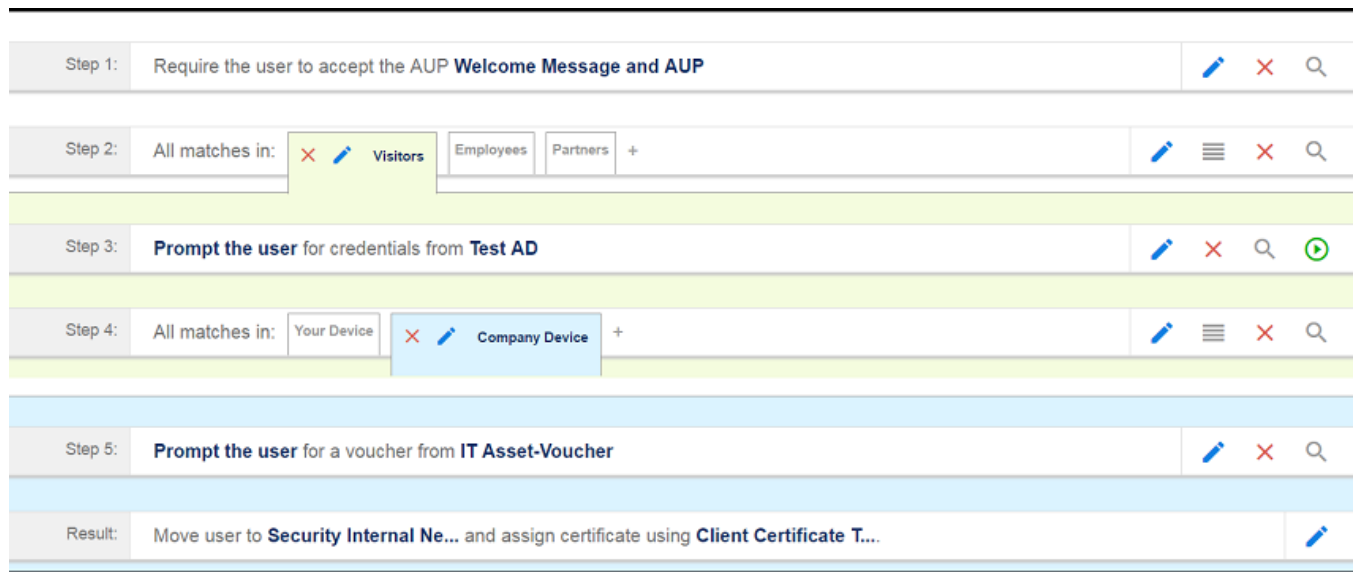
NOTE

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

7. Select any email notifications to be sent to the user related to the life-cycle of the certificate. Additional certificate notifications can be configured after the template is created.
8. Optional. Enter **RADIUS Options** to assign a VLAN ID or Filter ID to certificates that use this template. These settings only applies if you are using the Cloudpath onboard RADIUS server.
9. Click **Next**.

The completed workflow shows all enrollment paths. The last step shows the device configuration which is applied to the user device and the certificate template being used to assign a certificate to the user device.

FIGURE 30 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.

Publishing the Enrollment Workflow

- [How to Test a Published Workflow.....](#)50

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

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

FIGURE 31 Publish Workflows

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

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

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

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

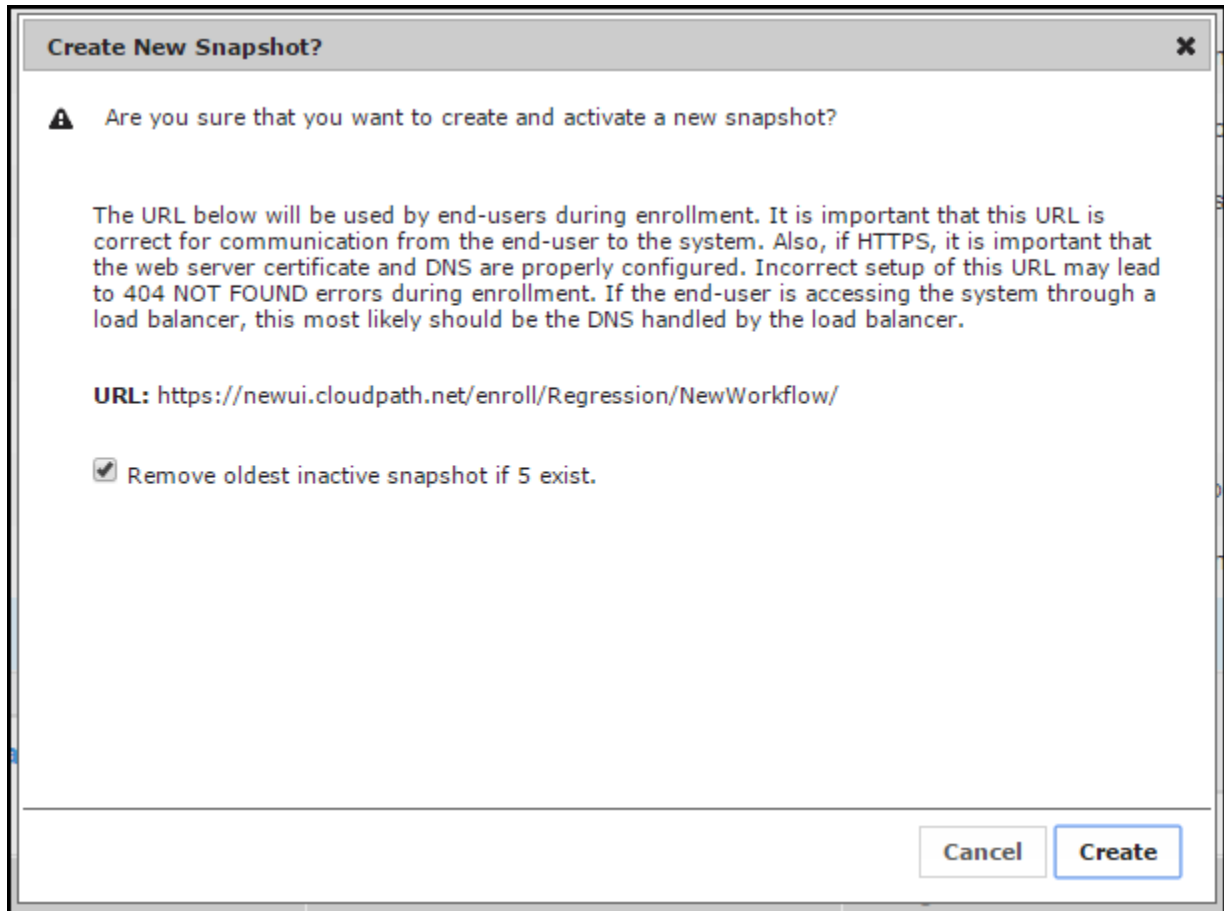
When you publish a workflow, this creates a snapshot of the workflow configuration.

To publish the workflow:

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

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

FIGURE 32 Create New Snapshot



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

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

How to Test a Published Workflow

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

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

Administration

- Administration Overview..... 51

Administration Overview

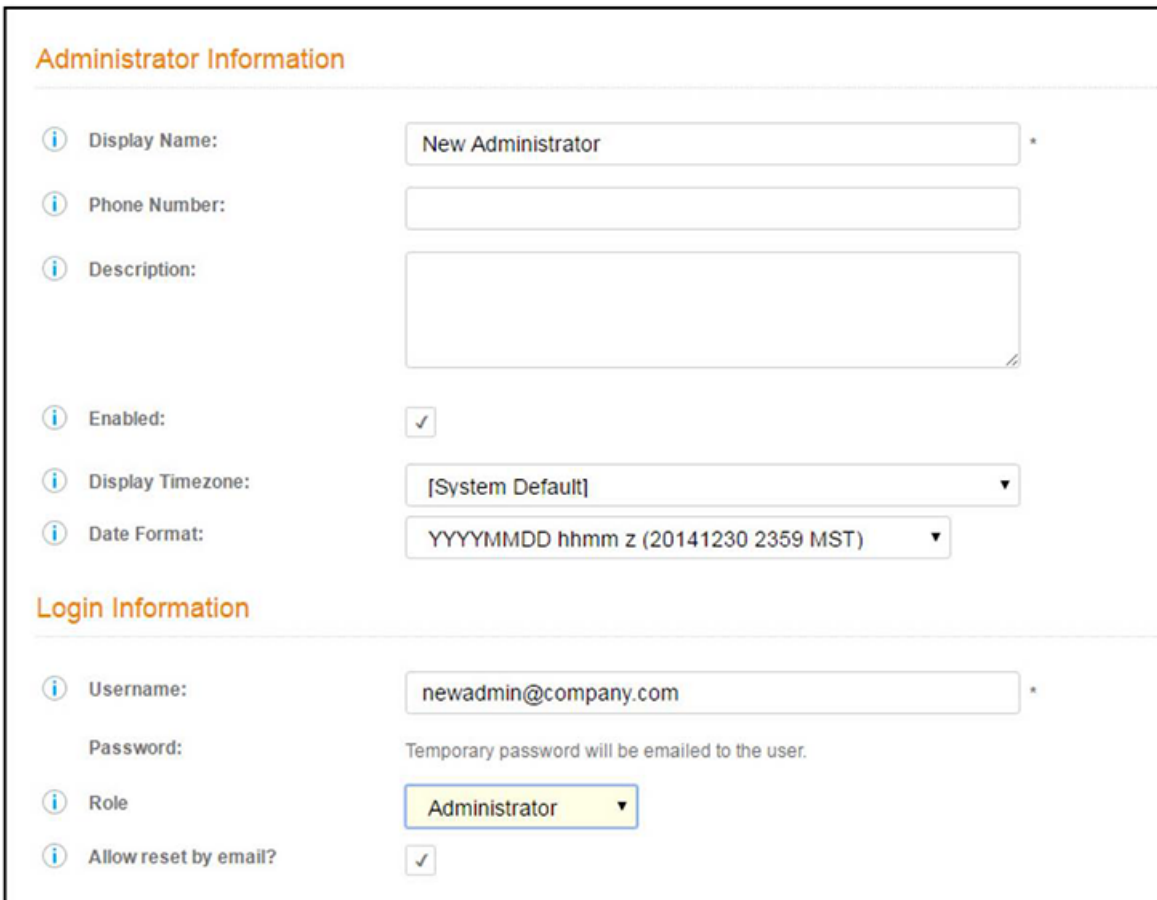
Access the **Cloudpath Administration** tab to manage system-related operations, using links in the following sections:

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 33 Add Administrator



Administrator Information

Display Name: New Administrator *

Phone Number:

Description:

Enabled:

Display Timezone: [System Default] ▼

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

Login Information

Username: newadmin@company.com *

Password: Temporary password will be emailed to the user.

Role: Administrator ▼

Allow reset by email?:

Cloudpath supports the following Administrator Roles:

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

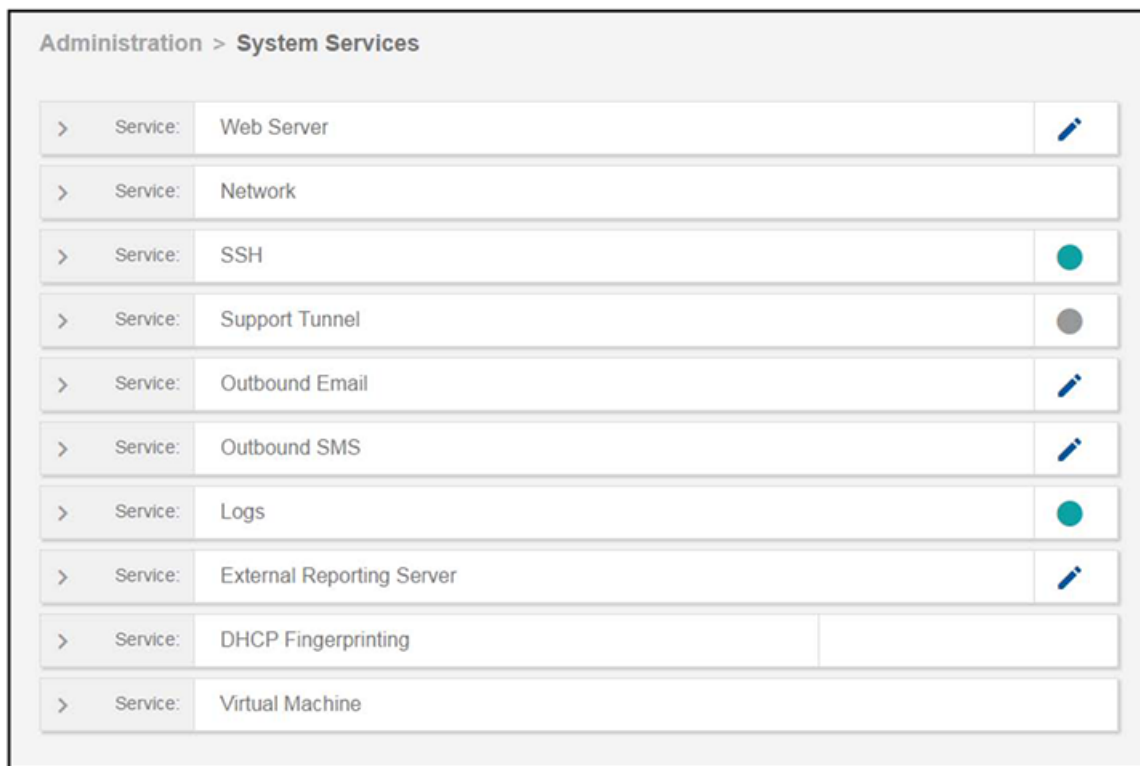
Company Information

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

System Services

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

FIGURE 34 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).
- DHCP Fingerprinting

DHCP fingerprinting is phase one of IoT. From the Cloudpath server you can enable DHCP Fingerprinting, for IPv4, or IPv6, or both on the **Administration > System Services > DHCP fingerprinting** page. The server discovers information about the devices on your network and displays it on the on the **Dashboard > DHCP Fingerprints** page.

This feature will only be available for locally deployed (on-premise) systems for 5.1, because currently cannot match the information in the DHCP packet exchange to a specific account on a hosted system.

You must enable ip helper on the router.

1. enable
 2. configure terminal
 3. interface type number
 4. ip helper-address address (where address is the IP address of the Cloudpath server)
 5. exit
- 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.

System Updates

System Updates - View and manage the Cloudpath build versions.

Replication

Replication - Configure two or more servers for replication. Cloudpath supports replication between two servers, for multiple data centers, and redundant servers.

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..... 55
- Device Configurations..... 55
- RADIUS Server..... 55
- Authentication Servers..... 57
- Firewall & Web Filter Integration..... 57
- MAC Registration Lists..... 57
- API Keys..... 57

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 [About the Enrollment Workflow](#) on page 31.

Device Configurations

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

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

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

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

RADIUS Server

View and manage the onboard RADIUS server.

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

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

NOTE

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

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

FIGURE 35 RADIUS Accounting

Status Policies Clients eduroam Attributes External Open Access Accounting									
Recent RADIUS Accounting Packets (Local)									
	Event Timestamp	Type	Session ID	Calling Station	Client IP	Username	NAS ID	NAS IP	NAS Port
Q	Dec 16 2016 13:42:14 MST	Start	599CBAD1-00000785	4C:8D:79:E9:16:18	192.168.95.181	anna@byod.company.com	38:FF:36:D2:6A:7E	192.168.92.135	58
Q	Dec 16 2016 13:43:02 MST	Start	599CBAD1-00000786	E4:F8:9C:87:B7:4D	192.168.95.251	bob@byod.company.com	38:FF:36:D2:6A:7E	192.168.92.135	59
Q	Dec 16 2016 13:44:34 MST	Start	599CBAD1-00000787	34:E6:AD:0E:CE:F5	192.168.95.195	jack@byod.company.com	38:FF:36:D2:6A:7E	192.168.92.135	60
Q	Dec 16 2016 13:47:04 MST	Start	599CBAD1-00000789	6C:94:F8:B9:DB:86	192.168.95.197	bill@byod.company.com	38:FF:36:D2:6A:7E	192.168.92.135	62
Q	Dec 16 2016 13:47:17 MST	Start	599CBAD1-0000078A	04:0C:CE:21:8D:A0	192.168.95.136	mike@byod.company.com	38:FF:36:D2:6A:7E	192.168.92.135	63
Q	Dec 16 2016 13:50:14 MST	Start	58545385-14A9E000	3C:A9:F4:01:02:50	192.168.95.40	anna@byod.company.com	6C:AA:B3:54:A9:EC	192.168.93.143	1
Q	Dec 16 2016 13:52:14 MST	Interim-Update	599CBAD1-00000785	4C:8D:79:E9:16:18	192.168.95.181	anna@byod.company.com	38:FF:36:D2:6A:7E	192.168.92.135	58
Q	Dec 16 2016 13:53:02 MST	Interim-Update	599CBAD1-00000786	E4:F8:9C:87:B7:4D	192.168.95.251	bob@byod.company.com	38:FF:36:D2:6A:7E	192.168.92.135	59
Q	Dec 16 2016 13:53:45 MST	Start	58545459-14A9E000	8C:3A:EE:15:6C:C6	192.168.95.209	bob@byod.company.com	6C:AA:B3:54:A9:EC	192.168.93.143	2
Q	Dec 16 2016 13:54:34 MST	Interim-Update	599CBAD1-00000787	34:E6:AD:0E:CE:F5	192.168.95.195	jack@byod.company.com	38:FF:36:D2:6A:7E	192.168.92.135	60

Authentication Servers

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

Firewall & 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..... 59
- Enrollments..... 59
- Connections..... 61
- Users & Devices..... 62
- Certificates..... 64
- DHCP Fingerprints..... 67
- Notifications..... 67
- Event Response..... 70

Overview

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

Enrollments

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

FIGURE 36 Enrollments Table



In-Progress															Completed Enrollments															Issued															Revoked															Expired															All															Paths														
															Range: All																																																																																									
Assistance ID	Enrollment Status	Name	Timestamp	Selections	Operating System	MAC Address	Device Name	Location	Common Name	Expiration Date	Serial Number	Thumbprint	Last OSCP Date	Voucher List	Auth Type																																																																																									
706C	Certificate Issued	bob	03/15/2016 17:00 MDT	Employees - Your Device	Windows 8	88:76:3F:11:48:4E	Heulect-Rackard HP Pavilion 15 Notebook PC		bob@anna43.company.com	03/15/2017	4884...F933	2790...4480	03/15/2016 17:01 MDT		Active Directory																																																																																									
4580	Completed		03/15/2016 15:55 MDT	B	Windows Phone 8		Microsoft Corporation Windows Phone 8																																																																																																	
878A	Completed		03/15/2016 15:20 MDT	B	Chrome OS		Google Inc. Chrome OS																																																																																																	
F76E	Completed		03/15/2016 15:19 MDT	B	Chrome OS		Google Inc. Chrome OS																																																																																																	
D607	Certificate Issued	bob	03/15/2016 14:43 MDT	Employees - Your Device	Windows 10	00:3F:5D:09:99:26	CHRIS-WORK-PC		bob@anna43.company.com	03/15/2017	4832...762A	C842...4D12	03/15/2016 14:45 MDT		Active Directory																																																																																									
457E	Completed		03/15/2016 14:29 MDT	A	Ubuntu	00:22:FA:7D:EA:D8	Canonical Ltd. Ubuntu																																																																																																	
1A7D	Completed		03/15/2016 14:27 MDT	A	Fedora		Vivante, Inc. Vivante Virtual Platform																																																																																																	
B414	Completed		03/15/2016 14:25 MDT	B	Ubuntu	9C:02:1E:A9:01:58	Heulect-Rackard HP 15 TouchSmart Notebook PC																																																																																																	
4A28	Completed	bob	03/15/2016 14:17 MDT	B	Android 4.1 Tablet	39:06:C9:09:A1:8C	samsung SM-T210R																																																																																																	
4211	Completed	bob	03/15/2016 14:13 MDT	B	Android 4.2	A0:0B:8A:8B:95:21	samsung Galaxy Nexus																																																																																																	
F1EE	Completed	bob	03/15/2016 14:13 MDT	A	Android 6.0	02:00:00:00:00:00	LG E Nexus 5																																																																																																	
A759	Completed	bob	03/15/2016 14:11 MDT	A	Android 4.4	CC:3A:61:40:6E:52	samsung SCH-I545																																																																																																	
844F	Completed	bob	03/15/2016 14:09 MDT	A	Android 6.0	02:00:00:00:00:00	Huawei Nexus 6p																																																																																																	
A648	Certificate Issued	bob	03/15/2016 11:51 MDT	Employees - Your Device	Windows 10	84:3A:48:13:63:02	Microsoft Corporation Windows 10		bob@anna43.company.com	03/15/2017	3953...71C5	FFAE...8072	03/16/2016 06:51 MDT		Active Directory																																																																																									
E844	Certificate Issued	bob	03/15/2016 11:35 MDT	Employees - Your Device	Windows 10	90:4C:E5:9D:8D:01	Heulect-Rackard HP Pavilion d14 Notebook PC		bob@anna43.company.com	03/15/2017	2F7A...E988	54FA...5CC3	03/15/2016 11:36 MDT		Active Directory																																																																																									

NOTE

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

Records Export

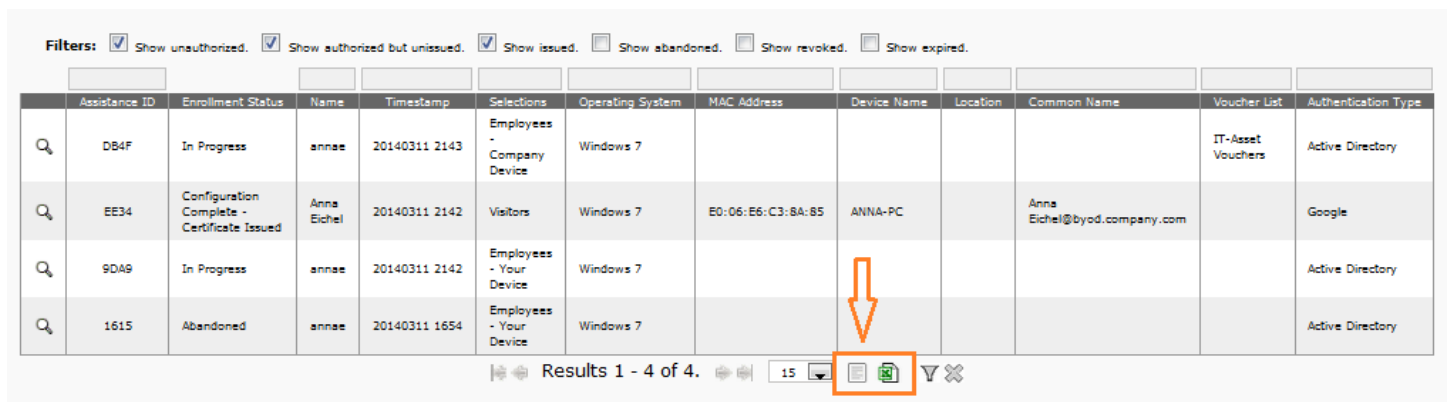
Enrollment and User data can be downloaded, as a CSV file or Microsoft Excel spreadsheet.

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

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

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

FIGURE 37 Download Enrollment Records



The screenshot shows a table with the following columns: Assistance ID, Enrollment Status, Name, Timestamp, Selections, Operating System, MAC Address, Device Name, Location, Common Name, Voucher List, and Authentication Type. There are four rows of data. At the bottom of the table, there are icons for CSV and XLS export, which are highlighted with an orange box and an arrow. The text 'Results 1 - 4 of 4.' is visible below the table.

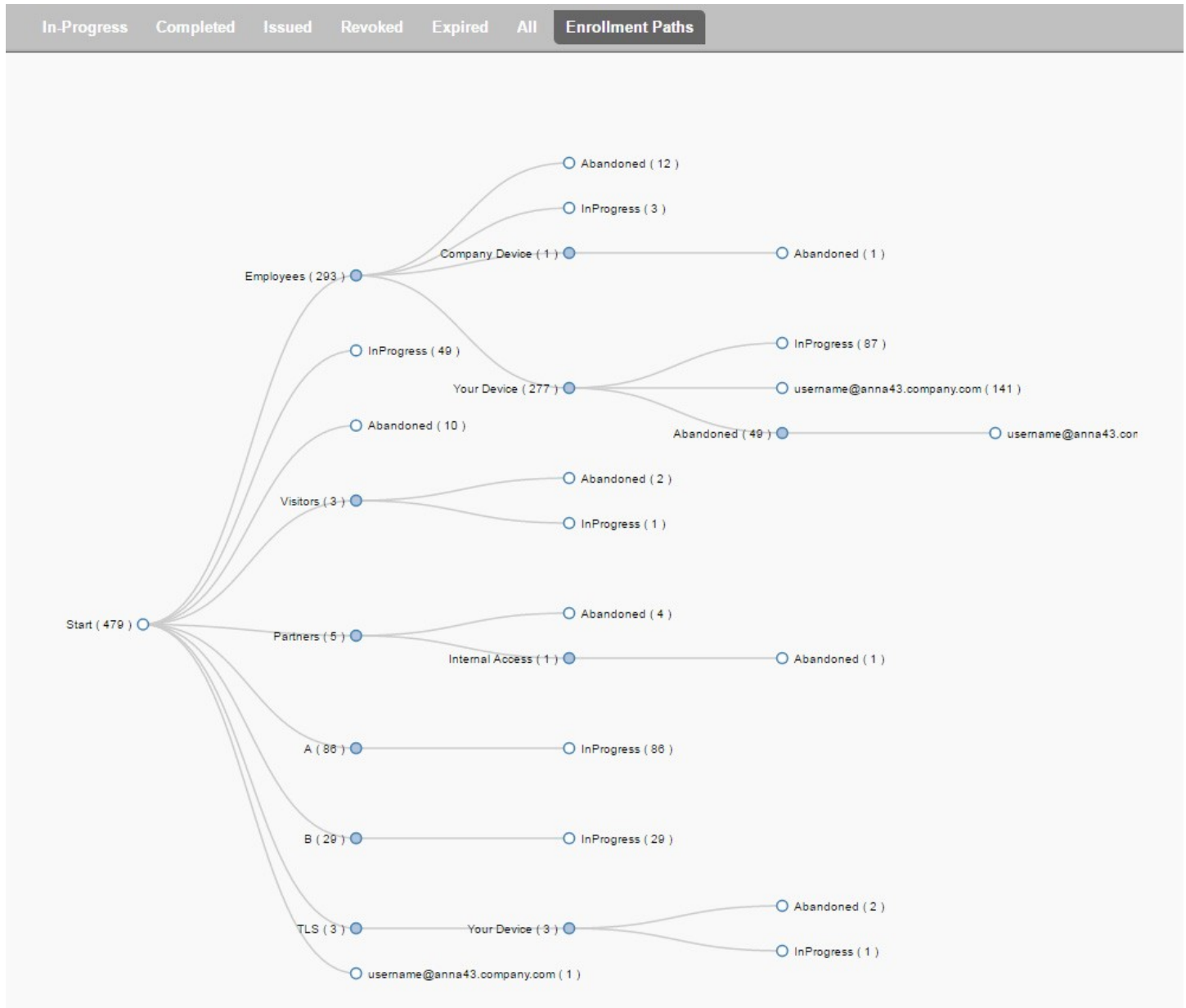
Assistance ID	Enrollment Status	Name	Timestamp	Selections	Operating System	MAC Address	Device Name	Location	Common Name	Voucher List	Authentication Type
DB4F	In Progress	annae	20140311 2143	Employees - Company Device	Windows 7					IT-Asset Vouchers	Active Directory
EE34	Configuration Complete - Certificate Issued	Anna Eichel	20140311 2142	Visitors	Windows 7	E0:06:E6:C3:8A:85	ANNA-PC		Anna Eichel@byod.company.com		Google
9DA9	In Progress	annae	20140311 2142	Employees - Your Device	Windows 7						Active Directory
1615	Abandoned	annae	20140311 1654	Employees - Your Device	Windows 7						Active Directory

Enrollment Paths

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

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

FIGURE 38 Enrollment Path



Connections

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

FIGURE 39 RADIUS Connections

Connections Disconnects All						
Status	IP Address	MAC Address	Username	SSID	Duration	
Connected	192.168.95.136	04:0C:CE:21:8D:A0	mike@byod.company.com	eng-Anna42	10 minutes ago	
Connected	192.168.95.40	3C:A9:F4:01:02:50	anna@byod.company.com	eng-Anna42	7 minutes ago	
Connected	192.168.95.197	6C:94:F8:B9:DB:86	bill@byod.company.com	eng-Anna42	11 minutes ago	
Connected	192.168.95.195	34:E6:AD:0E:CE:F5	jack@byod.company.com	eng-Anna42	13 minutes ago	
Connected	192.168.95.251	E4:F8:9C:87:B7:4D	bob@byod.company.com	eng-Anna42	15 minutes ago	
Connected	192.168.95.181	4C:8D:79:E9:16:18	anna@byod.company.com	eng-Anna42	16 minutes ago	
Connected	192.168.95.209	8C:3A:E3:15:6C:C6	bob@byod.company.com	eng-Anna42	4 minutes ago	

Results 1 - 7 of 7. 15

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

Users & Devices

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

FIGURE 40 User Table

Users Device Types Form Factors MAC Registrations							
Status	Photo	First Name	Last Name	Server Name	Authentication Type	Timestamp	
		Anna	Eichel	LinkedIn, Facebook, or Gmail	Google	20140326 1006 MDT	
		Anna	Eichel	Anna Test AD	Active Directory	20140326 1335 MDT	
		Bob	Johnson	Anna Test AD	Active Directory	20140326 1344 MDT	
		Bill	Smith	Anna Test AD	Active Directory	20140326 1348 MDT	
		Mark	Test	Anna Test AD	Active Directory	20140326 1415 MDT	
		Lynn	Test	Anna Test AD	Active Directory	20140326 1415 MDT	
		Mike	Test	Anna Test AD	Active Directory	20140331 1622 MDT	
		Anna	Test	Anna Test AD	Active Directory	20140331 1625 MDT	
		Anna	Eichel	LinkedIn, Facebook, or Gmail	Google	20140331 1638 MDT	

Results 1 - 9 of 9. 15

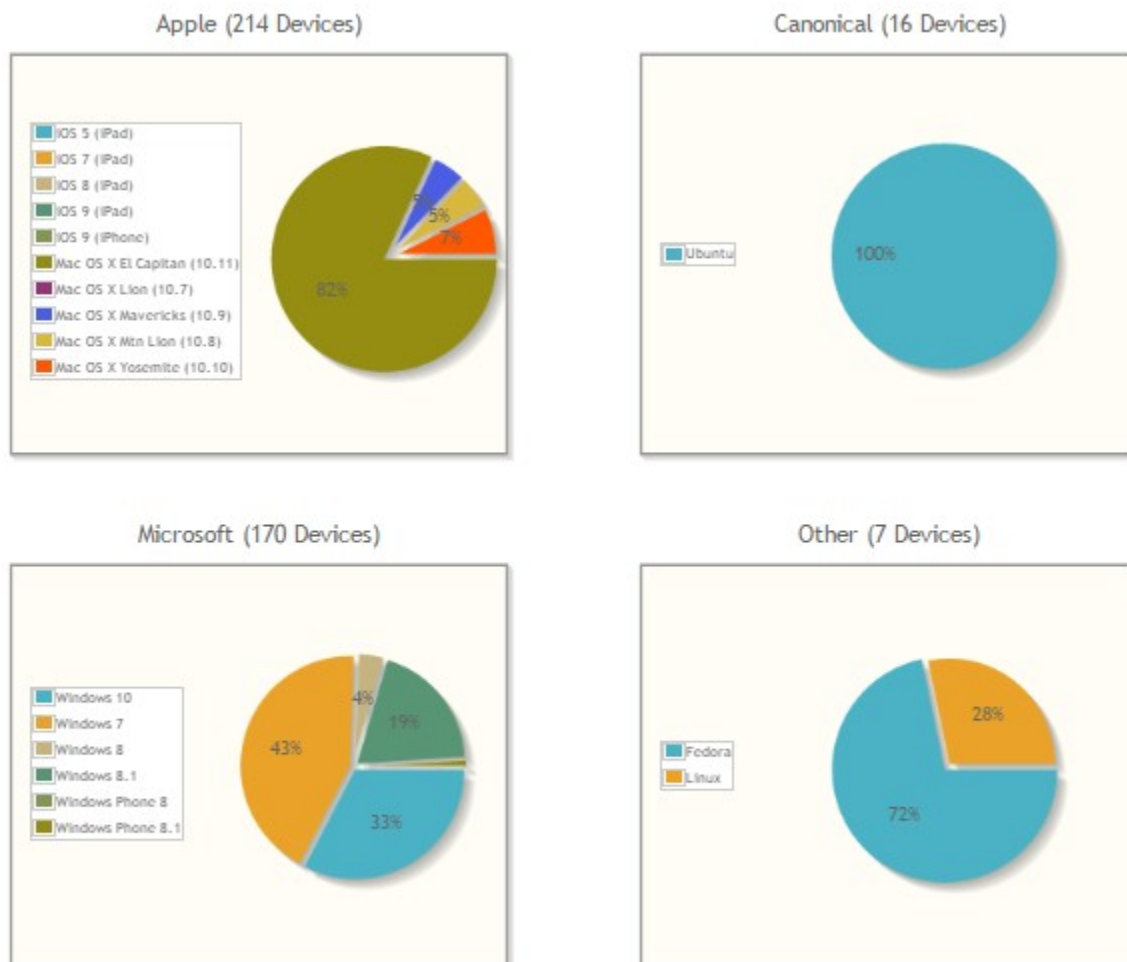
NOTE

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.

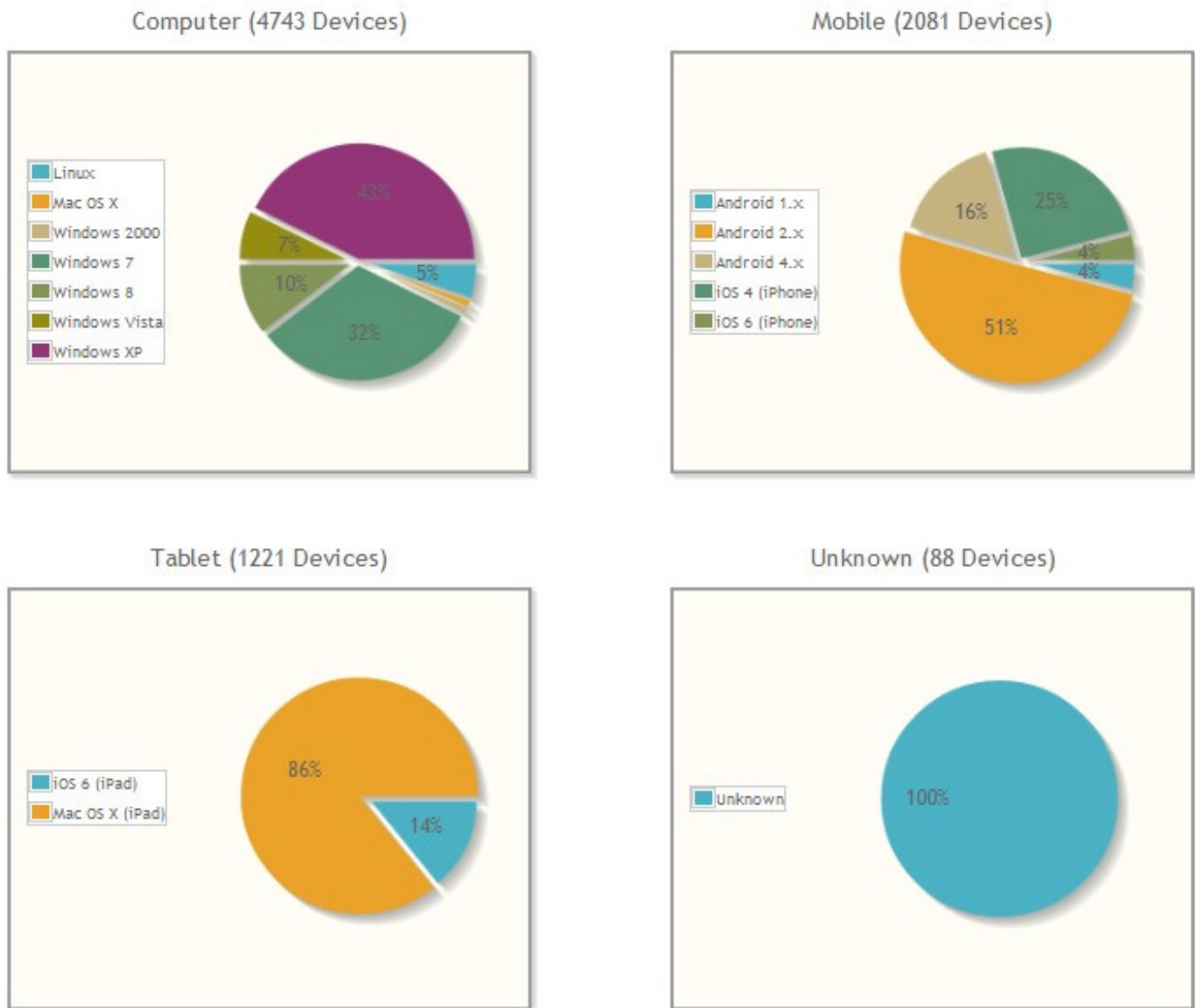
FIGURE 41 Device Types



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 42 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 43 Certificates Table

Active Certificates Revoked Expired All Active Trends Expiring Trends										
Status	Common Name	Timestamp	Expiration Date	CA Name	Template	Email	Revocation Date	Thumbprint	Last OCSP Date	
Q X	mark@byod.company.com	20140402 1056 MDT	20150402	Anna Test Intermediate CA I	username@byod.company.com			52CD...C610	20140402 1056 MDT	
Q X	anna@byod.company.com	20140402 1054 MDT	20150402	Anna Test Intermediate CA I	username@byod.company.com			1BCC...1B27	20140402 1054 MDT	
Q X	anna@byod.company.com	20140401 1415 MDT	20150401	Anna Test Intermediate CA I	username@byod.company.com			AA51...E2DA	20140401 1415 MDT	
Q X	lynn@byod.company.com	20140401 1402 MDT	20150401	Anna Test Intermediate CA I	username@byod.company.com			D472...768D	20140401 1402 MDT	
Q X	bob@byod.company.com	20140401 1351 MDT	20150401	Anna Test Intermediate CA I	username@byod.company.com			EC1A...1554	20140401 1351 MDT	
Q X	AnnaTest.cloudpath.net	20140401 1342 MDT	20170401	Anna Test Root CA I	Server Template	it@company.com		B2D4...45E1	20140401 1342 MDT	

Results 1 - 6 of 6. 15

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 44 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 45 Expiring Certificates



DHCP Fingerprints

This feature is supported only for on-premise deployments.

From the Cloudpath server you can enable DHCP Fingerprinting, for IPv4, or IPv6, or both on the **Administration > System Services > DHCP fingerprinting** page. The server discovers information about the devices on your network and displays it on the on the **Dashboard > DHCP Fingerprints** page.

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 46 Notifications Table

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

Results 1 - 2 of 2. 15

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**.

- On the **Scheduled Reports** page, click **Add Scheduled Report**.

FIGURE 47 Schedule Enrollment Records Export

Modify Scheduled Report Cancel Save

Name:

Description:

Enabled:

Email

Email Addresses:

Email Subject:

Schedule

Frequency: ▼

Time: MDT

Enrollment Status To Include

Include Abandoned?

Include Authorized?

Include Expired?

Include Initiated?

Include Certificate Issued?

Include Rejected?

Include Revoked?

Include In Progress?

Report Content

Columns To Include: ▼

- 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.
- 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.
- 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.
- Specify the **Report Content**, which determines the data columns that will be included in the report.

7. **Save** the scheduled task.

FIGURE 48 Scheduled Report

The screenshot shows a web interface with three tabs: 'Notifications', 'Events', and 'Scheduled Reports'. The 'Scheduled Reports' tab is active. Below the tabs, there is a text box stating 'The reports listed below are currently scheduled.' and a button labeled 'Add Scheduled Report'. A table lists three scheduled reports, each with a download icon, an edit icon, and a delete icon.

Report Name	Frequency	Actions
Abandoned Enrollments - Monthly	Executing once on 04/30/2014 at 12:00 AM	Download, Edit, Delete
Daily Expired	Every day at 8:00 AM	Download, Edit, Delete
Weekly Enrollments	Every week at 7:00 AM	Download, Edit, Delete

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 49 Event Response

Event Response

This page allows items to be revoked or unrevoked in bulk via an uploaded Excel (xls, xlsx, or csv) spreadsheet. The spreadsheet can be filtered and downloaded from the respective View-All page (with additional filtering possible within Excel) or generated separate from the system.

Block Enrollments By Upload

This option allows enrollments (and their related certificates) to be blocked or unblocked via an uploaded Excel file. Each row is processed using the following column headers, in order of preferences and case insensitive: Pk, GUID, Name, Enrollment Email, MAC Address.

Upload File To:

Revoke Certificates By Upload

This option allows certificates to be revoked or unrevoked via an uploaded Excel file. Each row is processed using the following column headers, in order of preferences and case insensitive: Certificate Pk, Full Serial Number, Serial Number, Common Name

Upload File To:

Block Users By Upload

This option allows users (and their related devices) to be blocked or unblocked via an uploaded Excel file. Each row is processed using the following column headers, in order of preferences and case insensitive: DN, CN, Username, Email

Upload File To:

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

Support

- [Overview.....73](#)

Overview

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

Documentation


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

Licensing

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

FIGURE 50 Licensing Information Page

Licensing Information Refresh

License Type:  Trial
Active trial through [Unknown].

System Utilization

Active Certificates: 1 Currently Active
1 Issued In Last 30 Days
1 Issued In Last 60 Days
1 Issued In Last 90 Days
1 Issued In Last Year

Statistics: [Users](#), [Authentications](#), [Certificates](#), [MAC Registrations](#), [Notifications](#)

License Server

License Server: <https://bvt.cloudpath.net>
Link Established: Yes, since 20160415 1048 MDT [Advanced](#)
Customer GUID: {000000-3EDC0222-E8C9-BEEA-D0AC-9DDFAAFC8194}
System Identifier: {000000-DF466E1A-52B2-065A-ED05-0FB6BE8E6B16-C019539F-A897-ACBD-EB7F}

Notices

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

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

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

Copyright Notice: Copyright 2012-2016 Ruckus Networks

Diagnostics

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

FIGURE 51 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.

Advanced Support

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

NOTE

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



© 2018 ARRIS Enterprises LLC. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com