RUCKUS®
COMMSCOPE

Cloudpath Enrollment System Deployment Administration Guide, 5.9R4

Supporting Cloudpath Software Release 5.9R4

Copyright, Trademark and Proprietary Rights Information

Contents

Cloudpath Security and Management Platform

Cloudpath Security and Management Platform

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

Cloudpath Enrollment System delivers secure network access for any device and any user on any network.
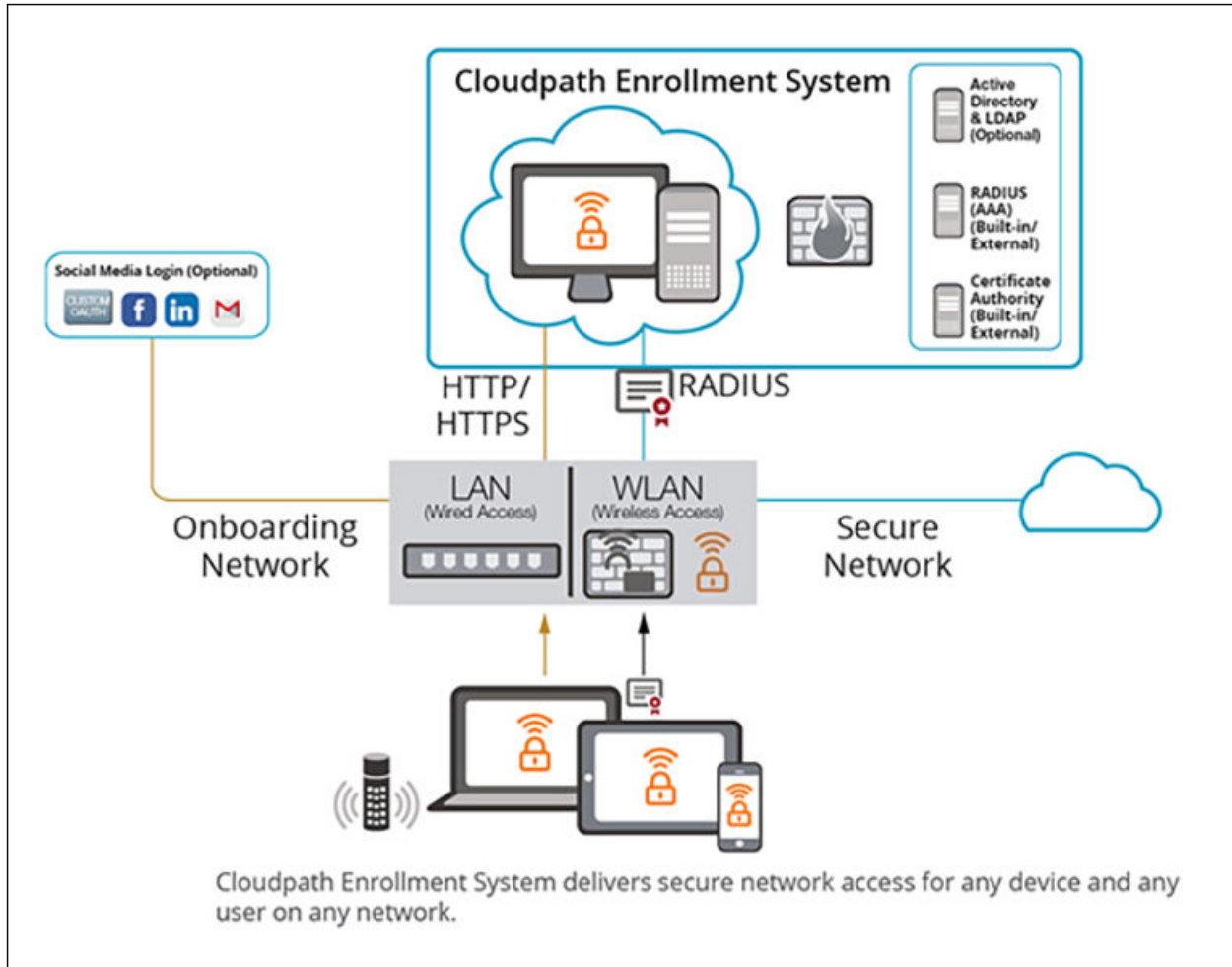
What is Cloudpath

There are two main components that make up Cloudpath: *Secure Onboarding* and *Advanced Certificate Management*. The combination of these two capabilities enable a powerful new way to secure and manage any and every device connecting to the network, while also making it extremely usable for the end user and the administrator. This combination delivers the industry's first *Automated Device Enablement* (ADE) solution.

Secure onboarding capabilities include:

- Self-service automated onboarding for a wide array of devices
- BYOD, partner, and guest access
- Automated configuration
- Secure WPA2-Enterprise encryption with PEAP or EAP-TLS
- Flexible enrollment options - AD, LDAP, OAuth, Social Networks
- Guest sponsorship, email, SMS, and voucher options
- Built-in certificate authorities and Microsoft CA integration

- Works with existing Wi-Fi infrastructure

- Automated system health compliance, including AV, firewalls, NAC, proxies, and software installation

Advanced Certificate Management capabilities include:

- Unique per-device certificate management

- Automated certificate distribution

- Self-service certificate enrollment and installation.

- Dynamic policies based on user, device, ownership (BYOD or IT-owned), access needs

- Manage access activation and termination based on employee status

- Visibility into every device connected to the network, enrollment options, form factor and expiring certificates using automated reports on the dashboard

- Per-device policy control, visibility, and utilization tracking

What Cloudpath Provides

Cloudpath provides one portal for automatically onboarding authorized devices on the secure network. The process is simple enough to be self-service, unobtrusive in that the application is dissolvable, automated so that the migration to the secure network can be managed without contacting the help desk. Cloudpath makes for a better Wi-Fi experience by simplifying the network, and it can be implemented in your existing WLAN infrastructure because it uses standards-based WPA2-Enterprise.

By using Cloudpath, you keep unauthorized devices off the secure network. With user and device authorization, issues with sniffers, snoopers and evil twins are prevented. The reporting capabilities allow user and device visibility and control, so that a network administrator has a view of what is happening on the network.

Guest Users

Cloudpath works entirely in the background as it delivers the most secure method of WPA2- Enterprise, EAP-TLS to mobile devices, including guest users. Through the use of non-intrusive native supplicant configuration, Cloudpath allows guest users to use the same entry point as employee or student users then automatically moves them to encrypted WPA2-Enterprise wireless networks. Guests can also sign in using third-party authentication, such as Facebook, LinkedIn or Gmail.

Workflow Engine

Workflow Building Blocks

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.

The enrollment workflow is built using a series of blocks, with each building block representing a step in the onboarding process. A workflow step might be an acceptable use policy, a display message, or an authentication hurdle. These steps, combined in a variety of different sequences, create an enrollment workflow for every device type and every user type on your network. The end result is a lot of flexibility for different use cases.

FIGURE 2 Basic Workflow
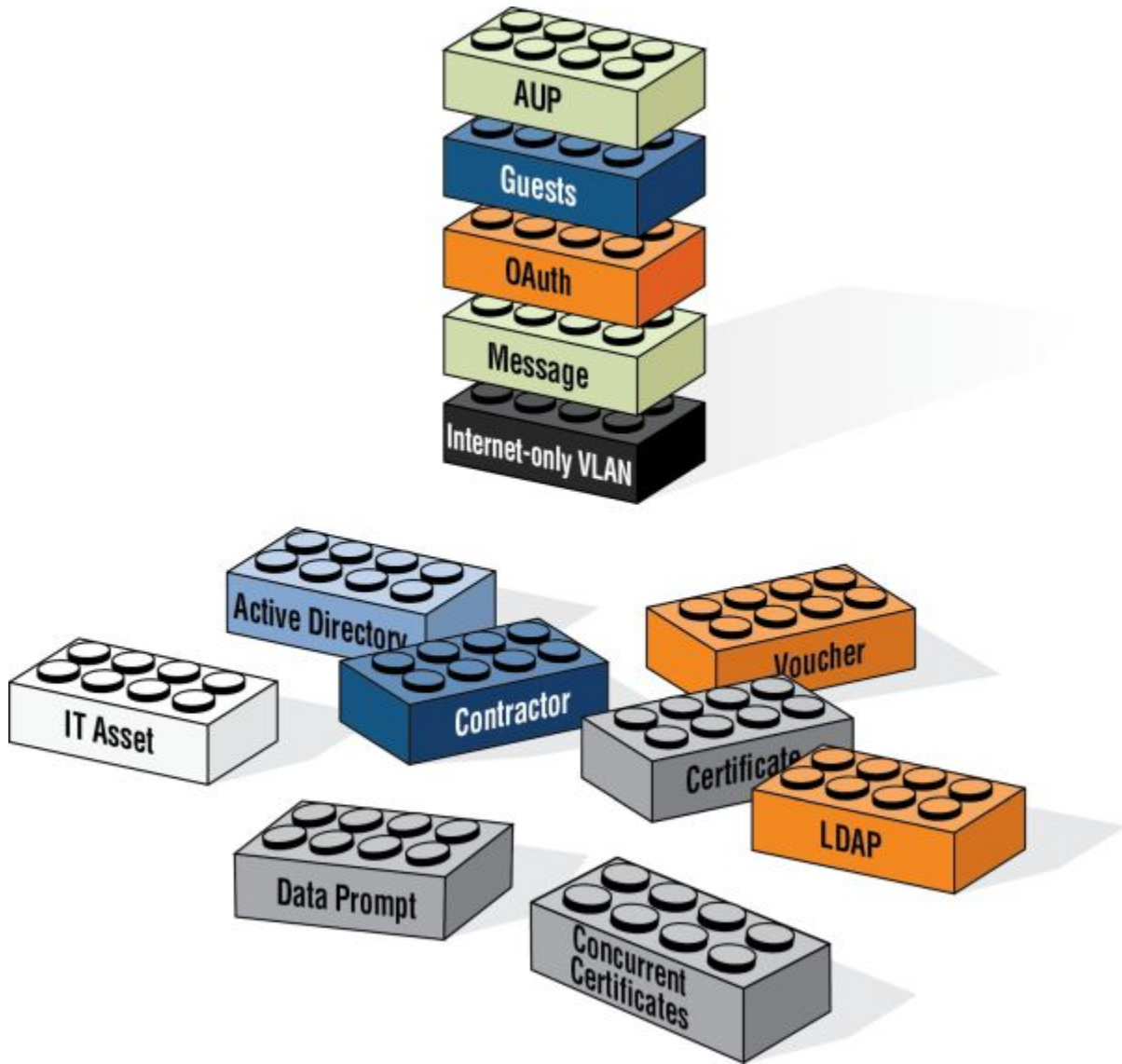
Available Workflow Plug-Ins

Cloudpath provides the following building blocks, called workflow "plug-ins," which are used when you add a step to the enrollment workflow.

FIGURE 3 Plug-ins That Can Be Used in a Workflow
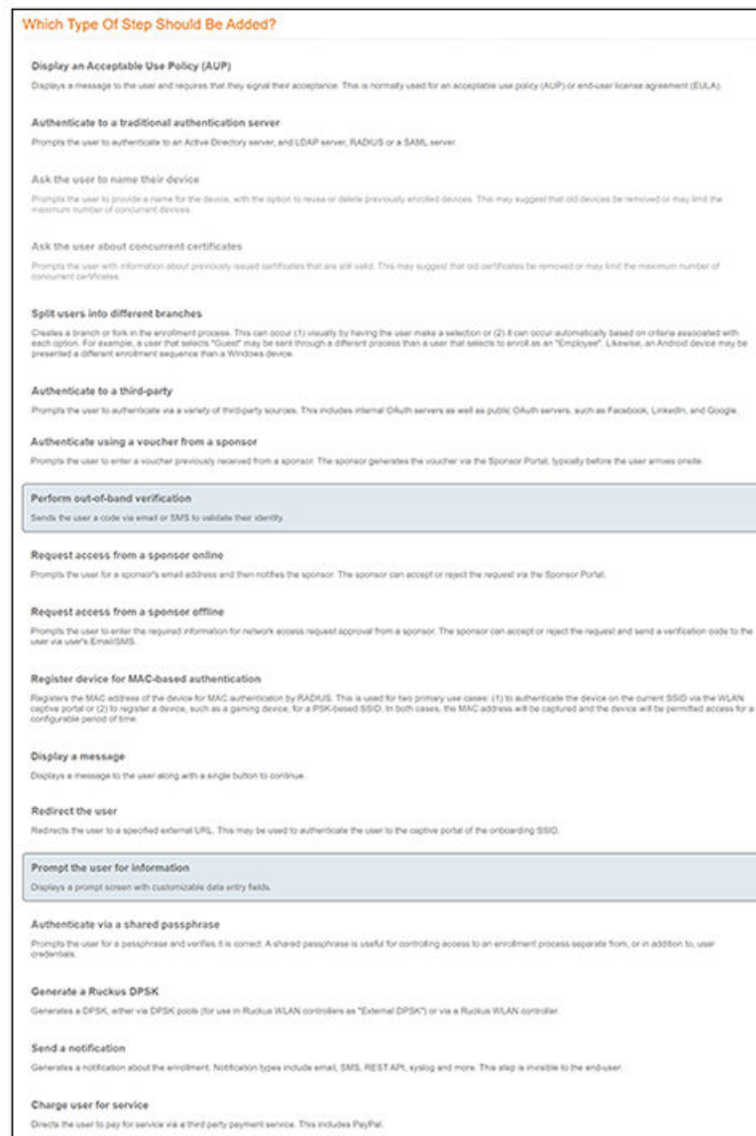
Display an Acceptable Use Policy

An acceptable use policy (AUP) prompt displays a message to the user and requires that they signal their acceptance. This is typically used for network policies or end-user license agreements (EULAs). For an example of using this plug-in in a workflow, refer to Acceptable Use Policy on page 68

Authenticate to a Traditional Authentication Server

If you authenticate users to a traditional authentication server, Cloudpath supports authentication using an Active Directory, LDAP (or LDAPS), via a RADIUS server using PAP, using Security Assertion Markup Language (SAML), or using an onboard database. For an example of using this plug-in in a workflow, refer to Authentication to a Traditional Authentication Server on page 70.

Ask the User to Name the Device

The **Cleanup Devices** plug-in prompts the user to provide a name for the device, with the option to reuse or delete previously enrolled devices. This may suggest that old devices be removed or may limit the maximum number of concurrent devices.

Ask the User About Concurrent Certificates

The **Cleanup Certificates** plug-in provides a method for allowing users to maintain the number of certificates registered to their devices. You can configure a certificate limit, and during the enrollment process, prompt the user to review information about previously distributed certificates.

Split Users Into Different Workflow Branches

Creates a branch or fork in the enrollment process. This can occur (1) visually by having the user make a selection or (2) it can occur automatically based on criteria associated with each option. For example, a user who selects **Guest** may be sent through a different process than a user who selects to enroll as an **Employee**. Likewise, an Android device may be presented a different enrollment sequence than a Windows device.

Examples:

- For an example of creating a user-type split, refer to User Type Split on page 69.
- For an example of creating a device-type split with the use of filters, refer to Device Type Split on page 72.
- For an example of using variables within a split, refer to Using Variables in a Workflow Split on page 119.

Authenticate to a Third-Party

When you combine third-party authentication with traditional authorization methods, the social media provides additional identity information during the onboarding process to deliver automated, self- service access to the WPA2-Enterprise wireless network. Cloudpath supports third-party integration using Facebook, LinkedIn, Google, or you can specify a custom OAuth 2.0 server.

For more information, refer to the *Cloudpath Enrollment System Third-Party Authentication Configuration Guide.*

Authenticate Using a Voucher From a Sponsor

When you use a voucher for authorization, the user is provided with a one-time password (OTP) and is prompted for this password during the enrollment process. Vouchers can be used to control access separate from, or in addition to, user credentials. For example, use vouchers for self-service registration of IT assets, or for authenticating network access for partners.

For more information, refer to the *Cloudpath Enrollment System Sponsored Guest Access Configuration Guide*, which is devoted solely to this one type of guest plug-in.

Perform Out-of-Band Verification Using Email or SMS

Out-of-band verification allows users to enter an email address or phone number to have the verification code or one-time password sent to them. The out-of-band prompt is tied to a voucher list, which controls the characteristics of the one-time password (OTP). You can create a new voucher list specifically for out-of-band verification, or you can use an existing list.

Request Access From a Sponsor Online

> **NOTE**
> This plug-in was named "Request Access From a Sponsor" in Release 5.5 and earlier.

Prompts the user for a sponsor's email address and then notifies the sponsor. The sponsor can accept or reject the request via the Sponsor Portal. The user's enrollment workflow stops in mid-process until the sponsor either accepts or rejects the request. For an example, see Request Access from a Sponsor Online on page 104.

Request Access From a Sponsor Offline

Prompts the user for a sponsor's email address and then notifies the sponsor. The sponsor can accept or reject the request via the Sponsor Portal. The user can be notified via email or text message. If the user's request is accepted, the user can return to the workflow to continue the enrollment process. For an example, see Request Access from a Sponsor Offline on page 108.

Register a Device for MAC-Based Authentication

Registers the MAC address of the device for MAC authentication by RADIUS. This is used for two primary use cases:

- To authenticate the device on the current SSID via the WLAN captive portal.
- To register a device, such as a gaming device, for a PSK-based SSID.

In both cases, the MAC address is captured and the device is permitted access for a configurable period of time.

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

Display a Message To Users

The message plug-in provides information to the end-user. The message is displayed, along with a single button to **Continue**. Use the message plug-in to welcome partners or guest users to your network and provide links for where to get additional information.

> **NOTE**
> To use this plug-in to indicate Wifi4EU support, refer to WiFi4EU Support Within the Display-a-Message Plugin on page 122.

Redirect Users to an External URL

Redirects the user to a specified external URL. This may be used to authenticate the user to the captive portal of the onboarding SSID.

Prompt User For Information

The data prompt plug-in provides a means for gathering information about a user. This user data can be used for informational purposes only, or for configuration purposes, such as personalizing certificates.

Authenticate Using a Shared PassPhrase

This authentication method prompts the user for a shared passphrase and verifies that it is correct. A shared passphrase is useful for controlling access to an enrollment process separate from, or in addition to, user credentials.

Generate a Ruckus DPSK

Selecting this plug-in invokes two choices:

- Create a new DPSK pool: This is called External DPSK because you can create the pools and manage them within the Cloudpath system; they are "external" to the controller. For more information, refer to the *Cloudpath Enrollment System Ruckus External Dynamic Pre-Shared Key (eDPSK) Configuration Guide*.

- Store DPSKs in a controller (Legacy): For this option, refer to the *Cloudpath Enrollment System Ruckus Legacy Dynamic Pre-Shared Key (DPSK) Configuration Guide*.

Send a Notification

Generates a notification about the enrollment, and can be added anywhere in the workflow. Notification types include email, SMS, REST API, syslog and more. This step is invisible to the end-user. All enrollment-related data is available for use in the notification via variables.

Charge User for Service

Directs the user to pay for service via a third-party payment service. This includes PayPal. For an example of using this plug-in, refer to Charge User for Service on page 99.

Example Workflow with Two Branches

The following image represents a workflow that is split into two branches, with one sequence of steps for employees, and another for guest users. Each branch in the workflow specifies a different authentication method and assigns different certificates to the user.

FIGURE 4 Workflow With 2 Branches
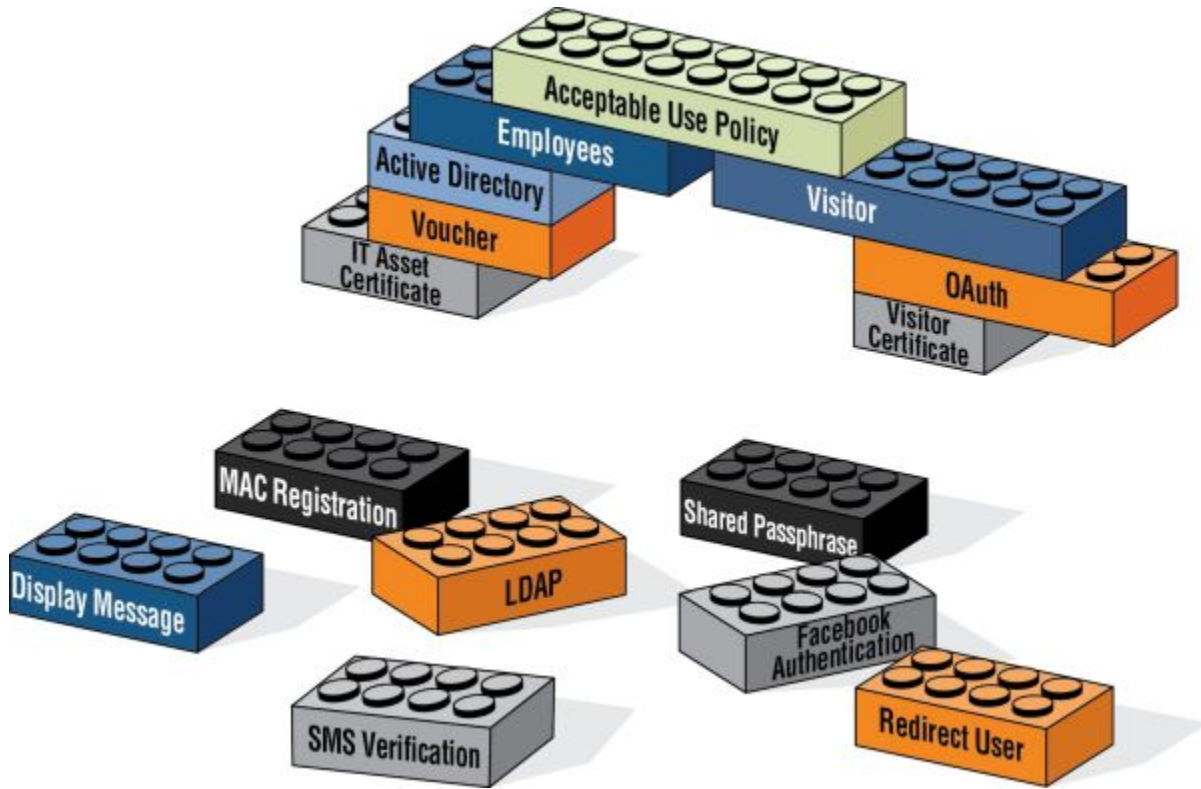
The model workflow above translates to the following example workflow in Cloudpath.

FIGURE 5 Cloudpath Simple Workflow
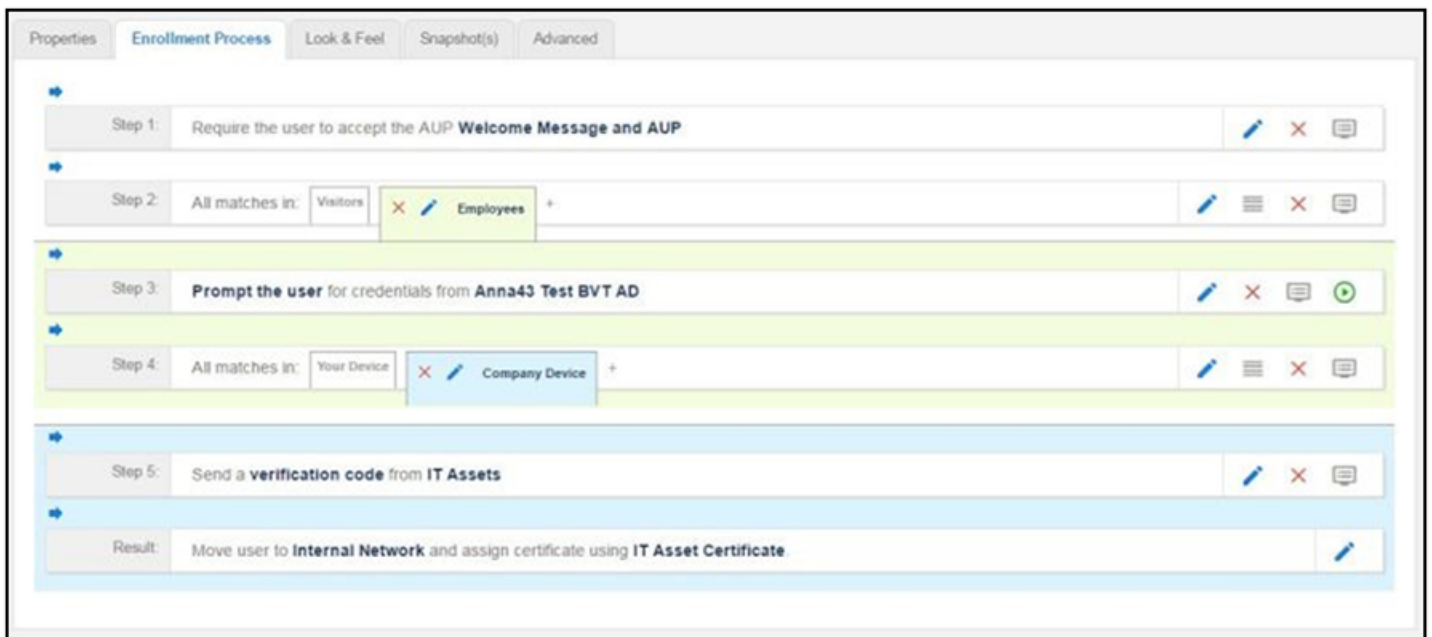
After the workflow is in place, you can fine-tune settings for specific OS versions, updates, and features, including customizations to the user experience. See Device Configuration and Client Certificate.

Example Complex Workflow

The following image represents a more complex, yet easy to configure workflow with multiple branches. The first split in the workflow accommodates different user types, and the other splits provide a different sequence of events for device types, internal and external network access, and provide client certificates with the appropriate validity period.

FIGURE 6 Complex Workflow
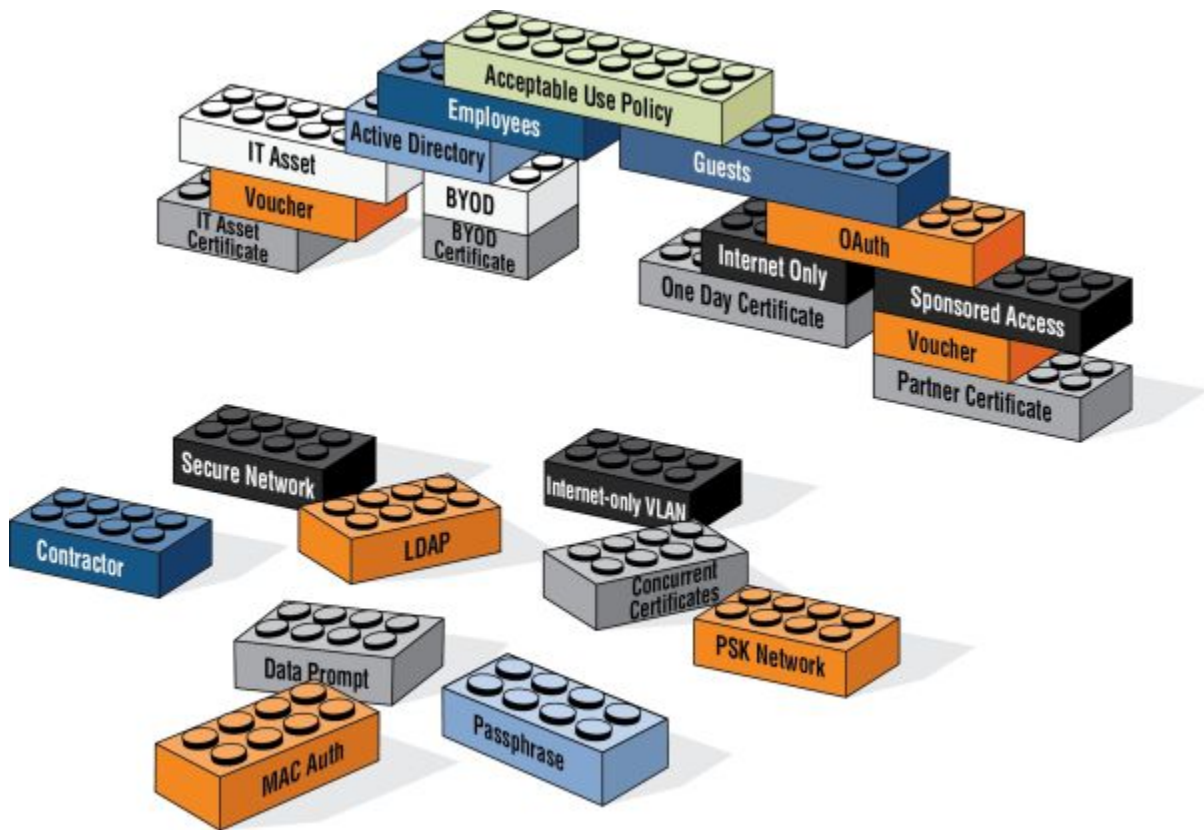
Enrollment Workflow Use Cases

Overview

This section provides some enrollment workflow examples to help you get familiar with the different types of steps that can be configured with Cloudpath.

Employee With IT Asset Authenticated to AD Group

This is an example workflow for an employee using an IT-assigned device to access the secure network. The employee is authenticated to an Active Directory group, and the device type split is managed with a filter, which moves the user to the Company Device workflow branch if they are a member of a specified AD group. They are prompted to enter a previously sent/assigned voucher and moved to a secure internal network.

FIGURE 7 Example Workflow for Employees with IT Assets
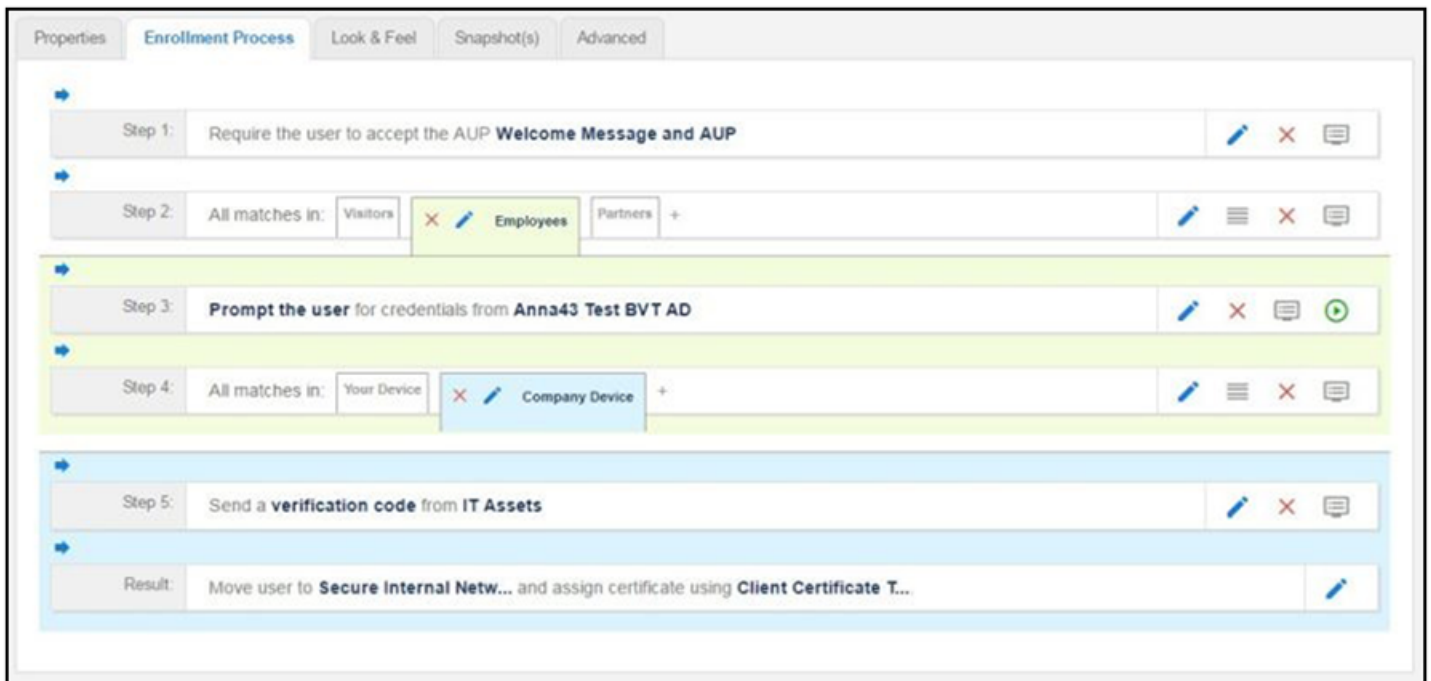
Your workflow does not have to be in the same order as the example. For example, you can move the authentication to LDAP step to immediately after the AUP step and then have the split for different workflow branches be immediately following. If you set up a filter on the LDAP group name, users can be moved to the appropriate workflow branch.

Employee With Personal Device Authenticated to AD Group

This is an example workflow for an employee using a personal device to access the secure network. The employee authenticates to an Active Directory group, and the device type split is managed with a filter, which displays the Personal Device workflow branch only if they are a member of a specified AD group. The user is asked to acknowledge a BYOD use policy before being moved to a secure internal network.

FIGURE 8 Example Workflow for Employees with Personal Devices (BYOD)
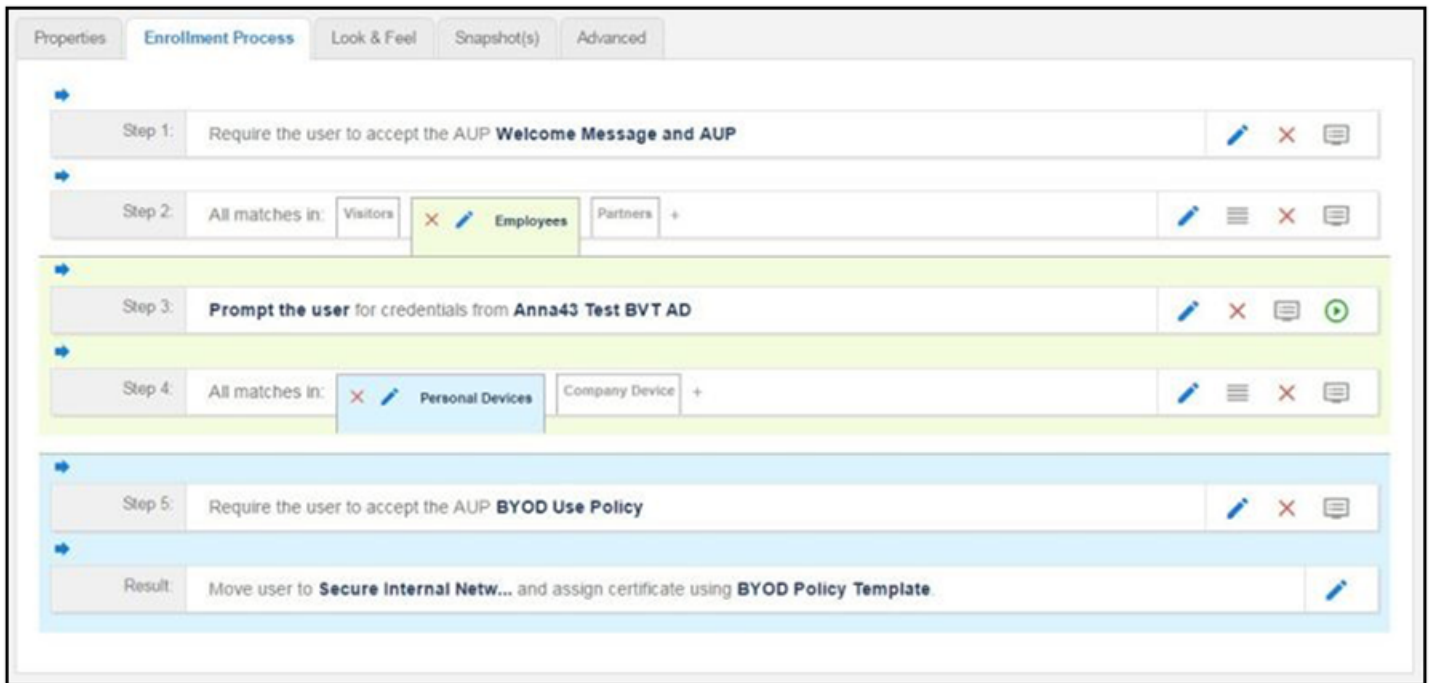
Employee With Personal Device on Internet-Only VLAN

This is an example workflow for an employee using a personal device on the secure network, but is limited to an Internet-only VLAN. The employee authenticates to an Active Directory group, and the device type split is managed with a filter, which moves the user to the Personal Device workflow branch if they are a member of a specified AD group. The user is asked to acknowledge a BYOD use policy before being moved to an Internet-only VLAN with a certificate that is limited to 30 days access.

FIGURE 9 Example Workflow for Employees with Personal Devices on Internet-only VLAN

Planning the Local Network Configuration

Overview

The process of configuring and connecting a device to the secure network requires the integration of many components of your network. The wireless LAN controller redirects to Cloudpath. Cloudpath issues a user certificate based on user store credentials. The client is authenticated by a RADIUS server, which verifies the certificate. The network Wizard installs the certificate in the local certificate store and migrates the user to the secure network.

Before you implement Cloudpath in your network, consider the following components of your network.

- WPA2-Enterprise Infrastructure
- Setting Up SSIDs
- Setting Up Captive Portal Redirect
- Certificate Authority
- RADIUS Servers
- Supported Authentication Servers
- DNS
- Firewall Configuration
- Use Cases

WPA2-Enterprise Infrastructure

Cloudpath works in your existing WLAN infrastructure using standards-based WPA2-Enterprise.

The following basic components are required for setting up a WPA2-Enterprise network. These components most likely exist in your network and can easily be configured to work with Cloudpath to complete the secure Wi-Fi configuration in your network.

- WPA2-Enterprise requires an external authentication server (RADIUS or NPS) to handle 802.1X user authentication.
- WPA2-Enterprise requires a CA to issue and install certificate on the RADIUS server
- The external authentication server (RADIUS or NPS) client database should be populated with the IP address and shared secret for each access point and user data with usernames and passwords for each end-user.
- On each AP, configure WPA2-Enterprise and add the authentication server (RADIUS or NPS) IP address and shared secret.

Setting Up SSIDs

Cloudpath requires an open SSID for onboarding, and one or more secure SSIDs, depending on your deployment scheme. The open SSID terminates to a captive portal that points to Cloudpath, and the secure SSID is the network to which your users migrate. We recommend creating an SSID specifically for Cloudpath.

Configure the secure SSID to use TLS, and point the RADIUS authentication requests to the RADIUS sever, whether that is the Cloudpath onboard RADIUS server, a Microsoft NPS, or other external RADIUS server.

Guest SSID

If your security policy provides a guest SSID for Internet-only or limited network access, you can set up an open SSID specifically for guests. The guest SSID redirects guest users to the Cloudpath captive portal, where they can onboard to a limited access network. The limited access is managed using VLAN assignment, which is configured in the wireless LAN controller, where you can also filter, shape or throttle the guest VLAN.

Conflicting SSIDs

Cloudpath provides a method for managing conflicting SSIDs to prevent a device from roaming away from the secure network. When setting up the device configuration, in the conflicting SSID section, you can set it up to either delete the open SSID or set it to connect manually. See Device Configuration and Client Certificate.

Setting Up Captive Portal Redirect

After the SSIDs are set up, configure a captive portal page on your wireless controller so that it redirects users from the open SSID to the Cloudpath web page to begin the enrollment process.

- On the Wireless LAN Controller (WLC), configure the open SSID pre-authentication ACLs to permit access to the IP address of the Cloudpath server. Configure the WLC to point to Cloudpath as an **External** captive portal.
- Set up the secure WPA2-Enterprise SSID to delegate authentication to the Cloudpath onboard RADIUS server, the NPS, or an external RADIUS server.

  NOTE
  If using an external RADIUS server, you must configure layer 3 access to the Cloudpath virtual appliance to allow certificate status verification.

For more information, see the following sections in this guide:

- Ruckus Controller Integration for Cloudpath
- Cloudpath Captive Portal Setup for Cisco Controller

Certificate Authority

A WPA2-Enterprise network requires a certificate authority (CA) to issue and verify certificates on the RADIUS server. Cloudpath supports many different CA configurations, including an onboard CA to act as your own private CA, certificates issued from an external CA, or Cloudpath acting as a proxy for an existing CA.

If you are using a Microsoft CA, the Cloudpath onboard CA can be configured as your intermediate CA, leaving the your Microsoft CA as your root CA.

Onboard CA

The Cloudpath onboard CA can issue a server certificate to the onboard RADIUS server and it can issue client certificates. After the client certificate issued, all authentications take place using the certificate.

The onboard CA is a full X.509 public key infrastructure (PKI), which can issue client and server certificates binding a public key to a particular common name.

RADIUS Servers

WPA2-Enterprise requires an authentication server for issuing client certificates for the wireless authentication. Cloudpath provides an onboard RADIUS server, supports integration with your existing RADIUS server, or integration with a Microsoft Network Policy Server acting as a RADIUS server.

For all configurations:

- The wireless controller requires the port number and shared secret from the RADIUS server.

    > **NOTE**
    > If using the onboard RADIUS server, the shared secret and port number can be found on the **Administration** > **System Services** > **RADIUS** component page.

- Apply the RADIUS authentication server to the secure SSID.

- Populate the client database for an external authentication server with the IP address and shared secret for each access point and the user data with usernames and passwords for each end- user.

Onboard RADIUS Server

The onboard RADIUS server, which is a a FreeRADIUS server that has been optimized for TLS, is configured as part of the initial system setup. The RADIUS server issues client certificates and the client validates the RADIUS server by hostname.The onboard RADIUS server supports all vendor-specific attributes in the FreeRADIUS dictionary.

If you are using the onboard RADIUS server, Cloudpath can generate a RADIUS server certificate using the onboard CA and server certificate template. This certificate can be installed on the onboard RADIUS server as part of the initial system setup.

Microsoft NPS Acting as a RADIUS Server

If you are using the NPS acting as a RADIUS server, you must set up the NPS server role and a RADIUS server.

These steps are required when configuring Cloudpath to integrate with the NPS:

- Create a server certificate template for the NPS.

- Generate a server certificate for the NPS. Use the FQDN of the NPS server as the **ServerName**

- when you generate the certificate using the onboard CA.

- Download the Private Key of the Root CA.

- Import the private key of RADIUS server certificate for NPS into the **Personal Trust** store. The private key must be in *.key format.

- Import the Public Key of the Root CA in to the **Enterprise Trust** store. The public key must be in *.cer format.

    > **NOTE**
    > See the *Cloudpath Integration with Microsoft NPS Configuration Guide* for configuration details.

External RADIUS Server

If you prefer to use an existing RADIUS server in your network, you must add the IP address of the RADIUS server to Cloudpath to allow signed certificates to be uploaded to Cloudpath and the public certificate of the CA (onboard or external).

Alternately, a CSR can be used within Cloudpath to create a usable RADIUS certificate.

RADIUS Proxy

Cloudpath supports RADIUS proxy from an external RADIUS servers. For example, you can set up a configuration so that a certificate from a specific domain (@guest) is proxied to Cloudpath for authentication. When the external RADIUS server receives a RADIUS request from user@guest, the request is forwarded to the onboard RADIUS server.

This proxy configuration is set up on the external server.

To set up RADIUS Proxy on a Network Policy Server (NPS):

1. Go to **RADIUS Clients and Servers** and add a Remote RADIUS Server Group. The group will have one member, the Cloudpath server. Enter the IP address and shared secret from NPS.

2. Go to **Connection Request Policies**, add a policy for the RADIUS proxy. Add a Condition so that the NPS looks for the @guest in the username and, if found, forwards the request to the "remote radius group", which is the Cloudpath server.

Cloudpath receives the request (similar to it coming straight from the access point) and responds.

Additional Radius Configuration Options

RADIUS Accounting

RADIUS Accounting, which provides start/stop information and byte counts on the connection, is supported on port 1813.

RADIUS Server VLAN Attributes

When setting up SSIDs in the WLC, you can use VLANS to apply policies for different groups by combining the VLAN in the RADIUS Request as a RADIUS attribute. RADIUS attributes are configured on the certificate template.

VLAN Tagging

The onboard RADIUS server can assign policy information for devices by defining VLAN tags in the certificate template.

If you are using the Microsoft NPS as a RADIUS server, VLAN tags are managed from the NPS.

Certificate Revocation

You can disable network access in Cloudpath by revoking the user or device certificates.

- When using the NPS acting as your RADIUS server, you can disable the AD account, and because the AD and RADIUS server are tied together, the disabled account status is registered by the RADIUS server.

- When using the onboard RADIUS server:

  - To disable access for a user, locate the certificates associated with the user account and revoke these certificates in Cloudpath.
  - To disable access for a device, revoke only the certificate associated with the device.

Supported Authentication Servers

Cloudpath supports Active Directory, LDAP and a variety of third-party authentication servers, such as Facebook, LinkedIn, or Google.

Active Directory

When using Active Directory with Cloudpath, the initial user authorization is established using AD credentials, and subsequent authentications are based on the client certificate.

Consider the following information when using Active Directory in your network.

- You need AD domain information (plus any sub domains) and the IP address of the AD server.
- Set up your AD groups for use with wireless BYOD access or Sponsorship Grounds (if needed).
  - Cloudpath must have layer 3 access to the AD server.
- The AD host is an LDAP call and must be an IP routable address.
- During authentication, the username is compared to the AD SAM attribute.
- The FQDN of your AD server or IP address maps to the internal AD server IP address.
- If you are using one of the hosted Cloudpath systems (onboard.cloudpath.net, onboard2.cloudpath.net, etc.), check the Firewall Requirements page for the DNS IP address.
- Cloudpath communicates to the AD server using TCP Port 389, LDAPS TCP/UDP 636.

LDAP or LDAPS

To use LDAP with Cloudpath, you need:

- DNS/IP of the active directory server
- DN of the domain
- Username and password to bind to the LDAP server
- Cloudpath communicates to the LDAP server using TCP Port 389.

Third-Party Authentication

When you combine third-party authentication with traditional authorization methods, the social media provides additional identity information during the onboarding process to deliver automated, self- service access to the WPA2-Enterprise wireless network. Cloudpath supports third-party integration using Facebook, LinkedIn, Google, or you can specify a custom OAuth 2.0 server.

To use third-party authentication, you need the following application information.

- Facebook - App ID and Secret
- LinkedIn - API Key and Secret Key
- Google - Client ID and Client Secret.
- Google LDAP - Client and Google LDAP client certificate zip file

  NOTE
  For details on configuring Facebook, LinkedIn, or Google applications, see the appropriate configuration guide on the Cloudpath Admin UI **Support** tab.

RADIUS Using PAP

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

SAML 2.0 IdP

Cloudpath allows a Security Assertion Markup Language (SAML) Identity Provider (IdP) to be configured as an Authentication Server. With traditional authentication server types (LDAP, AD, etc) Cloudpath prompts for username/password, and the authentication server verifies the credentials. With SAML, Cloudpath delegates the IdP to prompt the user for credentials and verify the authentication.

Cloudpath Onboard Database

Select this option to enable end-users to authenticate to accounts defined within this system. This option is not meant to replace AD or LDAP system, but is useful for trial and demo accounts. You can also set specific passwords for users, as opposed to having the system set the user passwords.

DNS

DNS should be configured for Cloudpath and other components in your network. Consider the following information when setting up DNS in your network.

- Configure DNS for use with Active Directory.
- The host name of Cloudpath is the FQDN hostname you assign for DNS.

See DNS Issues in the Troubleshooting section of this document.

Firewall Configuration

This section describes the firewall ports that may need to be configured to use Cloudpath and Wizard. Cloudpath must be able to communicate with:

- xpc.cloudpath.net (TCP 80/443-HTTP/HTTPS)
- NTP server, 0.centos.pool.ntp.org on the standard NTP port (123). This can be configured to point to a local server during system setup, if you prefer.

Depending on your network configuration, you might be required to configure other firewall ports. See the following table.

TABLE 1 Firewall Ports for Use with Cloudpath

Port	Protocol	Notes
80	TCP and UDP	Android Communications
443	TCP and UDP	Android communications with Google Play and Amazon Market.
5228	TCP and UDP	Android APK
389	TCP	Active Directory, LDAP queries
80	TCP	NPS query to Cloudpath for OCSP
1812	UDP	RADIUS Authentication
1813	UDP	RADIUS Accounting
8022		SSH. This is the default port for SSH.

TABLE 1 Firewall Ports for Use with Cloudpath (continued)

Port	Protocol	Notes
22		SSH. This port can be configured for SSH.
3268	TCP	LDAP recursive domains
	Windows RPC	I f you are using the Integration Module for Microsoft CA, the web server communicates with the Microsoft CA using Windows RPC.
3799	UDP	RADIUS Change of Authorization (CoA)
pool.ntp.org: 123		Perform NTP synchronization.

After Cloudpath is configured, a Firewall Requirements page is provided to help you understand the traffic to and from the system. Navigate to **Administration** > **Firewall Requirements** or see the Troubleshooting Your Deployment section for more information.

Use Cases

Before configuring your network for use with Cloudpath, you should have some idea about your deployment scheme for the different users in your network.

Use these questions to help you determine a deployment scheme.

- Will employees be allowed to access the secure network with personal devices?
- Do you want employees to sponsor guest user?
- How will guest users be authenticated? or do you want them to use a third-party authentication? or will you place them in an Internet-only VLAN?
- Should contractors have limited access? How long should we allow them on the secure network?
- How long do you want the different user types have access to the secure network?

The Enrollment Workflow Use Cases section provides common use cases that you can use as workflow templates when planning your own deployment scheme.

Deployment Scenarios

Prerequisites for Configuring Cloudpath

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

Deploying the Virtual Image File

- VMware server or Microsoft Hyper-V Manager on which you'll install the Cloudpath virtual appliance.
- The URL where the image file resides. A Cloudpath representative provides this information.
- Hostname of the virtual appliance
- IP address (and netmask) being assigned to Cloudpath on the VMware server. Not needed if using DHCP.
- IP address to restrict administrator access
- IP address of the DNS server(s).
- Gateway IP address

Setting up the Initial Account

- Login credentials for the Cloudpath License Server
- License Server URL
- 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.
- WWW 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.

- A list of conflicting SSIDs (open SSIDs, to prevent roaming)

- 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 passcode).

Deploying the Virtual Appliance to a VMware Server

> **NOTE**
> If using a Microsoft Hyper-V deployment, see Deploying the Virtual Appliance to a Hyper-V Server.

The deployment process consists of the following steps:

- Retrieve OVA File

- Deploying the Virtual Appliance Using a VMware vCenter Client

or

- Deploying the Virtual Appliance Using a Console-Based Client Test Network Connectivity

- Test Network Connectivity

Retrieve OVA File

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

When the download is complete, deploy the OVA file using a VMware client.

Deploying the Virtual Appliance Using a VMware vCenter Client

1. Open the VMware client.

2. Select **File** > **Deploy OVF Template**.

3. Enter the file path or URL where the OVA file resides.

4. Accept the EULA.

5. Enter a unique name for the virtual appliance.

6. Select a deployment configuration:

   - Non-Production POC - Deploys using 6GB RAM and 2 vCPUs x 1 Core. Recommended for software trials, feature testing, and other non-production systems.

   - 4,000 or Fewer Users - Deploys using 8GB RAM and 2 vCPUS x 2 Cores. Recommended for production systems with fewer than 4,000 users.

   - 8,000 or Fewer Users - Deploys using 12GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with fewer than 8,000 users.

   - More than 8,000 Users - Deploys using 16GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with more than 8,000 users.

   - More than 20,000 Users - Deploys using 20GB RAM and 2 vCPUS x 4 Cores. Recommended for production systems with more than 20,000 users.

7. If you are using VMware vCenter™ Server to manage your virtual environment, select the appropriate data center, cluster, host, and destination storage, as needed.

    ● 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.

8. Select a disk format.

9. Continue the configuration with vCenter, or a non-vCenter console.

    ● If you are using the vCenter to configure application and network properties, continue to the next section.

    ● If you are using the console to configure application and network properties, review the initial settings and click **Finish**. See Deploying the Virtual Appliance Using a Console-Based Client to complete the deployment process.

Application Properties (vCenter)

Customize the application properties for the deployment.

FIGURE 10 Application Properties

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

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

2. Enter the IP Address, Netmask, Default Gateway, and the DNS Servers for this VM. Leave blank for DHCP.

3. Specify an NTP Server or leave the default.

4. HTTPS is enabled by default. Leave unchecked only if Cloudpath is behind another web server using SSL.

5. Select the **Timezone**.

6. Select SSH port, or disable SSH access.

7. Enter the IP address(es) that can access the Cloudpath Admin UI. Leave this field blank if you do not want to limit administrative access.

8. Enter and confirm a **service user** password. The **service user** account is used by your support team for access to this system using SSH. The **service** account is not available if SSH access in not permitted.

Confirm Deployment Settings (vCenter)

1. Verify these properties before you begin the deployment.

    If you are using DHCP, the networking properties will be blank.

    FIGURE 11 Deployment Settings
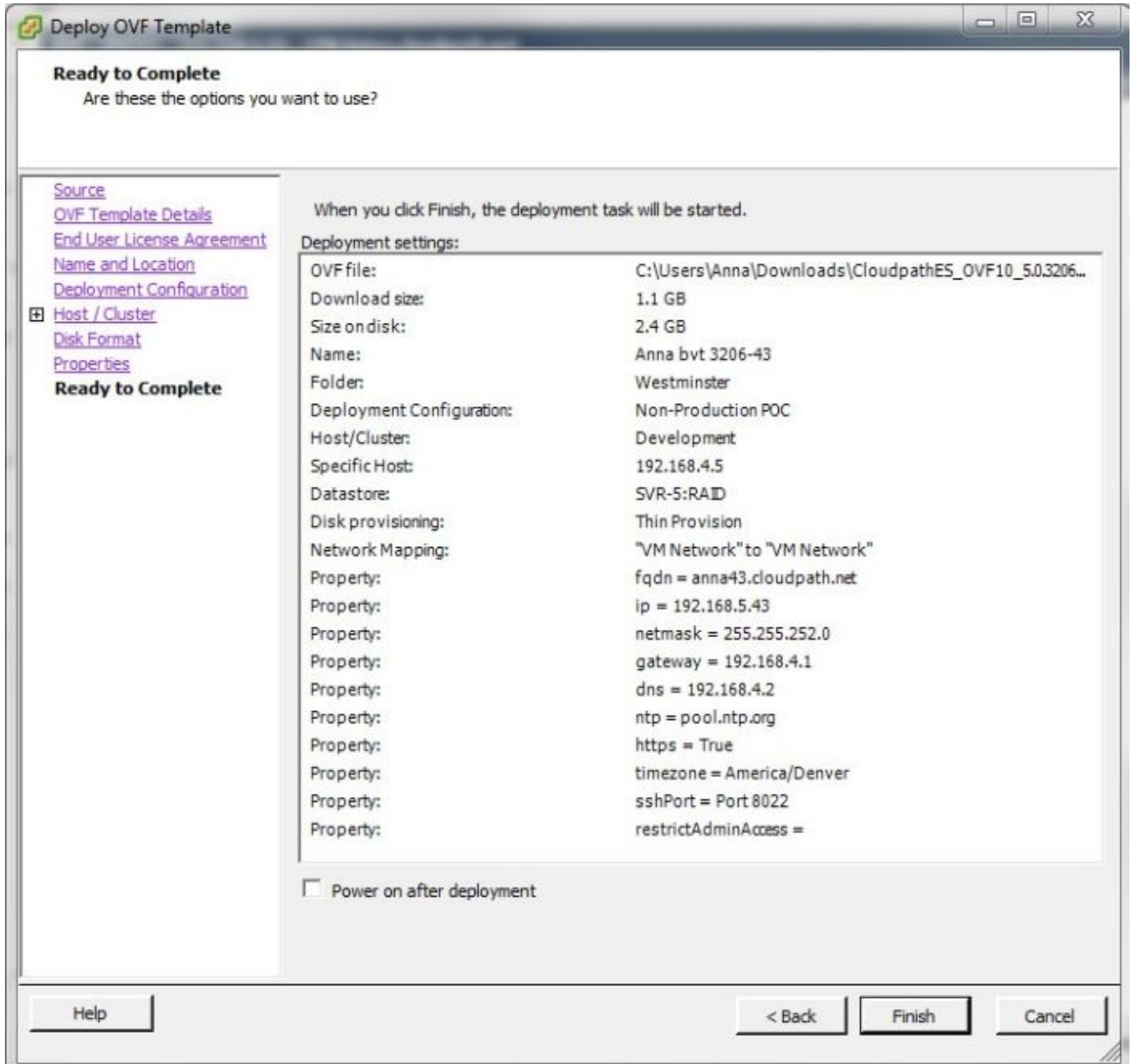
2. Click **Finish**

    Deployment takes approximately 2 minutes.

Deploying the Virtual Appliance to a Hyper-V Server

> **NOTE**
> If using a VMware deployment, see Deploying the Virtual Appliance to a VMware Server.

The deployment process consists of the following steps:

- Retrieve OVA File
- Deploying the Virtual Appliance Using a VMware vCenter Client
- Test Network Connectivity

Retrieve VHDX Image File

Retrieve 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 VHDX image file, binding your VHDX file with the activation code.

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

Deploying the Virtual Appliance Using Hyper-V Manager

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

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

   - For software trials, feature testing, and other non-production systems, we recommend using 6GB (6144MB) RAM and 2 virtual processors.
   - For production systems with 4,000 or fewer users, we recommend using 8GB (8192MB) RAM and 4 virtual processors.
   - For production systems with 8,000 or fewer users, we recommend using 12GB (12288MB) RAM and 8 virtual processors.
   - For production systems with more than 8,000 users, we recommend using 16GB (16384MB) RAM and 8 virtual processors.
   - For production system with more than 20,000 users, we recommend using 20GB (20480) RAM and 8 virtual processors.
7. Leave **Use Dynamic Memory** selected (the default) and click **Next**.
8. On the **Configure Networking** screen, select the appropriate virtual switch in the **Connections** field. Click **Next**.
9. On the **Connect Virtual Hard Disk** screen, select **Use an existing virtual hard disk**, and browse to the location where the vhdx file exists. Click **Next**.
10. Verify the setup summary and click **Finish**.

The system creates the new virtual machine.
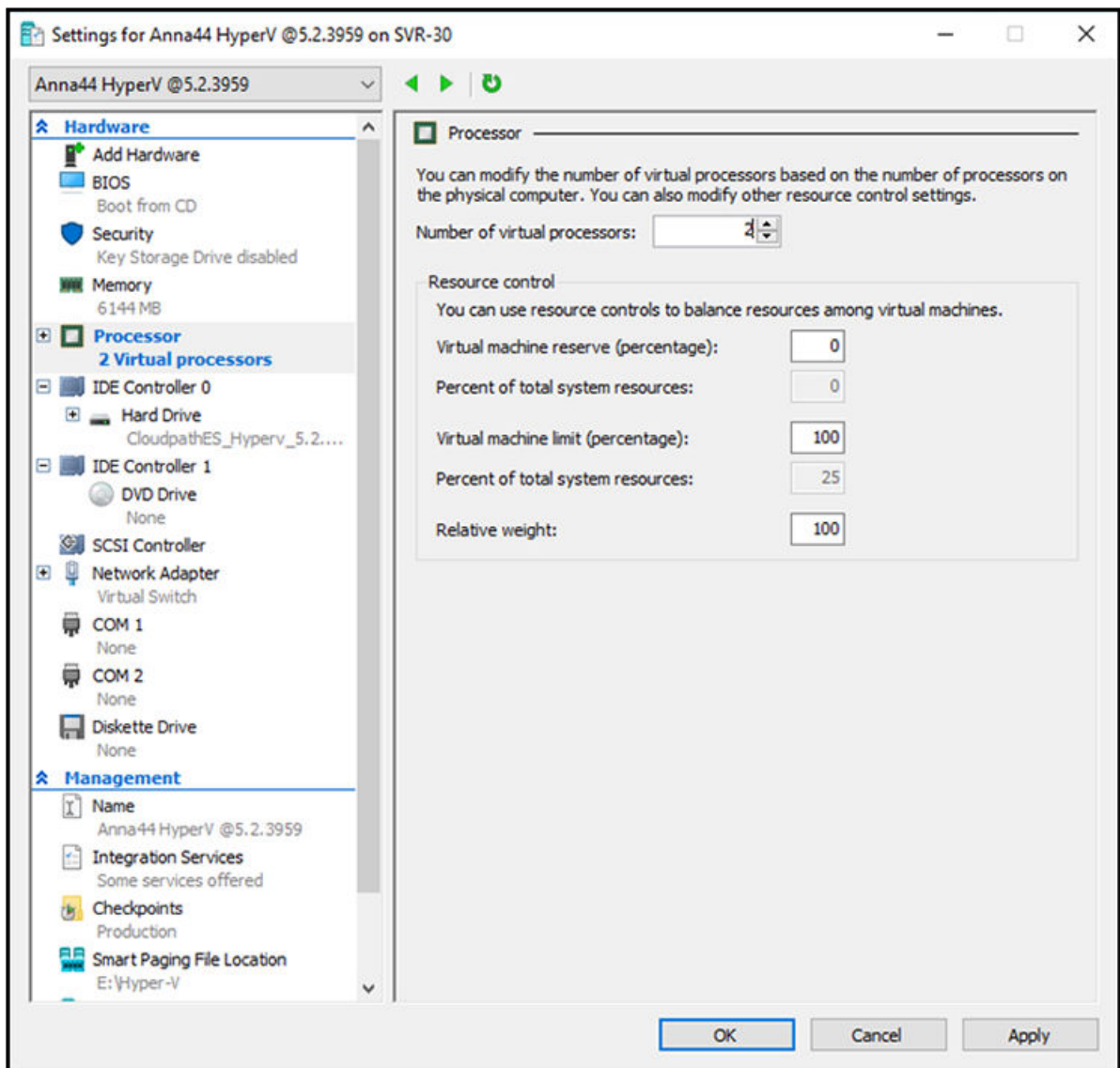
Configure Virtual Processors

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

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

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

2. Select **Processor**.

FIGURE 12 VM Settings

3. In the left pane, select **Processor**.

4. In the right pane, increase the value for **Number of virtual processors**.

5.   Click **Apply**, then **OK**.

Power on the virtual machine to continue with the configuration.

Deploying the Virtual Appliance Using a Console-Based Client

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

1.   Open the console on the VMware or Hyper-V Server.

2.   Enter **yes** (or **y**) to accept all license agreements.

3.   Enter the time zone. For example, enter **America/Denver**.

4.   Enter the **FQDN hostname** for the virtual appliance (ex., **onboard.company.com**).

5.   Do you want to enable HTTPS? **Enter** for yes (default) or **n**.

6.   Do you want to use a STATIC IP (rather than DHCP)? **Enter** for yes (default) or **n**.

  ●   If you enter yes (recommended), you assign the IP address of the virtual appliance, subnet mask, and gateway and DNS server IP addresses for your network.

  ●   If you enter no, DHCP is used to assign IP address of the virtual appliance 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** for yes (default) or **n**.

12.   Enter and confirm a **service** password.

The **service** password is used by your support team for access to this system using SSH. Refer to the *Cloudpath Command Reference* on the **Support** tab for details.

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

13.   Do you want to us an NTP server other than pool.net.org? **Enter** for no (default) or **y** to specify an NTP server.

The setup is complete.

14.   Press **Enter** to reboot the system.

After the reboot you are presented with the **shelluser** login prompt.

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

Service Account

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

To use the service account:

1.   Enter **cpn_service** at the login prompt, and then the service user password.

2.   Enter the **show config** command to verify your configuration. You may be prompted to re-enter the password.

     See the *Cloudpath Command Reference* on the left menu **Support** tab.

Test Network Connectivity

To verify that the virtual appliance is correctly deployed, perform the following operations from the VMware server console:

1.   Ping the gateway of your system.

2.   Ping the URL where the Cloudpath Licensing Server is hosted.

3.   Verify that the virtual appliance can resolve DNS.

How to Install VMware Tools

VMware Tools is a suite of utilities that you install in the operating system of a virtual machine. VMware Tools enhances the performance of a virtual machine and makes possible many of the ease- of-use features for managing your virtual appliance with the vCenter Client.

Use these instructions if you wish to install VMware Tools on the Cloudpath virtual appliance.

> **NOTE**
> We recommend that you take a VM snapshot before adding tools or making changes to the configuration.

From the vCenter Client

1.   From the powered-off state, select the VM, and right-click to **Edit Settings**.

2.   With the **Hardware** tab selected, click the **Add** button to open the **Add Hardware** page.

3.   Select **CD/DVD Drive** (or browse to locate the ISO for the media) and click **Next**.

4.   Continue with the configuration using the default settings. When finished, click **OK**.

5.   Power on the VM.

6.   Select the VM and right-click to select **Guest** > **Install/Upgrade VMware Tools**.

7.   Select **Interactive Tools Upgrade** and click **OK**.

     This popup does not occur on some systems.

From the Console

1.   Log in to the **cpn_service** account.

2.   Enter the following commands:

```
sudo mount -t iso9660 /dev/cdrom /media
cp /media/VMwareTools-XXXXX.tar.gz .
sudo umount /media
tar xvfzp VMwareTools-XXXXX.tar.gz
cd vmware-tools-distrib
sudo ./vmware-install.pl
```

> **NOTE**
> The VMware Tools version can vary within the same vCenter. Use the **Tab** button to auto-complete the VMwareTools-XXX.tar.gz commands to be sure you get the correct version.

3.   Select the default answers to the configuration questions.

       When finished, exit the `vmware-tools-distrib` directory.

When complete, select the **Summary** tab on the vSphere Client. The **General** section shows VMware Tools is **Running (Current)**. The **IP address** should match the IP address assigned to the Cloudpath virtual appliance.

How to Increase the Virtual Appliance Memory on VMware

> **NOTE**
> For Hyper-V deployments, refer to the *Deploying Cloudpath as a Virtual Appliance Using Microsoft™ Hyper-V Manager* configuration guide.
> We recommend that your VMware server have 12-16GB RAM, which is sufficient for most production environments. However, there may be circumstances (performance, larger deployments) that require adjustments to the memory allocation for Cloudpath.
> Use these instructions if you want to change the memory configuration of a virtual machine's hardware.

1.   From the vCenter client, power off the virtual appliance.

2.   Select the VM, and right-click to **Edit Settings**.

3.   With the **Hardware** tab selected, select **Memory**.

4.   On the right window pane, increase the **Memory Size**.

5.   Click **OK**.

6.   Power on and reboot the VM.

How to Expand the MySQL Partition Size

The database partition is designed to maximize performance of the Cloudpath operations. If needed, you can expand the size of the partition used for MySQL database operations.

From the vCenter Client

1.   With the VM running, select the VM and right-click to **Edit Settings**.

2.   With the **Hardware** tab selected, select **Hard disk 2**.

3.   On the right pane, in the **Disk Provisioning** section, increase the **Provisioned Size** to the desired size and click **OK**.

> **NOTE**
> If the Provisioned Size cannot be selected, try restarting the server using the **sudo halt** command.

From the Console

Enter the following commands as `root`.

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

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

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

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

3. Expand the physical volume.

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

4. Extend the size of the logical volume for MySQL operations.

   This example shows that we are extending the size of the logical volume by adding 25GB.

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

5. Resize the file system.

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

   This writes your changes to disk and completes the partition expansion process.

6. Verify the amount of free disk space available.

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

   The output should indicate the increased partition size.

Activate Account or Log In

Overview

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

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

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

Activate Account by Activation Code

If you have been sent an activation account, enter it on this activation page.
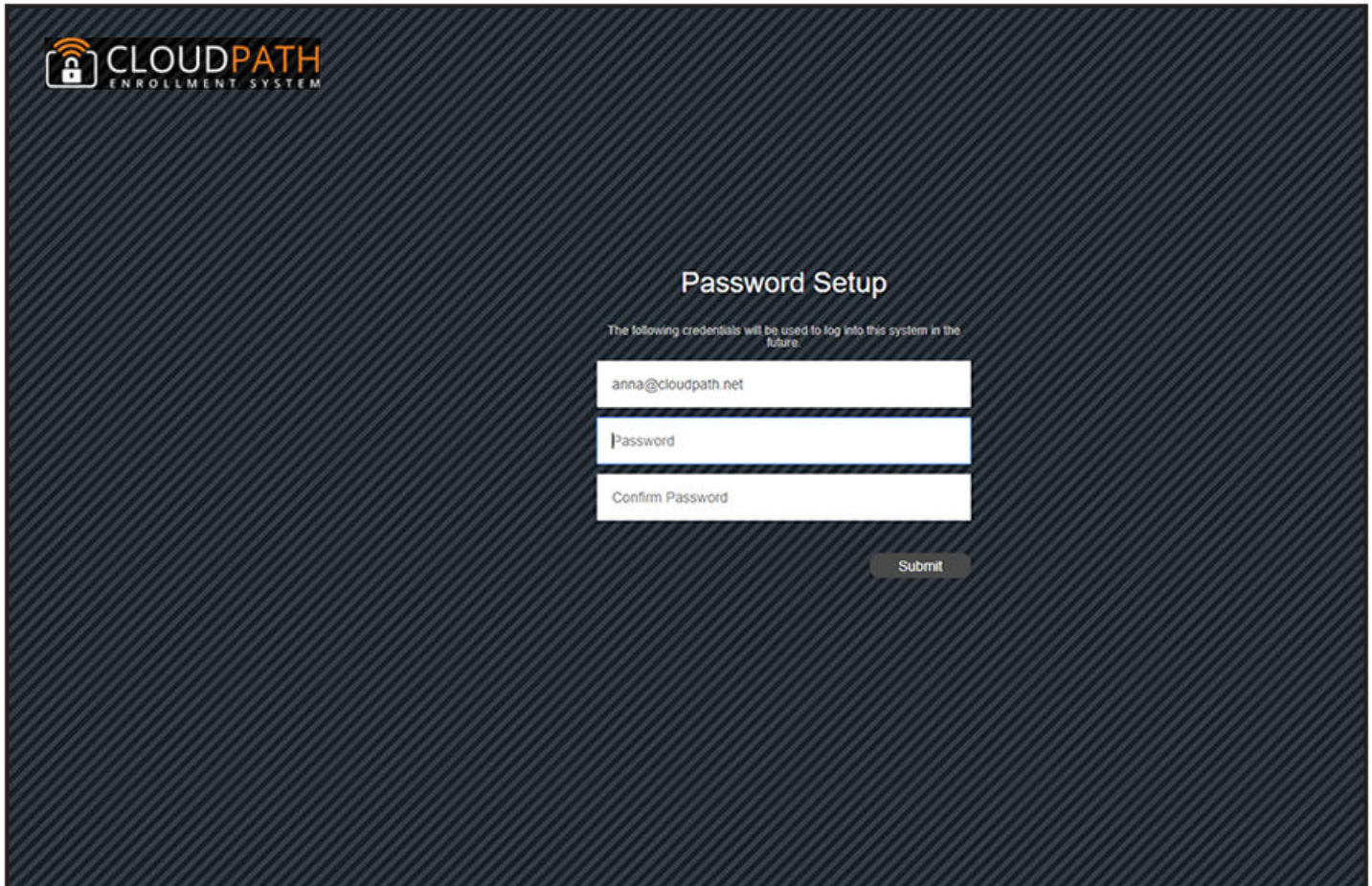
FIGURE 13 Activate Cloudpath Account
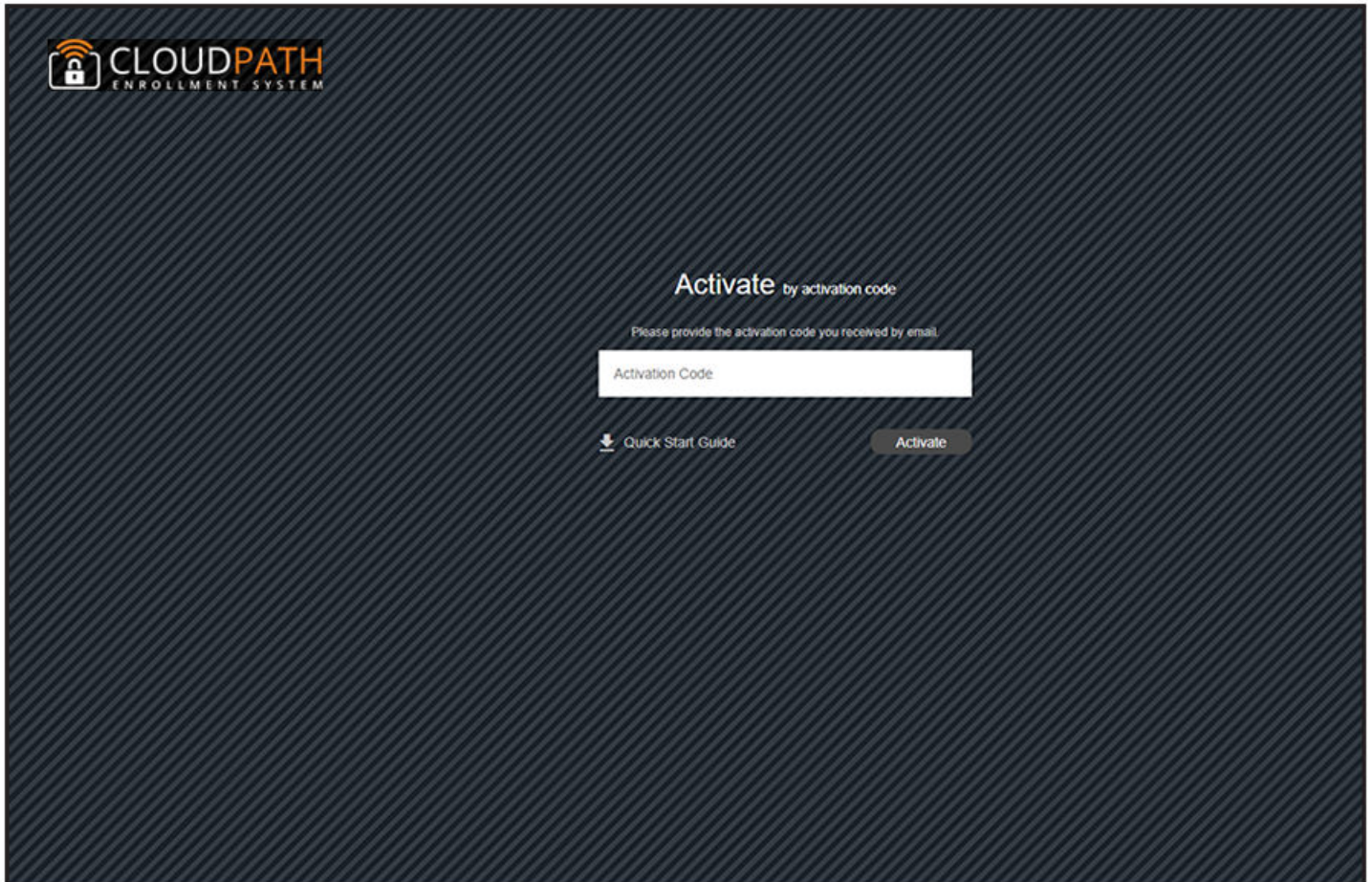
Set a Password for Account

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

FIGURE 14 Set Password
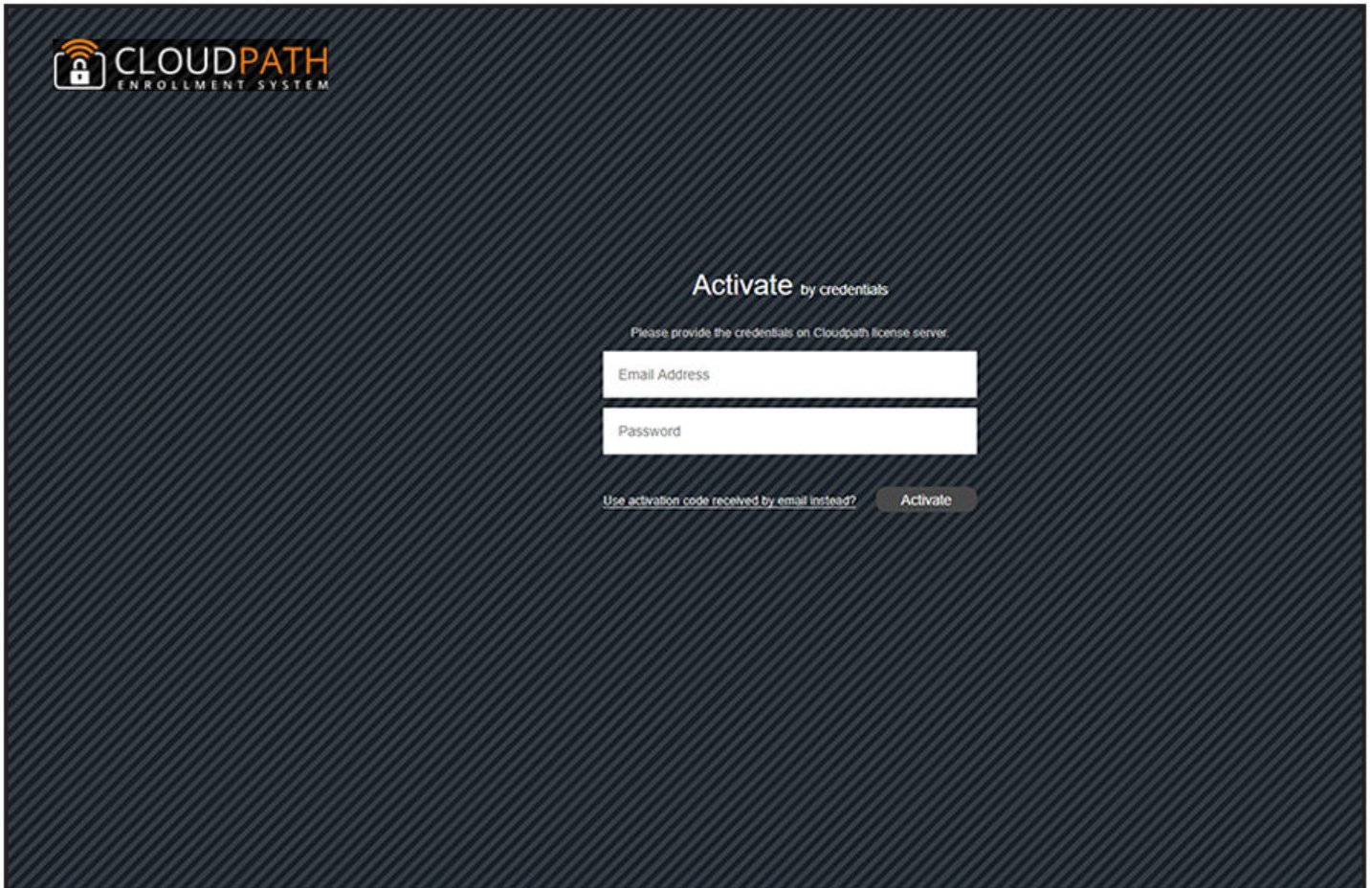
1. Your email address should display. If it does not, enter it on this page.

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 15 Activate Account With Existing Credentials

Initial System Setup

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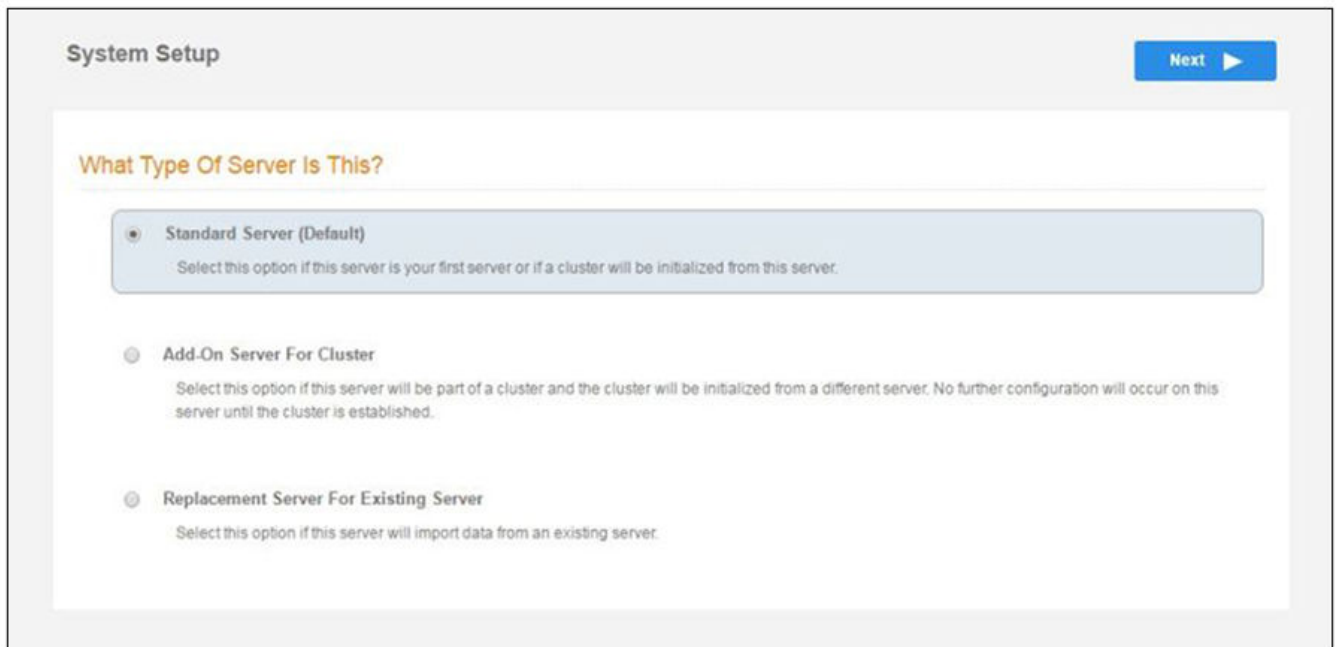
In most cases, select **Standard Server**, the default. This selection takes you through a setup wizard, which prompts you for the basic information required for an Cloudpath server.

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

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

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

2. Enter **Company Information**, then click **Next**.

This information is embedded in the onboard root CA certificate.

FIGURE 17 Company Information

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

    FIGURE 18 WWW Certificate for HTTPS Screen
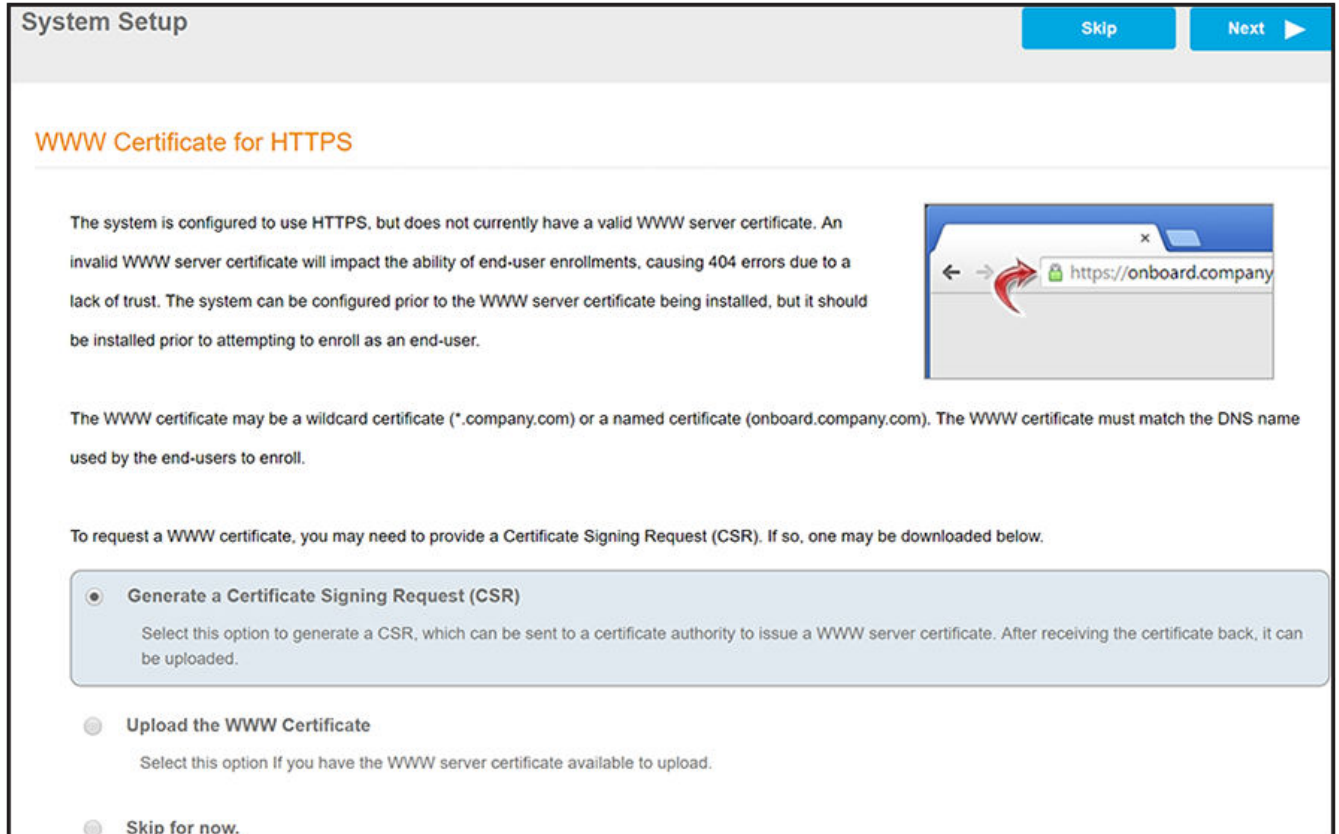
> **NOTE**
> Cloudpath supports web server certificates in P12 format, password-protected P12, or you can upload the individual certificate components: the public key, chain, and private key or password-protected private key.

- If you selected the "Generate CSR" radio button, perform Step 4.

- If you selected the "Upload the WWW Certificate" radio button, perform Step 5.

- You *can* select the "Skip for now" radio button for the initial configuration. However, you should perform this step prior to attempting to enroll as an end-user. To return at a later time to the screen shown above, navigate to **Administration > System Services** > Web Server service, then click **Upload WWW Certificate**. For now, proceed to Step 6

4. (Only if you selected "Generate CSR" radio button.) You should now be at the Create CSR for HTTPS screen:

FIGURE 19 Create CSR for HTTPS Screen

a) Enter the required information.

> **NOTE**
> In the Common Name field:
>
> ● If you are re-issuing a wildcard certificate, make sure the hostname includes ***.** For example: *.*domain*.com.
>
> ● If using a single-domain SSL certificate, the HTTPS server name should already be populated for you.

b) Click **Next**.

The Download CSR for HTTPS Screen is displayed:

FIGURE 20 Download CSR for HTTPS Screen
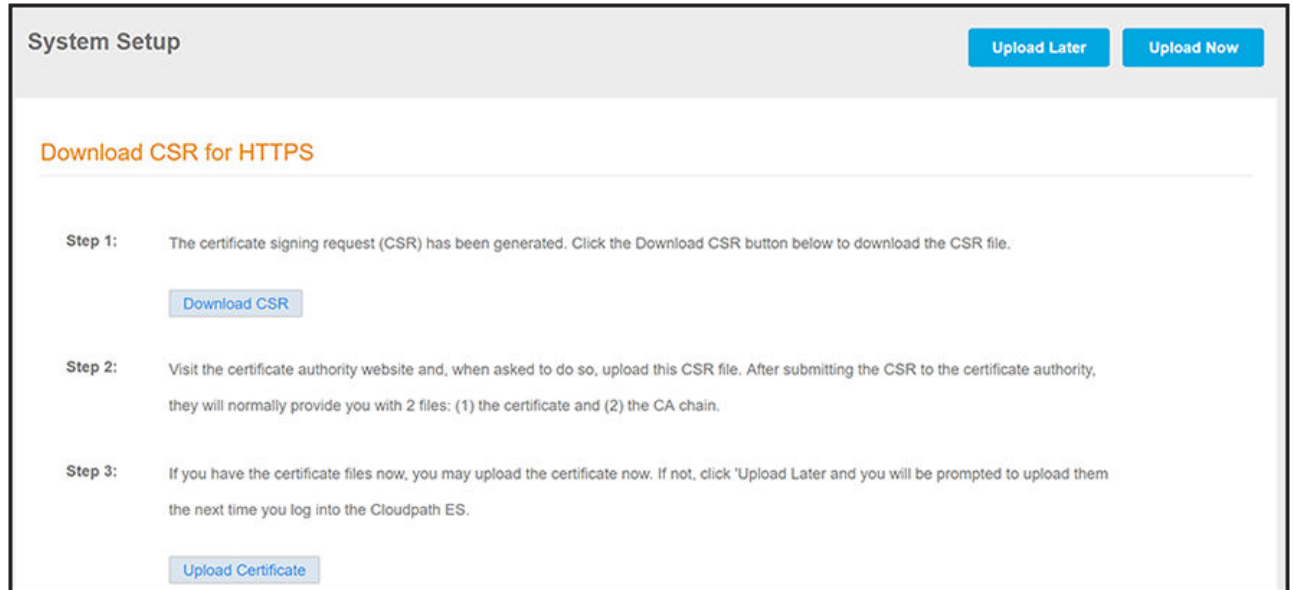
c) Click **Download CSR** to download the .csr file, which you can then open in Notepad.

d) Upload the CSR to any CA website to receive a certificate.

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

The public key usually has a filename similar to the domain name. The chain will vary depending on the CA, but it typically contains the word "Root," "Intermediate," " Bundle," or something similar, and may have the filename extension of .*chain*.

f) In the screen that is shown in , click **Upload Certificate**.

You are taken to the screen where you upload the files you received from the CA. The screen below shows the Private Key and the Chain already uploaded, and the Private Key Source is "Certificate is based on the downloaded CSR":

FIGURE 21 Upload WWW Certificate Based on the Downloaded CSR

g)   Upload your certificates using the screen shown above.

h)   Click **Next** to continue with the system setup.

i)   Proceed to Step 6.

5.   (Only if you selected the "Upload the WWW Certificate" radio button, which you should only have done if you already have received your WWW certificate from a public CA.) You should now be at the following screen:

FIGURE 22 Upload Existing WWW Certificate

a)   Upload your certificates using the screen shown above.

You can do one of the following: 1) Upload the Public Key, the Chain, *and* the Private Key, **or** 2) Upload the P12 file. The example in the screen above shows a P12 file has been uploaded.

b)   Click **Next** to continue with the system setup.

c)   Proceed to Step 6.

6. Select the Default Workflow.

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

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

FIGURE 23 Select Default Workflow
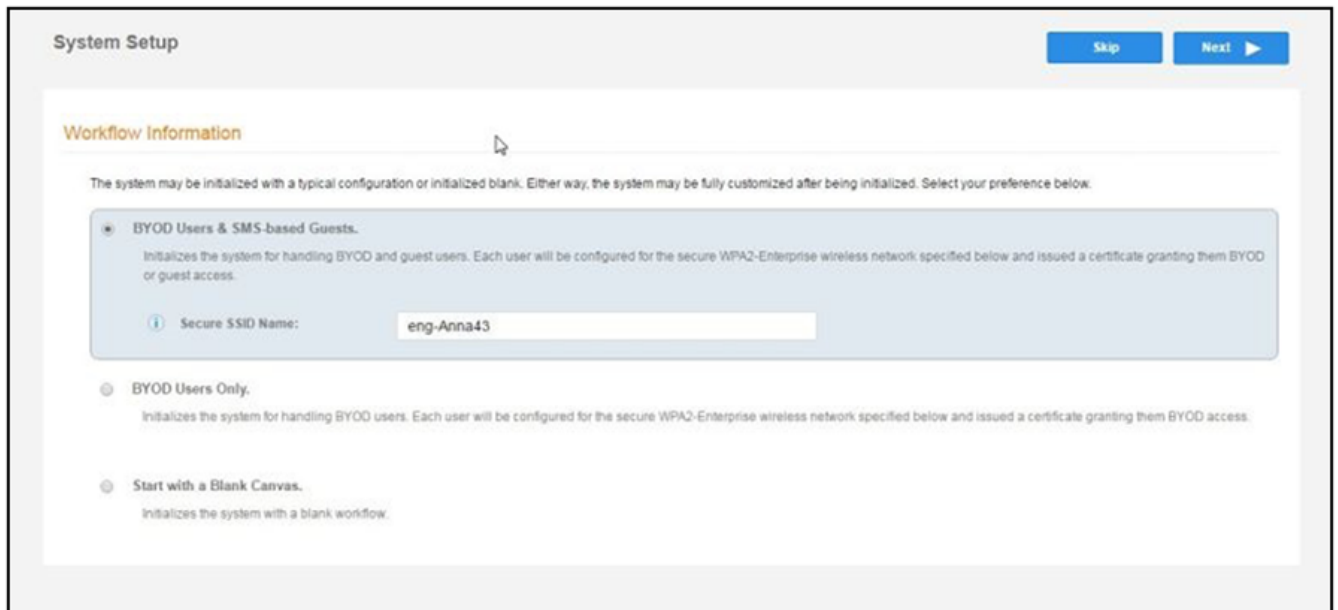
7.   Configure the Authentication Server.

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

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

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

FIGURE 24 Authentication Server Setup

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

b) Consider these optional settings for the authentication server:

- **Verify Account Status on Each Authentication** - If selected, Active Directory is queried during subsequent uses of the certificate to verify the user account is still enabled. You must provide the bind username and password for an authentication server administrator account.

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

- **Test Authentication** - If selected, an authentication will be attempted using the username and password provided to test connectivity to the authentication server. This test can also be run from the workflow.

8. Set up the Authentication Server Certificate:

a) To use LDAP over SSL (LDAPS), the system must know which server certificate to accept for the authentication server.

FIGURE 25 Authentication Server Certificate
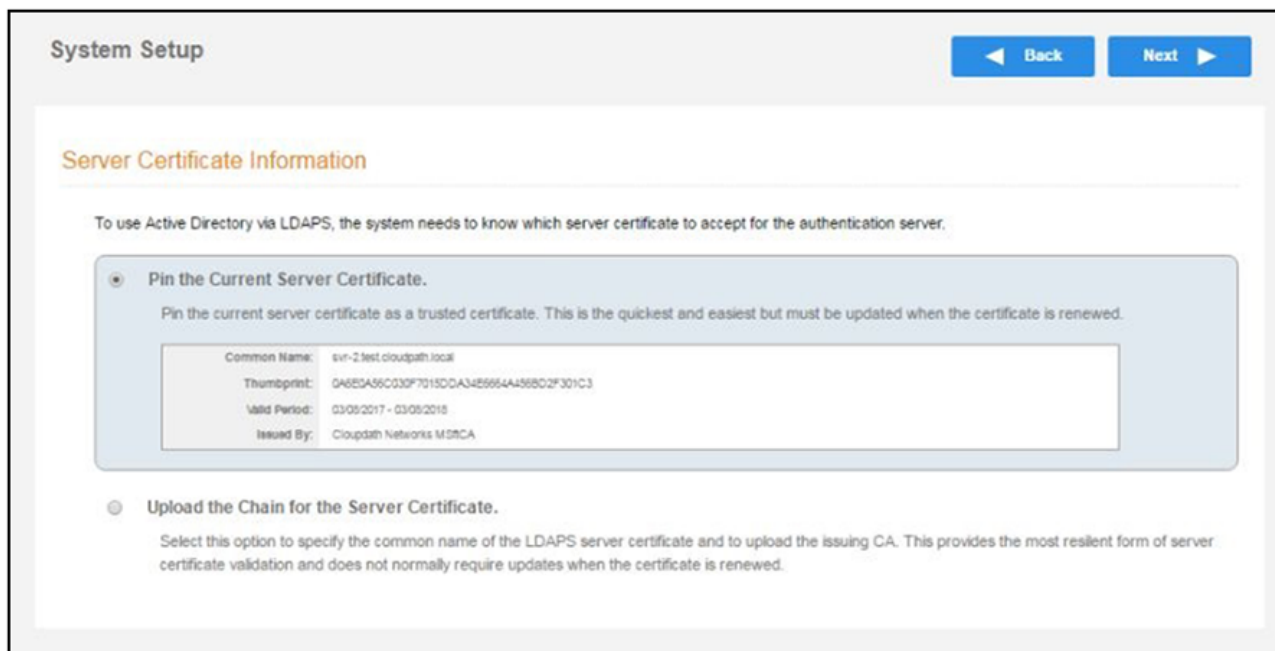
b) Select **Upload the Chain for the Server Certificate** to upload a certificate chain from an issuing CA. You must specify the common name for the LDAPS server certificate. This certificate does not need to be updated when the certificate is renewed.

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.

Setting Passwords for Onboard Database Users

The following steps show you how to add an onboard database user and specify a password:

1. Go to **Configuration > Authentication Servers** to display all the configured authentication servers; you are specifically looking for "Onboard database" servers.

FIGURE 26 Onboard Database Servers in the List of Configured Authentication Servers
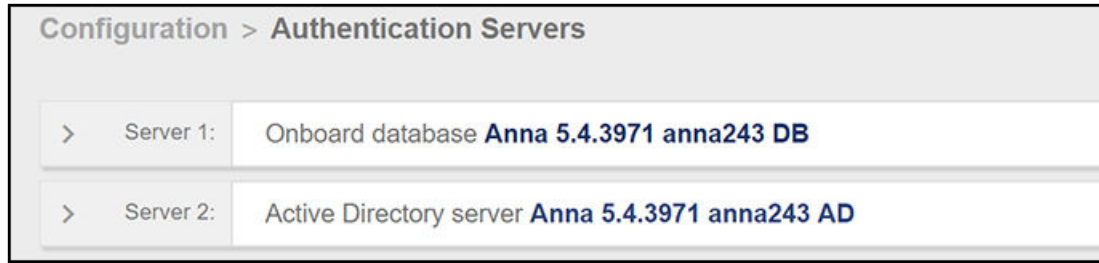
2. Click the arrow to the left of the desired onboard database server to display an expanded configuration for that onboard database:

FIGURE 27 Expanded Configuration Display for Onboard Database Server
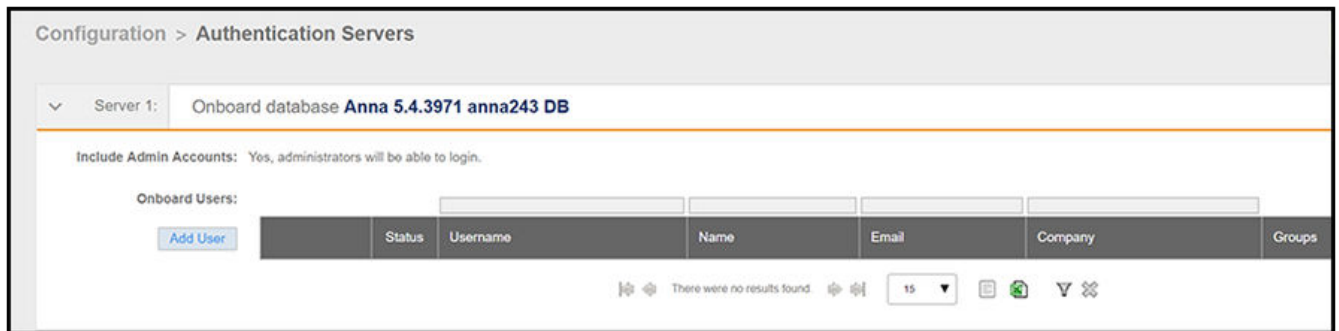
3. Click **Add User**. The Create User screen, where you can specify the user password, is displayed:

FIGURE 28 Create User Screen

4. Complete the User Information section, then, under "Credentials," check the Specify Password box. Enter the information for the Username, the Set Password, and the Confirm Password fields (shown below), and then click **Save** to complete the configuration. You need to notify new users of their credentials when you specify their passwords.

> **NOTE**
> If you do not use the Specify Password feature, the system notifies new users of their credentials.

FIGURE 29 Specifying the User Password

Editing User Passwords:

To edit the user configuration, click the arrow to the left of the desired onboard database server to display the configured user(s):

FIGURE 30 Editing the User Information

You can use the pencil, X, or key icons as follows:

- The pencil icon allows you to edit the user information, including an option to block the user.

- The X lets you delete the user.

- The Key icon lets you remove the password that you specified, and the system will email the user a new, randomly generated password.

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 31 System Initialization Status

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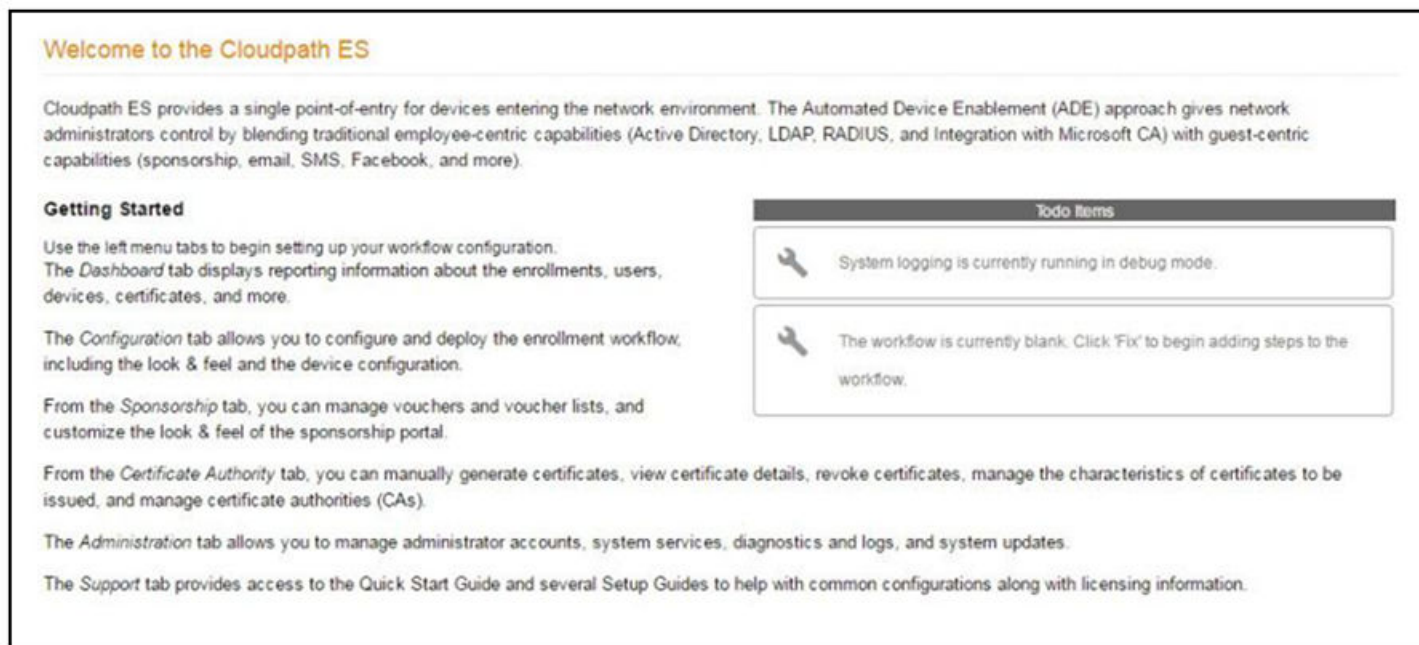
To configure Cloudpath, see the *Cloudpath Quick Start Guide*, and other Cloudpath configuration guides, which can be found on the Cloudpath **Support** tab.

Enrollment Workflow

Overview

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

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

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

Workflow Basics

Navigate to **Configuration** > **Workflows**.

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

- Use the **Properties** tab to update the workflow properties and the **Enrollment Portal URL Options**.

- Use the **Enrollment Process** tab to configure the steps presented to a user to create the workflow.

- Use the **Look & Feel** tab to configure the Cloudpath skin, and to customize the logos, colors, buttons, and images for the Cloudpath server, the Cloudpath Wizard, and the Download page.

- Use the **Snapshot(s)** tab to view the latest snapshot, the version, timestamp and the notes added to a particular workflow.

- Use the **Advanced** tab to view the **Enrollment Portal URL**, **Passpoint OSU URL**, and the **QR code**. You can also use it to **Manage Chromebook Setup and for Cleanup**.

FIGURE 33 Workflow Configuration Page
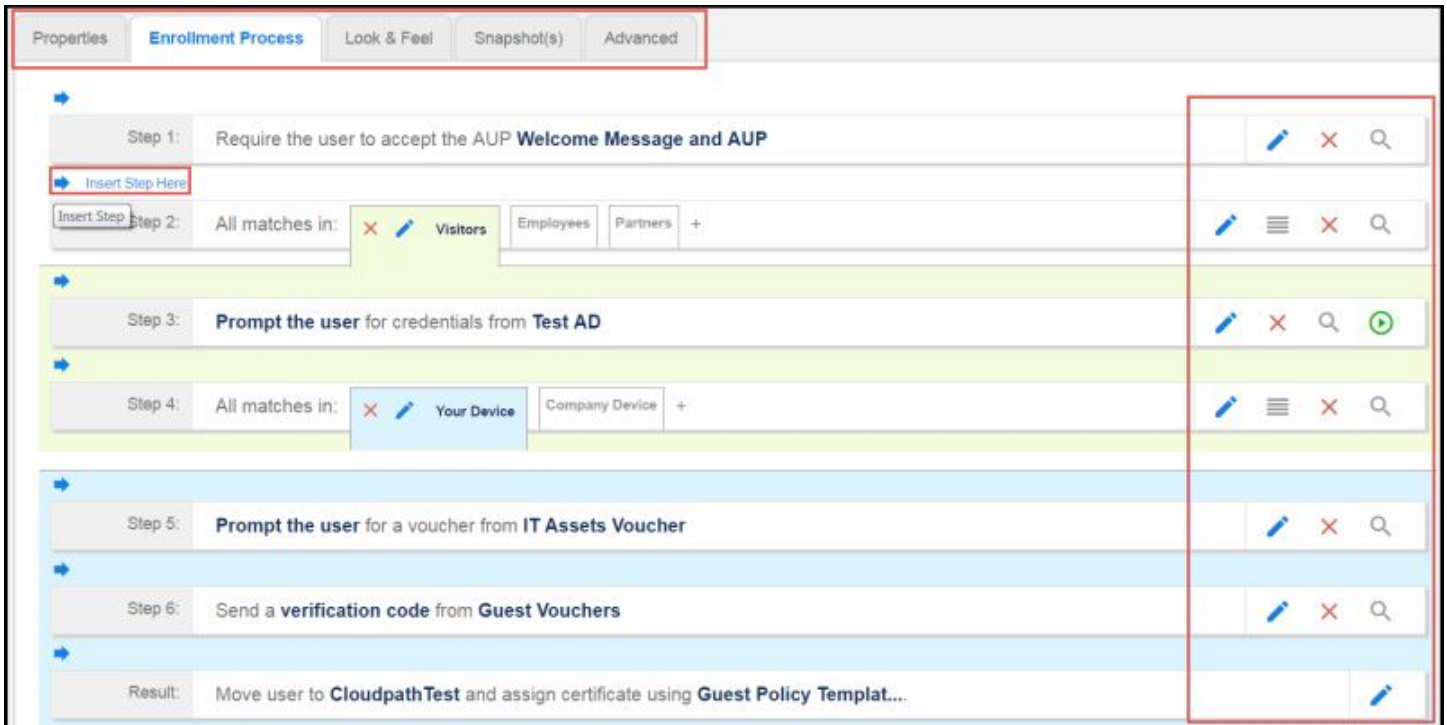
Use the icons along the side to make changes to the enrollment workflow:

- Use the icons on the right side of each step to edit, modify, delete, view the enrollment steps.

- Use the **Test Server** icon ⊙ to verify interaction with an authentication server.

- Use the **Edit List** icon ☰ to label options, to change the order of the selection options in a split, add more options, or add filters and restrictions.

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

- Use the icons on the split tabs to modify or delete a specific option.

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

Modifying a Workflow Template

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

To create a workflow from a template using sample data:

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

2. On the right hand side of the **Workflow** page, click **Add Workflow**, then, with the "Create a new Workflow" button selected, click **Next**.

   The Create Workflow screen is displayed:

   FIGURE 34 Create Workflow Screen - Selecting "BYOD and SMS Guest" For Workflow Template Type

3. On the **Create Workflow** screen, enter a **Display Name** and **Description**.

4. From the Workflow Template Type drop-down list, select "BYOD and SMS Guest."
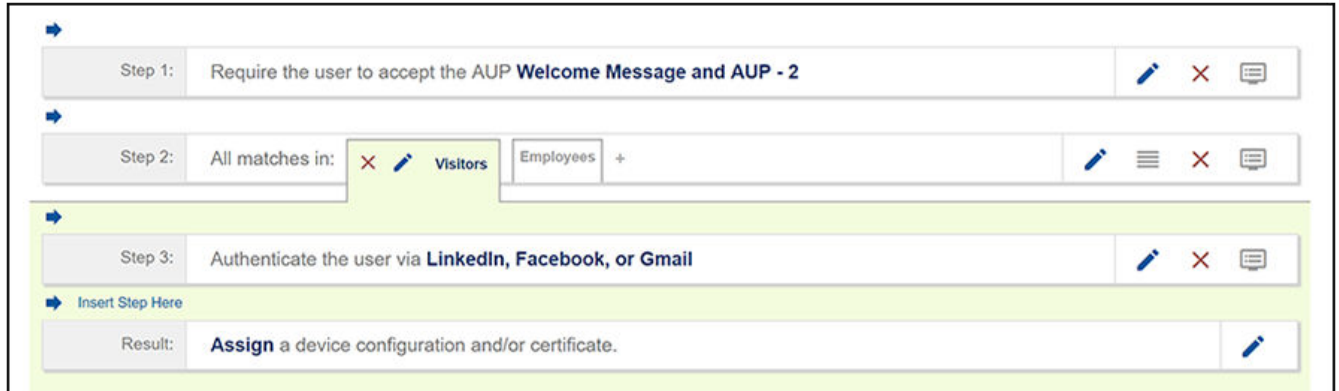
5. Fill out the URL Name field.

6. Click **Save**.

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

   FIGURE 35 Workflow Template

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

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

   FIGURE 36 Grid View of Configured Workflows
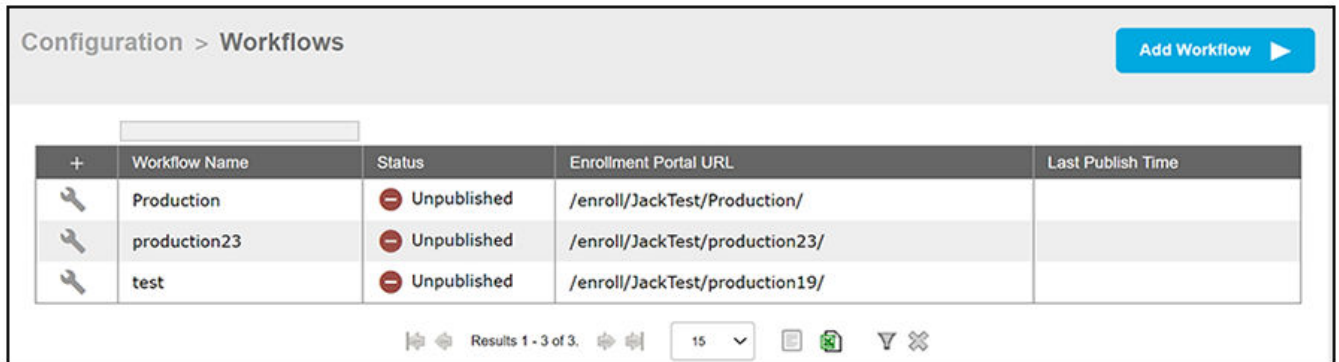
   To make changes to a workflow, click the wrench icon in the screen above (**Configuration > Workflows**).

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

TABLE 2 Example Workflow Template Steps

Step 1	Acceptable Use Policy.
Step 2	Split in the workflow to provide a different sequence of enrollment steps for Visitors and Employees. Splits can be modified for other industries (for example, Students, Faculty, and Guests).
Step 3	An authentication step for users.

TABLE 2 Example Workflow Template Steps (continued)

Result	The final step, which migrates the user to the secure network and assigns a client certificate, is not pre-populated as this information is specific to your network.

Creating a Workflow From a Blank Slate

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

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

2. On the right hand side of the **Workflow** page, click **Add Workflow**, then, with the "Create a new Workflow" button selected, click **Next**.

   The Create Workflow screen is displayed:

   FIGURE 37 Create Workflow Screen - Selecting "None" For Workflow Template Type

3. On the **Create Workflow** screen, enter a **Display Name** and **Description**.

4. From the Workflow Template Type drop-down list, select "None."

5. Fill out the URL Name field.

6. Click **Save**, and you are returned to a blank workflow page.

7. On the blank workflow page, click **Get Started** near the bottom of the page to add your first workflow step.

A selection page opens that allows you to choose which type of step (workflow plug-in) to add to the enrollment workflow. Every time you add a step, the **Step Selection** page appears.

FIGURE 38 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 39 Add Acceptable Use Policy

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

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

User Type Split

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

To create a **User Type** prompt:

1. **Insert** a step above the **Result**: step in the enrollment workflow.

2. Select **Split users into different processes**.

3. Select **Use an existing split** and choose **User Type** (a pre-existing split). The **User Type** split creates a prompt to select either the **Employee** User Type or the **Visitor** User Type. These labels can be modified.

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

    FIGURE 40 Workflow with User Type Split
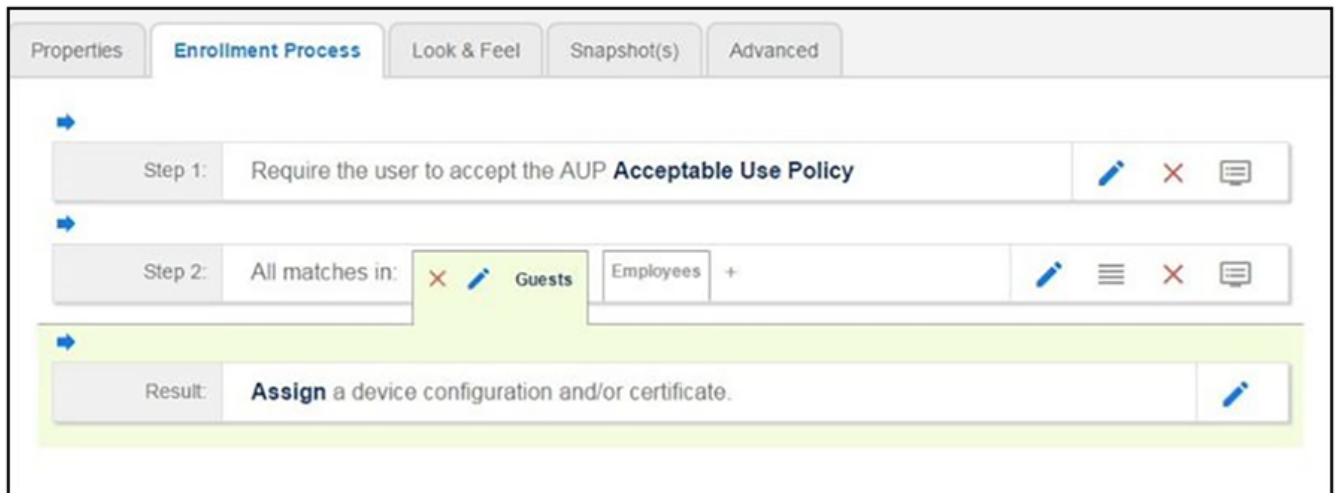
Authentication to a Traditional Authentication Server

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

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

1. Select the **Employee** tab in Step 2 of the example enrollment workflow.

2. **Insert** a step above the **Result**: step in the enrollment workflow.

3. Select **Authenticate to a traditional authentication server**.

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

   FIGURE 41 Add Authentication Server

5. Enter the **Reference** and **Active Directory Information** .

6. (Optional) To test connectivity to the authentication server, select the **Run Authentication Test** box, and enter a Test **Username** and **Password**.

7. (Optional) To allow users from a specific group to log in to the Cloudpath Admin UI as administrators, check the **Use for Login Admin** box and enter the **Admin Group Regex** for the authentication server group.

8. Click **Next**.

9. Select **Use a new webpage created from a standard template**.

   The **Create Credential Prompt** page opens.

Device Type Split

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

1. **Insert** a step above the **Result:** step in the enrollment workflow.

2. Select **Split users into different processes**.

3. Select **Use an existing split** and choose **Device Ownership**. The **Device Ownership** option prompts the user to select either **Your Device** or **Company Device**. These labels can be modified.

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

    FIGURE 42 Workflow with Device Ownership Split
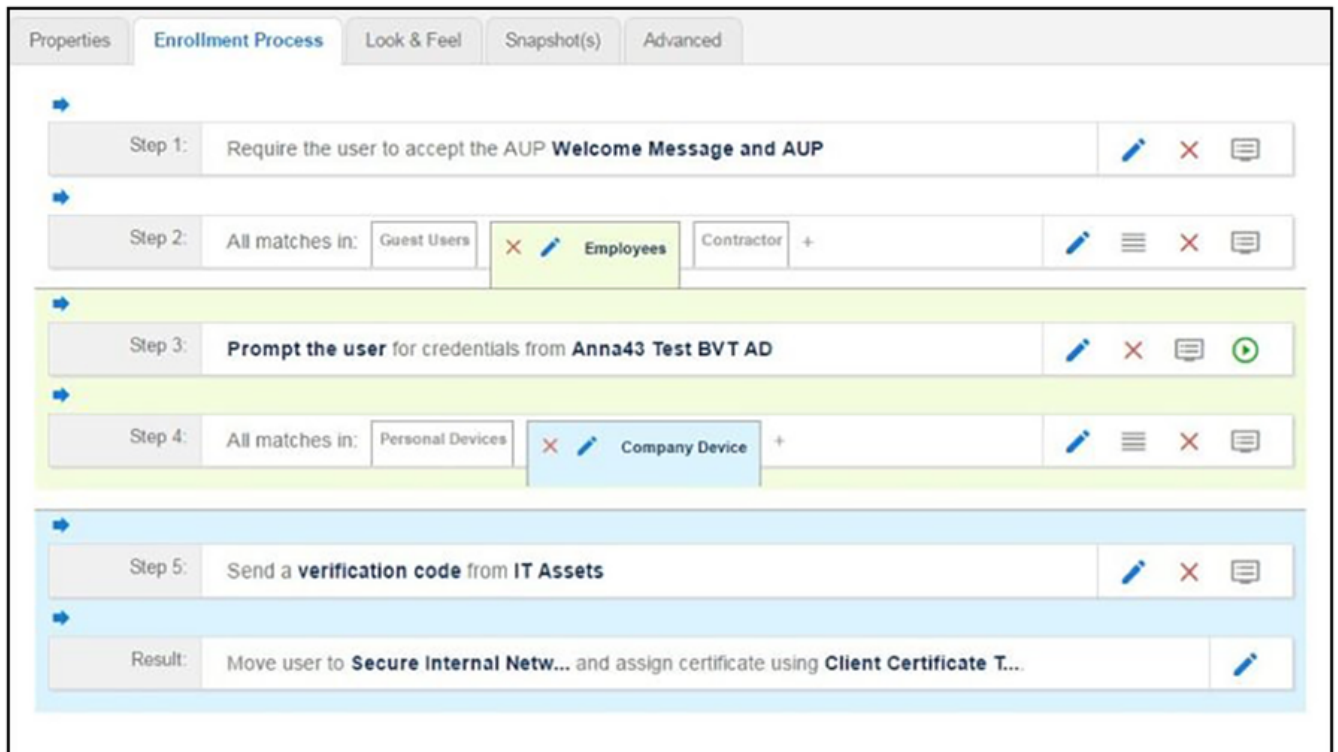
Create a Filter in the Device Type Split

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

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

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

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

    FIGURE 43 Modify Step - Filters and Restrictions

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

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

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

Prompt for Voucher

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

1. Select the **Employees** tab in Step 2 and the **Company Device** tab in Step 4 of the workflow.

2. **Insert** a step above the **Result:** step in the enrollment workflow.

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

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

FIGURE 44 Create Voucher List - Format and Notification Fields

4. On the **Create Voucher List** page, enter the voucher specifications for the Employees with Company Devices workflow.

    - **Format** - Describes voucher characteristics and validity.
    - **Notification** - Set up the template for emailing the voucher or sending as an SMS message.
    - **Sponsorship** - Use this section to configure the Sponsored Guest Access feature.
    - **Initial vouchers** - Create one or more initial vouchers.

    FIGURE 45 Create Voucher List - Sponsorship, Fields Displayed, and Initial Vouchers

5. For the voucher prompt, select **Create a new webpage from a standard template**.

6. On the **Create Voucher Prompt** page, enter the data for the voucher prompt and **Save**.

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

Device Configuration and Client Certificate

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

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

Device Configuration

1. On the right side of the **Result** step, click the **Edit** icon.

2. Select **A new device configuration**.

3. On the **Add Device Configuration** page, provide a name and optional description for the device configuration, then click **Next**.

4. Select **Wireless Connections** (the default) and enter the SSID of the secure wireless network.

   FIGURE 46 Configure SSID

5. Set the **Authentication Style**:

   - Select **Client Certificate** for TLS network configurations

   - Select **PEAP** for PEAP/MS-CHAPv2 network configurations

   - Select **Static Pre-Shared Key** for PSK network configurations

   - Select **Ruckus DPSK** for a Dynamic Pre-Shared Key network configuration on a Ruckus controller

6. For **Authentication Style**, use the default of "WPA2-Enterprise".

7. For **Encryption**, "AES" is the only option for the "WPA2-Enterprise" authentication style.

8. Leave the default **Broadcast** setting and click **Next**.

9. Specify **Conflicting SSIDs**.

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

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

10. Select the operating system families and versions that to support within this device configuration.

    You can restrict a particular version or service pack level after the device configuration is created.

    FIGURE 47 Select OS Versions
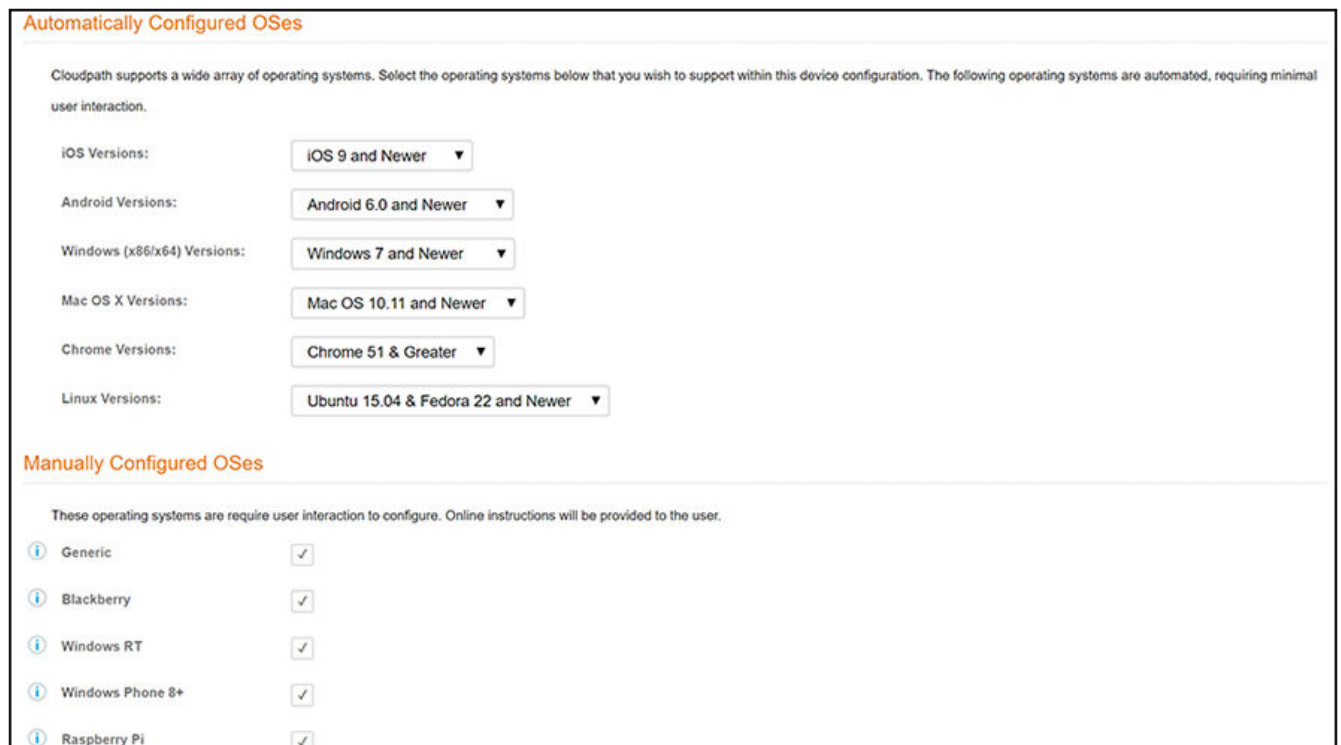
11. Select **Client will authenticate to the onboard RADIUS server**.

12. Configure additional settings for the device configuration.

13. On the screen called "What certificate template should issue the certificate?":

    - If you select **Do not issue a certificate to the user** and click **Next**, the configuration completes.

    - If you select **A new certificate template** and click **Next**, follow the instructions in the Client Certificates on page 79 to select the client certificate template with the appropriate user policy.
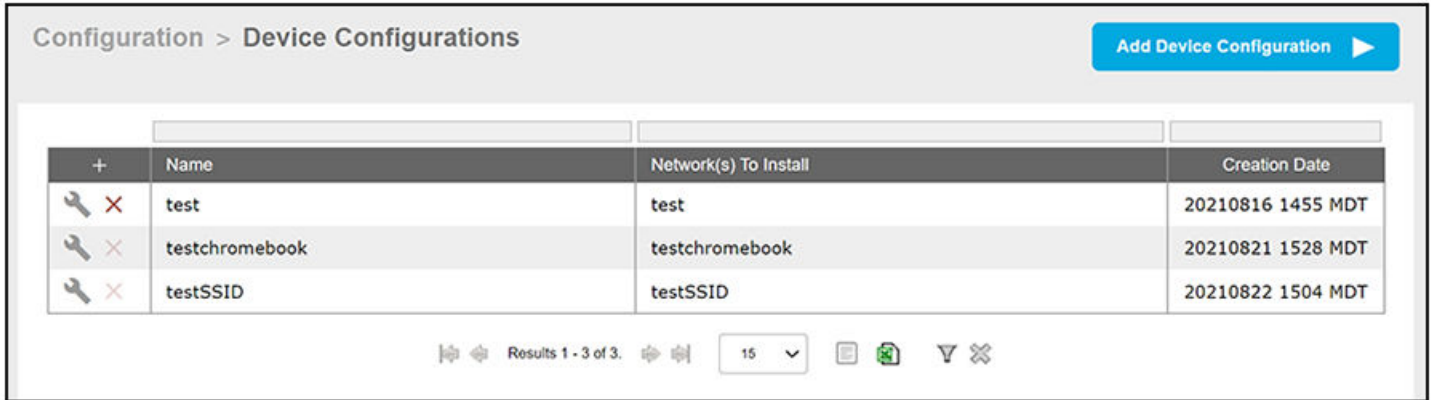
To make changes to a completed device configuration, as well as to view a list of additional settings, you can go to **Configuration > Device Configurations**.

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

FIGURE 48 Device Configurations Page Example
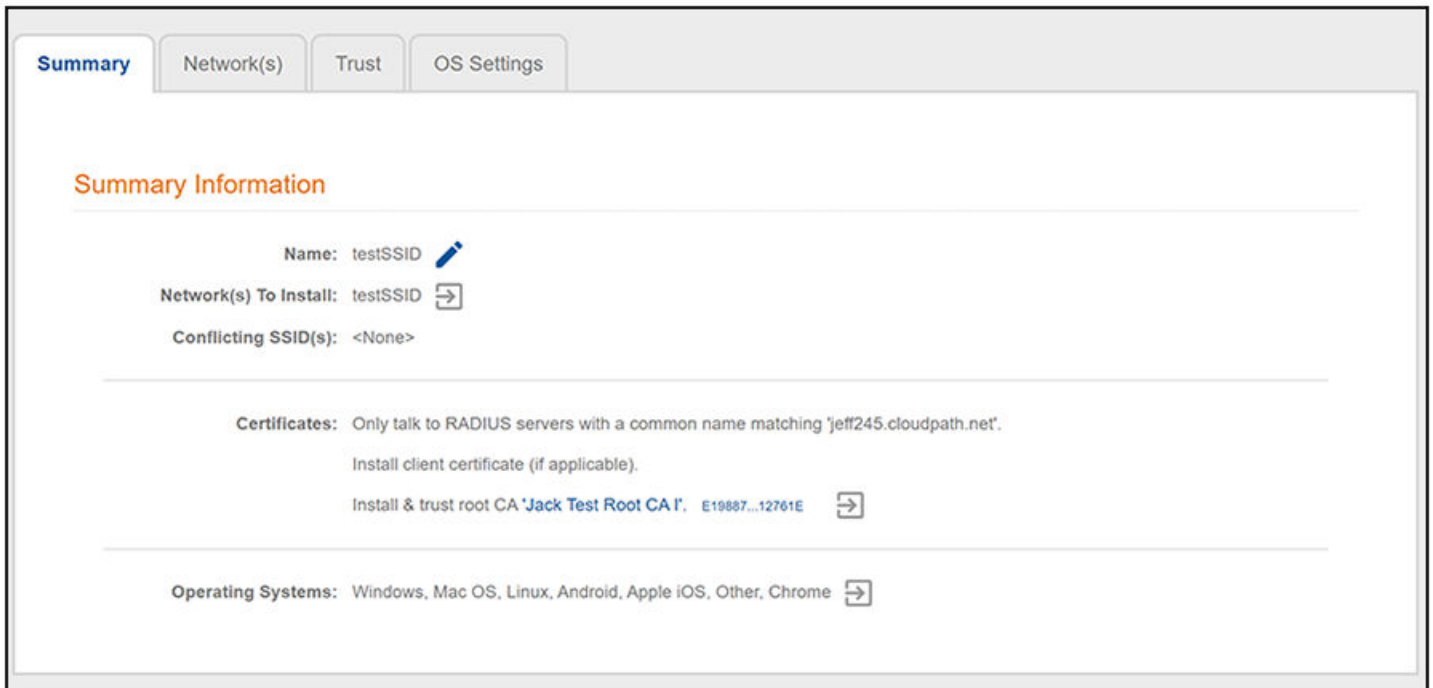
If you click the wrench icon, you are presented with the tabs view of the corresponding device configuration, from which you can view and make any desired changes.

FIGURE 49 Device Configuration Tabs View

Client Certificates

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

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

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

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

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

   FIGURE 50 Client Certificate Template

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

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

6. Grant access for the appropriate amount of time.

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

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

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

    Additional certificate notifications can be configured after the template is created.

8. Optional. Enter **RADIUS Options** to assign a VLAN ID or Filter ID to certificates that use this template. These settings only applies if you are using the Cloudpath onboard RADIUS server.

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

FIGURE 51 Completed Workflow
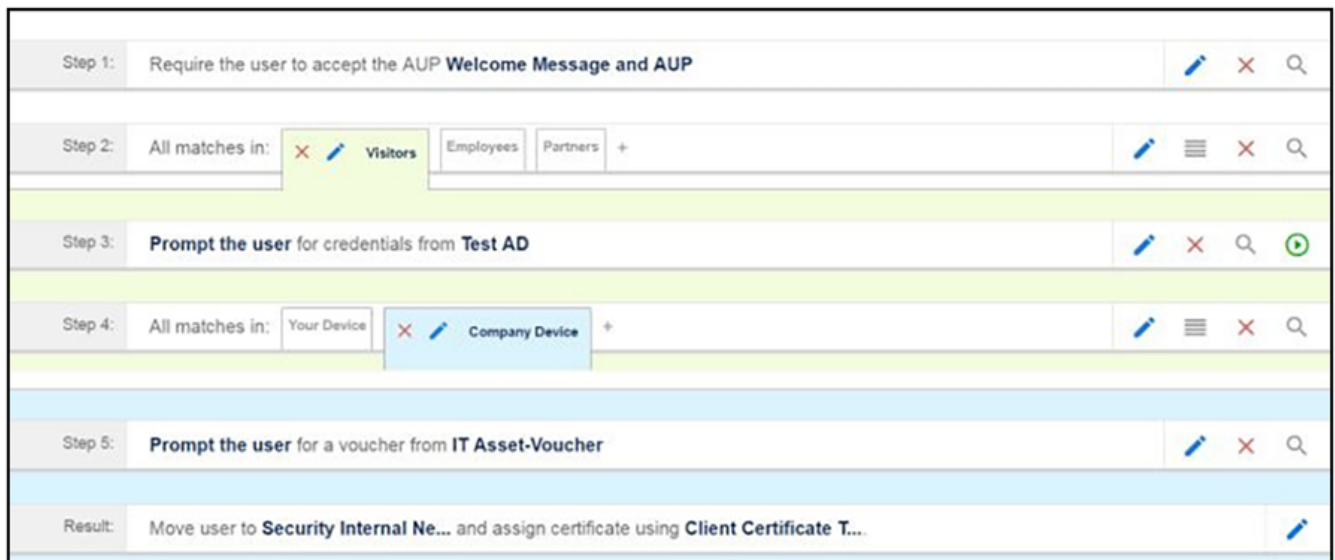
After you have finished configuring a enrollment workflow, create and deploy a snapshot of the workflow configuration to test before deploying to users.

Using the Timed Access Workflow Template

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

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

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

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

2. On the right hand side of the **Workflow** page, click **Add Workflow**, then, with the "Create a new Workflow" button selected, click **Next**.

    The Create Workflow screen is displayed:

    FIGURE 52 Create Workflow Screen - Selecting "Timed Access" For Workflow Template Type

3. On the **Create Workflow** screen, enter a **Display Name** and **Description**.

4. From the Workflow Template Type drop-down list, select "Timed Access."

5. Fill out the URL Name field.

6. Click **Save**, and you are returned to the workflow page that is shown in the following figure.

    FIGURE 53 Timed Access Workflow After Initial Creation

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

FIGURE 54 Timed Access Workflow Fully Expanded
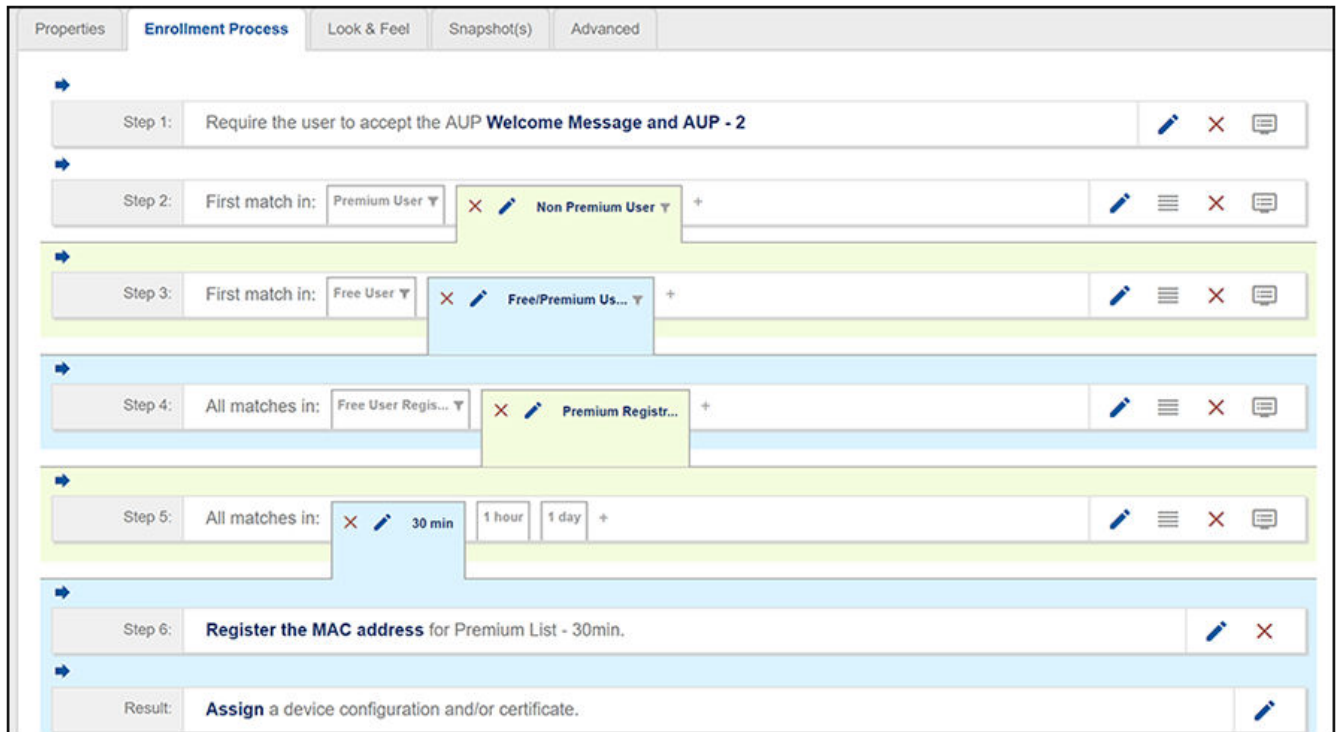
The following MAC registration lists are automatically created by this workflow template, and can be viewed in the **Configuration > MAC Registrations** portion of the UI:

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

Free User Registration

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

Workflow Logic:

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

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

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

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

TABLE 3 Description of Steps in Timed Access Workflow Template

Step 1	Acceptable Use Policy.
Step 2	First match in: • Premium User: An enrollment whose MAC address is already registered in one of the three premium lists is taken down this branch. This branch is never available to a first-time enrollment in a 24-hour period. If this option is a match, the enrollment then goes directly to the device configuration (Result step). • Non Premium User: Any enrollment that does not match the "Premium User" criteria is taken down this branch. A first-time enrollment in a new 24-hour period is taken down this branch.
Step 3	First match in: • Free User: An enrollment whose MAC address is already registered in the Free List (and has not yet expired) is taken down this branch. If this option is a match, the enrollment then goes directly to the device configuration (Result step). • Free/Premium User: Any enrollment that does not match the "Free User" criteria is taken down this branch.
Step 4	All matches in: • Free User Registration: Presented if the MAC address is *not* currently in the Free List, nor is the MAC address marked as "expired" or "revoked" in the Free List. If this branch is chosen, the MAC address is registered to the Free List and the enrollment is assigned a device configuration (Result step). • Premium Registration: Available to all enrollments A first-time enrollment (for a new 24-hour period) will either be presented with both options or will be taken down the Premium Registration branch.
Step 5	All matches in: • 30 min: Available to all enrollments • 1 hour: Available to all enrollments • 1 day: Available to all enrollments These options are presented to all enrollments who have gone down the Premium Registration branch. The user makes a selection, and the enrollment proceeds with the MAC address getting registered.
Step 6	Register the MAC address: The MAC address is registered in the selected premium MAC Registration list.

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

Publishing the Enrollment Workflow

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

To publish the workflow:

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

2.   Click the wrench icon of the workflow you wish to publish; for example "production23" in

The following screen is displayed:

FIGURE 55 Publish Icon Under "Publish" Column

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

   The following screen is displayed:

   FIGURE 56 Create New Snapshot
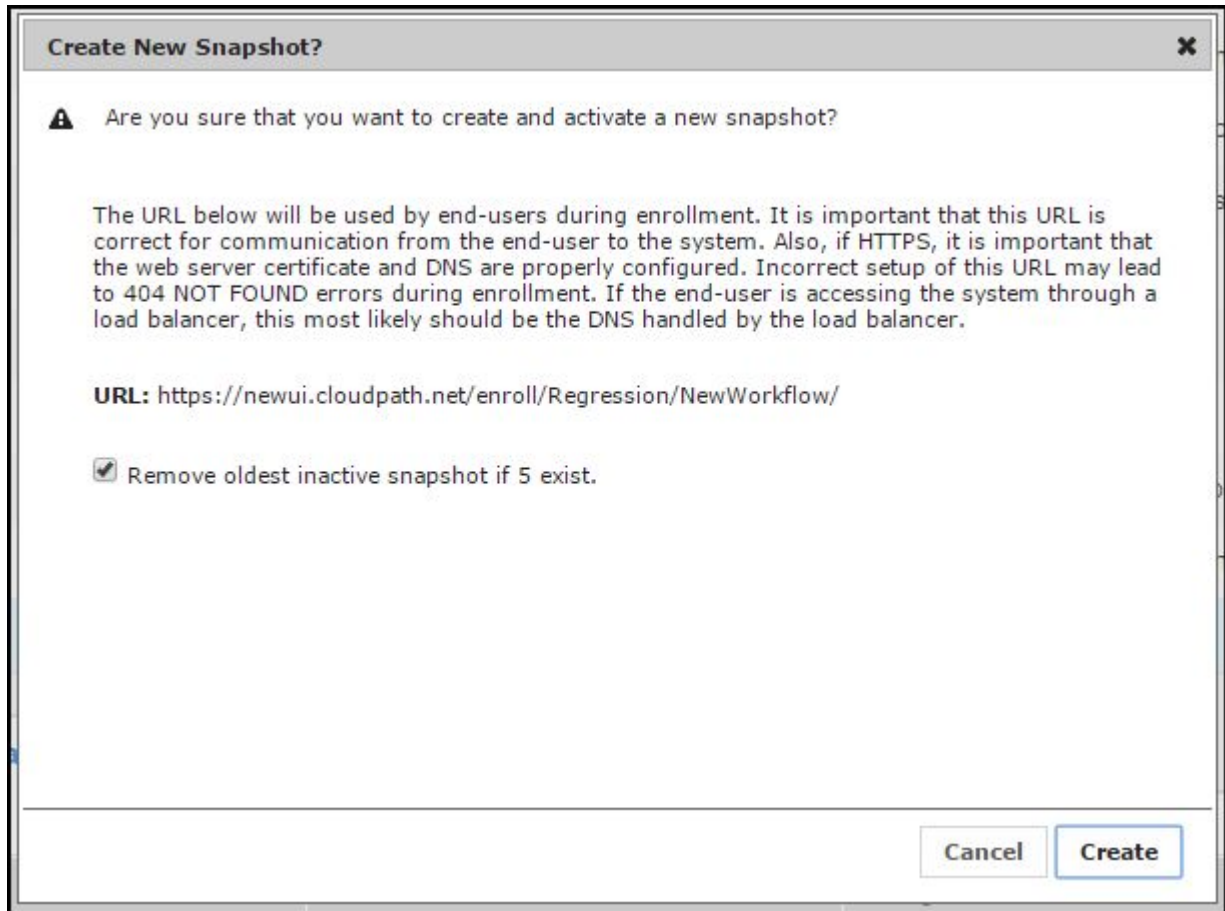
4. Select the Wizard version to use for the new snapshot. The **Cloudpath Wizard** is the application provided to users to automate the enrollment process.

5. Verify the Enrollment Portal URL for the snapshot.

6. Click **Create**.

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

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

FIGURE 57 Workflow Grid View Showing That All Workflows Have Been Published

How to Test a Published Workflow

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

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

2. On the workflow list, select the workflow to test.

3. Click the Enrollment Portal URL. Be sure that the snapshot you want to test is the **active** snapshot (green icon).

Cloning a Workflow

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

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

1. In the UI, go to **Configuration > Workflows** to display your current workflows. Suppose you want to clone the workflow called "Production_23" shown in the

2. Click **Add Workflow**.

3. On the ensuing screen, do the following:

   a. Select the "Clone an existing Workflow" button (see screen below).

   b. In the Clone Name field, enter the name you want for the cloned workflow. The name you provide will be pre-pended with an underscore to the name of the selected existing workflow.

   c. From the Existing Workflow drop-down, select the workflow you want to clone.

FIGURE 58 Selecting the Workflow to Clone
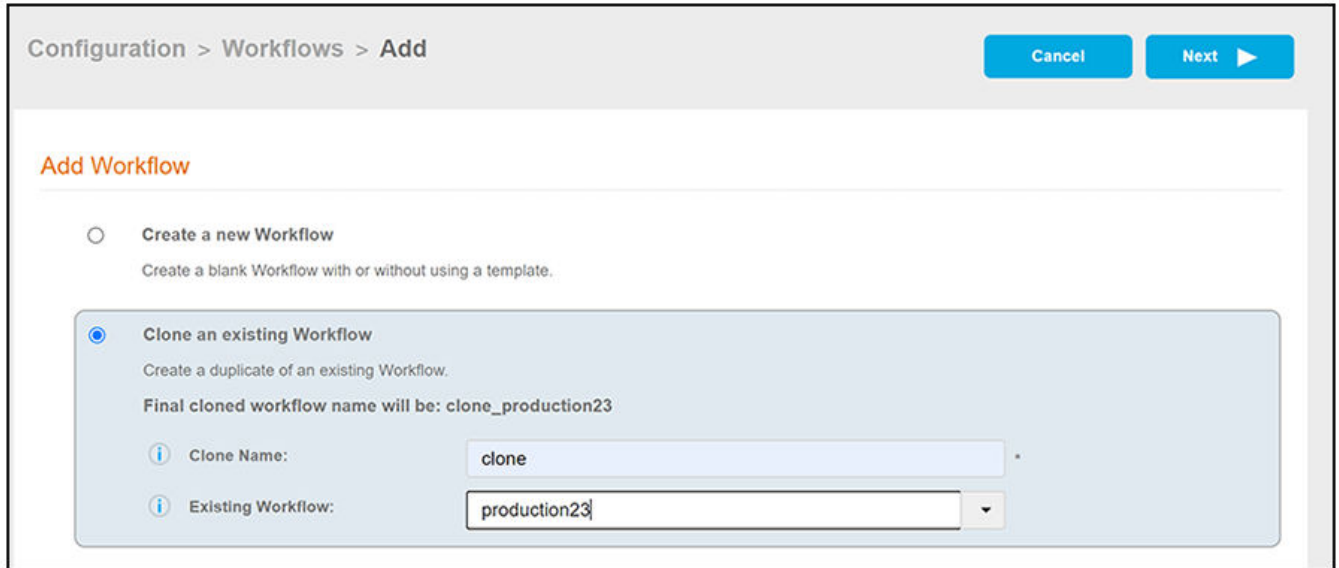
4. Click **Next**.

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

FIGURE 59 Cloned Workflow Added to Top of Workflow List
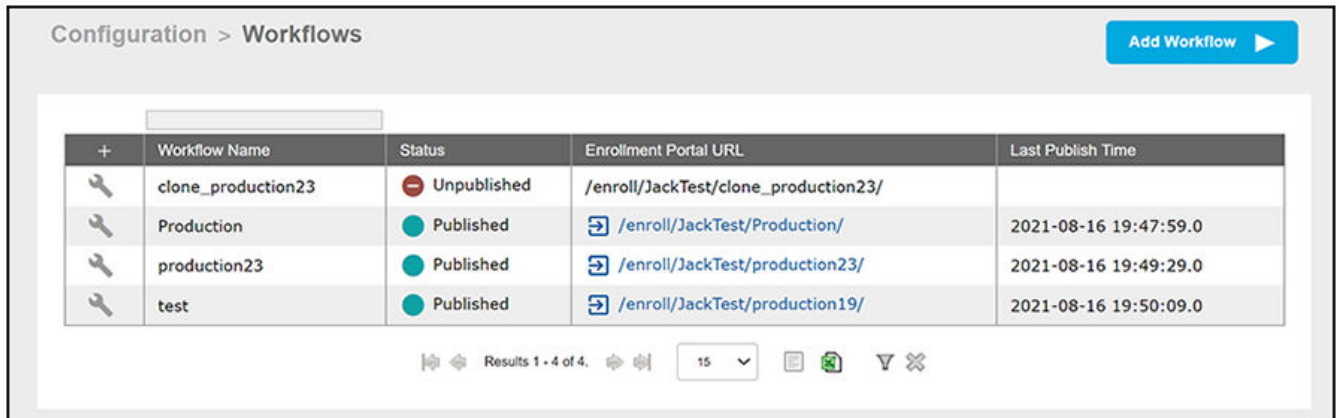
Basic behavior of cloning:

*   A cloned workflow appears in the list of workflows.

*   A cloned workflow is an identical copy of the workflow from which it was cloned.

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

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

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

- Editing a cloned workflow has no impact on the workflow from which it was cloned.

- You can also make a clone of a clone.

- A cloned workflow is not automatically published, but it can be published at any time.

Auto VLAN

Using Auto VLAN

You can use the Auto VLAN feature to assign available VLAN IDs from a configured range of VLANs to users during their enrollment.

The range of VLANs that you configure creates a VLAN pool in the database. Each customer account can have one VLAN pool. Once the pool has been created, you can increase its size by expanding its range. However, if you shrink the size of the pool, existing users who have a VLAN that is outside the new range will maintain that VLAN until the next time they enroll, at which time they are assigned a new VLAN.

There are three main steps to setting up the Auto VLAN feature:

- Assign the ${VLAN_POOL_ASSIGNMENT} variable: Using this variable allows the RADIUS server to select the VLAN port assigned to an authenticated user.

    - Assign the variable for a RADIUS attribute group.
    - Add the RADIUS attribute to a policy.
    - Assign the policy to the desired area of Cloudpath. For example, policies can be assigned to DPSK pools, PEAP that uses onboard RADIUS, and certificate templates.

        NOTE
        For detailed information about configuring RADIUS attribute groups and using policies, refer to the manuals for each of these categories.

        NOTE
        To use this feature with MAC Registrations, refer to Using Auto VLAN With MAC Registration.

- Enable the feature for your authentication server in the **Configuration > Authentication Servers** portion of the UI

- Define the VLAN Range and the default VLAN in the **Administration > System Services** portion of the UI.

Configuration Steps for Adding the ${VLAN_POOL_ASSIGNMENT} Variable

1. Go to **Configuration > Policies**.

    a. Click the RADIUS Attribute Groups tab.

    b. Either click **Add RADIUS Attribute Group** or click the pencil icon to edit an existing RADIUS attribute group.

    c. In the VLAN ID field, enter the variable: ${VLAN_POOL_ASSIGNMENT} thereby allowing the RADIUS server to select the VLAN port that gets assigned to an authenticated user.

FIGURE 60 Using the ${VLAN_POOL_ASSIGNMENT} Variable in a RADIUS Attribute Configuration

d. Click **Save**.

e. In the Policies tab, either click Add Policy or click the pencil icon to edit an existing policy.

f. In the "RADIUS Attribute Dropdown" list of the Policy configuration screen, select the attribute group that you have configured with the ${VLAN_POOL_ASSIGNMENT} Variable.

g. Click **Save**. The "Attributes" column in the ensuing screen should now indicate that the variable is being used.

FIGURE 61 Policy View Shows the ${VLAN_POOL_ASSIGNMENT} Variable
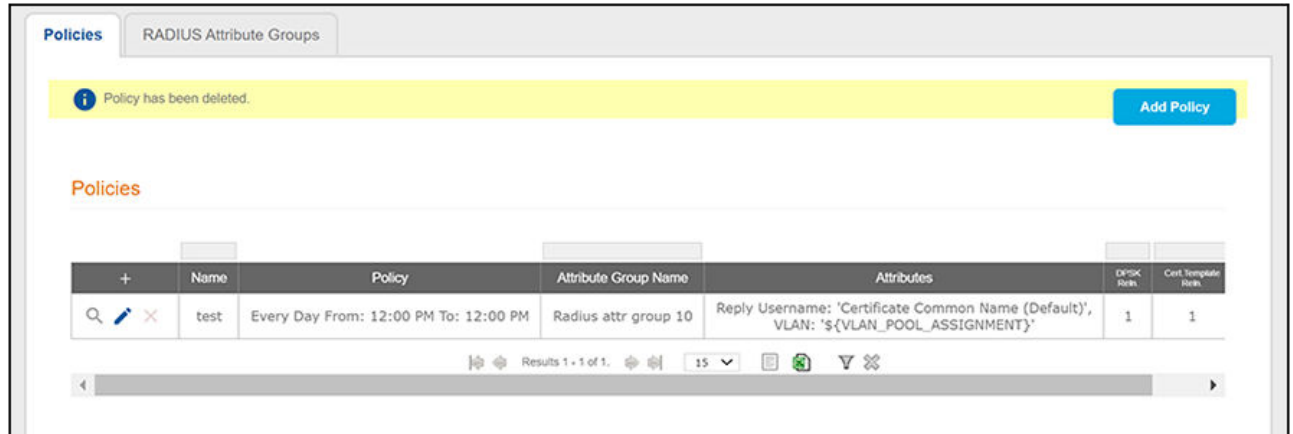
h.   Assign the policy to the desired usage; for example:

  ● DPSK Pool: **Configuration > DPSK Pools >** wrench icon > **DPSK Policies** tab

  ● Certificate template: **Certificate Authority > Manage Templates** > wrench icon > **RADIUS Policies** tab

  ● PEAP: **Configuration > RADIUS Server >PEAP** tab.

  ●

2.   For each traditional authentication server that you want to support this feature, you must enable the "Use VLAN Range" check box:

a.   Go to **Configuration > Authentication Servers**.

b.   Whether you are adding a new authentication server or need to edit the configuration of an existing authentication server, go to its configuration, as shown in the example figure below for an Active Directory authentication server.

c.   Enable the "Use VLAN Range" checkbox, as shown in the figure below. (Note that it is not enabled by default.)

FIGURE 62 Enabling Checkbox to Use VLAN Range on Active Directory Authentication Server

> **NOTE**
> Without this check box enabled, a VLAN will not be assigned to a user, and any currently assigned VLANs will be removed from users if they re-enroll by means of an authentication server where this box is not checked.

    d.   Click **Save**.

3.   Go to **Administration > System Services**:

FIGURE 63 System Services Page
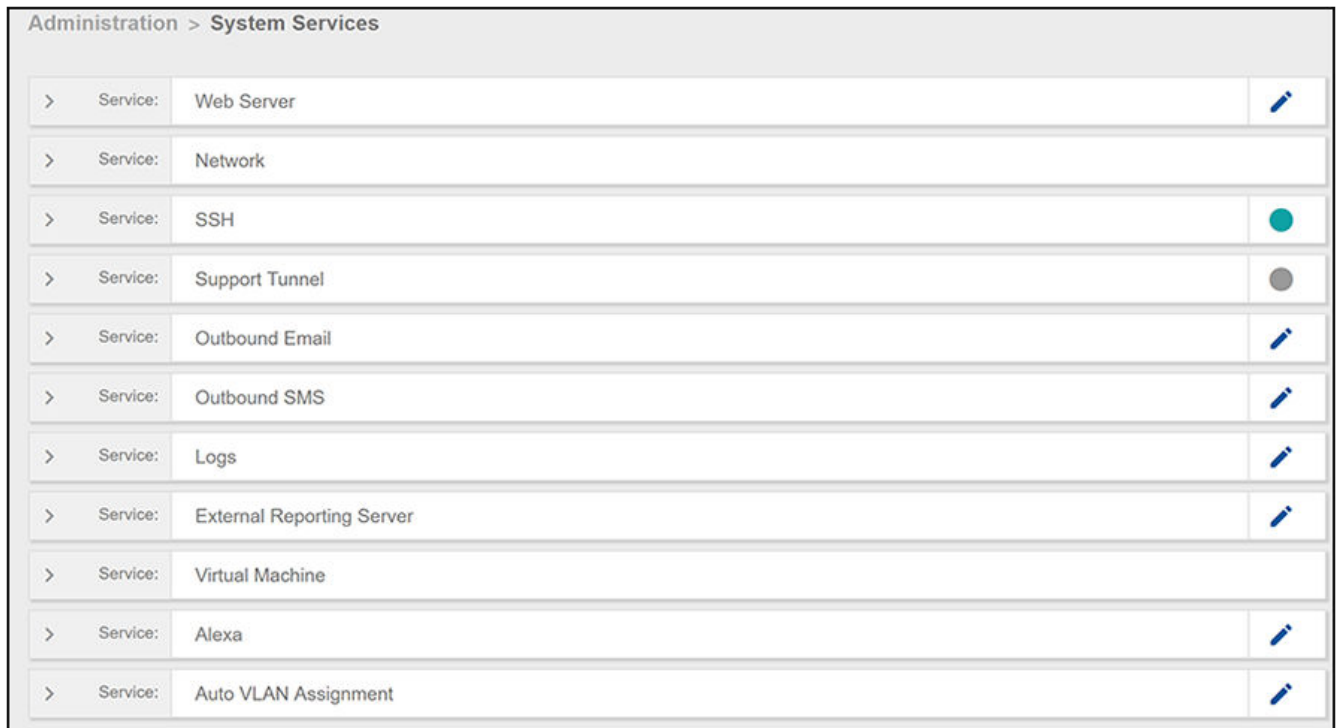
a.   Scroll down and click the pencil icon to the right of the "Auto VLAN Assignment" service.

b.   Set the values as desired in the VLAN Assignment window; an example is shown below:

   FIGURE 64 VLAN Assignment Window in System Services
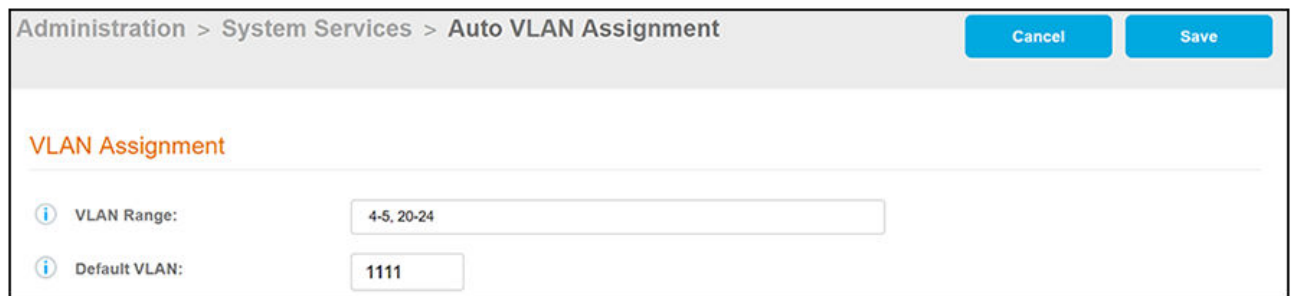
●   VLAN Range: Range to use for automatic VLAN assignment. A single user is assigned the same VLAN for all devices. Any changes to the range will affect future enrollments only.

   Example of how to specify a range in a valid format: 1-142, 532, 1000-1235

●   Default VLAN: The VLAN to use once all other VLANs defined in the pool have been assigned to other users.

c.   Click **Save**.

   The following figure shows the Auto VLAN Assignment service expanded after the VLAN assignments have been saved:

FIGURE 65 Auto VLAN Assignment Information
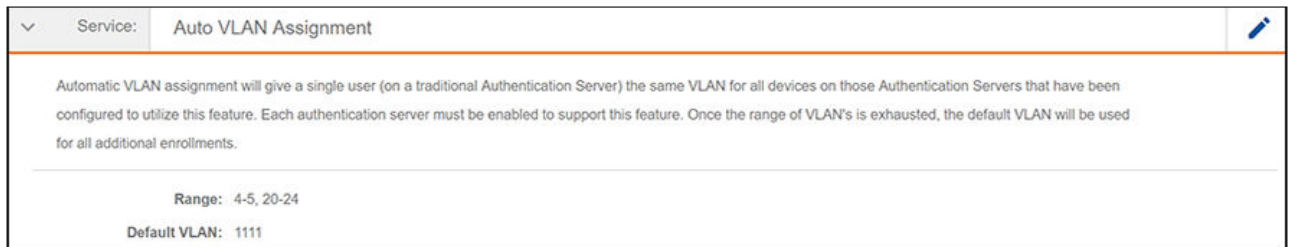
How the VLAN ID Gets Assigned During Enrollment

As an enrollment is made that uses a traditional authentication server (as specified when you create your workflow), an identity is either created or retrieved from the database. If the identity is on an authentication server with the "Use VLAN Range" checkbox enabled, a VLAN is selected (lowest available number), and the identity is assigned to this VLAN. This VLAN is shown in the User Information section of the **Dashboard > Users & Devices** page. For example, if the configured the VLAN ranges are 4-5 and 20-24, as shown in the figure above, the first user who enrolls would be assigned a VLAN ID of 4 because 4 would be the lowest available number (see the "VLan Assignment" field in the figure below):

FIGURE 66 Dashboard: Users & Devices Information Shows VLan Assignment

> **NOTE**
> All devices registered to the same user/identity are assigned the same VLAN ID.

If an authentication server has *not* been enabled to support the VLAN behavior, then any existing VLAN assignments are removed from the user during enrollment, and that VLAN ID then is released back into the VLAN pool for use by an authentication server that *does* support the VLAN behavior.

Viewing All VLAN Assignment Information

In the UI, navigate to **Dashboards > VLAN Assignments** for complete information about VLANs available, assigned, users for each VLAN, and so on.

Using Auto VLAN With MAC Registration

In addition to using Auto VLAN with RADIUS attribute groups (and therefore within policies), you can also use this feature with MAC registrations. From the UI, go to: **Configuration > MAC Registrations > Add MAC Registration**, "Authentication Attributes" section; add the following three Success Reply Attributes:

- Tunnel-Private-Group-Id (string) - Set this attribute to the variable ${VLAN_POOL_ASSIGNMENT}

- Tunnel-Type (integer) - Set this value appropriately for your system.

- Tunnel-Medium-Type (integer) - Set this value appropriately for your system.

Additional Plug-In Examples

Charge User for Service

You can build a step into a workflow that directs a user to pay for a service by using a third-party payment system such as PayPal. At this time, PayPal is the only service for which this step can be used.

The sole function of this plugin, called "Charge user for service," is to charge the user for a service, but you must build other steps in your workflow to define the service being provided. If a user is to be limited to a certain amount of times to use a service, such as being granted internet access, you must make sure that the correct timeouts on a corresponding MAC Registration step or Certificate-assignment step are set. Examples are provided later in this section.

To make this workflow step work properly, you need to do the following:

1. Add necessary entries to the walled garden on your controller.

2. Create an application using the PayPal developer's site.

3. Configure the workflow step in Cloudpath to communicate with your PayPal application.

Required Walled Garden Sites for Access

You need to add the following entries to the WISPr/captive portal walled garden for the enrollment to work correctly:

- www.sandbox.paypal.com

- www.paypal.com

- *.paypal.com

For information on setting up the walled garden, refer to #unique_92.

What You Need to Do on the PayPal Developer's Site

Follow these basic steps:

1. Create a business account on the PayPal developer's web site.

2. Refer to the available PayPal developer's documentation on how to create the application you desire for Cloudpath.

3. Give the application a meaningful name so that you know it's intended to communicate with Cloudpath. The following figure shows an example application on the PayPal developer's "Sandbox" (test) location:

FIGURE 67 PayPal Developer's Page
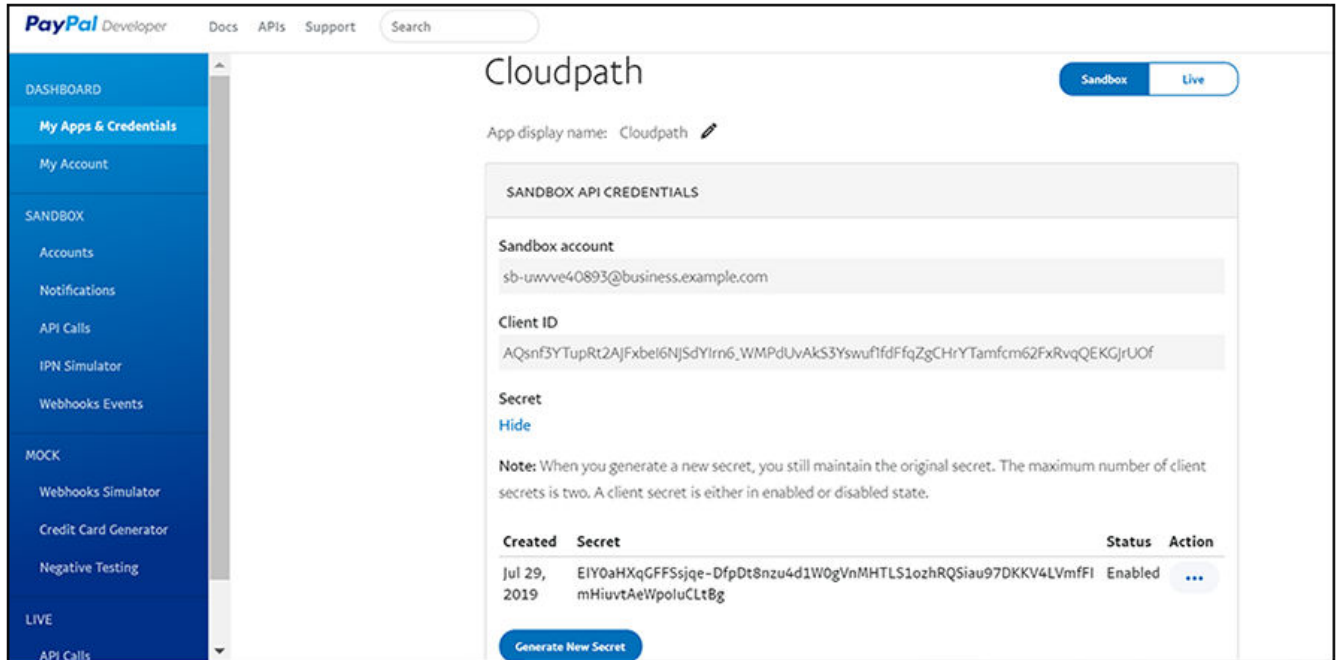
NOTE
The example figure above contains information that you will need when you configure the workflow step in Cloudpath. The Client ID and Secret are the key elements of this application because they will need to be copied and pasted into the Cloudpath configuration, described later. *Note that if you change those values in the PayPal application, they will need to be changed in exactly the same way in Cloudpath, or the plug-in will fail.*

Adding the Corresponding "Charge for Service" Workflow Step in Cloudpath

To add and configure the charge-for-service step in Cloudpath, follow these steps:

1. In your workflow, click the " Insert Step Here" right-pointing arrow at the desired location to invoke the "Which Type of Step Should Be Added" screen (refer to Figure 38 on page 68).

2. Scroll down and click the "Charge user for service" button:

3. The "Which pay application configuration do you want to use?" screen appears. If a pay application configuration already exists, the screen appears as shown below:

FIGURE 68 Inserting Pay Application Configuration Step

4.   For purposes of this example, select "A new pay application configuration," then click **Next** to invoke the Configure a Pay Application page.

5.   Configure the Pay Application page:

FIGURE 69 Cloudpath UI Pay Application Configuration Screen

- Display name: Name of the step as you want it to appear in the workflow. This name is visible only to Cloudpath administrators.

- Description (optional): Wording that you want the user to see when they are presented with the third-party service charge screen. (This description, if entered, will appear under the Ruckus logo shown in Figure 71.)

- Environment: Choose between "Test (Sandbox)" and "Production (Live)."

- Application ID: This ID is automatically assigned to your application by PayPal. In PayPal, however, it is called "Client ID," as shown in Figure 67. Copy the Client ID from the PayPal Developer's page and paste it directly into the Application ID field in the Cloudpath UI Pay Application Configuration Screen.

- Secret: This secret is automatically assigned to your application by PayPal. Copy the Secret from the PayPal Developer's page and paste it directly into the Secret field in the Cloudpath UI Pay Application Configuration Screen.

- Currency Type: From the drop-down list, select the currency type to use when the customer is billed.

- Amount: Enter the amount to be charged. You can use decimals for the appropriate currency. (Commas and other formatting are not permitted.)

Click **Save** when you are done configuring the values.

6. After you save the configuration in the previous step, you are returned to your workflow. Check that the PayPal step has been added, as shown in the following example:

FIGURE 70 Workflow After Adding PayPal "Charge User for Service" Step
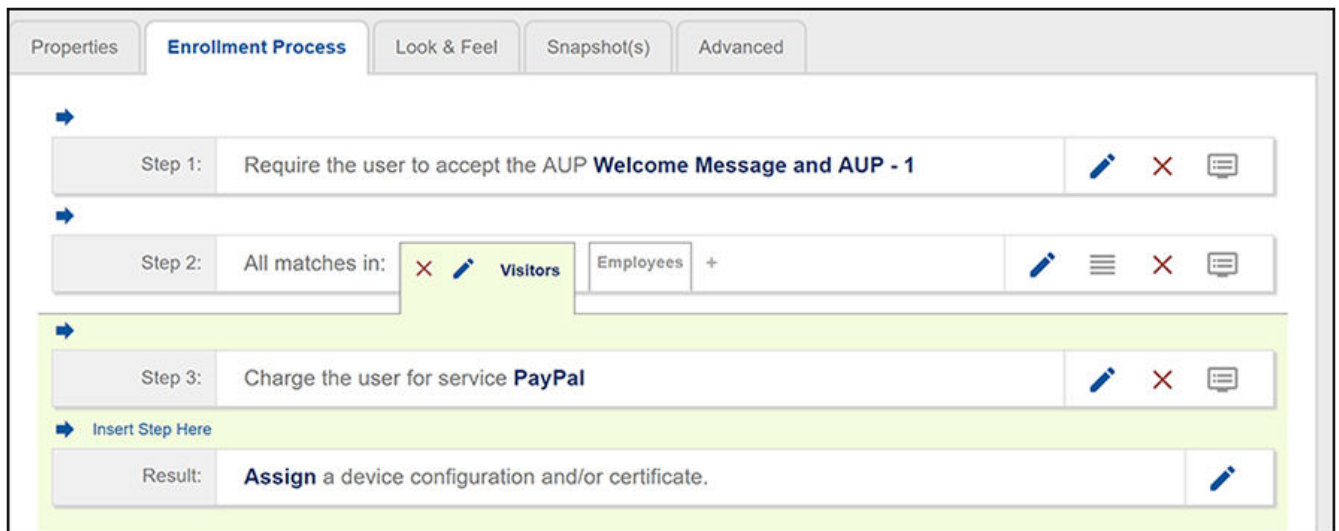
7. To the far right of the PayPal step, you can click the Preview icon to view how the user will be presented with this service-charge step:

FIGURE 71 Service Charge Screen Preview
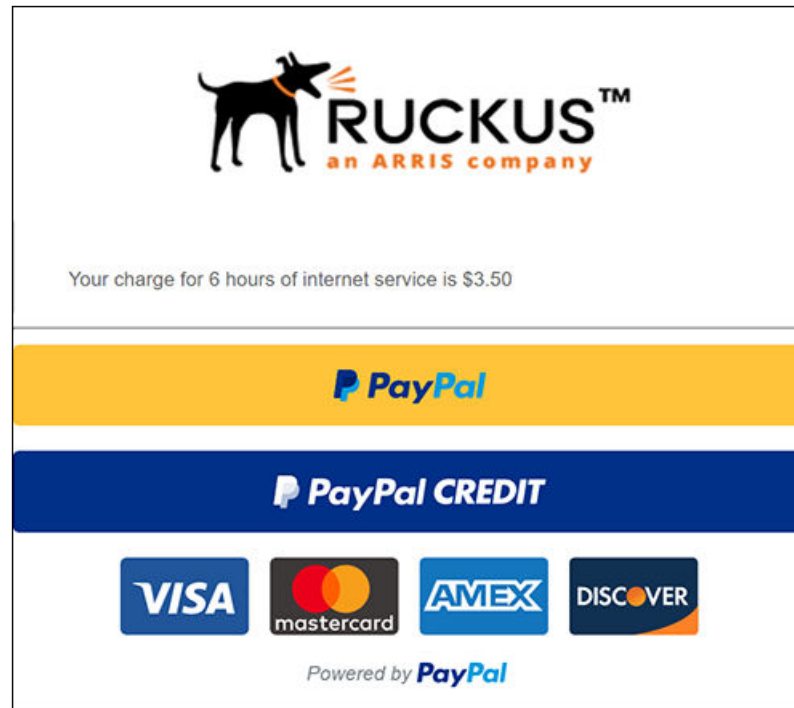
The user will then make a selection to proceed with their payment.

8. You can add additional steps as desired. You at least want to make sure that you add any other steps to support what the user is being charged for. In this example, the user is told there is a charge of $3.50 for six hours of internet use. Therefore, you want to be sure that the user's session ends after six hours. Methods for doing this include:

- Making sure to issue a certificate that expires after the desired amount of time. You can go to **Certificate Authority > Manage Templates**, click the pencil icon of the template you are using for onboarding in the workflow, scroll to the "Validity Period" section of the configuration screen for this template, and set the certificate to expire six hours after issuance, as shown below:

FIGURE 72 Expiration Date Setting for a Certificate
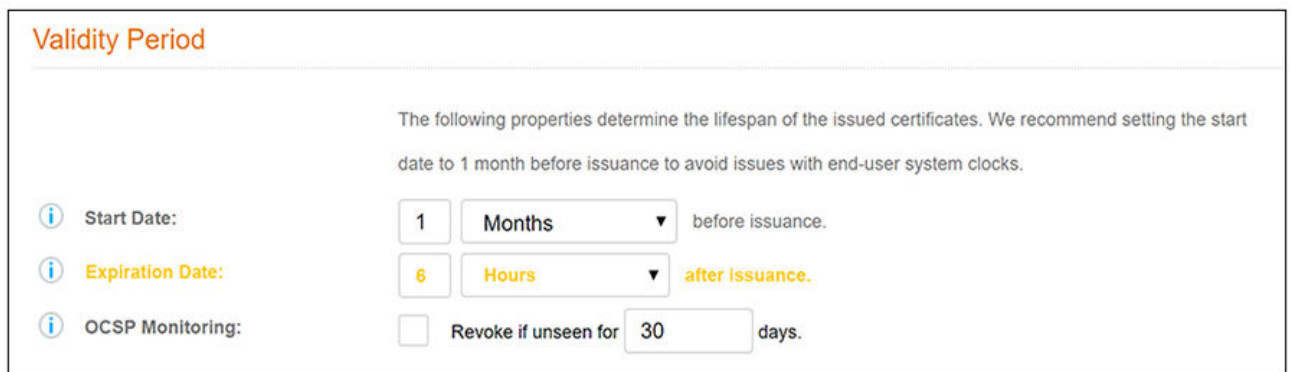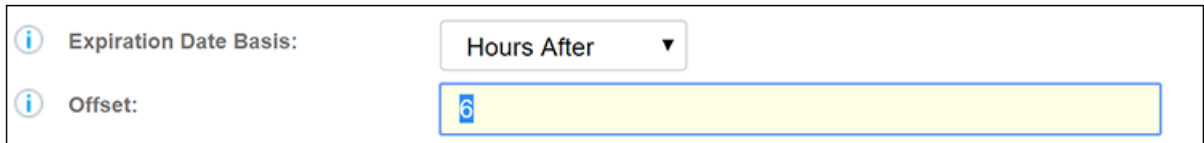
- Using a MAC Registration step in your workflow, and making sure that the expiration is set as desired. Go to **Configuration > MAC Registrations**. Click the pencil icon of the applicable MAC Registration, and in the "Registration Information" part of the screen, set the fields, as shown below:

FIGURE 73 Expiration Date Setting for a MAC Registration

You might be interested in using the "Charge for Service" plug-in with a Timed Access Workflow, described in the Using the Timed Access Workflow Template on page 81 section. At the end of that section, which shows a sample workflow that automatically creates and uses MAC Registration lists, you could place a "Charge for Service" plug-in between Steps 5 and 6 in the workflow shown in Figure 54 on page 83, and you could configure the timed MAC Reg lists to match the amount of time for which the user is being granted access.

NOTE
The Cloudpath environment for this plug-in is tied directly to the PayPal environment. Therefore, after you have tested your workflow and are ready to go "live," you need to obtain the Client ID and Secret from the live version of the application on the PayPal developer's site, then update the corresponding fields in the Cloudpath UI Pay Application Configuration Screen with those values, then publish the workflow again.

Request Access from a Sponsor Online

The "Request Access from a Sponsor Online" plug-in allows an enrolling user to request access from a sponsor while the user waits online for the sponsor's approval.

The figure below shows an example of a completed workflow that uses this plug-in:

NOTE
Prior to Release 5.5, this plug-in was called "Request Access for a User."

FIGURE 74 Sample Workflow That Uses the "Request Access from a Sponsor Online" Plug-in
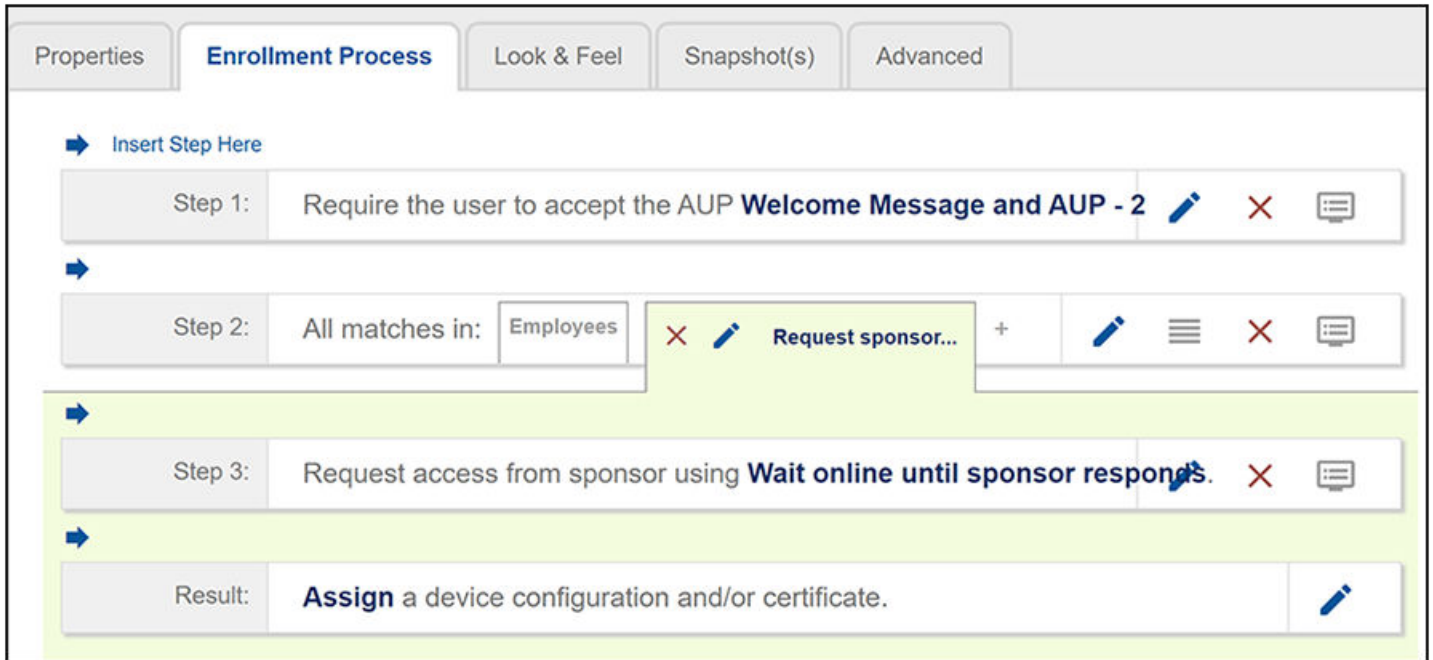
This information that follows instructs you how to configure this particular plug-in, and shows you how the interaction between user and sponsor can occur.

Configuring the "Request Access from a Sponsor Online" Plug-in

To use this plug-in, you would first want to create a tab such as the one shown above called "Request sponsor..." (full name could be "Request sponsor access while waiting online"). Then, follow these steps:

1. With the "Request sponsor..." tab highlighted, click the arrow below to insert a step into the workflow.

2. You will then create what is shown as Step 3 in the above workflow by scrolling down the list of available plug-ins and clicking the "Request access from a sponsor online" button.

3. On the ensuing page, select the button called "A new access request configuration," then click **Next**.

   NOTE
   If no existing access request configuration exists, you will be taken directly to the next step.

4. Configure the Create Access Request page:

FIGURE 75 Create Access Request Configuration Page for Sponsor Online

In the Default Sponsor Email field, enter the email address of the sponsor. The enrolling user's request for approval will be sent to this email address.

5. Set the other values as desired, then click **Save**. You can click the "i" icons to get information about the fields on the screen.

How the Enrollment Process Works for the "Request Access from a Sponsor Online" Plug-in

After your workflow is complete, you can publish the workflow, then test the enrollment process by clicking on the enrollment URL. The following example covers the basics of the online sponsor request:

1. After the enrolling user selects the branch for requesting access from a sponsor while the user remains online, the Request Network Access window is presented to the user. The user enters the requested information, as shown in the following example, then clicks **Send**.

FIGURE 76 User Completes Information for Online Request
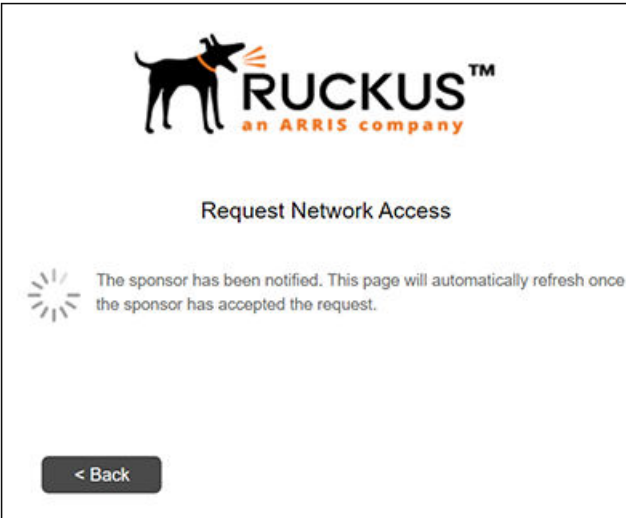
2. Once the user sends their information, the following occurs:

    - The user is presented with the following status screen, which will continue to display until the sponsor either rejects or approves the user's request for network access:

    FIGURE 77 Status Presented to User While Waiting Online for Sponsor's Response

    - The sponsor receives a notification about the user's request for access, such as the following email:

FIGURE 78 Email Sent to Sponsor for an Online Request for Network Access

Wi-Fi access has been requested by Bob.
Name: Bob
Company: Commscope
Reason: test

Review

3.   It is now up to the sponsor to take action. The sponsor must click "Review" in the notification. The sponsor is then presented with a screen where the request can either be rejected or approved:

FIGURE 79 Review Access Request Page for Sponsor

Review Access Request   Reject   Approve

The access request was submitted with the following information:

Status: Awaiting approval.
Name: Bob
Company: Commscope
Email:
User's Reason: test
Access Days (Approval Only):   30

Reason

Reason For Admins:

Reason For User:
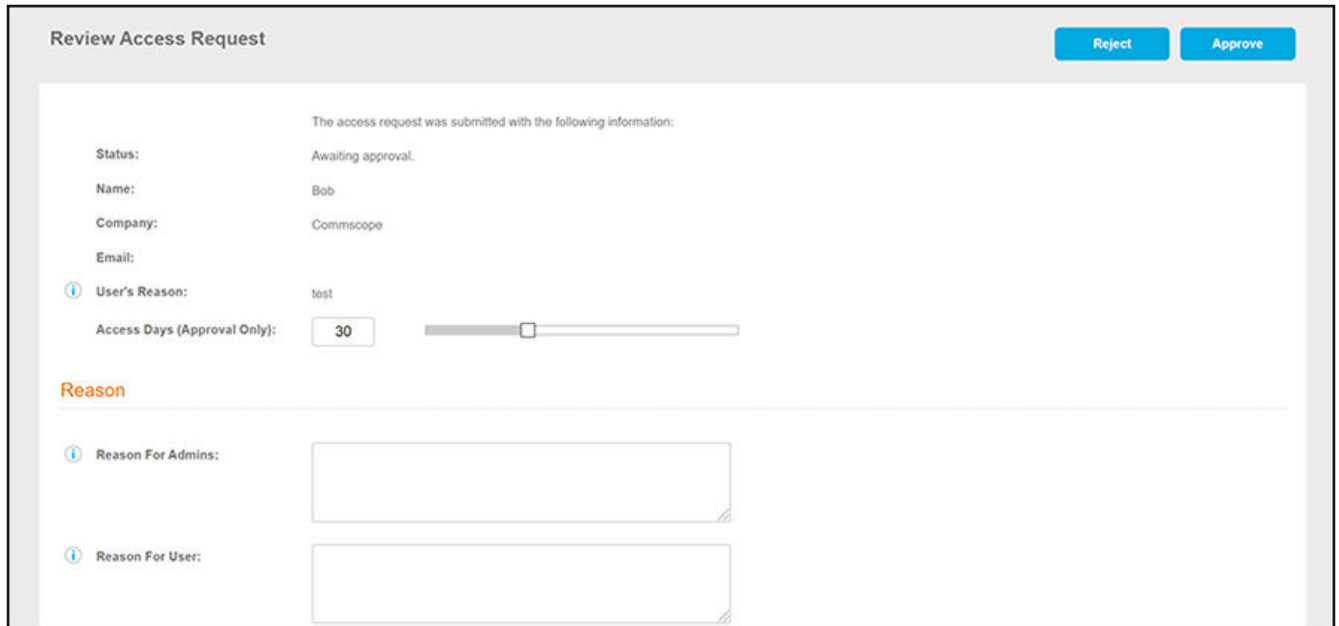
4.   The sponsor can enter information in the Reason section, if desired, and should then click either the **Reject** or **Approve** buttons.

5.   If the sponsor approves the request, the user is presented with a window that states the request has been approved, and the enrollment proceeds. If the sponsor rejects the request, the user is presented with a window that states the request was rejected and that the user should contact the sponsor for assistance.

Request Access from a Sponsor Offline

This plug-in can be used for a user to request access from a sponsor while the user can wait offline for the sponsor's approval.

The figure below shows an example of a completed workflow that uses this plug-in:

FIGURE 80 Sample Workflow That Uses the "Request Access from a Sponsor Offline" Plug-in
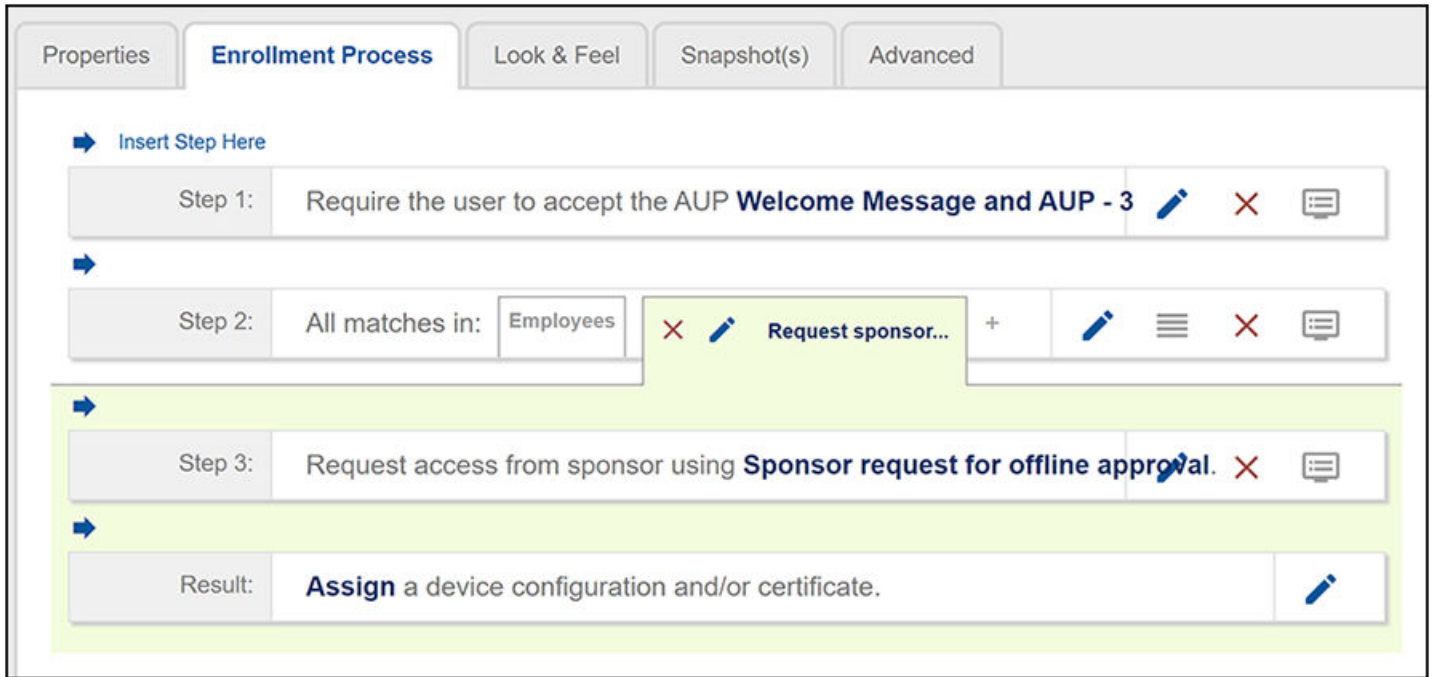
This information that follows instructs you how to configure this particular plug-in, and shows you how the interaction between user and sponsor can occur.

Configuring the "Request Access from a Sponsor Offline" Plug-in

To use this plug-in, you would first want to create a tab such as the one shown above called "Request sponsor..." (full name could be "Request sponsor access while waiting offline"). Then, follow these steps:

1. With the "Request sponsor..." tab highlighted, click the arrow below to insert a step into the workflow.

2. You will then create what is shown as Step 3 in the above workflow by scrolling down the list of available plug-ins and selecting the "Request access from a sponsor offline" button.

3. On the ensuing page, select the button called "A new access request configuration," then click **Next**.

   > **NOTE**
   > If no access request configuration exists, you will be taken directly to the next step.

4. Configure the Create Access Request page:

FIGURE 81 Create Access Request Configuration Page for Sponsor Offline

In the Default Sponsor Email field, enter the email address of the sponsor. The enrolling user's request for approval will be sent to this email address.

5. Set the other values as desired, then click **Save**. You can click the "i" icons to get information about the fields on the screen.

How the Enrollment Process Works for the "Request Access from a Sponsor Offline" Plug-in

After your workflow is complete, you can publish the workflow, then test the enrollment process by clicking on the enrollment URL. The following example covers the basics of the offline sponsor request:

1. After the enrolling user selects the branch for requesting access from a sponsor while the user can wait offline, the following window is presented to the user:

FIGURE 82 User Presented With Two Network Access Options

2. The user needs to select the Request Network Access button (which expands the window), then enter the requested information, as shown in the following example, then click **Send**. Note that, in the "Notify Via" fields, users must enter their contact information to receive the response from the sponsor.

FIGURE 83 User Enters Information to Request Network Access

3. Once the user sends their information, the following occurs:

- The user is presented with the following status screen, which will continue to display until the user clicks **Continue** (which the user should not do until receiving the verification code from the sponsor):

FIGURE 84 Status Presented to User While Waiting Offline for Sponsor's Response
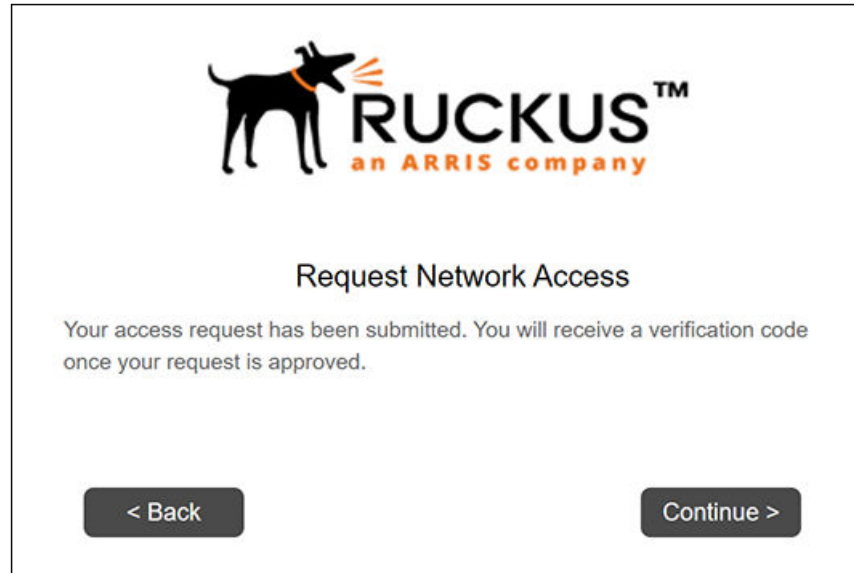
- The sponsor receives a notification about the user's request for access, such as the following email:

FIGURE 85 Email Sent to Sponsor for an Offline Request for Network Access

4. It is now up to the sponsor to take action. The sponsor must click "Review" in the notification. The sponsor is then presented with a screen where the request can either be rejected or approved:

FIGURE 86 Review Access Request Page for Sponsor

5. The sponsor can enter information in the Reason section, if desired, and should then click either the **Reject** or **Approve** buttons.

6. If the sponsor approves the request, the user receives an email or text with the verification code (continue to the next step below). (If the sponsor rejects the request, the user receives an email or text that their request was rejected.)

7. If the user's request was approved, and the user has received the verification code, the user should then click **Continue** on the currently displayed window (see Figure 84).

8. The following Request Network Access window reappears:

FIGURE 87 User Presented With Two Network Access Options for the Second Time

9. Now that the user has received the verification code from the sponsor, the user this time should select the top button in the screen above, then enter the verification code, and click **Send**.

10. The user enrollment continues.

Using CAPTCHA Options With Out-of-Band Workflow Plugins

If you select the "Onboard Via Cloud" option for either the Outbound Email or Outbound SMS system service, you must use either CAPTCHA or RECAPTCHA with either of the two existing out-of-band workflow plugins: "Perform out-of-band verification" or "Request access from a sponsor offline" workflow plugins. If you select any option other than "Onboard Via Cloud" for both the Outbound Email and Outbound SMS system services, you then have the additional option of not prompting the user for CAPTCHA or RECAPTCHA during an enrollment.

Follow the steps below to explore your options:

1. In the Cloudpath UI, navigate to **Administration > System Services**.

2. Scroll down to the Outbound Email service and click the edit icon.

3. Click on the Email Provider drop-down to invoke the email provider options:

FIGURE 88 Email Provider Options
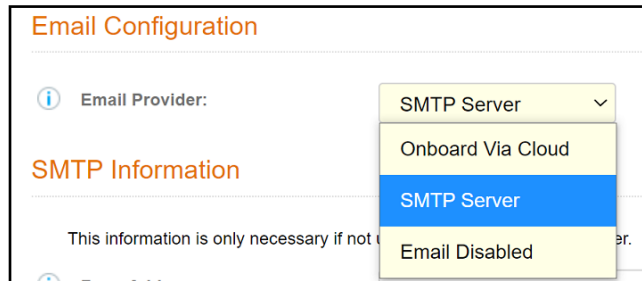
4. Make the selection of your choice:

a. Onboard Via Cloud: Emails are routed through cloud servers. If you select this option, the "Perform out-of-band verification" or "Request access from a sponsor offline" workflow plugins will use CAPTCHA or RECAPTCHA (based on how you configure those plugins) during user enrollment to help protect the system against malicious automated flooding for requests for access.

> **NOTE**
> If you select either of the other Email Provider options, and you also use your own SMS provider, you then have the option to disable CAPTCHA *and* RECAPTCHA for the two out-of-band workflow plugins (described later in this procedure).

b. SMTP Server: Emails are routed to your own email server, based on the information you configure in the SMTP Information portion of the screen.

c. Email Disabled: Outgoing emails are disabled.

5. Complete the Outbound Email configuration and click **Save**.

6. Scroll down to the Outbound SMS service and click the edit icon.

7. Click on the SMS Provider drop-down to invoke the SMS Provider options:

FIGURE 89 SMS Provider Options
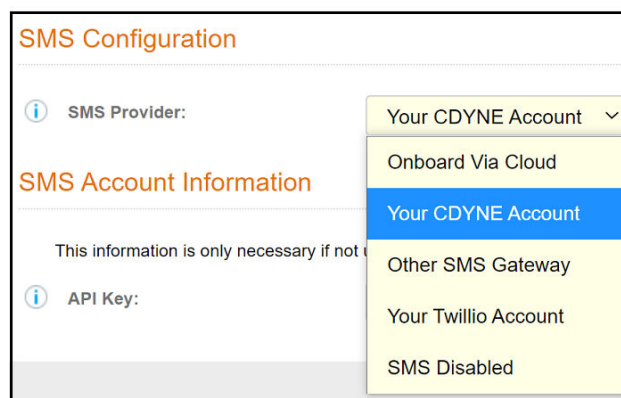
8. Make the selection of your choice:

a. Onboard Via Cloud: SMS messages are routed through cloud servers. If you select this option, the "Perform out-of-band verification" or "Request access from a sponsor offline" workflow plugins will use CAPTCHA or RECAPTCHA (based on how you configure those plugins) during user enrollment to help protect the system against malicious automated flooding for requests for access.

> **NOTE**
> If you select either of the other SMS Provider options, and you also use your own Email provider, you then have the option to disable CAPTCHA *and* RECAPTCHA for the two out-of-band workflow plugins (described later in this procedure).

    b.   Your CDYNE Account: SMS messages are routed through a customer-owned CDYNE account.

    c.   Other SMS Gateway: SMS messages are routed through a customer-owned account. The URL of the SMS gateway is required.

    d.   Your Twillio Account: SMS messages are routed through a customer-owned Twillio account.

    e.   SMS Disabled: No SMS messages are sent.

9. Select the desired CAPTCHA option in the "Perform out-of-band verification" or "Request access from a sponsor offline" workflow plugins as you add (or edit) them as a step in a workflow. Scroll to the Captcha Type drop down (the example screen is from the "Request access from a sponsor offline" plugin), and make your selection:

FIGURE 90 Captcha Type Drop-Down
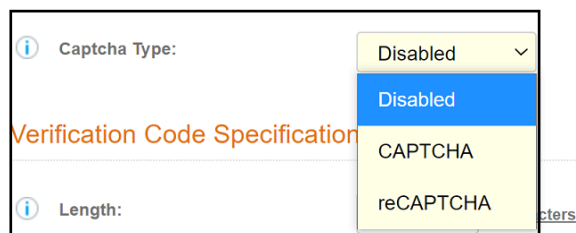
> **NOTE**
> The "Disabled" option appears only if you did not use the "Onboard Via Cloud" option in either Figure 88 or Figure 89.

Prompting Users to Name Their Device and Remove Old Devices

You can use the workflow plugin called "Ask the user to name their device" to let users manage their own devices.

The "Ask the user to name their device" workflow plug-in can be used however you see fit in a given workflow if you want to allow users to delete previous devices they have used to enroll with Cloudpath, and add new devices. This is demonstrated with the following example procedure, where this workflow step is used in conjunction with a "MAC Registration List" workflow plugin.

1. From the Cloudpath UI, begin building your workflow.

2. Be sure to include the "Authenticate to a traditional server" step early in the workflow (step 1 in Figure 92).
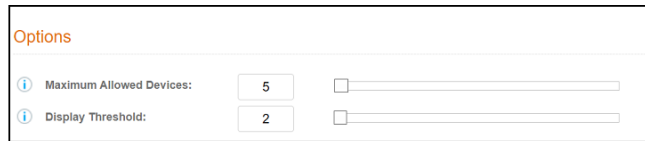
> **NOTE**
> You need an authentication step before Cloudpath will let you add the "Ask the user to name their device" step to the workflow.

3. You could choose to have a MAC Registration step next. Within that step, you have the option to prompt the user to enter the MAC address of their enrolling device.

4. Add the "Ask the user to name their device" step next. When you add this step, you have different options you can configure. The options that allow you to determine how you want to let users manage their devices is provided in the "Options" portion of the configuration screen:

FIGURE 91 Options Portion of "Ask the user to name their device" Workflow Step Configuration
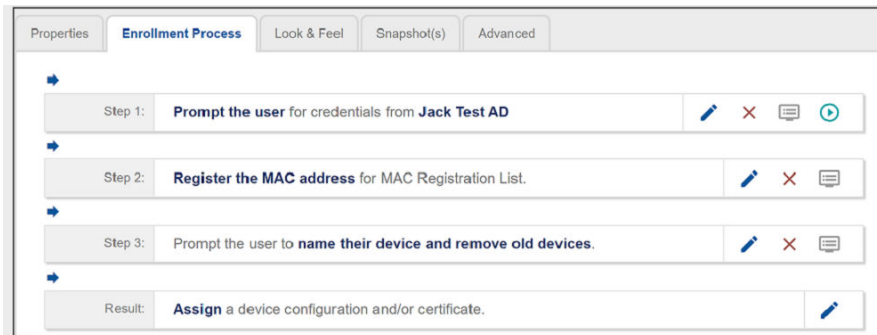
5. Set the options as desired.

   a. The "Maximum Allowed Devices" field can be set as high as 999. If you do not want to restrict the number of devices, set the value of this field to 0. In the example above, the administrator has chosen 5 as the maximum number of devices that the enrolling user can have in Cloudpath.

   b. The "Display Threshold" field is where you determine how enrolling users can manage their own devices. You can set this value to be equal to or less than the value set in the "Maximum Allowed Devices" field. As soon as the user has enrolled the number of devices that matches the value configured in this field (2 in the example in the screen above), the user receives a prompt that allows them to delete old devices or add a new device (Figure 93).

6. Save the above configuration. The configuration example would be displayed as:

FIGURE 92 Completed Workflow Example That Includes Users Naming Their Device and Removing Old Devices
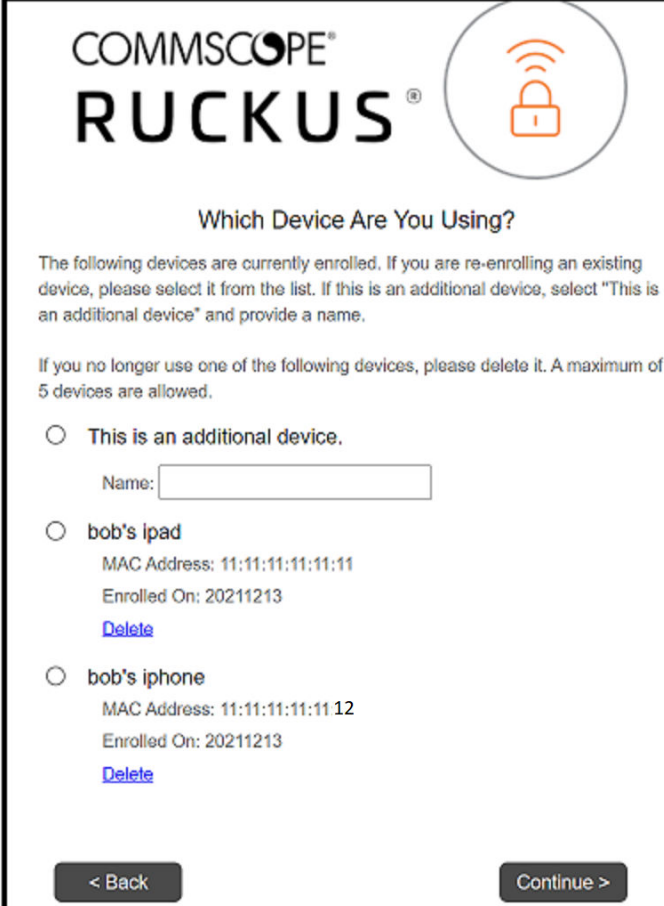
7. Publish the workflow.

8. Test out the workflow (by clicking on the Enrollment URL at the top of the workflow) by continuing to add devices. After you hit the display threshold of two devices, you should receive the prompt shown in the following screen:

FIGURE 93 Prompt the End User Will Get Once the Configured "Display Threshold" Number Has Been Met

You can take any action here that you want. Once you have enrolled the configured limit of five devices, the button to add an additional device is greyed out until you delete an old device.

> **NOTE**
> As you are adding devices, you do not need to restart the enrollment process each time; you can instead click **Start Over** that is displayed just above the screen shown above.

Using Variables in a Workflow Split

Once you use the "Split users into different branches" plug-in within a workflow, you can edit any of these branches to employ the usage of variables.

The following steps show an example of how to use variables within a branch of a workflow.

1. Create a workflow that includes a branch split, such as the one shown below, where the split is for "Engineering/Visitors":

FIGURE 94 Workflow Split Example
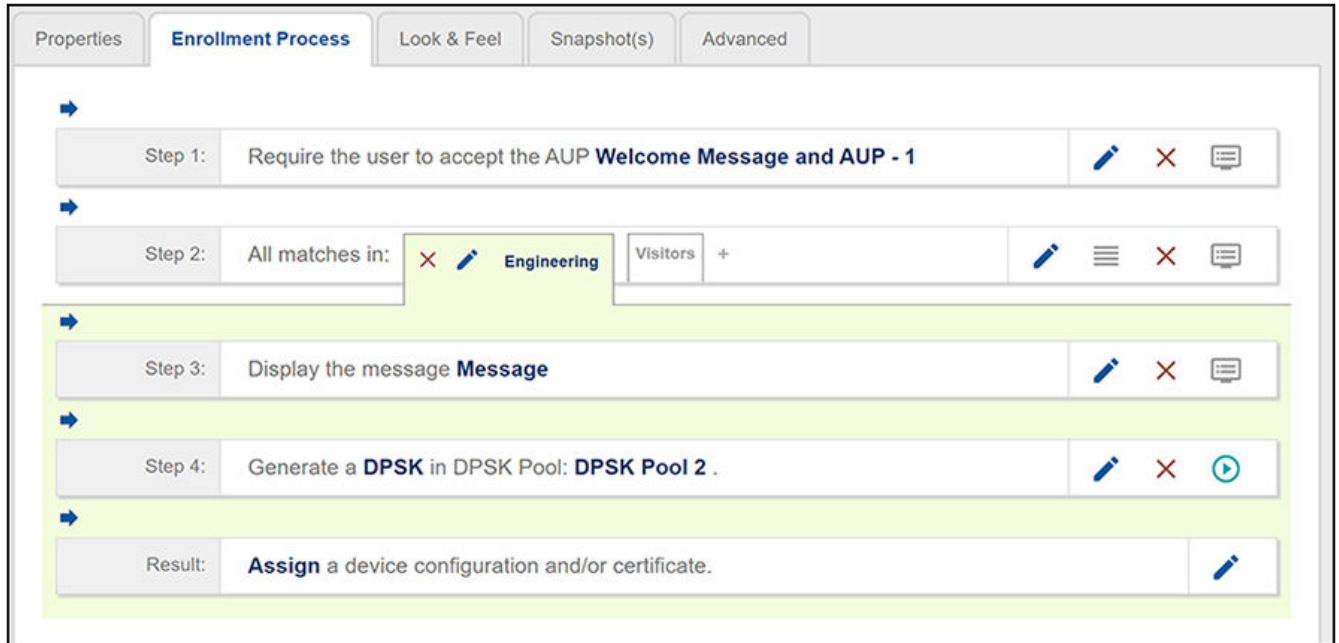
2.   Click the pencil icon within the "Engineering" split label to invoke the "Modify Step" screen.

3.   Scroll down to the "Variable Assignments" section, and click the arrow to view instructions for adding system-defined variables and/or any custom variables, then add as many variables (and assign corresponding values) as you wish, as demonstrated in the screen below.

> **NOTE**
> A custom variable can be any name you wish.

> **NOTE**
> Custom enrollment variables do not work with certificate templates.

FIGURE 95 Assigning Variables in a Workflow Split
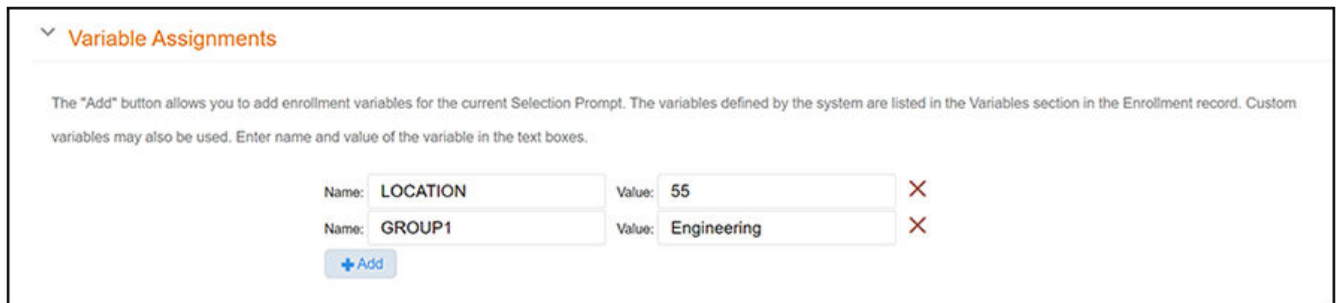
4.   When you are done adding variables, click **Save**.

5.   You can now use those variables elsewhere in your workflow. For example, you can use a "Display a Message" plug-in next to show the enrolling user what the values are for the variables you set in the previous step. (You might use the LOCATION variable as a VLAN ID,

described later in this procedure.) To add a "Display a Message" plug-in below the "Engineering" split (as shown in Figure 94), do the following:

a.   With the "Engineering" tab highlighted (in the example workflow), click the arrow under Step 2 to insert a step.

b.   Scroll down the list of steps and click "Display a message."

c.   On the ensuing screen, with the selection "A new message created from a standard template" selected, click **Next**.

d.   You can use the fields in the next screen as desired. The example below shows how you can use the "Webpage Display Information" area to include some text around the variables.

> **NOTE**
> The variables themselves, when referenced, must be enclosed in curly brackets that are preceded by a $.

FIGURE 96 Using Variables in Display-A-Message Step

e.   Click **Save**.

Possible Usage of LOCATION Variable

One way you could use the LOCATION variable is as the VLAN ID in a RADIUS attribute group (Go to **Configuration > Policies > RADIUS Attribute Groups**). You could enter $(LOCATION} in the VLAN ID field of a RADIUS attribute group, and the value of LOCATION becomes the VLAN ID of that attribute group. A RADIUS attribute group belongs to a policy that is in turned assigned to different entities, such as an eDPSK pool, which is a step shown in the example workflow in Figure 94.

How the Variables Are Presented to an Enrolling User

Once you publish the workflow, the "Display a message" configuration that is shown in Figure 96 would be presented to an an enrolling user as follows:

FIGURE 97 Message Displayed to User Based on Variables

Checking Variable Assignments in the Dashboard

After a user enrollment completes, you can go to **Dashboard > Enrollments**, then click the magnifying glass icon next to the enrollment you wish to view, and then scroll down to the "Enrollment Variables" section. The variables you assigned and their corresponding values should be in the list.

> **NOTE**
> Any custom variables you created should also appear next to: ${ROLLUP_CUSTOM_VARIABLES}

WiFi4EU Support Within the Display-a-Message Plugin

WIFI4EU is a program that allows countries in the European Union to apply for government grants for free wifi in municipalities.

The "Display a Message" workflow step in the Cloudpath UI includes four fields that allow the message step to act as a WiFi4EU "portal."

For compliancy information if you are setting up a Wifi4EU network, refer to the *WiFi4EU Policy Enforcement Component Implementation Guide*, which is easily located in an Internet search.

> **NOTE**
> A walled garden consists of web resources accessible before a user has been authenticated using the portal. In order for the snippet to function properly, the following address should be whitelisted in the walled garden: https://collection.wifi4eu.ec.europa.eu

Follow these steps to perform the Cloudpath UI configuration for Wifi4EU:

1. During creation of a workflow, insert the "Display a Message" step at the desired location.

2. When configuring the "Display a Message" step, use the following fields (see descriptions following the screen):

FIGURE 98 Setting the Wifi4EU Fields in the Display-a-Message Workflow Step

- Include Wifi4EU Script: Checking this box invokes the fields below this field.

- Wifi4EU Portal Language: Drop-down list from which you select the country.

- WiFi4EU Network Indentifier: Enter or paste in the network identiifer that you have been provided.

- WiFi4EU Self-Test Mode: Check this box to run the WiFi4EU-provided script in test mode. This will output compliance with Wifi4EU portal standards to the browser developer console.

  NOTE
  Uncheck this box, save the change, then republish your workflow before you use the workflow in a production environment.

3. Click **Save**.

4. Publish your workflow.

5. Click the enrollment portal URL link at the top of the main Workflows page.

6. Proceed through the enrollment workflow to be sure that you receive a screen such as the following:

FIGURE 99 Wifi4EU Screen Received During User Enrollment

7.   Be sure to uncheck the "Wifi4EU Self-Test Mode" box in Figure 98 before using the workflow in your production environment.

Ruckus Controller Integration for Cloudpath

Overview

This section describes how to configure RUCKUS Virtual SmartZone, RUCKUS Unleashed, and RUCKUS ZoneDirector to integrate with the Cloudpath system. The information provided here is specific to integrating Cloudpath with one of these controllers. Consult your controller documentation for more information.

Configuring Virtual SmartZone

This section includes tables of configuration fields and values for setting up the Vitrual SmartZone (vSmartZone) Controller. For more information, such as how to navigate the vSmartZone UI, how to find more information about configuration fields, and to view screen shots of the vSmartZone UI, refer to the *RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide*.

> **NOTE**
> For any configuration fields that are not described in the following sections, you can use their default values.

Setting up Cloudpath as an AAA RADIUS Authentication Server

TABLE 4 Fields/Values to Use for vSmartZone AAA Authentication Service

AAA Authentication Service Section in vSmartZone UI	Configuration Field and Corresponding Value
General Options	Name: Any descriptive name for the AAA authentication service
	Type: RADIUS
Primary Server	IP Address: The IP address of the Cloudpath Enrollment System.
	Port: 1812 is typically used and is the default.
	Shared Secret: This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
	Confirm Secret: The shared secret (entered again).

Creating AAA RADIUS Accounting Server (Optional)

TABLE 5 Fields/Values to Use for SmartZone AAA Accounting Service

AAA Accounting Service Section in vSmartZone UI	Configuration Field and Corresponding Value
General Options	Name: Any descriptive name for the AAA accounting service
	Type: RADIUS ACCOUNTING

TABLE 5 Fields/Values to Use for SmartZone AAA Accounting Service (continued)

AAA Accounting Service Section in vSmartZone UI	Configuration Field and Corresponding Value
Primary Server	IP Address: The IP address of the Cloudpath Enrollment System.
	Port: 1813 is typically used and is the default.
	Shared Secret: This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
	Confirm Secret: The shared secret (entered again).

Testing AAA Servers

To test the connection between the controller and the Cloudpath RADIUS server, RUCKUS strongly recommends testing the AAA server after you set it up. Refer to the instructions in the *RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide*.

Creating a Hotspot (WISPr) Portal

TABLE 6 Fields/Values to Use for Creating a Hotspot (WISPr) Portal

Creating a Hotspot (WISPr) Portal section in vSmartZone UI	Configuration Field and Corresponding Value
General Options	Portal Name: Any descriptive name for the hotspot portal.
Redirection	Login URL: Select "External."
	Redirect unauthenticated user: The Cloudpath Enrollment Portal URL, which should be contained in the applicable workflow in the Cloudpath UI (**Configuration > Workflows**).
	Start Page: After user is authenticated,: Select "Redirect to the URL that the user intends to visit." This lets you set a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address for the redirection.

Setting Up the Walled Garden

To add a walled garden configuration to your existing Hotspot Services, refer to the instructions in the *RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide*.

Also, when configuring the walled garden, include the following steps:

1. Include the DNS or IP address of the Cloudpath system, then click **OK**

2. Optionally, there are some domains that you can add to the walled garden on all controllers to:

   - Prevent the Apple CNA mini-browser from appearing on Apple devices.

   - Avoid being blocked or slowed when attempting to download the Cloudpath wizard.

      NOTE
      There will still be about a 15-to-20-second delay when the full application is 33 percent complete (about 40 MB) in its download.

   The recommended destinations to add for the walled garden are:

   ```
   *.ggpht.com
   *.play.googleapis.com
   *.googleapis.com
   *.play.google.com
   android.clients.google.com
   *.gvt1.com
   ```

```
connectivitycheck.android.com
connectivitiycheck.google.com
*.gstatic.com
*.clients3.google.com
*.thawte.com
```

> **NOTE**
>
> The *thawte.com destination is the OCSP URL of the SSL certificate of the Cloudpath server. This URL can be found by clicking the *lock* icon in your web browser and viewing the details of your certificate.

3. If you are still experiencing issues, you can try adding the following destinations to the walled garden:

```
*.clients.google.com
*.l.google.com
*.googleusercontent.com
*.appengine.google.com
*.cloud.google.com
*.android.com
*.cloudfront.net
*.akamaihd.net
172.217.0.0/16
216.58.0.0/16
```

Creating the Onboarding SSID

TABLE 7 Fields/Values to Use for SmartZone Onboarding SSID

Creating a WLAN Configuration (for Onboarding SSID) section in vSmartZone UI	Configuration Field and Corresponding Value
General Options	Name: Name of the SSID
	SSID: Name of the WLAN
	Zone: Zone in which the WLAN will reside
	WLAN Group: Group in which the WLAN will reside
Authentication Options	Authentication Type: Hotspot (WISPr)
	Method: MAC Address
	MAC Authentication: Unchecked
	MAC Address Format: Recommended format is AA:BB:CC:DD:EE:FF
Encryption options	Method: None
Hotspot Portal	Hotspot (WISPr) Portal: Drop-down list to select the already-created hotspot service.
	Bypass CNA: Enable
	Authentication Server: Drop-down list to select the Cloudpath RADIUS Authentication Server
	Accounting Server: Drop-down list to select the Cloudpath RADIUS Accounting Server

Configuring Unleashed

This section includes tables of configuration fields and values for setting up the RUCKUS Unleashed platform. For more information, such as how to navigate the Unleashed UI, how to find more information about configuration fields, and to view screen shots of the Unleashed UI, refer to the *RUCKUS Unleashed User Guide*.

> **NOTE**
> For any configuration fields that are not described in the following sections, you can use their default values.

Setting up Cloudpath as an AAA RADIUS Authentication Server

TABLE 8 Fields/Values to Use for Unleashed AAA Authentication Service

Configuration Field	Corresponding Value
Name	Name: Any descriptive name for the AAA authentication service
Type	RADIUS
Auth Method	PAP
IP Address	The IP address of the Cloudpath Enrollment System.
Port	1812 is typically used and is the default.
Shared Secret	This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
Confirm Secret	Confirm Secret: The shared secret (entered again).

Creating AAA Accounting Server (Optional)

TABLE 9 Fields/Values to Use for Unleashed AAA RADIUS Accounting Service

Configuration Field	Corresponding Value
Name	Name: Any descriptive name for the AAA accounting service
Type	RADIUS ACCOUNTING
IP Address	The IP address of the Cloudpath Enrollment System.
Port	1813 is typically used and is the default.
Shared Secret	This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
Confirm Secret	Confirm Secret: The shared secret (entered again).

Testing AAA Servers

To test the connection between Unleashed and the Cloudpath RADIUS server, RUCKUS strongly recommends testing the AAA server after you set it up. Refer to the instructions in the *RUCKUS Unleashed User Guide*.

Creating a Hotspot (WISPr) Portal

TABLE 10 Fields/Values to Use for Creating a Hotspot (WISPr) Portal

Creating a Hotspot (WISPr) Portal Section in Unleashed UI	Configuration Field and Corresponding Value
General tab	Name: Any descriptive name for the hotspot portal.
Redirection (General tab)	Redirect unauthenticated user: The Cloudpath Enrollment Portal URL, which should be contained in the applicable workflow in the Cloudpath UI (**Configuration > Workflows**).
	Start Page: After user is authenticated,: Select "Redirect to the URL that the user intends to visit." This lets you set a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address for the redirection.

TABLE 10 Fields/Values to Use for Creating a Hotspot (WISPr) Portal (continued)

Creating a Hotspot (WISPr) Portal Section in Unleashed UI	Configuration Field and Corresponding Value
Authentication/Accounting Servers (Authentication tab)	Authentication Server: Drop-down list to select the Cloudpath RADIUS Authentication Server. **NOTE** Enabling this option allows users with registered MAC addresses to be transparently authorized without having to log in. A user entry on the RADIUS server needs to be created using the client MAC address as both the user name and password. For the MAC address format, RUCKUS recommends using AA:BB:CC:DD:EE:FF.
Authentication/Accounting Servers (Authentication tab)	Accounting Server: Drop-down list to select the Cloudpath RADIUS Accounting Server (if applicable).

Setting Up the Walled Garden

To add a walled garden configuration, refer to the instructions in the *RUCKUS Unleashed User Guide*.

Also, when configuring the walled garden, include the following steps:

1. Include the DNS or IP address of the Cloudpath system, then click **OK**

2. Optionally, there are some domains that you can add to the walled garden on all controllers to:

   - Prevent the Apple CNA mini-browser from appearing on Apple devices.

   - Avoid being blocked or slowed when attempting to download the Cloudpath wizard.

        NOTE
        There will still be about a 15-to-20-second delay when the full application is 33 percent complete (about 40 MB) in its download.

   The recommended destinations to add for the walled garden are:

   ```
   *.ggpht.com
   *.play.googleapis.com
   *.googleapis.com
   *.play.google.com
   android.clients.google.com
   *.gvt1.com
   connectivitycheck.android.com
   connectivitiycheck.google.com
   *.gstatic.com
   *.clients3.google.com
   *.thawte.com
   ```

        NOTE
        The *thawte.com destination is the OCSP URL of the SSL certificate of the Cloudpath server. This URL can be found by clicking the *lock* icon in your web browser and viewing the details of your certificate.

3. If you are still experiencing issues, you can try adding the following destinations to the walled garden:

   ```
   *.clients.google.com
   *.l.google.com
   *.googleusercontent.com
   *.appengine.google.com
   *.cloud.google.com
   *.android.com
   *.cloudfront.net
   *.akamaihd.net
   ```

```
172.217.0.0/16
216.58.0.0/16
```

Creating the Onboarding SSID

TABLE 11 Fields/Values to Use for Unleashed Onboarding SSID

Configuration Field	Corresponding Value
Name	Name of the SSID
Usage Type	Hotspot Service known as WISPr
Hotspot Services	Drop-down list to selet the already-created hotspot service

> **NOTE**
> RUCKUS recommends enabling the "Bypass Apple CNA" feature. For instructions, refer to the *RUCKUS Unleashed User Guide*.

Configuring ZoneDirector

This section includes tables of configuration fields and values for setting up the ZoneDirector Controller. For more information, such as how to navigate the ZoneDirector UI, how to find more information about configuration fields, and to view screen shots of the vSmartZone UI, refer to the *RUCKUS ZoneDirector User Guide*.

> **NOTE**
> For any configuration fields that are not described in the following sections, you can use their default values.

Setting up Cloudpath as an AAA RADIUS Authentication Server

TABLE 12 Fields/Values to Use for ZoneDirector AAA Authentication Service

Configuration Field	Corresponding Value
Name	Name: Any descriptive name for the AAA authentication service
Type	RADIUS
Auth Method	PAP
IP Address	The IP address of the Cloudpath Enrollment System.
Port	1812 is typically used and is the default.
Shared Secret	This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
Confirm Secret	Confirm Secret: The shared secret (entered again).

Creating AAA RADIUS Accounting Server (Optional)

TABLE 13 Fields/Values to Use for ZoneDirector AAA Accounting Service

Configuration Field	Corresponding Value
Name	Name: Any descriptive name for the AAA accounting service
Type	RADIUS ACCOUNTUING
Auth Method	PAP
IP Address	The IP address of the Cloudpath Enrollment System.

TABLE 13 Fields/Values to Use for ZoneDirector AAA Accounting Service (continued)

Configuration Field	Corresponding Value
Port	1813 is typically used and is the default.
Shared Secret	This must match the shared secret for the Cloudpath ES onboard RADIUS server (**Configuration > RADIUS Server**).
Confirm Secret	Confirm Secret: The shared secret (entered again).

Testing AAA Servers

To test the connection between the controller and the Cloudpath RADIUS server, RUCKUS strongly recommends testing the AAA server after you set it up. Refer to the instructions in the *RUCKUS ZoneDirector User Guide*.

Creating a Hotspot (WISPr) Portal

TABLE 14 Fields/Values to Use for Creating a Hotspot (WISPr) Portal

Creating a Hotspot (WISPr) Portal section in ZoneDirector UI	Configuration Field and Corresponding Value
Top portion of configuration fields area	Name: Any descriptive name for the hotspot portal.
Redirection	Login URL: Select "External."
	Login Page Redirect unauthenticated user: The Cloudpath Enrollment Portal URL, which should be contained in the applicable workflow in the Cloudpath UI (**Configuration > Workflows**).
	Start Page After user is authenticated,: Select "Redirect to the URL that the user intends to visit." This lets you set a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address for the redirection.
Authentication/Accounting Servers (Authentication tab)	Authentication Server: Drop-down list to select the Cloudpath RADIUS Authentication Server. **NOTE** Enabling this option allows users with registered MAC addresses to be transparently authorized without having to log in. A user entry on the RADIUS server needs to be created using the client MAC address as both the user name and password. For the MAC address format, RUCKUS recommends using AA:BB:CC:DD:EE:FF.
Authentication/Accounting Servers (Authentication tab)	Accounting Server: Drop-down list to select the Cloudpath RADIUS Accounting Server (if applicable).

Setting Up the Walled Garden

To add a walled garden configuration to your existing Hotspot Services, refer to the instructions in the *RUCKUS ZoneDirector User Guide*.

Also, when configuring the walled garden, include the following steps:

1. Include the DNS or IP address of the Cloudpath system, then click **OK**

2. Optionally, there are some domains that you can add to the walled garden on all controllers to:

   - Prevent the Apple CNA mini-browser from appearing on Apple devices.

   - Avoid being blocked or slowed when attempting to download the Cloudpath wizard.

> **NOTE**
> There will still be about a 15-to-20-second delay when the full application is 33 percent complete (about 40 MB) in its download.

The recommended destinations to add for the walled garden are:

```
*.ggpht.com
*.play.googleapis.com
*.googleapis.com
*.play.google.com
android.clients.google.com
*.gvt1.com
connectivitycheck.android.com
connectivitiycheck.google.com
*.gstatic.com
*.clients3.google.com
*.thawte.com
```

> **NOTE**
> The *thawte.com destination is the OCSP URL of the SSL certificate of the Cloudpath server. This URL can be found by clicking the *lock* icon in your web browser and viewing the details of your certificate.

3. If you are still experiencing issues, you can try adding the following destinations to the walled garden:

```
*.clients.google.com
*.l.google.com
*.googleusercontent.com
*.appengine.google.com
*.cloud.google.com
*.android.com
*.cloudfront.net
*.akamaihd.net
172.217.0.0/16
216.58.0.0/16
```

Creating the Onboarding SSID

TABLE 15 Fields/Values to Use for ZoneDirector Onboarding SSID

Creating a WLAN Configuration (for Onboarding SSID) section in ZoneDirector UI	Configuration Field and Corresponding Value
General Options	Name/ESSID: Name of the SSID
	Zone: Zone in which the WLAN will reside
WLAN Usages	Type: Hotspot (WISPr)
Authentication Options	Method: Open
Encryption Options	Method: None
Options	Hotspot Services Drop-down list to selet the already-created hotspot service.

> **NOTE**
> RUCKUS recommends enabling the "Bypass Apple CNA" feature. For instructions, refer to the *RUCKUS ZoneDirector User Guide*.

Creating the Secure SSID

To configure the onboarding SSID, navigate to: For ZoneDirector and SmartZone, go to the Wireless LANS section of the controller UI; for Unleashed, go to **Wifi Networks** to create the WLAN.

1. Name the SSID.

2. Type=Standard Usage.

3. Authentication Option Method=802.1x EAP.

4. Encryption Option Method=WPA2 (not applicable for Unleashed once the 802.1x EAP authentication option method is selected).

5. Encryption Option Algorithm=AES (not applicable for Unleashed once the 802.1x EAP authentication option method is selected).

6. Select the Cloudpath RADIUS authentication server.

7. Select the Cloudpath RADIUS accounting server (required only if you are using Cloudpath onboard RADIUS Accounting and Connection Tracking). **Note**: For ZoneDirector, you need to expand the Advanced Options section of the screen to locate the drop-down selection for the accounting server.

8. Leave the defaults for the remaining settings and click **OK**.

FIGURE 100 Configure Secure SSID on the ZoneDirector controller

FIGURE 101 Select RADIUS Accounting Server on ZoneDirector

FIGURE 102 Configure Secure SSID on the SmartZone controller

FIGURE 103 Configure Secure SSID on the Unleashed controller

The SSIDs are now configured on the wireless LAN controller. When the user connects to the onboarding (open) SSID they are redirected to the Cloudpath web page. When the user successfully completes the enrollment process, they are migrated to the secure SSID.

The Certificate Truststore

Truststore Overview

The Cloudpath Truststore determines which external systems are trusted/allowed for outbound TLS connections.

The Cloudpath Trustsore must contain the root CA certificate of each external system that you plan to integrate with your Cloudpath system.

Some examples of external systems that can integrate with Cloudpath include:

- Firewalls, such as the Palo Alto firewall

- Ruckus SmartZone controllers

- SAML Identity Providers (IdPs) used as authentication servers

- Active Directory servers

  NOTE
  Before you configure any external systems, obtain the root CA of each system.
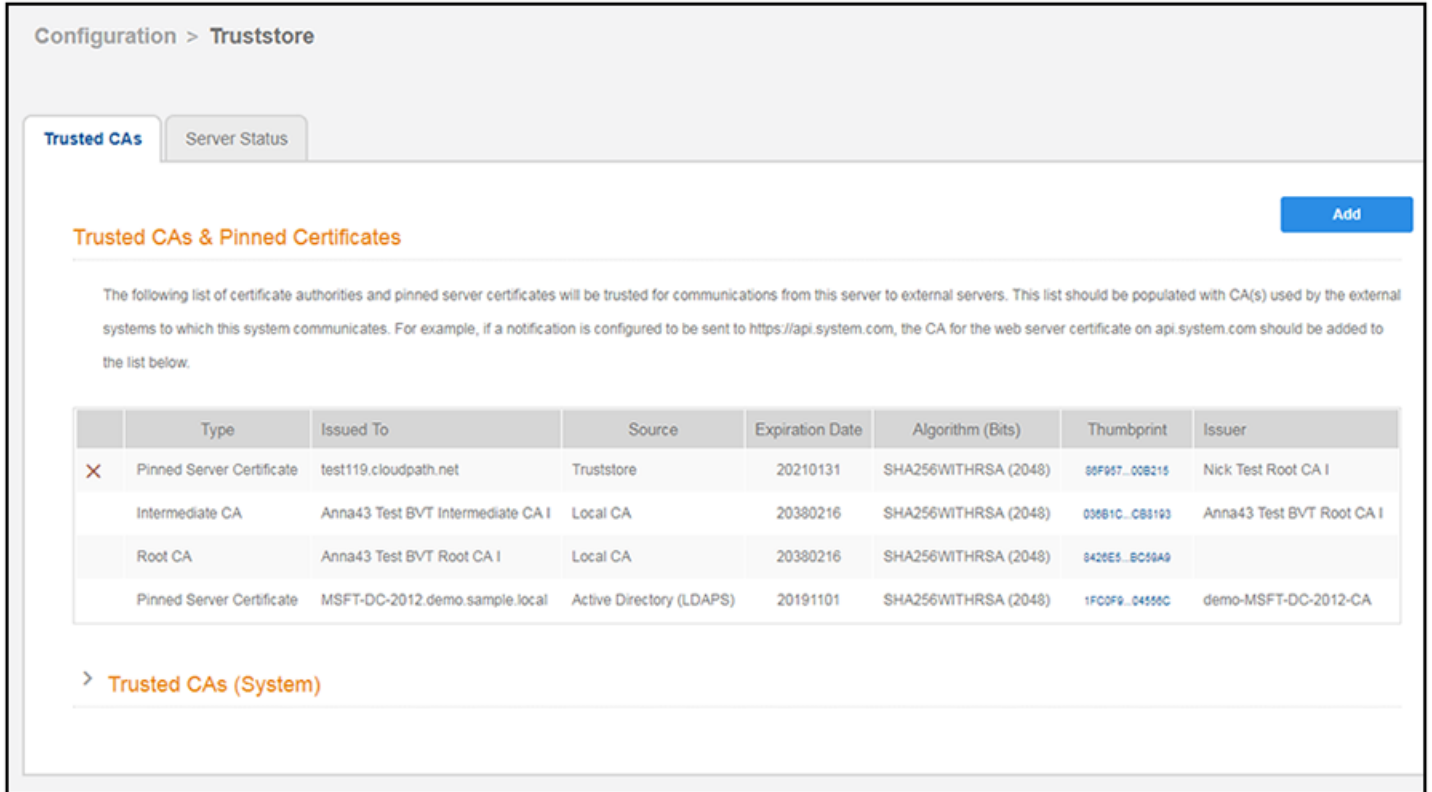
Navigating to the Cloudpath Truststore

To go to the Truststore on your Cloudpath system, click on **Configuration > Truststore**, as shown in the screen below. This screen shows the Truststore before any certificates have been added.

FIGURE 104 Truststore Screen Before Certificates Are Added
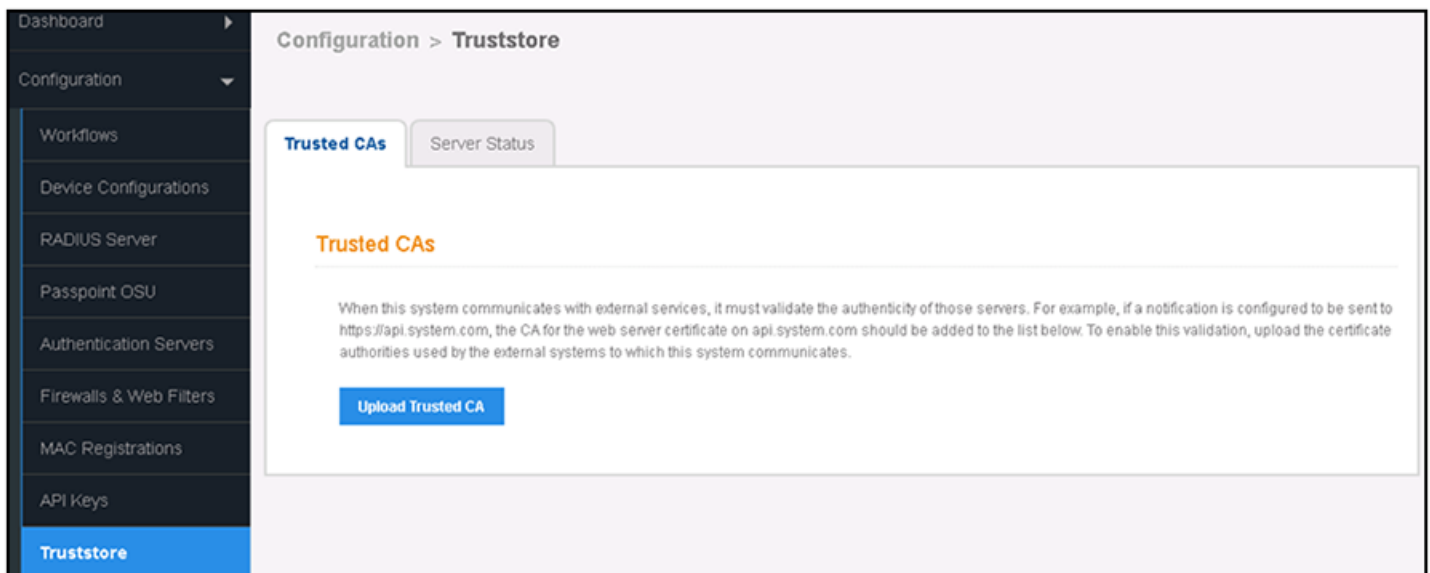
If there are already certificates in the Truststore, the certificates are listed, as in the following example:

FIGURE 105 Truststore Screen Listing All Certificates That Have Been Added

Basic Steps for Adding Certificates to the Cloudpath Truststore

Follow these steps to add your certificates to the Cloudpath Truststore:

1. Use the **Upload Trusted CA** button (or the **Add** button shown in the figure above) to manually upload the certificate. To manually add a certificate to the Truststore, refer to Recommended Method for Adding Certificates to the Cloudpath Truststore on page 141.

2. Continue to add certificates for all external systems with which your Cloudpath system needs to communicate.

3. Complete the necessary configuration steps to allow your Cloudpath system to communicate with all external systems. For additional information about required connectivity steps, refer to Cloudpath Connectivity with External Systems on page 142.

Recommended Method for Adding Certificates to the Cloudpath Truststore

It is recommended that you *manually* add the root CA certificate of all necessary external systems to the Cloudpath Truststore before you attempt to configure the external systems.

Follow the steps below to manually add certificates to the Truststore.

1. On your Cloudpath system, go to **Configuration > Truststore**. If there are already certificates in the Truststore, the screen shows the list of certificates, as in the following example:

FIGURE 106 Trusted CAs List Where You Can Manually Add More Certificates
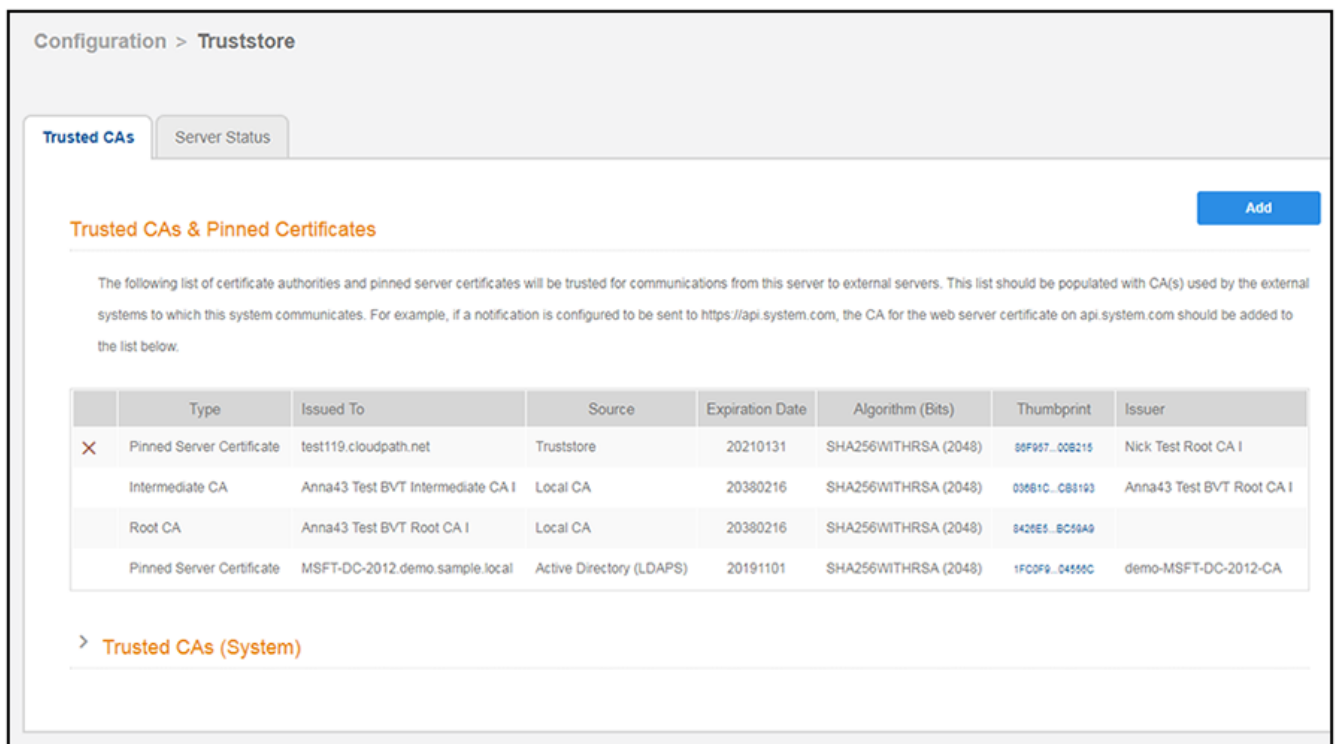
2. To add another certificate, click **Add**.

   The popup window appears:

   FIGURE 107 Truststore Upload Popup to Add New Certificate

3. Click **Choose File**, browse to the root CA of the external system you want, and upload it to the Truststore.
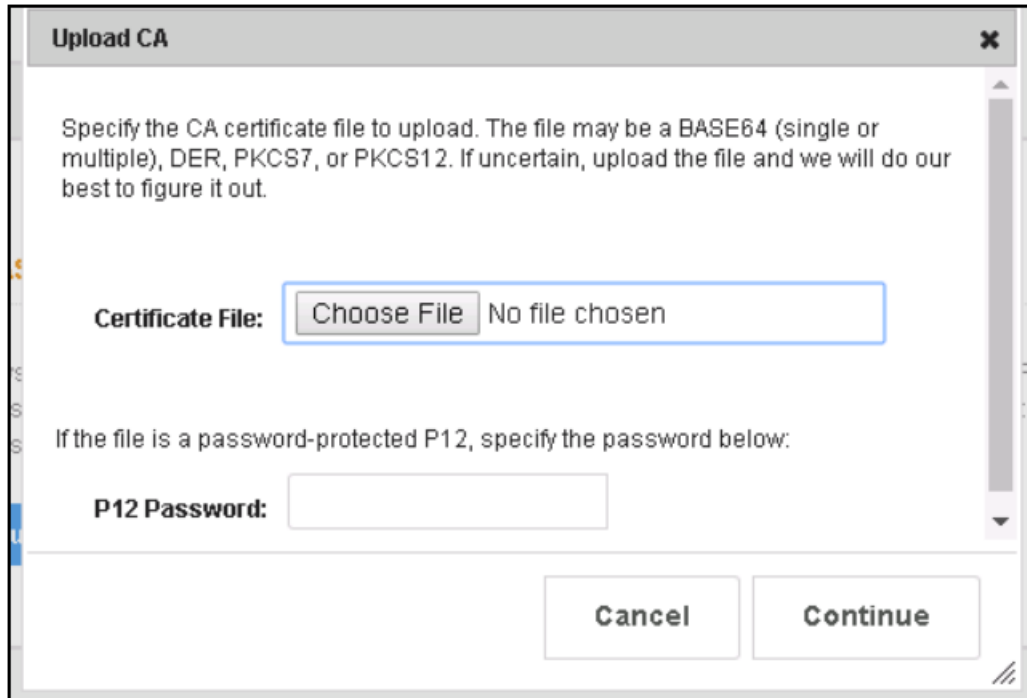4. Repeat the previous step until you have added the root CA of all required external systems.

Check to be sure that your certificates now appear in the list of certificates in the **Trusted CAs** tab of the Truststore screen.

Cloudpath Connectivity with External Systems

When connecting with external systems, there are some specific Cloudpath considerations.

The following sections provide information about various types of external systems that may be integrated with your Cloudpath system:

- Connecting to Ruckus Controllers
- Connecting to Firewalls
- Active Directory

Connecting to Ruckus Controllers

If you are using a Ruckus SmartZone controller to integrate with your Cloudpath system, there is a configuration field in Cloudpath that requires the hostname, not the IP address, of the controller so that Cloudpath can obtain the root certificate from the controller. For example, DPSK requires this field.

The field is called "WLAN IP/DNS," as shown in the screen below. You must enter the fully qualified domain name of the controller in this field.

FIGURE 108 Example of Controller Hostname Configuration in Cloudpath

For information about where this screen fits into the Cloudpath configuration process, you can refer to *Configuring Cloudpath to Work With Ruckus Dynamic Pre-Shared Key (DPSK)*. See the "Configuring DPSK on Cloudpath to Integrate with SmartZone" chapter.

Once you save this configuration, Cloudpath connects to the controller and pulls all the information available, including the root certificate.

Note about MAC Registration: With MAC registration, the client device communicates directly with an access point. Because the Cloudpath system is not directly involved in this communication, a certificate is not required for the Truststore.

Connecting to Firewalls

See the *Cloudpath Integration with Palo Alto Firewalls* manual for instructions to connect to a firewall by configuring the information in the following screen (**Configuration > Firewalls & Web Filters**):

FIGURE 109 Palo Alto Firewall Configuration Screen

After you have completed the instructions in the *Cloudpath Integration with Palo Alto Firewalls* manual, Cloudpath attempts to establish an SSL connection to the firewall. When configuring the information in the screen shown above, you might receive the following error:

FIGURE 110 Possible Error Message While Cloudpath Tries to Connect to Palo Alto Firewall
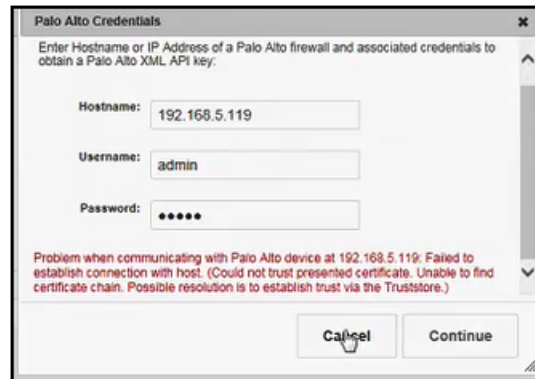
If you do receive this error, you *must* manually add the root certificate to Cloudpath by following the steps in

Active Directory

In the initial Cloudpath system setup, if you configured an active directory, then the associated root certificate should already be in the Truststore.

Troubleshooting Your Deployment

Overview

For general Cloudpath operations information, refer to the *Cloudpath Operations Manual*, which can be found on the **Support** > **Documentation** tab.

This section describes solutions to common troubleshooting issues with the Cloudpath deployment.

Connectivity Issues

Cloudpath License Server

Cloudpath communicates with the Cloudpath License Server for network and licensing information. Cloudpath must be able to communicate to xpc.cloudpath.net (72.181.151.75) over TCP ports 80/443 for HTTP/HTTPS.

RADIUS Server

The wireless controller must be able to communicate with the Cloudpath onboard RADIUS server on port 14650.

Firewall Requirements

The Firewall Requirements table is designed to help you understanding the inbound and outbound traffic of the Cloudpath server. The table is dynamically generated based on your system configuration and can change as the system configuration is modified.

To view this information, go to **Administration** > **Firewall Requirements**.

FIGURE 111 Firewall Configuration

Issues with User Credentials

Active Directory

If users receive errors about bad credentials, check the following:

- Make sure that RADIUS requests are going outbound from the AD server.

- Ping the AD server using the FQDN to verify that DNS is working.

- Verify that the RADIUS IP address and shared secret specified on the WLC matches what is on Cloudpath.

Credentials Mismatch

If you receive an error that an authentication failed due to a user credentials mismatch, either the user name provided does not map to an existing user account, or the password was incorrect.

LDAP

Using LDAP's default port (TCP-389) with a Base DN of the parent Active Directory domain only shows objects from the parent domain. Changing the port to 3268, but keeping the same Base DN allows LDAP access to users from the child AD domain.

Global Catalog queries are directed to port 3268, which indicates that Global Catalog semantics are required. By default, ordinary LDAP searches are received through port 389. If you bind to port 389, even if you bind to a Global Catalog server, your search includes a single domain directory partition. If you bind to port 3268, your search includes all directory partitions in the forest. If the server you attempt to bind to over port 3268 is not a Global Catalog server, the server refuses the bind.

DNS Issues

Verify that DNS is Working

Open a Command Prompt and enter the command: **nslookup**. The result should display the eth0 IP address of the Cloudpath virtual appliance.

Verify that DNS is Working

1. Open a Command Prompt.

2. Enter the command: **nslookup**

3. At the nslookup prompt (">"), enter the command: **set q=rr_type**

4. After the previous command completes, enter:

        _ldap._tcp.dc._msdcs.Active_Directory_domain_name

Review the output of the SRV query to determine if the query succeeded or failed:

- If the query succeeds, review the registered Service Location (SRV) resource record (RR)s returned in the query to determine if all domain controllers for your Active Directory domain are included and registered using valid IP addresses.

- If the query fails, continue troubleshooting dynamic update or DNS server related issues to determine the exact cause of the problem.

OSCP Issues

OSCP Validation

The RADIUS or NPS server first attempts to validate a client certificate using the Online Certificate Status Protocol (OSCP). If the OSCP validation is successful, the validation verification is satisfied; otherwise, it attempts to perform a CRL validation of the user or computer certificate.

OCSP provides the ability to revoke certificates. However, if using OCSP affects the performance of your system, you might disable OCSP and use CRL only.

OSCP Server in the DNS

When the client fetches the OCSP response from the CA, it looks up the domain name of the CA's OCSP server in the DNS, as well as establishing a connection to the OCSP server.

If you receive a message that indicates the server cannot resolve the OSCP URL, check the hostname listed in the OSCP URL for the onboard Root CA you created in Cloudpath. You might need to add this hostname to the DNS of the domain.

Certificate Issues

Certificate Chain Not Trusted

If you receive an error that indicates the certificate chain is not trusted, verify that you have the public certificate and any intermediate certificates for the root CA.

Common Name in Template

The CN in the certificate template may need to include domain information. This can be specified as ${USERNAME}@domain within Cloudpath on the specific certificate template.

SAN Other Name in Certificate Template

If the RADIUS or NPS logs show an issue with credentials, check the **SAN Other Name Pattern** in the certificate template. The variable listed in the **SAN Other Name Pattern** field should match the variable used in the **Common Name Pattern** field.

Missing EKU in the RADIUS Server Certificate

RADIUS certificates must contain Microsoft Server EKU-1.3.6.1.5.5.7.3.1. When you create the server certificate template in Cloudpath, you must check the box for the Microsoft Server EKU.

NPS-Specific Troubleshooting

For configuration details, see the *Cloudpath Integration with Microsoft NPS Configuration Guide* on the **Cloudpath Admin UI Support** tab.

If you are receiving a message that the EAP message is not available on the server, check the following configuration issues.

Register the NPS With the Domain

If the NPS is not registered to the domain, you might receive an error message that the EAP method is not available on the server.

To see if the NPS is registered with the domain, right-click the NPS server. If the server is registered, the **Register with domain** option is not available.

If there is a problem with your working registration, try deleting and re-adding the registration using the NPS **Administrator** prompt and the commands in this example:

```
net stop ias
netsh ras delete registeredserver domain=x server=y net start ias
net stop ias
netsh ras add registeredserver domain=samplecorp.local server=SAMPLE-NPS-Server net start ias
```

RADIUS Server Certificate Missing Private Key

If the RADIUS server certificate is missing the private key, you might receive an error message that the EAP Method is not available on the server, you might be missing the private key for the RADIUS server certificate.

Be sure that the RADIUS server certificate in the Local Computer Personal Certificate Store shows the 'certificate with key' icon next to it. This indicates that the certificate is signed with the private key. If it does not show the icon, you do not have the private key for the RADIUS certificate. Try downloading the RADIUS certificate and private key in P12 format.

Use the following command examples from the NPS **Administrator** prompt:

```
certutil -dspublish -f root.cer NTAuthCA
certutil -dspublish -f root.cer NTAuthCA certutil -enterprise -addstore NTAuth root.cer
```

Cloudpath Captive Portal Setup for Cisco Controller

The following example provides information about setting up a captive portal on a Cisco controller so that it automatically redirects the user to the Cloudpath webpage.

Define an ACL that allows access to the Cloudpath webpage

1. On the WLC, go to **Security** > **Access Control Lists**.

2. Add an ACL named **Unauthenticated**.

3. Add the following rules to the **Unauthenticated** ACL:

   - Sequence 1, Destination [Cloudpath IP Address], Protocol TCP, Destination Port HTTP, Action Permit

   - Sequence 2, Source [Cloudpath IP Address], Protocol TCP, Source Port HTTP, Action Permit

   - Sequence 3, Protocol UDP, Source Port DHCP Server, Action Permit

   - Sequence 4, Protocol UDP, Source Port DHCP Client, Action Permit

   - Sequence 5, Protocol UDP, Source Port DNS, Action Permit

     NOTE
     If using HTTPS, repeat sequence 1 and 2 for HTTPS.

Enable Portal Page on the Open SSID and Enforces the Preauthentication ACL

1. On the WLC, go to **WLANs** and **Edit** the open SSID.

2. Open the **Security** > **Layer 3** tabs.

3. Check the **Web Policy** box.

4. Select the **Authentication** option.

5. In the **Preauthentication ACL** field, select the open SSID.

Configure the Portal Page

1. On the WLC, go to the Security tab.

2. Open the **Web Auth** > **Web Login** Page.

3. Set **Web Authentication Type** to **Internal**.

4. Set **Cisco Logo** to **Hide**.

5. Add the following HTML to the **Message** field:

    ```
    <SCRIPT language="JavaScript"> window.location="[Cloudpath URL]";
    </SCRIPT>
    If you are not automatically redirected,
    <a href="[Cloudpath URL]">click here</a> to go to Cloudpath.
    ```

    > **NOTE**
    > The URL of the Cloudpath webpage must be populated into the HTML in the **Message** field.

6. Click **Apply** to save the changes.

7. Click **Preview** to preview the portal page. The browser should be redirected to the Cloudpath webpage.

8. Click **Save Configuration** at the top of the page.