
Ruckus
Simply Better Connections

Deploying Cloudpath for K-12

Best Practices and Design Guide

Copyright Notice and Proprietary Information

Destination Control Statement

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

Disclaimer

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

Limitation of Liability

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

Trademarks

Table of Contents

Intended Audience

This document addresses special factors and concerns related to deploying Cloudpath for K-12 environments. These environments include a large number of classroom devices that need to be onboarded simultaneously. After an initial Cloudpath deployment, possibly using our White Glove Sevice, School IT personnel may want to gradually taking more and greater advantage of Cloudpath ES's many options. Several of these are described her along configuration guidelines. The document describes what the Cloudpath ES does, and options that are particularly useful in K-12 / primary education

This document is written for and intended for use by technical engineers with a background in Wi-Fi design and 802.11/wireless engineering principles. An understanding of X.509 SSL certificates and public key infrastructure (PKI) is also highly recommended. This document covers special Cloudpath subjects, and is not an initial deployment guide. For initial deployment, the reader should see on the Ruckus Support Site:

- CP_ES 5.0 (GA) Quick Start Guide
- Cloudpath ES 5.0 (GA) Deployment Checklist
- Cloudpath ES 5.0 (GA) Deployment Guide

Best Practices & Design Guide

Configuring Cloudpath for K-12

April 2017

Overview

The Cloudpath Enrollment System (ES) is a Security and Policy Management platform that provides a single point-of-entry for devices entering the network environment. The Automated Device Enablement (ADE) approach gives network administrators control over the onboarding of new devices by blending traditional employee-centric capabilities (Active Directory, LDAP, RADIUS, and Integration with Microsoft CA) with guest-centric capabilities (sponsorship, email, SMS, Facebook, and more).
The Cloudpath ES can differentiate the devices by ownership, in addition to just device type, offering the world's first solution to extend secure Set-It-And-Forget-It-Wi-Fi™ to all users, devices, and networks without manual IT involvement.

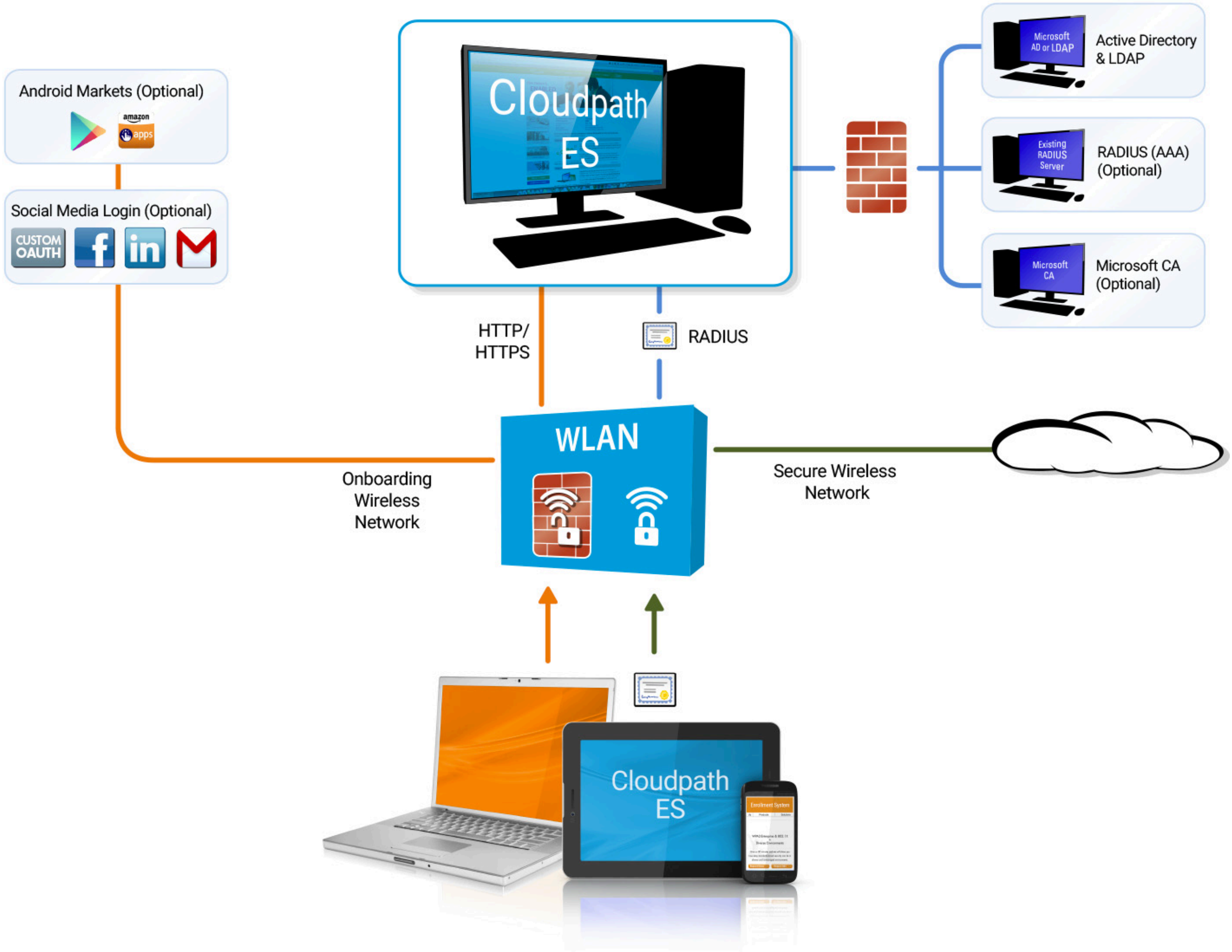


Figure 1: Cloudpath ES Deployment Example

What is the Cloudpath ES

Cloudpath Enrollment System is a security management platform with three components: Certificate Management, Policy Management, and Device Enablement. The combination of these capabilities creates a powerful new way to provision, secure and enforce policy on every device connecting to the network, through simple portal based self service for end users. Cloudpath ES is the industry's first Automated Device Enablement (ADE) solution.

Certificate Management

Cloudpath ES software includes a built-in, comprehensive Certificate Authority (CA) that enables any IT department to create and manage its own Public Key Infrastructure (PKI). A built-in RADIUS server and user database greatly simplifies installation and setup and helps in tying policies with certificates. In addition to built-in capabilities, APIs and other mechanisms enable Cloudpath software to easily integrate with existing external CA, RADIUS and user database infrastructures.

Policy Management

Cloudpath ES software provides IT with a simple, workflow-based policy management portal that can be used to establish granular policy-based access control for all users and all devices. The policy engine identifies client and user privileges and applies the correct policies to each user and each device. The software works together with policy enforcement points to ensure policies are properly exercised.

Device Enablement

Cloudpath ES software enables portal-based, self-service onboarding for end users and their devices and further enables pre-boarding for users and devices prior to their arrival at a given location. To ensure the network is properly protected, administrators can control which devices are allowed to join the network and can ensure the requisite on-device enforcement, such as enabling a firewall, installing certain applications, or updating anti-virus software.

Why Use Cloudpath?

The Cloudpath ES provides one portal for automatically onboarding and provisioning authorized devices on the secure network. The process is simple enough to be self-service by end users on an open captive portal, and automated so that the migration to the secure network can be managed without contacting the help desk. Cloudpath achieves this through the use of a dissolvable agent for the initial configuration and provisioning. Cloudpath creates a better Wi-Fi experience by simplifying the network, and implemented in your existing WLAN or wired infrastructure using standards-based security and policy mechanisms.

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 can easily view what is happening on the network.

Overall Benefits of Cloudpath

There are many configuration options and benefits that make Cloudpath a good choice in a variety of environments. These include:

- Reduce manual intervention by IT for network access and device provisioning – end password trouble tickets and end-user device configuration by IT
- Peace of mind – all users, including guests, and devices, including BYOD, are securely connected in a policy-compliant fashion. Network data is more secure because policies keep unauthorized users out
- Quick remediation – devices are associated with users, enabling identity-based policies and rapid remediation of usage violations
- Simplicity – intuitive workflows speed policy configuration. Per user licensing means there’s no need to guess device count. Price is all-inclusive. Works with the network you have
- Better end-user experience - provision and configure devices one time and one time only. Same process for all device and device types. Hassle-free roaming across campuses.

Benefits for Education

Cloudpath has specific benefits that are of interest to education environments. These include:

- Chromebook support – The K-12 market is seeing a tsunami of Chromebooks, more so than any other device. Cloudpath allows them to be configured with a click or remotely, using Google Console
- Sponsored guest access – allows authorized employees to grant network access to third parties. It is most commonly used to provide secure wireless network access to corporate visitors and partners, and is typically time-restricted. Cloudpath enables this without IT involvement while maintaining the security aspect of the solution.

- Support for headless devices - proliferation of headless devices like Apple TVs, Interactive whiteboards, printers etc pose a unique onboarding challenge that Cloudpath solves.
- Student Protection - enable a content filter (using 3rd party vendors) to filter encrypted/https content, including potentially harmful encrypted content.
- Student Typhoon – easily handle massive influxes of new devices common at the beginning of a school year. Incoming / returning students implies mass authentication, multiple, disparate devices
- Pre-boarding - incoming and returning students can "pre-board" their devices, even before they arrive on campus, further streamlining the process and easy onboarding experience
- Personal Student Network - students can easily access their own stuff as well as other data they've agreed to share. In the meantime the network much easier for IT to troubleshoot
- Eduroam-ready - all Cloudpath-secured devices are inherently Eduroam-ready.

Common Deployment Scenarios

This document discusses best practices for planning and deploying Cloudpath in K-12 environments, namely the following:

- Managed and unmanaged Chromebooks
- Sponsored guest access
- Headless devices
- Enable HTTPS inspection with a content filter

It also lists some of the additional benefits Cloudpath offers via third party vendor integration for a more integrated and complete end-to-end experience across multiple systems.

Configuration Requirements

This document requires the following:

- Cloudpath ES system (cloud or on premise) pre-configured for basic enrollment service
    - Please see the following documents on the Ruckus Support site (https://support.ruckuswireless.com/documents?filter=89#documents)
        - Cloudpath ES Deployment Checklist
        - Cloudpath ES Quick Start Guide
        - Cloudpath Es Deployment Guide
    - We offer a "White Glove Service for EDU" remote deployment assistance for initially deployment that you may wish to make use of.
- Wi-Fi network and access to the WLAN controller
- Appropriate user database
- Devices to be onboarded

Configuring Cloudpath for Chromebooks

The Cloudpath Enrollment System (ES) extends the benefits of certificates to Chromebooks with the additional security of Public Key Infrastructure (PKI). The certificate is installed in the Trusted Platform Module (TPM) of the Chromebook, and can be used for a variety of certificate-based security such as Wi-Fi (WPA2-Enterprise with EAP-TLS), web SSO authentication, web two-factor authentication and more. Cloudpath can automatically distribute user and device certificates to both IT-managed and unmanaged (BYOD) Chromebooks.

- For IT-managed Chromebooks, Cloudpath deploys both user and device certificates via a Chrome extension provisioned through the Chromebook management console. Whether tied to the user or the device, the certificates are TPM-backed, which means they are burned into hardware for maximum protection
- For unmanaged Chromebooks, Cloudpath provides a web portal for self-service and automated installation of the certificate and configuration of related services such as WPA2-Enterprise Wi-Fi with EAP-TLS
- Whether your network supports IT-managed or unmanaged Chromebook devices (or both), Cloudpath provides a secure method for Automatic Device Enablement. Cloudpath can differentiate the devices on your network by ownership, not just device type, offering the world's first solution to extend secure Set-It-And-Forget-It Wi-Fi to all users, devices and networks without IT involvement

Supported Devices

Cloudpath supports all Chrome OS devices supported by Google. To see a list of devices currently supported by Google, please consult the following URLs:

https://www.google.com/chrome/devices/eol.html

Configuration Requirements

Configuring Cloudpath to support Chromebooks requires the following:

- Google Console Integration
- User Or Device Certificates - support Installation Into the TPM of both user and device certificates. Certificates may be tied to the user, the device, or user+device
- User, IT, or distributor provisioned
- Built-In Cloudpath PKI or Microsoft CA -dDistribute Certificates From the Built-In PKI or Microsoft CA

Procedure Overview

To create a Chromebook configuration in the Cloudpath ES, enable the OS on the Cloudpath Admin UI and configure the user experience appropriate for your network. During user enrollment, if the Chrome OS is detected, the ES displays Chrome OS-specific instructions for downloading the configuration file and installing it on the device, or if extensions are configured, the certificate and Wi-Fi settings are installed in the TPM.

The basic procedure to configure Cloudpath for Chromebook support is as follows:

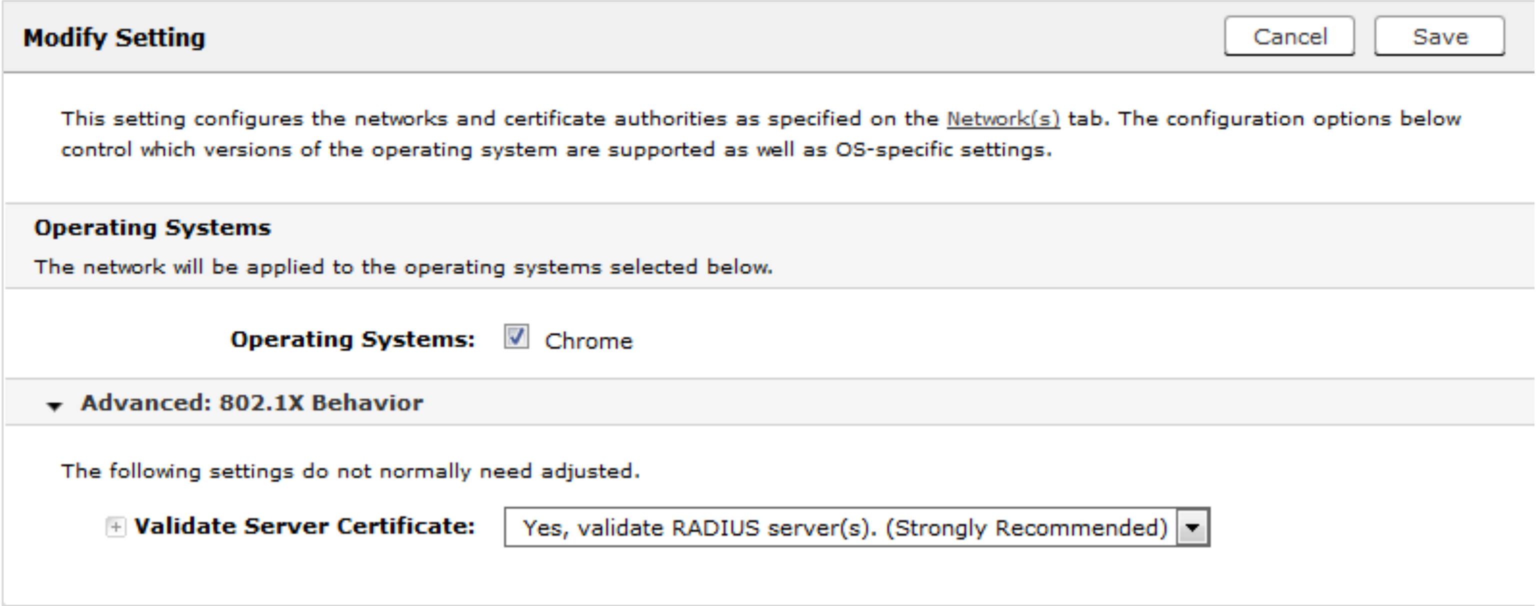
1. Enable Chrome OS device configuration for your workflow
2. Configure the Chromebook User Experience
3. Configure the Cloudpath Enrollment Workflow

Step 1: Enable Chrome OS Devices for Your Cloudpath Workflow

Each workflow in Cloudpath is configured for a specific set of devices and operating systems. The Chrome operating is enabled by default. If it is not, use the following steps to enable Chrome OS device configuration.

1. On the Cloudpath Admin UI, go to Configuration > Advanced > Device Configurations

2. Select the device configuration to support the Chrome OS
3. On the OS-Specific Settings page, edit the Chrome: User experience options



This setting configures the networks and certificate authorities as specified on the Network(s) tab. The configuration options below control which versions of the operating system are supported as well as OS-specific settings.

Operating Systems

The network will be applied to the operating systems selected below.

Operating Systems: ☑ Chrome

Advanced: 802.1X Behavior

The following settings do not normally need adjusted.

Validate Server Certificate: Yes, validate RADIUS server(s). (Strongly Recommended)

FIGURE 2: ENABLE CHROME OS DEVICE MANAGEMENT

4. Select Operating System: Chrome
5. Leave the default settings for Validate Server Certificate
6. Click Save to save your work

Step 2: Configure the Chromebook User Experience

The Chromebook user experience can be configured for managed (school owned) or unmanaged (student owned) Chromebooks

Unmanaged Devices

For unmanaged devices, the user downloads the ONC configuration file. This contains the X.509 SSL certificate and Wi-Fi settings required to connect to the secure network. It is similar in functionality to the mobileconfig file used by Mac OS X and iOS devices.

Managed Devices

For managed devices, the Cloudpath extension is used. This is configured in the Chrome Management Console. The extension installs the X.509 SSL certificate and settings into the TPM as the user or as the device.

After the configuration file is installed (manually, or using the extension), the user simply connects the secure network.

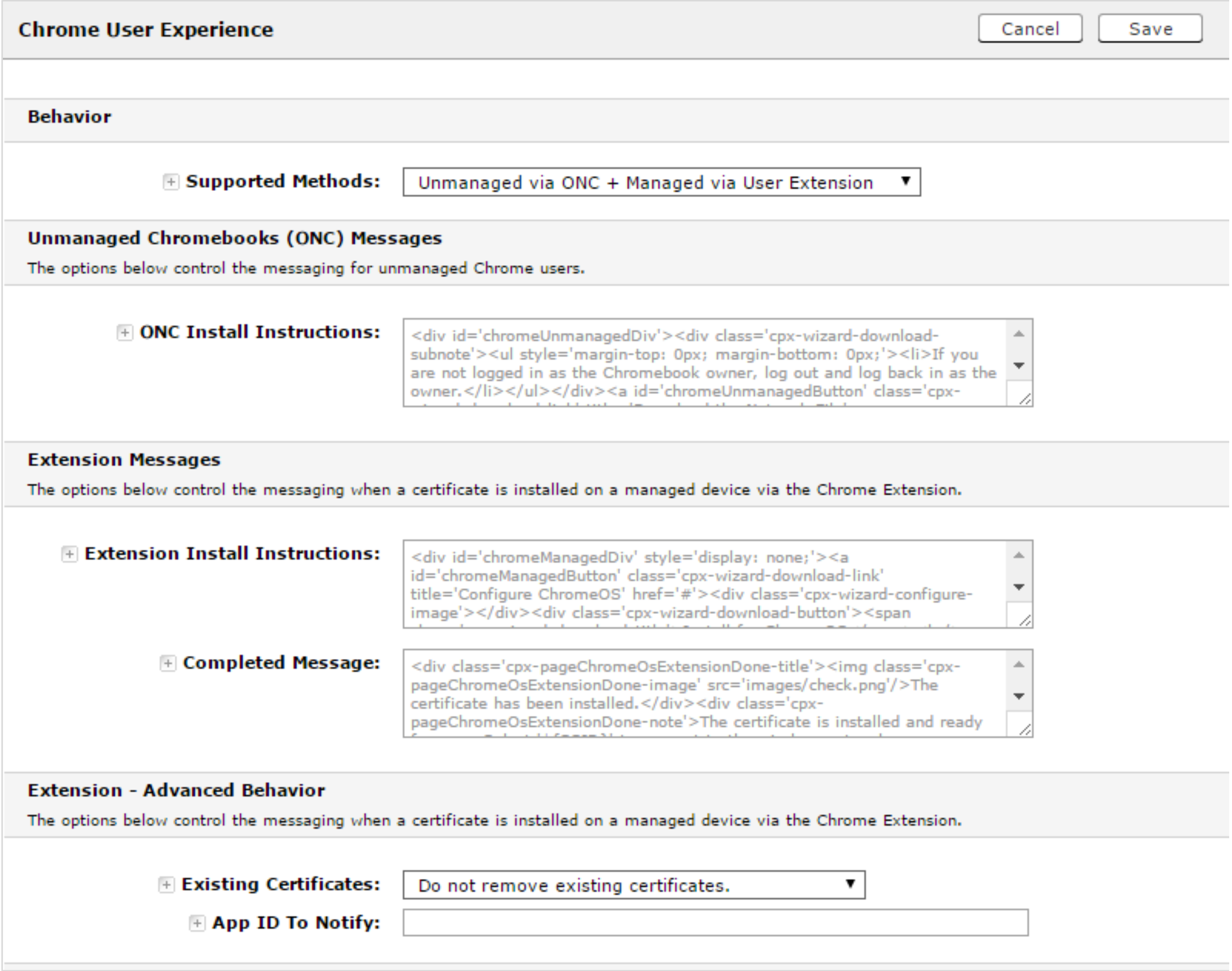
User Experience Settings

Cloudpath provides the prompts that guide the user through the sequence of steps that make up the enrollment workflow. During this process, the user enters information as requested, and makes selections about user type, device type, among others. The sequences of steps for the enrollment differ, depending on the selections that are made.

To configure the Chromebook user experience:

1. Log into the Cloudpath Admin Console
2. Go to Configuration > Advanced > Device Configuration
3. Select the OS Settings tab for the appropriate device configuration

4. Edit the Chrome: User experience options



Chrome User Experience

Behavior

Supported Methods: Unmanaged via ONC + Managed via User Extension

Unmanaged Chromebooks (ONC) Messages

The options below control the messaging for unmanaged Chrome users.

ONC Install Instructions:

```
<div id='chromeUnmanagedDiv'><div class='cpx-wizard-download-
subnote'><ul style='margin-top: 0px; margin-bottom: 0px;'><li>If you
are not logged in as the Chromebook owner, log out and log back in as the
owner.</li></ul></div><a id='chromeUnmanagedButton' class='cpx-
```

Extension Messages

The options below control the messaging when a certificate is installed on a managed device via the Chrome Extension.

Extension Install Instructions:

```
<div id='chromeManagedDiv' style='display: none;'><a
id='chromeManagedButton' class='cpx-wizard-download-link'
title='Configure ChromeOS' href='#'><div class='cpx-wizard-configure-
image'></div><div class='cpx-wizard-download-button'><span
```

Completed Message:

```
<div class='cpx-pageChromeOsExtensionDone-title'><img class='cpx-
pageChromeOsExtensionDone-image' src='images/check.png'/>The
certificate has been installed.</div><div class='cpx-
pageChromeOsExtensionDone-note'>The certificate is installed and ready
```

Extension - Advanced Behavior

The options below control the messaging when a certificate is installed on a managed device via the Chrome Extension.

Existing Certificates: Do not remove existing certificates.

App ID To Notify:

FIGURE 3: USER EXPERIENCE SETTINGS

5. Select the Behavior settings for the device configuration.
   - The Supported Method setting controls the installation methods available to end-users. By default, installation is handled using an ONC file, which can be used by both unmanaged and managed devices.
     - ONC Only - Allows installation using the ONC file only.
     - ONC + User Extension - Allows installation using the ONC file or Chrome extension. If the extension is used, the certificate is installed as the user.
     - ONC + Device Extension - Allows installation using the ONC file or Chrome extension. If the extension is used, the certificate is installed as the device.
     - User Extension Only - Allows installation to the user TPM using only the Chrome extension.
     - Device Extension Only - Allows installation to the device TPM using only the Chrome extension.

- The ONC Install Instructions contain the instructions displayed to the user if the ONC file is used to install the certificate and Wi-Fi settings. This occurs if ONC Only is enabled or if ONC + (User or Device) Extension is enabled, but the user does not have the extension installed.

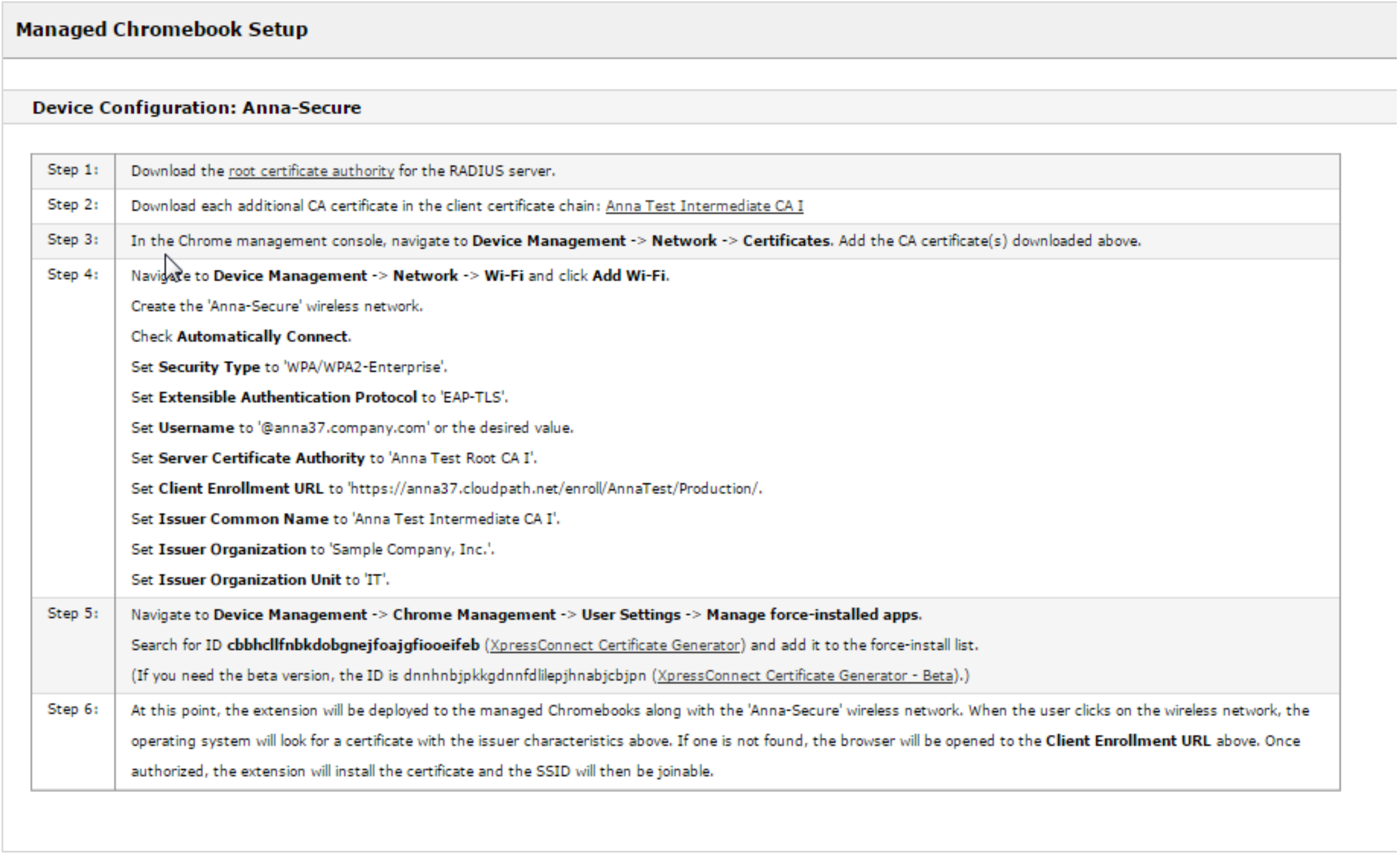
6. Configure Extension Messages.
    - The Extension Install Instructions are displayed to the user if an extension is used to install the certificate on the device.
    - After the certificate has been successfully installed using the extension, the Completed Message appears.
7. Configure ONC Messages.
    - The App ID to Notify notifies an app when the certificate installation is complete. This can be useful if an app is managing the enrollment process for the user.
    - If using extensions, you can specify that the extension remove existing certificates from the certificate manager. This can be useful in cleaning up the device.
8. Save the configuration settings. If the active workflow in Cloudpath supports the Chromebook OS with extensions, the Explain Chrome Setup button displays Chromebook setup instructions on the Configuration > Deploy page.

Download the Root CA

The Chrome extension (Cloudpath Certificate Generator) installs the root CA certificate (and any additional CAs) into the TPM as the user or as the device, depending on the Chrome OS configuration in Cloudpath. Use the link in Step 1 of the Managed Chromebook Setup page to download the root CA. This certificate will be imported into the Chrome management console later in this configuration process.

Download Additional CAs

If you have additional CAs configured (in the Cloudpath Admin UI, see the Trusted RADIUS chain in the device configuration network settings), use the link in Step 2 to download the additional CAs.



Managed Chromebook Setup

Device Configuration: Anna-Secure

Step 1:	Download the root certificate authority for the RADIUS server.
Step 2:	Download each additional CA certificate in the client certificate chain: Anna Test Intermediate CA I
Step 3:	In the Chrome management console, navigate to **Device Management** -> **Network** -> **Certificates**. Add the CA certificate(s) downloaded above.
Step 4:	Navigate to **Device Management** -> **Network** -> **Wi-Fi** and click **Add Wi-Fi**. Create the 'Anna-Secure' wireless network. Check **Automatically Connect**. Set **Security Type** to 'WPA/WPA2-Enterprise'. Set **Extensible Authentication Protocol** to 'EAP-TLS'. Set **Username** to '@anna37.company.com' or the desired value. Set **Server Certificate Authority** to 'Anna Test Root CA I'. Set **Client Enrollment URL** to 'https://anna37.cloudpath.net/enroll/AnnaTest/Production/. Set **Issuer Common Name** to 'Anna Test Intermediate CA I'. Set **Issuer Organization** to 'Sample Company, Inc.'. Set **Issuer Organization Unit** to 'IT'.
Step 5:	Navigate to **Device Management** -> **Chrome Management** -> **User Settings** -> **Manage force-installed apps**. Search for ID **cbbhcllfnbkdobgnejfoajgfiooeifeb** (XpressConnect Certificate Generator) and add it to the force-install list. (If you need the beta version, the ID is dnnhnbjpkkgdnnfdlilepjhnabjcbjpn (XpressConnect Certificate Generator - Beta).)
Step 6:	At this point, the extension will be deployed to the managed Chromebooks along with the 'Anna-Secure' wireless network. When the user clicks on the wireless network, the operating system will look for a certificate with the issuer characteristics above. If one is not found, the browser will be opened to the **Client Enrollment URL** above. Once authorized, the extension will install the certificate and the SSID will then be joinable.

FIGURE 4: MANAGED CHROMEBOOK SETUP INSTRUCTIONS

Configuring the Chrome Extension in the Chrome Management Console

Cloudpath provides all of the information you need to set up the Chrome extension, which is used to install the certificate and Wi-Fi settings on IT managed Chromebook devices. After configuring the Chrome OS settings in Cloudpath, move on to the Chrome management console to set up the extension.

Chrome Admin Console Settings

The web-based management console for the Chrome OS allows you to centrally configure network settings for users and extensions for your managed Chromebooks devices. The Admin Console > Device Management is the portal for configuring Wi-Fi and network settings for the user. Configured Wi-Fi and Certificates on the Networks page. Configure force-installed apps on the Chrome Management page.

The following steps are required to configure a device through the Chrome Admin Console:

1. Import any required certificates
2. Configure Wi-Fi settings
3. Configure policies for users

Import Certificates

Use the following steps to upload all required certificates:

1. Log into the Chrome management console at https://admin.google.com

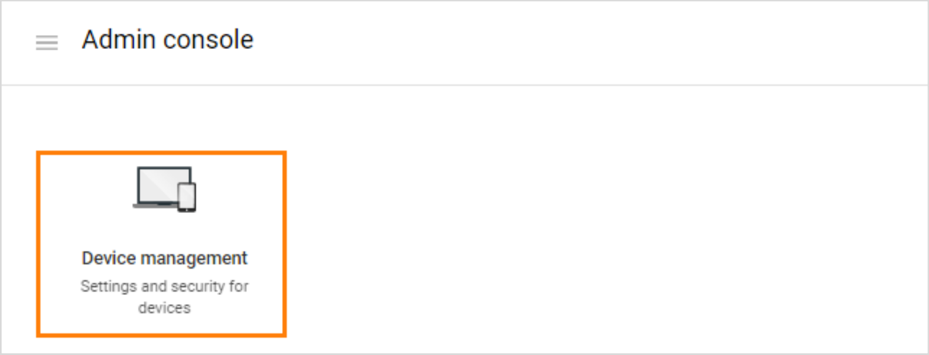


FIGURE 5: CHROME ADMIN CONSOLE

2. Select Device Management.

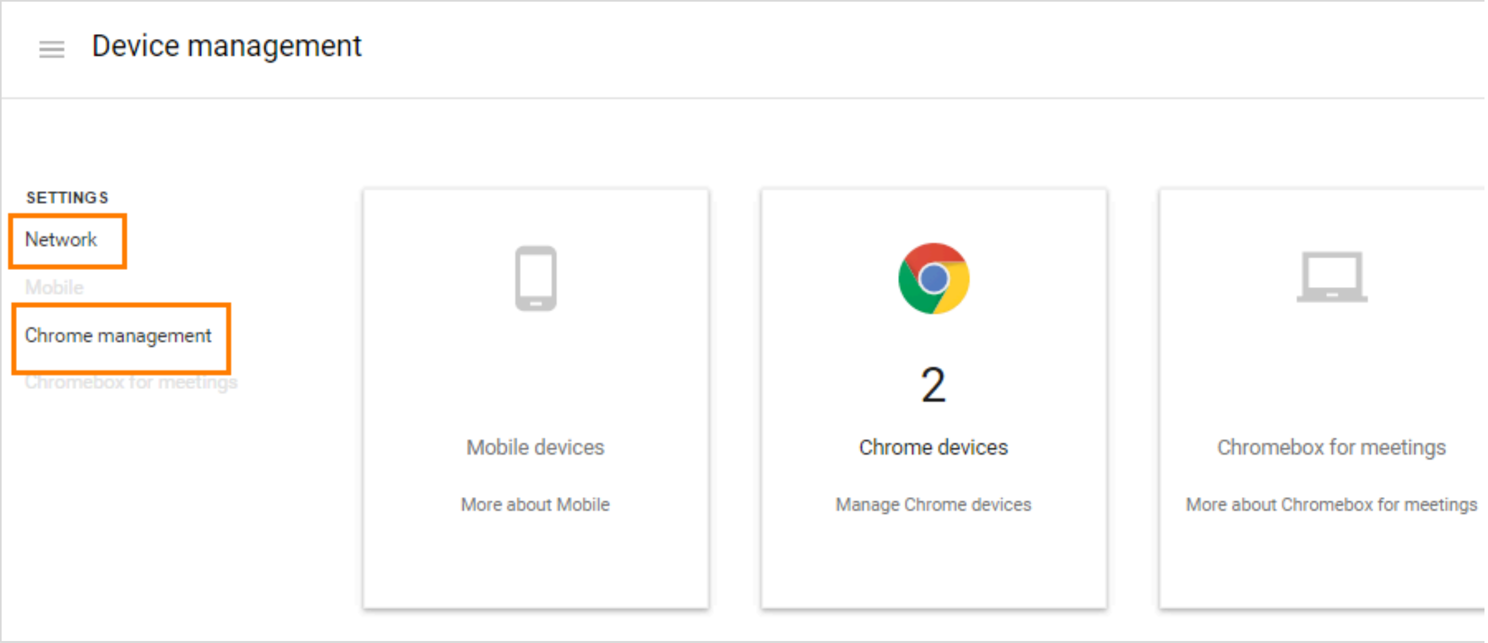
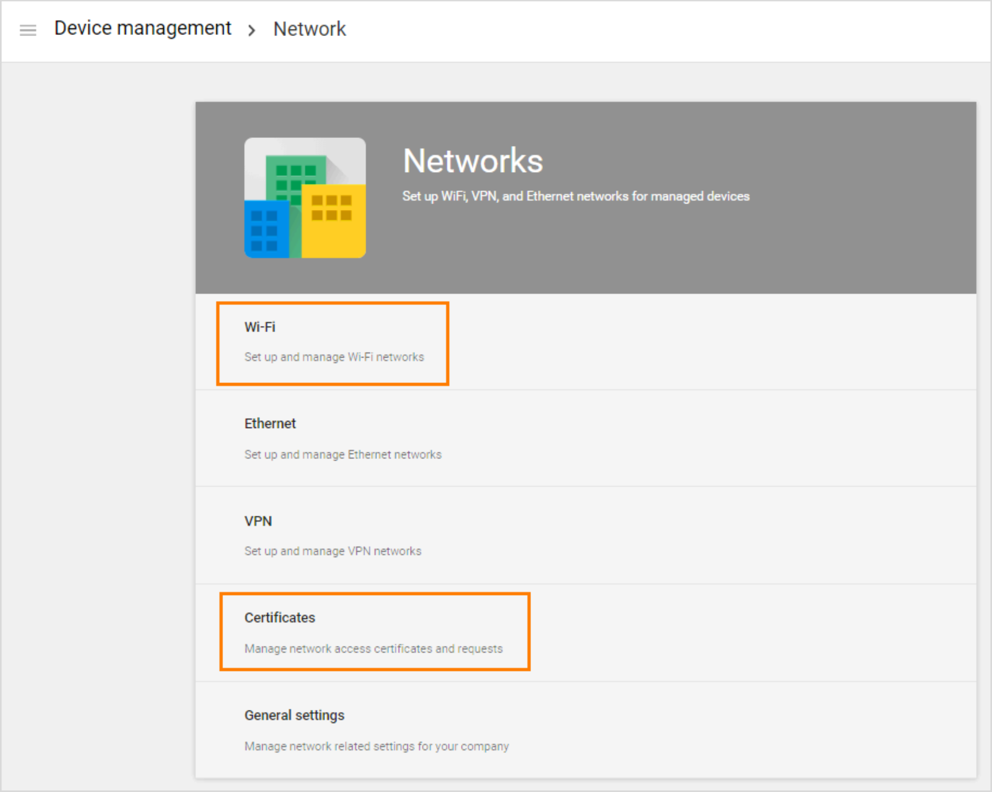


FIGURE 6: DEVICE MANAGEMENT

3. Click the Network link to set up Wi-Fi and Certificates for managed devices. Use the Chrome management link to set up Wi-Fi and Certificates for managed devices.
4. Navigate to the Networks page to import the CA certificate and configure the Wi-Fi settings, which will be dispersed to users or devices through the Chrome extension



Device management > Network

Networks

Set up WiFi, VPN, and Ethernet networks for managed devices

Wi-Fi

Set up and manage Wi-Fi networks

Ethernet

Set up and manage Ethernet networks

VPN

Set up and manage VPN networks

Certificates

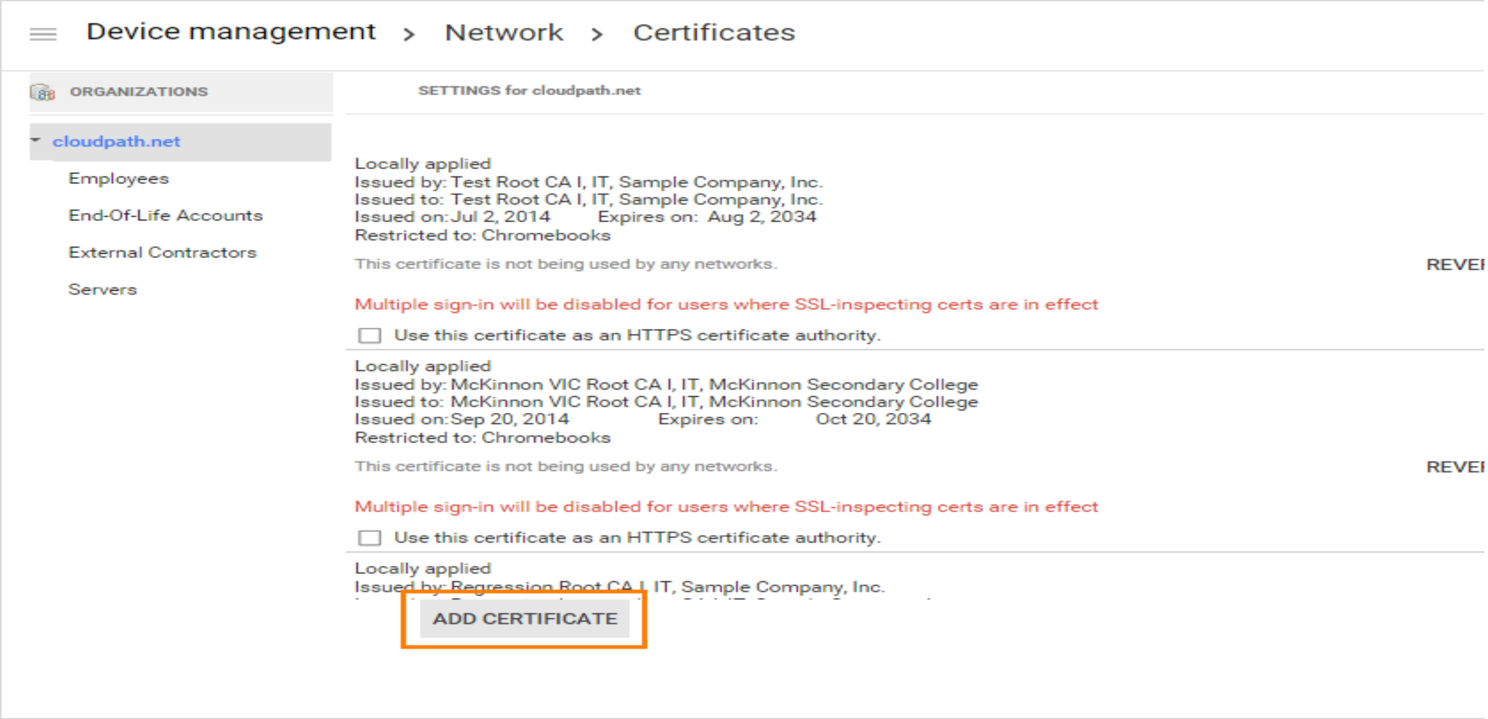
Manage network access certificates and requests

General settings

Manage network related settings for your company

FIGURE 7: NETWORK SETTINGS

5. Click the Networks > Certificates link to import the CA certificate.
6. On the left side, select the organization for which you want to import the certificate, or if you don't select an organization, the certificate settings apply to all organizations and groups.
7. Click Add Certificate.
8. Locate and import the root CA certificate that was downloaded from the Chrome Setup
9. If your Cloudpath configuration contains additional CAs, you must also import the additional CAs.
10. When the certificates have been successfully uploaded, return to the Networks page to configure Wi-Fi settings.



Locally applied
Issued by: Test Root CA I, IT, Sample Company, Inc.
Issued to: Test Root CA I, IT, Sample Company, Inc.
Issued on: Jul 2, 2014 Expires on: Aug 2, 2034
Restricted to: Chromebooks

This certificate is not being used by any networks.

REVEI

Multiple sign-in will be disabled for users where SSL-inspecting certs are in effect

□ Use this certificate as an HTTPS certificate authority.

Locally applied
Issued by: McKinnon VIC Root CA I, IT, McKinnon Secondary College
Issued to: McKinnon VIC Root CA I, IT, McKinnon Secondary College
Issued on: Sep 20, 2014 Expires on: Oct 20, 2034
Restricted to: Chromebooks

This certificate is not being used by any networks.

REVEI

Multiple sign-in will be disabled for users where SSL-inspecting certs are in effect

□ Use this certificate as an HTTPS certificate authority.

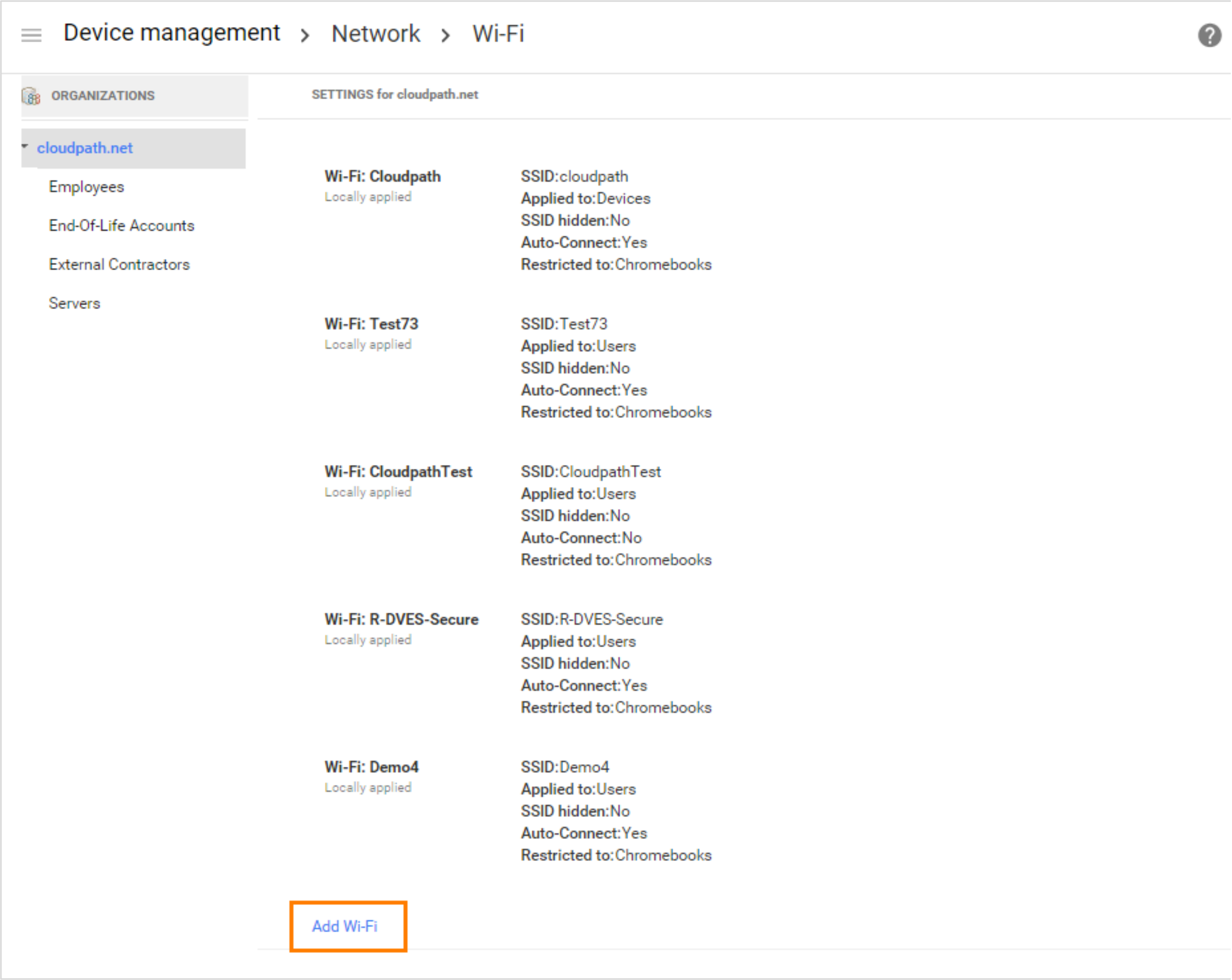
Locally applied
Issued by: Regression Root CA I, IT, Sample Company, Inc.

FIGURE 8: MANAGE CERTIFICATES

Configure Wi-Fi Settings

Configure Wi-Fi settings for the managed Chrome devices enrolled in your domain, or for logged-in users from specific sub-organizations within your domain.

1. Return to the Networks page and click the Networks >Wi-Fi link. On the left side, select the organization for which you want to import the certificate, or if you don't select an organization, the certificate settings apply to all organizations and groups



Wi-Fi: Cloudpath
Locally applied
SSID:cloudpath
Applied to:Devices
SSID hidden:No
Auto-Connect:Yes
Restricted to:Chromebooks

Wi-Fi: Test73
Locally applied
SSID:Test73
Applied to:Users
SSID hidden:No
Auto-Connect:Yes
Restricted to:Chromebooks

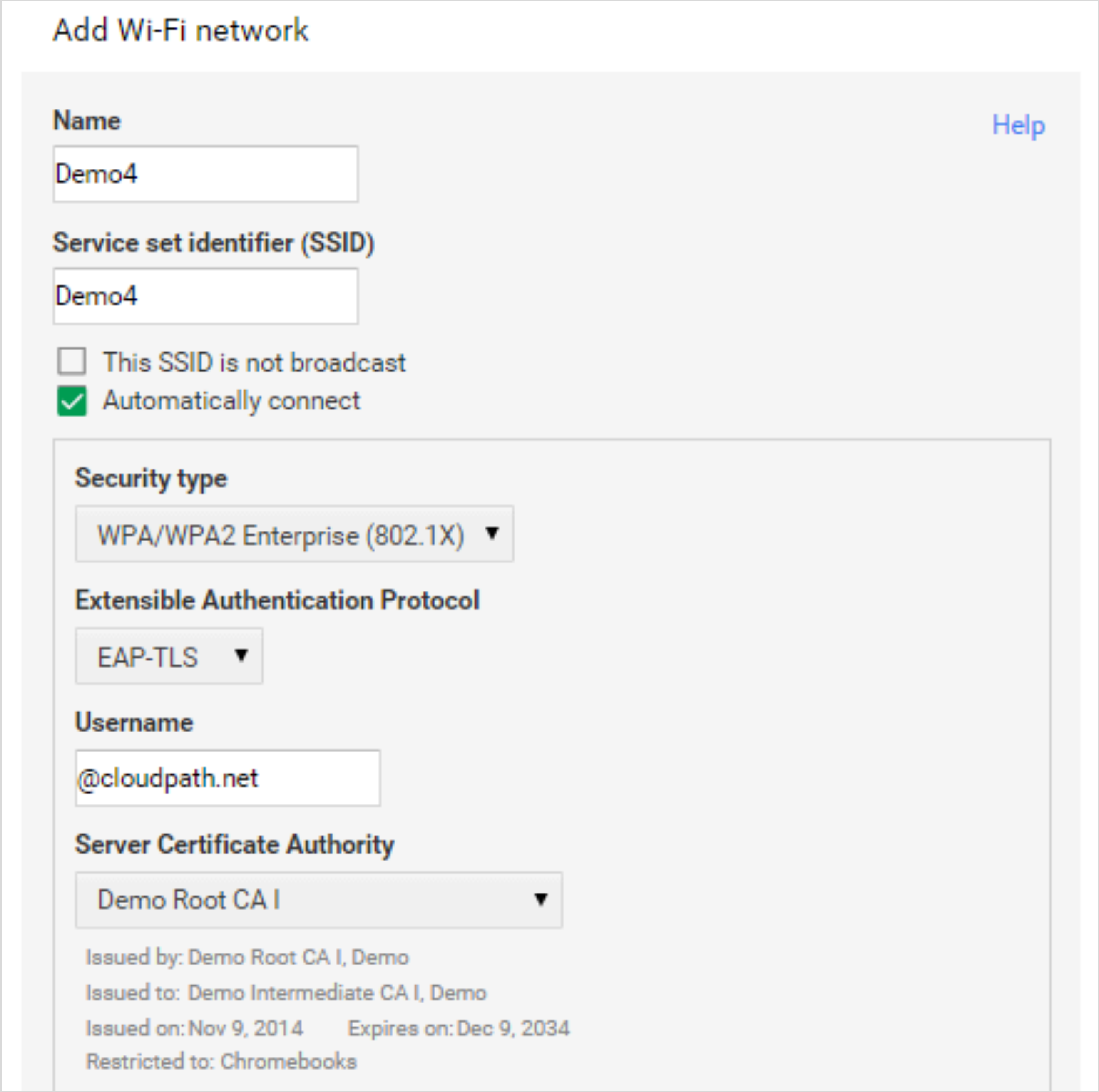
Wi-Fi: CloudpathTest
Locally applied
SSID:CloudpathTest
Applied to:Users
SSID hidden:No
Auto-Connect:No
Restricted to:Chromebooks

Wi-Fi: R-DVES-Secure
Locally applied
SSID:R-DVES-Secure
Applied to:Users
SSID hidden:No
Auto-Connect:Yes
Restricted to:Chromebooks

Wi-Fi: Demo4
Locally applied
SSID:Demo4
Applied to:Users
SSID hidden:No
Auto-Connect:Yes
Restricted to:Chromebooks

FIGURE 9: WI-FI NETWORKS

2. Click Add Wi-Fi. The Add Wi-Fi page displays.



Add Wi-Fi network

Name

Demo4

Service set identifier (SSID)

Demo4

☐ This SSID is not broadcast
☑ Automatically connect

Security type

WPA/WPA2 Enterprise (802.1X) ▼

Extensible Authentication Protocol

EAP-TLS ▼

Username

@cloudpath.net

Server Certificate Authority

Demo Root CA I ▼

Issued by: Demo Root CA I, Demo
Issued to: Demo Intermediate CA I, Demo
Issued on: Nov 9, 2014 Expires on: Dec 9, 2034
Restricted to: Chromebooks

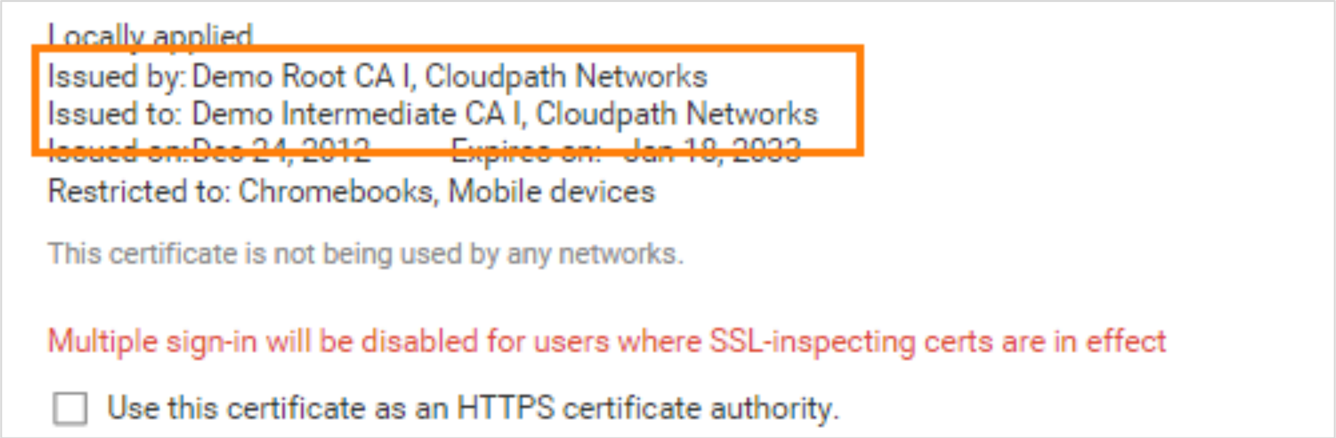
FIGURE 10: WI-FI SETTINGS

3. Enter the Wi-Fi data according to step 3 in the Chromebook setup instructions (Managed Devices). The Name and SSID do not need to match.

- Typically the SSID is broadcast
- Automatically connect is optional.
- Security type must be WPA/WPA2 Enterprise (802.1x).
- EAP type must be EAP-TLS.
- The Username must be populated. Typically, the value for this field is <user>@<domain>, but @<domain> also works.

4. Select the Root CA listed in the setup instructions (see Managed Chromebook Setup Instructions). When selecting the Server Certificate Authority, be sure to select the certificate that contains both the root and intermediate certificates
5. Enter the Client enrollment URL that is listed on the Chromebook setup instructions (see Managed Chromebook Setup Instructions)

6. Enter the Issuer pattern fields as directed by the Managed Chromebook Setup instructions. Common Name is a required field
7. Apply network by user



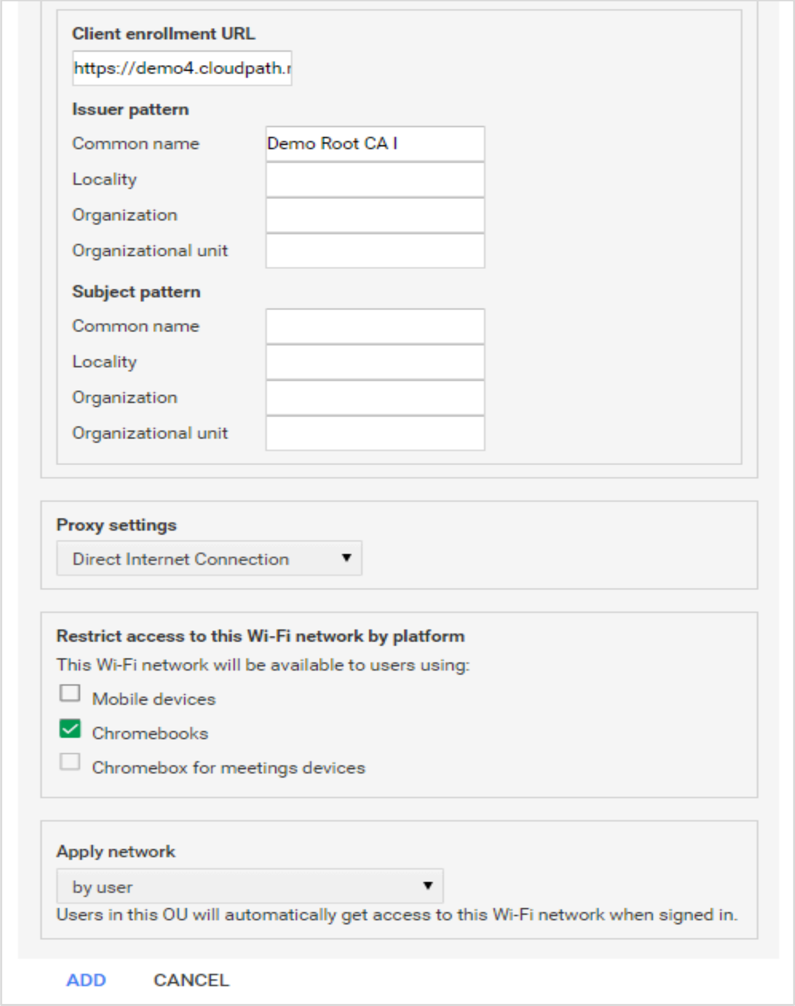
Locally applied
Issued by: Demo Root CA I, Cloudpath Networks
Issued to: Demo Intermediate CA I, Cloudpath Networks
Issued on: Dec 24, 2012 Expires on: Jan 18, 2033
Restricted to: Chromebooks, Mobile devices

This certificate is not being used by any networks.

Multiple sign-in will be disabled for users where SSL-inspecting certs are in effect

□ Use this certificate as an HTTPS certificate authority.

FIGURE 11: IMPORTED ROOT CA WITH INTERMEDIATE CA



Client enrollment URL
https://demo4.cloudpath.r

Issuer pattern

Common name	Demo Root CA I
Locality	
Organization	
Organizational unit	

Subject pattern

Common name	
Locality	
Organization	
Organizational unit	

Proxy settings
Direct Internet Connection ▾

Restrict access to this Wi-Fi network by platform
This Wi-Fi network will be available to users using:
□ Mobile devices
☑ Chromebooks
□ Chromebox for meetings devices

Apply network
by user ▾
Users in this OU will automatically get access to this Wi-Fi network when signed in.

FIGURE 12: WI-FI SETUP CONTINUED

8. Click Add to add the Wi-Fi configuration for the organization
9. Return to the Device Management page to configure the force-install for the Cloudpath Certificate Generator

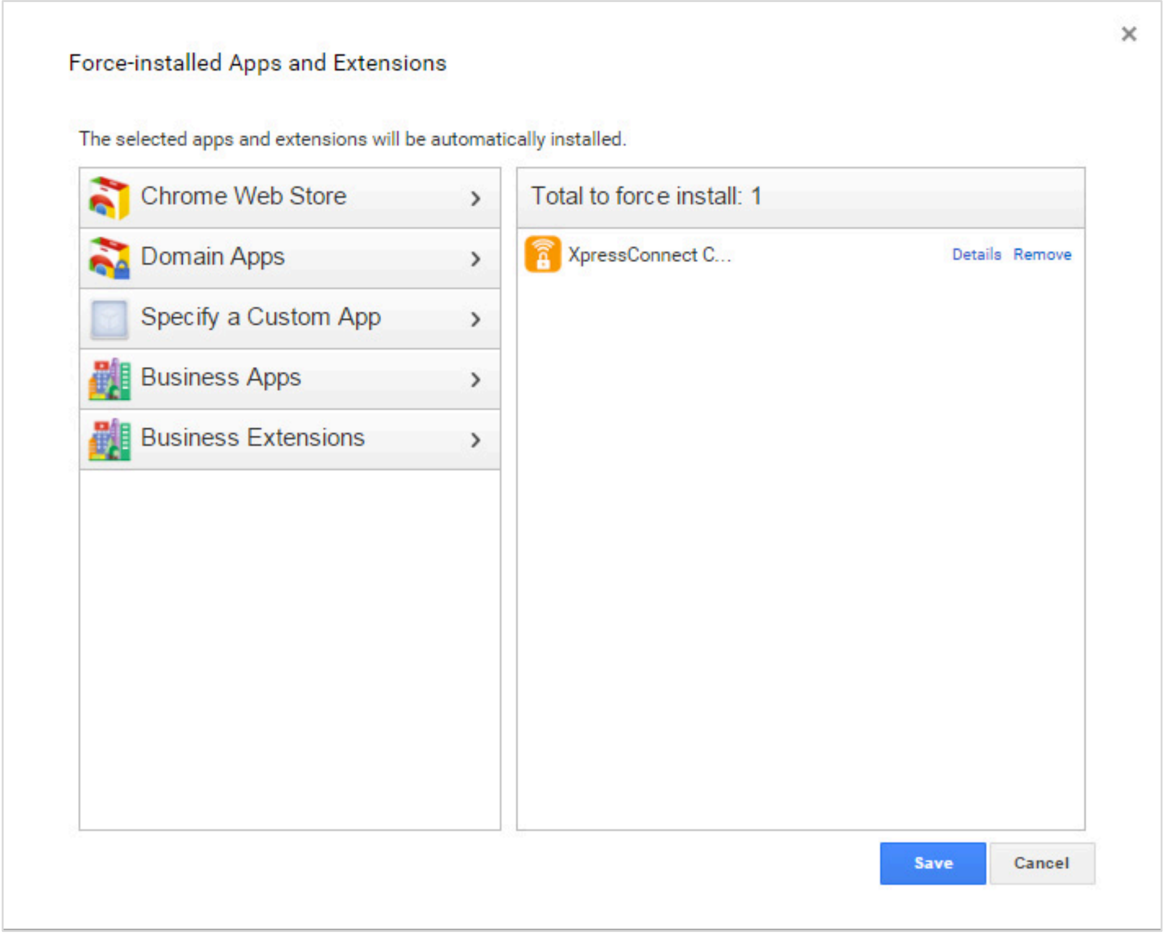
Configure Policies for Device Users

The Cloudpath Certificate Generator must be added to the "Force-installed Apps and Extensions." Configure policies for Chrome device users within a school, and configure the policy for the Cloudpath extension in the Apps and Extensions section.

> **Force-installed Apps:** You can force installation of specified apps on managed Chrome devices so that they see the apps from their apps list when they're signed in to their Chrome devices.

Configure Force Install Apps in User Settings

1. Navigate to Device Management > Chrome Management, and select User Settings
2. Scroll down to the Apps and Extensions section
3. Click Manage force-installed apps



Force-installed Apps and Extensions

The selected apps and extensions will be automatically installed.

Total to force install: 1

XpressConnect C...

FIGURE 13: FORCE INSTALLED APPS & EXTENSIONS

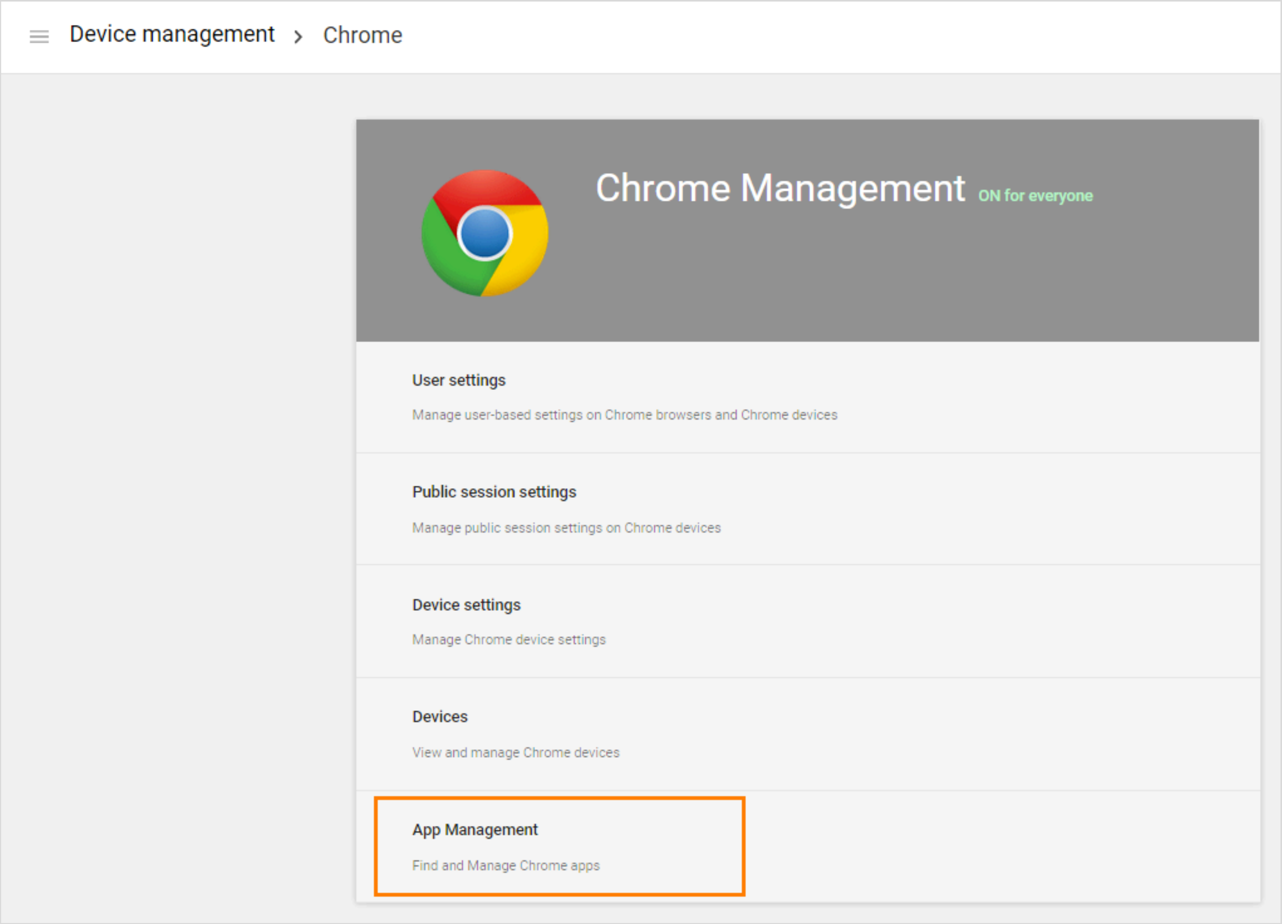
4. The left side lists the available apps and extensions, and the right side lists the apps and extensions to install on the managed devices
5. for this network. Search for the Cloudpath Certificate Generator and add it to the force-install list. The extension is installed on the user device according to the Chrome OS user experience Behavior setting in Cloudpath.

Force-install Unlisted Apps (beta)

If you have an application that is unlisted, you must load it as a custom application.

Configure Force Install Unlisted Apps in User Settings

10. Navigate to Device Management > Chrome > App Management



Device management › Chrome

Chrome Management ON for everyone

User settings
Manage user-based settings on Chrome browsers and Chrome devices

Public session settings
Manage public session settings on Chrome devices

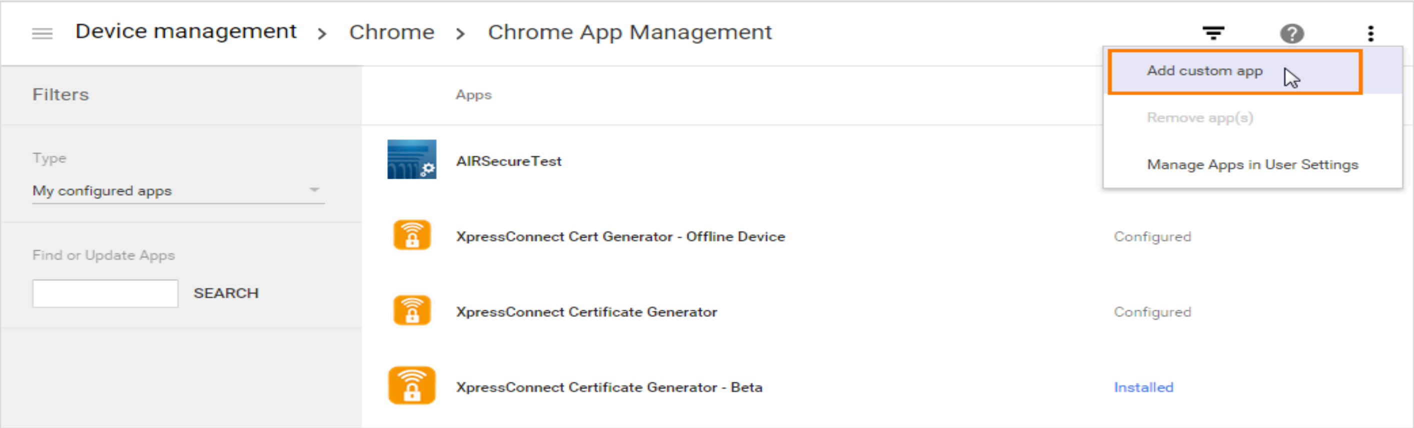
Device settings
Manage Chrome device settings

Devices
View and manage Chrome devices

App Management
Find and Manage Chrome apps

FIGURE 14: CHROME APP MANAGEMENT

11. From the top-right Settings menu, select Add Custom App



Device management › Chrome › Chrome App Management

Filters

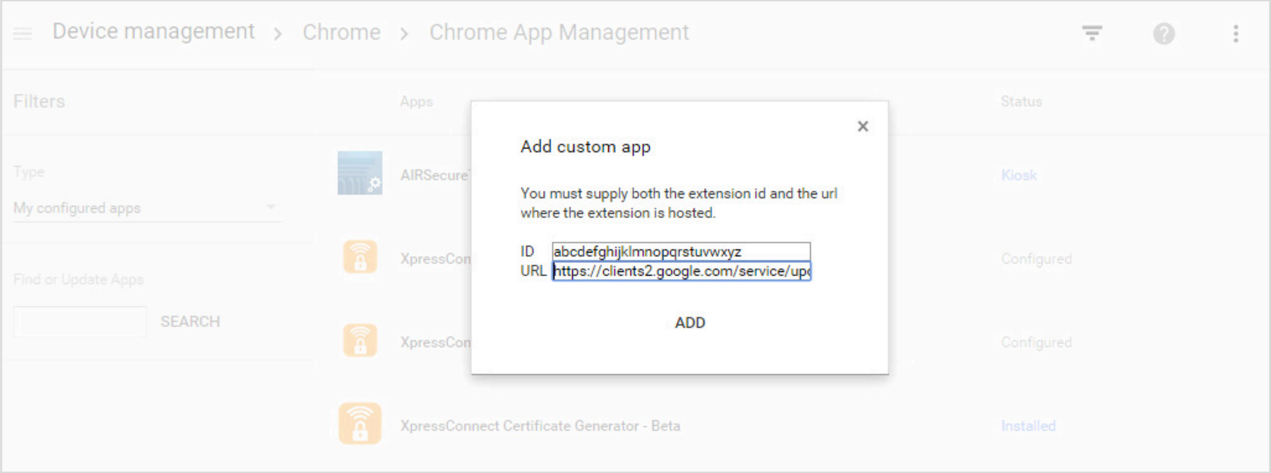
Type
My configured apps

Find or Update Apps
SEARCH

Apps	
AIRSecureTest	
XpressConnect Cert Generator - Offline Device	Configured
XpressConnect Certificate Generator	Configured
XpressConnect Certificate Generator - Beta	Installed

FIGURE 15: ADD A CUSTOM APP

12. Enter the App ID and URL



Add custom app

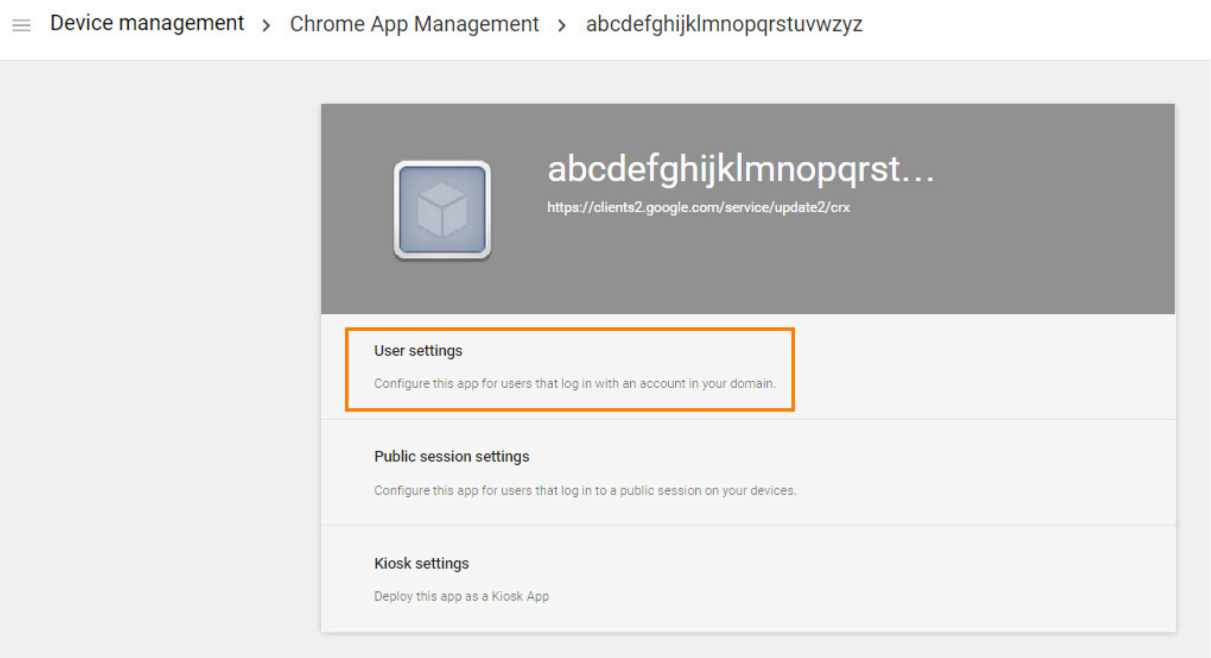
You must supply both the extension id and the url where the extension is hosted.

ID abcdefghijklmnopqrstuvwxyz
URL https://clients2.google.com/service/upd

ADD

FIGURE 16: CONFIGURE CUSTOM APP PARAMETERS

13. After the app is created, configure the settings for users that log in with an account in your domain.
14. Select User settings


Device management > Chrome App Management > abcdefghijklmnopqrstuvwzyz
abcdefghijklmnopqrst…
https://clients2.google.com/service/update2/crx

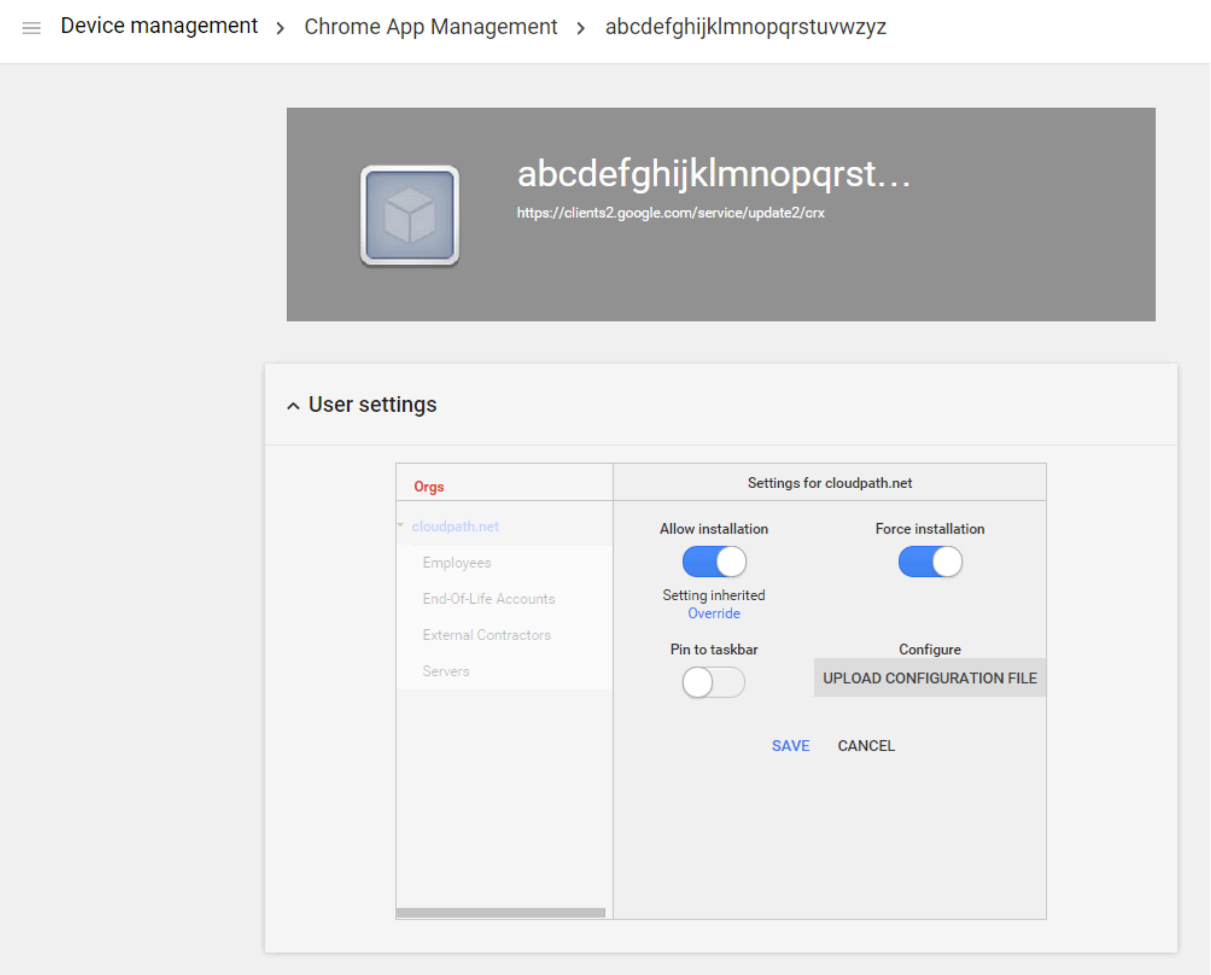
User settings
Configure this app for users that log in with an account in your domain.

Public session settings
Configure this app for users that log in to a public session on your devices.

Kiosk settings
Deploy this app as a Kiosk App

FIGURE 17: CUSTOM APP USER SETTINGS

15. On the User settings page for your application, select an organization under Orgs in the left pane



Device management › Chrome App Management › abcdefghijklmnopqrstuvwzyz

abcdefghijklmnopqrst...
https://clients2.google.com/service/update2/crx

User settings

Orgs
- cloudpath.net
  - Employees
  - End-Of-Life Accounts
  - External Contractors
  - Servers

Settings for cloudpath.net

Allow installation: on
Setting inherited
Override

Force installation: on

Pin to taskbar: off

Configure
UPLOAD CONFIGURATION FILE

SAVE CANCEL

FIGURE 18: CONFIGURE CUSTOM APP

16. In the right pane, enable Force installation
17. Save the configuration
18. The unlisted application can now be added as a Force-install app

Step 3: Enable Chrome OS Devices for Your Cloudpath Workflow

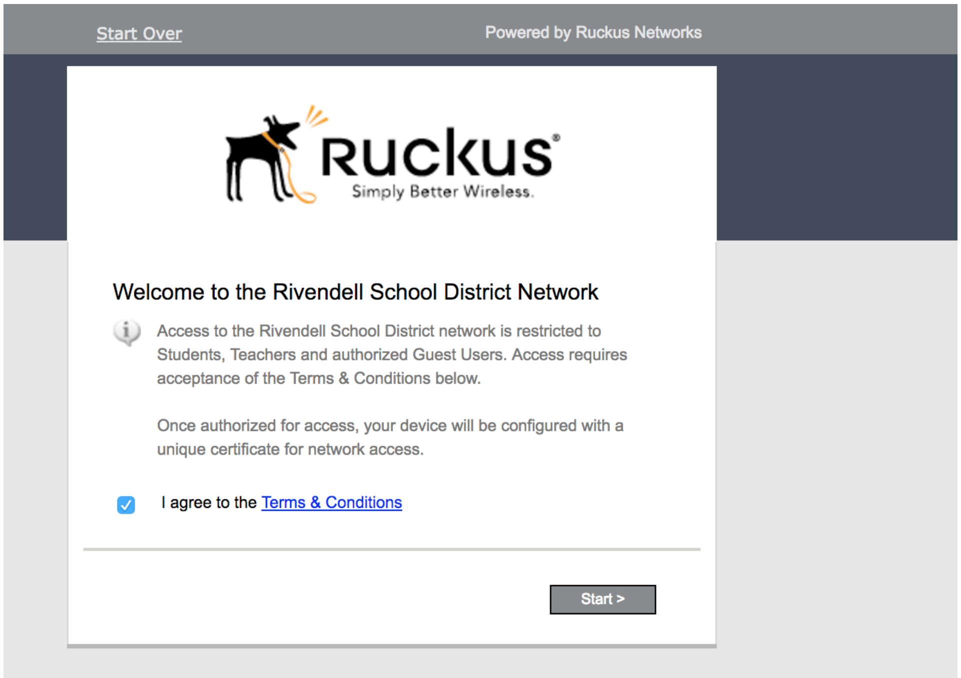
Cloudpath provides the prompts that guide the user through the sequence of steps that make up the enrollment workflow. During this process, the user enters information as requested, and makes selections about user type, device type, among others. The sequence of steps for the enrollment differs, depending on the selection that is made.

Enrollment Workflow

During enrollment, the Chrome OS is detected and Cloudpath provides Chrome OS-specific instructions for downloading the configuration file and installing it on the device manually, or automatically if extensions are configured. After the configuration file is installed, the Chromebook automatically connects to the secure network.

The following section provides an example of the one time Chromebook enrollment user experience for student owned or unmanaged devices and district owned managed devices. The exact sequence of steps for the enrollment differs, depending on the selections administrators have made. That is, the enrollment workflow will branch, and an IT person setting up a managed device will follow a slightly different path than an unmanaged student owned device.

1. The user connects to the deployment URL (either directly, or through a Captive Portal)
2. The Cloudpath Welcome screen displays. The login screen can be customized with the logo, colors, and text for the organization or institution. The screens in this example use the default look and feel of the application.



Welcome to the Rivendell School District Network

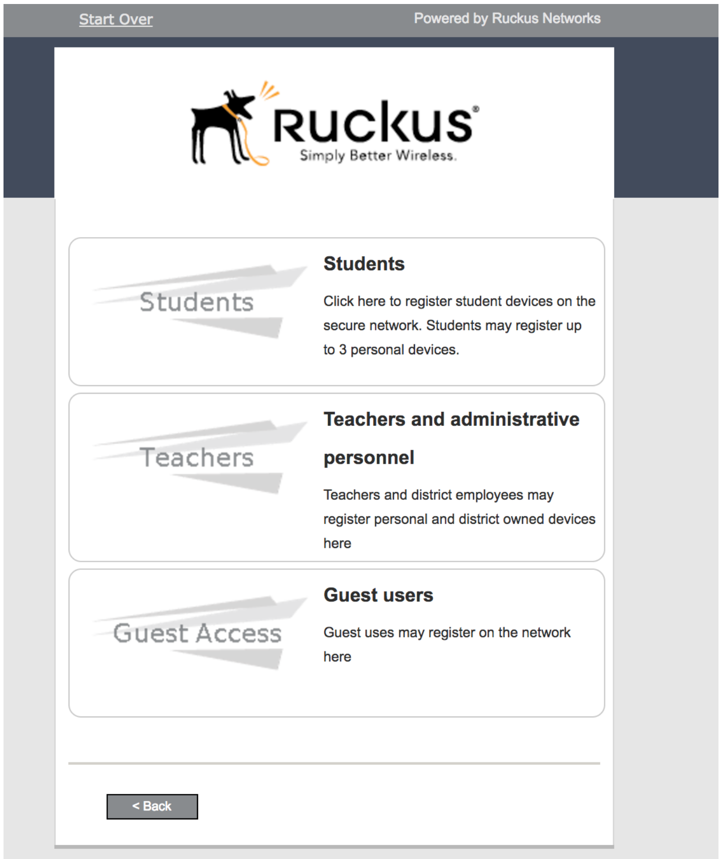
Access to the Rivendell School District network is restricted to Students, Teachers and authorized Guest Users. Access requires acceptance of the Terms & Conditions below.

Once authorized for access, your device will be configured with a unique certificate for network access.

☑ I agree to the Terms & Conditions

FIGURE 19: CLOUDPATH WELCOME SCREEN (CUSTOMIZABLE)

3. If required by the network, the user might see a User Type prompt. A user type prompt can provided as part of a branch in the workflow for the different types of users on your network. For example, in an education network, the user types might be Student/Staff/Faculty, or in Enterprise network, they might be Employees/Guests/Contractors.



Students

Click here to register student devices on the secure network. Students may register up to 3 personal devices.

Teachers and administrative personnel

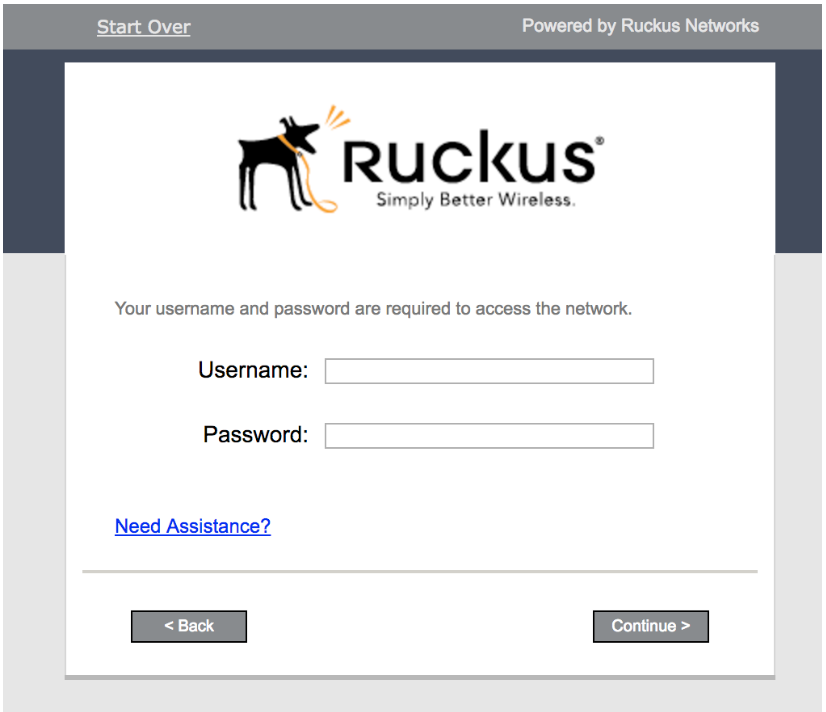
Teachers and district employees may register personal and district owned devices here

Guest users

Guest uses may register on the network here

FIGURE 20: USER TYPE PROMPT

4. If required by the network, the user can be prompted enter their credentials. A user credential prompt might request credentials from an AD or LDAP server, or from RADIUS



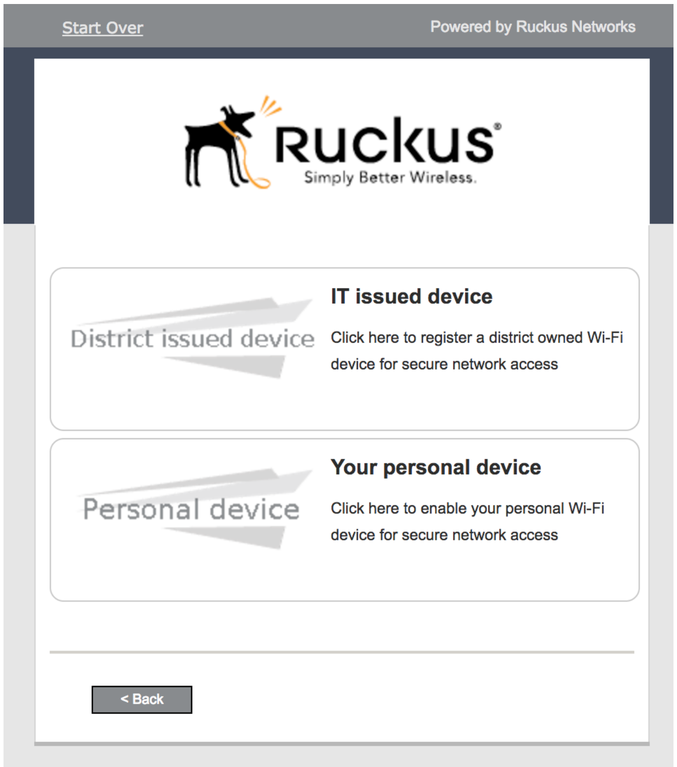
Your username and password are required to access the network.

Username:

Password:

FIGURE 21: USER CREDENTIALS PROMPT

5. If required by the network, the user might see a Device Type prompt. A device type prompt can be provided as a branch in the workflow for the different types of devices on your network.



IT issued device

Click here to register a district owned Wi-Fi device for secure network access

Your personal device

Click here to enable your personal Wi-Fi device for secure network access

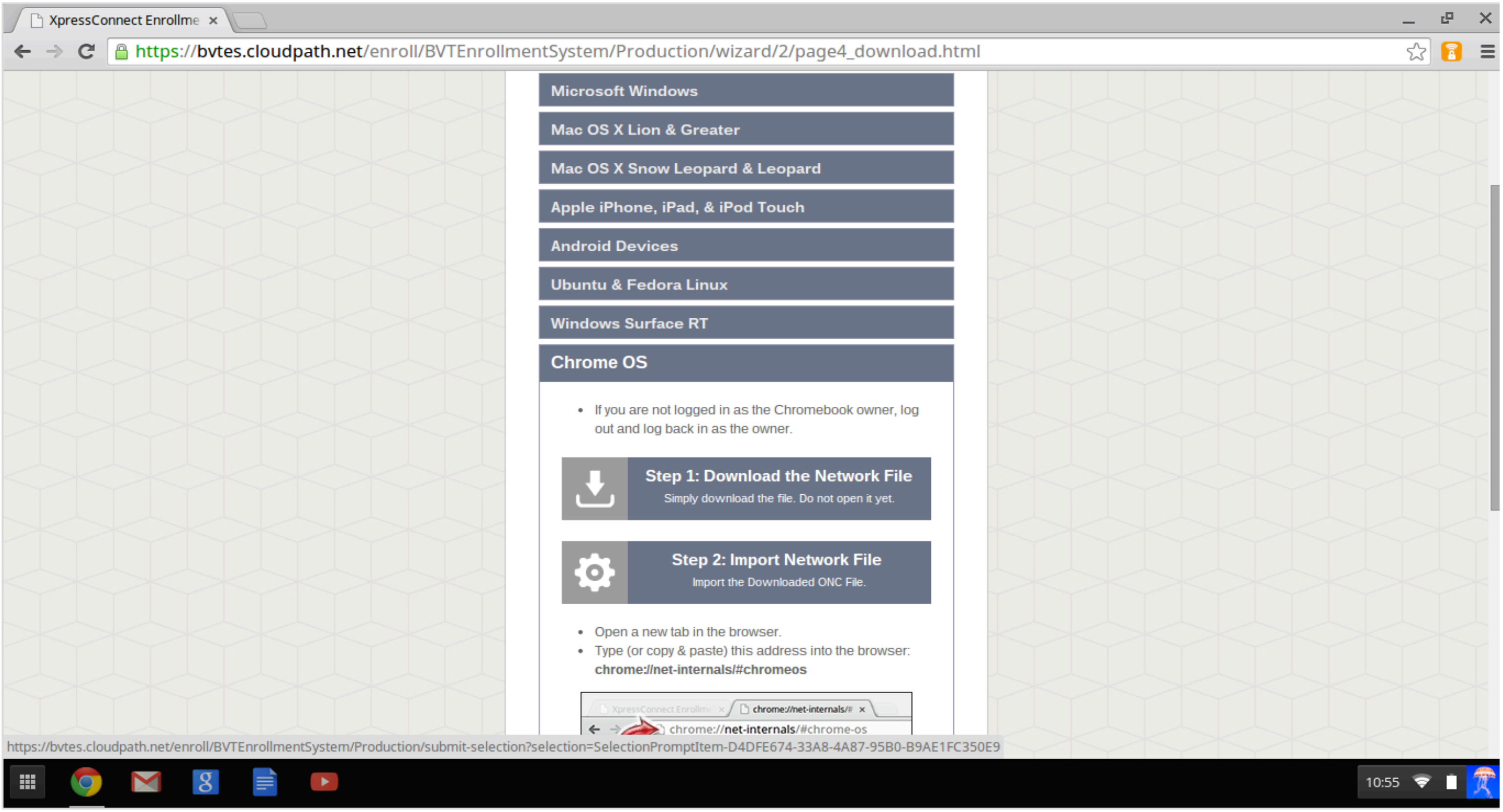
FIGURE 22: DEVICE OWNERSHIP TYPE PROMPT

6. The final portion of the user experience differs, depending on if the certificate and Wi-Fi settings are set for delivery using the ONC file (unmanaged devices) or an extension (managed devices). See the following links to continue with the user experience example for your configuration.

- Unmanaged Devices
- Managed Devices

Unmanaged Chromebook User Experience

With an unmanaged Chromebook device, the user downloads and installs the ONC file, which contains configuration information required to access the secure network, including the certificate and Wi-Fi settings. For unmanaged devices, the application detects the Chrome operating system and displays instructions for installing the Chrome configuration on the device.


XpressConnect Enrollme
https://bvtes.cloudpath.net/enroll/BVTEnrollmentSystem/Production/wizard/2/page4_download.html
Microsoft Windows
Mac OS X Lion & Greater
Mac OS X Snow Leopard & Leopard
Apple iPhone, iPad, & iPod Touch
Android Devices
Ubuntu & Fedora Linux
Windows Surface RT
Chrome OS
Step 1: Download the Network File
Step 2: Import Network File
XpressConnect Enrollme
chrome://net-internals/#
chrome://net-internals/#chrome-os
10:55

- If you are not logged in as the Chromebook owner, log out and log back in as the owner.

Step 1: Download the Network File
Simply download the file. Do not open it yet.

Step 2: Import Network File
Import the Downloaded ONC File.

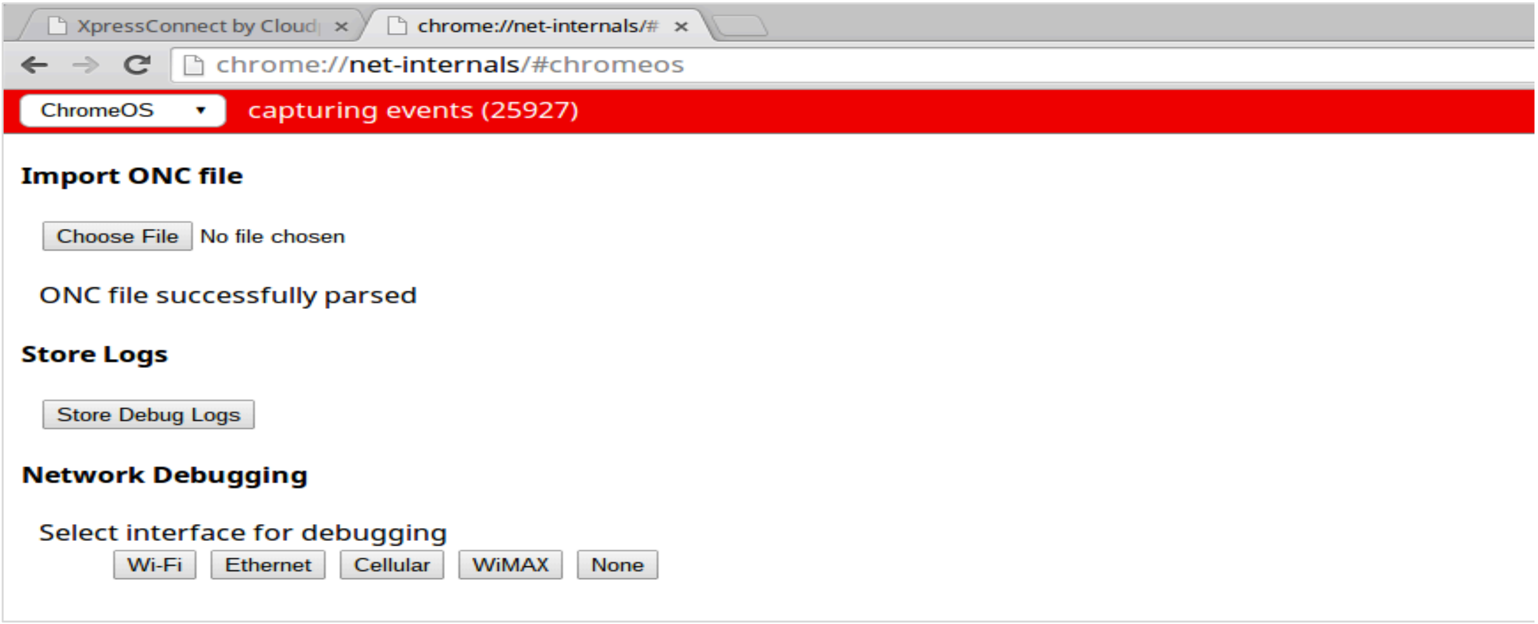
- Open a new tab in the browser.
- Type (or copy & paste) this address into the browser: **chrome://net-internals/#chromeos**

https://bvtes.cloudpath.net/enroll/BVTEnrollmentSystem/Production/submit-selection?selection=SelectionPromptItem-D4DFE674-33A8-4A87-95B0-B9AE1FC350E9

FIGURE 23: CONFIGURATION INSTALLATION INSTRUCTIONS

The manual download page shows the Chromebook instructions, which are as follows:

1. Step 1 provides the link to download the ONC file
2. Follow Step 2, which provides instructions for importing the ONC file
3. Copy the URL from the instructions and then paste the URL into a new browser window. The Chrome OS Import ONC File page will then display.



capturing events (25927)

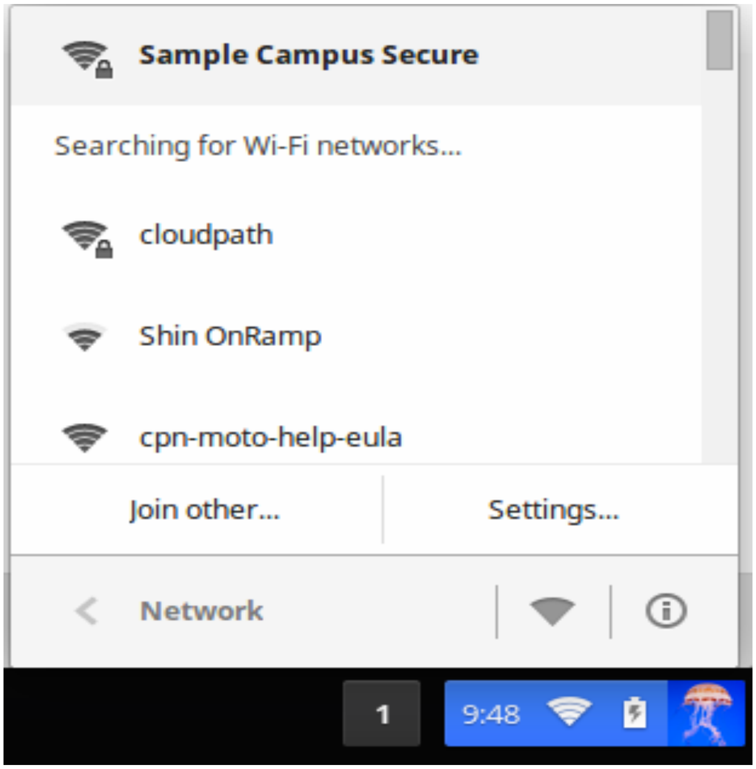
No file chosen

ONC file successfully parsed

Select interface for debugging

FIGURE 24: IMPORT ONC FILE

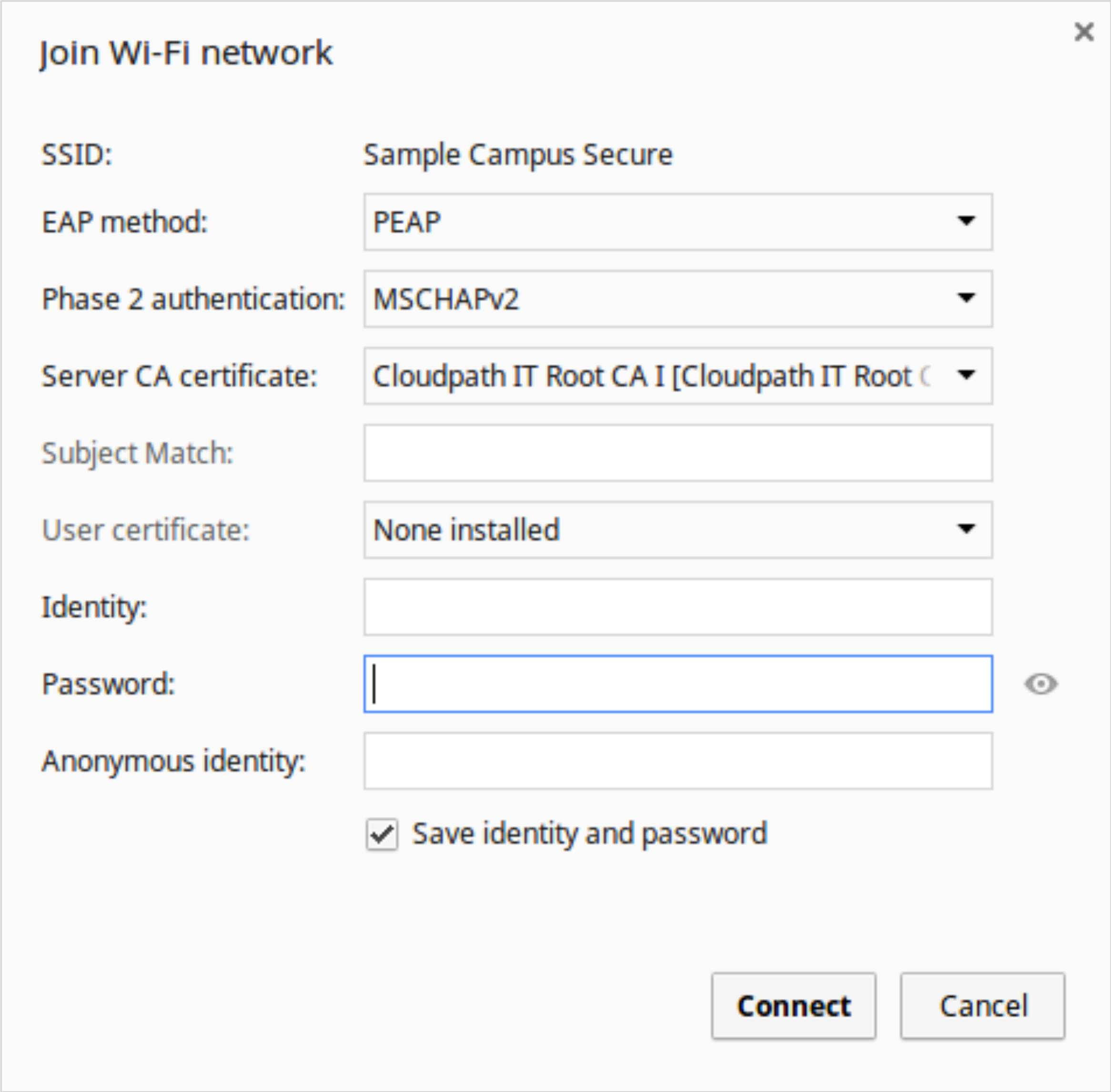
4. Click Choose File and browse to select the <NetworkName>.onc file.
5. After the ONC file has installed, click the Wi-Fi icon in the bottom right corner of your screen and select the secure network.



Searching for Wi-Fi networks...

FIGURE 25: CONNECT TO WI-FI NETWORK

6. The next screen shows the configuration settings and credentials that will be used. Typically, user credentials are populated using the information passed during the enrollment process. Click Connect.



SSID: Sample Campus Secure

EAP method: PEAP

Phase 2 authentication: MSCHAPv2

Server CA certificate: Cloudpath IT Root CA I [Cloudpath IT Root (

Subject Match:

User certificate: None installed

Identity:

Password:

Anonymous identity:

☑ Save identity and password

FIGURE 26: USER CREDENTIALS

The user should now be connected to the secure network and you have completed the configuration.

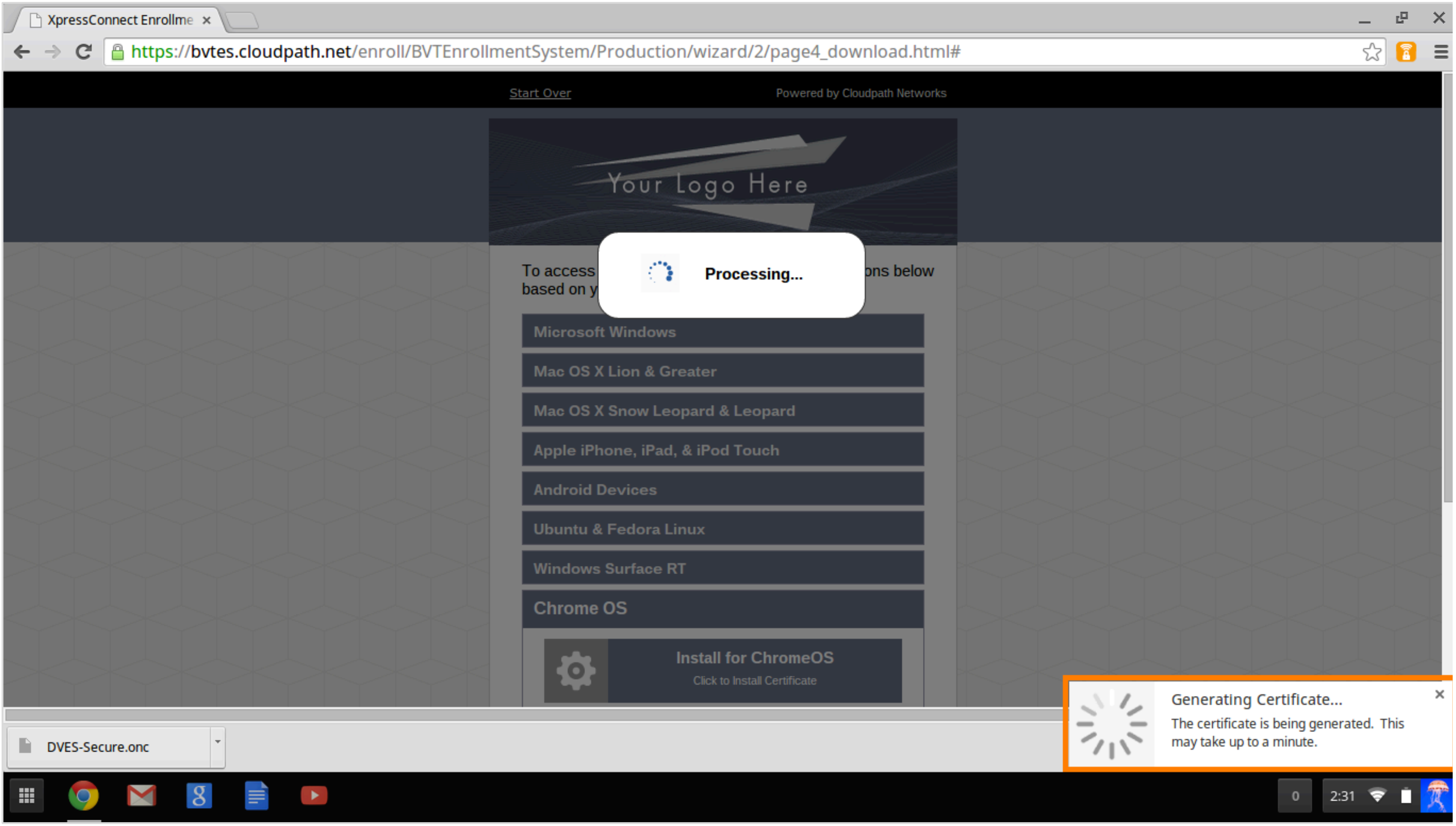
Managed Chromebooks With Extension User Experience

If managed Chromebooks are configured, the download page does not display. When Cloudpath detects the Chrome OS during enrollment, the extension automatically generates and installs the CA certificate into the TPM. The extension generates the certificate.

The process is as follows:

1. IT personal connect to the Cloudpath deployment URL (either directly, or through a Captive Portal)
2. Cloudpath detects the device is using Chrome OS
3. The extension imports the certificate into the TPM

4. When the certificate installation is complete, a message displays indicating that the certificate is installed and ready for use



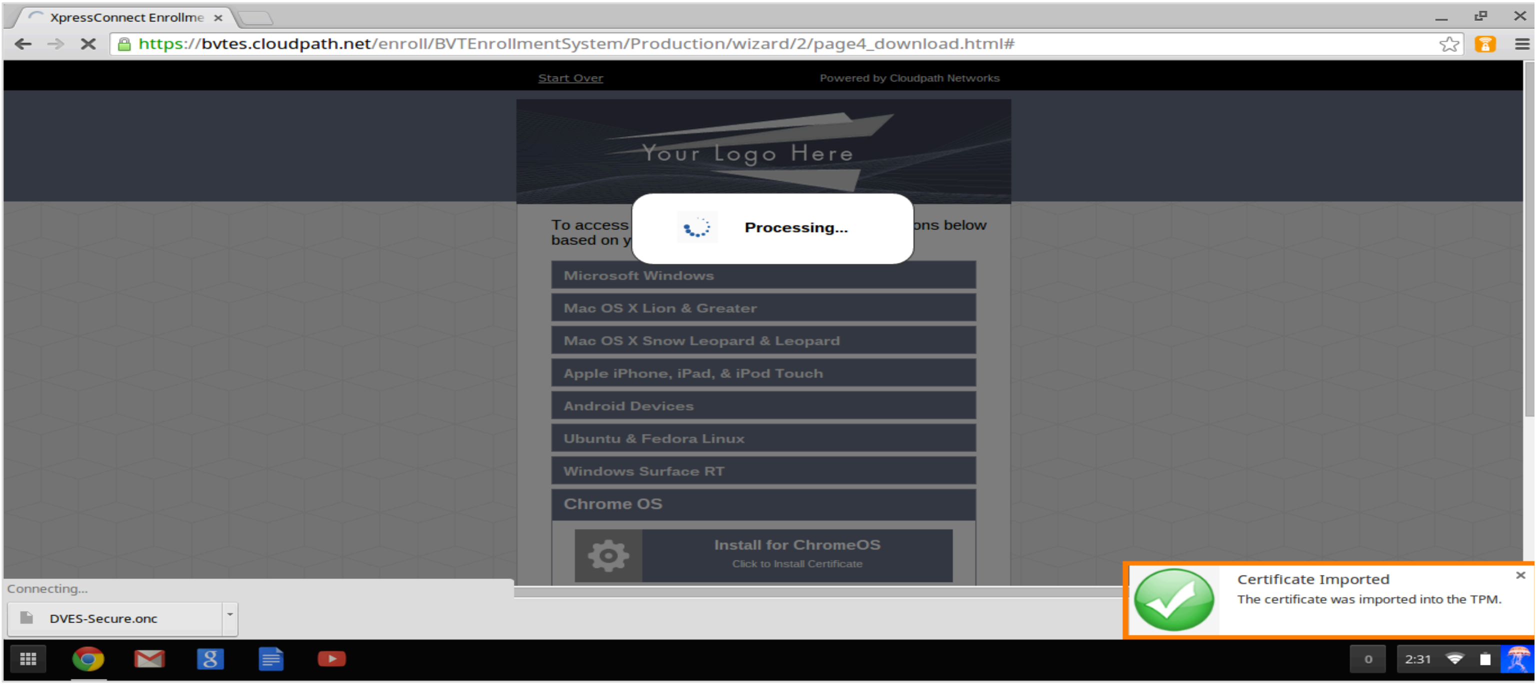
https://bvtes.cloudpath.net/enroll/BVTEnrollmentSystem/Production/wizard/2/page4_download.html#

Processing...

Generating Certificate...

The certificate is being generated. This may take up to a minute.

FIGURE 27: GENERATING CERTIFICATE



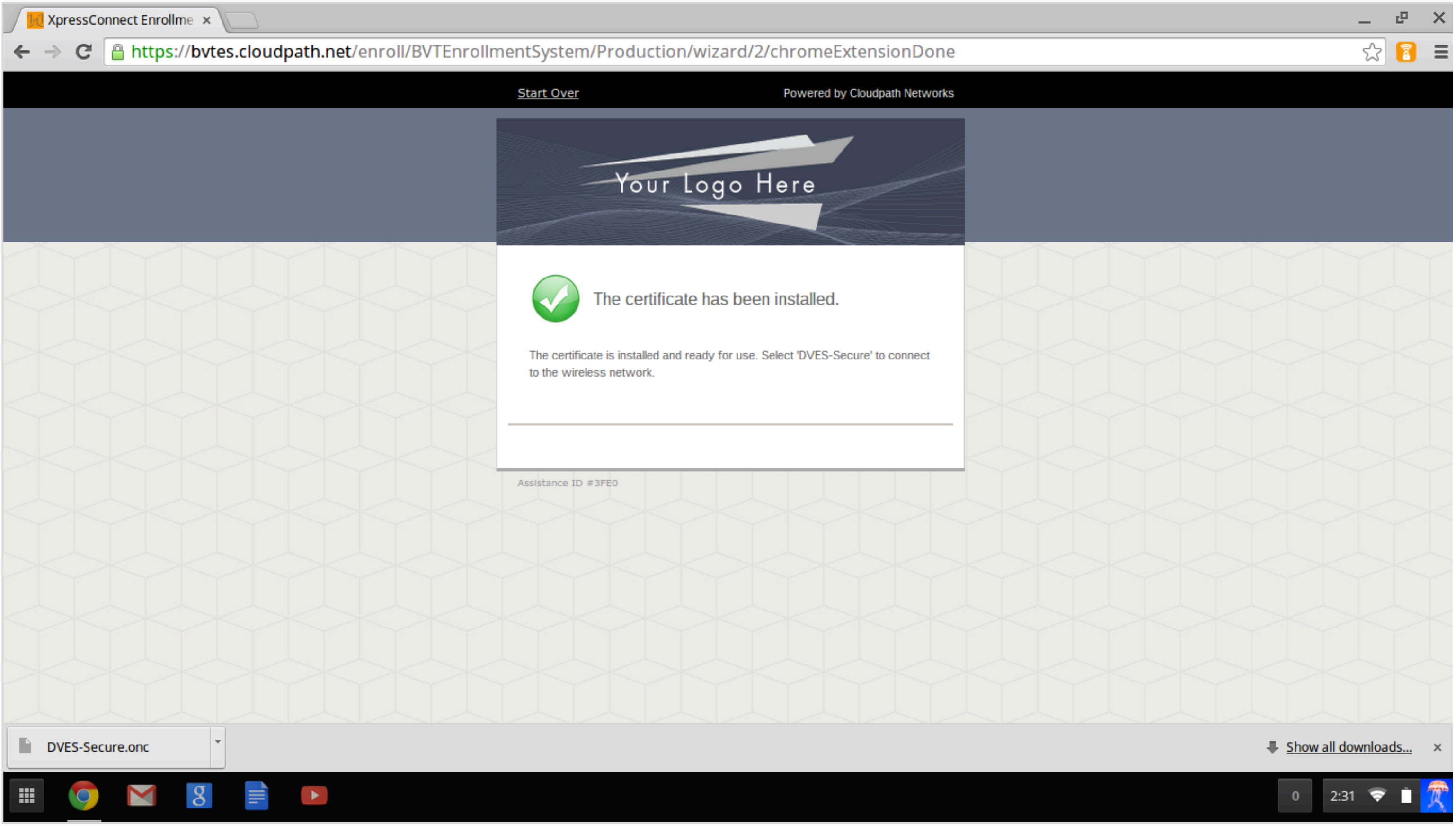
https://bvtes.cloudpath.net/enroll/BVTEnrollmentSystem/Production/wizard/2/page4_download.html#

Processing...

Certificate Imported

The certificate was imported into the TPM.

FIGURE 28: CERTIFICATE IMPORTED


XpressConnect Enrollme
https://bvtes.cloudpath.net/enroll/BVTEnrollmentSystem/Production/wizard/2/chromeExtensionDone
Start Over
Powered by Cloudpath Networks
Your Logo Here
Assistance ID #3FE0
DVES-Secure.onc
Show all downloads...
2:31

The certificate has been installed.

The certificate is installed and ready for use. Select 'DVES-Secure' to connect to the wireless network.

FIGURE 29: CERTIFICATE INSTALLED

5. Click the Wi-Fi icon in the bottom right corner of your screen and select the secure network.

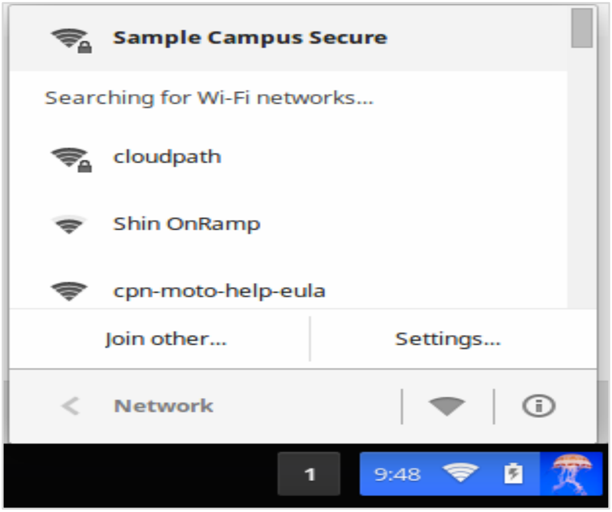


FIGURE 30: SELECT WI-FI NETWORK

The user should now be connected to the secure network and you have completed the configuration.

Troubleshooting Chrome OS Enrollment

This section describes issues to consider when testing or troubleshooting the configuration for the Cloudpath extension.

Error Messages

If a user receives a message "This device requires management controlled extension <extension name>", typically this means that the device does not have the extension installed.

Server CA

If the network does not accept the CA certificate, check that the Issued to section for the Server CA includes both the root and intermediate CA.

Access to URL

If the user unable to reach the enrollment URL, be sure that the client enrollment URL begins with HTTPS://.

Length of Private Key

While older versions of the Chromium OS did not enforce the minimum key length of 1024, the newer releases appear to enforce this change. However, it appears that this change does not support a 4096-bit key.

If you see an error that says "Error: The operation failed for an operation-specific reason.", view the page source on the page4download.html and locate the keylength/alg info. If it lists the following:

```
<input type='hidden' id='cpnKeyLength' value='4096'/>
<input type='hidden' id='cpnAlgorithm' value='SHA-512'/>
```

The fix for this issue is to navigate to the certificate template in the Cloudpath Admin UI and change the private key length to 2048 and the algorithm to SHA-256.

Chromebook Testing Shortcuts

Use the following browser shortcuts to manage different aspects of your Chrome configuration.

Shortcut URL	Description
chrome://policy	Displays all the policies which are currently in effect for the browser. Use the Reload policies button to force a re-sync with an updated policy.
chrome://extensions	Manage installed extensions. Check the Developer mode box (upper-right) to display the Update extensions now button. This is a useful testing tool.
chrome://settings	Directs you to the Menu > Settings page. From here you can control various browser related settings.
chrome://net-internals	This displays all networking related information. Use this to capture network events generated by the browser. You can also export this data.
chrome://certificate-manager	Manage user, server, and CA certificates.
chrome://dns	Displays the list of hostnames for which the browser will pre-fetch the DNS records.
chrome://chrome-urls	View all the available chrome:// commands.

TABLE 1

Sponsored Guest Access

Sponsored guest access allows authorized employees to grant network access to third parties. It is most commonly used to provide wireless network access to corporate visitors and partners, and is typically time-restricted. By distributing authorization to employees, third parties can quickly gain access without IT involvement and with appropriate traceability. Sponsored guest access is a useful scenario in a environment as it allows the school employees to sponsor guest access for visitors without involvement from the IT, cutting a large overhead.

Prerequisites - Authentication Server Setup

To configure the sponsored access feature, the network administrator must set up a sponsor group in the corporate AD or LDAP server for employees that can be authorized as sponsors. For example, create a group named Manager or Wireless Sponsors in Active Directory. This group name is then used by Cloudpath to determine which users can log into the sponsorship portal and sponsor guest users.

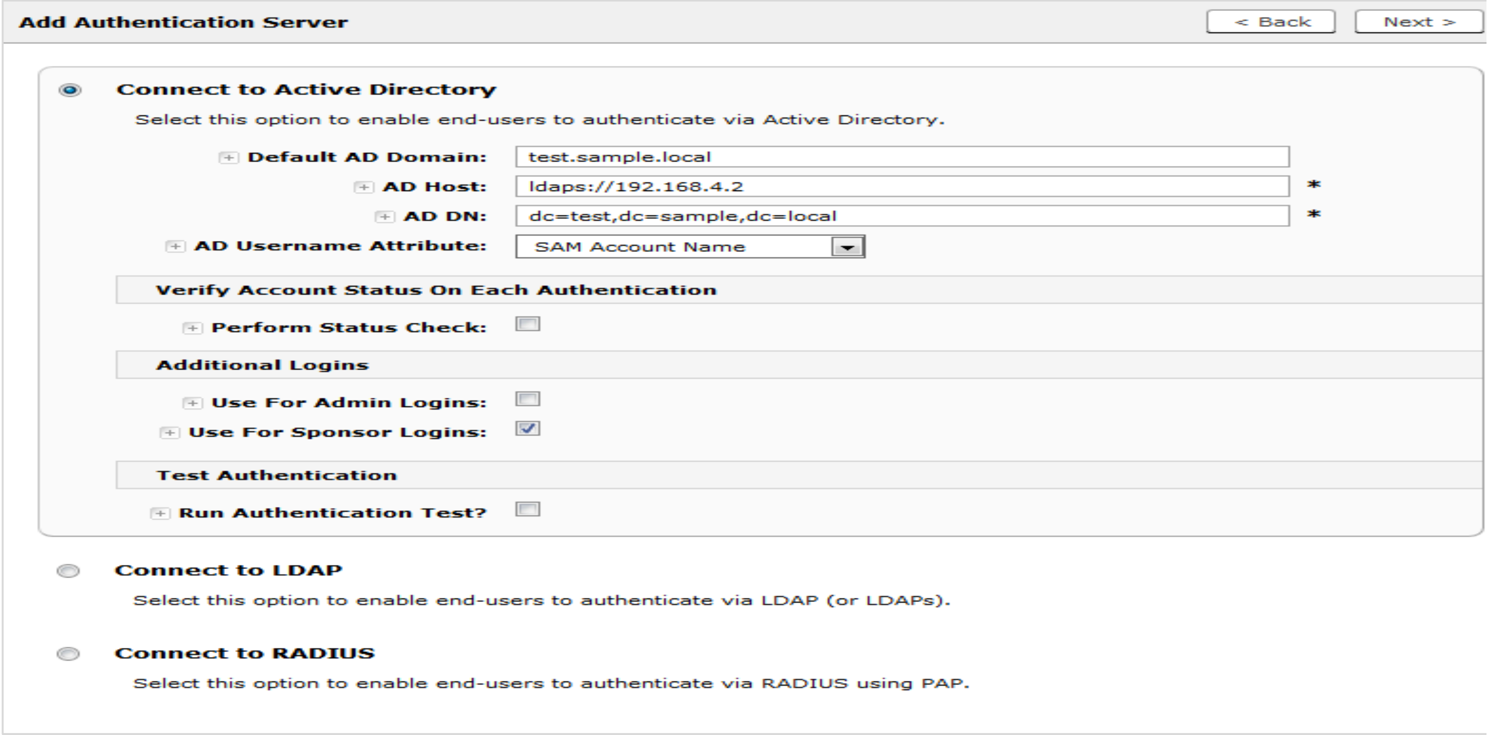
Configuring Cloudpath for Sponsored Guest Access

This section describes how to configure Cloudpath for sponsorship, add a voucher or request for access prompt to the enrollment workflow, and how to add vouchers and sponsors to the voucher list. The basic process is as follows:

1. Edit the authentication server profile in Cloudpath
2. Add a voucher prompt to the enrollment workflow
3. Add a request for access prompt

Edit the Authentication Server Profile in Cloudpath Admin Console

1. Log into the Cloudpath Admin Console and go to Administration > Advanced > Authentication Servers.
2. On the Authentication Servers page, edit the AD or LDAP server you will be using to authenticate sponsors and guest users



Add Authentication Server

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

Default AD Domain: test.sample.local
AD Host: ldaps://192.168.4.2 *
AD DN: dc=test,dc=sample,dc=local *
AD Username Attribute: SAM Account Name

Verify Account Status On Each Authentication
Perform Status Check: □

Additional Logins
Use For Admin Logins: □
Use For Sponsor Logins: ☑

Test Authentication
Run Authentication Test? □

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

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

FIGURE 31: EDIT THE AD SERVER CONFIGURATION IN CLOUDPATH ADMIN CONSOLE

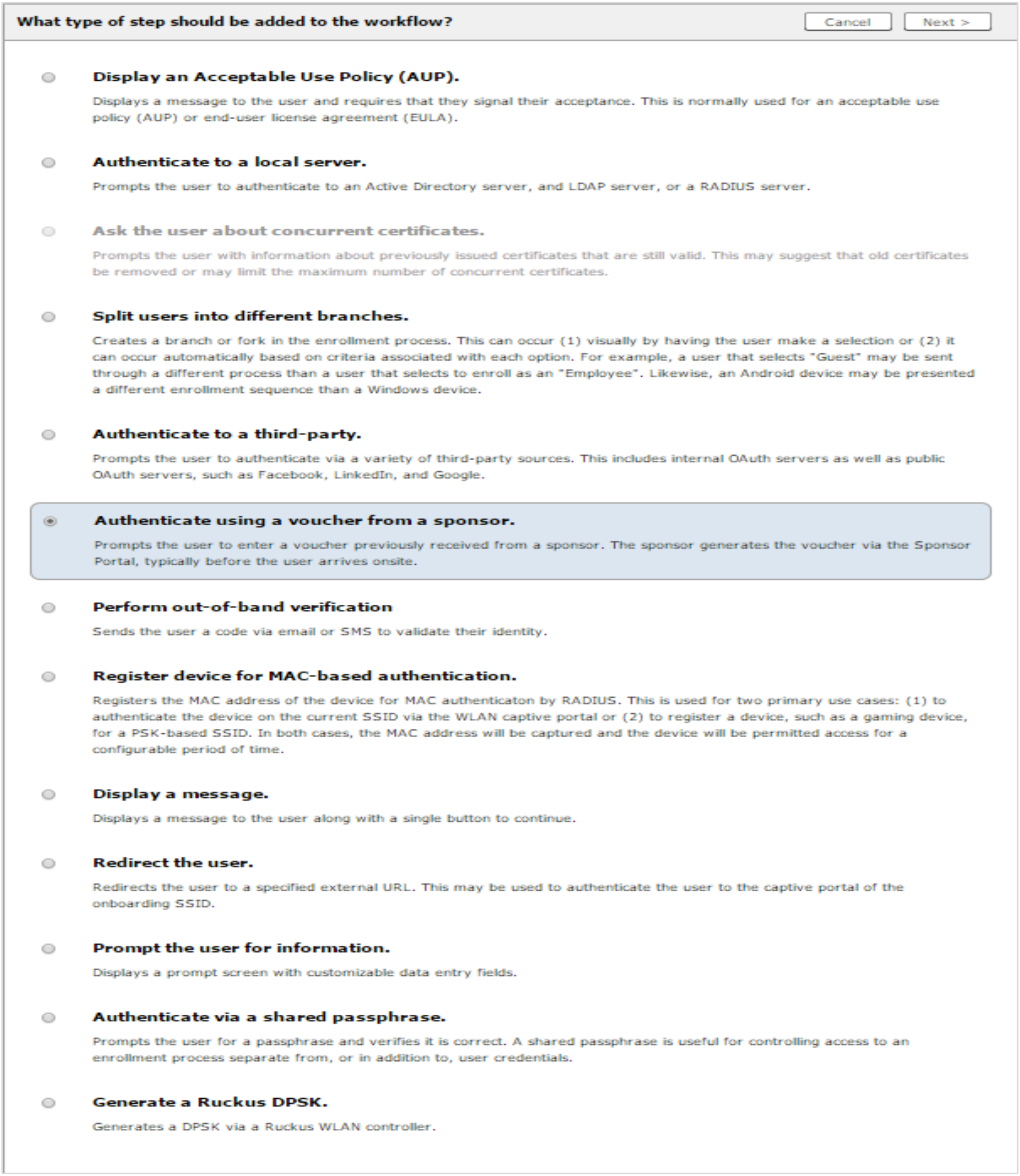
3. Select the User For Sponsor Logins box, to allow sponsors to log into the sponsorship portal using credentials from this authentication server.

Add a Voucher Prompt to the Enrollment Workflow

This section describes how to add a step in the enrollment workflow to prompt a guest user for a voucher or one-time password. Use this configuration if you plan to use generated voucher lists.

How to Add a Voucher Prompt for Guest Users in the Workflow

4. From the ES Admin UI, go to Configuration > Enrollment and create an enrollment workflow for guest users.
5. Add an enrollment step that prompts guest users to Authenticate via a voucher.



What type of step should be added to the workflow?

○ **Display an Acceptable Use Policy (AUP).**
Displays a message to the user and requires that they signal their acceptance. This is normally used for an acceptable use policy (AUP) or end-user license agreement (EULA).

○ **Authenticate to a local server.**
Prompts the user to authenticate to an Active Directory server, and LDAP server, or a RADIUS server.

○ **Ask the user about concurrent certificates.**
Prompts the user with information about previously issued certificates that are still valid. This may suggest that old certificates be removed or may limit the maximum number of concurrent certificates.

○ **Split users into different 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 that selects "Guest" may be sent through a different process than a user that selects to enroll as an "Employee". Likewise, an Android device may be presented a different enrollment sequence than a Windows device.

○ **Authenticate to a third-party.**
Prompts the user to authenticate via a variety of third-party sources. This includes internal OAuth servers as well as public OAuth servers, such as Facebook, LinkedIn, and Google.

● **Authenticate using a voucher from a sponsor.**
Prompts the user to enter a voucher previously received from a sponsor. The sponsor generates the voucher via the Sponsor Portal, typically before the user arrives onsite.

○ **Perform out-of-band verification**
Sends the user a code via email or SMS to validate their identity.

○ **Register device for MAC-based authentication.**
Registers the MAC address of the device for MAC authenticaton by RADIUS. This is used for two primary use cases: (1) to authenticate the device on the current SSID via the WLAN captive portal or (2) to register a device, such as a gaming device, for a PSK-based SSID. In both cases, the MAC address will be captured and the device will be permitted access for a configurable period of time.

○ **Display a message.**
Displays a message to the user along with a single button to continue.

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

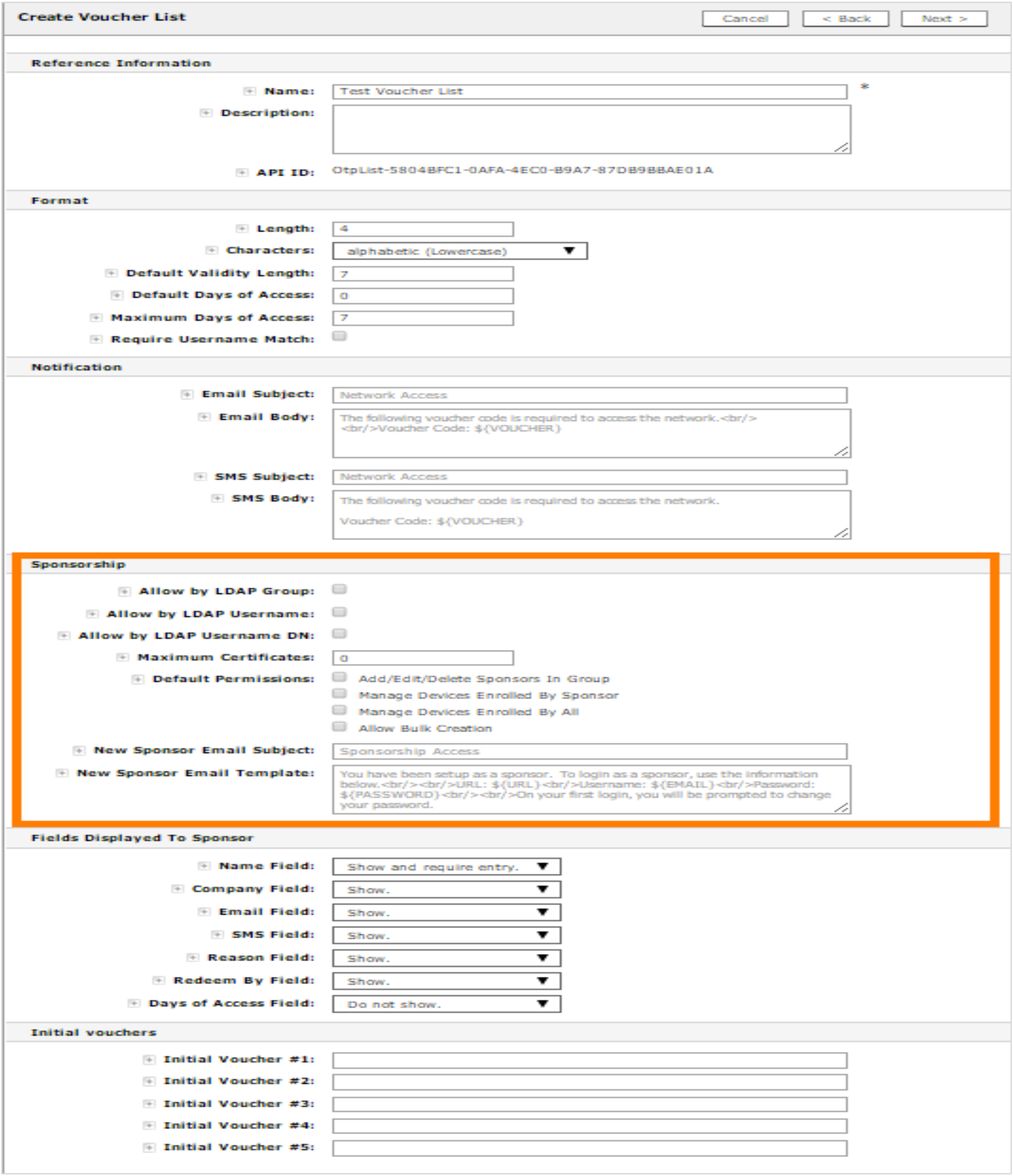
○ **Prompt the user for information.**
Displays a prompt screen with customizable data entry fields.

○ **Authenticate via a shared passphrase.**
Prompts the user for a passphrase and verifies 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.**
Generates a DPSK via a Ruckus WLAN controller.

FIGURE 32: CREATE VOUCHER ENROLLMENT STEP

6. Create a new voucher list for guest users.



Create Voucher List

Reference Information

Name: Test Voucher List *

Description:

API ID: OtpList-5804BFC1-0AFA-4EC0-B9A7-87DB9BBAE01A

Format

Length: 4

Characters: alphabetic (Lowercase)

Default Validity Length: 7

Default Days of Access: 0

Maximum Days of Access: 7

Require Username Match: □

Notification

Email Subject: Network Access

Email Body: The following voucher code is required to access the network.<br/><br/>Voucher Code: ${VOUCHER}

SMS Subject: Network Access

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

Voucher Code: ${VOUCHER}

Sponsorship

Allow by LDAP Group: □

Allow by LDAP Username: □

Allow by LDAP Username DN: □

Maximum Certificates: 0

Default Permissions:
□ Add/Edit/Delete Sponsors In Group
□ Manage Devices Enrolled By Sponsor
□ Manage Devices Enrolled By All
□ Allow Bulk Creation

New Sponsor Email Subject: Sponsorship Access

New Sponsor Email Template: You have been setup as a sponsor. To login as a sponsor, use the information below.<br/><br/>URL: ${URL}<br/>Username: ${EMAIL}<br/>Password: ${PASSWORD}<br/><br/>On your first login, you will be prompted to change your password.

Fields Displayed To Sponsor

Name Field: Show and require entry.

Company Field: Show.

Email Field: Show.

SMS Field: Show.

Reason Field: Show.

Redeem By Field: Show.

Days of Access Field: Do not show.

Initial vouchers

Initial Voucher #1:

Initial Voucher #2:

Initial Voucher #3:

Initial Voucher #4:

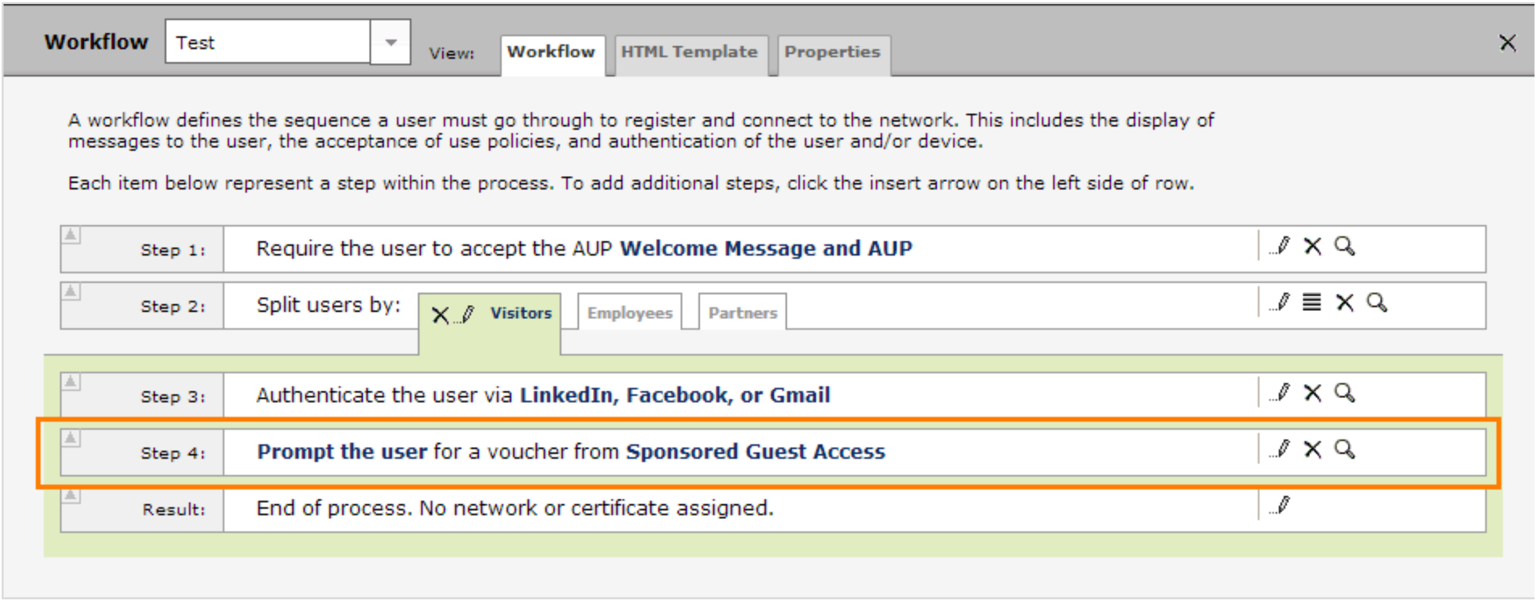
Initial Voucher #5:

FIGURE 33: CREATE VOUCHER LIST

7. In the Sponsorship section, enter the appropriate information in the following fields:

- Format - In addition to defining the voucher format, determine if you want to enable *RequireUsername Match*.
- LDAP Group Regex - Defines with groups within LDAP are allowed to be sponsors. For example, if you enter Wireless Sponsors, this means that anyone in the Wireless Sponsors AD group can sponsor a guest user. LDAP Username defines which usernames within LDAP are allowed to be sponsors, LDAP Username DN defines with username DNs are allowed to be sponsors.
- Maximum Certificates - Maximum number of vouchers that a sponsor is allowed to create and allocate for a particular voucher list.
- Default Permissions - The permissions to be used for sponsors authenticated using the *Sponsorship AD Group Regex*.
- Add/Edit/Delete Sponsors In Group - If checked, the sponsor can add, edit, and delete other sponsors within the group.
- Manage Devices Enrolled By Sponsor - If checked, the sponsor can review and revoke devices enrolled via vouchers issued by that sponsor.
- Manage Devices Enrolled By All - If checked, the sponsor can review and revoke devices enrolled via vouchers issued by any sponsor (within the Voucher List).
- New Sponsor Email Subject - When a new sponsor is added, an email is sent to the sponsor with this subject.
- New Sponsor Email Template - When a new sponsor is added, an email is sent to the sponsor with this message.

8. In the Fields Displayed to Sponsor section, select Do not show, Show, or Show and require entry to specify the information to be shown when a sponsor creates a voucher list for guest access.
9. If needed, create one or more Initial vouchers.
10. Create a webpage that will prompt the user to enter their voucher and Save. The voucher prompt is saved in the workflow.



A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.

Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row.

Step 1: Require the user to accept the AUP **Welcome Message and AUP**

Step 2: Split users by: Visitors | Employees | Partners

Step 3: Authenticate the user via **LinkedIn, Facebook, or Gmail**

Step 4: **Prompt the user** for a voucher from **Sponsored Guest Access**

Result: End of process. No network or certificate assigned.

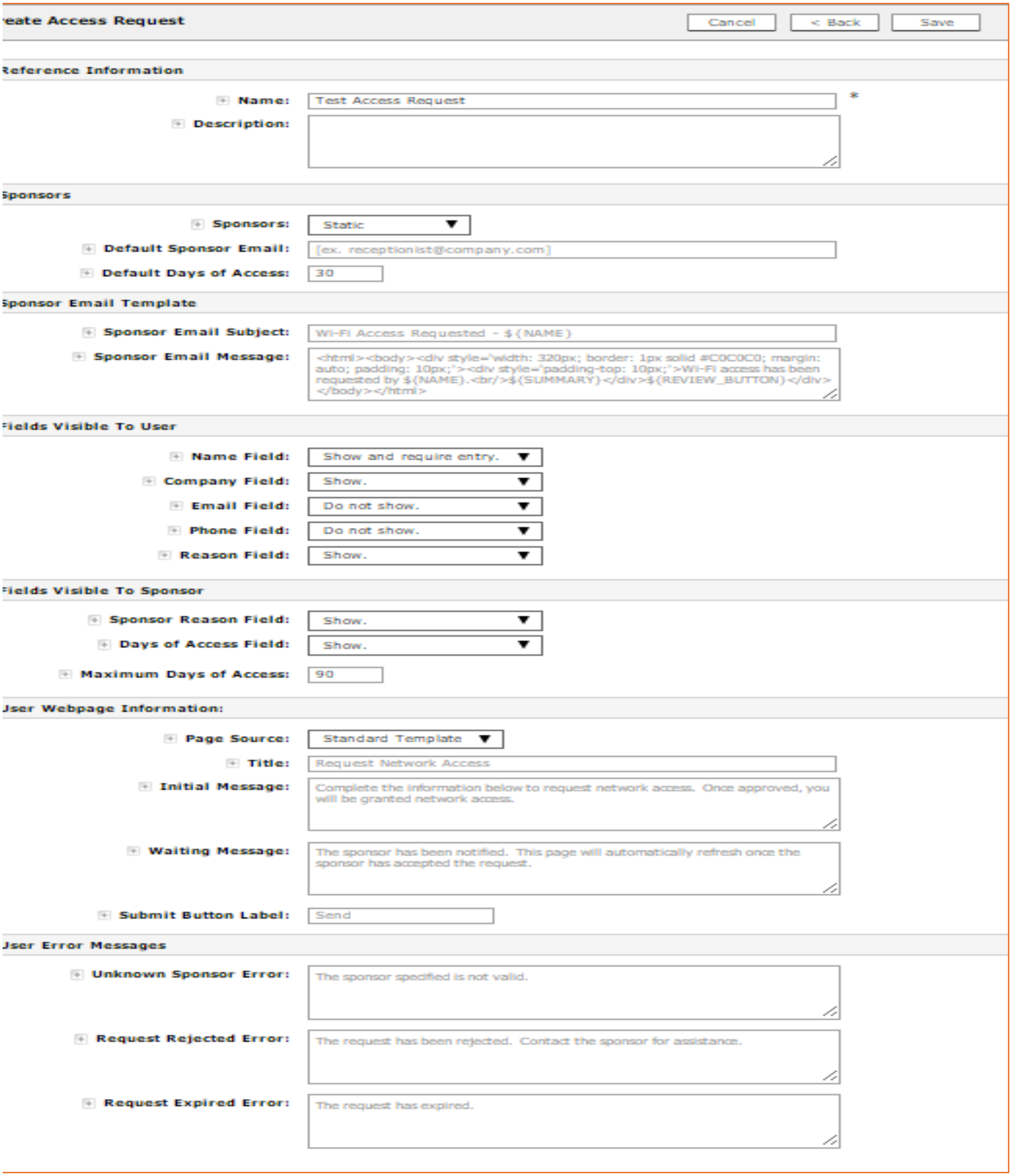
FIGURE 34: CLOUDPATH WORKFLOW

Adding a Request for Access Prompt

This section describes how to create a workflow plug-in that allows guests to request access via sponsorship upon arrival. Use this configuration if you want users to request immediate access from sponsors. While the voucher list workflow plug-in requires the sponsor to pre-sponsor the guest, the request for access workflow plug-in allows the guest to enter their information on a webpage and then request access. The guest is held in a pending state until the sponsor accepts or rejects the request. The request may go to a static user (like a receptionist), to a sponsor selected from a list by the guest, or to a sponsor that is entered by the guest upon arrival.

How to Add a Request for Access Prompt to the Workflow

1. From the ES Admin UI, go to Configuration > Enrollment and create an enrollment workflow for guest users.
2. Add an enrollment step that prompts guest users to Request Access From a Sponsor.



eate Access Request

Reference Information

Name: Test Access Request *

Description:

Sponsors

Sponsors: Static

Default Sponsor Email: [ex. receptionist@company.com]

Default Days of Access: 30

Sponsor Email Template

Sponsor Email Subject: Wi-Fi Access Requested - ${NAME}

Sponsor Email Message: <html><body><div style='width: 320px; border: 1px solid #C0C0C0; margin: auto; padding: 10px;'><div style='padding-top: 10px;'>Wi-Fi access has been requested by ${NAME}.<br/>${SUMMARY}</div>${REVIEW_BUTTON}</div></body></html>

Fields Visible To User

Name Field: Show and require entry.

Company Field: Show.

Email Field: Do not show.

Phone Field: Do not show.

Reason Field: Show.

Fields Visible To Sponsor

Sponsor Reason Field: Show.

Days of Access Field: Show.

Maximum Days of Access: 90

User Webpage Information:

Page Source: Standard Template

Title: Request Network Access

Initial Message: Complete the information below to request network access. Once approved, you will be granted network access.

Waiting Message: The sponsor has been notified. This page will automatically refresh once the sponsor has accepted the request.

Submit Button Label: Send

User Error Messages

Unknown Sponsor Error: The sponsor specified is not valid.

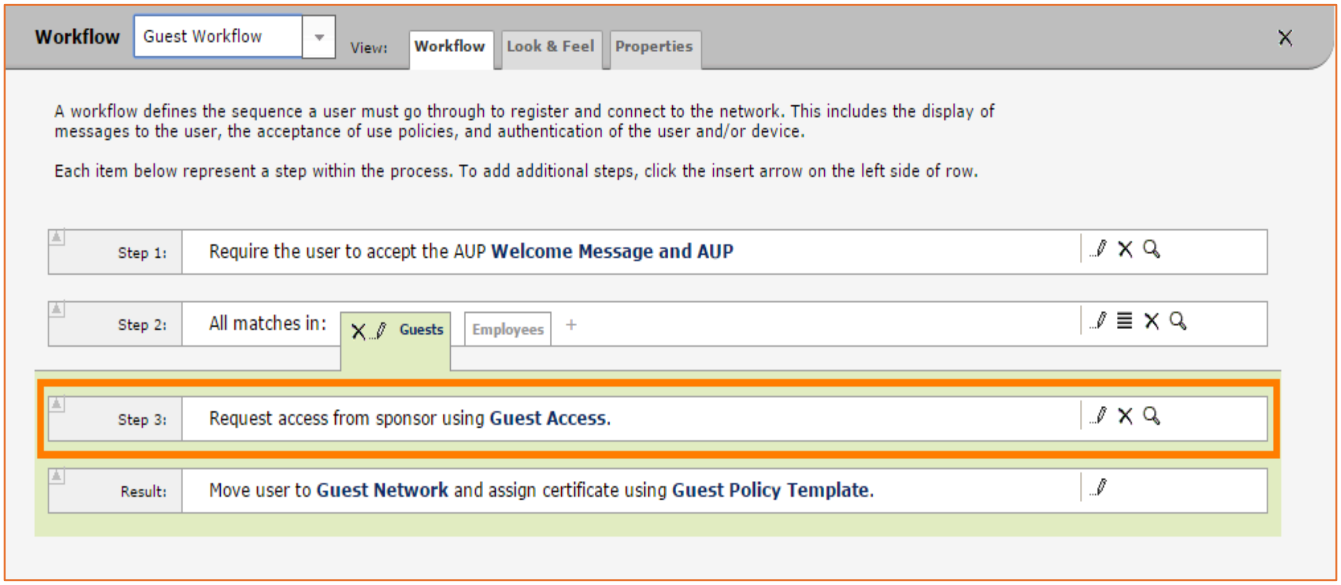
Request Rejected Error: The request has been rejected. Contact the sponsor for assistance.

Request Expired Error: The request has expired.

FIGURE 35: CREATE ACCESS REQUEST

3. For Sponsors, enter the email address for a dedicated contact, create a drop-down list of sponsors, or allow the guest to enter the
4. email address of a sponsor.

5. The Sponsor Email Template is the information sent to the sponsor when a guest is requesting access. Use the default sponsor
6. email template or create a custom email subject and message.
7. Specify the fields to display to the guest user.
8. Specify the fields to display to the sponsor receiving the access request.
9. The User Webpage Information is the prompt that displays to the guest during the enrollment process. Use the default guest
10. prompt, enter your own messaging, or upload a custom HTML file.
11. The User Error Messages display to the guest user if there is an issue with the access request.
12. Click Save.



A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.

Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row.

Step 1: Require the user to accept the AUP **Welcome Message and AUP**

Step 2: All matches in: Guests | Employees | +

Step 3: Request access from sponsor using **Guest Access.**

Result: Move user to **Guest Network** and assign certificate using **Guest Policy Template.**

FIGURE 36: REQUEST FOR ACCESS WORKFLOW

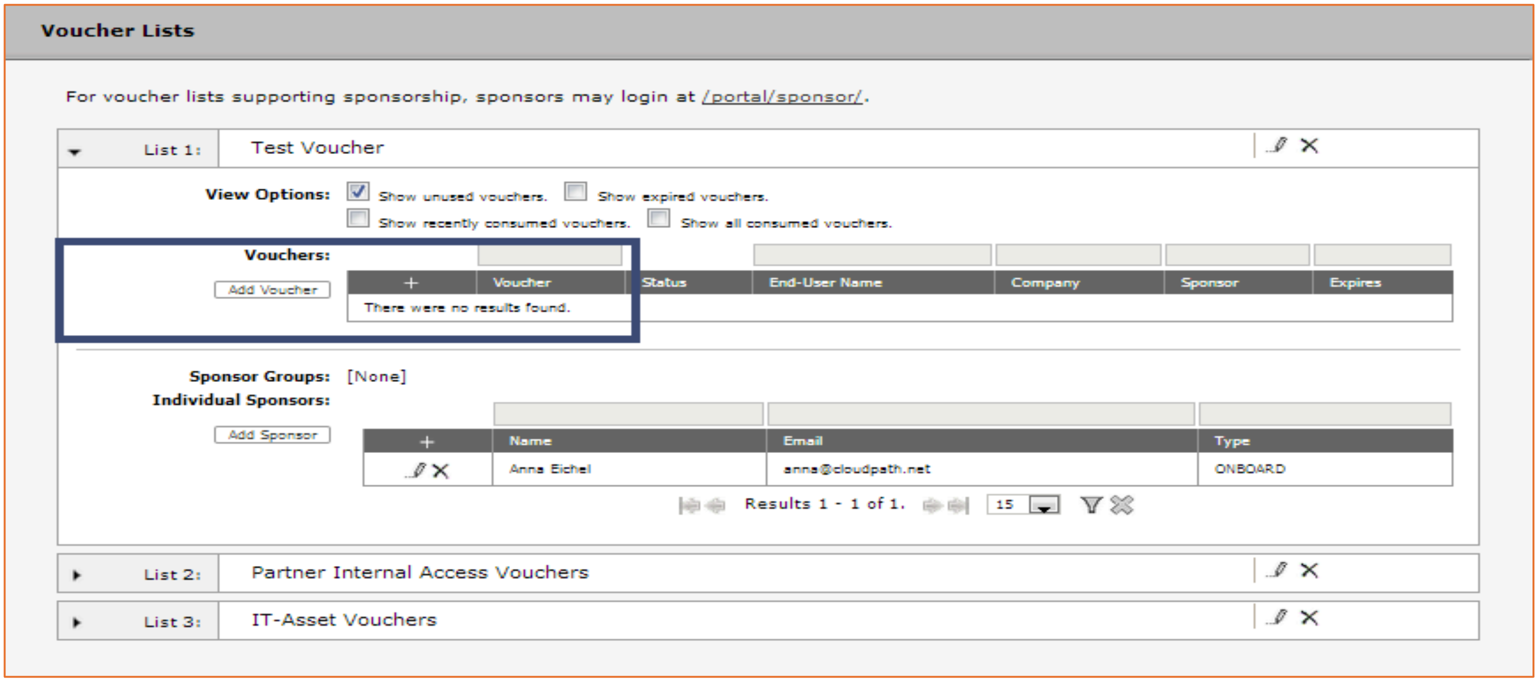
The workflow now includes the step for requesting guest access.

Adding Vouchers to a Voucher List

This section describes how to populate a voucher list. You can add a single voucher or upload multiple vouchers from a CSV file.

Voucher Lists

1. From the ES Admin UI, go to Sponsorship > Vouchers to view the voucher lists. (Alternately, you access the Voucher List page by double-clicking the Voucher List link in the enrollment workflow.)
2. Expand the voucher list.



Voucher Lists

For voucher lists supporting sponsorship, sponsors may login at /portal/sponsor/.

List 1: Test Voucher

View Options: ☑ Show unused vouchers. □ Show expired vouchers. □ Show recently consumed vouchers. □ Show all consumed vouchers.

Vouchers: Add Voucher

+	Voucher	Status	End-User Name	Company	Sponsor	Expires
There were no results found.						

Sponsor Groups: [None]

Individual Sponsors: Add Sponsor

+	Name	Email	Type
	Anna Eichel	anna@cloudpath.net	ONBOARD

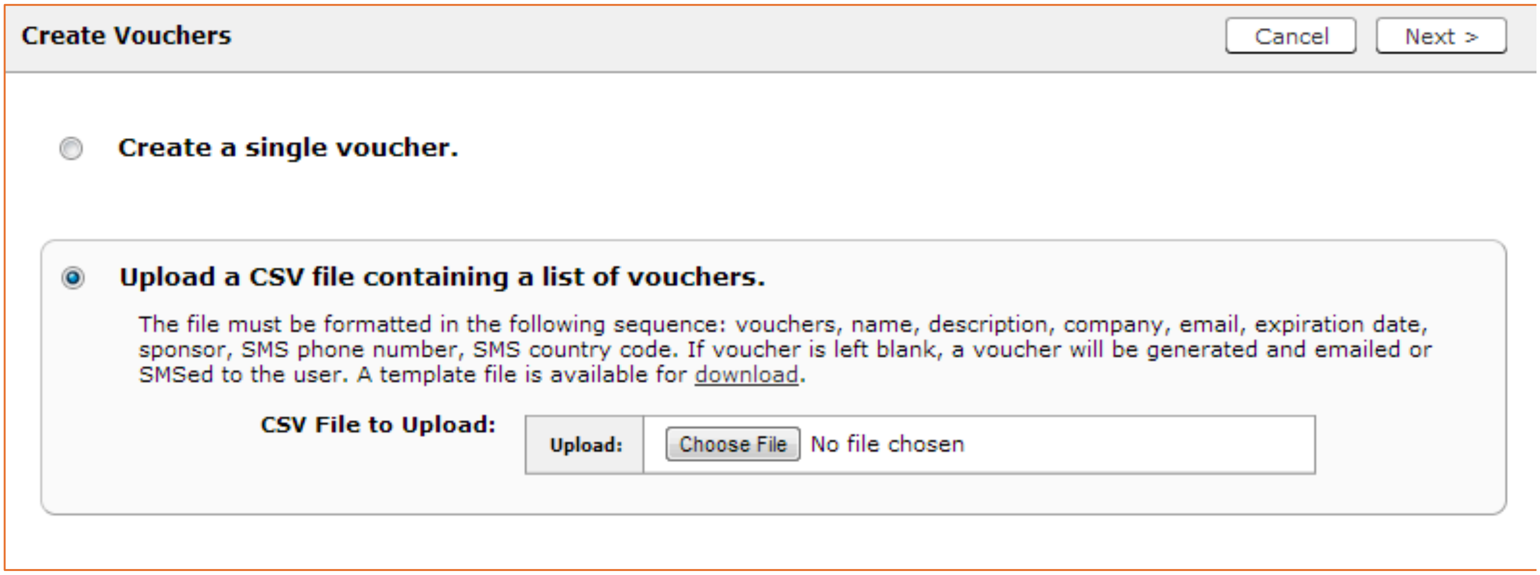
Results 1 - 1 of 1. 15

List 2: Partner Internal Access Vouchers

List 3: IT-Asset Vouchers

FIGURE 37: VOUCHER LIST

3. Click Add Vouchers to create a single voucher or upload a list of vouchers. The Create Vouchers page opens.



Create Vouchers

○ **Create a single voucher.**

● **Upload a CSV file containing a list of vouchers.**

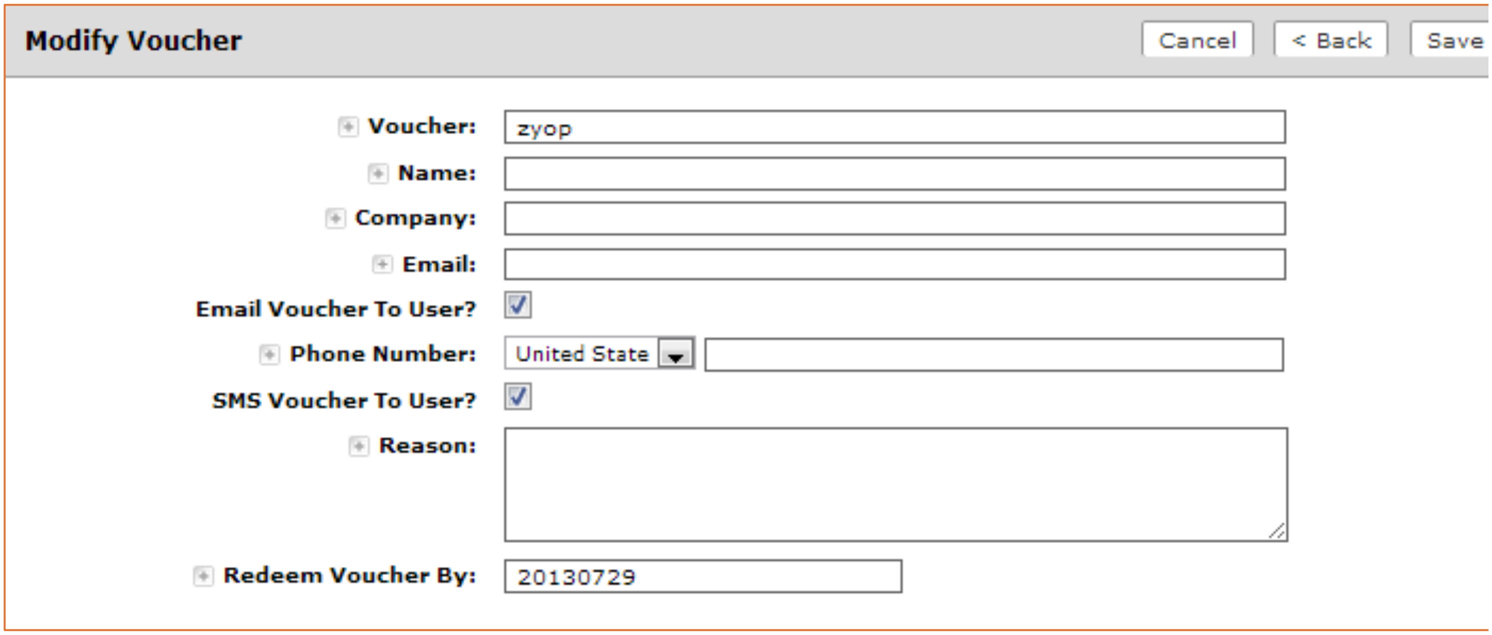
The file must be formatted in the following sequence: vouchers, name, description, company, email, expiration date, sponsor, SMS phone number, SMS country code. If voucher is left blank, a voucher will be generated and emailed or SMSed to the user. A template file is available for download.

CSV File to Upload: **Upload:** Choose File No file chosen

FIGURE 38: CREATE VOUCHERS

How to Add a Single Voucher to a Voucher List

4. On the Create Vouchers page, select Create a single voucher



Voucher: zyop

Name:

Company:

Email:

Email Voucher To User? ☑

Phone Number: United State

SMS Voucher To User? ☑

Reason:

Redeem Voucher By: 20130729

FIGURE 39: CREATE SINGLE VOUCHER

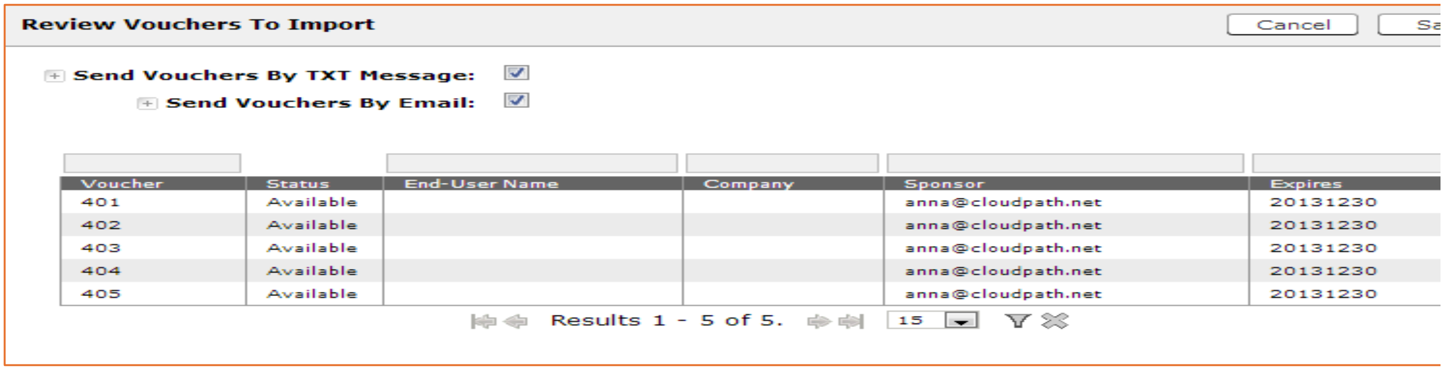
5. On the Modify Voucher page, enter the guest user information in the fields, as described below, and Save. Only the Voucher field is equired.

- Voucher - This field is pre-populated, but can be changed.
- Name - Guest user name.
- Company - Guest user company.
- Email - Guest user email address.
- Email Voucher to User? - Checked by default. If checked and email is entered, voucher is sent to guest user by email.
- Phone Number - Select country and enter guest user phone number.
- SMS Voucher to User? - Checked by default. If this is checked and Phone Number is entered, voucher is sent to guest user
- by SMS.
- Reason - The reason the guest user is provided access.
- Redeem Voucher By - The date after which the voucher may longer be redeemed.

How to Add Multiple Vouchers to a Voucher List

If you are using a comma-separated value (CSV) file to upload multiple vouchers, the information must be formatted according to the instructions on the Create Vouchers page. A template file is available for download.

6. On the Create Vouchers page, select Upload a CSV file containing a list of vouchers.
7. Click Choose File to navigate to the CSV file to upload and click Next.



Review Vouchers To Import

Send Vouchers By TXT Message: ☑
Send Vouchers By Email: ☑

Voucher	Status	End-User Name	Company	Sponsor	Expires
401	Available			anna@cloudpath.net	20131230
402	Available			anna@cloudpath.net	20131230
403	Available			anna@cloudpath.net	20131230
404	Available			anna@cloudpath.net	20131230
405	Available			anna@cloudpath.net	20131230

Results 1 - 5 of 5.

FIGURE 40: REVIEW VOUCHERS TO IMPORT

8. Verify the vouchers to import and specify if voucher should be sent to user by email or SMS, and Save.

- Send vouchers by TXT messages - If checked, the voucher is sent to the user by TXT, if a phone number is specified in the CSV file.
- Send vouchers by Email - If checked, the voucher is sent to the user by email, if an email address is specified in the CSV file.

The Voucher Lists page shows which vouchers have been used, the expiration dates, and any guest user details that were entered when the sponsor created the voucher, or contained in the CSV file.

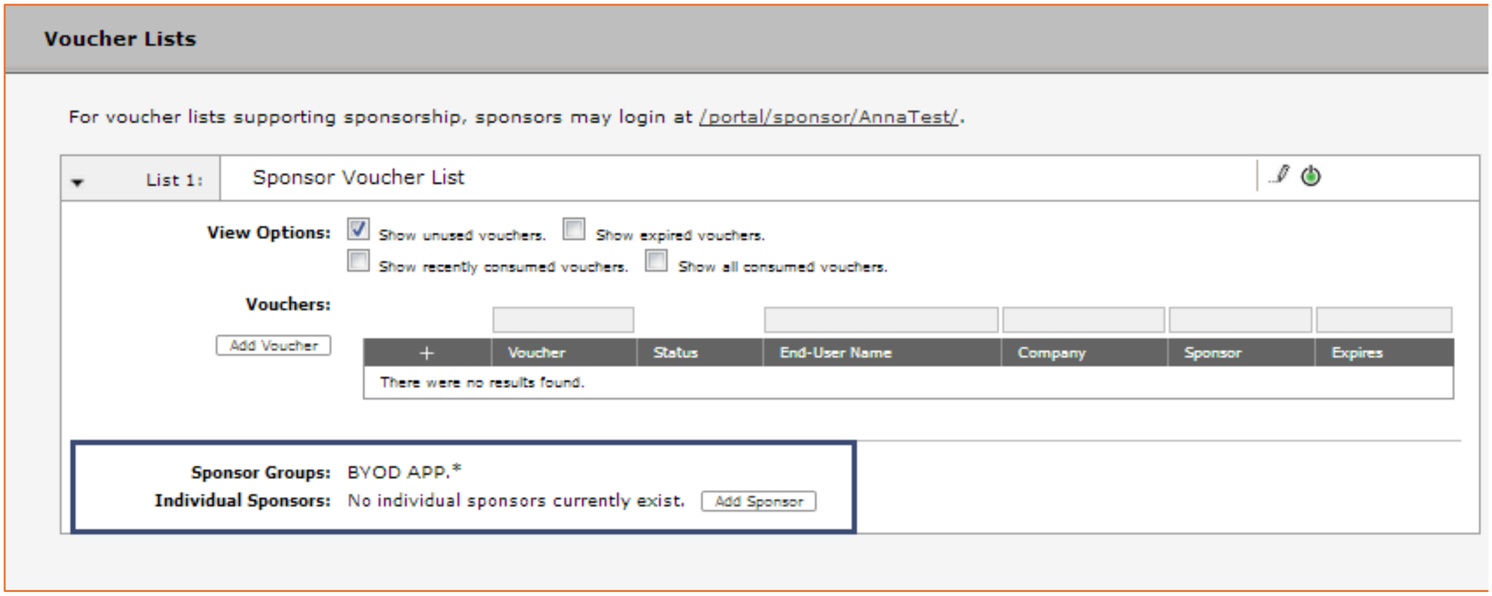
Adding Sponsors to a Voucher List

Administrators can add sponsors to a voucher list. Sponsors can create vouchers and invite guest users to join the secure network. Cloudpath supports Onboard and External sponsors. Onboard sponsors are created locally on the ES Admin UI. External sponsors can log into the Sponsorship Portal if they match a username or group name specified in the Authentication server.

How to Add Onboard Sponsors

An onboard sponsor is created locally on the ES Voucher list.

9. From the ES Admin UI, go to Sponsorship > Vouchers to view the voucher list to be used for sponsors. (Alternately, you access the Voucher List page by double-clicking the voucher list link in the enrollment workflow.)



Voucher Lists

For voucher lists supporting sponsorship, sponsors may login at /portal/sponsor/AnnaTest/.

List 1: Sponsor Voucher List

View Options: ☑ Show unused vouchers. □ Show expired vouchers.
□ Show recently consumed vouchers. □ Show all consumed vouchers.

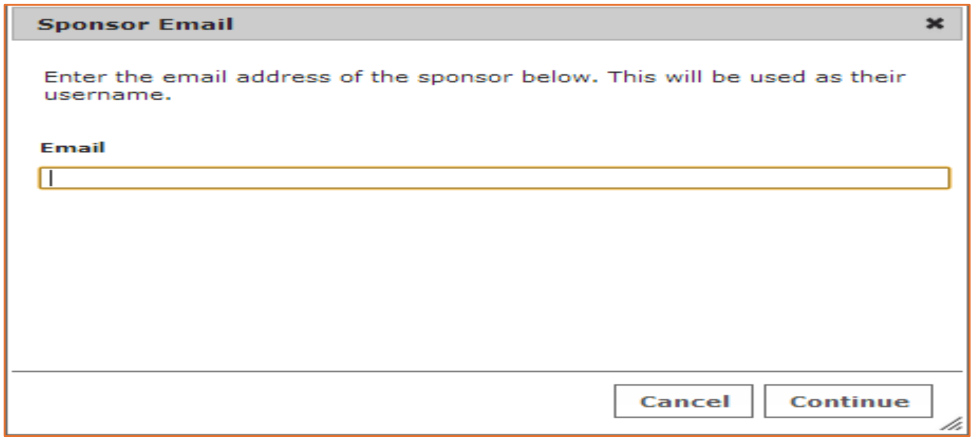
Vouchers:

+	Voucher	Status	End-User Name	Company	Sponsor	Expires
There were no results found.						

Sponsor Groups: BYOD APP.*
Individual Sponsors: No individual sponsors currently exist.

FIGURE 41: VOUCHER LIST - ADD SPONSOR

10. In the Sponsor Group section, click Add Sponsors. The Sponsor Email pop-up appears.



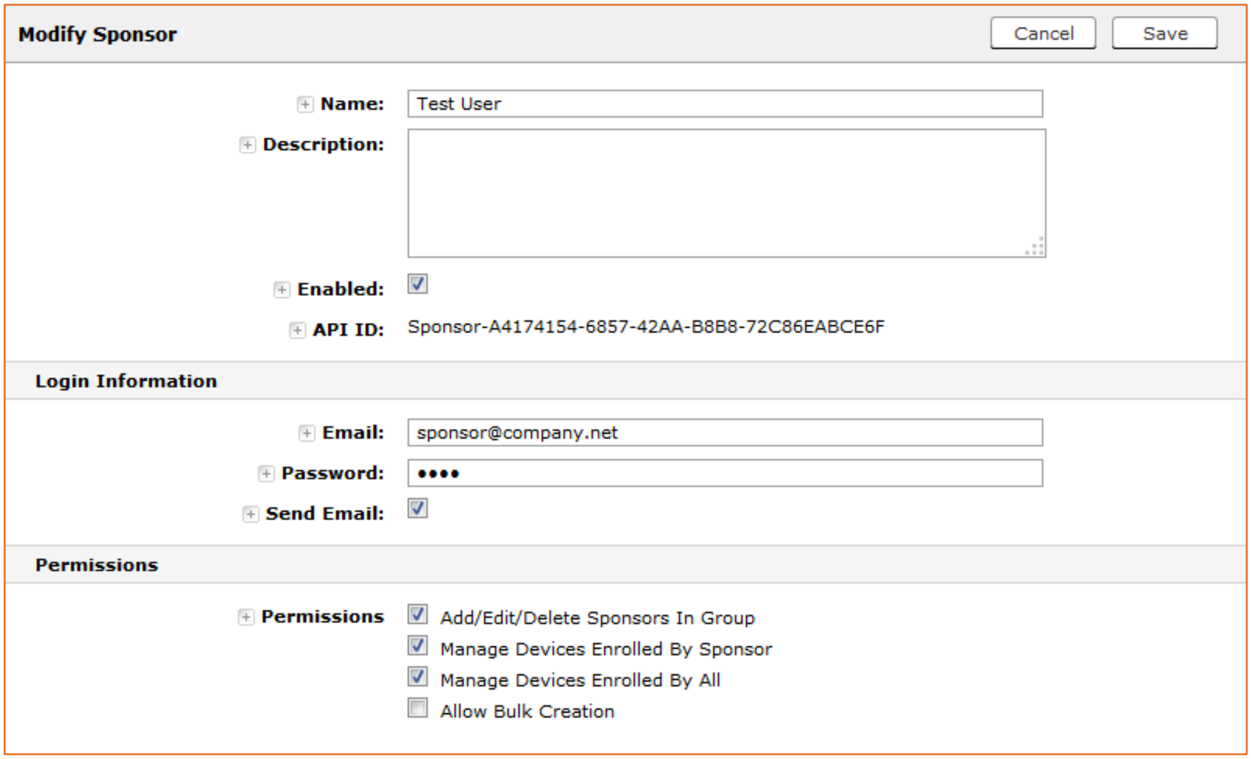
Sponsor Email

Enter the email address of the sponsor below. This will be used as their username.

Email: |

FIGURE 42: SPONSOR EMAIL

11. Enter the email address of the sponsor for this voucher list and click Continue. The email address becomes their Name.



Modify Sponsor

Name: Test User

Description:

Enabled: ☑

API ID: Sponsor-A4174154-6857-42AA-B8B8-72C86EABCE6F

Login Information

Email: sponsor@company.net

Password: ••••

Send Email: ☑

Permissions

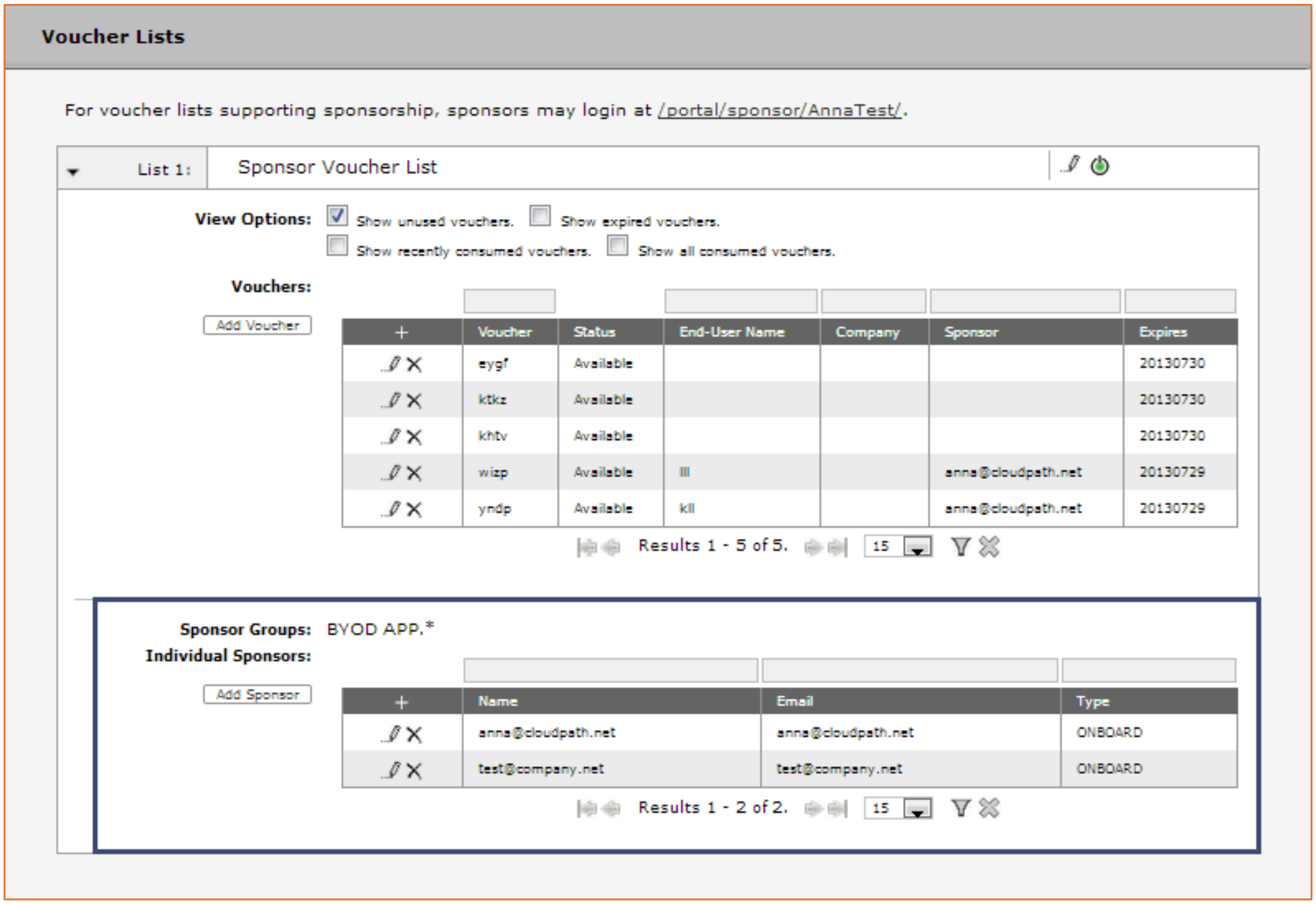
Permissions:
- ☑ Add/Edit/Delete Sponsors In Group
- ☑ Manage Devices Enrolled By Sponsor
- ☑ Manage Devices Enrolled By All
- ☐ Allow Bulk Creation

FIGURE 43: ES ADMIN UI - MODIFY SPONSOR

12. On the Modify Sponsor page, enter the sponsor Name, Description, and Enable the sponsor.
13. In the Login Information section, enter the sponsor's Email address and Password. If you check the Send Email box, this information is emailed to the sponsor.
14. In the Permissions section, check the box for the appropriate sponsor permissions.
    - Add/Edit/Delete Sponsors In Group - If checked, the sponsor can add, edit, and delete other sponsors within the group.
    - Manage Devices Enrolled By Sponsor - If checked, the sponsor can review and revoke devices enrolled via vouchers issued by that sponsor.
    - Manage Devices Enrolled By All - If checked, the sponsor can review and revoke devices enrolled via vouchers issued by any sponsor (within the Voucher List).
    - Allow Bulk Creation - If checked, the sponsor can create vouchers in bulk by importing a spreadsheet of vouchers. A default

template is provided.

15. Save the sponsor information. The sponsor information is displayed in the lower part of the voucher list.



Voucher Lists

For voucher lists supporting sponsorship, sponsors may login at /portal/sponsor/AnnaTest/.

List 1: Sponsor Voucher List

View Options: ☑ Show unused vouchers. ☐ Show expired vouchers. ☐ Show recently consumed vouchers. ☐ Show all consumed vouchers.

Vouchers:

+	Voucher	Status	End-User Name	Company	Sponsor	Expires
✎ ✕	eygf	Available				20130730
✎ ✕	ktkz	Available				20130730
✎ ✕	khtv	Available				20130730
✎ ✕	wizp	Available	lll		anna@cloudpath.net	20130729
✎ ✕	yndp	Available	kll		anna@cloudpath.net	20130729

Results 1 - 5 of 5. 15

Sponsor Groups: BYOD APP.*
Individual Sponsors:

+	Name	Email	Type
✎ ✕	anna@cloudpath.net	anna@cloudpath.net	ONBOARD
✎ ✕	test@company.net	test@company.net	ONBOARD

Results 1 - 2 of 2. 15

FIGURE 44: ES ADMIN UI - VOUCHER LISTS

External Sponsors

An external sponsor uses AD or LDAP credentials to log into the Sponsorship Portal. An external sponsor can create voucher, invite users to join the secure network, and if the voucher list permissions allow, they can manage other sponsors and enrolled devices. If you want to allow sponsors to log in to the Sponsorship Portal using AD or LDAP credentials, the authentication server must be configured with the specified username or group name filter.

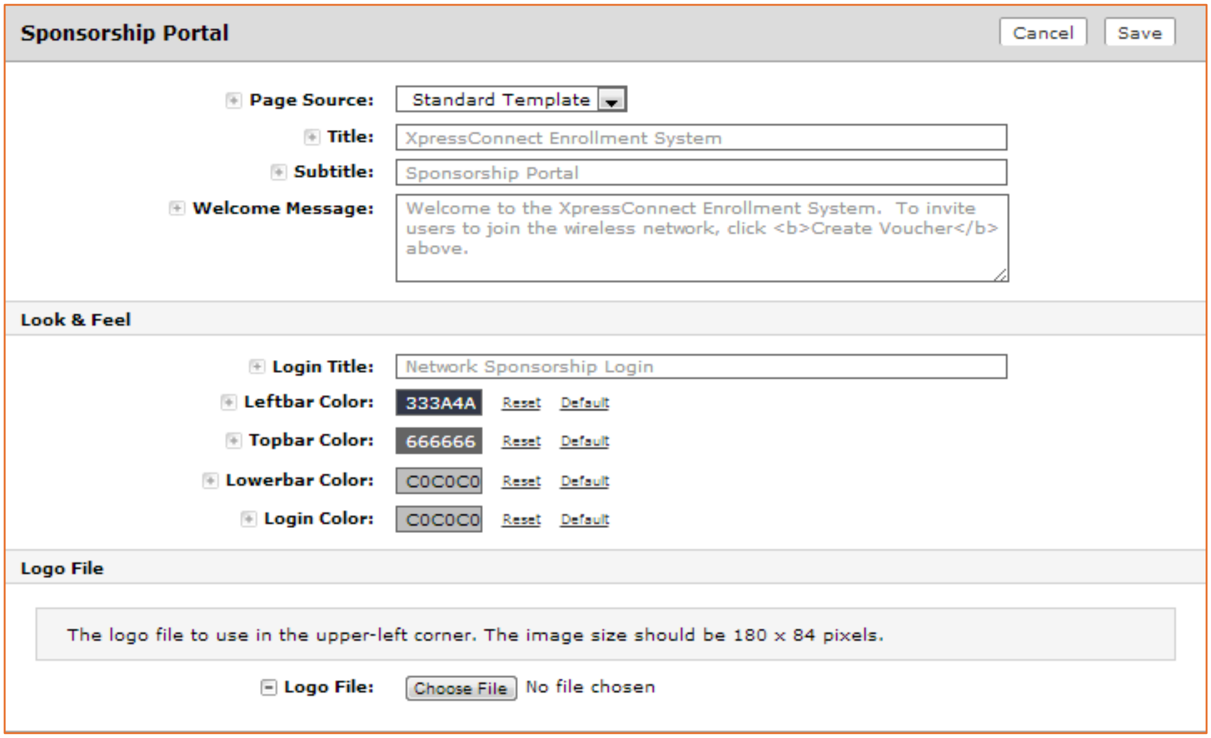
Sponsorship Portal

From the sponsorship portal, a sponsor can invite guest users to join the network by creating one or multiple vouchers, view outstanding, consumed, expired, and revoked vouchers, and manage devices, and sponsor accounts in your AD or LDAP group. Use the Sponsorship Portal if guest access is managed using voucher lists.

How to Customize Sponsorship Portal

You can customize the labeling, images, and colors for the sponsorship portal.

1. From the ES Admin UI, go to Sponsorship > Look & Feel. The sponsorship portal System Setup page displays the titles and colors for the sponsorship portal.
2. Click Edit to customize the sponsorship portal.



Sponsorship Portal

Page Source: Standard Template

Title: XpressConnect Enrollment System

Subtitle: Sponsorship Portal

Welcome Message: Welcome to the XpressConnect Enrollment System. To invite users to join the wireless network, click <b>Create Voucher</b> above.

Look & Feel

Login Title: Network Sponsorship Login

Leftbar Color: 333A4A

Topbar Color: 666666

Lowerbar Color: C0C0C0

Login Color: C0C0C0

Logo File

The logo file to use in the upper-left corner. The image size should be 180 x 84 pixels.

Logo File: No file chosen

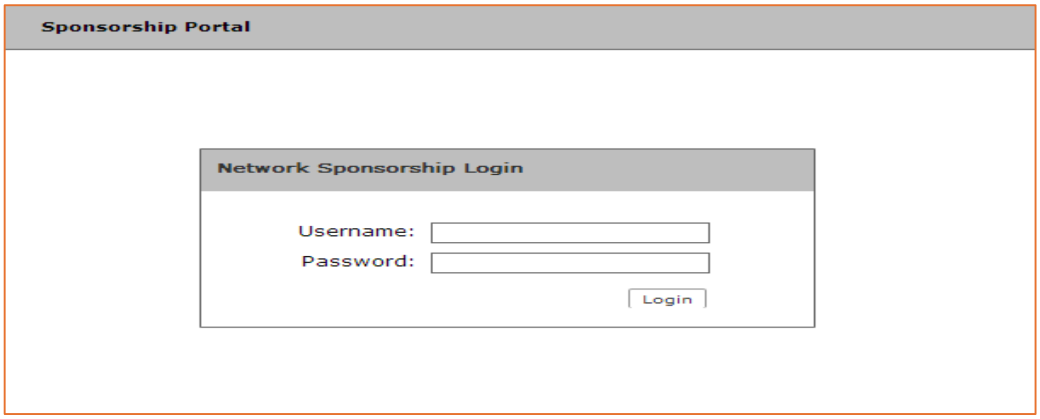
FIGURE 45: CUSTOMIZE SPONSORSHIP PORTAL

3. Modify titles and colors as needed.
4. 4. To import a customized logo file to display in the upper-left corner of the sponsorship portal, the image size should be 180 x 84
5. pixels.
6. Save the customizations.

Managing Vouchers From the Sponsorship Portal

Sponsors can access the sponsorship portal by entering the sponsorship URL https://<SponsorshipLoginIPaddress>/portal/sponsor/. When the portal login page opens, follow these steps to sponsor a guest:

1. Log into the sponsorship portal



Sponsorship Portal

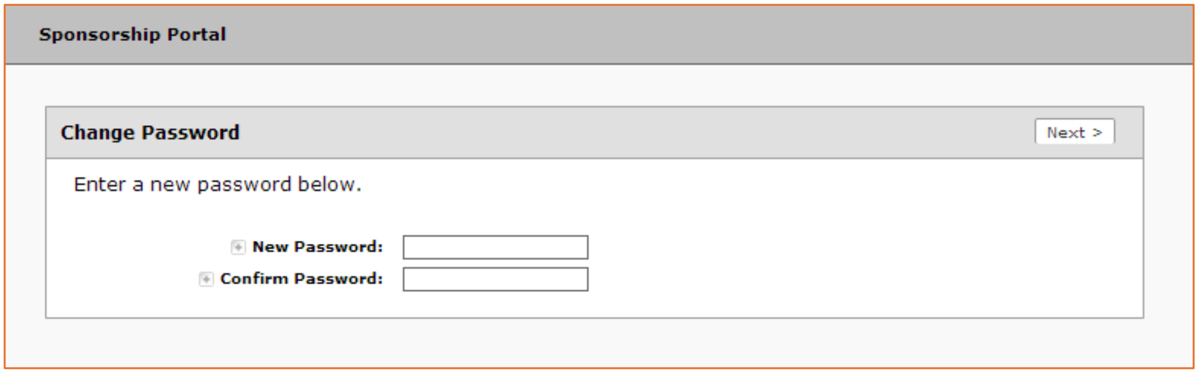
Network Sponsorship Login

Username:

Password:

FIGURE 46: SPONSORSHIP PORTAL LOGIN

2. Enter the Username and Password that was sent when the voucher list was created.
3. 4. The first time a sponsor logs in, the password must be changed.



Sponsorship Portal

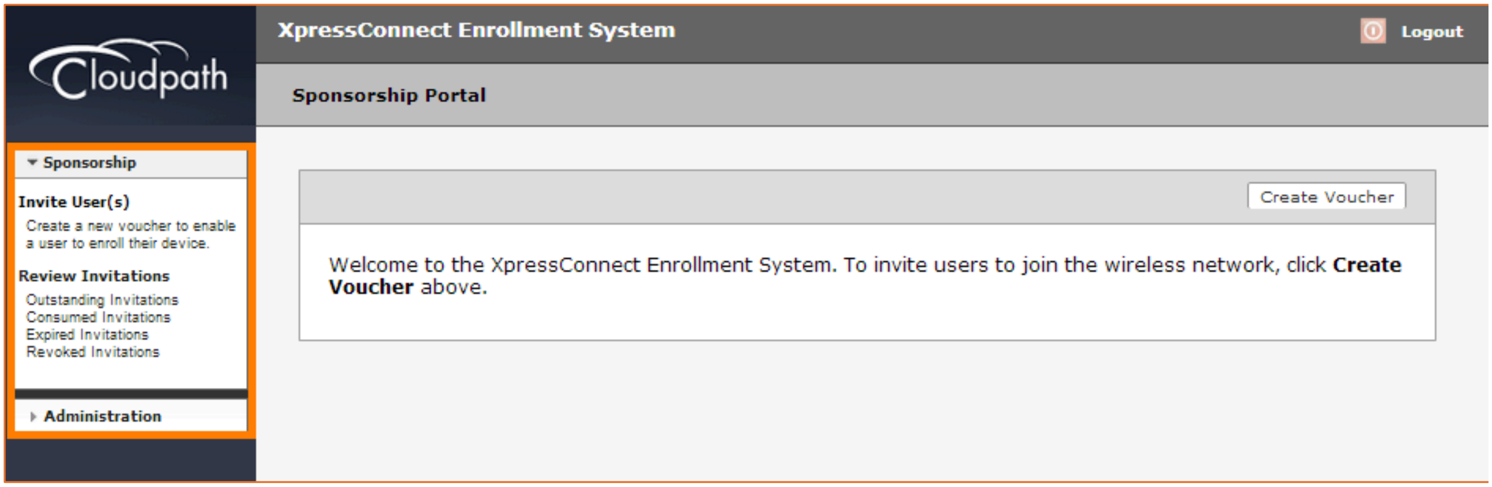
Change Password

Enter a new password below.

New Password:
Confirm Password:

FIGURE 47: SPONSORSHIP PORTAL - CHANGE PASSWORD

After the password updates, the Sponsorship Portal opens.



Welcome to the XpressConnect Enrollment System. To invite users to join the wireless network, click **Create Voucher** above.

FIGURE 48: SPONSORSHIP PORTAL NAVIGATION MENU

The left-hand navigation menu includes tabs for Sponsorship operations and Administration operations. Use the sponsorship tab to invite users and review outstanding, consumed, expired, and revoked invitations. The Administration tab is where sponsors can add, change, or remove other sponsors (if allowed by the administrator).

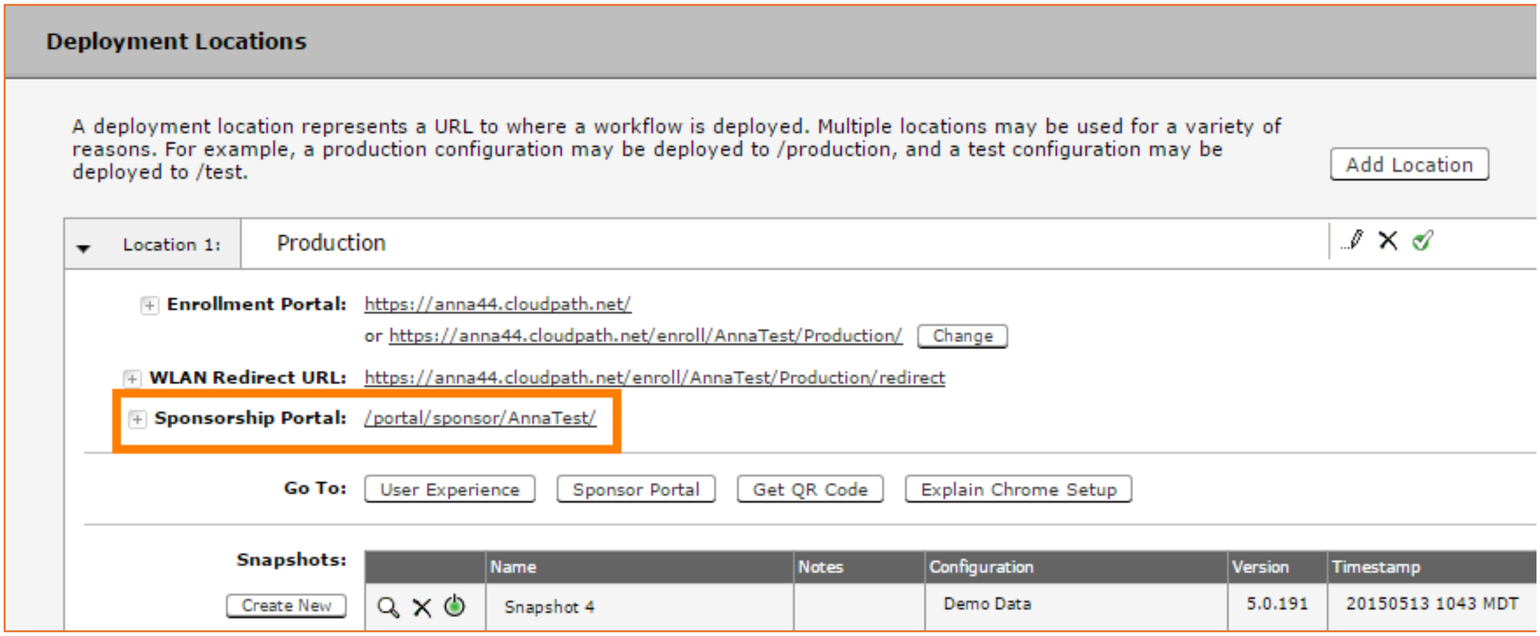
For more information on how to manage invitations and sponsors, please refer to the Cloudpath administrator's guide.

Sponsorship Process

The Sponsor Experience - Generated Voucher Lists

An administrator gives an employee permission to sponsor guest users by placing them in a Sponsor group in the corporate authentication server (AD or LDAP). When a visitor arrives, the employee sponsor checks the visitor in. To provide a guest user with network access, the sponsor must log in to the Sponsorship Portal to create a voucher for the guest user. Sponsors can access the Sponsorship Login Portal from:

- ES Admin UI Deployment Locations page or Sponsor Portal button.
- ES Admin UI Voucher Lists page
- The Sponsorship URL: https:<sponsorshipLoginIPaddress>/portal/sponsor



Deployment Locations

A deployment location represents a URL to where a workflow is deployed. Multiple locations may be used for a variety of reasons. For example, a production configuration may be deployed to /production, and a test configuration may be deployed to /test.

Location 1: Production

Enrollment Portal: https://anna44.cloudpath.net/
or https://anna44.cloudpath.net/enroll/AnnaTest/Production/

WLAN Redirect URL: https://anna44.cloudpath.net/enroll/AnnaTest/Production/redirect

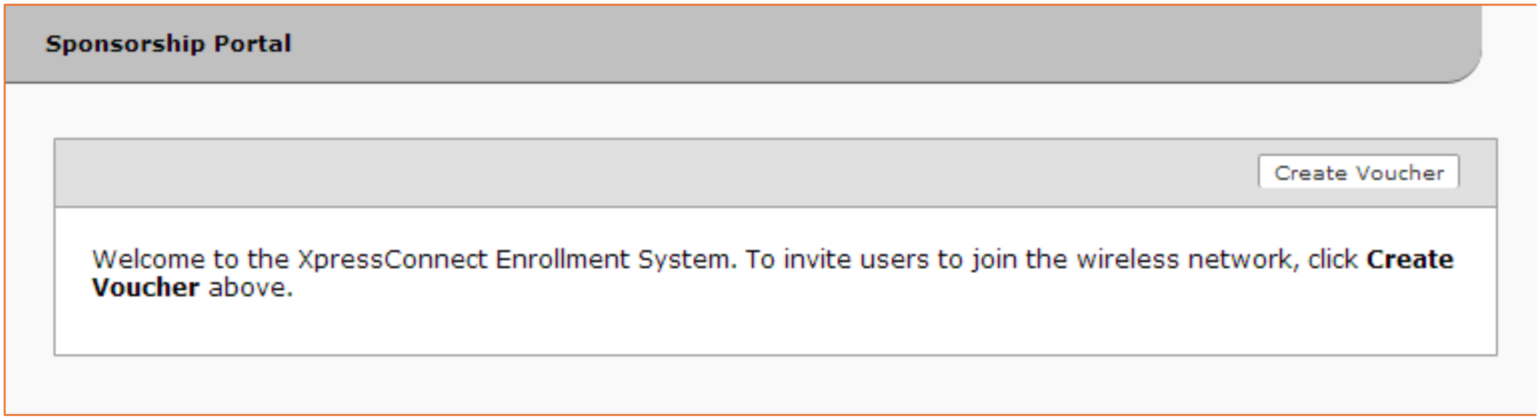
Sponsorship Portal: /portal/sponsor/AnnaTest/

Snapshots:

	Name	Notes	Configuration	Version	Timestamp
	Snapshot 4		Demo Data	5.0.191	20150513 1043 MDT

FIGURE 49: LINK TO SPONSORSHIP LOGIN PAGE - DEPLOYMENT LOCATIONS PAGE

After sponsor credentials are checked against the corporate authentication server, the sponsorship portal Welcome page appears.

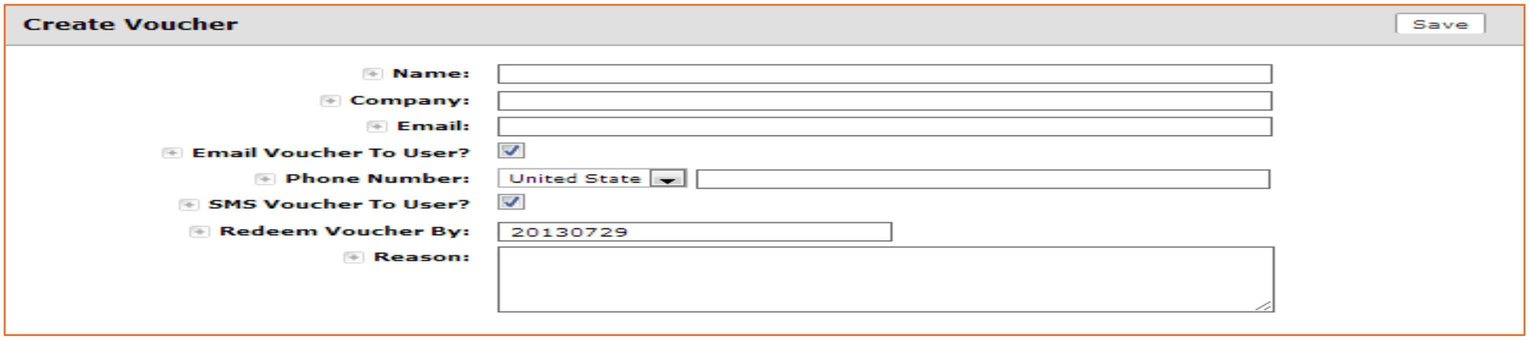


Sponsorship Portal

Welcome to the XpressConnect Enrollment System. To invite users to join the wireless network, click **Create Voucher** above.

FIGURE 50: SPONSORSHIP PORTAL WELCOME PAGE

The sponsor clicks the Create Voucher button to create a voucher for the guest user.



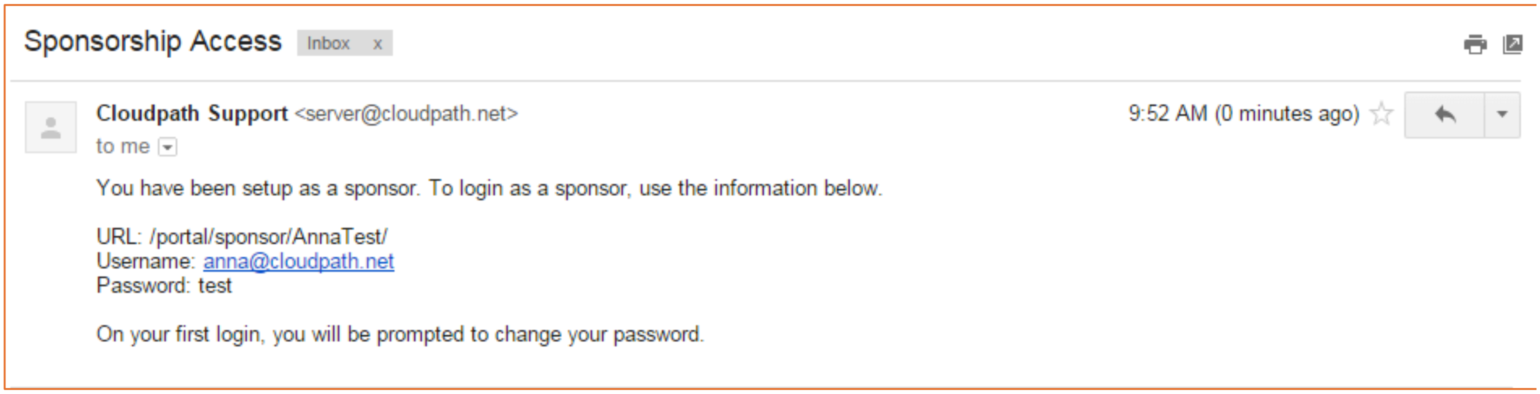
Name:
Company:
Email:
Email Voucher To User? ☑
Phone Number: United State
SMS Voucher To User? ☑
Redeem Voucher By: 20130729
Reason:

FIGURE 51: CREATE VOUCHER FOR GUEST USER

The sponsorship portal can be used to create vouchers, view voucher usage, and with the correct permissions, manage vouchers and sponsors. When finished, the sponsor must log out of the sponsorship portal.

Sponsor Experience - Request Network Access

A sponsor receives an email notification that indicates they are approved for granting network access to guest users.



Cloudpath Support <server@cloudpath.net>
to me
9:52 AM (0 minutes ago)

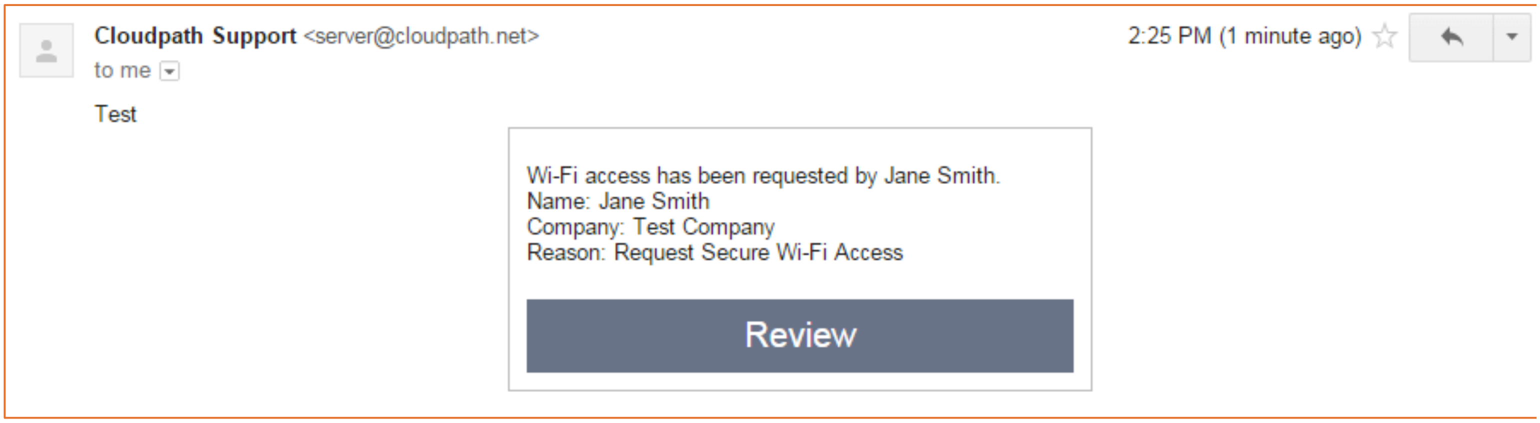
You have been setup as a sponsor. To login as a sponsor, use the information below.

URL: /portal/sponsor/AnnaTest/
Username: anna@cloudpath.net
Password: test

On your first login, you will be prompted to change your password.

FIGURE 52: EMAIL TO SPONSOR

The sponsor receives and email from the guest user requesting access. This messaging is configurable.



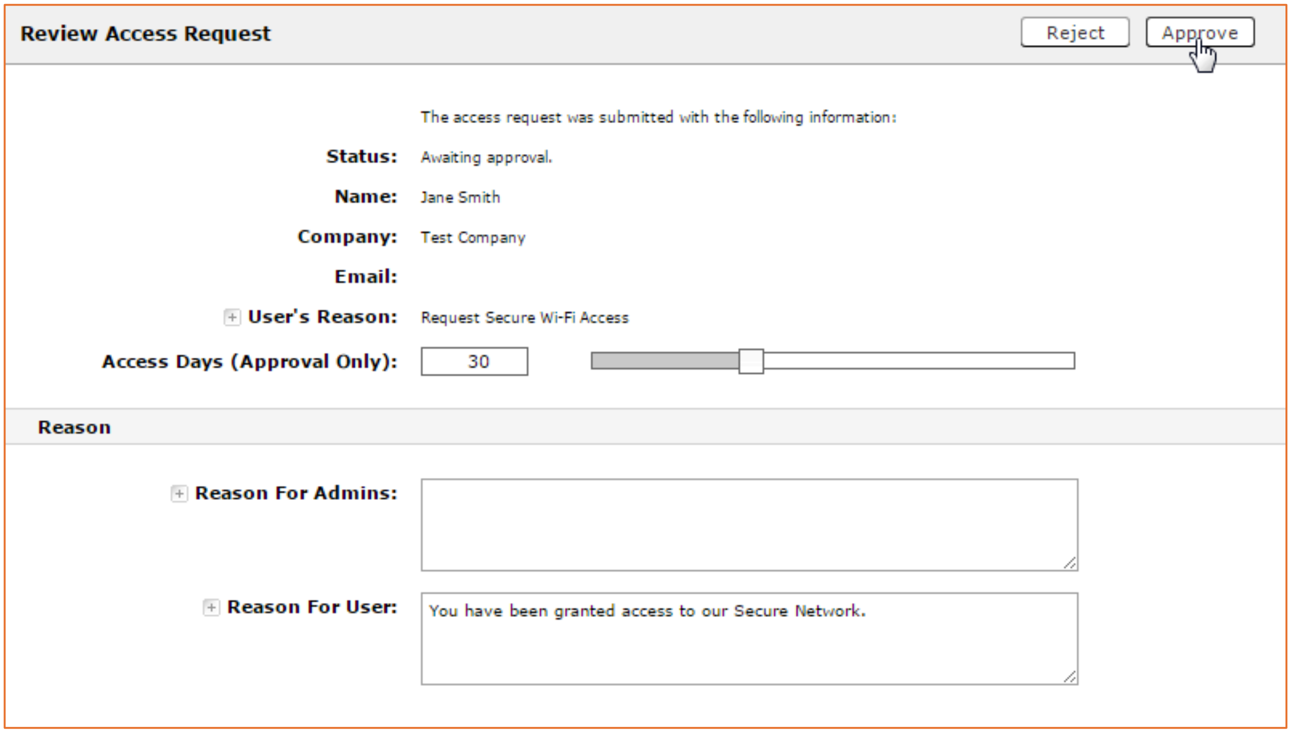
Cloudpath Support <server@cloudpath.net>
to me
2:25 PM (1 minute ago)

Test

Wi-Fi access has been requested by Jane Smith.
Name: Jane Smith
Company: Test Company
Reason: Request Secure Wi-Fi Access

FIGURE 53: EMAIL FROM SYSTEM

The sponsor clicks the Review button to review the request and respond to the user.



Review Access Request

The access request was submitted with the following information:

Status: Awaiting approval.

Name: Jane Smith

Company: Test Company

Email:

User's Reason: Request Secure Wi-Fi Access

Access Days (Approval Only): 30

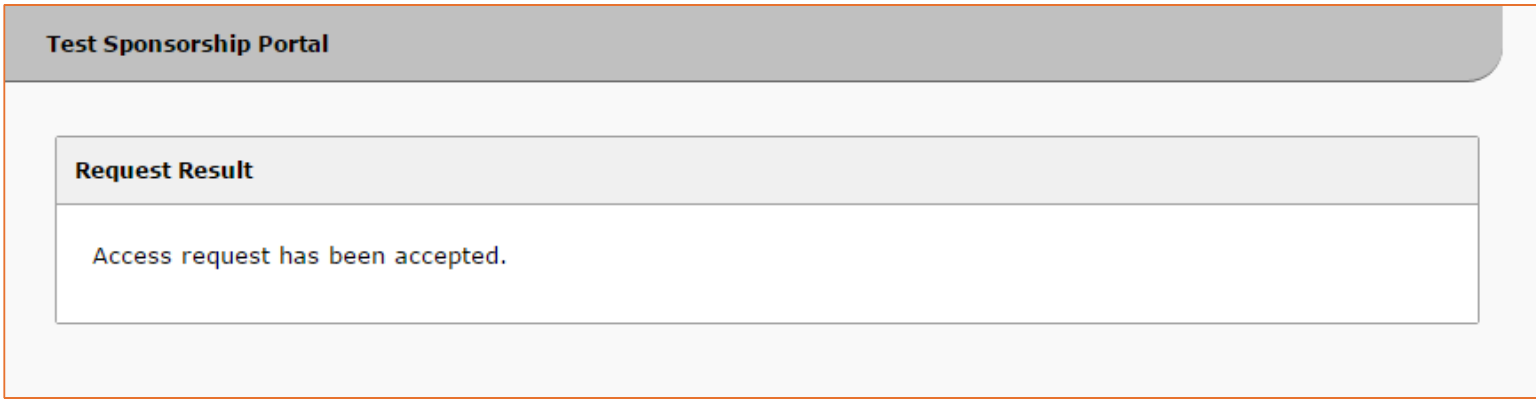
Reason

Reason For Admins:

Reason For User: You have been granted access to our Secure Network.

FIGURE 54: SPONSOR APPROVES GUEST ACCESS

Sponsor receives confirmation that access has been accepted.



Test Sponsorship Portal

Request Result

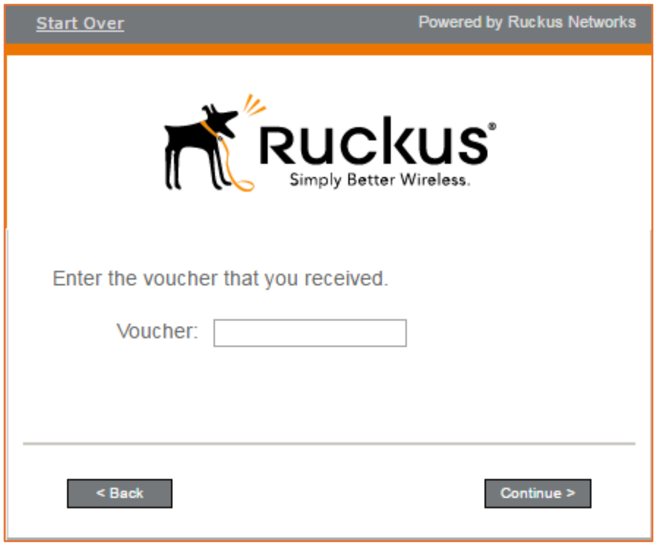
Access request has been accepted.

FIGURE 55: ACCESS ACCEPTED CONFIRMATION

Guest User Process

Guest User Experience - Generated Voucher Lists

The guest user receives the voucher from the sponsor (by email, SMS, or manual delivery), accesses the onboarding wireless network, and is redirected to the Cloudpath system. As part of the enrollment process, the visitor is prompted for the voucher code.



Enter the voucher that you received.

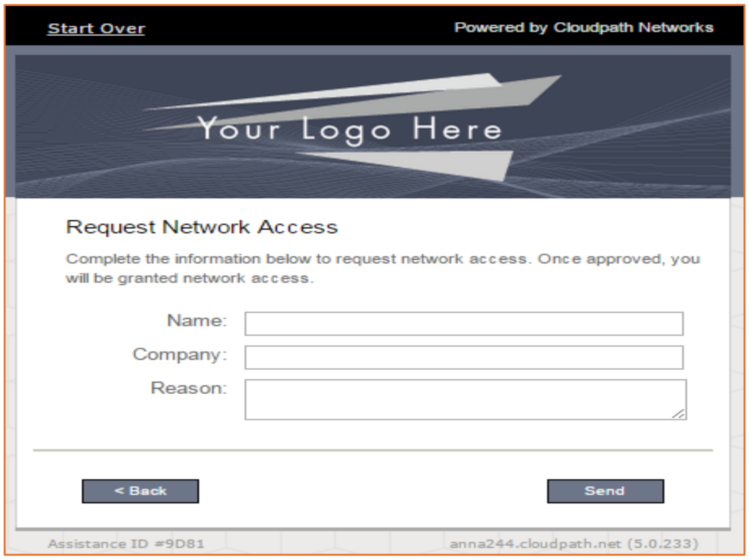
Voucher:

FIGURE 56: VOUCHER PROMPT FOR GUEST USER

The guest user enters the voucher code provided by the sponsor and continues with the enrollment process to gain access to the secure network.

Guest User Experience - Request Network Access

The guest user connects to the onboarding SSID. If you have a captive portal configured, they are redirected to the Cloudpath system to enroll their device for the secure SSID. If no captive portal is configured, an enrollment URL is provided to them. As part of the enrollment process, the guest is prompted for to request access to the secure network. The guest must wait for approval before they can continue.



Request Network Access

Complete the information below to request network access. Once approved, you will be granted network access.

Name:

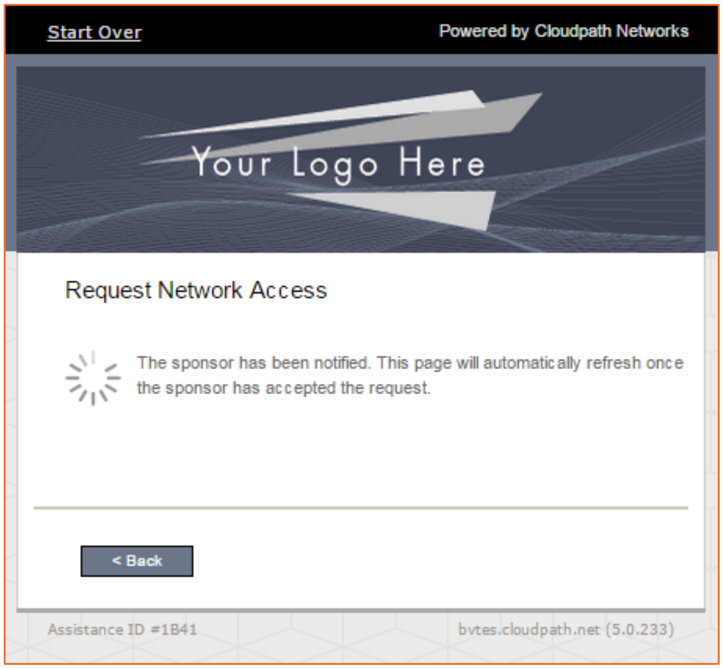
Company:

Reason:

Assistance ID #9D81 anna244.cloudpath.net (5.0.233)

FIGURE 57: ENROLLMENT PROCESS REQUEST ACCESS FORM

The user enters the required information. The list of required fields is configurable.



Request Network Access

The sponsor has been notified. This page will automatically refresh once the sponsor has accepted the request.

FIGURE 58: PENDING ACCESS REQUEST

If the access is approved, the user continues with the enrollment process. The next screen the users sees depends on how the network

Example Use Case – Generated Voucher Lists

During the setup of the Cloudpath Enrollment System (ES), the network administrator specifies that visitors may gain network access if they are sponsored. The network administrator specifies that anyone belonging to the Wireless Sponsors group within Active Directory can sponsor a guest. Along with this, the network administrator specifies that access is valid for three days.

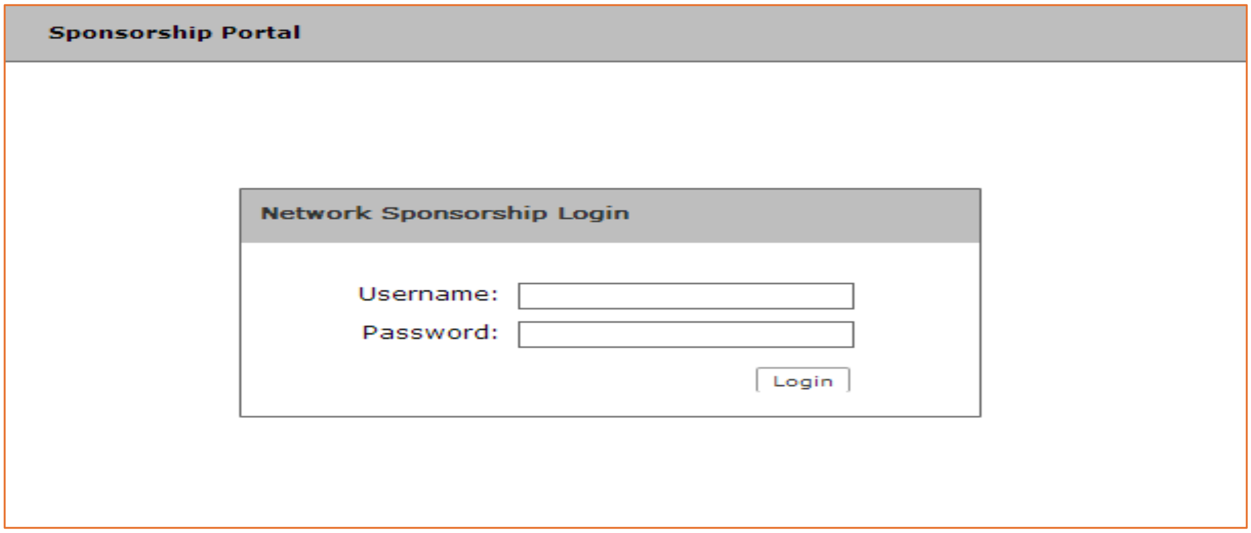


FIGURE 59: CLOUDPATH SPONSORSHIP LOGIN PAGE

Prior to the guest's arrival, the sponsor accesses the sponsorship portal. After authenticating with the Active Directory server, the sponsor can specify details about the guest user, including name, email address, and the reason for sponsorship. After doing so, a unique voucher is generated for the guest user.

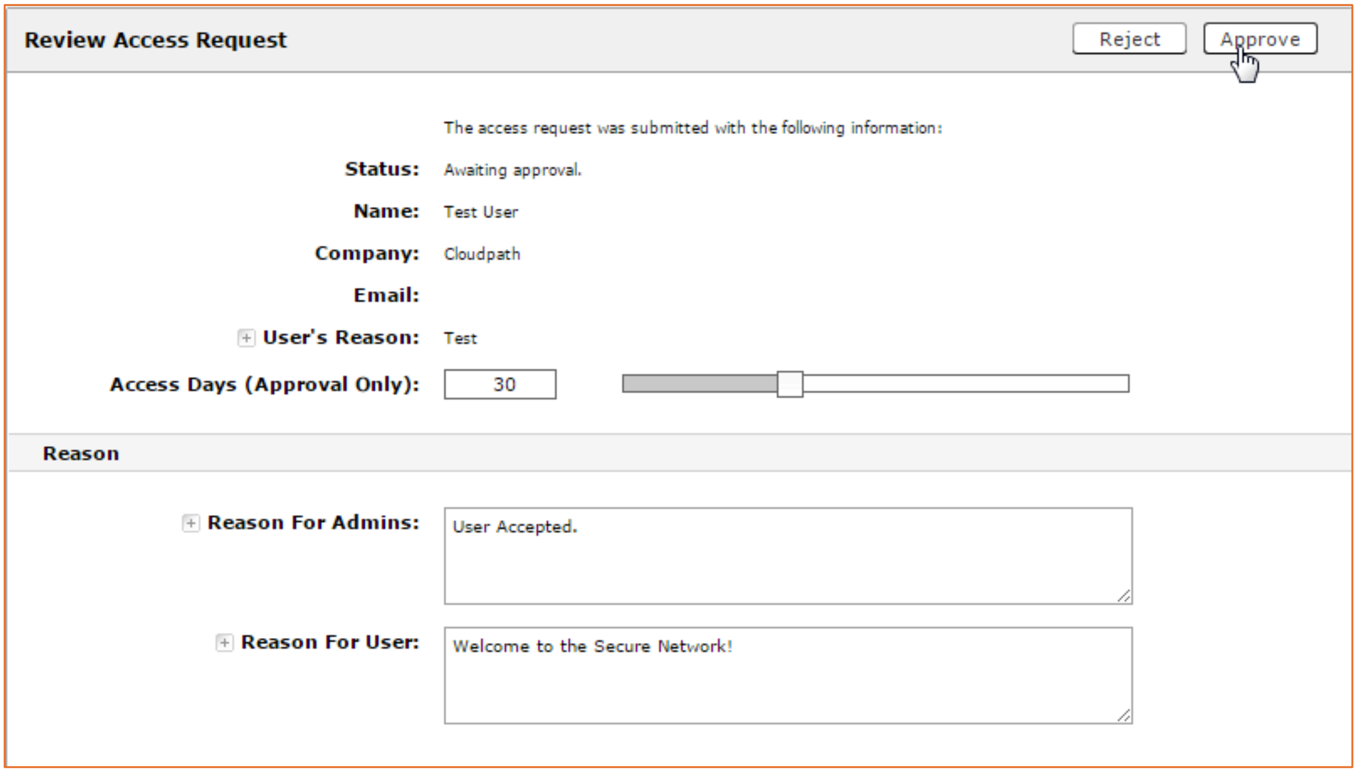
A voucher is a one-time password (OTP) and is useful for controlling access to an enrollment process separate from, or in addition to, user credentials. The system may automatically email the guest user or the sponsor can communicate the voucher manually.

Upon arrival, the guest user accesses the onboarding wireless network. The guest user is redirected to the Cloudpath system. The guest user completes the workflow specified by the network administrator, including specifying the voucher. Once authorized, the guest user is issued a certificate and moved to the secure wireless network.

Example Use Case – Request Network Access

While the Generated Vouchers use case requires the sponsor to pre-sponsor a user by generating a voucher ahead of time, the Request Network Access use case allows the user to enter their information on a webpage during the enrollment process, and request access. The user is held in a pending state until the sponsor accepts or rejects the request. The request may go to a static user (like a receptionist), to a sponsor selected from a list by the user, or to a sponsor entered by the user.

In this use case, Cloudpath is set up with a Request Access workflow plug-in, which allows the on-demand access to occur. This enrollment step allows the user to request access to the network as part of the enrollment process. It is not necessary to create a voucher list ahead of time.



Review Access Request

The access request was submitted with the following information:

Status: Awaiting approval.

Name: Test User

Company: Cloudpath

Email:

User's Reason: Test

Access Days (Approval Only): 30

Reason

Reason For Admins: User Accepted.

Reason For User: Welcome to the Secure Network!

FIGURE 60: REVIEW ACCESS REQUEST

Upon arrival, the guest user accesses the onboarding wireless network. The guest user is redirected to the Cloudpath system. The guest user completes the workflow specified by the network administrator, and when the guest encounters the request access step, they fill in the required information and this information is sent to an approved sponsor. The sponsor can approve the access request, which allows the user to continue with the enrollment process. Once authorized, the guest user is issued a certificate and moved to the secure wireless network.

Support for Headless Devices

What Are "Headless Devices"?

Unlike a laptop, smartphone or table, headless devices typically lack a traditional monitor and have a limited input. Examples include WebTV devices (Rocku, AppleTV, Chromecast), interactive whiteboards, printers, possibly game stations, etc. Typically, such devices do not support 802.1X security and are limited to PSK or open WLANs. They are generally marketed for home use, and the designers, not unreasonably, expect them to use home networks which typically do not rely on full blown RADIUS based PKI certificates.

Nevertheless, these devices are often useful in the classroom, even if the original design has not accounted for robust network security. However, Cloudpath ES can utilize another Ruckus technology, Dynamic Pre-Shared Key (DPSK) to enable simple onboarding and robust security of these devices.

What is Ruckus DPSK?

When a user asks "what's the Wi-Fi password?", in strict network security terms, they are asking for the Pre-Shared Key, or PSK, of the WLAN. "Pre-shared", because everyone knows it, and "key" because it unlocks the WLAN's privacy encryption. It is perfectly good security for a home WLAN or a small office with a limited number of users, but not good practice in even the smallest of schools. However, Ruckus has a technology that can piggy back on PSK WLANs and give every device a unique encryption key ("Wi-Fi password").

Dynamic Pre-Shared Key (DPSK) is a patented technology that can provide robust and secure wireless access for devices that can only accept PSK level security. Dynamic PSK creates a unique encryption key (up to 63 bytes) for each device accessing a PSK WLAN. Although there is a master PSK for the WLAN, there is no need to share it - although it can be used if needed by IT personnel. With Ruckus DPSK, devices that do not support 802.1X and certificates can still be uniquely registered and tracked on the network with a record of the registering owner.

Using Cloudpath with Ruckus DPSK

We can add a branch to the Cloudpath ES workflow for the user to "register a headless device" – or other language that will make sense to your users. Cloudpath can then be configured to check the user's credentials and, if accepted, communicate with the Ruckus Controller to generate a DPSK and keep a record of the registering user. The DPSK is sent to the user, and can be typed into the device like a normal "wi-fi password", at which point the DPSK is locked to that one device (bound to it's MAC address), and is already registered to the particular user.

Configuration Procedure

The following steps are required to configure Cloudpath with Ruckus DPSK.

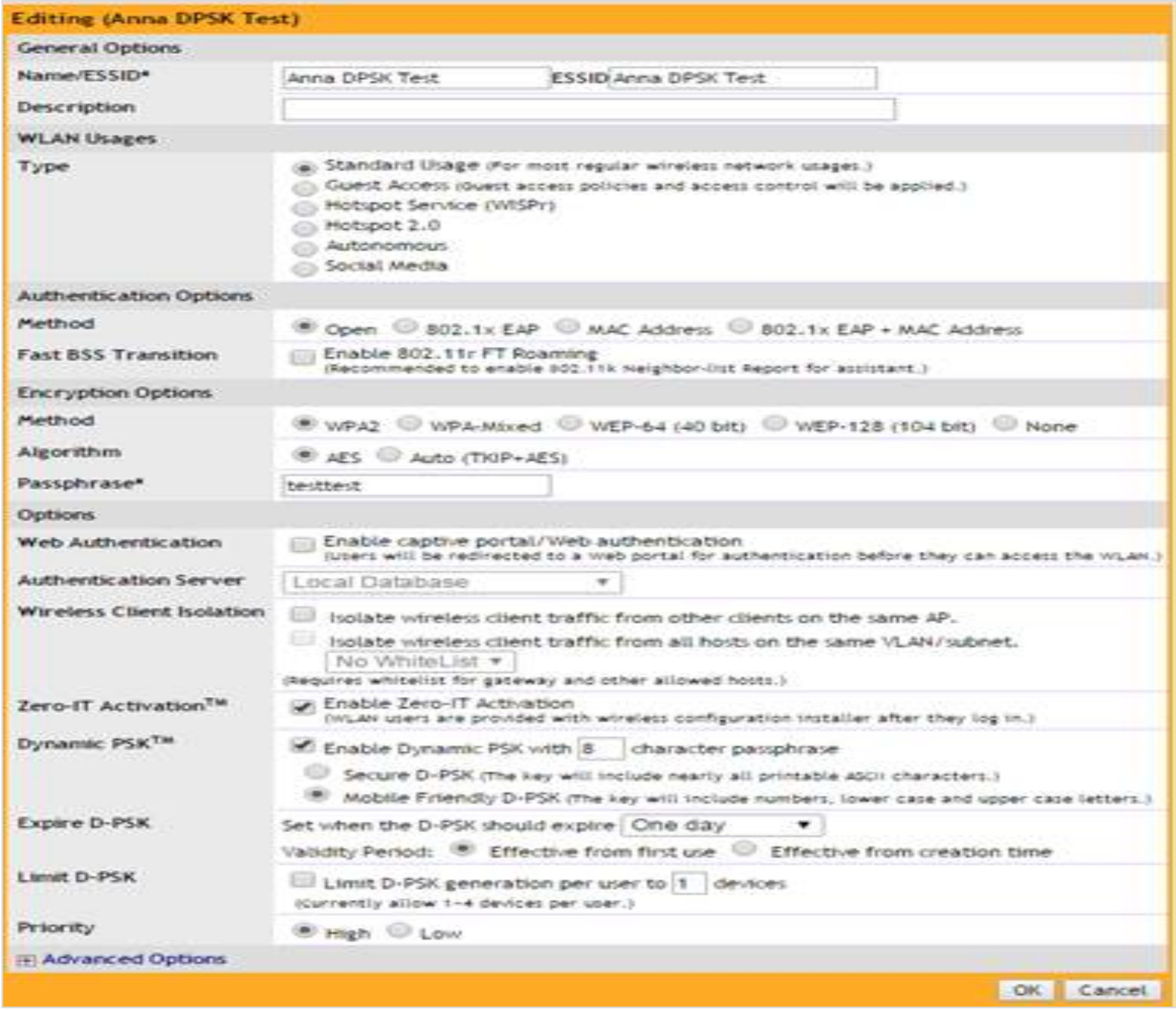
1. Configure Ruckus controller (ZoneDirector or SmartZone) with a DPSK-enabled SSID
2. Configure the access to the Ruckus WLAN controller for Cloudpath ES
3. Enable the Northbound Interface for ZoneDirector
4. Create a username/password identity on SmartZone
5. Configure the Cloudpath ES workflow and deploy

Step 1: Configure the DPSK-enabled SSID

ZoneDirector DPSK WLAN Configuration

Use these steps to configure a WLAN with DPSK enabled on it on ZoneDirector controllers. You will create a standard PSK WLAN and then check the necessary options to enable DPSK. Note that, for historical reasons, we will need to enable Zero-IT to configure DPSK. However, we will not be making use Zero-IT (a precursor to Cloudpath ES) . Also, we will add a "master" PSK to this WLAN. Keep in mind, this is a normal PSK ("Wi-Fi password") for the WLAN, and will work for any device or even any number of devices. Unlike the typical PSK WLAN, only the

WLAN administrator should know this PSK. Ideally, no device should use this key. ALL devices that access the WLAN should be registered via Cloudpath ES and all should use a unique DPSK.



Editing (Anna DPSK Test)

General Options	
Name/ESSID*	Anna DPSK Test ESSID Anna DPSK Test
Description	
WLAN Usages	
Type	● Standard Usage (For most regular wireless network usages.) ○ Guest Access (Guest access policies and access control will be applied.) ○ Hotspot Service (WISPr) ○ Hotspot 2.0 ○ Autonomous ○ Social Media
Authentication Options	
Method	● Open ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address
Fast BSS Transition	□ Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)
Encryption Options	
Method	● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ○ None
Algorithm	● AES ○ Auto (TKIP+AES)
Passphrase*	testtest
Options	
Web Authentication	□ Enable captive portal/Web authentication (Users will be redirected to a web portal for authentication before they can access the WLAN.)
Authentication Server	Local Database ▾
Wireless Client Isolation	□ Isolate wireless client traffic from other clients on the same AP. □ Isolate wireless client traffic from all hosts on the same VLAN/subnet. No WhiteList ▾ (Requires whitelist for gateway and other allowed hosts.)
Zero-IT Activation™	☑ Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
Dynamic PSK™	☑ Enable Dynamic PSK with 8 character passphrase ○ Secure D-PSK (The key will include nearly all printable ASCII characters.) ● Mobile Friendly D-PSK (The key will include numbers, lower case and upper case letters.)
Expire D-PSK	Set when the D-PSK should expire One day ▾ Validity Period: ● Effective from first use ○ Effective from creation time
Limit D-PSK	□ Limit D-PSK generation per user to 1 devices (Currently allow 1-4 devices per user.)
Priority	● High ○ Low
⊞ Advanced Options	

FIGURE 61: RUCKUS ZONEDIRECTOR WLAN CONFIG

1. Go to Configure > WLANs
2. Either Edit an existing WLAN or Create New to open the WLAN configuration form.
3. Under Type, select Standard Usage.
4. Under Authentication Options: Method, select MAC Address or Open.
5. Under Encryption Options: Method, select WPA2 (*not* WPA-Mixed, as selecting WPA-Mixed will disable the Zero-IT activation option).
6. Under *Encryption Options: Algorithm*, select AES (not Auto, as selecting Auto will disable the Zero-IT activation option).
7. If using MAC Address authentication, choose an Authentication Server to authenticate clients against--either Local Database or RADIUS Server.
8. Ensure that the Zero-IT Activation check box is enabled.
9. Next to Dynamic PSK, enable the check box next to Enable Dynamic PSK. Select a DPSK passphrase length (between 8 and 62

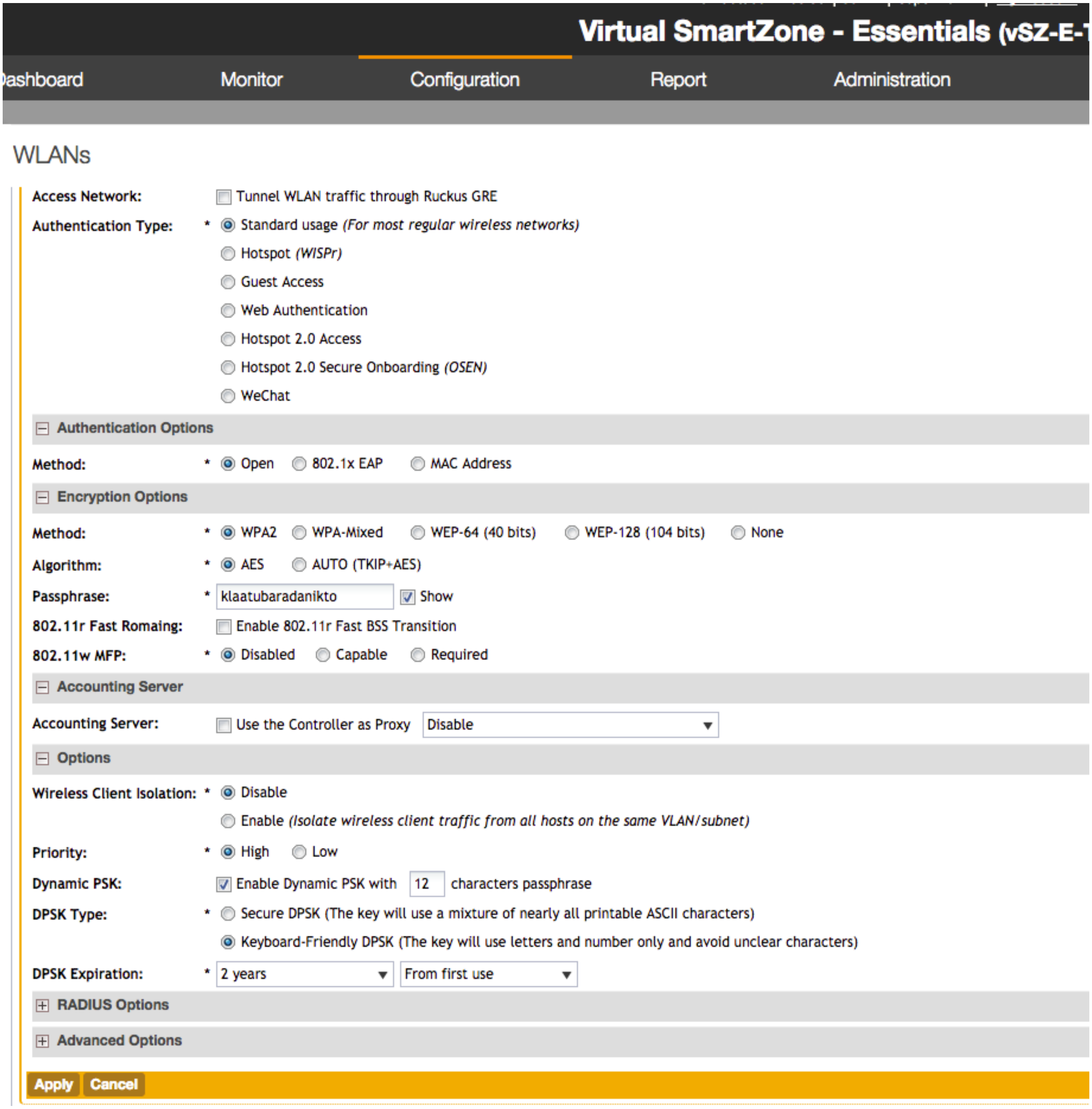
10. Note: users will type these characters into the PSK settings of their registered devices. They will not have to remember it, they only need to type it in at the initial configuration. Something reasonable like 8-12 characters is appropriate
11. Because we are creating this WLAN for 'headless devices,' choose **Mobile Friendly DPSK** rather than **Secure DPSK**
12. **Secure DPSK**: Includes almost all printable ASCII characters, including periods, hyphens, dashes, etc. This option is more secure, however it is difficult to input for mobile clients whose keyboards may not contain the entire set of printable ASCII characters.
13. **Mobile Friendly DPSK**: Choose this option if this WLAN will be used for mobile clients. This option limits the range of characters to lower case and upper case letters and numbers, which makes it easier for users to input the DPSK when activating a mobile client to a Zero-IT WLAN. (You may also want to limit the DPSK length to 8 characters for the convenience of your mobile client users.)
14. Expire DPSK: Set when the DPSK should expire. In Validity period, choose whether the DPSK expiration period will start from first use or creation time.
15. *Limit* DPSK: By default each authenticated user can generate multiple DPSKs. Select this option to limit the number of DPSKs each user can generate (1-4).
16. Click **OK** to save your settings.

SmartZone DPSK WLAN Configuration

Use these steps to configure a WLAN with DPSK enabled on physical and virtual SmartZone controllers. You will create a standard PSK WLAN and then check the necessary options to enable DPSK. Also, we will add a "master" PSK to this WLAN. Keep in mind, this is a normal PSK ("password") for the WLAN, and will work for any device or even any number of devices. Unlike the typical PSK WLAN, only the WLAN administrator should know this PSK. Ideally, no device should use this key. ALL devices that access the WLAN should be registered via Cloudpath and all should use a unique DPSK

1. Go to **Configuration** > **WLANs**
2. In a vSZ-H, you may have to navigate to the correct admistrative domain and Zone before choosing WLAN
3. Either **Edit** an existing WLAN or **Create New** to open the WLAN configuration form.
4. Give it a Name and SSID (by default, it will copy the name to SSID)
5. Under Type, select **Standard Usage**.
6. Under Authentication Options: Method, select **MAC Address** or **Open**.
7. Under Encryption Options: Method, select **WPA2**
8. Under Encryption Options: Algorithm, select **AES**
9. If using MAC Address authentication, choose an Authentication Server to authenticate clients against--either **Local Database** or **RADIUS Server**. Most likely this is unnecessary when using Cloudpath
10. Next to Dynamic PSK, enable the check box next to **Enable Dynamic PSK**. Select a DPSK passphrase length (between 8 and 62 characters).
11. Note: users will type these characters into the PSK settings of their registered devices. Something reasonable like 12 characters is appropriate
12. Because we are creating this WLAN for 'headless devices,' choose or **Mobile Friendly DPSK** rather than **Secure DPSK**
13. **Secure DPSK**: Includes almost all printable ASCII characters, including periods, hyphens, dashes, etc. This option is more secure, however it is difficult to input for clients whose keyboards may not contain the entire set of printable ASCII characters.
14. **Mobile Friendly DPSK**: Choose this option if this WLAN will be used for mobile clients. This option limits the range of characters to lower case and upper case letters and numbers, which makes it easier for users to input the **DPSK** when activating a mobile client to a Zero-IT WLAN. (You may also want to limit the **DPSK** length to 8 characters for the convenience of your mobile client users.)
15. Expire **DPSK**: Set when the **DPSK** should expire. In Validity period, choose whether the **DPSK** expiration period will start from first use or creation time.
16. *Limit* **DPSK**: By default each authenticated user can generate multiple **DPSKs**. Select this option to limit the number of **DPSK** s each user can generate (1-4).

17. Click OK to save your settings.
18. This WLAN is now ready to authenticate users using Dynamic Pre-Shared Keys, once Cloudpath ES has verified their credentials and issued a DPSK.



WLANs

Access Network: □ Tunnel WLAN traffic through Ruckus GRE

Authentication Type: * ● Standard usage *(For most regular wireless networks)*
○ Hotspot *(WISPr)*
○ Guest Access
○ Web Authentication
○ Hotspot 2.0 Access
○ Hotspot 2.0 Secure Onboarding *(OSEN)*
○ WeChat

⊟ Authentication Options

Method: * ● Open ○ 802.1x EAP ○ MAC Address

⊟ Encryption Options

Method: * ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

Algorithm: * ● AES ○ AUTO (TKIP+AES)

Passphrase: * klaatubaradanikto ☑ Show

802.11r Fast Romaing: □ Enable 802.11r Fast BSS Transition

802.11w MFP: * ● Disabled ○ Capable ○ Required

⊟ Accounting Server

Accounting Server: □ Use the Controller as Proxy Disable ▾

⊟ Options

Wireless Client Isolation: * ● Disable
○ Enable *(Isolate wireless client traffic from all hosts on the same VLAN/subnet)*

Priority: * ● High ○ Low

Dynamic PSK: ☑ Enable Dynamic PSK with 12 characters passphrase

DPSK Type: * ○ Secure DPSK (The key will use a mixture of nearly all printable ASCII characters)
● Keyboard-Friendly DPSK (The key will use letters and number only and avoid unclear characters)

DPSK Expiration: * 2 years ▾ From first use ▾

⊞ RADIUS Options

⊞ Advanced Options

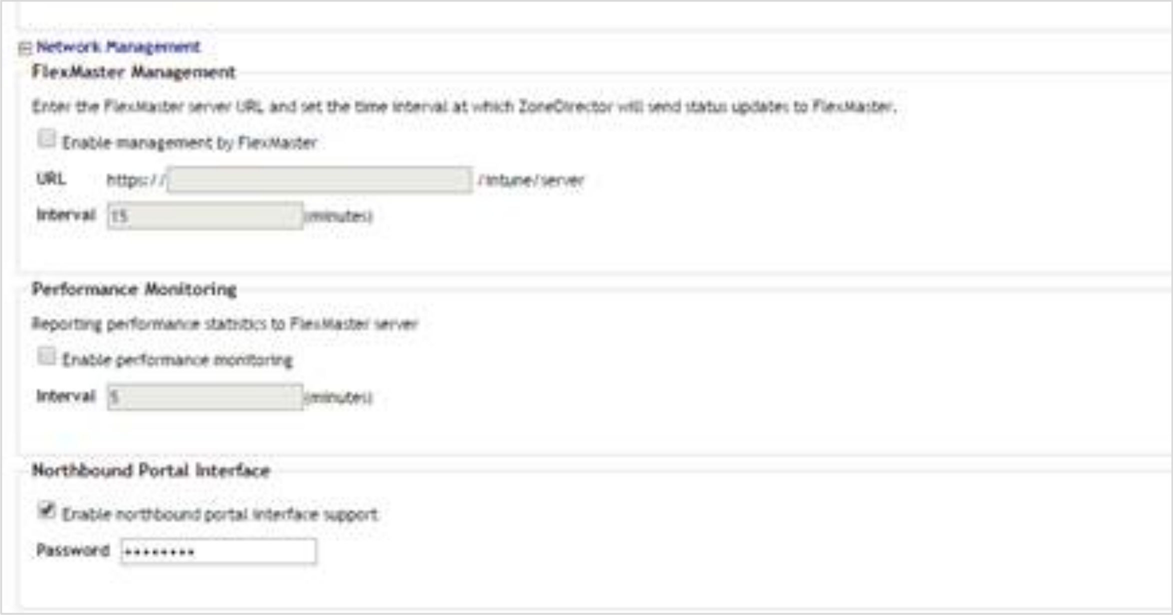
Figure 62: Ruckus SmartZone WLAN config

Step 2: Configure access to the Ruckus WLAN controller for Cloudpath ES

ZoneDirector: Configure the Northbound Interface API

Use these steps to configure a password for the NBI API.

1. Go to Configure->System
2. Scroll down to Network Management and click the plus (+) sign to expand it
3. Tick the box titled Enable northbound portal interface support and add a password
4. Click OK to save your changes



⊟ Network Management

FlexMaster Management

Enter the FlexMaster server URL and set the time interval at which ZoneDirector will send status updates to FlexMaster.

□ Enable management by FlexMaster

URL https:// /intune/server

Interval 15 (minutes)

Performance Monitoring

Reporting performance statistics to FlexMaster server

□ Enable performance monitoring

Interval 5 (minutes)

Northbound Portal Interface

☑ Enable northbound portal interface support

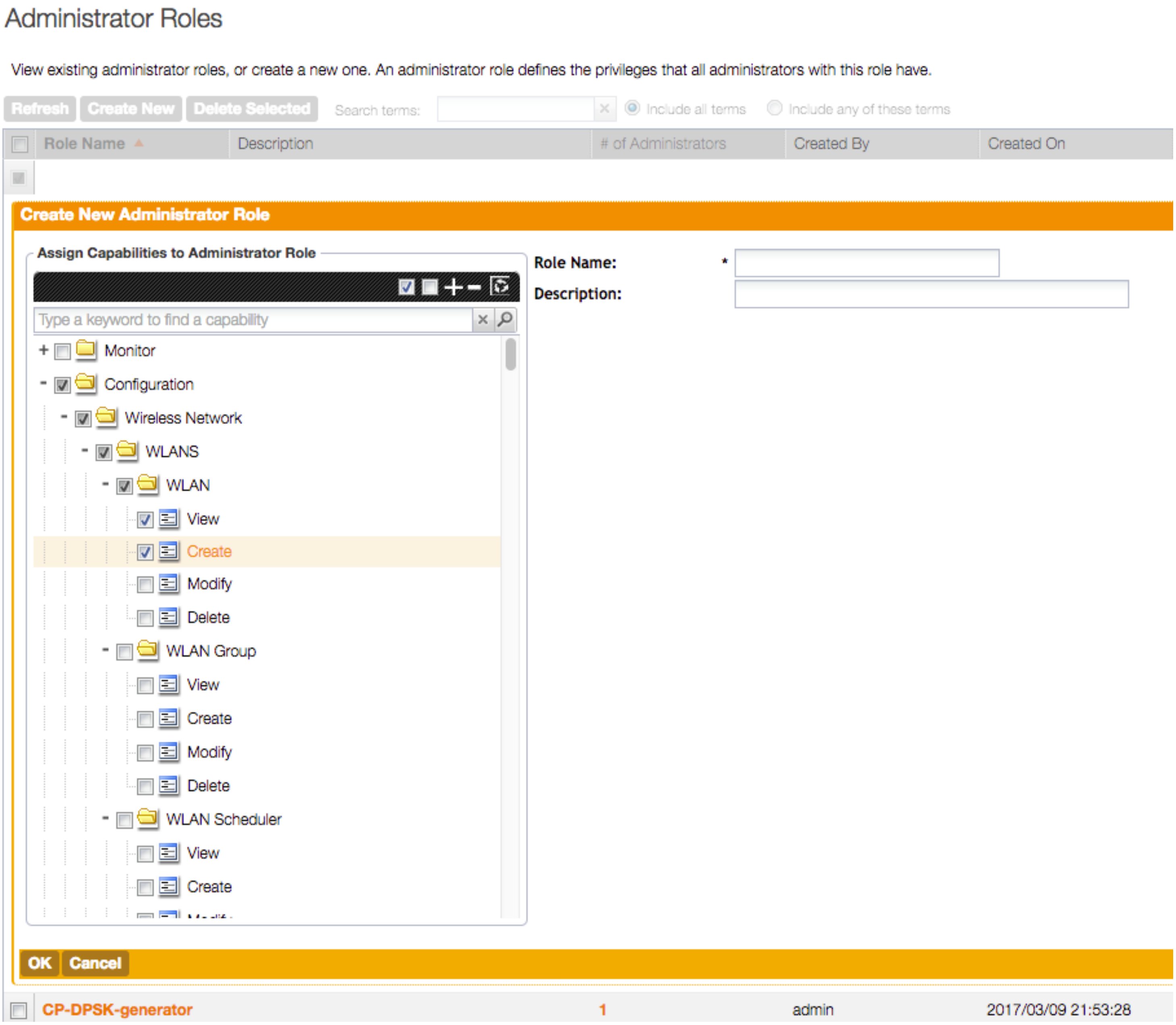
Password ••••••••

Figure 63: Ruckus Zone Director northbound interface

SmartZone: Configure a DPSK generator user role and login for Cloudpath

Create a user role for DPSK generation in SmartZone v 3.4

5. In vSZ-E or Smartzone-100, navigate to “Administration -> Administrators – >Administrator Roles., or
6. In vSZ-H or “Configuration -> Administrators” and scroll down to “Administrator Roles.
7. Choose Create New
8. Name the new role (Ex. “cloudpath-dpsk”)
9. Deselect everything with the deselect all button (square with no checkmark)
10. Navigate the tree to Configuration -> Wireless Network -> WLANs ->WLAN
11. Under WLAN, check “create” and “new”
12. Click OK in the lower left corner to save the new role



Administrator Roles

View existing administrator roles, or create a new one. An administrator role defines the privileges that all administrators with this role have.

□ Role Name	Description	# of Administrators	Created By	Created On
□ CP-DPSK-generator		1	admin	2017/03/09 21:53:28

Create New Administrator Role

Assign Capabilities to Administrator Role

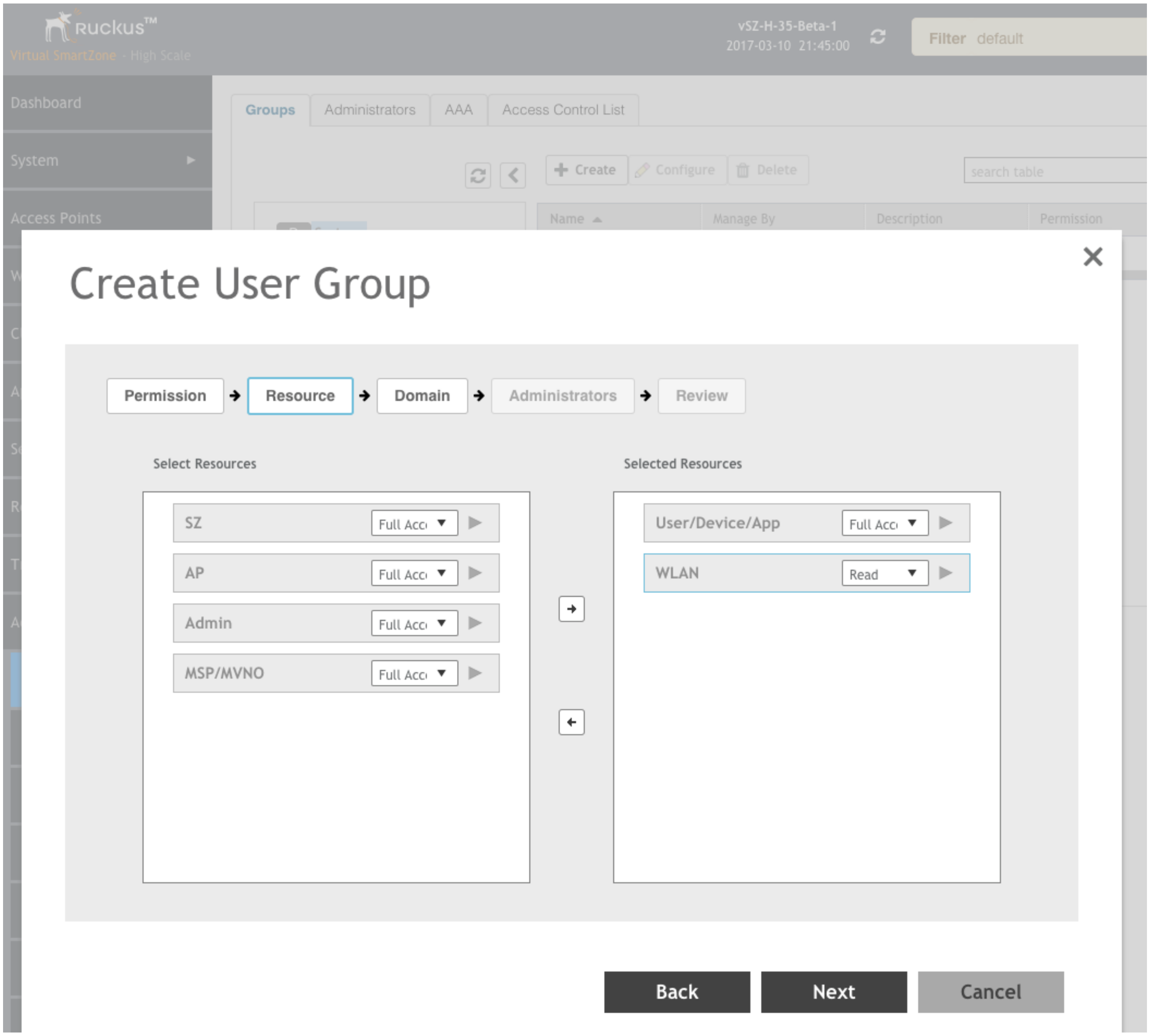
- + □ Monitor
- - ☑ Configuration
  - - ☑ Wireless Network
    - - ☑ WLANS
      - - ☑ WLAN
        - ☑ View
        - ☑ Create
        - □ Modify
        - □ Delete
      - - □ WLAN Group
        - □ View
        - □ Create
        - □ Modify
        - □ Delete
      - - □ WLAN Scheduler
        - □ View
        - □ Create

Role Name: *

Description:

Figure 64: Ruckus SmartZone administrator role config

Create a user role for DPSK generation in SmartZone v 3.5



User/Device/App: Full Acc

WLAN: Read

Figure 65: Ruckus SmartZone administrator role config

1. In all SZ variations, navigate to "Administration -> Admins and roles –> Groups.
2. Choose + **Create**
3. Name the new role (Ex. "cloudpath-dpsk")
4. Select "custom" in the permission drop down; click next
5. Select resources by clicking and then using the arrows to move to "selected resources"
6. User/Device/App – choose Full Access in the drop down
7. WLAN – choose Read Only in the drop down
8. Click next
9. In SZ-H, select domain(s), click Next
10. In "Configure User Group", click the plus sign ("+") near "Available users" to Create and Administrator Account
11. Create a login account for the Cloudpath ES; click OK

12. Select the new account by clicking on it, and use the arrows, to move it to "selected users." Click Next
13. Review and if acceptable, click "OK".

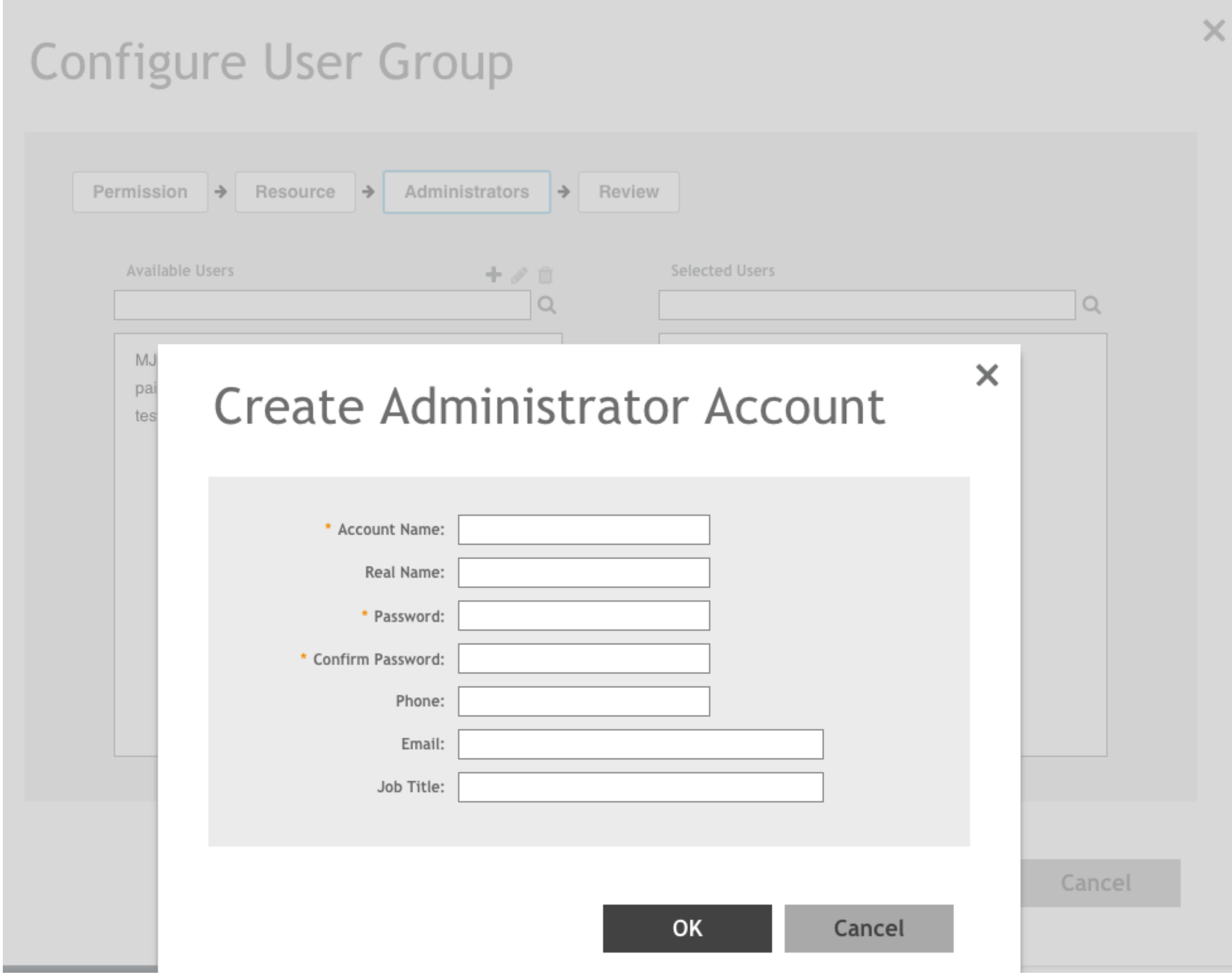
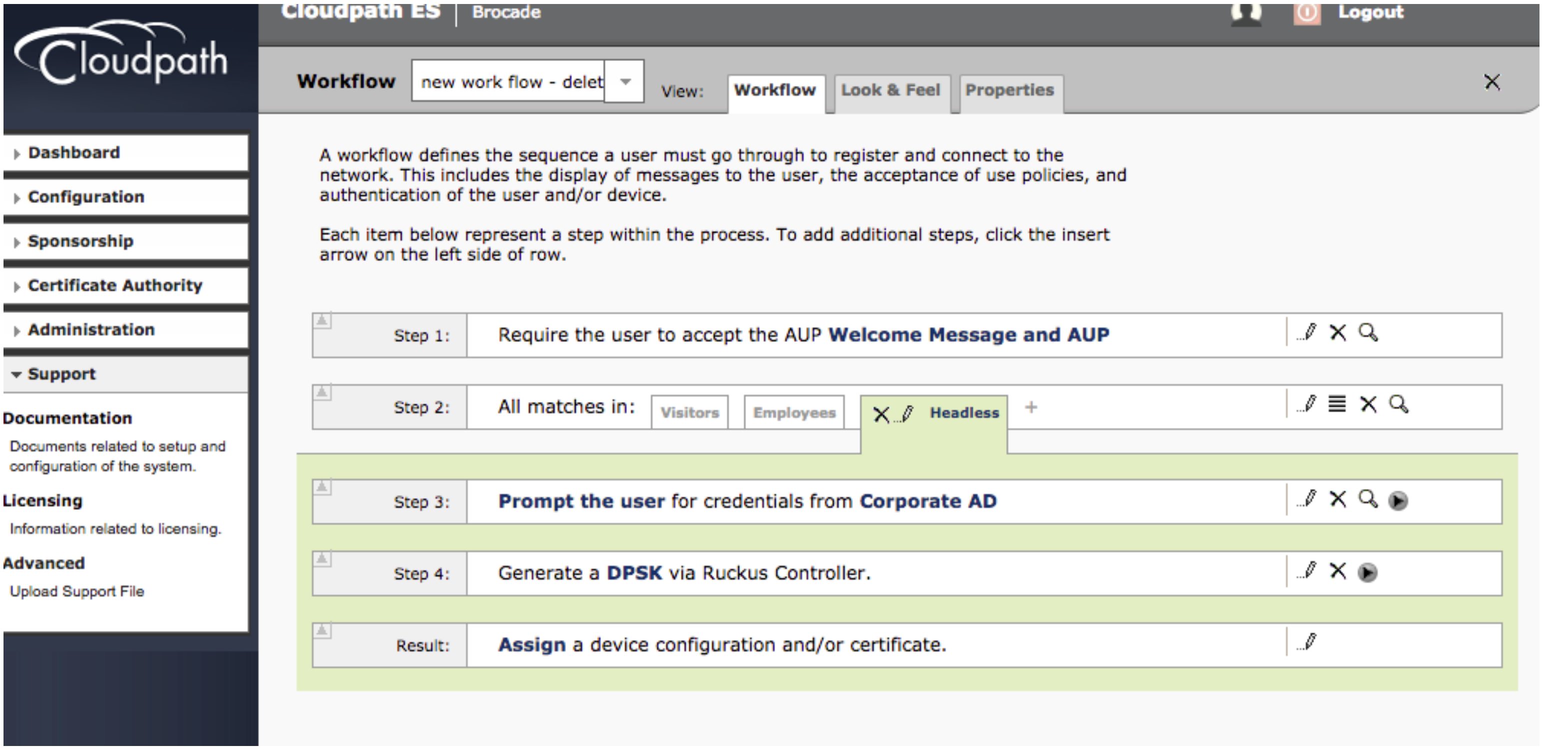


Figure 66: Ruckus SmartZone administrator account config

Step 3: Configure Cloudpath to distribute DPSKs

Use these steps to configure Cloudpath to use DPSK to onboard devices for this SSID. We will add a branch to an existing workflow. You should already be familiar with the basics of building a workflow in Cloudpath. If not, please see the "Cloudpath Deployment Guide" and related documentation on the Cloudpath ES server or the Ruckus support site.



Cloudpath ES | Brocade

Logout

Workflow: new work flow - delet

View: Workflow | Look & Feel | Properties

- Dashboard
- Configuration
- Sponsorship
- Certificate Authority
- Administration
- Support

Documentation
Documents related to setup and configuration of the system.

Licensing
Information related to licensing.

Advanced
Upload Support File

A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.

Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row.

Step 1: Require the user to accept the AUP **Welcome Message and AUP**

Step 2: All matches in: Visitors | Employees | Headless

Step 3: **Prompt the user** for credentials from **Corporate AD**

Step 4: Generate a **DPSK** via Ruckus Controller.

Result: **Assign** a device configuration and/or certificate.

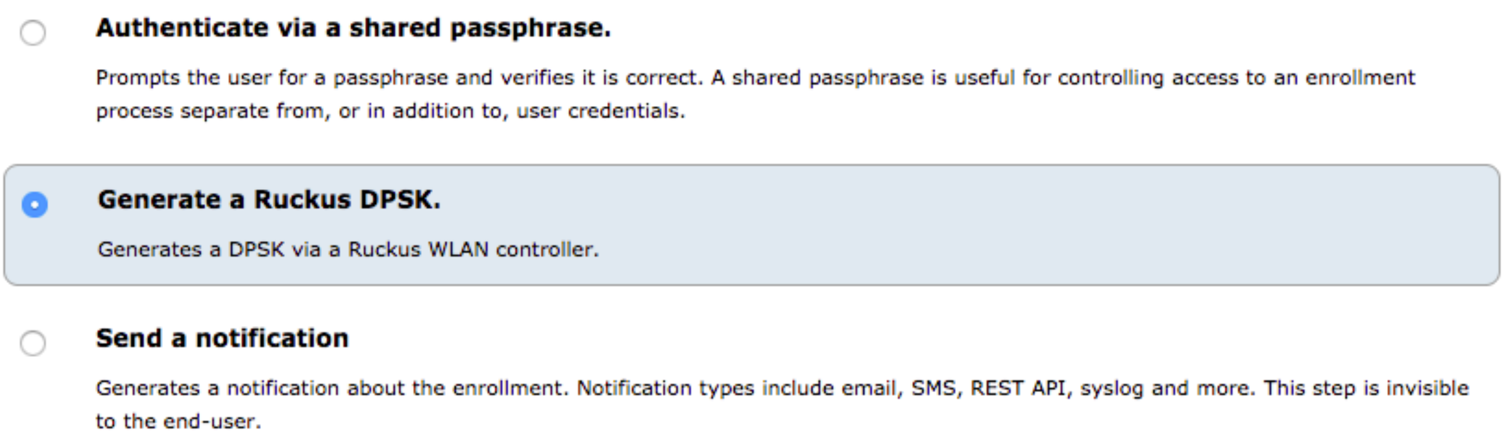
Figure 67: Ruckus SmartZone WLAN config

Minimal workflow for DPSK

1. Add a branch for headless devices
2. Add User authentication
3. Generate the DPSK – default behavior includes emailing it to user
4. Assign device configuration – this step is required for a workflow, but will be set to "none" since this is registration for another device.

Configure "Generate a DPSK via Ruckus Controller

1. Add a branch for Headless devices to the work flow
    - i.e. – "Teachers, Students, Media devices"
2. Add a user authentication step –
    - You probably want to reuse an existing user authentication, such as one for Teachers
3. After user authentication, insert a step, scroll down the list and choose "Generate a Ruckus DPSK. Click Next.
4. Choose a new DPSK configuration, click Next
5. Give it a name and choose "Zone Director" or "SmartZone", as appropriate
6. For SmartZone
    a. Use the username and password you created in the previous section
    b. IP/DNS of the Smartzone, SSID and Zone as desired.
    c. VLAN ID is optional. Dynamic VLANs will be addressed in the next section
7. For Zone Director
    a. Use the password for the northbound interface you created in the previous section
    b. Chose the key length with the slider bar
    c. VLAN ID is optional. Dynamic VLANs will be addressed in the next section
8. Click Save



○ **Authenticate via a shared passphrase.**

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

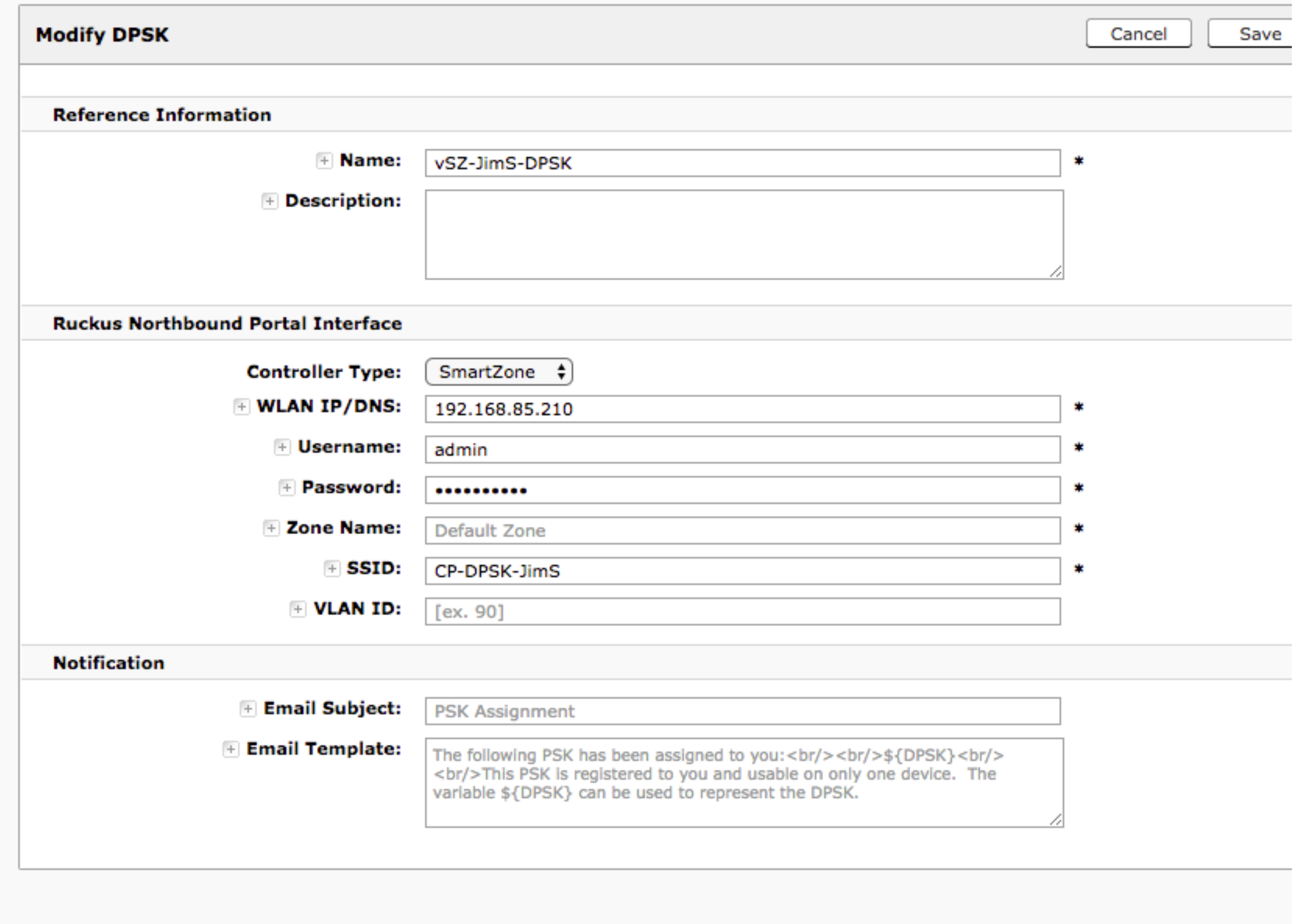
● **Generate a Ruckus DPSK.**

Generates a DPSK via a Ruckus WLAN controller.

○ **Send a notification**

Generates a notification about the enrollment. Notification types include email, SMS, REST API, syslog and more. This step is invisible to the end-user.

Figure 68: Ruckus Cloudpath insert a step



Modify DPSK

Reference Information

Name:	vSZ-JimS-DPSK *
Description:	

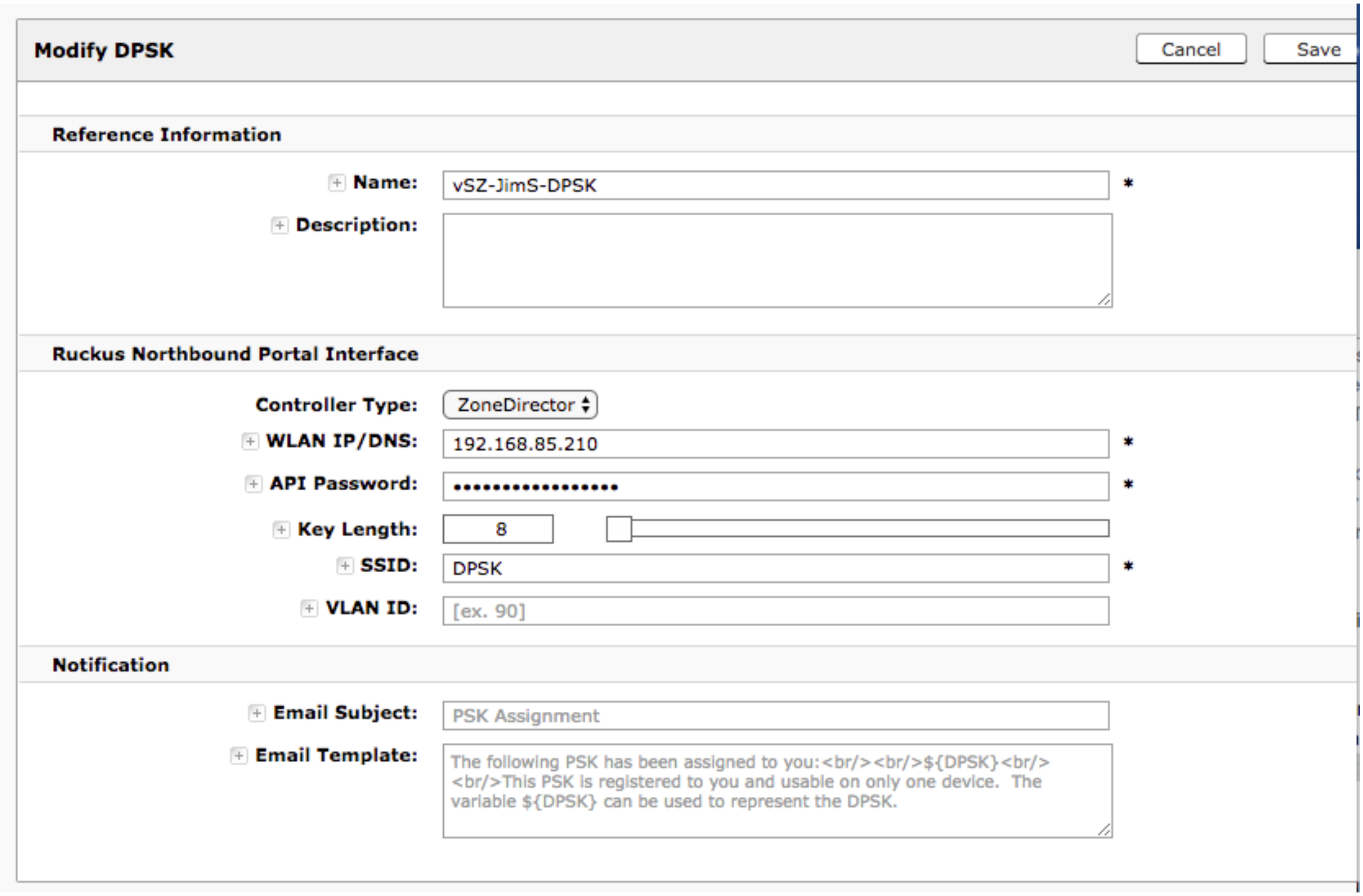
Ruckus Northbound Portal Interface

Controller Type:	SmartZone
WLAN IP/DNS:	192.168.85.210 *
Username:	admin *
Password:	•••••••••• *
Zone Name:	Default Zone *
SSID:	CP-DPSK-JimS *
VLAN ID:	[ex. 90]

Notification

Email Subject:	PSK Assignment
Email Template:	The following PSK has been assigned to you:<br/><br/>${DPSK}<br/><br/>This PSK is registered to you and usable on only one device. The variable ${DPSK} can be used to represent the DPSK.

Figure 69: Ruckus SmartZone DPSK config



Modify DPSK

Reference Information

Name:	vSZ-JimS-DPSK *
Description:	

Ruckus Northbound Portal Interface

Controller Type:	ZoneDirector
WLAN IP/DNS:	192.168.85.210 *
API Password:	••••••••••••••••• *
Key Length:	8
SSID:	DPSK *
VLAN ID:	[ex. 90]

Notification

Email Subject:	PSK Assignment
Email Template:	The following PSK has been assigned to you:<br/><br/>${DPSK}<br/><br/>This PSK is registered to you and usable on only one device. The variable ${DPSK} can be used to represent the DPSK.

Figure 70: Ruckus ZoneDirector DPSK config

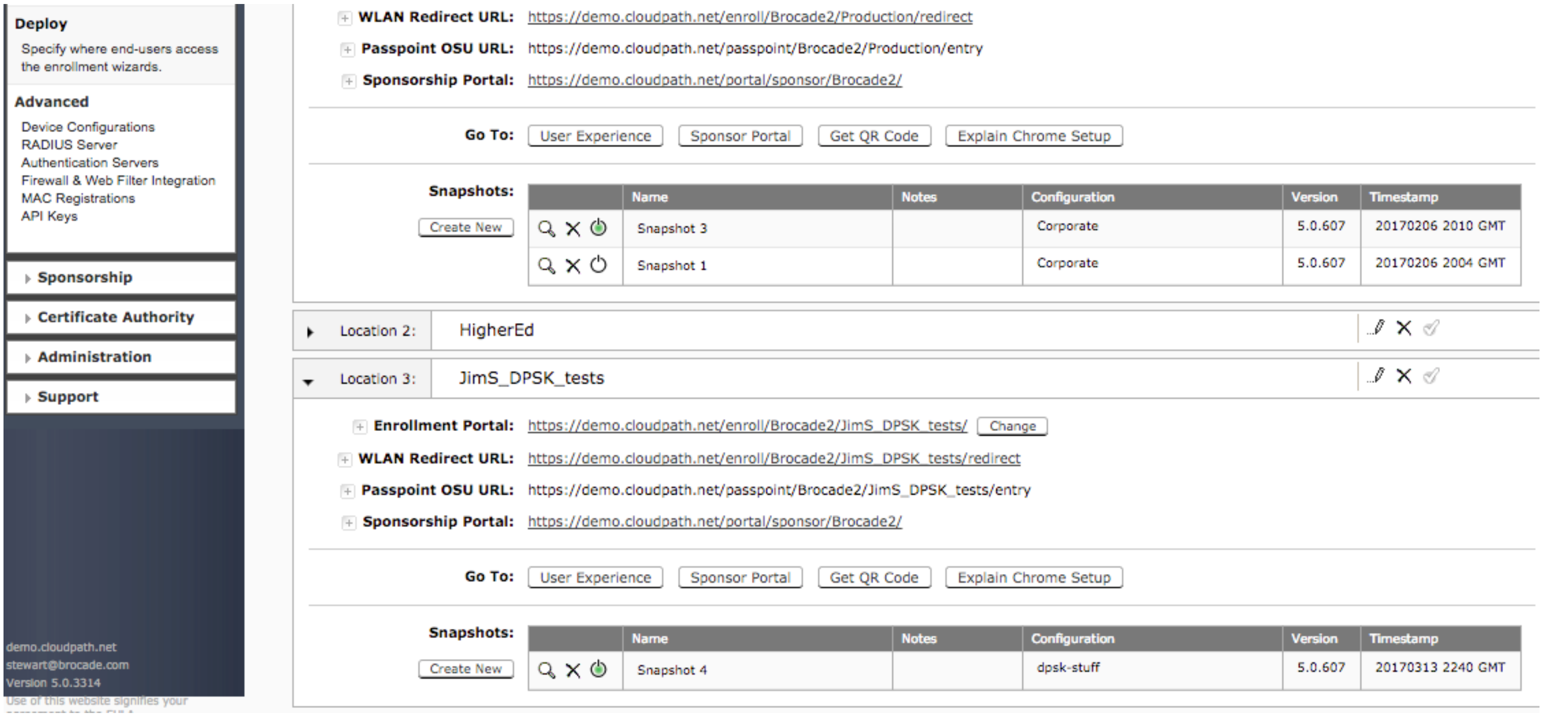
Modify the “assign a device configuration” step

Because this DPSK will be entered on another device, there is no need to download a profile unto the device doing the registration

1. Click on the pencil icon to Edit, and chose “none”
2. Click next
3. Choose ‘Do not issue a certificate”
4. Click Next

Deploy the workflow to the correct location and test

Don’t forget that a workflow must be deployed/published to the web server before an end user can access it. You can use the “User Experience” button for local testing.



WLAN Redirect URL: https://demo.cloudpath.net/enroll/Brocade2/Production/redirect
Passpoint OSU URL: https://demo.cloudpath.net/passpoint/Brocade2/Production/entry
Sponsorship Portal: https://demo.cloudpath.net/portal/sponsor/Brocade2/

Snapshots:

Name	Notes	Configuration	Version	Timestamp
Snapshot 3		Corporate	5.0.607	20170206 2010 GMT
Snapshot 1		Corporate	5.0.607	20170206 2004 GMT

Location 2: HigherEd

Location 3: JimS_DPSK_tests

Enrollment Portal: https://demo.cloudpath.net/enroll/Brocade2/JimS_DPSK_tests/
WLAN Redirect URL: https://demo.cloudpath.net/enroll/Brocade2/JimS_DPSK_tests/redirect
Passpoint OSU URL: https://demo.cloudpath.net/passpoint/Brocade2/JimS_DPSK_tests/entry
Sponsorship Portal: https://demo.cloudpath.net/portal/sponsor/Brocade2/

Snapshots:

Name	Notes	Configuration	Version	Timestamp
Snapshot 4		dpsk-stuff	5.0.607	20170313 2240 GMT

Figure 71: Cloudpath workflow deployment screen

Congratulations: you are done

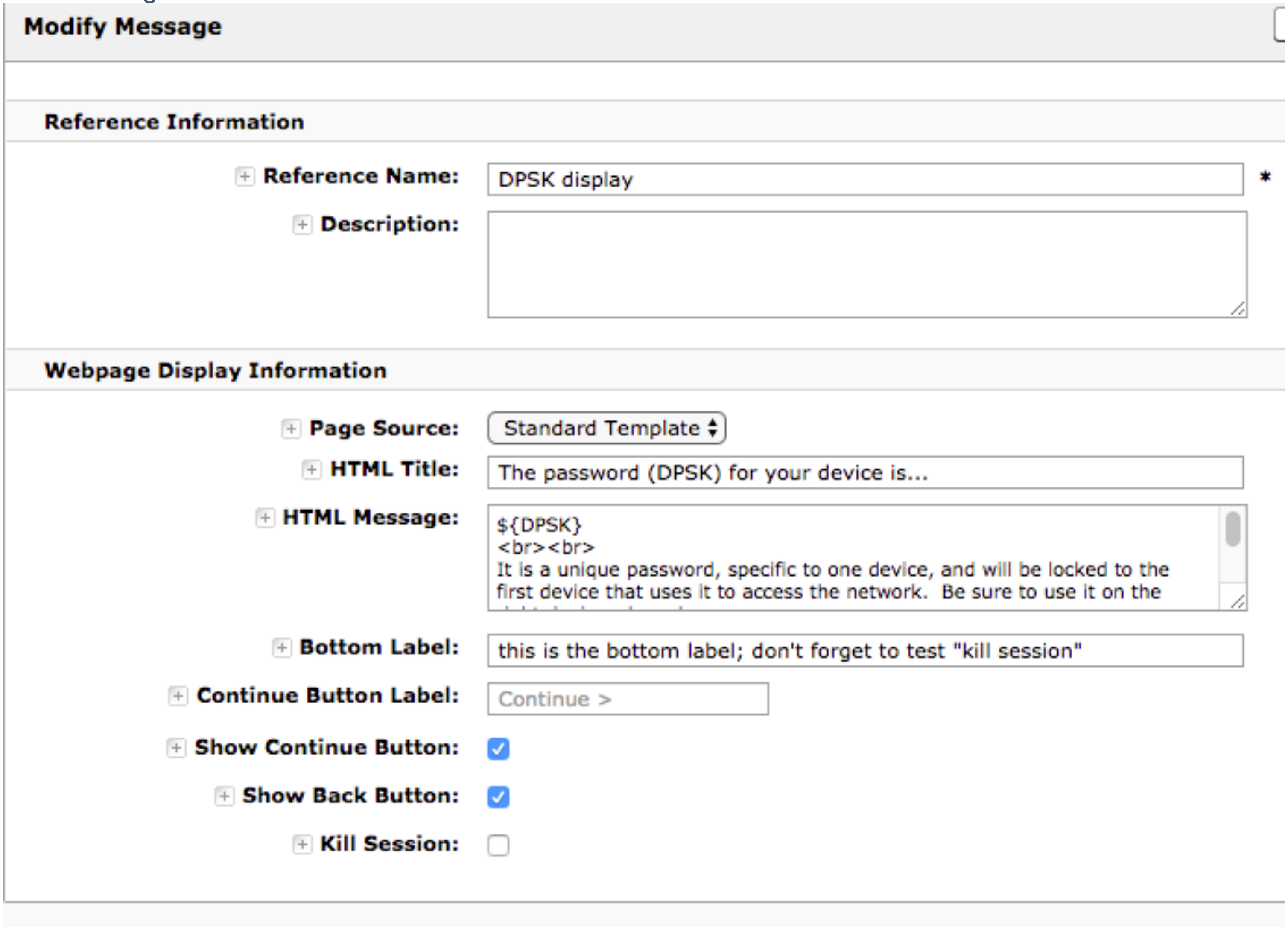
You have configured a DPSK WLAN and a Cloudpath ES registration portal for DPSK device registration. However, Cloudpath ES is almost infinitely configurable, and some special topics are discussed below.

Displaying the DPSK in the portal

By default, the DPSK is emailed to the user. You can add a message that displays it to the screen.

1. Insert a step in the workflow after the DPSK generation
2. Choose “Display a message”
3. Click Next
4. Choose “A New Message from a Standard Template”
5. Name and modify the template to display the DPSK and an appropriate message
    a. Note that the template accepts HTML
    b. The DPSK itself can be represented as a variable with ${DPSK}

This message:



Modify Message

Reference Information

Reference Name:	DPSK display *
Description:	

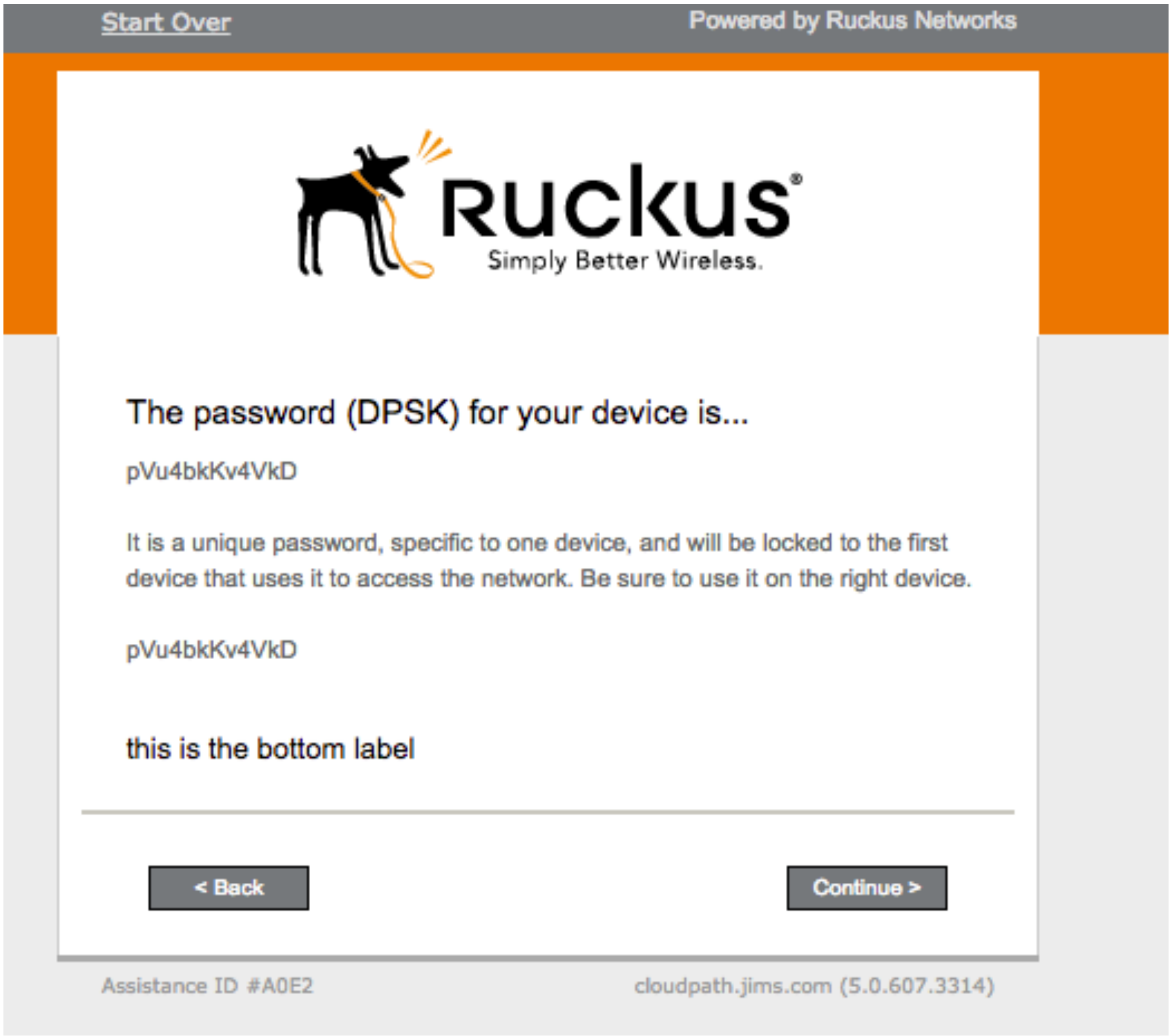
Webpage Display Information

Page Source:	Standard Template
HTML Title:	The password (DPSK) for your device is...
HTML Message:	${DPSK}

 It is a unique password, specific to one device, and will be locked to the first device that uses it to access the network. Be sure to use it on the
Bottom Label:	this is the bottom label; don't forget to test "kill session"
Continue Button Label:	Continue >
Show Continue Button:	☑
Show Back Button:	☑
Kill Session:	□

Figure 72: Cloudpath message display config

Produces this result:



The password (DPSK) for your device is...

pVu4bkKv4VkD

It is a unique password, specific to one device, and will be locked to the first device that uses it to access the network. Be sure to use it on the right device.

pVu4bkKv4VkD

this is the bottom label

Figure 73: Cloudpath message display screen result

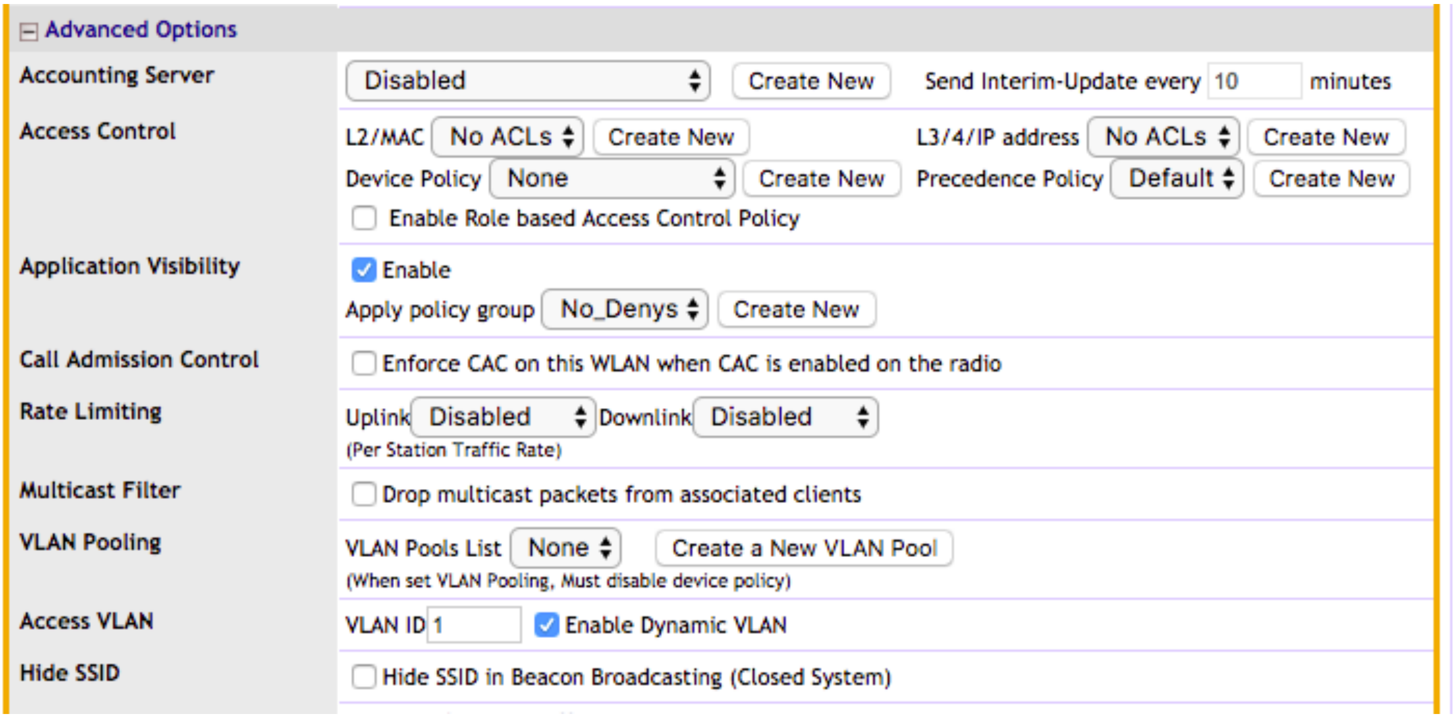
Branching users by identity and adding Dynamic VLANs to the DPSK assignment

Up to this point, we have assigned all DPSK devices to the same VLAN, whether tagged or native. That is, all DPSK devices are assigned to the same SSID and VLAN. However, VLANs and other options can be assigned based on user in put or credentials. For instance multiple DPSK devices can use the same WLAN/SSID but be VLAN tagged differently.

Please take note: this section is assuming that you are already applying user or user group based network Policy in your AAA servers. It is unlikely that this would make sense for headless devices other wise. This is intended to supplement an 802.1X based policy for supporting end user devices with a similar policy application for their headless devices. It usually does not make sense if the former is not in place, although network goals are infinitely variable. 802.1X policy is covered in the basic Cloudpath deployment documentation.

Configure WLAN controllers for Dynamic VLANs

1. SmartZones automatically include Dynamic VLANs with any DPSK WLANs. No changes are necessary
2. ZoneDirectors – in the edit screen for the DPSK WLAN, expand 'advanced options' and insure that the Enable Dynamic VLAN box is checked.



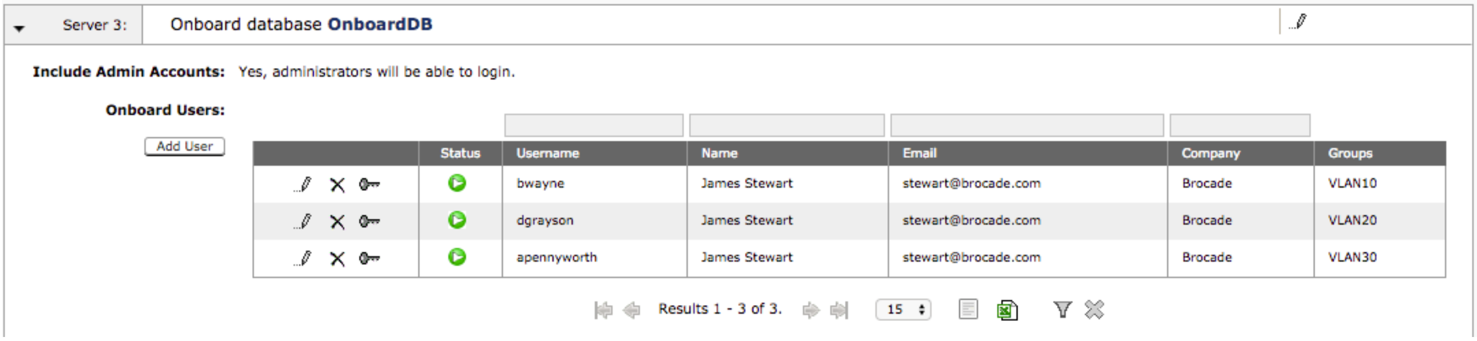
⊟ Advanced Options

Accounting Server	Disabled · Create New · Send Interim-Update every 10 minutes
Access Control	L2/MAC No ACLs · Create New · L3/4/IP address No ACLs · Create New Device Policy None · Create New · Precedence Policy Default · Create New □ Enable Role based Access Control Policy
Application Visibility	☑ Enable Apply policy group No_Denys · Create New
Call Admission Control	□ Enforce CAC on this WLAN when CAC is enabled on the radio
Rate Limiting	Uplink Disabled · Downlink Disabled (Per Station Traffic Rate)
Multicast Filter	□ Drop multicast packets from associated clients
VLAN Pooling	VLAN Pools List None · Create a New VLAN Pool (When set VLAN Pooling, Must disable device policy)
Access VLAN	VLAN ID 1 · ☑ Enable Dynamic VLAN
Hide SSID	□ Hide SSID in Beacon Broadcasting (Closed System)

Figure 74: ZoneDirector enable dynamic LVANs

Create a group value in your user database for VLAN assignment

This will vary depending on your database. For Active Directory, this will normally involve creating a network policy group. For simplicity's sake, we are using the Cloudpath onboard DB to illustrate this the process. Note we have included group assignments of VLANs



Server 3: Onboard database **OnboardDB**

Include Admin Accounts: Yes, administrators will be able to login.

Onboard Users: Add User

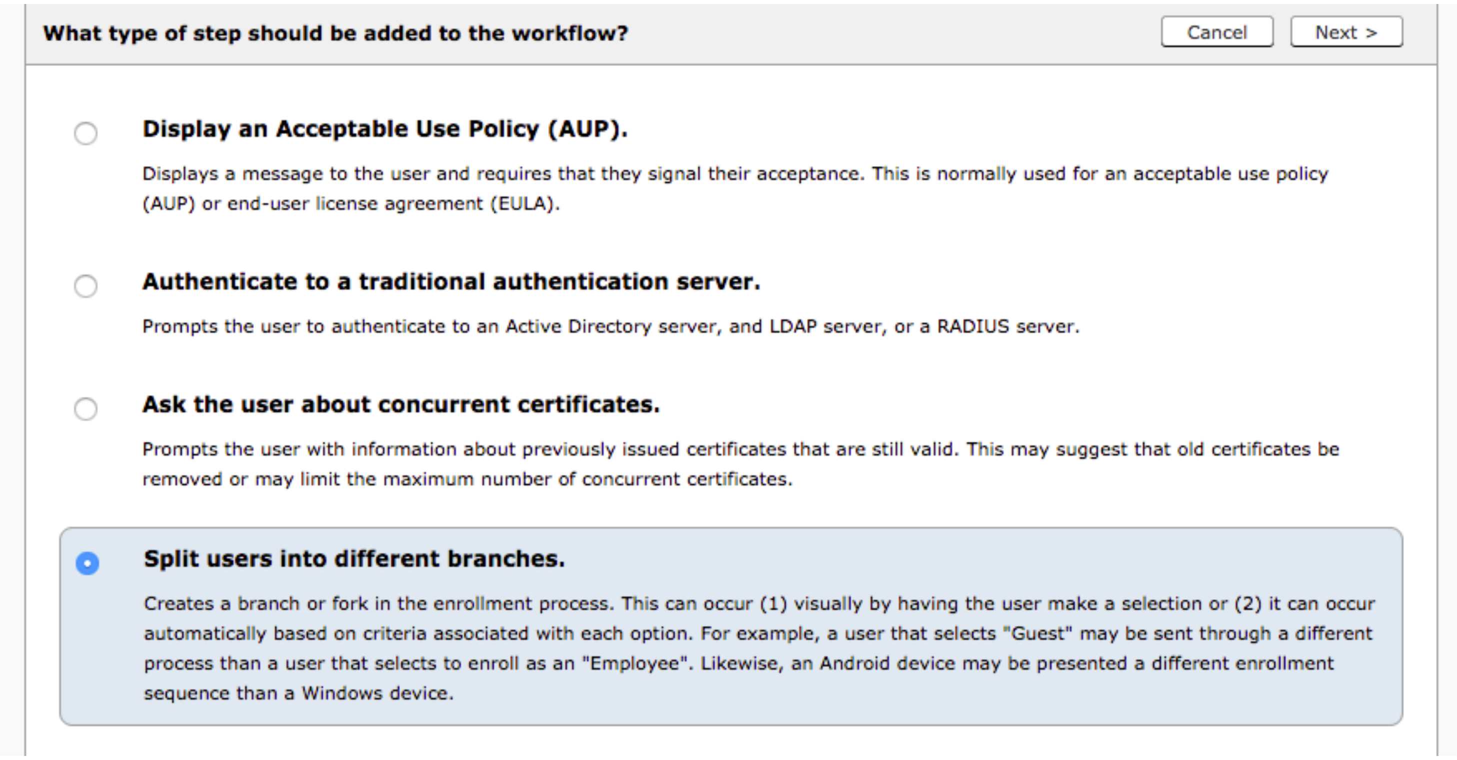
	Status	Username	Name	Email	Company	Groups
	●	bwayne	James Stewart	stewart@brocade.com	Brocade	VLAN10
	●	dgrayson	James Stewart	stewart@brocade.com	Brocade	VLAN20
	●	apennyworth	James Stewart	stewart@brocade.com	Brocade	VLAN30

Results 1 - 3 of 3. 15

Figure 75: Cloudpath onboard DB example

Modify the Cloudpath workflow

3. In the Cloudpath Workflow, insert a step after "Prompt the user for credentials"
4. Choose "Split users into different branches"
5. Choose "use a new split"



What type of step should be added to the workflow?

○ **Display an Acceptable Use Policy (AUP).**

Displays a message to the user and requires that they signal their acceptance. This is normally used for an acceptable use policy (AUP) or end-user license agreement (EULA).

○ **Authenticate to a traditional authentication server.**

Prompts the user to authenticate to an Active Directory server, and LDAP server, or a RADIUS server.

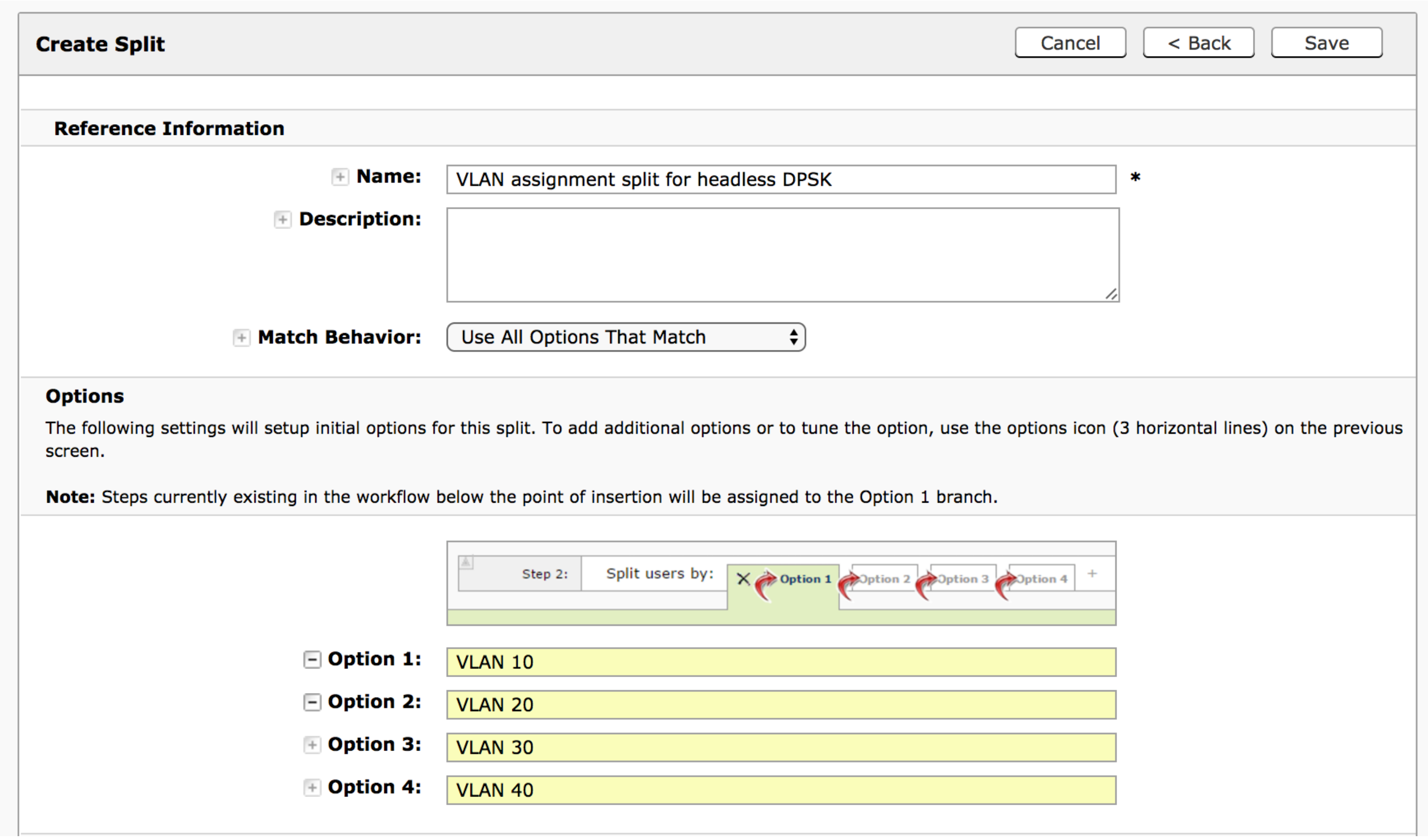
○ **Ask the user about concurrent certificates.**

Prompts the user with information about previously issued certificates that are still valid. This may suggest that old certificates be removed or may limit the maximum number of concurrent certificates.

● **Split users into different 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 that selects "Guest" may be sent through a different process than a user that selects to enroll as an "Employee". Likewise, an Android device may be presented a different enrollment sequence than a Windows device.

Figure 76: Cloudpath user split/branch config



Create Split

Reference Information

Name: VLAN assignment split for headless DPSK *

Description:

Match Behavior: Use All Options That Match

Options

The following settings will setup initial options for this split. To add additional options or to tune the option, use the options icon (3 horizontal lines) on the previous screen.

Note: Steps currently existing in the workflow below the point of insertion will be assigned to the Option 1 branch.

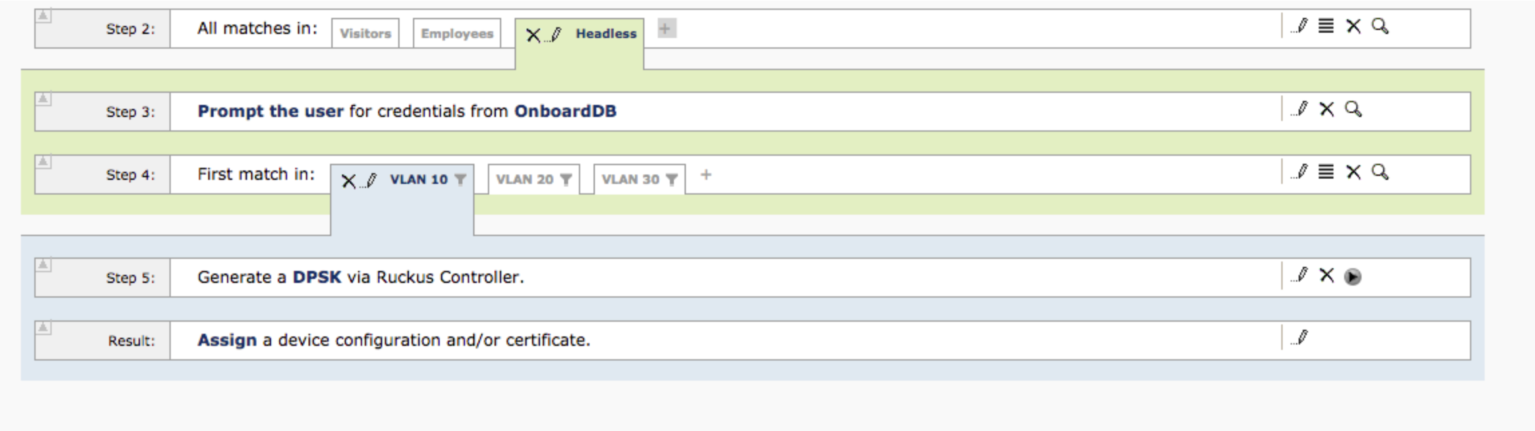
Option 1: VLAN 10

Option 2: VLAN 20

Option 3: VLAN 30

Option 4: VLAN 40

Figure 77: Cloudpath split/branch config, cont.



Step 2: All matches in: Visitors Employees Headless

Step 3: **Prompt the user** for credentials from **OnboardDB**

Step 4: First match in: VLAN 10 VLAN 20 VLAN 30

Step 5: Generate a **DPSK** via Ruckus Controller.

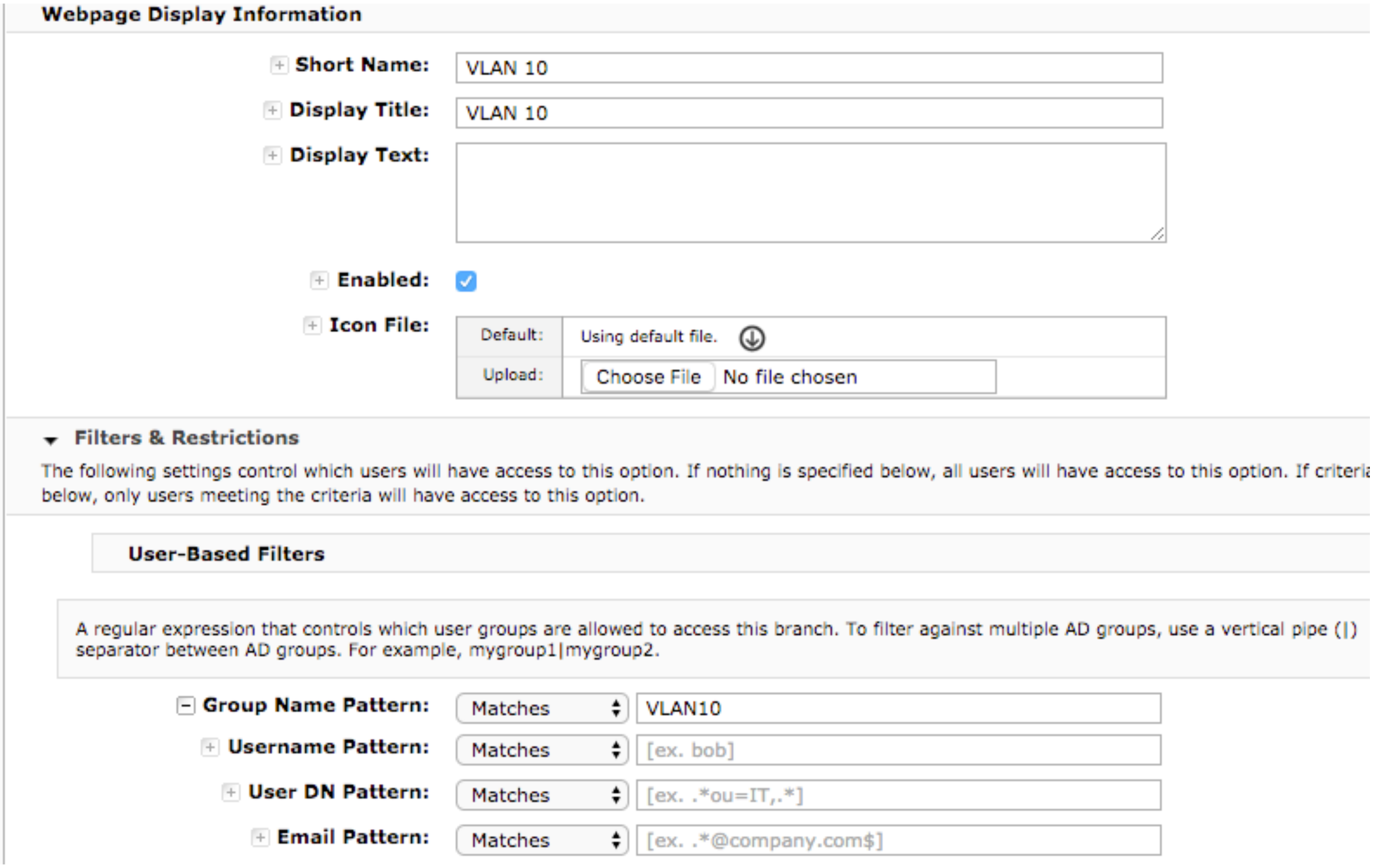
Result: **Assign** a device configuration and/or certificate.

Figure 78: Cloudpath user split/branch result

6. Give the split a name and name the desired options
7. In a split like this, whether the options are displayed to the end user depends on what they are. If, as in this case, the options are automatic, they will not be displayed to the end user

Edit each branch of the split

1. Click the pencil at the top of a branch (by “VLAN 10” in the example)
2. Expand the “Filters & Restrictions” section
3. Enter an appropriate filter value, such as a group ID
4. Click “save” at the top



Webpage Display Information

Short Name: VLAN 10

Display Title: VLAN 10

Display Text:

Enabled: ☑

Icon File:

Default:	Using default file.
Upload:	Choose File No file chosen

Filters & Restrictions

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

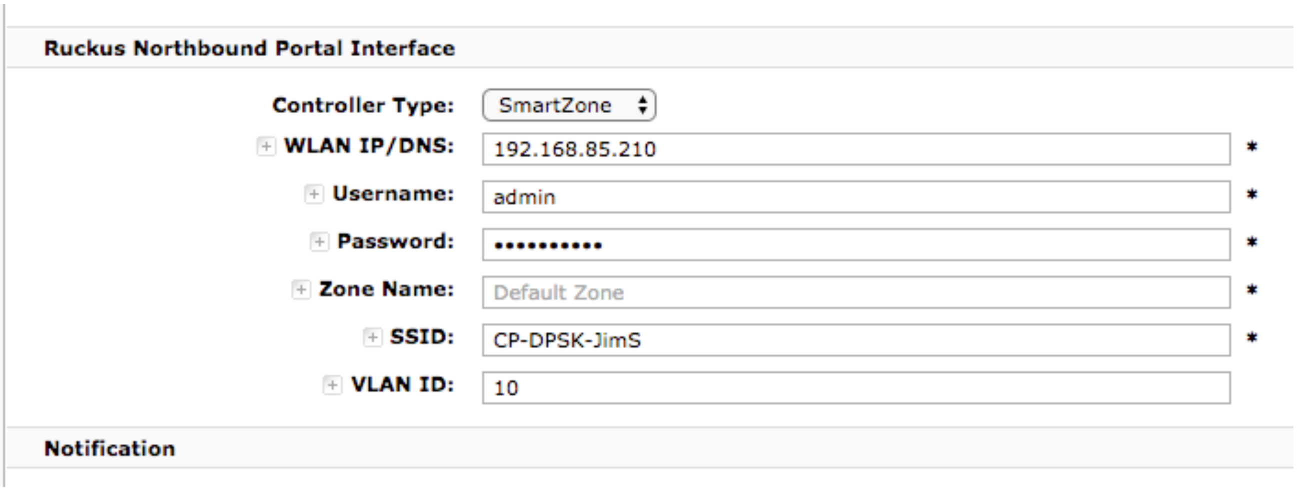
User-Based Filters

A regular expression that controls which user groups are allowed to access this branch. To filter against multiple AD groups, use a vertical pipe (|) separator between AD groups. For example, mygroup1|mygroup2.

Group Name Pattern:	Matches	VLAN10
Username Pattern:	Matches	[ex. bob]
User DN Pattern:	Matches	[ex. .*ou=IT,.*]
Email Pattern:	Matches	[ex. .*@company.com$]

Figure 79: Cloudpath filter config

5. add or edit a “generate a DPSK” step
6. This time, include the VLAN ID that you want to map to your filter condition
7. Click Save



Ruckus Northbound Portal Interface

Controller Type:	SmartZone	
WLAN IP/DNS:	192.168.85.210	*
Username:	admin	*
Password:	••••••••••	*
Zone Name:	Default Zone	*
SSID:	CP-DPSK-JimS	*
VLAN ID:	10	

Notification

Figure 80: DPSK with VLAN ID

8. Check that the "assign a device configuration" step leads to "none" and "Do not assign a device configuration"
9. Repeat for the other branches.

Filters are a powerful tool in Cloudpath, and can be used for a wide variety of branching and configuration options.

Web Content Filtering in an SSL/HTTPS World

Enable 3rd Party SSL Inspection and Decryption with Cloudpath

Web content filters are vital in a K-12 educational environment, but more and more web traffic is automatically encrypted https, rather than unencrypted http. Even Google searches are routinely encrypted, and encrypted traffic cannot be inspected. That is, unless your content filter can act as an SSL proxy, also known as a "Trusted Man in the Middle." The client device, instead of creating an SSL tunnel directly to a website passes through the proxy server/content filter and two related tunnels are created, one between the proxy server and the desired website, one between the client and proxy server. The proxy server is then able to decrypt and examine the web traffic, but it is always fully encrypted in transition. Details will vary with the content filter vendor. Often there are options to proxy or not proxy certain sites, such as banking and financial sites.

However, the whole system depends on the client trusting the web filter, which depends on recognizing a trusted root certificate. Web browsers come preinstalled with most major Certificate Authorities root certificates. On the other hand, the content filter certificate will not be pre-installed and will have to be distributed to each client device on the network – even personal BYOD devices – a challenging proposition for any IT organization.

This is where Cloudpath comes in. Cloudpath ES registration can distribute the content filter certificate at device registration. One only has to install the certificate one time on the Cloudpath Es server, and add the certificate to the Device Configuration the normal last step of most workflows. When the client gets its specific certificate that allows network access, it also get the certificate necessary for the content filter to act as an SSL proxy.

Obtain the Web Or Content Filter Root Certificate

This is going to vary from vendor to vendor, but every Content Filter will have clear instructions on this. See your vendor's documentation. As a rule, you will:

1. Download the certificate onto a local system
2. Upload it into Cloudpath as part of modifying the Device Configuration

Download the Content Filter Certificate

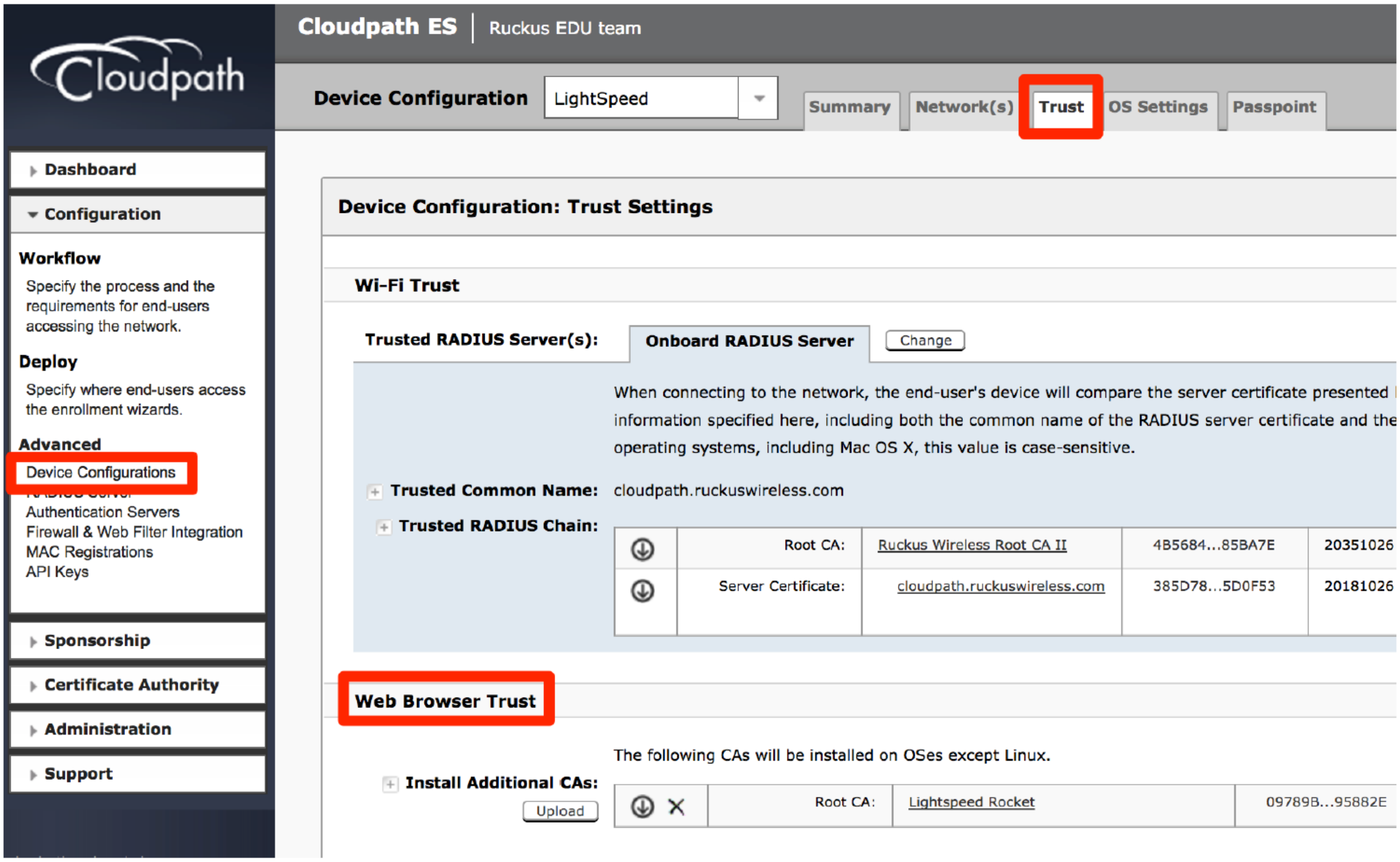
As stated, this will depend on the vendor. As an example, Ruckus partner Lighspeed certificate can be downloaded from the following link:

https://rukus.lightspeedsystems.com/lsaccess/proxycerthelp

The Lightspeed download automatically detects your operating system and browser and provides full instructions on install to your local machine. However, you interest in this case is to upload it to Cloudpath.

Add the Certificate to a Device Configuration

1. Go to Configuration -> advanced -> Device Configuration
2. Choose the correct device configuration from the drop down menu
3. Go to the Trust tab
4. Under Web Browser Trust, Install additional CAs, upload the certificate



Device Configuration: LightSpeed

Device Configuration: Trust Settings

Wi-Fi Trust

Trusted RADIUS Server(s): Onboard RADIUS Server

When connecting to the network, the end-user's device will compare the server certificate presented information specified here, including both the common name of the RADIUS server certificate and the operating systems, including Mac OS X, this value is case-sensitive.

Trusted Common Name: cloudpath.ruckuswireless.com

Trusted RADIUS Chain:

	Root CA:	Ruckus Wireless Root CA II	4B5684...85BA7E	20351026
	Server Certificate:	cloudpath.ruckuswireless.com	385D78...5D0F53	20181026

Web Browser Trust

The following CAs will be installed on OSes except Linux.

Install Additional CAs:

	Root CA:	Lightspeed Rocket	09789B...95882E

Figure 81: Add a certificate to Device Configuration

About Ruckus

Headquartered in Sunnyvale, CA, Ruckus Wireless, Inc. is a global supplier of advanced wireless systems for the rapidly expanding mobile Internet infrastructure market. The company offers a wide range of indoor and outdoor "Smart Wi-Fi" products to mobile carriers, broadband service providers, and corporate enterprises, and has over 36,000 end-customers worldwide. Ruckus technology addresses Wi-Fi capacity and coverage challenges caused by the ever-increasing amount of traffic on wireless networks due to accelerated adoption of mobile devices such as smartphones and tablets. Ruckus invented and has patented state-of-the-art wireless voice, video, and data technology innovations, such as adaptive antenna arrays that extend signal range, increase client data rates, and avoid interference, providing consistent and reliable distribution of delay-sensitive multimedia content and services over standard 802.11 Wi-Fi. For more information, visit http://www.ruckuswireless.com.

Ruckus and Ruckus Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries.

Destination Control Statement

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

Disclaimer

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

Limitation of Liability

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