

Cloudpath Enrollment System

Configuring Cloudpath to Support Managed and Unmanaged Chromebooks

Software Release 5.0

December 2016

Summary: This document describes how to set up Cloudpath to enroll Chromebooks on the secure network, including setting up managed and unmanaged Chromebooks, the Cloudpath Certificate Generator user extension, and the Chromebook user experience.

Document Type: Support **Audience:** Network Administrator



Configuring Cloudpath to Support Managed and Unmanaged Chromebooks

Software Release 5.0 December 2016

Copyright © 2016 Ruckus Wireless, Inc. All Rights Reserved.

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ZoneFlex[™], BeamFlex[™], MediaFlex[™], ChannelFly[™], and the Ruckus Wireless logo are trademarks of Ruckus Wireless, Inc. All other brands and product names are trademarks of their respective holders.

Copyright © 2016 Ruckus Wireless, Inc. All rights reserved.

Configuring Cloudpath to Support Managed and Unmanaged Chromebooks

Overview

The Cloudpath Enrollment System (ES) extends the benefits of certificates to Chromebooks in environments with an existing Public Key Infrastructure (PKI).

The certificate is installed in the Trusted Platform Module (TPM), and can be used for certificate-based 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 along with configuration of related services, such as WPA2-Enterprise Wi-Fi using 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 worlds 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, consult the following URLs:

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

Configuring Cloudpath

To create a Chromebook configuration in Cloudpath, enable the Chromebook OS on the ES Admin UI and configure the user experience appropriate for your network.

During user enrollment, if the Chrome OS is detected, Cloudpath 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.

Enable the Chrome OS

The Chrome operating is enabled by default. If needed, use these instructions to enable the Chrome OS for a 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.

FIGURE 1. Enable Chrome OS

Modify Setting		Cancel Save
This setting configures the networks and control which versions of the operating sy	certificate authorities as specified on the <u>Network(s)</u> tab. The stem are supported as well as OS-specific settings.	configuration options below
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 ne Validate Server Certificate:	ed adjusted. Yes, validate RADIUS server(s). (Strongly Recommended	

- 4. Select Operating System: Chrome.
- 5. Leave the default settings for Validate Server Certificate, and Save.

Chromebook User Experience

The Chromebook user experience can be configured for managed or unmanaged devices.

- For unmanaged devices, the user downloads the ONC file, which contains the certificate and Wi-Fi settings required to connect to the secure network. This is similar to the mobileconfig file process for Mac OS X and iOS devices.
- For managed devices, the Cloudpath extension, which is configured in the Chrome Management Console, installs the certificate and settings into the TPM as the user or as the device.

Note >>

The Chrome extension uses the information provided by the Cloudpath configuration. See Configuring the Chrome Extension to configure the Cloudpath extension to be dispersed to managed devices.

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

User Experience Settings

To configure the Chromebook user experience:

- 1. Go to Configuration > Advanced > Device Configuration.
- 2. Select the OS Settings tab for the appropriate device configuration.
- 3. Edit the Chrome: User experience options.

FIGURE 2. Chrome User Experience Settings

Chrome User Experience		Cancel	Save
Behavior			
🗄 Supported Methods:	Unmanaged via ONC + Managed via User Extension 🔻		
Unmanaged Chromebooks (ONC) Mess The options below control the messaging for un	ages imanaged Chrome users.		
ONC Install Instructions:	<pre><div id="chromeUnmanagedDiv"><div class="cpx-wizard-download-
subnote"><ul style="margin-top: 0px; margin-bottom: 0px;">If you are not logged in as the Chromebook owner, log out and log back in as owner.</div></div></pre>	the	
Extension Messages The options below control the messaging when	a certificate is installed on a managed device via the Chrome Extension.		
	<pre><div id="chromeManagedDiv" style="display: none;">'cdiv class='cpx-wizard-configure- image'></div><div class="cpx-wizard-download-button"><span< pre=""></span<></div></pre>	•	
🗄 Completed Message:	<pre><div class="cpx-pageChromeOsExtensionDone-title"><img class="cpx-
pageChromeOsExtensionDone-image" src="images/check.png"/>The certificate has been installed.</div></pre> /div> <div< pre="">/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div/div</div<>	↓ ▼ Y 2	
Extension - Advanced Behavior The options below control the messaging when	a certificate is installed on a managed device via the Chrome Extension.		
 Existing Certificates: App ID To Notify: 	Do not remove existing certificates.		

- 4. 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.
- 5. 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.
- 6. 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.
- 7. 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.

Note >>

If your root CA certificate chain includes an intermediate certificate, the Chromebook setup instructions provide a link to the Root CA on Step 1 and any intermediate CAs in step 2.

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.

FIGURE 3. Managed	Chromebook Setup	Instructions
-------------------	------------------	--------------

evice C	onfiguration: 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: <u>Anna Test Intermediate CA I</u>
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 (<u>XpressConnect Certificate Generator</u>) and add it to the force-install list.
	(If you need the beta version, the ID is dnnhnbjpkkgdnnfdillepjhnabjcbjpn (<u>XpressConnect Certificate Generator - Beta</u>).)
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.

Note >>

The extension ID is listed in the Chromebook Setup Instructions.

5

Configuring the Chrome Extension

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 Chromebook devices.

After configuring the Chrome OS settings in Cloudpath, use 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 configured network settings for users and configure 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.

To access network and wireless settings:

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

FIGURE 4. Chrome Admin Console

\equiv Admin console	
Device management	
Settings and security for devices	

Select Device Management.



≡ Device managemen	t		
SETTINGS Network Mobile Chrome management Chromebox for meetings	Mobile devices	2 Chrome devices	Chromebox for meetings
	More about Mobile	Manage Chrome devices	More about Chromebox for meetings

Use 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.

Network Settings

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.

FIGURE 6. Network Settings

\equiv Device manageme	ent > 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

Import CA certificate

Click the Networks > Certificates link to import the CA certificate.

8

≡ Device managem	nent > Network > Certificates	0
G ORGANIZATIONS	SETTINGS for cloudpath.net	
 cloudpath.net Employees End-Of-Life Accounts External Contractors 	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	DEVENT
Servers	Inis 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. Locally applied	REVERI
	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.	REVERT
	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 CAL IT, Sample Company, Inc. ADD CERTIFICATE	

FIGURE 7. Manage Certificates

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.

- 1. Click Add Certificate.
- 2. Locate and import the root CA certificate that was downloaded from the Chrome Setup Instructions page in the Cloudpath Admin UI (see Managed Chromebook Setup Instructions).

Note >>

You must install the entire certificate chain. If the root CA contains an intermediate certificate, you must install both the root and intermediate certificates. Additionally, the common name must match on the root and intermediate certs.

- If your Cloudpath configuration contains additional CAs, you must also import the additional CAs. The link for downloading additional CAs can be found in Step 2 of the Managed Chromebook Setup Instructions.
- 4. When the certificates have been successfully uploaded, return to the *Networks* page to configure *Wi-Fi* settings.

Configure Wi-Fi

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.

FIGURE 8. Wi-Fi Networks

\equiv Device management $ ightarrow$	Network > Wi-	Fi	?
B ORGANIZATIONS SE	TTINGS for cloudpath.net		
 cloudpath.net 			
Employees	Wi-Fi: Cloudpath	SSID:cloudpath	
End-Of-Life Accounts	Locary appred	SSID hidden:No	
End of Ene Accounts		Auto-Connect:Yes	
External Contractors		Restricted to:Chromebooks	
Servers			
	Wi-Fi: Test73	SSID:Test73	
	Locally applied	Applied to:Users	
		SSID hidden:No	
		Restricted to Chromebooks	
,	Wi-Fi: CloudpathTest	SSID:CloudpathTest	
	Locally applied	Applied to:Users	
		SSID hidden:No	
		Auto-Connect:No	
		Restricted to:Chromebooks	
	Wi-Fi: R-DVES-Secure	SSID:R-DVES-Secure	
1	Locally applied	Applied to:Users	
		SSID hidden:No	
		Auto-Connect:Yes	
		Restricted to: Chromebooks	
	Wi-Fi' Demod	SGD-Demo/	
	Locally applied	Applied to:Users	
		SSID hidden:No	
		Auto-Connect:Yes	
		Restricted to:Chromebooks	
Ad	dd Wi-Fi		

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

FIGURE 9. Wi-Fi Settings

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

3. Enter the Wi-Fi data according to Step 3 in the Chromebook setup instructions (see Managed Chromebook Setup Instructions).

Note >>

The instructions differ by configuration. Configure the Wi-Fi settings for your network according to the Managed Chromebook Setup Instructions in the Cloudpath Admin UI.

- It is not required that the *Name* and the *SSID* match. *Name* is an internal value.
- 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.

• 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.

Note >>

Be sure to select the Root CA that includes any intermediate CAs in your configuration. The following screen capture shows that the selected root CA also contains the intermediate CA.

FIGURE 10. Imported Root CA with Intermediate CA



https://demo4.crodd	path.r
lssuer pattern	
Common name	Demo Root CA I
Locality	
Organization	
Organizational unit	
Subject pattern	
Common name	
Locality	
Organization	
Organizational unit	
roxy settings Direct Internet Conne	ection •
Proxy settings Direct Internet Conne	ection •
Proxy settings Direct Internet Conne Restrict access to this	wi-Fi network by platform
Proxy settings Direct Internet Conne Restrict access to this This Wi-Fi network will	wi-Fi network by platform be available to users using:
Proxy settings Direct Internet Conne Restrict access to this his Wi-Fi network will Mobile devices	wi-Fi network by platform be available to users using:
Proxy settings Direct Internet Conne Restrict access to this This Wi-Fi network will Mobile devices Chromebooks	Wi-Fi network by platform be available to users using:
Proxy settings Direct Internet Conne Restrict access to this This Wi-Fi network will Mobile devices Chromebooks Chromebooks Chromebook for me	ection ▼ Wi-Fi network by platform be available to users using: eetings devices
Proxy settings Direct Internet Conne Restrict access to this This Wi-Fi network will Mobile devices Chromebooks Chromebook for me	wi-Fi network by platform be available to users using: wettings devices
Proxy settings Direct Internet Conne Restrict access to this This Wi-Fi network will Mobile devices Chromebooks Chromebooks Chromebox for me Apply network	ection Wi-Fi network by platform be available to users using: eetings devices
Proxy settings Direct Internet Conne Restrict access to this This Wi-Fi network will Mobile devices Chromebooks Chromebooks Chromebox for me Apply network by user	ection Wi-Fi network by platform be available to users using: vetings devices

FIGURE 11. WiFi Setup Continued

- Enter the *Client enrollment URL* that is listed on the Chromebook setup instructions (see Managed Chromebook Setup Instructions).
- Enter the *Issuer pattern* fields as directed by the Managed Chromebook Setup instructions. *Common Name* is a required field.
- Apply network by user.

- 4. Click Add to add the Wi-Fi configuration for the organization.
- 5. Return to the Device Management page to configure the force-install application.

Configure Policies for Device Users

Configure policies for Chrome device users within an organizational unit. Configure the policy for the Cloudpath extension in the *Apps and Extensions* section.

Force-installed Apps

You can force install apps on your users' 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.

Note >>

Even if the Cloudpath user experience settings (see User Experience Settings) are configured for *ONC* + *Device* extensions, the *Force install apps* are configured in *User* settings.

- 2. Scroll down to the Apps and Extensions section.
- 3. Click Manage force-installed apps.



Chrome Web Store	>	Total to force install: 1	
Domain Apps	>	XpressConnect C	Details Remove
Specify a Custom App	>		
Business Apps	>		
Business Extensions	>		

The left side lists the available apps and extensions, and the right side lists the apps and extensions to install on the managed devices for this network.

4. Search for the Cloudpath Certificate Generator and add to the force-install list.

The extension is installed on the user device according to the Chrome OS user experience *Behavior* setting in Cloudpath.

Note >>

Alternately, you can access policy settings by navigating to Device Management > Chrome Management App Management, select the Cloudpath Certificate Generator, and then User Settings.

Force Install Unlisted (Beta) Apps

If your application is unlisted, you must load it as a custom application.

1. Navigate to Device Management > Chrome > App Management.

FIGURE 13. Chrome App Management

\equiv Device management > Chr	ome
	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

16

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

FIGURE 14. Add Custom App

\equiv Device management $ ightarrow$ Cl	me > Chrome App Management	. 0 :
Filters	Apps	Add custom app
Type My configured apps 🔹	AIRSecureTest	Manage Apps in User Settings
Find or Update Apps	ApressConnect Cert Generator - Offline Device	Configured
SEARCH	ApressConnect Certificate Generator	Configured
	XpressConnect Certificate Generator - Beta	Installed

3. Enter the App *ID* and *URL*.

FIGURE 15. Custom App Parameters

\equiv Device management $>$ Chron	ne > Chrom	e App Management	. © :
Filters		×	
Type My configured apps	AIRSecure	Add custom app You must supply both the extension id and the url where the extension is hosted.	
Find or Update Apps	XpressCon	ID abcdefghijklmnopqrstuvwxyz URL https://clients2.google.com/service/up/	
SEARCH	XpressCon	ADD	
	XpressConnec	t Certificate Generator - Beta	Installed

Note >>

To find the app *ID*, hover over the *More Info* for the app on the *Developer Dashboard* page.

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

4. Select User settings.

Г

FIGURE 16. Custom App User Settings

E 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 Klosk App

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

\equiv Device management	> Ch	nrome App Management > a	bcdefghijklmnopqrs	tuvwzyz	
	~ Us	abcde https://clients2	fghijklmnop google.com/service/update2/c	oqrst	
		Orgs cloudpath.net Employees End-Of-Life Accounts External Contractors Servers	Settings f Allow installation Setting inherited Override Pin to taskbar	or cloudpath.net Force installation Configure UPLOAD CONFIGURATION FILE CANCEL	

FIGURE 17. Configure Custom App

- 6. In the right pane, enable Force installation.
- 7. Save the configuration.

The unlisted application can now be added as a Force-install app. See Force-installed Apps for more information.

Chromebook User Experience

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 differ, 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 user simply connects the secure network.

The following section provides an example of the Chromebook user experience. The sequence of steps for the enrollment differ, depending on the selection that is made.

- 1. The user connects to the deployment URL (either directly, or through a Captive Portal).
- 2. The Cloudpath Welcome screen displays.

XpressConnect Enrollme × _ ____ ☆ 🚹 🗉 Start Over Your Logo Here Welcome to the Anna Test Network Access to the Anna Test network is restricted to authorize and requires acceptance of the Terms & Conditions below. ce authorized for access, your device will be configured with a le certificate for network acc ✓ I agree to the <u>Terms & Conditions</u> Start > 2:58 😴 💈 0 8

FIGURE 18. Wizard Welcome Page

The login screen is typically 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.

User Type Prompt

If required by the network, the user might see a User Type prompt. A user type prompt can provided 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.

FIGURE 19. User Type Prompt



User Credentials

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 via PAP.

FIGURE 20. User Credentials

V PressConnect Enrollme ×	-	4P	×
← → C 🔒 https://anna44.cloudpath.net/enroll/AnnaTest/Production/process	5	2 🚹	Ξ
Start, Over Powered by Cloudpath Networks			
Your Logo Here			
Your username and password are required to access the network.			
Username:			
Password:			
Need Assistance?			
< Back Continue >			
Assistance jD #30/E			
	2:59 🤇	2 8	贡

Device Type

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

FIGURE 21. Device Type Prompt

← → C A https://anna44.cloudpath.net/enro	II/AnnaTest/Production/process		_ F ∧ F ☆ <mark>8</mark> =
	Start Over	Powered by Cloudpath Networks	
	Your Device	Personal Device Select this option if the device belongs to you.	
	Company Devic	IT-Issued Device Select this option if the device belongs to Sample Corporation. To join the network, you must enter the voucher included on the green label on the device's box.	
	< Bast		
III 📀 M 🗷 🖹 🕨			1 3:07 😴 🗳 🁮

Managed or Unmanaged Chromebooks

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 Chromebook User Experience
- Managed Chromebooks With Extension User Experience

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.

C XpressConnect Enrollme ×		-	Ъ	×
← → C 🔒 https://bvtes.cloudpath.net/enroll/BVTEnrollme	entSystem/Production/wizard/2/page4_download.html	☆		Ξ
	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			
	If you are not logged in as the Chromebook owner, log out and log back in as the owner.			4
	Step 1: Download the Network File Singly 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 & passib) this address into the browser: chromeriken-internativeromeos			
	Yoper Connect Involve →			
	10.5	55 😴		7
				\sim

FIGURE 22. Configuration Installation Instructions

The manual download page shows the Chromebook instructions.

Step 1 provides the link to download the ONC file.

Step 2 provides instructions for importing the ONC file.

- Copy the URL from the instructions.
- Paste the URL into a new browser window. The Chrome OS Import ONC File page displays.

XpressConnect by Cloud × chrome://net-internals/# ×
← → C C chrome://net-internals/#chromeos
ChromeOS Capturing events (25927)
Import ONC file
Choose File No file chosen
ONC file successfully parsed
Store Logs
Store Debug Logs
Network Debugging
Select interface for debugging Wi-Fi Ethernet Cellular WiMAX None

FIGURE 23. Import ONC File

• Click Choose File and browse to select the <NetworkName>.onc file.

After the ONC file installed, click the Wi-Fi icon in the bottom right corner of your screen and select the secure network.

FIGURE 24. Select Wi-Fi Network

🧟 Sample Campus	Secure
Searching for Wi-Fi netw	vorks
😪 cloudpath	
🗢 Shin OnRamp	
< cpn-moto-help-eu	la
Join other	Settings
< Network	•
	1 9:48 マ 💈 👮

Typically, user credentials are populated using the information passed during the enrollment process. Click *Connect*.

FIGURE 25. Enter User Credentials	IGURE 25.	Enter	User	Cred	lential	s
-----------------------------------	-----------	-------	------	------	---------	---

Join Wi-Fi network		×
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:		\odot
Anonymous identity:		
	Save identity and password	
	Connect Cane	cel

The user should now be connected to the secure network.

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.

FIGURE 26. Generating Certificate

C XpressConnect Enrollme ×		_ P	×
← → C 🔒 https://bvtes.cloudpath.net/enroll/BVTEnrollm	entSystem/Production/wizard/2/page4_download.html#	☆ 🚹	Ξ
	Your Logo Here		
	To access based on y Processing bns below		
	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		
	Install for ChromeOS Cick to Istal Centricate		×
DVES-Secure.onc *	The certificate is being general may take up to a minute.	ed. This	
	0 2.3	₹	Ŕ

The extension imports the certificate into the TPM.

FIGURE 27.	Certificate	Imported
------------	-------------	----------

/ XpressConnect Enrollme ×		_ @ ×
← → 🗙 🔒 https://bvtes.cloudpath.net/enroll/BVTEnrolln	nentSystem/Production/wizard/2/page4_download.html#	☆ 🚹 🔳
	Your Logo Here	
	To access based on y 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 Install for ChromeOS	
Connecting DVES-Secure.onc *	Certificate Imported The certificate was imported int	x the TPM.
📰 🧿 🛛 🖪 📄 🕨	0 231	🗢 🛯

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

FIGURE 28. Certificate Installed	ł
----------------------------------	---

XpressConnect Enrollme ×			_ & ×
← → C 🔒 https://bvtes.cloudpath.net/enroll/BVT	EnrollmentSystem/Productio	n/wizard/2/chromeExtensionDone	☆ 👔 🔳
	Start Over	Powered by Cloudpath Networks	
	Your	Logo Here	
	The certifica	ate has been installed.	
	The certificate is installed an to the wireless network.	d ready for use. Select TV/ES-Secure' to connect	
	Assistance ID #3FE0		
DVES-Secure.onc			\$ Show all downloads ×
III 🧿 🛛 💈 🖹 🔼			0 2:31 ኛ 🗎

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

FIGURE 29. Select Wi-Fi Network

(¢	Sample Campus	Secure	
Sear	ching for Wi-Fi netw	orks	
R	cloudpath		
¢	Shin OnRamp		
۲	cpn-moto-help-eu	la	
	Join other	Settings	
<	Network	•	
		9:48 💎 💈 🕺	Ţ

The user should now be connected to the secure network.

Troubleshooting Tips

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.

- 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 prefetch the DNS records.
- chrome://chrome-urls View all the available chrome:// commands.