CONFIGURATION GUIDE

Cloudpath Enrollment System Chromebook Configuration Guide, 5.5

Supporting Cloudpath Software Release 5.5

Part Number: 800-72397-001 Rev A
Publication Date: 28 August 2019

Copyright, Trademark and Proprietary Rights Information

© 2019 CommScope, Inc. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Overview **4**
Supported Devices 4

Configuring Cloudpath **4**
Enable the Chrome OS 4
Chromebook User Experience 5
Download the Root CA 7

Configuring the Chrome Extension **9**
Chrome Admin Console Settings 9
Network Settings 11
Configure Policies for Device Users 18

Chromebook User Experience **23**
Enrollment Workflow 24
Managed or Unmanaged Chromebooks 26

Troubleshooting Tips **34**
Error Messages 34
Server CA 34
Access to URL 34
Length of Private Key 35
Chromebook Testing Shortcuts 35

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.

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.

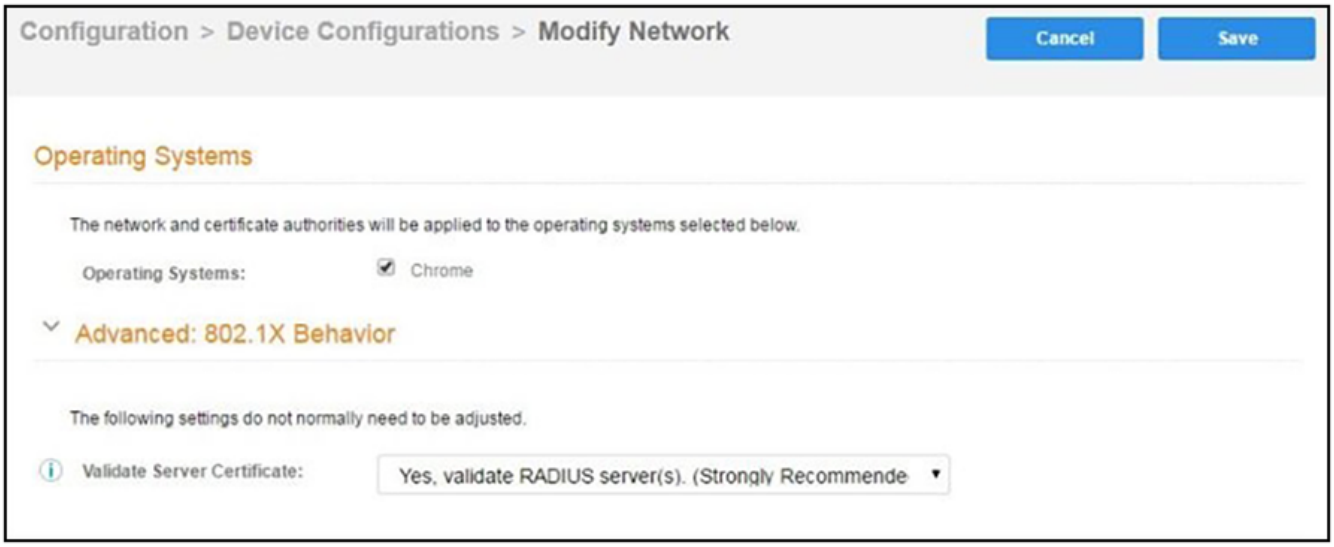
Enable the Chrome OS

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** > **Device Configurations**.
2. Select the device configuration to support the Chrome OS.

3. On the **OS Settings** tab, edit the **Chrome: Configuration from the Network(s) and Trust tabs**.

FIGURE 1 Enable Chrome OS



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.

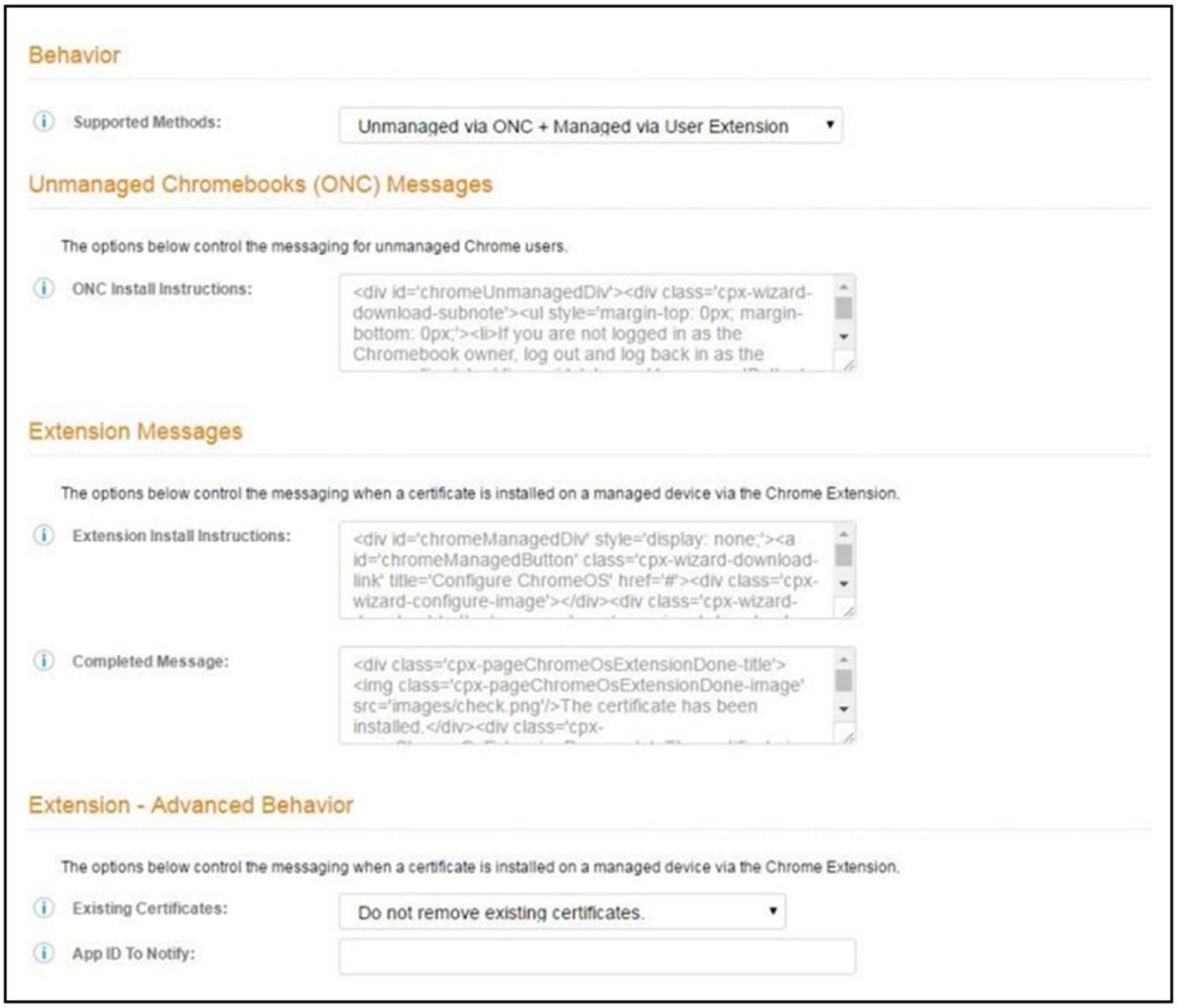
User Experience Settings

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



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.

> **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.

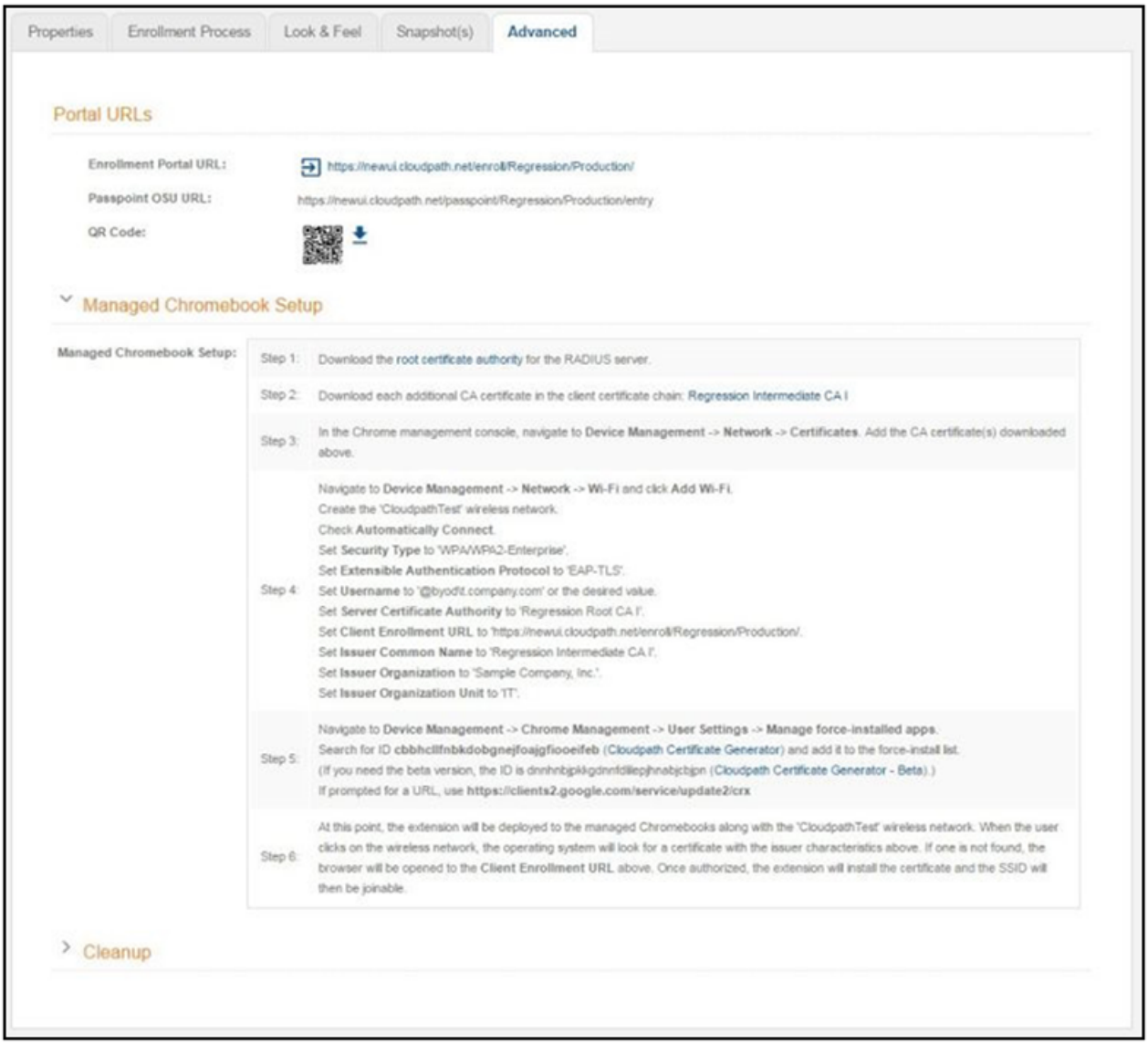
Use the link in Step 1 of the **Managed Chromebook Setup** page to download the root CA.

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.

FIGURE 3 Managed Chromebook Setup Instructions



NOTE
The extension ID is listed in the Chromebook Setup Instructions.

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. Configure Wi-Fi and Certificates on the **Networks** page. Configure force-installed apps on the **Chrome Management** page.

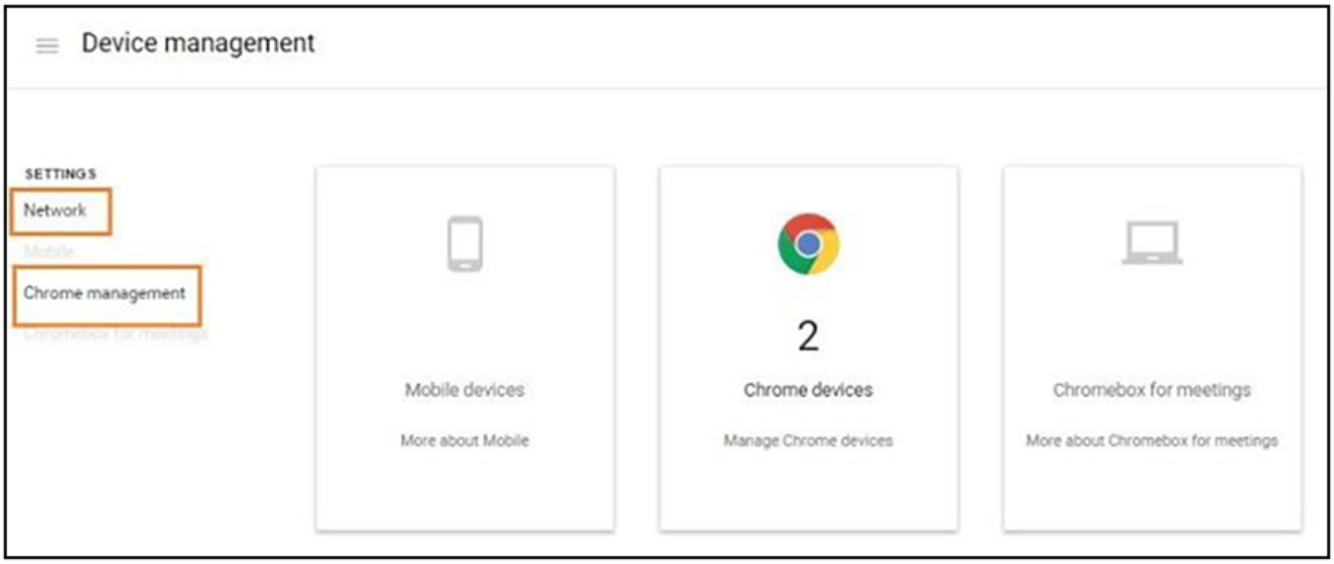
To access network and wireless settings:

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

FIGURE 4 Chrome Admin Console

2. Select **Device Management**.

FIGURE 5 Device Management

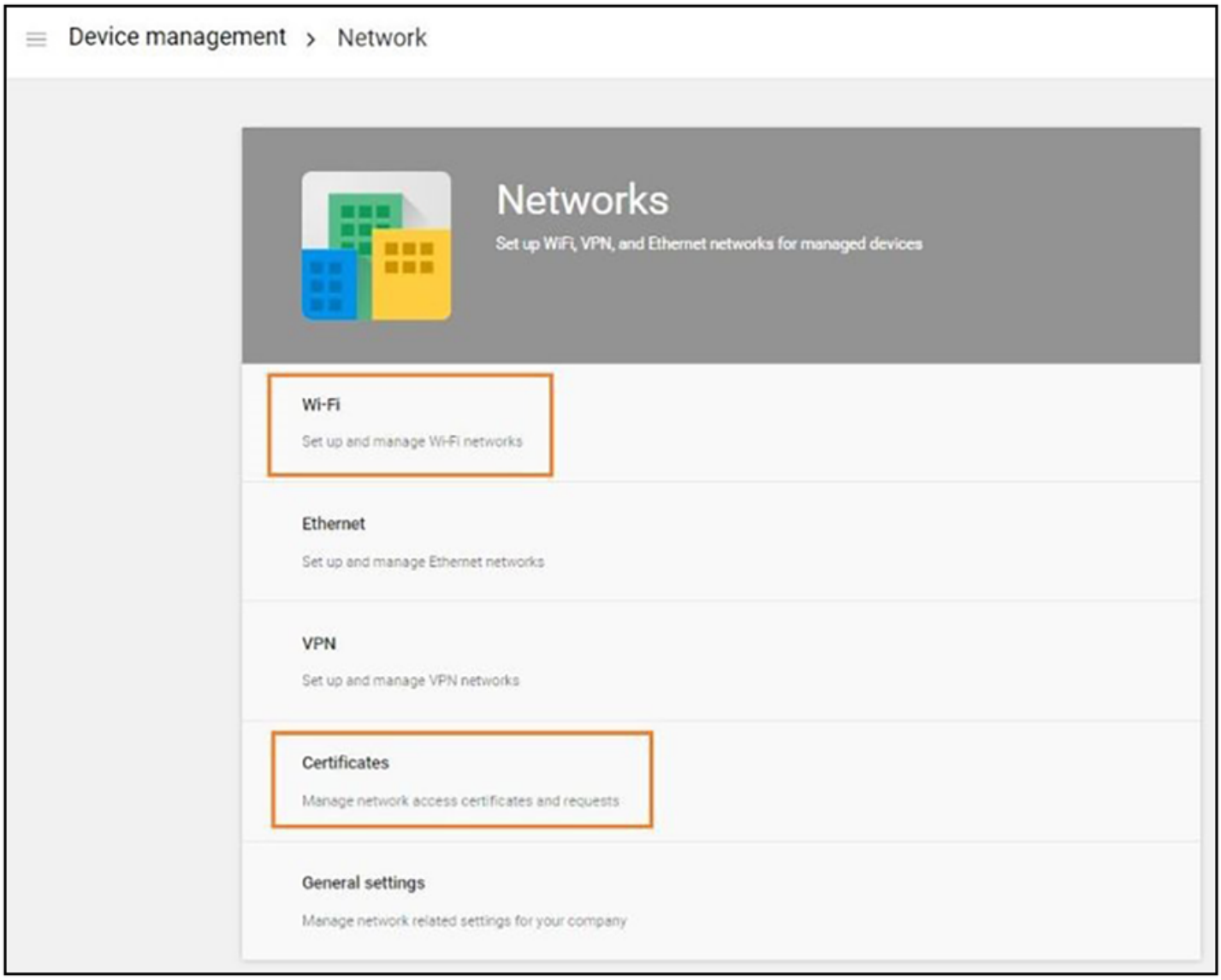


Use the **Network** link to set up Wi-Fi and **Certificates** for managed devices. Use the **Chrome management** link to set up Wi-Fi and Certificates for managed devices.

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.

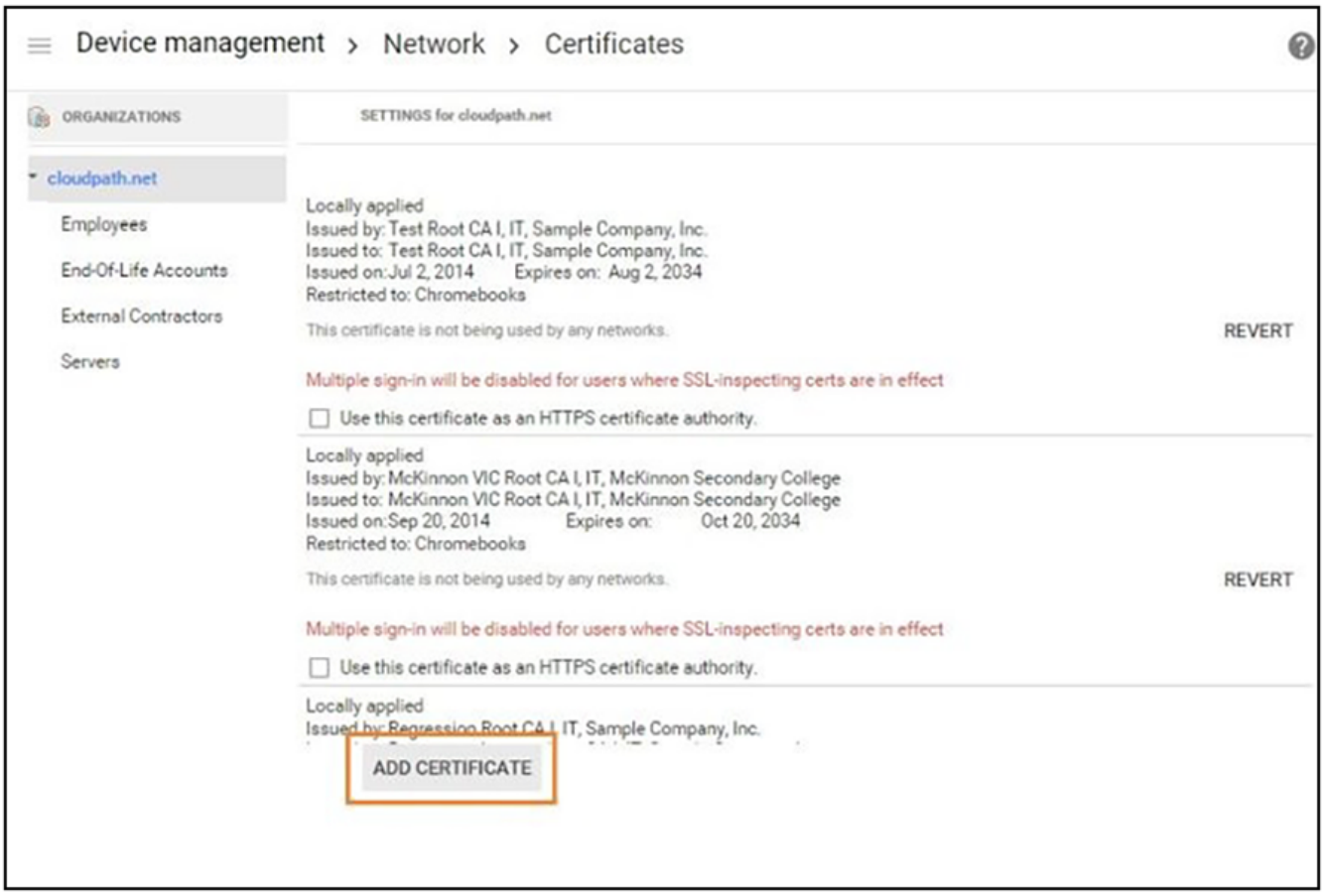
FIGURE 6 Network Settings



Import CA certificate

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

FIGURE 7 Manage Certificates



2. 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.
3. Click **Add Certificate**.
4. 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.

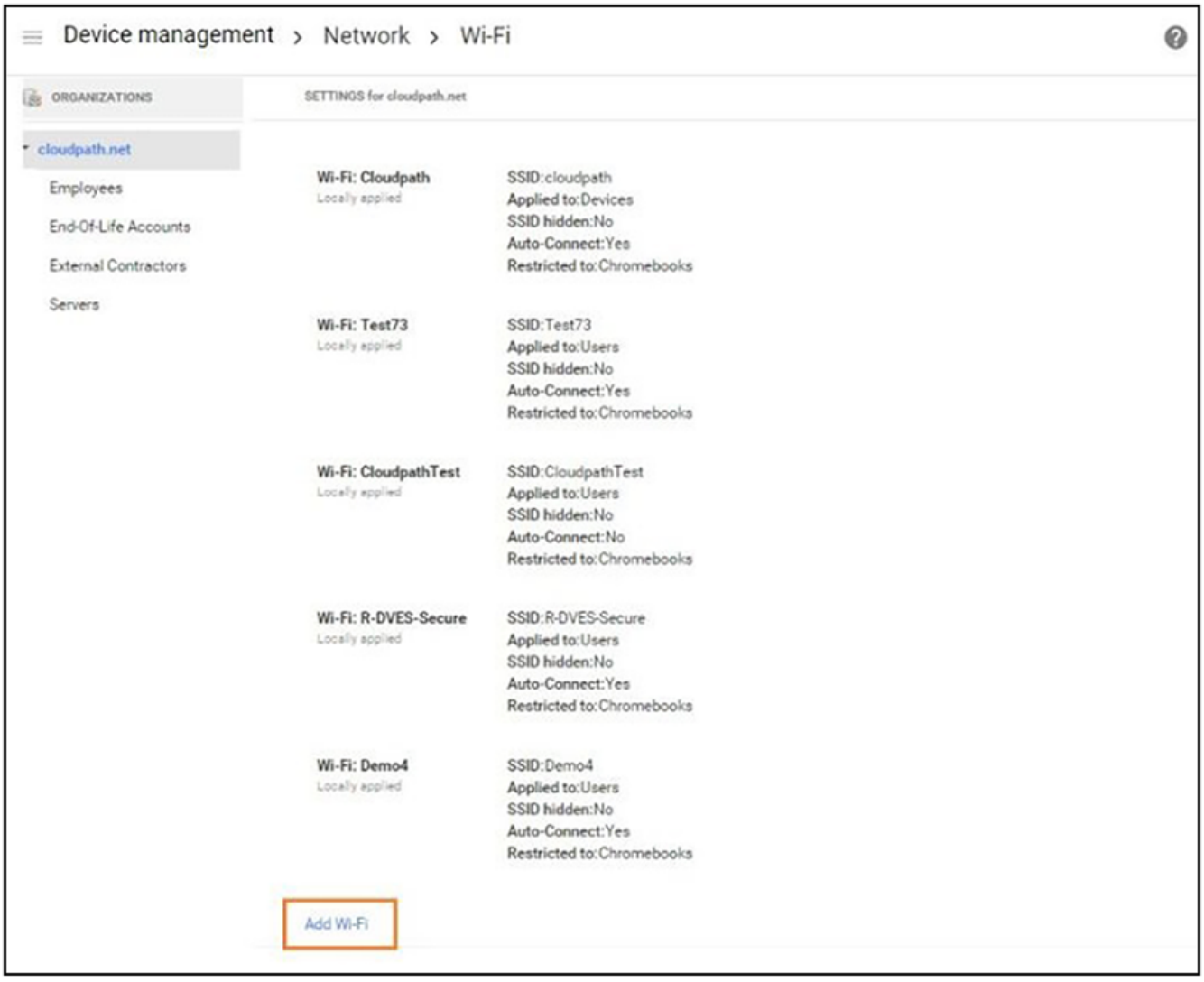
5. If your Cloudpath configuration contains additional CAs, you must also import the additional CAs.
   The link for downloading additional CAs can be found in Step 2 of the Managed Chromebook Setup Instructions.
6. When the certificates have been successfully uploaded, return to the **Networks** page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



3. Click **Add Wi-Fi**. The **Add Wi-Fi** page displays.

FIGURE 9 Wi-Fi Settings

4. 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.

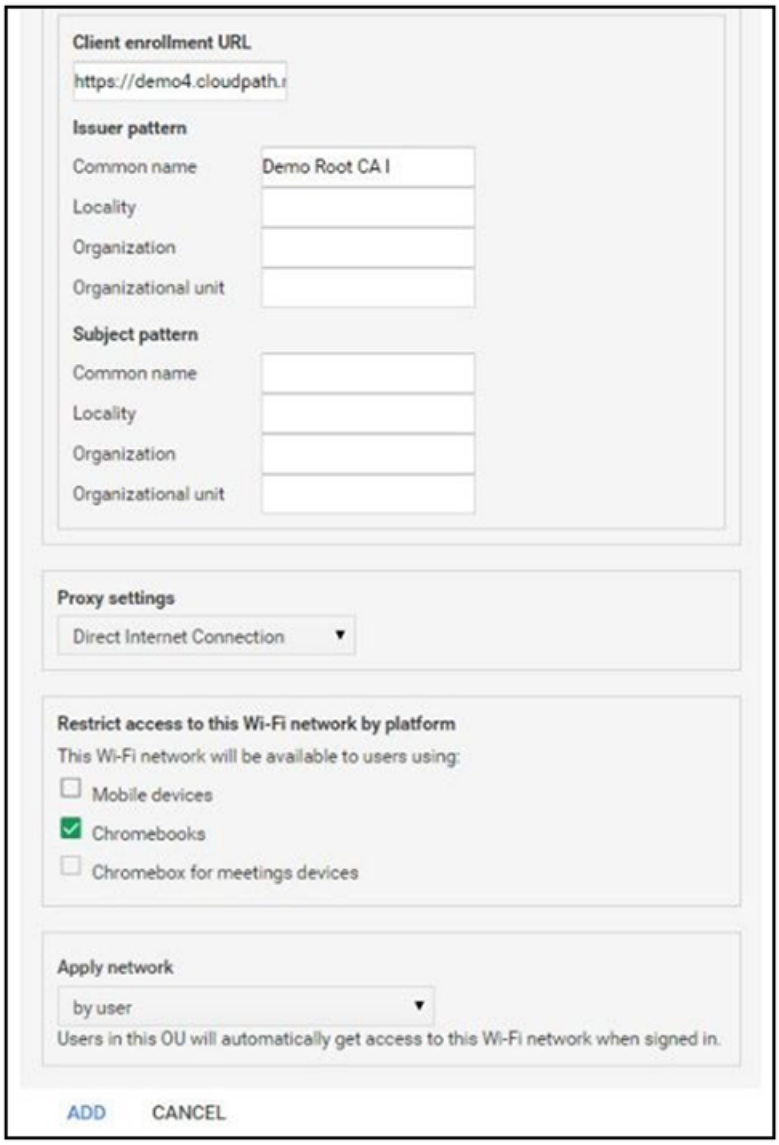
     NOTE
     If using a Microsoft CA instead of the Cloudpath onboard CA, use ${CERT_SAN_UPN} in the Username field to bring the Microsoft CA User Principle Name into the identity box. For more information, see this Google link for more information: https://support.google.com/chrome/a/answer/2634553?hl=en#top&add&wifi&thirdparty&variables&change&managecerts&autoconnect&

5. 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

FIGURE 11 WiFi Setup Continued



a) Enter the **Client enrollment URL** that is listed on the Chromebook setup instructions (see Managed Chromebook Setup Instructions).

b) Enter the **Issuer pattern** fields as directed by the Managed Chromebook Setup instructions.

Common Name is a required field.

> **NOTE**
> If using a Microsoft CA instead of the Cloudpath onboard CA, use the "Issued by" value of the CA certificate.

c) Apply network by **user**.

6. Click **Add** to add the Wi-Fi configuration for the organization.
7. 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.

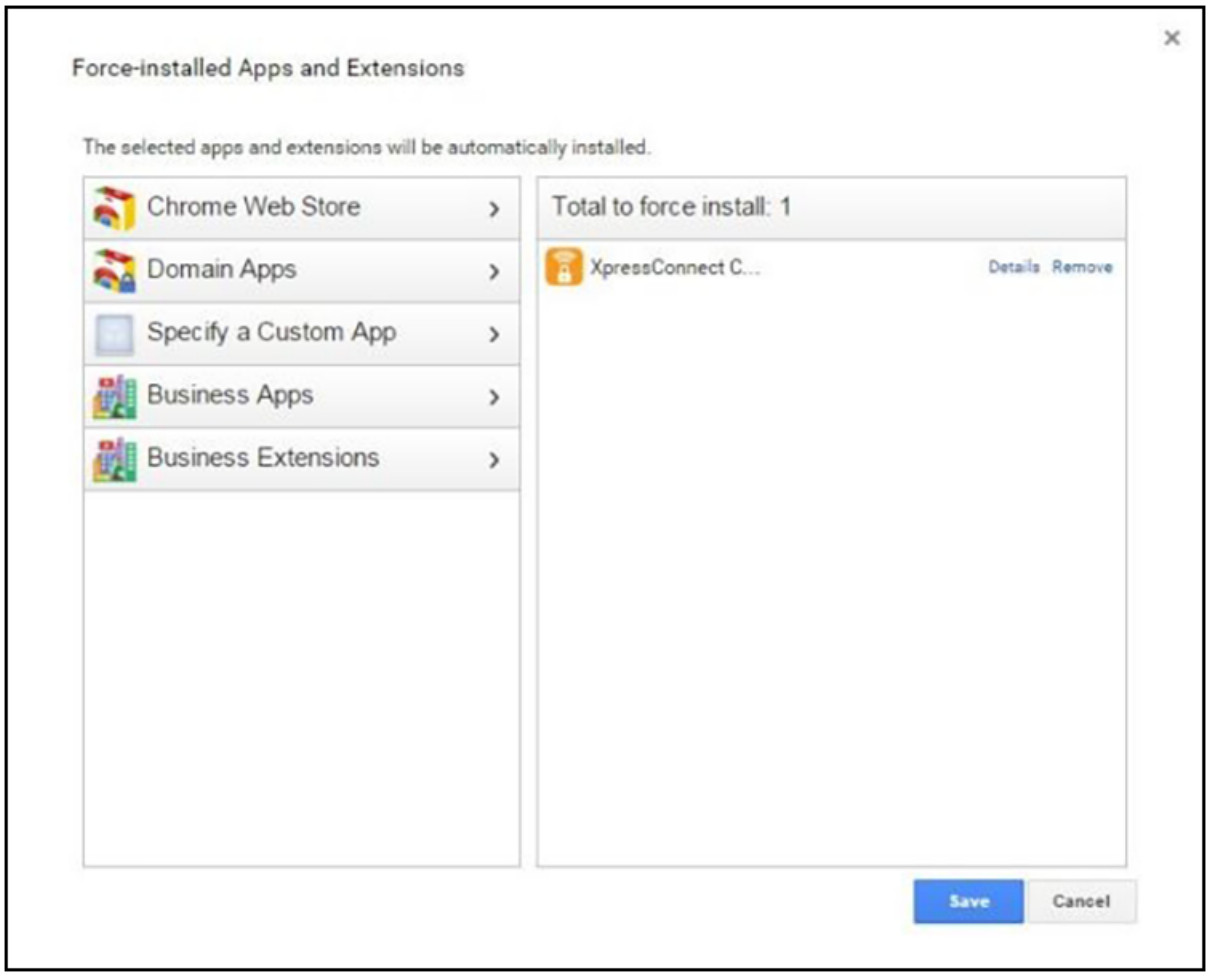
1. Navigate to **Device Management** > **Chrome Management**, and select **User Settings**.

   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**.

FIGURE 12 Force-Installed Apps and 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

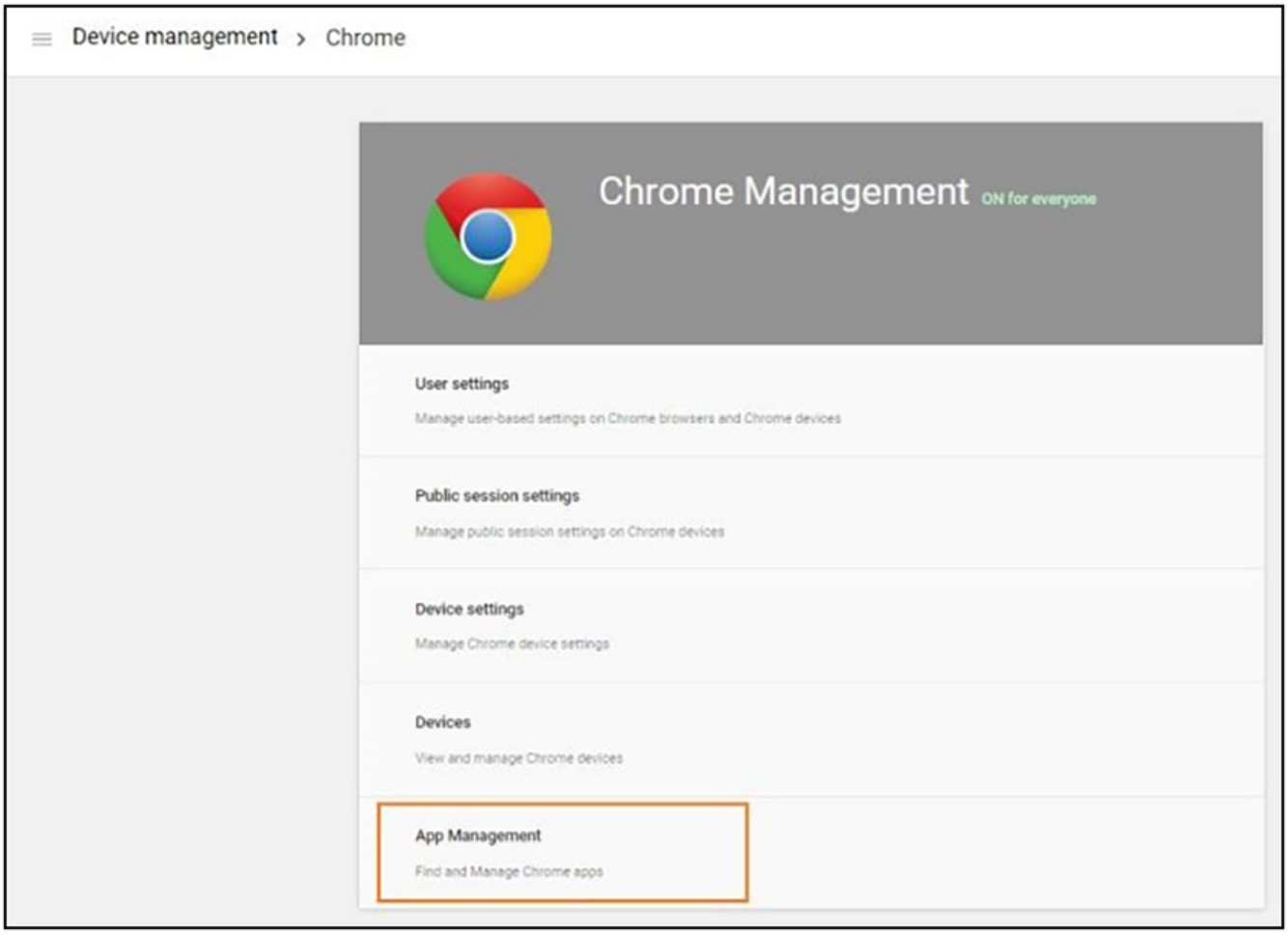
NOTE
Alternatively, you can access policy settings by navigating to **Device Management** > **Chrome Management** > **App Management**, select the **Cloudpath Certificate Generator**, and then **User Settings**.

Force Install Unlisted (Beta) Apps

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

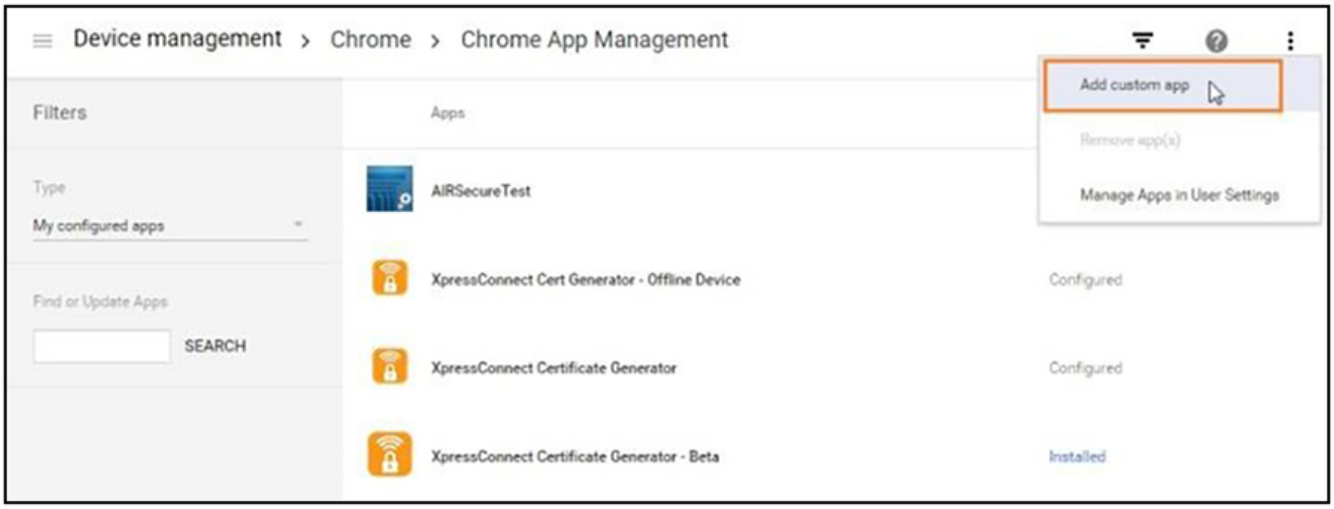
1. Navigate to **Device Management** > **Chrome** > **App Management**.

FIGURE 13 Chrome App Management



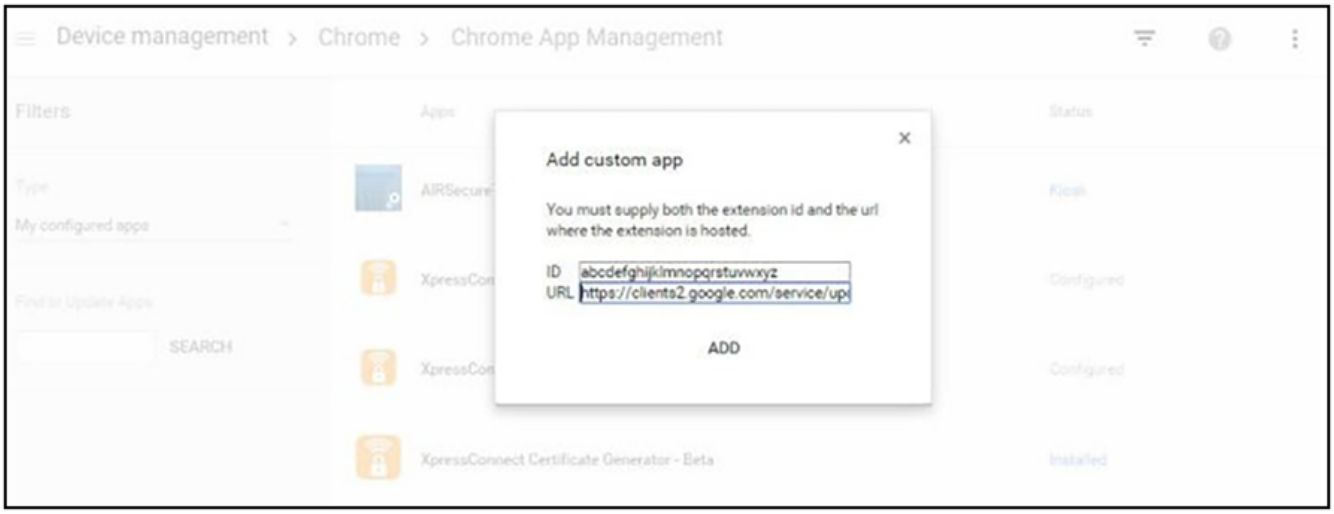
2. From the top-right **Settings** menu, select **Add Custom App**.

FIGURE 14 Add Custom App



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

FIGURE 15 Custom App Parameters

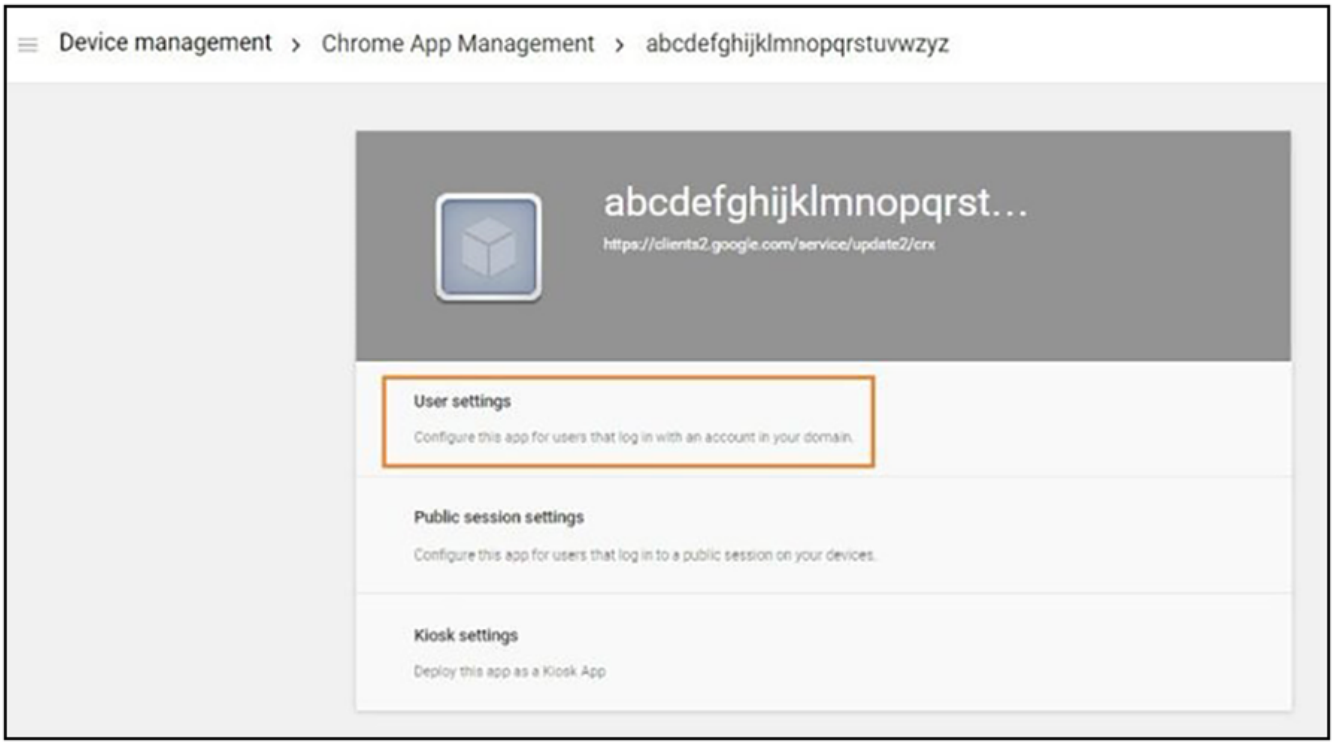


NOTE
To find the app **ID**, hover over the **More Info** for the app on the **Developer Dashboard** page.

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

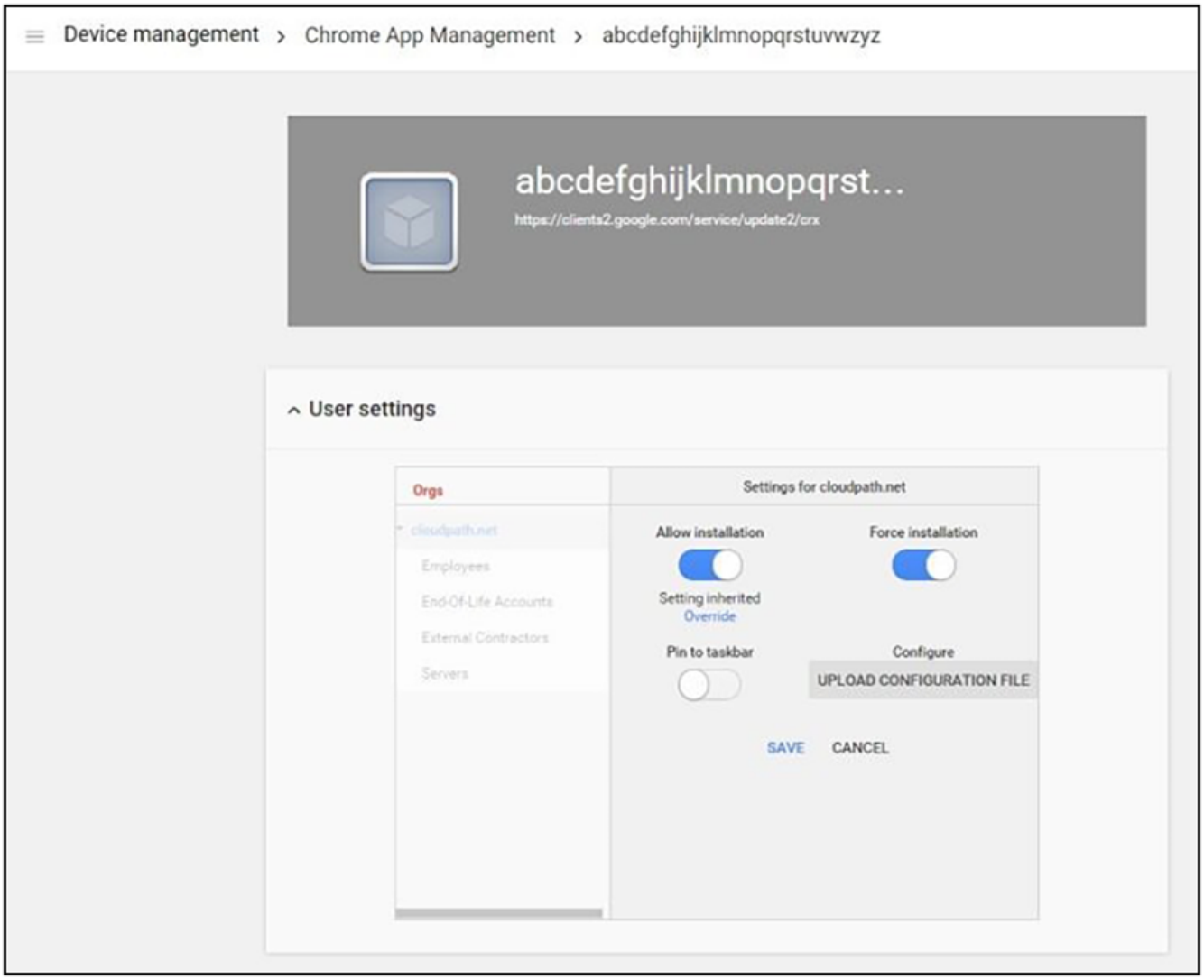
4. Select **User settings**.

FIGURE 16 Custom App User Settings



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

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.

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

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

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 sections to continue with the user experience example for your configuration.

- Unmanaged Chromebook User Experience
- Managed Chromebooks With Extension User Experience

Unmanaged Chromebook User Experience

1. 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.

2. For unmanaged devices, the application detects the Chrome operating system and displays instructions for installing the Chrome configuration on the device.

FIGURE 22 Configuration Installation Instructions

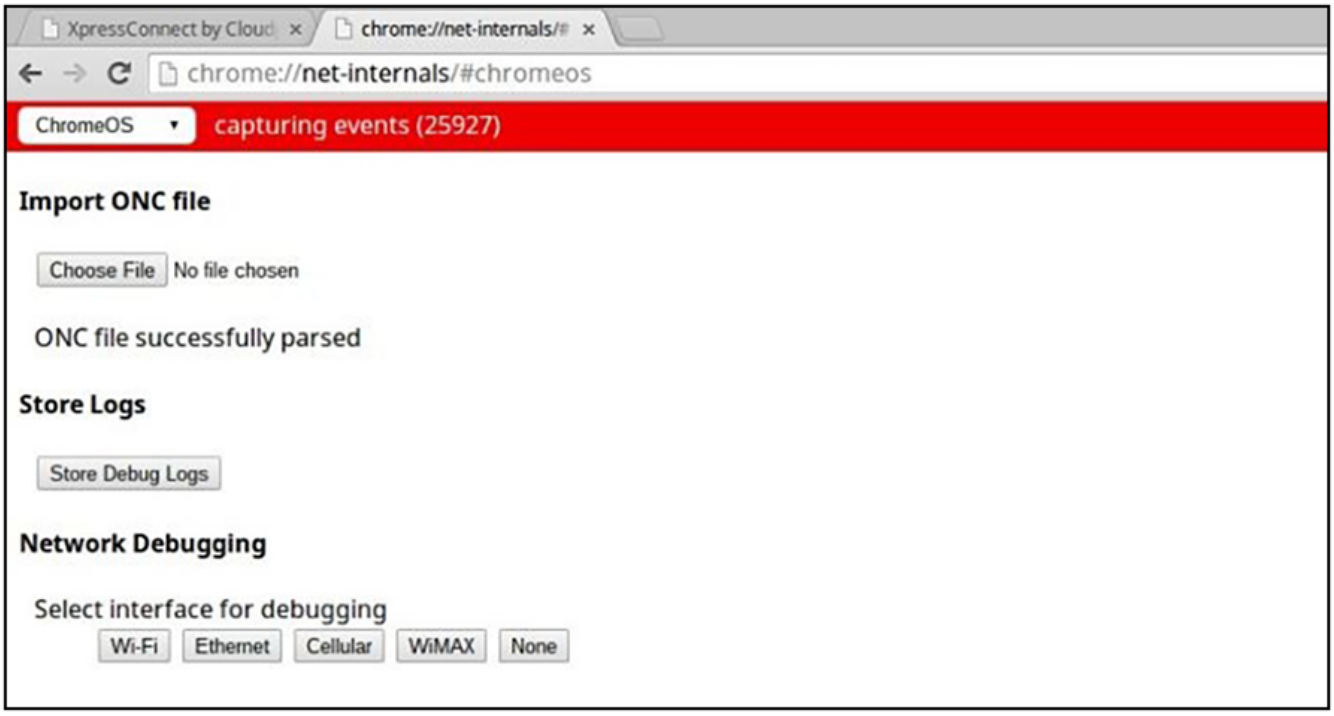
The manual download page shows the Chromebook instructions.

- **Step 1** provides the link to download the ONC file.
- **Step 2** provides instructions for importing the ONC file.

3. Copy the URL from the instructions.

4. Paste the URL into a new browser window. The Chrome OS **Import ONC File** page displays.

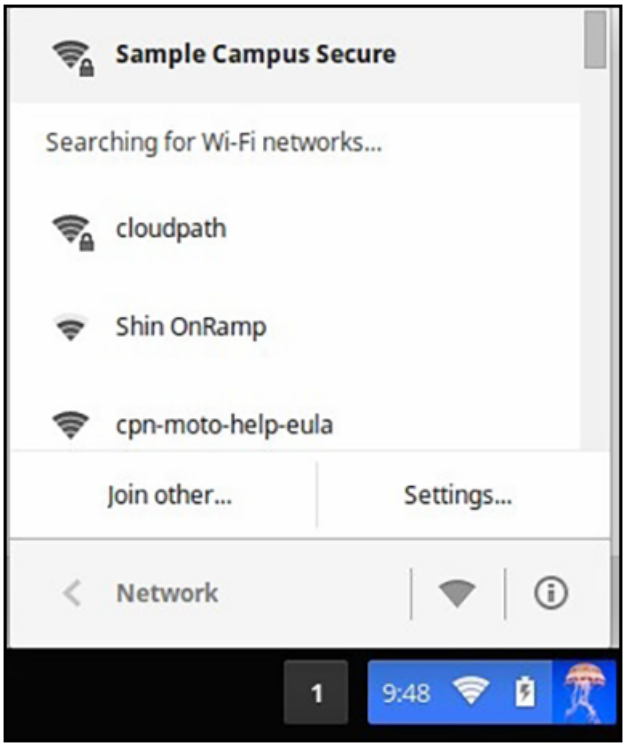
FIGURE 23 Import ONC File



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

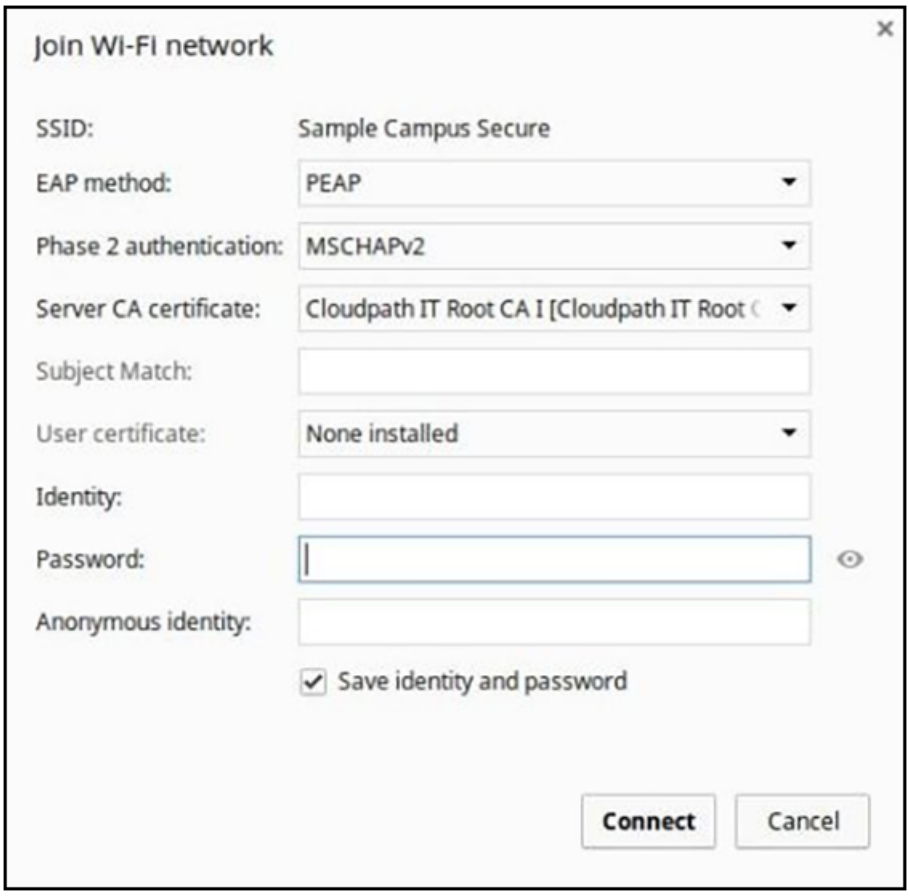
6. After the ONC file installed, click the **Wi-Fi** icon in the bottom right corner of your screen and select the secure network.

FIGURE 24 Select Secure Wi-Fi Network



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

FIGURE 25 Enter User Credentials



The user should now be connected to the secure network.

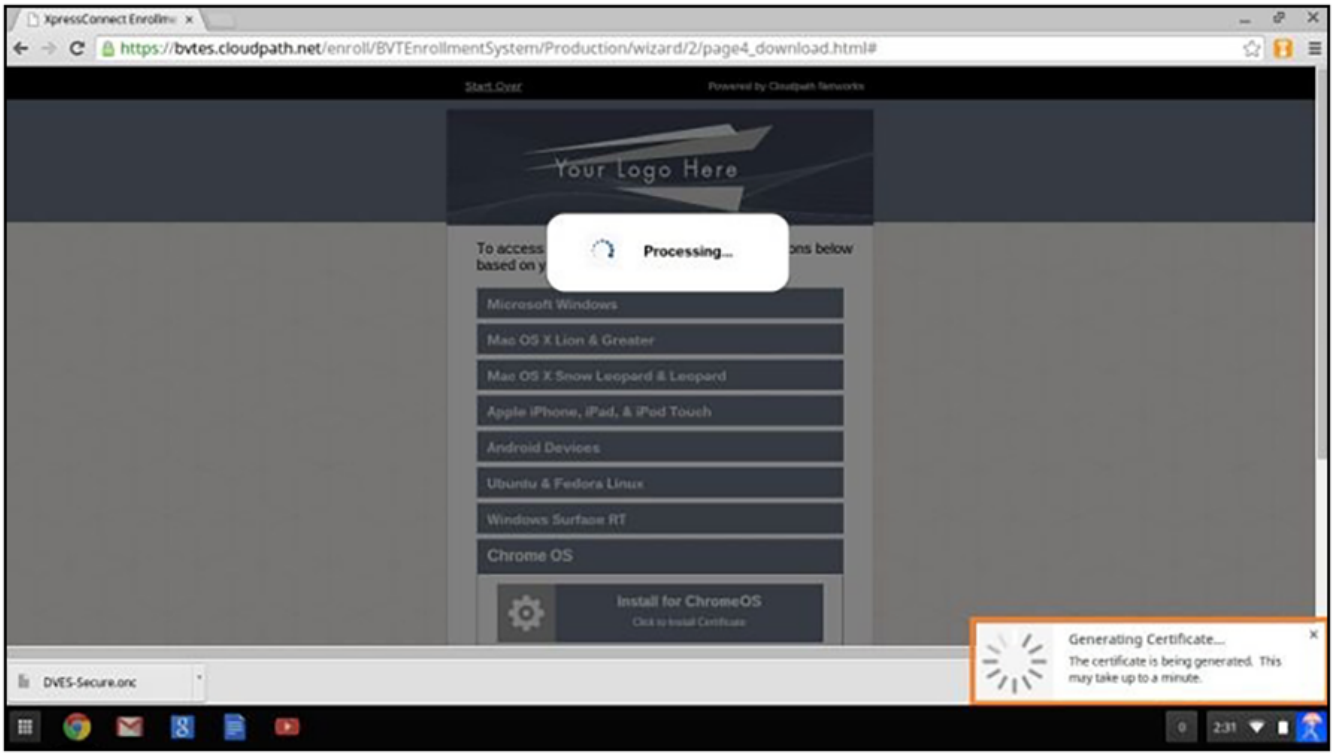
Managed Chromebooks With Extension User Experience

If managed Chromebooks are configured, the download page does not display.

1. When Cloudpath detects the Chrome OS during enrollment, the extension automatically generates and installs the CA certificate into the TPM.

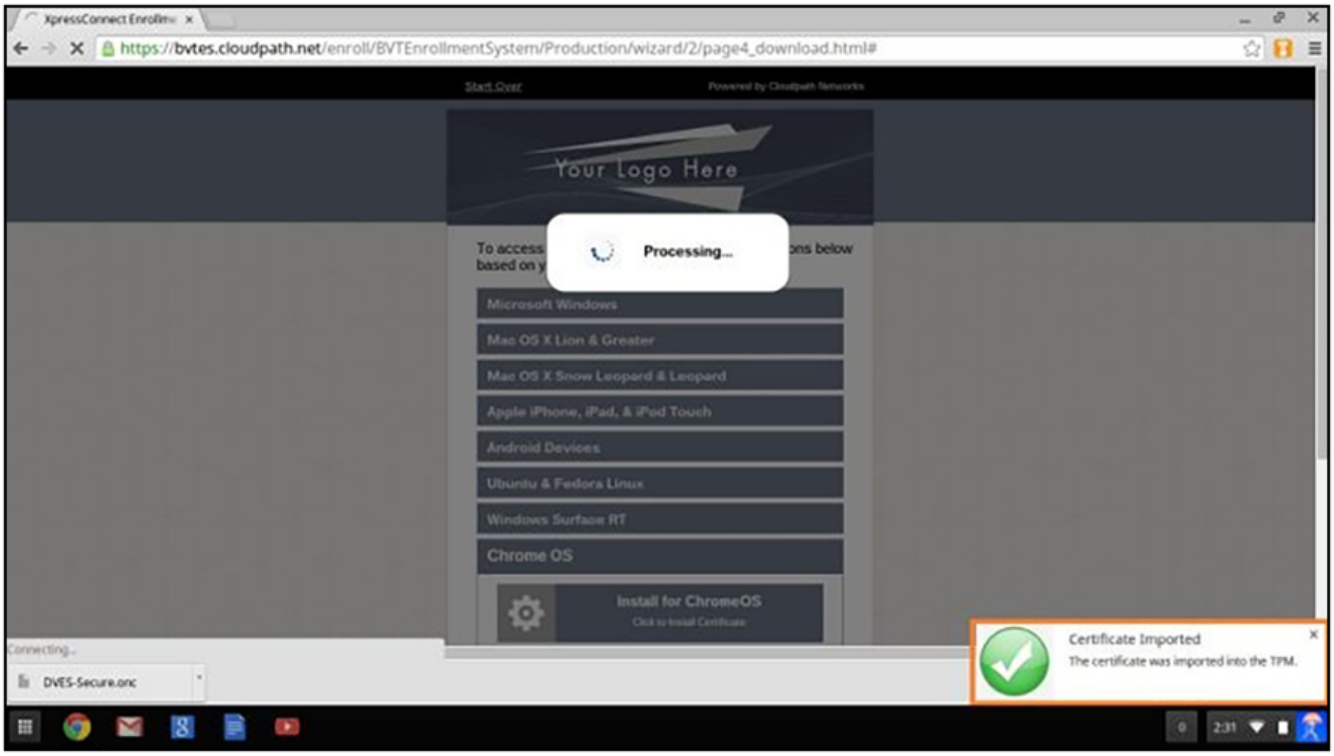
   The extension generates the certificate.

FIGURE 26 Generating Certificate



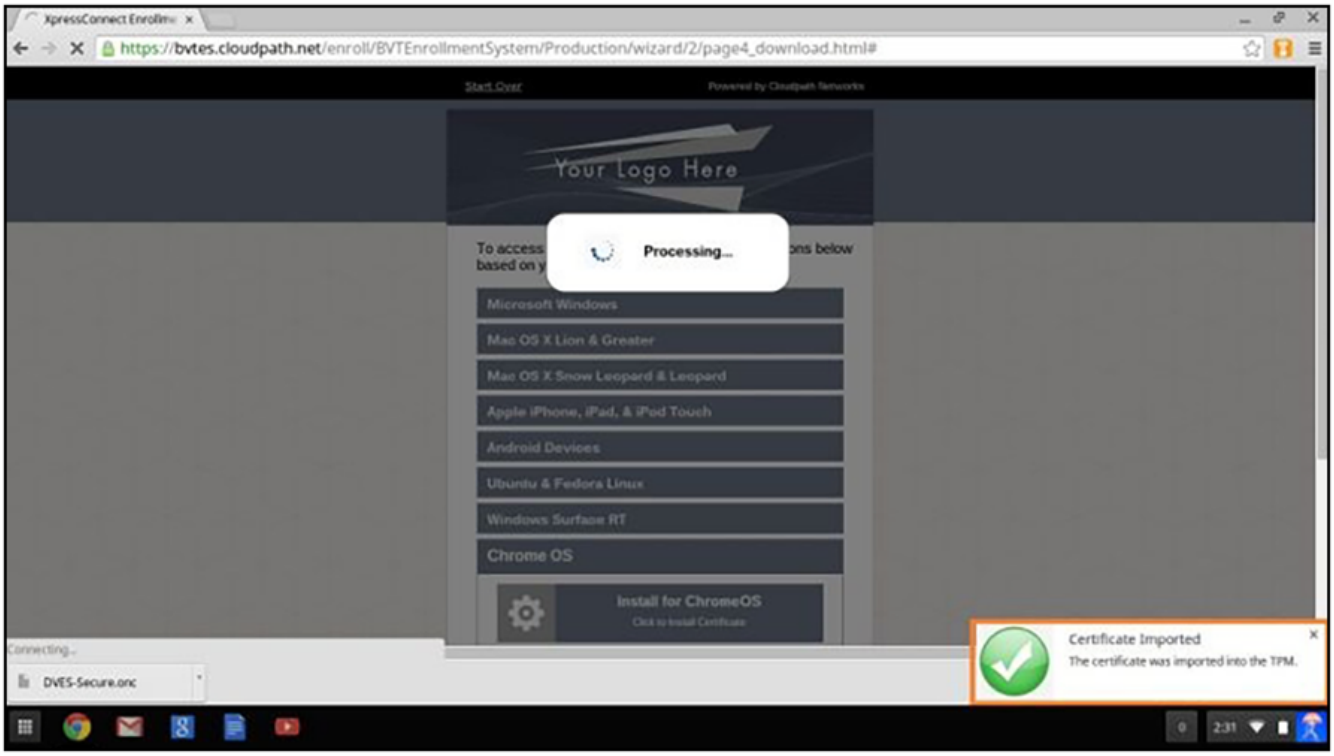
2. The extension imports the certificate into the TPM.

FIGURE 27 Certificate Imported



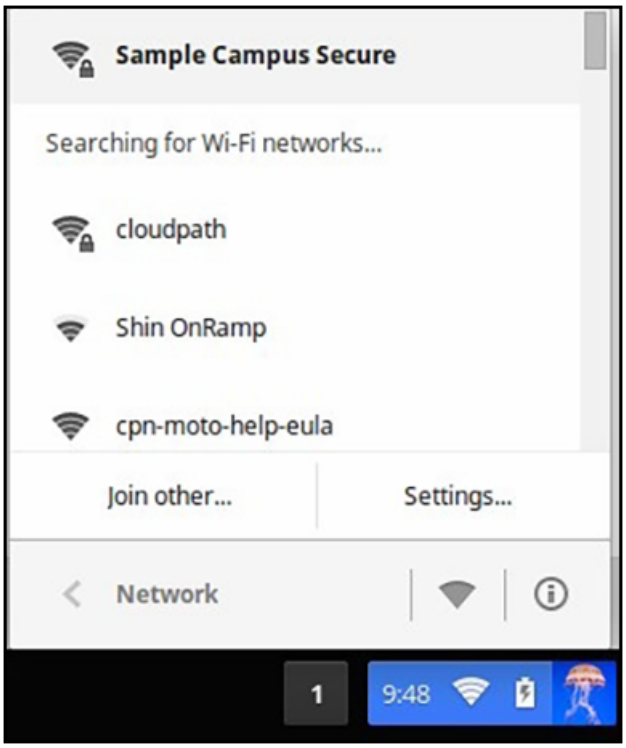
3. When the certificate installation is complete, a message displays indicating that the certificate is installed and ready for use.

FIGURE 28 Certificate Installed



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

FIGURE 29 Select Wi-Fi Network



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

© 2019 CommScope, Inc. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com