

XpressConnect Enrollment System

Configuring the Enrollment System to Support Managed and Unmanaged Chromebooks

Software Release 4.2

December 2015

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

Document Type: Support

Audience: Network Administrator



Configuring the Enrollment System to Support Chromebooks

Software Release 4.2

December 2015

Copyright © 2015 Cloudpath Networks, Inc. All rights reserved.

Cloudpath Networks and **XpressConnect** are trademarks of *Cloudpath Networks, Inc.*

Other names may be trademarks of their respective owners.

Configuring the Enrollment System to Support Managed and Unmanaged Chromebooks

Overview

The XpressConnect 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.

The Enrollment System (ES) can automatically distribute user and device certificates to both IT-managed and unmanaged (BYOD) Chromebooks.

- For IT-managed Chromebooks, the ES 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, the ES 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), the Enrollment System provides a secure method for Automatic Device Enablement.

The Enrollment System 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

The ES 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 the Enrollment System

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

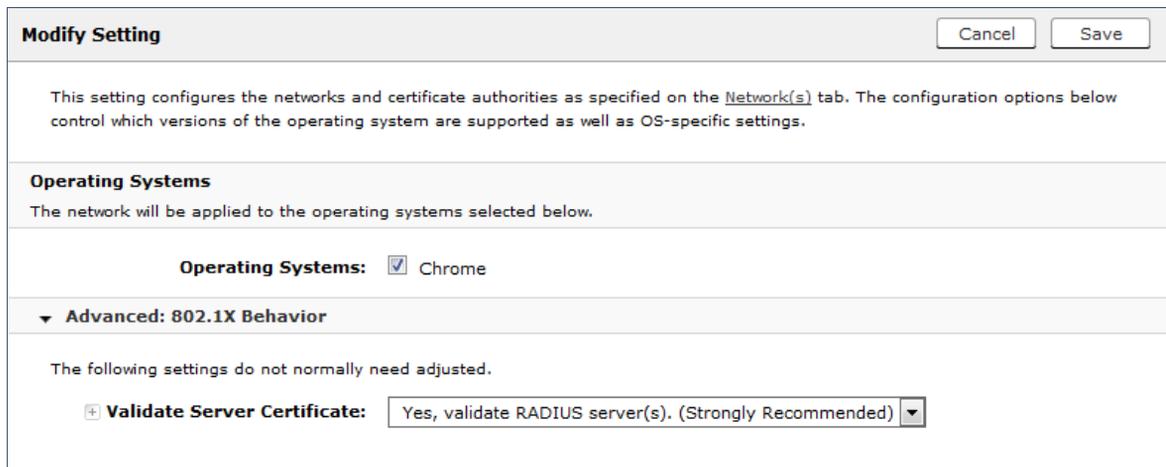
During user enrollment, if the Chrome OS is detected, the ES displays Chrome OS-specific instructions for downloading the configuration file and installing it on the device, or if extensions are configured, the certificate and Wi-Fi settings are installed in the TPM.

Enable the Chrome OS

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

1. On the ES 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



The screenshot shows a 'Modify Setting' dialog box. At the top right are 'Cancel' and 'Save' buttons. Below is a descriptive paragraph: '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.' The main section is titled 'Operating Systems' and contains the text 'The network will be applied to the operating systems selected below.' Underneath, 'Operating Systems:' is followed by a checked checkbox and the text 'Chrome'. Below this is a section titled 'Advanced: 802.1X Behavior' with a downward arrow. It contains the text 'The following settings do not normally need adjusted.' and a setting for 'Validate Server Certificate:' with a dropdown menu set to '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 XpressConnect 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 ES configuration. See [Configuring the Chrome Extension](#) to configure the XpressConnect 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** ONC + User Extension ▼

+ **ONC Install Instructions:**

<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 the owner.</div><a id='chromeUnmanagedButton' class='cpx-

Extension Messages

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

+ **Extension Install Instructions:**

<div id='chromeManagedDiv' style='display: none;'><div class='cpx-wizard-configure-image'></div><div class='cpx-wizard-download-button'><span

+ **Completed Message:**

<div class='cpx-pageChromeOsExtensionDone-title'>The certificate has been installed.</div><div class='cpx-pageChromeOsExtensionDone-note'>The certificate is installed and ready

ONC Messages

The options below control the messaging for Chrome users.

+ **App ID To Notify:**

+ **Existing Certificates:** 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 the Enrollment System 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 (*XpressConnect 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 the Enrollment System.

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 ES 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

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 1
Step 3:	In the Chrome management console, navigate to Device Management -> Network -> Certificates . Add the CA certificate(s) downloaded above.
Step 4:	<p>Navigate to Device Management -> Network -> Wi-Fi and click Add Wi-Fi.</p> <p>Create the 'Anna-Secure' wireless network.</p> <p>Check Automatically Connect.</p> <p>Set Security Type to 'WPA/WPA2-Enterprise'.</p> <p>Set Extensible Authentication Protocol to 'EAP-TLS'.</p> <p>Set Username to '@anna37.company.com' or the desired value.</p> <p>Set Server Certificate Authority to 'Anna Test Root CA 1'.</p> <p>Set Client Enrollment URL to 'https://anna37.cloudpath.net/enroll/AnnaTest/Production/'.</p> <p>Set Issuer Common Name to 'Anna Test Intermediate CA 1'.</p> <p>Set Issuer Organization to 'Sample Company, Inc.'.</p> <p>Set Issuer Organization Unit to 'IT'.</p>
Step 5:	<p>Navigate to Device Management -> Chrome Management -> User Settings -> Manage force-installed apps.</p> <p>Search for ID cbbhclfnbkdbognejfoajgfoioefeb (XpressConnect Certificate Generator) and add it to the force-install list.</p> <p>(If you need the beta version, the ID is dnnhnbjpkkgdnnfdllepjhnabjcbjpn (XpressConnect Certificate Generator - Beta).</p>
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.

Configuring the Chrome Extension

The Enrollment System 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 the Enrollment System, 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:

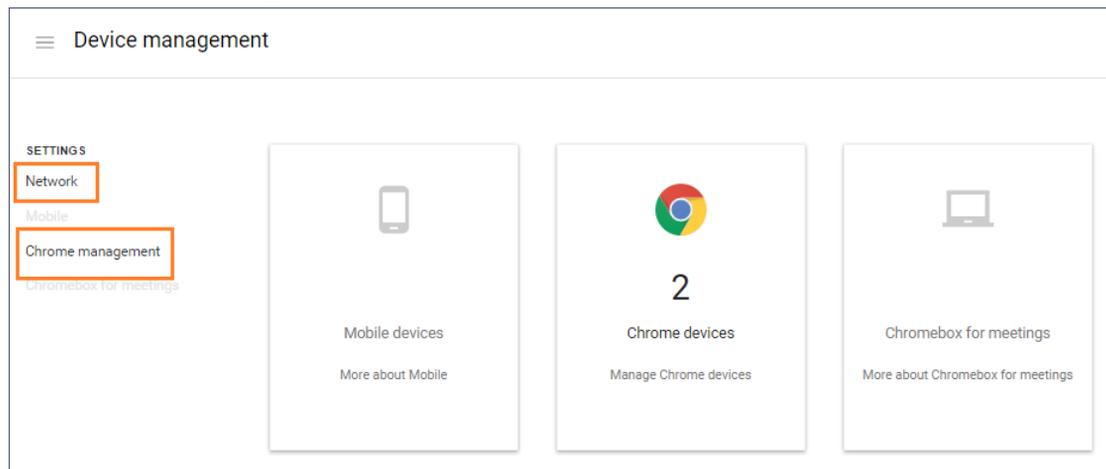
1. Log into the Chrome management console at <https://admin.google.com>.

FIGURE 4. Chrome Admin Console



2. Select *Device Management*.

FIGURE 5. Device Management

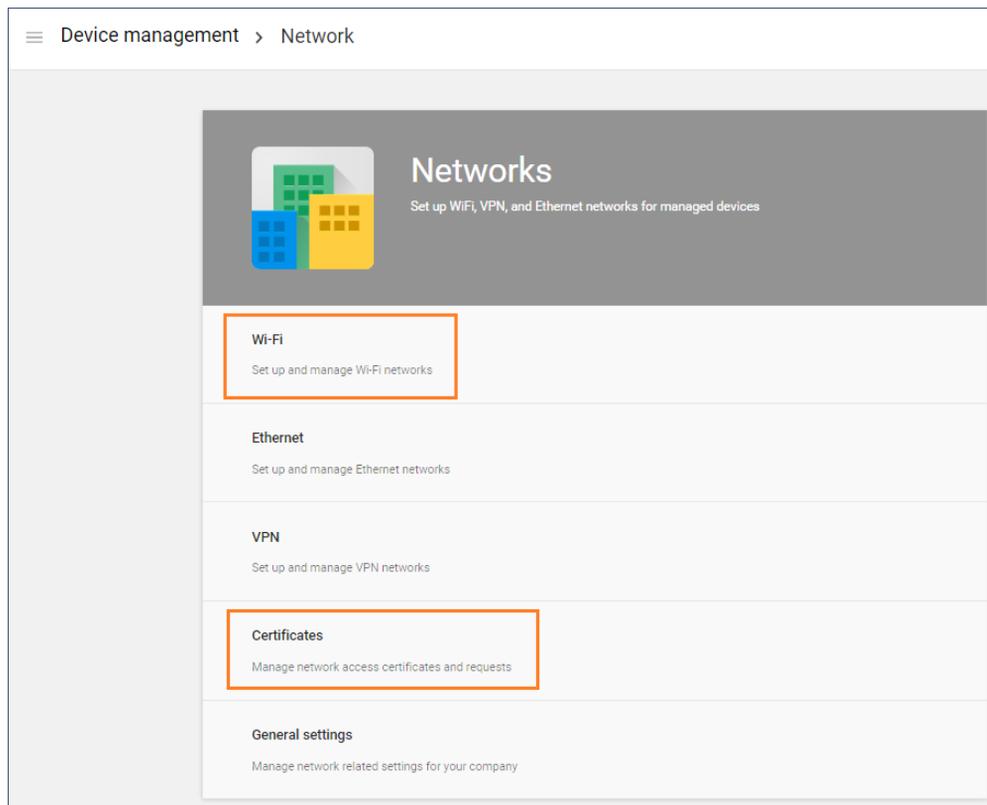


Use the *Network* link to set up *Wi-Fi* and *Certificates* for managed devices. Use the *Chrome management* link to set up *Wi-Fi* and *Certificates* for managed devices.

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.

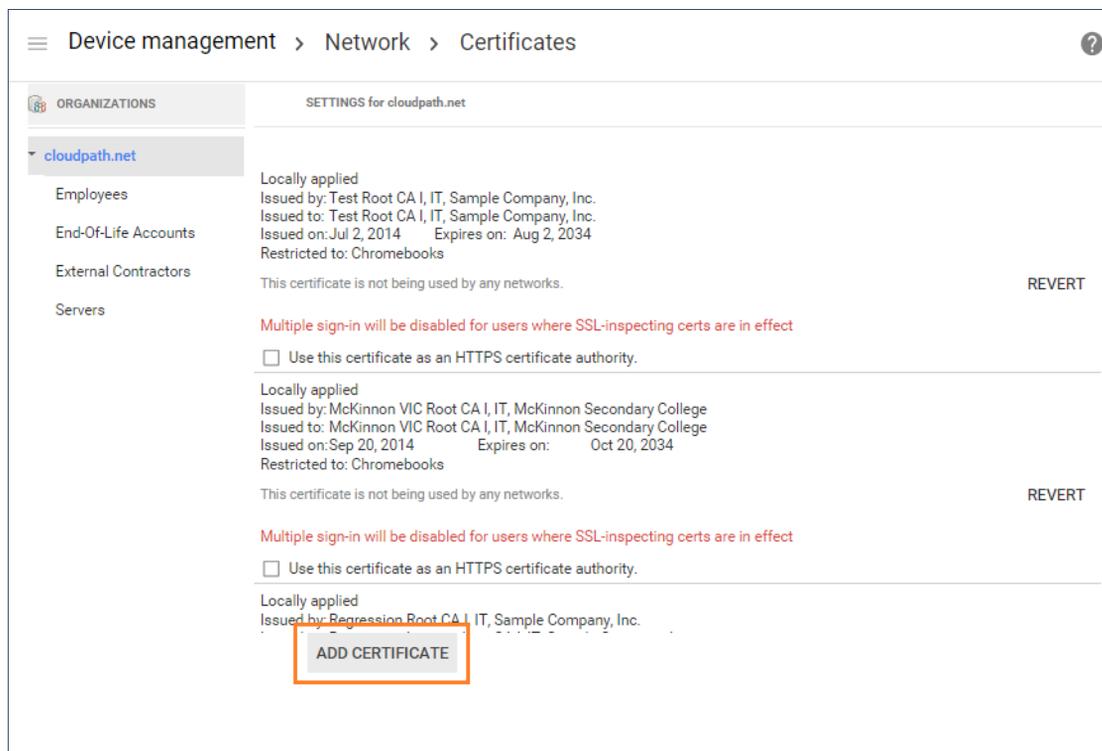
FIGURE 6. Network Settings



Import CA certificate

Click the *Networks > Certificates* link to import the CA 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 ES 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.

3. If your ES 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.

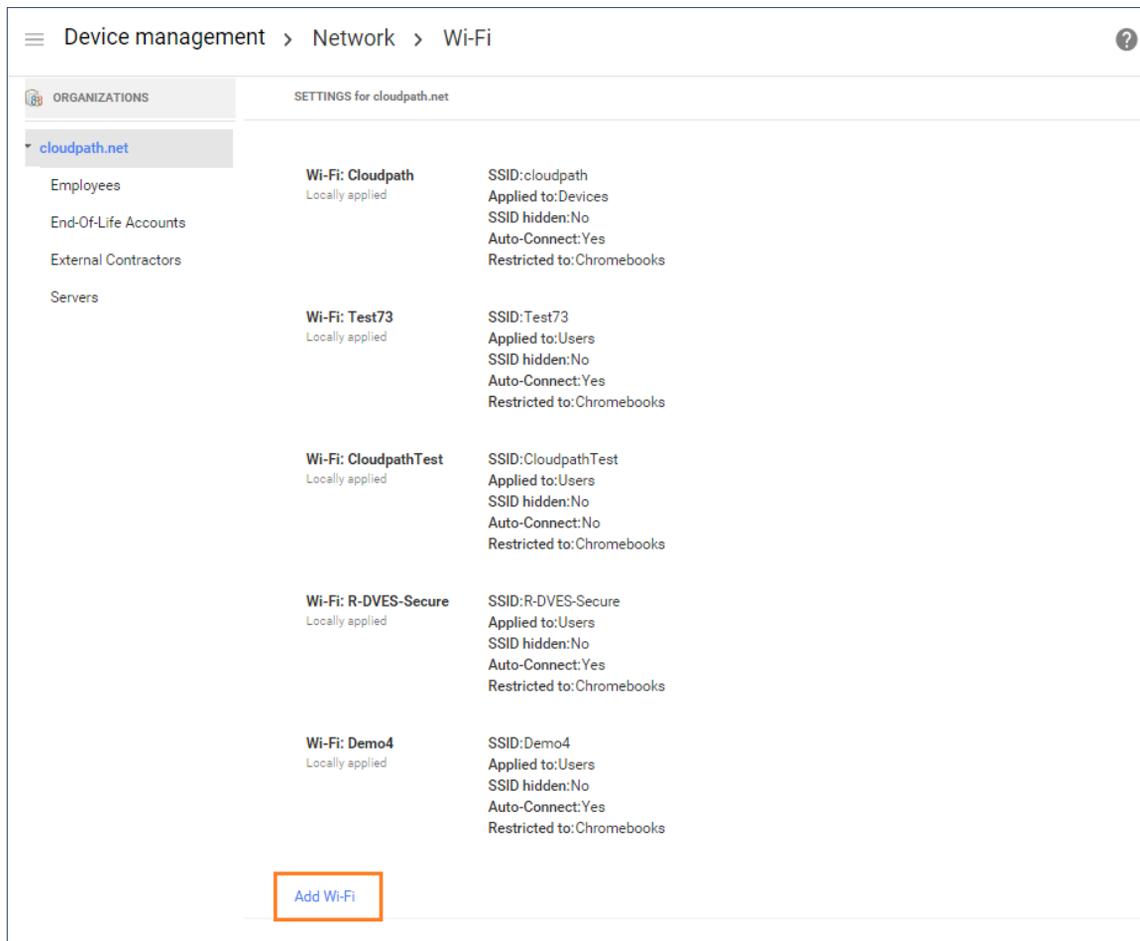
Configure Wi-Fi

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



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

FIGURE 9. Wi-Fi Settings

Add Wi-Fi network

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

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 ES 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

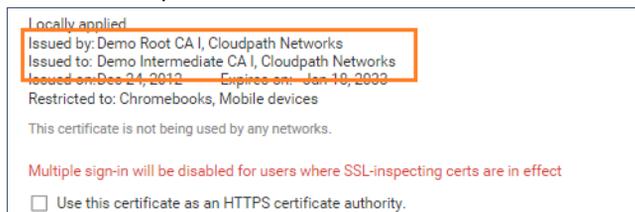


FIGURE 11. WiFi Setup Continued

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.

ADD **CANCEL**

- Enter the Client enrollment URL that is listed on the Chromebook setup instructions (see Managed Chromebook Setup Instructions). Typically, this value is
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.

Chrome Management User Settings

Configure policies for Chrome device users within an organizational unit. Configure the policy for the XpressConnect 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.

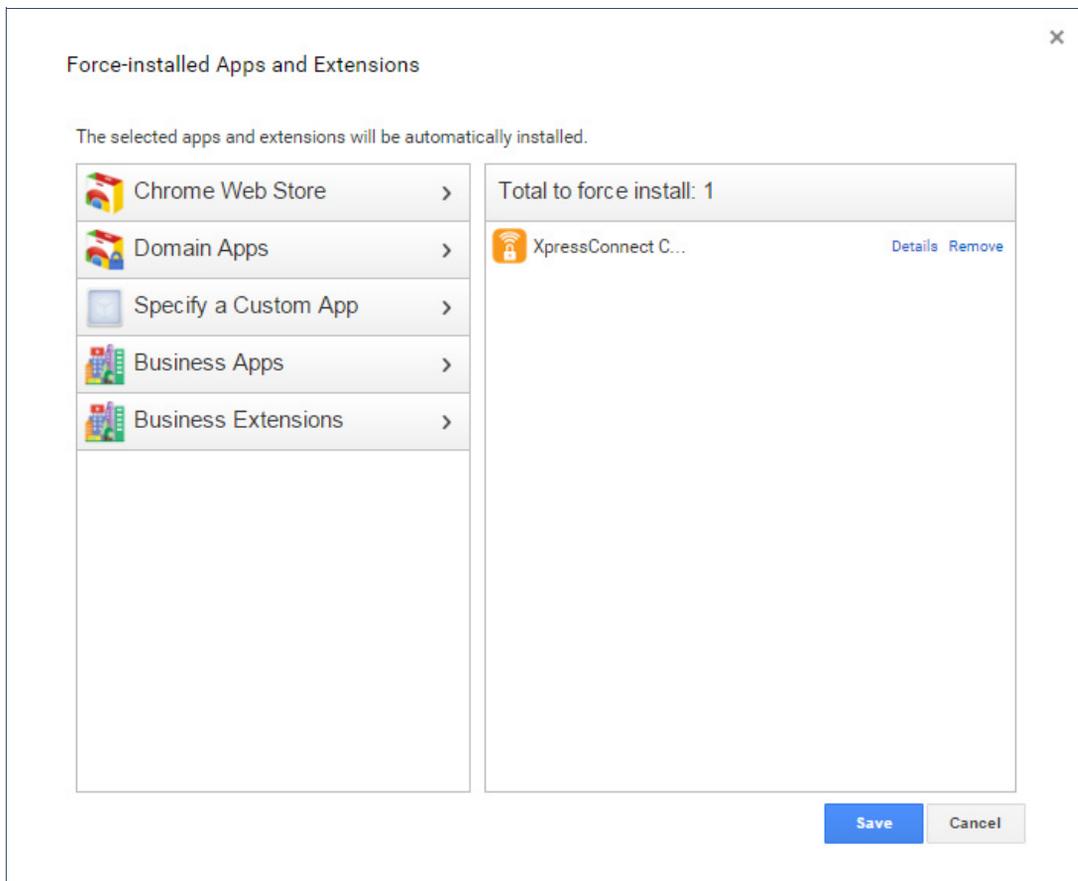
Configure *Force install apps* in *User* settings.

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

Note >>

Even if the Enrollment System 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 *XpressConnect Certificate Generator* and add to the force-install list.

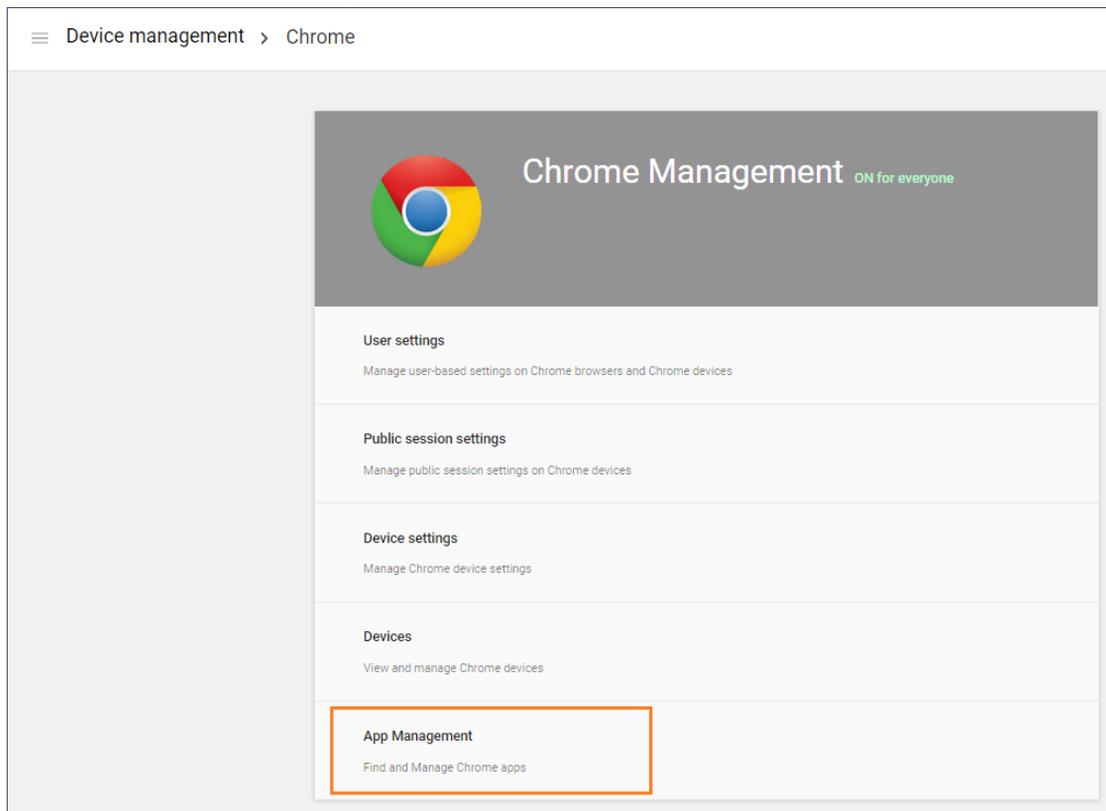
The extension is installed on the user device according to the Chrome OS user experience *Behavior* setting in the Enrollment System.

Force Install Unlisted (Beta) Apps

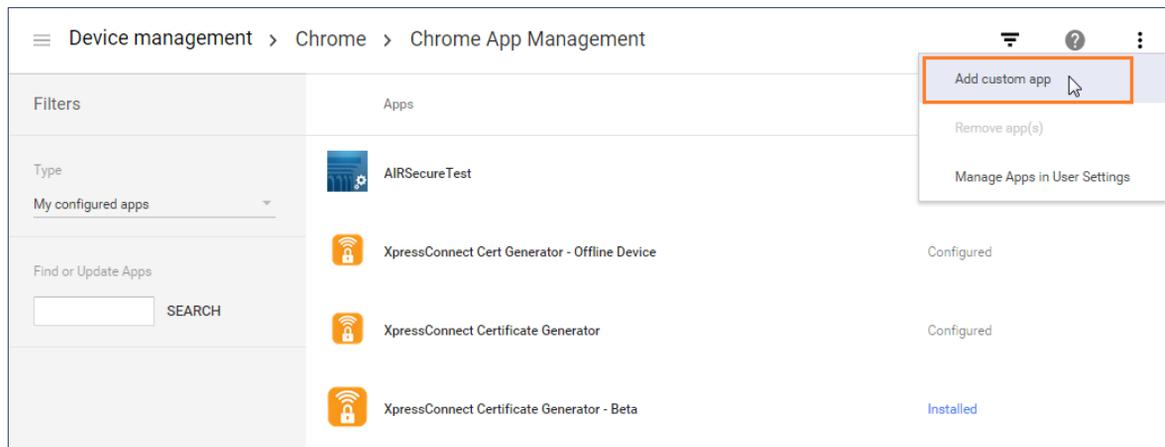
If your application is unlisted, you must load it as a custom application.

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

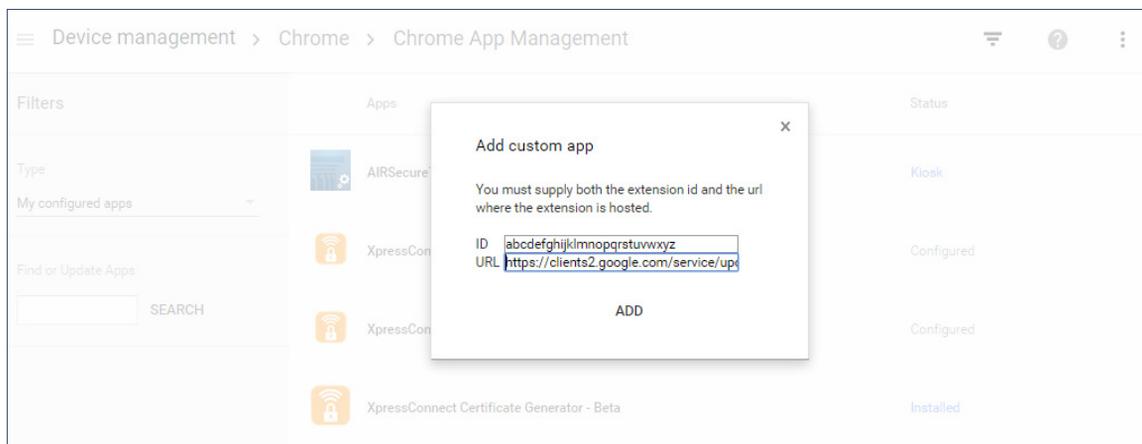
FIGURE 13. Chrome App Management



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

FIGURE 14. Add Custom App

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

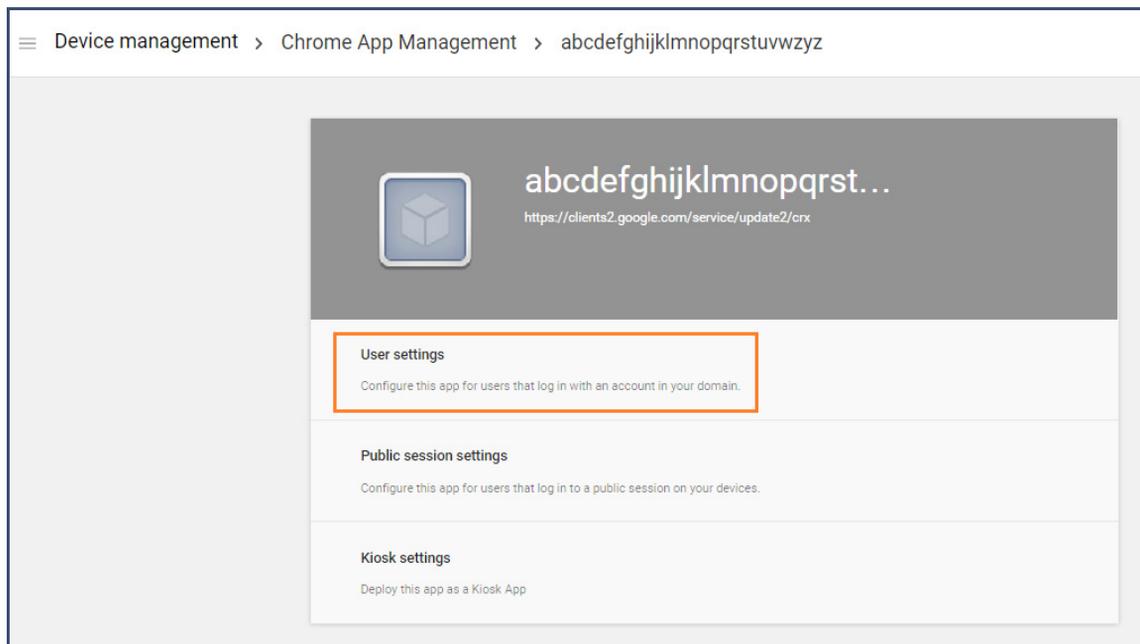
FIGURE 15. Custom App Parameters**Note >>**

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.

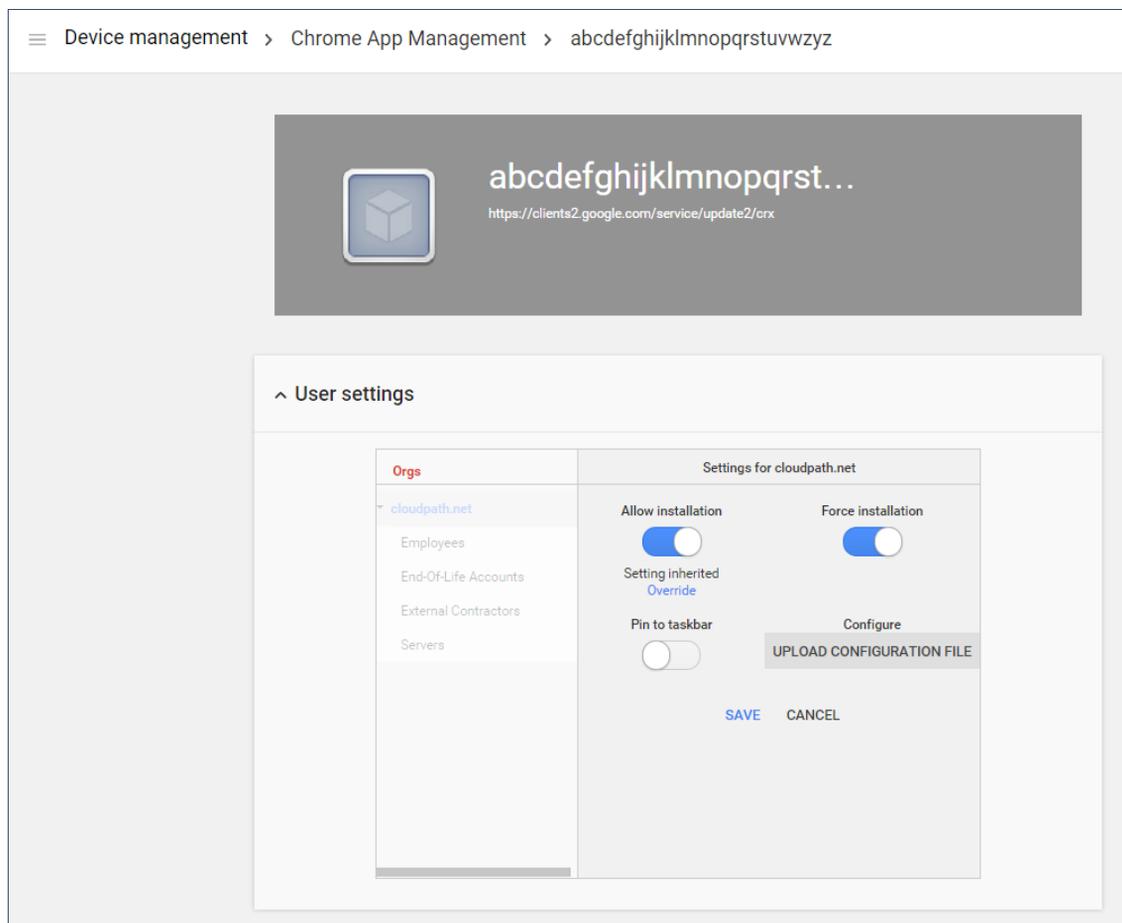
4. Select *User settings*.

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

The Enrollment System 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.

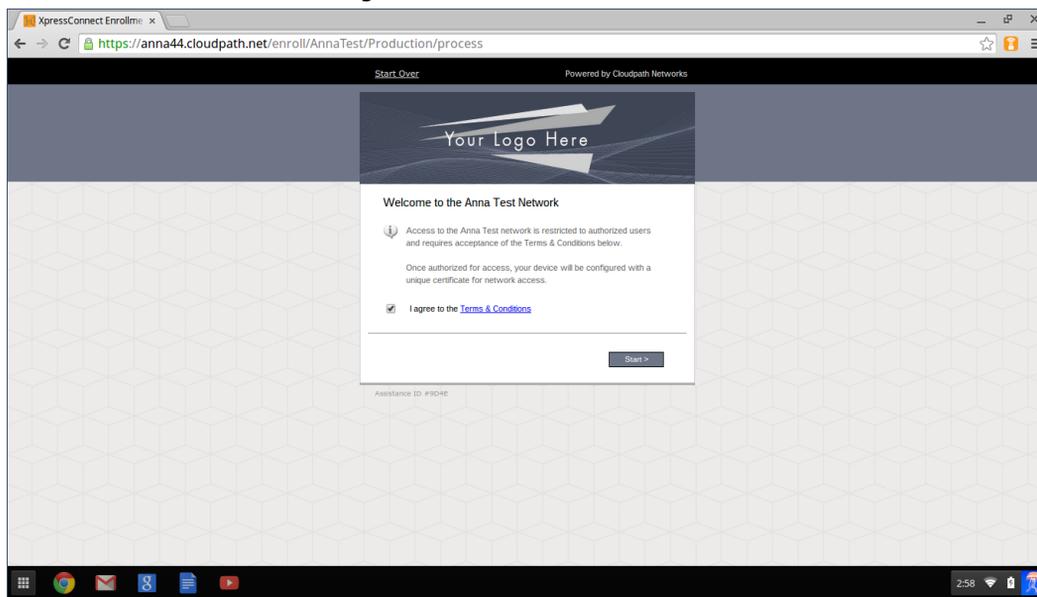
Enrollment Workflow

During enrollment, the Chrome OS is detected and the ES 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 ES *Welcome* screen displays.

FIGURE 18. Wizard Welcome Page

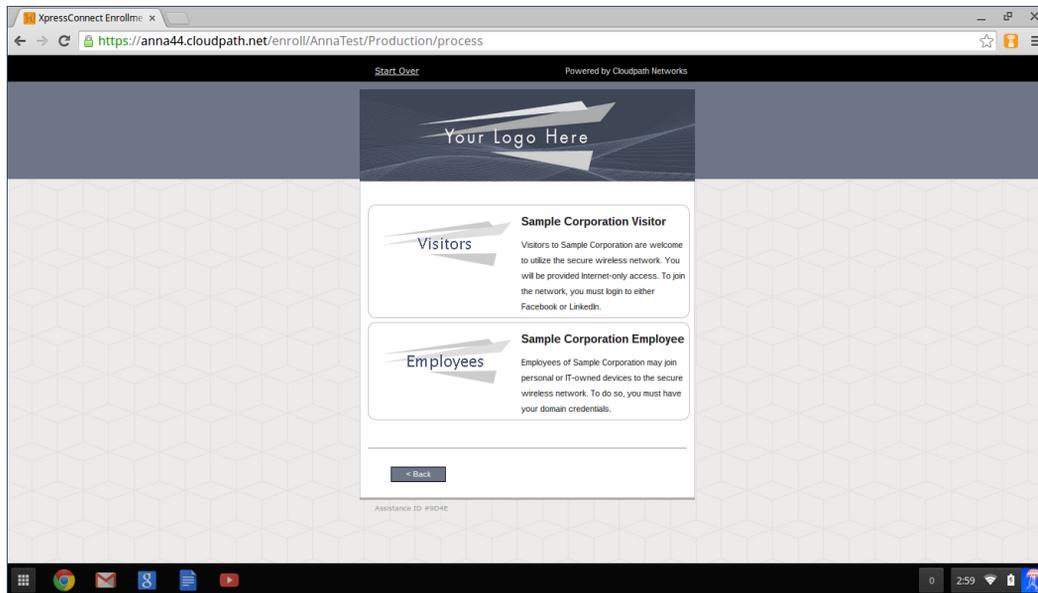


The login screen is typically customized with the logo, colors, and text for the organization or institution. The screens in this example use the default look and feel of the application.

User Type Prompt

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

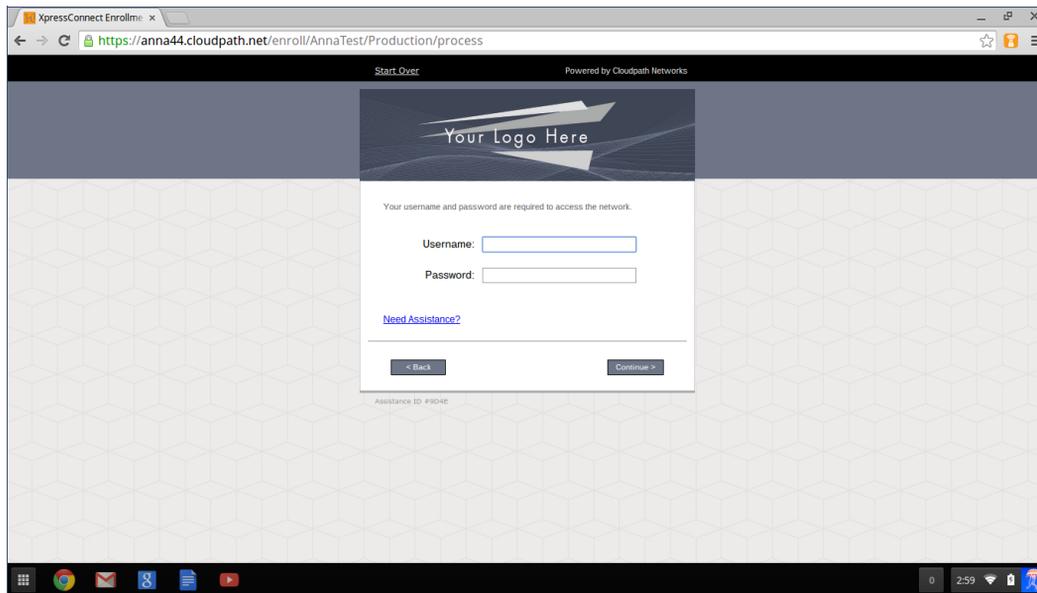
FIGURE 19. User Type Prompt



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.

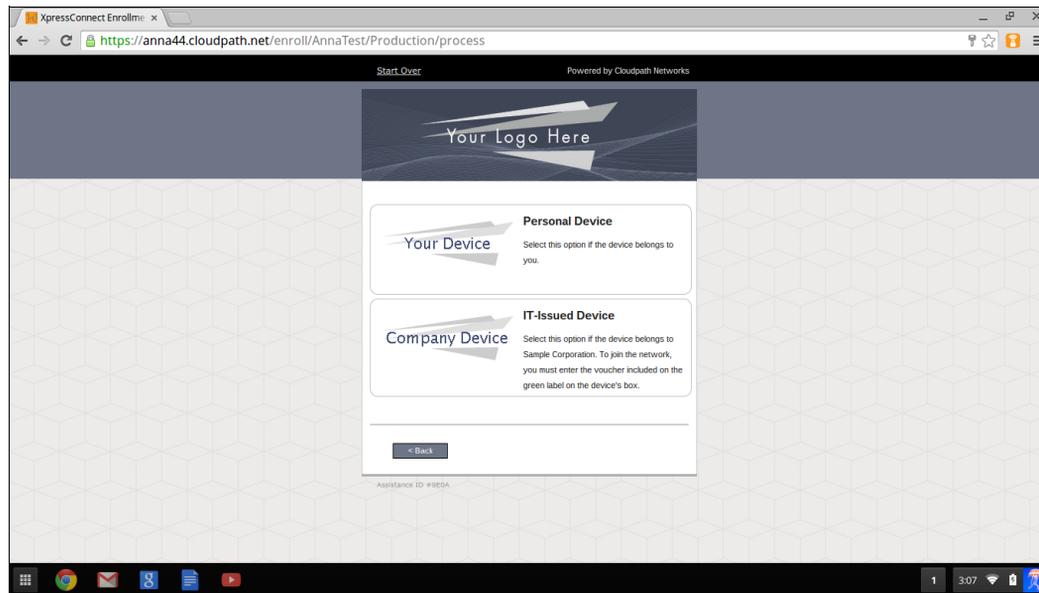
FIGURE 20. User Credentials



Device Type

If required by the network, the user might see a Device Type prompt. A device type prompt can provide 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 links to continue with the user experience example for your configuration.

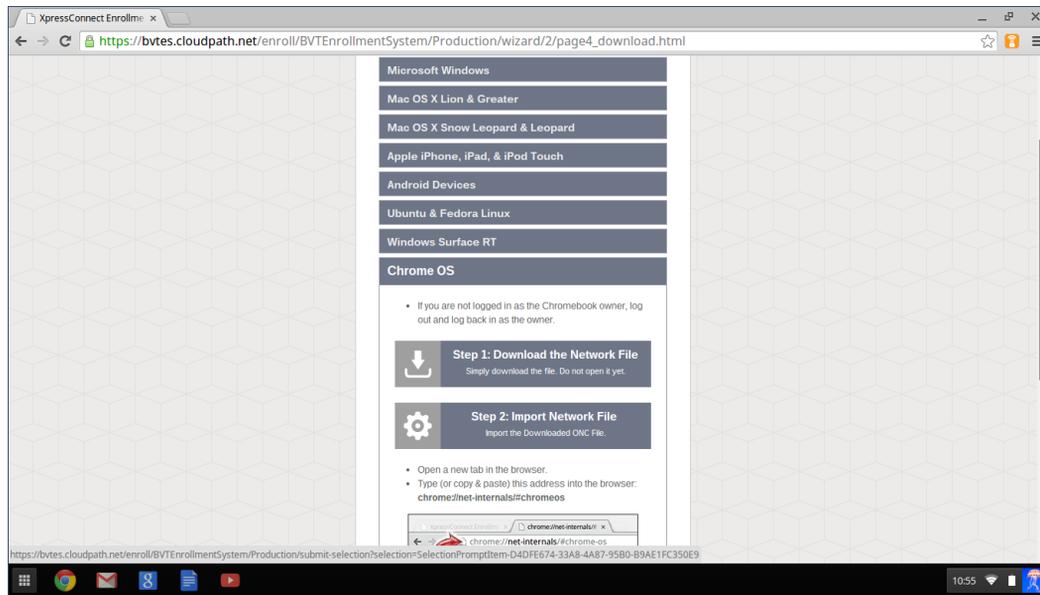
- Unmanaged Chromebook User Experience
- Managed Chromebooks With Extension User Experience

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.

FIGURE 22. Configuration Installation Instructions



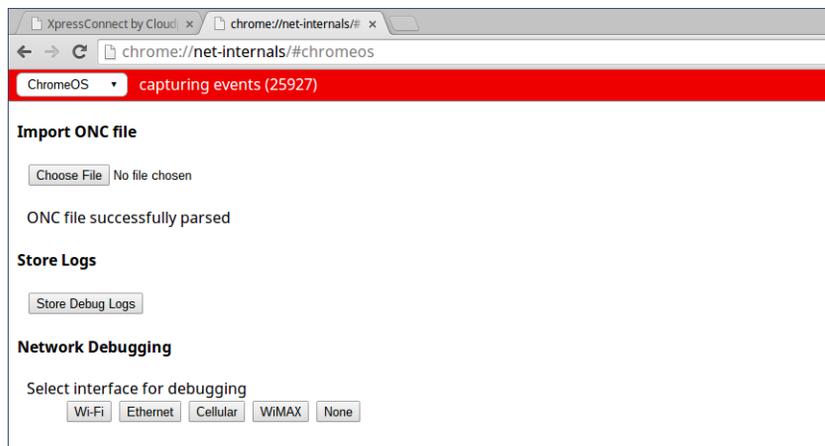
The manual download page shows the Chromebook instructions.

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.

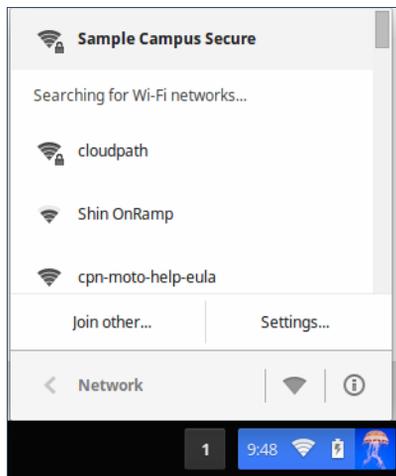
FIGURE 23. Import ONC File



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

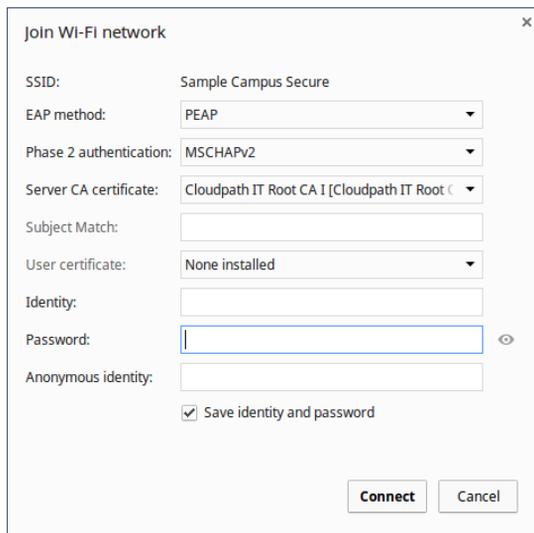
After the ONC file installed, click the *Wi-Fi* icon in the bottom right corner of your screen and select the secure network.

FIGURE 24. Select Wi-Fi Network



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

FIGURE 25. Enter User Credentials



The screenshot shows a dialog box titled "Join WI-Fi network" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- SSID: Sample Campus Secure
- EAP method: PEAP (dropdown menu)
- Phase 2 authentication: MSCHAPv2 (dropdown menu)
- Server CA certificate: Cloudpath IT Root CA I [Cloudpath IT Root C (dropdown menu)
- Subject Match: (empty text field)
- User certificate: None installed (dropdown menu)
- Identity: (empty text field)
- Password: (empty text field with a visibility toggle icon)
- Anonymous identity: (empty text field)
- Save identity and password
- Buttons: Connect and Cancel

The user should now be connected to the secure network.

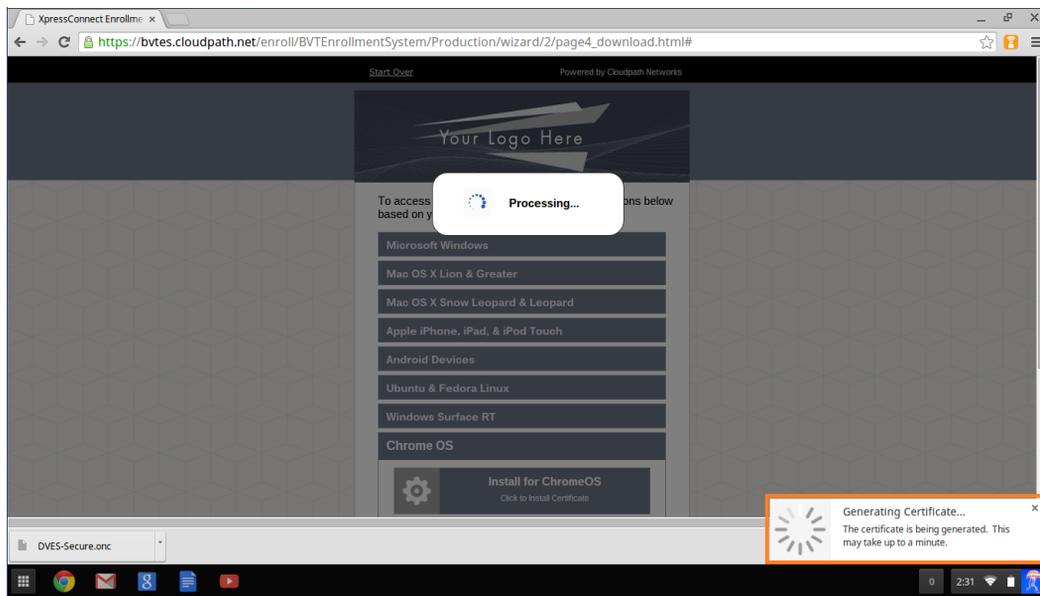
Managed Chromebooks With Extension User Experience

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

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

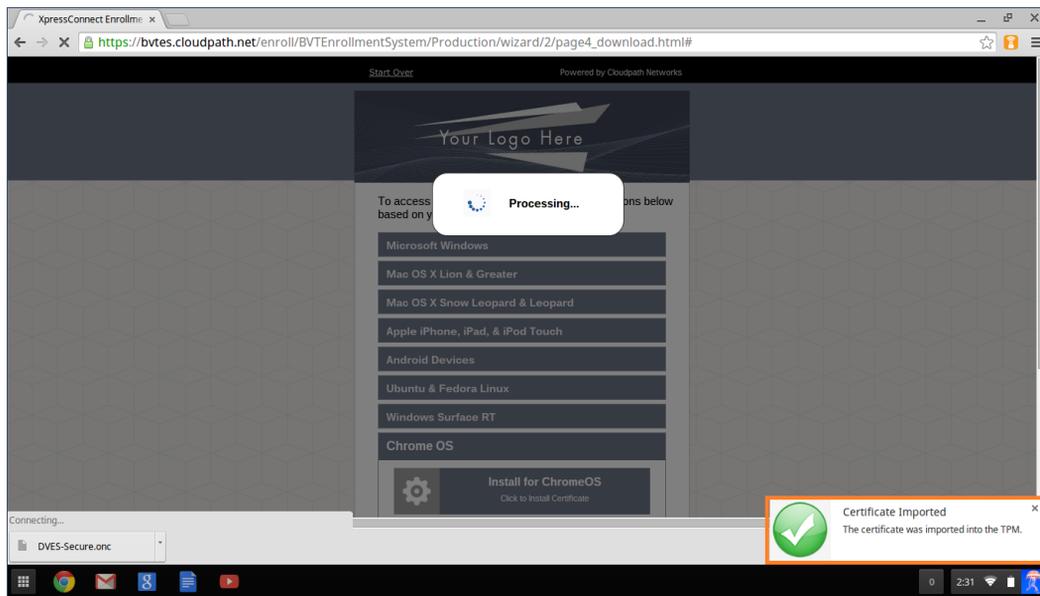
The extension generates the certificate.

FIGURE 26. Generating Certificate



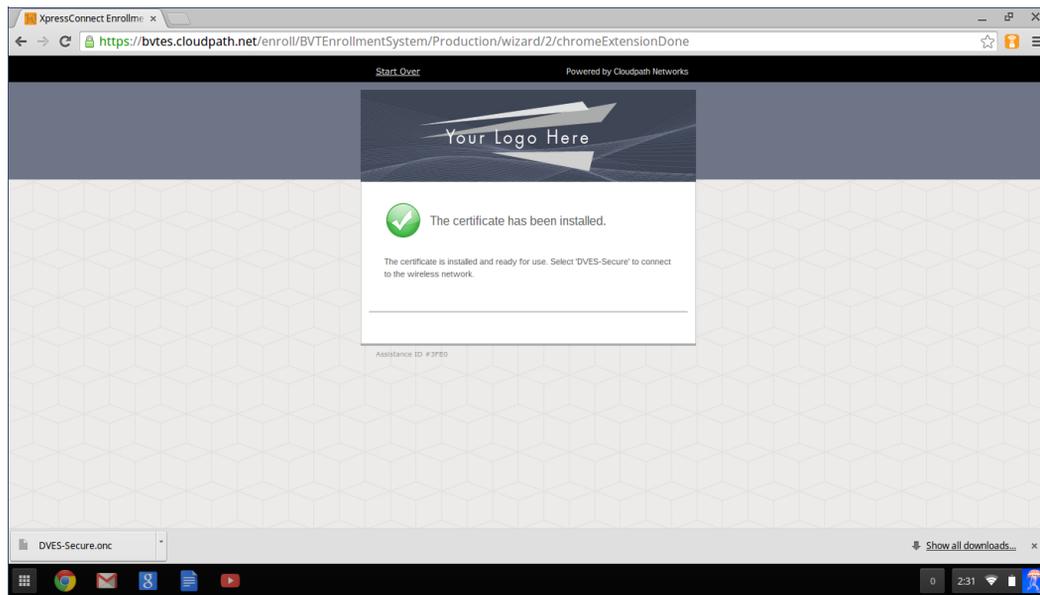
The extension imports the certificate into the TPM.

FIGURE 27. Certificate Imported



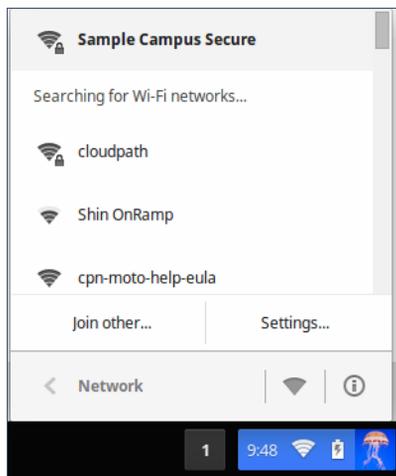
When the certificate installation is complete, a message displays indicating that the certificate is installed and ready for use.

FIGURE 28. Certificate Installed



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 XpressConnect 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 ES 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://dns - Displays the list of hostnames for which the browser will prefetch the DNS records.
- chrome://chrome-urls - View all the available chrome:// commands.

About Cloudpath

Cloudpath Networks, Inc. provides Automated Device Enablement (ADE) solutions that simplify the adoption of standards-based Wi-Fi security, including WPA2-Enterprise, 802.1X, and X.509, in diverse BYOD environments. Founded in 2006, Cloudpath Networks invented the modern onboarding model for personal devices and continues to drive the industry's adoption of standards-based security en masse. The Cloudpath XpressConnect solutions are proven worldwide to bring simplicity to secure networks through automated and easy-to-use form and function. To learn more, visit (www.cloudpath.net).

Contact Information

General Inquiries: info@cloudpath.net

Support: support@cloudpath.net

Sales: sales@cloudpath.net

Media: media@cloudpath.net

Marketing: marketing@cloudpath.net

Phone: +1 303.647.1495 (US)

+1 866.472.6053 (US)

+44 (01) 161.261.1400 (UK)

Fax: +1 760.462.4569

Address: 1120 W 122nd Ave, Suite 302

Westminster, CO 80234 USA