CONFIGURATION GUIDE

# Cloudpath Enrollment System Chromebook Configuration Guide, 5.11

## Supporting Cloudpath Software Release 5.11

*Part Number: 800-73235-001 Rev A*
*Publication Date: 16 September 2022*

# Copyright, Trademark and Proprietary Rights Information



## 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, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED 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



## Chromebook Basics

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 also differentiate the devices on your network by ownership, not just device type.

> **NOTE**
> For Chromebook enrollments, Cloudpath must use HTTPS.

## Supported Devices

Cloudpath supports all Chrome OS devices supported by Google. However, for verified access, Chrome OS version 50 or later is required.

## Two Types of Authentication for Chromebook Devices

This manual covers two types of authentication for Chromebook devices:

- Interactive Chromebook Authentication on page 19: This method requires a Chromebook device configuration and an enrollment workflow. 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 trusted platform module.

  > **NOTE**
  > Optionally, you can set up Chromebook verified access for this method of authentication.

- Non-Interactive Authentication for Chromebook Devices on page 27: This method does not require a separate device configuration or a workflow. It does, however, require Chromebook verified access, and the Chromebooks must be managed and use the Chromebook

extension. During enrollment, the extension automatically requests a certificate from Cloudpath and installs the certificate while displaying status notifications to the user.

**NOTE**
How to enable verified access is described in Enabling the Verified Access API on the Google Developer's Site on page 7.

For information about the user experience, refer to the *Cloudpath Enrollment System End-User Experience Guide For Supported Devices*.

# Enabling the Verified Access API on the Google Developer's Site

Verified access is required for the non-interactive authentication of Chromebook devices, but is an optional step if you are using a Chromebook device configuration within an enrollment workflow to onboard Chromebook devices.

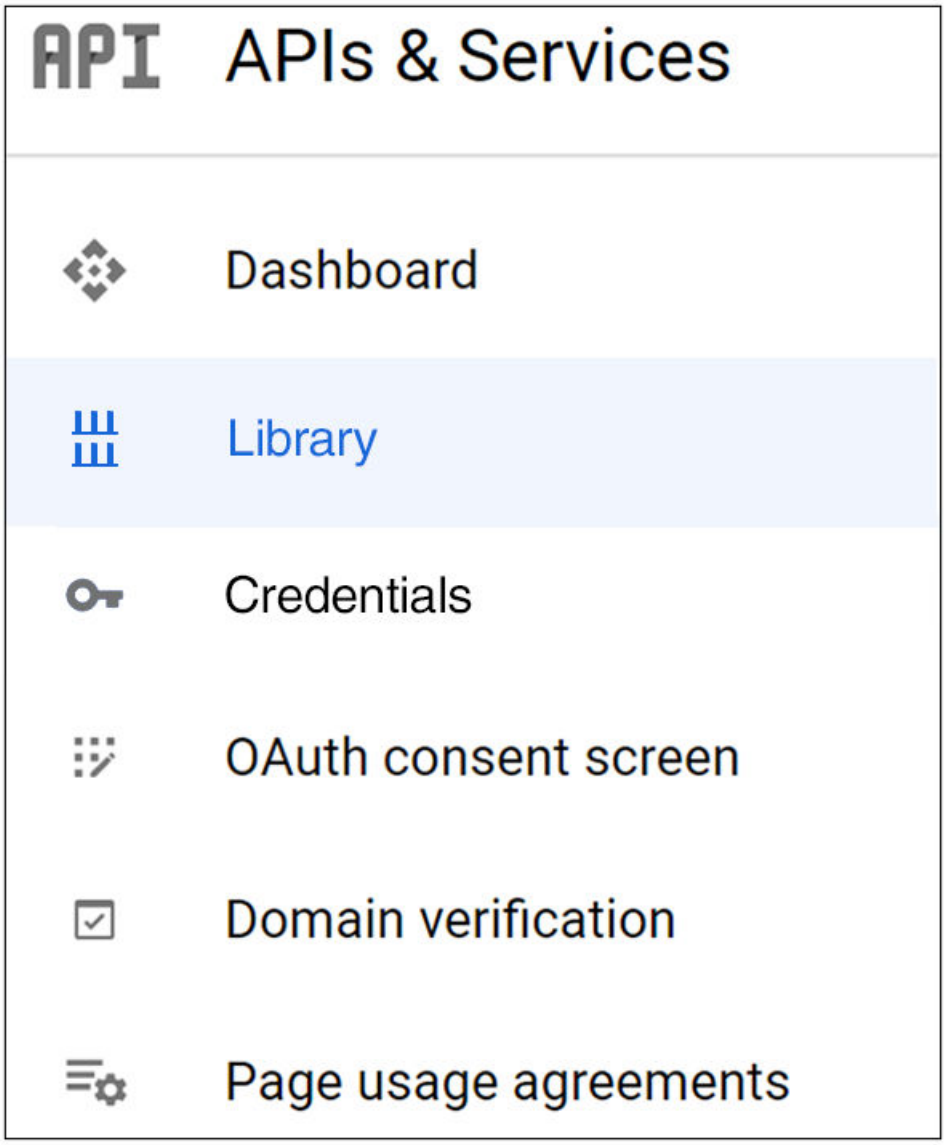
For this step, you need to have a Google developer's account and Google administrator account.

Follow these steps to enable the verified access API:

> **NOTE**
> You can also refer to Google developer's documentation for more information.

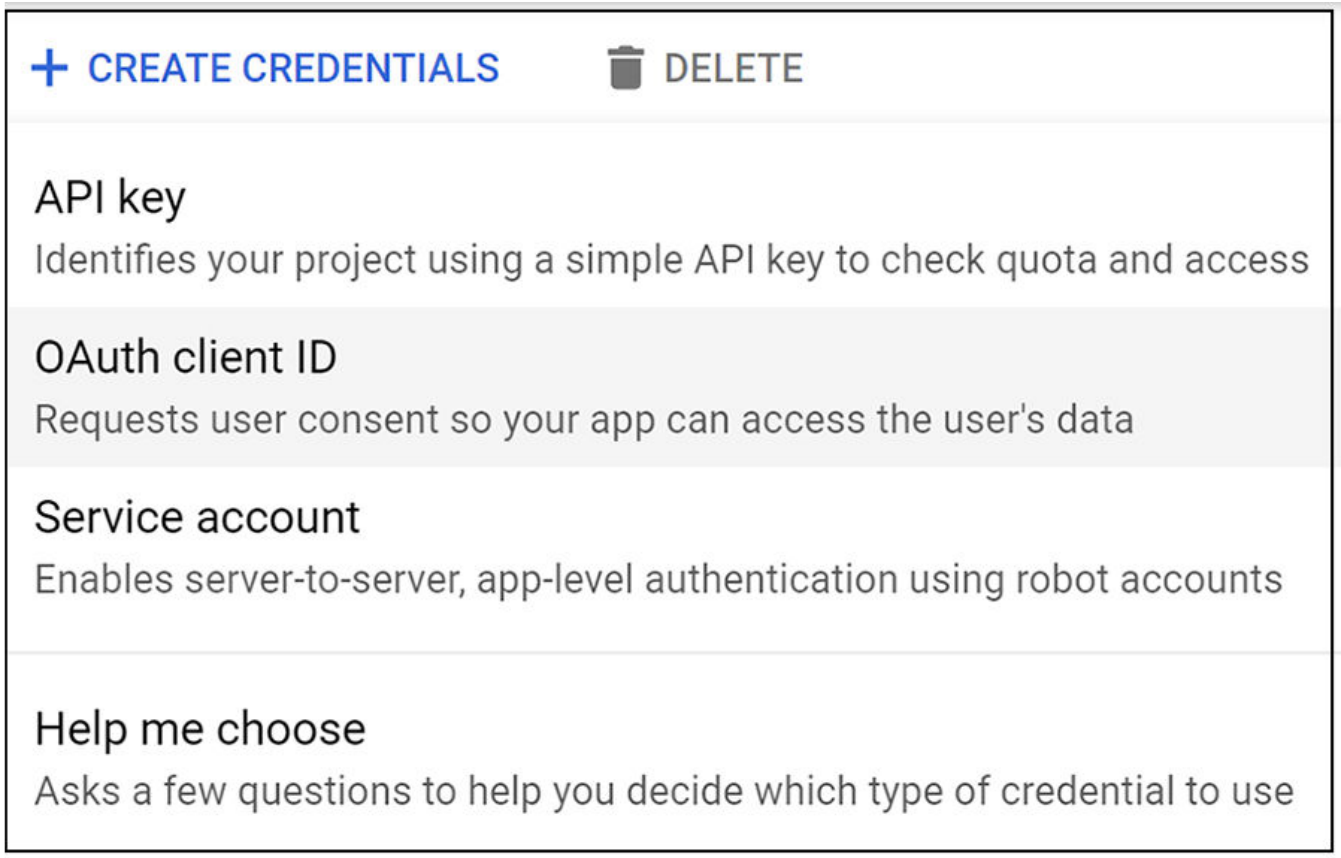
1. Log in to the Google developer's console.
2. Go to **APIs & Services > Library**.

**FIGURE 1** APIs & Services portion of Google Developer's Console



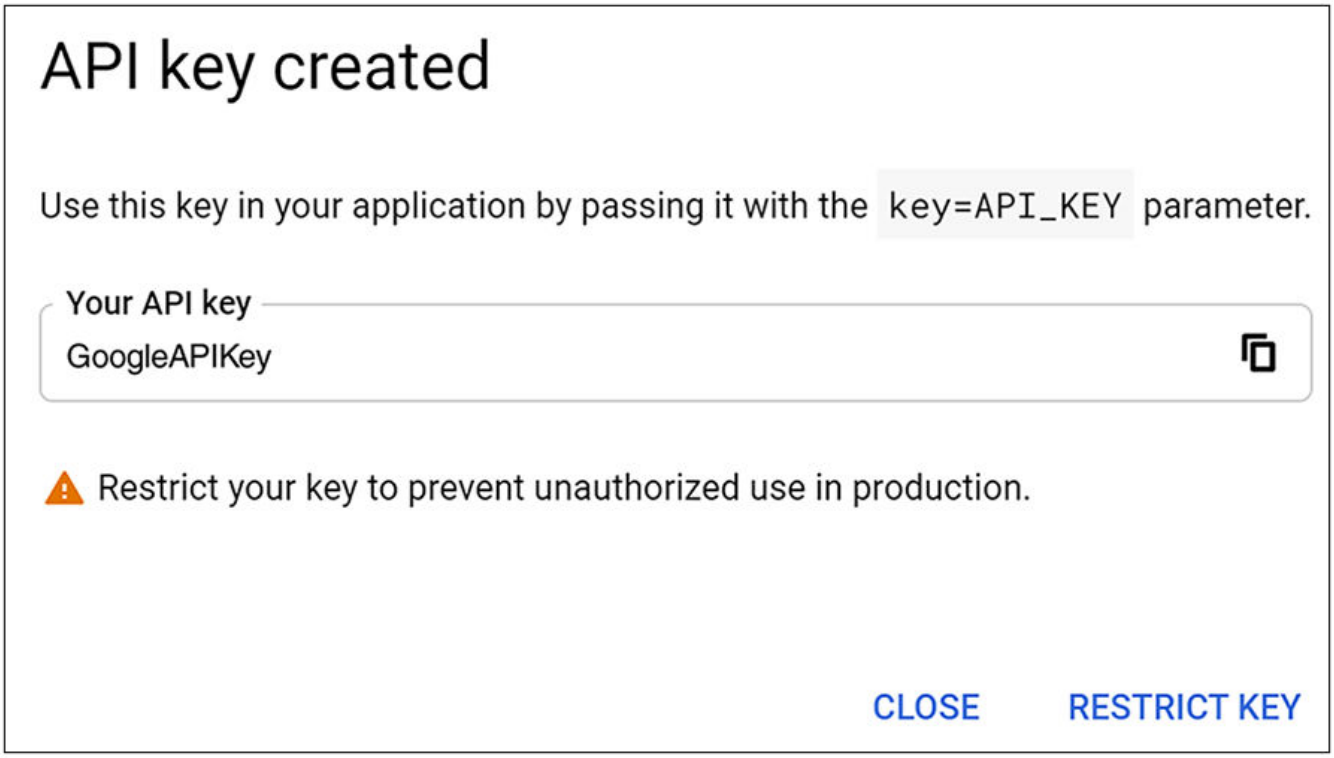

3. From the **APIs & Services > Library** area of the UI, search on "Chrome Verified Access API."
4. When the API appears, click on the name of the API, then click the **Enable** button.
5. Go to **APIs & Services > Credentials**.
6. At the top of the ensuing screen (see below), click **Create Credentials > API key**.

**FIGURE 2** Google Dev Console: APIs & Services > Credentials > Create Credentials




7. You are presented with a screen that shows the newly created API key. The value "GoogleAPIKey" in the screen below will be replaced with the actual key.

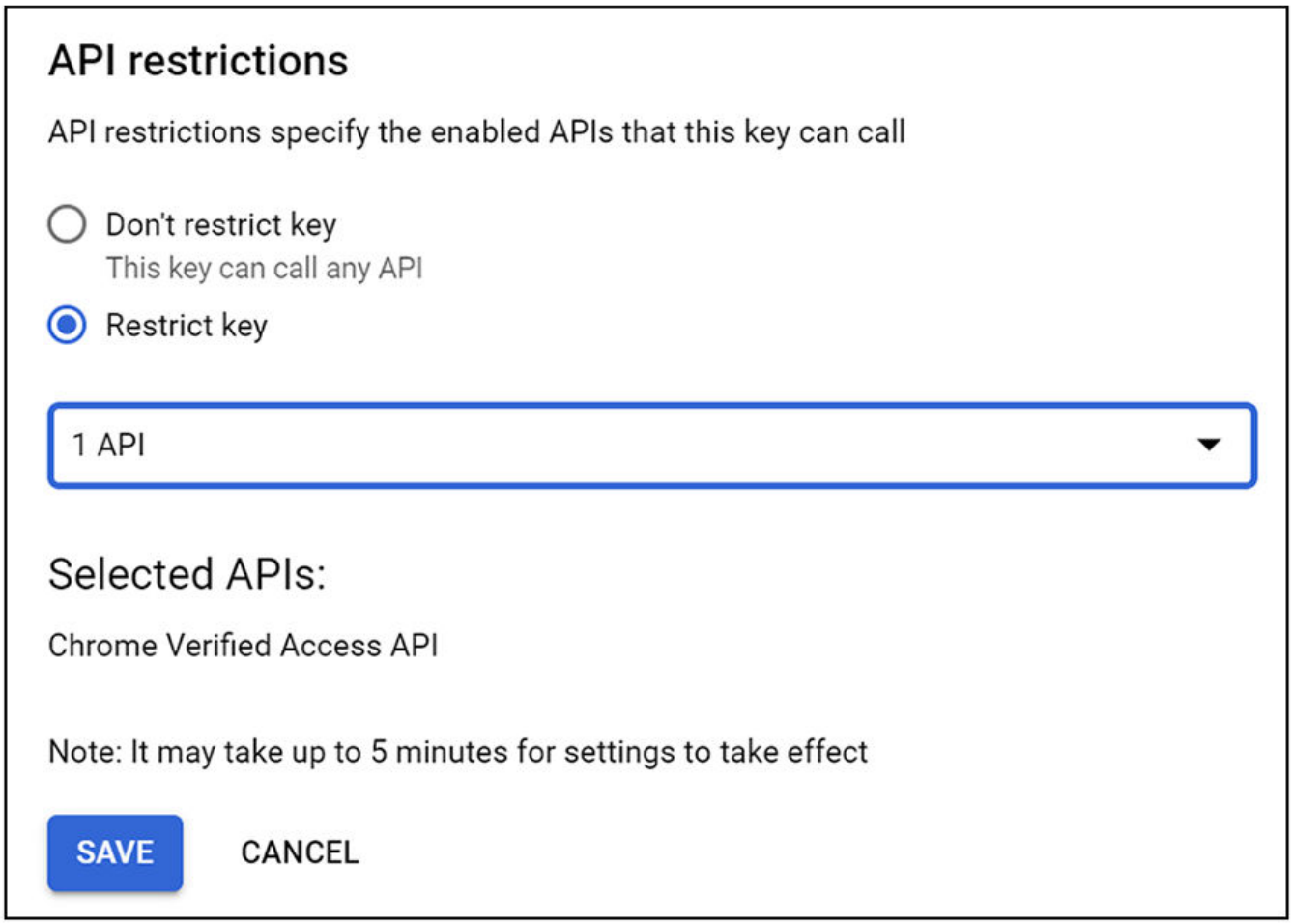
**FIGURE 3** API Key Created




**NOTE**
You will need the API key during Chromebook configuration in the Cloudpath UI.

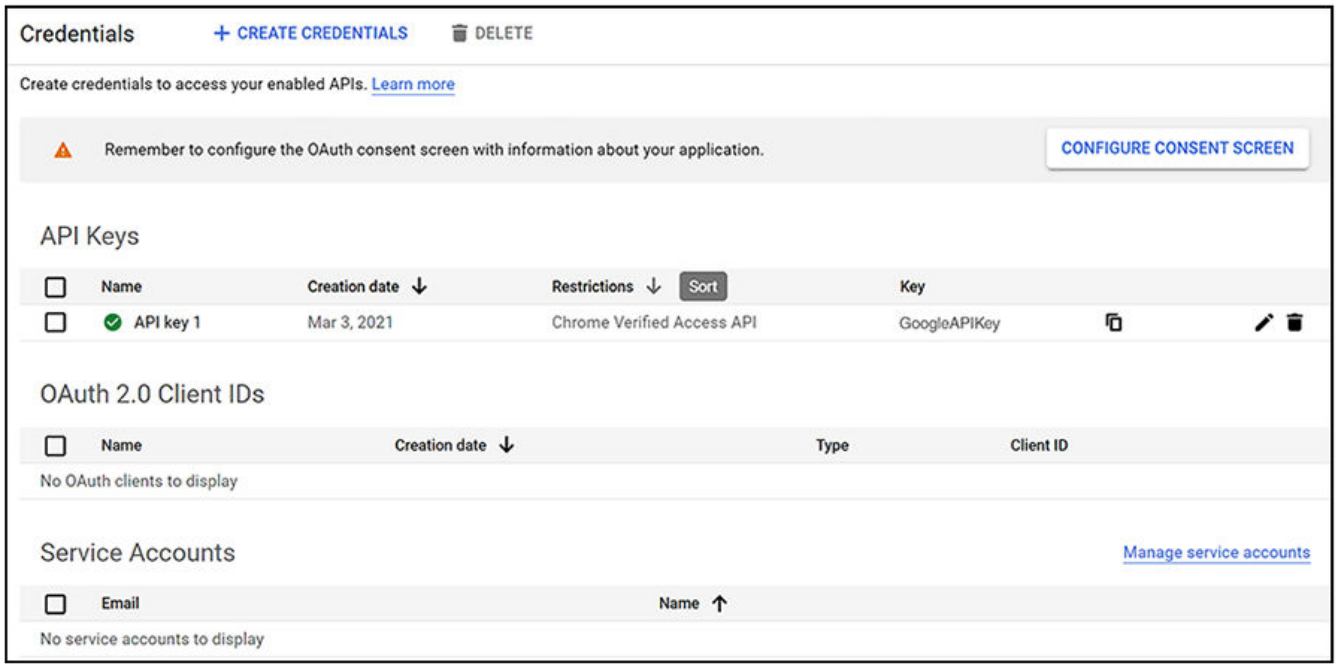
8. Click **RESTRICT KEY**.
9. On the ensuing screen, scroll to the bottom and do the following:
   a. Select the "Restrict key" radio button.
   b. From the drop-down list, select "Chrome Verified Access API."
   c. Click **Save**.

**FIGURE 4** Setting API Restrictions



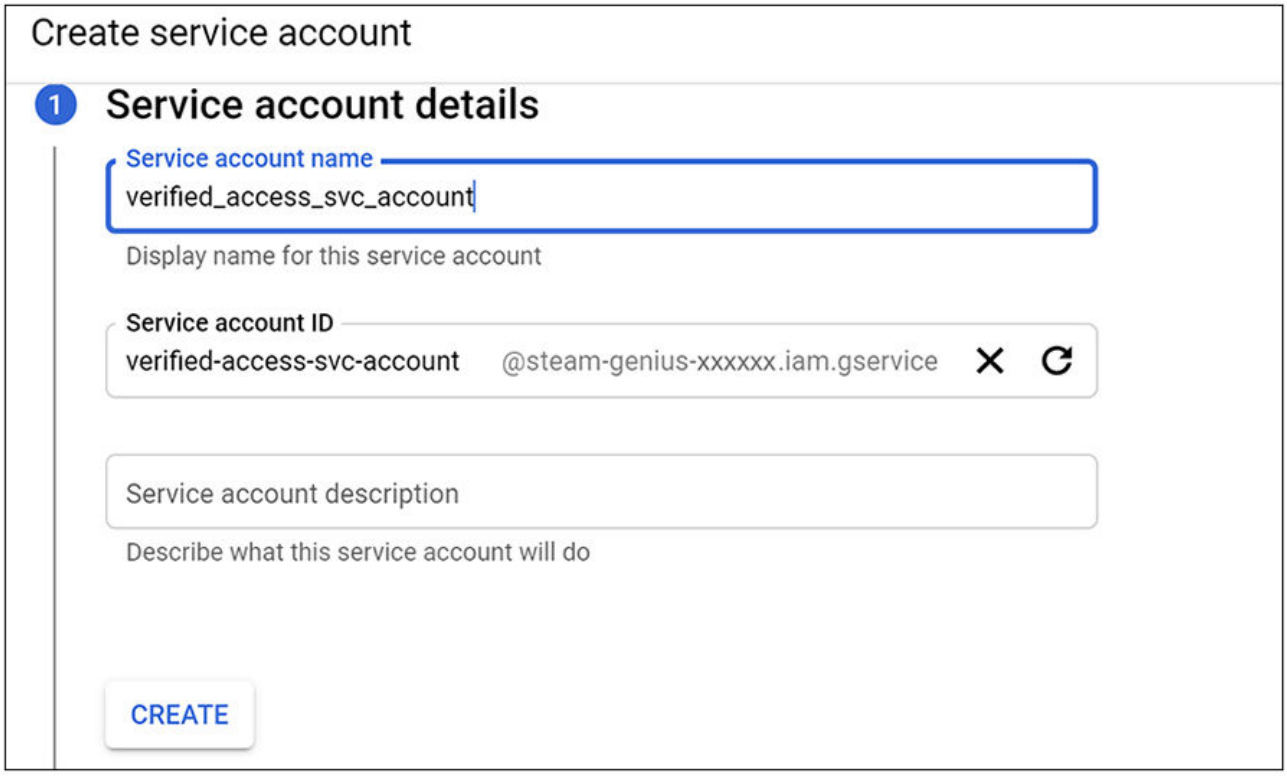

10. Check that the main Credentials Screen - with the API key and the restrictions you set - is now displayed:

**FIGURE 5** Main Credentials Screen: API Key and Restrictions




11. Create a service account by performing the following steps:
    a. Click "Manage service accounts" in the main Credentials screen.
    b. In the ensuing screen, click **+ CREATE SERVICE ACCOUNT**.
    c. In the Create Service Account screen, enter the credentials, then click **Create**.

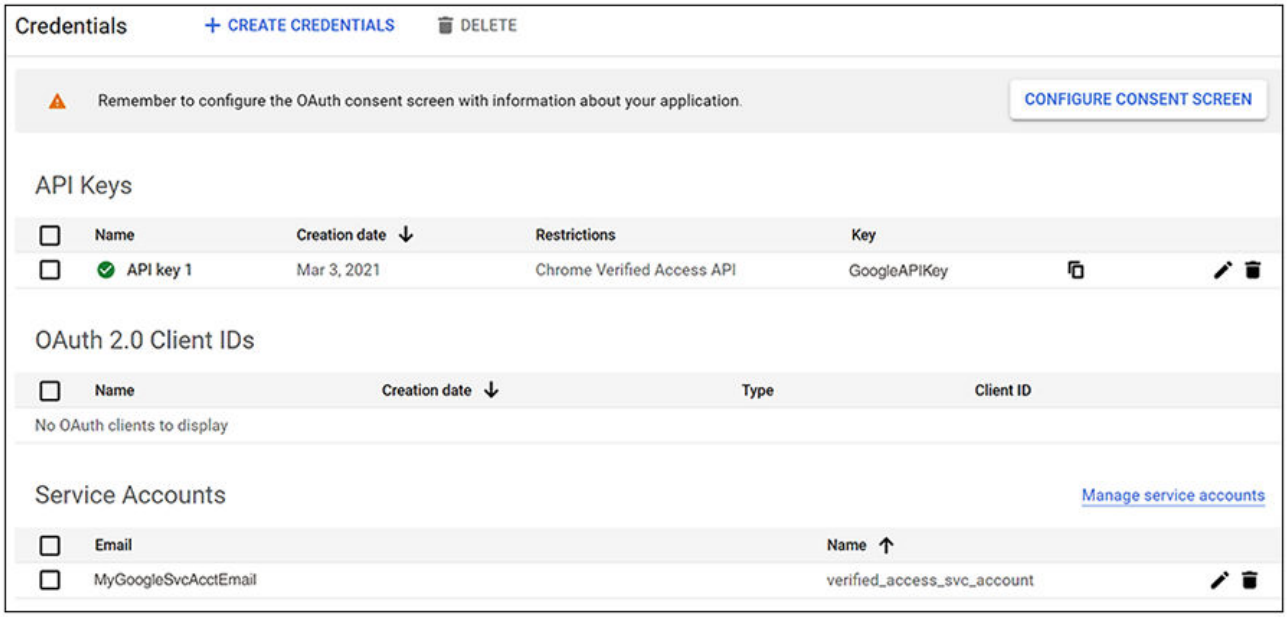
**FIGURE 6** Creating the Service Account




d. After you have created the service accound, click the **DONE** button.

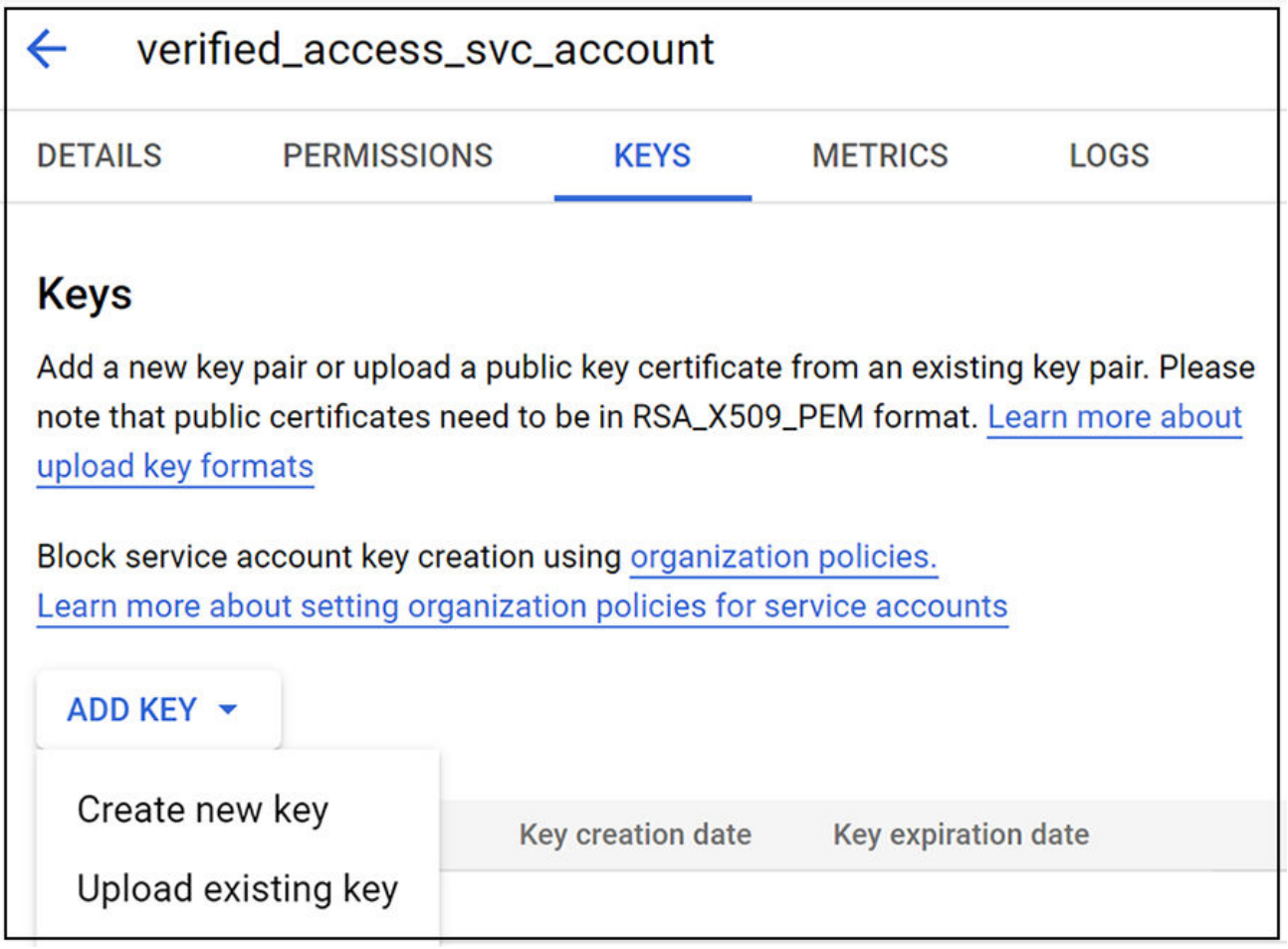
e. You can now go back to the main Credentials screen (**APIs & Services > Credentials**) to confirm that the service account has been added, such as in the example screen below.

**FIGURE 7** Credentials Screen After Service Account Has Been Created



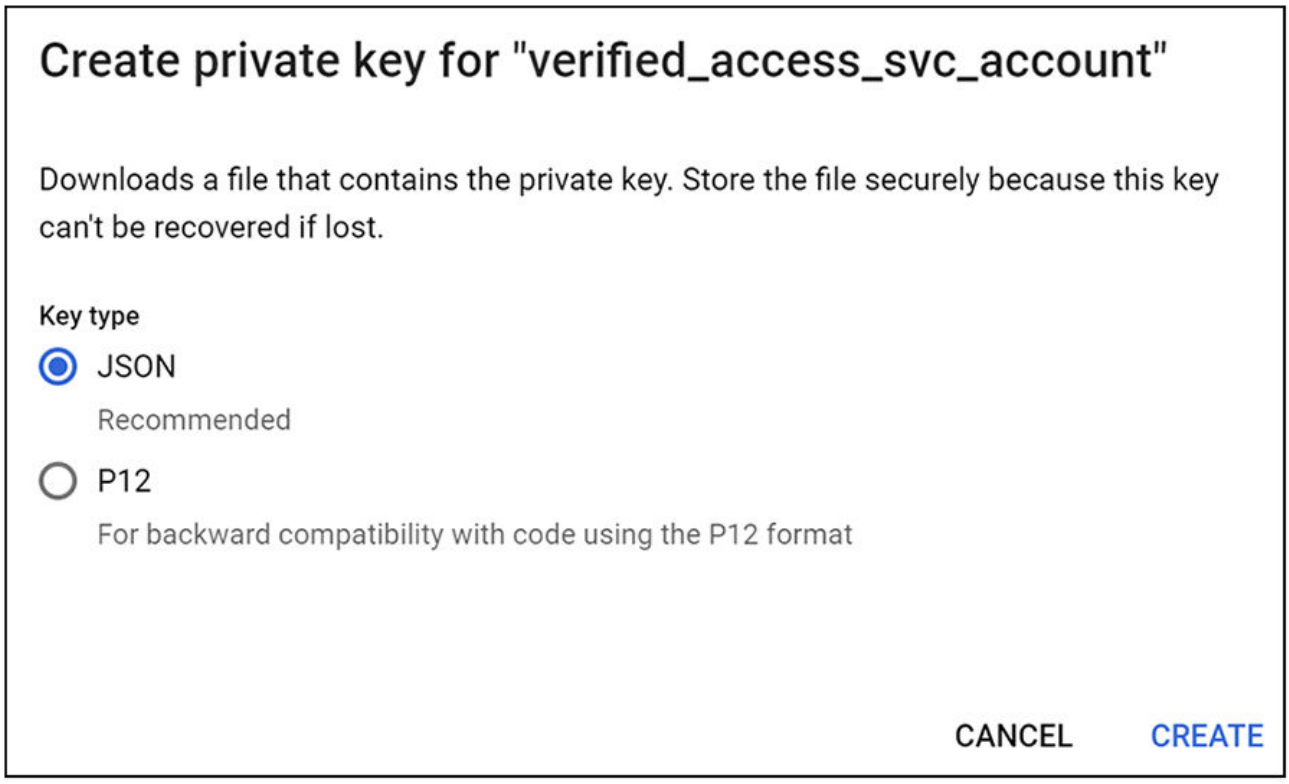

12. Create a JSON key for the service account by following these steps:
    a. Click on the service account email link (shown under "Service Accounts" in the preceding screen).
    b. In the ensuing screen, click **KEYS** near the top of the screen, then click the **ADD KEY** dropdown, then select "Create new key".

**FIGURE 8** Creating a New JSON Key for the Service Account




c. On the popup window (below), with JSON selected, click **Create**.

**FIGURE 9** JSON Popup Window to Create JSON Key




d. The private key is then created and saved. Be sure to take note where the private key gets saved on your computer because you will need this key in the Cloudpath UI.

**FIGURE 10** Private JSON Key Created and Saved

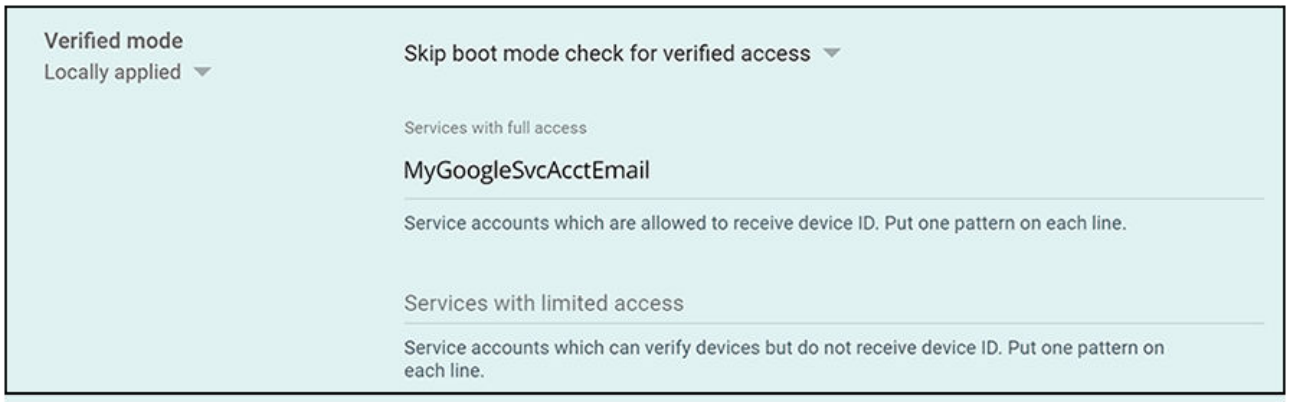

13. Now, log in to the Google **admin** console to perform steps related to user and browser or device settings:
    a. Go to **Devices > Chrome > Settings**.
    b. If performing a user enrollment, select the tab "USER & BROWSER SETTINGS"; if performing a device enrollment, select the tab "DEVICE SETTINGS".
    c. Set your options as desired.

d. Search for "Verified Mode" in the scroll list.

e. For the Verified Mode portion:

- Select the desired "Verified Mode boot check" type.
- For the "Services with full access" field, enter the service account email address that you created from the Google developer's console. (Note: If you selected the "USERS & BROWSER SETTINGS" tab, this field is called "Service accounts which are allowed to receive user data.")

**FIGURE 11** Verified Mode Settings on the Google Admin Console




f. Save your settings.

# Interactive Chromebook Authentication

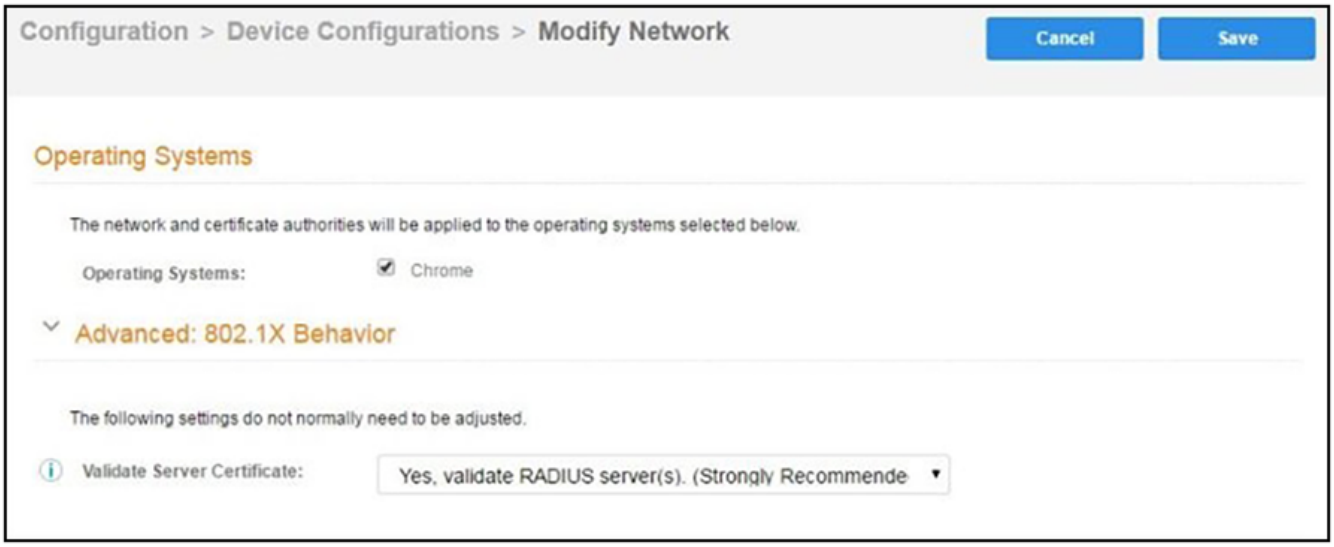


## Creating the Chromebook Device Configuration for a Workflow Enrollment

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 Cloudpath Admin UI, go to **Configuration** > **Device Configurations**.
2. Click **Add Device Configuration**.
3. You can use the defaults and continue clicking **Next** until you get to the OSes page.
4. On the OSes page, for the "Automatically Configured OSes," use the drop-down arrows to select "None" for all the OSes except Chrome. For the "Manually Configured OSes," you can un-check all the boxes.
5. Continue clicking **Next** until the device configuration is complete.
6. On the **OS Settings** tab, edit the **Chrome: Configuration from the Network(s) and Trust tabs** to enable the Chrome OS:

**FIGURE 12** Enabling Chrome OS




a) Select **Operating System: Chrome**.

b) Leave the default settings for **Validate Server Certificate**, and **Save**.

# Configuring Chromebook User Experience Settings

There are a variety of options you can set to determine the user experience, including two required settings if you are using Chromebook verified access.

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 Google Admin Console, installs the certificate and settings into the trusted platform module as the user or as the device.

  **NOTE**
  The Chrome extension uses the information provided by the Cloudpath configuration. See Configuring the Chrome Extension on Google Admin Console on page 25 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.

1. Go to **Configuration** > **Device Configurations**.
2. Select the **OS Settings** tab for the applicable device configuration.

3. Edit the **Chrome Settings: User experience** options. The settings that are available are shown in the following two screens.

**FIGURE 13** Chrome User Experience Settings: Screen 1 of 2

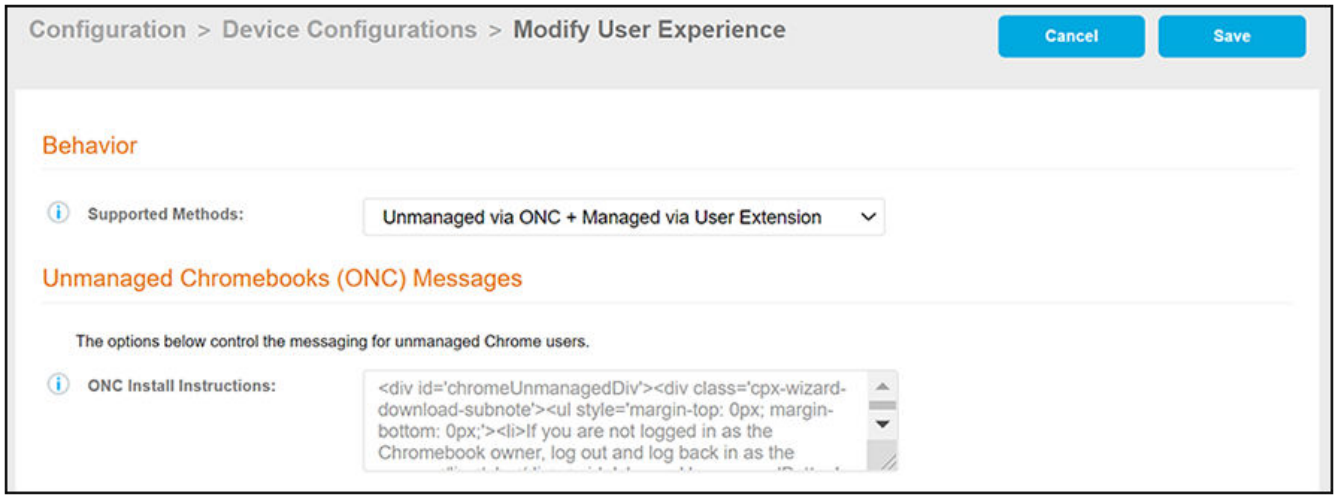
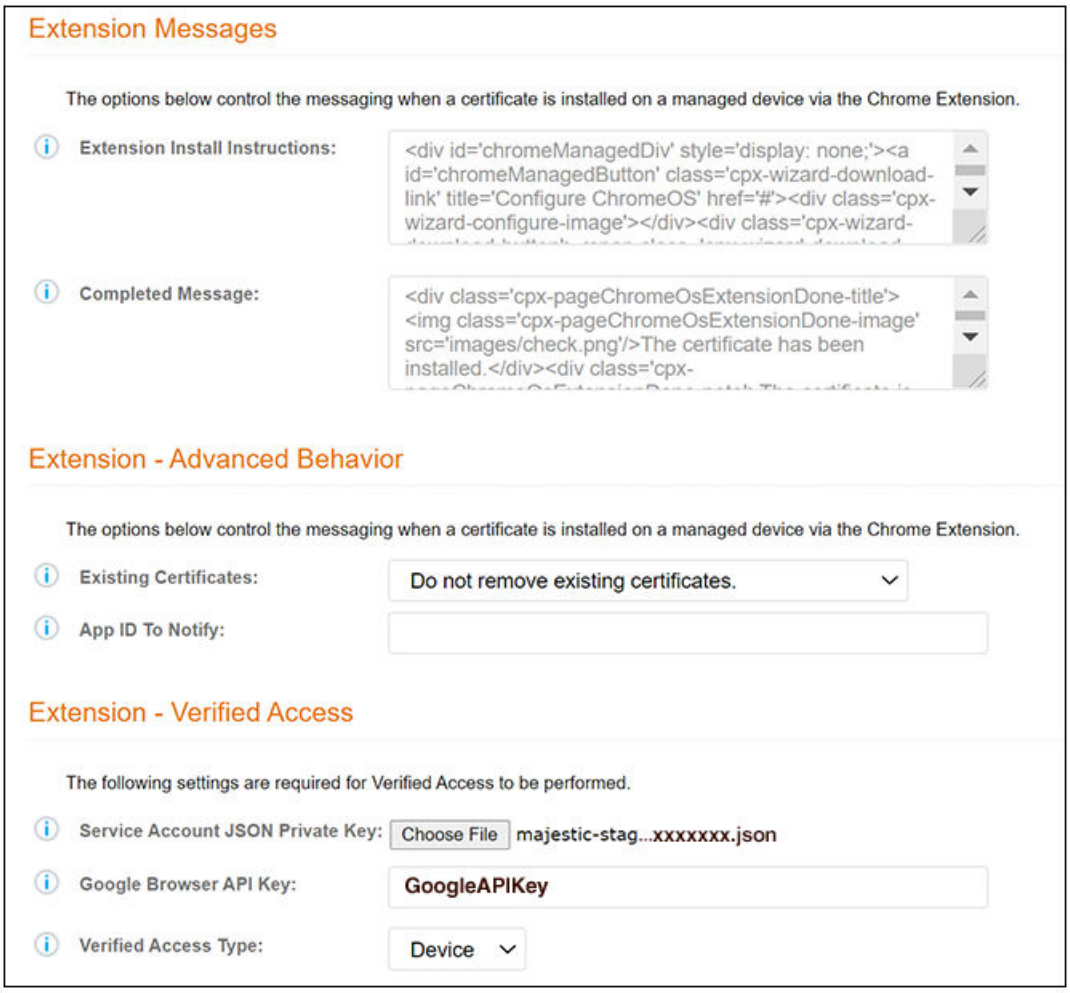


**FIGURE 14** Chrome User Experience Settings: Screen 2 of 2




4. Select the **Behavior** (Screen 1 above) 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.

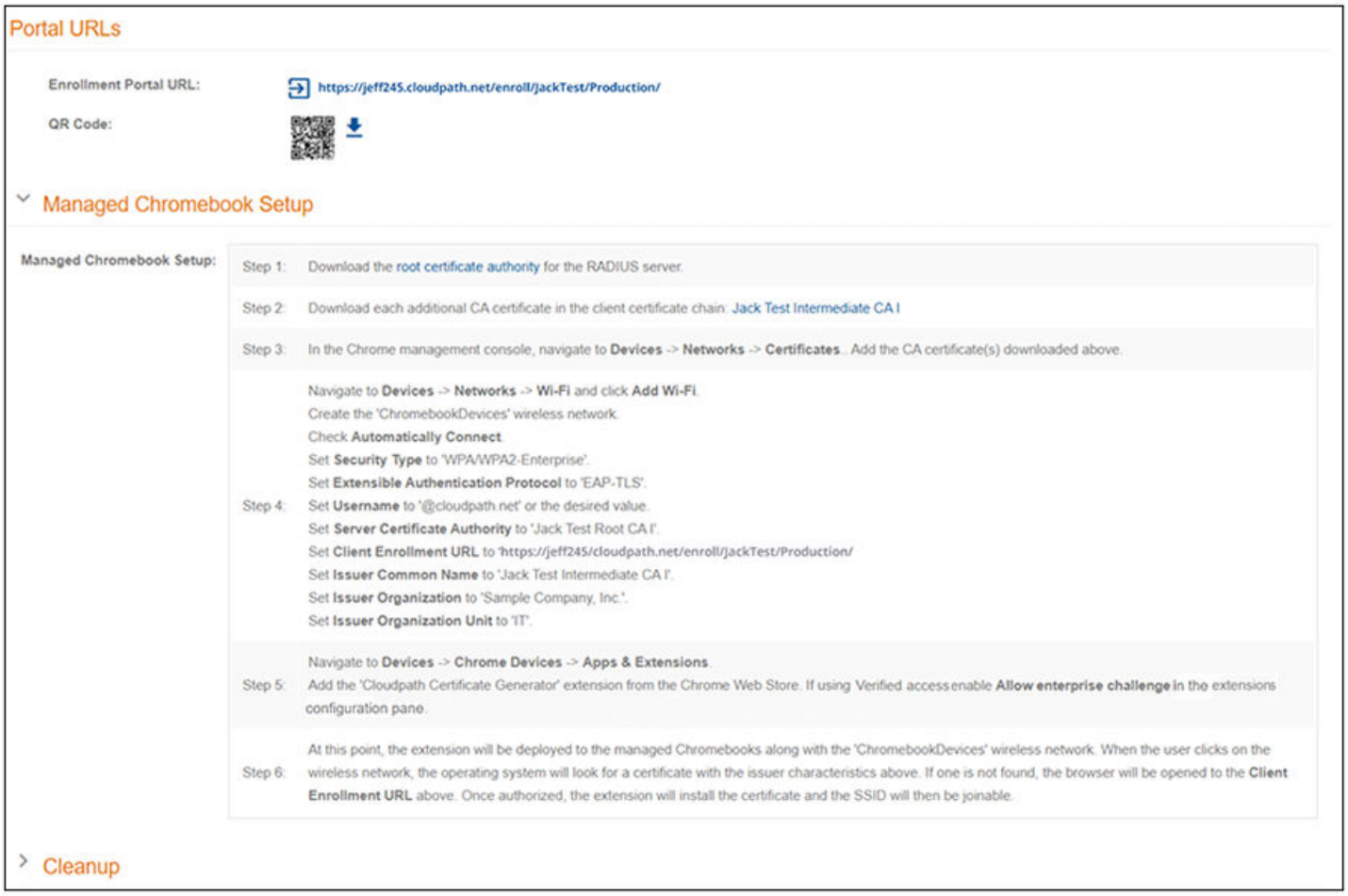
5. Configure **Extension Messages** (Screen 2 above).
   - The **Extension Install Instructions** are displayed to the user if an extension is used to install the certificate on the device.
   - After the certificate has been successfully installed using the extension, the **Completed Message** appears.
6. Configure **Extension - Advanced Behavior** (Screen 2 above).
   - 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. Configure **Extension - Verified Access** (Screen 2 above).

   You will need information from Enabling the Verified Access API on the Google Developer's Site on page 7.
   - Service Account JSON Private Key: Upload the JSON key from the service account that you created on your Google APIs & Services page.
   - Google Browser API Key: Enter or paste in the API key of the verified-access API from your Google APIs & Services page.
   - Verified Access Type: From the drop-down list, select either Device or User, depending on whether the verified access check is performed for the user or the device.
8. **Save** the configuration settings.

# Adding Chromebook Device Configuration to a Workflow

Once you add the Chromebook device configuration into an active workflow, you can click the "Advanced" tab of the workflow, then scroll down to the "Managed Chromebook Setup" section and click the arrow. You will then receive instructions on the remaining configuration to be performed:

**FIGURE 15** Managed Chromebook Setup Instructions for Interactive Chromebook Enrollment




**NOTE**
Specific names shown in the instructions are pulled in from the Cloudpath system being used, and are shown here as an example.

# Downloading the Root CA and Any Additional CAs

The root CA certificate and any intermediate certificates must be downloaded and added into the Google Admin console for use on managed chromebooks.

1. Use the link in Step 1 of the Figure 15 on page 24 page to download the root CA.
2. 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 of the Figure 15 on page 24 to download the additional CAs.

# Configuring the Chrome Extension on Google Admin Console

On the Google admin console, you can upload certificates, set up the Wi-fi network, add the Cloudpath certificate generator, and set any desired policies for managed Chromebook devices.

Log in to the Google admin console using your Google administrator account (not your Google developer's account).

## Uploading Certificates

To upload certificates, do the following:

1. Go to **Devices > Networks > Certificates**.
2. Select the organization for which you want to import the certificate. If you do not select an organization, the certificate settings apply to all organizations and groups.
3. Add all the certificates that you previously downloaded. You need to add them one at a time. When adding the CA, check the box to add the CA for Chromebooks.

   **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.

## Setting up the Wi-fi Network

To create the Chromebook wi-fi network, do the following:

1. Go to **Devices > Networks > Wi-Fi**.
2. Select the organization.
3. Click **Add Wi-fi**. This will invoke a page where you will enter many values. For "Platform access," check the applicable Chromebook platforms. Other important information to configure here, copied from Figure 15 on page 24, includes the following (your instructions will includes names that are specific to *your* own network setup):
   a. Check **Automatically Connect**.
   b. Set **Security Type** to 'WPA/WPA2-Enterprise'.
   c. Set **Extensible Authentication Protocol** to 'EAP-TLS'.
   d. Set **Username** to '@byod.company.com' or the desired value.

      **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, refer to the following link: https://support.google.com/chrome/a/answer/2634553?hl=en#top&add&wifi&thirdparty&variables&change&managecerts&autoconnect&

   e. Set **Server Certificate Authority** to 'Jack Test Root CA I'.
   f. Set **Client Enrollment URL** to 'https://jeff245.cloudpath.net/enroll/JackTest/Production/.
   g. Set **Issuer Common Name** to 'Jack Test Intermediate CA I'.

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

h. Set **Issuer Organization** to 'Sample Company, Inc.'.

i. Set **Issuer Organization Unit** to 'IT'.

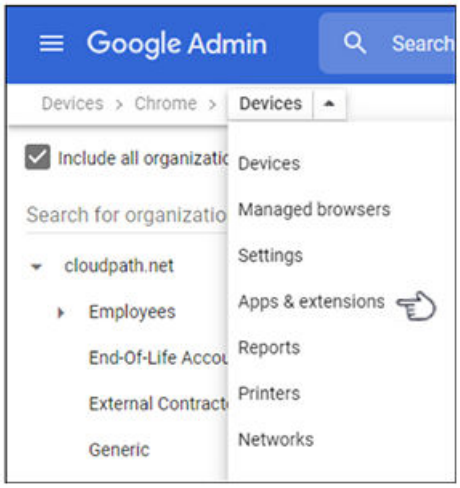
4. Configure any additional fields.
5. Click **Save**.

# Adding Cloudpath Certificate Generator

To add the Cloudpath Certificate Generator, do the following:

1. Go to **Devices > Chrome > Apps & Extensions**.

**FIGURE 16** Navigating to Apps & Extensions in the Google Admin Console




2. Be sure you are in the Users and Browsers area.
3. Open the Chrome Web Store by using the yellow plus button (**+**) on the bottom right of the screen.
4. Search the Chrome Web Store for "Cloudpath Certificate Generator."
5. Add the Cloudpath Certificate Generator.
6. With the generator selected, from the drop-down list to the right of the generator, select "Force Install."
7. If you are using verified access, enable the "Allow enterprise challenge" option under "Certificate Management" in the column on the right side.
8. Click **Save**.

The extension is now deployed to the managed Chromebooks, along with the 'chromebook' wireless network. When the user clicks on the wireless network, the operating system looks for a certificate with the necessary issuer characteristics. If no such certificate is found, the browser opens to the client enrollment URL. Once authorized, the extension installs the certificate, and the SSID can be joined.

# Non-Interactive Authentication for Chromebook Devices



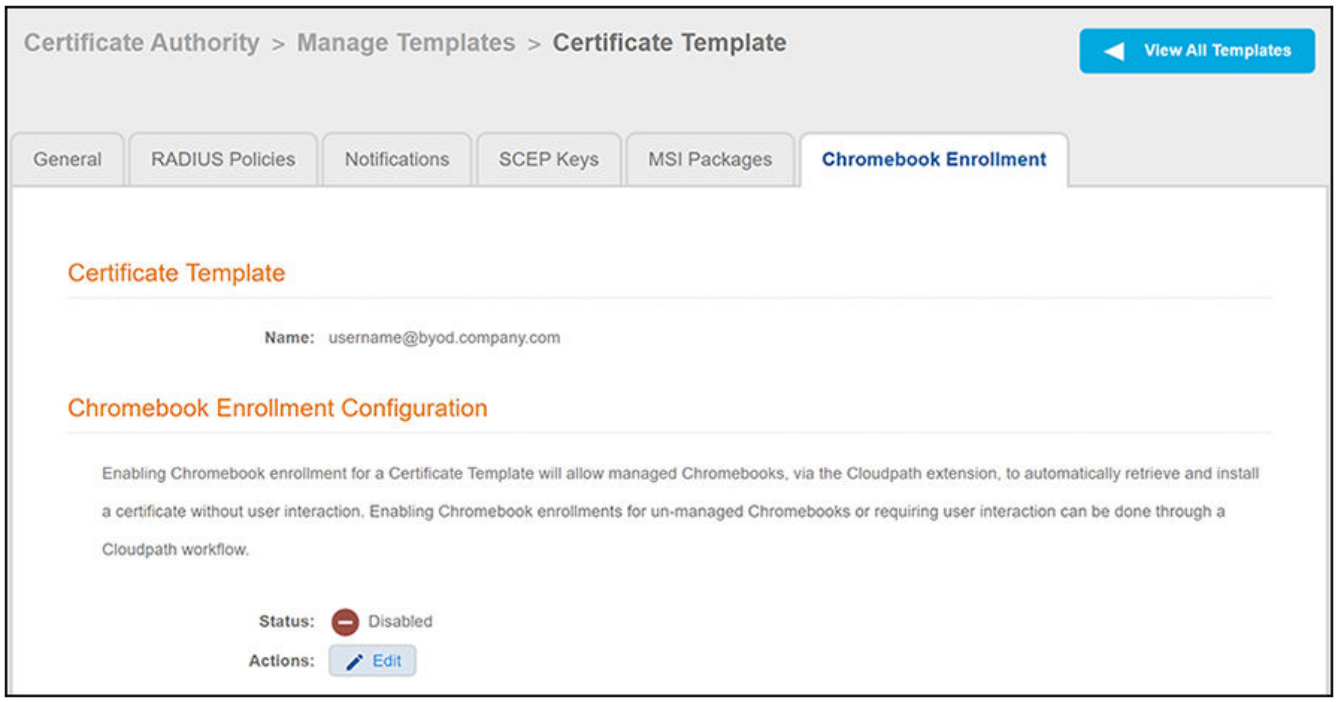
## Configuring a Certificate Template for Chromebook Enrollment

Using the Certificate Authority portion of the Cloudpath UI, you can create and configure a certificate template for Chromebook device enrollment without the use of workflows.

Follow the steps below to create the certificate template:

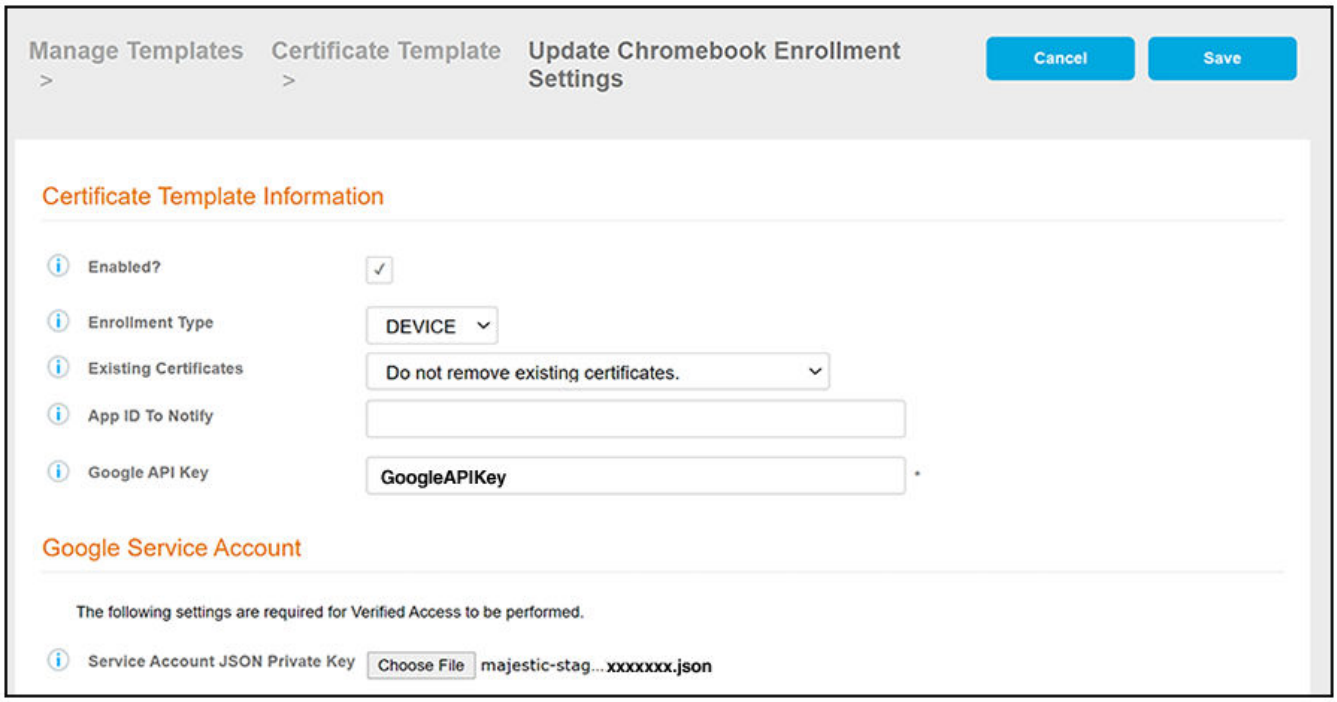
1. In the Cloudpath UI, go to **Certificate Authority > Manage Templates.**
2. Click **Add Certificate Template**.
3. Use an onboard certificate authority and click **Next**.
4. Continue the process until the certificate template is created. You do not necessarily need to use all the default values, but you do need to set the certificate template to generate client certificates.
5. Once the certificate is created, click the Chromebook Enrollment tab. The following view of the template is displayed:

**FIGURE 17** Chromebook Enrollment Tab of Newly Created Certificate Template




6. Click the **Edit** button on the screen.
7. On the ensuing screen, check the "Enabled?" box.
8. Configure the Chromebook Enrollment Settings screen values, as shown in the example below. Field descriptions follow the illustration.

**FIGURE 18** Chromebook Enrollment Settings




- Enrollment Type: This selection determines the type of verified access and certificate enrollment that is performed, as well as which variables are populated for use in the common name pattern. For more information, click the Information icon for this field on the screen.
- Existing Certificates: Choose the desired action from the drop-down list. For more information, click the Information icon for this field on the screen.
- App API to Notify (optional): If specified, the application is notified when the certificate installation is complete.
- Google API key: Enter or paste in the API key of the verified-access API from your Google APIs & Services page. Refer to Figure 3 on page 10.
- Service Account JSON Private Key: Click **Choose File**, then locate and upload the JSON key from the service account that you created on your Google APIs & Services page. For more information, refer to Figure 10 on page 16.
- Click **Save**. You are now presented with the following information, which includes instructions on the remaining configuration steps, shown in the following two illustrations:

**FIGURE 19** Managed Chromebook Setup Configuration and Instructions for Non-Interactive Chromebook Enrollment - Screen 1

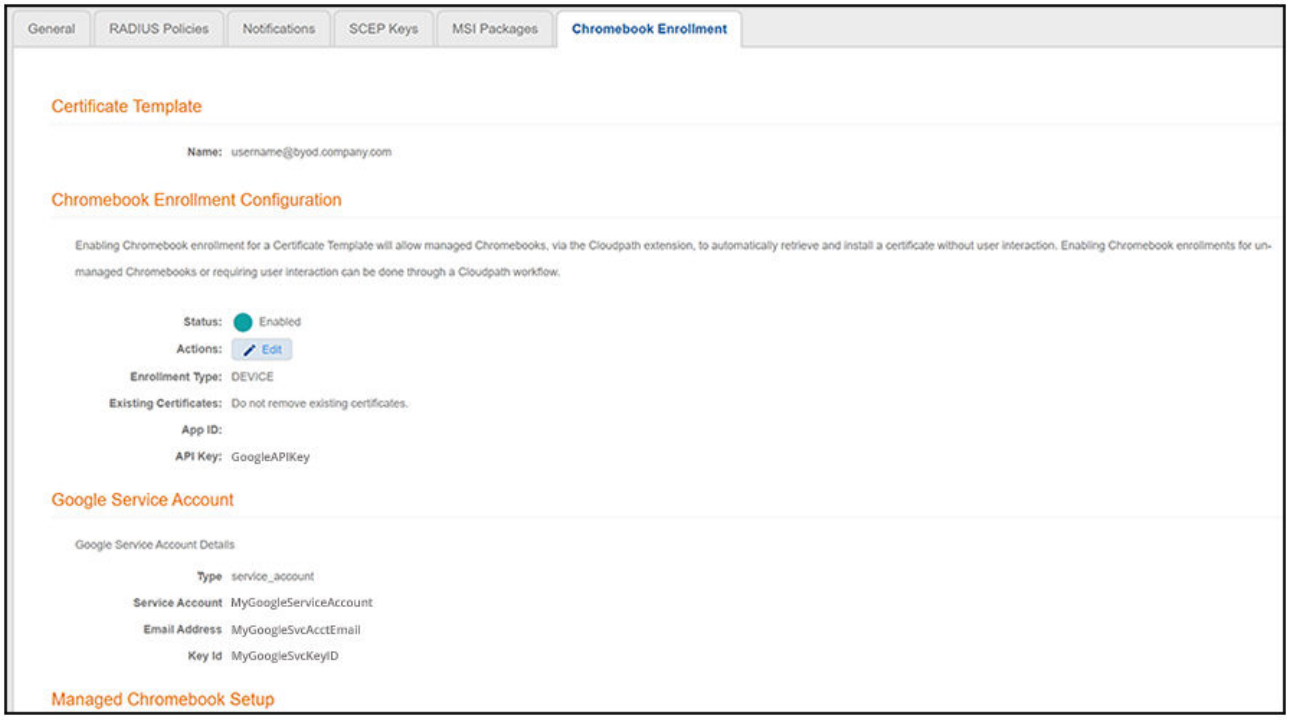


**FIGURE 20 Managed Chromebook Setup Configuration and Instructions for Non-Interactive Chromebook Enrollment - Screen 2**


**NOTE**
Specific names shown in the instructions are pulled in from the Cloudpath system being used, and are shown here as an example.

# Downloading the Root CA and Any Additional CAs

Download the PEM files of your root CA and any other CAs in the chain. You can download these from the **Certificate Authority > Manage CAs** portion of the Cloudpath UI.

# Configuring the Chrome Extension on Google Admin Console

On the Google admin console, you can upload certificates, set up the Wi-fi network, add the Cloudpath certificate generator, and set any desired policies for managed Chromebook devices.

Log in to the Google admin console using your Google administrator account (not your Google developer's account).

# Uploading Certificates

To upload certificates, do the following:

1. Go to **Devices > Networks > Certificates**.
2. Select the organization for which you want to import the certificate. If you do not select an organization, the certificate settings apply to all organizations and groups.
3. Add all the certificates that you previously downloaded. You need to add them one at a time. When adding the CA, check the box to add the CA for Chromebooks.

   **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.

# Setting up the Wi-fi Network

To create the Chromebook wi-fi network, do the following:

1. Go to **Devices > Networks > Wi-Fi**.
2. Select the organization.
3. Click **Add Wi-fi**. This will invoke a page where you will enter many values. For "Platform access," check the applicable Chromebook platforms. Other important information to configure here, copied from Figure 15 on page 24, includes the following (your instructions will includes names that are specific to *your* own network setup):
   a. Create a wireless network with your SSID.
   b. Check **Automatically Connect**.
   c. Set **Security Type** to 'WPA/WPA2-Enterprise'.
   d. Set **Extensible Authentication Protocol** to 'EAP-TLS'.
   e. Set **Username** to '@byod.company.com' or the desired value.

      **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, refer to the following link: https://support.google.com/chrome/a/answer/2634553?hl=en#top&add&wifi&thirdparty&variables&change&managecerts&autoconnect&

   f. Set **Server Certificate Authority** to the Certificate Authority configured in step 1.
   g. Set **Issuer Common Name** to 'Jack Test Intermediate CA I'.

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

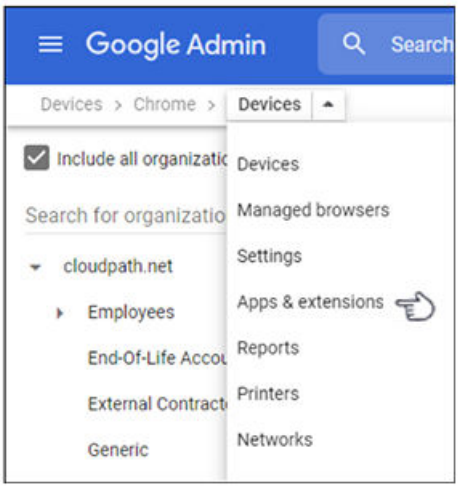
   h. Set **Issuer Organization** to 'Sample Company, Inc.'.
   i. Set **Issuer Organization Unit** to 'IT'.
4. Configure any additional fields.
5. Click **Save**.

# Adding Cloudpath Certificate Generator

To add the Cloudpath Certificate Generator, do the following:

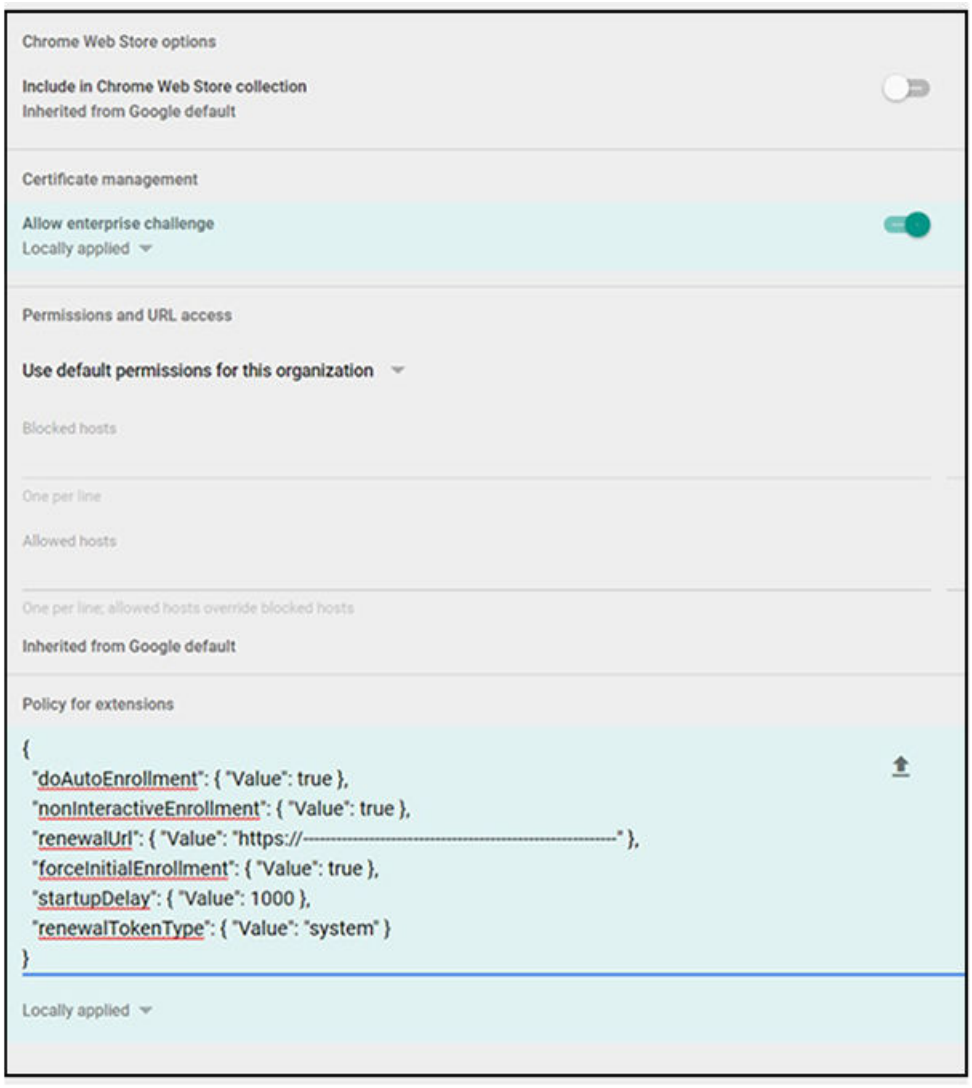
1. Go to **Devices > Chrome > Apps & Extensions**.

   **FIGURE 21** Navigating to Apps & Extensions in the Google Admin Console




2. Be sure you are in the Users and Browsers area.
3. Open the Chrome Web Store by using the yellow plus button (**+**) on the bottom right of the screen.
4. Search the Chrome Web Store for "Cloudpath Certificate Generator."
5. Add the Cloudpath Certificate Generator.
6. With the generator selected, from the drop-down list to the right of the generator, select "Force Install."
7. With the generator selected, set the following remaining values:

**FIGURE 22** Cloudpath Certificate Generator Settings




a. Enable "Allow enterprise challenge."

b. In the "Policy for extensions" section, paste in the JSON information from the Chromebook Extension tab in the Cloudpath UI (refer to Step 4 in Figure 20 on page 31).

c. Save the changes.

The extension is now deployed to the managed Chromebooks, along with the 'chromebook' wireless network. Once authorized, the extension installs the certificate, and the SSID can be joined. When the user clicks on the wireless network, the operating system looks for a certificate with the necessary issuer characteristics.

# 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



350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com