chrome enterprise



Migrating from legacy SCEP to Certificate Provisioning API

chrome enterprise

Contents

Overview

Before you begin

1. Set up Google Cloud Project with Billing Account
2. Verify ChromeOS version
3. Verify Google Cloud Certificate Connector version
4. Locate Legacy SCEP profile

Configure Google Cloud Project

1. Enable the Chrome Management API
2. Create a Pub/Sub topic
3. Grant Pub/Sub Publisher role to Google's Service Account
4. Create an IAM Service Account for the Google Cloud Certificate Connector

Create a SCEP configuration in the Admin console

1. Create a SCEP Certificate Authority Connection
2. Create a SCEP Profile Configuration

Configure Google Cloud Certificate Connector

1. Verify Google Cloud Certificate Connector version
2. Download Service Account Key
3. Add a challenge file
4. Add Adapter Configuration
5. Restart the Google Cloud Certificate Connector

Configure Wi-Fi profile

1. Link existing Wi-Fi profile with EAP-TLS to new certificate provisioning profile

FAQ

Certificate renewal period

Third-party products: This document describes how Google products work with the Microsoft Windows operating systems and the configurations that Google recommends. Google does not provide technical support for configuring third-party products. Google accepts no responsibility for third-party products. Please consult the product's website for the latest configuration and support information. You may also contact Google Solutions Providers for consulting services.

©2026 Google LLC All rights reserved. Google and the Google logo are registered trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated. [EXTENSIONS-en-1.0]

Overview

This document describes how to migrate from legacy SCEP profiles to the new Certificate Provisioning API. The instructions are aimed at customers who want to achieve feature parity with their legacy certificate enrollment workflow. Customers with advanced setups (for example, dynamic SCEP) should refer to the onboarding instructions in Configuring Certificate Provisioning for ChromeOS via SCEP and Use the Google Cloud Certificate in the Help Center.

We recommend to migrate as follows:

1. Set up a Certificate Authority Connection in the root OU.
2. Set up a new certificate provisioning profile for a small test OU.
3. Verify that a ChromeOS test device enrolled to the test OU receives a certificate from the updated deployment.
4. Set up a new certificate provisioning profile for a larger OU.
5. Let the legacy Secure SCEP profile and the new certificate provisioning profiles co-exist until the vast majority of devices have been issued a new certificate. The number of certificates recently issued by the Certificate Authority (CA) can indicate the proportion of devices that have already been issued a new certificate.
6. If a Wi-Fi profile with EAP-TLS is configured, let the Wi-Fi profile point to the new certificate profile.
7. Once you have verified that the new setup works as expected, you can delete the legacy SCEP profile from Google Admin console .

> ⚠️ Do **not** delete the legacy SCEP profile until ChromeOS devices are confirmed to be successfully receiving client certificates through the new Certificate Provisioning API. Deleting a legacy SCEP profile removes existing client certificates from all ChromeOS devices that rely on it. If new certificates have not yet been issued, devices may lose access to the internet or other resources.

Before you begin

1. Set up Google Cloud Project with Billing Account

You must have a Google Cloud Project with a functioning billing account. This billing account is necessary for using Pub/Sub. The vast majority (expected to be 98%+) of all existing customers are expected not to be charged anything because their data volume created by using the new Certificate Provisioning API stays in the free Pub/Sub tier.

2. Verify ChromeOS version

ChromeOS version 138 or later is required for the feature to work.

3. Verify Google Cloud Certificate Connector version

An instance of the Google Cloud Certificate Connector with version 5.21 or later.

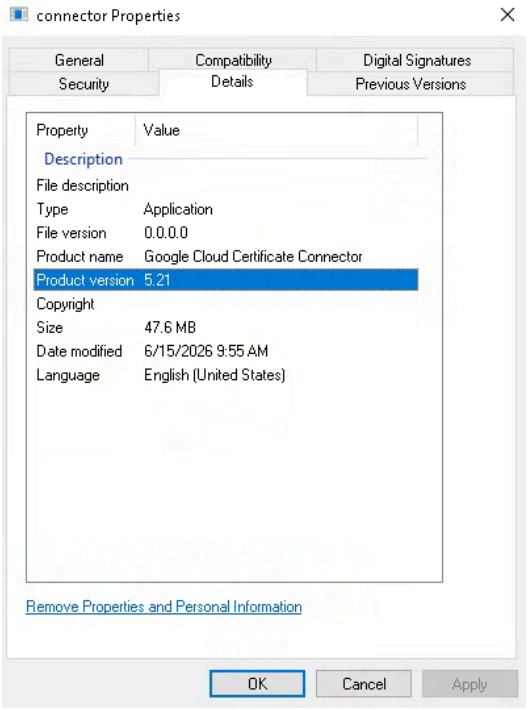
a. Sign in to the machine running the Google Cloud Certificate Connector.

b. Open the Google Cloud Certificate Connector installation directory.

c. Right-click on `connector.exe` to open **Properties** and select the **Details** tab.

d. Check the field **Product Version.**

Note: If the **Product version** field is empty, then you must update the Google Cloud Certificate Connector.



4. Locate Legacy SCEP profile

You have at least one existing SCEP profile to migrate to the new Certificate Provisioning API, while keeping feature parity with their existing client certificate provisioning setup.

Your legacy SCEP profile can be accessed through the Admin console.

a. Sign in to the Google Admin console. Learn more.

b. In the Admin console, navigate to **Devices** -> **Networks.**

c. Select the OU to which the SCEP profile applies.

d. Open the Secure SCEP card.

e. Click the SCEP profile that you wish to migrate.

Configure Google Cloud Project

1. Enable the Chrome Management API

a. Navigate to  -> **APIs & Services** -> **Library.**

b. Search for **Chrome Management API.**

c. Click **Enable.**

2. Create a Pub/Sub topic

a. Navigate from the search bar to the Pub/Sub page.

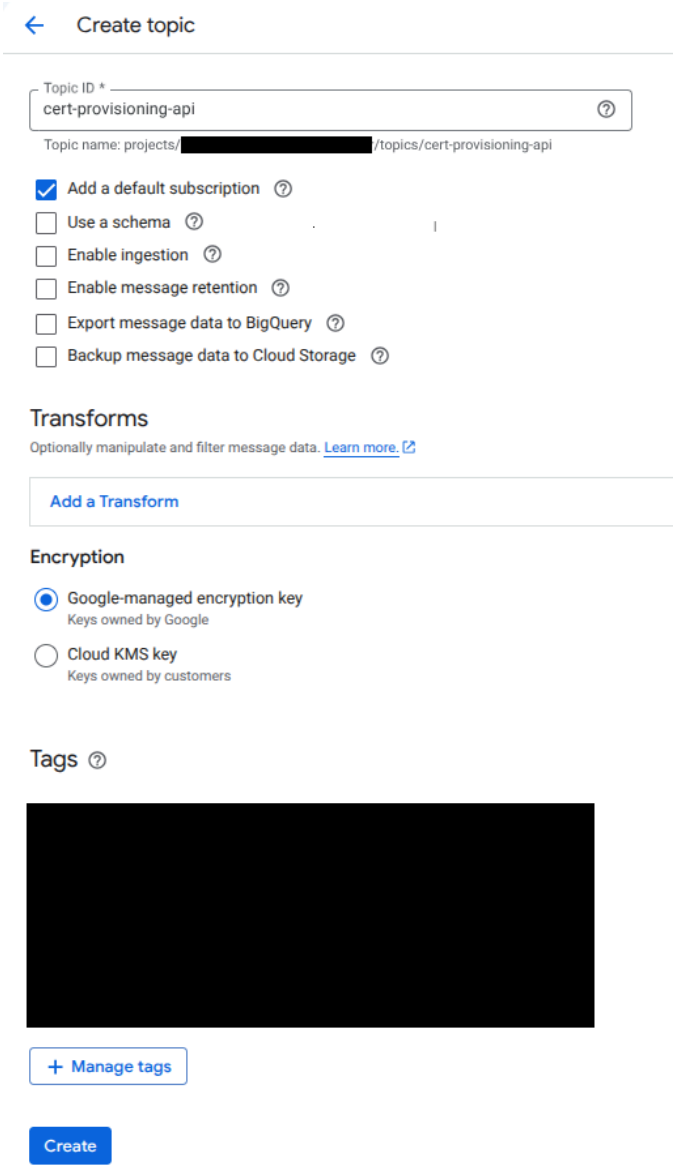
b. Click **Create Topic.**

i. Enter a topic ID (for example, **cert-provisioning-api**).

ii. Add a default subscription -> **Checked** (alternatively, a non-default subscription can be created later).

Note: You can customize the topic attributes.

iii. Click **Create.**



3. Grant Pub/Sub Publisher role to Google's Service Account

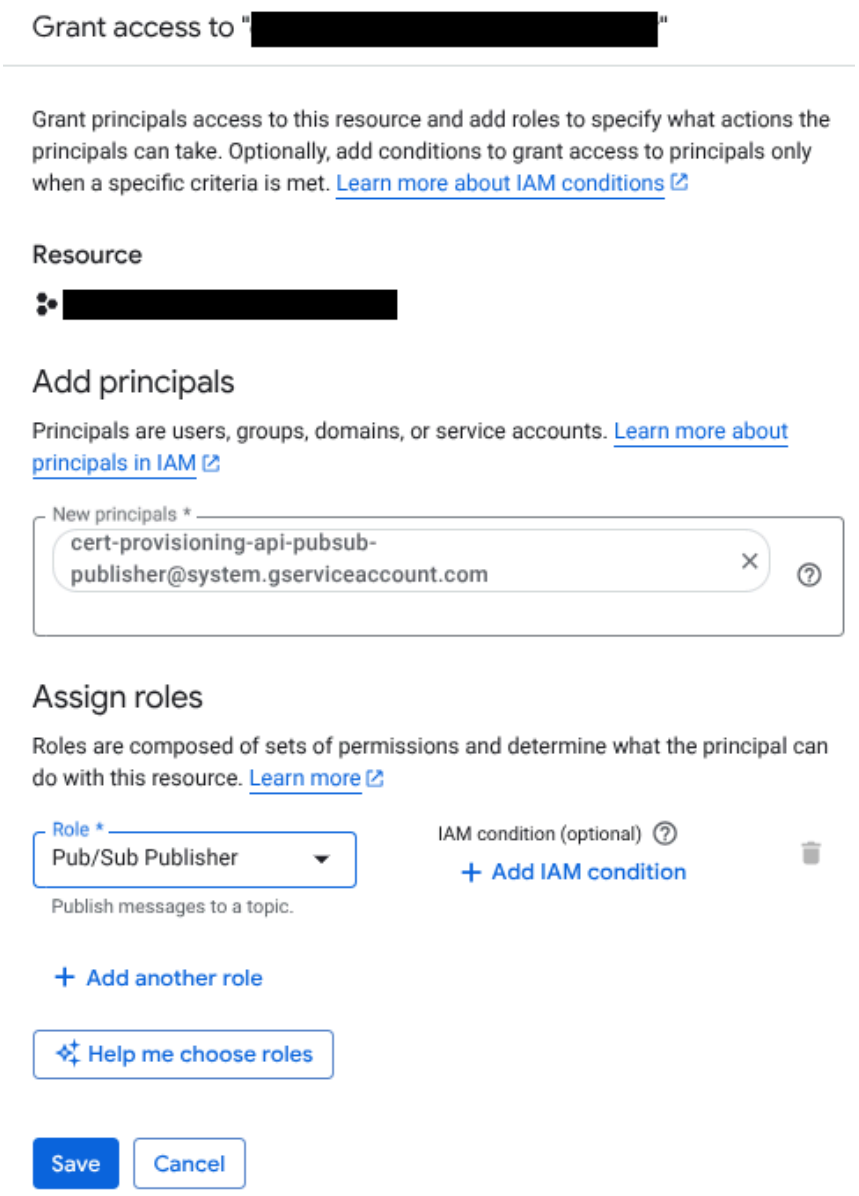
a. Navigate to ☰ -> **IAM & Admin** -> **IAM.**

b. Click **Grant access.**

c. Enter the principal **cert-provisioning-api-pubsub-publisher@system.gserviceaccount.com** and assign the **Pub/Sub Publisher** role to it. The principal is the well-known service account that Google's backend infrastructure will use to publish messages to the Pub/Sub topic.

Note: If Domain Restricted Sharing is enforced for your domain, you can follow these instructions to exempt the service account from the policy.

d. Click **Save**.



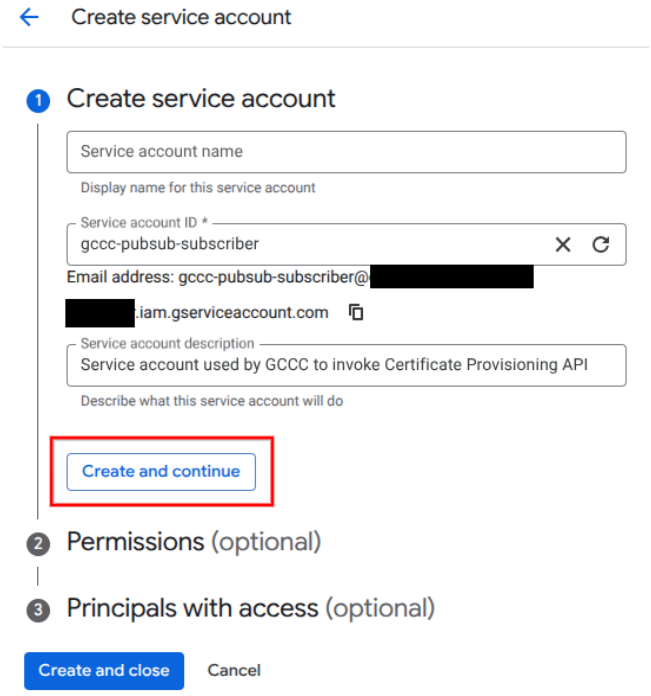
4. Create an IAM Service Account for the Google Cloud Certificate Connector

a. Navigate to ☰ -> **IAM & Admin** -> **Service accounts.**

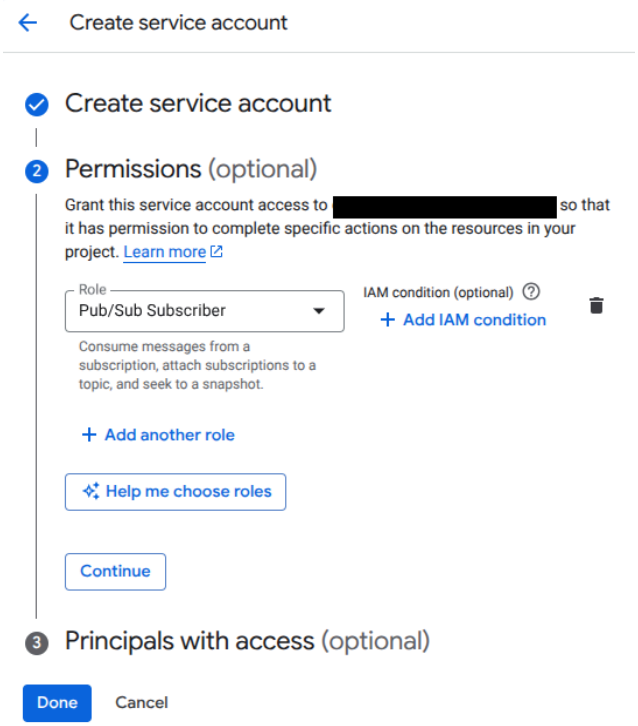
b. Click **Create service account.**

c. Choose a descriptive service account name (for example, **gccc-pubsub-subscriber@<project_id>.iam.gserviceaccount.com**).

d. Click **Create and continue.**



e. For Permissions, select **Pub/Sub Subscriber.**



f. Click **Done.**

Create a SCEP configuration in the Admin console

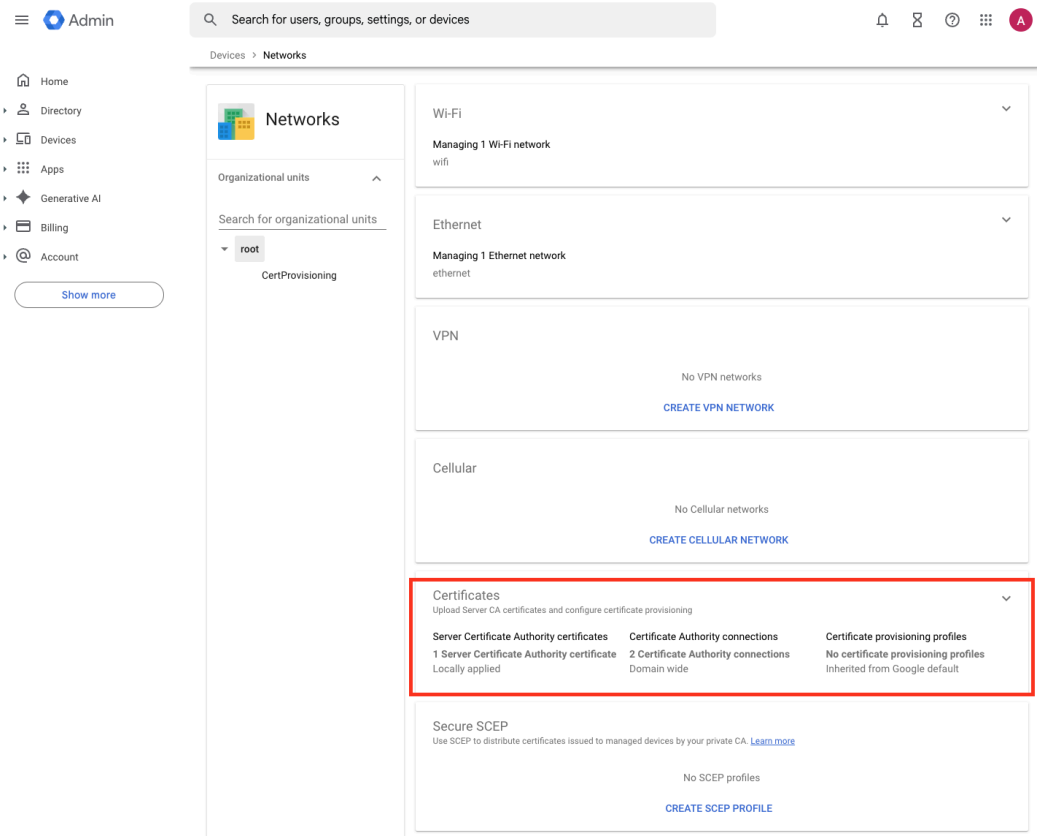
1. Create a SCEP Certificate Authority Connection

Note: Certificate Authority connections are domain wide and not per OU.

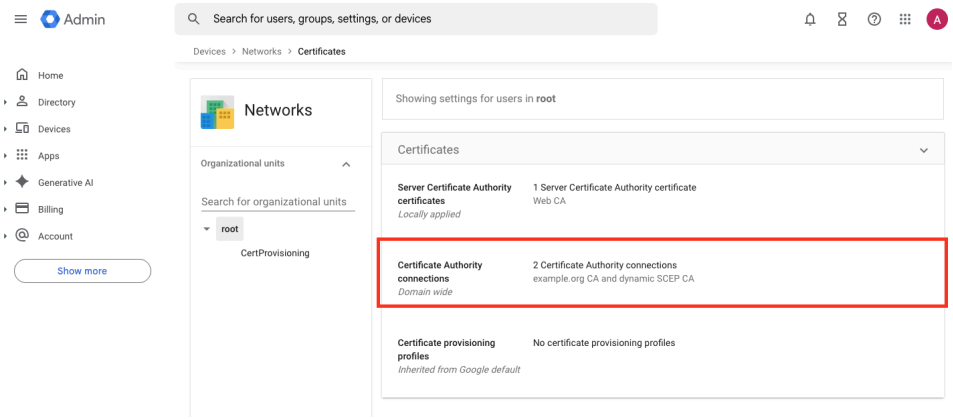
Note: A small set of CA connection attributes are configured on the admin console, the rest is configured in the Google Cloud Certificate Connector local configuration file. Both configurations are linked by the Certificate Authority connection configuration identifier value. It is important to make sure that the value entered in *Certificate Authority connection configuration identifier* has a corresponding CA configuration entry in the Google Cloud Certificate Connector's local configuration (ca_connection_config_id).

a. In the Admin console, open **Devices** -> **Networks.**

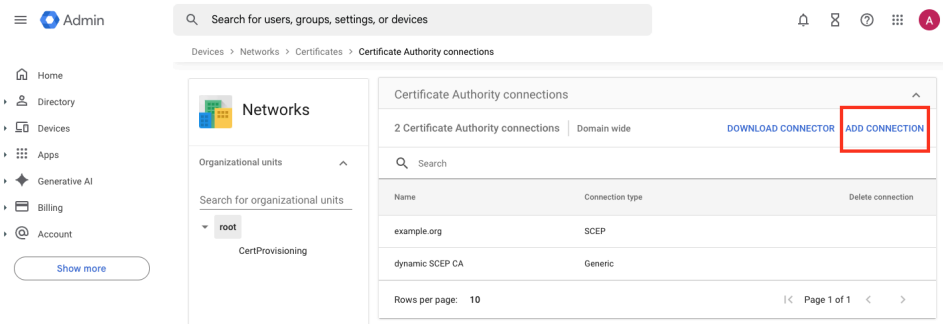
b. Scroll down to **Certificates.**



c. Click **Certificate Authority Connections.**

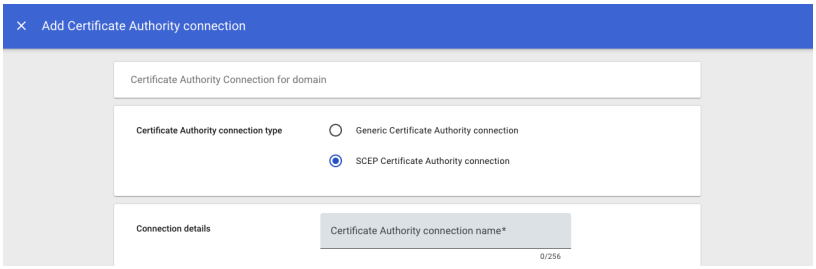


d. Click **Add Connection.**



e. Select **SCEP Certificate Authority connection** as Certificate Authority connection type.

f. Enter a Certificate Authority connection name.



g. Enter the email address of the Google Cloud Project service account (typically in the format **account-name@<project-id>.iam.gserviceaccount.com**) you created previously for the Google Cloud Certificate Connector. This account must have the **Pub/Sub Subscriber** role.

h. Enter the Pub/Sub topic (created earlier), which is used for communicating with the Google Cloud Certificate Connector.

i. Enter a Certificate Authority connection configuration identifier. This identifier will be used by the Google Cloud Certificate Connector to load a local configuration.

j. Click **ADD.**

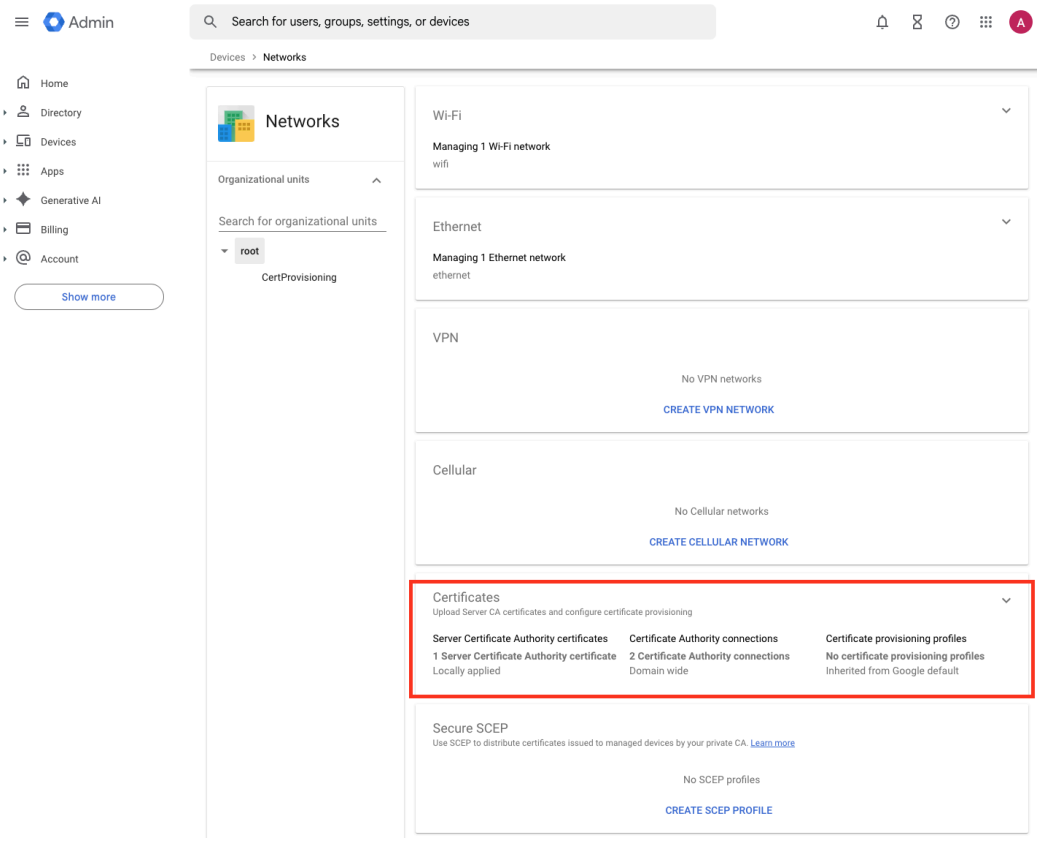
2. Create a SCEP Profile Configuration

Note: Do **not** delete the existing SCEP profile (see Overview).

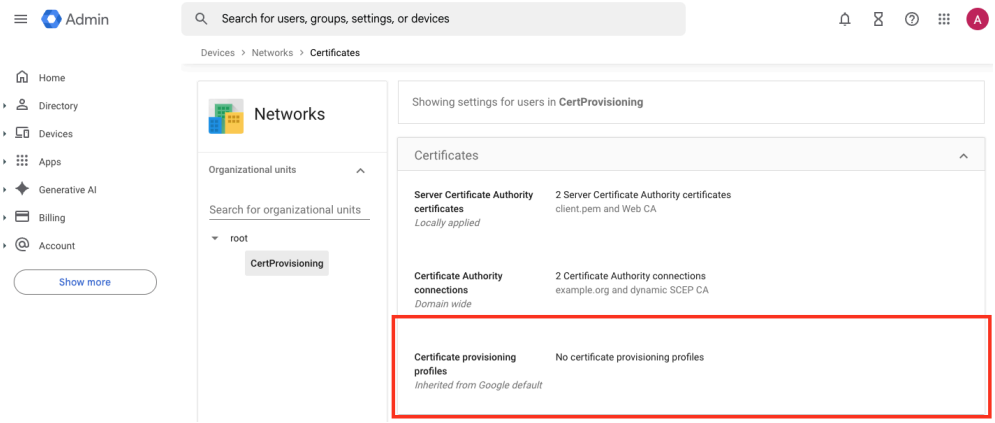
a. In the Admin console, navigate to **Devices** -> **Networks.**

b. Select the same organizational unit for which the legacy SCEP profile is active, which you wish to migrate.

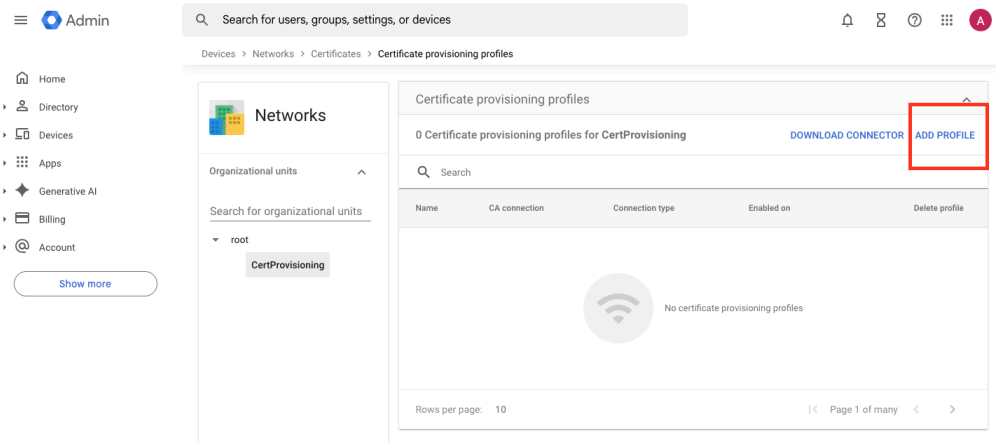
c. Scroll down to **Certificates.**



d. Click **Certificate provisioning profiles.**



e. Click **Add Profile**.



f. Select the Certificate Authority connection created in the previous step.

g. The fields in the certificate profile can mainly be populated with values from the legacy SCEP profile.

Note: The supported list of placeholders can be found here. The legacy SCEP placeholders ${DEVICE_ASSET_ID} and ${DEVICE_ANNOTATED_LOCATION} are no longer supported.

i. **Platform access**: Choose the same settings as in the Device platforms section of the legacy SCEP profile.

ii. **Certificate provisioning profile name**: Choose an arbitrary but descriptive name.

iii. **Days before expiration to initiate renewal**: Copy-paste from legacy SCEP field **Renew within days**.
Due to several misconfigurations in the past, only values between 1 and 90 are permitted. If the issued certificate has a validity period of 1 year, a commonly used value for the renewal period is 30 days.
Note that this value does not define the validity period of the issued certificate. It only defines the point in time when a device will try to renew an existing certificate before it expires, see FAQ.

iv. **Authentication type**: If the **Attestation requirements** in the legacy SCEP profile are set to **Strict**, choose **Remote attestation**. If they are set to **Relaxed**, choose **None.**

v. **Key usage**: Check the same boxes as in the SCEP profile.

vi. **Subject common name**: Copy-paste SCEP field **Common name.**

vii. **Organization**: Copy-paste SCEP field **Company name.**

viii. **Organizational units:** Copy-paste SCEP field **Organizational unit.**

ix. **Locality**: Copy-paste SCEP field **Locality.**

x. **State**: Copy-paste SCEP field **State / province.**

xi. **Country**: Copy-paste SCEP field **Country / region.** This value must be compliant to the standard**.**

xii. **Subject alternative names**: Copy-paste table entries from the **Custom Subject Alternative Names** table in the SCEP profile.

xiii. **Certificate template name**: Copy-paste SCEP field **Template name.**

xiv. **Encryption key type**: Select **RSA key - 2048bit**. If you would like to use this migration to onboard to ECC keys for better performance, you may also select **ECC key - 256bit** here.

h. Click **ADD**.

i. If your domain uses multiple SCEP profiles, repeat this entire section for the other SCEP profiles.

Configure Google Cloud Certificate Connector

1. Verify Google Cloud Certificate Connector version

a. Verify that the Google Cloud Certificate Connector instance is running version 5.21 or above (see instructions above).

b. If setting up a fresh instance of a Google Cloud Certificate Connector, download the Google Cloud Certificate Connector and install it as follows:

i. In the Admin console, open **Devices** -> **Networks.**

ii. Scroll down to **Certificates -> Certificate Authority connections.**

iii. Click **Download connector.**

2. Download Service Account Key

a. In the Google Cloud Project project, navigate to ☰ -> **IAM & Admin** -> **Service accounts.**

b. Click the service account created earlier for the Google Cloud Certificate Connector.

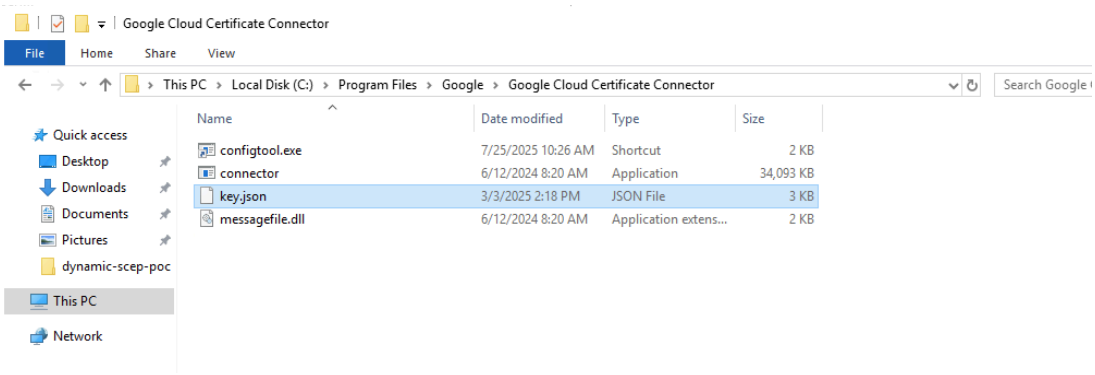
c. Select the **Keys** tab. Click **Add Key** -> **Create a new Key** -> **JSON -> Create.**

d. Move the downloaded **key.json** file to the Google Cloud Certificate Connector installation directory .

3. Add a challenge file

Note: The new Certificate Provisioning API supports dynamic SCEP challenges. If you would like to use this new feature, see instructions in the onboarding guide.

a. If a static challenge is used in the existing SCEP profile, create a file named **challenge-file.txt.**



b. Add the static SCEP challenge to this file. To retrieve the static SCEP challenge, choose one of the following two options:

   i. Open the existing legacy SCEP profile, inspect the HTML page in the browser by clicking **Ctrl + Shift + I** and searching for **Challenge** in the HTML code. This key will be followed by a value=<STATIC_SCEP_CHALLENGE>. Extract the challenge and copy-paste it to the file.

   ii. Extract it from the NDES /mscep_admin page as described in the onboarding guide.

4. Add Adapter Configuration

a. Add a file named **adapter_config.json** to the Google Cloud Certificate Connector installation directory.

b. Add the following content to this file:

```
JSON
{
  "adapter_configuration": {
    "request_subscriptions": [
      "<PUB/SUB_SUBSCRIPTION_NAME>"
    ],
    "key_filename": "adapter_key.json",
  },
  "ca_configurations": [
    {
      "type": "SCEP",
      "ca_connection_config_id": "<CA_CONNECTION_CONFIG_ID>",
      "ca_endpoint_url": "<CA_ENDPOINT_URL>",
       "challenge_filename": "challenge-file.txt"
    }
  ],
  "legacy_configuration": {
    "response_topic": "<LEGACY_PUB/SUB_TOPIC_NAME>",
    "request_subscription": "<LEGACY_SUBSCRIPTION_NAME>"
  }
}
```

c. Replace the placeholders in the file as follows:

   i. **<PUB/SUB_SUBSCRIPTION_NAME>**: Enter the full Pub/Sub subscription name of the Pub/Sub topic created in the Google Cloud Project. If a default subscription is used, the format is **projects/<PROJET_ID>/subscriptions/<TOPIC_NAME>-sub.**

   ii. **<CA_CONNECTION_CONFIG_ID>**: Enter the CA Connection configuration identifier of the CA Connection which was set up in the Admin console.

   iii. **<CA_ENDPOINT_URL>**: Copy-paste the **SCEP server URL** from the legacy SCEP profile.

   iv. Where no static challenge is used, remove the **challenge_filename** key-value pair from the JSON config.

   v. **legacy_configuration**: Copy-paste the content of the existing **config.json** file into this section. This section is necessary so that ChromeOS devices using the legacy SCEP profile are still issued certificates.

      1. The existing config also contains a poll_period parameter which is deprecated. If you decide to leave it in the legacy_configuration section, it will be ignored.

2. The existing **config.json** file will no longer be taken into account by the Google Cloud Certificate Connector when the **adapter_config.json** is present. We recommend keeping **config.json** until deleting the legacy SCEP profile to allow for easy rollbacks.

d. The **adapter_config.json** defined above only contains a small subset of configuration parameters. For the full list, see Use the Google Cloud Certificate Connector.

5. Restart the Google Cloud Certificate Connector

a. Open Windows **Services.**

b. Restart the **Google Cloud Certificate Connector.**

c. Verify that the new Google Cloud Certificate Connector setup works as expected both for the new certificate profile and the legacy profile.

d. In case of unforeseen errors, proceed as follows:

i. Delete the **adapter_config.json** from the Google Cloud Certificate Connector installation directory.

ii. Verify that the legacy **config.json** is still present in the installation directory.

iii. Restart the Google Cloud Certificate Connector.

Configure Wi-Fi profile

Note: This section is only relevant when using a Wi-Fi profile with EAP-TLS.

⚠️ Let the legacy Secure SCEP profile and the new certificate provisioning profiles co-exist until the vast majority of devices have been issued a new certificate. The number of certificates recently issued by the Certificate Authority (CA) can indicate the proportion of devices that have already been issued a new certificate. Only proceed after having verified that client certificates were deployed successfully with the new setup.

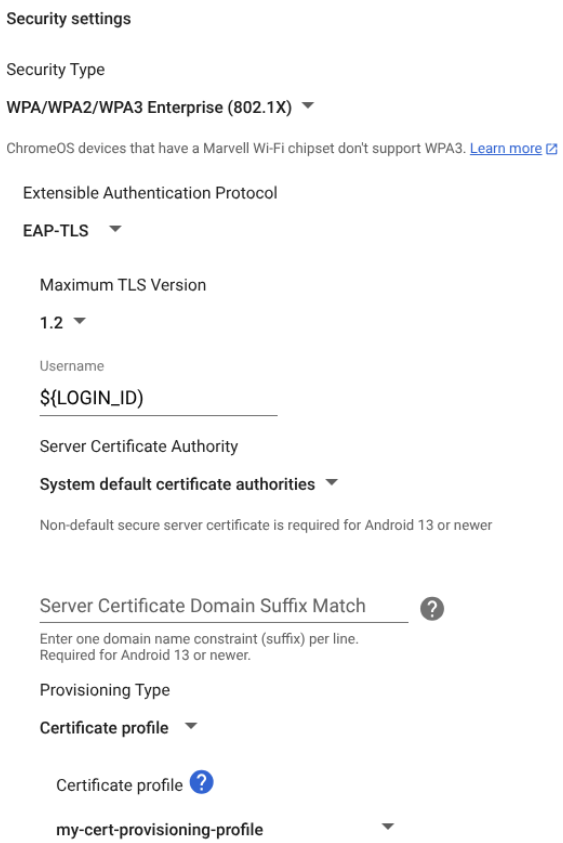
1. Link existing Wi-Fi profile with EAP-TLS to new certificate provisioning profile

a. In the Admin console, navigate to **Devices -> Networks -> WI-FI.**

b. Select an existing Wi-Fi profile that uses EAP-TLS and links to a legacy SCEP profile.

c. Choose **Certificate profile** as the **Provisioning Type.** Then select the new certificate profile from the drop-down menu.

d. Click **Save.**



FAQ

Certificate renewal period

Certificates are re-requested a certain number of days before an existing certificate expires. This ensures that the client device can always present a valid certificate. If the validity period of the certificate is 1 year, a commonly used value for the renewal period is 30 days.

Note that the renewal period does not define the validity period of an issued certificate. The latter can neither be defined in the certificate profile on the Admin console nor through the Google Cloud Certificate Connector config parameters; instead, it must be configured in the CA settings.