chrome enterprise

Notes from the field

Configuring Certificate Provisioning for ChromeOS via SCEP with Microsoft NDES

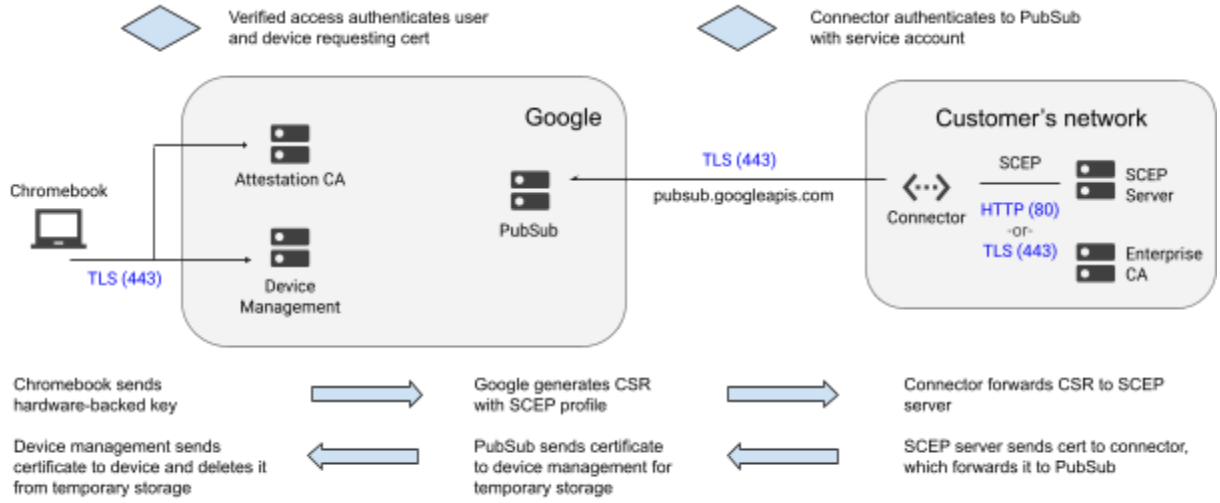
For administrators with Active Directory expertise

Contents

Overview

There are four components involved in setting up ChromeOS Certificate Enrollment with Simple Certificate Enrollment Protocol (SCEP):

- ChromeOS devices
- Google Admin Console
- Google Cloud Certificate Connector
- SCEP server (i.e. Microsoft NDES)



Google Admin Console

Google Admin Console is the web based administrative interface used to configure and apply policy to Chrome Enterprise devices and browsers.

In this document, it is used to configure a SCEP Certificate Enrollment Profile and Wi-Fi Profile that are assigned to users and/or devices based on the OU they belong to. The SCEP Profile specifies the SCEP enrollment URL, Certificate Authority, Certificate Template and other parameters. The Wi-Fi Profile specifies the SSID, Authentication (Certificate) and other network settings.

ChromeOS

During the certificate enrollment process, after successful authentication, the ChromeOS device generates a pair of keys for the device or user, and the public key is forwarded via a Certificate Signing Request (CSR) to Google Admin Console and then to the SCEP server, via the Google Cloud Certificate Connector. The Certificate Authority signs a user or device Certificate based on the CSR, and it is communicated via SCEP back to GCCC, Admin Console and the ChromeOS device.

In order for the enrollment process to be successful, the ChromeOS device needs to be able to communicate with Google Cloud services without interference of SSL decryption.

Microsoft Certificate Services and NDES/SCEP

This document outlines a set of steps necessary to configure Microsoft Network Device Enrollment Service (NDES) and related technologies to allow enrollment and issuance of certificates used to authenticate ChromeOS devices and users to WiFi access points via 802.1X, to VPN gateways and in other client certificate authentication scenarios.

Note that Certificate Connector for Microsoft Intune installs a custom policy module and thus is ***not compatible*** with standard SCEP requests. A separate NDES server should be used from the one running the Intune Connector.

Installation, configuration and security of Microsoft Active Directory Domain Controllers (AD DC), Certificate Services (CS), NDES, Internet Information Server (IIS) and other Microsoft technologies is outside the scope of this document. Please follow Microsoft recommendations and your organization's guidance for hardware and software system requirements.

Specific configuration choices shown are based on guidance in the Microsoft documents listed below, except where noted.

Implementation outside of an isolated lab environment should only be undertaken with full understanding of the technologies and security implications of each step.

The following Microsoft documentation can be used as reference, as of the time of writing:

Configure infrastructure to support SCEP, Network Device Enrollment Service (NDES), NDES Security Best Practices, Securing PKI: Introduction, Constraints and Key Usage, Decommission CA from NtAuthCertificates, Server Certificate Deployment Overview, Enrollment Options for End-Entity Certificates

Microsoft recommends a two- or three-tier PKI deployment for production environments. In such a deployment, the Root Certificate Authority (CA) and possibly the first tier Intermediate CAs are kept offline (not connected to the production network). Issuing CAs are kept online to facilitate issuing of End Entity (Client, Server) certificates.

Given the dynamic nature, and inherently lower security (no approval process) of automated device and user certificate provisioning via SCEP, it is recommended that a dedicated *Issuing CA for NDES* be created.

There are a number of best practice recommendations for securing the NDES infrastructure provided by Microsoft, which are outside the scope of this document. Additional Constraints (CAPathLength etc.) and Key Usage (Client Authentication etc.) limitations can be applied to the CA; it can be restricted to issuing certificates based only on the SCEP template(s); the CA can be removed from the Enterprise AD *NtAuth Store*, to prevent certificates issued by it from being used to authenticate against the rest of the AD infrastructure.

Microsoft does not support running NDES and IIS on the same server as the Issuing CA in production deployments, due to security considerations.

These concerns apply primarily when the CA used for ChromeOS devices and users is part of the existing AD PKI. In a lab environment, or when the PKI is solely used for ChromeOS SCEP, it may be possible to co-locate some components.

Google Cloud Certificate Connector

Google Cloud Certificate Connector (GCCC) allows ChromeOS devices to request certificates from SCEP servers via Google Cloud. Once a SCEP profile is configured in an organization or an Organizational Unit, whenever a device or user that matches that profile signs in, a SCEP certificate enrollment request is generated, if needed, and published to an organization-specific queue where it is picked up and processed by GCCC.

To complete the install and for GCCC to function it requires access to google API and software update endpoints. **See "GCCC Proxy configuration" before proceeding with install if a proxy is used**.

GCCC needs to be able to connect to https://pubsub.googleapis.com via HTTPS on TCP/443 (Direct or Proxy), to retrieve configuration and CSRs, and upload Certificates. ()

For self update these URLs must also be accessible by the connector (See FAQs for self update proxy configuration)

https://pubsub.googleapis.com

edgedl.me.gvt1.com/edgedl/release2
google.com/dl/release
google.com/dl/release2

Depending on the organization's security policy regarding servers with outbound Internet access, GCCC service can be installed directly on the NDES server, on a separate server, or on a completely separate network (DMZ).

If GCCC is being installed on a separate server, NDES IIS should be configured to only accept HTTPS connections and only from the GCCC IP address(es), to improve security.

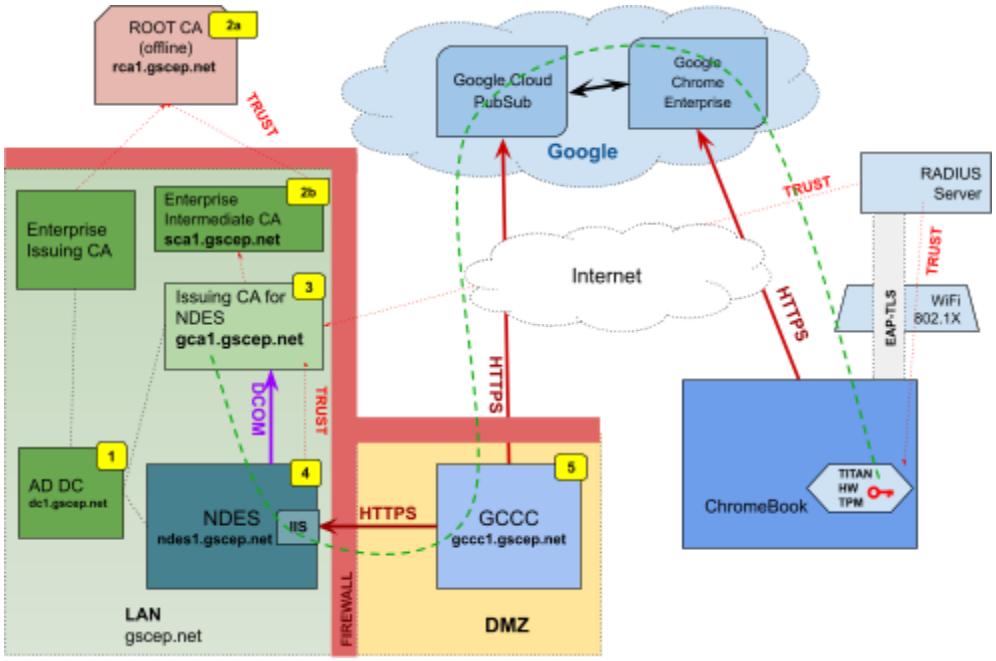
The NDES IIS server SSL certificate Subject Name needs to match the hostname used in the SCEP enrollment URL.

If GCCC is being installed on the NDES server itself, it can connect locally over HTTP and none of the HTTPS or IP restriction steps are required.

Multiple GCCC servers can be used to provide redundancy and load-sharing, as SCEP certificate enrollment requests are published to an organization-specific queue and will be picked up and acknowledged in first-come-first-served order by the connectors.

The system running GCCC requires a dual core CPU @ 2 Ghz and 2 GB RAM running Windows Server 2016 or higher.

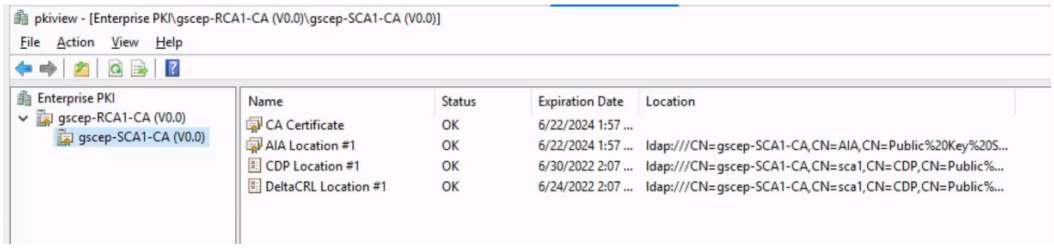
Enterprise Deployment with Microsoft NDES and Google Admin



Prerequisites

Note: Item numbers refer to respective numbered labels in the diagram.

1. Existing Windows **AD Domain**
    a. Domain Controller **- dc1.gscep.net**
2. Existing Microsoft Enterprise PKI
    a. **Root CA - rca1.gscep.net (offline)**
    b. At least one **Intermediate CA** - ***sca1*.gscep.net** available to issue a CA Certificate for *Issuing CA for NDES*
    c. Running ***pkiview.msc*** as an Administrator on the Root CA shows the existing CA infrastructure:

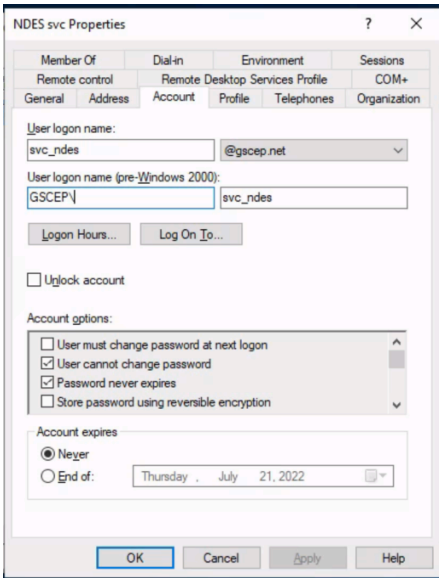


3. VM/Server joined to AD for ***Issuing CA for NDES*** **- gca1.gscep.net**
4. VM/Server joined to AD for ***NDES and IIS*** **- ndes1.gscep.net**
    a. Note: NDES 2016 or above is required
5. VM/Server for ***GCCC*** **-** [gccc1.gscep.net]

6. GCP project with a configured billing account

Create Service account for NDES

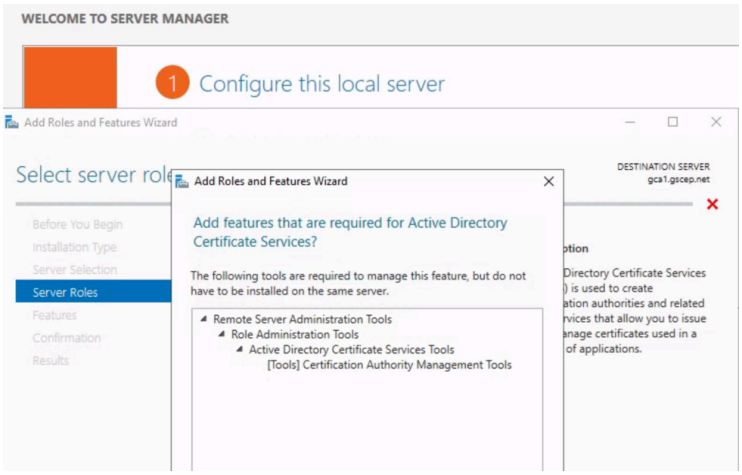
1. Active Directory Users and Computers on **dc1.gscep.net**
2. Create a new user.
3. Username: **svc_ndes**
4. Set password
5. *User cannot change password*
6. *Password never expires.*



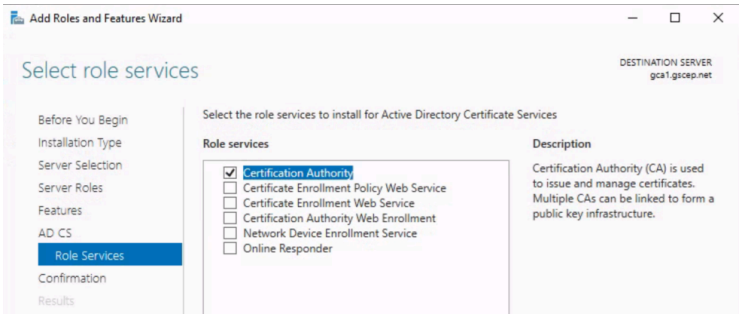
Configure Issuing CA for NDES

1. Add Active Directory Certificate Services role to the *Issuing CA server for NDES* **gca1.gscep.net**
   a. Log in as an ***Enterprise Domain Admin*** user, or another user with sufficient privileges to add *Certificate Services* role
   b. Start *Server Manager*
   c. Dashboard > Add roles and features > Choose **gca1.gscep.net**
   d. Select *Active Directory Certificate Services*

e. Confirm Adding required features

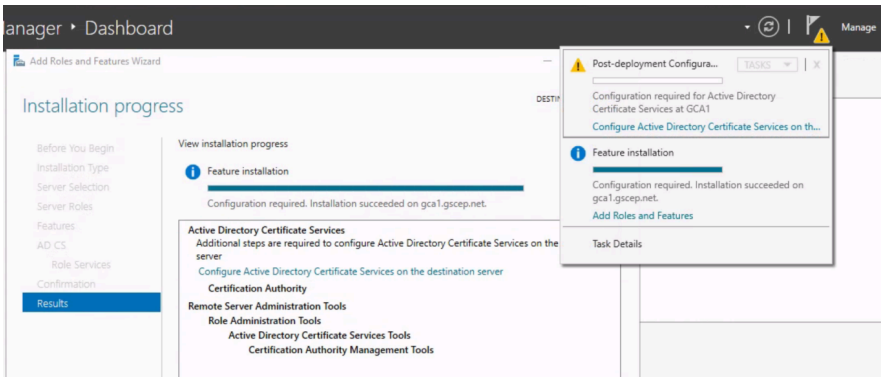


f. Select *Certification Authority* from *Role Services*

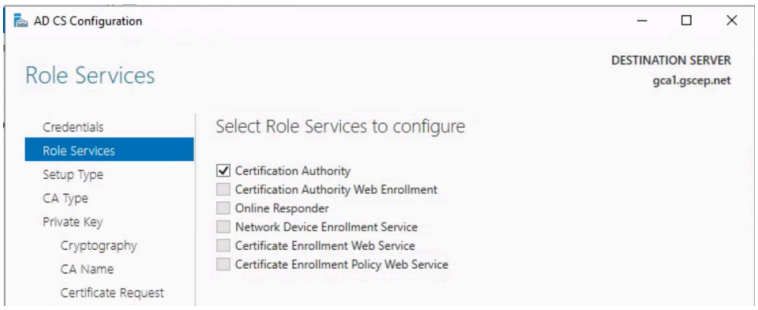


g. Wait for process to complete

2. Configure AD CS on **gca1.gscep.net** as a Subordinate CA to an existing CA ***sca1.gscep.net***
   a. In Server Manager click on yellow warning icon in the top bar
   b. Under *Post-Deployment Configuration*, click on *Configure Active Directory Certificate Services…*



c. Role Services: *Certification Authority*



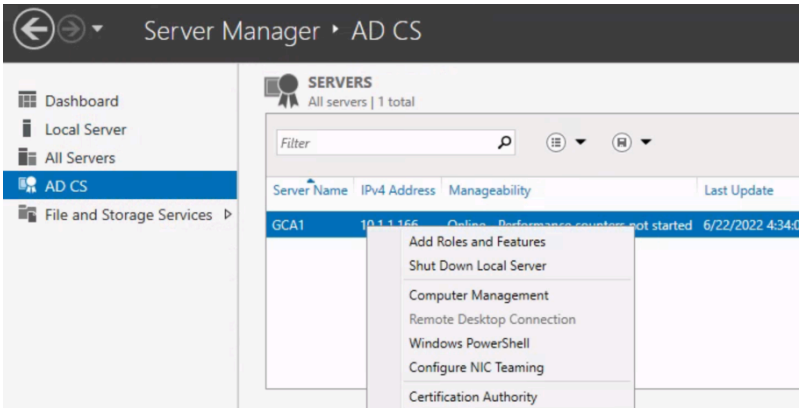
d. *Setup Type: Enterprise CA*
e. *CA Type: Subordinate CA*
f. *Create a new private key*
g. Select defaults or adjust as needed for Cryptography and CA Name
h. *Certificate Request*: *Send a certificate request to a parent CA*
i. *CA Name or Computer name*
j. Select appropriate existing ***Subordinate*** Issuing CA from which to request a CA certificate for the *Issuing CA for NDES* - ***sca1.gscep.net***

k. Accept defaults for the rest and click *Configure*

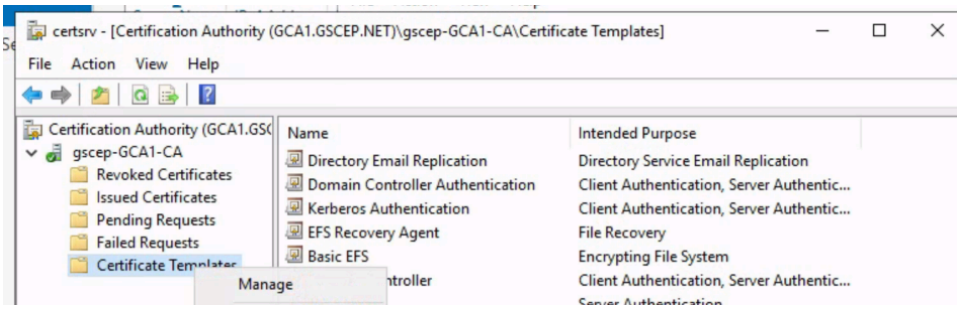
3. Create the SCEP certificate template

a. *Note that while these settings have been verified, your organization's policy might dictate different settings, which would need to be tested.*

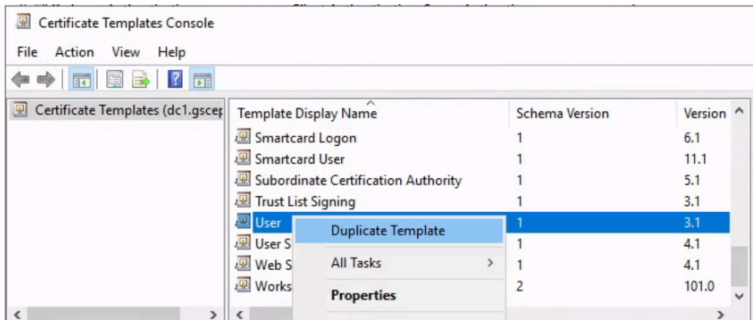
b. Open Certification Authority on **gca1.gscep.net**



c. Certificate Templates → Manage



d. Duplicate *User* Template



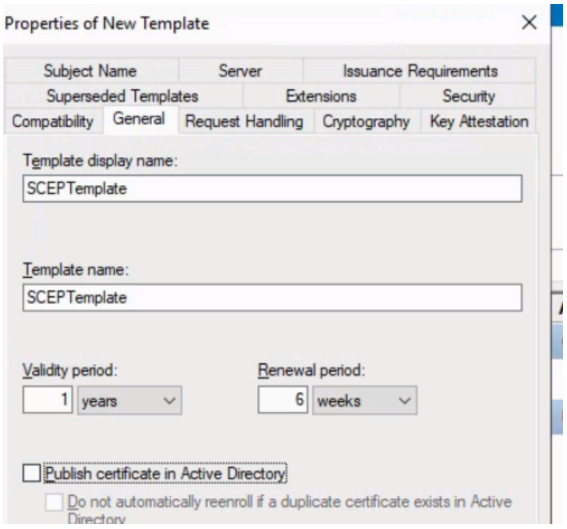
e. General

i. *Template Name*: **SCEPTemplate**

1. Note: the ***Template name*** is used for configuration, **not** the *Template display name.*

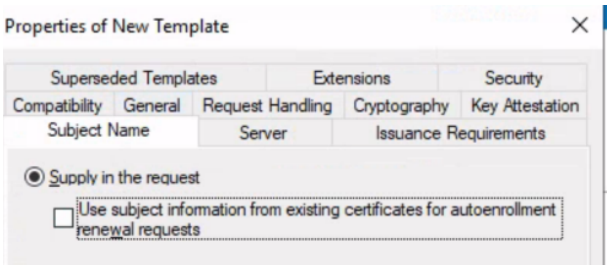
ii. *Publish certificate in Active Directory*: **Unchecked**

iii. Note: These certificates will not be used for Windows Authentication

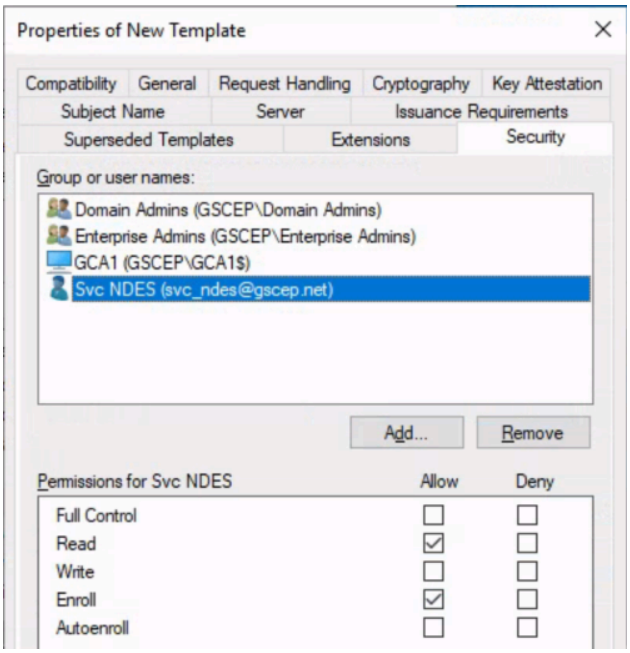


f. Subject Name → ***Supply in the request***

g. Note: This is necessary since the user or device name is supplied during enrollment via SCEP.

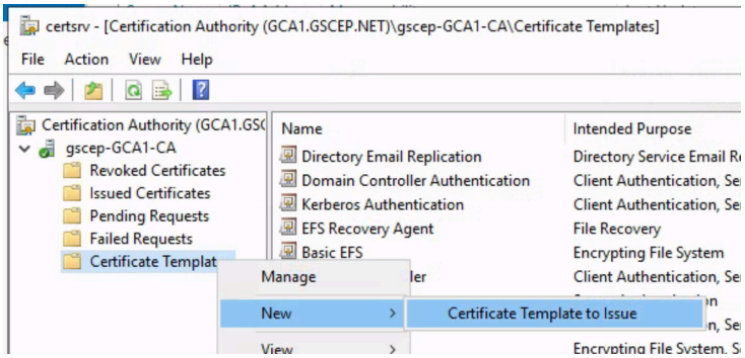


h. Security
   i. Add NDES service account **svc_ndes** with ***Read*** and ***Enroll*** permissions
   ii. Add CA computer account of **gca1.gscep.net** with *Read* permission
   iii. Remove *Authenticated Users*
   iv. Note: this ensures that NDES service, CA and Admins **ONLY** can issue or read the SCEP certificates.

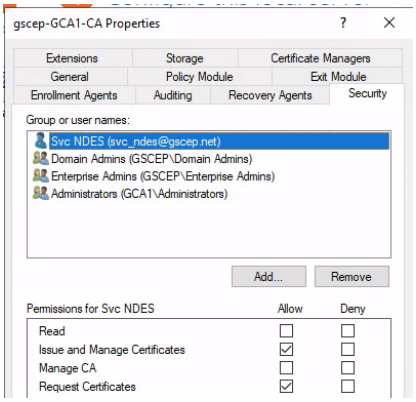


b. Close *Certificate Templates* Console

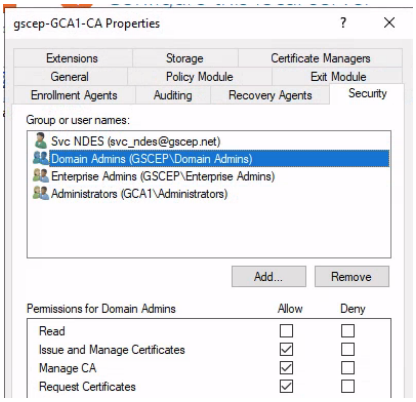
c. Back in *Certification Authority*
   i. *Certificate Templates → New → Certificate Template to Issue*
   ii. Select **SCEPTemplate**



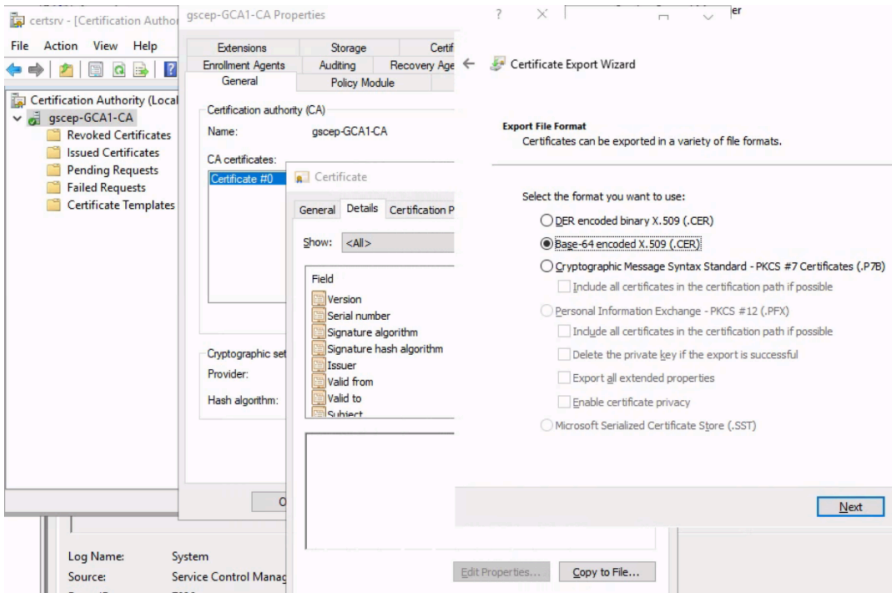
4. Allow NDES Service to enroll and manage certificates
    a. Open Certification Authority → **gscep-GCA1-CA** → Properties → Security
    b. Add **svc_ndes** with ***Issue and Manage*** and ***Request Certificates*** permissions



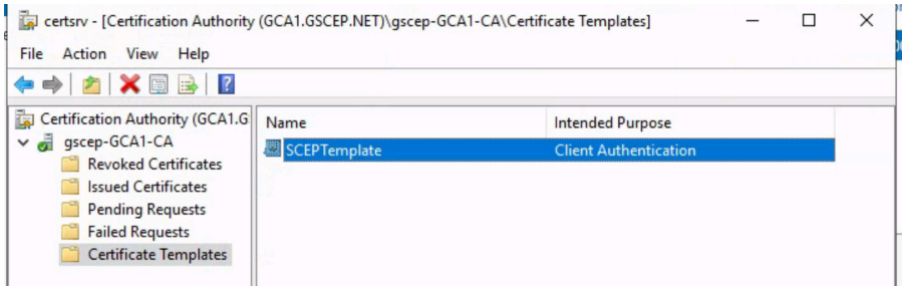
    c. **Optional** Remove *Authenticated Users*
    d. Note: This ensures that only NDES or Admins can issue certificates on this CA
    e. Make sure Domain Admins, or the account that is being used to install and configure NDES have the right to Request Certificates



5. Export Issuing CA Certificate
    a. Certification Authority → **gscep-GCA1-CA** → Properties → General → CA Certificates →*Certificate #0*
    b. Export the certificate from the Details tab and save as a Base-64 ***.CER*** *file, i.e.* ***gca.cer***
    c. Note: this certificate will be imported into Google Admin Console

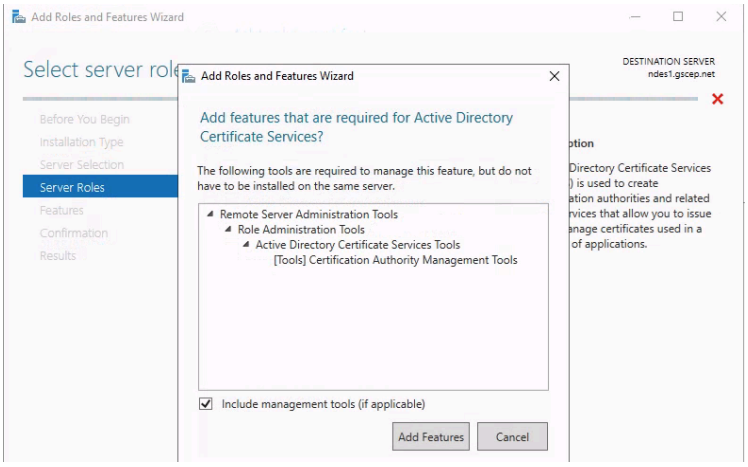


6. Disable all other Certificate Templates (Optional)

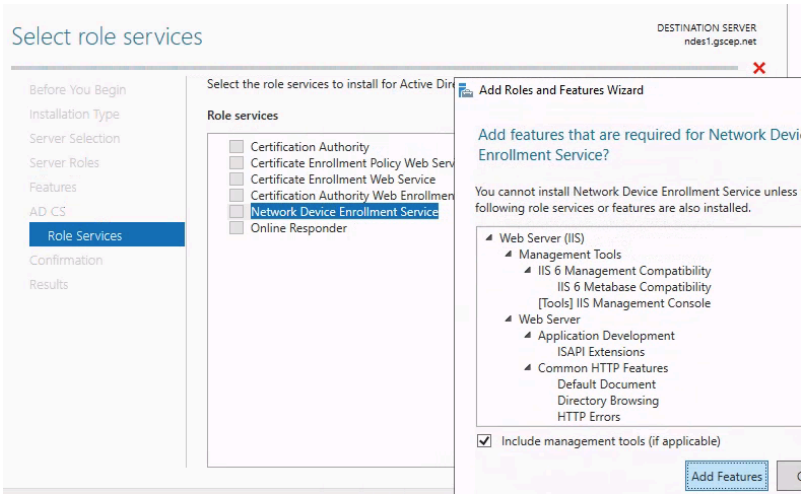


Configure NDES and IIS

1. Add Active Directory Certificate Services role to the server ***ndes1*.gscep.net**
    a. Log in as an ***Enterprise Domain Admin*** user, or another user with sufficient privileges to add Certificate Service role
    b. Start *Server Manager*
    c. Dashboard > Add roles and features > Select ***ndes1*.gscep.net**
    d. Select *Active Directory Certificate Services*



e. Select role services:
   i. Certification Authority - **Uncheck**
   ii. Network Device Enrollment Service - **Check**
   iii. This will add IIS role for installation

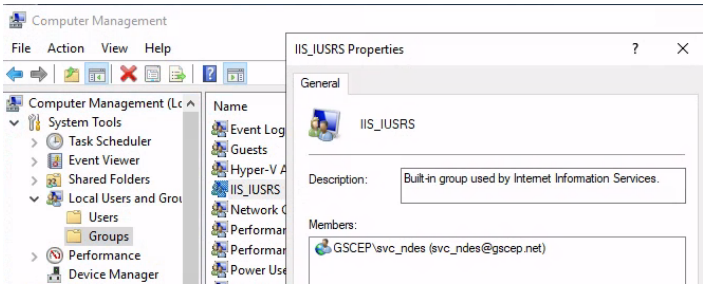


f. Accept defaults for the rest
g. Wait for process to complete

2. Add NDES Service Account to local IIS_IUSRS Group

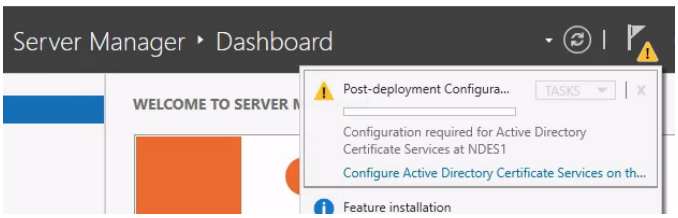
a. *Server Manager → Tools → Computer Management → Local Users and Groups*

b. Add user **svc_ndes** to group IIS_IUSRS

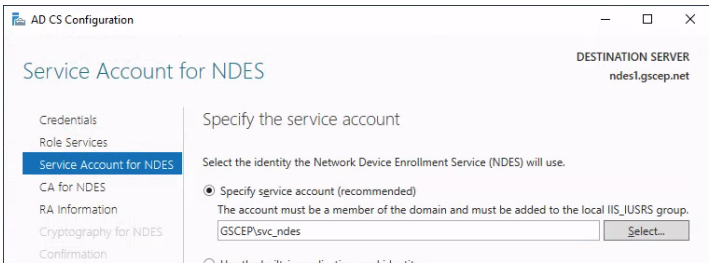


3. Configure NDES Service

a. In Server Manager click on yellow warning icon in the top bar
b. Under *Post-Deployment Configuration*, click on *Configure Active Directory Certificate Services…*



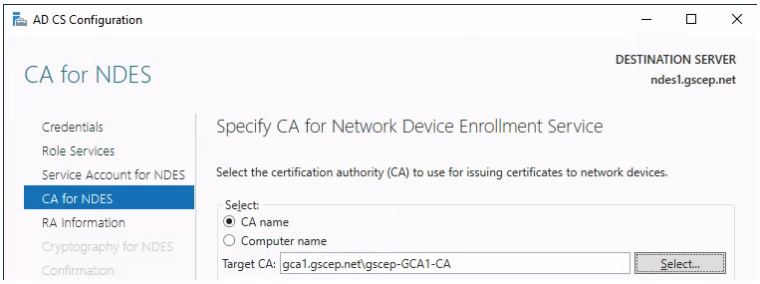
c. Role Services: *Network Device Enrollment Service*
d. Use the ***Enterprise Admin Credentials*** from step 1 to *configure role services*
e. *Service Account:* ***svc_ndes***



f. *CA for NDES: CA name*

i. *Select* **gca1.gscep.net**

ii. Note: This is the CA that will issue certificates for devices/users



g. RA Information and Crypto: as needed

h. Wait for Configuration to complete

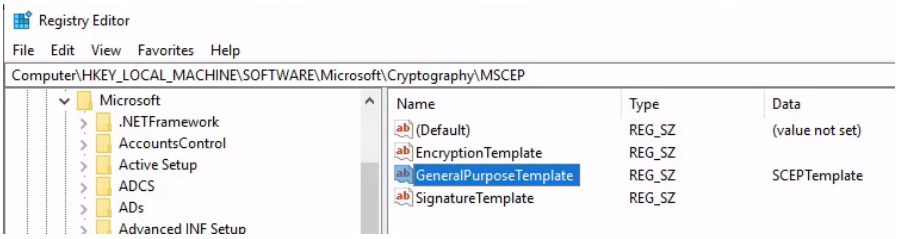
4. (Optional) Configure default NDES template

a. Open *regedit*

i. *`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\GeneralPurposeTemplate`*

ii. Set value to the Template Name (**not** Template display name) of SCEP template created above - **SCEPTemplate**

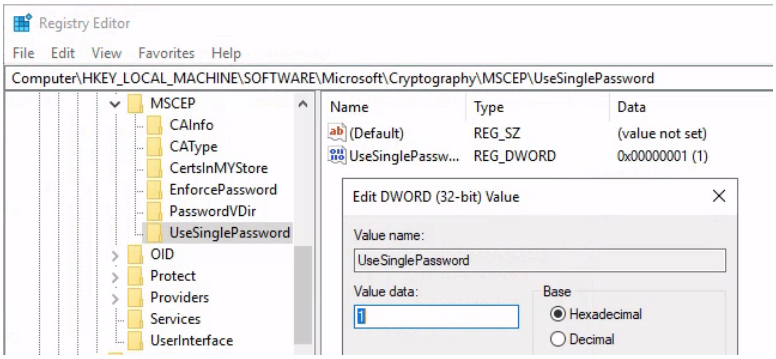
iii. EncryptionTemplate and SignatureTemplate should be blank or set to same value



5. Configure NDES to utilize a static SCEP challenge password

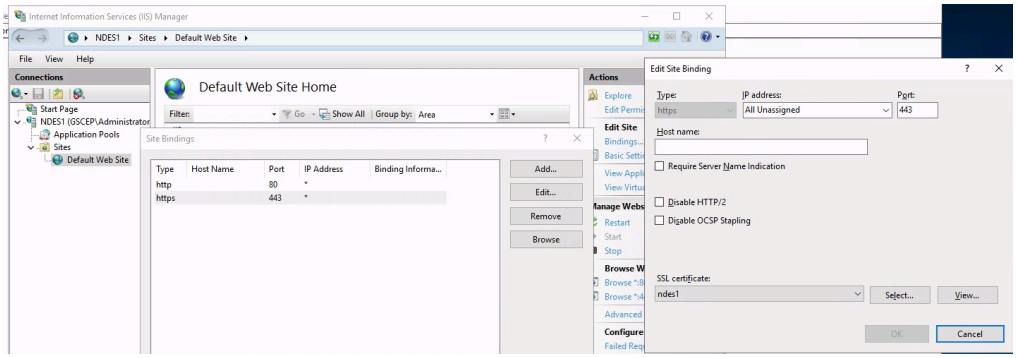
a. *`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\UseSinglePassword`*

b. Set value of *`UseSinglePassword`* to 1

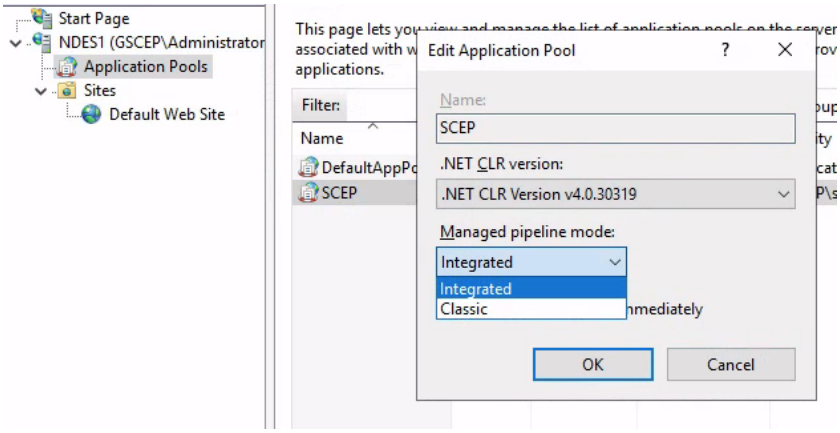


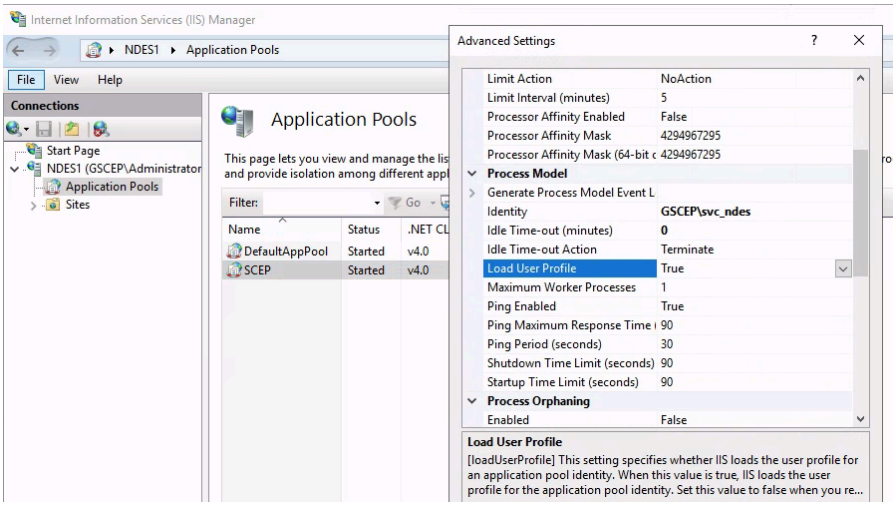
6. Bind SSL server certificate in IIS
    a. *Note that this step applies only if GCCC will be installed on a separate server.*

    b. *IIS Manager → Sites → Default Web Site*
    c. In the Actions pane, select *Bindings*
    d. Add or select *https* on port *443*
    e. Choose certificate with host name - **ndes1.gscep.net -** in *SSL certificate* list
    f. Note: If a certificate is not present, please follow standard vendor instructions for obtaining and installing an SSL certificate for your NDES IIS server. Make sure that the Subject of the SSL certificate matches the FQDN of the NDES server (**ndes1.gscep.net)** and the hostname used in the SCEP URL. Also be sure to obtain the signing certificates in the path, including the Root CA.



7. Configure IIS the application pool
    a. IIS Manager → Application Pools → *SCEP*
    b. Managed pipeline mode: ***Integrated***
    c. Note: this is necessary for authorization of NDES service with the service account

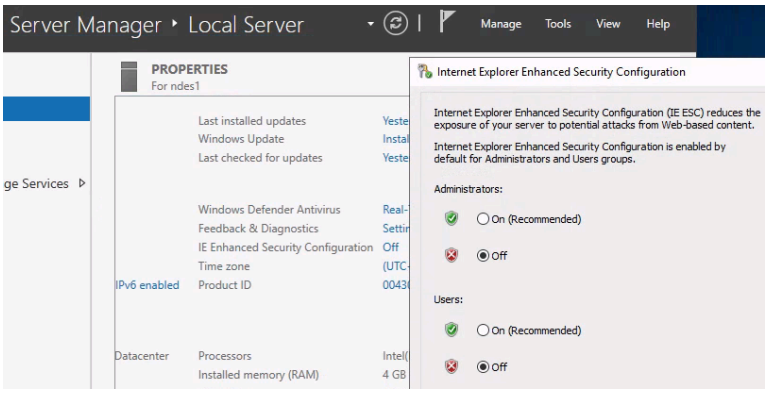


8. Enable IIS SCEP Application Pool Load User Profile
    a. Note: This step is necessary to enable the use of a static SCEP challenge password
    b. IIS Manager → Application Pools → *SCEP* → *Advanced Settings* → *Load User Profile* → ***True***
    c. 

9. (Optional) Adjust IIS Request Filtering parameters
    a. *Note that this step applies only if request filtering is enabled on IIS and/or there are URI Request too long errors* per Microsoft recommendations
    b. IIS manager → Default Web Site > Request Filtering > Edit Feature Setting
    c. *Maximum URL length (Bytes)* = **8096**
    d. *Maximum query string (Bytes)* = **8096**
    e. OR Run the following command as Administrator:
        i. `c:\windows\system32\inetsrv\appcmd.exe set config -section:system.webServer/security/requestFiltering /requestLimits.maxQueryString:"8096" /commit:apphost`

10. Disable Internet Explorer Enhanced Security Configuration

a. Server Manager → Local Server → *IE Enhanced Security Configuration: **Off***



11. (Optional) Set the SPN of the NDES Service account

a. *Note that this step applies only if multiple NDES instances are used behind a load balancer.*

b. Open Administrator elevated prompt and run command

c. `setspn -s http/<DNS name of the computer that hosts the NDES service> <Domain name>\<NDES Service account name>`

d. Example

i. `setspn -s http/ndes1.gscep.net gscep\svc_ndes`

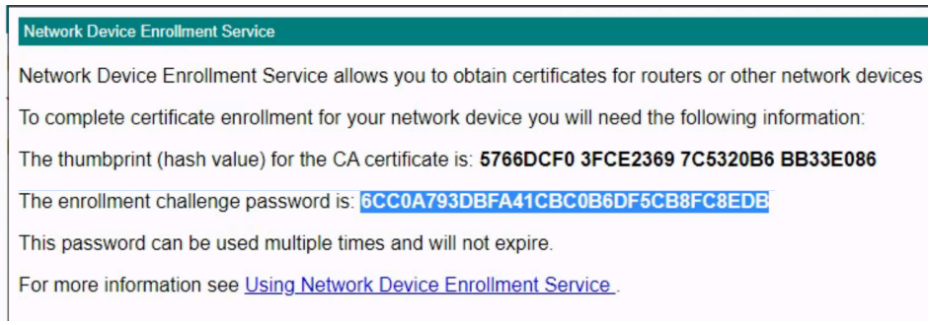
12. Restart NDES Server

13. Retrieve SCEP Challenge

a. Open ***incognito*** browser window to http://**ndes1.gscep.net**/certsrv/mscep_admin

b. Sign in using **svc_ndes** account.

c. Copy the enrollment challenge ***password*** without any leading or trailing spaces and record securely.



14. (Optional) Configure Windows Firewall

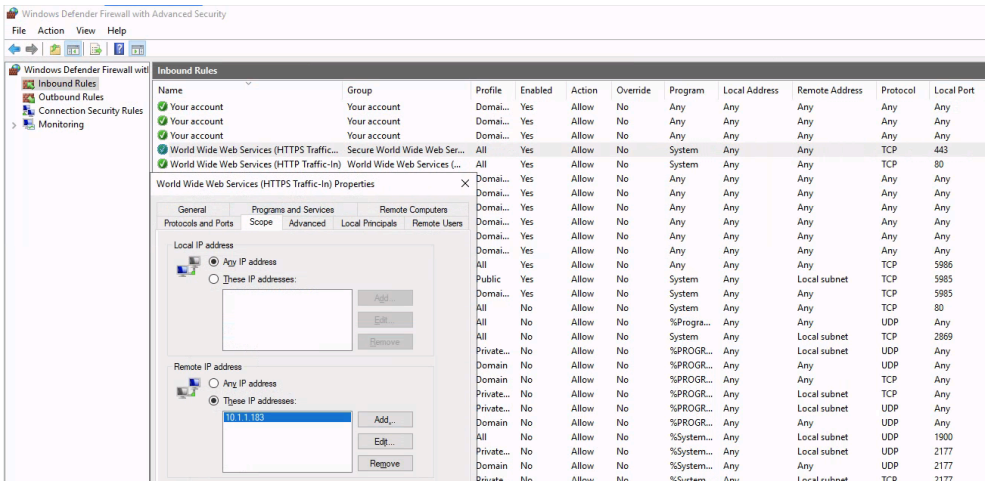
a. Open *Windows Firewall Advanced Settings → Inbound Rules*

b. Locate 2 Rules named *World Wide Web Services HTTP/S Traffic In*

c. For both, modify *Scope* → *Remote Addresses*

i. Select These IP Addresses

ii. Add IP of server running GCCC - **gccc1.gscep.net**



15. (Optional) Configure NDES to only use Kerberos for authentication

a. Open IIS Manager → Default Web Site → Authentication → Windows Authentication → **Enabled**

b. Windows Authentication → Providers

c. Remove **NTLM**

d. Remove **Negotiate**

e. Add **Negotiate:Kerberos**

f. Windows Authentication → Advanced settings

g. Enable Kernel-mode authentication → **Unchecked**

h. Extended Protection → **Accept**

16. (Optional) Configure NDES to utilize a dynamic SCEP challenge password

a. `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\UseSinglePassword`

b. Set value of `UseSinglePassword` to `0`

c. `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\PasswordMax`

d. (Optional) Set value of `PasswordMax` to `32` (decimal: 50)
Note: This increases the maximum number of unique, unused SCEP challenge passwords

that the Network Device Enrollment Service (NDES) can generate and keep in its cache, which helps smooth out the deployment of certificates

Configure Google Cloud Project

1. Enable the Chrome Management API
    a. Search for “Chrome Management API”
    b. Click on “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
        ii. Add a default subscription → **Checked** (alternatively, a non-default subscription can be created later)
        Note: You can customize the topic attributes.
3. Grant Pub/Sub Publisher role to Google’s SA
    a. Grant the "Pub/Sub Publisher" role to "**cert-provisioning-api-pubsub-publisher@system.gserviceaccount.com**". The latter is the well-known service account which Google's backend infrastructure will use to publish messages to the Pub/Sub topic. If Domain Restricted Sharing is enforced for your domain, you will have to follow these instructions to exempt the service account from the policy.
4. Create a GCP Service account for the Connector
    a. Hamburger menu → IAM & Admin → Service accounts
    b. Click on **Create service account**
    c. Give a descriptive service account name and a description
    d. Click on **Create and continue**
    e. Add roles:
        i. Pub/Sub Subscriber
    f. Optional: To grant more granular roles, specify the Pub/Sub topic and subscription as a resource in the IAM condition for this service account
    g. Click **Done**

chrome enterprise

Configure Google Admin and Google Cloud Certificate Connector

To install a certificate, configure a SCEP or generic profile and its corresponding CA connection and configuration on the GCCC.

(Option A) Create a SCEP configuration

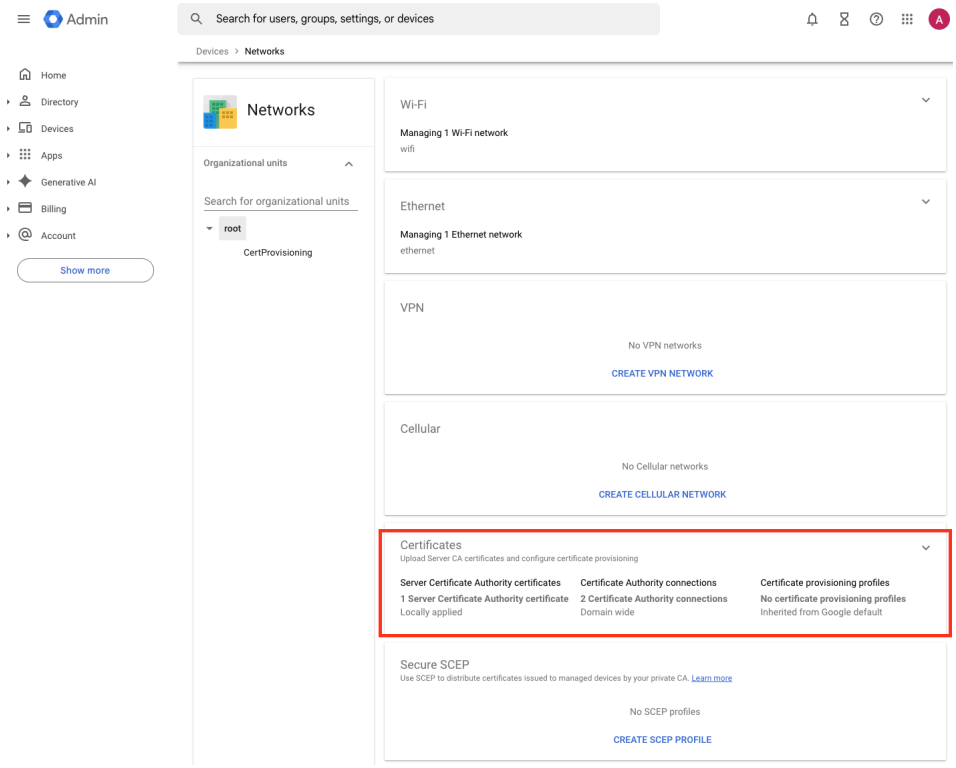
1. Create a SCEP Certificate Authority connection

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 GCCC 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 GCCC's local configuration (ca_connection_config_id).

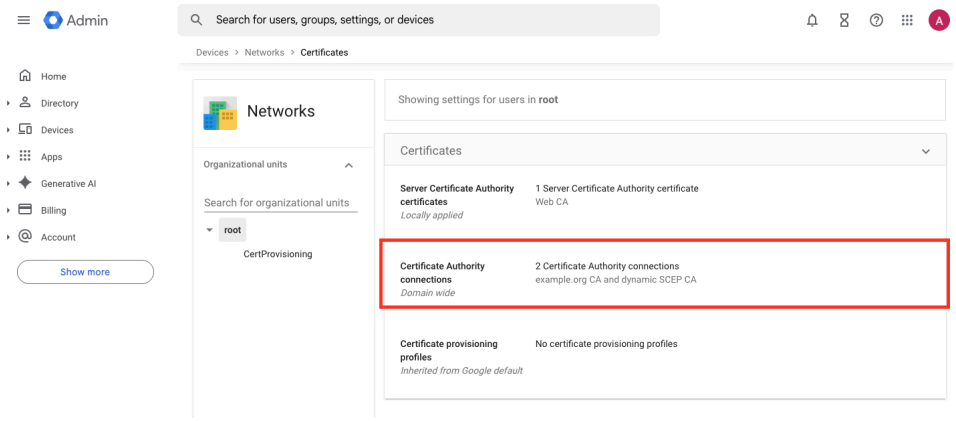
a. Sign in to the Google Admin console. Learn more

b. *Devices* → *Networks*
Requires having the Shared device settings administrator privilege.

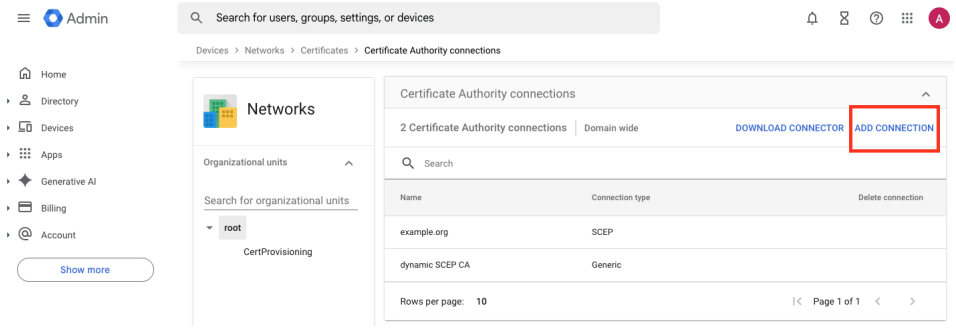
c. Scroll down to *Certificates*



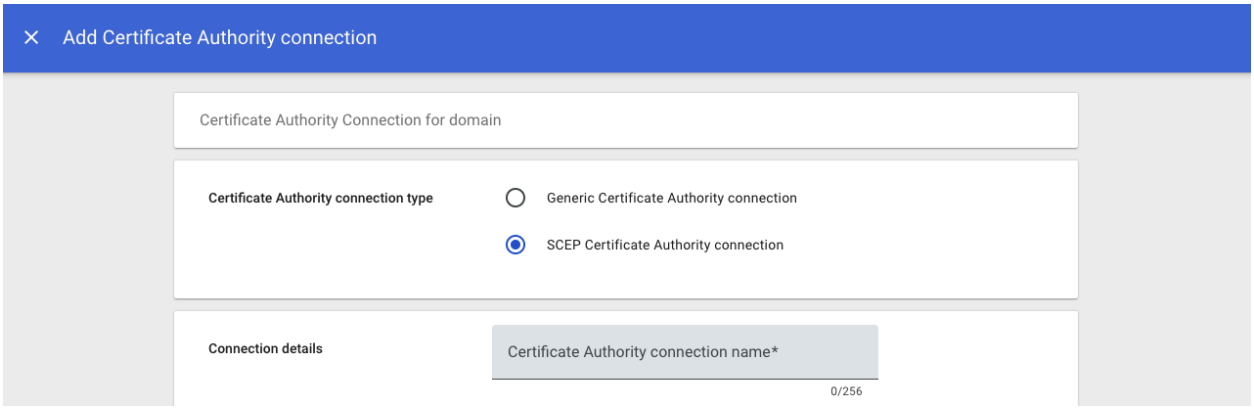
d. Click on Certificate Authority Connections



e. Click on **Add Connection**



f. *SCEP Certificate Authority connection* → **Selected**



g. Enter a Certificate Authority connection name

h. Enter the email address of the GCP service account (typically in the format **account-name@project-id.iam.gserviceaccount.com**) you created previously for the Google Cloud Certificate Connector (GCCC). This account typically has the "Pub/Sub Subscriber" role

i. Enter the Pub/Sub topic that contains a subscription a GCCC listens to (created earlier)

j. Enter a Certificate Authority connection configuration identifier. This identifier will be used by the GCCC to load a local configuration. The configuration will be created later in the "configure the GCCC" step

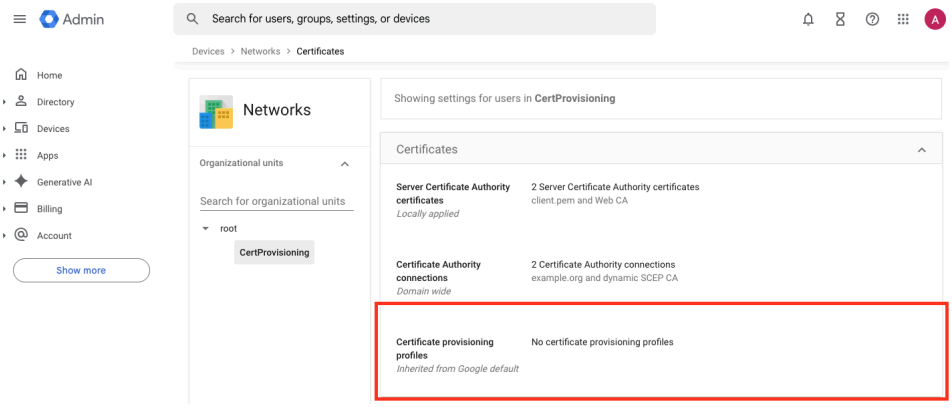
k. Click **ADD**

2. Create a *SCEP Profile Configuration*

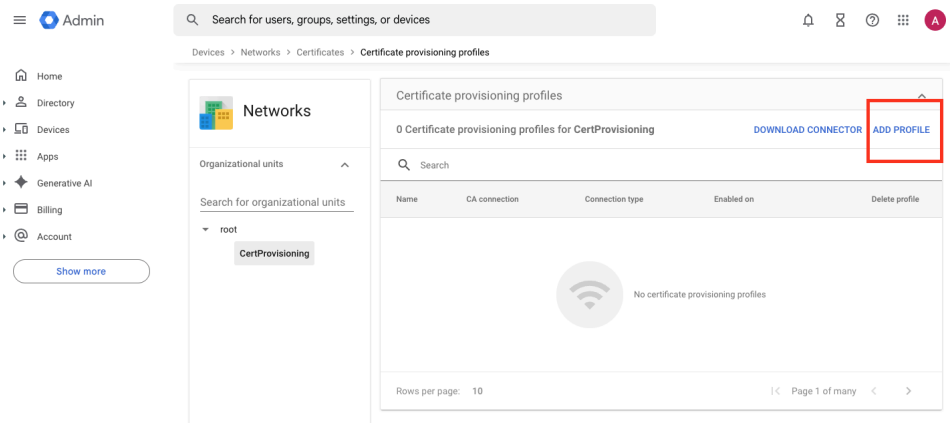
a. Go back to the Certificates page

b. Select a child organizational unit if desired

c. Click on the *Certificate provisioning profiles*



d. Click on Add Profile



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

f. Select whether this profile applies for a user or device

g. For *the profile name*, enter a descriptive name, shown in the list of profiles

h. Enter the *renewal period* (in days before expiration) as desired

i. The authentication type of *remote attestation forces* a Verified Access check that the device and user are affiliated (managed by the same domain) before issuing a

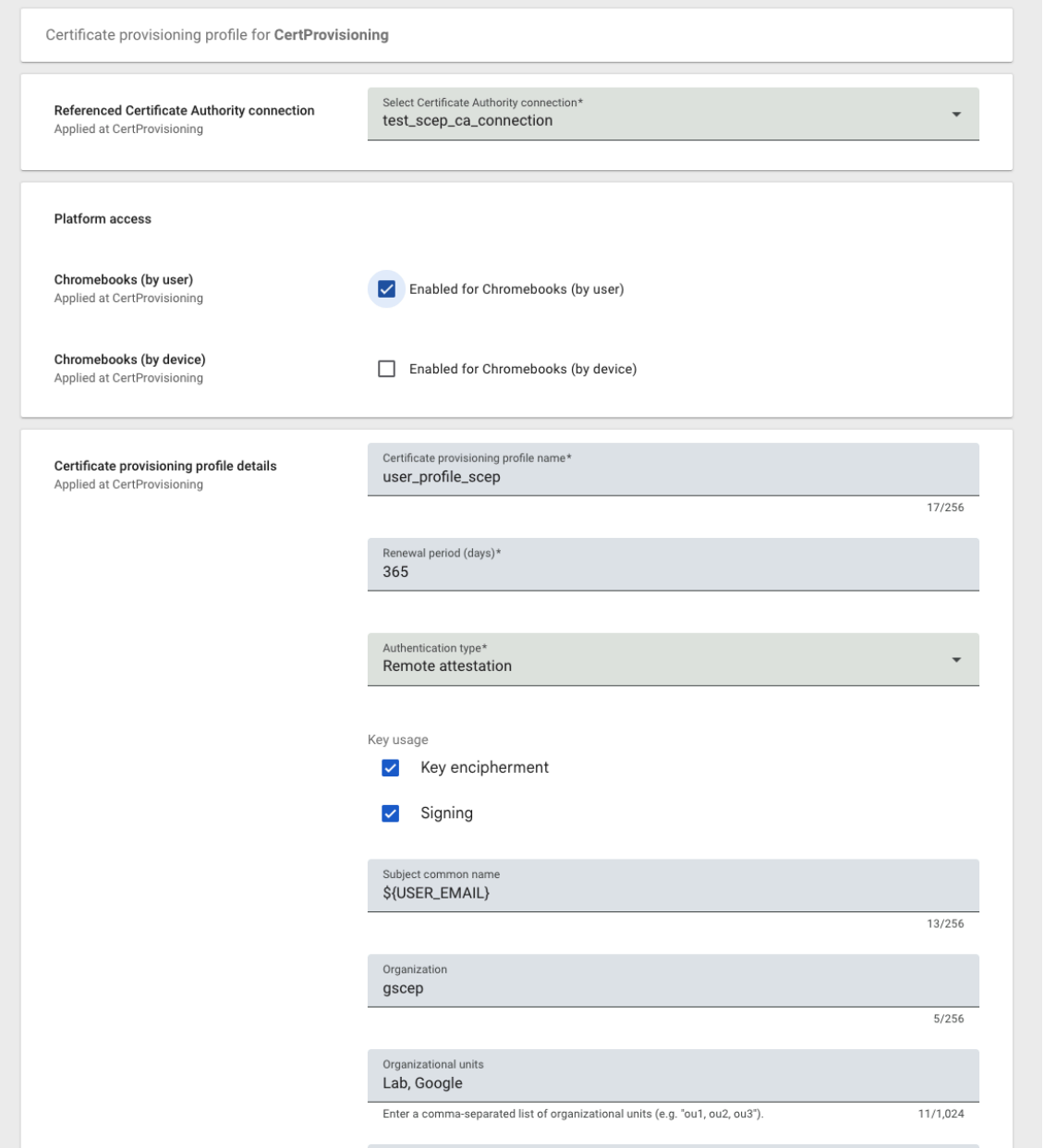
certificate and that the device is legitimate. *None* allows unmanaged and ChromeOS Flex devices.

j. For Key usage, choose the options for how the key will be used (key encipherment and signing). You can select more than one; typically, both are used.

k. Enter a *subject name*, a *subject alternative name*, or both. Placeholder variables can be used. For example, enter **${USER_EMAIL}** for Common name to automatically add the current user's User Principal Name (UPN) to the certificate request. For device certificates, **${DEVICE_SERIAL_NUMBER}** can be used as Common name. For the full list about the variables that you can use, see the placeholder list in the "Use the GCCC HC article")

l. Build a Relative Distinguished Name (RDN) for the subject name using relevant attributes from a Fully Distinguished Name (e.g., common name, organization, organizational units).

m. **If the certificate needs to include a country code, it must be standards compliant - e.g. US**



n. For Subject Alternative Names (SANs), enter the desired number of SANs

   i. Click on the + sign

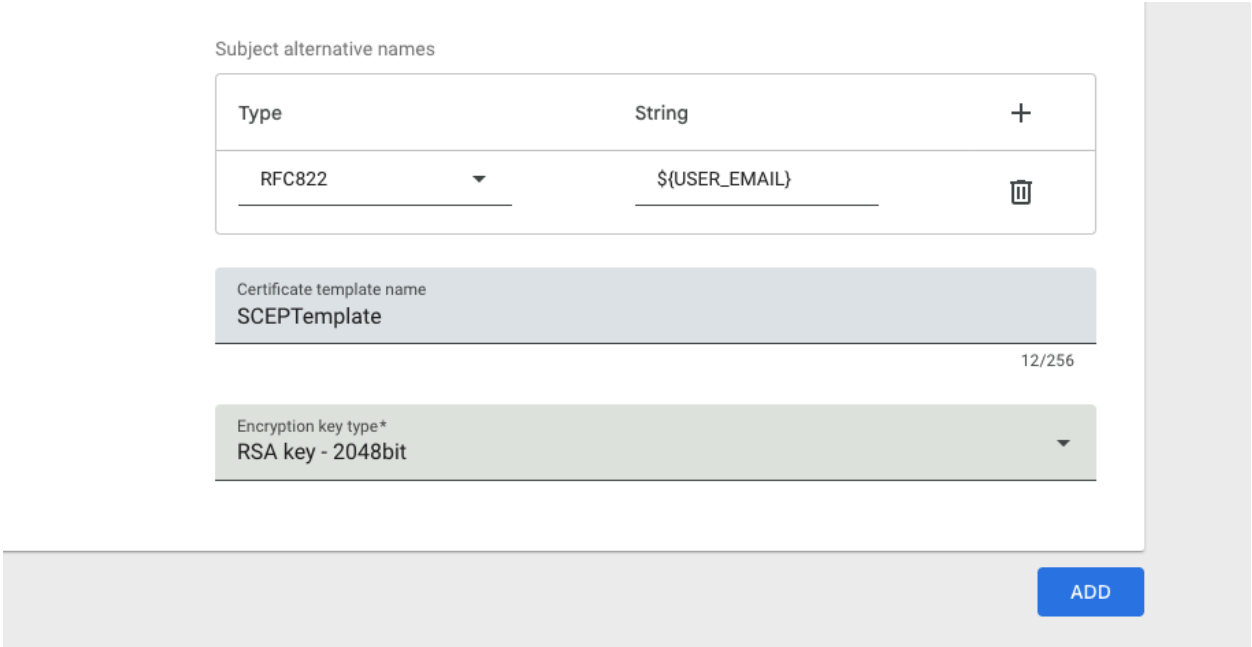
   ii. For *Subject alternative name type*, select ***RFC822***
   Note: The *Subject alternative name type* is dependent on the RADIUS server in use for WiFi client authentication. E.g. Cisco ISE uses RFC822 Email field

   iii. For String, enter ***${USER_EMAIL}***

   iv. Be sure not to add blank space before or after the variable name

o. Enter the CA template name. This name should correspond to a template name configured on the CA. The template created in this guide was named SCEPTemplate

p. Choose the required key type (RSA or ECC). ECC is recommended due to its



performance, unless you need to use static SCEP, then we recommend RSA

q. Click **ADD**

3. Configure Google Cloud Certificate Connector (for SCEP configuration)

a. Download Google Cloud Certificate Connector

   i. Sign in to the Admin console

   ii. Open ***Devices → Networks***
   Note: Requires having the Shared device settings administrator privilege.

iii. Scroll down to **Certificates → Certificate Authority connections**

iv. Click **Download connector**

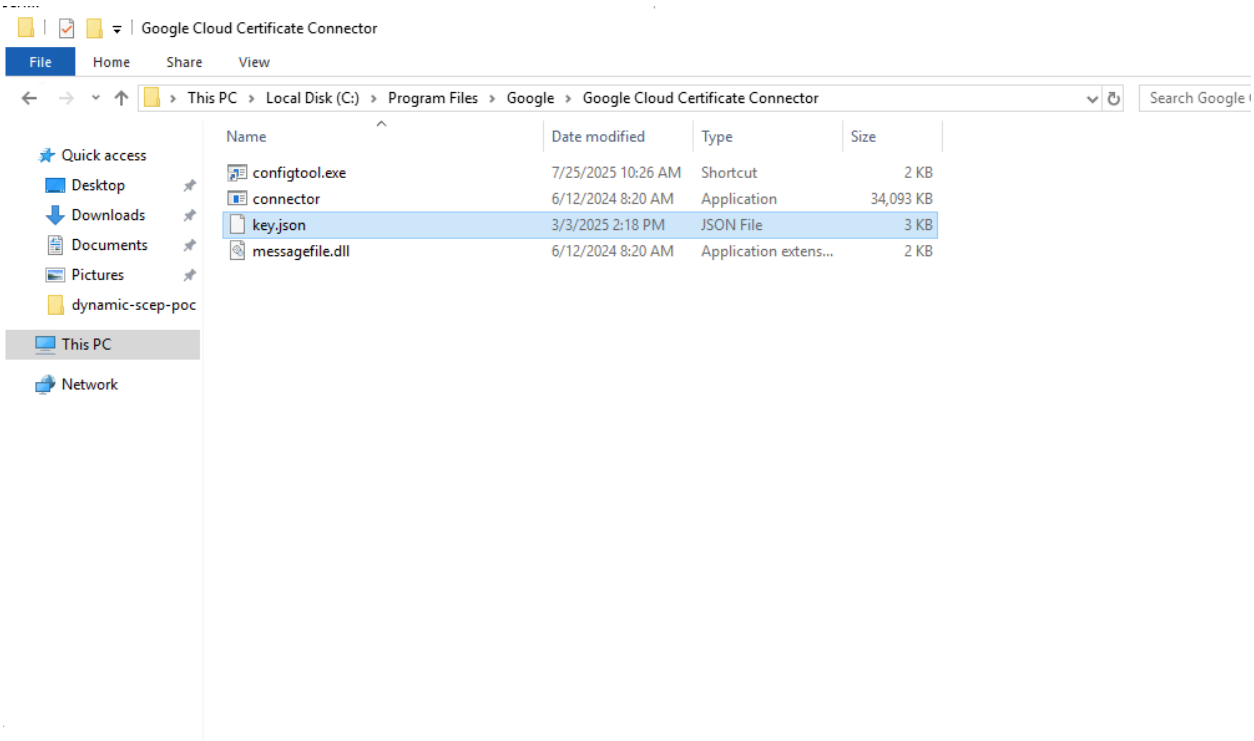
b. Install Google Cloud Certificate Connector installer
Note: If your network requires a proxy, see the "Auto Update Proxy Settings" FAQ as the installer will depend on this process

i. Run the ***connector_installer.exe*** as an administrator
Note: The installer will register the connector service with default credentials (LocalService). The service can be later changed to run as a different service account if desired, by launching the ConfigTool from the executable shortcut named **configtool.exe** found in the same installation directory as the connector

c. Download the service account key json file

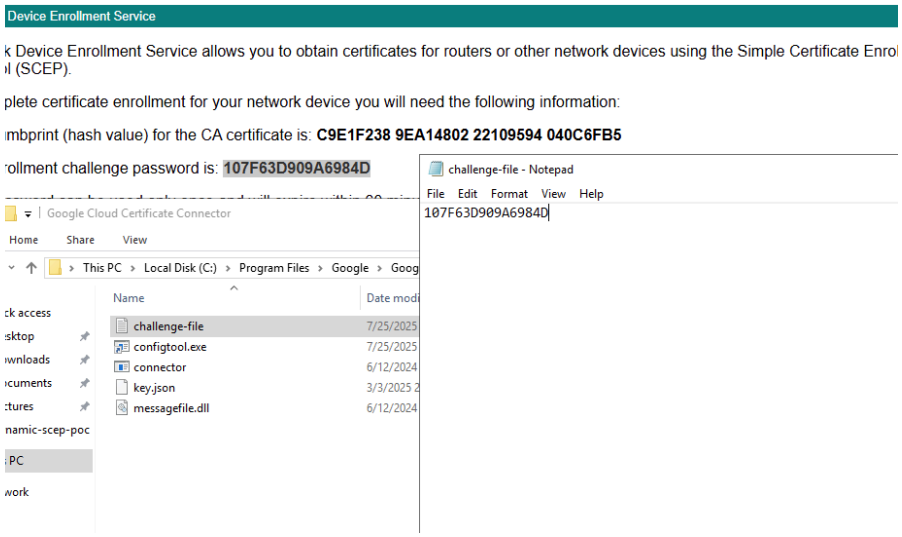
i. From GCP go to Service Accounts → click on the service account created earlier for the GCCC → goto **Keys** → Click **Add Key** → **Create a new Key** → **JSON** → **Create**

ii. Move the downloaded **key.json** file to the GCCC installation folder



d. Create an empty file and paste the challenge retrieved from the NDES ***/mscep_admin*** page (step 13). Name the file "*challenge-file.txt*". Note: The file name can be customized. The name will be given as a parameter in the GCCC

configuration at a later step



e. Create a json file with the name "**adapter_config.json**"

f. Populate the "adapter_config.json" with the following JSON object (replace the values between the <> symbols)
Note: Ensure that the *ca_connection_config_id* **matches** the *Certificate Authority connection configuration identifier* entered in the Certificate Authority connection previously created on the admin console

JSON

```
{
  "adapter_configuration": {
    "request_subscriptions": [
      "projects/<projectid>/subscriptions/<subscriptionid>"
    ],
    "key_filename": "key.json"
  },
  "ca_configurations": [
    {
      "type": "SCEP",
      "ca_connection_config_id": "<Certificate Authority connection
configuration identifier>",
      "ca_endpoint_url": "<SCEP endpoint>",
      "challenge_filename": "challenge-file.txt"
    }
  ]
}
```

Note: this is a minimal configuration. For the full list of supported configurations check the full parameter list section in the GCCC help center article.

g. Open the services list

h. Find "*Google Cloud Certificate Connector*" service

i. Start the service

(Option B) Create a Generic configuration

Note: With generic configuration, most settings are loaded locally from the GCCC configuration file. Only attributes related to the configuration identifier are entered in the admin console.

1. Create a *Generic Certificate Authority connection*

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

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

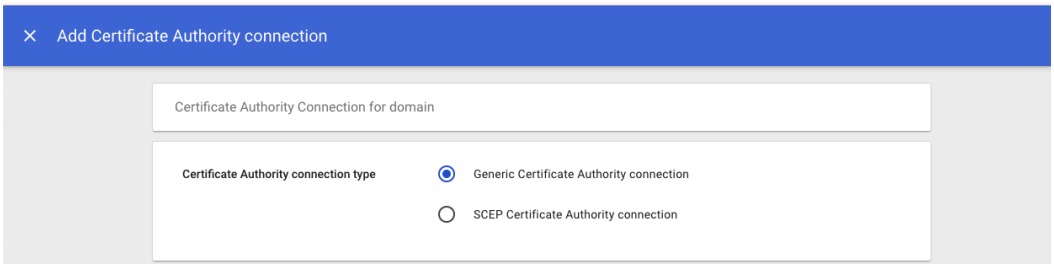
   b. *Devices* → *Networks*
   Requires having the Shared device settings administrator privilege.

   c. Scroll down to *Certificates*

   d. Click on Certificate Authority Connections

   e. Click on **Add Connection**

   f. Generic Certificate Authority connection → **Selected**



   g. Enter a Certificate Authority connection name

   h. Enter the email address of the GCP service account (typically in the format **account-name@project-id.iam.gserviceaccount.com**) you created previously for the Google Cloud Certificate Connector (GCCC). This account typically has the "Pub/Sub Subscriber" role

   i. Enter the Pub/Sub topic that contains a subscription a GCCC instance listens to (created earlier)

   j. Input a Certificate Authority connection configuration identifier. This identifier must match the `ca_connection_config_id` value within the GCCC CA configuration to ensure that the GCCC loads the correct local configuration. The GCCC configuration will be created later in the "configure the GCCC" step

   k. Click **ADD**

2. Create a *Generic Profile Configuration*

   a. Go back to the Certificates page

   b. Select a child organizational unit if desired

   c. Click on the *Certificate provisioning profiles*

   d. Click on Add Profile

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

   f. Select whether this profile applies for a user or device

   g. For *the profile name*, enter a descriptive name, shown in the list of profiles

   h. Input a Certificate provisioning profile config reference. This identifier must match the `profile_config_id` value within the GCCC profile configuration to ensure that the GCCC loads the correct local configuration. The GCCC configuration will be created later in the "configure the GCCC" step

   i. Enter the *renewal period* (in days before expiration) as desired

   j. The authentication type of *remote attestation forces* a Verified Access check that the device and user are affiliated (managed by the same domain) before issuing a certificate and that the device is legitimate. *None* allows unmanaged and ChromeOS Flex devices

   k. Choose the required key type (RSA or ECC). ECC is recommended due to its performance, unless you need to use static SCEP, then we recommend RSA

   l. Click ADD

3. Configure Google Cloud Certificate Connector (for Generic configuration)

   a. Download Google Cloud Certificate Connector

      i. Sign in to the Admin console

      ii. Open ***Devices*** → ***Networks***
      Note: Requires having the Shared device settings administrator privilege.

      iii. Scroll down to **Certificates** → **Certificate Authority connections**

      iv. Click **Download connector**

   b. Install Google Cloud Certificate Connector installer
   Note: If your network requires a proxy, see the "Auto Update Proxy Settings" FAQ as the installer will depend on this process

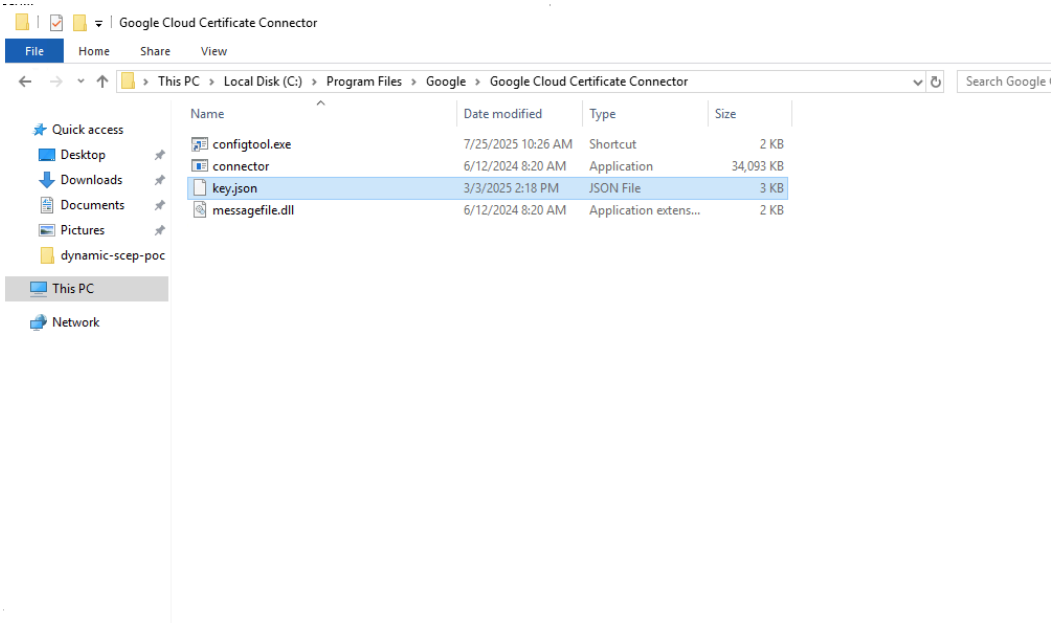
      i. Run the ***connector_installer.exe*** as an administrator
      Note: The installer will register the connector service with default credentials (LocalService). The service can be later changed to run as a different service

account if desired, by launching the ConfigTool from the executable shortcut named **configtool.exe** found in the same installation directory as the connector

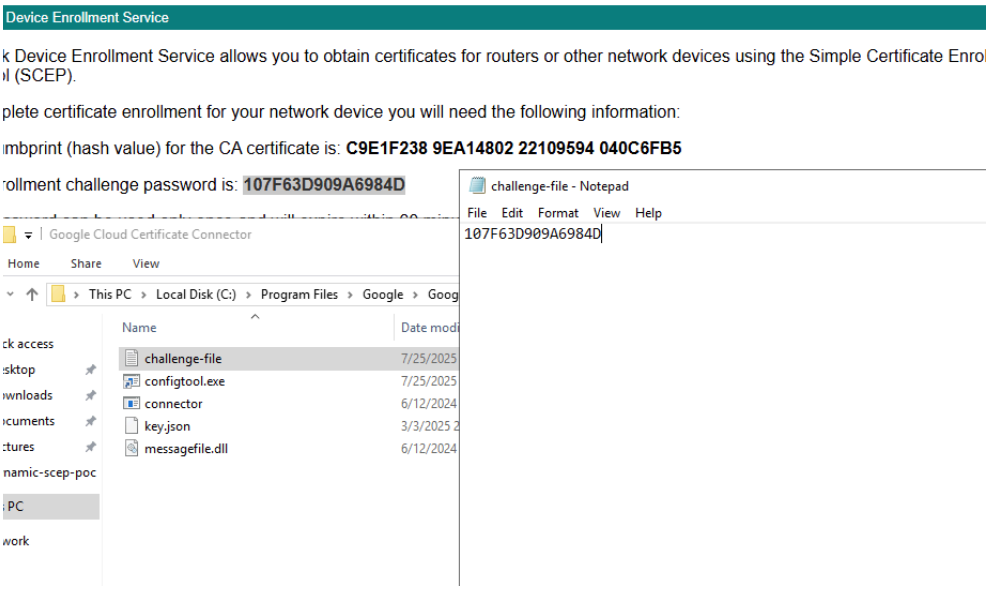
c. Download the service account key json file

   i. From GCP go to Service Accounts → click on the service account created earlier for the GCCC → goto **Keys** → Click **Add Key** → **Create a new Key** → **JSON** → **Create**

d. Move the downloaded **key.json** file to the GCCC installation folder



Create an empty file and paste the challenge retrieved from the NDES ***/mscep_admin*** page (step 13). Name the file "*challenge-file.txt*". Note: The file name can be customized. The filename will be passed as a parameter in the GCCC configuration in a later step



e. Create a json file with the name "**adapter_config.json**"

Populate the “adapter_config.json” with the following JSON object (replace the values between the <> symbols)
Note: Make sure that the profile_config_id and ca_connection_config_id matches the references entered in the admin console

JSON

```
{
  "adapter_configuration": {
    "request_subscriptions": [
      "projects/<projectid>/subscriptions/<subscriptionid>"
    ],
    "key_filename": "key.json"
  },
  "profile_configurations": [
    {
      "profile_config_id": "<Certificate provisioning profile config
reference>",
      "subject_name": {
        "common_name": "${USER_EMAIL_NAME}"
      },
      "key_usages": ["SIGNING","KEY_ENCIPHERMENT"],
      "template_name": "SCEPTemplate",
      "signature_algorithm": "RSA_SHA256"
    }
  ],
  "ca_configurations": [
    {
      "type": "SCEP",
      "ca_connection_config_id": "<Certificate Authority connection
configuration identifier>",
      "ca_endpoint_url": "<SCEP endpoint>",
      "challenge_filename": "challenge-file.txt"
    }
  ]
}
```

Import NDES Server Certificate into GCCC Keystore (Only for HTTPS)

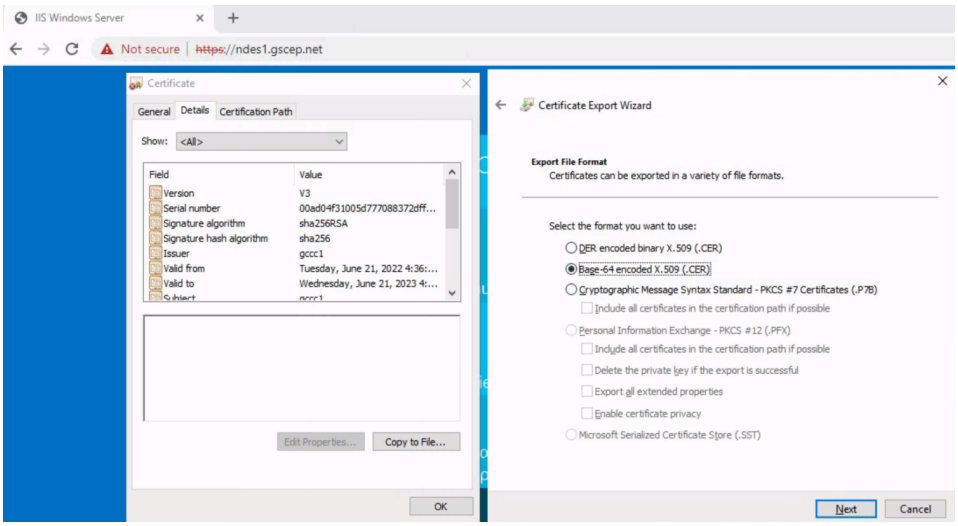
a. Download the Certificate from NDES server

   i. Open a browser window to the HTTPS URL of the NDES server: ***https://ndes1.gscep.net***

   ii. View site certificate

   iii. Details → Copy to file

iv. Select ***Base 64***



v. Save in a convenient location

b. Import NDES IIS server certificate into windows trusted root CA store

(Optional) Configure GCCC and admin console for dynamic SCEP

1. Prerequisites

For the GCCC to work with dynamic SCEP challenge passwords, optional steps 11 (set the SPN of the NDES service account) and 15 (configure NDES to only use Kerberos for authentication) are required

2. (Recommended) Create a separate Service Account (SA) for the Google Cloud Certificate Connector to run as

This account will be given permissions to access the mscep_admin page

a. Create a new service account

i. On the domain controller, open Active Directory Users and Computers

ii. Select Users under the configured domain

iii. Right click → New → User

iv. Enter a logon name (connectorsvc for example)

b. Grant "Log on as a service" permission

i. On the machine that will run the GCCC, open Local Security Policy

ii. Local Policies → User right assignment → Log on as a service → Properties → Add User or Group → Add

iii. Enter the SA name created in the previous step

iv. Click OK

c. Grant the Connector's SA *"read"* permission on the CA template

i. Open the certification authority as domain administrator (not local administrator)

ii. Under the CA name → Certificate Templates → right click → manage → find the template created earlier (Should be the same name in the mscep/ registry key)

iii. Right click on the CA template → properties → security → Add → enter the Connector's SA name → OK

iv. Make sure that the Connector SA has "Read" permission

3. Change the GCCC service log on credentials

a. Run the configtool.exe shortcut found in the GCCC installation directory as an administrator

b. Enter "y" for overwriting the existing config

c. Enter the service account name created in step. 2 prefixed by the domain name and a "\" (for example: "EXAMPLE\connectorsvc")

d. Enter the password

e. Press the enter key to skip the later options

4. Generate a kerberos Keytab file based on the Connector's SA

This Keytab file enables the Connector service to authenticate with the SA without requiring a password.

a. In the Connector's installation directory open an Administrator powershell (domain Admin)

b. Change directory to the GCCC installation directory

Generate the Keytab file by running the following command, the service-account used here should be the one created for the Connector:

```
None
ktpass /princ <service-account>@<DOMAIN> /ptype KRB5_NT_PRINCIPAL /mapuser
<service-account> /pass * /out <service-account>.keytab /crypto all -mapOp set
/target <domain controller fully qualified domain name>
```

This command prompts for the password of the Connector's Service Account (SA). If the entered password differs, the command will update the SA's password to the one provided.

Note: Access to this file grants access to the SA credentials. Therefore, only grant access to accounts that require it.

c. Right click the Keytab file → properties → security → advanced → disable inheritance → Remove users group → add → enter the Connector's SA

5. Create and configure a Kerberos configuration file
    i. Create a new file called kerb.conf (the name can be anything)
    ii. Populate the Kerberos configuration file. The full list of parameters is here. The most important part of the configuration is the [realms] section, particularly, the Key distribution center (*kdc*) address which is usually the fully qualified domain name of the domain controller
    iii. An example of a valid configuration for a domain name "EXAMPLE.ORG"

```
None
[libdefaults]
default_realm = EXAMPLE.ORG
ticket_lifetime = 24h
forwardable = yes
default_tkt_enctypes = aes256-cts-hmac-sha1-96
default_tgs_enctypes = aes256-cts-hmac-sha1-96
noaddresses = false

[realms]
EXAMPLE.ORG = {
kdc = <DomainController>.example.org
admin_server = <DomainController>.example.org
default_domain = example.org
}

[domain_realm]
.example = EXAMPLE.ORG
example = EXAMPLE.ORG
```

Note: the realms name should be in capital letters

6. Add a GCCC CA configuration

Add the following CA configuration object to the list of existing CA configurations in the GCCC configuration file ("adapter_config.json")

Note: Keep the ca_connection_config_id from this configuration in mind, as you will need it later for the CA connection created in the Admin console

```
None
    {
      "type": "SCEP",
      "ca_connection_config_id": "<Certificate Authority connection
configuration identifier>",
      "ca_endpoint_url": "<SCEP endpoint>",
     "dynamic_challenge": {
        "challenge_endpoint_url": "<SCEP challenge endpoint>",
```

```
    "kerberos": {
      "config_filename": "kerb.conf",
      "keytab_filename": "<service-account>.keytab",
      "realm": "<DOMAIN>",
      "username": "<service-account>",
      "server_spn": ""
    }
  }
}
```

7. Create a Profile and CA connection that references the dynamic SCEP configuration (using the *"ca_connection_config_id"* value)

    a. On the Admin console, create a new SCEP/generic certificate authority connection and a corresponding profile. Ensure the `ca_connection_config_id` value is referenced in the certificate authority connection configuration identifier attribute

Import EAP-TLS RADIUS server certificate

1. Obtain the TLS Server Certificate from the RADIUS server being used to authenticate 802.1X WI-FI clients

    a. E.g. for Cisco ISE - Administration → System → Certificates, choose the certificate *Used By* ***EAP Authentication*** and Export. Save as a ***.CER*** file i.e. ***cisco-ise.cer***

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

3. *Devices* → *Networks*
   Requires having the Shared device settings administrator privilege.

4. Scroll down to *Certificates*

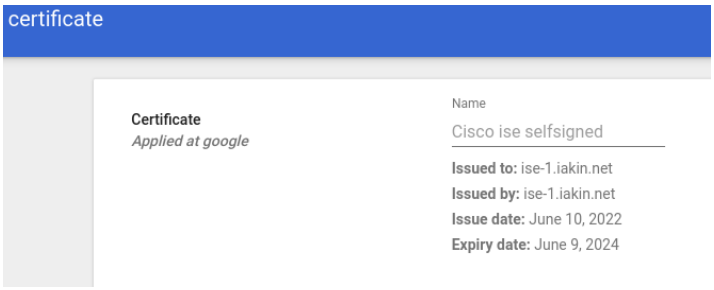
5. Select a child organizational unit if desired

6. Click *ADD CERTIFICATE*

7. Click *Upload*, select the RADIUS Server certificate - ***cisco-ise.cer***

    a. Check the *Issued to* and *by* to make sure it is the correct certificate

    b. Use a descriptive *Name* - **Cisco ISE Certificate**



Configure Wi-Fi profile

1. Sign in to the Google Admin console. Learn more
2. *Devices → Networks → WI-FI*
   Requires having the Shared device settings administrator privilege.
3. Click *ADD WI-FI*
4. ChromeOS devices can authenticate to a network without a user signed in - under *Platform Access* select *Chromebooks (by device),* otherwise the device will only connect to this Wi-Fi once a user signs in - *Chromebooks (by user)*.

a. In the *Details* section, set the following:

   i. Add the *Name (display)* and *SSID*

   ii. Check *Automatically connect* if desired

   iii. For *Security type*, select ***WPA/WPA2/WPA3 Enterprise (802.1 X)***

   iv. For the *Extensible Authentication Protocol*, select ***EAP-TLS***

   v. For *Maximum TLS Version*, select ***1.2***

   vi. For Username, enter ***${LOGIN_ID}***.

   vii. For Server certificate authority, choose the name of the RADIUS TLS Certificate imported earlier - **Cisco ISE Certificate**

   viii. Enter an issuer and/or subject pattern to match the certificate that should be presented when using Wi-Fi. For example:

WPA/WPA2/WPA3 Enterprise (802.1X)

ChromeOS devices that have a Marvell Wi-Fi chipset don't support WPA3. Learn more

Extensible Authentication Protocol

EAP-TLS

Maximum TLS Version

1.2

Username

${LOGIN_ID}

Server Certificate Authority

System default certificate authorities

Non-default secure server certificate is required for Android 13 or newer

Server Certificate Domain Suffix Match

Enter one domain name constraint (suffix) per line.
Required for Android 13 or newer.

SCEP profile

None

Client enrollment URLs

Issuer pattern

Common name

ise-1

Locality

BV

Organization

Cisco

Organizational unit

Subject pattern

Common name

${USER_EMAIL}

Locality

NY

Organization

gscep

Organizational unit

Lab, Google

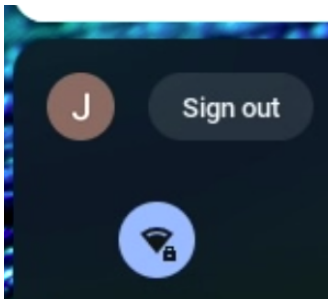
b. Click Save.

ChromeOS user experience

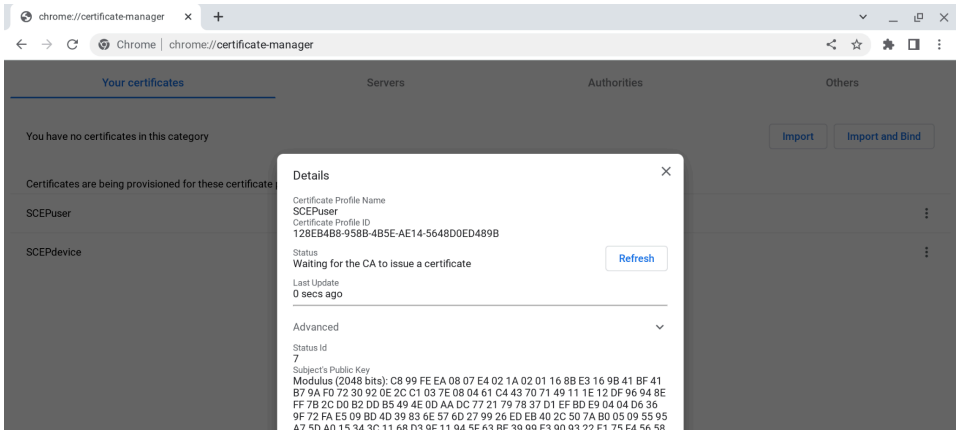
When users sign in to a managed ChromeOS device with their managed Google Account, they automatically get a user and/or device certificate. In this example, the ChromeOS device automatically connects to an EAP-TLS network using that certificate via a Cisco ISE radius server.

Note: Make sure that ChromeOS devices are in an organizational unit that your CA root cert will be pushed to and your users are in the organizational unit that you just created the SCEP and Wi-Fi profile for.

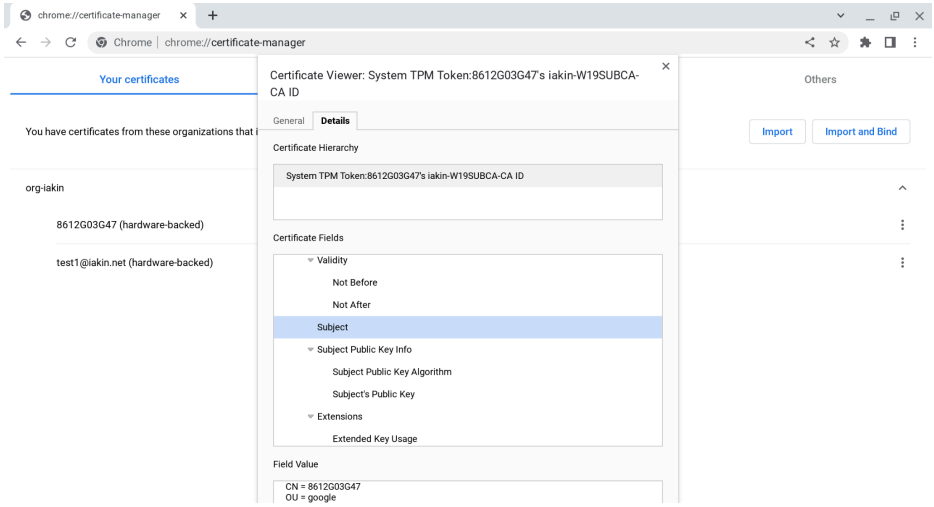
1. Managed user signs in to managed ChromeOS device.
2. At the bottom right of the ChromeOS device screen, click the time. You'll see the previous SSID used at startup.



3. Open Chrome and go to **chrome://certificate-manager**
4. Next to the request that contains the name of the SCEP profile that you just set up, click **More** . You can visually see the progress of getting the certificate, if it hasn't already completed.



5. Refresh the page. The certificate(s) should show up within 30 seconds.



6. At the bottom right of the ChromeOS device screen, click the time. You should have switched to the 802.1x Network

FAQ

Certificate renewal

Certificates are re-requested upon expiration or if they are deleted.

Certificate revocation

Certificate revocation should be handled by the PKI/CA.

GCCC Proxy Configuration

GCCC requires access to the following endpoints to install and function. If a proxy it used, it must allow access to these hosts:

https://pubsub.googleapis.com

https://oauth2.googleapis.com

https://update.googleapis.com

https://chromemanagement.googleapis.com

https://edgedl.me.gvt1.com/edgedl/release2

https://dl.google.com/release2

https://google.com/dl/release2

Troubleshooting

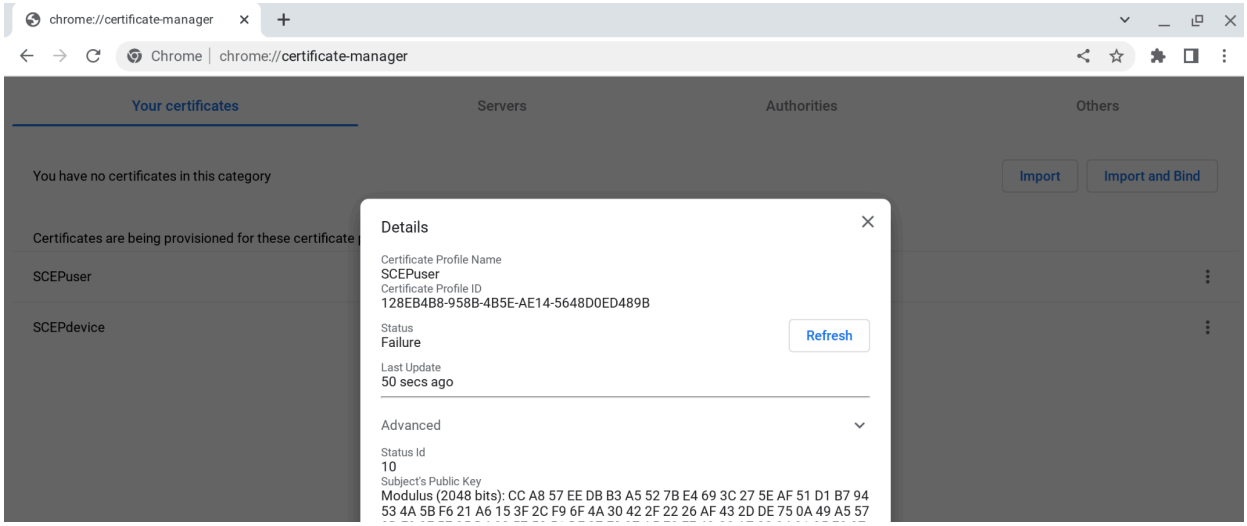
ChromeOS device

If ***chrome://certificate-manager*** does not show any entries for SCEP certificates being requested, verify that the user and/or device are assigned to the correct OU in the Admin Console, which includes appropriate user and/or device SCEP profiles.

Validate by navigating to **chrome://policy** from the ChromeOS device and make sure that the ***RequiredClientCertificateForUser*** policy and/or the ***RequiredClientCertificateForDevice*** policy are present.

If using strict mode, make sure the device is enrolled in the same domain as the user.

If a SCEP profile is assigned to the device/user, and there is a problem requesting a certificate, ***chrome://certificate-manager*** will show an error message similar to the below within the SCEP profile details:



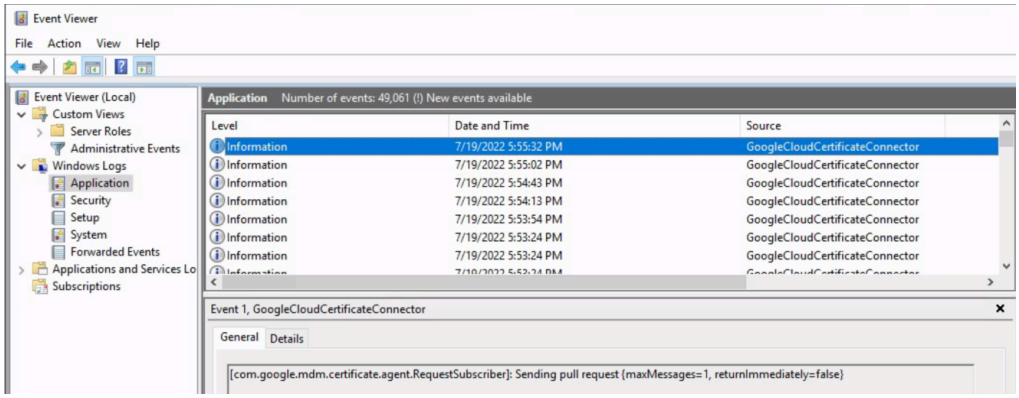
GCCC

Service Errors

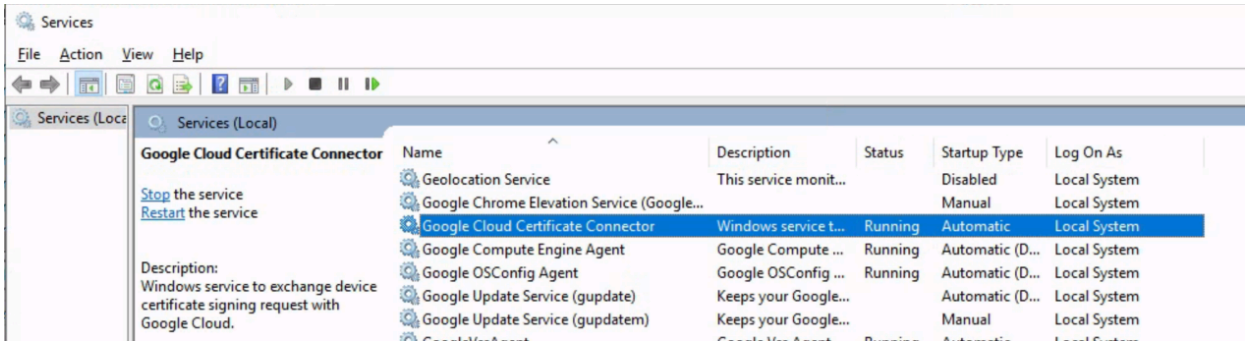
During normal operation, the following events will appear roughly every 30 seconds in Windows Application Log on the system running the GCCC Service from Source ***GoogleCloudCertificateConnector***:

```
[com.google.mdm.certificate.agent.RequestSubscriber]: Sending pull request
{maxMessages=1, returnImmediately=false}

[com.google.mdm.certificate.agent.RequestSubscriber]: Received pull response {}
```



If the events are not appearing, verify that the GCCC service is running and configured with the correct Log On As account via the Services Control Panel.

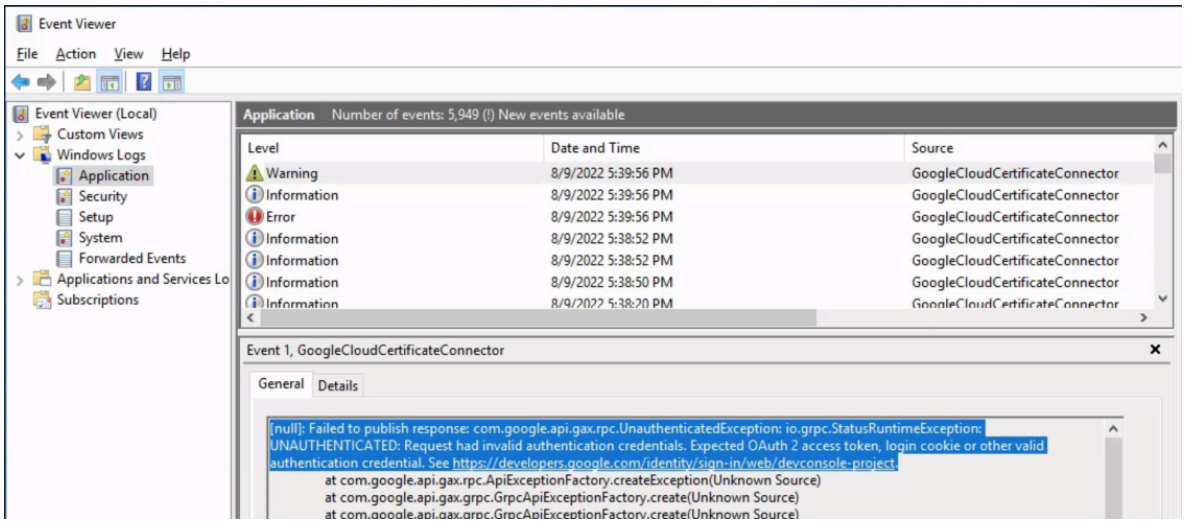


If the service fails to start repeatedly, verify that the installation steps were followed, including copying the json files to the GCCC Program directory.

If no certificate requests are being received by the connector, then check that outgoing TLS traffic to port 443 to PubSub servers is allowed (e.g. use your browser on the GCCC server to access https://pubsub.googleapis.com; a successful test should result in an error "404: Not found" page).

If an error is logged regarding Oauth, the GCCC service cannot connect to the Google cloud because the SCEP service account key credential has been invalidated. You will need to obtain or re-generate the key file re-install it and restart the GCCC service.

```
[null]: Failed to publish response: com.google.api.gax.rpc.UnauthenticatedException:
io.grpc.StatusRuntimeException: UNAUTHENTICATED: Request had invalid authentication
credentials. Expected OAuth 2 access token, login cookie or other valid
```



Enrollment Event Logs

Successful

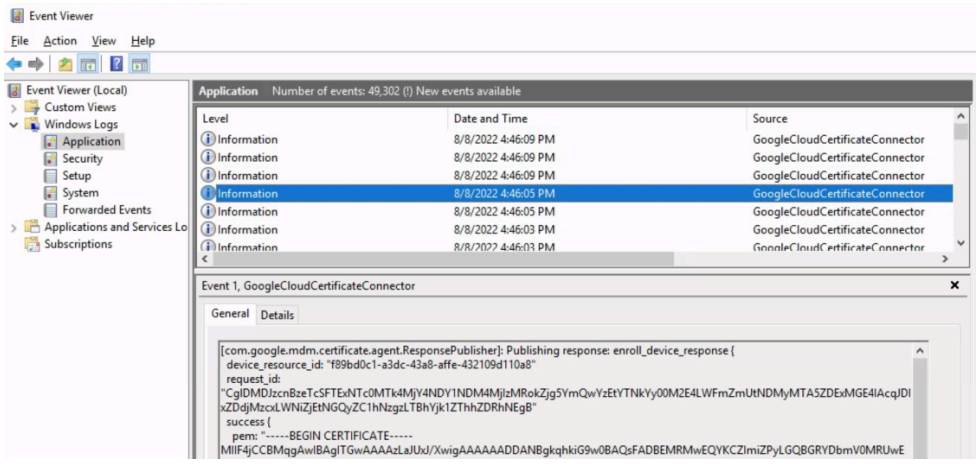
During a successful certificate enrollment, following events will be logged:

`[com.google.mdm.certificate.agent.RequestSubscriber]:` **`Received pull response`** `{"receivedMessages":[{"ackId":"UAYWLF1GSFE3GQhoUQ5PXiM_NSAoRRcJBE8CKF15MEg-...`

`[com.google.mdm.certificate.agent.RequestReceiver]:` **`Received pubsub payload:...`**

`[com.google.mdm.certificate.agent.EnrollDeviceRequestHandler]:` **`Received certificate`** `-----BEGIN CERTIFICATE-----...`

`[com.google.mdm.certificate.agent.ResponsePublisher]:` **`Publishing response:`** `enroll_device_response {...`



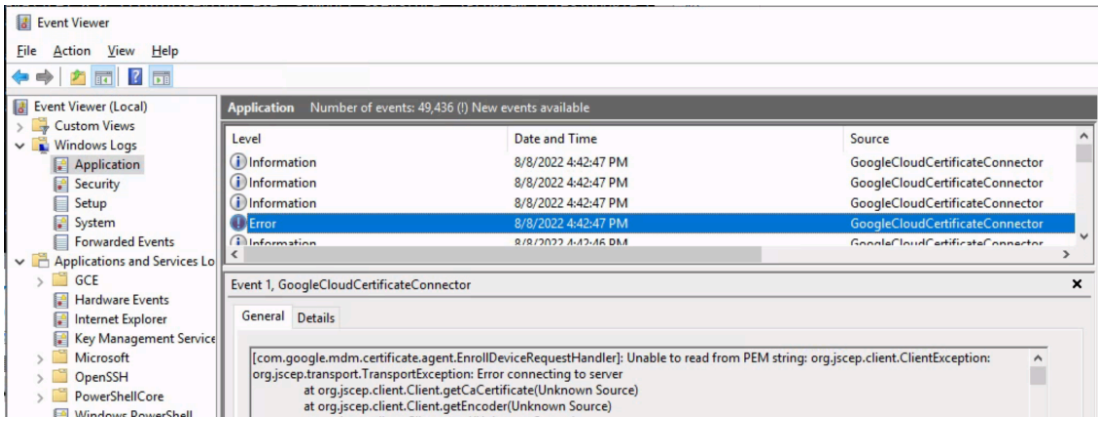
`[java.lang.String]: 123…|`

`[com.google.mdm.certificate.agent.RequestSubscriber]:` **`Acking messages`**…

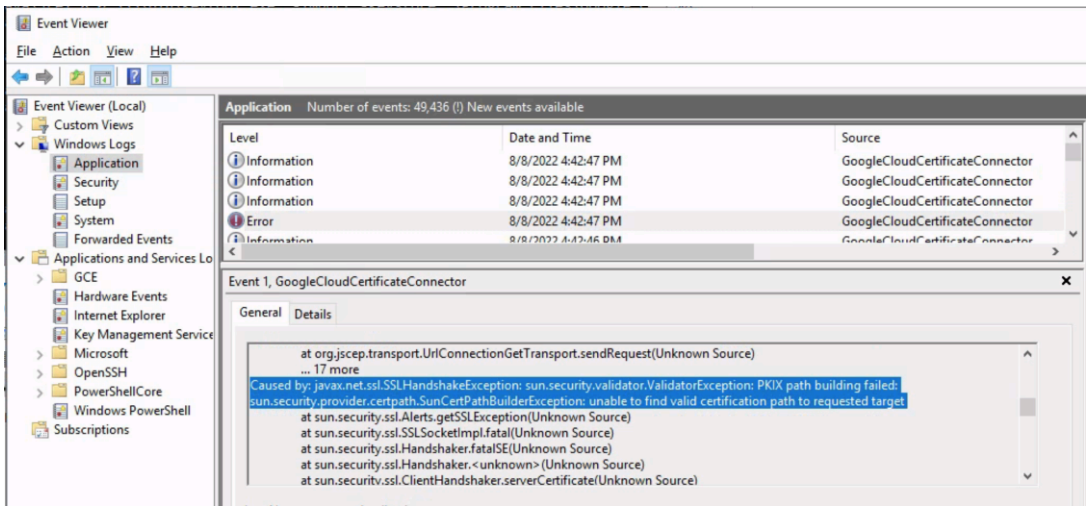
`[com.google.mdm.certificate.agent.RequestSubscriber]: **Acked messages**…`

NDES Server Communication issues

If **Error** level events appear, with ***Unable to read from PEM string…*** scroll down in message details to determine exact cause.

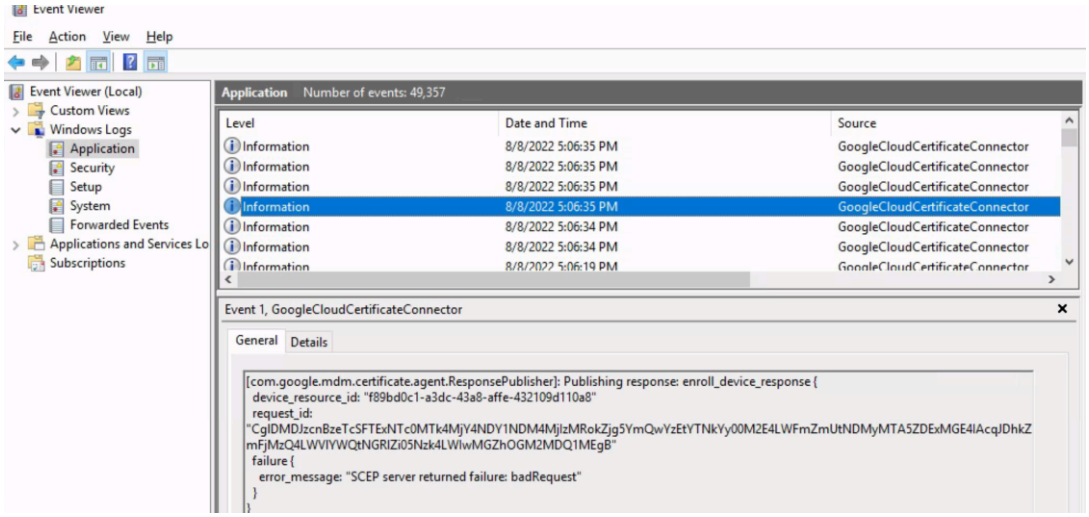


"***PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target***" means that GCCC cannot validate the SSL certificate presented by the NDES IIS Server. The NDES IIS SSL Certificate's signing CA and/or Root CA certificates must be imported into the GCCC key store.



"***No subject alternative DNS name matching ndes1.gscep.net found***" means that the SCEP server URL hostname (http://**ndes1.gscep.net/**certsrv/…) is not found in the **Subject** or **Alternative names** of the NDES Server SSL certificate, i.e. it was issued to a short/non-fully qualified name (**ndes1**) or some other name.

"failure { error_message: "SCEP server returned failure: badRequest" }" means that the SCEP challenge password in the SCEP Profile does not match the one configured on the NDES Server.



"***Caused by: java.net.ConnectException: Connection timed out: connect***" means that GCCC could not establish an HTTPS TCP session to the configured NDES server. This could mean:

1) The NDES server itself or the IIS service is down
2) The NDES hostname in the SCEP URL is incorrect
3) The NDES server is unreachable due to DNS resolution failure, routing issues, firewall blocking of TCP 443 or other network issues.

Make sure that the NDES server is reachable, by opening the SCEP URL in a browser on the GCCC server.

Certificate retrieval via SCEP

1. Download and compile sscep (binaries)
2. Run *sscep getca -u **http[s]://ndes.server.ip.ordns**/certsrv/mscep/mscep.dll -c ca.crt*

```
sscep getca -u https://ndes1.gscep.net/certsrv/mscep/mscep.dll -c ca.crt
```

Successful output:

```
C:\Users\iakin\Downloads\scep\scep>sscep getca -u
https://ndes.dom.net/certsrv/mscep/mscep.dll -c ca.crt

sscep: requesting CA certificate
sscep: valid response from server

sscep: found certificate with
  subject: /C=US/CN=NDES-MSCEP-RA
  issuer: /DC=net/DC=dom/CN=dom-SUBCA-CA
  usage: Digital Signature
  MD5 fingerprint: 49:6F:6E:81:20:E2:45:F9:2C:35:32:BC:6D:6A:77:DD
sscep: certificate written as ca.crt-0
```

Unsuccessful output:

```
C:\Users\iakin\Downloads\scep\scep>sscep getca -u
https://ndes1.dom.net/certsrv/mscep/mscep.dll -c ca.crt

sscep: requesting CA certificate
sscep: wrong MIME content type
sscep: error while sending message
```

Contact support

To further debug the issue that you're experiencing, contact Chrome Enterprise support and provide the following information.

Connector logs

Share the following files:

- After filtering events from the Windows event log with the connector's source name and with the time frame in which the problem has occurred, save the filtered logs in a file in .txt format and share it.

- Share your **config.json** file. It is generated by the Admin console during connector setup after downloading the connector installer.

ChromeOS device device logs

For a device or user failing to receive a certificate, collect full debug logs after the certificate provisioning process has failed. Full instructions for gathering full debug logs can be found under Collecting Full Debug Logs Documentation

FAQs

Appendix

Lab Deployment Diagram

For a Lab environment, it is possible to co-locate several of the functions on a single server.