chrome enterprise

Notes from the field

Configuring Certificate Enrollment for ChromeOS via SCEP with Microsoft NDES

For administrators with Active Directory expertise

January 2023

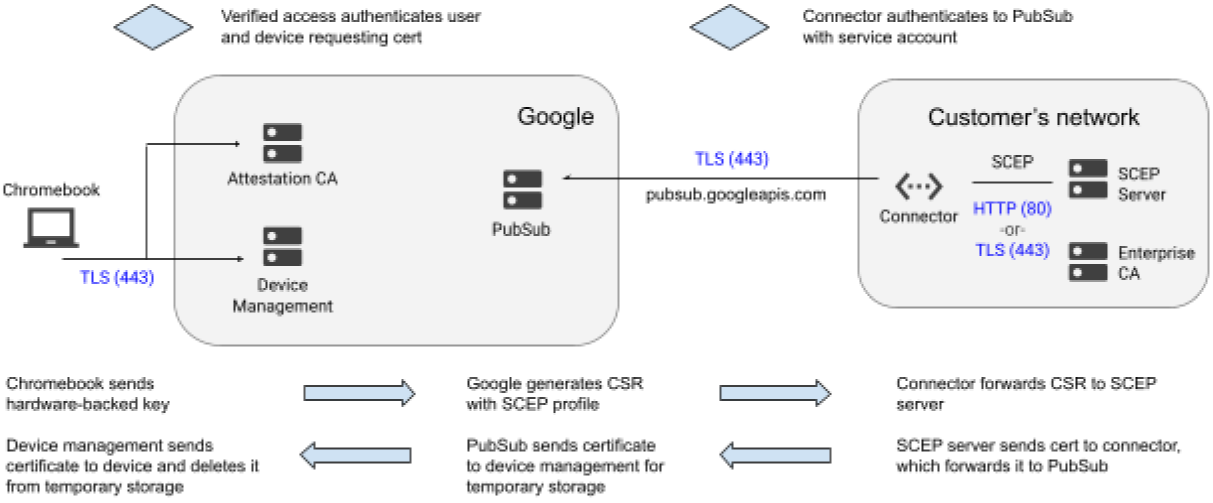
Contents

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.

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)


Verified access authenticates user and device requesting cert
Connector authenticates to PubSub with service account
Google
Attestation CA
PubSub
Device Management
Chromebook
TLS (443)
TLS (443)
pubsub.googleapis.com
Customer's network
SCEP
Connector
HTTP (80)
-or-
TLS (443)
SCEP Server
Enterprise CA
Chromebook sends hardware-backed key
Google generates CSR with SCEP profile
Connector forwards CSR to SCEP server
Device management sends certificate to device and deletes it from temporary storage
PubSub sends certificate to device management for temporary storage
SCEP server sends cert to connector, which forwards it to PubSub

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.

GCCC needs to be able to connect to https://pubsub.googleapis.com via HTTPS on TCP/443, without SSL proxy/decryption, to retrieve configuration and CSRs, and upload Certificates.

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.

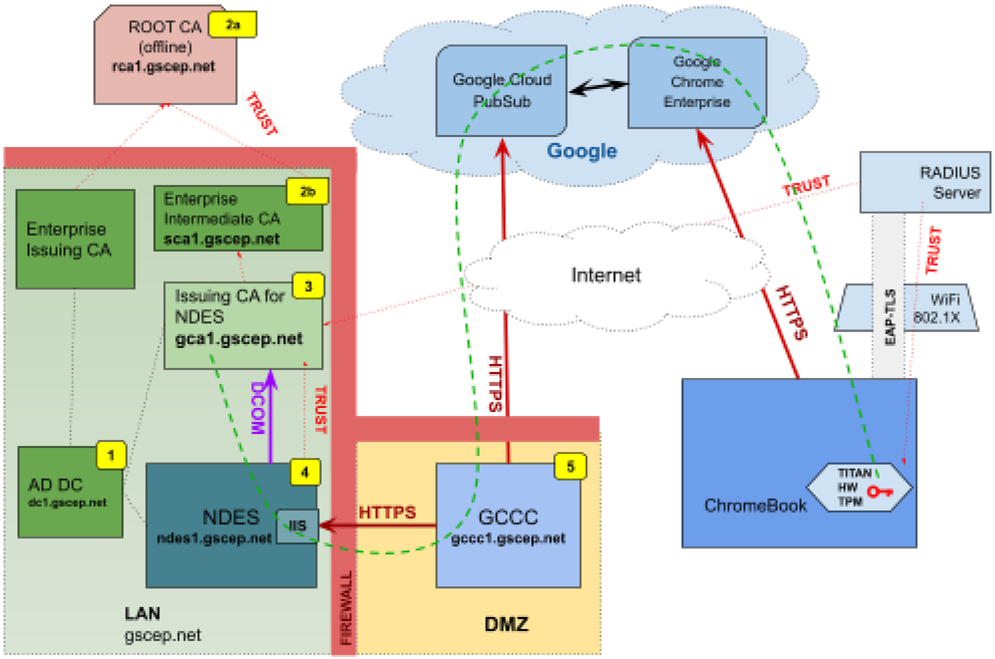
The NDES IIS server SSL certificate Subject Name needs to match the hostname used in the SCEP enrollment URL.

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.

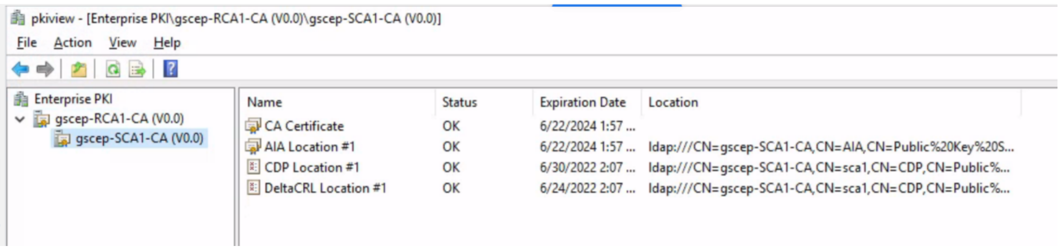
Enterprise Deployment with Microsoft NDES



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:



pkiview - [Enterprise PKI\gscep-RCA1-CA (V0.0)\gscep-SCA1-CA (V0.0)]

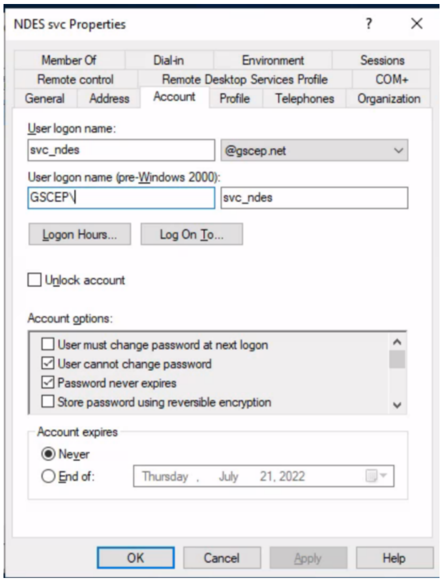
Enterprise PKI
gscep-RCA1-CA (V0.0)
gscep-SCA1-CA (V0.0)

Name	Status	Expiration Date	Location
CA Certificate	OK	6/22/2024 1:57 ...	
AIA Location #1	OK	6/22/2024 1:57 ...	ldap:///CN=gscep-SCA1-CA,CN=AIA,CN=Public%20Key%20S...
CDP Location #1	OK	6/30/2022 2:07 ...	ldap:///CN=gscep-SCA1-CA,CN=sca1,CN=CDP,CN=Public%...
DeltaCRL Location #1	OK	6/24/2022 2:07 ...	ldap:///CN=gscep-SCA1-CA,CN=sca1,CN=CDP,CN=Public%...

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**

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.*



NDES svc Properties

User logon name: svc_ndes @gscep.net

User logon name (pre-Windows 2000): GSCEP\ svc_ndes

□ Unlock account

Account options:

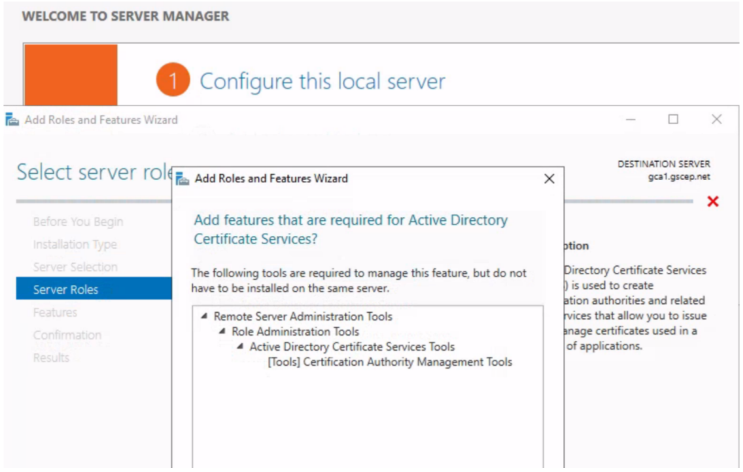
□ User must change password at next logon
☑ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Thursday , July 21, 2022

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



Directory Certificate Services) is used to create ation authorities and related rvices that allow you to issue nage certificates used in a of applications.

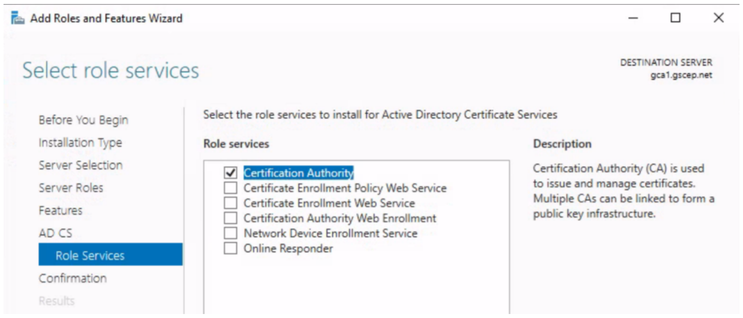
Add Roles and Features Wizard

Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
    - Role Administration Tools
        - Active Directory Certificate Services Tools
            - [Tools] Certification Authority Management Tools

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



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
gca1.gscep.net

Select the role services to install for Active Directory Certificate Services

Role services

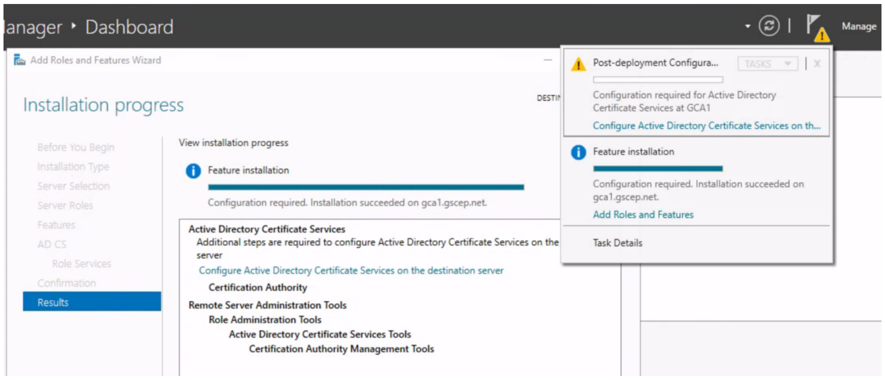
- ☑ Certification Authority
- ☐ Certificate Enrollment Policy Web Service
- ☐ Certificate Enrollment Web Service
- ☐ Certification Authority Web Enrollment
- ☐ Network Device Enrollment Service
- ☐ Online Responder

Description

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

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…*



Installation progress

View installation progress

Feature installation

Configuration required. Installation succeeded on gca1.gscep.net.

Active Directory Certificate Services
Additional steps are required to configure Active Directory Certificate Services on the server
Configure Active Directory Certificate Services on the destination server
Certification Authority
Remote Server Administration Tools
Role Administration Tools
Active Directory Certificate Services Tools
Certification Authority Management Tools

Post-deployment Configura...

Configuration required for Active Directory Certificate Services at GCA1

Configure Active Directory Certificate Services on th...

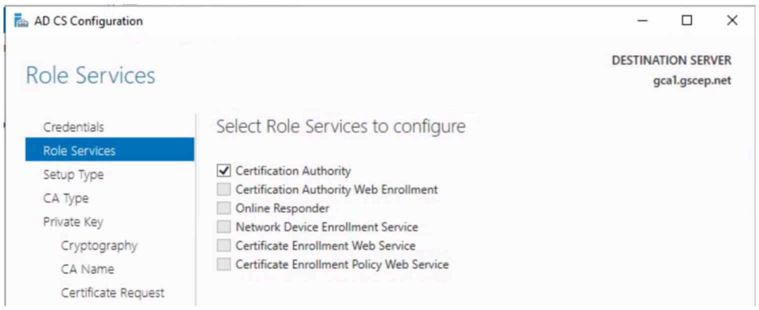
Feature installation

Configuration required. Installation succeeded on gca1.gscep.net.

Add Roles and Features

Task Details

   c. Role Services: *Certification Authority*



AD CS Configuration

Role Services

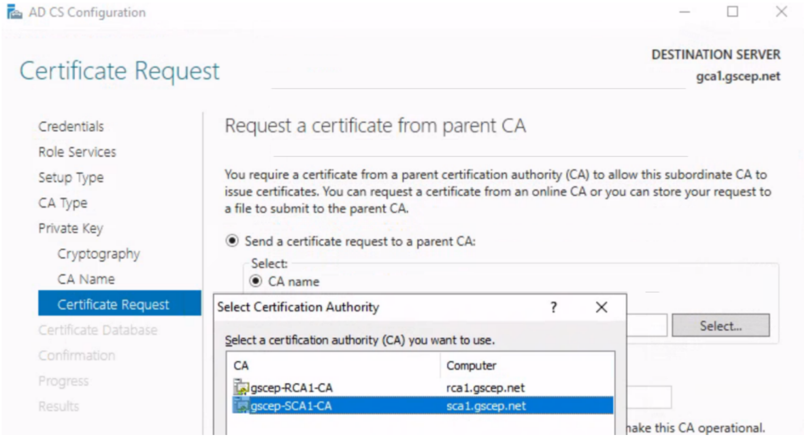
DESTINATION SERVER
gca1.gscep.net

Select Role Services to configure

- ☑ Certification Authority
- ☐ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

   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***



AD CS Configuration

Certificate Request

DESTINATION SERVER
gca1.gscep.net

Request a certificate from parent CA

You require a certificate from a parent certification authority (CA) to allow this subordinate CA to issue certificates. You can request a certificate from an online CA or you can store your request to a file to submit to the parent CA.

● Send a certificate request to a parent CA:

Select:
● CA name

Select Certification Authority

Select a certification authority (CA) you want to use.

CA	Computer
gscep-RCA1-CA	rca1.gscep.net
gscep-SCA1-CA	sca1.gscep.net

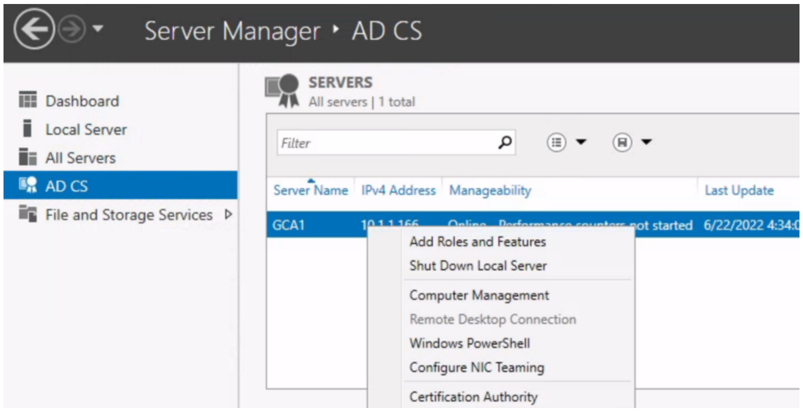
ake this CA operational.

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

3. Create the SCEP certificate template

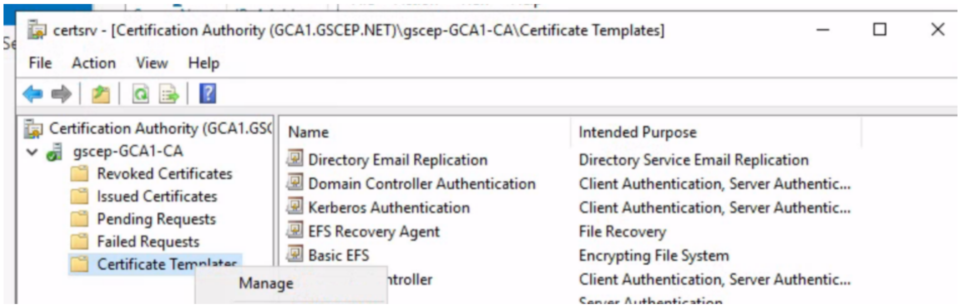
a. *Note that while these settings have been verified, your organization's policy might dictate different settings, which would need to be tested.*

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



Server Name	IPv4 Address	Manageability	Last Update
GCA1	10.1.1.166	Online - Performance counters not started	6/22/2022 4:34:0

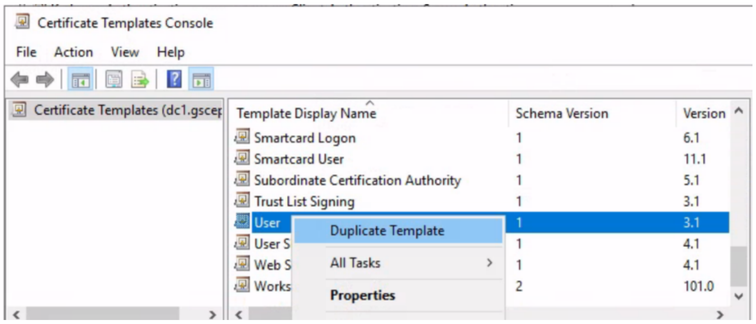
c. Certificate Templates -> Manage



certsrv - [Certification Authority (GCA1.GSCEP.NET)\gscep-GCA1-CA\Certificate Templates]

Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
ntroller	Client Authentication, Server Authentic...
	Server Authentication

d. Duplicate *User* Template


Certificate Templates Console
File
Action
View
Help
Certificate Templates (dc1.gscep
Duplicate Template
All Tasks
Properties

Template Display Name	Schema Version	Version
Smartcard Logon	1	6.1
Smartcard User	1	11.1
Subordinate Certification Authority	1	5.1
Trust List Signing	1	3.1
User	1	3.1
User S	1	4.1
Web S	1	4.1
Works	2	101.0

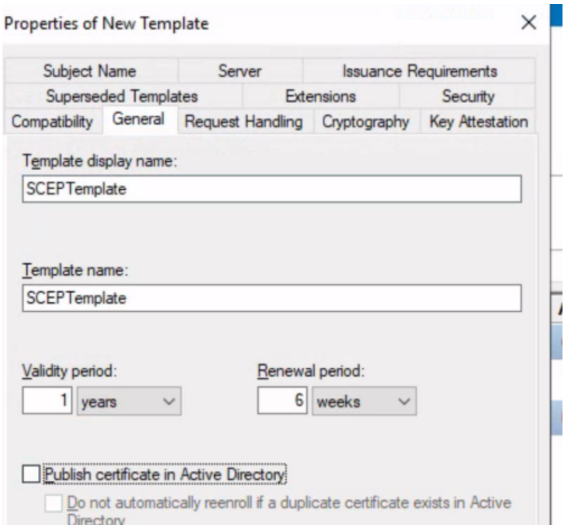
e. General

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



Template display name: SCEPTemplate

Template name: SCEPTemplate

Validity period: 1 years

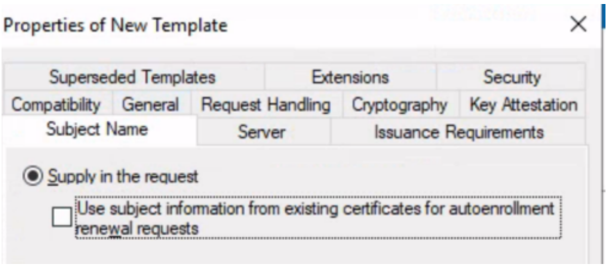
Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

f. Subject Name -> ***Supply in the request***

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



● Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests

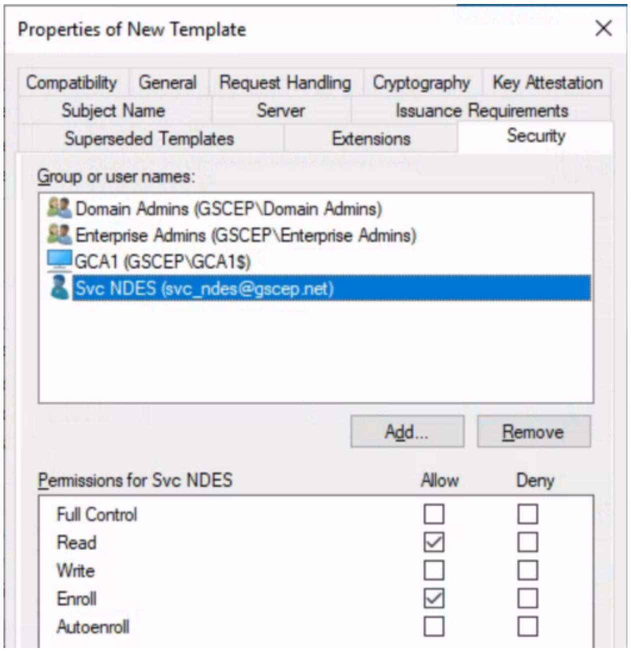
h. Security

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.



Group or user names:

- Domain Admins (GSCEP\Domain Admins)
- Enterprise Admins (GSCEP\Enterprise Admins)
- GCA1 (GSCEP\GCA1$)
- Svc NDES (svc_ndes@gscep.net)

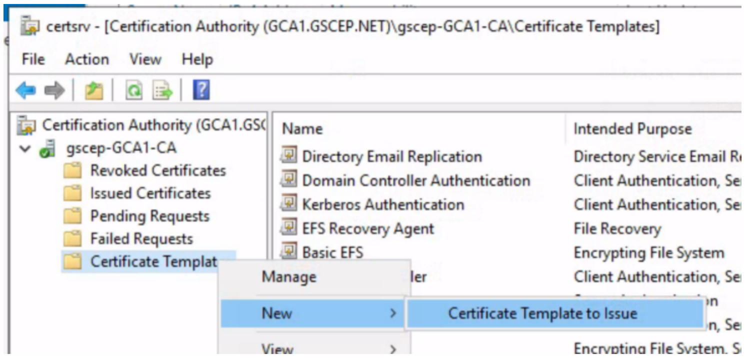
Permissions for Svc NDES	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

b. Close *Certificate Templates* Console

c. Back in *Certification Authority*

i. *Certificate Templates -> New -> Certificate Template to Issue*

ii. Select **SCEPTemplate**

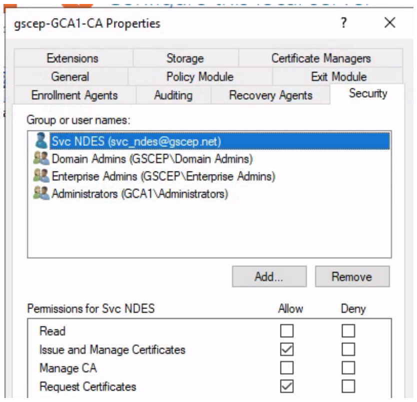

certsrv - [Certification Authority (GCA1.GSCEP.NET)\gscep-GCA1-CA\Certificate Templates]
File
Action
View
Help
Certification Authority (GCA1.GS(
gscep-GCA1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templat
Manage
New
Certificate Template to Issue
View

Name	Intended Purpose
Directory Email Replication	Directory Service Email R
Domain Controller Authentication	Client Authentication, Se
Kerberos Authentication	Client Authentication, Se
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
ler	Client Authentication, Se
n	
n, Se	
	Encrypting File System, S

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



Group or user names:

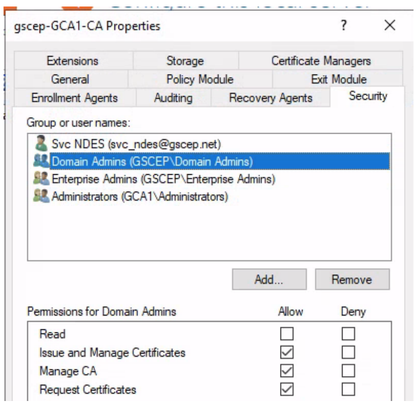
- Svc NDES (svc_ndes@gscep.net)
- Domain Admins (GSCEP\Domain Admins)
- Enterprise Admins (GSCEP\Enterprise Admins)
- Administrators (GCA1\Administrators)

Permissions for Svc NDES	Allow	Deny
Read	□	□
Issue and Manage Certificates	☑	□
Manage CA	□	□
Request Certificates	☑	□

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



gscep-GCA1-CA Properties

Group or user names:

- Svc NDES (svc_ndes@gscep.net)
- Domain Admins (GSCEP\Domain Admins)
- Enterprise Admins (GSCEP\Enterprise Admins)
- Administrators (GCA1\Administrators)

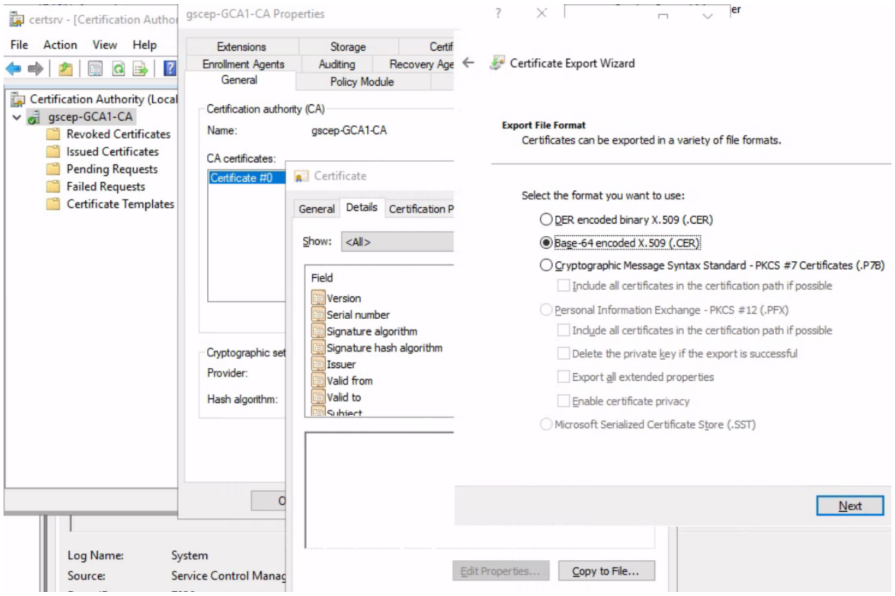
Permissions for Domain Admins	Allow	Deny
Read	□	□
Issue and Manage Certificates	☑	□
Manage CA	☑	□
Request Certificates	☑	□

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



gscep-GCA1-CA Properties

Certification authority (CA)

Name: gscep-GCA1-CA

CA certificates:

Certificate #0

Show: <All>

Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

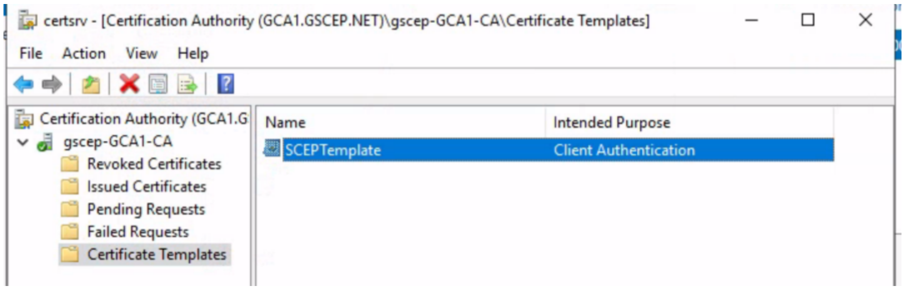
□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

6. Disable all other Certificate Templates (Optional)



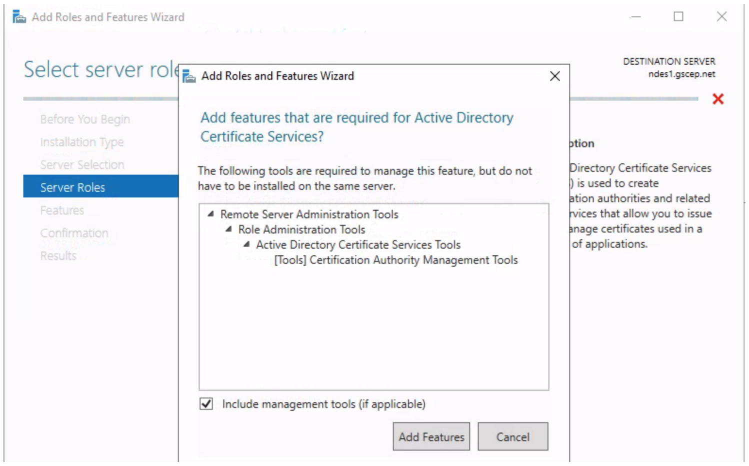
certsrv - [Certification Authority (GCA1.GSCEP.NET)\gscep-GCA1-CA\Certificate Templates]

- Certification Authority (GCA1.G
  - gscep-GCA1-CA
    - Revoked Certificates
    - Issued Certificates
    - Pending Requests
    - Failed Requests
    - Certificate Templates

Name	Intended Purpose
SCEPTemplate	Client Authentication

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*



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
ndes1.gscep.net

Add Roles and Features Wizard

Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - [Tools] Certification Authority Management Tools

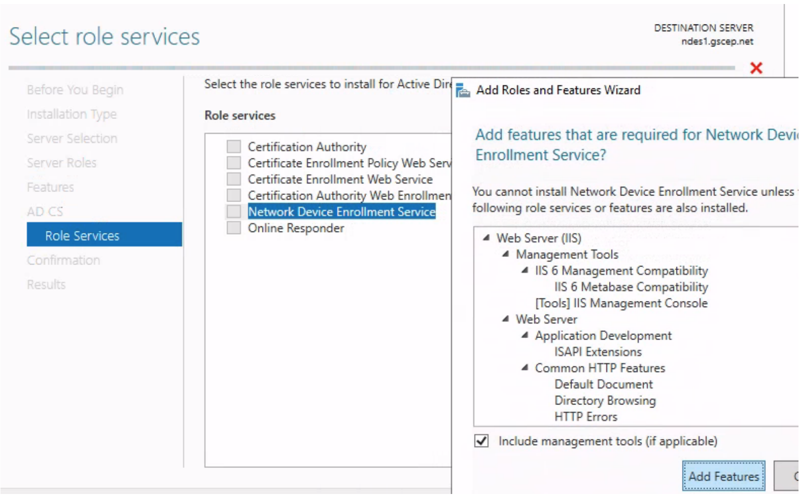
☑ Include management tools (if applicable)

ption

Directory Certificate Services) is used to create ation authorities and related rvices that allow you to issue anage certificates used in a of applications.

   e. Select role services:
      i. Certification Authority - **Uncheck**
      ii. Network Device Enrollment Service - **Check**

iii. This will add IIS role for installation



Select role services

DESTINATION SERVER
ndes1.gscep.net

Select the role services to install for Active Dir

Role services

- □ Certification Authority
- □ Certificate Enrollment Policy Web Serv
- □ Certificate Enrollment Web Service
- □ Certification Authority Web Enrollmen
- □ Network Device Enrollment Service
- □ Online Responder

Add Roles and Features Wizard

Add features that are required for Network Devi Enrollment Service?

You cannot install Network Device Enrollment Service unless following role services or features are also installed.

- Web Server (IIS)
  - Management Tools
    - IIS 6 Management Compatibility
      - IIS 6 Metabase Compatibility
    - [Tools] IIS Management Console
  - Web Server
    - Application Development
      - ISAPI Extensions
    - Common HTTP Features
      - Default Document
      - Directory Browsing
      - HTTP Errors

☑ Include management tools (if applicable)

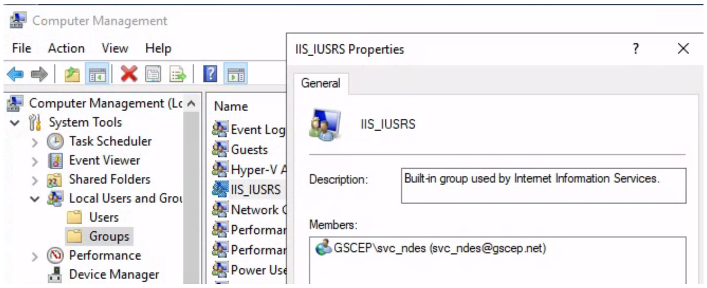
f. Accept defaults for the rest

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



IIS_IUSRS Properties

General

IIS_IUSRS

Description: Built-in group used by Internet Information Services.

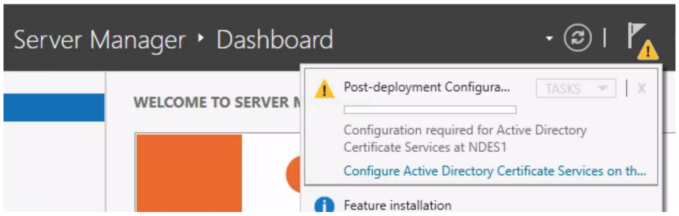
Members:

GSCEP\svc_ndes (svc_ndes@gscep.net)

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…*



Post-deployment Configura...

Configuration required for Active Directory Certificate Services at NDES1

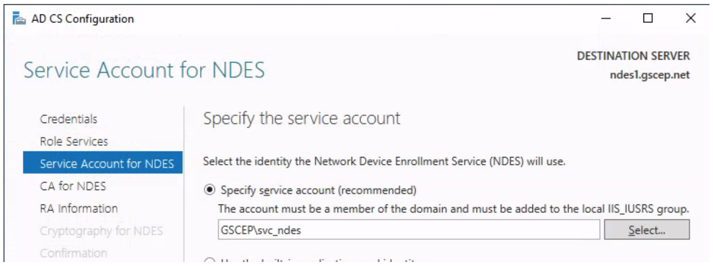
Configure Active Directory Certificate Services on th...

Feature installation

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***



Service Account for NDES

DESTINATION SERVER
ndes1.gscep.net

Specify the service account

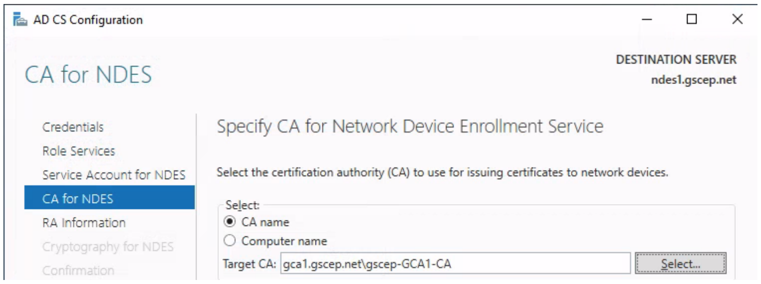
Select the identity the Network Device Enrollment Service (NDES) will use.

● Specify service account (recommended)

The account must be a member of the domain and must be added to the local IIS_IUSRS group.

GSCEP\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



CA for NDES

DESTINATION SERVER
ndes1.gscep.net

Specify CA for Network Device Enrollment Service

Select the certification authority (CA) to use for issuing certificates to network devices.

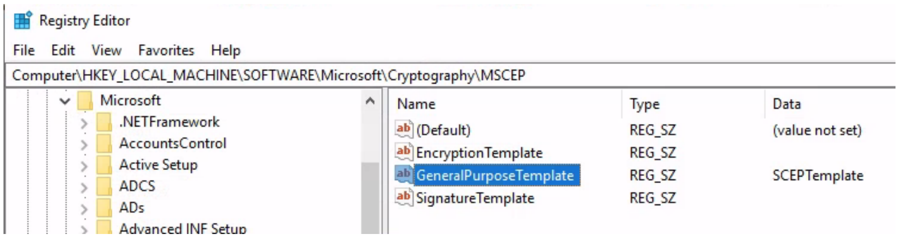
Select:
● CA name
○ Computer name

Target CA: gca1.gscep.net\gscep-GCA1-CA

- g. RA Information and Crypto: as needed
- h. Wait for Configuration to complete

4. Configure default NDES template

- a. Open *regedit*
  - i. `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\`
    - 1. *GeneralPurposeTemplate*
  - ii. Set value to the Template Name (**not** Template display name) of SCEP template created above - **SCEPTemplate**

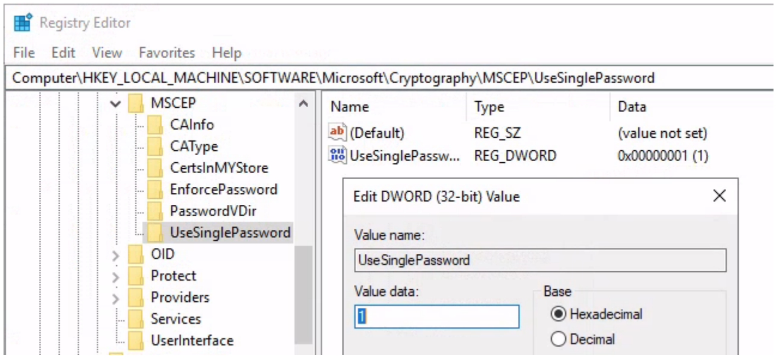


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP

Name	Type	Data
(Default)	REG_SZ	(value not set)
EncryptionTemplate	REG_SZ	
GeneralPurposeTemplate	REG_SZ	SCEPTemplate
SignatureTemplate	REG_SZ	

5. Configure NDES to utilize a static SCEP challenge password

- a. This step is necessary because multiple devices will be requesting certificates via GCCC
- b. `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\UseSinglePassword`
- c. `Set value of UseSinglePassword to 1`



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\UseSinglePassword

Name	Type	Data
(Default)	REG_SZ	(value not set)
UseSinglePassw...	REG_DWORD	0x00000001 (1)

Edit DWORD (32-bit) Value

Value name: UseSinglePassword

Value data: 1

Base
● Hexadecimal
○ Decimal

6. Bind SSL server certificate in IIS

a. *Note that this step applies only if GCCC will be installed on a separate server.*

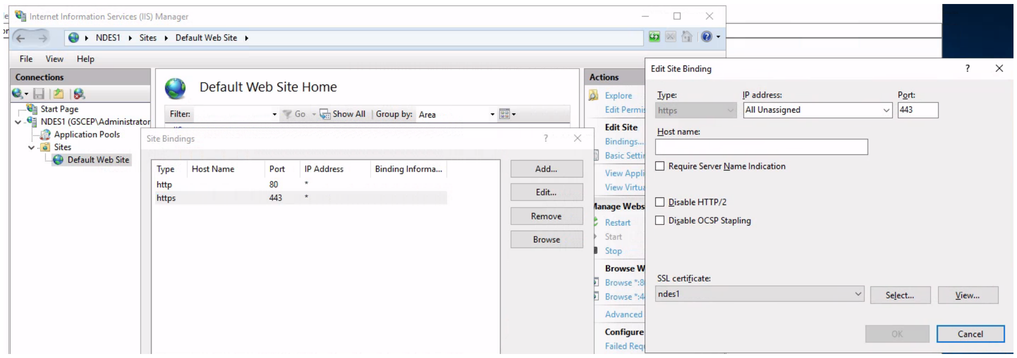
b. *IIS Manager -> Sites -> Default Web Site*

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.



Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

Edit Site Binding

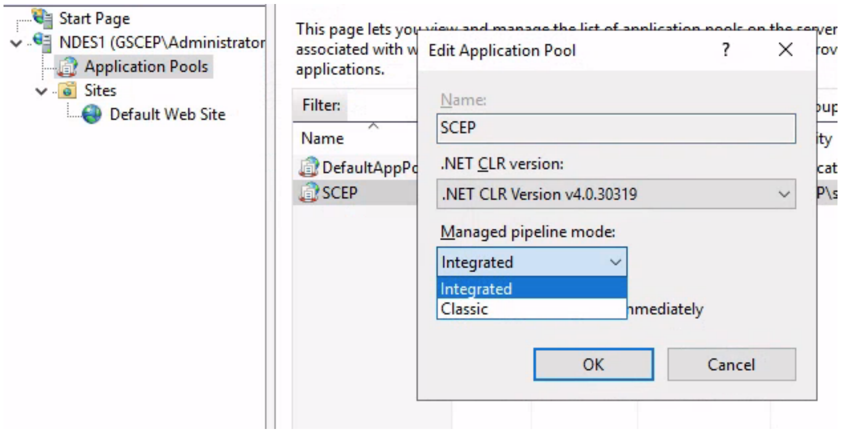
Type: https
IP address: All Unassigned
Port: 443
Host name:
□ Require Server Name Indication
□ Disable HTTP/2
□ Disable OCSP Stapling
SSL certificate: ndes1

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


Start Page
NDES1 (GSCEP\Administrator
Application Pools
Sites
Default Web Site
This page lets you view and manage the list of application pools on the server associated with w... applications.
Filter:
Name
DefaultAppPo
SCEP
Edit Application Pool
?
OK
Cancel

Name: SCEP

.NET CLR version: .NET CLR Version v4.0.30319

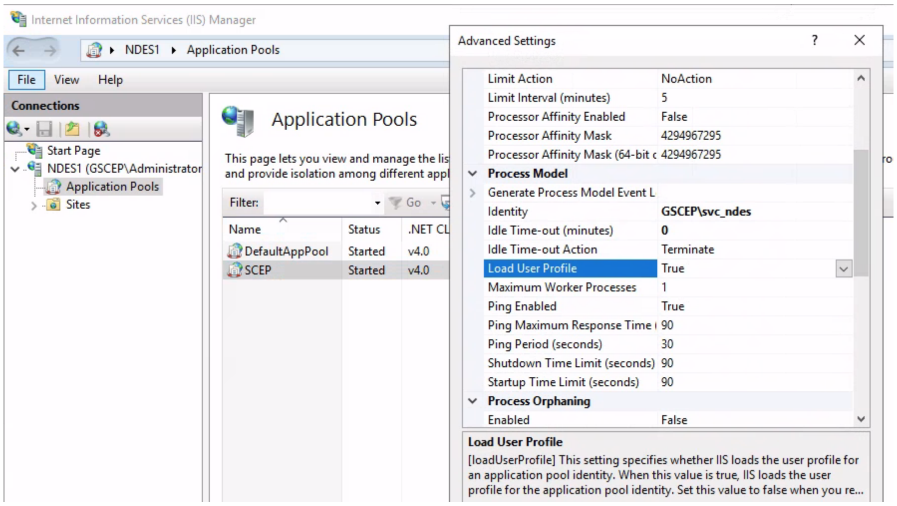
Managed pipeline mode: Integrated

Integrated
Classic

...mediately

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. 
Internet Information Services (IIS) Manager
NDES1
Application Pools
File
View
Help
Connections
Start Page
NDES1 (GSCEP\Administrator
Application Pools
Sites
Application Pools
This page lets you view and manage the lis and provide isolation among different appl
Filter:
Go
Advanced Settings
?

Name	Status	.NET CL
DefaultAppPool	Started	v4.0
SCEP	Started	v4.0

Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	**GSCEP\svc_ndes**
Idle Time-out (minutes)	**0**
Idle Time-out Action	Terminate
Load User Profile	True
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90
Process Orphaning	
Enabled	False

Load User Profile
[loadUserProfile] This setting specifies whether IIS loads the user profile for an application pool identity. When this value is true, IIS loads the user profile for the application pool identity. Set this value to false when you re...

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**

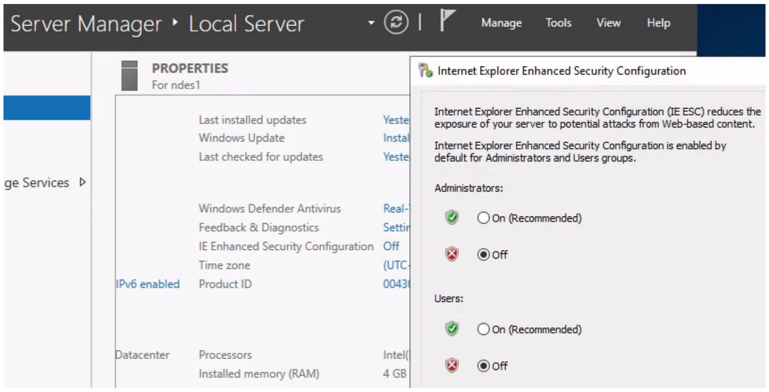
    d. *Maximum query string (Bytes)* = **8096**

    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***



PROPERTIES
For ndes1

Last installed updates Yeste
Windows Update Instal
Last checked for updates Yeste

Windows Defender Antivirus Real-
Feedback & Diagnostics Settir
IE Enhanced Security Configuration Off
Time zone (UTC-
IPv6 enabled Product ID 0043
Datacenter Processors Intel(
Installed memory (RAM) 4 GB

Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

○ On (Recommended)

● Off

Users:

○ On (Recommended)

● 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
```

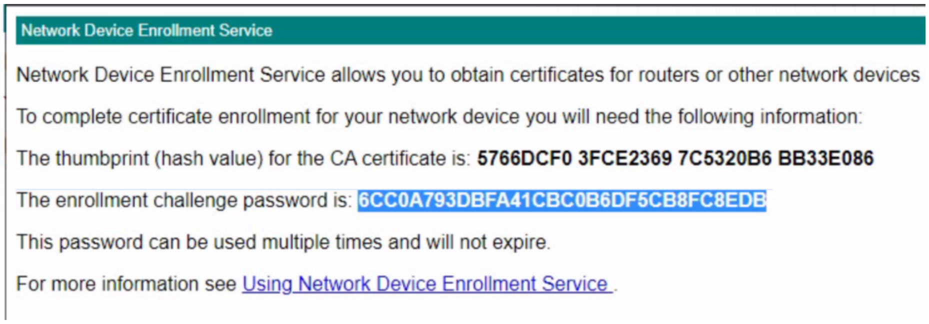
12. Restart NDES Server

13. Retrieve SCEP Challenge

a. Open ***incognito*** browser window to https://**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.



Network Device Enrollment Service

Network Device Enrollment Service allows you to obtain certificates for routers or other network devices

To complete certificate enrollment for your network device you will need the following information:

The thumbprint (hash value) for the CA certificate is: **5766DCF0 3FCE2369 7C5320B6 BB33E086**

The enrollment challenge password is: **6CC0A793DBFA41CBC0B6DF5CB8FC8EDB**

This password can be used multiple times and will not expire.

For more information see Using Network Device Enrollment Service .

14. (Optional) Configure Windows Firewall

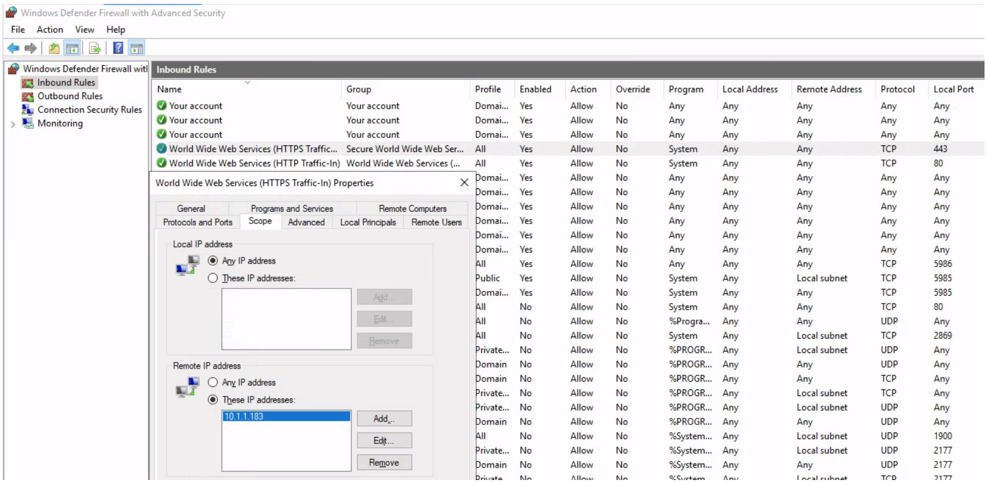
a. Open *Windows Firewall Advanced Settings -> Inbound Rules*

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**



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port
Your account	Your account	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
Your account	Your account	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
Your account	Your account	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
World Wide Web Services (HTTPS Traffic...	Secure World Wide Web Ser...	All	Yes	Allow	No	System	Any	Any	TCP	443
World Wide Web Services (HTTP Traffic-In)	World Wide Web Services (...	All	Yes	Allow	No	System	Any	Any	TCP	80
		Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
		Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
		Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
		Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
		Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
		Domai...	Yes	Allow	No	Any	Any	Any	Any	Any
		All	Yes	Allow	No	Any	Any	Any	TCP	5986
		Public	Yes	Allow	No	System	Any	Local subnet	TCP	5985
		Domai...	Yes	Allow	No	System	Any	Any	TCP	5985
		All	No	Allow	No	System	Any	Any	TCP	80
		All	No	Allow	No	%Progra...	Any	Any	UDP	Any
		All	No	Allow	No	System	Any	Local subnet	TCP	2869
		Private...	No	Allow	No	%PROGR...	Any	Local subnet	UDP	Any
		Domain	No	Allow	No	%PROGR...	Any	Any	UDP	Any
		Domain	No	Allow	No	%PROGR...	Any	Any	TCP	Any
		Private...	No	Allow	No	%PROGR...	Any	Local subnet	TCP	Any
		Private...	No	Allow	No	%PROGR...	Any	Local subnet	UDP	Any
		Domain	No	Allow	No	%PROGR...	Any	Any	UDP	Any
		All	No	Allow	No	%System...	Any	Local subnet	UDP	1900
		Private...	No	Allow	No	%System...	Any	Local subnet	UDP	2177
		Domain	No	Allow	No	%System...	Any	Any	UDP	2177
		Private...	No	Allow	No	%System...	Any	Local subnet	TCP	2177

World Wide Web Services (HTTPS Traffic-In) Properties

Local IP address
● Any IP address
○ These IP addresses:

Remote IP address
○ Any IP address
● These IP addresses:
10.1.1.183

Configure Google Cloud Certificate Connector

1. Download Google Cloud Certificate Connector

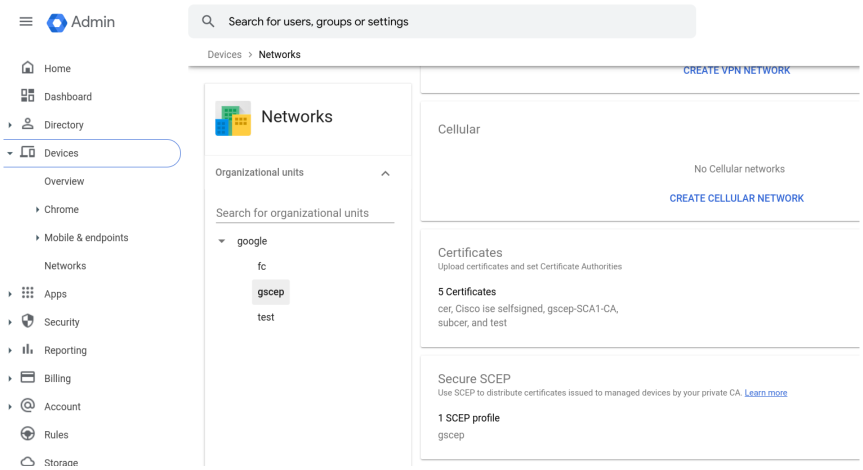
   a. Sign in to the Admin console

   b. Open ***Devices -> Networks***

      i. Requires having the Shared device settings administrator privilege.

   c. Scroll down to **Secure SCEP**

   d. To apply the setting to everyone, leave the top organizational unit selected. Otherwise, select an organizational unit.



Cellular

No Cellular networks

Certificates
Upload certificates and set Certificate Authorities

5 Certificates
cer, Cisco ise selfsigned, gscep-SCA1-CA, subcer, and test

Secure SCEP
Use SCEP to distribute certificates issued to managed devices by your private CA. Learn more

1 SCEP profile
gscep

e. Click **Create/Add Secure SCEP Profile**

f. Close the **Add secure SCEP** window

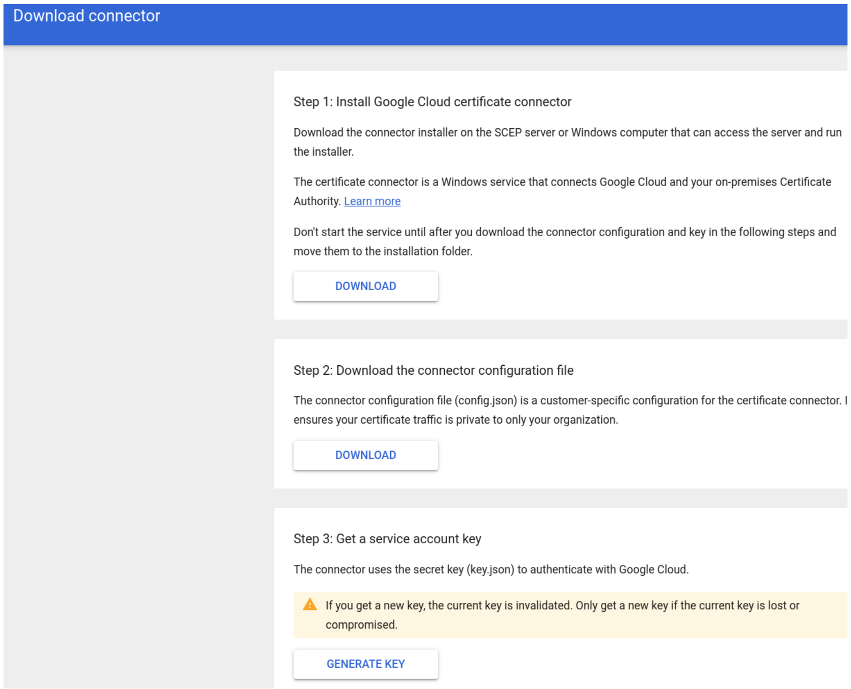
g. Click **Download connector**

h. In the **Google Cloud Certificate Connector** section, click **Download**

i. In the **Download the connector configuration file** section, click **Download**. The config.json file downloads.

j. **NOTE: The key is used for the entire organization and generating it again invalidates any existing GCCC installations. Be sure to save the key.json file securely for any additional installations.**

k. If this is the first time activating SCEP, click **Generate key** to download **key.json** file.



Download connector

Step 1: Install Google Cloud certificate connector

Download the connector installer on the SCEP server or Windows computer that can access the server and run the installer.

The certificate connector is a Windows service that connects Google Cloud and your on-premises Certificate Authority. Learn more

Don't start the service until after you download the connector configuration and key in the following steps and move them to the installation folder.

DOWNLOAD

Step 2: Download the connector configuration file

The connector configuration file (config.json) is a customer-specific configuration for the certificate connector. I ensures your certificate traffic is private to only your organization.

DOWNLOAD

Step 3: Get a service account key

The connector uses the secret key (key.json) to authenticate with Google Cloud.

⚠ If you get a new key, the current key is invalidated. Only get a new key if the current key is lost or compromised.

GENERATE KEY

l. If needed, transfer the GCCC installer and configuration and key files (**config.json** and **key.json**) to the GCCC server **gccc1.gscep.net**

2. Install Google Cloud Certificate Connector.

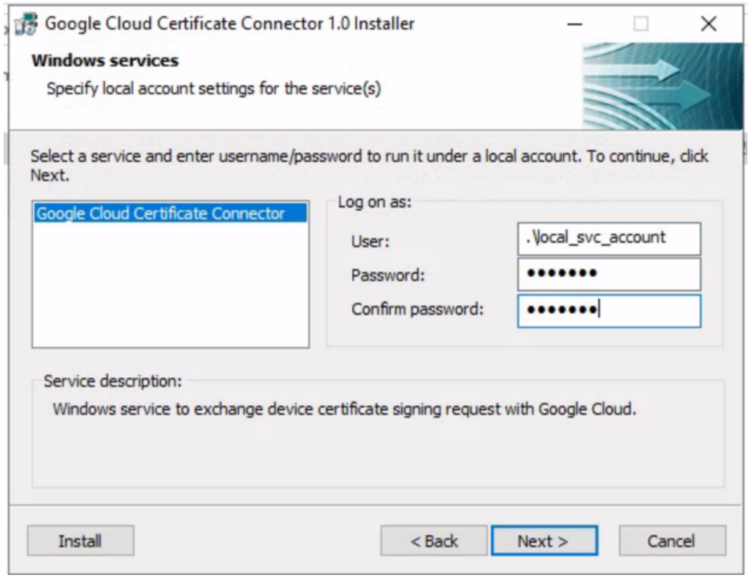
a. Right-click the ***google-cloud-certificate-connector-setup*** file and click **Run as administrator**.

b. On the **Windows services** screen, select **Google Cloud Certificate Connector** in the list of services.

c. Enter the name and password of an account that has *Log on as a service* Right on the GCCC Server.

i. *Note that there may be issues due to long passwords here and it may be necessary to temporarily change the password to a shorter one.*

ii. Local Security Policy -> Local Policies -> User Rights Assignment -> Log on as a service.



Google Cloud Certificate Connector 1.0 Installer

Windows services

Specify local account settings for the service(s)

Select a service and enter username/password to run it under a local account. To continue, click Next.

Google Cloud Certificate Connector

Log on as:

User: .\local_svc_account

Password: •••••••

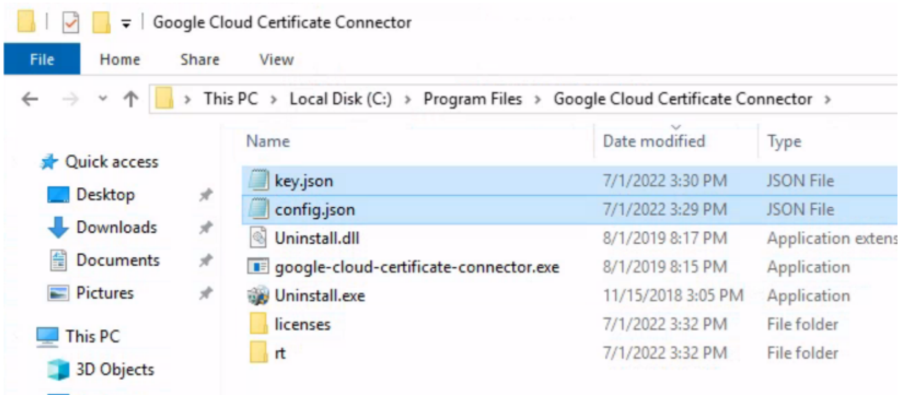
Confirm password: •••••••

Service description:

Windows service to exchange device certificate signing request with Google Cloud.

iii. Note: The service can be later changed to run as *Local System* if desired.

d. Once install is complete, copy config.json and key.json to the installation directory `C:\Program Files\Google Cloud Certificate Connector\`



Google Cloud Certificate Connector

This PC › Local Disk (C:) › Program Files › Google Cloud Certificate Connector ›

Name	Date modified	Type
key.json	7/1/2022 3:30 PM	JSON File
config.json	7/1/2022 3:29 PM	JSON File
Uninstall.dll	8/1/2019 8:17 PM	Application extens
google-cloud-certificate-connector.exe	8/1/2019 8:15 PM	Application
Uninstall.exe	11/15/2018 3:05 PM	Application
licenses	7/1/2022 3:32 PM	File folder
rt	7/1/2022 3:32 PM	File folder

3. Configure GCCC Service

a. Open *Administrative Tools > Services*

b. Locate *Google Cloud Certificate Connector*

c. Start service

4. (Optional) Install Java (If using HTTPS between GCCC and NDES)

a. Note: this step can be performed on the GCCC server itself or on another machine, as long as the keystore file can be manipulated and moved back to the GCCC server.

b. Java can be uninstalled after completion.

c. Download and install Oracle Java SE

d. If a GUI for keystore is preferable to CLI, download and install KeyStore Explorer

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

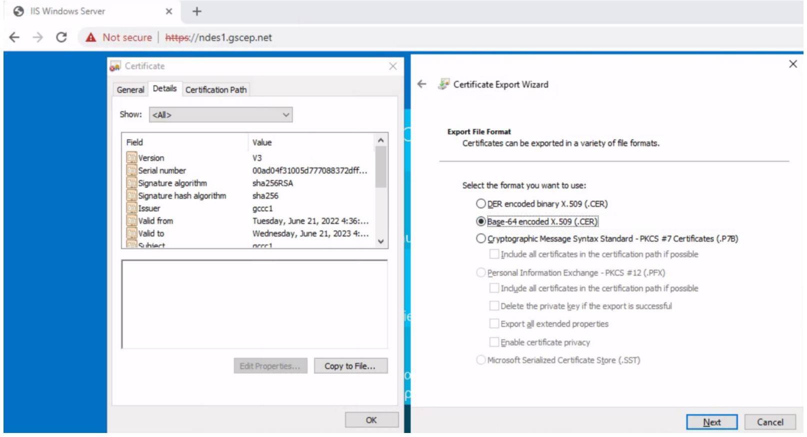
a. Download the Certificate from NDES server

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***



Field	Value
Version	V3
Serial number	00ad04f31005d777088372dff...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	gccc1
Valid from	Tuesday, June 21, 2022 4:36:...
Valid to	Wednesday, June 21, 2023 4:...
Subject	gccc1

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  □ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
  □ Include all certificates in the certification path if possible
  □ Delete the private key if the export is successful
  □ Export all extended properties
  □ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

v. Save in a convenient location

b. Import NDES IIS server certificate into GCCC Java certificate store

i. In an ***Elevated / Run as Administrator*** command window run the below command.

ii. Default Java keystore password is ***changeit***

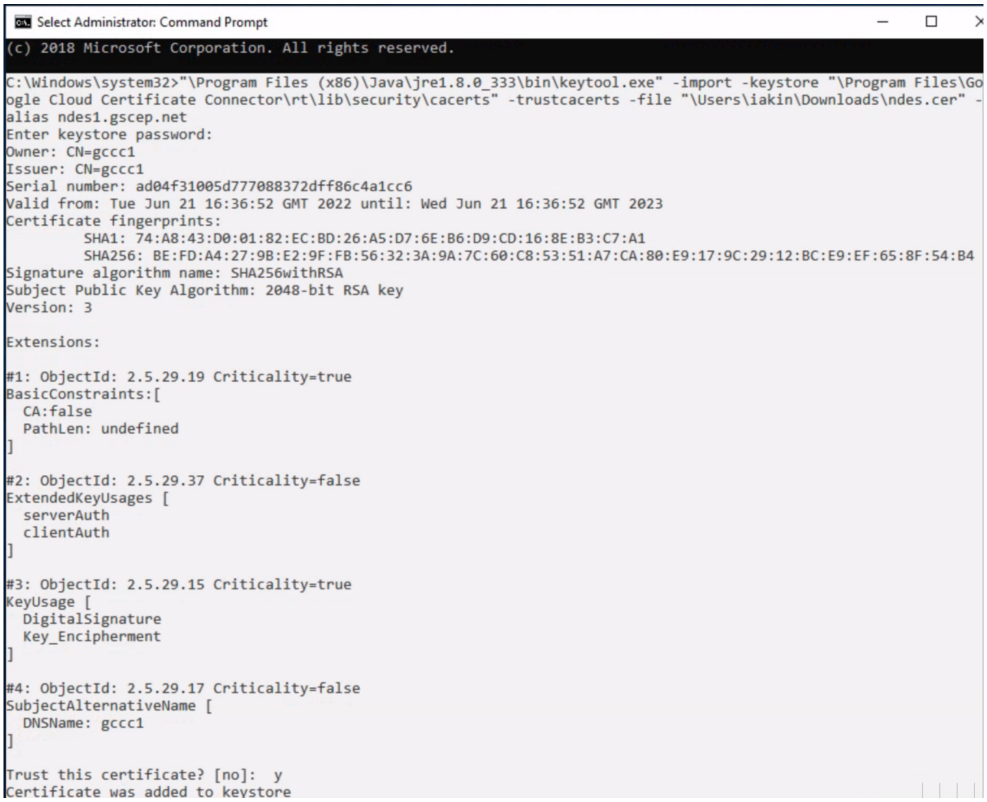
iii. Enter ***y*** to trust the certificate

iv.
```
<JRE_PATH>\bin\keytool.exe -import -keystore
<GCCC_PATH>\rt\lib\security\cacerts -trustcacerts -file
<NDES_CERT_LOCATION>\<NDES_CERT_FILE> -alias
<NDES_CERT_NICKNAME> -storepass changeit
```

v. Note: -alias is not required but is helpful to identify the imported CA certificate in the keystore

vi. Example:

```
1.  "\Program Files (x86)\Java\jre1.8.0_333\bin\keytool.exe"
    -import -keystore "\Program Files\Google Cloud Certificate
    Connector\rt\lib\security\cacerts" -trustcacerts -file
    "\Users\admin\Downloads\ndes.cer" -alias ndes1.gscep.net
    -storepass changeit
```



```
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>"\Program Files (x86)\Java\jre1.8.0_333\bin\keytool.exe" -import -keystore "\Program Files\Go
ogle Cloud Certificate Connector\rt\lib\security\cacerts" -trustcacerts -file "\Users\iakin\Downloads\ndes.cer" -
alias ndes1.gscep.net
Enter keystore password:
Owner: CN=gccc1
Issuer: CN=gccc1
Serial number: ad04f31005d777088372dff86c4a1cc6
Valid from: Tue Jun 21 16:36:52 GMT 2022 until: Wed Jun 21 16:36:52 GMT 2023
Certificate fingerprints:
         SHA1: 74:A8:43:D0:01:82:EC:BD:26:A5:D7:6E:B6:D9:CD:16:8E:B3:C7:A1
         SHA256: BE:FD:A4:27:9B:E2:9F:FB:56:32:3A:9A:7C:60:C8:53:51:A7:CA:80:E9:17:9C:29:12:BC:E9:EF:65:8F:54:B4
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:false
  PathLen: undefined
]

#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_Encipherment
]

#4: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: gccc1
]

Trust this certificate? [no]:  y
Certificate was added to keystore
```

Certificate attribute values will be different, but should match what is seen in the browser in step 5.a above.

Configure Google Admin SCEP and Wi-Fi profiles

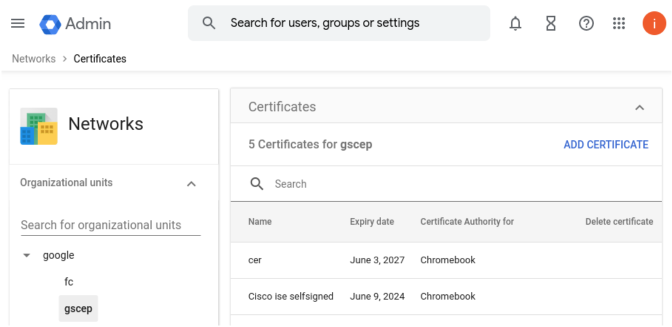
Configure the SCEP profile for static challenge and set up an EAP-TLS profile to automatically connect after a certificate is installed.

Import SCEP Issuing CA certificate

1. Sign in to the Google Admin console. Learn more
2. *Devices -> Networks*
   Requires having the Shared device settings administrator privilege.

3. Scroll down to *Certificates*

4. Select a child organizational unit if desired



5 Certificates for gscep

Name	Expiry date	Certificate Authority for	Delete certificate
cer	June 3, 2027	Chromebook	
Cisco ise selfsigned	June 9, 2024	Chromebook	

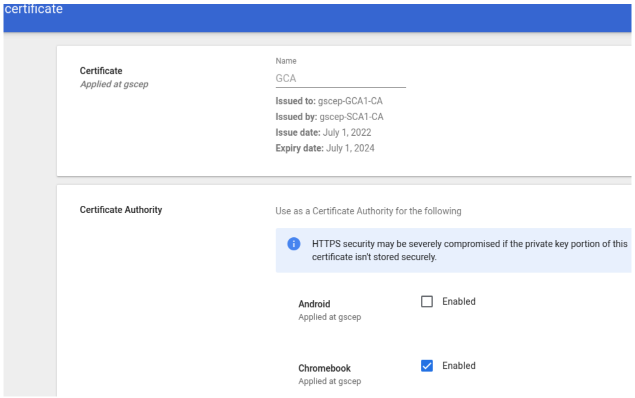
5. Click *ADD CERTIFICATE*

6. Click *Upload*, select the ***gca.cer*** NDES Issuing CA certificate exported earlier

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

    b. Use a descriptive *Name*

    c. Enable *Chromebook*



Certificate
Applied at gscep

Name
GCA

Issued to: gscep-GCA1-CA
Issued by: gscep-SCA1-CA
Issue date: July 1, 2022
Expiry date: July 1, 2024

Certificate Authority

Use as a Certificate Authority for the following

HTTPS security may be severely compromised if the private key portion of this certificate isn't stored securely.

Android
Applied at gscep
□ Enabled

Chromebook
Applied at gscep
☑ Enabled

Create SCEP Profile

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

2. *Devices -> Networks*
   Requires having the Shared device settings administrator privilege.

3. Scroll down to *Secure SCEP*

4. Select a child organizational unit if desired

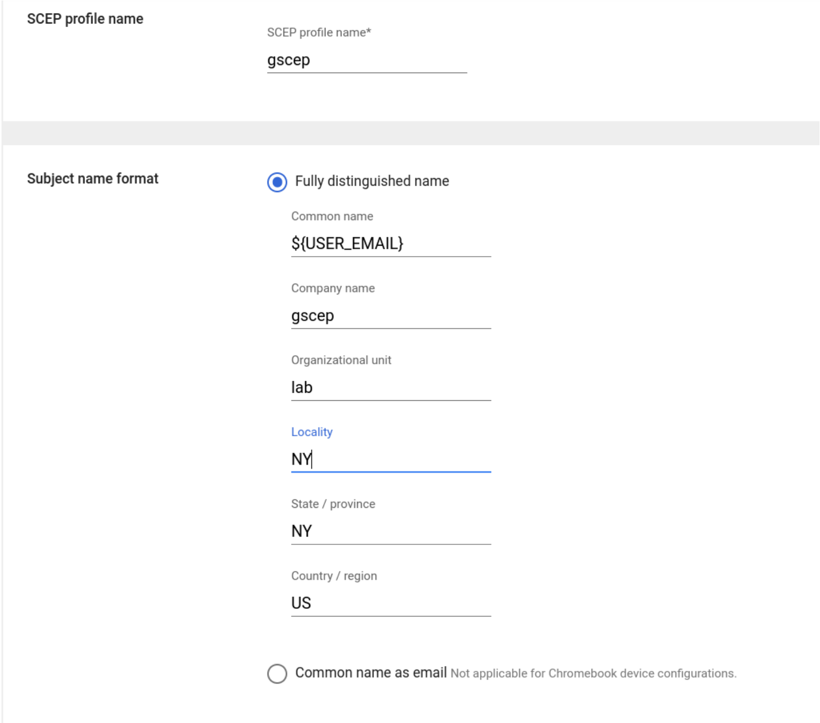
5. Click *Add secure SCEP profile*

6. Enter the configuration details for the profile.
    a. For details, see [Add a SCEP profile]

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

8. For *Subject name format*, choose how you want to identify the certificate owner.

9. For details about variables that you can use, see [Set up digital certificate provisioning].
    a. For user certificates, enter variable ***${USER_EMAIL}*** for *Common name* to automatically add the current user's User Principal Name (UPN) to the certificate request.
    b. For device certificates ***${DEVICE_SERIAL_NUMBER}*** can be used as *Common name*
    c. In Organizational unit, optionally include SCEP in the name to make the certificates easier to identify in the CA.
    d. **If the certificate needs to include a country code, it must be [standards compliant]- e.g. US**



SCEP profile name

SCEP profile name*: gscep

Subject name format

● Fully distinguished name

Common name: ${USER_EMAIL}

Company name: gscep

Organizational unit: lab

Locality: NY

State / province: NY

Country / region: US

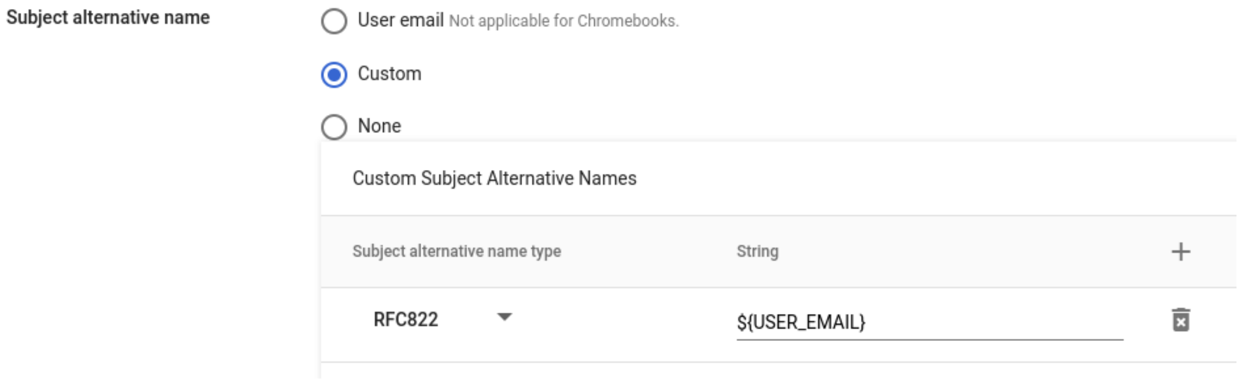
○ Common name as email Not applicable for Chromebook device configurations.

10. For *Subject Alternative Name*, provide an SAN.
    a. Click *Custom*
    b. For *Subject alternative name type*, select ***RFC822***.

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

i. 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

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



Subject alternative name

○ User email Not applicable for Chromebooks.

● Custom

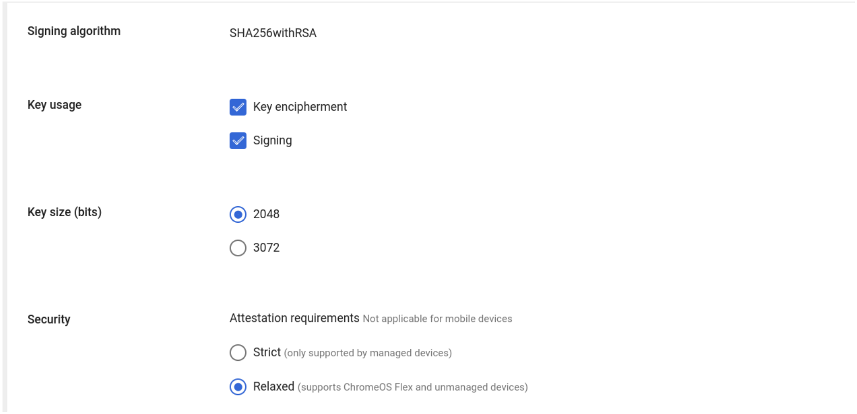
○ None

Custom Subject Alternative Names

Subject alternative name type	String	+
RFC822 ▾	${USER_EMAIL}	🗑

11. Signing algorithm and Key defaults are usually appropriate

12. Security setting of *Strict* enforces a [Verified Access](#) check that the device and user are affiliated (managed by the same domain) before issuing a certificate and that a device is in verified boot mode. *Relaxed* allows unmanaged and ChromeOS Flex devices.



Signing algorithm SHA256withRSA

Key usage

☑ Key encipherment

☑ Signing

Key size (bits)

● 2048

○ 3072

Security

Attestation requirements Not applicable for mobile devices

○ Strict (only supported by managed devices)

● Relaxed (supports ChromeOS Flex and unmanaged devices)

13. For *SCEP Server Attributes*:

a. Enter the URL of the SCEP server

b. Example:

i. https://ndes1.gscep.net/certsrv/mscep/mscep.dll

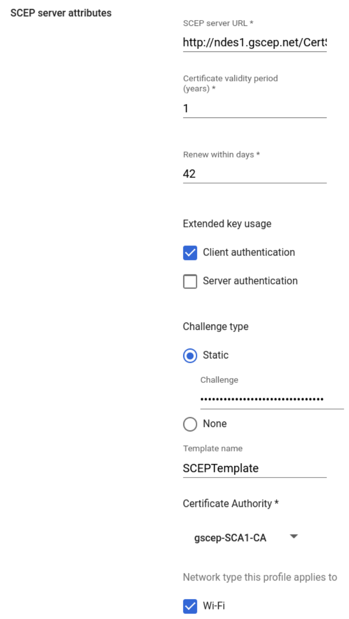
c. Check *Client authentication*

   d. Under *Challenge Type* select *Static* and paste the SCEP challenge password that was copied earlier.

   e. In the Template name field, enter the name of the template created earlier: ***SCEPTemplate***

   f. Under *Certificate Authority*, choose the name of the Issuing CA certificate imported to use as the Certificate Authority.

   g. Under *Network type this profile applies to*, check *Wi-Fi*.



SCEP server attributes

SCEP server URL *
http://ndes1.gscep.net/Certs

Certificate validity period (years) *
1

Renew within days *
42

Extended key usage

☑ Client authentication

□ Server authentication

Challenge type

● Static

Challenge
••••••••••••••••••••••••••••••••••

○ None

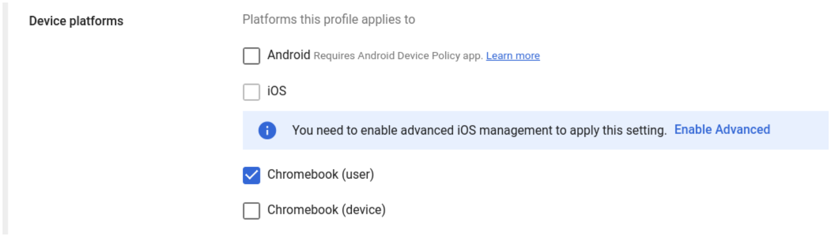
Template name
SCEPTemplate

Certificate Authority *
gscep-SCA1-CA

Network type this profile applies to

☑ Wi-Fi

14. For *Device platforms*, check the *Chromebook (user)* or *Chromebook (device)* box.



Device platforms

Platforms this profile applies to

□ Android Requires Android Device Policy app. Learn more

□ iOS

You need to enable advanced iOS management to apply this setting. Enable Advanced

☑ Chromebook (user)

□ Chromebook (device)

15. Save. If you configured a child organizational unit, you might be able to *Inherit or Override* a parent organizational unit's settings.

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*

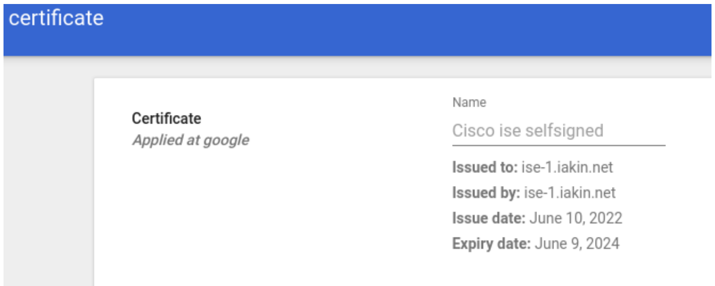
5. Select a child organizational unit if desired

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**



certificate

Certificate
Applied at google

Name
Cisco ise selfsigned

Issued to: ise-1.iakin.net
Issued by: ise-1.iakin.net
Issue date: June 10, 2022
Expiry date: June 9, 2024

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 Enterprise (802.1 X)***

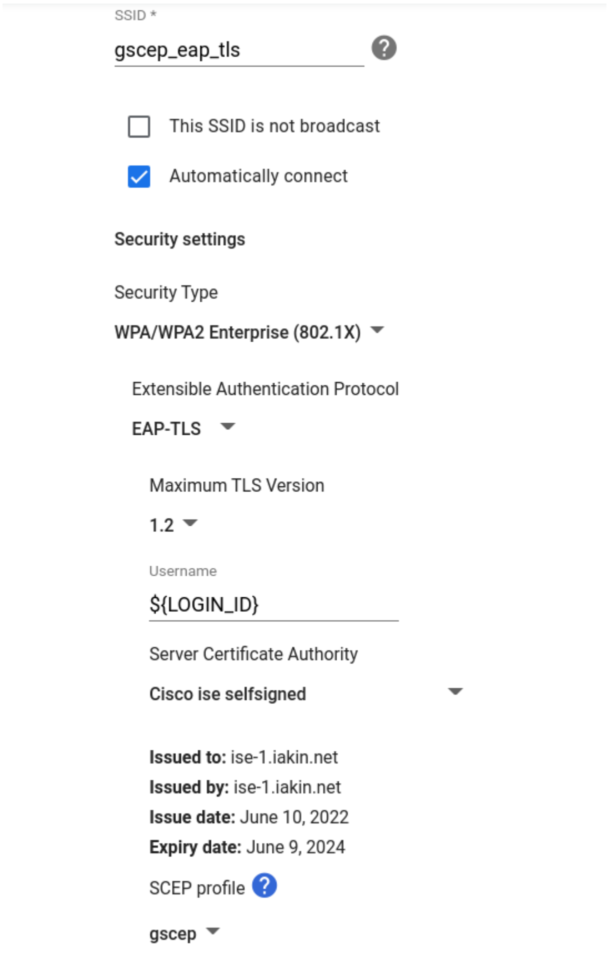
iv. For the *Extensible Authentication Protocol*, select ***EAP-TLS***

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. For *SCEP profile*, select the SCEP profile that you just created and want to apply to this network - ***gscep***



SSID *

gscep_eap_tls

□ This SSID is not broadcast

☑ Automatically connect

Security settings

Security Type

WPA/WPA2 Enterprise (802.1X)

Extensible Authentication Protocol

EAP-TLS

Maximum TLS Version

1.2

Username

${LOGIN_ID}

Server Certificate Authority

Cisco ise selfsigned

Issued to: ise-1.iakin.net
Issued by: ise-1.iakin.net
Issue date: June 10, 2022
Expiry date: June 9, 2024

SCEP profile

gscep

b. Click Save.

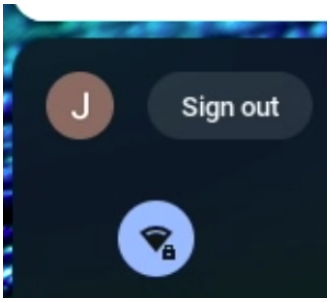
ChromeOS user experience

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.

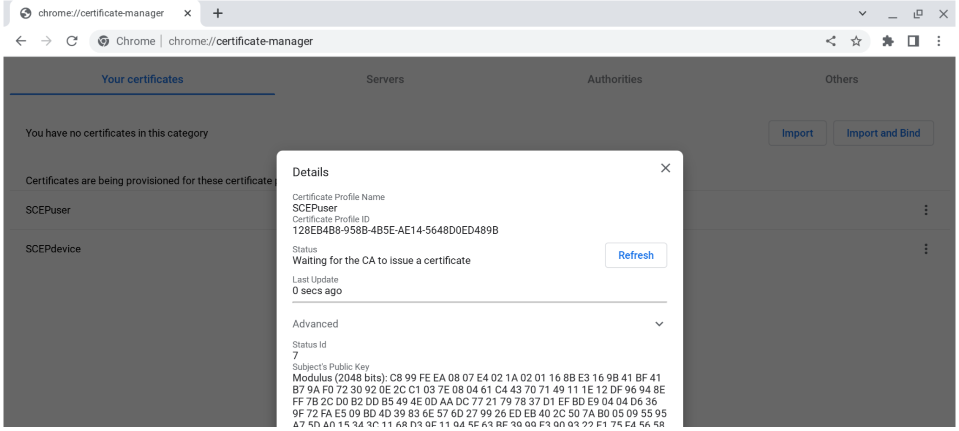
1. Managed user signs in to managed ChromeOS device.

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.



You have no certificates in this category

Certificates are being provisioned for these certificate

SCEPuser

SCEPdevice

Details

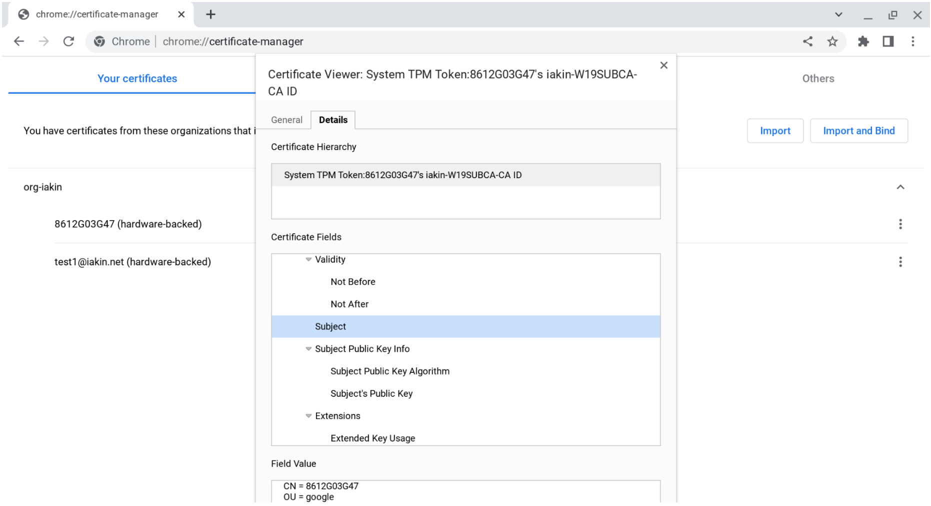
Certificate Profile Name
SCEPuser
Certificate Profile ID
128EB4B8-958B-4B5E-AE14-5648D0ED489B

Status
Waiting for the CA to issue a certificate

Last Update
0 secs ago

Status Id
7
Subject's Public Key
Modulus (2048 bits): C8 99 FE EA 08 07 E4 02 1A 02 01 16 8B E3 16 9B 41 BF 41
B7 9A F0 72 30 92 0E 2C C1 03 7E 08 04 61 C4 43 70 71 49 11 1E 12 DF 96 94 8E
FF 7B 2C D0 B2 DD B5 49 4E 0D AA DC 77 21 79 78 37 D1 EF BD E9 04 04 D6 36
9F 72 FA E5 09 BD 4D 39 83 6E 57 6D 27 99 26 ED EB 40 2C 50 7A B0 05 09 55 95
A7 5D A0 15 34 3C 11 68 D3 9F 11 94 5F 63 BF 39 99 F3 90 93 22 F1 75 F4 56 58

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



chrome://certificate-manager

Chrome | chrome://certificate-manager

Your certificates

Others

You have certificates from these organizations that i

Import

Import and Bind

org-iakin

8612G03G47 (hardware-backed)

test1@iakin.net (hardware-backed)

Certificate Viewer: System TPM Token:8612G03G47's iakin-W19SUBCA-CA ID

General

Details

Certificate Hierarchy

System TPM Token:8612G03G47's iakin-W19SUBCA-CA ID

Certificate Fields

- Validity
  - Not Before
  - Not After
- Subject
- Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key
- Extensions
  - Extended Key Usage

Field Value

CN = 8612G03G47
OU = google

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.

Troubleshooting

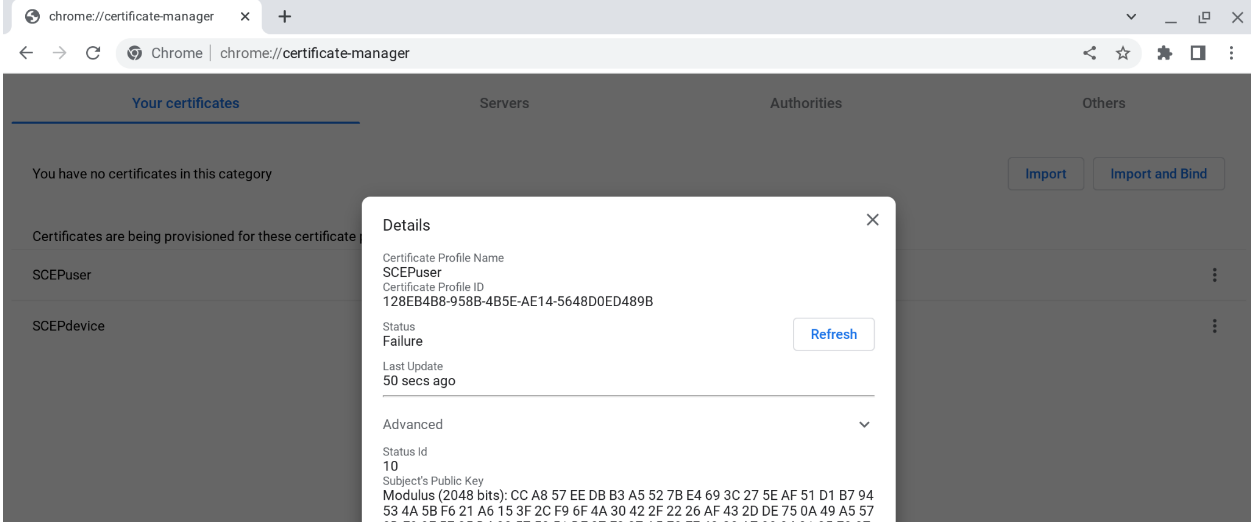
ChromeOS device

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:



chrome://certificate-manager
Chrome | chrome://certificate-manager
Your certificates
Servers
Authorities
Others
Import
Import and Bind

You have no certificates in this category

Certificates are being provisioned for these certificate

SCEPuser

SCEPdevice

Details

Certificate Profile Name
SCEPuser
Certificate Profile ID
128EB4B8-958B-4B5E-AE14-5648D0ED489B

Status
Failure

Last Update
50 secs ago

Status Id
10
Subject's Public Key
Modulus (2048 bits): CC A8 57 EE DB B3 A5 52 7B E4 69 3C 27 5E AF 51 D1 B7 94 53 4A 5B F6 21 A6 15 3F 2C F9 6F 4A 30 42 2F 22 26 AF 43 2D DE 75 0A 49 A5 57

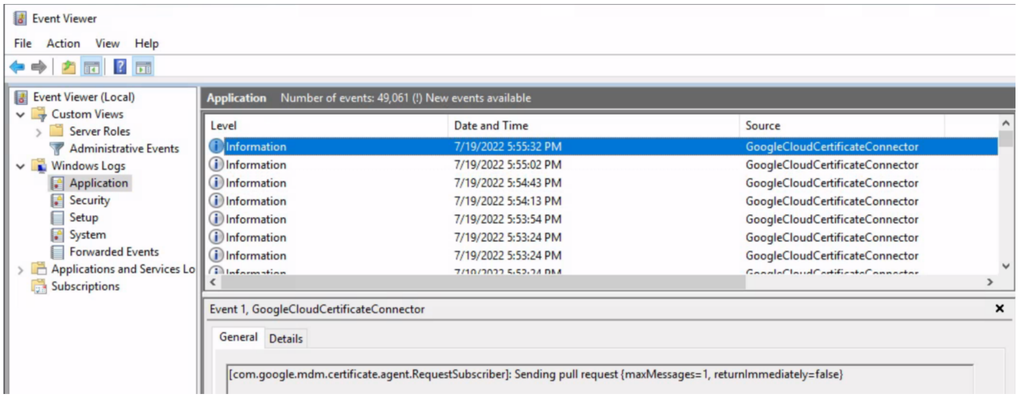
GCCC

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 {}
```



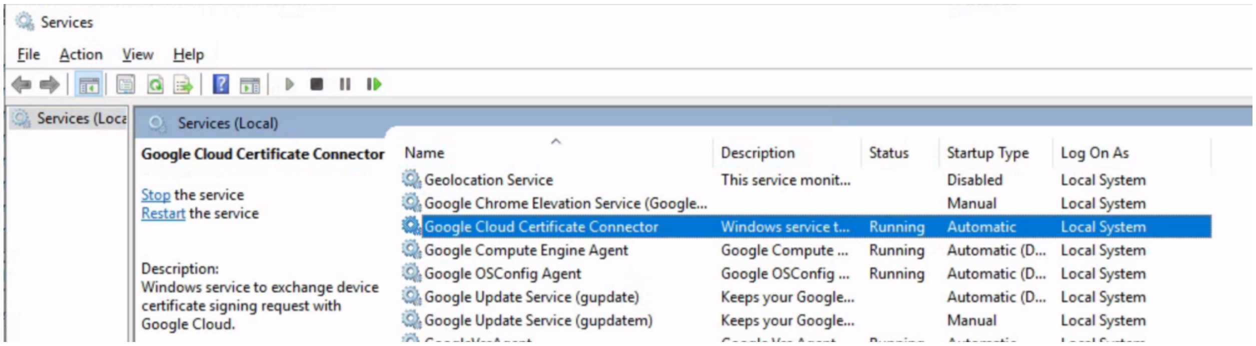
Application Number of events: 49,061 (!) New events available

Level	Date and Time	Source
Information	7/19/2022 5:55:32 PM	GoogleCloudCertificateConnector
Information	7/19/2022 5:55:02 PM	GoogleCloudCertificateConnector
Information	7/19/2022 5:54:43 PM	GoogleCloudCertificateConnector
Information	7/19/2022 5:54:13 PM	GoogleCloudCertificateConnector
Information	7/19/2022 5:53:54 PM	GoogleCloudCertificateConnector
Information	7/19/2022 5:53:24 PM	GoogleCloudCertificateConnector
Information	7/19/2022 5:53:24 PM	GoogleCloudCertificateConnector

Event 1, GoogleCloudCertificateConnector

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

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.



Google Cloud Certificate Connector

Stop the service
Restart the service

Description:
Windows service to exchange device certificate signing request with Google Cloud.

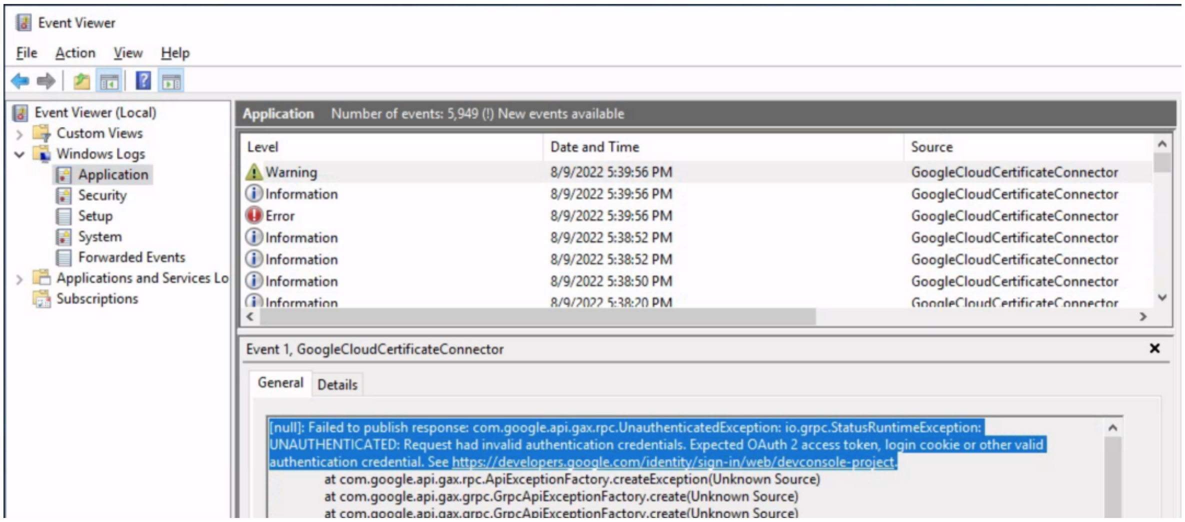
Name	Description	Status	Startup Type	Log On As
Geolocation Service	This service monit...		Disabled	Local System
Google Chrome Elevation Service (Google...			Manual	Local System
Google Cloud Certificate Connector	Windows service t...	Running	Automatic	Local System
Google Compute Engine Agent	Google Compute ...	Running	Automatic (D...	Local System
Google OSConfig Agent	Google OSConfig ...	Running	Automatic (D...	Local System
Google Update Service (gupdate)	Keeps your Google...		Automatic (D...	Local System
Google Update Service (gupdatem)	Keeps your Google...		Manual	Local System

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
```



Application Number of events: 5,949 (!) New events available

Level	Date and Time	Source
Warning	8/9/2022 5:39:56 PM	GoogleCloudCertificateConnector
Information	8/9/2022 5:39:56 PM	GoogleCloudCertificateConnector
Error	8/9/2022 5:39:56 PM	GoogleCloudCertificateConnector
Information	8/9/2022 5:38:52 PM	GoogleCloudCertificateConnector
Information	8/9/2022 5:38:52 PM	GoogleCloudCertificateConnector
Information	8/9/2022 5:38:50 PM	GoogleCloudCertificateConnector
Information	8/9/2022 5:38:20 PM	GoogleCloudCertificateConnector

Event 1, GoogleCloudCertificateConnector

```
[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
authentication credential. See https://developers.google.com/identity/sign-in/web/devconsole-project.
        at com.google.api.gax.rpc.ApiExceptionFactory.createException(Unknown Source)
        at com.google.api.gax.grpc.GrpcApiExceptionFactory.create(Unknown Source)
        at com.google.api.gax.grpc.GrpcApiExceptionFactory.create(Unknown Source)
```

Enrollment Event Logs

Successful

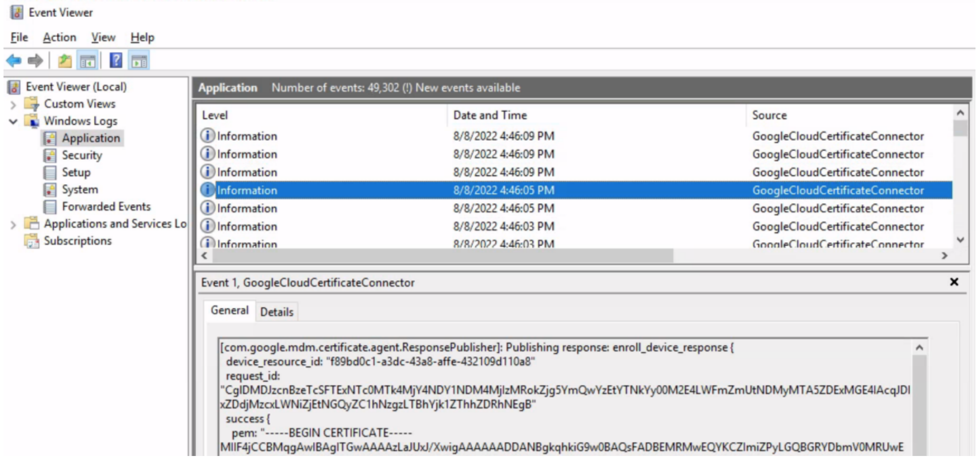
During a successful certificate enrollment, following events will be logged:

```
[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 {...
```



Application Number of events: 49,302 (!) New events available

Level	Date and Time	Source
Information	8/8/2022 4:46:09 PM	GoogleCloudCertificateConnector
Information	8/8/2022 4:46:09 PM	GoogleCloudCertificateConnector
Information	8/8/2022 4:46:09 PM	GoogleCloudCertificateConnector
Information	8/8/2022 4:46:05 PM	GoogleCloudCertificateConnector
Information	8/8/2022 4:46:05 PM	GoogleCloudCertificateConnector
Information	8/8/2022 4:46:03 PM	GoogleCloudCertificateConnector
Information	8/8/2022 4:46:03 PM	GoogleCloudCertificateConnector

```
[com.google.mdm.certificate.agent.ResponsePublisher]: Publishing response: enroll_device_response {
  device_resource_id: "f89bd0c1-a3dc-43a8-affe-432109d110a8"
  request_id:
"CgIDMDJzcnBzeTcSFTExNTc0MTk4MjY4NDY1NDM4MjIzMRokZjg5YmQwYzEtYTNkYy00M2E4LWFmZmUtNDMyMTA5ZDExMGE4IAcqJDI
xZDdjMzcxLWNiZjEtNGQyZC1hNzgzLTBhYjk1ZThhZDRhNEgB"
  success {
   pem: "-----BEGIN CERTIFICATE-----
MIIF4jCCBMqgAwIBAgITGwAAAAzLaJUxJ/XwigAAAAAADDANBgkqhkiG9w0BAQsFADBEMRMwEQYKCZImiZPyLGQBGRYDbmV0MRUwE
```

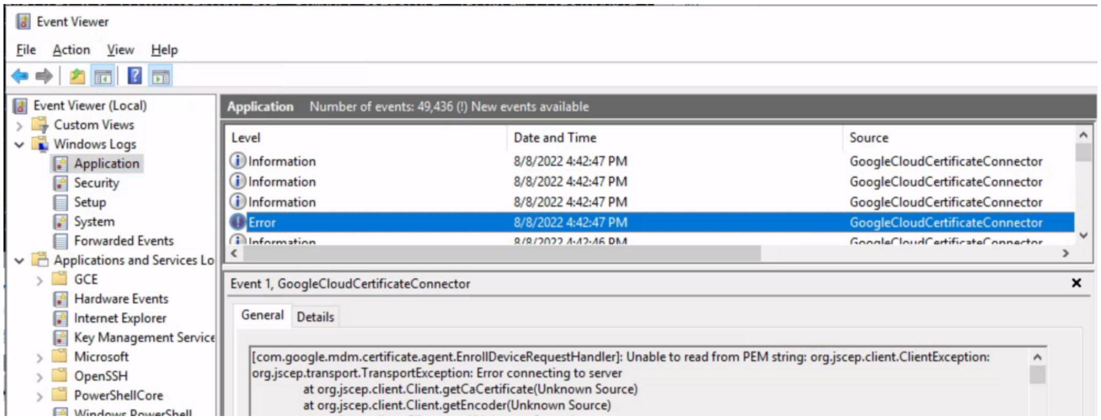
```
[java.lang.String]: 123…|
```

```
[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.

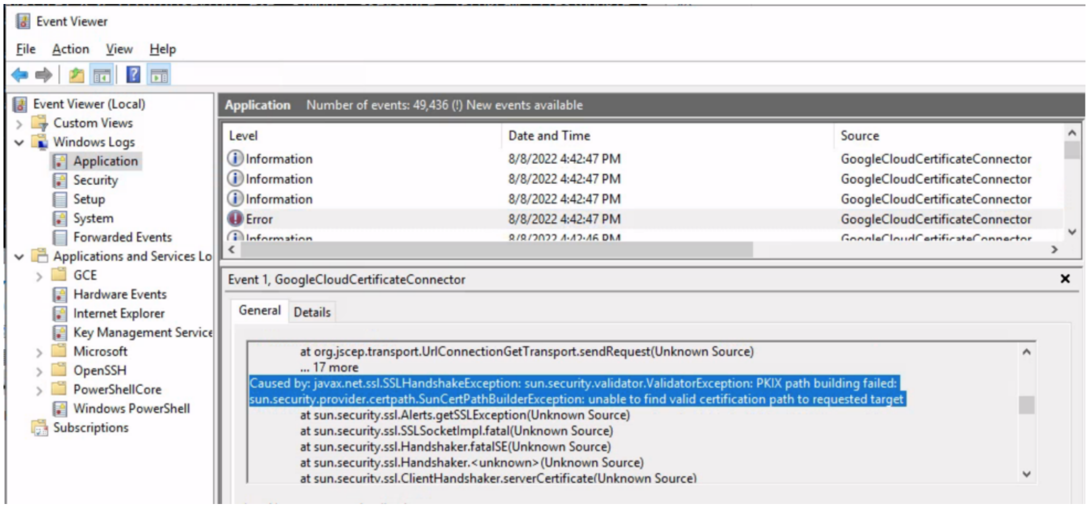


Application Number of events: 49,436 (!) New events available

Level	Date and Time	Source
Information	8/8/2022 4:42:47 PM	GoogleCloudCertificateConnector
Information	8/8/2022 4:42:47 PM	GoogleCloudCertificateConnector
Information	8/8/2022 4:42:47 PM	GoogleCloudCertificateConnector
Error	8/8/2022 4:42:47 PM	GoogleCloudCertificateConnector
Information	8/8/2022 4:42:46 PM	GoogleCloudCertificateConnector

```
[com.google.mdm.certificate.agent.EnrollDeviceRequestHandler]: Unable to read from PEM string: org.jscep.client.ClientException:
org.jscep.transport.TransportException: Error connecting to server
        at org.jscep.client.Client.getCaCertificate(Unknown Source)
        at org.jscep.client.Client.getEncoder(Unknown Source)
```

"***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.



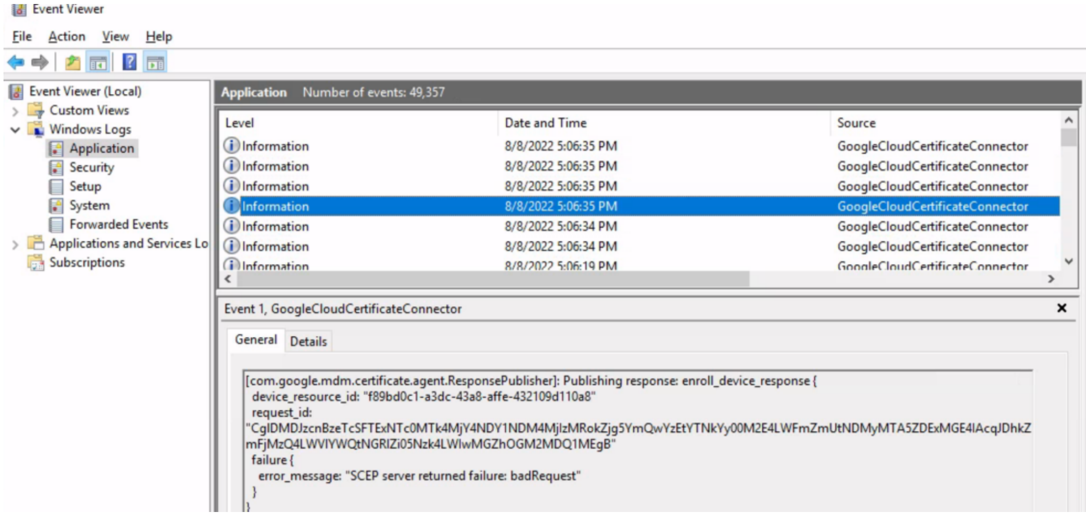
```
Application   Number of events: 49,436 (!) New events available

Level          Date and Time           Source
Information    8/8/2022 4:42:47 PM     GoogleCloudCertificateConnector
Information    8/8/2022 4:42:47 PM     GoogleCloudCertificateConnector
Information    8/8/2022 4:42:47 PM     GoogleCloudCertificateConnector
Error          8/8/2022 4:42:47 PM     GoogleCloudCertificateConnector
Information    8/8/2022 4:42:46 PM     GoogleCloudCertificateConnector
```

Event 1, GoogleCloudCertificateConnector

```
        at org.jscep.transport.UrlConnectionGetTransport.sendRequest(Unknown Source)
        ... 17 more
Caused by: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
        at sun.security.ssl.Alerts.getSSLException(Unknown Source)
        at sun.security.ssl.SSLSocketImpl.fatal(Unknown Source)
        at sun.security.ssl.Handshaker.fatalSE(Unknown Source)
        at sun.security.ssl.Handshaker.<unknown>(Unknown Source)
        at sun.security.ssl.ClientHandshaker.serverCertificate(Unknown Source)
```

"***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.



```
Application   Number of events: 49,357

Level          Date and Time           Source
Information    8/8/2022 5:06:35 PM     GoogleCloudCertificateConnector
Information    8/8/2022 5:06:35 PM     GoogleCloudCertificateConnector
Information    8/8/2022 5:06:35 PM     GoogleCloudCertificateConnector
Information    8/8/2022 5:06:35 PM     GoogleCloudCertificateConnector
Information    8/8/2022 5:06:34 PM     GoogleCloudCertificateConnector
Information    8/8/2022 5:06:34 PM     GoogleCloudCertificateConnector
Information    8/8/2022 5:06:19 PM     GoogleCloudCertificateConnector
```

Event 1, GoogleCloudCertificateConnector

```
[com.google.mdm.certificate.agent.ResponsePublisher]: Publishing response: enroll_device_response {
  device_resource_id: "f89bd0c1-a3dc-43a8-affe-432109d110a8"
  request_id:
"CgIDMDJzcnBzeTcSFTExNTc0MTk4MjY4NDY1NDM4MjIzMRokZjg5YmQwYzEtYTNkYy00M2E4LWFmZmUtNDMyMTA5ZDExMGE4IAcqJDhkZ
mFjMzQ4LWVlYWQtNGRlZi05Nzk4LWIwMGZhOGM2MDQ1MEgB"
  failure {
    error_message: "SCEP server returned failure: badRequest"
  }
}
```

"***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.

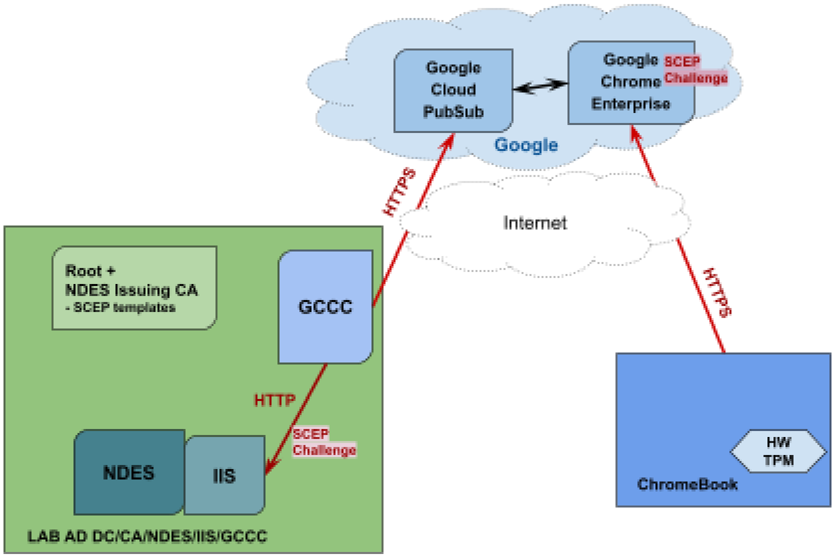
ChromeOS device device logs

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

Appendix

Lab Deployment Diagram

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


Google Cloud PubSub
Google Chrome Enterprise
SCEP Challenge
Google
HTTPS
Internet
HTTPS
Root + NDES Issuing CA - SCEP templates
GCCC
HTTP
SCEP Challenge
NDES
IIS
LAB AD DC/CA/NDES/IIS/GCCC
HW TPM
ChromeBook