



Notes from the field

Configuring Certificate Enrollment for ChromeOS via SCEP with Microsoft NDES

For administrators with Active Directory expertise

February 2024

Contents

Overview

Google Admin Console

ChromeOS

Microsoft Certificate Services and NDES/SCEP

Google Cloud Certificate Connector

Enterprise Deployment with Microsoft NDES

Prerequisites

Create Service account for NDES

Configure Issuing CA for NDES

- 1. Add Active Directory Certificate Services role to the Issuing CA server for NDES gca1.gscep.net
- 2. Configure AD CS on gca1.gscep.net as a Subordinate CA to an existing CA sca1.gscep.net
- 3. Create the SCEP certificate template
- 4. Allow NDES Service to enroll and manage certificates
- 5. Export Issuing CA Certificate
- 6. Disable all other Certificate Templates (Optional)

Configure NDES and IIS

- 1. Add Active Directory Certificate Services role to the server ndes1.gscep.net
- 2. Add NDES Service Account to local IIS_IUSRS Group
- 3. Configure NDES Service
- 4. (Optional) Configure default NDES template
- 5. Configure NDES to utilize a static SCEP challenge password
- 6. Bind SSL server certificate in IIS
- 7. Configure IIS the application pool
- 8. Enable IIS SCEP Application Pool Load User Profile
- 9. (Optional) Adjust IIS Request Filtering parameters
- 10. Disable Internet Explorer Enhanced Security Configuration
- 11. (Optional) Set the SPN of the NDES Service account
- 12. Restart NDES Server
- 13. Retrieve SCEP Challenge
- 14. (Optional) Configure Windows Firewall

Configure Google Cloud Certificate Connector

- 1. Download Google Cloud Certificate Connector
- 2. Install Google Cloud Certificate Connector.
- 3. Configure GCCC Service
- 4. Import NDES Server Certificate into GCCC Keystore (Only for HTTPS)

Configure Google Admin SCEP and Wi-Fi profiles

Import SCEP Issuing CA certificate

Create SCEP Profile

Import EAP-TLS RADIUS server certificate

Configure Wi-Fi profile

ChromeOS user experience

FAO



Certificate renewal
Troubleshooting
ChromeOS device
GCCC

Service Errors
Enrollment Event Logs

Successful

NDES Server Communication issues

Certificate retrieval via SCEP

Contact support

Connector logs

ChromeOS device device logs

Appendix

Lab Deployment Diagram

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.

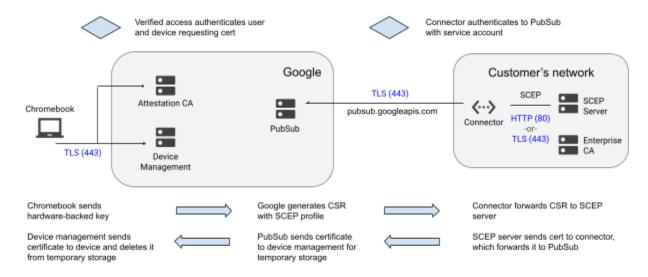
©2022 Google LLC All rights reserved. Google and the Google logo are registered trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated. [EXTENSIONS-en-1.0]



Overview

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

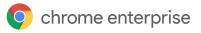
Google Admin Console is the web based administrative interface used to configure and apply policy to Chrome Enterprise devices and browsers.

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 <u>communicate with Google Cloud services</u> 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 <u>Certificate Connector for Microsoft Intune installs a custom policy module</u> 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

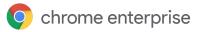
Microsoft <u>recommends</u> a <u>two- or three-tier PKI</u> deployment for production environments. In such a deployment, the Root Certificate Authority (CA) and possibly the first tier Intermediate CAs are kept offline (not connected to the production network). Issuing CAs are kept online to facilitate 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 <u>Issuing CA for NDES</u> 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 <u>Constraints</u> (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 <u>removed</u> 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 <u>does not support</u>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.

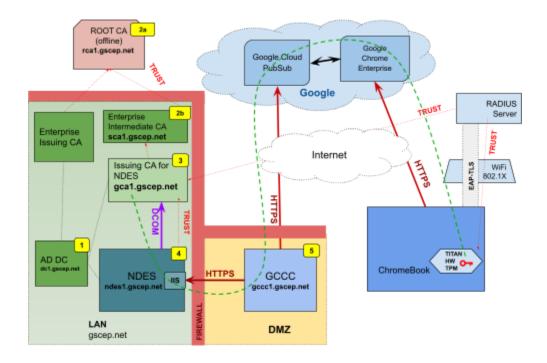
The NDES IIS server SSL certificate Subject Name needs to match the hostname used in the SCEP enrollment URL.

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.

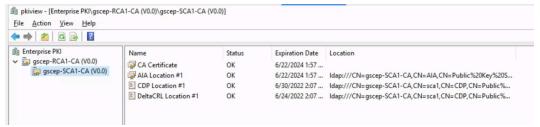
Enterprise Deployment with Microsoft NDES



Prerequisites

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

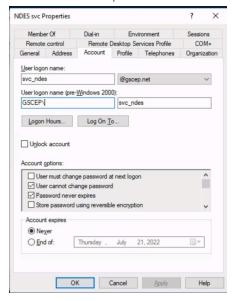
- 1. Existing Windows **AD Domain**
 - a. Domain Controller dc1.gscep.net
- 2. Existing Microsoft Enterprise PKI
 - a. Root CA rca1.gscep.net (offline)
 - b. At least one **Intermediate CA sca1.gscep.net** available to issue a CA Certificate for *Issuing CA for NDES*
 - c. Running **pkiview.msc** as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

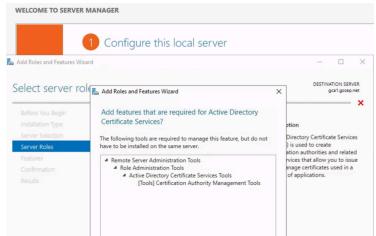
Create Service account for NDES

- 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.



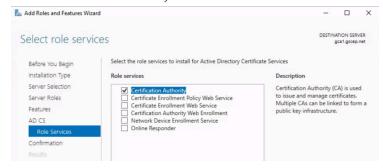
Configure Issuing CA for NDES

- 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

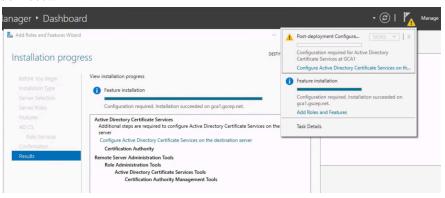




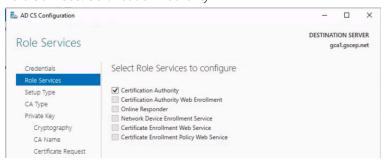
f. Select Certification Authority from Role Services



- 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

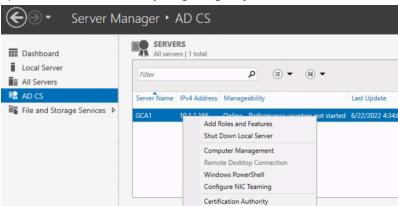


- d. Setup Type: Enterprise CA
- e. CA Type: Subordinate CA
- f. Create a new private key
- g. Select defaults or adjust as needed for Cryptography and CA Name
- h. Certificate Request: Send a certificate request to a parent CA
- i. CA Name or Computer name

j. Select appropriate existing **Subordinate** Issuing CA from which to request a CA certificate for the *Issuing CA for NDES* - **sca1.gscep.net**



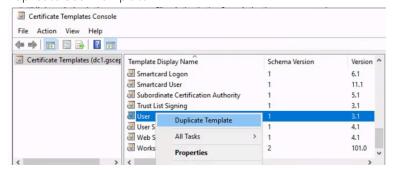
- k. Accept defaults for the rest and click Configure
- 3. Create the SCEP certificate template
 - a. Note that while these settings have been verified, your organization's policy might dictate different settings, which would need to be tested.
 - b. Open Certification Authority on gca1.gscep.net



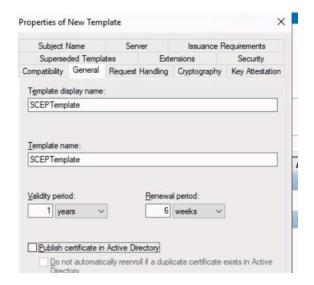
c. Certificate Templates -> Manage



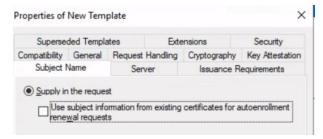
d. Duplicate User Template



- 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

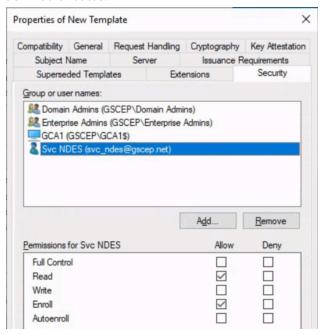


- f. Subject Name -> **Supply in the request**
- g. Note: This is necessary since the user or device name is supplied during enrollment via SCEP.

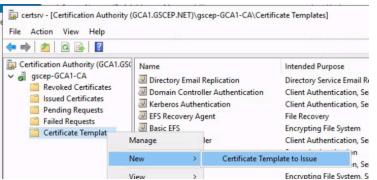


- h. Security
 - i. Add NDES service account **svc_ndes** with **Read** and **Enroll** permissions
 - ii. Add CA computer account of **gca1.gscep.net** with *Read* permission
 - iii. Remove Authenticated Users

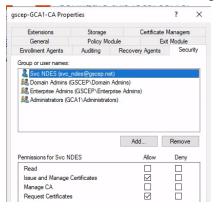
iv. Note: this ensures that NDES service, CA and Admins **ONLY** can issue or read the SCEP certificates.



- b. Close Certificate Templates Console
- c. Back in Certification Authority
 - i. Certificate Templates -> New -> Certificate Template to Issue
 - ii. Select **SCEPTemplate**

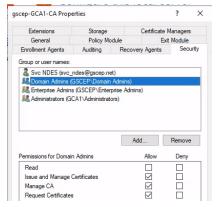


- 4. Allow NDES Service to enroll and manage certificates
 - a. Open Certification Authority -> gscep-GCA1-CA -> Properties -> Security
 - b. Add svc_ndes with Issue and Manage and Request Certificates permissions



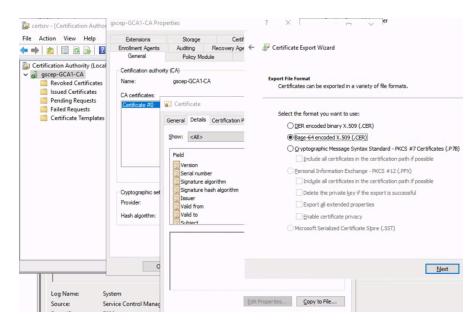


- c. **Optional** Remove Authenticated Users
- d. Note: This ensures that only NDES or Admins can issue certificates on this CA
- e. Make sure Domain Admins, or the account that is being used to install and configure NDES have the right to Request Certificates



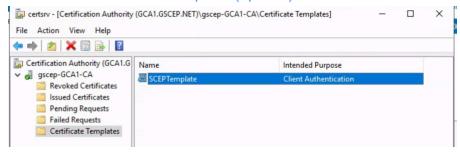
5. Export Issuing CA Certificate

- 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



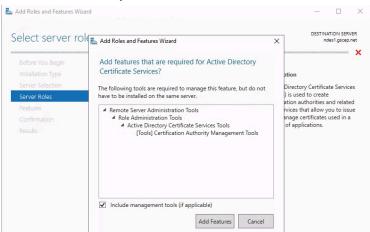


6. Disable all other Certificate Templates (Optional)



Configure NDES and IIS

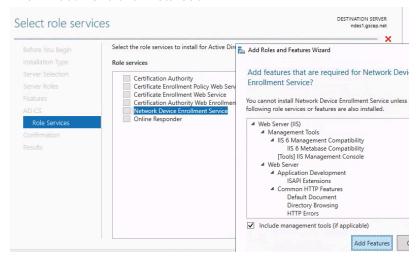
- 1. Add Active Directory Certificate Services role to the server ndes1.gscep.net
 - a. Log in as an **Enterprise Domain Admin** user, or another user with sufficient privileges to add Certificate Service role
 - b. Start Server Manager
 - c. Dashboard > Add roles and features > Select *ndes1.gscep.net*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



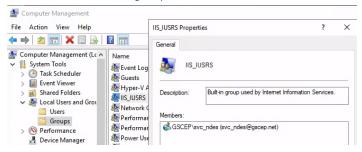
- e. Select role services:
 - i. Certification Authority Uncheck
 - ii. Network Device Enrollment Service Check



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...



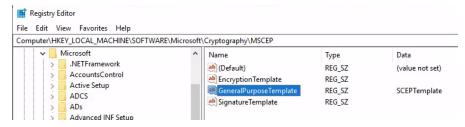
- c. Role Services: Network Device Enrollment Service
- d. Use the Enterprise Admin Credentials from step 1 to configure role services
- e. Service Account: **svc_ndes**



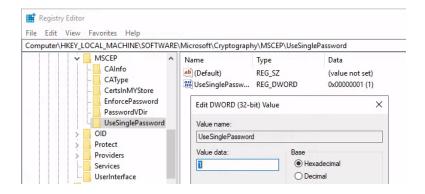
- f. CA for NDES: CA name
 - i. Select gca1.gscep.net
 - ii. Note: This is the CA that will issue certificates for devices/users



- 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\Ge\
 neralPurposeTemplate
 - 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

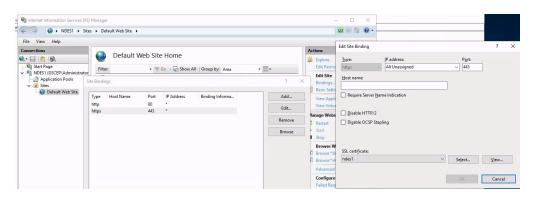


- 5. Configure NDES to utilize a static SCEP challenge password
 - a. This step is necessary because multiple devices will be requesting certificates via GCCC
 - $b. \ \textit{HKEY_LOCAL_MACHINE} \\ \ \textit{SOFTWARE} \\ \ \textit{Microsoft} \\ \ \textit{Cryptography} \\ \ \textit{MSCEP} \\ \ \textit{UseSingle Password}$
 - c. Set value of UseSinglePassword to 1



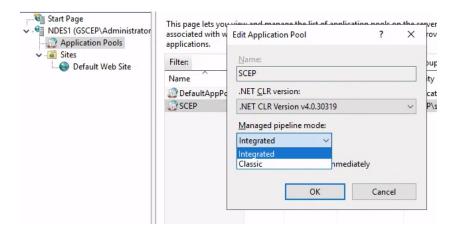
6. Bind SSL server certificate in IIS

- 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 <u>the SCEP URL.</u> Also be sure to obtain the signing certificates in the path, including the Root CA.



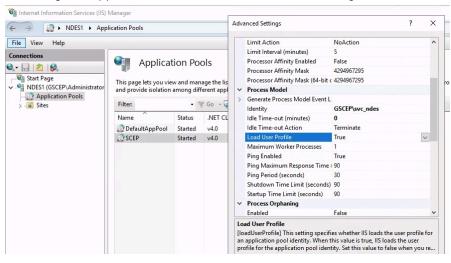
7. Configure IIS the application pool

- 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



9. (Optional) Adjust IIS Request Filtering parameters

C.

- a. Note that this step applies only if request filtering is enabled on IIS and/or there are URI Request too long errors <u>per Microsoft recommendations</u>
- b. IIS manager -> Default Web Site > Request Filtering > Edit Feature Setting
- c. Maximum URL length (Bytes) = **8096**
- d. Maximum guery 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



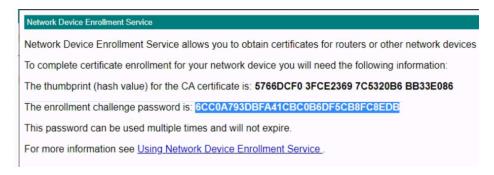
11. (Optional) Set the SPN of the NDES Service account

- 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.

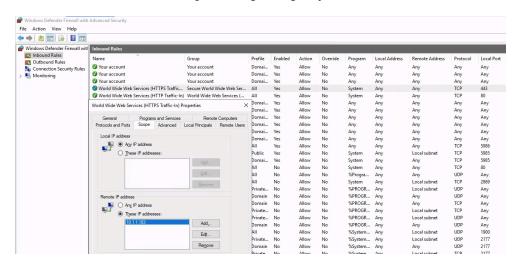


14. (Optional) Configure Windows Firewall

a. Open Windows Firewall Advanced Settings -> Inbound Rules

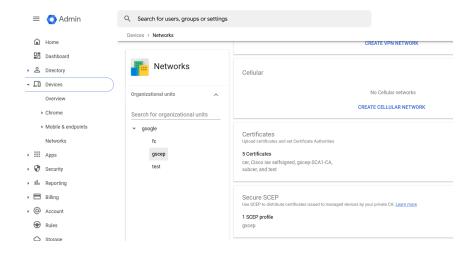


- b. Locate 2 Rules named World Wide Web Services HTTP/S Traffic In
- c. For both, modify Scope -> Remote Addresses
 - i. Select These IP Addresses
 - ii. Add IP of server running GCCC gccc1.gscep.net



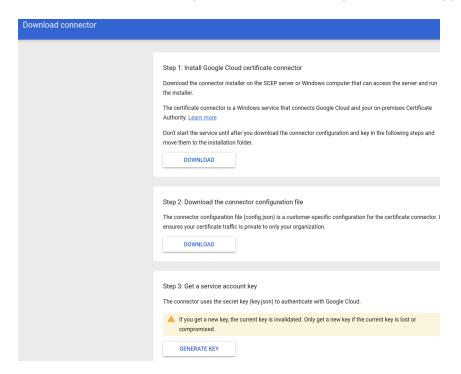
Configure Google Cloud Certificate Connector

- 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 <u>organizational unit</u>.





- 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.

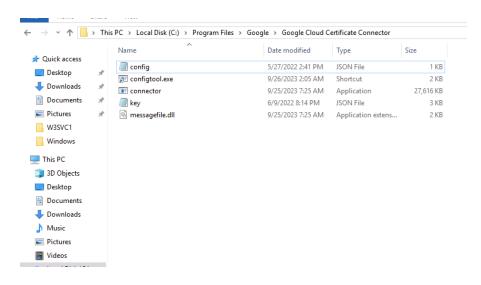


- I. If needed, transfer the GCCC installer and configuration and key files (**config.json** and **key.json**) to the GCCC server **gccc1.gscep.net**
- 2. Install Google Cloud Certificate Connector.
 - **a.** If your network requires a proxy, see the "Auto Update Proxy Settings" FAQ as the installer will depend on this process
 - b. Run the **google-cloud-certificate-connector-setup** as an administrator

c. On the ConfigTool command line window, enter the name and password of an account that has *Log on as a service* Right on the GCCC Server. (e.g. domain\account)



- i. Note: The service can be later changed to run as *Local System* if desired, by launching the ConfigTool from the executable shortcut named **configtool.exe** found in the same installation directory as the connector.
- d. Once install is complete, copy config.json and key.json to the installation directory C:\Program Files\Google Cloud Certificate Connector\



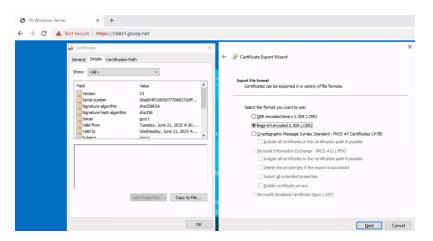


3. Configure GCCC Service

- a. Open Administrative Tools > Services
- b. Locate Google Cloud Certificate Connector
- c. Start service

4. 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

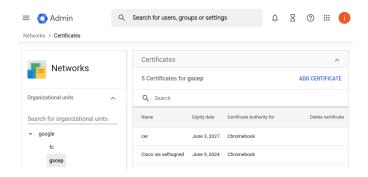
Configure Google Admin SCEP and Wi-Fi profiles

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

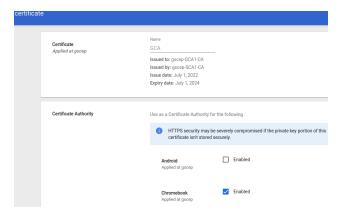
Import SCEP Issuing CA certificate

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

- 3. Scroll down to Certificates
- 4. Select a child organizational unit if desired



- 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

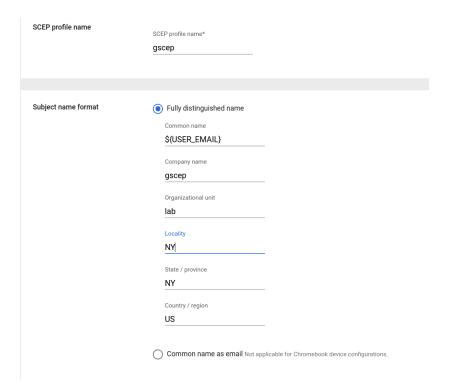


Create SCEP Profile

- 1. Sign in to the Google Admin console. Learn more
- 2. Devices -> Networks
 Requires having the <u>Shared device settings</u> administrator privilege.
- 3. Scroll down to Secure SCEP
- 4. Select a child organizational unit if desired
- 5. Click Add secure SCEP profile



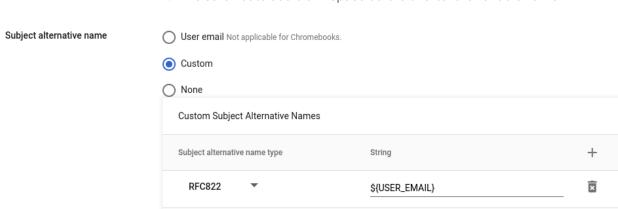
- 6. Enter the configuration details for the profile.
 - a. For details, see Add a SCEP profile
- 7. For SCEP profile name, enter a descriptive name, shown in the list of profiles.
- 8. For Subject name format, choose how you want to identify the certificate owner.
- 9. For details about variables that 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 <u>standards</u> <u>compliant</u> e.g. US



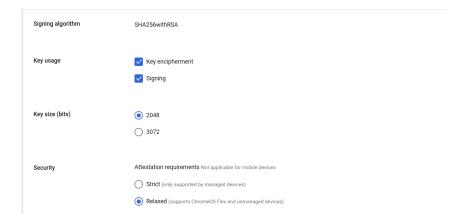
- 10. For Subject Alternative Name, provide an SAN.
 - a. Click Custom
 - b. For Subject alternative name type, select RFC822.



- c. For String, enter \${USER_EMAIL}
 - 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



- 11. Signing algorithm and Key defaults are usually appropriate
- 12. Security setting of *Strict* enforces a <u>Verified Access</u> 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.



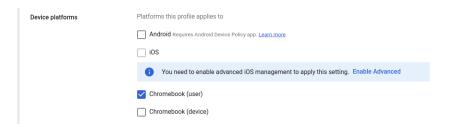
- 13. For SCEP Server Attributes:
 - a. Enter the URL of the SCEP server
 - **b.** Example:
 - i. https://ndes1.gscep.net/certsrv/mscep/mscep.dll
 - c. Check Client authentication



- **d.** Under *Challenge Type* select *Static* and paste the <u>SCEP challenge password</u> that was copied earlier.
- e. In the Template name field, enter the name of the <u>template created</u> earlier: **SCEPTemplate**
- **f.** Under *Certificate Authority*, choose the name of the <u>Issuing CA certificate imported</u> to use as the Certificate Authority.
- g. Under Network type this profile applies to, check Wi-Fi.



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



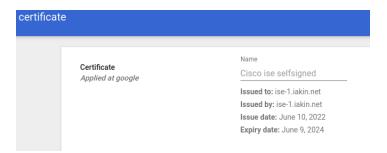
15. Save. If you configured a child organizational unit, you might be able to *Inherit or Override* a parent organizational unit's settings.

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
- Devices -> Networks
 Requires having the <u>Shared device settings</u> 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

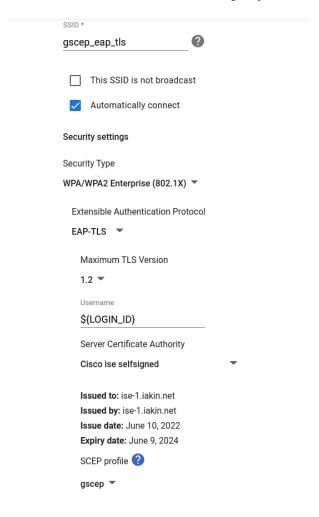


Configure Wi-Fi profile

- 1. Sign in to the Google Admin console. Learn more
- 2. Devices -> Networks -> WI-FI
 Requires having the <u>Shared device settings</u> 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 <u>RADIUS TLS Certificate</u> <u>imported earlier</u> **Cisco ISE Certificate**
- viii. For SCEP profile, select the SCEP profile that you just created and want to apply to this network **gscep**



b. Click Save.

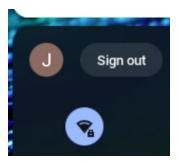
ChromeOS user experience

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.

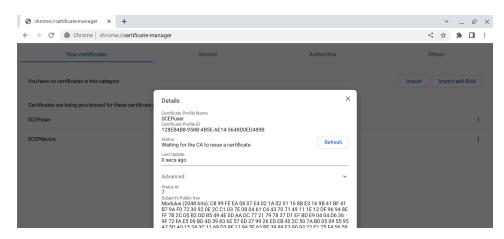


Note: Make sure that ChromeOS devices are in an organizational unit that your CA root cert will be pushed to and your users are in the organizational unit that you just created the SCEP and Wi-Fi profile for.

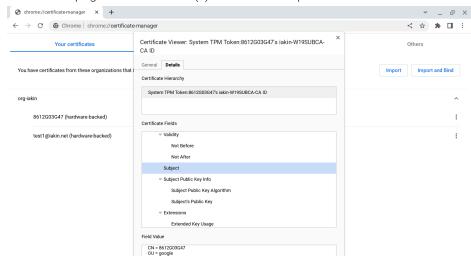
- 1. Managed user signs in to managed ChromeOS device.
- 2. At the bottom right of the ChromeOS device screen, click the time. You'll see the previous SSID used at startup.



- 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.



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

https://dl.google.com/release2

https://google.com/dl/release2



There are two configuration locations for proxy settings. Both are required and can be set through GPO or manually:

- 1) For installation and update: HKLM\Software\Policies\Google\Update should contain the proxy configuration as <u>detailed here</u>
 - ProxyMode (REG_SZ) one of the following values:
 - * direct -- Use a direct connection
 - * auto_detect -- Use autodetection with no PAC URL
 - * pac_script -- Use autodetection with an explicit PAC URL
 - * fixed_servers -- Uses a fixed set of proxy servers
 - * system -- <u>Uses system configuration</u>
 - * ProxyServer (REG_SZ) -- If ProxyMode == "fixed_servers", this contains the server list. Otherwise, this key is ignored.
 - * ProxyPacUrl (REG_SZ) -- If ProxyMode == "pac_script", this contains the URL of the WPAD script to use.
- 2) For the connector functionality: HKLM\Software\Google\GoogleCloudCertificateConnector: ProxyMode (REG_SZ) one of the following values:
 - * direct -- Use a direct connection
 - * system -- <u>Uses system configuration</u>

Troubleshooting

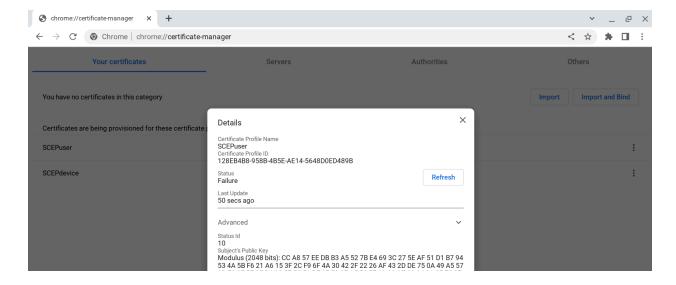
ChromeOS device

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 <u>SCEP profiles</u>.

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:



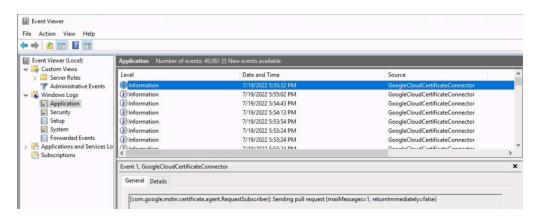
GCCC

Service Errors

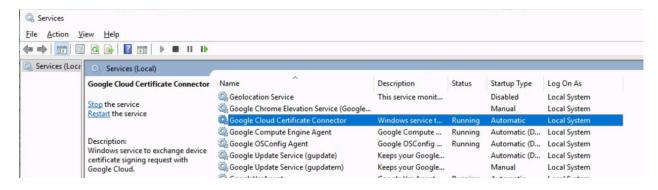
During normal operation, the following events will appear roughly every 30 seconds in Windows Application Log on the system running the GCCC Service from Source *GoogleCloudCertificateConnector*:

[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.

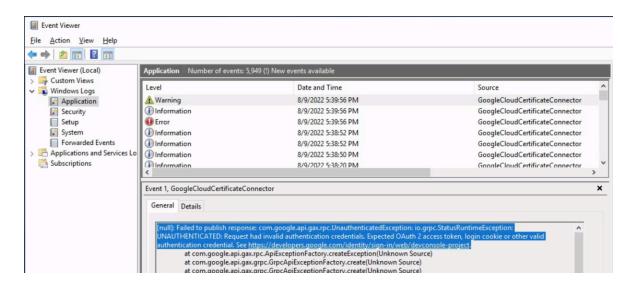


If the service fails to start repeatedly, verify that the <u>installation steps</u> were followed, including copying the json files to the GCCC Program directory.

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 <u>obtain or re-generate</u> 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

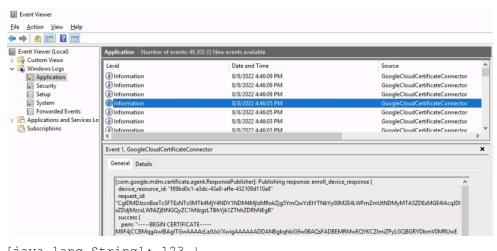
During a successful certificate enrollment, following events will be logged:

[com.google.mdm.certificate.agent.RequestSubscriber]: Received pull response {"receivedMessages":[{"ackId":"UAYWLF1GSFE3GQhoUQ5PXiM NSAoRRCJBE8CKF15MEq-...

[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 {...



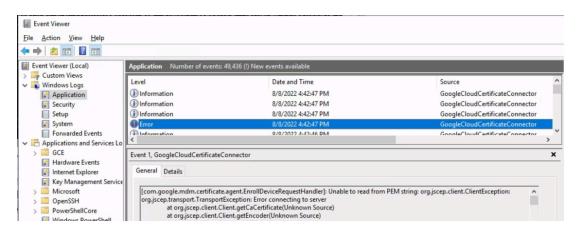
[java.lang.String]: 123...|

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

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

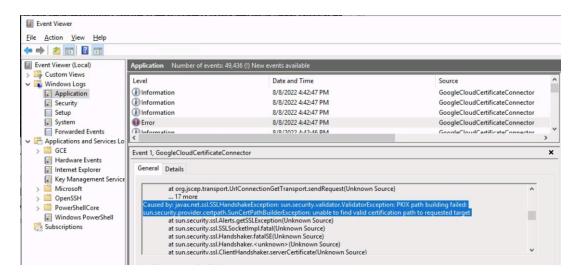
NDES Server Communication issues

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



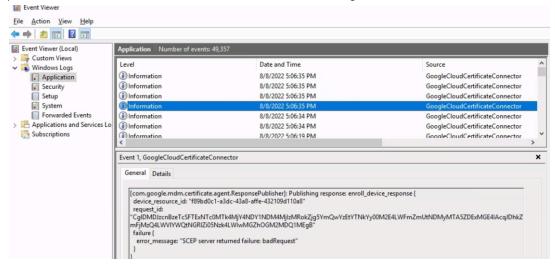


"PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target" means that GCCC cannot validate the SSL certificate presented by the NDES IIS Server. The NDES IIS SSL Certificate's signing CA and/or Root CA certificates 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\sscep\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, <u>contact Chrome Enterprise support</u> 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.

