Nexus Documentation

Example: SCEP Intune

Table of Contents

1 Example: SCEP Intune configuration in Protocol Gateway

This article describes a configuration example of the SCEP protocol with Azure Intune in Protocol Gateway.

2 Prerequisites

Prerequisites

The following prerequisites apply:

- Protocol Gateway must be installed. See Install Protocol Gateway.
- Initial configuration of Protocol Gateway must be done. See Initial configuration of Protocol Gateway.
- Microsoft Intune must be set up according to https://docs.microsoft.com/en-us/mem/intune/fundamentals/setup-steps
- The SCEP RA certificate must be issued by the same CA that issues the device certificates. Create an RA certificate in PKCS#12 format containing the full CA chain with the following keyusages or extended keyusages:
    - Digital Signature
    - Key Encipherment
    - TLS Server Authentication

3 Step-by-step instruction

3.1 Configure Intune for device certificate enrollment

Register app

To authorize communication between Protocol Gateway and Azure Intune you need to create a new registration app in your company Azure portal.

1. Navigate to the Azure Portal at https://portal.azure.com/.
2. Navigate to **Azure Active Directory > App registrations** and select **New registration**.
3. Give the app registration a **Name**, which is the user-facing display name, for example ***Intune App***.
4. Set **Supported account types** to ***Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)***.
5. In **Redirect URI**, select Web and set the URI to the Protocol Gateway SCEP Intune endpoint:

```
https://example.com/pgwy/scep/intune/pkiclient.exe
```

Code Block 1 Example: Protocol Gateway SCEP Intune endpoint

6. Click on **Register** to finalize the app registration.
7. You are directed to the App overview page. Copy the **Application (client) id**, this is your app id and needs to be configured in the Protocol Gateway SCEP properties later.
8. Navigate to **Certificates & secrets** and create a **Client secret**. Copy the value before leaving the page, it can not be retrieved later. This value needs to be configured in the Protocol Gateway SCEP properties later.
9. Navigate to **API permissions.** You need to add three separate application permissions.
   Click **Add a permission** and then:
   a. On the **Request API permissions** page, select **Intune** and then select **Application permissions**.
      i. Select the checkbox for **scep_challenge_provider** (SCEP challenge validation).
      ii. Click **Add permissions** to save this configuration.
      iii. Click **Add a permission** again.
   b. On the **Request API permissions** page, select **Microsoft Graph > Application permissions**.
      i. Expand **Application** and select the checkbox for **Application.Read.All** (Read all applications).
      ii. Click **Add permissions** to save this configuration.
      iii. Click **Add a permission** again.

c. On the **Request API permissions** page, change the tab from '**Microsoft APIs**' to '**APIs my organization uses**'

   i. In the search bar, type 'windows'

   ii. Select **Windows Azure Active Directory > Application permissions**.

   iii. Expand **Application** and select the checkbox for **Application.Read.All** (Read all applications).

   iv. Click **Add permissions** to save this configuration.

10. Click on **Grant admin consent for...** and click **Yes**.

Enable Intune MDM

To allow Windows 10 devices to enroll using Intune, *Microsoft Intune Mobility MDM (Mobile Device Management)* must be enabled.

1. Navigate to **Azure Active Directory > Mobility (MDM and MAM)** and select ***Microsoft Intune***.
2. Change **MDM user scope** to either ***All*** or limit the enrollment access to specific groups with the option ***Some***.
3. Make sure that **MAM user scope** is set to ***None***. Mobile Application Management (MAM) must be inactive for Intune to work.

Configure Trusted certificate profiles

To establish the necessary certificate trust stores for the devices to successfully enroll with Intune, the following Trusted certificate profiles need to be configured:

- Computers trusted root store - Root CA
- Computers trusted intermediate store - Root CA
- Computers trusted intermediate store - Intermediate CA

Follow this guide to configure each of the trusted certificate profiles:

1. Navigate to the Azure Endpoint manager (https://endpoint.microsoft.com/).
2. Navigate to Devices => Configuration Profiles, and select Create profile.
3. Perform the following settings:

   a. Set **Platform** to ***Windows 10 or later***.

   b. Set **Profile type** to ***templates***.

   c. Select **Template name** to ***trusted certificate*** and click **Create**.

   d. Enter a profile name and optionally a description, then click **Next**.

   e. Upload the certificate that should be trusted, in DER format, and specify the 'Destination store'. Then click on next.

      i. For Root CA in trusted root store: upload the root CA certificate and set **Destination store** to ***Computer certificate store - Root***.

      ii. For Root CA in trusted intermediate store: upload the root CA certificate and set **Destination store** to ***Computer certificate store - Intermediate***.

        iii. For Intermediate CA in trusted intermediate store: upload the intermediate CA certificate and set **Destination store** to ***Computer certificate store - Intermediate***.

    f. Configuring the access rights to this profile can be done either by applying it to all devices or by applying it to a selected group that the users requesting certificates via Intune will be a part of. Once the assignments have been configured click on next.

    g. If no device limitation is required, configuration of the accessibility rules can be skipped. Click on **Next** to proceed.

    h. Review your settings and verify that they are correct and then click on Create.

Create SCEP certificate profile

A SCEP Certificate Profile needs to be created for Intune to know how the end user certificate should be defined and which CA to deliver the CSR to.

1. Navigate to the Azure Endpoint manager at https://endpoint.microsoft.com/.
2. Navigate to **Devices > Configuration Profiles** and select **Create profile**.
3. Perform the following settings:
    a. Set **Platform** to ***Windows 10 or later***.

    b. Set **Profile type** to ***templates***.

    c. Select **Template name** to ***SCEP certificate*** and click **Create**.

    d. Enter a **Profile name** and optionally a **Description**. Click **Next**.

    e. The configurations determine the content of the CSR that will be sent to Protocol Gateway and should be adapted per installation.
    However, some settings are mandatory, for example the following:

        i. Set **Certificate type** to ***Device***.

        ii. Set **Key storage provider (KSP)** to ***Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP***.

        iii. Set **Root Certificate** to the ***Root CA Trusted Profile*** that was configured in the trusted root store.

        iv. In **Extended key usage**, add ***Client Authentication*** via the **Predefined values**.

        v. Set **SCEP Server URLs** to the Protocol Gateway Intune endpoint:

```
https://example.com/pgwy/scep/intune
```

Code Block 2 Example: Protocol Gateway SCEP Intune endpoint

    f. Click on **Next**.

4. Configure the access rights to the profile, either by applying it to all devices or by applying it to a selected group that the users requesting certificates via Intune will be a part of. Click on **Next**.
5. If no device limitation is required, the configuration of the accessibility rules can be skipped. Click on **Next**.
6. Verify the settings and click on **Create**.

3.2 Configure Protocol Gateway SCEP for Intune

Set SCEP properties

To set the properties for the SCEP protocols:

1. Open ***/cm-gateway/conf/SCEP.properties*** for editing.
   a. On Linux, this is found in ***/var/cm-gateway***.
   b. On Windows, this is found in ***C:/ProgramData/Nexus/cm-gateway***.
2. Set the SCEP properties as follows:
   a. Enable the SCEP protocol by setting `start` to `true`.
   b. Set `default.ra.keyfile` to the Protocol Gateway RA token file and `default.ra.password` to the related PIN.

      > The certificate format linked to the token procedure should not handle verifications (that is, rfc5280 can be used).

3. In a `handler`, set the following Intune parameters, to be able to verify the incoming device CSRs:
   a. Set `filter` and `format` according to the ***SCEP.properties*** example below.
   b. Set `tenant` to the fully qualified domain name (FQDN) of the organization configured in Intune.
   c. Set `azure_app_id` to the **Application (client) id** that was received in the **Register app** section above.
   d. Set `azure_app_key` to the **Client secret** that was received in the **Register app** section above.
   e. Set `certificateAuthority` to the name of the issuing CA for the end user certificates.

      > For more information on how to configure verifications of certificate requests in ***.properties*** files, see Certificate request verifications in Protocol Gateway.

4. If needed, scramble sensitive parameters in the configuration file. See Scramble sensitive data in configuration files in Protocol Gateway.
5. Save the file.

```
# SCEP parameters
start = true
default.tokenprocedure = SCEP Registration and Enroll Procedure
default.ra.keyfile = protocol-gateway-ra.p12
default.ra.password = <Protocol Gateway RA PIN>

# Intune parameters
handler.x.filter = intune/pkiclient.exe
handler.x.format = scep-intune
handler.x.tenant = {azure-tenant}
handler.x.azure_app_id = {app-id}
handler.x.azure_app_key = {app-key}
handler.x.certificateAuthority = {CA_name}
```

Code Block 3 Example: SCEP.properties

Restart Tomcat

1. Restart the Tomcat service.

3.3 Enroll Windows 10 device

Enroll Windows 10 devices

See the following Microsoft guide on how to enroll Windows 10 devices: https://docs.microsoft.com/en-us/mem/intune/enrollment/quickstart-enroll-windows-device.