Add a SAML 2.0 federation

This article describes how to add and set up a SAML 2.0 federation in Nexus Hybrid Access Gateway.

This article is valid from Nexus Hybrid Access Gateway 5.11.

Expand/Collapse All

Prerequisites

Before adding new SAML 2.0 federations, make sure you have completed the following tasks:

- Use server certificates when creating signatures. This is a requirement when acting as an identity provider. Server certificates are added using a wizard, see Add certificates.
- Use access point DNS names in SAML federations. Add these DNS names in the **DNS Name** tab, found in Global resource settings section.
- Note that there are three different licensed features when using SAML "Identity Federation", "Advanced Identity Federation" and "SAML Extension - Identity Provider Discovery".
- CA certificates shall be installed. They are used for verifying the signing certificate of requests and replies. These are automatically added if specified by imported metadata.
- If you are configuring an identity provider, at least one authentication method must have been configured.

Log in to Hybrid Access Gateway administration interface

1. Log in to the Hybrid Access gateway administration interface with your admin user.

Add SAML federation

1. In the Hybrid Access Gateway administration interface, go to **Manage Resource Access**.
2. Click **SAML Federation > Add SAML Federation...**
3. Enter **Display Name** and select a role: **Acting as Service Provider** and/or **Acting as Identity Provider**. When selecting a role a new tab will appear.
4. In **Metadata Import Settings** you can specify that metadata shall be fetched and published automatically in stead of manually. These settings are only accessible when licensed for feature "Advanced Identity Federation". For more information, click the **?**-sig n. The metadata is fetched automatically from the URL defined in **Download URL** and the integrity of the metadata is verified using the **Signature Verification Key**.
    1. Write the correct url in the **Download URL** field.
    2. Optional: Schedule the auto import according to the setting in **Cache Duration**.
    3. Optional: Enter an expiration date for the metadata in the **Valid Until** field.
    4. Upload the signing key of the metadata file in the **Signature Verification Key**.
    5. **Save** the SAML federation and click P**ublish**. The publish link needs is to be clicked manually the first time, to activate automatic import.
5. If **Acting as Service Provider** was selected, go to the **Export** tab.
   A SAML Discovery Service allows users to select any identity provider in the federation. The benefit of using a common discovery service is that users will see the same list of identity providers regardless which service is being accessed. When enabling SAML Discovery Service, the service provider will redirect the user to the discovery service, that presents a list of identity providers. The user selects preferred identity provider and the discovery service returns selected identity provider to the service provider. The service provider will validate the response and figure out to which identity provider the authentication request should be sent.
    1. Select a unique **Entity ID** to be exported in SAML metadata.
    2. Select server certificate, for help click the **?**-sign.
    3. Select **Access Point DNS Name** to enable SAML on a specific host-name.
    4. Check **Discovery Enabled** if the system shall provide a login link for SAML

Related information

- Add certificates
- Resources
- SAML 2.0 federation
- Set up access to Office 365

Discovery. If enabled, also provide the URL to the SAML Discovery Service. For help click the **?**-sign.
5. Use the **Metadata Extensions** check boxes to specify extensions to be added to the entity descriptor.
6. Click **Download metadata** to download metadata. This is used to inform external entities about this systems exported capabilities.
7. Go to the **Role Service Provider** tab. Here, you specify the entities that should be included in the SAML federation and how to interact with each one of them. Edit default values that will be applied to new Identity Providers imported by SAML 2.0 metadata. For more information, click the **?**-sign.
8. Click **Add** when done.

6. If **Acting as Identity Provider** was selected, go to the **Export** tab.

    1. Select a unique **Entity ID** to be exported in SAML metadata.
    2. Add a unique **API Path** to the standard resource administration service, to enable clients to manage the service providers for this identity provider. This setting is only visible when licensed for feature "SAML API". For more information, click the **?**-sign.
    3. Select server certificate, for help click the **?**-sign.
    4. Select **Access Point DNS Name** to enable SAML on a specific host-name.
    5. Use the **Metadata Extensions** check boxes to specify extensions to be added to the entity descriptor.
    6. Click **Download metadata** to download metadata. This is used to inform external entities about this systems exported capabilities.
    7. Go to the **Role Identity Provider** tab. Here, you specify the entities that should be included in the SAML federation and how to interact with each one of them. Edit default values that will be be applied to new Service Providers imported by SAML 2.0 metadata. For more information, click the **?**-sign.
    8. Click **Add** when done.

Enable use of SAML discovery service

1. Add, or edit a SAML Federation with SAML role **Service Provider** enabled.
2. Select the **Export** tab.
3. Check **Discovery Enabled** and enter correct URL to the discovery service
4. Choose an **Access Point DNS Name**; otherwise the Discovery Response Extension will not be included in the metadata downloaded in the next step.
5. Select to **Download metadata**.
6. Save the SAML federation when done, then click **Publish**.