Connect identity provider to PDF Signing

This article describes how to connect an external identity provider (IdP) to Nexus GO Signing.

To use an external identity provider, the connection must be configured both in the identity provider and in Nexus GO. For example, some user attributes must have the same names in both services, and metadata from each service must be uploaded in the other.

Mapping of attributes from the identity provider

Nexus GO uses attributes in the SAML response and add them to the PDF signature.

The attribute **`commonName`** is mandatory and is used to display the name of the signer in the PDF document.

The SAML response must contain either **`email`** or **`userId`**. Both of them can be included but at least one of them is mandatory. They are used to check the identity of the signer to verify that the signer has permission to view the signing request and the documents. It is configurable which attributes from the IdP that map **`commonName`**, **`email`** and **`userId`** in the SAML response.

The IdP can also provide the optional attribute **`title`**, which will be displayed in the visual signature in the PDF (for example **`Director`**).

Instructions for specific identity providers

For more information on how to set up specific identity providers in Nexus GO, see here:

- Set up Hybrid Access Gateway as identity provider to Nexus GO PDF Signing
- Set up Azure Active Directory as identity provider to Nexus GO PDF Signing
- Set up Forgerock as identity provider to Nexus GO PDF Signing
- Set up Microsoft AD FS as identity provider to Nexus GO PDF Signing
- Set up PhenixID Authentication Services as identity provider to Nexus GO PDF Signing

General instruction

For a general description of the steps to configure an Identity Provider in Nexus GO, see here:

1. Log in to Nexus GO.
2. Click **Services** > **Signing**.
3. Select the signing service you want to add an identity provider to, and click **Set up SAML IDP**.
4. In **Upload metadata**:
    a. Enter a **Display name**, which is the name of the Signing method that will be shown in the signing portal.
    b. Upload the xml file containing the **Identity Provider metadata**, for example *idp.xml*.
    c. Click **Next**.
5. In **Map SAML attributes**:
    a. Check the configured SAML attribute names in the identity provider for the following attributes: **`email`** and **`commonName`**, and enter them in the corresponding fields.

        ⚠ The attribute names in Nexus GO must match those that are configured in the identity provider for the connection to work.

    b. If you use an identity provider with **userId** as identifier instead of email, for example a personal identity number (personnummer in Swedish):
        i. Set **Include userId** to **On**.
        ii. In **userId**, enter the corresponding SAML attribute name.
    c. Click **Next**.

6. In **Select contributors**, define which users that are allowed to upload documents and send out requests in the signing portal:
    a. Either check **Everyone from this Identity Provider is a contributor**, or enter an attribute and values to define specific users to be contributors.
    Example
    To let all members of the user groups `admin` and `IT` be contributors, use these values:
    `attribute` `= memberOf,` **`value`** `= admin,` **`value`** `= IT`

    > ⚠ If there is no group already in the user directory to define the contributors, you can create such a group.

    b. Click **Next**.
7. In **Confirmation**, verify the details and click **Submit**.
The configured Identity Provider can now be used in the signing portal.