Guide: configuring Google Workspace IdP

This guide is a work in progress!

Read this before using Google as IdP

Google Workspace is popular amongst schools, particularly smaller schools, and we often receive the question: "Does the Google IdP work for Skolverket's DNP?"

To begin answering the question, you need to understand that both Skolverket, in their role as the service provider, and Skolfederation have requirements on what a SAML IdP should be capable of to conform with technical and security requirements.

In Skolverket's case, an IdP should have at least the below abilities (simplified):

- Authenticating students using single factor authentication (user/pass)
- Authenticating personnel using e-id
  - If a user has authenticated with an e-id, Skolverket requires the IdP to signal the assurance level of the e-id in the SAML Assertion (in AuthnContextClassRef). Otherwise, the authentication needs a separate "step up" using eduID.
  - If an IdP has support for signaling the e-id, it needs to be declared in the IdP metadata published in Skolfederation.
- The IdP must be able to send the required attribute eduPersonPrincipalName (EPPN) to the SP
  - The attribute must be sent with a correct NameFormat (more on this below)
  - The EPPN scope needs to be declared in the IdP metadata published in Skolfederation.

Check Skolverket's technical requirements for more details.

In Skolfederation, an IdP should conform with the technical requirements set in Skolfederation's Technical Profile.

The Google IdP does not conform with the above requirements on (at least) the below abilities:

1. It does not have the ability to automatically consume federation metadata containing several entities
2. It does not have the ability to signal the used level of assurance using AuthnContextClassRef.
3. It does not have the ability to send attributes using defined NameFormats (such as URI, used in Skolfederation and for DNP)

Furthermore, the Google IdP is not developed for usage in a federation. We do not see any signs of Google adapting their IdP to conform to widely regarded SAML WebSSO federation standards.

This means that in order to get your IdP working in a federation, you need to be aware of the limitations and the uncertainty of how Google chooses to provide their IdP service now and in the future.

There are two ways of using Google for logon for DNP:

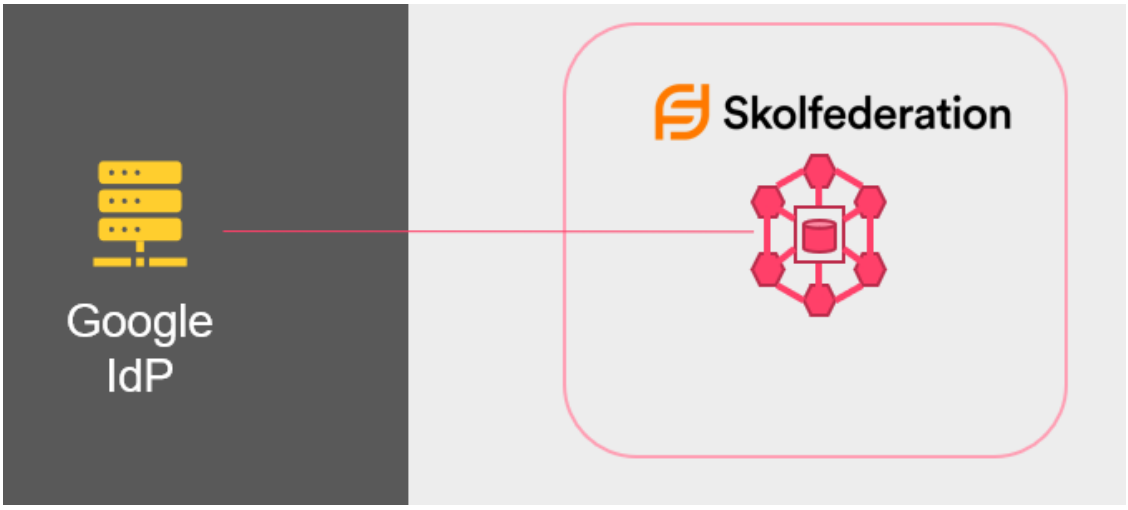
- Connecting the Google IdP to a SAML proxy (or "IdP proxy"), which is connected to the federation
- Connecting the Google IdP directly to the federation (not recommended)

Connecting the Google IdP to a SAML proxy (or "IdP proxy"), which is connected to the federation

A SAML/IdP proxy is a federation software that sits between your IdP (i.e. Google) and the services in a federation. By using a capable proxy, you will be able to use your "normal" Google sign-on and still be able to conform with the technical requirements provided by the federation.

Different proxy solutions provide different support and abilities, why it is important to choose a proxy that has a declared or generally recognized support for Skolfederation, and/or SAML 2.0 WebSSO identity federation, and/or DNP.

Connecting the Google IdP directly to the federation (not recommended)



By connecting the Google IdP directly to the federation, the school needs to be aware of Google not conforming with the above listed technical requirements, and will need to work around these issues.

1. **It does not have the ability to automatically (nor manually) consume federation metadata containing several entities**

   This means that updates in the federation (i.e. Skolverket updates the SP metadata of DNP) needs to be manually handled by technical personnel in a customized procedure, instead of it being automatically updated by the IdP.
   This is prone to human error and could result in not being able to access the service.

   Usually, and thankfully, SP metadata is updated rather infrequently. In the case of DNP, one would also assume that Skolverket would communicate changes beforehand.

2. **It does not have the ability to signal the level of assurance using AuthnContextClassRef.**

   This means that you are required to use the step up authentication workaround provided by eduID. Learn more at Skolverket's web page.

3. **It does not have the ability to send attributes using defined NameFormats (such as URI, used in Skolfederation and for DNP)**

   This means that you will have to send the EPPN attribute with a name and a format that does not conform with the Technical Profile or Attribute Profile.

Internetstiftelsen does not recommend using the Google IdP and connecting it directly to the federation due to the above reasons, but there may be resource or economical limitations that does not allow the school to choose another IdP solution. With that in mind, we have provided a step by step guide in how you can configure your Google IdP directly below.

Guide: configuring Google IdP directly to Skolfederation for DNP

> Please make sure you have read the previous chapter on the limitations of using the Google Workspace IdP and connecting it directly to Skolfederation before proceeding.

> **Disclaimer**
>
> We are not Google experts. Internetstiftelsen or Skolfederation are not held reliable for any errors or damage caused by using the guide below. Use caution and if possible consult a professional.

To successfully configure and test your Google Workspace IdP to work with Skolverket's DNP, you need to perform the following steps:

1. Membership in Skolfederation
2. Login to Google admin console
3. Set up ePPN
4. Set up DNP as a SAML application
5. Upload Google IdP metadata to Skolfederation
6. Skolverket's technical verification test: logon without e-id
7. Skolverket's technical verification test: logon with e-id "step-up"

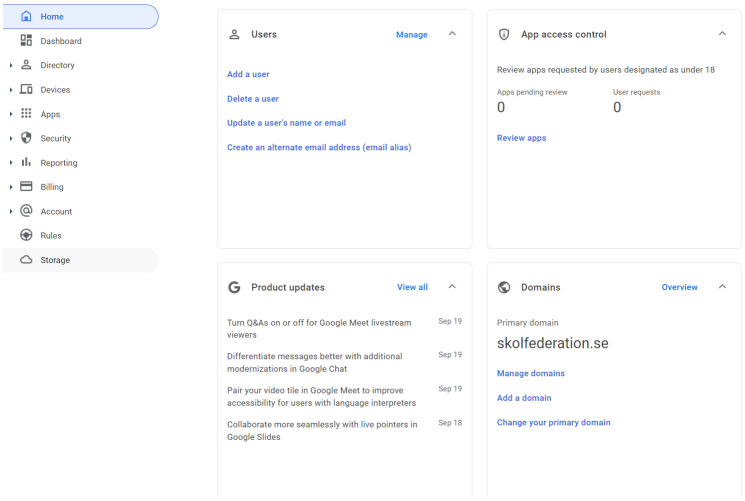
Membership in Skolfederation

If your organization already is a member of Skolfederation, you may proceed to the next step.

If you are not already a member, become a member by following the information provided here.

Login to Google admin console

Login to https://admin.google.com with admin credentials. Proceed to the next step.



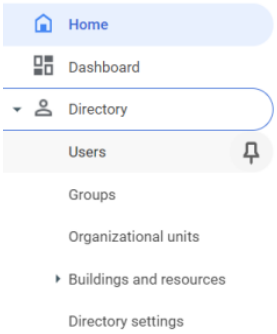
Set up ePPN and add ePPN to users

If you already have ePPN set up for your users, you may proceed to the next step.

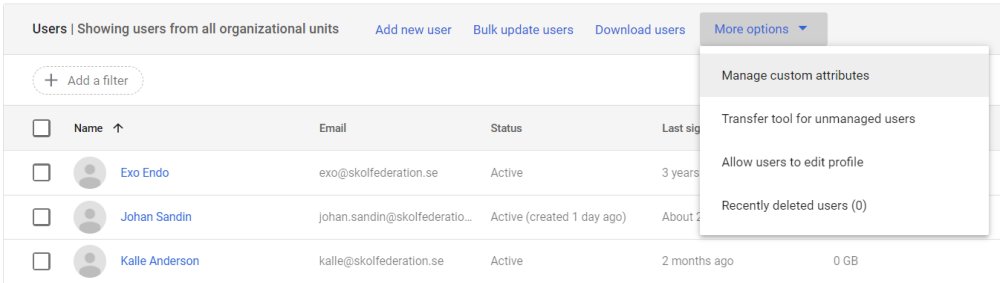
Below is a method to manually add the ePPN attribute to your users. Other methods, such as a directory sync, is not covered here.

Set up ePPN

In the menu to your left, go to **Directory > Users**

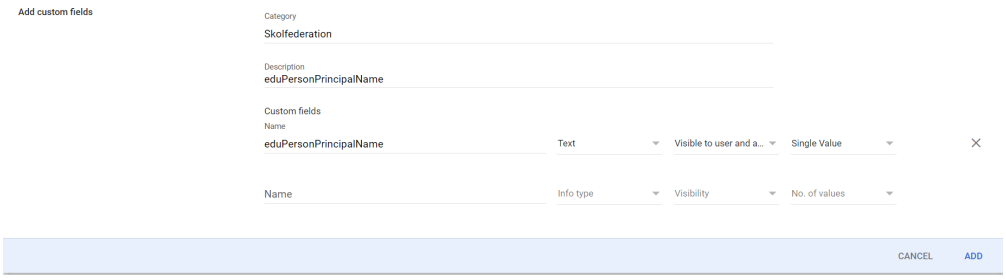


Open the drop down menu **More options** and select **Manage custom attributes**



Select **ADD CUSTOM ATTRIBUTE**

Add attribute



Fill in the form as follows:

1. **Category:** Skolfederation
2. **Description:** eduPersonPrincipalName
3. **Name:** eduPersonPrincipalName
4. **Info type:** Text

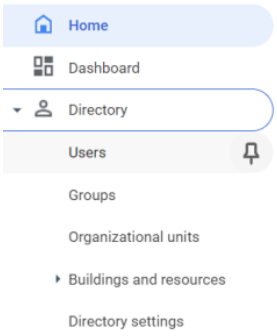
   Notice: if you cannot find Text and have Google Admin console in Swedish this may wrongly have been translated to "SMS"

5. **Visibility:** Visible to user and admins
6. **No. of values:** Single Value

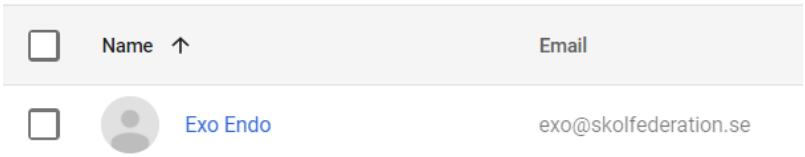
Then click **ADD**

Add ePPN to users

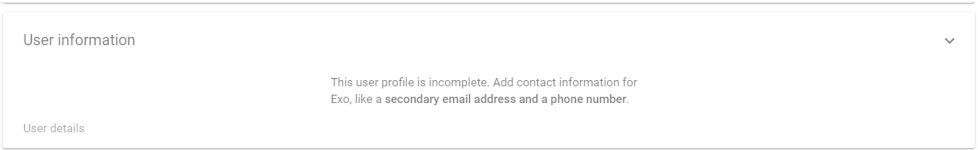
Go to **Directory > Users**



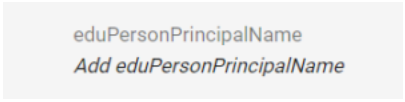
Click on the user you want to add the EPPN attribute to.



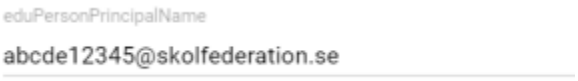
Expand User information by clicking it. By expanding the list all user attributes will be shown.



In the list **eduPersonPrincipalName** should be present under the **Skolfederation** category. Select **Add eduPersonPrincipalName**



Add ePPN for the user and click **Save**. This user now has an ePPN that can be used for DNP.

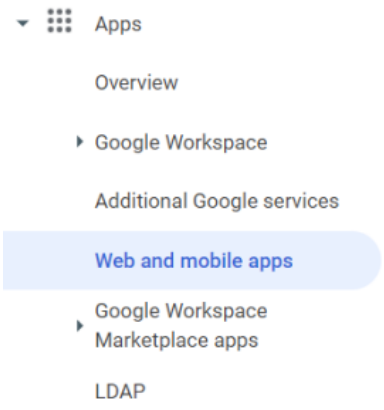


Repeat from step **Add ePPN to users** for all users that needs the ePPN attribute set.

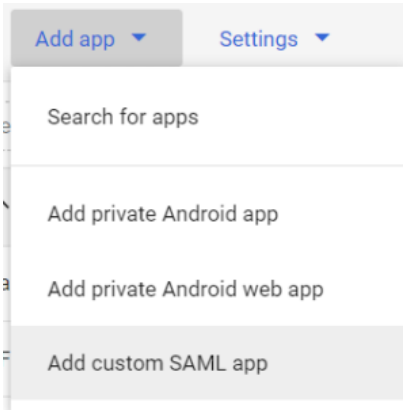
> **What value should I enter as ePPN for my users?**
>
> Read more on creating ePPN in the Guide: eduPersonPrincipalName (ePPN)

Set up DNP as a SAML application

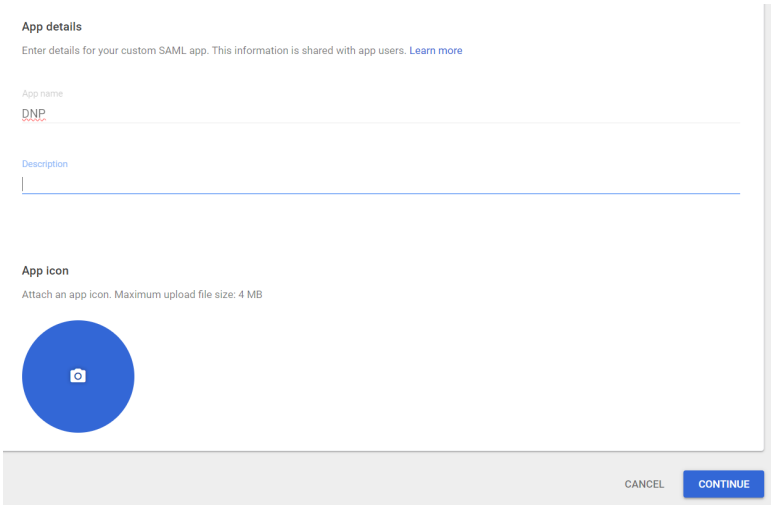
Go to **Apps > Web and mobile apps**



Navigate to **Add app** and select **Add custom SAML app**

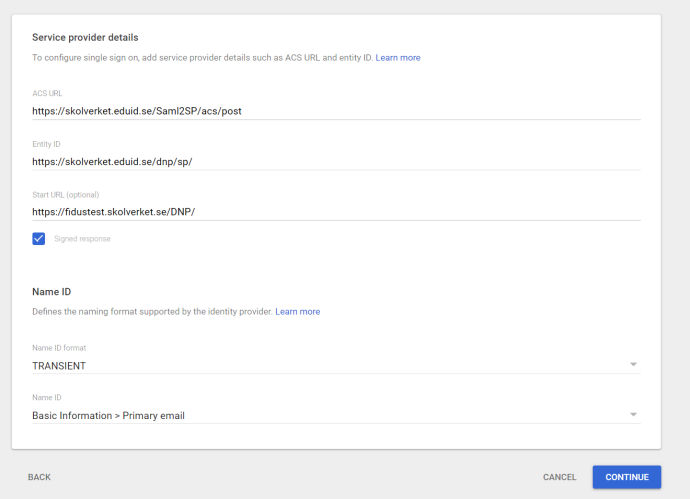


Name your app, perhaps "DNP verification test", and click **CONTINUE**



Under Option 1: Download IdP metadata, select **DOWNLOAD METADATA**. This will be use in a later step. Continue.

Add the service provider details

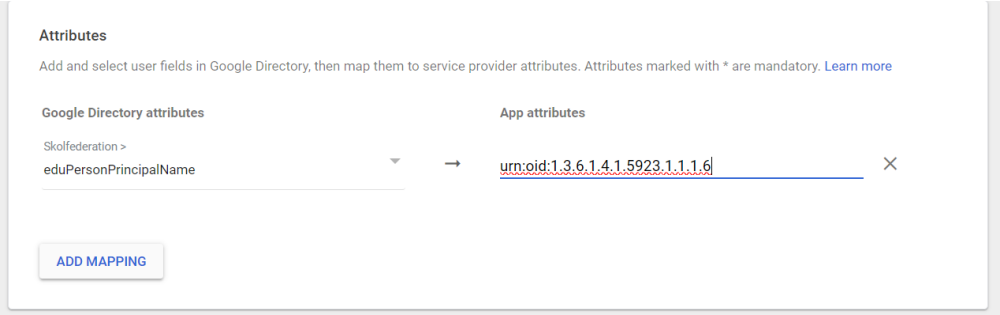


Add the following details for Skolverket's technical verification test service. **Note!** This is not a step that you would have to do with a federation capable IdP.

1. **ACS URL:** https://skolverket.eduid.se/SamlSP/acs/post
2. **Entity ID:** https://skolverket.eduid.se/dnp/sp/
3. **Start URL (optional):** https://fidustest.skolverket.se/DNP/
4. **Signed Response:** Aktiverad
5. **Name ID Format:** TRANSIENT
6. **Name ID:** Välj Basic Information och Primary Email

Select **CONTINUE**

Under Attributes, select **ADD MAPPING**. Here you configure your IdP to release the ePPN attribute to the Skolverket SP.

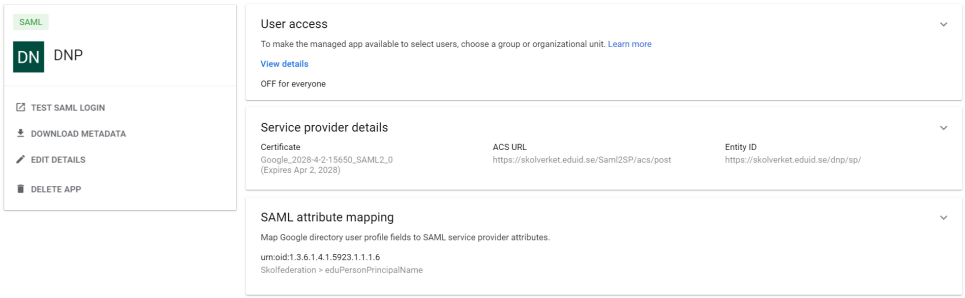


Note! If you recall, a limitation in the Google IdP is the inability to send a correct NameFormat for attributes. Usually, you would have to send the App attribute as the above listed urn:oid string. In this case, we have to workaround it. Do not add the urn:oid value as App attribute as the Skolverket service currently does not support this value without a correct NameFormat.

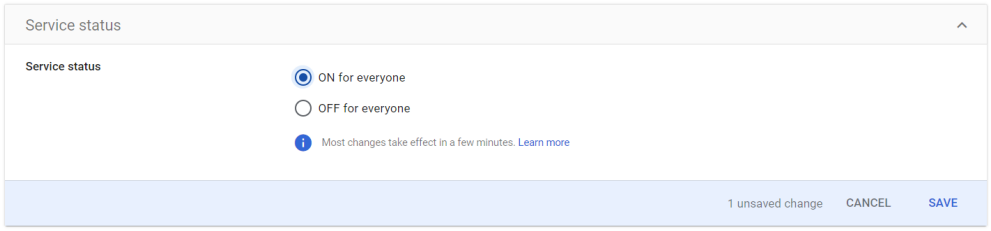
1. Under Google Directory attributes, select **eduPersonPrincipalName**
2. Under app attributes, write/copy **eduPersonPrincipalName** as value

Then select **FINISH**

Activate the service for your users. On the service screen that should appear, click on **User access**



Select **ON for everyone**, then **SAVE**



Now the Skolverket verification test SP is set up in your Google IdP, and configured to send ePPN as an attribute. Proceed to the next step.

Upload Google IdP metadata to Skolfederation

Now that the Google IdP is configured for the DNP technical verification test, you need to upload the Google IdP metadata to Skolfederation. Before doing so, you need to add missing metadata information to the file downloaded in the previous step.

Add missing metadata information to metadata

Go to https://gidp.swefed.se/. Perform the steps under "Metadataverktyg för Google IdP" and "Komplettering".

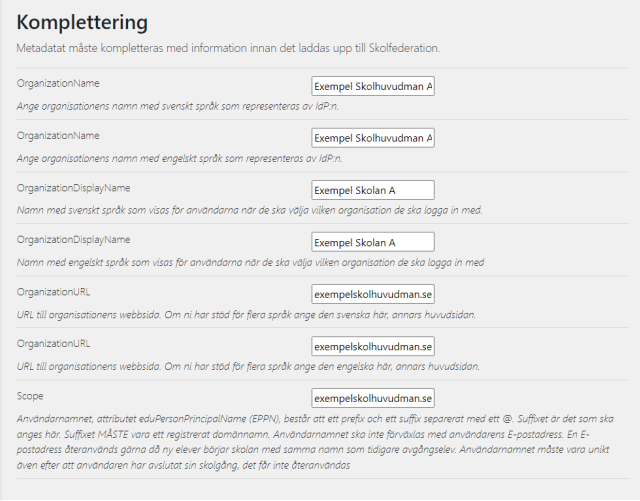
Under **Metadataverktyg för Google IdP**, click on **Ladda upp**

Select the metadata file downloaded in the previous step "Option 1: Download IdP metadata".

The metadata will be presented.

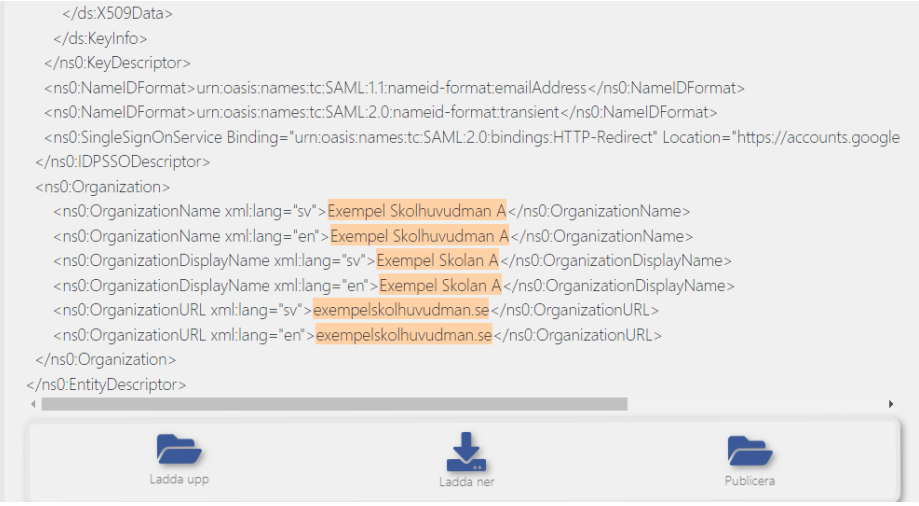
<ns0:EntityDescriptor entityID="https://accounts.google.com/o/saml2?idpid=C04kmvohx" xmlns:ns0="urn:oasis:names:tc:SAML:
<ns0:IDPSSODescriptor xmlns:ns0="urn:oasis:names:tc:SAML:2.0:metadata" WantAuthnRequestsSigned="false" protocolSupport
<ns0:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIDdDCCAlygAwIBAgIGAYLowXa5MA0GCSqGSIb3DQEBCwUAMHsxFDASBgNVBAoTC0dvb2dsZSB.
bmMuMRYwFAYDVQQHEw1Nb3VudGFpbiBWaWV3MQ8wDQYDVQQDEwZHb29nbGUxGDAWBgNVBAsTD0dv
b2dsZSBGb3IgV29yazELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWEwHhcNMjIwODI5
MDgzOTI4WhcNMjcwODI4MDgzOTI4WjB7MRQwEgYDVQQKEwtHb29nbGUgSW5jLjEWMBQGA1UEBxMN
TW91bnRhaW4gVmlldzEPMA0GA1UEAxMGR29vZ2xlMRgwFgYDVQQLEw9Hb29nbGUgRm9yIFdvcmsx
CzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAwzkpInArScgYMOVr5u2cklWyww8av3JB+WoHYjgMqffnOdwbYJwxJayRaQGPiwuG
1ioeOmz+kTNvP3g5djVyBYAmrZYp4yyu8+ah2rrA7SNPf2c2RC1yclF5CDKJU5z7BLJyisrKzA6b
+wZZHruf3g6Epcz7oqCg63ySw806Lbw3VxeOQU7uelyiB0O9mffQOhjHatyjvm88w5EjXyQUkO3+
9FW32ONjF2QejNebGMXPMa7GziMGaAmFHFILuYWahbluhlBdVtZwsSJZ3TUzY80Y613SVmePczxs
LfDC8t00mMZ4R0G3FDYhcxtxOOyBWL4TqnJ2O5XrBe9+agkvUwIDAQABMA0GCSqGSIb3DQEBCwUA
A4IBAQBxzrL/896KfoqwBGYrZ8YjywgO1TzxOJ/v13ZwiVFopVWMyeeguExYXLmfxFgCBXA0QWR+
orAGG/15tWfGSgOnAITY6qulBvU6V9U2sxJBa7eNw7C3omEh5ZqhCQY7tg3xJ/90eNvYlthwo/gB
F5JnuwM7/TNsmcou7pmienNkFu2MSwmOG9lNsgLeiKSAk9Q2M+y3LPs7knSTGhYxRDT0x/ZTbkTF
earpwVKg4un8Ql/t6h4mwXF6pvsJTOCEGbuec+2mx90zMmAg7PHy7cEEQm4sgP18JJyyajyk0Wzx
GL+wYC3qCpiEYk5Eg+BMwJ9KWlU5pmGgwYygqpLAii6+</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ns0:KeyDescriptor>
<ns0:KeyDescriptor use="signing">

Scroll down to **Komplettering** and add information as described in the guide, example below.



The info is then added to your metadata as shown in the previous view

<ns0:EntityDescriptor entityID="https://accounts.google.com/o/saml2?idpid=C04kmvohx" xmlns:ns0="urn:oasis:names:tc:SAML:
<ns0:Extensions>
<shibmd:Scope regexp="false" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0">exempelskolhuvudman.se</shibmd:Scop
</ns0:Extensions>
<ns0:IDPSSODescriptor xmlns:ns0="urn:oasis:names:tc:SAML:2.0:metadata" WantAuthnRequestsSigned="false" protocolSupport
<ns0:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIDdDCCAlygAwIBAgIGAYLowXa5MA0GCSqGSIb3DQEBCwUAMHsxFDASBgNVBAoTC0dvb2dsZSB.
bmMuMRYwFAYDVQQHEw1Nb3VudGFpbiBWaWV3MQ8wDQYDVQQDEwZHb29nbGUxGDAWBgNVBAsTD0dv
b2dsZSBGb3IgV29yazELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWEwHhcNMjIwODI5



Click on **Ladda ner** to download the new metadata file with the added changes.

Upload the metadata to Skolfederation

> **Uploading to Skolfederation**
>
> To be able to upload the metadata to Skolfederation, you have to be the organization's technical contact, or a technical agent added in Federationsadmin by the technical contact.

Login to Federationsadmin here with e-id.

Follow the five Metadata steps in the Federationsadmin user guide (in Swedish) to upload your metadata to the federation.

The first time a metadata is uploaded, the federation operator will review your metadata. If metadata is OK, it will be published to the federation. If there are any changes to be made before publishing, you will receive an email with what changes need to be made.

Wait for the metadata to publish

When the metadata is published, the metadata needs to be updated in Skolfederation, and Skolverket needs to retrieve the latest changes before you can proceed with the verification tests. This is usually done within two hours.

Skolverket's technical verification test: login without e-id (students)

Follow the steps at Skolverket's technical verification test login without e-id

Skolverket's technical verification test: login with e-id (personnel)

Follow the steps at Skolverket's technical verification test login with e-id