# Metadata of your Service

If you want your service to be connected to SURFconext, metadata must be exchanged between you and SURFconext. After this your service and SURFconext will know and trust each other. The exchange of metadata is done only once: there is no exchange in the authentication process itself.

The exchange is a two way process:

1. The Service Provider must read metadata from SURFconext.
2. SURFconext must read metadata from the Service Provider.

## Configure SURFconext as your Identity Provider

Preferably you configure SURFconext as your Identity Provider automatically, by using a SAML 2.0 metadata file, to be downloaded at https://metadata.surfconext.nl/idp-metadata.xml. The metadata for the test environment can be found at https://metadata.test.surfconext.nl/idp-metadata.xml. How you enter the metadata in your software depends on the software used. Generally you import the metadata file or place it in a specific location.

The metadata will configure your service to see SURFconext as the only IdP and will let SURFconext do the IdP discovery for you. This is the WAYF selection page. It is used for both the Test and the Production environment.

If your software cannot process the metadata file automatically, you must configure the necessary information manually:

- **EntityID**[1] of the SURFconext Identity Provider
  https://engine.surfconext.nl/authentication/idp/metadata (production environment)
- https://engine.test.surfconext.nl/authentication/idp/metadata (if testing on the test environment)
- **SingleSignOnService**
  Location: https://engine.surfconext.nl/authentication/idp/single-sign-on/key:20181213 or https://engine.test.surfconext.nl/authentication/idp/single-sign-on/key:20230403 for test.
  This location is used by your SAML software to send an AuthnRequest to
  Binding: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
- **Signing Certificate**
  You'll find the production certificate file here and the test certificate file here.
  The certificate is used to verify the SAML assertion sent to your Assertion Consumer Service endpoint, making it possible to have a safe connection between SURFconext (IdP) and your service (SP).
  If your software only needs the certificate fingerprint:
  ```
  $ openssl x509 -inform PEM -in SURFconext.pem -noout -fingerprint
  SHA1 Fingerprint=A3:6A:AC:83:B9:A5:52:B3:DC:72:4B:FC:0D:7B:BA:62:83:AF:5F:8E
  ```
- **NameIDFormat** must be one of:
  - urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
  - urn:oasis:names:tc:SAML:2.0:nameid-format:transient (default)
  - urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified (legacy, do not use)
  Name IDFormat tells an Identity Provider to return the NameID (user identifier) in a specific format.
  An SP can request a specific NameID format in the AuthnRequest using the NameIDPolicy - Format element. Whether this request is honored is subject to policy.

# Inform SURFconext about your service

To be able to configure a connection with your service, SURFconext Support needs some information about your service. This can be given by using the recommended SAML 2.0 metadata file or manually. Most SAML Service Provider enabled software can produce a metadata file. You can send the URL of the location of the metadata file on your web server to SURFconext via the SP Dashboard.

| **SAML metadata element** | **Description** | **Restrictions** | **Mandatory in SAML metadata[2]** | **Mandatory information[3]** |
|---|---|---|---|---|
| entityID | Technical name of your service | • Must be a URN, with at least one colon<br>• Unique within SURFconext<br>• An IdP and SP cannot have the same EntityID | Y | Y |
| AssertionConsumingService<br>• Location<br>• Binding | Endpoint where users need to be sent back to after authentication | Location: URL of your AssertionConsumingService (ACS). In production this must be HTTPS with a **trusted and valid** SSL certificate<br>Binding: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST | Y | Y |
| NameIDFormat | Format of the NameID you will receive when a user is authenticated via SURFconext | • urn:oasis:names:tc:SAML:2.0:nameid-format:transient or<br>• urn:oasis:names:tc:SAML:2.0:nameid-format:persistent | Optional | Y |

| | | | | |
|---|---|---|---|---|
| ContactPerson<br>• GivenName<br>• SurName<br>• EmailAddress | Information about your administrative, technical and support contacts. | Use contactType="administrative", contactType="technical" or contactType="support" in the ContactPerson element when adding this to your metadata | Optional | Y |
| name | Name of your service | | N | Y |
| description | Description of your service | | N | Y |
| RequestedAttributes | The attributes your service requires, including the reason why it is required | | N | Y |
| mdui:Logo | Logo of your service | 500 x 300 pixels, PNG format with transparent background | N | Y |

[1] Although it looks like the entityID is the location of the SAML metadata, it is actually not!

[2] If you provide SURFconext Support with a SAML metadata file, these fields must be part of that file.

[3] You must provide this information to SURFconext Support via the SP Dashboard.

### Navigate