FAQ

General

Can I test my (test)service on a permanent basis?

- In the Test environment DIY/test IdP is available for testing. Register your service(s) via the SP Dashboard. Note that the metadata for the Test environment is different from the Production environment.
- In the Production environment you can use eduID to test authentication for your application.
- If you haven't, also see the info about our different Environments .

How can I facilitate guest access for my service?

With eduID.

Does SURFconext support provisioning?

No, if your service needs provisioning, you must arrange this yourself.

Does SURFconext support Single Logout?

No. For more background information, see:

- Session duration in SURFconext: a balance between usability and security
- How relevant is logging out today?
- Shibboleth: SLO issues

How does SURFconext support rich clients and mobile applications?

Whether a rich client supports federated login with one of the standards used by SURFconext (e.g. SAML or OpenID Connect) depends on the developer of that rich client. The support must be built into the rich client and often also on the server of the service. SURFconext cannot make the rich client compatible. SURFconext can advise institutions about services that have rich clients associated with them. We can also pressure vendors to support federations in their designs.

More information.

My metadata has changed. What should I do?

Inform SURFconext and provide us with the new metadata before you upload it to the Production environment. If you inform us in time, there will be no downtime for the users.

Can I use SURFconext to login with a social ID (Facebook, Google, etc.)?

No. Use eduID for guest access.

Which attributes can SURFconext supply to my service?

SURFconext operates with a minimal disclosure principle: only the absolute necessary (personal) information is transferred to a service. When you request a connection to the Production environment, you must specify the attributes needed. We will review your request and configure an Attribute Release Policy accordingly.

What do 'single-tenant' and 'multi-tenant' mean?

See Use of single-tenant and multi-tenant services in SURFconext.

Can I implement my own discovery screen?

Yes.

Is there a way for my users to authenticate and not use Single Logon?

Yes. You can force users to authenticate when they log in. By setting `ForceAuthn` to `true`, single sign-on is disabled. If the user already had a session with their IdP, that will be ignored.

Can I add my own branding to the SURFconext discovery screen?

Yes, you can create your own WAYF selection page.

Why doesn't my service get attribute X?

Generally it is because the IdP did not release the required attribute. SURFconext operates with a minimal disclosure principle: only the absolute necessary (personal) information is transferred to a service.

Can I get statistics about the number of users who log in to my service?

Not from SURFconext: use your own logging.

Can I offer my service to foreign universities via SURFconext?

Yes, via eduGAIN. Please refer to this documentation for more information.

How can I use groups provided by SURFconext?

SURFconext Teams offers an easy way to manage collaborative groups. The groups are organised centrally and can be used with cloud services. A group can be set up so that only the members of that group have access to restricted data on a particular cloud service (more information).

Does SURFconext support authorisation?

See: Authorisation

Which authentication protocols does SURFconext support?

Currently only SAML2 and OpenID Connect are supported.

How do I relay a student or employee number to my SP?

With the `schacPersonalUniqueCode` attribute. Note that only a very limited number of IdPs are providing this attribute. If you want to use /provide this attribute contact support@surfconext.nl.

What IP-ranges do I need to allow connections from for SURFconext?

Note that SAML logins always run via the user's browser, so it is not usually necessary to allow any direct connections between our systems and yours for the login process.

Our SP registration systems need to be able to fetch your SP's metadata though. For that, you can whitelist:

- `2001:610:188::/48`
- `2001:610::/48`
- `145.100.0.0/15`
- `195.169.0.0/16`

Why is my SP being removed from SURFconext?

We check regularly if an SP is still being used. If no logins are recorded during some time (see below), we will remove the connection. Before doing so, we will notify the SP.

Currently, the timeout periods are defined as follows:

	timeout	**grace period**
Test connections	1 year	14 days
Production connections	unlimited	n/a

Test connections must receive minimum 1 login within the first 6 months. Otherwise they will be removed.

What are the rate limits for accessing SURFconext?

In order to protect our servers from being taken down by too many requests we have some rate limits in place:

1. An IP address is not allowed to generate more than 1000 requests every 10 seconds in total
2. An IP address cannot access a specific endoint more than 500 times a minute

SAML

Which attribute should I use to identify SURFconext users in my application?

NameID.

How do I transmit a custom (non-standard) attribute from an IdP to an SP?

Use the eduPersonEntitlement attribute:

(`urn:mace:dir:attribute-def:eduPersonEntitlement` / `urn:oid:1.3.6.1.4.1.5923.1.1.1.7`)

To scope the entitlement values, we include the SP's principle domain in the value.

The SP "bookkeeper.example.org" needs the "FinanceRole" attribute, with possible values "user", "manager" and "administrator". In SURFconext, this can be passed on in an eduPersonEntitlement:

```
urn:mace:dir:attribute-def:eduPersonEntitlement = urn:x-surf.nl:example.org:FinanceRole:manager
```

Microsoft .NET rejects the metadata signature, help?

This is a bug introduced by Microsoft in an attempt to fix a security issue. The security issue (CVE-2019-1006) is described here: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1006 In particular, the problem arises when using the following method for reading metadata: https://docs.microsoft.com/en-us/dotnet/api/system.identitymodel.metadata.metadataserializer.readmetadata?view=netframework-4.8

The patch that has been rolled out changes the way XML digital signatures are verified. It seems to “fix” things by ignoring all KeyInfo elements other than the first child of a Signature element, and expecting it to contain an X509Data element. We have spoken with the responsible Microsoft developers and they acknowledge that the implementation is faulty. However, until now they have not prioritized fixing this issue in .NET. It may be helpful to report that you are affected by this problem to Microsoft to give it more priority.

A workaround is to apply an XSLT transform to remove the first KeyValue element from the signed metadata file, for example like this: strip.xslt