Authorisation

Before users can use your service, their Identity Providers need to be coupled with your service. This is done by SURFconext Support, after the Identity Provider has given explicit permission. Generally the less attributes your service requires (in accordance with the minimal disclosure principle of SURFconext), the quicker they will give this permission.

In the SURFconext Dashboard administrators can see your service and decide to request a coupling with it. If your service is meant to be used by only one or a few Identity Providers, you can ask SURFconext not to show your service in the Dashboard.

Fine grained access to your service

When an IdP has been coupled with your service, typically **all** users at the institution are able to login. Below authorisation options are listed:

Attributes

Attributes are negotiated during the connection process.
With attributes, it's possible to restrict access to your service. For example, with the attribute 'Affiliation' you can give access only to students or staff. If you want to restrict access to a certain faculty, you can use the scoped affiliation attribute.

With services having some specific requests on certain attributes some coordination is necessary between SP and IdP.

Pre-provisioning

Alternatively, you can pre-provision the legitimate users of your service, and block the rest. Consequently you must find a way to map the user information you own to the information you receive from SURFconext.

SURFconext Authorisation Rules

IdP's have the possibility to restrict access to a service. With SURFconext Authorisation Rules (Dutch), key users at the institutions can restrict certain users, or user groups to have access to the service. This functionality can't be operated by Service Providers, but with deliberation with the institution, arrangements can be made.