

Single Sign-on Configuration of Google Workspace

Configuring your G Suite domain with SURFconext

In this tutorial, we will use the fictional Google Workspace domain of "myuniversity.com". This should be changed to your institution's Workspace domain name which you configured when creating your Workspace instance.



Note: uploading a file in the form (the certificate) may reset other, not yet saved, changes made in the form.

1. Login to the Google Workspace administrative interface located at <https://admin.google.com/myuniversity.com>
2. Go to Security Set up single sign-on (SSO)
3. Configure the fields as follows (see the screenshot below):
 - a. Check the "Setup SSO with third party identity provider" checkbox
 - b. Sign-in page URL:

<https://engine.surfconext.nl/authentication/idp/single-sign-on/key:20181213>

- c. Sign-out page URL:

<https://engine.surfconext.nl/logout>

This is an informative page telling the user to log out by closing their browser.

- d. Change Password URL

This field should point to your institution's change password page. See also the section here below

- e. Verification Certificate

This contains the file containing the SURFconext signing certificate. Use [this](#) file with the following certificate or browser to <https://metadata.surfconext.nl/> where you will find it under Security ([engine.surfconext.nl 20181213 certificate](#)):

```
-----BEGIN CERTIFICATE-----
MIID7DCCAtSgAwIBAgIJAiGmQnMYZ+t6MA0GCSqGSIb3DQEBCwUAMIGFMQswCQYD
VQQGEwJOTDEQMA4GA1UECAwHVXRyZWNoDEQMA4GA1UEBwwHVXRyZWNoDEVMBMG
A1UECgwMU1VSU0YyZmNvbmV4dC5ubCAyMDE4MTIxMzAeFw0xODEyMTMxNTI1MjBa
Fw0yMzEyMTMxNTI1MjBaMIGFMQswCQYDVQQGEwJOTDEQMA4GA1UECAwHVXRyZWNo
dDEQMA4GA1UEBwwHVXRyZWNoDEVMBMGMA1UECgwMU1VSU0YyZmNvbmV4dC5ubCAy
MDE4MTIxMzAeFw0xODEyMTMxNTI1MjBaMDE4MTIxMzAeFw0xODEyMTMxNTI1MjBa
mW1V8aV85z45QsuFw3gkq0HbWR1JGz7cjghjV6YZHFXYRt4ikG//9BIHS0xc/cw1
sOMnSuCjDhY80h/d0k01zfGFXUcv+0iNlKEKGMlT/xJpIDIY/N4WjpGvkJO2oJHf
rQUY115Du56MSMQd0gPvo10sDvXroYivqxYpTTHzaF5TYQYPf6n/3rEfsu3u6L3p
zE3/q38jnEyxfQ1UoZ9VF2Fy6oe/StlwhPUJhVwHLKDMqQ+T+tLjDt260k9QL3zz
W9JtBo+pnYdMT/rG5h7NW8A9HASLnRLK8rFD9nBEDAPKk+eLTE6QddRiTh9H84KC
s0fQiiT6YfScAwEAAandMFswHQYDVR00BBYEFAJuZa7u0f0o2kB9uRPoB/ekx04s
MB8GA1UdIwQYMBaAFAJuZa7u0f0o2kB9uRPoB/ekx04sMAsGA1UdDwQEAwIHGDAM
BGNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBXh5l8u+ncPXkMyDqDuikN
Le/X5j0KNjvqUtQ6QPRSt8MMvjRYWZdVC0gMOTKEAY1/cYnA2y+0yrGqmy9I/zBd
LV73BBLnLV2WYATY0ZLWNW36kjBtdSbH0oXBp7H0u/I4lP+Sv69eRN6p2/9CmDy
Kc5JupXU3PEftv5Lwsqco8MMmqENhwzYlXrb96LFq08Un2QQoV60HqX4Ks79qUrn
jRL5pKtoP4ujLmPqQIieHPTgsvHSQSa+9tZMnyEaJEvL7vpNn1M7v1bW0WwjQvML
YnSq5b0U5gHXgpdBYSfWnCwwpq4h8KHZ7/XVv0VsdYpjHap+9070GhqXGBsIqf9U
-----END CERTIFICATE-----
```

- f. Use a domain specific issuer

Make sure to check this box. This enables SURFconext to distinguish between all connected Google Workspace domains.

☒ **Setup SSO with third party identity provider**

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL	https://engine.surfconext.nl/authentication/ldap/single-sign-on/key:20
	URL for signing in to your system and G Suite
Sign-out page URL	https://engine.surfconext.nl/logout
	URL for redirecting users to when they sign out
Change password URL	https://engine.surfconext.nl
	URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled
Verification certificate	A certificate file has been uploaded. Replace certificate
	The certificate file must contain the public key for Google to verify sign-in requests. ?

☒ **Use a domain specific issuer** ?

Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

4. Register your Google Workspace domain with SURFconext using the [SP Dashboard](#). Send a mail to support@surfconext.nl to gain access to the dashboard. Make sure you have the following at hand:
 - a. There is no metadata file in Google Workspace. Please contact support@surfconext.nl if you are uncertain about what to use in the SP Dashboard.
 - b. The attribute(s) that is used to provision your users to Google Workspace. You can review the available attributes [here](#). Attributes like or combination of attributes like "urn:mace:dir:attribute-def:mail", "urn:mace:dir:attribute-def:uid", "urn:mace:terena.org:attribute-def:schacHomeOrganization" and more are used for this service across SURFconext. Consider them wisely. Also specify if additional processing is necessary, for example because some attributes are multi-valued and do not always contain the correct email domain.
 - c. This is a Single Tenant service. We can make sure this instance is hidden in Dashboards for other IdP's. On request you can whitelist IdP(s) that need access to your Google Workspace domain.