Using Onegini as IdP for testing SPs

For testing with the SURFsecureID test environment you need a user account. If you do not have access to an identity provider (IdP) that is connected to the SURFconext test environment, you can use Onegini. Onegini is an IdP that allows anybody to create an account.

For testing your connection on the SURFsecureID Production or Pilot Gateway you should use use an Onegini account instead of one of your regular IdP's accounts.

The second factor authentication tokens that you register in Test, Pilot or Production are separate. You can use the same token and OneGini account for Test, Pilot and Production, but you need to do the registration procedure for each environment that you wish to use.

> ⓘ If you use your Yubikey with the production environment, you must not use it for any other purpose, including using it with SURFsecureID Pilot or Test. Reusing your production Yubikey is a security risk because Yubikey OTP codes are not tied to the environment.

Production environment

> The procedure below applies to the SURFsecureID **Production** environment. The pilot environment and test and environment have a different policy. See Pilot environment and Test environment below.

Policy

SURFnet adheres to a strict policy for using Onegini for SURFsecureID:

- A SURFnet SRAA will do the vetting of a SP contact. The contact must be physically present with his token, activation code and ID. Skype/mail is **not** allowed for the Production environments.
- When the SP contact loses his token, he must register a new token and do the activation process all over again.
- Onegini accounts are **not** allowed to have RA(A) rights.
- Onegini IdP is aimed at SPs. SURFnet offers 'best effort support' only.
- The SP must allow Onegini as IdP for their service and is responsible for its own additional authorization rules.

Registration procedure

1. Register a Onegini account.
2. Make sure to complete Onegini's verification process for your mail address: this is required for registering a SURFsecureID token.
3. Go to https://sa.surfconext.nl and login with your Onegini account.
4. Request a second factor authentication token (SMS, tiqr or YubiKey) and complete the self-registration process until step 4 "Activation code'.
5. Contact us (support@surfconext.nl) for an appointment to finish the registration (ca. 5 minutes). The appointment must be face-to-face, remote vetting is not allowed.
6. Do not forget to bring/have your activation code and second factor authentication token (SMS, tiqr or YubiKey) and photo ID (passport or drivers license) ready.
7. After verification SURFnet will activate your token and you can login.

Pilot environment

Policy

- A SURFnet SRAA will do the vetting of a SP contact. The contact must be available during vetting with their activation code. Vetting using Skype/mail/phone is allowed for the Pilot environments.
- When the SP contact loses his token, he must register a new token and do the activation process all over again.
- Onegini accounts are **not** allowed to have RA(A) rights.
- Onegini IdP is aimed at SPs. SURFnet offers 'best effort support' only.
- The SP must allow Onegini as IdP for their service and is responsible for its own additional authorization rules.

Registration procedure

1. Register a Onegini account.
2. Make sure to complete Onegini's verification process for your mail address: this is required for registering a SURFsecureID token.
3. Go to https://selfservice.pilot.stepup.surfconext.nl/ and login with your Onegini account.
4. Request a second factor authentication token (SMS, tiqr or YubiKey) and complete the self-registration process until step 4 "Activation code'.
5. Contact us (support@surfconext.nl) for an appointment to finish the registration (ca. 5 minutes). For the Pilot environment, the appointment can be by telephone or Skype call.
6. Do not forget to bring/have your activation code and second factor authentication token (SMS, tiqr or YubiKey) ready.
7. After verification SURFnet will activate your token and you can login.

Test environment

Policy

- Strictly no policy 😉
- This environment is for testing purposes only.
- There is no assurance for the authentication with this environment.
- Support is 'best effort'.

Registration procedure

We use the same software in test as in production, and thus need to follow most of the procedural steps. For practical purposes we skip the face to face part of the process. We do however need you to perform an authentication with the token to be activated. This is why we ask you to make an appointment so you can perform the authentication once we initiate the activation of your token from our side.

1. Register a Onegini account.
2. Make sure to complete Onegini's verification process of your mail address: this is required for registering a SURFsecureID token.
3. Go to https://sa.test.surfconext.nl/ and login with your Onegini account.
4. Request a second factor authentication token (SMS, tiqr or YubiKey) and complete the self-registration process until step 4 "Activation code'.
5. Contact us (support@surfconext.nl) for an appointment to finish the registration (ca. 5 minutes). For the TEST environment, the appointment can be by telephone or Skype call, chat or email. You do NOT have to visit us.
6. Do not forget to bring/have your activation code and second factor authentication token (SMS, tiqr or YubiKey) ready, you will need it during the activation process. The activation code is shown in step 4 of the registration process, and is sent to you by email.
7. After verification SURFnet will activate your token and you can then use it login at LoA/level 2 or above.

Until you have activated your token, you can only use the account to authenticate at LoA 1. SFO authentication always requires an activated token.

Attributes

The following attributes are available when using a OneGini account. Whether you actually receive these attributes depends on the attribute release policy (ARP) that is configured for your SP in SURFconext:

Friendly name	Attribute name	Value
SURFconext ID	urn:oid:1.3.6.1.4.1.1076.20.40.40.1	urn:collab:person:surfguest.nl:<uid>
uid	urn:mace:dir:attribute-def:uid urn:oid:0.9.2342.19200300.100.1.1	Previous SURFguest username when this is a migrated account. Otherwise generated by Onegini.
Surname	urn:mace:dir:attribute-def:sn urn:oid:2.5.4.4	Registered surname
Given name	urn:mace:dir:attribute-def:givenName urn:oid:2.5.4.42	Registered first name
Common name	urn:mace:dir:attribute-def:cn urn:oid:2.5.4.3	Registered common name
Display name	urn:mace:dir:attribute-def:displayName urn:oid:2.16.840.1.113730.3.1.241	Same as common name
Email address	urn:mace:dir:attribute-def:mail urn:oid:0.9.2342.19200300.100.1.3	Registered email address ⚠ will only be provided after the user confirmed his email address (via the Onegini website).
Organization	urn:mace:terena.org:attribute-def:schacHomeOrganization urn:oid:1.3.6.1.4.1.25178.1.2.9	surfguest.nl
PrincipalName	urn:mace:dir:attribute-def:eduPersonPrincipalName urn:oid:1.3.6.1.4.1.5923.1.1.1.6	<uid>@surfguest.nl

There is no attribute that shows which authentication provider (Facebook, Google, LinkedIn, Twitter) the user used.