Setting up SAML

What is SAML?

SAML is a method of Single Sign on where you can redirect your user administration to a single Identity provider, instead of having your user management spread out a whole bunch of different applications. The two big terms you need to be aware of are:

- **Identity Provider (IDP):** A central database that contains all user data, where a user can log in.
- **Service Provider (SP):** An application that requires users to log in through the identity provider.

Whenever a user tries to log into the service provider, he gets redirected to the login page of the identity provider. There he can log in, and the identity provider redirects the user back to the service provider. The communication happens over SSL, using certificates in order to be able to trust each other.

SAML in NetYCE

NetYCE can act as a service provider. You can set it up so that users can log in through your identity provider, instead of the standard login page. If you have turned on SAML login, a button will appear on the main login page that redirects the user to your SAML identity provider. After logging in, you will be redirected to the main login page.

Users can log in both with NetYCE and SAML accounts, and a SAML account can also have a NetYCE password. If you log in with SAML and your user isn't yet known in NetYCE, a new user will be created. This user will have the Default user group, or have its group name provided through its SAML response (Note that the User group needs to be known in NetYCE).

The settings for SAML are provided in the login profiles.

Profiles

NetYCE login profiles can be found in the Yce_setup table. You can edit them in the Custom Data forms, if you go to the Yce_setup table. At the moment there unfortunately is no other way to modify login profiles. A login profile determines what kind of login settings are used for a given machine. There are two kinds of records in the Yce_setup table: those belonging to a profile, and those belonging to a server. We are interested here in the profile, but first you need to find the profile that your machine uses. You can find it by finding the record with your servername in the profile field and 'profile' in the parameter field. The Str_value contains the profile you want.

To enable SAML, find the line in your profile with parameter “enable_saml”, and change it from “yes” to “no”:

Beyond that, you can find a number of settings for SAML in your profile. Here are the relevant ones, and what they mean:

Parameter	Description
enable_saml	Turns on SAML. A button in the login page will appear that will redirect the user to your identity provider login page
enable_saml_logout	If SAML is enabled, logging out will be done through your SAML identity provider. If not, your cookies will be simply thrown away and you will be redirected to the front page, without notifying your identity provider
ca_certificate	The SSL certificate file of your identity provider. Default is saml.idp.crt in the /opt/yce/etc directory. If this value is wrong SAML won't work
metadata_filename	The path and name of the SAML metadata file of your identity provider. Default is saml.config.xml in the /opt/yce/etc directory. If this value is wrong then SAML won't work.
metadata_redirect	In your metadata file, there should be a reference to the url your user should be redirected to after a successful login. This should be the key to that value. Default is 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect'
idp_issuer	The name of the identity provider. This usually is in the form of a url
provider_name	The name of the identity provider's organization
user_id_attribute	The attribute name for the user's username in your identity provider. Defaults to 'user_id'
first_name_attribute	The attribute name for the user's first name in your identity provider. Defaults to 'first_name'
last_name_attribute	The attribute name for the user's last name in your identity provider. Defaults to 'last_name'
email_attribute	The attribute name for the user's email in your identity provider. Defaults to 'email'
group_names_attribute	The attribute name for the user's group names in your identity provider. Defaults to 'group_names'
grp_list_pattern	Filters group names from the SAML response. Supports ? and * wildcards. Defaults to '' (no filter)

Metadata

If your Identity provider supports the ability to parse service provider metadata, you can find it at the url “https:/{server}/operate/saml_metadata.pl”. This will provide:

- The public ssl key of your NetYCE server
- The login callback url that the user will be redirected to after a successful login
- The logout callback url that the user will be redirected to after a successful logout

Setting up SAML

In order to set up SAML, you need to configure NetYCE as a service provider. This is done through the saml login profile. You need to get the public SSL certificate and SAML metadata of your identity provider and upload it to your NetYCE VM. Recommended is to upload them into the “/opt/yce/etc/” directory. You also need to provide a number of settings to your identity provider. These are the values you need to provide to your identity provider:

- **Callback url:** “https:/{server}/operate/saml_callback.pl” - this is provided in the NetYCE SAML Metadata.
- **Logout callback url:** “https:/{server}/operate/saml_logout_callback.pl” - this is provided in the NetYCE SAML Metadata.
- **The public SSL key of your NetYCE machine:** For more information on how to generate the necessary keyfiles: mk_ssl_cert.pl

For each user, we also need the following:

- **User id:** The user's username. This will also be the user's username in NetYCE
- **First name:** The user's first name. Optional.
- **Last name:** The user's last name. Optional.
- **Email:** The user's email. Optional.
- **Group names:** A list of the user groups the user is a member of.

User Groups

When NetYCE processes a logged in user's response, it looks at the list of group names returned. It then checks all of them against the NetYCE database, and assigns the user to the group with the highest user level. If it can't find any, the user is assigned to the group “Default”. This group can be set up in NetYCE with the permissions you require.

If you want to be able to filter the list of group names on NetYCE's side, the profile setting grp_list_pattern can be used. This supports ? and * wildcards, and only the group names that match this pattern will be evaluated.

Note that Group names need to exist in NetYCE. Otherwise they will get ignored.

Logging in

When the login profile setting 'enable saml' is set, the login screen shows a “Login using SAML” button, next to the login button. When the user clicks on it, he gets redirected to the login page of your identity provider.

The user logs in in the identity provider, and the identity provider takes the specified callback url and redirects the user back to it. The callback url then processes the SAML response (after validating the certificates are all correct), and logs the user into NetYCE. The user then gets redirected to the main inventory page.

Logging out

When a SAML user clicks on the logout button, it depends wether the login profile setting “enable_saml_logout” is set to “yes” or “no”.

- If yes, then the user will be redirected to your identity provider logout page. This page then redirects to NetYCE's saml logout callback page, which logs out the user, deletes the user's cookies and redirects him back to the login page.
- If no, then the user's session and cookies will be removed and the user will be redirected to the

login page. The user is logged out, but the identity provider doesn't know about it.