MISP2 installation and configuration guide

Version 2.12

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti tuleviku heaks

Contents

1. Introduction

This document describes the installation and configuration of the MISP2 application.

2. Environment requirements

- Supported operating system: Ubuntu Server 18.04 Long-Term Support (LTS), 64-bit.
- Needs connection with an X-road security server (internal interface), which has an X-road setup in place; MISP2 operates through X-road.
- Recommended hardware requirements: 64-bit processor, 4 GB of RAM
- Optional requirements:
  - OCSP validation service contract with Estonian Certification Center if you enable query response signing in MISP2 web application and use OSCP to check user certificates during ID-card identification.
  - OCSP responder certificate for OCSP response signature check.

3. MISP2 Installation

This chapter describes the installation of MISP2 portal components.

Installation requires root privileges. These can be gained using the following command:

```
sudo -i
```

3.1. Updating the MISP2 package list

Configure MISP2 package repository location in the file /etc/apt/sources.list.d/misp.list. This command adds MISP2 repository location to the file: /etc/apt/sources.list.d/misp.list:

```
echo "deb https://x-tee.ee/packages/live/misp2/debs/packages-niis/ bionic main">> /etc/apt/sources.list.d/misp.list
```

As MISP2 packages are not part of the official Ubuntu repository, the public key used to sign them should be added to your list of trusted keys.

```
curl https://artifactory.niis.org/api/gpg/key/public | apt-key add
```

The package list should then be updated with the command:

```
apt-get update
```

3.2. MISP2 database package

The MISP2 database package *xtee-misp2-postgresql* is installed using the command:

```
apt-get install xtee-misp2-postgresql
```

Below is a list of questions and answers displayed after this command is run.

Enter a name for the database to be created, the default is ‘misp2db’:

```
Please provide a database name: [misp2db]
```

Enter a username for the database to be created, the default is ’misp2’:

```
Please provide a username for accessing the database: [misp2]
```

Once this information has been provided, the installation script will try to connect to the database. If this is not successful, the user will be asked to create a new database. If they answer ‘no’, the script will proceed to the next step. If you do wish to create a new database with the default name, you can proceed with the default answer (*enter*), otherwise, answer ‘n’, in which case the script will display an error once it has finished.

```
Are you sure you want to create a new database 'misp2db' (y/n)? [y]
```

If you answered ‘yes’ to the previous question, enter a password for the new database user (2 times):

```
Adding new user misp2

Enter password for new role:

Enter it again:
```

3.3. MISP2 application

Install the package *xtee-misp2-application*.

```
apt-get install xtee-misp2-application
```

This package is dependent on the *xtee-misp2-base* and *xtee-misp2-orbeon* packages, which, in turn, are dependent on the *apache2*, *libapache2-mod-jk,* and *tomcat8* packages. These packages will be installed automatically.

The installation utility will ask a number of questions, which will be explained in the chapters below.

3.3.1. Apache Tomcat + Apache HTTP Server + MISP2 base package

Answer ‘yes’ to the question below if you wish to use ID-card authentication. This will download the necessary certificates from the SK repository:

```
Do you want to update the SK certificates (y/n)? [y]
```

Overview of operations performed by the installation package:

1. Configures memory for Tomcat in the file */etc/default/tomcat8*:
   JAVA_OPTS="${JAVA_OPTS} –Xms512m –Xmx512m -XX:MaxPermSize=256m"

2. Opens the Tomcat AJP connector on port 8009: removes comment symbols from the line <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> in the Tomcat configuration file *server.xml*.
3. Prohibits access to the Tomcat port 8080 in the 8080 *server.xml* configuration file.
4. Creates the *mod_jk* configuration file and stores it in the */etc/apache2/mods-available* directory (see the supplied example file: *jk.conf*) and adds the corresponding link in the */etc/apache2/mods-enabled* directory (e.g.: a2enmod jk).
5. In addition, activates the following modules: *rewrite* (a2enmod rewrite), *ssl* (a2enmod ssl), *headers* (a2enmod headers) and *proxy_http* (a2enmod proxy_http – the proxy module required for *proxy_http* is activated automatically.
6. Creates a *virtualhost* using an SSL connection in the Apache configuration file.
7. Allows only SSL connections: redirects HTTP connections to HTTPS (443) port (to 4443 in the case of software-initiated queries).
8. Configures the *mod_jk* module in the Apache configuration file.
9. Installs the HTTPS server (generated) certificates, Estonian ID-card root certificates, and the Mobile-ID security certificate.
10. Installs the certificates of revocation lists and OCSP query.
11. Restarts Apache (apache2ctl restart).

Configuration files and directories installed:

```
/etc/apache2/sites-available/ssl.conf
/etc/apache2/ssl/
/etc/apache2/ssl/create_server_cert.sh
/etc/apache2/ssl/create_sslproxy_cert.sh
/etc/apache2/ssl/updatecrl.sh
/var/lib/tomcat8/conf/server.xml
```

3.3.2. MISP2 web application

Answer ‘y’ to the next question to configure MISP2 as an international (EU) version or ‘n’ to configure it as an Estonian version (see below for the configuration parameters corresponding to each):

```
Do you want to configure as an international version (if no, then it will be configured as an Estonian
version)? [y/n] [default: n]:
```

In the case of the international version, the following configuration is used:

```
languages = en
```

```
countries = GB

auth.IDCard=false

auth.certificate=true

xrd.namespace=http://x-road.eu/xsd/x-road.xsd
```

In the case of the Estonian version, the following configuration is used:

```
languages = et

countries = EE

xrd.namespace=http://x-road.ee/xsd/x-road.xsd
```

The next question will ask for the following MISP2 database parameters: database server IP, port, database name, database username, and password. In general, all the default values fit, except for the database password.

NB! These parameters must match the ones given during *xtee-misp2-postgresql* package installation.

```
Please provide a database host IP to be used [default: 127.0.0.1]:

Please provide a database port to be used [default: 5432]:

Please provide a database name to be used [default: misp2db]:

Please provide a username to be communicating with the database [default: misp2]:

Please enter a password for the database user 'misp2':
```

Answer ‘y’ to the next question to configure activities related to the Estonian ID-card:

```
Do you want to configure the signing and encryption of Estonian ID-card certificates? [y/n]
```

When answering ‘yes’ to the previous question, additional questions will be asked for activities related to the D-card.

Enter PIN2 – for server-side signing (the server assumes the existence of a digital stamp):

```
Please enter PIN2:
```

Answer ‘y’ to turn on encryption with the ID-card:

```
Turn on the use of encryption: [y/n]:
```

Answer ‘y’ to turn on server-side digital signing:

```
Turn on the use of digital signing: [y/n]:
```

Answer ‘y’ to the following question to enable Estonian mobile-ID authentication (also assumes a respective service contract):

```
Do you want to enable authentication with Mobile-ID? [y/n]
```

When answering ‘yes’ to the previous question, a mobile-ID service name must be entered:

```
Please provide a Mobile-ID service name:
```

Next, e-mail related parameters are specified (SMTP server address, e-mail address used by MISP2):

```
Please provide a SMTP host address [default: smtp.domain.ee]:

Please provide a server email address: [default: info@domain.ee]:
```

In the case of the international version, the user is also asked to provide X-road version 6 instances and member classes. Both must be provided in a comma separated list.

```
Please provide x-road v6 instances (comma separated list)? [default: eu-dev,eu-test,eu]

Please provide x-road v6 member classes (comma separated list)? [default: COM,NGO,GOV]
```

Once the configuration files have been created, the user is asked to create an administrator account. It is recommended to use the default setting by answering ‘yes’. Otherwise, an administrator account, which is needed to configure the portal using the administrator interface, will not be created.

```
Do you want to add a new administrator account? [y/n] [default: y]
```

Once the administrator account has been created, the user is prompted for the IP addresses to be allowed to access the administrator interface. If the administrator is logged in using SSH, the default value will be the IP address of the SSH client. The administrator of the application must determine whether this IP address should be allowed to access the administrator interface, in which case the default value can be used. Otherwise, a different IP address should be provided. Several IP addresses, separated using a space, may also be used. (X.X.X.X denotes the address of the SSH client).

```
IP address from which the administrator interface can be accessed is currently '127.0.0.1' in
/etc/apache2/sites-available/ssl.conf.

User remote IP is 'X.X.X.X'.

Please provide IP address(es) allowed to access the administrator interface: [default: X.X.X.X]
```

The IP addresses allowed to access the administrator interface can be changed later in the Apache2 configuration file (see chapter 5.1).

Answer ‘y’ to the following question to configure a HTTPS connection between the MISP2 application and the X-road security server during installation:

```
Do you want to enable a HTTPS connection between the MISP2 application and the security server? [y/n]
[default: n]
```

If the answer is ‘y’, the next step to configure HTTPS is to export the security server’s certificate file *certs.tar.gz* from the security server (see Chapter 9 of the X-Road 6 security server user guide: ‘*9 Communication with the Client Information Systems*’) and copy it to the MISP2 server’s /usr/xtee/apache2/ directory. The name of the certificate for X-road v6 security server is *certs.tar.gz*, while the name of the certificate for X-road v5 security server is *proxycert.tar.gz* – both formats are supported.

The installation script checks for the existence of this certificate file and if the file is not found, it asks the user to either copy it to the correct location or cancel the HTTPS configuration, as shown in the question below. If the file has been copied to the MISP2 server, the user should answer ‘y’. Answer ‘n’ if you wish to cancel the operation, in which case the HTTPS configuration can be performed again later as described in chapter 4.3.

```
Please add the Security Server certificate archive 'certs.tar.gz' to the MISP2 server directory
'/usr/xtee/apache2/'.

Proceed with HTTPS configuration? (Answering 'no' means that HTTPS configuration will not be done
this time) [y/n] [default: n]
```

Once this has been completed, the passwords for the *truststore* and *keystore* certificate repositories must be entered. These must be at least 6 characters long. The passwords will not be displayed while typing.

```
Enter the truststore password:

Enter the keystore password:
```

When the security server’s certificate is added to the certificate repository, the user will be asked if they trust the certificate. You should answer *yes*.

```
Trust this certificate? [no]: yes
```

The installation script will then generate a MISP2 certificate file and display its location to the user.

```
Get '/usr/xtee/app/cert.cer' and add it to your Security Server.
```

The certificate file (*/usr/xtee/app/cert.cer/* in this example) should be copied to the security server.

Set HTTPS as the connection method for the information system servers on the security server (see the security server user guide).

After installing the web application you can proceed to configuring the MISP2 portal through the administrator web interface as described in Section 5.1 of this guide.

In a production environment, the particular institution’s certificate should also be added to the Apache HTTP server to allow for HTTPS connections. This is described in chapter 4.1.

4. Configuration

4.1. Configuring an HTTPS certificate for the MISP2 Apache web server

During initial installation, a self-signed certificate is generated for the Apache HTTP server. In a production environment, it is advisory to replace this with an actual CA-issued certificate.

By default, Apache uses the following certificate files:

```
SSLCertificateFile /etc/apache2/ssl/httpsd.cert

SSLCertificateKeyFile /etc/apache2/ssl/httpsd.key
```

It is recommended to use the same filenames for your own certificates and use these to replace the default files (changing the apache configuration file is not recommended, as it is overwritten when MISP2 is updated, which can cause changes to be lost). The contents of the DH parameter file (/etc/apache2/ssl/dhparams.pem) should also be added at the end your certificate file (httpsd.cert).

4.2. MISP2 configuration file

The MISP2 installation script will configure the database connection and other parameters in the *config.cfg* configuration file. After installation, some parameters can be changed in the configuration file. By default, its location is:

/var/lib/tomcat8/webapps/misp2/WEB-INF/classes/config.cfg.

Below is a list of some parameters which, though automatically set during installation, may later need to be changed when the application is reconfigured.

After the configuration file is changed, tomcat must always be restarted using the command: service tomcat8 restart

Parameters for establishing a connection with a database server:

```
# DB Info – database server and user parameters
jdbc.driver=org.postgresql.Driver
jdbc.url=jdbc:postgresql://IP/DB-NAME
jdbc.username=USERNAME
jdbc.password=PASSWORD
jdbc.databasePlatform=org.hibernate.dialect.PostgreSQLDialect
```

Language and country parameters:

```
#Languages to which the user is allowed to switch and in which can descriptions be set for different elements. Defined in http://en.wikipedia.org/wiki/List_of_ISO_639-1_codes

#If no suitable languages are defined, then the system will use the default locale language

languages = et

#Countries which can be as the user's country. Defined in http://en.wikipedia.org/wiki/ISO_3166-1_alpha-2

#If no suitable countries are defined, then the system will use the default locale country

countries = EE
```

Server ID-card parameters (for server-side digital signing and encryption):

```
# ID Card and its usage settings
digidoc.config_file=jar://JDigiDocID.cfg
digidoc.PIN2=01497

email.allow.sign_query=false
email.allow.encrypt_query=false
```

Mail server parameters:

```
email.host = mailserver.domain.ee
email.sender.name = MISP2 Support
email.sender.email = info@asutus.ee
```

Mobile-ID authentication setup parameters:

```
# Mobile ID and its usage settings
mobileID.digidocServiceURL = https://digidocservice.sk.ee/
mobileID.serviceName = Testimine
```

4.3. *Configuring HTTPS connection between MISP2 application and X-Road security server*

The steps for configuring HTTPS:

1. Export the security server's certificate file *certs.tar.gz* from the security server (see Chapter 9 of the X-Road 6 security server user guide: '9 Communication with the Client Information Systems') and copy it to the MISP2 server's */usr/xtee/apache2/* directory.

   The name of the certificate for X-road v6 security server is *certs.tar.gz*, while the name for X-road v5 security server is *proxycert.tar.gz* – both formats are supported.

2. Run the configuration script on the MISP2 server:

```
/usr/xtee/app/create_https_certs_security_server.sh
```

The possible answers to questions asked by the script are described in this guide's web application installation chapter.

The script checks for the existence of the *certs.tar.gz* or *proxycert.tar.gz* security certificate archives in the MISP2 server's */usr/xtee/apache2/* directory, creates key repository *misp2truststore.jks,* generates the certificate for communication with the security server, installs the private key and certificate obtained in the *misp2keystore.jks* key repository, creates the key repository and imports the PKCS12 file obtained, sets the necessary system parameters for the MISP2 server in the Tomcat configuration file */etc/default/tomcat8,* and restarts Tomcat.

3. Configure the security server to use HTTPS to connect to the information system and add the certificate generated in step 2 (for X-road v6 */usr/xtee/app/cert.cer)* to the security server (see the security server's user manual for additional instructions).
4. Open the administrator interface of the MISP2 portal and change the 'address of the institution's security server' and 'the address of sending queries' options from HTTP→HTTPS. If the security server's IP or domain name is *SEC_SERVER_IP*, then replace:
   - *http://SEC_SERVER_IP → **https**:// SEC_SERVER_IP*
   - *http:// SEC_SERVER_IP /cgi-bin/consumer_proxy →*
     ***https**:// SEC_SERVER_IP /cgi-bin/consumer_proxy*

4.4. Configuration of Mobile-ID

4.4.1. Service parameters

In the configuration file, parameters *mobileID.rest.relyingPartyUUID* and *mobileID.rest.relyingPartyName* must be set up with the correct value. The Certification Centre (SK ID Solutions - https://www.skidsolutions.eu/en/services/mobile-id/technical-information-mid-rest-api/) assigns the respective service name value to every institution.

4.5. Other settings

4.5.1. Configuration of Java VM

If required, Java system parameters can be modified in the file */etc/default/tomcat8.*

The installation script configures the memory usage parameters as follows but increase the values provided, if required, for example:

```
JAVA_OPTS="${JAVA_OPTS} –Xms2048m –Xmx2048m-XX:MaxPermSize=256m"
```

4.5.2. Logging settings

Logging settings are set in file */var/lib/tomcat8/webapps/misp2/WEB-INF/classes/log4j2.xml*

The mainly used properties in the file are *<Root level="info">*, *<Logger name="org.hibernate" level="info" additivity="false">*, and *<Logger name="ee.aktors.misp2" level="info" additivity="false">*.

If there is a need to see more information in the log, set the level of these parameters as *DEBUG*.

For example, instead of
<Root level=”info”>
use
<Root level=”debug”>

4.5.3. Adding a HTTPS certificate

HTTPS certificates can be added using the keytool command.

```
keytool -import -keystore /etc/ssl/certs/java/cacerts -storepass changeit -file [CERT_PATH] -
alias
[CERT_ALIAS]
```

Restart the Tomcat service for the changes to take affect.

```
service tomcat8 restart
```

4.6. Administration of MISP2 administrator accounts from command line

There is a tool for administrating the administrator accounts of the MISP2 application. This tool is launched from the command line as follows:

```
/usr/xtee/app/admintool.sh
```

The list of existing administrator accounts is displayed by default.

Add the ‘-add’ parameter to the command line to add an administrator account:

```
/usr/xtee/app/admintool.sh -add
```

Add the ‘-delete’ parameter to the command line to delete the administrator account:

```
/usr/xtee/app/admintool.sh -delete
```

4.7. Enabling Orbeon inspector

The inspector (*Orbeon inspector*) is an Orbeon module, which allows the user to inspect X-road messages and other application data sent and received by services.

In MISP2, the inspector can be enabled by changing the value of the *oxf.epilogue.xforms.inspector* parameter in the */var/lib/tomcat8/webapps/orbeon/WEB-INF/resources/config/properties-local.xml* file.

By default, after MISP2 installation this line is set to *false*.

To enable the inspector, its value needs to be *true*:
*<property as="xs:boolean" name="oxf.epilogue.xforms.inspector" value="***true***"/>.*

Once changed, the file must be saved and the inspector should appear in the interface. The Tomcat server does not need to be restarted.

5. MISP2 administration interface

Append '/admin' to the portal URL to enter the administration interface. For example: *https://<portaali_aadress>/misp2/admin/.*

5.1. Additions to Apache web server configuration

If an administrator account has been created during the installation of the MISP2 web application and allowed IP addresses have been specified, the installation script will have automatically added them to the Apache configuration file. In this case, the steps described in this chapter do not need to be repeated.

If you wish to change or edit the IP addresses allowed to access the administrator interface, you can edit the Apache configuration file:

```
vi /etc/apache2/sites-available/ssl.conf
```

Find the following lines in this file:

```
<Location "/*/admin/*">

   Order deny,allow

   Deny from all

   Allow from 127.0.0.1

</Location>
```

Add the address of your own computer *<Location>* to the end of the line below, e.g.:

```
Allow from 127.0.0.1 192.168.215.233
```

Restart the web server:

```
/etc/init.d/apache2 restart
```

5.2. Portal administration

This chapter describes the administration of a portal in the MISP2 web application.

5.2.1. Creating portal

Enter the administration interface to create a portal. A form containing the following fields is displayed to create a new portal:

- **Portal name * –** the name of the portal
- **Portal short name * –** a short name for the portal used to identify the portal for the application and saving the history of activities. The short name of the portal must be unique within the application.
- **Organization name** * and **Organization code*** are the name and the registry code of the main institution associated with the portal. The registry code of the main institution is included with every query. If the registry code of the main institution corresponds to an existing institution in the application, the portal is associated with the existing institution and the existing institution name is overwritten with the name entered last.
  X-road version 6 also uses the institution's registry code as the member code in the header of an X-road query (*xrd:client/iden:memberCode*).
- **Portal type** – indicates the type of portal. Portal types are described in more detail in Chapter 1 of the user's guide. Possible options are as follows:
  - Open services portal
  - Organization's portal
  - Universal portal
- **X-road protocol version** determines the message format for the portal's users and meta services. This is used when communicating with the X-road security server. The user can choose between the following protocols: 3.1 (X-road version 5) and 4.0 (X-road version 6). X-road version 3.1 can be replaced globally for the entire application with protocol version 3.0 by changing the *xrd.v5.namespace* parameter as follows: *xrd.v5.namespace=http://x-rd.net/xsd/xroad.xsd*
  The X-road version 5 portal also supports the services of protocol 2.0 (X-road version 4).
- **X-road member class** – a configuration parameter of X-road version 6, which determines the general category of the X-road client, i.e. whether it is a government institution (GOV), commercial institution (COM) or some other kind of institution. The option becomes available if X-road has been configured to use protocol 4.0. The parameter is included in the header of X-road queries in the *xrd:client/iden:memberClass* line.
- **X-road subsystem code –** a configuration parameter of X-road version 6, which allows for the differentiation of various X-road client and server applications within the same institution. The option becomes available if X-road has been configured to use protocol 4.0. The parameter is included in the header of X-road queries in the *xrd:client/iden:subsystemCode* line.

- **Security host* –** the address of your security server.
- **X-road client instance** – a configuration parameter of X-road version 6, which determines the X-road environment used, e.g. *ee-dev* and *EE* denote the Estonian X-road development environment and production environment, respectively. The option becomes available if X-road has been configured to use protocol 4.0. The parameter is included in the header of X-road queries in the *xrd:client/iden:xRoadInstance* field.
- **X-road instances for services** – can be used to select from a predetermined list which X-road instances are used when services are updated in the portal manager. Based on this selection, the manager can determine which X-road instance services are included in the manager's interface.

  By default, the list of instances is loaded from the portal's configuration file.

  Pressing 'load instances from security server' will add all federated X-road instances from the X-road security server to the list. After this, they can be used in the portal.

  Pressing 'load default instances' will reload the list of instances from the configuration file.

  The service instance is included in X-road queries in the *xrd:service/iden:xRoadInstance* line*.*
- **Services sending address* –** the address of the server through which all queries pass
- **Developer view** – if set to 'On', adds an 'add database' (add database manually) button to the 'Services' section of the service- or portal manager. A 'From WDSL' button is added to the database subsection. This allows for a list of services to be updated by using WSDL.
- **Send audit log to security server** – determines whether a logOnly request will be sent to the security server, so that actions logged in the MISP2 application are also included in the security server's logs. X-road version 5 queries the security server's *xrd.logOnly* meta service. Support for this meta service has been removed in X-road version 6. Because of this, in a version 6 portal, the *logOnly* service data must also be entered: '**logOnly' service member class,** '"**logOnly" service member code'** and '**logOnly' service subsystem code'**. These fields are only displayed in the administrator portal if X-road version 6 is used.
  To start the *logOnly.v1* service, the *misp2-soap-service-v6*.war addon module is included in MISP2, which the manager can run in its environment. This is described in further detail in the installation guide for addon modules.
- **Topics in use –** if this is marked, services will be grouped for users according to topics. Portal administrator deals with topics administration. Topics administration will be discussed in another chapter. If topics are not used, services will be grouped per database as usual.
- **The folder field is used in the input of the service** – in an X-road version 5 portal, the header field of the folder is added in the input of the message.

After entering all of the required data, click on 'Save portal configuration'. The portal data is written to the database as a result.

Portal administration is somewhat different in the case of a *universal portal*.

The following fields must be completed for a universal portal in addition to the standard fields:

- **Unit registering is allowed –** a check box indicating whether the registration of new units by users is allowed in the application. If marked, the following fields marked with ** must be filled in.
- **Auth query service name** –** the name of the meta query used to check the unit's representation rights. In X-road version 4 and 5 portals, the full service name must be entered into a text field. X-road version 6 presents the user with a selection of services previously defined in the configuration file. In a universal portal, services are defined in the *uniportal-conf.cfg* file. In a legal person portal, the services for sending queries to determine the right of representation are defined in the *orgportal-conf.cfg* file.
- **Check query service name* –** the name of the query used to check the unit's validity. The full service name must be entered into a text field in X-road version 4 and 5 portals. X-road version 6 portal presents the user with a selection of services previously defined in the *uniportal-conf-cfg* configuration file.
- **Auth query control time (hours) ** –** the period of time after which a new query must be performed as the validity of the old query ends.
- **Auth query maximum control time (hours) ** –** the maximum time period allowed during which users can perform queries related to an institution's rights if the check query does not respond.
- **Use permission manager –** if checked, the 'user with representation rights' section will include an 'access rights manager' menu option, provided that the current role has been accessed via the 'registrar' role. If it has been accessed via the 'portal manager' role, this option is always visible. Using this menu option, users with representation rights can assign query-performing rights to access rights managers and users in the course of registering a new unit. Otherwise, assigning managers is not allowed. This field is also displayed for legal person portals, as they are a sub-type of the universal portal. Note that for legal person portals this value is valid only if institutions have rights of exclusive representation.
- **Portal unit is X-Road organization –** if selected, the code of the active unit is included in service message headers in the 'consumer' field. If left unselected, the code of the main institution is included in service message headers in the 'consumer' field and the code of the active unit is included in the 'unit' field.

5.2.2. Modifying portal

Enter the administrator interface to modify a portal. The portal registered to you is displayed. Click on ‘Save portal configuration’ to save the changes. You cannot change the portal type. To do this, you must delete the existing portal and add a new one. The registry code of the main institution associated with the portal cannot be changed.

5.2.3. Deleting portal

You can delete a portal via the administration interface by clicking on ‘Remove portal’ on the portal administration form. The portal and all objects associated with it are removed from the application if this button is pressed.

5.2.4. Adding portal manager

Click on ‘Add new manager’ on the portal configuration form to add a portal administrator. As a result, you will be directed to the managers view, where you can search for users from existing user accounts and add new portal managers. To add one, the portal in question must first be saved.

The mandatory fields – personal identification code and family name – must be filled in when adding a new administrator. The e-mail address and job title are associated with the main institution and will not include subsequently added units.

Click on ‘Add manager’ after filling in the user form. The user is then granted the roles of portal administrator and standard user of the main institution. The ‘Remove user’ button removes the user and all relationships of this user to institutions and groups.

If a user search is used, a search is conducted among all system users to find those matching the entered parameters. The matches found are then listed.

Clicking on a user’s name opens the edit user form filled in with the data of the selected user, whereas the e-mail address and job title are associated with the main institution.

Clicking on ‘Add as manager’ immediately adds the user as a portal administrator.

5.2.5. Removing portal administrator

Use the portal configuration form to remove a portal administrator. This form includes the list of existing administrators.

The user is removed from the portal administrator role by clicking on the X-icon in the administrator’s row.

5.3. Administration of global XSLs

In addition to managing the portal, administrator rights also include the adding and administration of global XSLs used by the portal. Global XSLs are XSLs applied last to all queries according to priorities. The administration of global XSLs is similar to the administration of XSLs internal to the portal. (See the description of the service administrator role in the User’s Guide.)