X-road MISP2 installation and configuration guide

Version 1.20

Contents

1. Introduction 3
2. Environment requirements 3
3.MISP2 Installation 3
3.1. Java 3
3.2. PostgreSQL 3
3.3. Apache Tomcat + Apache HTTP Server + MISP2 base package 5
3.4. Orbeon XForms 6
3.5. MISP2 web application 7
4. Settings 10
4.1. Configuring HTTPS connection between MISP2 web application and security server 10
4.3. Other settings 11
4.4. Administration of MISP2 administrator accounts from command line 12
5. MISP2 administration interface 13
5.1. Additions to Apache web server configuration 13
5.2. Portal administration 13
5.2.1. Creating portal 13
5.2.2. Modifying portal 15
5.2.3. Deleting portal 15
5.2.4. Adding portal manager 15
5.2.5. Removing portal administrator 15
5.3. Administration of global XSLs 16

1. Introduction

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

2. Environment requirements

- Supported operating system: Ubuntu server LTS 10.04 64bit
- Needs connection with X-road security server (internal interface), which has x-road setup in place, MISP2 operates through x-road.
- Hardware requirements: 64-bit processor, 4GB of RAM
- Optional requirements:
  - OCSP validation service contract with Estonian Certification Center, only required in case
    1) query response signing in MISP2 web application is used;
    2) user certificate OCSP check is performed during ID-card authentication
  - OCSP responder certificate for OCSP response signature check.

3.MISP2 Installation

3.1. Java

Install Java SDK:

```
apt-get install openjdk-6-jdk
```

3.2. PostgreSQL

Install the PostgreSQL database server according to the standard installation instructions:

```
apt-get install postgresql-8.4
```

Configure the *pg_hba.conf* file (most likely located in the */etc/postgresql/8.4/main* directory) before installing the *misp2-postgresql* package and specify *trust* as the postgres user authentication method. This simplifies installation of the *misp2-postgresql* package.

```
vi /etc/postgresql/8.4/main/pg_hba.conf
```

```
# Database administrative login by UNIX sockets
```

```
local  all     postgres             trust
```

Enable database connections over TCP in the (*/etc/postgresql/8.4/main/*) *postgresql.conf* file.

```
vi /etc/postgresql/8.4/main/postgresql.conf
```

```
listen_addresses = '*'
```

Restart the database server:

```
/etc/init.d/postgresql-8.4 restart
```

After configuring PostgreSQL, add MISP2 package repository location to the server configuration file:

```
vi /etc/apt/sources.list
```

add line:

```
deb http://x-road.ee/misp2/packages lucid main
```

Install *misp2-postgresql* package by executing commands

```
apt-get update

apt-get install xtee-misp2-keyring
```

Answer 'y' to the following question:

```
Install these packages without verification [y/N]? y
```

After that set up *xtee-misp2-postgresql* package with commands:

```
apt-get update

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

The following questions can be answered by default answer (Enter):

```
Is PostgreSQL 8.x installed and running (y/n)? [y]

Please provide PostgreSQL client working directory
[/usr/lib/postgresql/8.4/bin]?

Please provide PostgreSQL server port [5432]?
```

Next, enter the name of the database, the default will be "misp2db":

```
Please provide database name that will be used: [misp2db]
```

Enter the database username, the default will be "misp2":

```
Provide username that will be (or is)  host of database: [misp2]
```

If this is a new MISP2 database installation, answer „add”.
If the existing MISP2 database is updated, answer „upgrade”.
NB! The default value is „upgrade”:

```
Upgrade existing database "misp2db" or add new?  (upgrade | add)
[upgrade]
```

For the next question, leave the default answer "n" (enter), except in case the database user has already been created:

```
Does user "misp2" already exists in database? (y/n) [n]
```

Enter a password for the new database user (2 times):

```
Adding new user misp2

Enter password for new role:

Enter it again:
```

To following questions leave by the default answer (enter):

```
Shall the new role be allowed to create more new roles? (y/n) [n]

Load default classifiers (y/n)? [y]
```

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

Installing Apache Tomcat and Apache2
Install the Apache Tomcat server according to the standard installation instructions and install *xtee-misp2-base* package:

```
apt-get install tomcat6

apt-get install apache2 libapache2-mod-jk

apt-get install xtee-misp2-base
```

The following shows questions asked during the execution of the last command to which you can answer with the default reply (press „Enter“):

```
Please provide Apache Tomcat server working directory [/var/lib/tomcat6]?

Please provide Apache2 working directory [/etc/apache2]?
```

For next question answer “yes” during the first installation (and not when upgrading version):

```
Do you want to create new CA and server certificates? [y/N]
```

For next question answer “yes” if Estonian ID card will be used for authentication:

```
Do you want to update SK certificates? [Y/n]
```

Overview of operations performed by installation package:

1.1 Configures memory for Tomcat in file: */etc/default/tomcat6*:
JAVA_OPTS="${JAVA_OPTS} –Xms512m –Xmx512m -XX:MaxPermSize=256m"

1.2 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*.

1.3 Prohibits access to the Tomcat port 8080 in the *server.xml* configuration file.

1.4 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).

1.5 In addition to this, 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).

1.6 Creates a *virtualhost* using an SSL connection in the Apache configuration file.

1.7 Allows only SSL connections: redirects HTTP connections to HTTPS (443) (to 4443 in the case of software-initiated queries).

1.8 Configures the *mod_jk* module in the Apache configuration file.

1.9 Installs the server certificates,Estonian ID-card root certificates and Mobile-ID security certificate.

1.10 Installs revocation lists and OCSP certificates.

1.11 Restarts Apache (apache2ctl restart).

Configuration files and directories installed:

```
/etc/apache2/sites-available/ssl
/etc/apache2/ssl/
/etc/apache2/ssl/create_server_cert.sh
/etc/apache2/ssl/create_sslproxy_cert.sh
/etc/apache2/ssl/updatecrl.sh
/var/lib/tomcat6/conf/server.xml
```

3.4. Orbeon XForms

Install the Orbeon XForms package by entering the following command:

```
apt-get install xtee-misp2-orbeon
```

The following shows a question asked during the execution of the last command to which you can answer with the default reply (press „Enter“):

```
Please provide Apache Tomcat server working directory [/var/lib/tomcat6]?
```

The install script copies *orbeon.war* to the Tomcat directory, restarts the server and configures Orbeon according to the requirements of MISP2 .

3.5. MISP2 web application

Install the MISP2 web application on the Tomcat servlet container by entering the following command:

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

The following shows the last command execution to submit additional questions:

```
Please select either you upgrading or installing new application
(install | upgrade) [default: install]:
```

When installing for the first time, answer to the above question: "install". When upgrading an existing application, answer :"upgrade".
The following question can be answered with default answer (Enter):

```
Please provide Apache Tomcat server working directory [default:
/var/lib/tomcat6]?
```

Answer „y” to the next question to configure MISP2 as an international version:

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

In case of the international version the following configuration is used in *$TOMCAT_HOME/webapps/$APP_NAME/WEB-INF/classes/config.cfg*:

```
languages = en

countries = GB

auth.IDCard=false
auth.certificate=true

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

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

```
languages = et

countries = EE

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

Several database parameters are queried next: 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 set up):

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

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

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

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

Please enter username password: [default:]
```

Answer „y" to the next question if Estonian ID-card is used in the application:

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

Answering „yes" to the previous question, extra questions will be asked for activities related to ID-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 ID-card:

```
Turn on using of encrypting: [y/n]:
```

Answer „y" to turn on the server-side digital signature:

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

Answer „y" to the following question, if Estonian mobile-ID authentication is used (also assumes respective service contract existence):

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

Answering „yes" to the previous question, mobile-ID service name must be entered:

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

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

```
Please provide SMTP host address:

Please provide server email address:
```

After installing the web application you can proceed to configuring the MISP2 portal through the administrator web interface as described in Section 4 of this guide.

The install script of this web application configures the database connection and other parameters in its configuration file *config.cfg*.

If needed, you can modify some parameters after installing in the file:
$TOMCAT_HOME/webapps/$APP_NAME/WEB-INF/classes/config.cfg.
The parameters presented next are configured automatically during installation but may need to be changed later when re-configuring the application.

Parameters for establishing connection with 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 (both language and country codes are separated by a comma):

```
#Languages to which 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 uses system default locale
language

languages = et

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

#If no suitable countries are defined, then uses system default locale
country

countries = EE
```

Server ID-card parameters (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@institution.ee
```

Mobile-ID authentication setup parameters:

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

4. Settings

4.1. Configuring HTTPS connection between MISP2 web application and security server

1. Install the security server's certificate in the *misp2truststore.jks* key repository:
   1.1. Export the security server's certificate from the security server (see the security server guide).
   1.2. Create the truststore *misp2truststore.jks* and import the certificate obtained:
   ```
   keytool -import -keystore misp2truststore.jks -file cert.der
   ```
   (*cert.der* – the security server's certificate)
2. Generate the certificate for communication with the security server:
   2.1. Run */etc/apache2/ssl/create_sslproxy_cert.sh* script (the openssl configuration file *misp2.cnf* must be located in the same directory).
3. Install the private key and certificate obtained in the *misp2keystore.jks* key repository:
   3.1. Convert the private key and certificate to the PKCS12 format (java keytool cannot import any other format):
   ```
   openssl pkcs12 -export -in sslproxy.cert -inkey sslproxy.key -
   out misp2.p12
   ```
   3.2. Create the key repository and import the PKCS12 file obtained:
   ```
   keytool -importkeystore -srcstoretype PKCS12 -srckeystore
   misp2.p12 -destkeystore misp2keystore.jks
   ```
4. Set the following system parameters for the MISP2 web application: *javax.net.ssl.trustStore*, *javax.net.ssl.trustStorePassword*, *javax.net.ssl.keyStore*, *javax.net.ssl.keyStorePassword*.
   4.1. Example: Add the following to the Tomcat configuration file */etc/default/tomcat6*:
   JAVA_OPTS="${JAVA_OPTS} -Djavax.net.ssl.trustStore=<location of the *misp2truststore.jks* file created> -
   Djavax.net.ssl.trustStorePassword=<*misp2truststore.jks* password> -
   Djavax.net.ssl.keyStore=<location of the *misp2keystore.jks* file created> -
   Djavax.net.ssl.keyStorePassword=<*misp2keystore.jks* password>“
5. Set HTTPS as the connection method for the information system servers on the security server and load the certificate generated during Step 2 onto the security server (see the security server guide).
6. Restart Tomcat.
7. Change the protocols for the fields ”*security server's address*” (Organisatisn's security server URL) and ”*päringute saatmise aadress*” (Query transmitting URL) from HTTP to HTTPS in the portal administration view (e.g. replace http://192.168.219.153 with

https://192.168.219.153 and http://192.168.219.153/cgi-bin/consumer_proxy with https://192.168.219.153/cgi-bin/consumer_proxy).

4.2. Estonian mobile-ID settings

Service name

In configuration file parameter *mobileID.serviceName* certainly must be setup with the correct value. Concrete service name value outputs to every institution Certification Center.

Server's certificate

Go to an address https://digidocservice.sk.ee/ and download digidocservice server certification and name it as a digidocservice.cer.

With next command line import the downloaded cerificate file (digidocservice.cer) into the truststore file (misp2truststore.jks). Note: if the configuration of HTTPS connection between MISP2 and security server was done previously, then the truststore file must already exist before this command.

```
keytool -import -keystore misp2truststore.jks -file digidocservice.cer -
alias digidocservice
```

If that isn't done yet, then setup misp2truststore.jks in tomcat configuration file */etc/default/tomcat6*:

```
JAVA_OPTS="${JAVA_OPTS} -Djavax.net.ssl.trustStore=<loodud misp2truststore.jks
faili asukoht>-Djavax.net.ssl.trustStorePassword=<misp2truststore.jks parool>
```

4.3. Other settings

Configuration of Java VM

If required, Java system parameters can be modified in the file */etc/default/tomcat6*.

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

```
JAVA_OPTS="${JAVA_OPTS} -Xms512m -Xmx512m -XX:MaxPermSize=256m"
```

Logging settings

Logging setting are set in file:
/var/lib/tomcat6/webapps/misp2/WEB-INF/classes/log4j.properties
The mainly used properties are: "log4j.rootLogger", "log4j.category.org.hibernate" ja "log4j.category.ee.aktors.misp2".
If there is a need to see more information in log, set level as "DEBUG".
For example "log4j.rootLogger=WARN, output2" instead of "log4j.rootLogger=DEBUG, output2".
Possible logging levels are appointed here http://logging.apache.org/log4j/1.2/manual.html

4.4. 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/xroad/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/xroad/app/admintool.sh -add
```

Add the ”*-delete*” parameter to the command line to delete an administrator account.

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

5. MISP2 administration interface

Append ”/admin” to the portal URL to enter the administration interface. For example: https://<portal_address>/misp2/admin/.

5.1. Additions to Apache web server configuration

NB! By default the administrator interface is accessible only to localhost. To allow access to the administrator interface from other computers, the address of the desired computer must be added to the Apache configuration file.

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

Find the following lines in this file:

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

    Order deny,allow

    Deny from all

    Allow from 127.0.0.1

 </Location>
```

Add the desired address to the end of the line below:

```
      Allow from 127.0.0.1, 192.168.215.233
```

Restart the web server:

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

5.2. Portal administration

Instructions for administering the MISP portal are provided in this section.

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 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.
- ***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
    - Business portal
    - Universal portal
- **Security host –** the address of your security server.
- **Services sending address –** the address of the server through which all queries pass.
- **BPEL engine to address** - WS-BPEL processing engine service address.
- **Topics in use –** if this is signed, then services will be grouped for users according to topics. Portal administrator deals with topics administration. Later in another chapter will be discussed about topics administration. If topics aren't in use, services will be gouped as usual database.
- **Save users history** – if this is signed, then users history will be saved in portal, for example creating a new user or assigning rights by groups. In addition to database, this history will be saved also in security server encrypted file.

After entering all of the required data click on "Save portal configuration". The portal data are 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 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.
- **Check query service name** – the name of the query used to check the unit's validity.
- **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, 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** – indicates whether the code of the main institution is included in service message headers or whether the code of the active unit is inserted in the ”consumer” 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 when 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.

When 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 adding and administration of global XSLs used by the portal. Global XSLs are XSLs applied last to all queries according to priorities. Administration of global XSLs is similar to administration of XSLs internal to the portal. (See the description of the service administrator role in the User's Guide.)