

MISP2 paigaldus- ja seadistusjuhend

Version 2.16



Euroopa Liit
Euroopa
Regionaalarengu Fond



Eesti tuleviku heaks

Sisukord

Sisukord	2
1. Sissejuhatus	3
2. Nõuded keskkonnale.....	3
3. MISP2 Paigaldamine	3
3.1. MISP2 pakettide nimekirja uuendamine	3
3.2. MISP2 andmebaasipakett	3
3.3. MISP2 rakendus	4
3.3.1. Apache Tomcat + Apache HTTP Server + MISP2 baaspakett	4
3.3.2. MISP2 veebirakendus	5
4. Seadistamine	8
4.1. MISP2 Apache veebiserveri HTTPS sertifikaadi seadistamine	8
4.2. MISP2 konfiguratsioonifail	9
4.3. HTTPS ühenduse konfigureerimine MISP2 rakenduse ja X-tee turvaserveri vahel	10
4.4. Mobiil-ID seadistamine	11
4.4.1. Teenuse parameetrid	11
4.5. Muud seadistused	11
4.5.1. Java VM seadistamine	11
4.5.2. Logimise seadistamine	11
4.5.3. HTTPS sertifikaadi lisamine	12
4.6. MISP2 administraatori kontode haldamine käsurealt	12
4.7. Orbeon inspektori sisselülitamine	12
5. MISP2 Administreerimise liides	13
5.1. Apache veebiserveri konfiguratsiooni täiendamine	13
5.2. Portaali haldamine	13
5.2.1. Portaali loomine	13
5.2.2. Portaali muutmine	16
5.2.3. Portaali kustutamine	17
5.2.4. Portaali halduri lisamine	17
5.2.5. Portaali halduri eemaldamine	17
5.3. Globaalsete XSL-ide haldamine	17

1. Sissejuhatus

Käesolev dokument kirjeldab MISP2 rakenduse paigaldamist ning seadistamist.

2. Nõuded keskkonnale

- Toetatud operatsioonisüsteem: Ubuntu Server 18.04 Long-Term Support (LTS), 64-bitine. Veel toetatakse ka vanemat versiooni 16.04 LTS, millele paigaldamist käesolevas juhendis ei kaeta.
- Vajalik ühendus X-tee turvaserveriga (siseliidesega), milles on seadistatud X-tee asutus, millena MISP2 tegutseb X-teel
- Riistvara soovituslikud parameetrid: 64 bitine protsessor, 4GB RAM
- Vajalik tingimuslikult:
 - OCSP kehtivuskinnituse teenuse kasutamise leping Sertifitseerimiskeskusega, kui on soov võimaldada päringutulemuste allkirjastamist MISP2 veebirakenduses ning ID-kaardiga autenditud kasutajate sertifikaatide kontrolli OCSP kaudu.
 - OCSP responder sertifikaat OCSP vastuse signatuuri kontrolliks.

3. MISP2 Paigaldamine

Käesolevas peatükis kirjeldatakse MISP2 portaalikomponentide paigaldamist.

Paigaldamine eeldab, et kasutajal on süsteemis olemas *root* õigused, mille saamiseks tuleb käivitada käsurealt järgnev käsk:

```
sudo -i
```

3.1. MISP2 pakettide nimekirja uuendamine

Konfigureerida MISP2 pakettide repositooriumi asukoht failis `/etc/apt/sources.list`. Järgnev käsk lisab MISP2 repositooriumi aadressi faili: `/etc/apt/sources.list` :

```
apt-add-repository "https://artifactory.niis.org/xroad-extensions-release-deb main" >> /etc/apt/sources.list
```

Et MISP2 paketid ei pärine ametlikust Ubuntu repositooriumist, tuleks pakettide allkirjastamiseks kasutatud avalik võti lisada lubatud võtmete hulka.

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

Siis tuleks pakettide nimekiri uuendada käsuga

```
apt update
```

3.2. MISP2 andmebaasipakett

MISP2 andmebaasipakett `xtee-misp2-postgresql` paigaldatakse käsuga:

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

Järgnevalt on ära toodud viimase käsu täitmisel esitatavad küsimused ja nende vastused.

Sisestada loodava andmebaasi nimi, vaikimisi jääb selleks „misp2db“:

Please provide database name: [misp2db]

Järgnevalt sisestada loodava andmebaasi kasutaja nimi, vaikimisi jääb selleks „misp2“:

Please provide username for accessing database: [misp2]

Paigaldusskript püüab seejärel kirjeldatud baasiga ühendust võtta. Kui see ei õnnestu, antakse kasutajale baasiloomise küsimus, muidu minnakse järgmise sammu juurde. Juhul kui soovitakse luua vastavanimelist baasi, võib anda vaikevastuse (*enter*), muidu vastata „n“, sellisel juhul lõpetab paigaldusskript veaga.

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

Vastates eelmisele küsimusele jaatavalt, tuleb järgnevalt sisestada baasikasutaja parool (2 korda):

Adding new user misp2

Enter password for new role:

Enter it again:

3.3. MISP2 rakendus

Paigaldada pakett *xtee-misp2-application*.

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

Sellel paketil on sõltuvused *xtee-misp2-base* ja *xtee-misp2-orbeon* pakettidele, millest esimesel on omakorda sõltuvused *apache2*, *libapache2-mod-jk* ja *tomcat8* pakettidele. Kõik nimetatud paketid installeeritakse automaatselt.

Installeerimiskrakendus küsib kasutajalt rea küsimusi, mis seletatakse lahti järgnevates alapeatükkides.

3.3.1. Apache Tomcat + Apache HTTP Server + MISP2 baaspakett

Järgnevale küsimusele vastamine: kui ID-kaarti hakatakse autentimiseks kasutama, siis: “yes”, sel puhul laetakse SK repositooriumist vajalikud sertifikaadid:

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

Paigalduspaketi tegevuste ülevaade:

1. Seadistab Tomcati mälu failis */etc/default/tomcat8*:

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

2. Avab Tomcat AJP connector pordil 8009: eemaldab kommentaarid realt `<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />` Tomcat konfiguratsioonifailis *server.xml*.
3. Keelab pöördumise Tomcati pordile 8080 *server.xml* konfiguratsioonifailis.
4. Loob *mod_jk* konfiguratsioonifail ja paigutab kataloogi */etc/apache2/mods-available* (vt kaasasaolev näidisfail: *jk.conf*), lisab vastava lingi kataloogi */etc/apache2/mods-enabled* (nt: *a2enmod jk*).
5. Lisaks aktiveerib järgnevad moodulid: *rewrite* (a2enmod *rewrite*), *ssl* (a2enmod *ssl*), *headers* (a2enmod *headers*) ja *proxy_http* (a2enmod *proxy_http* – automaatselt aktiveeritakse *proxy_http* jaoks vajalik *proxy* moodul).
6. Loob Apache konfiguratsioonifailis SSL ühendusega *virtualhost'i*.
7. Lubab ainult SSL ühendused: HTTP ühendused suunab HTTPS (443) porti (programmsete päringute korral 4443 porti)
8. Seadistab *mod_jk* mooduli Apache konfiguratsioonifailis
9. Paigaldab HTTPS serveri (genereeritud) sertifikaadid, Eesti ID-kaardi juursertifikaadid ja mobiil-ID turvasertifikaadi.
10. Paigaldab tühistusnimekirjade ja OCSP päringu sertifikaadid
11. Taaskäivitab Apache (*apache2ctl restart*).

Paigaldatavad konfiguratsiooni failid ja kataloogid:

```

/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 veebirakendus

Järgmisele küsimusele vastata „y“ juhul, kui soovitakse konfigurereida rahvusvahelise (EU) versioonina või „n“ Eesti versiooni jaoks (vt allpoolt vastavate konfiguratsiooniparameetrite seadistatud väärtusi):

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

Rahvusvahelise versiooni korral seadistatakse konfiguratsiooniparameetrid järgmiselt:

```

-----
languages = en

countries = GB

auth.IDCard=false

```

auth.certificate=true

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

Eesti versiooni korral seadistatakse konfiguratsiooniparameetrid järgmiselt:

languages = et

countries = EE

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

Järgmistele küsimustele vastates tuleb sisestada MISP2 andmebaasi parameetrid: serveri IP, port, andmebaasi nimi, andmebaasi kasutajanimi ja parool. Üldjuhul sobivad kõigile vaikimisiväärtused, va parool.

NB! Parameetrid peavad kooskõlas olema *xtee-misp2-postgresql* paketi paigaldamisel seadistatud parameetritega.

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 password for database user 'misp2':

Järgmisele küsimusele Vastata „y“, kui on soov sisse lülitada mobiil-ID autentimist serveris (eeldab ka vastava teenuselepingu olemasolu):

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

Vastates eelmisele küsimusele jaatavalt, tuleb sisestada ka mobiil-ID teenuse *UUID* ja nimetus (*relying party name*) (vt ka <https://github.com/SK-EID/MID/wiki/Environment-technical-parameters>):

Please provide your Mobile-ID relying party UUID:

Please provide your Mobile-ID relying party name:

Järgnevalt küsitakse e-posti saatmise seadistamiseks vajalikke parameetreid (SMTP serveri aadress, MISP2 poolt kasutatav meiliaadress)

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

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

Rahvusvahelise versiooni korral küsitakse kasutajalt veel X-tee versiooni 6 parameetreid: liikmeklasse ja X-tee instantse, mis mõlemad antakse komaga eraldatud loendina.

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]

Pärast konfiguratsiooni failide loomist palutakse luua administraatori konto, soovitav on jätta vaikimisi vastus „jah“. Vastasel juhul ei looda administraatori kontot, millega saab administraatori liidese kaudu portaali seadistama hakata.

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

Administraatori konto loomise järel küsitakse, millistelt IP-aadressitelt lubada juurdepääs administreerimisliidesele. Kui rakenduse administraator on sisse loginud üle SSH, pakutakse vaikimisi variandina vastava SSH sessiooni kliendipoolset IP-aadressi. Rakenduse administraator peaks tegema kindlaks, kas sellelt IP-aadressilt võib rakenduse administreerimisliidest kasutada. Juhul kui võib, saab valida vaikimisi vastuse. Vastasel juhul tuleks sisestada sobiv IP aadress. Sisestada võib ka tühikutega eraldatult mitu IP-aadressi. (X.X.X.X tähistab kasutaja SSH sessiooni kliendipoolset aadressi).

IP address from which 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 administrator interface: [default: X.X.X.X]

Administreerimisliidesele ligi pääsevaid IP-aadresse saab hiljem muuta Apache 2 konfiguratsioonifailist (vt peatükk 5.1).

Järgmisele küsimusele vastata „y“ juhul, kui soovitakse paigaldamisel seadistada HTTPS ühendus MISP2 rakenduse ja X-tee turvaserveri vahel:

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

Kui eeltoodud küsimusele vastati „y“, siis järgmiseks sammuks HTTPS seadistamisel on vaja eksportida turvaserverist turvaserveri sertifikaadifail sertifikaadifail *certs.tar.gz* (vt X-tee 6 turvaserveri kasutusjuhendis peatükki: „9 Communication with the Client Information Systems“) ja kopeerida see MISP2 serverisse kausta */usr/xtee/apache2/*. Sertifikaadifaili nimi X-tee v6 turvaserveri puhul on *certs.tar.gz*.

Paigaldusskript kontrollib eelnimetatud sertifikaadifaili olemasolu ning selle puudumisel palub selle kopeerida õigesse asukohta või katkestada HTTPS seadistamise alloleva küsimusega. Kui fail on kopeeritud MISP2 serverisse, tuleb vastata „y“ või katkestamise soovi korral vastata „n“. Viimasel juhul võib HTTPS seadistamise käivitada hiljem uuesti nagu kirjeldatud peatükis 4.3.

Please add 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]

Seepeale pakib paigaldusskript turvaserveri sertifikaadi arhiivist lahti ja lisab selle Java *cacerts* sertifikaadihoidlasse, võimaldades turvaserveriga HTTPS ühendust luua.

Seejärel tuleb sisestada avaliku ja salajase võtmete hoidla *keystore* jaoks parool, mis on vähemalt 6 sümbolit pikk. Sissetrukitud parooli sisestamisel ei kuvata.

Enter keystore password:

Paigaldusskript loob seepeale */usr/xtee/apache2/misp2keystore.jks* faili ja seadistab selle Tomcat serveri vaikimisi konfiguratsioonifailis */etc/default/tomcat8*.

Seejärel tekitab paigaldusskript MISP2 sertifikaadifaili ja kuvab selle asukoha kasutajale.

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

Sertifikaadifail sellest asukohast (antud näites */usr/xtee/app/cert.cer*) tuleb laadida turvaserverisse.

Samuti tuleb määrata turvaserveris infosüsteemi serveri ühendusviisiks HTTPS (vt täpsemalt turvaserveri kasutusjuhend).

Peale veebirakenduse paigaldamist võib asuda MISP2 portaali seadistama läbi administraatori veebiliidese nagu kirjeldatud käesoleva juhendi punktis 5.1.

Toodangukeskkonnas peaks paigaldama Apache HTTP serverile ka asutuse sertifikaadi HTTPS ühenduse kasutamiseks nagu kirjeldatud juhendi punktis 4.1.

4. Seadistamine

4.1. MISP2 Apache veebiserveri HTTPS sertifikaadi seadistamine

Algsel paigaldusel luuakse Apache HTTP serverile iseallkirjastatud sertifikaat, mis on toodangukeskkonnas soovitatav asendada korrektse CA poolt valjastatud sertifikaadiga.

Vaikimisi on Apachel kasutusel järgmised sertifikaadifailid:

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

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

Seega oleks soovitatav oma sertifikaadifailid nimetada samade nimedega ja asendada nendega algsed failid (kuna MISP2 uuendamisel kopeeritakse apache konfigifail üle, pole seal soovitatav muudatusi teha, sest need võivad kaduma minna). Oma sertifikaadifailile (*httpsd.cert*) tuleks lisada lõppu ka paigaldusel genereeritud DH-parameetrite faili (*/etc/apache2/ssl/dhparams.pem*) sisu.

4.2. MISP2 konfiguratsioonifail

MISP2 paketi paigaldusskript seadistab andmebaasiühenduse ja ka muud parameetrid konfiguratsioonifailis *config.cfg*. Peale paigaldamist võib mõningaid parameetreid vajadusel muuta konfiguratsioonifailis, mille asukoht on vaikimisi:

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

Järgnevalt on välja toodud mõningad parameetrid, mis küll paigaldamisel seadistatakse automaatselt, kuid mille muutmise vajadus võib ka hiljem tekkida rakenduse ümberseadistamisel.

Peale konfiguratsioonifaili muutmist on vaja muudatuste jõustumiseks ka tomcat alati taaskäivitada näiteks käsuga: `service tomcat8 restart`

Andmebaasiserveriga ühenduse loomise parameetrid:

```
-----  
# DB Info – andmebaasi serveri ja kasutaja parameetrid  
jdbc.driver=org.postgresql.Driver  
jdbc.url=jdbc:postgresql://IP/BAASINIMI  
jdbc.username=USERNAME  
jdbc.password=PASSWORD  
jdbc.databasePlatform=org.hibernate.dialect.PostgreSQLDialect  
-----
```

Keelte parameeter ja riikide parameeter:

```
-----  
#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  
-----
```

Serveri ID-kaardi parameetrid (serveripoolseks digiallkirjastamiseks ning krüpteerimiseks):

```
-----  
# 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  
-----
```

E-posti serveri parameetrid:

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

Mobiil-ID autentimise seadistamise parameetrid:

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

4.3. HTTPS ühenduse konfigureerimine MISP2 rakenduse ja X-tee turvaserveri vahel

HTTPS seadistamise sammud on järgmised.

1. Eksportida turvaserverist turvaserveri sertifikaadifail *certs.tar.gz* (vt X-tee 6 turvaserveri kasutusjuhendis peatükki: „9 Communication with the Client Information Systems“) ja kopeerida see MISP2 serverisse kausta */usr/xtee/apache2/*.

Sertifikaadifaili nimi X-tee v6 turvaserveri puhul on *certs.tar.gz*.

2. Käivitada MISP2 serveris käsurealt seadistusskript:

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

Nimetatud skripti käivitamisel kasutajale esitatud küsimused ja vastusevariandid on täpsemalt kommenteeritud käesoleva juhendi veebirakenduse paigaldamise peatükis.

Skript kontrollib kas turvaserveri sertifikaati sisaldav *certs.tar.gz* arhiiv on MISP2 serveri kaustas */usr/xtee/apache2/*, pakib selle lahti ja lisab arhiivis sisalduva sertifikaadi Java *cacerts* sertifikaadihoidlasse, genereerib sertifikaadi turvaserveriga sidepidamiseks, paigaldab saadud privaatvõtme ja sertifikaadi võtmehoidlasse *misp2keystore.jks*, määrab MISP2 serveris vajalikud süsteemsed parameetrid Tomcati konfiguratsioonifailis */etc/default/tomcat8* ning teeb Tomcatile restardi.

3. Määrata turvaserveris infosüsteemi serveri ühendusviisiks HTTPS ja laadida punktis 2 genereeritud sertifikaat (X-tee v6 puhul */usr/xtee/app/cert.cer*) turvaserverisse (vt täpsemaid juhiseid turvaserveri kasutusjuhendist).
4. MISP2 portaali administreerimise liideses muuta „Asutuse turvaserveri aadress“ ja „Päringute saatmise aadress“ väljades protokoll HTTP→HTTPS.
Kui turvaserveri IP või domeeninimi on *SEC_SERVER_IP*, siis asendada *http://SEC_SERVER_IP* → ***https:// SEC_SERVER_IP***

Juhul kui käesolevas peatükis kirjeldatud sammud tehakse uuesti läbi mingi erineva *certs.tar.gz* failiga, siis eelmine turvaserveri sertifikaat asendatakse uuega Java sertifikaadihoidlas */etc/ssl/certs/java/cacerts* aliase all *xroad_security_server*. Juhul kui soovitakse jätta eelmine turvaserveri sertifikaat alles ja lisada juurde uus sertifikaat, tuleks seadistusksriptile anda ette erinev alias argumendiga *--alias*, näiteks:

```
/usr/xtee/app/create_https_certs_security_server.sh --alias sec_server_2
```

Muus osas jäävad ülalpool toodud juhised samaks.

Et näha muid ülejäänud argumente, mida skriptile saab ette anda, tuleks see käivitada argumendiga *--help*.

HTTPS sertifikaati on võimalik lisada ka nii nagu on kirjeldatud peatükis *HTTPS sertifikaadi lisamine*.

4.4. Mobiil-ID seadistamine

4.4.1. Teenuse parameetrid

Seadistada konfiguratsioonifailis õige väärtusega parameetrid *mobileID.rest.hostUrl*, *mobileID.rest.relyingPartyUUID* ja *mobileID.rest.relyingPartyName*. Konkreetsete parameetrite väärtused väljastab asutusele lepingu olemasolul SK ID Solutions (vt ka <https://www.skidsolutions.eu/teenused/mobiil-id/tehniline-lisainfo-mid-rest-api>).

4.5. Muud seadistused

4.5.1. Java VM seadistamine

Vajadusel võibmuuta java süsteemseid parameetreid failis */etc/default/tomcat8*.

Mälukasutuse parameetrid seadistatakse paigaldusskripti poolt, kuid vajadusel peab antud väärtusi suurendama, näiteks:

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

4.5.2. Logimise seadistamine

Logimise seadistamine toimub failis

/var/lib/tomcat8/webapps/misp2/WEB-INF/classes/log4j2.xml

Rakenduse poolt enamkasutatavamad parameetrid seal failis on *<Root level="info">*,

<Logger name="org.hibernate" level="info" additivity="false"> ja

<Logger name="ee.aktors.misp2" level="info" additivity="false">.

Kui on soovi näha rohkem infot, võiks nende tasemeks panna *level=„debug“*.

Näiteks

```
<Root level="info">
```

asemel võid kasutada

```
<Root level="debug">
```

4.5.3. HTTPS sertifikaadi lisamine

HTTPS sertifikaate on võimalik usaldatud sertifikaatide hoidlasse lisada *keytool* käsuga.

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

Et muutused veebirakendusse jõuaks, tuleb Tomcat veebiserver taaskäivitada.

```
service tomcat8 restart
```

4.6. MISP2 administraatori kontode haldamine käsurealt

MISP2 rakenduse administraatorite kontode haldamiseks käsurealt on tööriist mis käivitatakse käsurealt järgnevalt:

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

Vaikimisi kuvatakse olemasolevate administraatori kontode loetelu.

Administraatori konto lisamiseks lisada käsureale parameeter „-add“:

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

Administraatori konto eemaldamiseks lisada käsureale parameeter „-delete“:

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

4.7. Orbeon inspektori sisselülitamine

Inspektor (*Orbeon inspector*) on Orbeoni moodul, mis võimaldab vaadata teenuste saadetud ja vastuvõetud X-tee sõnumeid ning muid rakenduse-siseseid andmeid.

Orbeon inspektori saab MISP2-s sisse lülitada, muutes faili

/var/lib/tomcat8/webapps/orbeon/WEB-INF/resources/config/properties-local.xml parameetri *oxf.epilogue.xforms.inspector* väärtust.

Vaikimisi MISP2 paigalduse järel on selle parameetri väärtuseks *false*.

Inspektori näitamiseks tuleks parameetri väärtuseks anda *true*:

```
<property as="xs:boolean" name="oxf.epilogue.xforms.inspector" value="true"/>.
```

Seejärel tuleks fail salvestada ning inspektor peaks ilmuma liidesesse. Restarti Tomcat serverile pole vaja.

5. MISP2 Administreerimise liides

Administreerimise liidesele minemiseks sisestage portaali URLi lõppu „/admin“. Näiteks `https://<portaali_aadress>/misp2/admin/`.

5.1. Apache veebiserveri konfiguratsiooni täiendamine

Kui MISP2 veebirakenduse paigaldamise käigus loodi administraatori konto ning sisestati administreerimisliidese ligipääsuga IP-aadressid, sisestas paigalduskript need automaatselt Apache konfiguratsioonifaili ja käesolevas peatükis kirjeldatud samme pole tarvis uuesti läbi teha.

Juhul kui administreerimisliidesele juurdepääsu omavaid IP-aadresse soovitakse hiljem lisada või muuta, saab seda teha Apache konfiguratsioonifailist:

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

Otsida failist üles read:

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

```
    Order deny,allow
```

```
    Deny from all
```

```
    Allow from 127.0.0.1
```

```
</Location>  
-----
```

Lisada oma arvuti aadress `<Location>` elemendi sisu viimase rea lõppu, nt:

```
-----  
Allow from 127.0.0.1 192.168.215.233  
-----
```

Käivitada uuesti veebiserver:

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

5.2. Portaali haldamine

Antud peatükk kirjeldab, kuidas MISP2 veebirakenduses portaali hallatakse.

5.2.1. Portaali loomine

Portaali loomiseks sisenege administreerimisliidessesse. Teile kuvatakse uue portaali loomise jaoks vorm väljadega:

- **Portaali nimi *** - Portaali nimi
- **Portaali lühinimi *** – portaali lühinimi, mida kasutatakse portaali identifitseerimiseks rakenduses ja tegevuste ajaloo salvestamisel. Portaali lühinimi peab olema rakenduses piires unikaalne.

- **Asutuse nimi*** ja **registrikood*** on portaaliga seotud peasutuse nimi ja registrikood. Peasutuse registrikood lisatakse igale päringule. Kui peasutuse registrikood vastab rakenduses juba olemasolevale asutusele, siis seotakse portaal olemasoleva asutusega ja olemasolev asutuse nimi kirjutatakse viimati sisestatud nimega üle. X-tee versioonis 6 kasutatakse asutuse registrikoodi ühtlasi X-tee päringu päises liikmekoodina (*xrd:client/iden:memberCode*).



- **Portaali tüüp** - näitab, mis tüüpi portaal on. Portaali tüüpidest saate lugeda lähemalt kasutusjuhendi peatükis 1. Võimalikud valikud on
- **X-tee protokollide versioon** määrab, milline on portaali metateenuste ja kasutaja päringute sõnumiformaat, mida X-tee turvaserveriga suhtlemiseks kasutatakse. Kasutaja saab valida järgnevate protokollide hulgast: 3.1 (X-tee versioon 5) ja 4.0 (X-tee versioon 6). X-tee versiooni 3.1 on võimalik kogu rakenduse raames globaalselt asendada protokolliga 3.0, muutes MISP2 konfiguratsioonifailis parameetrit *xrd.v5.namespace* järgnevalt: *xrd.v5.namespace=http://x-rd.net/xsd/xroad.xsd*
X-tee versioon 5 portaalil on toetatud ka protokollide 2.0 (X-tee versioon 4) teenused.
- **X-tee liikmeklass** – X-tee versiooni 6 konfiguratsiooniparameeter, mis näitab X-tee kliendi üldist kategooriat, kas tegu on riigiasutusega (GOV), eraettevõttega (COM) või mingit muud tüüpi asutusega. Valik tuleb nähtavale, kui X-tee protokolliks on eelnevalt valitud 4.0. Parameeter kirjutatakse X-tee päringute päistes väljale *xrd:client/iden:memberClass*.
- **X-tee alamsüsteemi kood** – X-tee versiooni 6 konfiguratsiooniparameeter, mis võimaldab eristada sama asutuse erinevaid X-tee klient- ja serverrakendusi. Valik tuleb nähtavale, kui X-tee protokolliks on eelnevalt valitud 4.0. Antud parameeter kirjutatakse X-tee päringute päistes väljale *xrd:client/iden:subsystemCode*.
- **Asutuse turvaserveri aadress*** – teiepoolse turvaserveri aadress
- **X-tee kliendi instants** – X-tee versiooni 6 konfiguratsiooniparameeter, mis defineerib kasutatava X-tee keskkonna, näiteks *ee-dev* ja *EE* märgivad vastavalt Eesti X-tee arenduskeskkonda ja toodangukeskkonda. Valikut näidatakse, kui X-tee protokolliks on valitud 4.0. Parameetri väärtus kirjutatakse X-tee päringute päistes väljale *xrd:client/iden:xRoadInstance*.

- **X-tee instantsid teenustele** – siin saab märkida tabelis etteantud nimekirjast, millised X-tee instantsid on kasutusel teenuste värskendamisel portaali haldurile. Selle valiku baasil saab haldur määrata, milliste X-tee instantside teenustega ta tegeleb halduri liideses.

Tabelis etteantud X-tee instantside nimekiri võetakse vaikumisi portaali konfiguratsioonifailist.

Nupuga „Lae instantsid turvaserverist“ laetakse tabelisse kõik födereeritud X-tee instantsid X-tee turvaserverist ja seejärel saab need kasutusele võtta portaalis.

Nupuga „Lae vaikumisi instantsid“ laetakse instantside nimekiri uuesti konfiguratsioonifailist.

Teenuse instants määrab ära X-tee päringute päises välja: *xrd:service/iden:xRoadInstance*.

- **Päringute saatmise aadress*** – serveri aadress, millest läbi käivad kõik päringud
- **Arendaja vaade** – valik „Sees“ paneb teenuste halduri või portaali haldurile vaates „Teenused“ juurde nupu „Lisa andmekogu“ (andmekogu käsitsi lisamine) ja andmekogu alavaates lisab nupu „WSDL-st“, mis võimaldab WSDList teenuste nimekirja uuendada.
- **Saada auditlogi turvaserverisse** – määrab, kas auditlogi salvestamisel tehakse *logOnly* päring turvaserverile, et MISp2 rakenduse auditlogisse kantud tegevused ka turvaserveri logides kajastuks. X-tee versiooni 5 puhul tehakse päringud turvaserveri metateenusele *xrd.logOnly*. X-tee versioonis 6 turvaserverist on aga selle metateenuse tugi eemaldatud, mistõttu X-tee versiooni 6 portaalis tuleb täita veel kohaliku andmekogu *logOnly* teenuse andmed: „teenuse 'logOnly' liikmeklass“, „teenuse 'logOnly' liikmekood“ ja „teenuse 'logOnly' alamüsteemi kood“. Vastavad väljad tulevad nähtavale administreerimisliideses portaali muutmise vormil vaid juhul, kui on valitud X-tee versioon 6. Teenuse *logOnly.v1* käivitamiseks on MISp2-le loodud andmekogu lisamoodul nimetusega *misp2-soap-service-v6.war*, mida saab haldur soovi korral oma keskkonnas käivitada. Seda kirjeldatakse täpsemalt lisamoodulite paigaldusjuhendis.
- **Teemad kasutusel** – kui see on märgitud, siis grupeeritakse kasutajatele teenused vastavalt teemadele. Teemade haldusega tegeleb portaali haldur. Teemade haldusest tuleb juttu veidi hiljem vastavas peatükis. Kui teemad ei ole kasutusel, grupeeritakse teenused tavapäraselt andmekogude järgi.
- **Toimiku väli kasutusel teenuse sisendis** – X-tee versioon 5 portaalis lisatakse toimiku päiseväli sõnumi sisendis.

Kui kõik vajalikud andmed on sisestatud, tuleb teil nende kinnitamiseks vajutada nuppu „Salvesta portaali konfiguratsioonid“, mispeale kirjutatakse portaali andmed andmebaasi.

Universaalse portaali korral on portaali haldamine mõnevõrra teistsugune.

Universaalse portaali korral peate sisestama lisaks tavapärastele väljadele väljad:

- **Üksuse registreerimine lubatud** – märkeruut, tähistamaks seda, kas kasutajate poolt uute üksuste registreerimine on rakenduses lubatud. Juhul kui see on märgitud, peavad olema täidetud järgnevad **-ga tähistatud väljad.
- **Esindusõiguse kontrollpäringu nimi**** - metapäringu nimi üksuse esindusõiguste kontrollimiseks. X-tee versiooniga 4 ja 5 portaalides sisestatakse teenuse nimi tervikuna tekstiväljale. X-tee versiooni 6 portaali korral antakse kasutajale ette valik konfiguratsioonifailis defineeritud teenustest. Universaalse portaali korral defineeritakse teenused failis *uniportal-conf.cfg*, juriidilise isiku portaali korral defineeritakse esindusõiguse kontrollpäringu teenused aga failis *orgportal-conf.cfg*.
- **Kehtivuse kontrollpäringu nimi**** – päringu nimi üksuse kehtivuse kontrollimiseks. X-tee versiooniga 4 ja 5 portaalides sisestatakse teenuse nimi tervikuna tekstiväljale. X-tee versiooni 6 portaali korral antakse kasutajale ette valik *uniportal-conf.cfg* konfiguratsioonifailis defineeritud teenustest.
- **Kontrollpäringu kehtivusaeg (tundides)**** – ajavahemik, mille möödudes on vaja teha uus kontrollpäring, kuna vana kaotab kehtivuse.
- **Kontrollpäringu maksimaalne kehtivusaeg (tundides)**** - lubatud maksimaalne aeg, mille jooksul saab kasutaja teha asutuse õigustes päringuid juhul kui kontrollpäring ei vasta.
- **Pääsuõiguste halduriga** – kui see on valitud, siis rollis „Esindusõigustega kasutaja“ ilmub menüüvalik „Pääsuõiguste haldurid“ juhul kui antud rolli pääseti läbi „Registreerija“ rolli, kui pääseti läbi „Portaali haldur“-i rolli siis on menüüvalik igal juhul olemas. Sellest menüüpunktist saab „Esindusõigustega kasutaja“ määrata uue üksuse registreerimise käigus pääsuõiguste haldureid ja päringuõigustega kasutajaid. Vastasel korral haldureid määrata ei saa. Kuna juriidilise isiku portaal on universaalse portaali alamtüüp, siis on ka seal see väli näha. Juriidilise isiku portaali juures peab arvestama sellega, et see väärtus kehtib ainult ainuesindusõigusega asutuste juures.
- **Portaali üksus on X-tee asutus** –kui on valitud, siis sõnumi päisesse pannakse aktiivse üksuse kood väljale „consumer“(asutus).Kui ei ole valitud, siis sõnumi päisesse pannakse peasutusekood väljale „consumer“(asutus)ja aktiivse üksuse kood väljale „unit“ (allasutus).

5.2.2. Portaali muutmine

Portaali muutmiseks peate sisenema administraatori liidesesse, kus kuvatakse teile registreeritud portaal. Muudatuste salvestamiseks vajutage nuppu „Salvesta portaali konfiguratsioonid“. Portaali tüüpi muuta ei saa, selle jaoks tuleb olemasolev portaal kustutada ja lisada uus. Samuti ei ole lubatud muuta portaaliga seotud peasutuse registrikoodi.

5.2.3. Portaali kustutamine

Portaali kustutamine käib administreerimise liidese kaudu, kasutades selleks „Kustuta portaal“ nuppu portaali haldamise vormil, millele vajutades kustutatakse portaal ja temaga seotud objektid rakendusest.

5.2.4. Portaali halduri lisamine

Portaali halduri lisamiseks vajutage portaali konfiguratsiooni vormil nuppu „Lisan uue halduri“. Selle tulemusena suunatakse teid edasi haldurite lehele, kus on võimalik kasutajaid otsida olemasolevatest kasutajakontodest ning lisada täiesti uusi portaali haldureid. Portaali halduri lisamiseks peab olema portaal salvestatud.

Uue halduri lisamisel on vaja täita kohustuslikud väljad: isikukood ja perekonnanimi. E-post ja ametinimetus seotakse peaaasutusega ja ei laiene hiljem lisatud üksustele.

Kui kasutaja ankeet on täidetud, vajutage nuppu „Lisa halduriks“, mille tagajärjel antakse kasutajale portaali halduri ja tavakasutaja roll peaaasutuses. Nupp „Kustuta kasutaja“ kustutab kasutaja ja kõik tema seosed asutuste ja gruppidega.

Kasutaja otsingut kasutades otsitakse vastavalt sisestatud parameetritele süsteemist kõikide kasutajate hulgast sobivad ja kuvatakse need nimekirjana:

Vajutades kasutaja nimel, avatakse kasutaja muutmise vorm, mis on täidetud valitud kasutaja andmetega, kusjuures e-post ja ametinimetus on seotud peaaasutusega.

Vajutades nuppu „Lisa halduriks“ lisatakse kasutaja, mille real nuppu vajutati, koheselt portaali halduriks.

5.2.5. Portaali halduri eemaldamine

Portaali halduri eemaldamine käib portaali konfigureerimise vormil. Sellel vormil on nimekiri olemasolevatest halduritest.

Vajutades halduri real ristiga tähistatud ikoonile, võetakse kasutajalt ära portaali halduri roll.

5.3. Globaalsete XSL-ide haldamine

Administraatori õigustesse kuulub lisaks portaali haldamisele ka portaalis kasutatavate globaalsete XSL-ide lisamine ja haldamine. Globaalsed XSL-id on XSL-ild mis rakendatakse päringutele kõige viimasena vastavalt prioriteetidele. Globaalsete XSL-ide haldamine käib samamoodi kui portaali siseste XSL-ide haldamine. (vt kasutusjuhendist „teenuste halduri“ rolli alt).