|  |
| --- |
| X-Road 6  Central Server User Guide  2.3 |
|  |

Version history

|  |  |  |
| --- | --- | --- |
| Date | Version | Description |
| 28.08.2014 | 0.1 | Initial version |
| 28.09.2014 | 0.2 | Translation to English |
| 09.10.2014 | 0.3 | Minor updates and corrections. Security Categories removed. |
| 09.10.2014 | 0.4 | Add service CA OCSP responder changed to Add top CA OCSP responder |
| 14.10.2014 | 0.5 | Title page, header, footer modified |
| 28.11.2014 | 0.6 | Logback information added (Chapter 17). Introduction added (Chapter 1). Security Officer user role added (Section 2.1). System Settings added (Chapter 4). Configuration Management added (Chapter 5). Database Management Chapter deleted. |
| 1.12.2014 | 1.0 | Minor corrections |
| 23.01.2015 | 1.1 | License information. Certification services management and time stamping services management chapters updated (Chapters 11 and 12). |
| 30.04.2015 | 1.2 | “sdsb” changed to “xroad” |
| 30.06.2015 | 1.3 | Minor corrections done |
| 3.07.2015 | 1.4 | Audit Log chapter added (Chapter 14) |
| 31.08.2015 | 1.5 | Information about high availability added (Chapter 3) |
| 15.09.2015 | 1.6 | Reference to the audit log events added |
| 17.09.2015 | 1.7 | Corrections related to high availability added |
| 18.09.2015 | 1.8 | Minor corrections done |
| 21.09.2015 | 1.9 | References fixed |
| 22.10.2015 | 1.10 | Corrections in Chapter 17 |
| 04.11.2015 | 1.11 | Updates related to backup and restore (Chapter 13) |
| 30.11.2015 | 2.0 | Management service provider configuration updated (Section 4.2); management requests system updated (Chapter 6); key label added to configuration signing key generation (Section 5.4.1); section about adding a subsystem to an X-Road member added (Section 7.3); only subsystems can be registered as security server clients or be members of global groups; certification service settings updated (11.1). Editorial changes made. |
| 17.12.2015 | 2.1 | Added user instructions for monitoring. |
| 14.4.2016 | 2.2 | Added chapter for additional configuration options. |
| 5.9.2016 | 2.3 | Added instructions for configuring OCSP fetch interval. |

**TABLE OF CONTENTS**

[1.Introduction 7](#__RefHeading___Toc8301_570983057)

[1.1.Target Audience 7](#__RefHeading___Toc8303_570983057)

[1.2.References 7](#__RefHeading___Toc8305_570983057)

[2.User Management 8](#__RefHeading___Toc8307_570983057)

[2.1.User Roles 8](#__RefHeading___Toc8309_570983057)

[2.2.Managing the Users 8](#__RefHeading___Toc8311_570983057)

[3.Standalone and High-Availability Systems 9](#__RefHeading___Toc8313_570983057)

[3.1.Detecting the Type of Deployment in the User Interface 9](#__RefHeading___Toc8315_570983057)

[3.2.Checking the Status of the Nodes of the Cluster 9](#__RefHeading___Toc8317_570983057)

[4.System Settings 10](#__RefHeading___Toc8319_570983057)

[4.1.Managing the Member Classes 10](#__RefHeading___Toc8321_570983057)

[4.2.Configuring the Management Service Provider 10](#__RefHeading___Toc8323_570983057)

[4.2.1.Appointing the Management Service Provider 10](#__RefHeading___Toc8325_570983057)

[4.2.2.Registering the Management Service Provider as a Security Server Client 11](#__RefHeading___Toc8327_570983057)

[4.2.3.Configuring the Management Services in the Management Services’ Security Server 11](#__RefHeading___Toc8329_570983057)

[4.3.Configuring the Central Server Address 12](#__RefHeading___Toc8331_570983057)

[4.3.1.Notes on HA Setup 12](#__RefHeading___Toc8333_570983057)

[4.3.2.Changing the Central Server Address 12](#__RefHeading___Toc8335_570983057)

[5.Configuration Management 14](#__RefHeading___Toc8337_570983057)

[5.1.Viewing the Configuration Settings 14](#__RefHeading___Toc8339_570983057)

[5.2.Downloading the Configuration Anchor 14](#__RefHeading___Toc8341_570983057)

[5.3.Re-Creating the Configuration Anchor 14](#__RefHeading___Toc8343_570983057)

[5.4.Changing the Configuration Signing Keys 15](#__RefHeading___Toc8345_570983057)

[5.4.1.Generating a Configuration Signing Key 16](#__RefHeading___Toc8347_570983057)

[5.4.2.Activating a Configuration Signing Key 16](#__RefHeading___Toc8349_570983057)

[5.4.3.Deleting a Configuration Signing Key 17](#__RefHeading___Toc8351_570983057)

[5.5.Viewing the Contents of a Configuration Part 17](#__RefHeading___Toc8353_570983057)

[5.6.Uploading a Trusted Anchor 17](#__RefHeading___Toc8355_570983057)

[5.7.Viewing the Contents of a Trusted Anchor 17](#__RefHeading___Toc8357_570983057)

[5.8.Deleting a Trusted Anchor 18](#__RefHeading___Toc8359_570983057)

[6.The Management Requests System 19](#__RefHeading___Toc8361_570983057)

[6.1.Registration Requests 19](#__RefHeading___Toc8363_570983057)

[6.1.1.State Machine Model for Registration Requests 19](#__RefHeading___Toc8365_570983057)

[6.2.Deletion Requests 20](#__RefHeading___Toc8367_570983057)

[6.3.Viewing the Management Request Details 20](#__RefHeading___Toc8369_570983057)

[7.Managing the X-Road Members 22](#__RefHeading___Toc8371_570983057)

[7.1.Adding a Member 22](#__RefHeading___Toc8373_570983057)

[7.2.Viewing the Member Details 22](#__RefHeading___Toc8375_570983057)

[7.3.Adding a Subsystem to an X-Road Member 22](#__RefHeading___Toc8377_570983057)

[7.4.Registering a Member's Security Server 23](#__RefHeading___Toc8379_570983057)

[7.5.Registering a Client to a Security Server 24](#__RefHeading___Toc8381_570983057)

[7.6.Removing a Client from a Security Server 26](#__RefHeading___Toc8383_570983057)

[7.7.Changing the Global Group Membership of an X-Road Member’s Subsystem 27](#__RefHeading___Toc8385_570983057)

[7.8.Deleting a Subsystem 27](#__RefHeading___Toc8387_570983057)

[7.9.Deleting an X-Road Member 27](#__RefHeading___Toc8389_570983057)

[8.Managing the Security Servers 29](#__RefHeading___Toc8391_570983057)

[8.1.Viewing the Security Server Details 29](#__RefHeading___Toc8393_570983057)

[8.2.Changing the Security Server Address 29](#__RefHeading___Toc8395_570983057)

[8.3.Registering a Security Server's Authentication Certificate 30](#__RefHeading___Toc8397_570983057)

[8.4.Deleting a Security Server's Authentication Certificate 31](#__RefHeading___Toc8399_570983057)

[8.5.Deleting a Security Server 31](#__RefHeading___Toc8401_570983057)

[9.Managing the Central Services 33](#__RefHeading___Toc8403_570983057)

[9.1.Adding a Central Service 33](#__RefHeading___Toc8405_570983057)

[9.2.Changing the Service Implementing a Central Service 33](#__RefHeading___Toc8407_570983057)

[9.3.Deleting a Central Service 33](#__RefHeading___Toc8409_570983057)

[10.Managing the Global Groups 34](#__RefHeading___Toc8411_570983057)

[10.1.Adding a Global Group 34](#__RefHeading___Toc8413_570983057)

[10.2.Viewing the Global Group Details 34](#__RefHeading___Toc8415_570983057)

[10.3.Changing the Description of a Global Group 34](#__RefHeading___Toc8417_570983057)

[10.4.Changing the Members of a Global Group 34](#__RefHeading___Toc8419_570983057)

[10.5.Deleting a Global Group 35](#__RefHeading___Toc8421_570983057)

[11.Managing the Approved Certification Services 36](#__RefHeading___Toc8423_570983057)

[11.1.Adding an Approved Certification Service 36](#__RefHeading___Toc8425_570983057)

[11.2.Changing an Approved Certification Service 36](#__RefHeading___Toc8427_570983057)

[11.3.Deleting an Approved Certification Service 37](#__RefHeading___Toc8429_570983057)

[12.Managing the Approved Timestamping Services 38](#__RefHeading___Toc8431_570983057)

[12.1.Adding an Approved Timestamping Service 38](#__RefHeading___Toc8433_570983057)

[12.2.Changing the URL of an Approved Timestamping Service 38](#__RefHeading___Toc8435_570983057)

[12.3.Deleting an Approved Timestamping Service 38](#__RefHeading___Toc8437_570983057)

[13.Configuration Backup and Restore 39](#__RefHeading___Toc8439_570983057)

[13.1.Backing Up the System Configuration 39](#__RefHeading___Toc8441_570983057)

[13.2.Restoring the System Configuration in the User Interface 39](#__RefHeading___Toc8443_570983057)

[13.3.Restoring the Configuration from the Command Line 39](#__RefHeading___Toc8445_570983057)

[13.4.Downloading, Uploading and Deleting Configuration Backup Files 40](#__RefHeading___Toc8447_570983057)

[14.Audit Log 41](#__RefHeading___Toc8449_570983057)

[14.1.Changing the Configuration of the Audit Log 41](#__RefHeading___Toc8451_570983057)

[14.2.Archiving the Audit Log 42](#__RefHeading___Toc8453_570983057)

[15.Monitoring 43](#__RefHeading___Toc8455_570983057)

[16.Additional configuration options 44](#__RefHeading___Toc8457_570983057)

[16.1 Verify next update 44](#__RefHeading___Toc8459_570983057)

[16.2 OCSP fetch interval 44](#__RefHeading___Toc8461_570983057)

[17.Logs and System Services 45](#__RefHeading___Toc8463_570983057)

# Introduction

## Target Audience

The intended audience of this User Guide are X-Road central server administrators who are responsible for everyday management of the X-Road central server.

Instructions for the installation and initial configuration of the central server can be found in the Central Server Installation Guide [CSI]. Instructions for installing the central server in a cluster for achieving high availability can be found in the Central Server High Availability Installation Guide [IG-CSHA].

## References

1. [CSI] Cybernetica AS. X-Road 6. Central Server Installation Guide. Document ID: IG-CS
2. [IG-CSHA] Cybernetica AS. X-Road 6. Central Server High Availability Installation Guide. Document ID: IG-CSHA
3. [JSON] Introducing JSON, <http://json.org/>
4. [SPEC-AL] Cybernetica AS. X-Road: Audit log events. Document ID: SPEC-AL
5. [SSI] Cybernetica AS. X-Road 6. Security Server Installation Guide. Document ID: IG-SS
6. [IG-CS] Cybernetica AS. X-Road 6. Central Server Installation Guide. Document ID: IG-CS
7. [UC-GCONF] Cybernetica AS. X-Road 6: Use Case Model for Global Configuration Distribution. Document ID: UC-GCONF
8. [RFC-OCSP] Online Certificate Status Protocol – OCSP, <https://tools.ietf.org/html/rfc6960>

# User Management

## User Roles

The central server supports the following user roles:

* **Registration Officer** (xroad-registration-officer) is responsible for handling the information about X-Road members.
* **System Administrator** (xroad-system-administrator) is responsible for the installation, configuration, and maintenance of the central server.
* **Security Officer** (xroad-security-officer) is responsible for the application of the security policy and security requirements.

One user can have multiple roles, and multiple users can fulfill the same role. Each role has a corresponding system group, created upon the installation of the system. The system user names are used for logging in to the user interface of the central server.

The document indicates in sections similar to the following example, which user role is required for performing a particular action in the user interface. For example

**Access rights:** System Administrator

**Caution:** If the logged-in user does not have a permission to carry out a task, the button that initiates the action is hidden (and neither is it possible to run the task using its corresponding keyboard combinations or mouse actions). Only the permitted information and actions are visible and available to the user.

## Managing the Users

During the installation, a super user equipped with all the roles is created. You can create additional users that have restricted rights. User management is carried out in root user's permissions using the command line.

To add a new user, issue the command:

adduser username

To grant permissions to the user you created, add it to the corresponding system groups, for example:

adduser username xroad-registration-officer

adduser username xroad-system-administrator

adduser username xroad-security-officer

To remove a user’s permission, remove the user from the corresponding system group, for example:

deluser username xroad-registration-officer

To remove a user, enter:

deluser username

# Standalone and High-Availability Systems

The central server can be installed and configured in two ways:

* ***A standalone*** server
* A cluster of independent central servers (*nodes*) providing ***high availability*** (HA). In an HA setup, the system continues to function if one or more of the nodes are experiencing problems or are down for maintenance.

In the case of an HA setup, the changes to the databases of each central server are replicated to the other nodes. While most of the system settings described in this document apply to the whole cluster, some have a meaning that is local to each node, although the database records are replicated. In addition, all the configuration signing keys are local to each node and must be generated separately. This distinction will be stated explicitly throughout this document, where necessary.

In an HA setup, if the system is configured using different nodes in parallel, the effect will be similar to several people updating the configuration of a standalone server at the same time.

## Detecting the Type of Deployment in the User Interface

In order to detect the type of deployment and the name of the node in the cluster in the case of HA setup, the logged-in user should check the instance identifier displayed in the left upper corner of the user interface. In the case of an HA setup, the name of the node is displayed to the right of the instance identifier in parentheses.

## Checking the Status of the Nodes of the Cluster

In order to check the status of the nodes in an HA setup, the following script can be used on the command line:

/usr/share/xroad/scripts/check\_ha\_cluster\_status.py

# System Settings

## Managing the Member Classes

**Access rights:** Security Officer

To add a member class, follow these steps.

1. On the **Management** menu, select **System Settings**.
2. Locate the **Member Classes** section and click **Add**.
3. In the window that opens, enter the member class code and description. Click **OK**.

To edit the description of a member class, follow these steps.

1. On the **Management** menu, select **System Settings**.
2. Locate the **Member Classes** section, select a member class and click **Edit**.
3. In the window that opens, enter the member class description and click **OK**.

To delete a member class, follow these steps.

1. On the **Management** menu, select **System Settings**.
2. Locate the **Member Classes** section, select a member class and click **Delete**.

Only the member classes that are used by none of the X-Road members can be deleted.

## Configuring the Management Service Provider

The central server provides management services to the security servers that are part of the (local) X-Road infrastructure (see Chapter 6).

A subsystem of an X-Road member acting as a service provider for the management services must be appointed in the central server (see 4.2.1), registered as a client of the management services’ security server (see 4.2.2) and configured to provide the services in the management services’ security server (see 4.2.3).

The management services’ security server must be installed and registered in the central server before the management service provider can be registered as a client of the security server and the management services can be configured (see [SSI]).

### Appointing the Management Service Provider

**Access rights:** Security Officer

To appoint the management service provider in the central server, follow these steps.

1. On the **Management** menu, select **System Settings**.
2. Locate the **Management Services** section and click **Edit**.
3. In the window that opens, find the subsystem of an X-Road member to be appointed as the management service provider and click **OK**.

### Registering the Management Service Provider as a Security Server Client

**Access rights:** Security Officer

The management service provider can be registered as a security server client as described in this section only if the management service provider is not registered as a client of any security servers. In case the management service provider is already a client of a security server then the identifier of the security server is displayed instead of the **Register** button.

To register the appointed management service provider as a security server client to the management services’ security server, follow these steps.

1. On the **Management** menu, select **System Settings**.
2. Locate the **Management Services** section and click **Register**.
3. Locate the "Security Server Information" section on the registration request form, click **Search** and select the security server that will be used as the management services’ security server.
4. Click **Submit** to submit the registration request.

On successful registration the identifier of the management services’ security server is displayed instead of the **Register** button.

### Configuring the Management Services in the Management Services’ Security Server

**Access rights: Security server’s Service Administrator**

The data necessary for configuring the management services in the security server can be found at the central server **Management** -> **System Settings** -> **Management Services** section.

To configure management services in the management services’ security server, follow these steps.

1. On the **Configuration** menu of the security server, select **Security Server Clients**, select the client who will provide the management services and click the **Services** icon on that row.
2. Click **Add WSDL**, enter the management services WSDL address in the window that opens and click **OK**.
3. Expand the WSDL, by clicking the **+** icon, select a service and click **Edit**.
4. In the window that opens, enter the management services address. If necessary, edit other service parameters. Check the **Apply to All in WSDL** checkbox and click **OK**. Ensure that the parameters of all the management services have changed.
5. Activate the management service’s WSDL by selecting the row of the WSDL and clicking **Enable**.
6. Navigate to the **Service Clients** tab.
7. Click **Add** and search for the global group **security-server-owners**. Select the group and click **Next**.
8. In the window that opens, click **Add All to ACL** to add all management services (authCertDeletion, clientDeletion, clientReg) to the security-server-owners group’s access rights list.

## Configuring the Central Server Address

**Access rights:** Security Officer

In the System Settings view, the central server's public DNS name or its external IP address is displayed. This address is used by the security servers to access the services provided by the central server (configuration download, management services).

**ATTENTION!** When the central server address is changed,

* the management services address in the management services’ security server needs to be reconfigured,
* the internal configuration anchor need to be redistributed to the security server administrators and
* the external configuration anchor needs to be redistributed to the federation partners.

The services provided by the central server must be available from both the new and old address, until all servers using the services have uploaded the configuration anchor containing the new address.

### Notes on HA Setup

In an HA setup, the address of the central server is local to the node that is being configured.

In an HA setup, internal and external configuration anchors contain information about each central server that is part of the cluster. If the address of one of the servers is changed, configuration anchors will be re-generated automatically on all the nodes.

### Changing the Central Server Address

To change the central server address, follow these steps.

1. In the **Management** menu, select **System Settings**.
2. Locate the **System Parameters** section and click **Edit**.
3. Enter the central server’s address and click **OK**.  
   When the address is changed, the system:

* changes the management services WSDL address,
* changes the management services address,
* changes the configuration source addresses,
* generates new configuration anchors for the internal and external configuration sources.

1. After the central server address is changed, act as follows.

* Download the internal configuration source anchor and distribute the anchor along with the anchor’s hash value to the security server administrators of the local X-Road infrastructure.
* In case of federated X-Road systems, download the external configuration source anchor and distribute the anchor along with the anchor’s hash value to the federation partners.
* Reconfigure the management services addresses in the management service security server.

# Configuration Management

## Viewing the Configuration Settings

**Access rights:** Security Officer**,** System Administrator

The configuration management view consists of three sections.

* **The Internal Configuration View**. The internal configuration is distributed by the central server to the security servers of the local X-Road infrastructure. The information needed to download and verify the internal configuration is included in the internal configuration anchor, which must be distributed to the security server administrators and uploaded to the security servers. Along with the internal configuration anchor, the anchor file hash value must be distributed. The hash value is used by the security server administrators to verify the integrity of the anchor file.
* **The External Configuration View**. The external configuration is distributed by the central server to the federation partners (either to the security servers directly or through a configuration proxy). The information needed to download and verify the external configuration is included in the external configuration anchor, which must be distributed to the federation partner’s central server (or configuration proxy) administrators and uploaded to the central server (or configuration proxy). Along with the external configuration anchor, the anchor file hash value must be distributed. The hash value is used by the federation partners to verify the integrity of the anchor file.
* **The Trusted Anchors View**. A trusted anchor is the configuration anchor of the configuration source(s) distributing the external configuration of a federation partner. Upon loading the trusted anchor into the central server, the anchor is included into the internal configuration, allowing the security servers to download the external configuration of a federation partner as well as the internal configuration of the local X-Road infrastructure.

## Downloading the Configuration Anchor

**Access rights:** Security Officer

To download a configuration anchor, follow these steps.

1. On the **Management** menu, select **Configuration Management** and select either the **Internal Configuration** or **External Configuration** view, as appropriate.
2. In the **Anchor** section, click **Download** and save the prompted file.

## Re-Creating the Configuration Anchor

**Access rights:** Security Officer

Normally, the configuration anchors are generated (and in an HA setup, distributed to every node) automatically by the system upon changes in the data included in the anchor (one or more central server addresses, signing keys). The re-creation of an anchor is necessary only for recovering from error situations.

To re-create an anchor, follow these steps.

1. On the **Management** menu, select **Configuration Management** and select either the **Internal Configuration** or **External Configuration** view, as appropriate.
2. In the **Anchor** section, click **Re-Create**.

## Changing the Configuration Signing Keys

**Access rights:** Security Officer

Key change can be either

* **regular change** – the key is changed periodically (for example, annually) to minimize the risk of exposure;
* **emergency change** – the key and all its back-ups have been destroyed or the key has been exposed.

As the key change must be carried out efficiently without disrupting the operation of X-Road, the procedure is completed in two stages, wherein the old key and the new key can exist in parallel.

Note that in an HA setup, each node has its own set of configuration signing keys. The old and new key can exist in parallel on each node. Regular key change should cover all the nodes in a cluster and the new configuration anchor should be distributed after the keys have been changed on each node.

The steps of key change are as follows:

* First, a new key is generated (on each node in HA setups) and the configuration anchor containing the public key part(s) of the key(s) is distributed to X-Road participants. Until all participants have received the public key(s), the old (i.e. current) key(s) is/are used for signing configuration.
* Then, after all participants have received and uploaded the new public key(s), the old key(s) is/are removed and the new key(s) is/are used to sign configuration.

To perform a **regular key change**, follow these steps.

1. Generate, but do not activate a new configuration signing key (see 5.4.1) (in an HA setup, for each node). The system uses the old (active) key(s) to sign the configuration. Upon the generation of a new key, the system generates a new anchor for the corresponding configuration sources.
2. Download the anchor (see 5.2) containing the public key part(s) of the new signing key(s) and distribute the anchor along with the anchor file hash value either to the security server administrators (in case of internal configuration anchor) or to the federation partners (in case of external configuration anchor).
3. Activate the new signing key(s) (see 5.4.2).   
   The new signing key(s) should only be activated after all the affected server administrators have received and uploaded the distributed anchor. The central servers use the active key to sign configuration. If a server administrator has not uploaded the configuration anchor containing the public key part of the new key before the new key is activated, the verification of the downloaded configuration in the security servers will fail and the services exchange with the X-Road participants described in the configuration will be discontinued.
4. Delete the old signing key (in an HA setup, delete the old keys on all the nodes) (see 5.4.3). Upon the deletion of a key, the system generates a new configuration anchor.
5. Download the generated anchor (it does not contain the public key part(s) of the old signing key(s)) and distribute the anchor along with the anchor file hash value either to the security server administrators (in case of internal configuration anchor) or to the federation partners (in case of external configuration anchor).

To perform an **emergency key change**, the new key must be activated and the old key deleted immediately after the generation of the new key (in the steps described above, step 2 is skipped). The configuration anchor distributed to the security server administrators (in case of internal configuration anchor) or to the federation partners (in case of external configuration anchor) must only contain the public key part of the new signing key.

### Generating a Configuration Signing Key

**Access rights:** Security Officer

To generate a configuration signing key, follow these steps.

1. On the **Management** menu, select **Configuration Management** and select either the **Internal Configuration** or **External Configuration** view, as appropriate.
2. In the **Signing Keys** section, click **New Key**.
3. In a window that opens, select a key device, insert a label for the key, and click **OK**.
4. If needed, enter the key device’s PIN (PIN is asked, when the device has not been logged in to).

The system will automatically generate the corresponding configuration anchor containing the public key part of the generated key.   
If the generated key is the only signing key for the configuration source, the key will automatically be set as active (the active key is displayed in bold font style).

### Activating a Configuration Signing Key

**Access rights:** Security Officer

To activate a configuration signing key, follow these steps.

1. On the **Management** menu, select **Configuration Management** and select either the **Internal Configuration** or **External Configuration** view, as appropriate.
2. In the **Signing Keys** section, select an inactive key (the active key is displayed in bold font style) and click **Activate**.

### Deleting a Configuration Signing Key

**Access rights:** Security Officer

To delete a configuration signing key, follow these steps.

1. On the **Management** menu, select **Configuration Management** and select either the **Internal Configuration** or **External Configuration** view, as appropriate.
2. In the **Signing Keys** section, select an inactive key (the active key is displayed in bold font style) and click **Delete**.
3. Confirm the deletion by clicking **Confirm**.

## Viewing the Contents of a Configuration Part

**Access rights:** Security Officer**,** System Administrator

The contents of a configuration part can be viewed by downloading the configuration part file.

1. On the **Management** menu, select **Configuration Management** and select either the **Internal Configuration** or **External Configuration** view, as appropriate.
2. In the **Configuration Parts** section, select a configuration part and click **Download**.
3. Save or open the prompted file.

## Uploading a Trusted Anchor

**Access rights:** Security Officer

To upload a trusted anchor, follow these steps.

1. On the **Management** menu, select **Configuration Management** and select the **Trusted Anchors** view.
2. Click **Upload Anchor**, find the external configuration anchor received from a federation partner and click **Upload**.
3. Verify the integrity of the anchor file by comparing the displayed anchor file hash value with the hash value provided by the federation partner and confirm the anchor upload by clicking **Confirm**.

In case a previous anchor from the same federation partner has been uploaded to the system, the new anchor will replace the old one.

## Viewing the Contents of a Trusted Anchor

**Access rights:** Security Officer**,** System Administrator

The contents of a trusted anchor can be viewed by downloading the anchor file.

To download an anchor file, follow these steps.

1. On the **Management** menu, select **Configuration Management** and select the **Trusted Anchors** view.
2. In the anchor section, click **Download**.
3. Save or open the prompted file.

## Deleting a Trusted Anchor

**Access rights:** Security Officer

To delete an anchor file, follow these steps.

1. On the **Management** menu, select **Configuration Management** and select the **Trusted Anchors** view.
2. In the anchor section, click **Delete**.
3. Confirm the deletion by clicking **Confirm**.

# The Management Requests System

## Registration Requests

As the registration of associations in the X-Road governing authority is security-critical, the following measures are applied to increase security:

* The registration request must be submitted to the X-Road governing authority over two channels, or in other words, the registration wish must be expressed through two **complementary requests**:
  + one request is submitted to the X-Road central server through the security server,
  + the other request is submitted to the X-Road governing authority through means independent of the X-Road (for example, over a digitally signed e-mail). This request must be formalized in the central server by the central server administrator.
* The association must be approved by the X-Road governing authority.

There are two types of registration requests:

* authentication certificate registration request (see Sections 7.4 and 8.3);
* security server client registration request (see Section 7.5).

### State Machine Model for Registration Requests

A registration request can be in one of the following states. See Figure 1 for the state machine diagram.

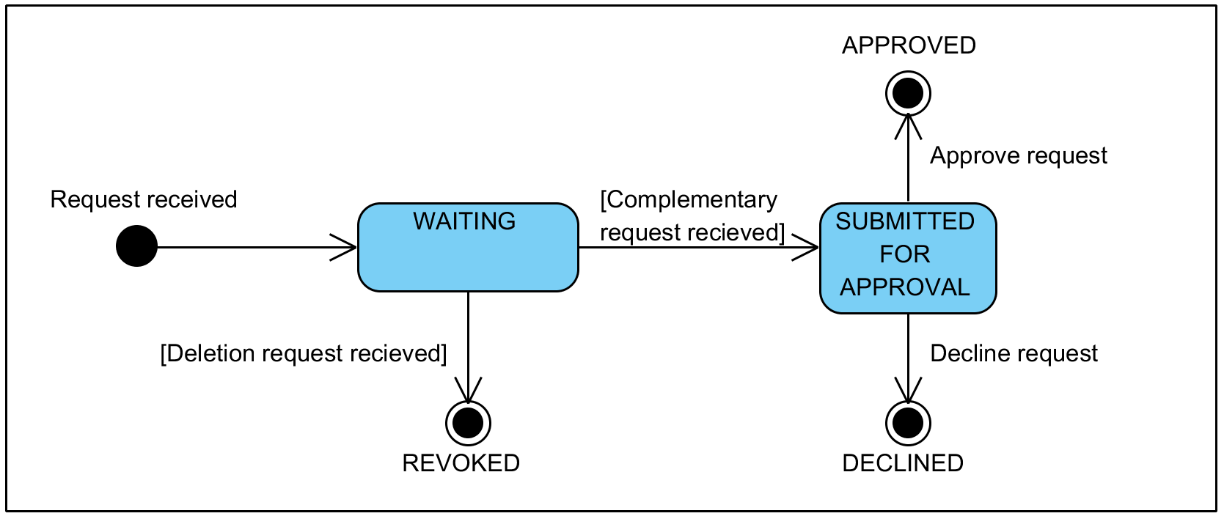


Figure 1. State machine diagram for registration requests

**Waiting** – a registration request has been submitted either from a security server or formalized in the central server, but the complementary request has not been submitted. From this state, the request can move to the following states.

* “Submitted for approval”, if the complementary request is received (see 7.4, 7.5 and 8.3).
* “Revoked”.
  + Registration request received from a security server are automatically revoked by deletion requests sent from the security server for the same object that was submitted for registration with the registration request.
  + Registration request formalized in the central server can be revoked by the central server administrator in the central server (see 7.4, 7.5 and 8.3). A deletion request for the same object that was submitted for registration with the registration request is created upon revocation.

**Submitted for approval** – both complementary requests have been submitted to the central server, but the association between the objects of the registration request has not been approved. From this state, the request can move to the following states.

* “Approved”, if the registration request is approved in the central server (see 7.4, 7.5 and 8.3).
* “Declined”, if the registration request is declined in the central server (see 7.4, 7.5 and 8.3).

**Approved** – the complementary registration requests have been approved. The association between the objects of the registration request has been created.

**Declined** – the complementary registration requests have been declined.

**Revoked** – a registration request has been revoked.

## Deletion Requests

Complementary requests are not needed for association deletion requests. Associations are deleted on the basis of a single request, which is either submitted through a security server or formalized in the central server.

Deletion requests are

* authentication certificate deletion request (see Section 8.4);
* security server client deletion request (see Section 7.6).

## Viewing the Management Request Details

**Access rights:** Registration Officer

To open the detail view, follow these steps.

1. On the main menu, select **Management** and then **Management Requests**.
2. Select from the table a request and either double-click it or click **Details**.

There are three data sections in the view.

1. Information about the request.

* Request ID – the identifier of the request;
* Received – the date and time of saving the request in the central server;
* Source – the source of the request. The request can be either submitted through a security server (SECURITY\_SERVER) or created in the central server (CENTER);
* Status (only for registration requests) – the state of the request, see Figure 1;
* Complementary/Revoking request ID (only for registration requests) – the identifier of the request that caused the status change of this request from "Waiting" to "Submitted for approval" or from "Waiting" to "Revoked";
* Comments – the source event for the automatic generation of the request. For example, when a security server is deleted from the central server, deletion requests are automatically generated for all the clients and authentication certificates registered for this security server. In the "Comments" field of the generated requests, a comment with the server identifier is added in such case. This field is left empty for requests that are not automatically generated by the central server.

1. Information about the security server associated with the request.

* Owner Name – the name of the security server owner (X-Road member);
* Owner Class – the member class of the security server owner;
* Owner Code – the member code of the security server owner;
* Server Code – the code of the security server;
* Address – the address of the security server. The field is filled only for authentication certificate registration requests submitted through a security server, and only if the security server's administration deemed it necessary to provide an address upon request submission.

1. Information about the request object – that is, the client or the authentication certificate being registered or deleted.

For the authentication certificate:

* CA – the name of the certification authority that issued the certificate;
* Serial Number – the serial number of the certificate;
* Subject – all attributes of the certificate's *Subject* field;
* Expires – the expiration date of the certificate;

For the security server client:

* Name – the name of the X-Road member managing the subsystem;
* Class – the member class of the X-Road member managing the subsystem;
* Code – the member code of the X-Road member managing the subsystem;
* Subsystem – the code of the subsystem.

# Managing the X-Road Members

## Adding a Member

**Access rights:** Registration Officer

To add a new X-Road member, follow these steps.

1. On the **Configuration** menu, select **Members** and click **Add**.
2. In the window that opens, enter the member's information and click **OK**. The new member appears in the list of members.

## Viewing the Member Details

**Access rights:** Registration Officer

To open the detail view, follow these steps.

1. On the **Configuration** menu, select **Members**.
2. Select from the table an X-Road member and either double-click it or click **Details**.

The view consists of six sections.

1. "Member Details" – displays the member's class, code, and name.
2. "Owned Servers" – displays the codes of servers owned by this member.   
   *Hint: Click a server's code to open the server's detail view.*
3. "Global Group Membership" – displays information about the group membership of the member or its subsystems.   
   *Hint: Click a group's code to open the group's detail view.*
4. "Subsystems" – displays the member's subsystem codes, as well as the code of the security server the subsystem is a client of. If a subsystem is not a client of any security servers, it is displayed in red.   
   *Hint: Click the related security server's code to open the security server's detail view.*
5. "Used Servers" – displays information about security servers that provide hosting service to the member’s subsystems. The following information is displayed: the code of the security server hosting the subsystem, the code of the subsystem that is being hosted and the name of the security server owner.   
   *Hint: Click the security server's code to open the server's detail view. Click the owner's name to open the owner's detail view.*
6. "Management Requests" – displays all management requests related to the member and the security servers in the member's ownership.   
   *Hint: Click a request ID to open the request's detail view.*

## Adding a Subsystem to an X-Road Member

**Access rights:** Registration Officer

To add a subsystem to an X-Road member, follow these steps.

1. On the **Configuration** menu, select **Members**, select the member to whom you wish to add a subsystem and click **Details**.
2. In the view that opens, locate the **Subsystems** section and click **Add**.
3. Enter the code of the subsystem and click **OK**.

## Registering a Member's Security Server

**Access rights:** Registration Officer

To register an X-Road member's security server, the following actions must be taken.

* An authentication certificate registration request must be sent from the security server to the central server by the security server administrator;
* The complementary authentication certificate registration request must be formalized in the central server by the central server administrator, on the appeal of the security server's owner.
* The complimentary requests must be approved by the central server administrator.

**To formalize the central server-side request to register a security server**, follow these steps.

1. On the **Configuration** menu, select **Members**, select a member whose security server you wish to register and click **Details**.
2. In the window that opens, select the **Owned Servers** section and click **Add**.
3. Enter the code of the security server being registered on the registration form.
4. Click **Upload** and locate the authentication certificate file of the security server.
5. Click **Submit** to submit the registration request.

If the request is successfully submitted, a corresponding record appears in the member's detail view in the "**Management Requests**" section (Request Type "Certificate registration"), and in the list of management requests (on the main menu select **Management** and then **Management Requests**).

The central server-side request is in "**Waiting**" state if the request submitted through the security server has not arrived in the central server by the time the central server-side request is submitted.

The complementary requests are in "**Submitted for approval**" state if the request submitted through the security server has arrived in the central server by the time the central server-side request is submitted.

Registration requests in the state "Submitted for approval" can be **approved** or **rejected** by the central server administrator.

**To approve a request**

* open one of its complementary requests in detail view and click **Approve**.

**On the approval of the request**

* the complementary requests move to the "Approved" state;
* the registered security server appears both in the "Owned Servers" section of its owner’s detail view and in the list of security servers (on the main menu, select **Configuration** and then **Security Servers**);
* the security server's owner is added to the global "security-server-owners" group.

**To decline a request**

* open one of the complementary requests in detail view and click **Decline**. Upon declining a request, both complementary requests move to the "Declined" state.

The registration requests formalized in the central server that are in the "**Waiting**" state can be **revoked** (e.g., if the request was submitted erroneously).

**To revoke a request**, follow these steps.

1. Open a registration request in the "Waiting" state. You can either:
   * Locate the request in the list of management requests: on the main menu, click **Management**, click **Management Requests** and then click **Details**;
   * Locate the request from the detail view section **Management Requests** of the object associated with the request (security server or security server's owner).
2. Click **Revoke**. Upon revoking a request, a deletion request corresponding to the registration request is automatically generated and the registration request is moved to the "Revoked" state.

## Registering a Client to a Security Server

**Access rights:** Registration Officer

To register a subsystem of an X-Road member as a security server client, the following actions must be taken.

* A security server client registration request must be sent from the security server to the central server by the security server administrator;
* The complementary security server client registration request must be formalized in the central server by the central server administrator, on the appeal of the security server's owner.
* The complimentary requests must be approved by the central server administrator.

The central server-side client registration request can be formalized either through the security server's detail view or a member's detail view.

**To formalize the request through the member's detail view**, follow these steps.

1. On the **Configuration** menu, select **Members**, select the member that wishes to register its subsystem as a security server client from the list and click **Details**.
2. In the window that opens, open the **Used Servers** section and click **Add**.
3. On the registration request form that opens, do the following:

* enter the code of the subsystem in the "Client Information" section on the **Subsystem** field;
* locate the "Security Server Information" section, click **Search** and in the window that opens, select the appropriate security server.

1. Click **Submit** to submit the registration request.

**To formalize the request through the security server's detailed view**, follow these steps.

1. On the **Configuration** menu, select **Security servers**, select from the list a security server where a new client wishes to register and click **Details**.
2. In the window that opens, locate the **Clients** section and click **Add**.
3. On the registration request form, locate the "Client Information" section, click **Search** and in the window that opens, select the registrant's information, or enter the information manually.
4. Click **Submit** to submit the registration request.

If the request is successfully submitted, a corresponding record appears in the member's detail view in the "Management Requests" section (Request Type "Client registration"), and in the list of management requests (on the main menu select **Management** and then **Management Requests**).

The central server-side request is in "**Waiting**" state if the request submitted through the security server has not arrived in the central server by the time the central server-side request is submitted.

The complementary requests are in "**Submitted for approval**" state if the request submitted through the security server has arrived in the central server by the time the central server-side request is submitted.

Registration requests in the state "Submitted for approval" can be **approved** or **rejected** by the central server administrator.

**To approve a request**

* open one of its complementary requests in detail view and click **Approve**.

**On the approval of the request**, follow these steps.

* The complementary requests move to the "Approved" state.
* Information about the security server is displayed in the "Used Servers" section of the detail view of the member whose subsystem was registered as client.
* The client's information is displayed in the "Clients" section of the detailed view of the security server to which the client was registered.

**To decline a request**

* open one of the complementary requests in detail view and click **Decline**. Upon declining a request, its complementary requests move to the "Declined" state.

The registration requests formalized in the central server that are in the "**Waiting**" state can be **revoked** (e.g., if the request was submitted erroneously).

**To revoke a request**, follow these steps.

1. Open a registration request in the "Waiting" state. You can either:

* locate the request in the list of management requests: on the main menu, click **Management**, click **Management Requests** and then click **Details**;
* locate the request from the “Management Requests” section of the detail view of the object associated with the request (security server or security server's owner), and click the request ID.

1. Click **Revoke**. Upon revoking a request, a deletion request corresponding to the registration request is automatically generated and the registration request is moved to the "Revoked" state.

## Removing a Client from a Security Server

**Access rights:** Registration Officer

The association between an X-Road member and a security server is deleted by the corresponding security server's client deletion request. The request can be submitted through the security server or in the central server.

**The association between the security server's owner and the security server cannot be deleted.**

Removing a client from the security server clients can be carried out either through the security server's detail view or a member's detail view.

**To submit a security server client deletion request through a member's detail view**, follow these steps.

1. On the **Configuration** menu, select **Members**, select the member whose subsystem is to be removed from a security server and click **Details**.
2. In the window that opens, locate the **Used Servers** section, select the association between the client subsystem and the security server, and click **Delete**.
3. Review the information displayed on the client deletion request and click **Submit** to submit the request.
4. The submitted request appears in the "Management Requests" section of the member's detail view and in the requests management view (on the main menu, select **Management** and then **Management Requests**).

**To submit a security server client deletion request through security server's detail view**, follow these steps.

1. On the **Configuration** menu, select **Security Servers**, select a security server from where the client is to be removed and click **Details**.
2. In the window that opens, locate the **Clients** section, select the client subsystem and click **Delete**.
3. Review the information displayed on the client deletion request and click **Submit** to submit the request.
4. The submitted request appears in the "Management Requests" section of the security server's detail view and in the requests management view (on the main menu, select **Management** and then **Management Requests**).

## Changing the Global Group Membership of an X-Road Member’s Subsystem

**Access rights:** Registration Officer

To change the group membership of X-Road members’ subsystems, two options are provided:

* member-based – use it if you need to change a specific X-Road member's subsystem's group membership. The procedure is described in this section;
* group-based – use it if you need to change the membership of a specific group. The procedure is described in section 10.4

**To add a member’s subsystem to a global group**, follow these steps.

1. On the **Configuration** menu, select **Members**, select a member whose subsystem you wish to add to a global group and click **Details**.
2. In the view that opens, locate the **Global Group Membership** section and click **Add**.
3. Select the subsystem from the **Subsystem** drop-down. On the **Group** drop-down, select the group where the member’s subsystem should be added to.
4. Click **OK**.

**To remove a member’s subsystem from a global group**, follow these steps.

1. On the **Configuration** menu, select **Members**, select a member whose subsystem you wish to remove from a global group and click **Details**.
2. In the view that opens, locate the **Global Group Membership** section.
3. Select the row containing the association between the subsystem and the global group and click **Delete** to remove the subsystem from the selected group.
4. In the confirmation window that opens, click **Confirm**.

## Deleting a Subsystem

**Access rights:** Registration Officer

In the central server, the X-Road member's subsystem can be deleted only if the subsystem is not associated with any security servers, that is, not registered as a client of any security servers. If the subsystem is not associated with any security servers, its code is displayed in red.

To delete an X-Road member's subsystem, follow these steps.

1. On the **Configuration** menu, select **Members**, select a member whose subsystem you wish to delete and click **Details**.
2. In the view that opens, find from the **Subsystems** section the subsystem you wish to delete and click **Delete**. *Note:* The "Delete" button is enabled only if the subsystem is not a client of any security servers.

## Deleting an X-Road Member

**Access rights:** Registration Officer

When an X-Road member is deleted, information about all security servers in its ownership will be deleted as well.

To delete an X-Road member, follow these steps.

1. On the **Configuration** menu, select **Members**, select a member that you wish to delete, and click **Details**.
2. In the view that opens, locate the **Member Details** section and click **Delete**. In the confirmation window that opens, click **Confirm**.

# Managing the Security Servers

## Viewing the Security Server Details

**Access rights:** Registration Officer

To open the detail view, follow these steps.

1. On the main menu, select **Configuration** and then select **Security Servers**.
2. Choose from the table a security server and either double-click it or click **Details**.

The view contains four sections.

* "Security Server Details" – information about the server and its owner.
* "Clients" – information about clients registered for this security server.   
  *Hint: Click a client's code to open the client's detail view.*
* "Authentication Certificates" – information about the security server's registered authentication certificates.   
  *Hint: Click a certificate's serial number to open the certificate's detail view.*
* "Management Requests" – a list of all management requests associated with the security server.   
  *Hint: Click a request ID to open the request's detail view.*

## Changing the Security Server Address

**Access rights:** Registration Officer

By default, the security server's address is provided in the registration request of the authentication certificate sent from the security server. The address must be changed if it was not set when the request was submitted or if it is no longer valid.

There are several reasons why setting the security server’s address matters.

* The services that are relayed through a security server become available once the security server’s address is set.
* By registering the addresses of security servers, the service clients are certain to receive a response to their queries in a reasonable time, even if the relaying security server is overloaded with service requests (e.g., the requests from addresses belonging to registered security servers are served before requests coming from unknown addresses).

To change the security server address, follow these steps.

1. On the **Configuration** menu, select **Security Servers**, select the security server whose address you wish to change and click **Details**.
2. In the view that opens, locate the "Security Server Details" section and click **Edit** adjacent to the "Address" field.
3. Enter the security server's address and click **OK**.

## Registering a Security Server's Authentication Certificate

**Access rights:** Registration Officer

To register a security server's authentication certificate, the following actions must be taken.

* An authentication certificate registration request must be sent from the security server to the central server by the security server administrator;
* The complementary authentication certificate registration request must be formalized in the central server by the central server administrator, on the appeal of the security server's owner.
* The complimentary requests must be approved by the central server administrator.

**To formalize the registration request of an authentication certificate in the central server**, follow these steps.

1. On the **Configuration** menu, select **Security servers**, select the security server whose authentication certificate you wish to register and click **Details**.
2. In the window that opens, locate the "Authentication Certificates" section and click **Add**.
3. On the registration request form that opens, click **Upload** and locate the authentication certificate file of the security server being registered.
4. Click **Submit** to submit the registration request.

If the request is successfully submitted, a corresponding record appears in the server's and server owner's detail view in the **Management Requests** section (Request Type "Certificate registration"), and in the list of management requests (on the main menu, select **Management** and then **Management Requests**).

The central server-side request is in "**Waiting**" state if the request submitted through the security server has not arrived in the central server by the time the central server-side request is submitted.

The complementary requests are in "**Submitted for approval**" state if the request submitted through the security server has arrived in the central server by the time the central server-side request is submitted.

Registration requests in the state "Submitted for approval" can be **approved** or **rejected** by the central server administrator.

**To approve the request**

* open the detailed view of one of its complementary requests and click **Approve**.

**Upon approving the request**

* the complementary requests move to the "Approved" state;
* the registered authentication certificate appears in the security server's detail view, in the "Authentication Certificates" section.

**To decline the request**

* open one of the complementary requests in detail view and click **Decline**. Upon declining a request, its complementary requests move to the "Declined" state.

The registration requests formalized in the central server that are in the "**Waiting**" state can be **revoked** (e.g., if the request was submitted erroneously).

**To revoke a request**, follow these steps.

1. Open a registration request in the "Waiting" state. You can either:

* locate the request in the list of management requests: On the main menu, select **Management**, click **Management Requests** and then click **Details** or double-click the request row;
* locate the request from the “Management Requests” detail view section of the security server associated with the request and click the request ID.

1. Click **Revoke**. Upon revoking, the request it is moved to the "Revoked" state.

## Deleting a Security Server's Authentication Certificate

**Access rights:** Registration Officer

The authentication certificate registered for a security server is deleted when an authentication certificate deletion request is received for that certificate. The request can be submitted through the security server or in the central server.

**To submit an authentication certificate deletion request in the central server**, follow these steps.

1. On the **Configuration** menu, select **Security Servers**, select the security server whose certificate you wish to delete and click **Details**.
2. In the view that opens, locate the **Authentication Certificates** section, find the correct authentication certificate and click **Delete**.
3. Review the information displayed on the deletion request and click **Submit** to submit the request.
4. The submitted request appears in the "Management Requests" section of the security server's and its owner's detail view and in the requests management view (on the main menu, select **Management** and then **Management Requests**).

## Deleting a Security Server

**Access rights:** Registration Officer

To delete a security server, follow these steps.

1. On the **Configuration** menu, select **Security Servers**, select from the list the security server that you wish to delete and click **Details**.
2. In the view that opens, locate the "Security Server Details" section and click **Delete**. Confirm the action by clicking **Confirm**.

If the security server being deleted has registered clients or authentication certificates, deletion requests for those associations are automatically generated.

# Managing the Central Services

## Adding a Central Service

**Access rights:** System Administrator

To add a central service, follow these steps.

1. On the **Configuration** menu, select **Central Services** and click **Add**.
2. In the window that opens:

* enter the central service's code in the **Central Service Code** field;
* enter the implementing service's code in the **Code** field and the service version in the **Version** field;
* click **Search Provider** to find and enter the subsystem providing the central service.

1. When all required fields are filled, click **OK**.

## Changing the Service Implementing a Central Service

**Access rights:** System Administrator

To change or delete a service that implements a central service, follow these steps.

1. On the **Configuration** menu, select **Central Services**, select a service from the list and click **Edit**.
2. In the window that opens, change or delete (**Clear**) information about the implementing service.
3. Click **OK** when done.

## Deleting a Central Service

**Access rights:** System Administrator

To delete a central service, follow these steps.

1. On the **Configuration** menu, select **Central Services**.
2. Select from the list a central service that you wish to delete and click **Delete**.
3. In the window that opens, click **Confirm**.

# Managing the Global Groups

## Adding a Global Group

**Access rights:** Registration Officer

To add a new global group, follow these steps.

1. On the main menu, select **Configuration**, select **Groups** and click **Add**.
2. In the window that opens, enter the new group's code and description, and click **OK**. The new group is added to the list of global groups.

## Viewing the Global Group Details

**Access rights:** Registration Officer

To see the details of a global group, follow these steps.

1. On the main menu, select **Configuration** and then **Groups**.
2. Select a global group from the table and either double-click it or click **Details**.

In the global group detail view, a list of the group's members is displayed. The detail view allows you to change the group's description, delete the group, and add or remove its members.

## Changing the Description of a Global Group

**Access rights:** Registration Officer

To change the description of a global group, follow these steps.

1. On the main menu, select **Configuration** and then **Groups**.
2. Select a global group from the table and click **Details**.
3. In the view that opens, click **Edit**, change the group’s description and click **OK**.

## Changing the Members of a Global Group

**Access rights:** Registration Officer

*Note that the members of the global group* ***security-server-owners*** *are managed automatically by the central server and cannot be added or removed manually.*

To add subsystems of X-Road members to a global group, follow these steps.

1. On the main menu, select **Configuration** and then **Groups**.
2. Select the global group from the table and click **Details**.
3. In the view that opens, click **Add Members**.
4. Locate and select one or more subsystems and click **Add Selected Members**. Or filter a selection of subsystems with the search function and add them all to the group by clicking **Add All**.

To remove members from a group, follow these steps.

1. On the main menu, select **Configuration** and then **Groups**.
2. Select the global group from the table and click **Details**.
3. Select one or more subsystems from the list of group members and click **Remove Selected Members**. To remove all group members, click **Remove All Members**.
4. In the confirmation window that opens, click **Confirm**.

## Deleting a Global Group

**Access rights:** Registration Officer

To delete a global group, follow these steps.

1. On the main menu, select **Configuration** and then **Groups**.
2. Select a global group from the table and click **Details**.
3. In the view that opens, click **Delete Group** and in the confirmation window click **Confirm**.

# Managing the Approved Certification Services

## Adding an Approved Certification Service

**Access rights:** System Administrator

To add a certification service, follow these steps.

1. On the **Configuration** menu, select **Certification Services** and click **Add**.
2. Locate the certification service CA certificate file and click **Next**.
3. Set the certification service settings as follows.

* If the certification service issues only authentication certificates, check the **This CA can only be used for TLS authentication** checkbox. However, if the certification service issues additionally or only signing certificates, leave the checkbox empty.
* Enter the fully qualified class name that implements the ee.ria.xroad.common.certificateprofile.CertificateProfileInfo interface to the field **Certificate Profile Info** (for example: ee.ria.xroad.common.certificateprofile.impl.SkKlass3CertificateProfileInfoProvider).

If the CA certificate contains the certification service CA’s OCSP service information, and the PKI does not have intermediate CAs, the procedure is complete.

1. If necessary, enter the certification service CA’s OCSP service URL and/or certificate in the **OCSP responders** tab by clicking **Add**.
2. Information about intermediate CAs can be added in the **Intermediate CAs** tab.  
   To add a new intermediate CA
   * click **Add**;
   * in the window that opens, locate the certificate file of the intermediate CA and click **OK**;
   * to add OCSP service information to the new intermediate CA, open the **OCSP responders** tab and click **Add**.

## Changing an Approved Certification Service

**Access rights:** System Administrator

While it is not possible to change the certification service's CA certificate, it is possible to

* change the service settings;
* add, change, and delete the certificate service CA’s OCSP services;
* add, change, and delete the certificates and OCSP service information of intermediate CAs.

To edit a certification service, follow these steps.

1. On the **Configuration** menu, select **Certification Services**.
2. Select from the list the certification service you want to edit and click **Edit**.

## Deleting an Approved Certification Service

**Access rights:** System Administrator

To delete a certification service from the list of approved services, follow these steps.

1. On the **Configuration** menu, select **Certification Services**.
2. Select from the list the approved certification service you wish to remove and click **Delete**.
3. In the window that opens, click **Confirm**.

# Managing the Approved Timestamping Services

## Adding an Approved Timestamping Service

**Access rights:** System Administrator

To add an approved timestamping service, follow these steps.

1. On the **Configuration** menu, select **Time Stamping Services** and click **Add**.
2. In the window that opens, enter the timestamping service URL and click **Upload** to locate the certificate file of the timestamping service.
3. Verify that you have loaded the correct certificate and click **OK**. Information about the new timestamping service appears in the list.

## Changing the URL of an Approved Timestamping Service

**Access rights:** System Administrator

To change the timestamping service URL, follow these steps.

1. On the **Configuration** menu, select **Time Stamping Services**, select a timestamping service from the list and click **Edit**.
2. In the window that opens, edit the URL and click **OK**.

## Deleting an Approved Timestamping Service

**Access rights:** System Administrator

To remove a timestamping service, follow these steps.

1. On the **Configuration** menu, select **Time Stamping Services**, select a timestamping service from the list and click **Delete**.
2. In the window that opens, click **Confirm**.

# Configuration Backup and Restore

**Access rights:** System Administrator

The central server backs up

* the database (excluding the schema\_migrations table and the database schema) and
* the directories /etc/xroad/ and /etc/nginx/sites-enabled/.

## Backing Up the System Configuration

To back up the configuration, follow these steps.

1. On the **Management** menu, select **Back Up and Restore**.
2. Click **Back Up Configuration** to start the backup process.
3. A window opens displaying the output from the backup script; click **OK** to close it.
4. When done, the configuration backup file appears in the list of configuration backup files.

## Restoring the System Configuration in the User Interface

To restore configuration, follow these steps.

1. On the **Management** menu, select **Back Up and Restore**.
2. Select a file from the list of configuration backup files and click **Restore**.
3. Click **Confirm** to proceed.
4. A window opens displaying the output from the restore script; click **OK** to close it.

## Restoring the Configuration from the Command Line

To restore configuration from the command line, the following data must be available:

* the instance ID of the central server and,
* in HA setup, the node name of the central server.

It is expected that the restore command is run by the xroad user.

Use the following command to restore configuration in **non-HA setup**:

/usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh \

-i <instance\_ID> -f <path + filename>

In **HA setup**, this command has an additional mandatory parameter, the node name:

/usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh \

-i <instance\_ID> -n <node\_name> -f <path + filename>

For example (all in one line, non-HA setup):

/usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh \

-i EE \

-f /var/lib/xroad/backup/conf\_backup\_20140707\_200916.tar

For example (all in one line, HA setup):

/usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh \

-i EE -n node\_0 \

-f /var/lib/xroad/backup/conf\_backup\_20140707\_200916.tar

If it is absolutely necessary to restore the system from a backup made on a different central server, the forced mode of the restore command can be used with the –F option. For example:

/usr/share/xroad/scripts/restore\_xroad\_center\_configuration.sh \

-F -f /var/lib/xroad/backup/conf\_backup\_20140707\_200916.tar

## Downloading, Uploading and Deleting Configuration Backup Files

The following actions can be performed in the **Back Up and Restore** view.

To save the configuration backup file locally:

* click **Download** on the respective row and save the prompted file.

To delete the configuration backup file:

* click **Delete** on the respective row and confirm the action by clicking **Confirm**.

To upload a configuration file from the local file system to the security server:

* click **Upload Backup File**, select a file to be uploaded and click **OK**. The uploaded configuration file appears in the list of configuration files.

# Audit Log

The central server keeps an audit log of the events performed by the central server administrator. The audit log events are generated by the user interface when the user changes the system’s state or configuration. The user actions are logged regardless of whether the outcome of the action was a success or a failure. The complete list of the audit log events is described in [SPEC-AL].

Actions that change the system’s state or configuration but are not carried out using the user interface are not logged (for example, X-Road software installation and upgrade, user creation and permission granting, and changing of the configuration files in the file system).

An audit log record contains

* the description of the user action,
* the date and time of the event,
* the username of the user that performed the action, and
* the data related to the event.

For example, adding a new member in the central server produces the following log record:

2015-07-03T11:40:52+03:00 my-central-server-host INFO [X-Road Center UI] 2015-07-03 11:40:52+0300 - {"event":"Add member","user":"admin1", "data":{"memberName":"member1 name","memberClass":"COM", "memberCode":"member1"}}

The event is present in JSON [JSON] format, in order to ensure machine processability. The field event represents the description of the event, the field user represents the user name of the performer, and the field data represents data related with the event. The failed action event record contains an additional field reason for the error message. For example:

2015-07-03T11:51:24+03:00 my-central-server-host INFO [X-Road Center UI] 2015-07-03 11:51:24+0300 - {"event":"Log in to token failed","user":"admin1", "reason":"PIN incorrect","data":{"tokenId":"0","tokenSerialNumber":null, "tokenFriendlyName":"softToken-0"}}

By default, audit log is located in the file

/var/log/xroad/audit.log

## Changing the Configuration of the Audit Log

The X-Road software writes the audit log to the *syslog* (*rsyslog*) using UDP interface (default port is 514). Corresponding configuration is located in the file

/etc/rsyslog.d/90-udp.conf

The audit log records are written with level INFO and facility LOCAL0. By default, log records of that level and facility are saved to the X-Road audit log file

/var/log/xroad/audit.log

The default behavior can be changed by editing the *rsyslog* configuration file

/etc/rsyslog.d/40-xroad.conf

Restart the *rsyslog* service to apply the changes made to the configuration file

restart rsyslog

The audit log is rotated monthly by *logrotate*. To configure the audit log rotation, edit the *logrotate* configuration file

/etc/logrotate.d/xroad-center

## Archiving the Audit Log

In order to save hard disk space and avoid loss of the audit log records during central server crash, it is recommended to archive the audit log files periodically to an external storage or a log server.

The X-Road software does not offer special tools for archiving the audit log. The *rsyslog* can be configured to redirect the audit log to an external location.

# Monitoring

Monitoring is taken to use by installing the monitoring support (see [IG-CS]) and appointing the central monitoring client as specified below.

Identity of central monitoring client (if any) is configured using central server's admin user interface. Configuration is done by updating a specific optional configuration file (see [UC-GCONF]) monitoring-params.xml. This configuration file is distributed to all security servers through the global configuration distribution process (see [UC-GCONF]).

<tns:conf xmlns:id="http://x-road.eu/xsd/identifiers"

xmlns:tns="http://x-road.eu/xsd/xroad.xsd"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://x-road.eu/xsd/xroad.xsd">

<monitoringClient>

<monitoringClientId id:objectType="SUBSYSTEM">

<id:xRoadInstance>fdev</id:xRoadInstance>

<id:memberClass>GOV</id:memberClass>

<id:memberCode>1710128-9</id:memberCode>

<id:subsystemCode>LIPPIS</id:subsystemCode>

</monitoringClientId>

</monitoringClient>

</tns:conf>

One can configure either one member or a member's subsystem to be the central monitoring client. Permission to execute monitoring queries is strictly limited to that single member or subsystem - defining one subsystem to be a monitoring client does **not** grant the corresponding member access to querying monitoring data (and vice versa).

To disable central monitoring client altogether, update configuration to one which has no client:

<tns:conf xmlns:id="http://x-road.eu/xsd/identifiers"

xmlns:tns="http://x-road.eu/xsd/xroad.xsd"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://x-road.eu/xsd/xroad.xsd">

<monitoringClient>

</monitoringClient>

</tns:conf>

# Additional configuration options

## 16.1 Verify next update

For additional robustness the OCSP [RFC-OCSP] response verifier can be configured to skip checking of nextUpdate parameter. By default the checking is turned on and to turn it off the user has to take action.

Configuration is done by updating a specific optional configuration file (see [UC-GCONF]) nextupdate-params.xml. This configuration file is distributed to all security servers through the global configuration distribution process (see [UC-GCONF]).

<xro:conf xmlns:xro="http://x-road.eu/xsd/xroad.xsd">

<verifyNextUpdate>true</verifyNextUpdate>

</xro:conf>

With verifyNextUpdate element value “false” the nextUpdate parameter checking is switched off.

## 16.2 OCSP fetch interval

The xroad-signer component has a specific interval how often it downloads new OCSP [RFC-OCSP] responses. By default the fetch interval is configured to 3600 seconds. To use something else than the default value a global configuration extension part (see [UC-GCONF]) of specific format can be uploaded to central server.

<xro:conf xmlns:xro="http://x-road.eu/xsd/xroad.xsd">

<ocspFetchInterval>3600</ocspFetchInterval>

</xro:conf>

The value is the fetch interval in seconds for new OCSP responses.

# Logs and System Services

Most significant central server services are the following:

|  |  |  |
| --- | --- | --- |
| **Service** | **Purpose** | **Log** |
| xroad-jetty | The application server providing the user interface and the request acceptance service. | /var/log/xroad/jetty/ |
| xroad-signer | The service that manages key settings. | /var/log/xroad/signer.log |
| nginx | The Web server that distributes configuration and implements the TLS protocol in the user interface. | /var/log/nginx/ |

System services can be managed using the *upstart* facility.

**To start a service**, issue the following command as a root user:

service <service> start

**To stop a service**, enter:

service <service> stop

**To read logs**, a user must have root user's rights or belong to the xroad system group.

For logging, the **Logback** system is used.

Logback configuration files are stored in the /etc/xroad/conf.d/ directory.

Default settings for logging are the following:

* logging level: INFO;
* rolling policy: whenever file size reaches 100 MB.