

|  |
| --- |
| X-ROAD 6  Central Server Installation Guide  2.2 |
|  |

Version HISTORY

|  |  |  |
| --- | --- | --- |
| Date | Version | Description |
| 01.12.2014 | 1.0 | Initial version |
| 19.01.2015 | 1.1 | License information added |
| 02.02.2015 | 1.2 | References fixed |
| 18.03.2015 | 1.3 | Meta-package for central server |
| 02.04.2015 | 1.4 | „sdsb” changed to „xroad” |
| 30.06.2015 | 1.5 | Minor corrections done |
| 06.07.2015 | 1.6 | New repository address |
| 17.09.2015 | 1.7 | Notes about high availability added, references updated |
| 18.09.2015 | 1.8 | Minor corrections done |
| 18.09.2015 | 2.0 | Editorial changes made |
| 13.12.2015 | 2.1 | Installing support for HW tokens updated (2.6) Initial configuration (Chapter 3) updated. |
| 16.05.2016 | 2.2 | Merged changes from xtee6-doc repo.  Added Chapter 2.7 installation instructions for monitoring. |

Table of Contents

[1 Introduction 4](#_Toc451440842)

[1.1 Target Audience 4](#_Toc451440843)

[1.2 References 4](#_Toc451440844)

[2 Installation 5](#_Toc451440845)

[2.1 Prerequisites to Installation 5](#_Toc451440846)

[*2.2* Reference Data 5](#_Toc451440847)

[2.3 Requirements to the Central Server 6](#_Toc451440848)

[2.4 Preparing OS 6](#_Toc451440849)

[2.5 Installation 6](#_Toc451440850)

[2.6 Installing the Support for Hardware Tokens 7](#_Toc451440851)

[2.7 Installing the Support for Monitoring 8](#_Toc451440852)

[3 Initial Configuration 9](#_Toc451440853)

[*3.1* Reference Data 9](#_Toc451440854)

[3.2 Initialising the Central Server 9](#_Toc451440855)

[3.3 Configuring the Central Server and the Management Services' Security Server 9](#_Toc451440856)

[4 Installation Error Handling 11](#_Toc451440857)

[4.1 Cannot Set LC\_ALL to Default Locale 11](#_Toc451440858)

[4.2 PostgreSQL Is Not UTF8 Compatible 11](#_Toc451440859)

[4.3 Could Not Create Default Cluster 11](#_Toc451440860)

[4.4 Is Postgres Running On Port 5432? 12](#_Toc451440861)

# Introduction

## Target Audience

The intended audience of this installation guide are the X-Road central server administrators responsible for installing and configuring the X-Road central server software.

The document is intended for readers with a good knowledge of Linux server management, computer networks, and the X-Road functioning principles.

## References

1. [UG-CS] Cybernetica AS. X-Road 6. Central Server User Guide
2. [IG-SS] Cybernetica AS. X-Road 6. Security Server Installation Guide
3. [UG-SS] Cybernetica AS. X-Road 6. Security Server User Guide
4. [IG-CSHA] Cybernetica AS. X-Road 6. Central Server High Availability Installation Guide

# Installation

## Prerequisites to Installation

The central server software assumes an existing installation of the **Ubuntu 14.04** operating system, on an **x86-64bit** platform.

To provide management services, a security server is installed alongside the central server.

The central server’s software can be installed both on physical and virtualized hardware (of the latter, Xen and Oracle VirtualBox have been tested).

**Note:** If the central server is a part of a cluster for achieving high availability, the database cluster must be installed and configured before the central server itself can be installed. Please refer to the Central Server High Availability Installation Guide [IG-CSHA] for details.

## Reference Data

*Note*: The information in empty cells will be determined at the latest during the server’s installation, by the person performing the installation.

**Caution**: Data necessary for the functioning of the operating system is not included.

|  |  |  |  |
| --- | --- | --- | --- |
| Ref |  | | Explanation |
| 1.0 | Ubuntu 14.04, 64-bit  2 GB RAM, 3 GB free disk space | | Minimum requirements |
| 1.1 | http://x-road.eu/packages | | X-Road package repository |
| 1.2 | http://x-road.eu/packages/xroad\_repo.gpg | | The repository key |
| 1.3 |  | | Account name in the user interface |
| 1.4 | TCP 4001 | service for authentication certificate  registration | Ports for inbound connections (from the external network to the central server) |
| TCP 80 | distribution of the global configuration |
| 1.5 | TCP 80 | software updates | Ports for outbound connections (from the central server to the external network) |
| 1.6 | TCP 80 | HTTP between the central server and the management services' security server | Internal network ports, the user interface port, and management service ports for the management services' security server |
| TCP 4000 | user interface |
| TCP 4001 | HTTPS between the central server and the management services' security server |
| TCP 4400 | HTTP between central server and management services' security server |
| 1.7 |  | | central server internal IP address(es) and hostname(s) |
| 1.8 |  | | central server public IP address, NAT address |
| 1.9 | <by default, the server’s IP addresses and names are added to the certificate’s Distinguished Name (DN) field> | | Information about the user interface TLS certificate |
| 1.10 | <by default, the server’s IP addresses and names are added to the certificate’s Distinguished Name (DN) field> | | Information about the services TLS certificate |

## Requirements to the Central Server

Minimum recommended hardware parameters:

* the server hardware (motherboard, CPU, network interface cards, storage system) must be supported by Ubuntu 14.04 in general;
* a 64-bit dual-core Intel, AMD or compatible CPU;
* 2 GB RAM;
* 100 Mbps network interface card.

Requirements for software and settings:

* an installed and configured Ubuntu 14.04 LTS x86-64 operating system;
* the necessary connections are allowed in the firewall (reference data: 1.4; 1.5; 1.6),
* if the central server has a private IP address, a corresponding NAT record must be created in the firewall (reference data: 1.8).

## Preparing OS

* Add a system user (reference data: 1.3) whom all roles in the user interface are granted to. Add the new user with the command:

sudo adduser username

User roles are discussed in detail in the X-Road Security Server User Guide [UG-SS]

* Set the operating system locale. Add the following line to the file /etc/environment.

LC\_ALL=en\_US.UTF-8

## Installation

Add the addresses of the X-Road package repository (reference data: 1.1), and the *nginx* and *opendjdk* repositories to the file /etc/apt/sources.list.d/xroad.list

deb http://x-road.eu/packages trusty main

deb http://ppa.launchpad.net/nginx/stable/ubuntu trusty main

deb http://ppa.launchpad.net/openjdk-r/ppa/ubuntu trusty main

Add the signing keys of the X-Road and external repositories to the list of trusted keys (reference data: 1.2):

curl http://x-road.eu/packages/xroad\_repo.gpg | sudo apt-key add –

sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys \ 00A6F0A3C300EE8C

sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys \ EB9B1D8886F44E2A

Issue the following commands to install the central server packages:

sudo apt-get update

sudo apt-get install xroad-centralserver

Upon the first installation of the central server software, the system asks for the following information.

* Account name for the user who will be granted the rights to perform all activities in the user interface (reference data: 1.3).
* The Distinguished Name of the owner of the user interface self-signed TLS certificate (*subjectDN*) and its alternative names (*subjectAltName*). The certificate is used for securing connections to the user interface (reference data: 1.7; 1.9).  
  The name and IP addresses detected from the operating system are suggested as default values.
  + The certificate owner’s Distinguished Name must be entered in the format:

/CN=server.domain.tld

* + All IP addresses and domain names in use must be entered as alternative names in the format:

IP:1.2.3.4,IP:4.3.2.1,DNS:servername,DNS:servername2.domain.tld

* Identification of the TLS certificate that is used for securing the HTTPS access point used for providing management services (reference data: 1.7; 1.10).  
  The name and IP addresses detected from the operating system are suggested as default values.

ATTENTION: The central server IP address or DNS name that security servers will use to connect to the server must be added to the certificate owner’s Distinguished Name (*subjectDN*) or alternative name forms (*subjectAltName*) list (reference data: 1.8).

* + The certificate owner’s Distinguished Name must be entered in the format:

/CN=server.domain.tld

* + All IP addresses and domain names in use must be entered as alternative names in the format:

IP:1.2.3.4,IP:4.3.2.1,DNS:servername,DNS:servername2.domain.tld

## Installing the Support for Hardware Tokens

To configure support for hardware security tokens (smartcard, USB token, Hardware Security Module), act as follows.

1. Install the hardware token support module using the following command:

sudo apt-get install xroad-addon-hwtokens

1. Install and configure a PKCS#11 driver for the hardware token according to the manufacturer's instructions.
2. Add the path to the PKCS#11 driver to the file /etc/xroad/devices.ini (as described in the example given in the file).
3. After installing and configuring the driver, the xroad-signer service must be restarted:

sudo service xroad-signer restart

## Installing the Support for Monitoring

The optional configuration for monitoring parameters is taken into use by installing package xroad-securityserver-monitoring. This package also includes the components that validate the updated xml monitoring configuration.

sudo apt-get install xroad-centralserver-monitoring

After installing the package the central monitoring client may be configured as specified in the [UG-CS].

# Initial Configuration

## Reference Data

*Note*: The information in empty cells will be entered at the latest during the installation, by the person performing the installation.

**Attention**: Data necessary for the functioning of the operating system is not included.

|  |  |  |
| --- | --- | --- |
| Ref |  | Explanation |
| 2.1 |  | The X-Road instance identifier |
| 2.2 |  | The external DNS name or IP address of the central server |
| 2.3 |  | The softtoken PIN |
| 2.4 |  | Codes and descriptions of the member classes used in the X-Road instance |

## Initialising the Central Server

The central server user interface can be accessed at https://CENTRALSERVER:4000/ (**reference data: 1.7; 1.6**)

* Set the X-Road instance identifier (**reference data: 2.1).**
* Set the central server public DNS hostname or public IP address (**reference data: 2.2).**
* Set the PIN of the software token **(reference data: 2.3)**. The PIN will be used to protect the keys stored in the software token. The PIN must be stored in a secure place, because it will be no longer possible to use or recover the private keys in the token once the PIN is lost.

## Configuring the Central Server and the Management Services' Security Server

Upon the first configuration of the central server and the management services' security server, the following actions must be carried out.

The actions that must be performed in the management services' security server are marked with yellow background.

1. Generate the internal and external configuration signing keys. Refer to [UG-CS] section „Generating a Configuration Signing Key“.
2. Configure the member classes. Refer to [UG-CS] section „Managing the Member Classes“. **(reference data: 2.4)**.
3. Configure the management service provider:
   * add the X-Road member who will be responsible for management services - [UG-CS] section „Adding a Member“;
   * add the subsystem that will provide the management services to the X-Road member - [UG-CS] section “Adding a Subsystem to an X-Road Member”;
   * appoint the subsystem as the management service provider - [UG-CS] section “Appointing the Management Service Provider”.
4. Configure the certification services. Refer to [UG-CS] section „Managing the Approved Certification Services“.
5. Configure the timestamping services. Refer to [UG-CS] section „Managing the Approved Timestamping Services“.
6. Verify that the global configuration generation succeeds (no global error messages should be displayed in the user interface at this point) and download the internal configuration anchor - [UG-CS] section “Downloading the Configuration Anchor”. The anchor is needed to set up the management services' security server.
7. Install and configure the management services' security server as described in [IG-SS].
8. Register the management services' security server in the central server. Refer to [UG-SS] section „Security Server Registration“.
9. Complete the registration of the management services' security server - [UG-CS] section “Registering a Member's Security Server”.
10. Register the management service provider as a client of the management services' security server - [UG-CS] section “Registering the Management Service Provider as a Security Server Client”.
11. Add the management service provider as a client to the management services' security server. Refer to [UG-SS] section „Adding a Security Server Client”. (The client should appear in “Registered” state, as the association between the client and the security server was already registered in the central server in the previous step). If necessary, configure the signing keys and certificates for the client - [UG-SS] section „Configuring a Signing Key and Certificate for a Security Server Client”
12. Configure the management services. Refer to [UG-CS] section „Configuring the Management Services in The Management Services’ Security Server”.

# Installation Error Handling

## Cannot Set LC\_ALL to Default Locale

If running the locale command results in the error message

locale: Cannot set LC\_ALL to default locale: No such file or directory,

then the support for the particular language has not been installed. To install it, run the command (example uses the English language):

sudo apt-get install language-pack-en

Then, to update the system’s locale files, run the following commands (this example uses the US locale):

sudo locale-gen en\_US.UTF-8

sudo update-locale en\_US.UTF-8

Set the operating system locale. Add following line to /etc/environment file.

LC\_ALL=en\_US.UTF-8

After updating the system’s locale settings, it is recommended to restart the operating system.

## PostgreSQL Is Not UTF8 Compatible

If the central server installation is aborted, with the error message

postgreSQL is not UTF8 compatible ,

then the PostgreSQL package is installed with the wrong locale. One way to fix it is to remove the data store created upon the PostgreSQL installation and recreate it with the correct encoding.

WARNING: All data in the database will be erased!

sudo pg\_dropcluster --stop 9.3 main

LC\_ALL="en\_US.UTF-8" sudo pg\_createcluster --start 9.3 main

To complete the interrupted installation, run the command:

sudo apt-get -f install

## Could Not Create Default Cluster

If the following error message is displayed during PostgreSQL installation

Error: The locale requested by the environment is invalid.

Error: could not create default cluster. Please create it manually with pg\_createcluster 9.3 main –start ,

use the following command to create the PostgreSQL data cluster:

LC\_ALL="en\_US.UTF-8" sudo pg\_createcluster --start 9.3 main

The interrupted installation can be finished using

sudo apt-get -f install

## Is Postgres Running On Port 5432?

If the following error message appears during installation

Is postgres running on port 5432 ?

Aborting installation! please fix issues and rerun with apt-get -f install ,

then check if any of the following errors occurred during the installation of PostgreSQL.

* Error installing the data cluster. Refer to section 4.3.
* The PostgreSQL data cluster installed during the installation of the security server is not configured to listen on port 5432. To verify and configure the listening port, edit the PostgreSQL configuration file in /etc/postgresql/9.3/main/postgresql.conf. If you change the listening port, the postgresql service must be restarted.

The interrupted installation can be finished using

sudo apt-get -f install