



|  |
| --- |
| X-Road: System Parameters  User Guide |
| Version: 2.9  28.1.2016  23 pages  Doc. ID: UG-SYSPAR |

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 29.05.2015 | 1.0 | First draft | Siim Annuk |
| 01.06.2015 | 1.1 | Some corrections done, typos fixed | Siim Annuk |
| 30.06.2015 | 1.2 | Minor corrections done | Vello Hansen, Imbi Nõgisto |
| 26.08.2015 | 1.3 | Corrections regarding SQL done | Marju Ignatjeva |
| 09.09.2015 | 2.0 | Editorial changes made | Imbi Nõgisto |
| 11.09.2015 | 2.1 | Global configuration generation interval added | Martin Lind |
| 20.09.2015 | 2.2 | Editorial changes made | Imbi Nõgisto |
| 23.09.2015 | 2.3 | Warning added about changing system parameters | Siim Annuk |
| 24.09.2015 | 2.4 | Note added about setting the *timeStampingIntervalSeconds* system parameter | Siim Annuk |
| 07.10.2015 | 2.5 | Default value of the parameter *acceptable-timestamp-failure-period* set to 14400 | Kristo Heero |
| 8.12.2015 | 2.6 | New parameters for configuring signature algorithms and key length, proxy client-side TLS protocols, and software token pin policy | Jarkko Hyöty |
| 8.12.2015 | 2.7 | Added parameters for toggling SOAP body logging on/off | Janne Mattila |
| 17.12.2015 | 2.8 | Added monitoring parameters | Ilkka Seppälä |
| 28.1.2016 | 2.9 | Added configuration client admin port | Ilkka Seppälä |

Table of Contents

[1 Introduction 5](#_Toc433278602)

[1.1 References 5](#_Toc433278603)

[2 Changing the System Parameter Values 6](#_Toc433278604)

[2.1 Changing the System Parameter Values in Configuration Files 6](#_Toc433278605)

[2.2 Changing the System Parameter Values in the Central Server Database 6](#_Toc433278606)

[2.3 Changing the Global Configuration Generation Interval in the Central Server 7](#_Toc433278607)

[3 Security Server System Parameters 9](#_Toc433278608)

[4 Central Server System Parameters 13](#_Toc433278609)

[4.1 System Parameters in the Configuration File 13](#_Toc433278610)

[4.2 System Parameters in the Database 14](#_Toc433278611)

[4.3 Global Configuration Generation Interval Parameter 15](#_Toc433278612)

[5 Configuration Proxy System Parameters 17](#_Toc433278613)

License

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-sa/3.0/.

# Introduction

This document describes the system parameters of the X-Road components – of the security server (chapter 3), the central server (chapter 4) and the configuration proxy (chapter 5). Additionally, changing the default values of the system parameters is explained (chapter 2).

## References

1. [INI] INI file, <http://en.wikipedia.org/wiki/INI_file>
2. [CRON] Quartz Scheduler CRON expression, [http://www.quartz-scheduler.org/generated/2.2.1/html/qs-all/#page/Quartz\_Scheduler\_Documentation\_Set%2Fco-trg\_crontriggers.html](http://www.quartz-scheduler.org/generated/2.2.1/html/qs-all/" \l "page/Quartz_Scheduler_Documentation_Set%2Fco-trg_crontriggers.html)

# Changing the System Parameter Values

The system parameters specify various characteristics of the system, such as port numbers, timeouts and paths to files on disk. The system parameters of the X-Road components are mainly stored in configuration files. Additionally, X-Road central server stores some system parameters in the database.

**Changing the values of the system parameters is strongly discouraged, since it may cause unexpected system behaviour.**

## Changing the System Parameter Values in Configuration Files

The configuration files are INI files [INI], where each section contains parameters for a particular server component.

In order to override the default values of system parameters, create or edit the file

/etc/xroad/conf.d/local.ini

Each system parameter affects a specific server component. To change the value of a system parameter, a section for the affected component must be created in the INI file. The name-value pairs of the system parameters for that component are written under the section, one pair per line.

The following format is used for the sections:

[ServerComponent]

SystemParameterName1=Value1

SystemParameterName2=Value2

For example, to configure the parameter *client-http-port* for the *proxy* component, the following lines must be added to the configuration file:

[proxy]

client-http-port=1234

Multiple parameters can be configured under the same section:

[proxy]

client-http-port=1234

server-listen-port=20000

**NB! Changing the parameter values in the configuration files requires restarting of the server.**

**WARNING! The value of the parameter is not validated, thus care must be taken when changing the value. For example, setting the port number to a non-numeric value in the configuration will cause the system to crash.**

## Changing the System Parameter Values in the Central Server Database

The central server database can be accessed with the psql utility using the following command (password: *centerui*):

psql -U centerui -h localhost centerui\_production

The default value of a system parameter can be overridden by adding the parameter name and value to the *system\_parameters* table:

INSERT INTO system\_parameters (key, value, created\_at, updated\_at)

VALUES ('*parameter\_name*', '*parameter\_value*',

(now() at time zone 'utc'), (now() at time zone 'utc'));

To edit the value of a system parameter already inserted into the *system\_parameters* table:

UPDATE system\_parameters

SET value = '*parameter\_value*', updated\_at = (now() at time zone 'utc')

WHERE key = '*parameter\_name*';

To restore the default value of a system parameter, delete the parameter from the *system\_parameters* table:

DELETE FROM system\_parameters

WHERE key = '*parameter\_name*';

**NB! Modifying or deleting system parameters other than the ones listed in section** 4.2 **will cause the system to crash.**

## Changing the Global Configuration Generation Interval in the Central Server

In order to override the default value of the global configuration generation interval, edit the cron expression[[1]](#footnote-2) HYPERLINK "http://www.quartz-scheduler.org/documentation/quartz-1.x/tutorials/crontrigger" in the file

/etc/cron.d/xroad-center

The default contents of the file are the following:

#!/bin/sh

**\* \* \* \* \*** xroad curl http://127.0.0.1:8084/managementservice/gen\_conf 2>&1 >/dev/null;

**NB!** Global configuration generation interval must be modified with extreme care. Misuse of the global configuration generation interval may hinder the operation of the whole X-Road instance.

The configuration generation interval must be shorter than the value of global configuration expiration interval (*confExpireIntervalSeconds*, see section 4.2), or else the configuration downloaded by the configuration clients (security servers or configuration proxies) will always expire before valid configuration becomes available. It is highly recommended that the global configuration generation interval is multiple times smaller than the global configuration expiration interval.

# Security Server System Parameters

This chapter describes the system parameters used by the components of the X-Road security server. For instructions on how to change the parameter values, see section 2.1.

| **Server component** | **Parameter** | **Default value** | **Explanation** |
| --- | --- | --- | --- |
| common | configuration-path | /etc/xroad/globalconf/ | Absolute path to the directory where global configuration is stored. |
| common | temp-files-path | /var/tmp/xroad/ | Absolute path to the directory where temporary files are stored. |
| common | default-signature-algorithm | SHA1withRSA | Global default digital signature algorithm. Possible values:   * SHA1withRSA * SHA256withRSA * SHA384withRSA * SHA512withRSA   (since version 6.7) |
| proxy | client-http-port | 80  8080 (RHEL) | TCP port on which the service client's security server listens for HTTP requests from client applications. |
| proxy | client-https-port | 443  8443 (RHEL) | TCP port on which the service client's security server listens for HTTPS requests from client applications. |
| proxy | client-timeout | 300000 | Defines the time period (in milliseconds), for which the service client's security server waits for a response from the service provider's security server. When the timeout is reached, the service client's security server informs the service client's information system that a service timeout has occurred. |
| proxy | configuration-anchor-file | /etc/xroad/configuration-anchor.xml | Absolute file name of the configuration anchor that is used to download global configuration. |
| proxy | connector-host | 0.0.0.0 | IP address on which the service client's security server listens for connections from client applications. The value 0.0.0.0 allows listening on all IPv4 interfaces. |
| proxy | database-properties | /etc/xroad/db.properties | Absolute file name of the properties file for the configuration of the security server database. |
| proxy | enforce-token-pin-policy | false | Controls enforcing the token pin policy. When set to true, software token pin is required to be at least 10 ASCII characters from at least tree character classes (lowercase letters, uppercase letters, digits, special characters).  (since version 6.7.7) |
| proxy | ocsp-cache-path | /var/cache/xroad | Absolute path to the directory where the cached OCSP responses are stored. |
| proxy | ocsp-responder-listen-address | 0.0.0.0 | IP address on which the service provider's security server listens for requests for OCSP responses from the service client's security server. The service client's security server downloads OCSP responses from the service provider's security server while establishing a secure connection between the security servers. The value 0.0.0.0 allows listening on all IPv4 interfaces. Must match the value of proxy.server-listen-address. |
| proxy | ocsp-responder-port | 5577 | TCP port on which the service provider's security server listens for requests for OCSP responses from the service client's security server. The service client's security server downloads OCSP responses from the service provider's security server while establishing a secure connection between the security servers. |
| proxy | server-listen-address | 0.0.0.0 | IP address on which the service provider's security server listens for connections from the service client's security servers. The value 0.0.0.0 allows listening on all IPv4 interfaces. |
| proxy | server-listen-port | 5500 | TCP port on which the service provider's security server listens for connections from the service client's security server. |
| proxy | server-port | 5500 | Destination TCP port for outgoing queries in the service client's security server. |
| proxy | jetty-clientproxy-configuration-file | /etc/xroad/jetty/clientproxy.xml | Absolute filename of the Jetty configuration file for the service client's security server. For more information about configuring Jetty server, see https://wiki.eclipse.org/Jetty/Reference/jetty.xml\_usage. |
| proxy | jetty-serverproxy-configuration-file | /etc/xroad/jetty/serverproxy.xml | Absolute filename of the Jetty configuration file for the service provider's security server. For more information about configuring Jetty server, see https://wiki.eclipse.org/Jetty/Reference/jetty.xml\_usage. |
| proxy | ssl-enabled | true | If true, TLS is used for connections between the service client's and service provider's security servers. |
| proxy | client-tls-ciphers | See [[2]](#footnote-3) | TLS ciphers enabled on the client-side interfaces (for both incoming and outgoing requests).  (since version 6.7) |
| proxy | client-tls-protocols | TLSv1.2,TLSv1.1 | TLS protocols enabled on the client-side interfaces (for both incoming and outgoing requests)  (since version 6.7) |
| proxy | server-conf-cache.period | 60 | ServerCionf database cache period. Tells how long (in seconds) ServerConf database values *getTspUrl, getMemberStatus and getIsAuthentication* are cached in security server memory.  It should be noted that when changing those values in the security server ui, they are effective only after the cache period. According to tests, increasing the cache period from 60 seconds, does not necessarily improve performance. Smaller period might be give rather good performance in some situations. However, performance with cache is much better than without.  (since version 6.9) |
| signer | client-timeout | 15000 | Signing timeout in milliseconds. |
| signer | device-configuration-file | /etc/xroad/signer/devices.ini | Absolute filename of the configuration file of the signature creation devices. |
| signer | key-configuration-file | /etc/xroad/signer/keyconf.xml | Absolute filename of the configuration file containing signature and authentication keys and certificates. |
| signer | port | 5556 | TCP port on which the signer process listens. |
| signer | key-length | 2048 | Key length for generating authentication and signing keys  (since version 6.7) |
| signer | csr-signature-algorithm | (see common.default-signature-algorithm) | Certificate Signing Request signature algorithm. If not specified, same as common default.  (since version 6.7) |
| anti-dos | enabled | true | Flag for enabling or disabling the AntiDOS system. |
| anti-dos | max-cpu-load | 1.1 | Maximum allowed CPU load for accepting new connections. If set to > 1.0, then CPU load is not checked. |
| anti-dos | max-heap-usage | 1.1 | Specifies the maximum allowed Java heap usage when accepting new connections. If set to > 1.0, then heap usage is not checked. |
| anti-dos | max-parallel-connections | 5000 | Maximum number of parallel connections for AntiDOS. |
| anti-dos | min-free-file-handles | 100 | Minimum amount of free file handles in the system for accepting new connections. At least one free file handle must be available to accept a new connection. |
| configuration-client | port | 5665 | TCP port on which the configuration client process listens. |
| configuration-client | update-interval | 60 | Global configuration download interval in seconds. |
| configuration-client | admin-port | 5675 | TCP port on which the configuration client process listens for admin commands. |
| message-log | soap-body-logging | true (overridden to false in Finnish installation) | Whether SOAP body of the messages should be logged or not.  If true, SOAP messages are logged in original form. If false, SOAP body is cleared of its contents and only has an empty child element inside it. As a side effect, details such as formatting and namespace labels of the xml message can be changed and new elements may be introduced for default values in SOAP header.  Removal of SOAP body is usually done for confidentiality reasons (body contains data that we do not want to have in the logs).  Note that changing the message this way prevents verifying its signature with the asicverifier tool. |
| message-log | enabled-body-logging-local-producer-subsystems |  | Subsystem-specific overrides for SOAP body logging when soap-body-logging = false.  This parameter defines logging for **local producer** subsystems, that is, our subsystems that produce some service which external clients use.  Comma-separated list of client identifiers for which SOAP body logging is enabled. For example FI/ORG/1710128-9/SUBSYSTEM\_A1, FI/ORG/1710128-9/SUBSYSTEM\_A2 where   * FI = x-road instance * ORG = member class * 1710128-9 = member code * SUBSYSTEM\_A1 = subsystem code   This parameter can only be used on subsystem-level, it is not possible to configure SOAP body logging per member.  If a subsystem has forward slashes “/” in for example subsystem code, those subsystems can’t be configured with this parameter. |
| message-log | enabled-body-logging-remote-producer-subsystems |  | Subsystem-specific overrides for **remote producer** subsystems, that is, remote subsystems that produce services which we use.  Parameter is used when soap-body-logging = false. |
| message-log | disabled-body-logging-local-producer-subsystems |  | Same as enabled-body-logging-local-producer-subsystems, but this parameter is used when soap-body-logging = true. |
| message-log | disabled-body-logging-remote-producer-subsystems |  | Same as enabled-body-logging-remote-producer-subsystems, but this parameter is used when soap-body-logging = true. |
| message-log | acceptable-timestamp-failure-period | 14400 | Defines the time period (in seconds) for how long is time-stamping allowed to fail (for whatever reasons) before the message log stops accepting any more messages (and consequently the security server stops accepting requests). Set to 0 to disable this check. The value of this parameter should not be greater than the value of the central server system parameter *timeStampingIntervalSeconds.* |
| message-log | archive-interval | 0 0 0/6 1/1 \* ? \* | CRON expression [CRON] defining the interval of archiving the time-stamped messages. |
| message-log | archive-max-filesize | 33554432 | Maximum size for archived files in bytes. Reaching the maximum value triggers file rotation. |
| message-log | archive-path | /var/lib/xroad | Absolute path to the directory where time-stamped log records are archived. |
| message-log | clean-interval | 0 0 0/12 1/1 \* ? \* | CRON expression [CRON] for deleting any time-stamped and archived records that are older than *message-log.keep-records-for* from the database. |
| message-log | hash-algo-id | SHA-512 | The algorithm identifier used for hashing in the message log.  Possible values are   * SHA-224, * SHA-256, * SHA-384, * SHA-512. |
| message-log | keep-records-for | 30 | Number of days to keep time-stamped and archived records in the database of the security server. If a time-stamped and archived message record is older than this value, the record is deleted from the database. |
| message-log | timestamp-immediately | false | If true, the time-stamp is created synchronously for each request message. This is a security policy requirement to guarantee the time-stamp at the time of logging the message. |
| message-log | timestamp-records-limit | 10000 | Maximum number of message records to time-stamp in one batch. |
| monitor | port | 2552 | TCP port number used in communications with xroad-proxy and xroad-monitor components. |

# Central Server System Parameters

The system parameters described in this chapter are used by the X-Road central server, except for the parameters *ocspFreshnessSeconds* and *timeStampingIntervalSeconds.*

The values of *ocspFreshnessSeconds* and *timeStampingIntervalSeconds* are distributed to the security servers via the global configuration. These parameters determine the interval of calling OCSP responder services and time-stamping services (respectively) by the security servers.

## System Parameters in the Configuration File

For instructions on how to change the parameter values, see section 2.1.

| **Server component** | **Name** | **Default value** | **Description** |
| --- | --- | --- | --- |
| common | temp-files-path | /var/tmp/xroad/ | Absolute path to the directory where temporary files are stored. |
| center | conf-backup-path | /var/lib/xroad/backup/ | Absolute path to the directory where configuration backups are stored. |
| center | database-properties | /etc/xroad/db.properties | Absolute path to file where the properties of the database of the central server are stored. |
| center | external-directory | externalconf | Name of the signed external configuration directory that is distributed to the configuration clients (security servers and/or configuration proxies) of this and federated X-Road instances. |
| center | generated-conf-dir | /var/lib/xroad/public | Absolute path to the directory where both the private and shared parameter files are created for distribution. |
| center | internal-directory | internalconf | Name of the signed internal configuration directory that is distributed to the configuration clients (security servers and/or configuration proxies) of this X-Road instance. |
| center | trusted-anchors-allowed | false | True if federation is allowed for this X-Road instance. |

## System Parameters in the Database

This section describes the system parameters used by the X-Road central server. For instructions on how to change the parameter values, see section 2.2.

| **Name** | **Value type** | **Default value** | **Description** |
| --- | --- | --- | --- |
| confExpireIntervalSeconds | integer | 600 | Time in seconds of the validity of the configuration after creation. |
| confHashAlgoUri | string | http://www.w3.org/2001/04/xmlenc#sha512 | URI of the algorithm used for calculating the hash values of the global configuration files.  Possible values are   * http://www.w3.org/2001/04/xmlenc#sha256, * http://www.w3.org/2001/04/xmlenc#sha512. |
| confSignAlgoId | string | SHA512withRSA | Identifier of the algorithm used for signing the global configuration.  Possible values are   * SHA256withRSA, * SHA384withRSA, * SHA512withRSA. |
| confSignCertHashAlgoUri | string | http://www.w3.org/2001/04/xmlenc#sha512 | URI of the algorithm used for calculating the hash value of the certificate used to sign the global configuration.  Possible values are   * http://www.w3.org/2001/04/xmlenc#sha256, * http://www.w3.org/2001/04/xmlenc#sha512. |
| ocspFreshnessSeconds | integer | 3600 | Defines the validity period (in seconds) for the OCSP responses retrieved from the OCSP responders. OCSP responses older than the validity period are considered expired and cannot be used for certificate verification.  Also, this parameter determines the interval of OCSP responder calls. To guarantee the sufficiently frequent refresh time for the OCSP responses, the OCSP responder call interval is set to ocspFreshnessSeconds/10 (with the restriction, that the responder call interval cannot be less than 5 seconds. |
| timeStampingIntervalSeconds | integer | 60 | Defines the interval of time-stamping service calls. Interval in seconds after which message log records must be timestamped. The interval must be between 60 and 86400 seconds. **Note: this value must be less than *ocspFreshnessSeconds.*** |

## Global Configuration Generation Interval Parameter

The global configuration generation interval parameter regulates the timing for global configuration generation. Global configuration generation is invoked by the Cron daemon[[3]](#footnote-4). The parameter is located at following file:

/etc/cron.d/xroad-center

The file is deployed during X-Road installation and by default has following content[[4]](#footnote-5):

#!/bin/sh

\* \* \* \* \* xroad curl http://127.0.0.1:8084/managementservice/gen\_conf 2>&1 >/dev/null;

The parameter regulating the timing of global configuration generation is the cron expression at the start of the last line (\* \* \* \* \*), which means that global configuration generation is invoked every minute by default.

# Configuration Proxy System Parameters

This chapter describes the system parameters used by the X-Road configuration proxy.

| **Server component** | **Name** | **Default value** | **Description** |
| --- | --- | --- | --- |
| configuration-proxy | address | 0.0.0.0 | The public IP or NAT address which is accessed for downloading the distributed global configuration. |
| configuration-proxy | configuration-path | /etc/xroad/configurationproxy/ | Absolute path to the directory containing the configuration files of the configuration proxy instance. |
| configuration-proxy | generated-conf-path | /var/lib/xroad/public | Absolute path to the public web server directory where the global configuration files that this configuration proxy generates are be placed for distribution. |
| configuration-proxy | signature-algorithm-id | SHA512withRSA | ID of the algorithm the configuration proxy uses when computing global configuration signatures.  The possible values are   * SHA256withRSA, * SHA384withRSA, * SHA512withRSA. |
| configuration-proxy | hash-algorithm-uri | http://www.w3.org/2001/04/xmlenc#sha512 | URI that identifies the algorithm the configuration proxy uses when calculating hash values for the global configuration files.  The possible values are   * http://www.w3.org/2001/04/xmlenc#sha256, * http://www.w3.org/2001/04/xmlenc#sha512 |
| configuration-proxy | download-script | /usr/share/xroad/scripts/download\_instance\_configuration.sh | Absolute path to the location of the script that initializes the global configuration download procedure. |

1. See also http://www.quartz-scheduler.org/documentation/quartz-1.x/tutorials/crontrigger. [↑](#footnote-ref-2)
2. Default value for proxy.client-tls-ciphers.

   TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384, TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256, TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA, TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

   (see [https://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider](https://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html" \l "SunJSSEProvider) for possible values)

   Note. OpenJDK 8 on RHEL 7 does not support ECDHE key agreement protocol, only DHE cipher suites are supported. [↑](#footnote-ref-3)
3. See also <http://linux.die.net/man/8/cron>. [↑](#footnote-ref-4)
4. For exact format specification see also <https://help.ubuntu.com/community/CronHowto>. [↑](#footnote-ref-5)