

CryptoServer

Troubleshooting

Imprint

Copyright 2024	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet e-mail	https://support.hsm.utimaco.com/ support@utimaco.com
Document Version	1.4.11
Product Version	6.0.0
Date	2024-10-23
Document No.	M011-0008-en
Status	PUBLISHED

All rights reserved	<p>No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems.</p> <p>Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. Any mention of the company name Utimaco in this documents refers to the Utimaco IS GmbH.</p> <p>All trademarks and registered trademarks are the property of their respective owners.</p>
---------------------	--

Table of Contents

1	Introduction	4
1.1	Document Conventions	4
2	Troubleshooting	6
2.1	Gathering Diagnostic Information	6
2.1.1	Gathering Diagnostic Information with CAT	6
2.1.2	Gathering Diagnostic Information with csadm	8
2.1.3	Gathering Diagnostic Information with CryptoServer LAN	8
2.2	Problem Analysis.....	9
2.2.1	The CryptoServer is in Maintenance Mode	9
2.2.2	Firmware Package not loading correctly	10
2.2.3	Problems with the Network	14
2.2.4	CryptoServer LAN does not Boot	15
2.3	Problem Analysis for PKCS#11	16
2.4	Problem Analysis for CSP/CNG Provider 1.x and 2.x.....	18
2.4.1	Logfile for CSP/CNG Provider 1.x	18
2.4.2	Logfile for CSP/CNG Provider 2.x	19
2.5	Problem Analysis for EKM	19
2.6	Problem Analysis for Java-based GUI Applications	20
3	Contacting Support	22
3.1	Providing Information for a CryptoServer PCIe	22
3.2	Providing Information for a CryptoServer LAN	22
3.3	Contact Address for Support Queries.....	23

1 Introduction

This manual is intended for administrators of the CryptoServer PCIe cards (referred to below as CryptoServer PCIe) and the network appliances CryptoServer LAN.

The manual contains useful information for analyzing and solving problems that might occur when the two products are in use. We use examples to show solutions to problems and problem analysis methods that can help you if problems occur. This manual should be used as a quick reference guide. For more in-depth information about the setup and functionality of the CryptoServer device, please refer to the respective Administration Manual.

1.1 Document Conventions

We use the following document conventions:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press OK
<code>Monospaced</code>	Code that is given for explanation or as an example, file paths	<code>chsm-create</code>
<i>Italic</i>	References and important terms	See <i>Sample Chapter</i> in the <i>CryptoServer - Sample Manual</i>

Table 1: Document conventions

We use special icons to highlight the most important notes and information.



Here, you find important safety information that should be followed.



Here, you find additional notes or supplementary information.



This message marks the result expected after the successful execution of an instruction.

2 Troubleshooting

2.1 Gathering Diagnostic Information

If a problem occurs whilst the CryptoServer is running, you can call a range of status information that may help you sort out the problem.

To view the most important status information, you can use CAT or csadm.

2.1.1 Gathering Diagnostic Information with CAT

If a problem occurs while the CryptoServer is running, you can call a range of status information that may help you sort out the problem.

To view the most important status information, perform the following steps:

1. Start CAT.
2. Click the **Show** menu.
3. Select **Diagnostics**.
 - The **Save Diagnostics** dialog box opens. The following diagnostic information is displayed:
 - The current date and time on the host computer when the diagnostics query was sent to the CryptoServer.
 - The CAT version
 - The address of the CryptoServer or the IP address of the CryptoServer LAN
 - The CryptoServer status
 - The boot log
 - Driver information (GetInfo)
 - The battery state of the carrier battery and the external battery
 - All files currently present on the CryptoServer
 - All active firmware modules on the CryptoServer
 - All users set up on the CryptoServer
 - Date and time on the CryptoServer

- The alarm log (only displayed if bootloader version ≤ 2.5 is loaded on the CryptoServer)
 - Information about the Master Backup Key that is saved on the CryptoServer
4. Click **Save**.
→ A dialogue box opens to determine the file location.
 5. Select the location, e.g., on your computer, for saving the file and enter an appropriate file name.
 6. Click **Save** to save the `.txt` file.
 7. Click **Cancel**.
→ The **Save Diagnostics** dialog box closes.
 8. Click the **Show** menu.
 9. Select **Audit Log**.
→ The **CryptoServer Audit Log** dialog box opens.
You can filter the display containing the log entries by users and by commands.
 10. Click **Save Log**.
→ A dialogue box opens to determine the file location.
 11. Select the location, e.g., on your computer, for saving the audit log and enter an appropriate file name.
 12. Click **Save** to save the `.log` file.
 13. Click **Close** to close the **CryptoServer Audit Log** dialog box



The diagnostic information has been retrieved and saved successfully and can be sent to Utimaco for further analysis.



To change the audit log configuration for showing more detailed logging information than provided by default, you must log in to the CryptoServer with at least authentication status 22000000, click the **Manage** menu and select **Audit Log Settings**.

2.1.2 Gathering Diagnostic Information with csadm

Perform the following csadm commands in a command prompt/shell and save the output in a text file to send it to the manufacturer Utimaco for problem analysis:

```
csadm [Dev=<device>] GetState
csadm [Dev=<device>] GetBootLog
csadm [Dev=<device>] GetAuditLog
csadm [Dev=<device>] GetInfo
csadm [Dev=<device>] GetBattState
csadm [Dev=<device>] ListFiles
csadm [Dev=<device>] ListFirmware
csadm [Dev=<device>] ListUser
csadm [Dev=<device>] GetTime
csadm [Dev=<device>] <Authentication> MBKListKeys
```

For csadm versions < 2.5.3, the command

```
csadm [Dev=<device>] <Authentication> MBKListKeys
```

does not need any authentication. In this case, replace this command by the following one:

```
csadm [Dev=<device>] MBKListKeys
```

2.1.3 Gathering Diagnostic Information with CryptoServer LAN

If you have a CryptoServer LAN, you can use the syslog and csxlan.log logfiles to help you with problem analysis. You can find these logfiles on the CryptoServer LAN in the `/var/log/` directory.

- All events relating to the system are recorded in the syslog.
- All events relating to the central control process are recorded in the log.

2.2 Problem Analysis

2.2.1 The CryptoServer is in Maintenance Mode

Normally, the CryptoServer only switches to Maintenance Mode after an alarm and remains in that mode until the alarm has been reset by a CryptoServer user with system administration permissions. However, there can also be other causes for the Maintenance Mode.

Possible cause: Firmware Modules not started correctly

When the CryptoServer was booted or restarted (reset), one of the essential firmware modules could not be started. In this case, it is not possible to operate the CryptoServer correctly and it changes to Maintenance Mode.

Possible solution 1: Restart the CryptoServer

Restart the CryptoServer:

- Using CAT: Click the **Manage** menu and select **Reboot CryptoServer**.
- Using csadm: In a command prompt/shell type `csadm Dev=<device> Restart` and press **ENTER**.

Possible solution 2: Reinstall Firmware Packages

If the CryptoServer is not in Operational Mode after a restart, follow these steps:

1. View the boot log file to determine what was started when the CryptoServer was switched on, and whether the essential firmware modules were initialized or not.
 - Using CAT: Click the **Show** menu and then click **Boot Log**. The boot log entries appear in the CAT information field.
 - Using csadm: In a command prompt/shell type `csadm Dev=<device> GetBootLog` and press **ENTER**.
The version of CryptoServer's operating system SMOS (Security Module Operating System) is shown and the module state is displayed as started.
The essential firmware modules should be listed in the Bootlog with their module ID (in hexadecimal format), module name and the comment `initialized successfully`.
If one of the firmware modules was not initialized successfully (e.g., due to dependencies to other firmware modules that could not be fulfilled), or is missing, the CryptoServer cannot be operated correctly.

2. Reinstall the firmware package from the product CD and ensure that all sensitive data (user and key databases) including the Master Backup Key is deleted in the CryptoServer.



Make sure to have prepared recent backups of all sensitive data and the MBK stored on the CryptoServer. Otherwise, they will be lost after loading the SecurityServer firmware package as mentioned above and you will not be able to import your sensitive data into the CryptoServer again. See the *CryptoServer – CAT Manual* and the *CryptoServer - csadm Manual* for detailed information about how to back up the CryptoServer databases storing the sensitive data.

- Using CAT: For detailed instructions see *Installing/Updating the Firmware* in the *CryptoServer - CAT Manual*.
 - Using csadm: Execute the following csadm command: `csadm Dev=<device> <Authentication> LoadPkg=<package>,ForceClear`
For details about the syntax of the `csadm LoadPkg` command see the csadm in-tool help or *LoadPkg* in the *CryptoServer - csadm Manual*.
3. Import the database backup into your CryptoServer by using CAT, see *Restoring Databases* in the *CryptoServer - CAT Manual*, or by using csadm, see *RestoreDatabase* in the *CryptoServer - csadm Manual*.

2.2.2 Firmware Package not loading correctly

Possible causes 1: Wrong Firmware Package

- You have a CryptoServer Se-Series Gen2 and have attempted to load a firmware package for the CSe-Series. The system displays an error message in this case.
- You have a CSe-Series CryptoServer and have attempted to load a firmware package for the CryptoServer Se-Series Gen2. The system displays an error message in this case.

Possible solution 1: Load correct Firmware Package

Load the appropriate firmware package into your CryptoServer. The firmware packages are provided on the SecurityServer/CryptoServer SDK product CD in `Firmware\SecurityServer-<Series>\` .

- If you have a CryptoServer Se-Series Gen2, load the SecurityServer package
`SecurityServer-Se2-Series-<version>.mpkg`.
- If you have a CryptoServer CSe-Series, load the SecurityServer package
`SecurityServer-CSe-Series-<version>.mpkg`.

Possible causes 2: Invalid Module Loaded

You have attempted to load a firmware package into the CryptoServer and receive the error message Invalid Package. This error message can only occur if you attempt to load a firmware package of your own.

Possible reasons for the error message:

- You have entered an incorrect file name for the firmware package.
- The package format version is incorrect.
- The number of files specified does not match the actual number of files in the `*.mpkg` file.
- The entered file size does not match the actual file size.
- The `.mpkg` file contains no firmware module.
The following file extensions are important here:
`.mmc` = Module Manufacturer Container
`.mtc` = Module Transport Container

Possible cause 3: Self-Programmed Firmware Modules signed with no Alternative Module Signature Key loaded

You have attempted to load a firmware package containing one or more self-programmed firmware modules into the CryptoServer. The public part of the Alternative Module Signature Key has not been imported yet into the CryptoServer. Therefore, the verification of the module signature fails.

Possible solution 3: Import Alternative Module Signature Key

1. Import the public part of the Alternative Module Signature Key into the CryptoServer.

Example:

```
csadm [Dev=<device>] LogonSign=ADMIN,:cs2:cjo:USB0  
LoadAltMdlSigKey=MyMdlSig.key
```

2. Load the firmware package or only the self-signed firmware module into the CryptoServer.

Example:

```
csadm [Dev=<device>] LogonSign=ADMIN,:cs2:cjo:USB0
```

```
LoadPkg=cs-1.2.2.0.mpkg,NoClear+NoDelete
```

or

```
csadm [Dev=<device>] LogonSign=ADMIN,:cs2:cjo:USB0 LoadFile=myMDL.mtc
```

3. Restart the CryptoServer for the new firmware to become effective.

Example:

```
csadm [Dev=<device>] Restart
```

Possible cause 4: Self-Programmed Firmware Modules signed with a wrong Alternative Module Signature Key

You have attempted to load a firmware package containing one or more self-programmed firmware modules into the CryptoServer that has/have been signed with a different Alternative Module Signature Key as the one that has been imported into the CryptoServer. Therefore, the verification of the module signature fails.

Possible solution 4: Sign Self-Programmed Firmware Modules with correct Alternative Module Signature Key

1. Sign the self-programmed firmware module with the same Alternative Module Signature Key as the one imported in the CryptoServer.

Example:

```
csadm Model=c86 MMCSignKey=c:\keys\MyMdlSig.key MakeMTC=c:\firmware\myMDL.out
```

2. Optionally, create your own firmware package containing Utimaco's standard firmware and your own firmware module.

Example:

```
csadm Pack=E:\cs\fw\fw_pkg\CS-Se2-1.2.3.4
```

The firmware package CS-Se2-1.2.3.4.mpkg is created.

3. Load your own firmware module/package into the CryptoServer.

Example:

```
csadm [Dev=<device>] LogonSign=ADMIN,:cs2:cjo:USB0 LoadPkg=CS-Se2-1.2.3.4.mpkg,NoClear+NoDelete
```

or

```
csadm [Dev=<device>] LogonSign=ADMIN,:cs2:cjo:USB0 LoadFile=myMDL.mtc
```

4. Restart the CryptoServer for the new firmware to become effective.

Example:

```
csadm [Dev=<device>] Restart
```

Possible cause 5: Self-Programmed Firmware Modules signed with correct Alternative Module Signature Key still fails

You have attempted to load a firmware package containing one or more self-programmed firmware modules into the CryptoServer. However, the verification of the module signature fails even though you have loaded the Alternative Module Signature Key used to sign your self-programmed firmware module.

Possible solution 5: Generate a new Alternative Module Signature Key and re-sign Self-Programmed Firmware Modules

Proceed as follows:

1. Generate a new Alternative Module Signature Key.

Example:

```
csadm KeyType=RSA GenKey=E:\cskeys\altMDLsig.key,2048,altMDLsigKey
```

2. Load its public part into the CryptoServer.

Example:

```
csadm [Dev=<device>] LogonSign=ADMIN,:cs2:cjo:USB0 LoadAltMdlSigKey= E:\cskeys\altMDLsig.key
```

3. Sign the self-programmed firmware module with the new Alternative Module Signature Key.

Example:

```
csadm Model=c86 MMCSignKey=E:\cskeys\altMDLsig.key MakeMTC=:\firmware\myMDL.out
```

4. Optionally, create your own firmware package containing Utimaco's standard firmware and your own2 firmware module.

Example:

```
csadm Pack=E:\cs\fw\fw_pkg\CS-Se2-1.2.3.4
```

5. Load your own firmware package into the CryptoServer.

Example:

```
csadm [Dev=<device>] LogonSign=ADMIN,:cs2:cjo:USB0 LoadPkg=CS-Se2-1.2.3.4.mpkg,ForceClear
```

or

```
csadm [Dev=<device>] LogonSign=ADMIN,:cs2:cjo:USB0 LoadFile=myMDL.mtc
```

6. Restart the CryptoServer for the new firmware to become effective.

Example:

```
csadm [Dev=<device>] Restart
```

2.2.3 Problems with the Network



If the reason for a problem with the Network is not immediately apparent, you can view the `syslog` and `csxlan.log` log files, which may contain information that helps you resolve the problem, see [Gathering Diagnostic Information with CryptoServer LAN \(p. 8\)](#).

Possible cause 1: Internet Protocols not supported

The CryptoServer LAN cannot be addressed over the network.

The CryptoServer LAN with operating system CSLANOS version 4.2.0 and later support the Internet Protocols IPv4 and IPv6.

Possible solution 1: Correct network settings on the LAN device

1. Use the menu options on the CryptoServer LAN to assign an IP address for the device.
2. Use the menu options on the CryptoServer LAN to assign the IP address of the default gateway.
3. Check whether you have connected the network cable to the network port connection (eth0 or eth1) for which you have specified an IP address.
4. Use the menu options on the CryptoServer LAN to enable the SSH daemon, if you want to configure the CryptoServer LAN via an SSH connection.
5. If you cannot address the CryptoServer LAN over the network after these actions, you can use the menu options on the CryptoServer LAN to send a PING to your Admin PC or from your Admin PC to your CryptoServer LAN.

For detailed descriptions of the CryptoServer LAN menu navigation, see *CryptoServer LAN V5 - Operating Manual*.

Possible cause 2: Standard port 288 cannot be reached

The standard port 288 cannot be reached. The possible reasons for this include problems with the routing, the firewall or the address conversion in IT networks (NAT).

Possible solution 2: Release port 288

Check the firewall rules. The default protocol is TCP.

Possible cause 3: Maximum number of permitted connections has been reached

The maximum number of permitted connections to the CryptoServer LAN (MaxConnections) has been reached. For the CryptoServer LAN with CryptoServer version $\geq 3.2.0$, we have set

MaxConnections, to 256. For CryptoServer LAN version $\geq 4.5.4$, we have set MaxConnections, to 4100.

Possible solution 3: Increase number of permitted connections

You must increase the maximum number of permitted connections (MaxConnections) in the `csxlan.conf` file. The following below is based on making changes to the `csxlan.conf` file via SSH-access with WinSCP for Windows.



The default system configuration of CSLANOS version 4.5.x and higher prohibits remote login for the root user via SSH connection.

To enable SSH-login for the user root, you should edit the configuration file for the SSH daemon `/etc/ssh/sshd_config` to change the default setting `PermitRootLogin no` to `PermitRootLogin yes`. Afterwards, the SSH daemon has to be reloaded for the setting to become effective (`/etc/init.d/sshd reload`).

Data required for SSH access:

Computer name or IP address	Name of the CryptoServer LAN/IP address of the CryptoServer LAN
Port number	22
User name	root
Password	utimaco

1. Start your SCP client (e.g. WinSCP) and open the `/etc` directory.
In this directory, you find the `csxlan.conf` (`/etc/csxlan.conf`).
2. Right-click on the file and select **Edit** from the context menu.
→ The `csxlan.conf` file opens.
3. For the CryptoServer LAN with CryptoServer version $\geq 3.2.0$ and CryptoServer LAN version $< 4.5.4$, increase the value set for the `MaxConnections=256` entry to the value you require. The value that you set here for `MaxConnections` should not be greater than 1000, as this can cause performance problems under some circumstances.
4. Save and close the `csxlan.conf` file.
5. Reboot your CryptoServer LAN so that the changed `csxlan.conf` file is used.

2.2.4 CryptoServer LAN does not Boot

Under some circumstances it is possible that the CryptoServer LAN does not boot and the mode Offline is displayed in the display.

Possible cause 1: Error in the file system

Due to an error in the file system, the current boot partition cannot be booted. One possible reason for this is that the flash memory has failed or that the number of write cycles has been exceeded.

Possible solution 1: Repair file system

1. Connect a keyboard and a screen to the CryptoServer LAN.
2. If there really is an error in the file system, you may see a prompt, in CSLANOS versions 3.0.0 to 3.0.4 of the CryptoServer LAN, asking whether you want the file system to be repaired. Answer **yes** to this prompt.
3. Alternatively, reboot your CryptoServer LAN and select a different boot partition.

Possible cause 2: Power Supply Unit is defect

As of CSLANOS version 4.1.0 the CryptoServer LAN has two power supplies. Hardware on the CryptoServer LAN, or one or both of the power supply units, are defective.

Possible solution 2: Exchange Power Supply Unit

If only one power supply unit is defective, contact the manufacturer Utimaco to order a new one and follow the instructions in *Removing/Swapping a Power Supply Module* in the *CryptoServer LAN V5 - Operating Manual*.

If both power supply units are defective, send the CryptoServer LAN back to the manufacturer Utimaco. Before you do so, please use our online portal to open a new RMA case <https://support.hsm.utimaco.com/support/rma/new>.

Possible cause 3: No connection to PCIe Card

The CryptoServer LAN cannot communicate with the mounted CryptoServer PCIe card.

Possible solution 3: Review Error Message

Connect a keyboard and a screen to the rear side of the CryptoServer LAN and check whether an error message has been generated.

2.3 Problem Analysis for PKCS#11

As from SecurityServer/CryptoServer SDK 3.2 product CD the PKCS#11 R2 (as from SecurityServer/CryptoServer SDK 4.40.0 product CD the PKCS#11 R3) implementation is supplied.

You may find useful information to help you solving any problems with PKCS#11 if you enable logging for PKCS#11. The system records information, errors and warnings in the `cs_pkcs11_R3.log` logfile. By default, no log entries are generated by the Utimaco PKCS#11 R3 API. This must be enabled in the `cs_pkcs11_R3.cfg` configuration file.



We recommend enabling logging for the Utimaco PKCS#11 R3 API for the purpose of problem analysis. After it is enabled, log entries will be generated from then on. This can result in considerable volumes of data.



The Utimaco PKCS#11 R3 API only generates log entries if PKCS#11 R3 is configured correctly.

On a computer with a Windows operating system, you will find the `cs_pkcs11_R3.cfg` configuration file after the installation of the CryptoServer host software here, by default:

`C:\ProgramData\Utimaco\PKCS11_R3\`

1. Use a text editor to open the `cfg` file.
2. To enable logging for Utimaco's PKCS#11 R3 interface, set the log level you require in the Global section by configuring the `Logpath` and `Logging` entry as shown in the following example:

```
[Global]
# Path to the logfile (name of logfile is attached by the API)
# For unix:
#Logpath = /tmp
# For windows:
Logpath = C:/tmp

# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 3
# Maximum size of the logfile in bytes (file is rotated with a backup file
if full)
Logsize = 10mb
```

The following table shows an overview of the different log levels and their meanings.

Name	Level	Description
NONE	0	No logging output will be produced (default)
ERROR	1	Log errors of the CryptoServer PKCS#11 library and CryptoServer firmware modules
WARNING	2	Log errors and warnings of the CryptoServer PKCS#11 library and CryptoServer modules
INFO	3	Log errors and warnings of the CryptoServer PKCS#11 library and CryptoServer firmware modules. Additionally, information of the CryptoServer PKCS#11 library will be logged.
TRACE	4	Log errors, warnings and information of the CryptoServer PKCS#11 library and CryptoServer firmware modules. Additionally, trace output like function calls will be logged.

Table 2: Logging levels

3. Save the cfg configuration file and close your text editor.



Delete the logfile as soon as it is no longer needed.

2.4 Problem Analysis for CSP/CNG Provider 1.x and 2.x

You may find useful information to help you if there are problems with CSP and CNG in the `cs2cng.log` logfile.

2.4.1 Logfile for CSP/CNG Provider 1.x

Up to SecurityServer/CryptoServer SDK 4.10, the CSP/CNG Provider 1.x has been provided.

By default, errors and warnings are recorded in the logfile.

1. Click **Start > All Programs > Utimaco > CryptoServer > CSP Configuration**.
→ The **CryptoServer CSP Configuration, Version <1.x.x>** dialog box opens.
2. Click **Settings**.
3. Click **View Log** button if you want to view the log entries, or click **>>** if you want to change the directory to which the logfile is saved.
4. Click a different log level to enable it, and click the **Apply** button if you want to change the default setting.
5. Click **OK**.
→ The **CryptoServer CSP Configuration, Version <1.x.x>** dialog box closes.

2.4.2 Logfile for CSP/CNG Provider 2.x

As from SecurityServer/CryptoServer SDK 4.10 the CSP/CNG Provider 2.x is provided.

The CSP/CNG Provider 2.x is configured with the `cs_cng.cfg` configuration file. The storage location for the configuration file is defined in the system environment variable `CS_CNG_CFG`, which is by default `C:\ProgramData\Utimaco\CNG`.

The logging along with other important settings is configured in the `cs_cng.cfg` configuration file. You can individually set the location for storing the logfile (`Logpath`) and the log level (`Logging`). By default, the log level setting is `Logging = 0`, i.e. no logging information is written. You can find the `cs2cng.log` logfile, by default, in the `C:\ProgramData\Utimaco\CNG\log` directory.

For detailed information about CSP/CNG 1.x and 2.x configuration, see *CryptoServer CSP and CryptoServer Key Storage Provider 1.x and 2.x Manual for System Administrators* provided on the delivered product CD in the `\Documentation\Administration Guides` directory.

2.5 Problem Analysis for EKM

You may find useful information to help you if there are problems with Extensible Key Management (EKM) in the EKM logfile. By default, the Utimaco EKM API generates log entries for log level 3.

You will find an example configuration file `cssqlek.m.cfg` in the following directory on your SQL Server: `C:\ProgramData\Utimaco\EKM`

1. Use a text editor to open the configuration file.
The top part of the `cssqlek.m.cfg` configuration file looks like this on your SQL Server:

```
This is a sample configuration file
# path to logfile
LogFile = C:/ProgramData/Utimaco/EKM/cssqlekm.log

# loglevel
LogLevel = 3
```

In the following table you will find an overview of the different log levels and their individual meanings.

0 = NONE	<i>No log entries are generated.</i>
1 = ERROR	Errors are recorded in the log file.
2 = WARNING	Warnings and errors are recorded in the log file. Contains log level 1.
3 = INFO	Information, warnings and errors are recorded in the log file. Contains log level 1 and 2.
4 = TRACE	All available information is recorded in the log file. Contains log level 1, 2 and 3.

If you want to enable a different log level, you must enter the appropriate number for the required log level value for LogLevel.



We recommend that you only enable logging from the Utimaco EKM API with log level 4 (TRACE) for the purpose of problem analysis and then to use the default setting (LogLevel = 3) again.

2. Save the `cssqlekm.cfg` and close your text editor.
3. Restart your SQL-Server.

2.6 Problem Analysis for Java-based GUI Applications

If you start a Java-based application (for example, CryptoServer Administration Tool (CAT) or P11CAT) on a Linux computer and an error according to the examples

```
java.lang.UnsatisfiedLinkError: /tmp/jcsapi6247226668792798062.so: /tmp/
jcsapi6247226668792798062.so: failed to map segment from shared object:
Operation not permitted
```

or

```
Caused by: java.lang.UnsatisfiedLinkError: /tmp/  
jcsapi7418373955164564681.so: /tmp/jcsapi7418373955164564681.so: Fehler  
beim Mappen des Shared Objects
```

occurs, the `XDG_RUNTIME_DIR` environment variable must be created and set to, for example, `/var/run` or `/run`. Then restart the Java-based application.

3 Contacting Support

To avoid unnecessary Support queries, refer to the respective product manuals. You can find detailed descriptions of all the most important and fundamental operating instructions and administration tasks in the manuals listed there.



The majority of support queries will be answered if you refer to the manuals listed in the Chapter "Other manuals", and carry out the performance- and solution-oriented administration steps described in them.

3.1 Providing Information for a CryptoServer PCIe

If you have a CryptoServer PCIe card and want to contact Utimaco's support, get the following information ready for us:

- Your customer or company name
- Give an exact description of the problem.
- Can the problem be reproduced?
- The version number of the product CD or of the SecurityServer package used.
The version number of the product CD is identical to the version number of the SecurityServer package that is supplied on the product CD.
- The Diagnostic Information, saved as a `.txt` file, see [Gathering Diagnostic Information \(p. 6\)](#).

3.2 Providing Information for a CryptoServer LAN

If you have a CryptoServer LAN and want to contact Utimaco's support, get the following information ready for us:

- The CryptoServer LAN's serial number.
 - You can find the CryptoServer LAN's serial number via the menu options on the front panel of the CryptoServer LAN.
CSLAN admin. > CSLAN Info > Show Version

- Alternatively, you can find the serial number on the right-hand side of the CryptoServer LAN.
- If you can only access the CryptoServer LAN remotely, execute the `csadm CSLGetSerial` command on your administration computer.
`csadm [Dev=<device>] CSLGetSerial`
For further details about this `csadm` command, read the corresponding chapter in the *CryptoServer - csadm Manual*.
- The CSLANOS and `dsp_admin` version number.
 - You can find out the `dsp_admin` version number via the menu options on the front panel the CryptoServer LAN.
CSLAN admin. > CSLAN Info > Show Version
 - If you can only access the CryptoServer LAN remotely, execute the `csadm CSLGetVersion` command on your administration computer.
`csadm [Dev=<device>] CSLGetVersion`
For further details about this `csadm` command, read the corresponding chapter in the *CryptoServer - csadm Manual*.
- Give an exact description of the problem.
- Can the problem be reproduced?
- The Diagnostic Information, saved as a .txt file.
To save the Diagnostic Information as a .txt file on your computer, see [Gathering Diagnostic Information \(p. 6\)](#). Additionally, provide the logfiles, see [Gathering Diagnostic Information with CryptoServer LAN \(p. 8\)](#).



The default system configuration of CSLANOS version 4.5.x and higher prohibits remote login for the root user via SSH connection.

To enable SSH-login for the user root, you should edit the configuration file for the SSH daemon `/etc/ssh/sshd_config` to change the default setting `PermitRootLogin no` to `PermitRootLogin yes`. Afterwards, the SSH daemon has to be reloaded for the setting to become effective (`/etc/init.d/sshd reload`).

3.3 Contact Address for Support Queries

If an error occurs while operating the CryptoServer, read [Troubleshooting \(p. 6\)](#) to solve it.

If the error still occurs, prepare information as described in [Providing Information for a CryptoServer PCIe \(p. 22\)](#) and [Providing Information for a CryptoServer LAN \(p. 22\)](#).

If you have any further questions on CryptoServer, feel free to contact us.

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Germanusstr. 4
52080 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

<https://support.hsm.utimaco.com/support/rma/new>

Other Support Queries

- Mail (preferred contact method)
support@utimaco.com¹
Attach the diagnostic information to your email.
- Web portal
<https://support.hsm.utimaco.com/support/cases/new/>
The diagnostic information will be requested in our response if necessary.
- By phone
AMERICAS +1-844-UTIMACO (+1 844-884-6226)
EMEA +49 800-627-3081
APAC +81 800-919-1301
The diagnostic information will be requested in our response if necessary.

¹ <mailto:support@utimaco.com>