CryptoServer LAN
CryptoServer

Troubleshooting

Imprint

Copyright 2016	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	+49 (0)241 / 1696-200
Fax	+49 (0)241 / 1696-199
Internet	http://hsm.utimaco.com
e-mail	hsm@utimaco.com
Document Version	1.1.1
Date	27.05.2016
Status	Final
Document No.	M011-0008-en
All Rights reserved	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. 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. All trademarks and registered trademarks are the property of their respective owners.

Table of Contents

1 Introduction 5

1.1 About this Manual 5

1.1.1 Target Audience for this Manual 5

1.1.2 Document Conventions 5

1.2 Other Manuals 6

2 Troubleshooting 8

2.1 General Problem Analysis 8

2.2 Problems with the Smartcards? 9

2.3 The CryptoServer Is in Maintenance Mode 9

2.4 Problems when Loading the Firmware Package? 11

2.5 General Problem Analysis for the Network 12

2.6 Problems with the Network? 12

2.7 CryptoServer LAN Does Not Boot? 14

2.8 Problem Analysis for PKCS#11 15

2.9 Problem Analysis for CSP and CNG 17

2.10 Problem Analysis for OpenSSL 17

2.11 Problem Analysis for EKM 18

3 Contacting Support 20

3.1 Do You Have a CryptoServer PCI or PCIe Expansion Card? 20

3.2 Do You Have a CryptoServer LAN? 21

3.3 Contact Address for Support Queries 21

1 Introduction

Thank you for purchasing our CryptoServer or CryptoServer LAN security system. We hope you are satisfied with our product. Please do not hesitate to contact us if you have any complaints or comments.

1.1 About this Manual

This manual contains useful information for analyzing or solving problems that might occur while the CryptoServer or the CryptoServer LAN are in use.

It uses examples to show you solutions to problems and problem analysis methods that can help you if problems occur.

1.1.1 Target Audience for this Manual

This manual is primarily designed to be used by administrators who are responsible for configuring the CryptoServer and CryptoServer LAN products.

1.1.2 Document Conventions

We use the following conventions in this manual:

Bold	Items of the Graphical User Interface (GUI), e. g. menu options
`Monospaced`	File names, folder and directory names, commands, file outputs, programming code samples
Italic	References and important terms

We have used icons to highlight the most important notes and information.

⚠ *Here you find important safety information that should be followed.*

ℹ *Here you find additional notes or supplementary information.*

1.2 Other Manuals

The CryptoServer is supplied as a PCI-Express (PCIe) plug-in card in the following series:

- CryptoServer CSe-Series
- CryptoServer Se-Series
- CryptoServer Se-Series Gen2

The CryptoServer LAN (appliance) is supplied in the following series:

- CryptoServer LAN CSe-Series
- CryptoServer LAN Se-Series
- CryptoServer LAN Se-Series Gen2

We provide the following manuals on the product CD for the CryptoServer PCIe CSe-, Se-Series and Se-Series Gen2 plug-in cards and for the CryptoServer LAN (appliance) CSe- and Se-Series:

Quick Start Guides

You will find these Manuals in the main folder of the SecurityServer product CD. They are available only in English, do not cover all possible scenarios, and are intended as a supplement to the product documentation provided on the SecurityServer product CD.

- *CryptoServer LAN - Quick Start Guide*
  If you are looking for step-by-step instructions on how to bring the CryptoServer LAN into service, how to prepare a computer (Windows 7) for the CryptoServer administration and how to start administrating your CryptoServer with the Java-based GUI CryptoServer Administration Tool (CAT), read this document.
- *CryptoServer PCIe - Quick Start Guide*
  If you are looking for step-by-step instructions on how to bring the CryptoServer PCIe plug-in card into service, how to install the CryptoServer driver on a computer with minimal RHEL 7.0 installation and how to start administrating your CryptoServer with the CryptoServer Command-line Administration Tool (csadm), read this document.

Manuals for System Administrators

You will find these manuals on the product CD in the following folder:
`…Documentation\Administration Guides\`

- *CryptoServer - Manual for System Administrators*
  If you need to administer a CryptoServer PCIe plug-in card or a CryptoServer LAN using the CryptoServer Administration Tool (CAT), read this manual. Furthermore, this manual provides a detailed description of the CryptoServer functions, required for the correct and effective operation of the product.

- *CryptoServer LAN - Manual for System Administrators*
  If you need to administer a CryptoServer LAN (appliance), read this manual. Since a CryptoServer plug-in card is integrated into the CryptoServer LAN, please read the C*ryptoServer - Manual for System Administrators*, as well.
- *CryptoServer LAN/CryptoServer - Troubleshooting*
  If problems occur while you are using a CryptoServer PCIe plug-in card or a CryptoServer LAN (appliance), read this manual.
- *CryptoServer LAN/ CryptoServer*
  PKCS#11 CryptoServer Administration Tool – Manual for System Administrators
  If you need to administer the PKCS#11 R2 interface with the PKCS#11 CryptoServer Administration Tool (P11CAT), read this manual.
- *CryptoServer LAN/CryptoServer*
  CryptoServer Command-line Administration Tool - csadm - Manual for System Administrators
  If you need to administer a CryptoServer PCIe plug-in card or a CryptoServer LAN using the CryptoServer Command-line Administration Tool (csadm), read this manual (only English version available).

Operating Manuals

You will find these manuals on the product CD in the following folder: `…Documentation\Operating Manuals\`. They contain all the necessary information for using the hardware of the CryptoServer PCIe plug-in card respectively the CryptoServer LAN (appliance).

2 Troubleshooting

The Troubleshooting Manual is intended for administrators of the CryptoServer (PCI and PCIe) and CryptoServer LAN (network variant of the CryptoServer) and contains information that they will find useful for analyzing or solving problems that might occur when the two products are in use.

In it we use examples to show you solutions to problems and problem analysis methods that can help you if problems occur.

This manual is a supplement to the manuals listed in the previous section, "Other manuals", for the CryptoServer and CryptoServer LAN products.

Consequently, we ask you always to refer to the other manuals if a problem affecting one of the two products, CryptoServer or CryptoServer LAN, occurs. You will find detailed descriptions of all the most important and fundamental operating instructions and administration tasks in these manuals.

2.1 General Problem Analysis

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:

1. Start the CryptoServer Administration Tool (CAT).
2. Go to the Show main menu item and click on the Diagnostics sub menu item.

   The following Diagnostic Information then appears in a separate window:

   - 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 (Get Info)
   - the battery status of the carrier battery and the external battery
   - all files currently present in the CryptoServer
   - all active firmware modules in the CryptoServer
   - all the users who are set up in the CryptoServer
   - date and time on the CryptoServer
   - the Alarm Log (only displayed if Bootloader version ≤ 2.5 is loaded in the CryptoServer).
   - information about the Master Backup Key that is saved in the CryptoServer

3. To send the Diagnostic Information to the manufacturer Utimaco for problem analysis, click Save and save the `*.txt` file on your computer.

Viewing the Audit Log

You can view the Audit Log in the CAT by selecting Show in the main menu and then selecting Audit Log.

You can filter the display containing the log entries by users and by commands.

If you want more detail than is provided in the entries displayed there, you can select more events, for display and saving in the Audit Log, by selecting Status in the main menu and then selecting items Logfile and then Audit Log Configuration.

If you want to process the Audit Log Configuration, you must log onto the CryptoServer with at least authentication status 22000000.

Viewing the syslog

If you have a CryptoServer LAN, you can use the `syslog` to help you with problem analysis. All events that relate to the system are recorded in the `syslog`. You will find the `syslog` file on the CryptoServer LAN, in `/var/log/syslog`.

Viewing the csxlan.log

If you have a CryptoServer LAN, you can use the `csxlan.log` to help you with problem analysis. All events that relate to the central control process, `csxlan.log`, are recorded in the `csxlan.log`. You will find the `csxlan.log` file on the CryptoServer LAN, in `//var/log/csxlan.log`.

2.2 Problems with the Smartcards?

If you do not use the REINER SCT PIN pad, this can cause problems with the TCOS 3.0 or JavaCard smartcards. You will recognize the TCOS 3.0 smartcards by the printed label TC30 on the front left side, and the JavaCard smartcards by the printed label JC10 on the front left side.

If you use the TCOS 3.0 or JavaCard smartcards, you must use the REINER SCT PIN pad supplied by Utimaco.

2.3 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 an Administrator. However, there can also be other causes for *Maintenance Mode*.

Possible cause:

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 solutions:

1. Restart the CryptoServer.

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

2. In the main window of the CAT, click the **Get Bootlog** button to determine what was started when the CryptoServer was switched on, and whether the essential firmware modules were initialized or not. The system displays the Bootlog directly in the main CAT window.

   SMOS is the operating system used by the CryptoServer.

   The following essential firmware modules should be listed in the Bootlog with the comment INITIALIZED:

   - SMOS (Small Multitasking Operating System)
   - HCE (Hardware Crypto Engine) only in the Se400 and Se1000 models
   - PKCS#11 (Public Key Cryptography Standards)
   - CXI (Cryptographic eXtended Interface)
   - VDES (DES algorithm)
   - PP (PIN Pad Driver)
   - CMDS (Command Scheduler) command processing and user management
   - VRSA (RSA algorithm)
   - SC (Smartcard Driver)
   - UTIL (utilities) access to the real time clock and random number generator
   - ADM Administration of firmware modules
   - DB database used to store keys and other data
   - HASH different hash algorithms
   - AES (AES algorithm)
   - DSA (Digital Signature Algorithm)
   - LNA (Long Number Arithmetic)
   - ECA (Elliptical Curve Algorithm)

- ▣ ASN1 (Abstract Syntax Notation One)
- ▣ MBK (Master Backup Key Management)
- ▣ NTP (Network Time Protocol)
- ▣ ECDSA (Elliptical Curve Algorithm, DSA)

If one of the firmware modules listed above was not initialized successfully, or is missing, the CryptoServer cannot be operated correctly.

3. Reinstall the firmware package from the product CD (New Installation) and ensure that all data including the Master Backup Key is deleted in the CryptoServer.
   If you select Update instead of New Installation, all data and the Master Backup Key (MBK) remains in the CryptoServer.

2.4 Problems when Loading the Firmware Package?

Possible causes:

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

Possible solution:

1. Load the appropriate firmware package into your CryptoServer.
   - ▣ If you have a CS Series CryptoServer, you must load the SecurityServer Package with the suffix `CS-Series`.
   - ▣ If you have a CSe Series CryptoServer, you must load the SecurityServer Package with the suffix `CSe-Series`.
   - ▣ If you have a Se Series CryptoServer, you must load the SecurityServer Package with the suffix `Se-Series`.

Possible causes:

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 Invalid Package:

- 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:

You have attempted to load a firmware package of your own, with an invalid digital signature, into the CryptoServer. An invalid cryptographic key has been used for the digital signature.

Possible solution:

Assign the correct digital signature to the firmware package and load it into the CryptoServer. To do so, follow these steps:

1. Generate an RSA key and save it either on a smartcard or as a key file.
2. Load the RSA key into the CryptoServer as an alternative Module Signing Key.
3. Use the "new" Module Signing Key to sign the firmware module.
4. Load the signed firmware module into the CryptoServer.

2.5 General Problem Analysis for 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.
All events that affect the system are recorded in the `syslog`.
All events that relate to the central control process, are recorded in the `csxlan.log`.

- You will find the `syslog` file on the CryptoServer LAN, in `/var/log/syslog)`.
- You will find the `csxlan.log` file on the CryptoServer LAN, in `/var/log/`.

2.6 Problems with the Network?

Possible cause:

From CryptoServer Version 4.2.0 onwards the Internet Protocols IPv4 and IPv6 are supported.

The CryptoServer LAN cannot be addressed over the network.

Possible solutions:

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.

Possible cause:

The standard port SG CS-LAN 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:

Release Port 288. Check the firewall rules. The default protocol is TCP.

Possible cause:

The maximum number of permitted connections to the CryptoServer LAN (`MaxConnections =20`) has been reached. For the CryptoServer LAN with CRYPTOSERVER Version ≥ 3.2.0 we have set the maximum number of connections, `MaxConnections`, to 256.

Possible solution:

You must increase the maximum number of permitted connections (`MaxConnections`) in the `csxlan.conf` file.

The description below is based on making changes to the `csxlan.conf` file with WinSCP for Windows.

The data required for SSH access is listed in the table below:

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 in it open the `/etc` folder.
   In this folder you will find the `csxlan.conf (/etc/csxlan.conf)`.
2. Open the `csxlan.conf` file by right-clicking on it, and selecting **Edit** from the context menu.
3. Increase the value set for the `MaxConnections=20` 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.

2.7 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:

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:

Connect a keyboard and a screen to the CryptoServer LAN. If there really is an error in the file system, you may see a prompt, in versions 3.0.0 to 3.0.4 of the CryptoServer LAN, asking whether you want the file system to be repaired. Answer **yes** at this prompt.

Possible solution:

Reboot your CryptoServer LAN and select a different boot partition.

Possible causes:

Hardware on the CryptoServer LAN, or one or both of the power supply units, are defective.

Possible solution:

From CryptoServer LAN Version 4.1.0 the CryptoServer LAN has two power supplies.

Send the CryptoServer LAN back to the manufacturer Utimaco in Aachen, Germany. Before you do so, please send an e-mail with a brief description of the problem to this e-mail address: RMA-@utimaco.de.

Possible causes:

The CryptoServer LAN cannot communicate with the PCI or the PCIe expansion card.

Possible solution:

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

2.8 Problem Analysis for PKCS#11

From version 3.0 of the Security Server product CD we supply two PKCS#11 implementations. The previous implementation is called PKCS#11, and the new one is called PKCS#11 R2.

This section describes possible problems with the PKCS#11 version.

You may find useful information to help you if there are problems with PKCS#11 if you enable logging for PKCS#11. The system records information, errors and warnings in the PKCS#11 log. By default, no log entries are generated by the Utimaco PKCS#11 API. This must be enabled in the `cs2_pkcs11.ini` configuration file.

⚠ *We recommend that you only enable logging for the Utimaco PKCS#11 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.

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

In a Windows system you will find the `cs2_pkcs11.ini` configuration file here, by default:
`C:\Program Files\Utimaco\CryptoServer\Lib\`

1. Use a text editor to open the `cs2_pkcs11.ini` file.

   The top, `Global` part of `cs2_pkcs11.ini` looks like this, in the case of a CryptoServer LAN in a Windows system:

   ```
   [Global]
   Timeout     = 5000
   Logging     = 0
   Logpath     = c:/tmp
   [CryptoServer]
   Device = 192.168.0.1
   ```

   If you want to enable logging for the Utimaco PKCS#11 interface, you must set a log level. In the table below you will find an overview of the different log levels and their individual meanings.

Log level	*Description*
1	If the CryptoServer responds with an error, this is written to the log file.
2	Debug information (slot number, information etc.) is written to the log file.
4	Each PKCS#11 function is written to the log file with its name.
8	All commands exchanged between the Utimaco PKCS#11 API and the CryptoServer are written to the log file.

If you only want to enable log level 1, you must enter the value 1 for `Logging` in the `cs2_pkcs11.ini` configuration file.

```
[Global]
Timeout      = 5000
Logging      = 1
Logpath      = c:/tmp
```

If you want to combine several log levels, you must enter them as a total.

If you want to enable all Log level, you must enter the value 15 for `Logging`. 1+2+4+8=**15**

```
[Global]
Timeout      = 5000
Logging      = 15
Logpath      = c:/tmp
```

If you want to enable the two log levels 2 and 4, you must enter the value 6 for `Logging`. 2+4=**6**

```
[Global]
Timeout      = 5000
Logging      = 6
Logpath      = c:/tmp
```

2. Save the `cs2_pkcs11.ini` configuration file and close your text editor.

Delete the log file as soon as it is no longer required. The log file may contain the passwords of the Security Officer and the PKCS#11 User for the PKCS#11 Slots in plain (unencrypted) text.

2.9 Problem Analysis for CSP and CNG

You may find useful information to help you if there are problems with CSP and CNG in the CSP log. By default, Log Errors and Warnings are recorded in the log. If you want to view the CSP log and change the settings for the log, follow these steps:

1. Click Start > All Programs > Utimaco > CryptoServer > CSP Configuration. The CryptoServer CSP Configuration dialog box opens.
2. In the CryptoServer CSP Configuration dialog box, click on the Settings tab.
3. Click the View Log button if you want to view the log entries.
4. Click the >> button If you want to change the directory to which the log is to be saved.
5. Click on a different log level (LogLevel) with the left-hand mouse button to enable it, and click the Apply button if you want to change the default setting.
6. End processing in this window by clicking OK.

2.10 Problem Analysis for OpenSSL

You may find useful information to help you if there are problems with OpenSSL in the OpenSSL log. By default, the Utimaco OpenSSL API generates log entries.

In a Windows system you will find the `cs_openssl.ini` configuration file here, by default: `C:\Program Files\Utimaco\CryptoServer\Software\OpenSSL\openssl-<version>\Windows-x86-32\engine-api\` or `Windows-x86-64\engine-api\`

1. Use a text editor to open the `cs_openssl.ini` file.

   The `CS_OpenSSL.ini` file looks like this, in the case of a CryptoServer LAN in a Windows system:

   ```
   [Default]
   Device=192.168.4.111
   ConnectTimeout=5000
   TCPTimeout=60000
   Logging=7
   Logpath=D:\tmp
   AuthUser=SHA1Pwd=openssl, secret
   # end
   ```

   The default setting is `Logging=7`. The number 7 is the total of 1+2+4=7. This means that, when this default setting applies, the log levels 1, 2 and 4 are set.

   If you want to change logging for the Utimaco OpenSSL interface, you must change the log level. If you want to combine several log levels, you must enter them as a total.

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

Log level	*Description*
1	If the CryptoServer responds with an error, this is written to the log file. Internal Utimaco OpenSSL API errors are not recorded in the log file.
2	Internal debug information (slot number, information etc.) is written to the log file.
4	Each OpenSSL function is written to the log file with its name.
8	All commands exchanged between the Utimaco OpenSSL API and the CryptoServer are written to the log file.

If you want to enable all Log levels, you must enter the value 15 for `Logging`. 1+2+4+8=**15**

We recommend that you only enable logging from the OpenSSL API with log level 15 for the purpose of problem analysis and then to use the default setting (LogLevel = 3) again.

If you want to enable the two log levels 2 and 4, you must enter the value 6 for `Logging`. 2+4=**6**

2. Save the `cs_openssl.ini` configuration file and close your text editor.

2.11 Problem Analysis for EKM

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

You will find an example configuration file `cssqlekm.cfg` in the following folder on your SQL Server:

`C:\Program Files\Utimaco\CryptoServer\Software\EKM`

1. Use a text editor to open the configuration file.

   The top part of the `cssqlekm.cfg` configuration file looks like this on your SQL Server:

```
This is a sample configuration file
# path to logfile
LogFile = C:/Program Files/Utimaco/
CryptoServer/Lib/cssqlekm.log

# loglevel
LogLevel = 3
```

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

LogLevel	*Description*
0 = NONE	No log entries are generated.
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+2.
4 = TRACE	All available information is recorded in the log file. Contains log level 1+2+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.

3 Contacting Support

To avoid unnecessary Support queries, please refer to the manuals listed in the "Other manuals" section. You will 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 "Other manuals" section, and carry out the performance- and solution-oriented administration steps described in them.

3.1 Do You Have a CryptoServer PCI or PCIe Expansion Card?

If you have a PCI or PCIe expansion card, and want to contact Support, please get the following information ready for us:

- Your customer or company name.
- Please 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.

  To save the **Diagnostic Information** as a `.txt` file on your computer, follow these steps:

  1. Start the CryptoServer Administration Tool (CAT).
  2. Go to the **Show** main menu item and click the **Diagnostics** sub-menu item.

     The most important **Diagnostic Information** then appears in a separate window:
  3. Click the **Save** button to save the txt file on your computer.

- The Audit Log.
  You can view the Audit Log in the CAT by selecting **Show** in the main menu and then selecting **Audit Log**.
  In the **CryptoServer Audit Log** dialog box, click on **Save Log** to save the Audit Log on your Admin PC. The complete Audit Log is saved in a file.

3.2 Do You Have a CryptoServer LAN?

If you have a CryptoServer LAN, and want to contact Support, please get the following information ready for us:

- The CryptoServer LAN serial number.
  You will find the CryptoServer LAN serial number via the menu options of the CryptoServer LAN.
  CSLAN Administration > Show CSLAN Info > Show Version
  Alternatively you will find the serial number on the right-hand side of the CryptoServer LAN.
- The **dsp_admin** version number.
  You will find the **dsp_admin** version number via the menu options on the CryptoServer LAN.
  CSLAN Administration > Show CSLAN Info > Show Version
- Please 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, follow these steps:

  1. Start the CryptoServer Administration Tool (CAT).
  2. Go to the **Show** main menu item and click the **Diagnostics** sub-menu item.

     The most important **Diagnostic Information** then appears in a separate window:
  3. Click the **Save** button to save the txt file on your computer.

3.3 Contact Address for Support Queries

Please feel free to contact us if an error occurs while operating the CryptoServer LAN, or if you have any further questions on CryptoServer LAN.

Utimaco IS GmbH
Germanusstraße 4
52080 Aachen
Germany

You can reach us from Monday to Friday 09.00 a.m. to 05.00 p.m., apart from public holidays and other customs days, under the following phone/fax number and e-mail address:

Phone:	+49 (0) 241 1696-153
Fax:	+49 (0) 241 1696-58153

e-mail: support-cs@utimaco.com

If you need to send the CryptoServer LAN back to the manufacturer, we request that you first send us an e-mail containing a short description of the problem, to this email address:

rma-cs@utimaco.com