

CryptoServer LAN V5

Administration Manual



utimaco[®]

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	1.5.10
Product Version	6.0.0
Date	2024-10-23
Document No.	2018-0010
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	8
1.1	About this Manual	8
1.1.1	Target Audience for this Manual	8
1.1.2	Contents of this Manual	8
1.1.3	Document Conventions	9
1.2	Other Manuals	10
2	The CryptoServer LAN - Overview.....	13
2.1	Administration.....	14
2.2	Transferring Files to or from the CryptoServer LAN	15
2.3	Authenticating Commands.....	16
2.4	CryptoServer LAN System Users	17
2.5	Boot Partitions in the CryptoServer LAN	17
2.6	The Simple Network Manager Protocol (SNMP).....	18
2.7	The Internet Protocol Version 6 (IPv6)	19
2.8	The Intelligent Platform Management Interface (IPMI).....	19
3	Bringing the CryptoServer LAN into Operation.....	20
3.1	Menu Options on the Front Panel of the CryptoServer LAN	20
3.2	Switching on the CryptoServer LAN	24
3.3	Passwords for the root and cslagent Users.....	27
3.3.1	Changing the Default Passwords	27
3.3.1.1	Changing the Default Password via an SSH Connection	27
3.3.1.2	Changing the Default Password via a Terminal.....	28
3.4	Setting up the IP Configuration	29
3.4.1	Setting up Static IP Adresses.....	32
3.4.1.1	Entering the a static IPv4 Address With the Front Panel.....	32
3.4.1.2	Entering the IPv4 Default Gateway With the Front Panel	34
3.4.2	Setting up Dynamic IPv4 Addresses With the Front Panel.....	34
3.4.3	Setting up the IPv4 Configuration With a Command-Line	35
3.4.4	Setting up the IPv6 Configuration With a Command-Line	37
4	Administering the CryptoServer LAN	42
4.1	Supported PIN Pads	42
4.2	Connecting the PIN Pad	42
4.3	Enabling/Disabling the SSH Daemon	45

4.4	Logging in Remotely to the CryptoServer LAN	48
4.5	Setting up SNMP	49
4.5.1	Enabling SNMPv2c and SNMPv2c Traps for IPv4	49
4.5.2	Enabling SNMPv3 and SNMPv3 Traps for IPv4	51
4.5.3	Enabling SNMP and SNMP Traps for IPv6.....	55
4.5.4	Configuring SNMP Traps	56
4.5.5	Configuring Multiple SNMP Trap Destinations	65
4.5.6	Setting the Date and Time on the CryptoServer LAN.....	68
4.5.7	Specifying the Keyboard Layout.....	69
4.5.8	Exporting/Importing the File csxlan.conf	70
4.5.9	Importing the Network Configuration	72
4.6	Showing CryptoServer LAN Information.....	74
4.6.1	Showing the CryptoServer LAN Version and Serial Number	75
4.6.2	Showing the Network State	75
4.6.3	Showing the Services on the CryptoServer LAN	76
4.6.4	Showing the Date and Time on the CryptoServer LAN	77
4.6.5	Showing the Partitions	77
4.6.6	Showing the Fan Speed	78
4.6.7	Showing the PCIe Clock Card Information.....	79
4.7	Changing the Default Hostname of the CryptoServer LAN	79
4.8	Update and Maintenance.....	80
4.8.1	Updating the Operating System.....	80
4.8.1.1	Performing a Local Update	82
4.8.1.2	Performing a Remote Update	85
4.8.2	Selecting a Boot Partition.....	86
4.8.3	Reverting the Configuration of the CryptoServer LAN	87
4.8.4	Verifying the Reachability in the Network (ping)	88
4.9	Rebooting the CryptoServer LAN.....	89
4.10	Shutting down the CryptoServer LAN	90
4.11	Setting up PCIe Clock Cards	91
4.12	Setting up NTP	95
4.12.1	Preparations	96
4.12.2	Setting up NTP Mainly Using the Front Panel	98
4.12.3	Setting up NTP Mainly Using Scripts.....	108

4.12.4	Disabling NTP	116
4.13	Configuring the NTP Firmware Module	124
4.13.1	Configuring Time Synchronization between the CryptoServer LAN and the CryptoServer	124
4.13.2	Viewing NTP Log Entries	126
4.13.3	Changing the Time Zone for the CryptoServer LAN	127
4.14	Setting up Bonding	127
4.15	Using IPMI	130
4.15.1	Accessing the CryptoServer LAN	130
4.15.2	Showing Sensor Values	131
4.15.3	Showing Chassis Information	135
4.15.4	Showing System Event Log Information	136
4.15.5	Showing LAN Information	137
4.15.6	Showing User Information	138
4.15.7	Default IPMI Interface Configuration	140
4.15.8	Changing the Default IPMI Interface Configuration	141
4.15.8.1	Setting up IP Reachability	141
4.15.8.2	Setting up the IPMI Web Server	142
4.16	Changing the SSH Login Banner	144
5	Administering the CryptoServer	146
5.1	Showing CryptoServer Information	146
5.1.1	Showing the CryptoServer Status	146
5.1.2	Showing Symbols	151
5.1.3	Showing the Battery Status	151
5.1.4	Showing the Date and Time on the CryptoServer	152
5.1.5	Showing Files in the CryptoServer	153
5.1.6	Showing the Current Firmware Modules	153
5.1.7	Showing the Boot Log	154
5.2	Administering Keys and Files	155
5.2.1	Exporting the HSM Authentication Key	155
5.2.2	Loading a File onto the CryptoServer	156
5.2.3	Deleting a File in the CryptoServer	158
5.2.4	Changing the Administrator's Authentication Key	160
5.2.5	Loading the Firmware Encryption Key into the CryptoServer	163
5.3	Recovery	166
5.3.1	Restarting the CryptoServer	166

5.3.2	Resetting an Alarm	167
5.3.3	Performing the Clear Command	168
5.3.4	Performing the Clear to Factory Command	169
5.3.5	Performing an External Erase	170
5.4	Performing MBK Management on the CryptoServer LAN	171
5.4.1	Generating an AES Key and Saving It to a Smartcard	172
5.4.2	Using the PIN Pad to Import an MBK and Save it to a Smartcard	173
5.4.3	Changing the PIN for the MBK Smartcard	173
5.4.4	Copying an MBK from One Smartcard to Another	174
5.4.5	Showing MBK Key Information on the Smartcard	174
5.4.6	Generating an MBK (AES) on a Smartcard	174
5.4.7	Importing an MBK (AES) from a Smartcard	175
6	Advanced Administration on the CryptoServer LAN	176
6.1	Configuring the Transfer Speed for Ethernet	176
6.2	The Configuration File csxlan.conf	177
6.3	Restricting the Network Access on the CryptoServer LAN	190
6.3.1	iptables for IPv4	190
6.3.2	iptables for IPv6	194
6.4	Setting up Remote Logging	195
6.4.1	Configuring the csxlan.conf File	195
6.4.2	Configuring the syslog.conf File	196
6.4.3	Configuring the Remote Syslog Daemon	197
6.4.4	Configuring logrotate	197
6.5	Adjusting the Menu Structure for the Menu Options	198
6.6	Adding a Standard Screen to the Idle Screens	201
6.7	Adding a Customer-Specific Screen to the Idle Screens	208
6.8	Setting up Static Routing	211
6.9	Setting up fcron Jobs	212
7	SNMP Objects and SNMP Traps	214
7.1	SNMP Objects	214
7.1.1	CryptoServer LAN	215
7.1.2	Fan Table	217
7.1.3	Power Supply and Temperature	219
7.1.4	Power SupplyTable	220

1 Introduction

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

Third party (Open Source) software is used in the CryptoServer LAN.

You will find the license conditions for this software in the document

`CryptoServerLAN_<version>_Licenses.pdf` corresponding to your CryptoServer LAN version on the delivered SecurityServer product CD in the directory `Documentation\Administration Guides\Licenses`.

1.1 About this Manual

This manual describes how to configure the CryptoServer LAN, either via the menu options on the front panel of the device, via SSH access, or directly using a keyboard and monitor connected to the device.

1.1.1 Target Audience for this Manual

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

1.1.2 Contents of this Manual

- [Introduction \(p. 8\)](#)

This chapter gives a general overview of the scope and content of this manual.

- [The CryptoServer LAN - Overview \(p. 13\)](#)

This chapter provides an overview about the CryptoServer LAN and its administration..

- [Bringing the CryptoServer LAN into Operation \(p. 20\)](#)

This chapter describes all the necessary configuration steps for bringing the CryptoServer LAN into operation.

- [Administering the CryptoServer LAN \(p. 42\)](#)

This chapter shows how you can locally administer the CryptoServer LAN by using the menu options on its front panel.

- [Administering the CryptoServer \(p. 146\)](#)

This chapter shows how you can locally administrate the CryptoServer (all series), mounted into the CryptoServer LAN, by using the menu options which are available on the front panel of the CryptoServer LAN.

- [Advanced Administration on the CryptoServer LAN \(p. 176\)](#)

This chapter describes advanced administration functions for the CryptoServer LAN.

- [SNMP Objects and SNMP Traps \(p. 214\)](#)

This chapter describes which OIDs and Traps CryptoServer LAN can output, and what information they can provide you with.

- [Contact Address for Support Queries \(p. 239\)](#)

This chapter provides the manufacturer's contact data in case you have questions on CryptoServer LAN or problems occurred while operating the CryptoServer LAN.

- [References \(p. 240\)](#)

This chapter lists all references used in this manual.

As not all the administration tasks for the CryptoServer PCIe card can be configured within the CryptoServer LAN using the device's own menu options, we recommend you configure the PCIe card remotely using the CryptoServer Administration Tool (CAT) or with the CryptoServer command line tool (csadm). The most important settings, for example for user management and for the cryptographic interfaces, can only be made with the CryptoServer Administration Tool (CAT) or with the CryptoServer command line tool (csadm).

1.1.3 Document Conventions

We use the following document conventions:

<i>Convention</i>	<i>Use</i>	<i>Example</i>
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>Convention</i>	<i>Use</i>	<i>Example</i>
<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.

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 Gen2

The CryptoServer LAN V5 (appliance) is supplied in the following series:

- CryptoServer LAN V5 CSe-Series, i.e., a CSe-Series CryptoServer PCIe card is mounted in the CryptoServer LAN
- CryptoServer LAN V5 Se-Series Gen2, i.e., a Se-Series Gen2 CryptoServer PCIe card is mounted in the CryptoServer LAN.

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

Quick Start Guides

You will find these Manuals in the main directory of the 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 product CD.

- *CryptoServer LAN V5 - Quick Start Guide*
This guide provides 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).
- *CryptoServer PCIe - Quick Start Guide for Linux*
This guide provides a step-by-step instruction on how to bring the CryptoServer PCIe 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).
- *CryptoServer PCIe - Quick Start Guide for Windows*
This guide provides for step-by-step instructions on how to bring the CryptoServer PCIe card into service, how to install the CryptoServer driver on a Windows computer and how to start administrating your CryptoServer with the CryptoServer Command-line Administration Tool (csadm).

Manuals for System Administrators

You will find the administration manuals on the product CD in the following directory: ...
Documentation\Administration Guides\

- *CryptoServer – Administration Manual*
This manual provides provides a detailed description of the CryptoServer functionality, concepts and security mechanisms. It also describes CryptoServer setup and maintenance.

- *CryptoServer LAN V5 – Administration Manual*

This manual describes how to administer a CryptoServer LAN appliance by using the front panel of the appliance.

- *CryptoServer - Troubleshooting*

If problems occur during the use of the PCIe card or a LAN (appliance), read this manual.

- *CryptoServer - PKCS#11 P11CAT - Manual*

If you need to administer the PKCS#11 R3 interface with the PKCS#11 CryptoServer Administration Tool (P11CAT), read this manual.

- *CryptoServer - csadm Manual*

This manual provides information on how to administer a CryptoServer PCIe card or a LAN appliance by using the CryptoServer Command-line Administration Tool (csadm). It includes detailed descriptions of all available commands and their syntax, as well as detailed procedures of common administration tasks.

Operating Manuals

You will find these manuals on the product CD in the following directory: ...

Documentation\Operating Manuals\.

2 The CryptoServer LAN - Overview

The CryptoServer LAN is a 19-inch appliance in which a CryptoServer PCIe card CSe-Series or Se-Series Gen2 is mounted. It can easily be mounted in a 19-inch cabinet and integrated into a network.

The CryptoServer LAN V5 (appliance) is supplied in the following series:

- CryptoServer LAN V5 CSe-Series, i.e., a CSe-Series CryptoServer PCIe card is mounted in the CryptoServer LAN
- CryptoServer LAN V5 Se-Series Gen2, i.e., a Se-Series Gen2 CryptoServer PCIe card is mounted in the CryptoServer LAN.

The environment in which a CryptoServer LAN can be implemented looks like this:

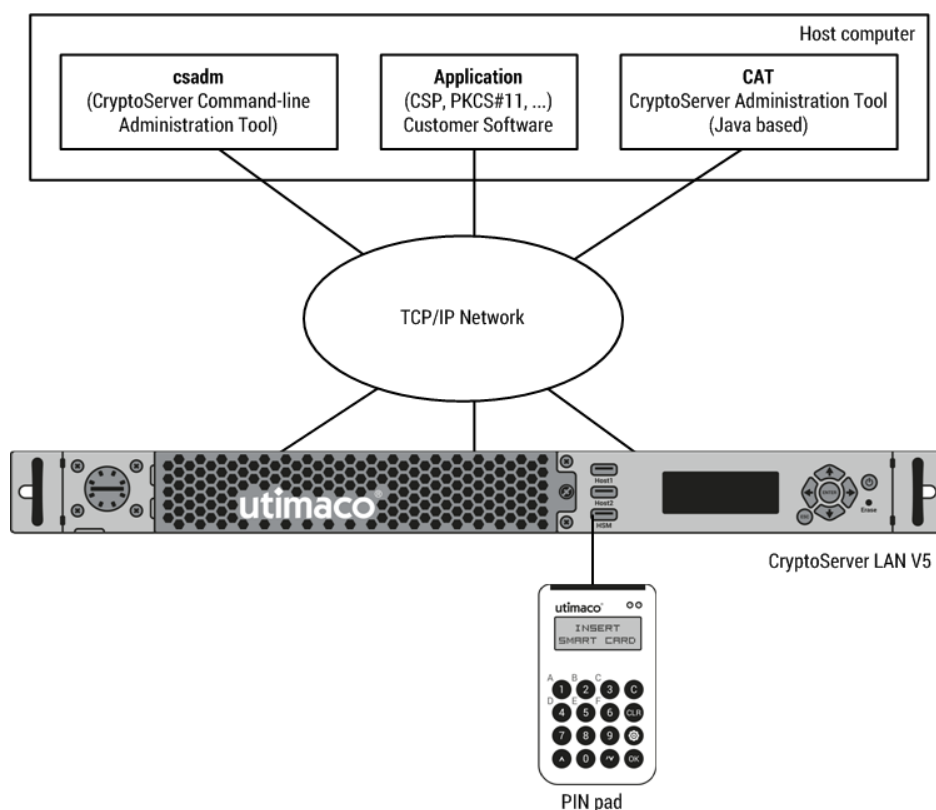


Figure 1 : Example for a CryptoServer LAN implementation environment

The CryptoServer LAN can be administered over a network from a host computer. You can find the current and complete list of supported operating systems in the document [CS_PD_SecurityServer_SupportedPlatforms.pdf](#) on the product CD in the directory ... \Documentation\Product Details.

2.1 Administration

When using the administration functions, you can choose between administering the CryptoServer LAN or the CryptoServer PCIe card. Installing the Host Software and CryptoServer Simulator

You can use the following methods to administer the CryptoServer LAN:

- Local administration via the CryptoServer LAN menu options
On the front panel of the CryptoServer LAN you see a display with a number of control buttons. Use this display and the control buttons to access the menu options.
- Local administration by using a monitor and a keyboard that are directly connected to the CryptoServer LAN.
- Remote administration via an SSH connection (for example under Windows with PuTTY, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#))
- Remote administration with the command line administration tool (csadm)
The csadm tool is a program that is installed on a host computer and can be called from a command-line interface or from a script.

You can administer the CryptoServer PCIe card within the CryptoServer LAN as follows:

- Remotely by using the CryptoServer Administration Tool (CAT) which is installed on a host computer.
The CAT is a Java application that can only be used to administer the CryptoServer PCIe card. It is provided by Utimaco on the SecurityServer product CD, and is installed per default during the SecurityServer software installation, see *Installing the Host Software and CryptoServer Simulator* in the [CryptoServer – Administration Manual \(p. 240\)](#).
- Remotely with the CryptoServer command-line Administration tool (csadm) installed on a host computer.
- Locally with the CryptoServer LAN menu options mentioned above.
To enable this, a PIN pad and ten smartcards are included in the CryptoServer LAN deliverables. [Connecting the PIN Pad \(p. 42\)](#) explains in detail how to connect the PIN pad depending on your CryptoServer LAN hardware version, PIN pad model and administration task to be performed.

2.2 Transferring Files to or from the CryptoServer LAN

You may sometimes need to transfer files to your CryptoServer LAN, for example to update the CSLAN operating system (also referred to below as CSLANOS) in all or only a single CryptoServer LAN partition.

You can do this in the following ways:

- **Using a trustworthy USB flash drive which has been formatted with the FAT32 file system**

The USB flash drive must be connected to a USB port of the CryptoServer LAN which has no access to the mounted CryptoServer. Connect the USB flash drive to the Host1 or Host2 USB port (f4) on the front panel of the CryptoServer LAN.



Figure 2 : Front view of the device



The file (a firmware module, *.mtc or a firmware package, *.mpkg) you want to upload has to be placed in the main directory of a USB flash drive, so that it is shown on the display of the CryptoServer LAN and can be selected for upload.



CryptoServer LAN can access data from and write data on only a single trustworthy USB flash drive connected to it. Although more than one USB flash drive can be simultaneously connected to the CryptoServer LAN, the USB device that has been inserted as first gets connected with the CryptoServer LAN. To establish a connection to another USB flash drive, you should first disconnect the currently connected one and then plug the next USB flash drive into the corresponding USB port of the CryptoServer LAN.

- **Using an SSH client (for example with PuTTY under Windows)**

The CryptoServer LAN has an integrated SSH server. This SSH server supports the SCP file transfer protocol.

SCP offers significantly higher levels of security than FTP because the connection is encrypted. This protocol also uses an SSH server key to provide extremely effective server

authentication. In addition, it can use either password (default setting) or SSH key authentication to check the client.

Visit <http://www.openssh.org> to get an overview of the available SSH clients.

2.3 Authenticating Commands

Some of the commands you trigger using the menu options on the CryptoServer LAN must also be authenticated. This process is performed exclusively using the user authentication key stored on the delivered smartcards. When the CryptoServer LAN is supplied, the `ADMIN.key` is already stored on the ten delivered smartcards.



If you have changed this user authentication key in the CryptoServer, you must use the new user authentication key to authenticate the commands. This new user authentication key must be saved to a smartcard.

To do this, connect the supplied PIN pad to the **HSM USB port (f5)** on the front panel of the CryptoServer LAN or to the USB port on the CryptoServer PCIe card (a10) on the rear side of the CryptoServer LAN. For a detailed description of ports, interfaces and buttons see "*Ports and Interfaces on the Rear Side*" and "*Ports and Operating Elements on the Front Panel*" in the [CryptoServer LAN V5 - Operating Manual \(p. 240\)](#) and the corresponding topics in the [CryptoServer LAN V5 - Betriebsanleitung \(p. 240\)](#).



Figure 3 : Front view of the device

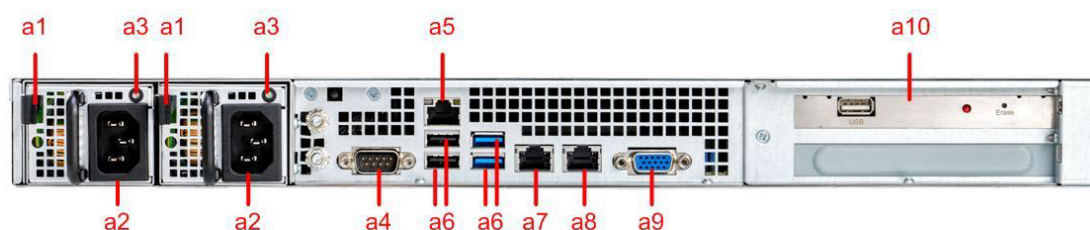


Figure 4 : Rear view of the device

You cannot authenticate the commands by using any other keys or by entering a password via the CryptoServer LAN menu options.

2.4 CryptoServer LAN System Users

There are two users, the system user `root`, who has access to all administrative functions and a second user, `cs_lagent`, who has no privileges but is used to avoid direct SSH login as `root`. He is able to do some monitoring, but he is not privileged to execute any administrative functions.

2.5 Boot Partitions in the CryptoServer LAN

The CryptoServer LAN has three boot partitions:

- `factory`
- `user1`
- `user2`

The boot partition `user1` is started when the CryptoServer LAN is in its initial state. If you have not used the menu options to select a different boot partition, the last boot partition selected via the CryptoServer LAN menu options is the one that now boots automatically.

You can access the **factory** boot partition at any time if the **user1** and **user2** boot partitions fail to boot.

These two boot partitions, **user1** and **user2**, give you the option of booting the CryptoServer LAN with two different configurations. You can also reset any user settings in boot partitions **user1** and **user2**.

- **factory**

This boot partition corresponds to the state in which the CryptoServer LAN is supplied.

You cannot make any permanent configuration changes here. This initial configuration is

created again after every restart. From this boot partition you can update the CSLAN operating system on one of the other two boot partitions, **user1** or **user2**.

- **user1**

This boot partition is where you launch the CryptoServer LAN in the state in which it is supplied. You can also make permanent changes to its configuration here. From this boot partition you can update the CSLAN operating system on boot partition **user2**. If you then boot the **user2** boot partition, the configuration of boot partition **user1** is transferred to boot partition **user2**.

- **user2**

You can make permanent configuration changes in this boot partition. From this boot partition you can update the CSLAN operating system on boot partition **user1**. If you then boot the **user1** boot partition, the configuration is transferred from boot partition **user2** to boot partition **user1**.

For step-by-step instructions on how to update the operating system of the CryptoServer LAN, see [Updating the Operating System \(p. 80\)](#).

2.6 The Simple Network Manager Protocol (SNMP)

The Simple Network Management Protocol is a network protocol developed by the Internet Engineering Task Force (IETF) to provide a way of monitoring network devices from a central management station.

What are known as *agents* (programs) are used for monitoring. They run directly on the devices that are to be monitored. These programs can record the status of a device, make settings, and trigger actions. SNMP enables these programs to communicate with a central management station over a network.

However, the SNMP protocol does not define which values are supplied by a network device. These values (Managed Objects) are described in a Management Information Base (MIB). An MIB is a description file which lists the individual values.

Versions SNMPv2c and SNMPv3 of CryptoServer LAN support the SNMP protocol. In the CryptoServer LAN, SNMP is disabled by default.

2.7 The Internet Protocol Version 6 (IPv6)

It is possible to assign an IPv4 and an IPv6 address for every network connection of the CryptoServer LAN. DHCPv6 and static IPv6 addresses are supported but SLAAC (Stateless Address Autoconfiguration) is not.

2.8 The Intelligent Platform Management Interface (IPMI)

The Intelligent Platform Management Interface is a standard interface allowing to monitor and control a computer remotely and independently from the host system's CPU, firmware and operating system. IPMI can be applied as well before an operating system has booted, when the system is powered down and after an operating system failure. IPMI offers, for example, to retrieve the CPU temperature, peripheral temperature, fan speed, voltage, power consumption, LAN settings, LAN statistics, IPMI user accounts etc.

Port a5 in the following figure is the CryptoServer LAN V5's IPMI port.

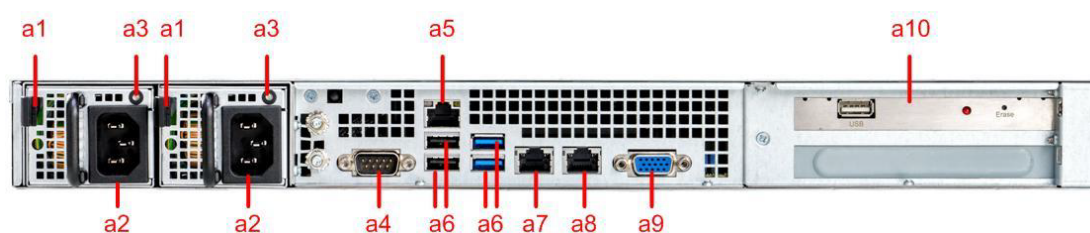


Figure 5 : Rear view of the device

3 Bringing the CryptoServer LAN into Operation

This chapter describes all the configuration steps you must perform to bring the CryptoServer LAN into operation.

The accompanying operating guidelines tell you how to integrate CryptoServer LAN into a network and which connections the device has for that purpose. You should also take note of the network connection, either **eth0** or **eth1**, to which you have connected the network cable to the CryptoServer LAN.

Refer to the accompanying operating manuals for details of the network connections to the device.

The following sections describe how you can bring the CryptoServer LAN into operation by using the menu options on the front panel of the CryptoServer LAN.

3.1 Menu Options on the Front Panel of the CryptoServer LAN

For administrating the LAN device, a display (4 x 20 characters) and six buttons are available on the front panel of the LAN device. You can use the buttons to access the LAN device menu options which are then shown on the display.



Figure 6 : Menu control buttons

Button	Function
ESC	Quit the currently displayed menu level or menu item
ENTER	Select the menu level or confirm the menu item
↑	Move up in the menu control
→	Move to the right in the menu control
↓	Move down in the menu control

Button	Function
←	Move to the left in the menu control

Table 2: Menu control buttons and their function

The last item in the menu is saved automatically. When you press a button, you automatically access the most recently selected menu item. If you press the ESC button to quit the most recently selected menu item, the last item in the menu will not be saved.

The menu items shown on the display on the front panel of the LAN device are organized in the following structure.

Menu Item	Description
CSLAN admin	Administration of the LAN device (host)
└ Configuration	Configuration of the LAN device (host)
└ Network IP4	IP v4 network configuration
└ eth0	Configuration of the eth0 interface
└ DHCP	Setting up Dynamic IPv4 Addresses With the Front Panel (p. 34)
└ Address	Entering the a static IPv4 Address With the Front Panel (p. 32)
└ eth1	Configuration of the eth1 interface
└ DHCP	Setting up Dynamic IPv4 Addresses With the Front Panel (p. 34)
└ Address	Entering the a static IPv4 Address With the Front Panel (p. 32)
└ eth2	Optional: Configuration of the eth2 interface
└ DHCP	Setting up Dynamic IPv4 Addresses With the Front Panel (p. 34)
└ Address	Entering the a static IPv4 Address With the Front Panel (p. 32)
└ eth3	Optional: Configuration of the eth3 interface
└ DHCP	Setting up Dynamic IPv4 Addresses With the Front Panel (p. 34)
└ Address	Entering the IPv4 Default Gateway With the Front Panel (p. 34)
└ Default gateway	Entering the IPv4 Default Gateway With the Front Panel (p. 34)
└ Services	Services running on the LAN device
└ SSH	Enabling/Disabling the SSH Daemon (p. 45)
└ SNMP	Enabling SNMPv2c and SNMPv2c Traps for IPv4 (p. 49)
└ IPTABLES	Restricting the Network Access on the CryptoServer LAN (p. 190)
└ NTP	Setting up NTP Mainly Using the Front Panel (p. 98)

Menu Item	Description
_ NTP server IP addr.	Setting up NTP Mainly Using the Front Panel (p. 98) If a PCIe clock card has been mounted, this menu item is disabled. This is indicated on the display by a small no way sign to the right of the menu item. For details about PCIe clock cards, see Setting up PCIe Clock Cards (p. 91) .
_ CSLAN	CryptoServer LAN (host)
_ Set time	See Setting the Date and Time on the CryptoServer LAN (p. 68) . If a PCIe clock card has been mounted, this menu item is disabled. This is indicated on the display by a small no way sign to the right of the menu item. For details about PCIe clock cards, see Setting up PCIe Clock Cards (p. 91) .
_ Keyboard	Specifying the Keyboard Layout (p. 69)
_ Export csxlan.conf	Exporting/Importing the File csxlan.conf (p. 70)
_ Import csxlan.conf	
_ Import network conf	
_ CSLAN Info	Importing the Network Configuration (p. 72)
_ Show version	Showing CryptoServer LAN Information (p. 74)
_ Show network state	Showing the CryptoServer LAN Version and Serial Number (p. 75)
_ eth0	
_ eth1	
_ eth2	
_ eth3	
_ Routing	
_ Show services info	Showing the Network State (p. 75) eth2 and eth3 are optional.
_ Show time info	Showing the Services on the CryptoServer LAN (p. 76)
_ Show partition info	Showing the Date and Time on the CryptoServer LAN (p. 77)
_ Show fan info	Showing the Partitions (p. 77)
_ Show time source	Showing the Fan Speed (p. 78)
_ Update & Maint.	This menu item is only available if a PCIe clock card has been mounted. PCIe clock cards are supported as of CSLANOS v5.1. Showing the PCIe Clock Card Information (p. 79) and Setting up PCIe Clock Cards (p. 91)
_ Update	Update and Maintenance (p. 80)
_ Set boot partition	Performing a Local Update (p. 82)
_ Revert configuration	Selecting a Boot Partition (p. 86)
_ Ping IP4 address	Reverting the Configuration of the CryptoServer LAN (p. 87)
_ Reboot	Verifying the Reachability in the Network (ping) (p. 88)
_ Shutdown	Rebooting the CryptoServer LAN (p. 89)
	Shutting down the CryptoServer LAN (p. 90)

Menu Item	Description
HSM admin.	Administering the CryptoServer LAN (p. 42)
_ HSM Info	Showing CryptoServer Information (p. 146)
_ State	Showing the CryptoServer Status (p. 146)
_ Battery state	Showing the Battery Status (p. 151)
_ Time	Showing the Date and Time on the CryptoServer (p. 152)
_ List FLASH files	Showing Files in the CryptoServer (p. 153)
_ List SYS files	
_ List NVRAM files	
_ List FW modules	
_ Show boot log	Showing the Boot Log (p. 154)
_ Key&file admin.	Administering Keys and Files (p. 155)
_ Export HSM authKey	Exporting the HSM Authentication Key (p. 155)
_ Load file	Loading a File onto the CryptoServer (p. 156)
_ Delete file	Deleting a File in the CryptoServer (p. 158)
_ Change ADMIN authKey	Changing the Administrator's Authentication Key (p. 160)
_ Load FW decrKey	Loading the Firmware Encryption Key into the CryptoServer (p. 163)
_ HSM time sync	Setting up NTP Mainly Using the Front Panel (p. 98) and Disabling NTP (p. 116)
_ Recovery	Recovery (p. 166)
_ Restart HSM	Restarting the CryptoServer (p. 166)
_ Reset alarm	Resetting an Alarm (p. 167)
_ Clear (firm/data)	Performing the Clear Command (p. 168)
_ Clear to factory	Performing the Clear to Factory Command (p. 169)
PIN Pad applications	Performing MBK Management on the CryptoServer LAN (p. 171)
_ Generate AES Key Shares & store on SC	Generating an AES Key and Saving It to a Smartcard (p. 172)
_ Import MBK from PIN pad & write to SC	Using the PIN Pad to Import an MBK and Save it to a Smartcard (p. 173)
_ Change MBK smartcard PIN	Changing the PIN for the MBK Smartcard (p. 173)
_ Copy MBK smartcard	Copying an MBK from One Smartcard to Another (p. 174)
_ List MBKs on smartcard	Showing MBK Key Information on the Smartcard (p. 174)
_ Generate AES MBK on smartcard	Generating an MBK (AES) on a Smartcard (p. 174)
_ Import AES MBK from smartcard	Importing an MBK (AES) from a Smartcard (p. 175)

Table 3: Display menu structure

3.2 Switching on the CryptoServer LAN

To turn on the CryptoServer LAN, follow these steps:

1. Put the CryptoServer LAN in a 19" rack, see *Mounting the CryptoServer LAN V5 in a 19" Rack* in the [CryptoServer LAN V5 Operating Manual](#) (p. 240).
2. Connect two independent 100 V - 240 V mains power supplies (a2).

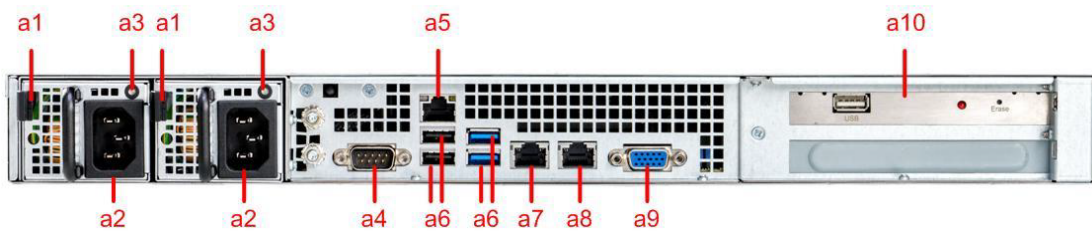


Figure 7 : Rear view of the device

3. Connect an RJ45 network cable to Ethernet port **eth0** (a7).
4. Press the CryptoServer LAN power switch (f8). This step is only necessary if automatic power on has been disabled in the BIOS.



Figure 8 : Front view of the device

5. After a few seconds you will hear a short signal tone and see the first messages on the display panel on the front of the device.



After approximately 90 seconds, CryptoServer LAN is ready for use.

You will see, for example, the following idle screens one after another on the display. They are shown as well when the menu control buttons have not been used for 60 seconds:

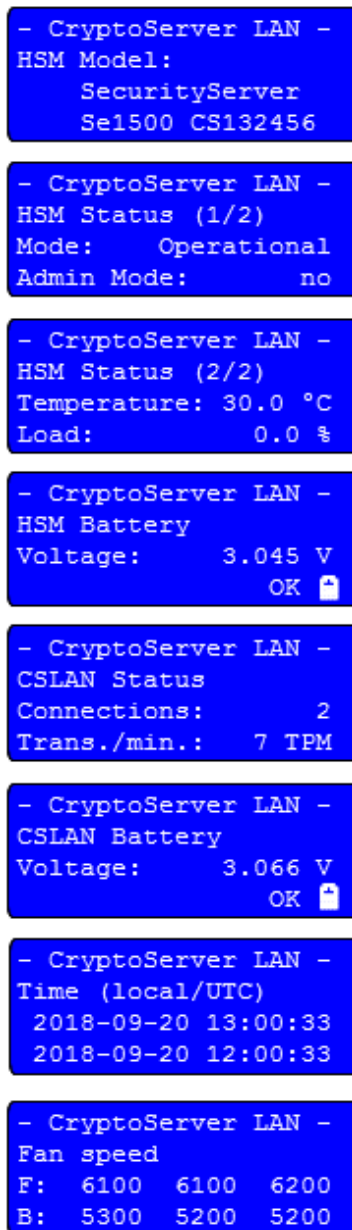


Figure 9 : Idle Screens

The entries displayed in the figure above have the following meaning.

- **HSM Model**

The CryptoServer model (for example, Se1500) and the unique serial number of the CryptoServer's PCIe card (for example, CS123456)

- **Mode**

Operating mode (values: Operational, Maintenance, Bootloader)

The most important thing at this point is that the CryptoServer is running in Operational Mode (Mode: Operational) after it has been booted and is therefore ready for use.

- **Admin Mode**

Indication whether the operating mode has been set to Operational Mode –

Administration-Only (values: yes and no). If set to yes, only functions needed for the CryptoServer administration are available, and all cryptographic functions are blocked.

See also *SetAdminMode* and *SetStartupMode* in the [CryptoServer – csadm Manual](#) (p. 240).

- **Temperature**

Current temperature of the CryptoServer in °C

- **Load**

CryptoServer load for the last 60 seconds in %

- **HSM Battery**

The voltage and the status of the carrier battery

- **Connections**

The number of IP client connections to the CryptoServer

If, for example, a csadm GetState command is performed, which takes a fraction of a second, Connections is increased by 1 for this period of time.

- **Trans./min.**

The number of transactions number per minute

- **CSLAN Battery**

The voltage and the status of the external battery

- **Time (local/UTC)**

The local time and the UTC (Coordinated Universal Time) of the CryptoServer LAN (not of the CryptoServer PCIe card)

- **Fan speed**

The speed of the 6 fans in the 3 fan modules. There is no CPU fan. F stands for the front row of fans and B stands for the back row. The left values are the values of fan 5 and fan 6, the middle values are the values of fan 3 and fan 4, and the right values are the values of fan 1 and fan 2.

A value of 0 for the fan speed indicates a broken fan. In this case, create an RMA (Return

Merchandise Authorization) according to [Contact Address for Support Queries \(p. 239\)](#). f10 in the following figure indicates the fan module.



Figure 10 : Front panel with removed fan compartment grill

The information shown in the idle screens and described above is defined in the `/etc/dspd_idle_window.conf` configuration file.

As of CSLANOS v5.1, pressing the ESC button lets you jump to the next screen of the idle screens.

As of CSLANOS v5.1, an additional customized screen might have been added to the idle screens. For details, see [Adding a Customer-Specific Screen to the Idle Screens \(p. 208\)](#).

3.3 Passwords for the root and csagent Users

SHA512 is the default authentication method of the root user and the `csagent` user.

3.3.1 Changing the Default Passwords

As the manufacturer, Utimaco, has already set the password for accessing the operating system CSLANOS as the root user and the `csagent` user, we strongly recommend you to change this password as soon as possible.

```
User = root, csagent
```

```
Password = utimaco
```

3.3.1.1 Changing the Default Password via an SSH Connection

If you want to change the password for the root user or the `csagent` user remotely via an SSH connection from your administration computer, follow the steps described below.

1. Log in remotely to the CryptoServer LAN according to [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).

2. To enable you to change the password for the root user, enter `passwd` and press the **Enter** key.
3. Enter the old password.
4. Enter the new password. Make sure the password consists of at least six characters. It must be a combination of lower case letters, upper case letters and numbers.



The default password has successfully been changed via the SSH connection.

3.3.1.2 Changing the Default Password via a Terminal

To change the password for the `root` or `csagent` user by using a terminal directly connected to the CryptoServer LAN, proceed as follows:

1. Connect a keyboard to the **Host1** or **Host2** USB port on the front panel of the CryptoServer LAN.
2. Connect a monitor to the VGA connector on the rear side of the CryptoServer LAN.
3. Log in to the CryptoServer LAN.
 - a. Enter `csagent` as the **CryptoServer login** and confirm by pressing the Enter key.
 - b. As the **Password**, enter `utimaco` and confirm by pressing the **Enter** key.
4. To enable you to change the password for the root or csagent user, enter `passwd` and press the **Enter** key.
5. Enter the old password.
6. Enter the new password. Make sure the password consists of at least six characters. It must be a combination of lower case letters, upper case letters and numbers.
7. Log out from CryptoServer LAN with the exit command.
8. Perform the exit command once more.
9. Disconnect the monitor and the keyboard from CryptoServer LAN.



The password has successfully been changed via the terminal.

3.4 Setting up the IP Configuration

The CryptoServer LAN supports several networking features like IPv6 and bonding of network interfaces.

The CryptoServer LAN supports up to 4 NICs, two on-board network adapters (a7: eth0, a8: eth1) and a PCIe card (to be mounted at a11) with additional 2 x 1 Gbit/s SFP+ (optical fiber) network adapters or 2 x 1 Gbit/s RJ45 (copper) network adapters. The left network port (a19 in Figure 12 and a24 in Figure 13) is eth2 and the right (a22/a25) is eth3.

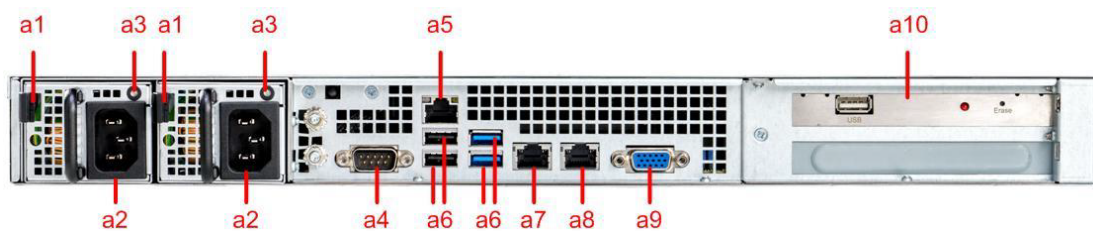


Figure 11 : Rear view of the device

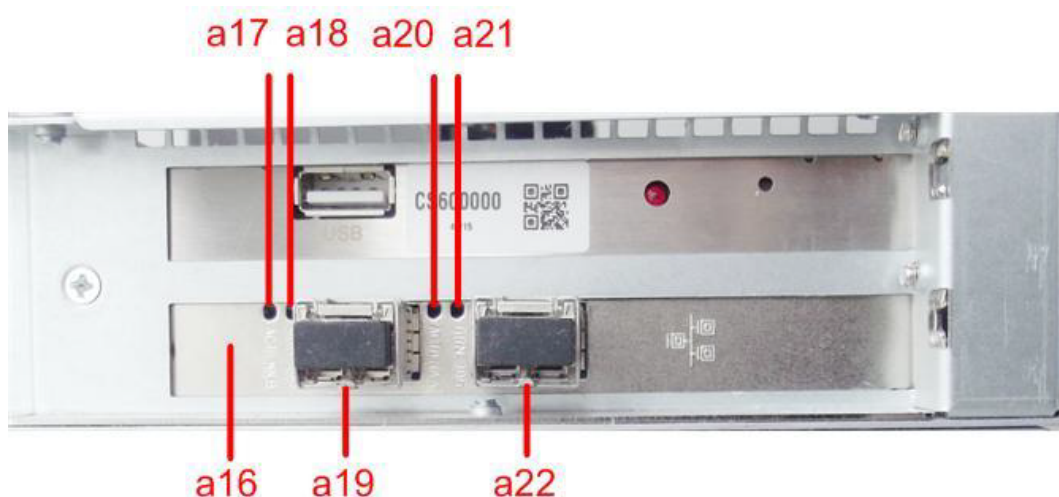


Figure 12 : Optional optical fiber network interface card on the rear side



Figure 13 : Optional Copper Network Interface Card on the Rear Side



eth2 and eth3 are only supported as of CSLANOS v5.1.

The IP configuration is done persistently in the `/etc/sysconfig/networking` file.



By default, a dynamic IP address (DHCP) is assigned to the eth0 interface, and the static IP address 10.10.10.10 has been assigned to the eth1 interface.



If the network interfaces are in the same network, do not configure more than one eth<x> with dynamic IP addresses. The IP addresses of the different network interface cards should not be in the same address range because this would lead to routing problems.

The following table describes the parameters used in this file. Not all parameters described in the following table are necessarily available.

Parameter	Description
NETCONFIG	<p>The network interface this networking file applies to.</p> <ul style="list-style-type: none"> <code>_0</code> This networking file applies only to the eth0 interface. <code>_1</code> This networking file applies only to the eth1 interface. <code>_0 _1</code> This networking file applies to the eth0 interface and to the eth1 interface. <code>_0 _1 _3</code> This networking file applies to the eth0, eth1 and eth3 interface but ignores eth2.
NET_DEV_<x>="eth<x>"	Configuration for the eth<x> interface
DHCP_<x>	<p>DHCP for IPv4 addresses for <code>eth<x></code> .</p> <ul style="list-style-type: none"> <code>yes</code> DHCP for IPv4 addresses is enabled for <code>eth<x></code> . This assignment overrides any assignment for <code>IP_ADDR_<x></code> . <code>no</code> DHCP for IPv4 addresses is disabled for <code>eth<x></code> . This is the default value. It is used if <code>DHCP_<x></code> is not configured.
DHCP_v6_<x>	<p>DHCP for IPv6 addresses for <code>eth<x></code> .</p> <ul style="list-style-type: none"> <code>yes</code> DHCP for IPv6 addresses is enabled for <code>eth<x></code> . This assignment overrides any assignment for <code>IP_ADDR_v6_<x></code> . <code>no</code> DHCP for IPv6 addresses is disabled for <code>eth<x></code> . This is the default value. It is used if <code>DHCP_v6_<x></code> is not configured.
IP_ADDR_<x>	IPv4 address and prefix for eth<x>, for example, <code>192.168.1.111/24</code>
IP_ADDR_v6_<x>	IPv6 address and prefix for eth<x>, for example, <code>2002::2/64</code>
GATEWAY	IPv4 default gateway, for example, <code>192.168.1.1</code> Only one default gateway per protocol is supported
GATEWAY_v6	IPv6 default gateway, for example, <code>2001::1</code> Only one default gateway per protocol is supported.
#	# starts a comment line.

Table 4: Parameters in the /etc/sysconfig/networking file

This file can either be changed by using the front panel of the CryptoServer LAN or a command-line. See the following subchapters for details.

Example

```
# Begin /etc/sysconfig/networking
NETCONFIG="_0 _1"
#NETCONFIG="_0 _1 _2 _3"

NET_DEV_0="eth0"
DHCP_0="yes"

#IP_ADDR_0="192.168.100.203/24"

NET_DEV_1="eth1"
DHCP_1="no"
IP_ADDR_1="10.10.10.10/24"

#NET_DEV_2="eth2"
#DHCP_2="no"
#IP_ADDR_2="10.10.11.10/24"

#NET_DEV_3="eth3"
#DHCP_3="no"
#IP_ADDR_3="10.10.12.10/24"

# IP_ADDR_v6_1="2002::2/64"
# DHCP_v6_1="no"

GATEWAY="192.168.100.254"
# GATEWAY_v6="2002::254"

# End /etc/sysconfig/networking
```

The following subsections describe how to set up the IP configuration manually. If you want import a network configuration instead, see [Importing the Network Configuration \(p. 72\)](#).

3.4.1 Setting up Static IP Addresses

3.4.1.1 Entering the a static IPv4 Address With the Front Panel

You must assign an IP address to the CryptoServer LAN to ensure it can be accessed over the network. You must use the menu options on the CryptoServer LAN to input this IP address.

1. On the front panel of the device, press **ENTER**.
2. Press **ENTER** to open the **CSLAN admin.** menu item.
3. Press **ENTER** to open the **Configuration** menu item.
4. Press **ENTER** to open the **Network IP4** menu item.
5. Use the ↓ key to select **eth0** or **eth1** (optional: **eth2** or **eth3**) and press **ENTER** to open the menu item.
6. Use the ↓ key to select Address and press **ENTER**.

The cursor under a number shows that you can change that number with the ↑ and ↓ keys. Press the → key to move the cursor to the next number. Press the ← key to move the cursor back to the previous symbol.

If you have selected the symbol **■** by using the ↑ and ↓ keys, you can use the → key to insert a zero at this point or you can use the ← key to delete the current symbol.

If the cursor is positioned on the right below the last symbol, you can use the → key to insert a zero at this point. If you press the ← key several times, the zero entry will be repeated.
7. Use the menu options to assign an IPv4 address for the network connection you require and press **ENTER**.
8. If you have assigned a valid IP address, please respond to the prompt that follows with Yes, by pressing the → key to insert the x in the brackets **[x] Yes** and confirm by pressing **ENTER**.



A message confirming that you have successfully entered the IP address is displayed.



Each part of an IP V4 address is shown on the display as a three-digit number, e.g. 123.123.001.123. When using this IP address in a `csadm` command or in the CryptoServer Administration Tool (CAT), you have to remove leading zeros, e.g., use the following command:

```
csadm Dev=123.123.1.123 GetState
```

3.4.1.2 Entering the IPv4 Default Gateway With the Front Panel

1. On the front panel of the device, press **ENTER**.
2. Press **ENTER** to open the **CSLAN admin.** menu item.
3. Press **ENTER** to open the **Configuration** menu item.
4. Press **ENTER** to open the **Network IP4** menu item.
5. Press **ENTER** to open the **Default Gateway** menu item.

The cursor under a number shows that you can change that number with the ↑ and ↓ keys. Press the → key to move the cursor to the next number. Press the ← key to move the cursor back to the previous symbol.

If you have selected the symbol ■ by using the ↑ and ↓ keys, you can use the → key to insert a zero at this point or you can use the ← key to delete the current symbol.

If the cursor is positioned on the right below the last symbol, you can use the → key to insert a zero at this point. If you press the ← key several times, the zero entry will be repeated.
6. Use the menu options to assign an IPv4 address for the network connection you require and press **ENTER**.
7. If you have assigned a valid IP address, respond to the prompt that follows with Yes, by pressing the → key to insert the x in the brackets **[x] Yes** and confirm by pressing **ENTER**.



A message confirming that you have successfully entered the IP address of the default gateway is displayed.

3.4.2 Setting up Dynamic IPv4 Addresses With the Front Panel

The Dynamic Host Configuration Protocol (DHCP) enables a computer to automatically access an IP address and therefore to be integrated in an existing network. This means that the computer (here the device) is automatically assigned an IP address and the IP address of the default gateway by the DHCP server.



Again, if the network interfaces are in the same network, do not configure more than one eth<x> with dynamic IP addresses.

You must use the menu options of the device to enable DHCP.

1. On the front panel of the device, press **ENTER**.
2. Press **ENTER** to open the **CSLAN admin.** menu item.
3. Press **ENTER** to open the **Configuration** menu item.
4. Press **ENTER** to open the **Network IP4** menu item.
5. Use the ↓ key to select **eth0** or **eth1** (optional: **eth2** or **eth3**) and press **ENTER** to open the menu item.
6. Press **ENTER** to open the **DHCP** menu item.
The currently applied setting (disabled or enabled) is indicated by a full circle.
7. If you want to enable that the IPv4 addresses for the device and for the default gateway are provided by a DHCP server, proceed as follows:
 - a. Use the ↓ key to select **enabled** and press **ENTER** to open the menu item.
 - b. To enable DHCP, use the **←** or the **→** key to insert the x in the **[x] Yes** brackets and press **ENTER** to confirm this.



A message confirming that you have successfully configured DHCP is displayed.

3.4.3 Setting up the IPv4 Configuration With a Command-Line

To set up the IPv4 configuration using a command-line instead of the front panel, follow these steps:

Prerequisites

- Attach a keyboard to the a6 USB port in Figure 14 on the rear side or to the f4 USB on the front panel of the CryptoServer LAN.

- Attach a monitor to the VGA port (a9 in Figure 15) of the CryptoServer LAN on the rear side.

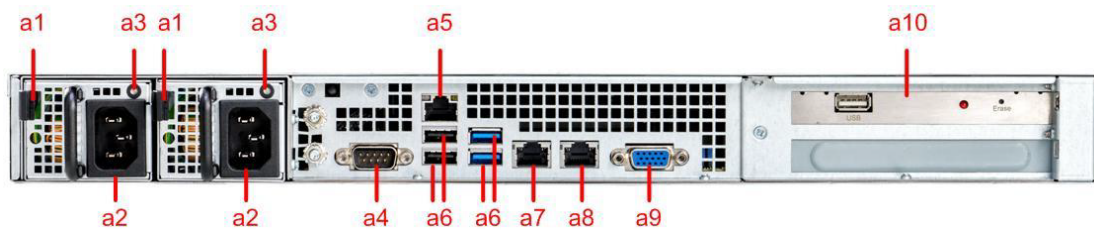


Figure 14 : Rear view of the device

1. Switch on the CryptoServer LAN (f8).



Figure 15 : Front view of the device

2. Log in as the `root` user and press the **Enter** key.
3. As the **Password**, enter `utimaco` and confirm by pressing the Enter key.
4. As an alternative, log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
5. Open the `/etc/sysconfig/networking` file in a text editor.

Example

```
Begin /etc/sysconfig/networking

NETCONFIG="_0 _1"
#NETCONFIG="_0 _1 _2 _3"

NET_DEV_0="eth0"
DHCP_0="yes"

#IP_ADDR_0="192.168.100.203/24"
```



```
NET_DEV_1="eth1"
DHCP_1="no"
IP_ADDR_1="10.10.10.10/24"

#NET_DEV_2="eth2"
#DHCP_2="no"
#IP_ADDR_2="10.10.11.10/24"

#NET_DEV_3="eth3"
#DHCP_3="no"
#IP_ADDR_3="10.10.12.10/24"

# IP_ADDR_v6_1="2002::2/64"
# DHCP_v6_1="no"

GATEWAY="192.168.100.254"
# GATEWAY_v6="2002::254"

# End /etc/sysconfig/networking
```

6. Change this file according to your needs. For details, see [Setting up the IP Configuration \(p. 29\)](#).
7. Save the changes and perform the following command to apply the changes:

```
/etc/init.d/network restart
```


If the `/etc/sysconfig/bonding` file is present, that file is applied instead. For details, see [Setting up Bonding \(p. 127\)](#).



The Pv4 configuration has been successfully set up with the command line.

3.4.4 Setting up the IPv6 Configuration With a Command-Line

The IPv6 protocol is disabled by default. To enable IPv6, follow the steps below in this chapter.

The following IPv6 features are supported using the front panel:

- Importing a network configuration enabling IPv6
- Opening an IPv6 port for the csxlan daemon

All other IPv6 features cannot be enabled, disabled or configured using the front panel. An IPv6 address can be assigned to the CryptoServer LAN using a static IPv6 address or DHCPv6.

Step 1 to 8 are mandatory, the rest is optional

1. Switch on the CryptoServer LAN (f8).



Figure 16 : Front view of the device

2. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).

3. Open the `/etc/sysctl.conf` file in a text editor.

```
vi /etc/sysctl.conf
```

Example

```
kernel.printk= 1 3 1 1
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

4. Change the values of `net.ipv6.conf.all.disable_ipv6` and `net.ipv6.conf.default.disable_ipv6` to 0.

Example

```
kernel.printk= 1 3 1 1
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
```

5. Save the file.
6. To apply the changes, perform the `sysctl -p` command.
7. Configure `ip6tables` to limit access to all IPv6 services on the CryptoServer LAN by performing the instructions in [iptables for IPv4 \(p. 190\)](#) and [iptables for IPv6](#)

- (p. 194). Especially copy the `/etc/ip6tables.conf.example` file to the `/etc/ip6tables.conf` file and make it executable (`chmod +x /etc/ip6tables.conf`). This action enables the IPv6 firewall. Thus, you do not have to adapt the configuration files for every network service.
8. To apply the changes, restart iptables by performing the `/etc/init.d/iptables restart` command.
 9. Open the `/etc/sysconfig/networking` file in a text editor. `vi /etc/sysconfig/networking`

Example

```
# Begin /etc/sysconfig/networking

NETCONFIG="_0"
# NETCONFIG="_0 _1"

NET_DEV_0="eth0"
DHCP_0="yes"
IP_ADDR_0="192.168.1.1/24"

# NET_DEV_1="eth1"
# DHCP_1="yes"
# IP_ADDR_1="10.10.10.10/24"
# IP_ADDR_v6_1="2002::2/64"
# DHCP_v6_1="no"

GATEWAY="192.168.2.1"

# End /etc/sysconfig/networking
```

10. Change this file according to your needs. For details, see [Setting up Static IP Adresses \(p. 32\)](#).

Example: An IPv4 address is assigned by DHCP to eth0 and an IPv6 address is assigned to eth1. 192.168.1.111 is the IPv4 default gateway, and 2001::1/64 is the IPv6 default gateway.

Example

```
Begin /etc/sysconfig/networking

# NETCONFIG="_0"
NETCONFIG="_0 _1"
```

```
NET_DEV_0="eth0"
DHCP_0="yes"
IP_ADDR_0="192.168.1.1/24"

NET_DEV_1="eth1"
DHCP_1="no"
# IP_ADDR_1="192.168.5.222/24"
IP_ADDR_v6_1="2002::2/64"
DHCP_v6_1="yes"

GATEWAY="192.168.1.111"
GATEWAY_v6="2001::1"

# End /etc/sysconfig/networking
```

11. Save the file.
12. Depending on your configuration you may have to modify the `/etc/resolv.conf` file to add, for example, an IPv6 name server.
13. To apply the changes, restart the network by performing the `/etc/init.d/network restart` command.
14. Change the `/etc/csxlan.conf` file according to your specific IPv6 configuration. You may set `IPv6_disable=0` or omit this option. For details, see [Configuring the csxlan.conf File \(p. 195\)](#).
15. To apply the changes, restart the csxlan daemon by performing the `/etc/init.d/cs2 restart` command.
16. Perform the following steps to use the SSH daemon for IPv6 addresses. Open the `/etc/ssh/sshd_config` file in a text editor.
`vi /etc/ssh/sshd_config`
17. Go to the beginning of the following line.
`AddressFamily inet`
18. Change it as follows:
`AddressFamily any`



`AddressFamily inet` indicates IPv4 only, `AddressFamily inet6` indicates IPv6 only, and `AddressFamily any` indicates IPv4 and IPv6,

19. Save the file and quit the text editor.
20. To apply the changes, perform the `/etc/init.d/sshd reload` command.
21. If you apply SNMPv2c or SNMPv3, follow the steps in [Setting up SNMP \(p. 49\)](#), especially in [Enabling SNMP and SNMP Traps for IPv6 \(p. 55\)](#).
22. Follow the steps in [Setting up NTP \(p. 95\)](#). Especially set the IPv6 address of the NTP server in the `/etc/ntp.conf` file.
23. Reboot the CryptoServer LAN to ensure a correct boot process, see [Rebooting the CryptoServer LAN \(p. 89\)](#).



The IPv6 Configuration has been successfully set up with the command line.

4 Administering the CryptoServer LAN

In the next few sections we describe how you can administer the CryptoServer LAN by using the menu options on the front panel of the CryptoServer LAN.

4.1 Supported PIN Pads

The PIN pads are smartcard readers to be used with the CryptoServer which have an integrated display and a keypad, and are also supplied exclusively by Utimaco IS GmbH. You cannot use any other PIN pads for the CryptoServer.



The CryptoServer LAN is supplied along with a PIN pad.

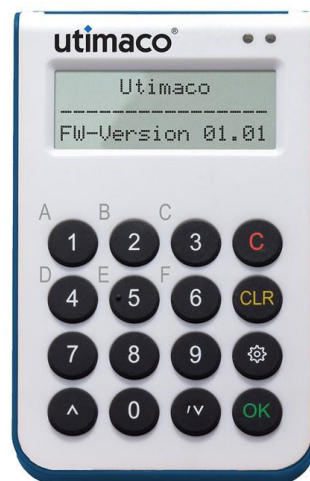


Figure 17 : Utimaco cyberJack one PIN Pad

4.2 Connecting the PIN Pad

There are the following options to connect a PIN pad.

- **Host1/Host2** connection of a PIN pad

The PIN pad is either connected to the USB port labelled **Host1** or **Host2** on the front panel of the CryptoServer LAN (f4) or to one of the a6 USB ports on the rear side of the CryptoServer LAN. All these USB ports are directly connected to the Linux host inside the

CryptoServer LAN.

Chapter *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual \(p. 240\)](#) does not apply here.

- **HSM connection of a PIN pad**

The PIN pad is either connected to the USB port labelled **HSM** on the front panel of the CryptoServer LAN (f5) or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN (a1). All these USB ports are directly connected to the CryptoServer.



Figure 18 : Front view of the device

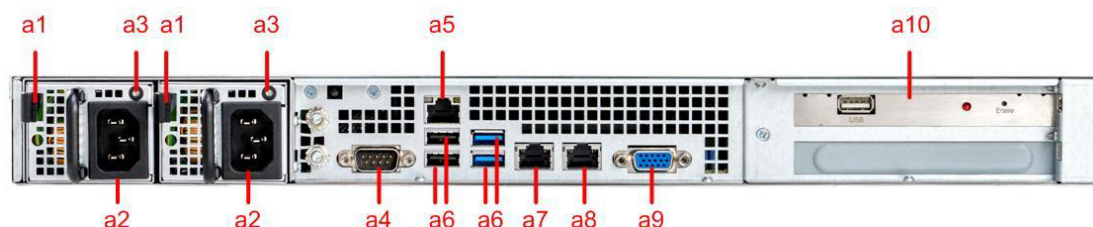


Figure 19 : Rear view of the device

- **Administration computer connection of a PIN pad**

The PIN pad is connected to a USB port of the computer the CryptoServer tools (csadm, p11tool2, CAT, P11CAT etc.)/APIs are running on (administration computer).

As an alternative, the PIN pad might be connected to any computer in the network. For details, see scenario 3, 4 and 5 in *Scenarios* in the [CryptoServer – Administration Manual \(p. 240\)](#). Chapter *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual \(p. 240\)](#) can be applied here.

It depends on the following situations which PIN pad connection is used.

- **Command initiated by menu options on the front panel**

Some actions that are initiated by selecting a menu option on the display and pressing the

ENTER button on the front panel of the CryptoServer LAN must be authenticated by a user. This user is specified either by the `AdminName` parameter or the `NTPManagerName` parameter in the `/etc/csxlان.conf` file.

If this user uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a smartcard or a keyfile), the Host1/Host2 connection of a PIN pad is used.

However, if this user uses RSA smartcard authentication, the HSM connection of a PIN pad is used. See the following chapters for examples:

- [Setting up NTP Mainly Using the Front Panel \(p. 98\)](#) (see step 2 for specifying the user and see step 8g) for performing the command)
 - [Disabling NTP \(p. 116\)](#) (step 6f for performing the command)
 - [Loading a File onto the CryptoServer \(p. 156\)](#)
 - [Deleting a File in the CryptoServer \(p. 158\)](#)
 - [Changing the Administrator's Authentication Key \(p. 160\)](#)
 - [Loading the Firmware Encryption Key into the CryptoServer \(p. 163\)](#)
 - For details about authentication mechanisms, see *Authentication Mechanisms* in the [CryptoServer – Administration Manual \(p. 240\)](#).
- Remote command-line
Assume that the following conditions apply:
 - You log in from a local administrator computer into a remote CryptoServer LAN using an SSH connection.
 - You perform, for example, a `csadm` or `p11tool2` command in this command line.
 - This command should be performed on this CryptoServer LAN (i.e., for example, `Dev=127.0.0.1`).
 - This command needs to be authenticated by a user.
 - This user uses RSA signature authentication, ECDSA signature authentication or RSA smartcard authentication.

If this user uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a smartcard or a keyfile), the **Host1/Host2** connection of a PIN pad is used.

However, if this user uses RSA smartcard authentication, the HSM connection of a PIN pad is used.

Example: `csadm Dev=127.0.0.1 LogonSign=ADMIN,:cs2:cjo:USB0`

`ShowAuthState`

Example output: `current AUTH state: 22000000`

- PIN pad applications

In this case, the HSM connection of a PIN pad is always used. For details, see [Performing MBK Management on the CryptoServer LAN \(p. 171\)](#) and its subchapters.

- Command performed on an administration computer accessing a CryptoServer LAN
Assume that the following conditions apply:

- csadm, p11tool2, CAT or P11CAT is running on a computer, the administration computer, and is used to perform a command.
- This command should be applied to a CryptoServer LAN.
- This command needs to be authenticated by a user.
- This user uses RSA signature authentication with a smartcard, ECDSA signature with a smartcard or RSA smartcard authentication.

If this user uses RSA signature authentication with a smartcard or ECDSA signature authentication with a smartcard, the administration computer connection of a PIN pad is used.

However, if this user uses RSA smartcard authentication, the **HSM** connection of a PIN pad is used.

Example: `csadm Dev=123. 123. 123. 123 LogonSign=ADMIN,:cs2:cjo:USB0`

`ShowAuthState`

123.123.123.123: IP address of the CryptoServer LAN

Example output: `current AUTH state: 22000000`

For details about authentication mechanisms, see *Authentication Mechanisms* in the [CryptoServer – Administration Manual \(p. 240\)](#).

4.3 Enabling/Disabling the SSH Daemon

The SSH daemon creates a secured, authenticated and encrypted connection between two computers over an unsecured network. It is enabled by default.



Consider that device uses different SSH keys for each boot partition.

The device supports only version 2 of the SSH protocol. Previous versions of the SSH protocol are not supported.

To enable the SSH daemon to set up remote SSH access, do the following:



Since the SSH daemon is enabled by default, these steps are only needed if it has been disabled for some reason.

1. Press **ENTER** on the front panel of the device.
2. Press **ENTER** to select **CSLAN admin**.
3. Press **ENTER** again to select **Configuration**.
4. Press the ↓ key to select **Services** and confirm by pressing **ENTER**.
5. Press **ENTER** to select **SSH**.
The currently applied setting (**disabled** or **enabled**) is indicated by a full circle.
6. Use the ↓ key to select **enabled** and press **ENTER** to open the menu item.
7. Use the ← or the → key to move the x into the brackets **[x] Yes** and press **ENTER**.



A message confirming that you have successfully enabled SSH is displayed.

If you use IPv6 addresses, perform the following steps as well:

1. Attach a keyboard to the Host1 or Host2 USB port on the front panel of the device or to the a6 USB port on the rear side of the device.
2. Attach a monitor to the VGA port (a9) of the device on the rear side.

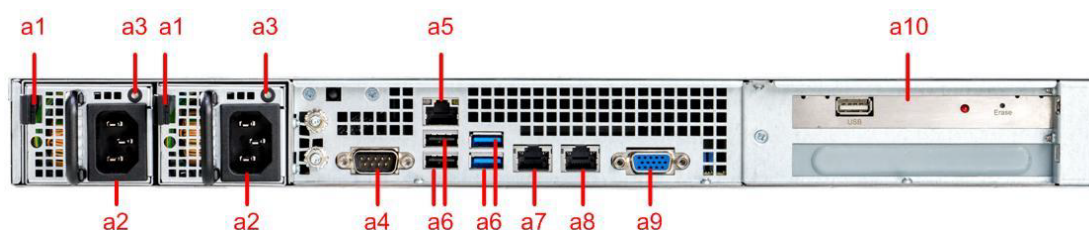


Figure 20 : Rear view of the device

3. Switch on the device (f8).



Figure 21 : Front view of the device

4. Log in as the `root` user and press **Enter**.
5. As the Password, enter `utimaco` and confirm by pressing **Enter**.
6. Open the `/etc/ssh/sshd_config` file in a text editor
`vi /etc/ssh/sshd_config`
7. If you want to have IPv4 disabled and IPv6 enabled, perform the following substeps.
 - a. Insert `#` at the beginning of the following line.
`AddressFamily inet`
 - b. Remove the `#` in the following line.
`# AddressFamily inet6`
8. If you want to have IPv4 and IPv6 enabled instead, perform the following substeps.
 - a. Search for the following line.
`AddressFamily inet`
 - b. Change it as follows.
`AddressFamily any`
9. Save the file and quit the text editor.
10. Restart the SSH daemon to apply the changes. `/etc/init.d/sshd reload.`

4.4 Logging in Remotely to the CryptoServer LAN

For some actions, it is necessary to log in remotely to the CryptoServer LAN. Perform the following steps to do so.

Prerequisites

- An IP address must have been assigned to the CryptoServer LAN. For details, see [Setting up the IP Configuration \(p. 29\)](#).
- If the SSH daemon has been disabled, enable it, see [Enabling/Disabling the SSH Daemon \(p. 45\)](#). The SSH daemon is enabled by default.

Procedure

1. Start your SSH client (for example, PuTTY on Windows or ssh on Linux).
2. Log in to your CryptoServer LAN via SSH, for example, with the following access data:
`Host name = <computer name/IP address of the CryptoServer LAN>`
`Port number = 22`
`User name = cslagent`
`Password = utimaco`
3. Perform the following command to log in as the `root` user.
`su -`
4. Press the **Enter** key.
5. As the **Password**, enter `utimaco` and confirm by pressing the **Enter** key.



The Internet Protocols IPv4 and IPv6 are supported.



If you want to change and save a configuration file on the remote CryptoServer LAN, we highly recommend to perform the changing and saving operations on the CryptoServer LAN itself. Do not perform the changes on a Windows computer and copy the changed file onto the CryptoServer LAN (Linux computer) because the return/line feed representation on Windows differs from the one on Linux.

4.5 Setting up SNMP

CryptoServer LAN supports SNMPv2c and v3 (Simple Network Management Protocol).

4.5.1 Enabling SNMPv2c and SNMPv2c Traps for IPv4

You can enable SNMPv2c for IPv4, and you can decide whether to enable sending messages (SNMP traps) about monitored events, like for example, error messages, too high or too low temperature of the CryptoServer, alarm status and other.



You can only enable SNMPv2c traps if you first enable SNMPv2c.

To enable SNMPv2c, follow these steps:

1. Press the **ENTER** button on the front panel of the CryptoServer LAN.
2. Press the **ENTER** button to open the **CSLAN admin.** menu item.
3. Then press the **ENTER** button to open the **Configuration** menu item.
4. Use the ↓ button to select Services and then press **ENTER** to open the menu item.
5. Use the ↓ button to select SNMP and then press **ENTER** to open the menu item.
The currently applied setting (**disabled** or **enabled**) is indicated by a full circle.
6. Use the ↓ button to select enabled and press the **ENTER** button to open the menu item.
7. Use the ← or the → button to insert the x in the **[x] Yes** brackets and press the **ENTER** button to confirm this.



The system displays a message confirming that you have successfully enabled SNMP.

If you do not want to enable SNMP traps, the SNMP configuration is finished. No further steps in this chapter are mandatory. If you want to enable SNMP traps, perform the following steps.



SNMP2vc traps cannot be enabled, disabled or configured using the front panel.

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
2. Open the `/etc/snmp/snmpd.conf` file into a text editor.
3. You see for example the following entries right at the end of the `/etc/snmp/snmpd.conf` file:

```
trapcommunity CryptoServer
trap2sink 127.0.0.1
```
4. Replace `127.0.0.1` by the IPv4 address of your SNMP trap destination (SNMP manager). If you need multiple destinations, add several lines. See [Configuring Multiple SNMP Trap Destinations \(p. 65\)](#) as well.
5. Save the file after you have finished editing it.
6. Go to the `/etc/snmp` directory.
7. So that the CryptoServer sends the SNMP traps, the `/etc/snmp/csln_mib.conf` configuration file must be edited.
The parameter enabled for all traps in section `[AllTraps]` must be activated, i.e., `enabled = yes` or `enabled = configured`. The default value is `no`.



Do not change the `csln_mib.conf` file name for SNMP to be able to use it.

For important details about using the `[AllTraps]` trap and its influence on specific traps, see [Configuring SNMP Traps \(p. 56\)](#).

8. Save the file after you have finished editing it.
9. Perform the `/etc/init.d/snmpd` restart command for any changes you made in the SNMP configuration files to come into effect.



You have successfully enabled SNMP traps.

Consider that crontab performs logrotate, logrotate performs `/etc/logrotate.d/snmp`, this performs `/usr/bin/killall -HUP snmpd`, this causes a `/etc/init.d/snmpd restart` and this sends an `n sNotifyRestart trap` (object identifier 1.3.6.1.4.1.8072.4.0.3).

4.5.2 Enabling SNMPv3 and SNMPv3 Traps for IPv4

In contrast to earlier SNMP versions, SNMPv3 offers encryption features. In addition to that, SNMPv3 offers acknowledgment messages for the reception of SNMP traps.

You can decide whether to enable sending messages (SNMP traps) about monitored events, like for example, error messages, too high or too low temperature of the CryptoServer, alarm status and other.



Enabling SNMPv3 or SNMPv3 traps cannot be done by using the front panel of the CryptoServer LAN.

To enable SNMPv3 (and SNMPv3 traps as an option), follow these steps:

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
2. Perform the following command to stop a running SNMP agent.

```
/etc/init.d/snmpd stop
```

3. Perform a command according to the following pattern to create an SNMPv3 user. This user is used for the authentication of SNMP messages.

```
net-snmp-create-v3-user -a SHA -A <AuthPassword> -x AES -X  
<EncryptPassword> <UserName>
```

Parameter	Description
a	Authentication method (cryptographic hash function), either MD5 or SHA . Do not use MD5 because it has only poor security quality.
A	Password for the authentication method

Parameter	Description
x	Encryption algorithm, either DES or AES . Do not use DES because it has only poor security quality.
X	Password for the encryption algorithm. The password must have at least 10 characters.
<UserName>	The SNMPv3 user to be created

Table 5: Parameters for creating an SNMPv3 user



We recommend you use the `-a`, `-A`, `-x` and `-X` parameters due to security reasons.

- Make sure that the created SNMPv3 user, the authentication parameters and the encryption parameters are known to the SNMP manager. The description of the SNMP manager is beyond the scope of this documentation.
- If you do not want to enable SNMPv3 traps, perform the `/etc/init.d/snmpd restart` command to start SNMP and to finish enabling SNMPv3. In this case, there is no need to perform the following steps in this chapter. However, if you want to enable SNMPv3 traps, perform the following steps.
- Open the `/etc/snmp/snmpd.conf` file in a text editor.



If you want to change and save a configuration file on the remote CryptoServer LAN, we highly recommend performing the changing and saving operations on the CryptoServer LAN itself. Do not perform the changes on a Windows computer and copy the changed file onto the CryptoServer LAN (Linux computer) because the return/line feed representation on Windows differs from the one on Linux.

You see for example the following entry right at the end of it:

```
trapcommunity CryptoServer
trap2sink 10.17.2.1
```

- Below these lines, add a line according to the following pattern.

```
trapssess -v 3 -u <UserName> -e <EngineId> -l <PrivacyLevel> -a SHA -A
<AuthPassword> -x AES -X <EncryptPassword> <IpAddr>
```


This line defines the destination that SNMPv3 traps are sent to. If you need multiple destinations, add several lines.

Parameter	Description
u	The SNMPv3 user that just has been created
e	<p><code>EngineId</code> parameter identifying the SNMPv3 agent. This parameter has been created during the user creation above. You find it in the <code>snmpd.conf</code> file. The path to this file depends on the Linux distribution or the configuration or the compilation of the SNMPv3 agent. Example value: <code>/var/net-snmp/snmpd.conf</code></p> <p>SNMPv3 requires an SNMP agent to define a unique "engine ID" in order to respond to SNMPv3 requests. This ID will normally be determined automatically, using two reasonably non-predictable values - a (pseudo-)random number and the current time in seconds. This is the recommended approach. However, the capacity exists to define the <code>engineID</code> in other ways (in the <code>snmpd.conf</code> file):</p> <ul style="list-style-type: none"> <code>engineID STRING</code> specifies that the <code>engineID</code> should be built from the given text STRING. <code>engineIDType 1 2 3</code> specifies that the <code>engineID</code> should be built from the IPv4 address (1), IPv6 address (2) or MAC address (3). Note that changing the IP address (or switching the network interface card) may cause problems. <code>engineIDNic INTERFACE</code> defines which interface to use when determining the MAC address. If <code>engineIDType 3</code> is not specified, then this directive has no effect. The default is to use <code>eth0</code>.
l	<p>Security level</p> <p>noAuthNoPriv No authentication method (parameters <code>-a</code> and <code>-A</code>) and no encryption algorithm (privacy; parameters <code>-x</code> and <code>-X</code>) are used. Do not use <code>noAuthNoPriv</code> because <code>authPriv</code> has a better security quality.</p> <p>authNoPriv An authentication method is used but no encryption algorithm is used. Do not use <code>authNoPriv</code> because <code>authPriv</code> has a better security quality.</p> <p>authPriv An authentication method and an encryption algorithm are used.</p>
a	Authentication method (cryptographic hash function), either MD5 or SHA . Do not use MD5 because it has only poor security quality.
A	Password for the authentication method
x	Encryption algorithm, either DES or AES . Do not use DES because it has only poor security quality.

Parameter	Description
x	Password for the encryption algorithm. The password must have at least 10 characters.
<IpAddr>	IP address of the SNMPv3 trap destination (SNMP manager). It is possible to configure multiple IP addresses. For details, see Configuring Multiple SNMP Trap Destinations (p. 65) .

Table 6: Parameters for creating SNMPv3 traps



We recommend you use the `-l`, `-a`, `-A`, `-x` and `-X` parameters due to security reasons.

8. Save the file after you have finished editing it.
9. Go to the `/etc/snmp` directory.
10. So that the CryptoServer sends the SNMP traps, a specific configuration file, `/etc/snmp/csln_mib.conf`, must be edited.
The parameter enabled for all traps in section `[AllTraps]` must be activated, i.e., `enabled = yes` or `enabled = configured`. The default value is `no`.



Do not change the file name for SNMP to be able to use it.

For details, especially for important details about using the `[AllTraps]` trap and its influence on specific traps, see [Configuring SNMP Traps \(p. 56\)](#).

11. Save the file after you have finished editing it.
12. Perform the `/etc/init.d/snmpd restart` command to enable SNMP – and SNMP traps, if configured by the steps above. Consider that crontab performs logrotate, logrotate performs `/etc/logrotate.d/snmp`, this performs `/usr/bin/killall -HUP snmpd`, this causes a `/etc/init.d/snmpd restart` and this sends an `nsNotifyRestart trap` (object identifier 1.3.6.1.4.1.8072.4.0.3).



SNMPv3 and SNMPv3 Traps for IPv4 were successfully enabled.

4.5.3 Enabling SNMP and SNMP Traps for IPv6

If you want to enable SNMPv2c or SNMPv3 for IPv6, perform the following steps. It is assumed that SNMP has been enabled for IPv4 before.

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
2. If you want to enable SNMP for IPv6, perform the following substeps.
 - a. Go to the `/etc/sysconfig` directory.
 - b. Open the `/etc/sysconfig/snmpd` file in a text editor.

Example

```
# Begin /etc/sysconfig/snmpd
# Default settings for snmpd. This file is sourced by /bin/sh from
# /etc/init.d/snmpd.

# Start snmpd yes|no
START_SNMPD=yes

# Options to pass to snmpd with IPv4 only support
SNMPD_OPTS="udp:161 -A -LF 4 /var/log/snmpd.log"

# Options to pass to snmpd with IPv4 and IPv6 support
# SNMPD_OPTS="udp:161,udp6:161 -A -LF 4 /var/log/snmpd.log"

# End /etc/sysconfig/snmpd
```

- c. Insert a `#` at the beginning of `SNMPD_OPTS="udp:161 -A -LF 4 /var/log/snmpd.log"`.
 - d. Remove the `#` at the beginning of `# SNMPD_OPTS="udp:161,udp6:161 -A -LF 4 /var/log/snmpd.log"`. This enables the SNMP traps for IPv4 and IPv6.
 - e. Save the file after you have finished editing it.
3. To enable the SNMP access for IPv6, perform the following substeps.
 - a. Open `/etc/snmp/snmpd.conf` file in a text editor.
 - b. Add the following line:
`AddressFamily inet6`
 - c. You see for example the following entries:
`# sec.name source community`
`com2sec mynetwork 0.0.0.0/0 CryptoServer`

```
#com2sec6 mynetwork ::/0 CryptoServer
```

The line `com2sec mynetwork 0.0.0.0/0 CryptoServer` enables SNMP for IPv4.

- d. Remove the `#` at the beginning of `#com2sec6 mynetwork ::/0 CryptoServer`. This enables SNMP for IPv6.

4. You see for example the following entries right at the end of the `/etc/snmp/snmpd.conf` file:

```
trapcommunity CryptoServer trap2sink 127.0.0.1
```

- a. Add an additional line `trap2sink <IPv6 address>` with the IPv6 address of your SNMP trap destination (SNMP manager). This sets the SNMP trap destination. If you need multiple destinations, add several lines. See [Configuring Multiple SNMP Trap Destinations \(p. 65\)](#) as well.

```
trapcommunity CryptoServer
```

```
trap2sink 127.0.0.1
```

```
trap2sink 3ffe:9001:f20::101
```

- b. Save the file after you have finished editing it.

5. To apply the changes, perform the following command.

```
/etc/init.d/snmpd restart
```

Consider that crontab performs logrotate, logrotate performs `/etc/logrotate.d/snmp`, this performs `/usr/bin/killall -HUP snmpd`, this causes a `/etc/init.d/snmpd restart` and this sends an `nsNotifyRestart` trap (object identifier 1.3.6.1.4.1.8072.4.0.3).



SNMP and SNMP Traps for IPv6 have successfully been enabled.

4.5.4 Configuring SNMP Traps



This chapter applies to all supported SNMP versions.

The `cslan_mib.conf` stored in the `/etc/snmp/` directory is the configuration file for the supported SNMP traps. You can configure the SNMP traps in this file.


To execute the configuration options, perform the following steps.

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN](#) (p. 48).

2. Open the configuration file specified above in a text editor

The configuration options for each individual CryptoServer trap are described in the following table:

<i>SNMP Trap name / Section</i>	<i>Parameter/Description</i>
[StateDevice]	device IP address of the CryptoServer to be monitored. Default: device = 127.0.0.1 (localhost) connect_timeout Timeout on connection establishment in milliseconds. Default: connect_timeout = 3000 read_timeout Timeout on command execution between sending data and receiving the answer in milliseconds. Default: read_timeout = 60000

<i>SNMP Trap name / Section</i>	<i>Parameter/Description</i>
[AllTraps]	<p>enabled This is where you specify whether SNMP traps are to be sent or not. Possible values: <code>no</code> (default) - AllTraps is disabled. No traps are sent even if specific traps (for example, <code>ErrorTrap</code> or <code>ModeChangeTrap</code>) are enabled by setting <code>enabled = yes</code>). <code>yes</code> - AllTraps is enabled. All specific traps are sent irrespective of their specified parameter, for example, if <code>ErrorTrap</code> or <code>ModeChangeTrap</code> has been enabled or disabled. <code>configure</code> - Only those specific traps are sent that are enabled by setting their specified parameter (<code>enabled = yes</code>). Use the sections listed below in this table to enable (<code>enabled = yes</code>) or disable (<code>enabled = no</code>) a specific trap.</p> <hr/> <div>  <p>A specific trap from the list below is enabled only if</p> <ul style="list-style-type: none"> <code>[AllTraps] enabled = yes</code> has been set or <code>[AllTraps] enabled = configured</code> and <code>[<specific>Trap(s)] enabled = yes</code> have been set. </div> <hr/> <p>frequency Interval at which the Callback function for traps is called, in seconds. Default: <code>frequency = 60</code> (every 60 seconds)</p>
[ErrorTrap]	<p>enabled This is where you specify whether or not error messages are to be displayed. <code>no</code> - ErrorTrap disabled <code>yes</code> (default) - ErrorTrap enabled If</p> <ul style="list-style-type: none"> <code>[AllTraps] enabled = yes</code> has been set or <code>[AllTraps] enabled = configured</code> and the default setting for <code>ErrorTrap</code> have been set, <p>error messages are enabled.</p>

<i>SNMP Trap name / Section</i>	<i>Parameter/Description</i>
[ModeChangeTrap]	<p>enabled This is where you enable or disable messages about a change of the operating mode of a CryptoServer in the CryptoServer LAN. The operating mode may be BOOTLOADER, OPERATIONAL, MAINTENANCE, ALARM or POWERDOWN.</p> <p>no - ModeChangeTrap disabled yes (default) - ModeChangeTrap enabled</p> <p>If</p> <ul style="list-style-type: none"> • [AllTraps] enabled = yes has been set or • [AllTraps] enabled = configured and the default setting for ModeChangeTrap have been set, <p>messages about a change of mode are enabled.</p>
[AlarmTraps]	<p>enabled This is where you enable or disable messages about alarms.</p> <p>no - AlarmTraps disabled yes (default) - AlarmTraps enabled</p> <p>If</p> <ul style="list-style-type: none"> • [AllTraps] enabled = yes has been set or • [AllTraps] enabled = configured and the default setting for AlarmTraps have been set, <p>messages about alarms are enabled.</p>

<i>SNMP Trap name / Section</i>	<i>Parameter/Description</i>
[HighTempTraps]	<p>enabled This is where you enable or disable messages about the temperature being too high. no - HighTempTraps disabled yes (default) - HighTempTraps enabled If</p> <ul style="list-style-type: none"> • <code>[AllTraps] enabled = yes</code> has been set or • <code>[AllTraps] enabled = configured</code> and the default setting for <code>HighTempTraps</code> have been set, <p>messages about the temperature being too high are enabled. You can also configure the following parameter: <code>threshold</code> - CryptoServer high temperature threshold value Valid range: <code>threshold: [-30, 100]</code> and <code>> [LowTempTraps]</code> <code>threshold</code> Default: <code>threshold = 50</code> <code>delta</code> - a value in °C for repeating the message Default: <code>delta = 0</code> Setting <code>delta = 0</code> results in a single trap being sent when the threshold is exceeded and a single trap being sent when the temperature falls back to or under the threshold. Example 1: <code>threshold = 50, delta = 0</code> A single <code>notifyCsTemperatureHigh</code> trap is sent when the temperature rises to <code>> 50°C</code>. A single <code>notifyCsTemperatureHighBack</code> trap be sent when the temperature falls back to <code><= 50°C</code>. Example 2: <code>threshold = 50, delta = 5</code> The <code>notifyCsTemperatureHigh</code> trap is sent when the temperature rises to <code>> 50°C, > 55°C, > 60°C</code>, etc. The <code>notifyCsTemperatureHighBack</code> trap will be sent when the temperature falls back to <code><= 55°C, <= 50°C, <= 45°C</code>.</p>

SNMP Trap name / Section	Parameter/Description
[LowTempTraps]	<p>enabled This is where you enable or disable messages about the temperature being too low. no - LowTempTraps disabled yes (default) - LowTempTraps enabled If</p> <ul style="list-style-type: none"> • [AllTraps] enabled = yes has been set or • [AllTraps] enabled = configured and the default setting for LowTempTraps have been set, <p>messages about the temperature being too low are enabled. You can also configure the following parameter: threshold - CryptoServer low temperature threshold value Valid range: threshold: [-30, 100] and > [HighTempTraps] threshold Default: threshold = 10 delta - a value in °C for repeating the message Default: delta = 0 Setting delta = 0 results in a single trap being sent when the temperature falls under the threshold and a single trap being sent when the temperature rises back to or above the threshold. Example 1: threshold = 10, delta = 0 A single notifyCsTemperatureLow trap is sent when the temperature falls to < 10°C. A single notifyCsTemperatureLowBack trap is sent when the temperature rises back to >= 10°C. Example 2: threshold = 10, delta = 5 The notifyCsTemperatureLow trap is sent when the temperature falls to < 10°C, < 5°C, < 0°C, etc. The notifyCsTemperatureLowBack trap is sent when the temperature rises back to >= 5°C, >= 10°C, >= 15°C.</p>
[BatteryTraps]	<p>enabled This is where you enable or disable messages about the battery status of the CryptoServer and CryptoServer LAN to be sent. no - BatteryTraps disabled yes (default) - BatteryTraps enabled Default: enabled = yes If</p> <ul style="list-style-type: none"> • [AllTraps] enabled = yes has been set or • [AllTraps] enabled = configured and the default setting for BatteryTraps have been set, <p>messages about the battery status of the CryptoServer and CryptoServer LAN are enabled. If the BatteryTraps are enabled a BatteryTrap is generated and sent every time the status of the CryptoServer or CryptoServer LAN battery has changed (from OK to LOW, UNKNOWN or ABSENCE). A single trap is generated and displayed in this case (for example, "CryptoServer LAN battery low" or "CryptoServer battery low").</p>

SNMP Trap name / Section	Parameter/Description
[LoadTraps]	<p>enabled This is where you enable or disable messages about the workload on the CryptoServer PCIe card. The workload is the ratio of the time that requests/ commands spend in the CryptoServer PCIe card to the total time. no (default) - LoadTraps disabled yes - LoadTraps enabled Default: enabled = no If</p> <ul style="list-style-type: none"> • [AllTraps] enabled = yes has been set or • [AllTraps] enabled = configured and for [LoadTraps] enabled = yes have been set, <p>messages about the load on the CryptoServer LAN are enabled. You can also configure the following parameters: threshold – a threshold value for the load Valid range: threshold = [0, 100] Default: threshold = 75 delta – a value in % for repeating the message. Valid range: delta = [0, 100] Default: delta = 0 Setting delta = 0 will result in a single trap being sent when the threshold is exceeded and a single trap being sent when the load falls back to or under the threshold. Example 1: threshold = 75, delta = 0: A single notifyCslLoadHigh trap is sent when the load rises to > 75%. A single notifyCslLoadHighBack trap is sent when the load falls back to <= 75%. Example 2: threshold = 75, delta = 10: The notifyCslLoadHigh trap is sent when the load rises to > 75%, > 85%, > 95% etc. The notifyCslLoadHighBack trap is sent when the load falls back to <= 85%, <= 75%, <= 65%.</p>

SNMP Trap name / Section	Parameter/Description
[ClientsTraps]	<p>enabled This is where you enable or disable messages about the usage of the CryptoServer LAN connections. no - ClientsTraps disabled yes (default) - ClientsTraps enabled</p> <p>If</p> <ul style="list-style-type: none"> • [AllTraps] enabled = yes has been set or • [AllTraps] enabled = configured and the default setting for ClientsTraps have been set, <p>messages about the usage of the CryptoServer LAN connections are enabled.</p> <p>You can also configure the following parameters: threshold – a threshold value for the client connection load Valid range: threshold = [0, 100] Default: threshold = 75</p> <p>delta - a value in % for repeating the message. Valid range: delta = [0, 100] Default: delta = 0</p> <p>The client connection load is relative to the maximal number of client connections specified in the configuration file <code>csxlan.conf</code>. When the system is supplied, the maximum number of connections set in the <code>csxlan.conf</code> file is 256. You can only change this setting in this file. Setting <code>delta = 0</code> results in a single trap being sent when the threshold is exceeded and a single trap being sent when the number of clients falls back to or under the threshold.</p> <p>Example 1: <code>threshold = 75, delta = 0:</code> A single <code>notifyCslClientsHigh</code> trap is sent when the client connection load rises to > 75%.</p> <p>A single <code>notifyCslClientsHighBack</code> trap is sent when the client connection load falls back to <= 75%.</p> <p>Example 2: <code>threshold = 75, delta = 10:</code> The <code>notifyCslClientsHigh</code> trap is sent when the client connection load rises to > 75%, > 85%, > 95%, etc. The <code>notifyCslClientsHighBack</code> trap is sent when the client connection load falls back to <= 85%, <= 75%, <= 65%.</p>
[BootTrap]	<p>enabled This is where you enable or disable messages about the boot process. no - BootTrap disabled yes (default) - BootTrap enabled</p> <p>If</p> <ul style="list-style-type: none"> • [AllTraps] enabled = yes has been set or • [AllTraps] enabled = configured and the default setting for BootTrap have been set, <p>messages about the boot process are enabled.</p>

<i>SNMP Trap name / Section</i>	<i>Parameter/Description</i>
[ShutdownTrap]	<p>enabled This is where you enable or disable messages about the shutdown process. no - ShutdownTrap disabled yes (default) - ShutdownTrap enabled If</p> <ul style="list-style-type: none"> • [AllTraps] enabled = yes has been set or [AllTraps] enabled = configured and the default setting for ShutdownTrap have been set, messages about the shutdown process are enabled.
[FanSpeedTraps]	<p>enabled Here you can enable or disable messages about the speed (rotations per minute - rpm) of the cooler fan. no - FanSpeedTraps disable yes (default) - FanSpeedTraps enabled If</p> <ul style="list-style-type: none"> • [AllTraps] enabled = yes has been set or • [AllTraps] enabled = configured and the default setting for FanSpeedTraps have been set, messages about the speed of the cooler fan are enabled. <p>You can also configure the following parameters: threshold – a threshold value for the fan speed Valid range: threshold >= 0 Default: threshold = 600 delta - a value in % for repeating the message. Valid range: delta >= 0 Default: delta = 200 Setting delta = 0 results in a single trap being sent when the fan speed falls under the threshold and a single trap being sent when the fan speed rises back to or above the threshold. Example 1: threshold = 600, delta = 0: A single notifyCslFanSpeedLow trap is sent when the fan speed falls to < 600 rpm. A single notifyCslFanSpeedLowBack trap is sent when the fan speed rises back to >= 600 rpm. Example 2: threshold = 600, delta = 200 The notifyCslFanSpeedLow trap is sent when the fan speed falls to < 600 rpm, < 400 rpm, < 200 rpm, etc. The notifyCslFanSpeedLowBack trap is sent when the fan speed rises back to >= 400 rpm, >= 600 rpm, >= 800 rpm.</p>

<i>SNMP Trap name / Section</i>	<i>Parameter/Description</i>
[PowerSupplyFailureTrap]	<p>enabled Here you can enable or disable messages to be send if one of the two power supplies fails or is switched off. no - PowerSupplyFailureTraps disabled yes (default) - PowerSupplyFailureTraps enabled If</p> <ul style="list-style-type: none"> • [AllTraps] enabled = yes has been set or • [AllTraps] enabled = configured and the default setting for PowerSupplyFailureTrap have been set, <p>messages about the failure of one of the two power supplies or one of the two power supplies being switched off are enabled.</p>

Table 7: Configuration parameters for SNMP traps

3. Save the file after you have finished editing it.
4. Perform the `/etc/init.d/snmpd restart` command for any changes you made in this file to come into effect .



The SNMP traps have successfully been configured.

4.5.5 Configuring Multiple SNMP Trap Destinations



This section applies to all supported SNMP versions.

If you want to send the SNMP traps to more than one IP address, you must edit the `/etc/snmp/snmpd.conf` file.

Perform the following steps to specify more than one IP address for receiving SNMP traps:

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
2. Open the `/etc/snmp/snmpd.conf` file in a text editor.

3. You see for example the following entry right at the end of it:

```
trapcommunity CryptoServer
trap2sink 10.17.2.1
```

4. If you use SNMPv2c, perform this step.

After `trap2sink` you then see the IP address you have specified as the address to which the SNMP traps are to be sent.

Enter the IPv4 or IPv6 addresses you require by using the following format:

```
trapcommunity CryptoServer
trap2sink 10.17.2.1
trap2sink 10.17.4.3
trap2sink 10.17.3.2
trap2sink 3ffe:9001:f20::101
```

5. If you use SNMPv3, perform this step.

Below these lines, add a line according to the following pattern.

```
trapssess -v 3 -u <UserName> -e <EngineId> -l <PrivacyLevel> -a SHA -
A <AuthPassword> -x AES -X <EncryptPassword> <IpAddr>
```

This line defines the destination that SNMPv3 traps are sent to. If you need multiple destinations, add several lines.

<i>Parameter</i>	<i>Description</i>
u	The SNMPv3 user that just has been created

Parameter	Description
e	<p>EngineId parameter identifying the SNMPv3 agent. This parameter has been created during the user creation. You find it in the <code>snmpd.conf</code> file. The path to this file depends on the Linux distribution or the configuration or the compilation of the SNMPv3 agent. Example value: <code>/var/net-snmp/snmpd.conf</code></p> <p>SNMPv3 requires an SNMP agent to define a unique "engine ID" in order to respond to SNMPv3 requests. This ID will normally be determined automatically, using two reasonably non-predictable values - a (pseudo-)random number and the current time in seconds. This is the recommended approach. However, the capacity exists to define the engineID in other ways (in the <code>snmpd.conf</code> file):</p> <ul style="list-style-type: none"> • engineID STRING specifies that the engineID should be built from the given text STRING. • engineIDType 1 2 3 specifies that the engineID should be built from the IPv4 address (1), IPv6 address (2) or MAC address (3). Note that changing the IP address (or switching the network interface card) may cause problems. • engineIDNic INTERFACE defines which interface to use when determining the MAC address. If <i>engineIDType 3</i> is not specified, then this directive has no effect. The default is to use eth0.
l	<p>Security level</p> <p>noAuthNoPriv No authentication method (parameters <code>-a</code> and <code>-A</code>) and no encryption algorithm (privacy; parameters <code>-x</code> and <code>-X</code>) are used. Do not use noAuthNoPriv because authPriv has a better security quality.</p> <p>authNoPriv An authentication method is used but no encryption algorithm is used. Do not use AuthNoPriv because authPriv has a better security quality.</p> <p>authPriv An authentication method and an encryption algorithm are used.</p>
a	Authentication method (cryptographic hash function), either MD5 or SHA . Do not use MD5 because it has only poor security quality.
A	Password for the authentication method
x	Encryption algorithm, either DES or AES . Do not use DES because it has only poor security quality.
X	Password for the encryption algorithm. The password must have at least 10 characters.
<IpAddr>	IP address of the SNMPv3 trap destination (SNMP manager). IPv4 and IPv6 are supported.

Table 8: Parameters for creating SNMPv3 traps

6. Save the file after you have finished editing it.
7. Perform the `/etc/init.d/snmpd restart` command for any changes you made in this file to come into effect.



Multiple SNMP trap destinations were configured successfully.

4.5.6 Setting the Date and Time on the CryptoServer LAN

You can use the function Set CSLAN Time to set the date and time on the CryptoServer LAN.



If a PCIe clock card is mounted on the CryptoServer LAN, see [Setting up PCIe Clock Cards \(p. 91\)](#), the date and the time are set automatically and cannot be set manually. In this case, the steps in this chapter are obsolete.

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.
2. Press the **ENTER** button to open the **CSLAN admin.** menu item.
3. Press the **ENTER** button to open the **Configuration** menu item.
4. Use the **↓** button to select CSLAN and press the **ENTER** button to open the menu item.
5. Press the **ENTER** button to open the **Set Time** menu item.

On the display of the CryptoServer LAN, the local date and time of the CryptoServer LAN is shown in the format YYYY-MM-DD and HH:MM:SS.

The cursor under a number shows that you can change that number with the **↑** and **↓** buttons. Press the **→** button to move the cursor to the next number.

Only values up to December 31, 2037 can be set.
6. Press the **↑** / **↓** and **→** buttons to set the new date and time and then press **ENTER**.
7. Use the **←** or the **→** button to move the x into the square brackets **[x] Yes** and confirm by pressing **ENTER**.



The system displays a message confirming that you have successfully configured the local time.

4.5.7 Specifying the Keyboard Layout

If you want to use a keyboard and a monitor to configure the CryptoServer LAN, you can specify the layout (language) of the keyboard you are going to connect. To change the keyboard layout, follow these steps:

1. If you want to use the front panel, perform the following substeps, If you want to use a remote login instead, continue with step 2.
 - a. On the front panel of the CryptoServer LAN, press the **ENTER** button.
 - b. Press the **ENTER** button to open the **CSLAN admin. menu** item.
 - c. Press the **ENTER** button to open the **Configuration menu** item.
 - d. Use the **↓** button to select **CSLAN** and press the **ENTER** button to open the menu item.
 - e. Use the **↓** button to select **Keyboard** and press the **ENTER** button to open the menu item. This opens a list of different countries.
 - f. Use the **↓** button to select the country you require and then press **ENTER** to confirm.



The system displays a message confirming that you have successfully configured the keyboard layout.

2. If you want to use a remote login, perform the following substeps.
 - a. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
 - b. Perform the following command to show the available keyboard layouts.

Example Output

```
# Begin /etc/keymap.lst
```

```

Belgium      /usr/share/keymaps/i386/azerty/be-  

Bulgaria     /usr/share/keymaps/i386/qwerty/bg-  

Finland      /usr/share/keymaps/i386/qwerty/fi-  

France       /usr/share/keymaps/i386/azerty/fr-  

Germany      /usr/share/keymaps/i386/qwertz/de-  

nodeadkeys.map.gz  

Italy        /usr/share/keymaps/i386/qwerty/it-  

Netherlands  /usr/share/keymaps/i386/qwerty/nl-  

Norway       /usr/share/keymaps/i386/qwerty/no-  

Portugal     /usr/share/keymaps/i386/qwerty/pt-  

UK           /usr/share/keymaps/i386/qwerty/uk-  

USA          /usr/share/keymaps/i386/qwerty/us-  

# End /etc/keymap.lst

```

A value in the left column is needed in the next command to be executed.

- c. If you want a German keyboard layout, perform the following command.

```
set_keyboard_config.sh Germany
```



The keyboard layout has been specified, and is confirmed in the output message. Example Output: Keymap for Germany loaded!



The character set ISO 8859-15 (i.e., Latin-9) is supported for the following countries: Belgium, Bulgaria, France, Germany, Great Britain, the Netherlands, and the USA.

4.5.8 Exporting/Importing the File csxlan.conf

If you want to export the `csxlan.conf` file, which contains the configuration details for the csxlan daemon, from the CryptoServer LAN, so you can process it and then import it back into the CryptoServer LAN, you must work through the following steps:

Export

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.
2. Press the **ENTER** button to open the **CSLAN admin.** menu item.
3. Press the **ENTER** button to open the **Configuration** menu item.
4. Use the **↓** button to select **CSLAN** and press the **ENTER** button to open the menu item.

5. Use the ↓ button to select **Export csxlan.conf** and press the **ENTER** button to open the menu item.
6. Connect a USB flash drive to one of the two Host1 or Host2 ports on the front panel of the CryptoServer LAN.



CryptoServer LAN can write data on only a single trustworthy USB flash drive connected to it. Although more than one USB flash drives can be simultaneously plugged in to the CryptoServer LAN, the USB device that has been inserted as first gets connected with the CryptoServer LAN. This USB device can be configured by the `OSUpdateDevice` variable in the `[DisplayAdmin]` section of the `/etc/csxlan.conf` file (example value: `/dev/sdb1`). To establish a connection to another USB flash drive, you should first disconnect the currently connected one and then plug the next USB flash drive into the corresponding USB port of the CryptoServer LAN.

7. Use the ← or the → button to insert the x in the **[x] Yes** brackets and press the **ENTER** button to confirm this.
8. Press the **ENTER** button. The successful export of the `csxlan.conf` file is confirmed on the display.



The file has been exported successfully and is stored in the main directory on the USB flash drive.

Import

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.
2. Press the **ENTER** button to open the **CSLAN admin.** menu item.
3. Press the **ENTER** button to open the **Configuration** menu item.
4. Use the ↓ button to select **CSLAN** and press the **ENTER** button to open the menu item.
5. Use the ↓ button to select **Import csxlan.conf** and press the **ENTER** button to open the menu item.



Ensure that the `csxlan.conf` file is stored in the main directory on the USB flash drive. The `csxlan.conf` file must be stored by definition in this directory of the USB flash drive.

6. Use the `←` or the `→` button to insert the `x` in the `[x] Yes` brackets and press the **ENTER** button to confirm this.
7. Press the **ENTER** button. The successful import of the `csxlan.conf` file is confirmed on the display.
8. Restart the CryptoServer LAN so you can use the `csxlan.conf` file you have just imported.
 - a. Press the **ESC** button several times to get back to the main menu.
 - b. Press the **ENTER** button to open the **CSLAN admin.** menu item.
 - c. Use the `↓` button to select **Reboot** and press the **ENTER** button to open the menu item.
 - d. Press the `←` or the `→` button to insert the `x` in the brackets `[x] Yes` and confirm by pressing the **ENTER** button.
This reboots the CryptoServer LAN.



The file has been imported

4.5.9 Importing the Network Configuration

As of CSLANOS v5.1, the network configuration can be imported from a network configuration file. This file is divided into the following sections.

- **csl_network_conf**

The start of this section is defined by the `[>csl_network_conf]` tag and the end of this section is defined by the `[<csl_network_conf]` tag.

The `csl_network_conf` section is mandatory and it must contain the following line.

```
version = 1.00
```

Version 1.00 is the only supported version.

- **csl_network**

The start of this section is defined by the `[>csl_services]` tag and the end of this section is defined by the `[<csl_services]` tag.

This section is optional and contains a list of services that can be disabled or enabled by the network configuration file.

- `IPv6_stack = [disable | enable]`

Optional. This variable disables or enables the IPv6 stack in the Linux kernel.

- `IPv6_csxlan = [disable | enable]`

Optional. This variable disables or enables the IPv6 port for the csxlan daemon.

Ensure that the tags do not contain any spaces and that they are not preceded by spaces.

Example of a network configuration file

```
[>csl_network_conf]
version = 1.00
[<csl_network_conf]

[>csl_network]
# Begin /etc/sysconfig/networking
NETCONFIG="_0 _1"

NET_DEV_0="eth0"
DHCP_0="yes"
#IP_ADDR_0="192.168.4.203/24"

NET_DEV_1="eth1"
DHCP_1="no"
IP_ADDR_1="10.10.10.10/24"

IP_ADDR_v6_1="2002::2/64"
DHCP_v6_1="no"

GATEWAY="192.168.4.254"
GATEWAY_v6="2002::254"

# End /etc/sysconfig/networking
[<csl_network]

[>csl_services]
ipv6_stack = enable
ipv6_csxlan = enable
[<csl_services]
```

To import the prepared network configuration file, perform the following steps.

1. Copy the network configuration file to the main directory on a USB flash drive. The filename must be a valid Linux filename. No further restrictions need to be fulfilled.
2. On the front panel of the CryptoServer LAN, press the **ENTER** button.
3. Press the **ENTER** button to open the **CSLAN admin.** menu item.
4. Press the **ENTER** button to open the **Configuration** menu item.
5. Use the ↓ button to select **CSLAN** and press the **ENTER** button to open the menu item.
6. Use the ↓ button to select **Import network conf** and press the **ENTER** button to open the menu item.
7. Connect the USB flash drive with the network configuration file on it to the Host1 or Host2 USB port on the front panel of the CryptoServer LAN or to the a6 USB port on the rear side of the CryptoServer LAN.
8. Press the **ENTER** button. On the display, you can now see which files (not directories and subdirectories) are present in the main directory on the USB flash drive.
9. Use the ↓ button to select the relevant file and confirm your selection by pressing **ENTER**.
10. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
11. Reboot the CryptoServer LAN, see [Rebooting the CryptoServer LAN \(p. 89\)](#).
If the `/etc/sysconfig/bonding` file is present, that file is applied.



The network configuration has successfully been imported.

For details, see [Setting up Bonding \(p. 127\)](#). Importing a bonding file by using the front panel of the CryptoServer LAN is not supported.

4.6 Showing CryptoServer LAN Information

You can show the version of the CryptoServer LAN software.

4.6.1 Showing the CryptoServer LAN Version and Serial Number

1. On the front panel of the device, press **ENTER**.
2. Press **ENTER** to open the **CSLAN admin.** menu item.
3. Use the **↓** key to select **CSLAN Info** and press the **ENTER**.
4. Press **OK** to select **Show version** and press **ENTER** to open the menu item.

Example output:

```
CSLAN 5.1.0 Serial Number: MD1234567
```



The version of the CSLAN operating system (CSLANOS), and the serial number of the device are displayed.

4.6.2 Showing the Network State

You can show which services are enabled on the device. In addition to that the NTP server's IPv4 address is shown.

1. On the front panel of the device, press **ENTER**.
2. Press **ENTER** to open the **CSLAN admin.** menu item.
3. Use the **↓** key to select **CSLAN Info** and press **ENTER**.
4. Use the **↓** key to select **Show network state** and press **ENTER** to open the menu item.
5. Use the **↓** key to open either the eth0, eth1, eth2 or eth3 menu item.

Example Output

```
Address:
  123.123.123.123 N
Network mask:
  255.255.255.0
MAC:
  1F:1F:1F:1F:1F:1F
MTU:          1500
Link up:      yes
Link speed:   1000Mb/s
Mode:         full duplex
```

```

Interface up:      yes
IPv6 address #1:   ---
                  ---
prefix length:     ---
IPv6 address #1:   ---
                  ---
prefix length:     ---

```

6. If you want to show the IP address of the IPv4 default gateway instead, use the ↓ key to open the **Routing** menu item.

Example output:

```
Default Gateway: 123.123.123.123
```



The network state is displayed.

4.6.3 Showing the Services on the CryptoServer LAN

You can show which services are enabled on the device. In addition to that the NTP server's IPv4 address is shown.

1. On the front panel of the device, press **ENTER**.
2. Press **ENTER** to open the **CSLAN admin.** menu item.
3. Use the ↓ key to select **CSLAN Info** and press **ENTER**.
4. Use the ↓ key to select **Show services info** and press **ENTER** to open the menu item.

Example output:

```

SSH: enabled
SNMP: disabled
IP tables: enabled
NTP: disabled NTP
IP4: 123.123.123.123

```




The services of the device are displayed.

4.6.4 Showing the Date and Time on the CryptoServer LAN

You can show the current date and the time of the device on the device display. Not only the UTC time but also the time zone and the local time is shown. You do not require authentication for this action.

1. On the front panel of the device, press **ENTER**.
2. Press **ENTER** to open the **CSLAN admin.** menu item.
3. Use the ↓ key to select **CSLAN Info** and press **ENTER**.
4. Use the ↓ key to select **Show time info** and press **ENTER**. Date and time of the device is displayed in the format YYYY-MM-DD and HH:MM:SS.

Example Output:

```
Date(UTC) : 2019-01-31
Time(UTC) : 14:14:14
Timezone: +0100 Date(loc) : 2019-01-31
Time(loc) : 15:14:14
```



The date and time of the device are displayed.

4.6.5 Showing the Partitions

You can show the partitions used for booting and for running the system.

1. On the front panel of the device, press **ENTER**.
2. Press **ENTER** to open the **CSLAN admin.** menu item.
3. Use the ↓ key to select **CSLAN Info** and press **ENTER**.
4. Use the ↓ key to select **Show partition info** and press **ENTER** to open the menu item.

Example output:

```
Boot part.: user1
```

```
Run part.: user1
```

 The partitions are displayed.

4.6.6 Showing the Fan Speed

You can show the fan values.

1. On the front panel of the device, press **ENTER**.
2. Press **ENTER** to open the **CSLAN admin.** menu item.
3. Use the **↓** key to select **CSLAN Info** and press **ENTER**.
4. Use the **↓** key to select **Show fan info** and press **ENTER** to open the menu item.

Example output:

```
Fan #1 speed: 6200
```

```
Fan #2 speed: 5300
```


```
Fan #3 speed: 6200
```

```
Fan #4 speed: 5400
```

```
Fan #5 speed: 6100
```

```
Fan #6 speed: 5300
```

A value of 0 for the fan speed indicates a broken fan. In this case, create an RMA (Return Merchandise Authorization) according to the chapter *Contact Address for Support Queries*.

 The speed of each fan is displayed.

The device has 6 fans in 3 fan modules and no CPU fan. Fan modules are exchangeable but fans are not. f10 in the following figure indicates the fan module containing fan 5 and fan 6. f11 indicates fan 3 and fan 4, and f12 indicates fan 1 and fan 2.



Figure 22 : Front panel with removed fan compartment grill

4.6.7 Showing the PCIe Clock Card Information

You can show information about the PCIe clock card. For details about PCIe clock cards, see [Setting up PCIe Clock Cards \(p. 91\)](#).

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.
2. Press the **ENTER** button to open the **CSLAN admin.** menu item.
3. Use the **↓** button to select **CSLAN Info** and press the **ENTER** button to open the menu item.
4. Use the **↓** button to select **Show time source** and press the **ENTER** button to open the menu item.

Example output:

```
Card:PZF180PEX DCF77
Clock: Synchronized
Signal: 100 %
```



The PCIe clock card information is displayed.

4.7 Changing the Default Hostname of the CryptoServer LAN

By default, the LAN device is delivered with a Linux hostname CryptoServer. To change this setting, follow the following steps.

1. Connect to the device via SSH or log in with a local command-line.
2. Open the `/etc/sysconfig/hostname` file in a text editor.

```
root@CryptoServer:~# vi /etc/sysconfig/hostname
```
3. Change the name according to your needs.

```
HOSTNAME=XYZ
```

4. Save the changes.
5. Close the text editor.
6. Restart the CryptoServer LAN OS.

```
root@CryptoServer:~# reboot
```
7. After the CryptoServer LAN has restarted, you can verify the changed setting by logging in a command console and performing the hostname command.

```
root@XYZ:~# hostname
```
8. The name is displayed.

```
XYZ
```



The hostname has been changed.

4.8 Update and Maintenance

4.8.1 Updating the Operating System

Utimaco IS GmbH supplies updates for the operating system of the CryptoServer LAN (CSLAN) in the compressed archive file `cslan-x.y.z.tar.gz` (x.y.z. is the version number of the update).

The files provided in the update contain the entire CryptoServer LAN operating system. `cslan-x.y.z.tar.gz` can be imported into the CryptoServer LAN from a USB flash drive directly connected to the CryptoServer LAN ([Performing a Local Update \(p. 82\)](#)) or remotely via SSH connection ([Performing a Remote Update \(p. 85\)](#)). After the import `cslan-x.y.z.tar.gz` is automatically unpacked and saved in the CryptoServer LAN.

A CSLAN update can only be performed from one boot partition to one of the others. For further details about the boot partitions of the CryptoServer LAN please read [Boot Partitions in the CryptoServer LAN \(p. 17\)](#).



All configuration files are retained after an update and are not replaced or overwritten by new versions.

- If you have currently booted the **factory** boot partition, you must select the boot partition into which you want to import the update: **user1** or **user2**. As you cannot make permanent user settings in the factory boot partition, you cannot simply transfer the configuration settings in this case. In this situation, you can only import an update for the operating system.

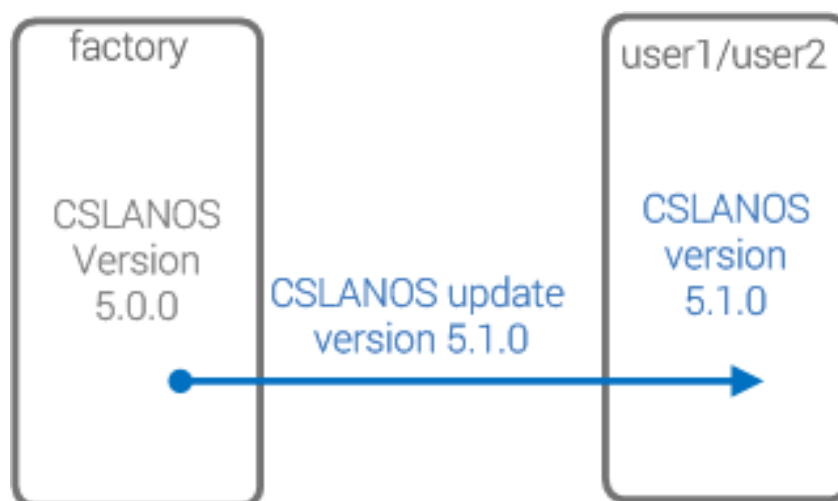


Figure 23 : Updating the operating system CSLANOS in user1 or user2 from the factory boot partition

- If you have currently booted the **user1** boot partition, the update is imported to the **user2** boot partition. Your individual configuration settings are then transferred from the **user1** boot partition to the **user2** boot partition.

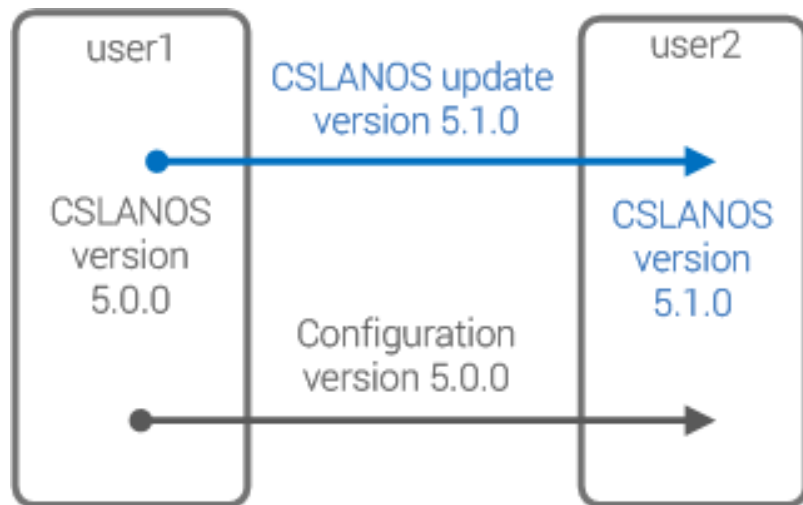


Figure 24 : Updating the operating system CSLANOS in boot partition user2

- If you have currently booted the **user2** boot partition, the update is imported to the **user1** boot partition. Your individual configuration settings are then transferred from the **user2** boot partition to the **user1** boot partition.

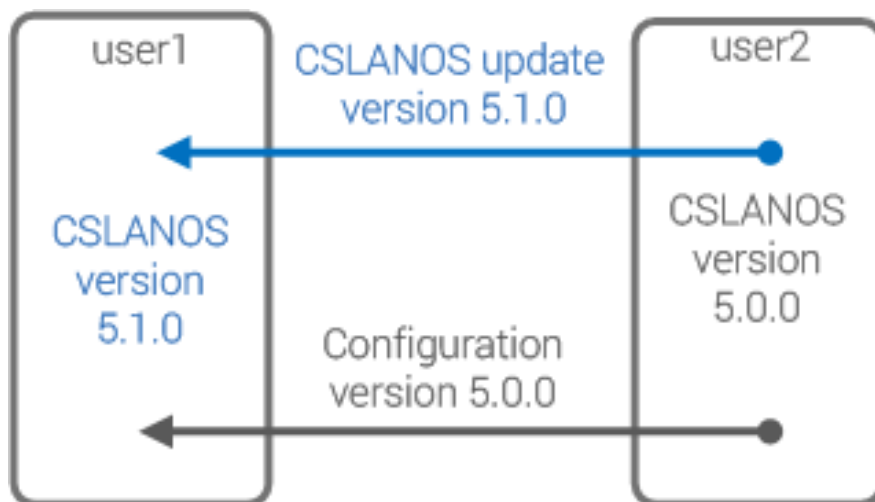


Figure 25 : Updating the operating system CSLANOS in boot partition user1

4.8.1.1 Performing a Local Update

Prerequisites

- You must already have copied the new version of `cslan-x.y.z.tar.gz` to the main directory of a trustworthy USB flash drive.

- You have booted the appropriate boot partition of the device:
 - If you want to update the boot partition **user1**, you must have booted the boot partition **user2**.
 - If you want to update the boot partition **user2**, you must have booted the boot partition **user1**.
 - If you have booted factory, you can choose to update either boot partition **user1** or boot partition **user2**.

This is how you update the operating system for the device:


1. On the front panel of the device, press the → key.
2. Press **ENTER** to open the **CSLAN admin.** menu item.
3. Use the ↓ key to select **Update & Maint.** and press **ENTER**.
4. Press **ENTER** to open the **Update** menu item. Follow the instructions on the display.
 - a. Connect a USB flash drive to the **Host1** or **Host2** USB port on the front panel of your device.

The `cslan-x.y.z.tar.gz` file you want to upload has to be placed in the main directory of a trustworthy USB flash drive, so that it is shown on the display of the device and can be selected for upload.



The device can access data from and write data on only a single trustworthy USB flash drive connected to it. Although more than one USB flash drives can be simultaneously connected to the device, the USB device that has been inserted as first gets connected with the device. To establish a connection to another USB flash drive, you should first disconnect the currently connected one and then plug the next USB flash drive into the corresponding USB port of the device.

- b. Press **ENTER**. Now you should see the files available in the main directory of the connected USB flash drive.
 - c. If you have currently booted the **factory** boot partition, you must select the boot partition into which you want to import the update: **user1** or **user2**. Use the ↑ and ↓ keys to select either **Partition: user1** or **Partition: user2**.
 - d. If you have currently booted the **user1** boot partition, you cannot select a boot partition into which you want to import the update. It is automatically set to **user2**.

- e. If you have currently booted the **user2** boot partition, you cannot select a boot partition into which you want to import the update. It is automatically set to **user1**.
 - f. Use the ↑ and ↓ keys to select the required `cs1an-x.y.z.tar.gz` file and press **ENTER**.
 - g. Use the ↑ and ↓ keys to select **[Start update]** and press **ENTER**. The successful update of the operating system of the device is confirmed on the display.
 - h. Press **ESC** to get back to the device menu.
5. Select the boot partition to which you imported the update.
- a. Use the ↓ key to select **Set boot partition** and press **ENTER** to open the menu item.
One of the entries (factory, user1 or user2) is indicated by a full circle.
 - If the circle is currently set for the boot partition **user1**, the currently used boot partition is **user1**. The operating system update has been performed in boot partition **user2**. So you have to select boot partition **user2**.
 - If the circle is currently set for the boot partition **user2**, the currently used boot partition is **user2**. The operating system update has been performed in boot partition **user1**. So you have to select boot partition **user1**.
- 

Consider that device uses different SSH keys for each boot partition. An SSH key is created for a boot partition when the device is booted for the very first time from this boot partition.
- b. Use the ↑ and ↓ keys to move to the boot partition you want to use after a restart and confirm your selection by pressing **ENTER**.
 - c. Press **ESC** twice to get to the **CSLAN admin.** menu.
6. Remove the USB flash drive from the **Host1** or **Host2 USB** port on the front panel of your device.
7. Reboot the device so you can start using the selected boot partition.
- a. Use the ↓ key to select **Reboot** and press **ENTER** to open the menu item.

- b. Press the ← or → keys to insert the **x** in the brackets [**x**] **Yes** and confirm by pressing **ENTER**.

This restarts the device, and then boots the boot partition you have just selected.

8. Reboot the device so the operating system update comes into effect, and the change of boot partition is applied.



The local update has been performed successfully.

4.8.1.2 Performing a Remote Update

If you do not have a direct/local access to the CryptoServer LAN, you can also update the operating system of the CryptoServer LAN remotely using an SSH client (for example with PuTTY under Windows) from a host computer in the same network.

Prerequisites

- You have the new `cslan-x.y.z.tar.gz` at hand (product CD or boot stick).
- You have enabled the SSH daemon locally by using the control menu buttons of the CryptoServer LAN. see [Setting up Dynamic IPv4 Addresses With the Front Panel \(p. 34\)](#).
- You have booted the appropriate boot partition of the CryptoServer LAN locally, see [Selecting a Boot Partition \(p. 86\)](#) or remotely by using SSH access and command line `set_boot.sh <boot partition>` and rebooting the CryptoServer LAN afterwards with reboot:
 - If you want to update the boot partition **user1**, you must have booted the boot partition **user2**.
 - If you want to update the boot partition **user2**, you must have booted the boot partition **user1**.
 - If you have booted **factory**, you can choose to update either boot partition **user1** or boot partition **user2**.

To update the operating system of the CryptoServer LAN remotely, proceed as follows:

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
2. Copy the `cslan-x.y.z.tar.gz` to the CryptoServer LAN root directory.

3. Call the script `update.sh` in the same directory where you have previously copied the `cslan-x.y.z.tar.gz` file:
`update.sh cslan-x.y.z.tar.gz [partition]`
The `partition` entry – **user1** or **user2** – is only required if the currently booted partition is factory.
Example: `update.sh cslan-x.y.z.tar.gz`
4. Set the boot partition you have just updated to be started after reboot:
`set_boot.sh <boot partition>`
5. Reboot the CryptoServer LAN:
`reboot`
6. Check that the updated boot partition has been started by executing the script `get_boot.sh`. The output is either **user1** or **user2**.
7. Execute `csadm [Dev=<device>] CSLGetVersion` to check that the required version of the CryptoServer LAN has been installed.



The remote update has been performed successfully.

4.8.2 Selecting a Boot Partition

This section describes how to use the menu options to select the CryptoServer LAN's boot partition. For details about the boot partitions, see [Boot Partitions in the CryptoServer LAN](#) (p. 17).



Consider that CryptoServer LAN uses an SSH key only for one boot partition. An SSH key is created for a boot partition when the CryptoServer LAN is booted for the very first time from this boot partition.

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.
2. Press the ENTER button to open the **CSLAN admin.** menu item.

3. Use the ↓ button to select **Update & Maint.** and press the **ENTER** button to open the menu item.
4. Use the ↓ button to select **Set boot partition** and press the **ENTER** button to open the menu item.
The currently applied setting (**factory**, **user1** or **user2**) is indicated by a full circle.
5. Use the ↓ button to select the desired entry and press the **ENTER** button.
6. Use the ← or the → button to insert the x in the brackets **[x] Yes** and confirm by pressing the **ENTER** button.
7. Press the **ESC** button to leave the **Update & Maint.** menu and enter the **CSLAN admin.** menu.
8. Reboot the CryptoServer LAN so you can start using the selected boot partition.
 - a. Use the ↓ button to select **Reboot** and press the **ENTER** button to open the menu item.
 - b. Use the ← or the → button to insert the x in the brackets **[x] Yes** and confirm by pressing the **ENTER** button. This restarts the CryptoServer LAN, and then boots the boot partition you have just selected.



The boot partition has been selected and applied successfully.

4.8.3 Reverting the Configuration of the CryptoServer LAN

Resetting the configuration of the CryptoServer LAN means you reset the entire configuration in a particular boot partition. This process deletes all the settings you have made in this boot partition.

Prerequisites

Before you reset the CryptoServer LAN configuration in a particular boot partition you may need to select the boot partition you require as described in [Selecting a Boot Partition \(p. 86\)](#).

To reset the configuration of the CryptoServer LAN in a specific boot partition, follow these steps:

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.

2. Press the **ENTER** button to open the **CSLAN admin.** menu item.
3. Use the ↓ button to select **Update & Maint.** and press the **ENTER** button to open the menu item.
4. Use the ↓ button to select **Revert configuration** and press the **ENTER** button to open the menu item.
5. Respond to the prompt Really revert '**factory**' | '**user1**' | '**user2**' by pressing the ← or the → button to insert the x in the brackets **[x] Yes** and then press **ENTER** to confirm.
6. Reboot the CryptoServer LAN, see [Rebooting the CryptoServer LAN \(p. 89\)](#), to reset the configuration.



The CryptoServer LAN has the default configuration as provided on delivery by the manufacturer Utimaco.



Now change the default password for the root user, see [Changing the Default Passwords \(p. 27\)](#).
Make sure that you have booted the same boot partition as the one you have previously reverted to default configuration.

4.8.4 Verifying the Reachability in the Network (ping)

You can send Internet Control Message Protocol (ICMP) messages (pings) from the device to check whether the device can contact other computers over the network.

To send a ping from the device:

1. On the front panel of the device, press **ENTER**.
2. Press **OK** to open the **CSLAN admin.** menu item.
3. Use the ↓ key to select **Update & Maint.** and press **ENTER**.
4. Use the ↓ key to select **Ping IP4 address** and press **ENTER** to open the menu item.

5. You can enter the IP address of the computer to which you want to send the ping.
The cursor under a number shows that you can change that number with the ← and → keys. Press the → key to move the cursor to the next number.
If you have selected the symbol ■ by using the ← and → keys you can use the → key to insert a zero at this point or you can use the ← key to delete the current symbol.
If the cursor is positioned on the right below the last symbol, you can use the → key to insert a zero at this point. If you press the → key several times, the zero entry will be repeated.
6. Use the menu options to assign an IPv4 address for the network connection you require and press **ENTER**.
7. Use the ← or → keys to insert the x in the brackets [x] **Yes** and confirm by pressing **ENTER**. A success message is displayed.



The reachability in the network has been verified successfully.

4.9 Rebooting the CryptoServer LAN

Some of the settings you make on the CryptoServer LAN requires you to reboot the device before the changes come into effect.

There are the following options to reboot the CryptoServer LAN:

- **Local command-line**
Perform the reboot command
- **Remote command-line**
 - a. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
 - b. Perform the reboot command.
- **Front panel**
 - a. On the front panel of the CryptoServer LAN, press the **ENTER** button.
 - b. Press the **ENTER** button to open the **CSLAN admin.** menu item.

- c. Use the ↓ button to select Reboot and press the **ENTER** button to open the menu item.
- d. Use the ← or the → button to insert the x in the brackets **[x] Yes** and confirm by pressing the **ENTER** button.
After a few seconds, this reboots the CryptoServer LAN.

4.10 Shutting down the CryptoServer LAN

There are the following options to shut down the CryptoServer LAN:

- **Local command-line**

Perform the following command.

```
shutdown -h now
```

The `-h` option is necessary. Otherwise, only the CryptoServer shuts down but not the CryptoServer LAN.

- **Remote command-line**

- a. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#)
- b. Perform the following command.

```
shutdown -h now
```

The `-h` option is necessary. Otherwise, only the CryptoServer shuts down but not the CryptoServer LAN.

- **Front panel**

- a. On the front panel of the CryptoServer LAN, press the **ENTER** button.
- b. Press the **ENTER** button to open the **CSLAN admin.** menu item.
- c. Use the ↓ button to select Shutdown and press the → button to open the menu item.
- d. Use the ← or the → button to insert the x in the brackets **[x] Yes** and confirm by pressing the **ENTER** button.
The CryptoServer LAN then shuts down after a few seconds.



The CryptoServer LAN should be kept running constantly to prevent the batteries from being used. If a system is inactive for a long period, the batteries will be used up. After a while this can result in the CryptoServer no longer being supplied with power, and all the data will be deleted. The resulting maintenance tasks are not covered by Utimaco IS GmbH's liability. On the other hand, a brief interruption to the power supply (if the device is being moved around etc.) does not place a serious demand on the batteries and consequently there is no danger of data and settings etc. being deleted.

4.11 Setting up PCIe Clock Cards

As of CSLANOS v5.1, the CryptoServer LAN supports PCIe clock cards providing a permanent time source for the NTP daemon on the CryptoServer LAN.

Examples for PCIe clock cards:

- Meinberg GPS180PEX using the GPS time as input
- Meinberg PZF180PEX using the DCF77 time signal as input (PZF: Pseudozufallsfolge, pseudo-random sequence)

The PCIe clock cards are already mounted on the CryptoServer LAN.



The CryptoServer LAN retrieves its time from a time source. This time source might be an NTP server. As of CSLANOS 5.1, a PCIe clock card is supported as a time source as well.

If you set the time on the CryptoServer LAN manually and if this causes the time difference between the time on the CryptoServer LAN and the time of the time source to be larger than 1000 s, this causes an error message and the NTP daemon is terminated automatically. In such case, the time on the CryptoServer will not be set.

To set up the PCIe clock card, proceed as follows:

1. Switch off the CryptoServer LAN by pressing the f8 button.



Figure 26 : Front view of the device

2. Attach the antenna cable to the right BNC port (a14) of the PCIe clock card (a11) according to the antenna manufacturer's manual.

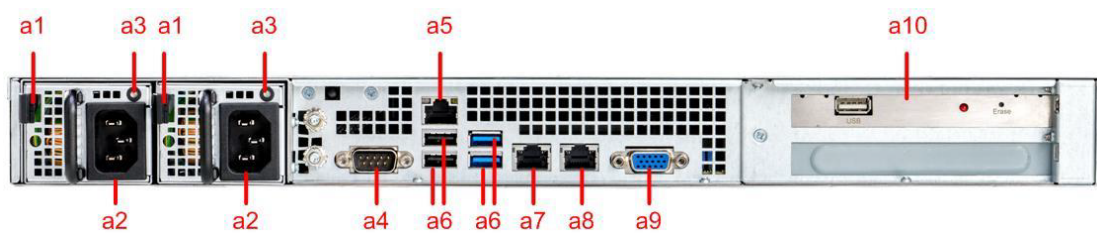


Figure 27 : Rear view of the device



Figure 28 : PCIe Clock Card



Figure 29 : Sample for a DCF77 antenna with cable

3. Switch on the CryptoServer LAN by pressing the f8 button.
4. Position and align the antenna according the antenna manufacturer's manual.
The signal strength shown at **CSLAN admin. > CSLAN Info > Show time source** may help you to do so, see [Showing the PCIe Clock Card Information \(p. 79\)](#).
5. Verify in the antenna manufacturer's manual whether an LED (a13) on the PCIe clock card should indicate a certain status.
6. To set up NTP, follow the instructions in [Setting up NTP \(p. 95\)](#). Consider the differences described below.

The differences between a CryptoServer LAN with and without a PCIe clock card are as follows.

- **Disabled menu items**

The following menu items are shown on the display but they are disabled. This is indicated on the display by a small no way sign to the right of the menu item.

- **CSLAN admin. > Configuration > Services > NTP server IP addr.**
- **CSLAN admin. > Configuration > CSLAN > Set Time**

- **New menu item**
 - CSLAN admin. > CSLAN Info > Show time source, see [Showing the PCIe Clock Card Information \(p. 79\)](#)

- **Changed menu item**
 - CSLAN admin. > CSLAN Info > Show services info > NTP IPv4
This menu item does not show a reachable IP address but 127.127.28.0 to indicate to the NTP daemon to get the time from the PCIe clock card.

- **The `/etc/ntp.conf` file**

The NTP configuration of a CryptoServer LAN with a PCIe clock card differs slightly from the usual case. The IP address given by the server parameter in the `/etc/ntp.conf` file is not a reachable IP address but indicates to the NTP daemon to get the time from the PCIe clock card.

Example for the `/etc/ntp.conf` file:

```
# Servers can be configured with ip address only!
# This configuration doesn't allow request from non-configured IP addresses

server 127.127.28.0 minpoll 4 maxpoll 4 iburst

restrict 127.0.0.1
restrict default ignore d

riftfile /var/tmp/ntp.drift
pidfile /var/run/ntpd.pid
```

Additional servers may be configured. This can only be done by editing the `/etc/ntp.conf` file but not by using the `set_ntpd_server_config.sh` script or by using the front panel of the CryptoServer LAN. To do so, first log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#). Then edit the file and perform the following command to apply the changes.

```
/etc/init.d/ntpd restart
```

- **The `/etc/sysconfig/ntpd` file**

On the CryptoServer LAN with PCIe clock card support, the NTP daemon is enabled by default. In contrast to the CryptoServer LAN versions without a PCIe clock card, `ntpd` is not executed at the `ntpd` start because the given server IP address for the PCIe clock card is not accessible by `ntpd`. To ensure that the time can be set at the start, `ntpd` is started with the `-g` option, which causes `ntpd` to set the system time once regardless of

the time difference.

Example for the `/etc/sysconfig/ntpd` file:

```
# Begin /etc/sysconfig/ntpd

# Default settings for ntpd. This file is sourced by /bin/sh from
# /etc/init.d/ntpd.

# Start ntpclient yes|no
START_NTPD="yes"

# ntpd uses Meinberg Card as time source
# Do not change this!
USE_MBG="yes"

# Options to pass to ntpd
NTPD_OPTS="-g"

# End /etc/sysconfig/ntd
```

4.12 Setting up NTP

The Network Time Protocol (NTP) is a standard for synchronizing clocks in computer systems via packet-based communication networks.

The following subsections describe how to set up NTP for the CryptoServer.



If there is a CryptoServer CP5 in your CryptoServer LAN, NTP is not supported.

To verify whether a CryptoServer CP5 is in your CryptoServer LAN, perform the steps in section [Showing Files in the CryptoServer \(p. 153\)](#) and select **List FLASH files** in step 4. If there is a CryptoServer CP5 available, some lines in the output contain `CP5`.

Output example:

```
...
FLASH\adm.msc 75644 ADM 0x087 C64 3.0.25.4 Administration Module
CP5
...
FLASH\cmds.msc 91580 CMDS 0x083 C64 3.6.0.6 Command Scheduler CP5
FLASH\cxi.msc 274380 CXI 0x068 C64 2.2.3.4 Crypto.eXtended Interf.
CP5
...
FLASH\mbk.msc 66252 MBK 0x096 C64 2.2.7.3 Master Backup Key Module
CP5
```

...

FLASH\smos.msc 240972 SMOS 0x000 C64 5.5.9.1 Operating System CP5

...

FLASH\util.msc 17452 UTIL 0x086 C64 3.0.5.0 Utility Module CP5

This action is equivalent to the `csadm ListFiles` command, see *ListFiles* in the [CryptoServer Se-Series Gen2 CP5 – Administration Manual \(p. 240\)](#) for the CryptoServer CP5 variant and see *ListFiles* in the [CryptoServer – csadm Manual \(p. 240\)](#) for the non-CP5 CryptoServer variant.

4.12.1 Preparations

The following software is involved in time synchronization.

- **NTP daemon**

When you run the NTP daemon on the CryptoServer LAN, the time is automatically synchronized from the NTP server to the CryptoServer LAN.

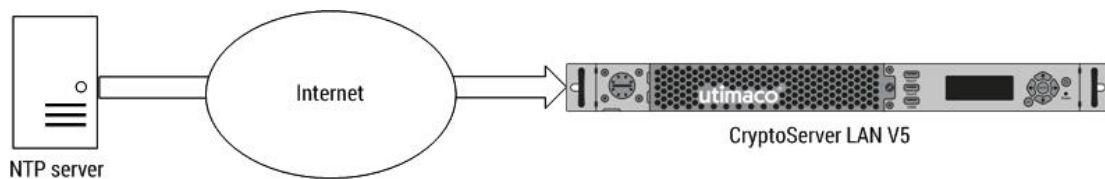


Figure 30 : Automatic time synchronization from an NTP server to the CryptoServer LAN



The CryptoServer LAN retrieves its time from a time source. This time source might be an NTP server. As of CSLANOS 5.1, a PCIe clock card is supported as a time source as well. If you set the time on the CryptoServer LAN manually and if this causes the time difference between the time on the CryptoServer LAN and the time of the time source to be larger than 1000 s, this causes an error message and the NTP daemon is terminated automatically. In such case, the time on the CryptoServer will not be set.

- **NTP client**

When you run the NTP client on the CryptoServer LAN, the time is automatically synchronized from the CryptoServer LAN to the CryptoServer, i.e., to the CryptoServer PCIe card mounted in the CryptoServer LAN.

`ntpcclient` is a daemon written by Utimaco IS GmbH and it is not a standard Linux tool

like `ntpd` or `ntdupdate`. Perform the `ntpcclient -h` command for the online help.

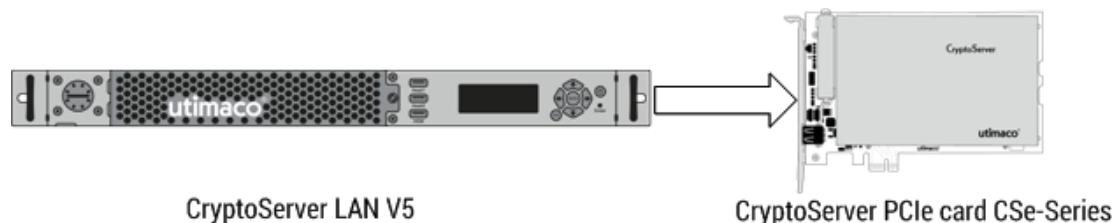


Figure 31 : Automatic time synchronization from the CryptoServer LAN to the CryptoServer PCIe card



If a time difference between the time on the CryptoServer LAN and the time on the CryptoServer that is greater than certain thresholds, the time on the CryptoServer is not corrected but an error message is created instead, see [Configuring Time Synchronization between the CryptoServer LAN and the CryptoServer \(p. 124\)](#).

▪ NTP firmware module

The NTP firmware module is a software component running on the CryptoServer. Among other things, it is needed to verify some actions the NTP client performs.

Prerequisites

- Unless you use a local command-line on the CryptoServer LAN, make sure that the SSH daemon has been enabled, see [Enabling/Disabling the SSH Daemon \(p. 45\)](#). By default, the SSH daemon is enabled. A remote or local command-line is needed in any case for performing certain commands on the CryptoServer LAN.
- Setting up NTP needs a user account on the CryptoServer with NTP management permissions. This user account is needed on the CryptoServer PCIe card, not on the CryptoServer LAN, and it will be created in the chapters below.
- For details about authentication mechanisms, see [CryptoServer – Administration Manual \(p. 240\)](#).
- Clarify whether you perform some steps with physical local access to the CryptoServer LAN by using the front panel of the CryptoServer LAN and a PIN pad or whether you mainly use scripts. In the first case, continue with the instructions in [Setting up NTP Mainly Using the Front Panel \(p. 98\)](#). In the latter case, continue with [Setting up NTP Mainly Using Scripts \(p. 108\)](#). The effect of the instructions in these chapters are identical.



Not all steps can be performed remotely. At least the actual time synchronization step must be authenticated by a PIN pad that either is connected to the CryptoServer LAN or to the CryptoServer (PCIe card).

4.12.2 Setting up NTP Mainly Using the Front Panel

To set up NTP, perform the following steps.



Ensure you perform the individual steps in exactly the sequence described.

1. Creating an NTP manager user account

To perform this step, you can use the csadm command-line tool. For details, see [CryptoServer – csadm Manual \(p. 240\)](#).

Use the CryptoServer Administration Tool (CAT) to set up one or two user accounts for NTP administration (NTP Manager). CAT provides the appropriate role-based user profiles **NTP Manager one-person rule** and **NTP Manager two-person rule**. For details, see [CryptoServer – CAT Manual \(p. 240\)](#).

- a. Start CAT on your administration computer.
- b. Click the **Login/Logoff** button in the toolbar.
- c. Select a user with at least the permission 20000000.
- d. Click the **Login** button.

The dialog box Choose **User Token for Login** opens.

- e. Select the appropriate authentication mechanism.

- **Smartcard Token**

If the user is using an RSA or an ECDSA user authentication key stored on a smartcard, click **Smartcard Token** and then click OK in the Choose **User Token for Login** dialog box. Follow the instructions on the PIN pad.



Consider that if the selected user manager uses the RSA smartcard authentication, the PIN pad must be connected either to the USB port labelled HSM on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) at the rear side of the CryptoServer LAN. For details about the USB ports, see [Connecting the PIN Pad \(p. 42\)](#).

Only if the selected user manager uses RSA signature authentication with a smartcard or ECDSA signature authentication with a smartcard, the PIN pad must be connected to the computer CAT is running on.

As an alternative you may use a USB port of any computer in the network. For details, see *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual \(p. 240\)](#). For details about the authentication mechanism, see *Authentication Mechanisms* in the [CryptoServer – Administration Manual \(p. 240\)](#).

• Keyfile Token

If the user is using an RSA or ECDSA user authentication key stored in a keyfile,

click Keyfile Token, and proceed as follows:

1. Click the search button (...) next to the **Key Path** text box.
The **Set Name and Path for User Keyfile Token** dialog box opens.
2. Select the keyfile you require, e.g., `ADMIN.key`.
3. Click Open.
4. In case the keyfile is protected with a password, enter the password in the **Password** text box of the **Choose User Token for Login** dialog box.
5. If the user is using a password for authentication, click **Keyfile Token**, and enter the password in the Password text box.
- f. Click **OK** in the **Choose User Token for Login** dialog box. The dialog box closes. If the user login succeeded, a green check mark appears on the left hand side of the user item.
- g. Click **Close** to close the **Logon/Logoff User** dialog box.
- h. Click the **Manage User** button in the toolbar.
- i. In the **User Management** dialog box, click the **Add User** button.
- j. In the **Name of New User** field, enter a unique name for the NTP Manager.



Do not use the characters <, >, :, ", !, ?, *, /, \, | in user names.

- k. Under **User Profile**, select the NTP Manager one person rule option if you only want to set up one NTP user. If you want to set up secondary confirmation, select NTP manager two-person rule.
- l. Under **Authentication Mechanism**, select the required authentication mechanism.



Select either **Smartcard (RSA Signature)**, **Keyfile (RSA Signature)**, **Smartcard (ECDSA Signature)**, **Keyfile (ECDSA Signature)** or **Smartcard (PIN Pad at CryptoServer)**.

If you select the RSA smartcard authentication (Smartcard (PIN Pad at CryptoServer) radio button), this means that once the new user is created this user needs a PIN pad directly connected to the USB port labelled HSM on the front panel of the CryptoServer LAN

or to the USB port of the CryptoServer (PCIe card) at the rear side of the CryptoServer LAN.

Do not select the HMAC password authentication (Password (HMAC) radio button) because this authentication mechanism is not supported by some actions described below in certain situations.

- m. Enter an attribute if you wish to do so.
- n. Click **OK**.
 - i. If you have selected the HMAC password authentication mechanism (**Password (HMAC)** radio button), the **Set Password of new User** dialog box opens.
 If you want to enable the NTP firmware module by using a remote command-line, do not select Password (HMAC) because the script used in this command-line does not support HMAC password authentication. However, if you want to enable the NTP firmware module by using CAT, HMAC password authentication is supported.
 In addition to that, if you select the **HSM time sync** menu item at a later date without having enabled the NTP firmware module before, a script for enabling the NTP firmware module is performed automatically. This script

needs the NTP manager for authentication but does not support HMAC password authentication. This means that if you want to use HMAC password authentication for the NTP manager, you always have to manually enable the NTP firmware module by using CAT before enabling the time synchronization.

- Enter a unique, secure password in the **Password** text box.
 - Confirm your password entry in the **Confirm Password** text box.
 - Close the **Set Password of new User** dialog box by clicking **OK**. The dialog box **Add User** closes automatically.
- ii. If you have selected the authentication mechanism **Smartcard (RSA Signature)**, **Smartcard (ECDSA Signature)** or **Smartcard (PIN Pad on CryptoServer)**, the **Choose User Token to Add a New User** dialog box opens with preselected option **Smartcard Token**.
- Connect the PIN pad to the computer CAT is running on.
 - Click the **OK** button and follow the instructions on the display of the PIN pad.
 - Insert the smartcard, where the key is stored on, and press **OK** on the PIN pad. The dialog box **Add User** closes automatically.
- iii. If you have selected the authentication mechanism **Keyfile (RSA Signature)** or **Keyfile (ECDSA Signature)**, the **Choose User Token to Add a New User** dialog box opens with preselected option **Keyfile Token**.
- Click the **OK** button.
 - Click the search button (...) next to the **Key Path** field.
 - Select the keyfile path and click **Open**.
 - Click **OK** in the **Choose User Token to Add a New User** dialog box. The dialog box **Add User** closes automatically.
- o. The new user is created and appears in the list of users in the User Management dialog box.
- If you want to set up the two-person rule for NTP users, you must now use the procedure described above to set up another NTP user account (NTP Manager two-person rule).

2. Editing the `/etc/csxlan.conf` file

The following substeps describe how to store the names of the NTP manager created above and the user manager used above to create the NTP manager. The names are

stored in the `/etc/csxlan.conf` file. Thus, certain actions initiated by using the menu control buttons on the front panel of the CryptoServer LAN can be authenticated by the appropriate user accounts.

- a. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
- b. Open the `/etc/csxlan.conf` file with a text editor.
- c. Search for the `[CryptoServer]` section in this file.
- d. Search for the parameters `AdminName` and `NTPManagerName` within this section.
- e. If they are not available, create them.
- f. Assign the user name of the user manager and of the NTP Manager to them.

Example: Example:

```
[CryptoServer]
AdminName=ADMIN
NTPManagerName=ntp
```



Do not store user names using the HMAC password authentication because this authentication mechanism is not supported by some of the actions performed below.

For details about the authentication mechanism, see *Authentication Mechanisms* in the [CryptoServer – Administration Manual \(p. 240\)](#).

- g. Save the changes and close the text editor.
 - h. Do not close the SSH connection. Depending on your preferences, it is needed below.
3. As of CSLANOS v5.1, PCIe clock cards providing a high-precision time signal received by radio are supported. For details, see [Setting up PCIe Clock Cards \(p. 91\)](#). If a PCIe clock card is mounted on the CryptoServer LAN, continue with step 6 because the NTP server's IP address cannot be set manually and the NTP daemon is started by default. If no PCIe clock card is mounted, continue with step 4. To verify whether a PCIe clock card is mounted, open **CSLAN admin. > CSLAN Info > Show services info > NTP IPv4** on the display on the front panel. If it shows `127.127.28.0`, a PCIe clock card is mounted. As an alternative, log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#) and verify whether the following line is present in the `/etc/ntp.conf` file:

```
server 127.127.28.0 minpoll 4 maxpoll 4 iburst
```

If this line is present, a PCIe clock card is mounted.

4. Configuring the NTP server's IP address

- a. Press the **ENTER** button on the front panel of the CryptoServer LAN.
- b. Press the **ENTER** button to select **CSLAN admin..**
- c. Press the **ENTER** button to select **Configuration**.
- d. Press the ↓ button to select **Services** and confirm by pressing **ENTER**.
- e. Press the ↓ button to select **NTP Server IP4 addr.** and confirm by pressing **ENTER**.



The cursor under a number shows that you can change that number with the ← and → buttons. Press the → button to move the cursor to the next number. Press the ← button to move the cursor back to the previous symbol.

If you have selected the symbol ■ by using the ← and → buttons you can use the ↓ button to insert a zero at this point or you can use the ← button to delete the current symbol.

If the cursor is positioned on the right below the last symbol, you can use the → button to insert a zero at this point. If you press the → button several times, the zero entry will be repeated.

- f. Use the menu options to assign an IPv4 address for the network connection you require and press the **ENTER** button.
- g. If you have assigned a valid IP address, respond to the prompt that follows with Yes, by pressing the ← or → button to insert the x in the brackets **[x] Yes** and confirm by pressing the **ENTER** button.
- h. You see a system message that you have performed the configuration successfully. Confirm by pressing **ENTER**.

5. Starting the NTP daemon

- a. Press the **ENTER** button on the front panel of the CryptoServer LAN.
- b. Press the **ENTER** button to select **CSLAN admin..**
- c. Press the **ENTER** button to select **Configuration**.
- d. Press the ↓ button to select **Services** and confirm by pressing **ENTER**.
- e. Press the ↓ button to select **NTP** and confirm by pressing **ENTER**.
The currently applied setting (disabled or enabled) is indicated by a full circle.

- f. Use the → button to select enabled and press the **ENTER** button to open the menu item.
 - g. Use the ← or the → button to move the x into the square brackets **[x] Yes** and confirm by pressing **ENTER**.
 - h. You see a system message that you have performed the configuration successfully. Confirm by pressing **ENTER**.
6. Enabling the NTP firmware module on the CryptoServer

If you want to use CAT (CryptoServer Administration Tool) to enable the NTP firmware module, perform the following substeps. However, if you want to use a remote command-line to do so, continue with step 7.

 - a. Start CAT on your administrator computer.
 - b. Click the **Login/Logoff** button in the toolbar.
 - c. Select a user with at least the permission 00200000, for example, the user account(s) created in the preceding step.
 - d. Click the **Login** button. The dialog box **Choose User Token for Login** opens.
 - e. Select the appropriate authentication mechanism.
 - **Smartcard Token**

If the user is using an RSA or an ECDSA user authentication key stored on a smartcard, click Smartcard Token, and proceed as follows:

 1. If the NTP manager to be logged in uses RSA signature authentication with a smartcard or ECDSA authentication with a smartcard, connect the PIN pad to a USB port of the computer CAT is running on. As an alternative you may use a USB port of any computer in the network. For details, see *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual \(p. 240\)](#).
 2. However, if the NTP manager uses RSA smartcard authentication, connect the PIN pad to the USB port labelled **HSM** on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN.
 3. Click **OK** in the **Choose User Token for Login** dialog box. The dialog box closes. Follow the instructions on the PIN pad.
 - **Keyfile Token**

- If the user is using an RSA or ECDSA user authentication key stored in a keyfile, click **Keyfile Token**, and proceed as follows:
 - a. Click the search button (...) next to the Key Path text box. The **Set Name and Path for User Keyfile Token** dialog box opens.
 - b. Select the keyfile you require, e.g., `NTP.key`.
 - c. Click **Open**.
 - d. In case the keyfile is protected with a password, enter the password in the **Password** text box of the **Choose User Token for Login** dialog box.
 - e. If the user is using a password for authentication, click **Keyfile Token**, and enter the password in the **Password** text box. Click **OK** in the **Choose User Token for Login** dialog box. The dialog box closes.
 - f. If the user login succeeded, a green check mark appears on the left hand side of the user item.
 - g. Click **Close** to close the **Login/Logoff User** dialog box.
 - h. Click on **Manage** in the menu bar and select the **NTP Settings...** menu item. The **Network Time Protocol (NTP) Configuration** dialog box opens.
 - i. Select **Enabled**.
 - j. Optionally, you can change the default values for Max. time to set per day and Max. time to set per operation. We recommend not to change these default values, see [Configuring Time Synchronization between the CryptoServer LAN and the CryptoServer \(p. 124\)](#).
 - k. Click **Apply** to transfer the values you have entered to the CryptoServer.
 - l. Finish entering your data in this dialog box by clicking on **OK**. The dialog box **Network Time Protocol (NTP) Configuration** closes.
 - m. Open **Manage > NTP Settings... > NTP Status in CAT** again to verify the result.
 - n. Continue with step 8.
7. If you want to use a remote command-line to enable the NTP firmware module, perform the following substeps.
- a. Verify that the SSH connection established above is still open.
 - b. Connect the PIN pad to the appropriate USB port.

- If the user name you use in the next step uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a smartcard or a keyfile), connect the PIN pad to the USB port labelled Host1 or Host2 on the front panel of the CryptoServer LAN or to one of the USB ports on the rear side of the CryptoServer LAN (a6).
As an alternative you may use a USB port of any computer in the network. For details, see *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual \(p. 240\)](#).
 - If the user name you use in the next step uses RSA smartcard authentication, connect the PIN pad to the USB port labelled **HSM** on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN (a10). For further information, see [Connecting the PIN Pad \(p. 42\)](#).
- c. Perform the following command to enable the NTP firmware module.
- ```
activate_ntp_module.sh <user name> yes
```
- `<user name>` is the user with at least permission 00200000 that you have created in step 1.
- Only users with RSA signature authentication, ECDSA signature authentication and RSA smartcard authentication are supported. Users with HMAC password authentication are not supported.
- Output: `Activate time synchronisation Enter Smart card PIN for ntp!`
- d. Follow the instructions shown on the display of the PIN pad.
- Output in the command-line: `ANSW:`
- e. Open **Manage > NTP Settings... > NTP Status in CAT** to verify the result.
- f. Continue with step 8.
8. Starting the time synchronization from the CryptoServer LAN to the CryptoServer
- When the time between the NTP server and the CryptoServer LAN (host time; system time) has been synchronized, it is important to synchronize the time between the CryptoServer LAN and the CryptoServer (PCIe card) mounted into the CryptoServer LAN. Otherwise, a time difference (deviation) between the time on the CryptoServer LAN and the time on the CryptoServer (PCIe card) might become greater than the maximum time deviation permitted for the time on the CryptoServer per day. This would cause an error, and the clock of the CryptoServer will not be set.

- a. Starting the time synchronization needs to be authenticated by a user manager (minimum permission 20000000) being specified by the `AdminName` parameter in the `/etc/csxlan.conf` file. Connect the PIN pad to the appropriate USB port.
  - If the user name you use in the next step uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a smartcard or a keyfile), connect the PIN pad to the USB port labelled **Host1** or **Host2** on the front panel of the CryptoServer LAN or to one of the a6 USB ports on the rear side of the CryptoServer LAN.  
Chapter *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual](#) (p. 240) does not apply here.
  - If the user name you use in the next step uses RSA smartcard authentication, connect the PIN pad to the USB port labelled **HSM** on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN (a10). For further information, see [Connecting the PIN Pad](#) (p. 42).
- b. Press the **ENTER** button on the front panel of the CryptoServer LAN.
- c. Press the ↓ button to select the **HSM admin.** menu item and confirm by pressing **ENTER**.
- d. If CSLANOS < 5.1.0: Press the ↓ button to select the **Key&file admin.** menu item and confirm by pressing **ENTER**.
- e. Press the ↓ button to select the **HSM time sync** menu item and confirm by pressing **ENTER**.  
The currently applied setting (disabled or enabled) is indicated by a full circle.
- f. Use the ↓ button to select **enabled** and press the **ENTER** button to open the menu item.
- g. Use the ← key to move the x into the brackets **[x] Yes** and then press **ENTER**.  
This action starts the NTP client and causes a periodic transfer of the CryptoServer LAN time to the CryptoServer (PCIe card).
- h. Follow the instructions on the display of the PIN pad to authenticate the time synchronization. The PIN of the user manager defined by the `AdminName` parameter in the `/etc/csxlan.conf` file is needed.  
If you select the **HSM time sync** menu item and confirm by pressing **ENTER** at a later date, the NTP firmware module might not be enabled. In this case, the PIN of the NTP manager defined by the `NTPManagerName` parameter in the `/etc/csxlan.conf` file is needed as well. Depending on this NTP manager's

authentication mechanism, the PIN pad might need to be connected to a different USB port than for the user manager.

- i. You see a system message that you have performed the configuration successfully. Confirm by pressing **ESC**.



The NTP was successfully set up.

---

### 4.12.3 Setting up NTP Mainly Using Scripts

To set up NTP, perform the following steps.



Ensure you perform the individual steps in exactly the sequence described.

- 
1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
  2. Creating an NTP manager user account  
To perform this step, you can use the csadm command-line tool. This is not described in this manual. For details, see [CryptoServer – CAT Manual \(p. 240\)](#).  
Use the CryptoServer Administration Tool (CAT) to set up one or two user accounts for NTP administration (NTP Manager). CAT provides the appropriate role-based user profiles **NTP Manager one-person rule** and **NTP Manager two-person rule**. For details, see [CryptoServer – CAT Manual \(p. 240\)](#).
    - a. Start CAT on your administration computer.
    - b. Click the **Login/Logoff** button in the toolbar.
    - c. Select a user with at least the permission 20000000.
    - d. Click the **Login** button.  
The dialog box Choose User Token for Login opens.
    - e. Select the appropriate authentication mechanism.



- **Smartcard Token**

If the user is using an RSA or an ECDSA user authentication key stored on a smartcard, click **Smartcard Token** and then click **OK** in the **Choose User Token** for Login dialog box. Follow the instructions on the PIN pad.



Consider that if the selected user manager uses the RSA smartcard authentication, the PIN pad must be connected either to the USB port labelled HSM on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) at the rear side of the CryptoServer LAN. For details about the USB ports, see [Connecting the PIN Pad \(p. 42\)](#).

Only if the selected user manager uses RSA signature authentication with a smartcard or ECDSA signature authentication with a smartcard, the PIN pad must be connected to the computer CAT is running on.

As an alternative you may use a USB port of any computer in the network. For details, see *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual \(p. 240\)](#).

- **Keyfile Token**

If the user is using an RSA or ECDSA user authentication key stored in a keyfile, click **Keyfile Token**, and proceed as follows:

- Click the search button (...) next to the **Key Path** text box.  
The **Set Name and Path for User Keyfile Token** dialog box opens.
  - Select the keyfile you require, e.g., ADMIN.key.
  - Click Open.
  - In case the keyfile is protected with a password, enter the password in the **Password** text box of the **Choose User Token for Login** dialog box.
  - If the user is using a password for authentication, click **Keyfile Token**, and enter the password in the **Password** text box.
- f. Click **OK** in the **Choose User Token for Login** dialog box. The dialog box closes. If the user login succeeded, a green check mark appears on the left hand side of the user item.
- g. Click **Close** to close the **Logon/Logoff User** dialog box.
- h. Click the **Manage User button** in the toolbar.
- i. In the **User Management** dialog box, click the **Add User** button.
- j. In the **Name of New User** field, enter a unique name for the NTP Manager.



Do not use the characters <, >, :, ", !, ?, \*, /, \, | in user names

- k. Under **User Profile**, select the NTP Manager one person rule option if you only want to set up one NTP user. If you want to set up secondary confirmation, select NTP Manager two-person rule.
- l. Under **Authentication Mechanism**, select the required authentication mechanism.



Select either **Smartcard (RSA Signature)**, **Keyfile (RSA Signature)**, **Smartcard (ECDSA Signature)**, **Keyfile (ECDSA Signature)** or **Smartcard (PIN Pad at CryptoServer)**.

If you select the RSA smartcard authentication (**Smartcard (PIN Pad at CryptoServer)** radio button), this means that once the new user is created this user needs a PIN pad directly connected to the USB port labeled HSM on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) at the rear side of the CryptoServer LAN.

Do not select the HMAC password authentication (**Password (HMAC)** radio button) because this authentication mechanism is not supported by some of the sh scripts used below.

- m. Enter an attribute if you wish to do so.
- n. Click **OK**.
  - If you have selected the **Password (HMAC)** authentication mechanism, the **Set Password of new User** dialog box opens.

If you want to enable the NTP firmware module by using a remote command line, do not select **Password (HMAC)** because the script used in this command line does not support HMAC password authentication. However, if you want to enable the NTP firmware module by using CAT, HMAC password authentication is supported.

    - Enter a unique, secure password in the **Password** text box.
    - Confirm your password entry in the **Confirm Password** text box.

- Close the **Set Password of new User** dialog box by clicking **OK**.  
The dialog box **Add User** closes automatically.
- If you have selected the authentication mechanism **Smartcard (RSA Signature)**, **Smartcard (ECDSA Signature)** or **Smartcard (PIN Pad on CryptoServer)**, the **Choose User Token to Add a New User** dialog box opens with the preselected option **Smartcard Token**.
  - Connect the PIN pad to the computer CAT is running on.
  - Click the **OK** button and follow the instructions on the display of the PIN pad.
  - Insert the smartcard, where the key is stored on, and press **OK** on the PIN pad. The dialog box **Add User** closes automatically
- If you have selected the authentication mechanism **Keyfile (RSA Signature)** or **Keyfile (ECDSA Signature)**, the **Choose User Token to Add a New User** dialog box opens with the preselected option **Keyfile Token**.
  - Click the **OK** button.
  - Click the search button (...) next to the **Key Path** field.
  - Select the keyfile path and click **Open**.
  - Click **OK** in the **Choose User Token to Add a New User** dialog box.
  - The new user is created and appears in the list of users in the **User Management** dialog box.

If you want to set up the two-person rule for NTP users, you must now use the procedure described above to set up another NTP user account (NTP Manager two-person rule).

3. As of CSLANOS v5.1, PCIe clock cards providing a high-precision time signal received by radio are supported. For details, see [Setting up PCIe Clock Cards \(p. 91\)](#).

If a PCIe clock card is mounted on the CryptoServer LAN, continue with step 6 because the NTP server's IP address cannot be set manually and the NTP daemon is started by default. If no PCIe clock card is mounted, continue with step 4.

To verify whether a PCIe clock card is mounted, open **CSLAN admin. > CSLAN Info > Show services info > NTP IPv4** on the display on the front panel. If it shows

`127.127.28.0`, a PCIe clock card is mounted. As an alternative, log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#), and verify whether the following line is present in the `/etc/ntp.conf` file:

```
server 127.127.28.0 minpoll 4 maxpoll 4 iburst
```

If this line is present, a PCIe clock card is mounted.

#### 4. Configuring the NTP server's IP address

Perform the following command. `set_ntpd_server_config.sh <IP address>`

Replace `<IP address>` by the IP address of the NTP server

As an alternative, perform the following substeps.

- a. Open the `ntp.conf` configuration file in the `/etc` directory in a text editor.
- b. Enter the IP address for the NTP server next to the entry `server`.
- c. As of CSLANOS V5.1, search restrict 127.0.0.1 and replace 127.0.0.1 by the IP address for the NTP server.
- d. Save and close the `ntp.conf` file.
- e. To restart the NTP daemon, perform the `/etc/init.d/ntpd restart` command.

#### 5. Starting the NTP daemon

- a. Perform the `set_ntpd_config.sh yes` command.
- b. Verify the result by performing the `get_ntpd_config.sh` command.

#### 6. Enabling the NTP firmware module on the CryptoServer

If you want to use CAT (CryptoServer Administration Tool) to enable the NTP firmware module, perform the following substeps. However, if you want to use a remote command line to do so, continue with step 7.

- a. Start CAT on your administrator computer.
- b. Click the **Login/Logoff** button in the toolbar.
- c. Select a user with at least the permission 00200000, for example, the NTP manager user account(s) created in the preceding step.
- d. Click the **Login** button. The dialog box **Choose User Token for Login** opens.
- e. Select the appropriate authentication mechanism.

- **Smartcard Token**

If the user is using an RSA or an ECDSA user authentication key stored on a smartcard, click **Smartcard Token**, and proceed as follows:

- If the NTP manager to be logged in uses RSA signature authentication with a smartcard or ECDSA authentication with a smartcard, connect the PIN pad to a USB port of the computer CAT is running on. However, if the NTP manager uses RSA smartcard authentication, connect the PIN pad to the USB port labelled **HSM** on the front panel

of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN.

- Click **OK** in the **Choose User Token for Login** dialog box.
- Follow the instructions on the PIN pad.

- **Keyfile Token**

- If the user is using an RSA or ECDSA user authentication key stored in a keyfile, click **Keyfile Token**, and proceed as follows:
- Click the search button (...) next to the **Key Path** text box. The **Set Name and Path for User Keyfile Token** dialog box opens.
- Select the keyfile you require, e.g., `NTP.key`.
- Click **Open**.
- In case the keyfile is protected with a password, enter the password in the **Password** text box of the **Choose User Token for Login** dialog box.
- If the user is using a password for authentication, click **Keyfile Token**, and enter the password in the **Password** text box.

- f. Click **OK** in the **Choose User Token for Login** dialog box. The dialog box closes. If the user login succeeded, a green check mark appears on the left hand side of the user item.
- g. Click **Close** to close the **Login/Logoff User** dialog box.
- h. Click on **Manage** in the menu bar and select the **NTP Settings...** menu item. The **Network Time Protocol (NTP) Configuration** dialog box opens.
- i. Select **Enabled**.
- j. Optionally, you can change the default values for Max. time to set per day and Max. time to set per operation. We recommend not to change these default values, see [Configuring Time Synchronization between the CryptoServer LAN and the CryptoServer \(p. 124\)](#).
- k. Click **Apply** to transfer the values you have entered to the CryptoServer.
- l. Finish entering your data in this dialog box by clicking on **OK**. The dialog box **Network Time Protocol (NTP) Configuration** closes.
- m. Continue with step 8.

7. If you want to use a remote command-line to enable the NTP firmware module, perform the following substeps.

- a. Connect the PIN pad to the appropriate USB port.
  - If the user name you use in the next step uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a smartcard or a keyfile), connect the PIN pad to the USB port labelled **Host1** or **Host2** on the front panel of the CryptoServer LAN or to one of the USB ports on the rear side of the CryptoServer LAN (a6). Chapter *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual \(p. 240\)](#) does not apply here.
  - If the user name you use in the next step uses RSA smartcard authentication, connect the PIN pad to the USB port labelled **HSM** on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN (a10). For further information, see [Connecting the PIN Pad \(p. 42\)](#).

- b. Perform the following command to enable the NTP firmware module.

```
activate_ntp_module.sh <user name> yes
```

**<user name>** is the user with at least permission 00200000 that you have created in step 2.

Only users with RSA signature authentication, ECDSA signature authentication and RSA smartcard authentication are supported. Users with HMAC password authentication are not supported.

Output: `Activate time synchronisation Enter Smart card PIN for ntp!`

- c. Follow the instructions shown on the display of the PIN pad.  
Output in the command-line: `ANSW:`
- d. Open **Manage > NTP Settings... > NTP Status in CAT** to verify the result.
- e. Continue with step 8.

8. Starting time synchronization from the CryptoServer LAN to the CryptoServer  
When the time between the NTP server and the CryptoServer LAN (host time; system time) has been synchronized, it is important to synchronize the time between the CryptoServer LAN and the CryptoServer (PCIe card) mounted into the CryptoServer LAN. Otherwise, a time difference (deviation) between the time on the CryptoServer LAN and the time on the CryptoServer (PCIe card) might become greater than the maximum time deviation permitted for the time on the CryptoServer per day. This would cause an error,

and the clock of the CryptoServer will not be set.

Perform the following substeps.

- a. Perform the following command to verify whether the NTP client is enabled.

```
get_ntpclient_config.sh
```

The result is either `yes` or `no`.

- b. Connect the PIN pad to the appropriate USB port.

- If the user name you use in the next step uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a smartcard or a keyfile), connect the PIN pad to the USB port labelled **Host1** or **Host2** on the front panel of the CryptoServer LAN or to one of the USB ports on the rear side of the CryptoServer LAN (a6). Chapter *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual \(p. 240\)](#) does not apply here.
- If the user name you use in the next step uses RSA smartcard authentication, connect the PIN pad to the USB port labelled HSM on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN (a10). For further information, see [Connecting the PIN Pad \(p. 42\)](#).

- c. Perform the following command to start the NTP client as and cause a periodic transfer of the CryptoServer LAN time to the CryptoServer (PCIe card).

```
enable_hsm_time_sync.sh <user name> yes
```



This command cannot be performed remotely because the PIN pad must be connected to a USB port of the CryptoServer LAN or the CryptoServer (PCIe card).

`<user name>` is not the user with at least permission 00200000 that you have created in step 2. However, `<user name>` is a system manager with at least the permission 02000000, for example, the ADMIN user with 22000000. Only users with RSA signature authentication, ECDSA signature authentication and RSA smartcard authentication are supported. Users with HMAC password authentication are not supported. For details about the authentication mechanism, see *Authentication Mechanisms* in the [CryptoServer – Administration Manual \(p. 240\)](#).

Example output:

```
Start time synchronisation
```

```
ntpd is running with PID = 4636
NTPCLIENT not running
Set system time to HSM
Enter Smart card PIN for ADMIN!
```

- d. Follow the instructions on the display of the PIN pad to enter the PIN.

Example output:

```
Time successfully set to:
date: 09.01.2019 time: 16:55:59.015 (local time)
date: 09.01.2019 time: 15:55:59.015 (UTC/internal)
Starting ntpclient...
```

- e. Perform the following command again to verify the result.

```
get_ntpclient_config.sh
```



The NTP has been successfully set up.

#### 4.12.4 Disabling NTP

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).

2. Creating an NTP manager user account

To perform this step, you can use the csadm command-line tool. This is not described in this manual. For details, see [CryptoServer – csadm Manual \(p. 240\)](#).

Use the CryptoServer Administration Tool (CAT) to set up one or two user accounts for NTP administration (NTP Manager). CAT provides the appropriate role-based user profiles **NTP Manager one-person rule** and **NTP Manager two-person rule**. For details, see [CryptoServer – CAT Manual \(p. 240\)](#).

- a. Start CAT on your administration computer.
- b. Click the **Login/Logoff** button in the toolbar.
- c. Select a user with at least the permission 20000000.
- d. Click the **Login** button. The dialog box **Choose User Token for Login** opens.
- e. Select the appropriate authentication mechanism.



- **Smartcard Token**

If the user is using an RSA or an ECDSA user authentication key stored on a smartcard, click Smartcard Token and then click **OK** in the **Choose User Token for Login** dialog box. Follow the instructions on the PIN pad.



Consider that if the selected user manager uses the RSA smartcard authentication, the PIN pad must be connected either to the USB port labelled HSM on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) at the rear side of the CryptoServer LAN. For details about the USB ports, see [Connecting the PIN Pad \(p. 42\)](#).

Only if the selected user manager uses RSA signature authentication with a smartcard or ECDSA signature authentication with a smartcard, the PIN pad must be connected to the computer CAT is running on. As an alternative you may use a USB port of any computer in the network. For details, see *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual \(p. 240\)](#).

For details about the authentication mechanism, see *Authentication Mechanisms* in the [CryptoServer – Administration Manual \(p. 240\)](#).

- **Keyfile Token**

If the user is using an RSA or ECDSA user authentication key stored in a keyfile, click **Keyfile Token**, and proceed as follows:

- Click the search button (...) next to the **Key Path** text box. The **Set Name and Path for User Keyfile Token** dialog box opens.
  - Select the keyfile you require, e.g., `ADMIN.key`.
  - Click **Open**.
  - In case the keyfile is protected with a password, enter the password in the **Password** text box of the **Choose User Token for Login** dialog box.
  - If the user is using a password for authentication, click **Keyfile Token**, and enter the password in the Password text box.
- f. Click **OK** in the **Choose User Token for Login** dialog box. The dialog box closes. If the user login succeeded, a green check mark appears on the left hand side of the user item.
- g. Click **Close** to close the **Logon/Logoff User** dialog box.
- h. Click the **Manage User** button in the toolbar.
- i. In the **User Management** dialog box, click the **Add User** button.

- j. In the **Name of New User** field, enter a unique name for the NTP Manager.



Do not use the characters <, >, :, ", !, ?, \*, /, \, | in user names.

- k. Under **User Profile**, select the NTP Manager one person rule option if you only want to set up one NTP user. If you want to set up secondary confirmation, select **NTP Manager two-person rule**.
- l. Under **Authentication Mechanism**, select the required authentication mechanism.



Select either **Smartcard (RSA Signature)**, **Keyfile (RSA Signature)**, **Smartcard (ECDSA Signature)**, **Keyfile (ECDSA Signature)** or **Smartcard (PIN Pad at CryptoServer)**.

If you select the RSA smartcard authentication (Smartcard (PIN Pad at CryptoServer) radio button), this means that once the new user is created this user needs a PIN pad directly connected to the USB port labelled HSM on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) at the rear side of the CryptoServer LAN.

Do not select the HMAC password authentication (Password (HMAC) radio button) because this authentication mechanism is not supported by some of the sh scripts used below.

For details about the authentication mechanism, see *Authentication Mechanisms* in the [CryptoServer – Administration Manual \(p. 240\)](#).

- m. Enter an attribute if you wish to do so.
- n. Click **OK**.
- If you have selected the **Password (HMAC)** authentication mechanism, the **Set Password of new User** dialog box opens.  
If you want to enable the NTP firmware module by using a remote command-line (see step 7), do not select **Password (HMAC)** because the script used in this command-line does not support HMAC password authentication. However, if you want to enable the NTP firmware module by using CAT (see step 6 on page 103), HMAC password authentication is supported.
  - Enter a unique, secure password in the **Password** text box.

- Confirm your password entry in the **Confirm Password** text box.
  - Close the **Set Password of new User** dialog box by clicking **OK**.  
The dialog box **Add User** closes automatically.
  - If you have selected the authentication mechanism **Smartcard (RSA Signature)**, **Smartcard (ECDSA Signature)** or **Smartcard (PIN Pad on CryptoServer)**, the **Choose User Token to Add a New User** dialog box opens with preselected option **Smartcard Token**.
    - Connect the PIN pad to the computer CAT is running on.
    - Click the **OK** button and follow the instructions on the display of the PIN pad.
    - Insert the smartcard, where the key is stored on, and press **OK** on the PIN pad. The dialog box **Add User** closes automatically
  - If you have selected the authentication mechanism **Keyfile (RSA Signature)** or **Keyfile (ECDSA Signature)**, the **Choose User Token to Add a New User** dialog box opens with preselected option **Keyfile Token**.
    - Click the **OK** button.
    - Click the search button (...) next to the **Key Path** field.
    - Select the keyfile path and click **Open**.
    - Click **OK** in the **Choose User Token to Add a New User** dialog box. The dialog box **Add User** closes automatically.  
The new user is created and appears in the list of users in the User Management dialog box.  
If you want to set up the two-person rule for NTP users, you must now use the procedure described above to set up another NTP user account (**NTP Manager two-person rule**).
3. Disabling the NTP firmware module on the CryptoServer
- If you want to use CAT (CryptoServer Administration Tool) to disable the NTP firmware module, perform the following substeps. However, if you want to use a remote command-line to do so, continue with step 4 instead.
- a. Start CAT on your administrator computer.
  - b. Click the **Login/Logoff** button in the toolbar.
  - c. Select a user with at least the permission 00200000, for example, the NTP manager user account(s) created in the preceding step.

- d. Click the **Login** button. The dialog box **Choose User Token for Login** opens.
- e. Select the appropriate authentication mechanism.
  - **Smartcard Token**

If the user is using an RSA or an ECDSA user authentication key stored on a smartcard, click **Smartcard Token**, and proceed as follows:

    - If the NTP manager to be logged in uses RSA signature authentication with a smartcard or ECDSA authentication with a smartcard, connect the PIN pad to a USB port of the computer CAT is running on. However, if the NTP manager uses RSA smartcard authentication, connect the PIN pad to the USB port labelled **HSM** on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN.
    - Click **OK** in the **Choose User Token for Login** dialog box.
    - Follow the instructions on the PIN pad.
  - **Keyfile Token**

If the user is using an RSA or ECDSA user authentication key stored in a keyfile, click **Keyfile Token**, and proceed as follows:

    - Click the search button (...) next to the Key Path text box. The **Set Name and Path for User Keyfile Token** dialog box opens.
    - Select the keyfile you require, e.g., `NTP.key`.
    - Click **Open**.
    - In case the keyfile is protected with a password, enter the password in the **Password** text box of the **Choose User Token for Login** dialog box.
    - If the user is using a password for authentication, click **Keyfile Token**, and enter the password in the **Password** text box.
- f. Click **OK** in the **Choose User Token for Login** dialog box. The dialog box closes. If the user login succeeded, a green check mark appears on the left hand side of the user item.
- g. Click **Close** to close the **Login/Logoff User** dialog box.
- h. Click on **Manage** in the menu bar and select the **NTP Settings...** menu item. The **Network Time Protocol (NTP) Configuration** dialog box opens.

- i. Select **Disabled**.
  - j. Click **Apply** to transfer the values you have entered to the CryptoServer.
  - k. Finish entering your data in this dialog box by clicking on **OK**. The dialog box **Network Time Protocol (NTP) Configuration** closes.
  - l. Continue with step 5.
4. If you want to use a remote command-line to disable the NTP firmware module, perform the following substeps.
  - a. Connect the PIN pad to the appropriate USB port.
    - If the user name you use in the next step uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a smartcard or a keyfile), connect the PIN pad to the USB port labeled **Host1** or **Host2** on the front  
Administering the CryptoServer LAN panel of the CryptoServer LAN or to one of the USB ports on the rear side of the CryptoServer LAN (a6). Chapter *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual](#) (p. 240) does not apply here.
    - If the user name you use in the next step uses RSA smartcard authentication, connect the PIN pad to the USB port labeled **HSM** on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN (a10). For further information, see [Connecting the PIN Pad](#) (p. 42).
  - b. Perform the following command to disable the NTP firmware module.

```
activate_ntp_module.sh <user name> no
```

**<user name>** is the user with at least permission 00200000 that you have created in step 2.

Only users with RSA signature authentication, ECDSA signature authentication and RSA smartcard authentication are supported. Users with HMAC password authentication are not supported.

Output:

```
Deactivate time synchronisation
Enter Smart card PIN for ntp!
```
  - c. Follow the instructions shown on the display of the PIN pad.

Output in the command line:

```
ANSW:
```
  - d. Open **Manage > NTP Settings... > NTP Status** in CAT to verify the result.

- e. Continue with step 5.
5. If you want to disable the time synchronization using the front panel, continue with step 6.
6. If you want to disable the time synchronization using scripts, continue with step 7.
6. Disabling time synchronization using the front panel.
  - a. Press the **ENTER** button on the front panel of the CryptoServer LAN.
  - b. Press the ↓ button to select the HSM admin. menu item and confirm by pressing **ENTER**.
  - c. If CSLANOS < 5.1.0: Press the ↓ button to select the **Key&file admin.** menu item and confirm by pressing **ENTER**.
  - d. Press the ↓ button to select the **HSM** time sync menu item and confirm by pressing **ENTER**.
  - e. The currently applied setting (disabled or enabled) is indicated by a full circle.
  - f. Use the ↓ button to select disabled and press the **ENTER** button to open the menu item.
  - g. Use the ← key to move the x into the brackets **[x] Yes** and then press **ENTER**.  
This action stops the NTP client.  
If you select the HSM time sync menu item and confirm by pressing **ENTER** at a later date, the NTP firmware module might be enabled. In this case, the PIN of the NTP manager defined by the `NTPManagerName` parameter in the `/etc/csxlan.conf` file and a PIN pad connected to the appropriate USB port is needed.
  - h. You see a system message that you have performed the configuration successfully. Confirm by pressing **ESC**.
  - i. Disabling the time synchronization is finished. No further steps are necessary.
7. Disabling time synchronization using scripts  
Perform the following substeps.
  - a. Perform the following command to verify whether the NTP client is enabled.  
`get_ntpclient_config.sh`  
The result is either yes or no. If the result is no, no further steps are required. The time synchronization is disabled. If the result is yes, continue with the steps below.
  - b. Connect the PIN pad to the appropriate USB port.
    - If the user name you use in the next step uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a

smartcard or a keyfile), connect the PIN pad to the USB port labeled **Host1** or **Host2** on the front panel of the CryptoServer LAN or to one of the USB ports on the rear side of the CryptoServer LAN (a6).

- Chapter *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual](#) (p. 240) does not apply here.
  - If the user name you use in the next step uses RSA smartcard authentication, connect the PIN pad to the USB port labeled **HSM** on the front panel of the CryptoServer LAN or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN (a10). For further information, see [Connecting the PIN Pad](#) (p. 42).

- c. Perform the following command to disable the NTP client and to stop a periodic transfer of the CryptoServer LAN time to the CryptoServer (PCIe card).
- ```
enable_hsm_time_sync.sh <user name> no
```



This command cannot be authenticated remotely because the PIN pad must be connected to a USB port of the CryptoServer LAN or the CryptoServer (PCIe card).

`<user name>` is not the user with at least permission 00200000 that you have created in step 2. However, `<user name>` is a system manager with at least the permission 02000000, for example, the ADMIN user with 22000000. Only users with RSA signature authentication, ECDSA signature authentication and RSA smartcard authentication are supported. Users with HMAC password authentication are not supported. For details about the authentication mechanism, see *Authentication Mechanisms* in the [CryptoServer – Administration Manual](#) (p. 240).

Example Output

```
Stop time synchronisation
ntpd is running with PID = 4636
NTPCLIENT not running
Stop time synchronisation
Stopping ntpclient... [ OK ]
/scripts_dsdp/enable_hsm_time_sync.sh: line 115: [: -ne: unary
operator expected
```

- d. Perform the following command again to verify the result.

```
get_ntpclient_config.sh
```



NTP has successfully been disabled.

4.13 Configuring the NTP Firmware Module

This chapter describes options you can use to configure the NTP firmware module for the CryptoServer LAN.

4.13.1 Configuring Time Synchronization between the CryptoServer LAN and the CryptoServer

When the time between the NTP server and the CryptoServer LAN (host time; system time) has been synchronized, it is important to synchronize the time between the CryptoServer LAN and the CryptoServer (PCIe card) mounted into the CryptoServer LAN. If the NTP client is enabled, it verifies every `LoopTime` seconds whether the time difference between the time on the CryptoServer LAN and the time on the CryptoServer is greater than Deviation milliseconds. If this is the case, it transfers the time on the CryptoServer LAN to the CryptoServer.

The following parameters are used for time synchronization:

- `LoopTime`

Verification time interval in seconds

Default value: `LoopTime = 3600` (i.e., once per hour)

We recommend not to change the default value. Do not set a value higher than 86400 (i.e., one day).

`LoopTime` is a parameter of the NTP client on the CryptoServer LAN. It is configured in the `/etc/csxlan.conf` file on the CryptoServer LAN. See the steps below to perform this configuration.

- `Deviation`

Time deviation in milliseconds between the CryptoServer LAN and the CryptoServer for which the time on the CryptoServer is to be corrected

Default value: `Deviation = 500`

Recommended value range: 1 – 2500.

A value below 1 is automatically set to 1, and a value higher than 2500 is automatically set to 2500. A value higher than **Max. time to set per operation** (see below) does not initiate a time correction but produces an error.

Deviation is a parameter of the NTP client on the CryptoServer LAN. It is configured in the `/etc/csxlan.conf` file on the CryptoServer LAN. See the steps below to perform this configuration.

- **Max. time to set per operation**

Max. time to set per operation specifies the maximum value in milliseconds permitted for the Deviation parameter. If the time difference between the time on the CryptoServer LAN and the time on the CryptoServer is greater than **Max. time to set per operation**, the time on the CryptoServer is not corrected but an error message is created instead.

The default value is 3000 (i.e., 3 seconds). We recommend not to change this default value.

Max. time to set per operation is a parameter of the NTP firmware module on the CryptoServer (PCIe card). It can only be configured by using the CryptoServer Administration Tool (CAT). Click the **Manage > NTP Settings** menu to open the corresponding dialog.

- **Max. time to set per day**

If the per day accumulated time by which the CryptoServer time has been corrected, is greater than **Max. time to set per day**, the CryptoServer time is not corrected but an error message is created instead.

The default value is 30000 (in milliseconds, i.e., 30 seconds). We recommend not to change this default value.

Max. time to set per day is a parameter of the NTP firmware module on the CryptoServer (PCIe card). It can only be configured by using the CryptoServer Administration Tool (CAT). Click the **Manage > NTP Settings** menu to open the corresponding dialog.

If you want to change the LoopTime value or the Deviation value, perform the following steps.

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN](#) (p. 48).
2. Got to the `/etc` directory. Here you will find the `csxlan.conf` configuration file (`/etc/csxlan.conf`).
3. Open the `csxlan.conf` file with a text editor.
In our example, the time synchronization (`LoopTime`) should be performed every 3600 seconds (one hour), and for any time variation (`Deviation`) of more than 2500

milliseconds (2,5 seconds).

To do so, you should adjust the following entries in the `[NTPClient]` section of the `csxlan.conf` configuration file:

```
[NTPClient]
```

```
Deviation = 2500
```

```
LoopTime = 3600
```

4. Save and close the `csxlan.conf` configuration file.
5. Make the changes in the `csxlan.conf` configuration file effective by performing the following substeps.
 - If you use the front panel of the CryptoServer LAN, perform the following substeps.
 - i. On the front panel of the CryptoServer LAN, press the **ENTER** button.
 - ii. Use the **ENTER** button to select **CSLAN admin..**
 - iii. Use the **↓** button to select Reboot and confirm by pressing **ENTER**.
 - iv. Use the **←** or the **→** button to move the x into the square brackets **[x] Yes** and confirm by pressing **ENTER**.
 - If you use the remote access to the CryptoServer LAN instead, perform the following substep.
 - i. Perform the following commands in exactly this order.

```
set_ntpclient_config.sh no
```

```
set_ntpclient_config.sh yes
```
 - ii. Shut down your SSH client.



Time Synchronization has successfully been configured.

4.13.2 Viewing NTP Log Entries

All log entries or error messages relating to the NTP daemon and the NTP client to stand are stored in the `syslog` file, and you can view them there. We describe how you use SSH for Windows to modify the `syslog` file.

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
2. Go to the `/var/log` directory and open the syslog file in a text editor.
3. Look for these entries: `ntpclient` and `ntpd`.
4. Close the `syslog` file and shut down your SSH client.



The NTP log entries are being displayed.

4.13.3 Changing the Time Zone for the CryptoServer LAN

Perform the following steps to change the time zone:

1. Log in remotely to the CryptoServer LAN, see section [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
2. Getting the time on the CryptoServer LAN (optional).
Perform the `date` command in the command line.
3. Enter the `tzconfig` command in the command line and confirm this by pressing the **Enter** key on the keyboard.
4. Follow the instructions in the command line.
5. To verify the result, perform the `date` command in the command line.



The time zone has been changed successfully. The changed time zone comes into effect immediately.

4.14 Setting up Bonding

Bonding is a method to provide a high availability network access to the LAN device.

You can use Linux bonding for bundling the two real network interface cards (NIC) `eth0` and `eth1` available in the CSLAN to one bonding NIC (`bond0`). The LAN device then appears to have only this bonding NIC and a single IP address in the network. The bonding NIC is the master

device, the real NICs are the slave devices. The real NICs are also called eth devices. If one of the real NICs fails, the remaining one takes care of the entire data traffic, i.e., an automatic failover mechanism is provided. No load balancing solution is configured.

Bonding is also called "NIC teaming", "NIC bonding", "Channel bonding", "Ethernet bonding", "Trunking", "Link bundling" or "Link aggregation" (LAG).

The bonding NIC and the real NICs all have the same MAC address. If not otherwise configured, the bonding NIC copies the MAC address of the first slave device. This MAC address is then assigned to all other slaves also and remains persistent even if the first slave device is removed. It does not change until the bonding NIC is disabled or reconfigured.

The bonding configuration is done persistently in the `/etc/sysconfig/bonding` file. Consider that the values are enclosed by ".

Parameter	Description
NETCONFIG	<p>The network interface this networking file applies to.</p> <ul style="list-style-type: none"> "_0" This networking file applies only to the bond0 interface. "_1" This networking file applies only to the bond1 interface. "_0_1" This networking file applies to the bond0 interface and to the bond1 interface.
NET_DEV_<x>="bond<x>"	Configuration for the bond<x> interface
DHCP_<x>	<p>DHCP for IPv4 addresses for bond<x>.</p> <ul style="list-style-type: none"> "yes" DHCP for IPv4 addresses is enabled for bond<x>. This assignment overrides any assignment for <code>IP_ADDR_<x></code>. "no" DHCP for IPv4 addresses is disabled for bond<x>. This is the default value. It is used if <code>DHCP_<x></code> is not configured.
DHCP_v6_<x>	<p>DHCP for IPv6 addresses for bond<x>.</p> <ul style="list-style-type: none"> "yes" DHCP for IPv6 addresses is enabled for bond<x>. This assignment overrides any assignment for <code>IP_ADDR_v6_<x></code>. "no" DHCP for IPv6 addresses is disabled for bond<x>. This is the default value. It is used if <code>DHCP_v6_<x></code> is not configured.
IP_ADDR_<x>	IPv4 address and prefix for bond<x>, for example, "192.168.1.111/24"

<i>Parameter</i>	<i>Description</i>
IP_ADDR_v6_<x>	IPv6 address and prefix for bond<x>, for example, " 2002::2/64 "
BOND_NICS_<x>	List of eth interfaces that are bonded
GATEWAY	IPv4 default gateway, for example, " 192.168.1.1 "
GATEWAY_v6	IPv6 default gateway, for example, " 2001::1/64 "
#	# starts a comment line

Table 9: Parameters in the /etc/sysconfig/bonding file



Bonding features cannot be enabled, disabled or configured using the front panel.

Perform the following steps to set up bonding.

1. Log in remotely to the LAN device.
2. Copy the `/etc/sysconfig/bonding_example` file to the `/etc/sysconfig/bonding` file.
The bonding file contains configuration data of the bonding network card (bond0). The structure of this file is similar to the structure of the `/etc/sysconfig/networking` file.
3. Open the `/etc/sysconfig/bonding` file in a text editor.
4. The contents of this file is for example:

```
# Begin /etc/sysconfig/bonding

NETCONFIG="_0"

NET_DEV_0="bond0"
DHCP_0="yes"
IP_ADDR_0="192.168.100.228/24"
BOND_NICS_0="eth0 eth1"

# NET_DEV_1="bond1"
# DHCP_1="no"
# IP_ADDR_1="10.10.10.2/24"
# BOND_NICS_1="eth2 eth3"

GATEWAY="192.168.100.254"
```

```
# GATEWAY_v6="2002::254"

# End /etc/sysconfig/bonding
```

5. If you use dynamic IP addresses for IPv4, leave the following line unchanged.
`DHCP_0=yes`
The static IP address (`IP_ADDR_0`) in the file is then ignored.
6. If you use dynamic IP addresses for IPv6, use one of the following assignments.
`DHCP_v6_0=yes`
The static IP address (`IP_ADDR_v6_0`) in the file is then ignored.
7. If you use static IP addresses instead, set `DHCP_0="no"` or `DHCP_v6_0="no"` and set the `IP_ADDR_0` parameter value according to your needs.
8. Save the file after you have finished editing it.
9. Perform the `/etc/init.d/network start` command to start bonding.
10. If you want to stop bonding at a later date, delete or rename the `/etc/sysconfig/bonding` file and perform the `/etc/init.d/network restart` command. Then, the `/etc/sysconfig/networking` file is applied for the eth0 and eth1 NICs.



Binding has been successfully set up.

4.15 Using IPMI

4.15.1 Accessing the CryptoServer LAN

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).

Make sure to log in as `root`, not as `csagent`. Otherwise, you will get an error message when performing an `ipmitool` command.

Example of an error:

```
csagent@CryptoServer:~$ ipmitool sdr
```

```
Could not open device at /dev/ipmi0 or /dev/ipmi/0 or /dev/ipmidev/0:
No such file or directory
```

2. Enter `ipmitool` to show the help of the ipmitool.

Commands:

```
raw          Send a RAW IPMI request and print response
i2c          Send an I2C Master Write-Read command and print response
spd          Print SPD info from remote I2C device
lan          Configure LAN Channels chassis Get chassis status and set power
state
power        Shortcut to chassis power commands event Send pre-defined events
to MC
mc           Management Controller status and global enables
sdr          Print Sensor Data Repository entries and readings
sensor       Print detailed sensor information
fru          Print built-in FRU and scan SDR for FRU locators
gendev       Read/Write Device associated with Generic Device locators sdr
sel          Print System Event Log (SEL) pef Configure Platform Event
Filtering (PEF)
sol          Configure and connect IPMIv2.0 Serial-over-LAN
tsol         Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
isol         Configure IPMIv1.5 Serial-over-LAN
user         Configure Management Controller users
channel      Configure Management Controller channels
session      Print session information
dcmi         Data Center Management Interface
nm           Node Manager Interface
sunoem       OEM Commands for Sun servers
kontron OEM Commands for Kontron devices
picmg        Run a PICMG/ATCA extended cmd
fwum         Update IPMC using Kontron OEM Firmware Update Manager
firewall     Configure Firmware Firewall
delloem      OEM Commands for Dell systems
exec         Run list of commands from file
set          Set runtime variable for shell and exec
hpm          Update HPM components using PICMG HPM.1 file
ekalyzer     run FRU-Ekeying analyzer using FRU files
ime          Update Intel Manageability Engine Firmware
vita         Run a VITA 46.11 extended cmd
lan6         Configure IPv6 LAN Channels
```

4.15.2 Showing Sensor Values

The `ipmitool sdr` command shows an overview of the sensors.

Example Output

CPU Temp		34 degrees C		ok
PCH Temp		38 degrees C		ok
System Temp		26 degrees C		ok
Peripheral Temp		35 degrees C		ok
VcpuVRM Temp		36 degrees C		ok
DIMMA1 Temp		no reading		ns
DIMMA2 Temp		no reading		ns
DIMMB1 Temp		no reading		ns
DIMMB2 Temp		no reading		ns
FAN1 5200		ns FAN2 6000		ns
FAN3 5300		ns FAN4 6200		ns
FAN5 5300		ns FAN6 6200		ns
12V		12.13 Volts		ok
5VCC		5 Volts		ok
3.3VCC		3.35 Volts		ok
VBAT		3.07 Volts		ok
Vcpu		0.13 Volts		ok
VDIMMAB		1.18 Volts		ok
0.95V VCCIO		0.97 Volts		ok
1.5VSB		1.54 Volts		ok
5VSB		5.03 Volts		ok
3.3VSB		3.21 Volts		ok
1.05V VCCSA		1.06 Volts		ok
1.2V BMC		1.21 Volts		ok
1.0V PCH		1.01 Volts		ok
Chassis Intru		0x01		ok
PW Consumption		5 Watts		ok

The `ipmitool sdr elist full` command shows additional information. The second column shows the sensor ID, and the fourth column the entity ID.

Example Output

CPU Temp		01h		ok		3.1		34 degrees C
PCH Temp		0Ah		ok		7.3		37 degrees C
System Temp		0Bh		ok		7.1		27 degrees C
Peripheral Temp		0Ch		ok		7.2		35 degrees C
VcpuVRM Temp		10h		ok		8.1		35 degrees C
DIMMA1 Temp		B0h		ns		32.64		No Reading
DIMMA2 Temp		B1h		ns		32.68		No Reading
DIMMB1 Temp		B4h		ns		32.72		No Reading
DIMMB2 Temp		B5h		ns		32.76		No Reading
FAN1		41h		ns		29.1		5200

FAN2	42h ns 29.2 6000
FAN3	43h ns 29.3 5300
FAN4	44h ns 29.4 6200
FAN5	45h ns 29.5 5300
FAN6	46h ns 29.6 6200
12V	30h ok 7.17 12.13 Volts
5VCC	31h ok 7.33 5 Volts
3.3VCC	32h ok 7.32 3.35 Volts
VBAT	33h ok 7.18 3.07 Volts
Vcpu	34h ok 3.3 0.13 Volts
VDIMMAB	35h ok 32.1 1.18 Volts
0.95V VCCIO	36h ok 7.12 0.97 Volts
1.5VSB	37h ok 7.20 1.54 Volts
5VSB	38h ok 7.15 5.03 Volts
3.3VSB	39h ok 7.19 3.21 Volts
1.05V VCCSA	3Ch ok 7.20 1.06 Volts
1.2V BMC	3Dh ok 7.21 1.21 Volts
1.0V PCH	3Eh ok 7.12 1.01 Volts
Chassis Intru	AAh ok 23.1 General Chassis intrusion
PW Consumption	1Ah ok 21.0 5 WattsTh

The `ipmitool sdr-v` command gives a more detailed output of all sensors. The following excerpt shows only the values of the first two sensors (CPU temperature and PCH temperature).

Example Output

```
Running Get PICMG Properties my_addr 0x20, transit 0, target 0
Error response 0xc1 from Get PICMG Properties
Running Get VSO Capabilities my_addr 0x20, transit 0, target 0
Invalid completion code received: Invalid command
Discovered IPMB address 0x0
Sensor ID           : CPU Temp (0x1)
Entity ID           : 3.1 (Processor)
Sensor Type (Threshold) : Temperature (0x01)
Sensor Reading      : 34 (+/- 0) degrees C
Status              : ok
Nominal Reading     : 40.000
Normal Minimum      : -4.000
Normal Maximum      : 89.000
Upper non-recoverable : 100.000
Upper critical       : 100.000
Upper non-critical   : 95.000
Lower non-recoverable : 0.000
Lower critical       : 0.000
Lower non-critical   : 5.000
Positive Hysteresis  : 2.000
Negative Hysteresis  : 2.000
Minimum sensor range : Unspecified
```

```

Maximum sensor range : Unspecified
Event Message Control : Per-threshold
Readable Thresholds : lnr lcr lnc unc ucr unr
Settable Thresholds : lnr lcr lnc unc ucr unr
Threshold Read Mask : lnr lcr lnc unc ucr unr
Assertion Events :
Assertions Enabled : lcr- ucr+
Deassertions Enabled : lcr- ucr+

Sensor ID : PCH Temp (0xa)
Entity ID : 7.3 (System Board)
Sensor Type (Threshold) : Temperature (0x01)
Sensor Reading : 38 (+/- 0) degrees C
Status : ok
Nominal Reading : 25.000
Normal Minimum : -4.000
Normal Maximum : 67.000
Upper non-recoverable : 100.000
Upper critical : 95.000
Upper non-critical : 90.000
Lower non-recoverable : 0.000
Lower critical : 5.000
Lower non-critical : 10.000
Positive Hysteresis : 2.000
Negative Hysteresis : 2.000
Minimum sensor range : Unspecified
Maximum sensor range : Unspecified
Event Message Control : Per-threshold
Readable Thresholds : lnr lcr lnc unc ucr unr
Settable Thresholds : lnr lcr lnc unc ucr unr
Threshold Read Mask : lnr lcr lnc unc ucr unr
Assertion Events :
Assertions Enabled : lcr- lnr- ucr+ unr+
Deassertions Enabled : lcr- lnr- ucr+ unr+

```

The `ipmitool` sensor `get <sensor name>` command shows information about one sensor, for example, the `ipmitool sensor get "CPU Temp"` command shows information about the CPU temperature. Notice to use `"` if the sensor name contains at least one blank.

Example Output

```

Locating sensor record...
Sensor ID : CPU Temp (0x1)
Entity ID : 3.1
Sensor Type (Threshold) : Temperature
Sensor Reading : 34 (+/- 0) degrees C
Status : ok
Lower Non-Recoverable : 0.000

```

```

Lower Critical      : 0.000
Lower Non-Critical  : 5.000
Upper Non-Critical  : 95.000
Upper Critical      : 100.000
Upper Non-Recoverable : 100.000
Positive Hysteresis  : 2.000
Negative Hysteresis  : 2.000
Assertion Events     :
Assertions Enabled   : lcr- ucr+
Deassertions Enabled : lcr- ucr+

```

The `ipmitool sensor` command shows a table of all sensors. The following example shows an excerpt of the entire table.

Example Output

```

CPU Temp|34.000|degrees C|ok|0.000|0.000|5.000|95.000|100.000|100.000
PCH Temp|37.000|degrees C|ok|0.000|5.000|10.000|90.000|95.000|100.000
System Temp|26.000|degrees C|ok|-10.000|-5.000|0.000|80.000|85.000|90.000
...
VBAT  | 3.074  | Volts      | ok | 2.407 | 2.494      | 2.610  | 3.509 | 3.596 |
3.712
...
Chassis Intru | 0x1      | discrete | 0x0100| na | na          | na      | na | na |
na
PW Consumption| 5.000    | Watts     | ok | na      | na          | na      | na | na |
na

```

4.15.3 Showing Chassis Information

The `ipmitool chassis status` command shows the chassis status.

Example Output

```

System Power      : on
Power Overload    : false
Power Interlock    : inactive
Main Power Fault   : false
Power Control Fault : false
Power Restore Policy : always-on
Last Power Event   :
Chassis Intrusion  : active
Front-Panel Lockout : inactive
Drive Fault        : false
Cooling/Fan Fault  : false

```

In addition to that, the `ipmitool chassis power status` command can be performed.

```
Chassis Power is on
```

The `ipmitool chassis policy list` command shows whether after a reboot the CryptoServer LAN returns to the previous state, power is always on or power is always off.

Example output:

```
Supported chassis power policy: previous
```

4.15.4 Showing System Event Log Information

The `ipmitool sel` command shows the system event log.

Example Output

```
SEL Information
Version          : 1.5 (v1.5, v2 compliant)
Entries          : 483
Free Space       : 580 bytes
Percent Used     : 93%
Last Add Time    : 08/02/2018 07:46:45
Last Del Time    : Not Available
Overflow         : false
Supported Cmds   : 'Reserve' 'Get Alloc Info'
# of Alloc Units : 512
Alloc Unit Size  : 20
# Free Units     : 29
Largest Free Blk : 29
Max Record Size  : 20
```

The `ipmitool sel -v` command shows additional information.

Example Output

```
Running Get PICMG Properties my_addr 0x20, transit 0, target 0
Error response 0xc1 from Get PICMG Properties
Running Get VSO Capabilities my_addr 0x20, transit 0, target 0
Invalid completion code received: Invalid command
Discovered IPMB address 0x0
SEL Information
Version          : 1.5 (v1.5, v2 compliant)
```

```

Entries          : 483
Free Space       : 580 bytes
Percent Used     : 93%
Last Add Time    : 08/02/2018 07:46:45
Last Del Time    : Not Available
Overflow         : false
Supported Cmds   : 'Reserve' 'Get Alloc Info'
# of Alloc Units : 512
Alloc Unit Size  : 20
# Free Units     : 29
Largest Free Blk : 29
Max Record Size  : 20

```

4.15.5 Showing LAN Information

The `ipmitool lan print` command shows information about the LAN.

Example Output

```

Set in Progress      : Set Complete
Auth Type Support    : NONE MD2 MD5 PASSWORD
Auth Type Enable     : Callback : MD2 MD5 PASSWORD
                    : User      : MD2 MD5 PASSWORD
                    : Operator : MD2 MD5 PASSWORD
                    : Admin   : MD2 MD5 PASSWORD
                    : OEM     : MD2 MD5 PASSWORD

IP Address Source    : Static Address
IP Address           : 10.10.10.10
Subnet Mask          : 255.255.255.0
MAC Address          : ac:1f:6b:6b:3f:2a
SNMP Community String : public
IP Header            : TTL=0x00 Flags=0x00 Precedence=0x00 TOS=0x00
BMC ARP Control      : ARP Responses Enabled, Gratuitous ARP Disabled
Default Gateway IP   : 0.0.0.0
Default Gateway MAC   : 00:00:00:00:00:00
Backup Gateway IP    : 0.0.0.0
Backup Gateway MAC    : 00:00:00:00:00:00
802.1q VLAN ID       : 333
802.1q VLAN Priority  : 0
RMCP+ Cipher Suites  : 1,2,3,6,7,8,11,12
Cipher Suite Priv Max : XaaaXXaaaXXaaXX
                    : X=Cipher Suite Unused
                    : c=CALLBACK
                    : u=USER
                    : o=OPERATOR
                    : a=ADMIN
                    : O=OEM

Bad Password Threshold : Not Available

```

If you use IPv6, use the `ipmitool lan6 print` command instead.

The `ipmitool lan stats get` command shows some LAN statistics.

Example Output

```
IP Rx Packet           : 4096
IP Rx Header Errors    : 0
IP Rx Address Errors   : 0
IP Rx Fragmented       : 0
IP Tx Packet           : 4096
UDP Rx Packet          : 0
RMCP Rx Valid          : 0
UDP Proxy Packet Received : 0
UDP Proxy Packet Dropped : 0
```

4.15.6 Showing User Information

The `ipmitool user summary` command shows the number of the IPMI user accounts.

Example Output

```
Maximum IDs           : 10
Enabled User Count     : 2
Fixed Name Count      : 2
```

The `ipmitool user list` command shows details of the IPMI user accounts.

Example Output

ID	Name	Callin	Link Auth	IPMI Msg	Channel Priv Limit
1		true	false	false	Unknown (0x00)
2	manager	true	false	false	Unknown (0x00)
3		true	false	false	Unknown (0x00)
4		true	false	false	Unknown (0x00)
5		true	false	false	Unknown (0x00)
6		true	false	false	Unknown (0x00)
7		true	false	false	Unknown (0x00)
8		true	false	false	Unknown (0x00)
9		true	false	false	Unknown (0x00)

10	true	false	false	Unknown (0x00)
----	------	-------	-------	----------------

This output does not show whether a user is enabled or disabled.

The `ipmitool user set name <user ID> <user name>` command sets the name of the <ID> IPMI user account.

Example: `ipmitool user set name 4 test02`

The `ipmitool user list` command shows the result.

Example Output

ID	Name	Callin	Link Auth	IPMI Msg	Channel Priv Limit
1		true	false	false	Unknown (0x00)
2	manager	true	false	false	Unknown (0x00)
3		true	false	false	Unknown (0x00)
4	test02	true	false	false	Unknown (0x00)
5		true	false	false	Unknown (0x00)
6		true	false	false	Unknown (0x00)
7		true	false	false	Unknown (0x00)
8		true	false	false	Unknown (0x00)
9		true	false	false	Unknown (0x00)
10		true	false	false	Unknown (0x00)

The `ipmitool user set password <user ID> [password <16|20>]` command sets the password of the user <user ID>.

Example output: `Set User Password command successful (user 4)`

The `ipmitool user disable <user ID>` command disables an IPMI user account, and the `ipmitool user enable <user ID>` command enables it. There is no output for these commands.



Only use the `ipmitool` commands described in this section to change settings. Use the other commands only for retrieving data.

4.15.7 Default IPMI Interface Configuration



Because the use of IPMI via the network is a security risk, measures have been taken to minimize this risk. Before you change the default IPMI configuration, we strongly recommend that you are aware of best practice security proposals for IPMI.

The third network interface (**a5**) of the CryptoSever LAN is the IPMI interface.

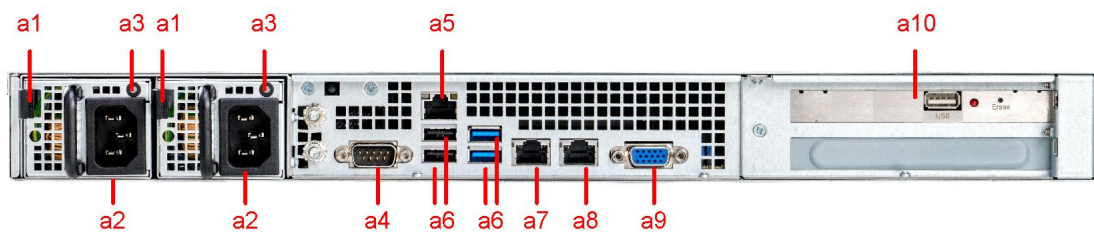


Figure 32 : Rear View

For security reasons, a specific default configuration has been chosen to avoid accidental access to this interface. It is configured as a dedicated interface. This means that other network interfaces (**a7** and **a8**) do not respond to IPMI requests.

Default configuration:

- IPv4 address: 10.10.10.10/24
- IPv6 address: fe80::
- VLAN ID: 333
- RMCP port: 59

The configuration shows that only access to a non-routable address in a specific VLAN is possible. This prevents access from the internet.

Remark: The RMCP port can be changed using the web interface. The default IPMI RMCP UDP port is 623.

4.15.8 Changing the Default IPMI Interface Configuration

4.15.8.1 Setting up IP Reachability

The following steps describe how to change the IP reachability.



The inadequate use of IPMI is a security risk. We highly recommend being aware of the best practices security proposals for IPMI.

1. Ensure that the eth0 (a7) or eth1 (a8) port is connected to your network.
2. Ensure that the IPMI port (a5) is connected to your network.

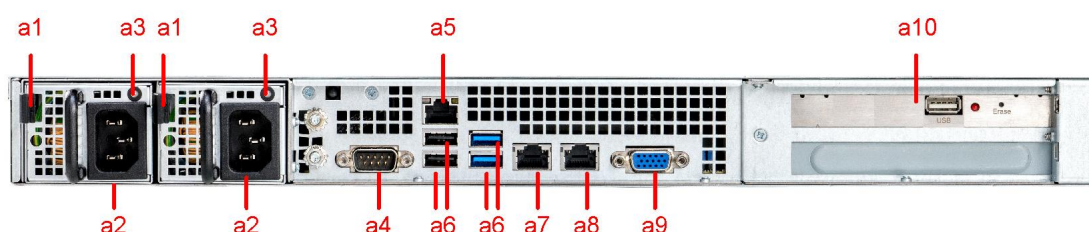


Figure 33 : Rear View

The a5 port is the only port that can be used for IPMI, and this port can be used only for IPMI.

3. Log in remotely to the device according to chapter [2018-0010 Logging in Remotely to the u.trust Anchor LAN \(p. 141\)](#).

Make sure to log in as `root`, not as `cslagent`. Otherwise, you will get an error message when performing an `ipmitool` command.

Example of an error:

```
cslagent@CryptoServer:~$ ipmitool sdr
Could not open device at /dev/ipmi0 or /dev/ipmi/0 or /dev/ipmidev/0:
No such file or directory
```

4. Verify the current interface configuration by performing the `ipmitool lan print` command. For details, see [Showing LAN Information \(p. 137\)](#).
5. Depending on the needs in your network, enable or disable the VLAN ID.
 - Enabling the VLAN ID with `<x>` being an integer value.


```
ipmitool lan set 1 vlan id <x>
```

- Disabling the VLAN ID.

```
ipmitool lan set 1 vlan id off
```

6. If you want to use DHCP to assign an IPv4 address dynamically, perform the following command.

```
ipmitool lan set 1 ipsrc dhcp
```

7. If you want to assign a static IPv4 address, perform the following substeps.

- a. Enable a static IPv4 address.

```
ipmitool lan set 1 ipsrc static
```

- b. Assign the static IPv4 address of the IPMI port.

```
ipmitool lan set 1 ipaddr <IPMI IP address>
```

- c. Set the IPv4 netmask.

```
ipmitool lan set 1 netmask <netmask>
```

Example:

```
ipmitool lan set 1 netmask 255.255.255.0
```

- d. Set the IPv4 default gateway.

```
ipmitool lan set 1 defgw ipaddr <IP address of the default gateway>
```

- e. Set the MAC address.

```
ipmitool lan set 1 defgw macaddr <MAC address of the default gateway>
```



As already mentioned above, the inadequate use of IPMI is a security risk. Changes in the configuration are performed at your own risk.

4.15.8.2 Setting up the IPMI Web Server

The following steps describe how to set up the IPMI web server. This web server provides easy access to almost all IPMI settings.



Enable the IPMI web server access only if you have a deep knowledge of IPMI.



Using the IPMI web server access is not recommended for the CryptoServer LAN since it may conflict with the internal use of IPMI for the CryptoServer LAN. The inadequate use of IPMI is a security risk. We highly recommend being aware of the best practices security proposals for IPMI.

1. Ensure that the instructions in [Setting up IP Reachability \(p. 141\)](#) have been performed and that you are still logged in to the device as `root`, not as `csagent`.
2. Verify the setting of the HTTP and/or HTTPS port by performing the following substeps. Ports are always given in two bytes. The first one is the low byte and the second one is the high byte, for example, `0x50 0x00` is port 80.
 - a. Verify the HTTP port:

```
ipmitool raw 0x30 0x70 0x67 0 0
```
 - b. Set the HTTP port to `80`:

```
ipmitool raw 0x30 0x70 0x67 1 0 0x50 0x00
```
 - c. Verify the HTTPS port:

```
ipmitool raw 0x30 0x70 0x67 0 1
```
 - d. Set the HTTPS port to `443`:

```
ipmitool raw 0x30 0x70 0x67 1 1 0xbb 0x01
```
3. Enable the IPMI web services (HTTP and HTTPS) by performing the following substeps. To disable or enable services, information is coded in two bytes. Disabling is `0x00 0x00` and enabling is `0x01 0x00`.
 - a. Verify the HTTP service:

```
ipmitool raw 0x30 0x70 0x67 0 6
```
 - b. Enable the HTTP service:

```
ipmitool raw 0x30 0x70 0x67 1 6 0x01 0x00
```

If you want to disable the IPMI web service (HTTP) at a later date, perform the following command.

```
ipmitool raw 0x30 0x70 0x67 1 6 0x00 0x00
```
 - c. Verify the HTTPS service:

```
ipmitool raw 0x30 0x70 0x67 0 7
```
 - d. Enable the HTTPS service:

```
ipmitool raw 0x30 0x70 0x67 1 7 0x01 0x00
```

If you want to disable the IPMI web service (HTTPS) at a later date, perform the

following command.

```
ipmitool raw 0x30 0x70 0x67 1 7 0x00 0x00
```

4. Enter the IPMI IP address of the CryptoServer LAN in a web browser.



As already mentioned above, the inadequate use of IPMI is a security risk. Changes in the configuration are performed at your own risk.

5. Log in as the `manager` user with the password `utimacoipmi`.
6. Browse the IPMI web server according to your needs.

4.16 Changing the SSH Login Banner

The SSH daemon can be modified to present a custom banner. This banner will be present if using either shared key login or normal password-prompted login.

1. Create a banner file that will be printed when a user logs in via ssh. A good place to keep this file is in the ssh configuration directory `/etc/ssh`

```
# cd /etc/ssh
# vi example_banner
```

2. Add your banner text.

```
This is the ssh example banner
```

3. Edit the sshd configuration file `/etc/ssh/sshd_config` and uncomment this entry, pointing it to the path of the file you just created:

```
# no default banner path
#Banner none
Banner /etc/ssh/example_banner
```

4. Stop and restart sshd to have it re-read the configuration file and use the banner:

```
# service sshd restart
```



The next time a user connects via ssh they will see the banner:

```
$ ssh cslagent@10-118.180.125  
This is the ssh example banner  
  
cslagent@10.118.180.125's password:
```

5 Administering the CryptoServer

You can use the menu options on the CryptoServer LAN to administer the CryptoServer mounted within the CryptoServer LAN. This chapter describes the range of administration options available to you here.

5.1 Showing CryptoServer Information

5.1.1 Showing the CryptoServer Status

If you want to see the CryptoServer's status, follow these steps:

1. Press the **ENTER** button you see on the front panel on the CryptoServer LAN.
2. Use the **↓** button to select **HSM admin.** and press the **ENTER** button to open the menu item.
3. Press the **ENTER** button to open the HSM Info menu item.
4. Press the **ENTER** button to open the **State menu** item.

This step is equivalent to the `csadm GetState` command. For details about this command, see [CryptoServer – csadm Manual \(p. 240\)](#).

You then see, for example, the following information in the CryptoServer LAN's display:

Example Output

```
mode      = Operational Mode
state     = INITIALIZED (0x00100004)
temp      = 31.6 [C°]
alarm     = OFF
bl_ver    = 5.01.0.5
hw_ver    = 5.01.0.0
uid       = d8000008 c2cafe01
adm1=53653530 20202020 43533430 30303039
         CSe100 CS507903
adm2=494e5445 524e0000 32303039 30390000
         SecurityServer
adm3=496e6974 5f646576 5f707276 00000000
         INSTALLED
```

Use the **↑** and the **↓** button to scroll the text down and up.

The following table explains what the serial numbers and the codings mean, their format and their appearance.

Status Information	Meaning and Coding
mode	<p>Operating mode of the CryptoServer:</p> <p>Operational The regular set of firmware modules (<code>*.msc</code>) is started. All administration and cryptographic functions are available.</p> <p>Operational Mode – Administration-Only The regular set of firmware modules (<code>*.msc</code>) is started. All administration functions are available. All cryptographic functions are blocked.</p> <p>Maintenance Backup set of firmware modules (<code>*.sys</code>) is started (e.g., in alarm state)</p> <p>Bootloader The Bootloader is running. The operating system and the regular set of firmware modules have not been started yet.</p>
state	<p>Current operating state of the CryptoServer (should be INITIALIZED):</p> <p>MANUFACTURED This state is only relevant during production process.</p> <p>INITIALIZED Firmware modules and all system keys (Production Key, Module Signature Key, default Administrator Key (<code>ADMIN.key file</code>)) are loaded.</p> <p>DEFECT CryptoServer is defect. Contact the manufacturer, Utimaco IS GmbH.</p>
temp	<p>Current temperature (in °C).</p> <p>You find detailed information about the CryptoServer's behavior depending on its internal temperature in <i>Temperature Monitoring</i> in the CryptoServer – Administration Manual (p. 240).</p>

Status Information	Meaning and Coding
alarm	<p>Current alarm status. It can be either ON or OFF. If ON, the following reasons are possible and shown in case of an alarm state:</p> <ul style="list-style-type: none"> • Power is too low (empty battery) • Power is too high • Temperature too high (> 66°C) • Temperature too low (< -13 °C) • Outer foil is broken (This alarm is only relevant for CryptoServer CSe-Series.) • Inner foil is broken (This alarm is only relevant for CryptoServer CSe-Series.) • External Erase is executed (manually by a short-circuit of the corresponding pins on the PCIe card) • Invalid/Corrupted Master Key • Communication to sensor controller failed <p>In addition it is shown if the alarm reason is still present or if it has been removed in the meantime (for example, an empty battery has been replaced).</p>
bl_ver	Current bootloader version and the model type of the CryptoServer
hw_ver	Version of the hardware for the CryptoServer CSe-Series and CryptoServer Se-Series Gen2.
uid	<p>UID is an 8-byte binary data field. The UID is a "Universal Identification" that uniquely identifies every CryptoServer PCIe card. It is stored on a hardware component and loaded onto the PCIe card during production. The UID is displayed when the status information is extracted. It is not stored on the CryptoServer.</p>
adm1	<p>adm1 is a readable character string, with a length of 16 characters. The first 8 characters of adm1 contain a short form of the CryptoServer's model type, filled with blank spaces CSe10, Se12, CSe100, Se52, Se500 or Se1500. The second 8 characters represent the unique serial number of the CryptoServer's PCIe card. This serial number is assigned by Utimaco IS GmbH during manufacture and then loaded into the CryptoServer. The serial number starts with the letters CS, followed by a 6-digit number. The adm1 character string is displayed when you select the status information. The 8-character serial number CSxxxxxx is also stored on the CryptoServer PCIe card.</p>

Status Information	Meaning and Coding
adm2	<p>adm2 is a readable 16-character string.</p> <p>The contents of the adm2 character string is also assigned by Utimaco IS GmbH and loaded onto the CryptoServer during production. Whilst the CryptoServer is being manufactured, the name of the firmware module package loaded for the customer is also recorded here, according to which CryptoServer model series is being produced.</p> <p>The adm2 character string is displayed when you select the status information. It is not stored on the CryptoServer.</p> <p>This field may be empty.</p>
adm3	<p>adm3 is a readable 16-character string.</p> <p>During production, a default value is recorded here, according to which CryptoServer model is being manufactured.</p> <p>For a CryptoServer CSe-Series and Se-Series Gen2, the value <code>INSTALLED</code> is recorded here.</p>
error state	Error code indicating that a power-on self-test has failed. If these tests succeed, nothing is shown.

Table 10: CryptoServer status information fields

The bit representation of the state field has the following meaning:

Bit(s)		Value	Description
	CryptoServer state		
0 ... 6		1	DEFECT
		2	MANUFACTURED
		4	INITIALIZED
		5	OPERATIONAL
	Alarm		
7		0	OFF
		1	ON
	Sensor		
8		0	The temperature is too low.
		1	No temperature low alarm has been registered.
9		0	The temperature is too high.
		1	No temperature high alarm has been registered.
10		0	The inner foil has been broken. This is only possible for CryptoServer CSe-Series.
		1	No inner foil alarm has been registered. This is only possible for CryptoServer CSe-Series.
11		0	The outer foil has been broken. This is only possible for CryptoServer CSe-Series.
		1	No outer foil alarm has been registered. This is only possible for CryptoServer CSe-Series.

Bit(s)		Value	Description
12		-	This bit is not used anymore. This bit was only used by CryptoServer 2000 and CryptoServer CS-Series with boot loader version < 2.5.0.0, which is not in the scope of this document.
13		0	The power is too high (power overdrive).
		1	No power high alarm has been registered.
14		0	The power is too low.
		1	No power low alarm has been registered.
15		0	The external erase has been executed.
		1	No external erase alarm has been registered.
16		0	No alarm is present.
		1	An alarm is still present.
17		0	No alarm has occurred.
		1	An alarm has occurred.
FIPS140 mode			
18		0	FIPS mode OFF
		1	Some FIPS mode (restricted (CryptoServer Se-Series only) or validated, see bit 26 below)
Boot Mode			
19 ... 20		0	The boot loader is started (not possible here).
		1	*.sys modules are started.
		2	*.msc modules are started.
...			
FIPS140 (2)			
26		0	FIPS mode = ON
		1	FIPS Mode = OFF but FIPS restrictions are applied (CryptoServer Se only)
Administration-only mode			
27		0	Administration-Only Mode = OFF
		1	Administration-Only Mode = ON

Table 11: Table 11: The bit representation of the state field

5.1.2 Showing Symbols

The following symbols are used on the display of the CryptoServer LAN.

Symbol	Description
Full battery	Sufficient voltage in the external battery
Low battery	Low voltage in the external battery. To exchange it, see <i>Replacing the External Battery</i> in the CryptoServer LAN V5 - Operating Manual (p. 240) . For details about voltage threshold values, see <i>Power Supply Monitoring</i> in the CryptoServer Administration Manual (p. 240) .
No battery	No external battery available
Arrows	The cursor on the far left-hand side of the display shows you which submenu you can select with the ENTER button. The down arrow ↓ and the up arrow ↑ in the first line indicate that this menu contains more menu items below or above the currently shown menu items.

Table 12: Symbols on the display

5.1.3 Showing the Battery Status

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.
2. Use the ↓ button to select **HSM admin.** and press the **ENTER** button to open the menu item.
3. Press the **OK** button to open the **HSM Info** menu item.
4. Use the ↓ button to select **Battery State** and press the **ENTER** button to open the menu item.

This step is equivalent to the `csadm GetBattState` command. For details about this command, see [CryptoServer – csadm Manual \(p. 240\)](#).

The CryptoServer LAN's display shows you the status and the voltage (in V) of the carrier battery and the external battery. The carrier battery is mounted on the CryptoServer PCIe card. The external battery is mounted in the CryptoServer LAN. Both batteries supply power to the CryptoServer in the CryptoServer LAN.



If the system could not find out the battery status, because the CryptoServer register is currently being accessed by another process, then you should try to find out the battery state again after waiting a few minutes.



The battery power level shown on the display of the CryptoServer LAN is not updated very frequently. Therefore, after replacing the External Battery we recommend you to wait for at least three minutes before checking the battery state.

5.1.4 Showing the Date and Time on the CryptoServer

To display the CryptoServer's date and time on the CryptoServer LAN display:

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.
2. Use the ↓ button to select **HSM admin.** and press the **ENTER** button to open the menu item.
3. Press the **ENTER** button to open the **HSM Info** menu item.
4. Use the ↓ button to select **Time** and press the **ENTER** button to open the menu item.

You now see the following items on the CryptoServer:

- UTC date and time
- The local time zone, date and time
- The time difference
- Indicator whether the time synchronization has been enabled, see [Setting up NTP \(p. 95\)](#).

Example Output

```
Date(UTC):2019-02-14
Time(UTC): 09:17:52
Timezone:    +0100
Date(loc):2019-02-14
Time(loc): 10:17:52
Time Diff:    0.0 s
NTP module state:
               active
```

5.1.5 Showing Files in the CryptoServer

You can use the menu options on the LAN device to display the files held in the device.

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **HSM Admin.** and press **ENTER**.
3. Press **ENTER** to open the **HSM Info** menu item.
4. Use the ↓ key to select one of the following menu items and then press **ENTER** to open the menu item.

- **List FLASH files**

This step is equivalent to the `csadm ListFiles=FLASH` command.

This displays all the files that are present in the flash memory (RAM) of the device.

You can display all the firmware modules (`*.msc`), databases (`*.db`) and log files (`*.log`) that have been loaded, as well as the license file (`*.slf`).

- **List SYS files (system files)**

This step is equivalent to the `csadm ListFiles=SYS` command. This displays all the system files that are present in the flash memory. These include all the firmware modules (`*.sys`), the bootloader configuration file (`bl.cfg`) and a system log (`sys.log`).

The following keys are also displayed in this directory:

- `mdlsig.key` , the key used to sign the firmware modules.
- `init.key` , the authentication key for device administration tasks.
- `prod.key` , the key used when the device was manufactured.

- **List NVRAM files**

This step is equivalent to the `csadm ListFiles=NVRAM` command. The NVRAM is non-volatile memory which is not deleted if an alarm is triggered.

5.1.6 Showing the Current Firmware Modules

You can use the menu options on the LAN device to display a list of currently active firmware modules which the device could start when it boots up.

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **HSM admin.** and press **ENTER**.
3. Press **ENTER** to select **HSM Info**.

4. Use the **↓** key to select **List FW modules** and press **ENTER** to open the menu item.

This step is equivalent to the `csadm ListModulesActive` command.

The following information is displayed from left to right:

- Firmware module ID and name of the firmware module
- Firmware module version
- Status of the firmware module

Example Output

0000SMOS	5.6.5.2	OK
0004POST	2.2.1.0	OK
0068CXI	2.4.11.1	OK
0081VDES	2.2.1.0	OK
0082PP	1.4.1.2	OK
0083CMDS	3.8.6.0	OK
0084VRSA	2.2.1.0	OK
0085SC	1.2.0.7	OK
0086UTIL	3.0.7.1	OK
0087ADM	3.1.4.0	OK
0088DB	2.0.0.2	OK
0089HASH	2.2.1.0	OK
008aSTUN	0.0.0.1	OK
008bAES	2.2.1.0	OK
008dDSA	2.2.1.0	OK
008eLNA	2.2.1.0	OK
008fECA	2.2.1.0	OK
0091ASN1	2.2.1.0	OK
0096MBK	2.5.2.0	OK
009aNTP	1.2.1.1	OK
009cECDSA	2.2.1.0	OK
009fCRYPT	2.2.1.0	OK

5.1.7 Showing the Boot Log

The boot log is generated every time the device is restarted. If problems occur during the boot process, you can use the boot log for error analysis purposes. The boot log is completely overwritten every time the device is rebooted. The boot log contains the following entries:

- The version number of the loaded operating system.
- FPGA version

- Hardware version
- Compiler version
- If a license file has been loaded, its name is displayed here.
- Depending on which license file has been loaded, after CMD5: you can see whether the transactions per second (TPS) are limited, or whether there are no limits specified for TPS (no TPS limit).
 - The **No Hardware Crypto Engine installed** display tells you that no cryptographic accelerator chip has been installed in the Se12 or Se52 model of the device. If a cryptographic accelerator chip is present in the Se500 or Se1500 models, you see the **Hardware Crypto Engine detected** message.
- If the initialization was successful, you see the configuration settings for the **Pseudo Random Number Generator** and the **Real Random Number Generator**.
- A short description (for example, MBK for Master Backup Key) and a unique identification code (0x96) are displayed for all the firmware modules started by the operating system. The boot log also records whether or not it was possible to start the firmware module successfully (and specifies the reason) and whether it is therefore either ready, or not ready, for use.

To display the boot log on the display of the LAN device:

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **HSM admin.** and press **ENTER**.
3. Press **ENTER** to open the **HSM Info** menu item.
4. Use the ↓ key to select **Show Boot Log** and press **ENTER** to open the menu item.
This step is equivalent to the `csadm GetBootLog` command.

5.2 Administering Keys and Files

5.2.1 Exporting the HSM Authentication Key

Perform the following steps to retrieve the public part of the HSM Authentication Key which is used for the establishment of a mutually authenticated Secure Messaging session for the communication between the CryptoServer and the host applications.

Prerequisites

A USB flash drive is connected to the Host1 or Host2 port on the front panel of the CryptoServer LAN.

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.
2. Use the ↓ button to select **HSM admin.** and press the **ENTER** button to open the menu item.
3. Use the ↓ button to select **Key&file admin.** and press the **ENTER** button to open the menu item.
4. Use the ↓ button to select **Export HSM AuthKey** and press the **ENTER** button.
This step is equivalent to the `csadm GetHSMAuthKey` command. For details about this command, see [CryptoServer – csadm Manual \(p. 240\)](#).
5. Press the **ENTER** button once more to perform this command.
A file with the name `<CryptoServer serial number>.key`, for example, `CS601234.key` is created in the root directory of the USB flash drive. Now mutual authenticating can be enabled. For details, see *Enabling Mutual Authentication* in the [CryptoServer – csadm Manual \(p. 240\)](#).

5.2.2 Loading a File onto the CryptoServer

You can use the menu options on the CryptoServer LAN to upload files to the CryptoServer. However, you can only upload files to the CryptoServer's RAM (FLASH).

You can only upload license files and firmware modules to the CryptoServer's RAM via the CryptoServer LAN's menu options. You must authenticate the command before you can start uploading firmware modules or license files to the CryptoServer. To do so, you require the current user authentication key, and this must be saved on a smartcard.

The accompanying PIN pad must therefore have been prepared, using the CryptoServer LAN menu options.

If you want to upload a new license file to the CryptoServer, you must first delete the old license file. The CryptoServer can only ever hold one license file at a time. If you want to upload a firmware module to the CryptoServer, you must ensure that this file has the correct file extension (`.mtc`). If you want to upload a firmware package, the file must have `.mpkg` as its file extension.



If the file you want to upload (for example a firmware module) is already present in the CryptoServer, and has the same name, the current file will be replaced by the new one.



The file (a firmware module, `*.mtc` or a firmware package, `*.mpkg`) you want to upload has to be placed in the main directory of a USB flash drive, so that it is shown on the display of the CryptoServer LAN and can be selected for upload.



CryptoServer LAN can access data only from a single trustworthy USB flash drive connected to it. Although more than one USB flash drives can be simultaneously plugged in to the CryptoServer LAN, the USB device that has been inserted as first gets connected with the CryptoServer LAN. To establish a connection to another USB device, you should first disconnect the currently connected one and then plug the next USB flash drive into the corresponding USB port of the CryptoServer LAN.

Prerequisites

- PIN pad connection

In a later step, loading a file is initiated by selecting a menu option on the display and pressing the **ENTER** button on the front panel of the CryptoServer LAN. This action must be authenticated by a user. This user is specified by the `AdminName` parameter in the `/etc/csxlan.conf` file.

- If this user uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a smartcard or a keyfile), the PIN pad must either be connected to the USB port labelled **Host1** or **Host2** on the front panel of the CryptoServer LAN (f4) or to one of the a6 USB ports on the rear side of the CryptoServer LAN.
All these USB ports are directly connected to the Linux host inside the CryptoServer LAN. Chapter *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer - Administration Manual](#) (p. 240) does not apply here.
- If this user user RSA smartcard authentication, the PIN pad must either be connected to the USB port labelled HSM on the front panel of the CryptoServer LAN (f5) or to the USB port of the CryptoServer (PCIe card) on the rear side of the

CryptoServer LAN (a10). All these USB ports are directly connected to the CryptoServer, see also [Connecting the PIN Pad \(p. 42\)](#).

- Permission

In a later step, you need the user authentication key of the user specified by the `AdminName` parameter in the `/etc/csxlan.conf` file. You need this user authentication key saved on a smartcard to load files onto the CryptoServer. This user authentication key must have at least permission 2 in group 6, i.e., permission 02000000. Make sure that the appropriate smartcard is available.

To load a file, perform the following steps.

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.
2. Use the ↓ button to select **HSM admin.** and press the **ENTER** button to open the menu item.
3. Use the ↓ button to select **Key&file admin.** and press the **ENTER** button to open the menu item.
4. Use the ↓ button to select **Load file** and press the **ENTER** button to open the menu item. Follow the instructions on the display.
 - a. Connect the USB flash drive to the **Host1** or **Host2** USB port on the front panel of the CryptoServer LAN or to the a6 USB port on the rear side of the CryptoServer LAN.
 - b. Press the **ENTER** button. On the display, you can now see which files (not directories and subdirectories) are present in the main directory on the USB flash drive.
5. Use the ↓ button to select the relevant file and confirm your selection by pressing **ENTER**.
6. Follow the instructions on display of the PIN pad. If the file loads successfully, it appears on the CryptoServer LAN's display.

5.2.3 Deleting a File in the CryptoServer

You can only use the menu options on the CryptoServer LAN to delete the following files from the CryptoServer:

- License files with the `.slf` file extension
- Firmware modules with the `.msc` file extension

The files you can delete here are deleted from the CryptoServer's RAM (FLASH).

Prerequisites

- PIN pad connection

In a later step, deleting a file is initiated by selecting a menu option on the display and pressing the ENTER button on the front panel of the CryptoServer LAN. This action must be authenticated by a user. This user is specified by the AdminName parameter in the `/etc/csxlan.conf` file.

- If this user uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a smartcard or a keyfile), the PIN pad must either be connected to the USB port labelled Host1 or Host2 on the front panel of the CryptoServer LAN (f4) or to one of the a6 USB ports on the rear side of the CryptoServer LAN. All these USB ports are directly connected to the Linux host inside the CryptoServer LAN. Chapter *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer - Administration Manual \(p. 240\)](#) does not apply here.
- If this user uses RSA smartcard authentication, the PIN pad must either be connected to the USB port labelled **HSM** on the front panel of the CryptoServer LAN (f5) or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN (a10).
All these USB ports are directly connected to the CryptoServer, see also [Connecting the PIN Pad \(p. 42\)](#).
- Permission
In a later step, you need the user authentication key of the user specified by the AdminName parameter in the `/etc/csxlan.conf` file. You need this user authentication key saved on a smartcard to delete a file on the CryptoServer. This user authentication key must have at least permission 2 in group 6, i.e., permission 02000000. Make sure that the appropriate smartcard is available.

To delete a file, perform the following steps.

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.
2. Perform the following sub-steps verify whether the CryptoServer is in operational mode.

- a. Use the ↓ button to select **HSM admin.** and press the **ENTER** button to open the menu item.
 - b. Press the **ENTER** button to open the **HSM Info menu** item.
 - c. Press the **ENTER** button to open the State menu item. Verify whether the CryptoServer in the CryptoServer LAN is in Operational Mode, i. e. the display shows the following line. mode = Operational
 - d. Continue with the following steps only if this line is shown.
3. Press the ESC button twice.
4. Use the ↓ button to select **Key&file admin.** and press the **ENTER** button to open the menu item.
5. Use the ↓ button to select Delete file and press the **ENTER** button to open the menu item. You now see a list of files.
6. Use the ↓ button to select the file you want to delete and confirm your selection by pressing **ENTER**. This step is equivalent to the `csadm ... DeleteFile` command. For details about this command, see [CryptoServer - csadm Manual \(p. 240\)](#).
7. Follow the instructions on the PIN pad. The CryptoServer LAN's display then shows whether you have deleted the file successfully.

5.2.4 Changing the Administrator's Authentication Key

The AdminName parameter in the `/etc/csxlan.conf` file specifies the user that is used for authenticating commands that are initiated by selecting a menu option on the display and pressing the ENTER button on the front panel of the CryptoServer LAN. By default, this user is the ADMIN user.

See the following chapters for examples:

- [Setting up NTP Mainly Using the Front Panel \(p. 98\)](#) (see step 2 for specifying the user and see step 8g) for performing the command)
- [Loading a File onto the CryptoServer \(p. 156\)](#)
- [Deleting a File in the CryptoServer \(p. 158\)](#)
- [Loading the Firmware Encryption Key into the CryptoServer \(p. 163\)](#)

This chapter deals with assigning a new RSA user authentication key to this user.

Before delivery Utimaco creates the default ADMIN user on every CryptoServer as the default administrator. The authentication token of the user ADMIN is shipped by Utimaco as clear text keyfile (`ADMIN.key`) on the SecurityServer product CD in the following directories.

- `...\Software\Linux\Administration\key`
- `...\Software\Windows\Administration\key`

This keyfile is initially stored on every smartcard that is delivered by Utimaco IS GmbH (with default PIN 123456).

For security reasons you should replace the authentication token of the user ADMIN with a self-generated RSA key as described in this chapter. Alternatively, you can create other users with sufficient permissions on the CryptoServer, and then delete the user ADMIN. For details, see [CryptoServer – csadm Manual \(p. 240\)](#) and [CryptoServer – CAT Manual \(p. 240\)](#).

Prerequisites

Before you can change the user authentication key of the user specified by `AdminName` by using the menu options on the front panel of the CryptoServer LAN, there are some preparation steps required.

- PIN pad connection
In a later step, changing the user authentication key is initiated by selecting a menu option on the display and pressing the ENTER button on the front panel of the CryptoServer LAN. This action must be authenticated by a user. This user is specified by the `AdminName` parameter in the `/etc/csxlan.conf` file.
 - If this user uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a smartcard or a keyfile), the PIN pad must either be connected to the USB port labelled **Host1** or **Host2** on the front panel of the CryptoServer LAN (f4) or to one of the a6 USB ports on the rear side of the CryptoServer LAN. All these USB ports are directly connected to the Linux host inside the CryptoServer LAN. Chapter *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer - Administration Manual \(p. 240\)](#) does not apply here.
 - If this user user RSA smartcard authentication, the PIN pad must either be connected to the USB port labelled HSM on the front panel of the CryptoServer LAN (f5) or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN (a10). All these USB ports are directly connected to the CryptoServer. See also [Connecting the PIN Pad \(p. 42\)](#).

- You have generated a new user authentication key (RSA) and have stored it on one of the smartcards delivered by Utimaco. You can do that by using either the csadm tool commands `GenKey` and `SaveKey` (see [CryptoServer – csadm Manual \(p. 240\)](#)), or CAT (see [CryptoServer – CAT Manual \(p. 240\)](#)).
- Two smartcards delivered by Utimaco are available:
 - One containing the current user authentication key for the user specified by `AdminName`.
 - One where the new RSA user authentication key is stored on.
- The CryptoServer in the CryptoServer LAN is in Operational Mode, i. e. on the display of the CryptoServer LAN, you see **mode = Operational**. Perform **HSM admin. > HSM Info > State**, to see this on the display.

These following steps are equivalent to the `csadm ChangeUser=<user>` command with `<user>` being the user specified by `AdminName` in the `/etc/csxlan.conf` file. For details about this command, see [CryptoServer – csadm Manual \(p. 240\)](#).

1. Press the **ENTER** button on the front panel of the CryptoServer LAN.
2. Use the **↓** button to select the **HSM admin.** menu item, and press **ENTER** to open the menu item.
3. Use the **↓** button to select **Key&file admin.** and press the **ENTER** button to open the menu item.
4. Use the **↓** button to select **Change ADMIN authKey** and press the **ENTER** button to open the menu item.

You should see on the CryptoServer LAN display:

```
Change User auth key
First the OLD token card,
then the card with the card with the NEW token
Press ENTER key ...
```

5. Follow the instructions on the display of the PIN pad:
 - a. Insert the smartcard where the current user authentication key (default: `ADMIN.key`) is stored on into the PIN pad.
 - b. Press the **OK** button on the PIN pad.
 - c. Enter the smartcard PIN (default 123456) and press the **OK** button on the PIN pad.

- d. Remove the smartcard and press **OK** on the PIN pad.
- e. Insert the smartcard where the new user authentication key is stored on into the PIN pad.
- f. Press the **OK** button on the PIN pad

The successful change of the user authentication key for the user specified by AdminName is confirmed on the display of the CryptoServer LAN.

5.2.5 Loading the Firmware Encryption Key into the CryptoServer

Utimaco customers can develop their own CryptoServer firmware modules corresponding to their individual needs and providing customer specific functions. These firmware modules have to be signed with a customer-individual key *Alternative Module Signature Key*. The public part of this key has to be loaded into the CryptoServer before the firmware modules can be loaded into the CryptoServer.

Optionally, the self-developed firmware modules can be encrypted with the public part of a customer-specific *Firmware Encryption Key* (RSA key). In this case the private part of this key has to be loaded into the CryptoServer. This chapter describes how to load the private part of a previously generated *Firmware Encryption Key* into the CryptoServer by using the menu options on the front panel of the CryptoServer LAN.

Prerequisites

Before you can start loading the Firmware Decryption Key into the CryptoServer by using the menu options on the front panel of the CryptoServer LAN, there are some preparation steps required.

- PIN pad connection for the smartcards with the firmware decryption key shares
In any case, one PIN pad must either be connected to the USB port labelled **Host1** or **Host2** on the front panel of the CryptoServer LAN (f4) or to one of the a6 USB ports on the rear side of the CryptoServer LAN. All these USB ports are directly connected to the Linux host inside the CryptoServer LAN.
- PIN pad connection for the smartcard with the user authentication key
In a later step, loading the firmware decryption key is initiated by selecting a menu option on the display and pressing the **ENTER** button on the front panel of the CryptoServer LAN. This action must be authenticated by a user. This user is specified by the `AdminName` parameter in the `/etc/csxlan.conf` file. The user authentication key of this user is needed on a smartcard in a PIN pad.

- If this user uses RSA signature authentication (with a smartcard or a keyfile) or ECDSA signature authentication (with a smartcard or a keyfile), the PIN pad must either be connected to the USB port labelled Host1 or Host2 on the front panel of the CryptoServer LAN (f4) or to one of the a6 USB ports on the rear side of the CryptoServer LAN. All these USB ports are directly connected to the Linux host inside the CryptoServer LAN. Chapter *Using a Local PIN Pad for a Remote CryptoServer* in the [CryptoServer – Administration Manual \(p. 240\)](#) does not apply here.

Because a PIN pad connected to this USB port is already required for the firmware decryption key, no second PIN pad is needed.

- If this user user RSA smartcard authentication, the PIN pad must either be connected to the USB port labelled HSM on the front panel of the CryptoServer LAN (f5) or to the USB port of the CryptoServer (PCIe card) on the rear side of the CryptoServer LAN (a10). All these USB ports are directly connected to the CryptoServer. In this case, we need a total of two PIN pads, one for the firmware decryption key shares (**Host1/Host2** PIN pad connection) and one for the user authentication key (**HSM** PIN pad connection). See also [Connecting the PIN Pad \(p. 42\)](#).
- The CryptoServer in the CryptoServer LAN is in Operational Mode, i. e. on the display of the CryptoServer LAN you see Mode: Operational. Perform **HSM admin. > HSM Info > State**, to see this on the display.
- You have created your firmware module, for example, `expm.out`, which you have signed with your self-generated Alternative Module Signature Key (for example, `FWSignKey.key`, 2048 bits RSA key) and encrypted with your self-generated Firmware Encryption Key (for example, `FWEncKey.key`, 2048 bits RSA key). For details about how to sign and encrypt self-developed firmware modules, see [CryptoServer – csadm Manual \(p. 240\)](#).
- You have loaded the Alternative Module Signature Key into the CryptoServer, for example, by using the `csadm LoadAltMdlSigKey` command, see [CryptoServer – csadm Manual \(p. 240\)](#).
- You have copied the private part of the Firmware Encryption Key on two smartcards, for example, by using the `csadm BackupKey` command, see [CryptoServer – csadm Manual \(p. 240\)](#).
- Three smartcards delivered by Utimaco are at hand:

- One where the user authentication key for the user specified by the `AdminName` parameter in the `/etc/csxlan.conf` file (default user ADMIN) is stored on
- Two smartcards where the private part of your Firmware Encryption Key split in two shares is stored on.

1. Press the **ENTER** button on the front panel of the CryptoServer LAN.
2. Use the ↓ button to select the **HSM admin.** menu item, and press **ENTER** to open the menu item.
3. Use the ↓ button to select **Key&file admin.** and press the **ENTER** button to open the menu item.

4. Use the ↓ button to select **Load FW DecrKey** and press the **ENTER** button to open the menu item

This step is equivalent to the `csadm LoadFWDecrKey` command. For details about this command, see [CryptoServer – csadm Manual \(p. 240\)](#).

The CryptoServer LAN display shows the following text.

```
Change FW decr key
in progress...
```

The display on the PIN pad shows the following text.

```
Insert Smartcard
press OK/CANCEL
```

or

```
Insert Smartcard
and press key..
```

5. You have the smartcard where the user authentication key for the user specified by the `AdminName` parameter in the `/etc/csxlan.conf` file (default user ADMIN) is stored on. Insert this smartcard into the PIN pad.

If this user uses RSA smartcard authentication, this PIN pad is not the PIN pad that is used for the smartcards containing the firmware decryption key shares (see the prerequisites above).

6. Press the **OK** button on the PIN pad.
The display on the PIN pad shows the following text.

```
Enter PIN
```

7. Enter the PIN of the smartcard and press **OK** on the PIN pad.

8. The display on the PIN pad that is connected to the USB port labelled **Host1** or **Host2** on the front panel of the CryptoServer LAN (f4) or to one of the a6 USB ports on the rear side of the CryptoServer LAN shows the following text.

```
Insert FwDecKey  
card & confirm
```

9. Insert the smartcard where the first key share of the Firmware Encryption Key is stored on into the PIN pad.
10. Press the **OK** button on the PIN pad.
The display on the PIN pad shows the following text.

```
Enter PIN
```

11. Enter the PIN of the smartcard (default 123456) and press **OK** on the PIN pad.
The display on the PIN pad shows the following text.

```
Insert FwDecKey  
card & confirm
```

12. Insert the smartcard where the second key share of the Firmware Encryption Key is stored on into the PIN pad.
 13. Press the **OK** button on the PIN pad.
The display on the PIN pad shows the following text.
14. Enter the PIN of the second smartcard and press **OK** on the PIN pad.

```
Enter PIN
```

The display of the CryptoServer LAN shows you that you have successfully loaded the Firmware Encryption Key into the CryptoServer. You can now load your self-developed firmware module into the CryptoServer by using the `csadm LoadFile` command, see [CryptoServer – csadm Manual \(p. 240\)](#).

5.3 Recovery

5.3.1 Restarting the CryptoServer

Some of the settings you make on the CryptoServer will require you to reboot the device before the changes come into effect.

1. On the front panel of the CryptoServer LAN, press the **ENTER** button.

2. Use the ↓ button to select **HSM admin.** and press the **ENTER** button to open the menu item.
3. Use the ↓ button to select **Recovery** and press the **ENTER** button to open the menu item.
4. Press the **ENTER** button to open the **Restart HSM** menu item. This step is equivalent to the `csadm Restart` command. For details about this command, see [CryptoServer – csadm Manual \(p. 240\)](#).

The system displays the successfully performed action on the display of the CryptoServer LAN.

5.3.2 Resetting an Alarm

Every alarm on the device must be reset by an administrator. This ensures that the alarm is noticed and investigated properly.

Before you reset an alarm you should find out why it was triggered in the first place. If the alarm is a temporary alarm triggered, for example, because the mains power supply is too low, or because the internal temperature is either too high or too low, you must resolve the cause of the alarm before resetting it.

If you do not resolve the cause, the device will return to Maintenance Mode after you restart it. The device will only enter Operational Mode after a restart if you have removed the cause for the alarm.



The Reset Alarm command must be authenticated. To do so the current user authentication key is required, and must be saved on a smartcard.

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **HSM admin.** and press **ENTER**.
3. Use the ↓ key to select **Recovery** and press **ENTER** to open the menu item.
4. Use the ↓ key to select **Reset Alarm** and press **ENTER**.
This step is equivalent to the `csadm ResetAlarm` command.
5. Then follow the instructions on the PIN pad and authenticate this command.



A message that the action was executed successfully is displayed.

5.3.3 Performing the Clear Command

You can use the `Clear` command to delete any sensitive data and firmware modules from the device by hand. The following actions are triggered after you enter this command:

- All the firmware modules are deleted from the flash directory. Only the system firmware modules required for base administration remain on the device.
- All users who have to log in to the device with an HMAC password are deleted.
- A new master key is generated for the device. This automatically makes any other keys (including the MBK) and sensitive data stored on the device unusable, because they can no longer be decrypted, as the "old" master key has been replaced.


However, users who log in to the device with RSA signatures, RSA Smartcard or ECDSA are not deleted.

Once you have performed the `Clear` command, the device is no longer in **Operational Mode** and returns automatically to **Maintenance Mode** after a restart.

The device does not return to Operational Mode until the SecurityServer package's firmware modules are reloaded. You should only perform a `Clear` command if you want to set up or reinstall the device again.

You must authenticate the command before you can perform the `Clear` command using the menu options on the LAN device. To do so, you need the current user authentication key, which must be saved on a smartcard.

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **HSM admin.** and press **ENTER**.
3. Use the ↓ key to select **Recovery** and press **ENTER**.
4. Use the ↓ key to select **Clear (firm/data)** and press **ENTER** to open the menu item.
This step is equivalent to the `csadm ... Clear=INIT` command.
5. Follow the instructions on the PIN pad and authenticate this command.

- 
- The system displays the successfully performed action on the display of the LAN device.

5.3.4 Performing the Clear to Factory Command

When you perform the `Clear to Factory` command, you return the device to the state it was in when it was supplied.

- This command deletes the firmware modules from the flash directory. Only the system firmware modules required for base administration remain on the device.
- All users in the device user database are deleted.
- ADMIN, the default administrator, is set up again and can log in to the device again using the original user authentication key `ADMIN.key`.
- A new master key is generated for the device. This automatically makes any other keys (including the MBK) and sensitive data stored on the device unusable, because they can no longer be decrypted, as the "old" master key has been replaced.
Before you can perform the `Clear to Factory` command, you must first perform an External Erase on the LAN device whilst the alarm is enabled.

Triggering the Clear to Factory Settings command

To perform a **Clear to Factory** on the LAN device, follow these steps:

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **HSM admin.** and press **ENTER**.
3. Use the ↓ key to select **Recovery** and press **ENTER** to open the menu item.
4. Use the ↓ key to select **Clear to Factory** and press **ENTER**.
This step is equivalent to the `csadm Clear=DEFAULT` command.

Resetting the alarm

Finally, you must reset the alarm that was triggered by the *External Erase*.

You must authenticate the command before you can perform the *Reset Alarm* function using the menu options on the LAN device. To do so, you need the current user authentication key, which must be saved on a smartcard.

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **HSM admin.** and press **ENTER**.
3. Use the ↓ key to select **Recovery** and press **ENTER** to open the menu item.
4. Use the ↓ key to select **Reset Alarm** and press **ENTER**.
This step is equivalent to the `csadm ResetAlarm` command.
5. Follow the instructions on the PIN pad and authenticate this command.

5.3.5 Performing an External Erase

Performing an External Erase on the LAN device

To perform an External Erase on the LAN device, follow these steps:

1. Push the corresponding **ERASE** pushbutton by using an appropriate screwdriver.
If a PCIe card CSe-Series has been mounted in the LAN device, pushing the **ERASE** pushbutton is only effective if the LAN device has been switched on.
If pushing the **ERASE** pushbutton should be applied to a PCIe card Se-Series Gen2 in the LAN device, it is not necessary that the LAN device has been switched on.

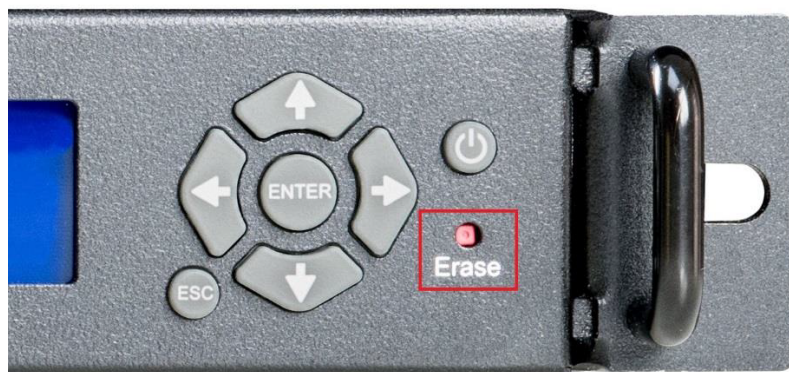


Figure 34 : ERASE pushbutton for performing External Erase

An *External Erase* has been performed on the device, and an Alarm has been triggered.



Regardless of whether you have performed an External Erase (pressing the ERASE push-button) or not, the following applies:

If you remove the PCIe card from the LAN device and remove any battery from this PCIe card, the sensitive data on this PCIe card is deleted automatically in any case after a maximum of 30 minutes.

2. Restart the LAN device using the menu control buttons (CSLAN admin. > Reboot).

5.4 Performing MBK Management on the CryptoServer LAN

The CryptoServer provides secure storage for secret data and keys. This includes, for example, the keys used by the PKCS#11, CSP/CNG, JCE and other interfaces. As any perceived attack will cause the CryptoServer to permanently delete all the sensitive data and keys stored on it, we strongly recommend you backup this data or the keys so they can be reimported (restored) once the alarm has been resolved. To ensure this backup copy of the sensitive data or keys can be stored securely, even outside of the CryptoServer, it is encrypted with the MBK, see *Master Backup Key (MBK)* in the [CryptoServer Administration Manual \(p. 240\)](#) for details.

If you generate the MBK using the menu options on the CryptoServer LAN, you can only store it on a smartcard.

You must connect the PIN pad directly to one of the CryptoServer's USB ports so that the MBK can be managed locally on the CryptoServer. Either use the HSM USB port (f5) on the front panel of the CryptoServer LAN or the USB port on the CryptoServer PCIe card (a10) on the rear side of the CryptoServer LAN.



Figure 35 : Front view of the device

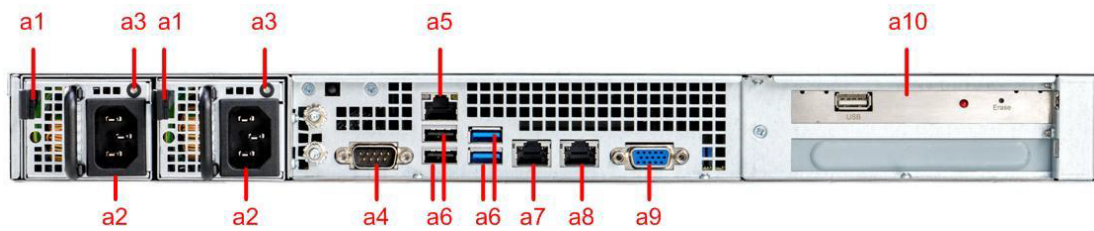


Figure 36 : Rear view of the device

5.4.1 Generating an AES Key and Saving It to a Smartcard

Use the Generate AES Key Shares & Store on SC function to generate an AES key (with 32 bytes) in the secure environment provided by the device and then save it to several smartcards.

When the MBK is saved to a smartcard or to a key file it is always split up into several parts. Splitting the MBK into several parts, known as key shares, is one of the important security functions of the device because it enables the responsibility for the MBK to be given to more than one person.

Before you generate an MBK, you must take the following decisions:

- How many parts should the MBK be split into? This is specified as n (*shares*).
- What is the minimum number of parts that still allow the MBK to be used? This is given as m (*shares*).

Here, n (*shares*) is the number of people to which the key is to be distributed and m (*shares*) is the minimum number of people required to use the key.

You should ensure that you have the corresponding number of smartcards available. The examples below illustrate the relationship between n (*shares*) and m (*shares*) and show which combinations are sensible:

Key Shares	Number	Meaning
n (<i>shares</i>)	4	The MBK has been split in four parts.
m (<i>shares</i>)	2	Two people must be present to use the MBK.

Table 13: Example for an MBK split into four shares

Key Shares	Number	Meaning
n (<i>shares</i>)	2	The MBK has been split in two parts.
m (<i>shares</i>)	2	Two people must be present before the MBK can be used. This corresponds to the familiar principle of requiring approval from a second person.

Table 14: Example for an MBK split into two shares

To generate an MBK (AES) and save it on a smartcard by using the menu control buttons of the LAN device follow these steps:

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **PIN-Pad Applications** and press **ENTER** to open the menu item.
3. Use the ↓ key to select **Generate AES Key Shares & store on SC**.
4. Press **ENTER** and follow the instructions on the PIN pad.

5.4.2 Using the PIN Pad to Import an MBK and Save it to a Smartcard

Use the *Import MBK from PIN-Pad & write it to SC* function to import a plaintext MBK into the device, using the PIN pad, and then to store it on a smartcard.

You must use the PIN pad to enter a total of 32 hexadecimal numbers (16 bytes) for each (XOR) half of the MBK. You can only import one 16-byte DES key (32 hexadecimal numbers) via the PIN pad and then save it to a smartcard. The MBK must not be split into more than 2 parts, to ensure it can be imported into the device via the PIN pad and then saved to a smartcard.

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **PIN Pad Applications** and press **ENTER**.
3. Use the ↓ key to open the **Import MBK from PIN pad & write it to SC** menu item.
4. Press **ENTER** and follow the instructions on the PIN pad.

Note the following:

If you want to enter a letter, you must first press the ^ key (on the bottom left) every time before you enter the letter. Buttons 1 to 6 represent letters A to F. For example, to enter the letter A, you must press the ^ key and then 1 on the PIN pad.

5.4.3 Changing the PIN for the MBK Smartcard

Use the *Change MBK Smartcard PIN* function to change the PIN for the smartcard on which an MBK key is stored.

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **PIN Pad Applications** and press **ENTER**.
3. Use the ↓ key to open the **Change MBK smartcard PIN** menu item.

4. Press **ENTER** and follow the instructions on the PIN pad.

5.4.4 Copying an MBK from One Smartcard to Another

1. You use the *Copy MBK Smartcard* function to copy the MBK key stored on one smartcard to a different smartcard, to create a backup of the MBK on a smartcard.

As a complete MBK is made up of at least two parts and is therefore stored on two smartcards, you must perform this action twice to copy an entire MBK to different smartcards or to create a backup of the MBK on a smartcard.

- a. On the front panel of the LAN device, press **ENTER**.
- b. Use the ↓ key to select **PIN Pad Applications** and press **ENTER**.
- c. Use the ↓ key to open the **Copy MBK smartcard** menu item.
- d. Press **ENTER** and follow the instructions on the PIN pad.
- e. Repeat the process with the second smartcard, on which the second part of the MBK is stored.

5.4.5 Showing MBK Key Information on the Smartcard

Use the *List MBKs on Smartcard* function to display information about an MBK key that is stored on a smartcard.

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **PIN Pad Applications** and press **ENTER**.
3. Use the ↓ key to open the **List MBKs on smartcard** menu item.
4. Press **ENTER** and follow the instructions on the PIN pad.

5.4.6 Generating an MBK (AES) on a Smartcard

Use the *Generate AES MBK on smartcard* function to generate an MBK (AES key with 32 bytes) in the secure environment provided by the device, and then store this MBK on a smartcard.

This function saves the MBK to the smartcard but not to the device. As the MBK is automatically split into two parts, you will need two smartcards to perform this function. The two individual parts of the MBK are then stored on separate cards.

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **PIN-Pad Applications** and press **ENTER**.
3. Use the ↓ key to open the **Generate AES MBK on smartcard** menu item.
4. Press **ENTER** and follow the instructions on the PIN pad.

5.4.7 Importing an MBK (AES) from a Smartcard

You use the *Import AES MBK from Smartcard* function to import an AES key (32 bytes) from a smartcard to the device.

1. On the front panel of the LAN device, press **ENTER**.
2. Use the ↓ key to select **PIN-Pad Applications** and press **ENTER**.
3. Use the ↓ key to open the **Import AES MBK from smartcard** menu item.
4. Press **ENTER** and follow the instructions on the PIN pad.

6 Advanced Administration on the CryptoServer LAN

This chapter describes advanced administration functions for the CryptoServer LAN. None of the administration tasks detailed in this chapter can be performed using the menu options on the CryptoServer LAN. Instead, you must use one of the two following methods to perform advanced administration tasks:

- You can connect a monitor and a keyboard to the CryptoServer LAN. If you do this, you must be familiar with the functions of the standard UNIX vi editor.
- You can also perform extended administration tasks on the CryptoServer LAN remotely by using an SSH client (for example with PuTTY under Windows) from a host computer. You must also be familiar with the functions of the standard UNIX vi editor if you want to access the CryptoServer LAN from a Windows-based host computer using PuTTY.



You must log in as the root user for extended administration tasks and with the password `utimaco` if the device is in its initial state. If you have changed the password for the `root` user, you must input the current password.



If you want to change and save a configuration file on the remote CryptoServer LAN, we highly recommend to perform the changing and saving operations on the CryptoServer LAN itself. Do not perform the changes on a Windows computer and copy the changed file onto the CryptoServer LAN (Linux computer) because the return/line feed representation on Windows differs from the one on Linux.

6.1 Configuring the Transfer Speed for Ethernet

The parameters used to link Ethernet interfaces are usually negotiated automatically. By default, there are two Ethernet interfaces available. Two more interfaces can be added.

However, if you cannot use auto negotiation in your network, you can also configure the network using the following parameters:

<i>Parameter</i>	<i>Description</i>
Speed	Possible values: [10, 100, 1000] Sets the network interface speed in MBit/s.

Parameter	Description
Duplex	Possible values: half or full Sets the network interface duplex mode.
Autoneg	Possible values: on or off Sets auto negotiation for the network interface.

Table 15: Configuration parameter for network usage

You will find the networking file in which the network interface can be configured without auto negotiation here on the LAN device:

```
/etc/sysconfig/networking
```

The example below shows a part of the networking configuration file for the Ethernet eth0 connection and a possible configuration for the network interface.

Example

```
# Begin /etc/sysconfig/networking

NETCONFIG="_0"

NET_DEV_0="eth0"
DHCP_0="no"
IP_ADDR_0="10.10.10.10/24"
ETHTOOL_0="speed 100 duplex half autoneg off"
GATEWAY="10.10.10.254"

# End /etc/sysconfig/networking
```

As you can see from the networking file shown above, you can also modify a range of other configuration parameters, such as IP address or default gateway.



You must ensure that you have set autoneg for auto negotiation to off so your configuration can be used.

6.2 The Configuration File csxlan.conf

The `/etc/csxlan.conf` file is the configuration file for CSXLAN. This is where you configure the majority of the settings for the CryptoServer LAN.

This configuration file is split into the sections `[Csxlan]`, `[CryptoServer]`, `[Listener]` and `[DisplayAdmin]`. Each area includes an assignment of variable tasks.

A simple assignment of a value to a parameter looks like this:


VARIABLE = VALUE

A list of assignments of several values to one parameter looks like this:

VARIABLE = { value1 value2 ... }

The variables for the individual areas are described in the tables below:

Variables for the [Csxlan] section


Parameter	Description
LogLevel	<p>Depending on the log level, more or less information is written into the log file <code>/var/log/csxlan.log</code>. The log level supports the following values. See Configuring the csxlan.conf File (p. 177) for how to use it.</p> <ul style="list-style-type: none"> OFF – Stop producing messages, useful for benchmarks. The corresponding hexadecimal value is <code>-0x01</code>. ERROR – Error messages (<code>0x03</code>) WARNING – Warning messages (<code>0x04</code>) NOTICE – Normal but significant condition (<code>0x05</code>). Default value. INFO – Informational messages (<code>0x06</code>) DEBUG – Debug level messages (<code>0x07</code>) <hr/> <p> If <code>LogLevel</code> is set to <code>DEBUG</code>, a large amount of data is written to the <code>csxlan.log</code> file. Depending on requests and traffic, this may result in a logfile size of 2 GB within 15 minutes quickly leading to a full file system. Therefore, the following items are highly recommended:</p> <ul style="list-style-type: none"> Do not set <code>LogLevel</code> to <code>DEBUG</code>. If you want to set <code>LogLevel</code> to <code>Info</code> or <code>DEBUG</code>, do it only for a short period of time to avoid a blocked file system. Configure <code>fcron</code> to start <code>logrotate</code> every 5 minutes. For details, see Setting up fcron Jobs (p. 212) step 4. <hr/> <p>All values but the <code>OFF</code> value can be overwritten until the next (re)start of the CryptoServer LAN using the <code>csadm CSLSetTracelevel</code> command. For details about the <code>csadm CSLSetTracelevel</code> command, see CryptoServer – csadm Manual (p. 240). If the log file <code>/var/log/csxlan.log</code> has been deleted, restart the syslog daemon (<code>/etc/init.d/syslogd restart</code>) to re-create this log file.</p>

Parameter	Description
LogFacility	<p>The log facility supports the following values. See Configuring the csxlan.conf File (p. 195) for how to use it.</p> <ul style="list-style-type: none"> local0 – Reserved for local use. local1 – Reserved for local use. local2 – Reserved for local use. local3 – Reserved for local use. local4 – Reserved for local use. local5 – Reserved for local use. local6 – Reserved for local use. local7 – Reserved for local use. Default value.
Watchdog	<p>The watchdog is a hardware timer that is used to monitor the CryptoServer LAN and to detect malfunctions. This timer continuously decreases from its initial value until it reaches 0 after 5 minutes. If the csxlan daemon works properly, it resets the timer to its initial value every 10 seconds. If the csxlan daemon malfunctions and does not reset the timer, the timer reaches 0 and the CryptoServer LAN then automatically restarts to solve the malfunction. The following values of the <code>Watchdog</code> variable are supported.</p> <ul style="list-style-type: none"> 0 – The watchdog is disabled. 1 – The watchdog is enabled. <p>If no value has been set, the watchdog is disabled. At delivery, <code>Watchdog</code> has been set to 1. No BIOS settings are watchdog-related.</p>
IPv6_disable	<p>This global setting overrides other IPv6 settings in the configuration file.</p> <ul style="list-style-type: none"> 0 – Use IPv6 sockets. 1 – Do not use IPv6 sockets.
IPv4_disable	<p>This global setting overrides other IPv4 settings in the configuration file.</p> <ul style="list-style-type: none"> 0 – Use IPv4 sockets. 1 – Do not use IPv4 sockets.
MaxConnections	<p>Number of connections that can be performed simultaneously by the csxlan daemon. Default setting is 4100 connections.</p>

Parameter	Description
AuthReset	<p>Shows whether the <code>csadm Reset</code>, <code>csadm ResetToBL</code> and <code>csadm Restart</code> commands must be authenticated by the Cryptoserver LAN root user. For details, see CryptoServer – csadm Manual (p. 240) for details. No authentication is necessary if the commands were input using the menu options on the CryptoServer LAN.</p> <p>Example:</p> <ul style="list-style-type: none"> ▪ <code>AuthReset = 0</code> <p>No authentication</p> <ul style="list-style-type: none"> ▪ <code>AuthReset = 1</code> <p>Authentication required</p>
DenyLock	<p>Disables the LOCK command used for maintenance tasks on the CryptoServer. If the <code>DenyLock</code> variable is not present, the LOCK command is permitted.</p> <p>Example:</p> <ul style="list-style-type: none"> ▪ <code>DenyLock = 0</code> <p>The LOCK command is permitted.</p> <ul style="list-style-type: none"> ▪ <code>DenyLock = 1</code> <p>The LOCK command is not permitted.</p>

Table 16: Variables in the [Csxlan] section of csxlan.conf

Variables for the [CryptoServer] section

<i>Parameter</i>	<i>Description</i>
Label	Unique ID for the CryptoServer PCIe card in the CryptoServer LAN.
Device	File name of the devices file assigned to the CryptoServer PCIe card in the CryptoServer LAN (for example <code>/dev/cs2.n</code> where $n=\{0, 1, 2, 3, \dots\}$).
Timeout	Time in milliseconds to define when the CryptoServer device driver rejects a command because the CryptoServer does not respond. The default value is 60000 milliseconds.
AdminName	<p>This variable specifies the user with user management permissions (at least 20000000) that is used to authenticate some commands that are initiated by the menu items on the front panel of the CryptoServer LAN. Default value: <code>ADMIN</code> Example: <code>AdminName = ADMIN</code></p> <hr/> <p> Do not store user names using the HMAC password authentication because this authentication mechanism is not supported by commands initiated by the menu items on the front panel. For details about the authentication mechanisms, see <i>Authentication Mechanisms</i> in the CryptoServer Administration Manual (p. 240).</p> <hr/> <p>The AdminName variable is for example described at the following locations:</p> <ul style="list-style-type: none"> ▪ Setting up NTP Mainly Using the Front Panel (p. 98), see step 2 for specifying the user and see step 8g) for performing the command. ▪ Loading a File onto the CryptoServer (p. 156) ▪ Deleting a File in the CryptoServer (p. 158) ▪ Changing the Administrator's Authentication Key (p. 160) ▪ Loading the Firmware Encryption Key into the CryptoServer (p. 163)


<i>Parameter</i>	<i>Description</i>
NTPManagerName	<p>This variable specifies the user with NTP management permissions (at least 00200000) that is used to authenticate some commands that are initiated by the menu items on the front panel of the CryptoServer LAN. Default value: <code>ntp</code> Example: <code>NTPManagerName = ntp</code></p> <hr/> <p> Do not store user names using the HMAC password authentication because this authentication mechanism is not supported by commands initiated by the menu items on the front panel. For details about the authentication mechanisms, see <i>Authentication Mechanisms</i> in the CryptoServer Administration Manual (p. 240).</p> <hr/> <p>The NTPManagerName variable is for example described at the following locations:</p> <ul style="list-style-type: none"> ▪ Setting up NTP Mainly Using the Front Panel (p. 98), see step 2 for specifying the user. ▪ Disabling NTP (p. 116), see step 6f) for performing the command.


Table 17: Variables in the [CryptoServer] section of csxlan.conf

Variables for the [Listener] section

Parameter	Description
IP_version	<p>Protocol of the listener socket.</p> <ul style="list-style-type: none"> ▪ IPv4 – Use IPv4. ▪ IPv6 – Use IPv6. <p>If omitted, IPv4 and IPv6 are used. If the <code>IPv6_disable</code> variable or the <code>IPv4_disable</code> variable in the <code>[Csxlan]</code> section has been set to 1, the <code>IP_version</code> variable in any <code>[Listener]</code> section becomes overridden</p>
Address	<p>The local interface address to which the socket was assigned. If this is missing, the server socket is assigned for all local interfaces.</p> <p>Examples: <code>localhost</code></p> <p>Make sure that this <code>Address</code> information is used in the <code>Device</code> variable in the <code>[DisplayAdmin]</code> section.</p>
Port	<p>Number of the port used to handle csxlan daemon connections. Unless otherwise specified, port 288 is used here.</p> <p>Make sure that this port is identical to the port used in the <code>Device</code> variable in the <code>[DisplayAdmin]</code> section.</p>
Protocol	<p>This is where you specify whether the TCP or UDP protocol is to be used. Unless otherwise specified, the TCP protocol is used.</p> <p>Make sure that this protocol is identical to the protocol used in the <code>Device</code> variable in the <code>[DisplayAdmin]</code> section.</p>
Multicast	<p>This is where you specify whether multicast (multiple connections) is to be used.</p> <p><code>Multicast = 0</code> means that multicast is disabled. <code>Multicast = 1</code> means that multicast is enabled. <code>Multicast</code> can only be used together with the UDP protocol.</p>
Keepalive	<p>Enables or disables TCP keepalive data packets that search for interrupted connections.</p> <p><code>Keepalive = 0</code> means that TCP keepalive data packets are disabled <code>Keepalive = 1</code> means TCP keepalive data packets are enabled.</p>
Linger	<p>For TCP connections, this is where you input the time in seconds during which a connection to the socket is to be kept open before the socket is closed by mutual agreement. If you input a value greater than 0, the socket is closed by mutual agreement and an additional TCP packet is exchanged.</p>
Priority	<p>Allocates a priority to every query to the ports.</p> <p>Possible values are 1 (highest) and 100 (lowest) priority.</p>
Route_to	<p>This mandatory option assigns the <code>[Listener]</code> to a specific CryptoServer. The data you input here is the same as you input in the <code>[CryptoServer]</code> area as the <code>Label</code>.</p>

Table 18: Variables in the [Listener] section of csxlan.conf

Variables for the [DisplayAdmin] section

Parameter	Description
LogLevel	<p>The log level supports the following values. See Configuring the csxlan.conf File (p. 195) for how to use it.</p> <ul style="list-style-type: none"> OFF – Stop producing messages, useful for benchmarks ERROR – Error conditions WARNING – Warning conditions NOTICE – Normal but significant condition. Default value. INFO – Informational DEBUG – Debug level messages <hr/> <p> If <code>LogLevel</code> is set to <code>DEBUG</code>, a large amount of data is written to the <code>csxlan.log</code> file. Depending on requests and traffic, this may result in a logfile size of 2 GB within 15 minutes quickly leading to a full file system. Therefore, the following items are highly recommended:</p> <ul style="list-style-type: none"> Do not set <code>LogLevel</code> to <code>DEBUG</code>. If you want to set <code>LogLevel</code> to <code>Info</code> or <code>DEBUG</code>, do it only for a short period of time to avoid a blocked file system. Configure <code>fcron</code> to start <code>logrotate</code> every 5 minutes. For details, see Setting up fcron Jobs (p. 212), step 4. <hr/>
LogFacility	<p>The log facility supports the following values. See Configuring the csxlan.conf File (p. 195) for how to use it.</p> <ul style="list-style-type: none"> local0 – Reserved for local use. local1 – Reserved for local use. local2 – Reserved for local use. local3 – Reserved for local use. local4 – Reserved for local use. local5 – Reserved for local use. local6 – Reserved for local use. local7 – Reserved for local use. Default value.


Parameter	Description
Device	<p>Device name that is used for the communication between the display on the front panel of the CryptoServer LAN and the CryptoServer PCIe card.</p> <p>This device name consists of the protocol, the port and the address with the protocol and the port being optional. If no protocol is specified, TCP is used, and if no port is specified, port 288 is used. Make sure that the <code>Port</code> variable and the <code>Protocol</code> variable in the <code>[Listener]</code> section are identical to the port and the protocol used here, and make sure that the information in the <code>Address</code> variable in the <code>[Listener]</code> section is used here.</p> <p>The pattern is <code>protocol:port@address</code>.</p> <p>Examples:</p> <ul style="list-style-type: none"> ▪ <code>TCP:288@localhost</code> ▪ <code>UDP:288@localhost</code> ▪ <code>TCP:localhost</code> ▪ <code>288@localhost</code> ▪ <code>localhost</code> <p><code>UDP:localhost</code> is the default entry.</p>
Display	<p><code>Display</code> defines the display port of the CryptoServer LAN</p> <p>Example:</p> <p><code>Display = /dev/ttyS0</code></p>
PINPad	<p><code>PINPad</code> specifies which PIN pad is connected. <code>PINPad</code> is deprecated. The name has this format:</p> <p><code>:<smartcard ID>:<PIN pad ID>:USB0</code></p> <p>Example:</p> <p><code>:cs2:auto:USB0</code></p> <p>For details, see <i>Storage and Specification of RSA and ECDSA Keys for Authentication</i> in the CryptoServer – csadm Manual (p. 240).</p>
OSUpdateDevice	<p><code>OSUpdateDevice</code> defines the device for firmware updates.</p> <p>Example:</p> <p><code>OSUpdateDevice = /dev/sdb1</code></p>
IdleWindowTitle	<p><code>IdleWindowTitle</code> defines the title line of all idle screens.</p> <p>Example:</p> <p><code>IdleWindowTitle = "CryptoServer LAN"</code></p> <p>When shown on the display and if there is enough space in this line, this text is embraced by spaces and hyphens.</p>
MenuWindowTitle	<p><code>MenuWindowTitle</code> defines the title line of all menu screens.</p> <p>Example:</p> <p><code>MenuWindowTitle = "CSLAN menu"</code></p> <p>When shown on the display and if there is enough space in this line, this text is embraced by spaces and hyphens.</p>

Parameter	Description
CustomerValueFileType	<p>Idle screens can contain up to three lines of text. It is possible to replace the existing lines by customer-specific lines of arbitrary text or to add new additional idle screens containing these customer-specific lines. If you want to add three new lines of text, the <code>CustomerValueFileType</code> variable indicates whether the text to be shown is defined in one file containing the three new lines of text (<code>PANEL</code>) or in three files each of them containing one line of text (<code>LINES</code>).</p> <p>Example:</p> <pre>CustomerValueFileType = PANEL</pre> <p>For details, see Adding a Customer-Specific Screen to the Idle Screens (p. 208).</p> <p>The number of new lines of text is defined by the <code>CustomerValueCount</code> variable (default value: <code>3</code>).</p>
CustomerValueFileName	<p>Depending on the <code>CustomerValueFileType</code> variable, the <code>CustomerValueFileName</code> variable indicates the name of one or several files containing the text to be shown in the additional customer-specific lines of text on the idle screens.</p> <p>Examples:</p> <ul style="list-style-type: none"> <pre>CustomerValueFileName = "/tmp/dspd_customer.val"</pre> <p>The file contains three (default value of the <code>CustomerValueCount</code> variable) lines of text to be shown on the display.</p> <pre>CustomerValueFileName = "/tmp/DspCompanyCustomLine*"</pre> <p>The three (default value of the <code>CustomerValueCount</code> variable) files <code>/tmp/DspCompanyCustomLine0</code>, <code>/tmp/DspCompanyCustomLine1</code> and <code>/tmp/DspCompanyCustomLine2</code> contain one line of text to be shown on the display.</p> <p>Consider that files in the <code>/tmp</code> directory are removed after a reboot of the CryptoServer LAN.</p> <p>For details, see Adding a Customer-Specific Screen to the Idle Screens (p. 208).</p>
CustomerValueCount	<p>The <code>CustomerValueCount</code> variable defines the number of customer-specific lines of text that are used in the idle screens, its default value is <code>3</code> , and its maximum value is <code>6</code> .</p> <p>The number of idle screens is determined by the entries in the <code>/etc/dspd_idle_window.conf</code> file. The entries specifying the customer-specific lines can be anywhere in this file.</p> <p>For details, see Adding a Customer-Specific Screen to the Idle Screens (p. 208).</p>

Parameter	Description
CustomerValueErrorText	<p>If there are problems when retrieving a customer-specific line of text, an error message is shown instead of the intended line of text. The text of the error message is defined by the <code>CustomerValueErrorText</code> variable.</p> <p>If this variable has the value <code>"#ERROR#"</code>, an error message produced by the CryptoServer is shown instead of a line of text on the display. If this variable has the value <code>" "</code>, an empty line is shown on the display.</p> <p>Reasons to cause this error are, for example, as follows:</p> <ul style="list-style-type: none"> ▪ <code>CustomerValueFileName</code> specifies a non-existing file. ▪ The <code>CustomerValueFileName</code> variable or the <code>CustomerValueFileType</code> variable is written incorrectly.
RenameCustomerValueFile	<p>When the file(s) specified by the <code>CustomerValueFileType</code> variable is accessed, it is renamed for a very short period of time. This might cause problems if other processes try to access this file(s) as well. If problems occur, renaming the file(s) can be avoided by setting the <code>RenameCustomerValueFile</code> variable to 0.</p> <ul style="list-style-type: none"> ▪ <code>0</code> – Renaming is disabled. ▪ <code>1</code> – Renaming is enabled (default value).
HSMValueUpdateInterval	<p>Time in milliseconds between two connections to the csxlan daemon. This is also the interval between two updates of the values of, for example, the idle screens. The default value is 30000.</p>

Table 19: : Variables in the [DisplayAdmin] section of csxlan.conf

Variables for the [NTPClient] section

Parameter	Description
LogLevel	<p>The log level supports the following values. See Configuring the csxlan.conf File (p. 195) for how to use it.</p> <ul style="list-style-type: none"> OFF – Stop producing messages, useful for benchmarks ERROR – Error conditions WARNING – Warning conditions NOTICE – Normal but significant condition. Default value. INFO – Informational DEBUG – Debug level messages <hr/> <p> If <code>LogLevel</code> is set to <code>DEBUG</code>, a large amount of data is written to the <code>csxlan.log</code> file. Depending on requests and traffic, this may result in a logfile size of 2 GB within 15 minutes quickly leading to a full file system. Therefore, the following items are highly recommended:</p> <ul style="list-style-type: none"> Do not set <code>LogLevel</code> to <code>DEBUG</code>. If you want to set <code>LogLevel</code> to <code>Info</code> or <code>DEBUG</code>, do it only for a short period of time to avoid a blocked file system. Configure <code>fcron</code> to start <code>logrotate</code> every 5 minutes. For details, see Setting up fcron Jobs (p. 212), step 4. <hr/>
LogFacility	<p>The log facility supports the following values. See Configuring the csxlan.conf File (p. 195) for how to use it.</p> <ul style="list-style-type: none"> local0 – Reserved for local use. local1 – Reserved for local use. local2 – Reserved for local use. local3 – Reserved for local use. local4 – Reserved for local use. local5 – Reserved for local use. local6 – Reserved for local use. local7 – Reserved for local use. Default value.

Parameter	Description
LoopTime	<p>If the NTP client is enabled, it verifies every <code>LoopTime</code> seconds whether the time difference between the time on the CryptoServer LAN and the time on the CryptoServer is greater than <code>Deviation</code> milliseconds. If this is the case, it transfers the time on the CryptoServer LAN to the CryptoServer.</p> <p><code>LoopTime</code> : Verification time interval in seconds Default value: <code>LoopTime = 3600</code> (i.e., once per hour) We recommend not to change the default value. Do not set a value higher than 86400 (i.e., one day). For details about how to set this variable, see Configuring Time Synchronization between the CryptoServer LAN and the CryptoServer (p. 124).</p>
Deviation	<p>Time deviation in milliseconds between the CryptoServer LAN and the CryptoServer for which the time on the CryptoServer is to be corrected Default value: <code>Deviation = 500</code> Recommended value range: <code>1 - 2500</code>.</p> <p>A value below 1 is automatically set to 1, and a value higher than 2500 is automatically set to 2500. A value higher than <code>Max. time to set per operation</code> (see below) does not initiate a time correction but produces an error. For details about how to set this variable, see Configuring Time Synchronization between the CryptoServer LAN and the CryptoServer (p. 124).</p>

Table 20: Variables in the [NTPClient] section of `csxlan.conf`

You can insert commented lines at any point in the `csxlan.conf` file. Commented lines start with the character `#` and run to the end of the line.

6.3 Restricting the Network Access on the CryptoServer LAN

If you want to restrict the network access to the CryptoServer LAN and only want to permit specific network services (SSH etc.) to connect to the CryptoServer LAN, you shall use `iptables`.

6.3.1 `iptables` for IPv4

By default, `iptables` is started at boot time, and the following rules are applied:

- The default policy is to drop everything.
- Allow localhost to localhost connections.
- Drop invalid packets.

- Allow DHCP via UDP.
- Allow echo request and echo reply as source and destination.
- Allow DNS via UDP.
- Allow NTP via UDP.
- Allow SNMP via UDP.
- Allow SNMP traps via UDP.
- Allow SSH with the LAN device as the source and the destination.
- Allow the access to the device via TCP and the default port.
- Rejected packets cause an ICMP host unreachable messages.

Iptables can be operated by the `/etc/init.d/iptables` script, which supports IPv4 and IPv6. IPv6 is only handled, if the file `/etc/ip6tables` exists and is executable. The iptables script supports the following commands:

- `start` : Execute the `/etc/iptables.conf` script.
- `restart` : Execute the `/etc/iptables.conf` script
- `lock` : Block all outside traffic.
- `clear` : Accept all traffic.
- `stop` : Accept all traffic.
- `status` : Shows active rules.

Example for the output of the `/etc/init.d/iptables status` command:

Example Output

```
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  127.0.0.1              127.0.0.1
DROP       tcp  --  0.0.0.0/0             0.0.0.0/0             ctstate INVALID
ACCEPT     udp  --  0.0.0.0/0             0.0.0.0/0             udp spts:67:68
dpts:67:68
REJECT     tcp  --  0.0.0.0/0             0.0.0.0/0             tcp dpt:113
reject-with tcp-reset
ACCEPT     icmp --  0.0.0.0/0             0.0.0.0/0             icmp type 8
ACCEPT     icmp --  0.0.0.0/0             0.0.0.0/0             icmp type 0
```

```

ACCEPT      udp  --  0.0.0.0/0          0.0.0.0/0          udp spt:53
ACCEPT      udp  --  0.0.0.0/0          0.0.0.0/0          udp spt:123
ACCEPT      udp  --  0.0.0.0/0          0.0.0.0/0          udp dpt:161
ACCEPT      tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:22
ACCEPT      tcp  --  0.0.0.0/0          0.0.0.0/0          tcp spt:22
ACCEPT      tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:288
REJECT      all  --  0.0.0.0/0          0.0.0.0/0          reject-with
icmp-host-unreachable

Chain FORWARD (policy DROP)
target     prot opt source                destination

Chain OUTPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  127.0.0.1             127.0.0.1
ACCEPT     udp  --  0.0.0.0/0             0.0.0.0/0          udp spts:67:68
dpts:67:68
ACCEPT     icmp --  0.0.0.0/0             0.0.0.0/0          icmptype 8
ACCEPT     icmp --  0.0.0.0/0             0.0.0.0/0          icmptype 0
ACCEPT     udp  --  0.0.0.0/0             0.0.0.0/0          udp dpt:53
ACCEPT     udp  --  0.0.0.0/0             0.0.0.0/0          udp dpt:514
ACCEPT     udp  --  0.0.0.0/0             0.0.0.0/0          udp dpt:123
ACCEPT     udp  --  0.0.0.0/0             0.0.0.0/0          udp spt:161
ACCEPT     udp  --  0.0.0.0/0             0.0.0.0/0          udp dpt:162
ACCEPT     tcp  --  0.0.0.0/0             0.0.0.0/0          tcp spt:22
ACCEPT     tcp  --  0.0.0.0/0             0.0.0.0/0          tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0             0.0.0.0/0          tcp spt:288
ACCEPT     icmp --  0.0.0.0/0             0.0.0.0/0          icmptype 3

```

If you want to change the default behavior remotely via an SSH connection from your administration computer, follow the steps described below.

1. Log in remotely to the LAN device.
2. To verify whether iptables is automatically started, execute following command.

```
get_iptables_config.sh
```

The output is either `yes` or `no`.
3. If you want to enable the automatic start, execute the following command.

```
set_iptables_config.sh yes
```

As an alternative, open the `/etc/sysconfig/iptables` file with a text editor, change the `START_IPTABLES=no` line to `START_IPTABLES=yes`, and save the file.
As another alternative, perform the following substeps using the menu control buttons.
 - a. Press **ENTER** on the front panel of the device.
 - b. Press **ENTER** to select **CSLAN admin..**

- c. Press **ENTER** again to select **Configuration**.
- d. Press the ↓ key to select **Services** and confirm this by pressing **ENTER**.
- e. Press **ENTER** to select **IPTABLES**.
The currently applied setting (disabled or enabled) is indicated by a full circle.
- f. Use the ↓ key to select **enabled** and press **ENTER** to open the menu item.
- g. Use the ← or the → key to move the x into the brackets **[x] Yes** and press **ENTER**.



A message confirming that you have successfully enabled iptables is displayed.

1. Execute the following command.

```
/etc/init.d/iptables restart
```

2. If you want to change the iptables rules permanently, for example, to enable or disable access to a certain service via the network, open the `/etc/iptables.conf` file with a text editor. This can only be done by the root user.

If you do not want to change the iptables rules permanently, the iptables configuration is finished. There is no need to perform the following steps in this chapter.



Only if you have profound knowledge of iptables, perform this step. Otherwise, you might block any remote access to the LAN device.

In this case, the only solution is to disable iptables using the menu control buttons on the front panel of the LAN device and selecting **CSLAN admin. > Configuration > Services > IPTABLES > disabled > YES**.

Edit this file according to your needs.

3. Execute the following command to apply the changes.

```
/etc/init.d/iptables restart
```

4. Execute the following command to verify the changed settings.

```
/etc/init.d/iptables status
```

6.3.2 iptables for IPv6

Chapter [iptables for IPv4 \(p. 190\)](#) applies as well to IPv6 addresses with the following differences:

- IPv6 in iptables is disabled by default.
- If you want to apply iptables to IPv6 addresses, enable IPv6, see [Setting up the IPv6 Configuration With a Command-Line \(p. 37\)](#)", copy the `/etc/ip6tables.conf.example` file to the `/etc/ip6tables.conf` file and make it executable (`chmod +x /etc/ip6tables.conf`). This file contains the ip6tables configuration. It loads the ip6tables rules when it is executed. To change ip6tables rules permanently, this file must be changed.



Only if you have profound knowledge of ip6tables, edit the `/etc/ip6tables.conf` file. Otherwise, you might block any remote access to the CryptoServer LAN. In this case, the only solution is to disable iptables using the menu control buttons on the front panel of the CryptoServer LAN and selecting **CSLAN admin. > Configuration > Services > IPTABLES > disabled > YES**.

- By default, the `/etc/ip6tables.conf` file contains almost the same rules for IPv6 as the `/etc/iptables.conf` file does for IPv4. Only one rule is different: Rejected packets cause an ICMPv6 address unreachable message but no ICMP address unreachable message as for IPv4. If an `/etc/ip6tables.conf` file is present, iptables automatically uses this file for handling IPv6 addresses.
- That means that the configuration file name for IPv6 (`/etc/ip6tables.conf`) differs from the configuration file name for IPv4 (`/etc/iptables.conf`). But the script file names for IPv4 and IPv6 are the same:
 - `/etc/init.d/iptables`
 - `get_iptables_config.sh`
 - `set_iptables_config.sh`
 - `/etc/sysconfig/iptables`

6.4 Setting up Remote Logging

The LAN device supports remote logging. This means it passes syslog messages on to a remote syslog which records the syslog messages in log files.

Syslog is a standard system for collecting log messages, which can also be used to transfer log messages within an IP computer network and therefore also to remotely monitor computer systems. If all syslog messages are sent to a central syslog server, you can then use syslog to monitor and check several computers from one location.

If you are already using remote logging via syslog in your computer network, you can easily integrate the LAN device into this system.

You must edit the `syslogd` so it can transfer the log messages to a remote syslog. Finally, you must edit the remote syslog to ensure it can receive and handle log messages correctly. The chain along which log messages are passed looks like this:

```
csxlan → syslog → remote syslog
```

6.4.1 Configuring the csxlan.conf File

The csxlan daemon uses syslogd as the logging daemon. To write messages via syslog to a remote computer, you have to edit the `/etc/csxlan.conf` file. Make sure that there are the `LogLevel` and `LogFacility` variables in the `[Csxlan]` section. These variables can be present not only in the `[Csxlan]` section but also in the `[DisplayAdmin]` and the `[NTPClient]` section. The `[Listener]` section and the `[CryptoServer]` section use the `LogLevel` and `LogFacility` variables values of the `[Csxlan]` section.

Example:

```
[Csxlan]
LogLevel = NOTICE
LogFacility = local7
```

This is how you edit the `csxlan.conf` file with with PuTTY for Windows:

1. Log in remotely to the LAN device.
2. Open the `csxlan.conf` configuration file in the `/etc` directory with a text editor.
3. Insert the needed variables in the `[Csxlan]`, `[DisplayAdmin]` and/or `[NTPClient]` section.


Example

```
[Csxlan]
LogLevel = NOTICE
```

```
LogFacility = local7
...
[DisplayAdmin]
LogLevel    = NOTICE
LogFacility = local7
...
[NTPClient]
LogLevel    = NOTICE
LogFacility = local7
...
```

The chosen values are important for the configuration of the syslog daemon because there have to be the corresponding values in the `/etc/syslog.conf` file.

4. Save these changes and then close the `conf` file.
5. If the `conf` file has been changed, you must restart the csxlan daemon.
`/etc/init.d/cs2 restart`
6. Close your SSH client.

 All messages of csxlan are redirected to the local syslog daemon.

6.4.2 Configuring the syslog.conf File

To ensure the log messages collected by the syslog daemon of the LAN device are also transferred to a remote syslog daemon, you must edit the `/etc/syslog.conf` file. This is how you edit the `syslog.conf` file with PuTTY for Windows.

1. Log in remotely to the CryptoServer LAN..
2. Open the `syslog.conf` configuration file in the `/etc` directory with a text editor.
3. If you want to transfer only specific local syslog messages to the remote syslog daemon, add the following line to the `syslog.conf` file:

```
local<x>.* @<host name>
```

In this example, we have used `<x>` as a placeholder after local. Replace this placeholder `<x>` by the number of the syslog channel you specified as the `LogFacility` variable in the `[CSLAN]` section of the `/etc/csxlan.conf` file in step 3. If you have set `LogFacility` to `local7` (default value), you must also enter `local7.*` in the `/etc/`

syslog.conf file. As the `<host name>`, input the host name or IP address of the remote syslog daemon to which the log messages are to be sent. A syslog daemon must listen on this host to receive the sent messages.

Example: `local7.* @192.168.123.234`

4. If you want to transfer all syslog messages to the remote syslog daemon, add the following line to the `syslog.conf` file:

```
*.* @<host name>
```

As the `<host name>`, input the host name or IP address of the remote syslog daemon to which the log messages are to be sent.

5. You may add an entry to the `/etc/syslog.conf` file to log messages to a file, for example, `-/var/log/csxlan.log`.

Example:

```
local7.* -/var/log/csxlan.conf
```

6. Save the changes and close the `syslog.conf` file.
7. If you have changed the `syslog.conf` file, you must restart the syslog daemon.
`/etc/init.d/syslogd restart`
8. Close your SSH client.

You will find all the other information you need about how to configure `syslogd` in the Linux/UNIX manual, page SYSLOG(8).

6.4.3 Configuring the Remote Syslog Daemon

Configuring the remote syslog daemon is beyond the scope of this manual.

On the remote logging server, you have to start `syslogd` with the `-r` option to enable the remote logging. In some cases, you may have to change the firewall ports. Per default, port number 514 is used by `syslogd`, and UDP is the default protocol.

6.4.4 Configuring logrotate

The jobs that are controlled by logrotate are used to avoid that the size of the local log file, for example, `/var/log/csxlan.log`, exceeds a certain threshold, set how many archive versions of the log files are created and if they should be compressed or not. Make sure that not only on the local computer but also on the remote computer, logrotate is configured according to your needs.

6.5 Adjusting the Menu Structure for the Menu Options

The `/etc/dspd_menu.conf` configuration file contains the menu structure that appears in the LAN device display along with the texts displayed there. You can configure this file to adjust both the menu structure and its texts to your specific requirements.



Before you make any changes to the configuration file `dspd_menu.conf`, and therefore also change the menu structure, we strongly recommend you save a copy of the configuration file on your host computer so you can access the original file if you need to.

The individual levels in the menu structure are illustrated here using an extract from the `dspd_menu.conf` file as an example.

For CSLANOS V5.0.x:

```
# CSLAN Menu Config #,1.0
# Ein Kommentar
#CSLAN Administration
Show commands,EXECUTE,Func,DSPD.TEST
CSLAN admin.
.Configuration
..Network IP4
...Default Gateway,EDIT,NETWORK.IP4_DEFAULT_GATEWAY
...eth0
....DHCP,EDIT,NETWORK.ETH0.IP4_DHCP
....Address,EDIT,NETWORK.ETH0.IP4_ADDR
...eth1
....DHCP,EDIT,NETWORK.ETH1.IP4_DHCP
....Address,EDIT,NETWORK.ETH1.IP4_ADDR
```

For CSLANOS V5.1.x and later:

```
# CSLAN Menu Config #,1.0
# Ein Kommentar
#CSLAN Administration
Show commands,EXECUTE,Func,DSPD.TEST
CSLAN admin.
.Configuration
..Network IP4
...Default Gateway,EDIT,NETWORK.IP4_CONFIG_DEFAULT_GATEWAY
...eth0
....DHCP,EDIT,NETWORK.ETH0.IP4_CONFIG_DHCP
....Address,EDIT,NETWORK.ETH0.IP4_CONFIG_ADDR
...eth1
....DHCP,EDIT,NETWORK.ETH1.IP4_CONFIG_DHCP
....Address,EDIT,NETWORK.ETH1.IP4_CONFIG_ADDR
```

`CSLAN admin.` is the top level of the menu structure here and is shown without leading points, justified to the left.

`Configuration` , with one preceding point, is a submenu item of `CSLAN admin.` .

`Network IP4` with two preceding points, is a submenu item of `Configuration` .

`Default Gateway` , with three preceding points, is a submenu item of `Network IP4` .



The individual levels in the menu structure are structured according to the number of points that appear before the text.

You also have the option of translating the texts of individual menu items into different languages and therefore tailoring the entire menu structure to your own specific requirements.



After you have modified the menu structure, you can either restart the LAN device or the `dspd` .

You also have the option of disabling a line in the `/etc/dspd_menu.conf` configuration file. The corresponding menu option is still shown on the display but it provides no action anymore. This is indicated on the display by a small no way sign to the right of the menu item. Disabling a menu option can only be done for leaves of the menu tree but not for nodes. It is done by inserting `,DISABLED` (Do not forget the comma.) in the configuration file behind the

text that should be shown on the display and removing the rest of this line. A line in the configuration file represents a leaf if the next line does not have more leading points.

Example:

If you want to avoid configuring the eth1 address by using the menu items, replace the following text for CSLANOS V5.0.x

Example

```
...eth1
....DHCP,EDIT,NETWORK.ETH1.IP4_DHCP
....Address,EDIT,NETWORK.ETH1.IP4_ADDR
```

or the following text for CSLANOS V5.1.x and later

Example

```
...eth1
....DHCP,EDIT,NETWORK.ETH1.IP4_CONFIG_DHCP
....Address,EDIT,NETWORK.ETH1.IP4_CONFIG_ADDR
```

by the following text

```
...eth1
....DHCP,DISABLED
....Address,DISABLED
```

If you not only want to disable a menu item but to remove it, remove the corresponding line in the configuration file. Consider to remove all submenu items as well.

To apply the changes, restart the csxlan daemon by performing the following steps:

1. Log in remotely to the LAN device.
2. To restart the csxlan daemon, enter the `/etc/init.d/cs2 restart` command and confirm by pressing **Enter**.
3. Close your SSH client.



All the submenu items for `PIN Pad applications,EXECUTE,FUNC,HSM.PINPAD_APPS` are made available directly by the PCIe card and are therefore not described in this configuration file.

6.6 Adding a Standard Screen to the Idle Screens

The idle screens shown in the next figure can be extended by an additional screen containing the headline and three additional lines of text.

```

- CryptoServer LAN -
HSM Model:
  SecurityServer
  Se1500 CS132456

- CryptoServer LAN -
HSM Status (1/2)
Mode:      Operational
Admin Mode:      no

- CryptoServer LAN -
HSM Status (2/2)
Temperature: 30.0 °C
Load:        0.0 %

- CryptoServer LAN -
HSM Battery
Voltage:      3.045 V
              OK 🔋

- CryptoServer LAN -
CSLAN Status
Connections:      2
Trans./min.:      7 TPM

- CryptoServer LAN -
CSLAN Battery
Voltage:      3.066 V
              OK 🔋

- CryptoServer LAN -
Time (local/UTC)
  2018-09-20 13:00:33
  2018-09-20 12:00:33

- CryptoServer LAN -
Fan speed
F:  6100  6100  6200
B:  5300  5200  5200

```

Figure 37 : Idle Screens

An idle screen is defined by three non-empty lines in the `/etc/dspd_idle_window.conf` file. Append three lines for an additional screen. A comma precedes a command. The text before a comma is interpreted as hard-coded text.

Example:

HSM Battery

Voltage: ,HSM.INT_BAT_VOLTAGE
,HSM.INT_BAT_STATE

HSM Battery and Voltage: is hard-coded text, and the rest is for example a command for retrieving the value of a variable. HSM.INT_BAT_VOLTAGE retrieves for example the text 3.049 V and ,HSM.INT_BAT_STATE retrieves for example the text OK and a battery symbol. The following table shows some examples of variables that can be used in the /etc/dspd_idle_window.conf file. You find a complete collection of variables in the /etc/dspd_value_panels.conf file.

Variable	Description
CSLAN.DATE_TIME_UTC	Date and time of the UTC time on the CryptoServer LAN (not on the CryptoServer PCIe card)
CSLAN.DATE_UTC	Date of the UTC time on the CryptoServer LAN (not on the CryptoServer PCIe card)
CSLAN.TIME_UTC	UTC time on the CryptoServer LAN (not on the CryptoServer PCIe card)
CSLAN.TIMEZONE_OFS	Timezone offset of the local time on the CryptoServer LAN (not on the CryptoServer PCIe card) to UTC
CSLAN.DATE_TIME_LOCAL	Date and time of the UTC time on the CryptoServer LAN (not on the CryptoServer PCIe card)
CSLAN.DATE_LOCAL	Date of the local time on the CryptoServer LAN (not on the CryptoServer PCIe card)
CSLAN.TIME_LOCAL	Local time on the CryptoServer LAN (not on the CryptoServer PCIe card)
HSM.DATE_TIME_UTC	Date and time of the UTC time on the CryptoServer PCIe card
HSM.DATE_UTC	Date of the UTC time on the CryptoServer PCIe card
HSM.TIME_UTC	UTC time on the CryptoServer PCIe card
HSM.DATE_TIME_LOCAL	Date and time of the UTC time on the CryptoServer PCIe card
HSM.DATE_LOCAL	Date of the local time on the CryptoServer PCIe card
HSM.TIME_DIFF	Difference between the time on the CryptoServer LAN and the time on the CryptoServer PCIe card
HSM.LOAD_PER_CENT	CryptoServer load for the last 60 seconds in %
HSM.TRANS_PER_MINUTE	The number of transactions number per minute
HSM.NO_OF_CONNECTIONS	The number of IP client connections to the CryptoServer. If, for example, a csadm GetState command is performed, which takes a fraction of a second, Connections is increased by 1 for this period of time.
CSLAN.SSH_ENABLED	Indication whether the SSH daemon is enabled or disabled, see Enabling/Disabling the SSH Daemon (p. 45) .
CSLAN.SNMP_ENABLED	Indication whether the SNMP daemon is enabled or disabled, see Setting up SNMP (p. 49) .

Variable	Description
<code>CSLAN.IPTABLES_ENABLED</code>	Indication whether IPTABLES is enabled or disabled, see Restricting the Network Access on the CryptoServer LAN (p. 190) .
<code>CSLAN.NTP_ENABLED</code>	Indication whether the NTP daemon on the CryptoServer LAN is enabled or disabled, see Setting up NTP (p. 95) .
<code>CSLAN.NTP_SERVER_IP4</code>	IPv4 address of the NTP server
<code>HSM.NTP_MDL_STATE</code>	Indication whether the NTP firmware module on the CryptoServer PCIe card is active or not active
<code>CSLAN.BOOT_PARTITION</code>	Name of the partition to boot from, for example, <code>user2</code>
<code>CSLAN.RUN_PARTITION</code>	Name of the running partition
<code>NETWORK.IP4_STATE_DEFAULT_GATEWAY</code>	IP address of the IPv4 default gateway
<code>NETWORK.IP6_STATE_DEFAULT_GATEWAY_UPPER</code>	First half of the IPv6 default gateway. The IPv6 gateway value is split into two halves, <code>..._UPPER</code> and <code>..._LOWER</code> , because the unsplit value is too long for one line of the display.
<code>NETWORK.IP6_STATE_DEFAULT_GATEWAY_LOWER</code>	Second half of the IPv6 default gateway
<code>NETWORK.ETH0.IP4_STATE_ADDRESSES</code>	IPv4 address of the eth0 port. Exchange ETH0 in the variable name by ETH1, ETH2 or ETH3 to obtain the corresponding values of the eth1, eth2 or eth3 port. eth2 and eth3 are ports on an optional PCIe card.
<code>NETWORK.ETH0.IP4_STATE_NETMASK</code>	Network mask of the eth0 port
<code>NETWORK.ETH0.IP4_STATE_MAC</code>	MAC Address of the eth0 port
<code>NETWORK.ETH0.IP4_STATE_MTU</code>	Maximum transmission unit of the eth0 port in byte, for example, <code>1500</code>
<code>NETWORK.ETH0.IP4_STATE_LINK_UP</code>	Indicator whether the link of the eth0 port is up and running. Example value: yes. <code>..._LINK_UP</code> represents the hardware connection to the network. If, for example, the network cable has been disconnected from the network interface card, <code>..._LINK_UP</code> is no and <code>..._LINK_SPEED</code> is 0Mb/s. In contrast to <code>..._LINK_UP</code> , <code>..._IF_UP</code> (interface up) represents the addressability of the network port by the software.
<code>NETWORK.ETH0.IP4_STATE_LINK_SPEED</code>	Transmission rate via the eth0 port, for example, <code>1000Mb/s</code> . <code>1000Mb/s</code> corresponds to an orange control light in the upper left corner of the eth0 port. <code>10/100Mb/s</code> corresponds to a green control light.
<code>NETWORK.ETH0.IP4_STATE_DUPLEX_MODE</code>	Duplex mode of the eth0 port, for example, <code>full duplex</code>

Variable	Description
NETWORK.ETH0.IP4_STATE_IF_UP	Indicator whether the eth0 interface is up and running. Example value: <code>yes</code> . In contrast to <code>..._LINK_UP</code> , <code>..._IF_UP</code> represents the addressability of the network port by the software.
NETWORK.ETH0.IP6_STATE_ADDRESSES_0_UPPER	First half of the first IPv6 address. The IPv6 address is split into two halves, <code>..._UPPER</code> and <code>..._LOWER</code> , because the unsplit value is too long for one line of the display. One of the IPv6 addresses <code>..._ADDRESS_0_...</code> and <code>..._ADDRESS_1_...</code> is the link-local address.
NETWORK.ETH0.IP6_STATE_ADDRESSES_0_LOWER	Second half of the first IPv6 address
NETWORK.ETH0.IP6_STATE_PREFIX_0	Prefix length of the first IPv6 address
NETWORK.ETH0.IP6_STATE_ADDRESSES_1_UPPER	First half of the second IPv6 address. The IPv6 address is split into two halves, <code>..._UPPER</code> and <code>..._LOWER</code> , because the unsplit value is too long for one line of the display. One of the IPv6 addresses <code>..._ADDRESS_0_...</code> and <code>..._ADDRESS_1_...</code> is the link-local address.
NETWORK.ETH0.IP6_STATE_ADDRESSES_1_LOWER	Second half of the second IPv6 address
NETWORK.ETH0.IP6_STATE_PREFIX_1	Prefix length of the second IPv6 address
CSLAN.FAN1_SPEED	Fan speed in revolutions per minute, for example, <code>6100</code> . A CryptoServer LAN V5 has 6 fans in 3 fan modules and no CPU fan. Fan modules are exchangeable but fans are not. f10 in the following figure indicates the fan module containing fan 5 and fan 6. f11 indicates fan 3 and fan 4, and f12 indicates fan 1 and fan 2. A value of 0 for the fan speed indicates a broken fan. In this case, create an RMA (Return Merchandise Authorization) according to Contact Address for Support Queries (p. 239) .
CSLAN.FAN2_SPEED	
CSLAN.FAN3_SPEED	
CSLAN.FAN4_SPEED	
CSLAN.FAN5_SPEED	
CSLAN.FAN6_SPEED	
TIME_SOURCE.CARD_TYPE	Type of the optional PCIe clock card, for example, <code>PZF180PEX DCF77</code> . For details about PCIe clock cards, see Setting up PCIe Clock Cards (p. 91) .
TIME_SOURCE.CLOCK_STATE	State of the PCIe clock card, <code>Synchronized</code> or <code>no synch</code>
TIME_SOURCE.ANTENNA_SIGNAL	Strength of the signal coming from the antenna to the PCIe clock card in percent, for example, <code>77 %</code> or <code>Error</code> .

Table 21: Examples of idle screen configurations



Figure 38 : Front panel with removed fan compartment grill

Comment lines start with a `#`.

If the output of the hard-coded text and the text delivered by the command are too long for the one line of the display, the last characters of the hard-coded text are overwritten.

If you want to add an empty line, add the following line to the configuration file:

```
%EMPTYLINE%
```

Example of a line in the configuration file:

```
Local: ,CSLAN.DATE_TIME_LOCAL
```

Example output:

```
L2019-03-01 11:09:30
```

Example of an extended `/etc/dspd_idle_window.conf` file:

Example Output

```
# CSLAN Idle Window Config #,1.0
HSM Model
, HSM.ADM2
, HSM.ADM1

HSM Status (1/2)
Mode: ,HSM.BOOT_MODE
Admin. Mode: ,HSM.ADMIN_MODE

HSM Status (2/2)
Temperature: ,HSM.TEMPERATURE
Load: ,HSM.LOAD_PER_CENT

HSM Battery
Voltage: ,HSM.INT_BAT_VOLTAGE
, HSM.INT_BAT_STATE
```

CSLAN Status

Connections: ,HSM.NO_OF_CONNECTIONS
 Trans./min.: ,HSM.TRANS_PER_MINUTE

CSLAN Battery

Voltage: ,HSM.EXT_BAT_VOLTAGE
 ,HSM.EXT_BAT_STATE

Time (local/UTC)

,CSLAN.DATE_TIME_LOCAL
 ,CSLAN.DATE_TIME_UTC

Fan speed

, "F: " + CSLAN.FAN5_SPEED + " " + CSLAN.FAN3_SPEED + " " + CSLAN.FAN1_SPEED
 , "B: " + CSLAN.FAN6_SPEED + " " + CSLAN.FAN4_SPEED + " " + CSLAN.FAN2_SPEED

eth0 IPv4

Addr.: ,network.eth0.ip4_state_address
 Mask: ,network.eth0.ip4_state_netmask

eth0 MAC:

,NETWORK.ETH0.IP4_STATE_MAC
 MTU: ,NETWORK.ETH0.IP4_STATE_MTU

eth0 link (1/2)

State: ,NETWORK.ETH0.IP4_STATE_LINK_UP
 Speed: ,NETWORK.ETH0.IP4_STATE_LINK_SPEED

eth0 link (2/2)

Mode: ,NETWORK.ETH0.IP4_STATE_LINK_duplex_mode
 Interface up: ,NETWORK.ETH0.IP4_STATE_if_up

IPv4 default gateway

,NETWORK.IP4_STATE_DEFAULT_GATEWAY
 .

IPv6 default gateway

Upper: ,NETWORK.IP6_STATE_DEFAULT_GATEWAY_UPPER
 Lower: ,NETWORK.IP6_STATE_DEFAULT_GATEWAY_LOWER

CSLAN loc. date time

,CSLAN.DATE_TIME_LOCAL
 Time zone: ,CSLAN.TIMEZONE_OFS

CSLAN local: ,CSLAN.TIME_LOCAL

HSM local: ,HSM.TIME_LOCAL
 Time diff.: ,HSM.TIME_DIFF

State of the NTP

daemon on the CSLAN:
 ,CSLAN.NTP_ENABLED

```

State of the NTP
firmware module:
,HSM.NTP_MDL_STATE

SSH: ,CSLAN.SSH_ENABLED
SNMP: ,CSLAN.SNMP_ENABLED
IPTABLES: ,CSLAN.IPTABLES_ENABLED

Partitions
Boot part.: ,CSLAN.BOOT_PARTITION
Run. part.: ,CSLAN.RUN_PARTITION
#This is a comment.

PCIe clock card(1/2)
Card type:
,TIME_SOURCE.CARD_TYPE

PCIe clock card(2/2)
State:,TIME_SOURCE.CLOCK_STATE
Signal str.: ,TIME_SOURCE.ANTENNA_SIGNAL

```

To extend the idle screens with one or several additional standard screens, perform the following steps:

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the CryptoServer LAN \(p. 48\)](#).
2. Open the `/etc/dspd_idle_window.conf` file in a text editor.
3. Change this file.
4. Save and exit the file.
5. To apply the changes, restart the csxlan daemon by performing the `/etc/init.d/cs2 restart` command.
6. Close your SSH client.

6.7 Adding a Customer-Specific Screen to the Idle Screens

To extend the idle screens with one or two customer-specific screens, perform the following steps:

1. Log in remotely to the LAN device.
2. Open the `/etc/csxlan.conf` file in a text editor.
3. Go to the `[DisplayAdmin]` section.

4. Set the `CustomerValueCount` variable to the number of lines of text that shall be shown in the new screen(s). 6 is the maximum value. If the value is lower than 4, there is only one new screen and all the new lines are shown on this screen. If the value is 4 or higher, there are two new screens and the last three new lines are shown on the second new screen. That means that the second and third new line of the first new screen might be repeated on the second new screen. If the `CustomerValueCount` variable is not set, it is automatically set to 3.
Example: `CustomerValueCount = 5`
5. Decide whether it is necessary to set the `RenameCustomerValueFile` variable.
6. Decide whether the text of the `CustomerValueCount` new lines to be shown should be stored in one file or there should be `CustomerValueCount` files each of them containing one line of text.
7. If you want to use one file containing `CustomerValueCount` lines of text, perform the following substeps.
 - a. Insert the following line into the `[DisplayAdmin]` section.
`CustomerValueFileType = PANEL`
 - b. Insert the following line specifying the file containing the `CustomerValueCount` lines of text, for example `/tmp/dspd_customer.val`. Consider that files in the `/tmp` directory are removed after a reboot of the LAN device.
`CustomerValueFileName = "/tmp/dspd_customer.val"`
 - c. Save and exit the file.
 - d. Create the `/tmp/dspd_customer.val` file and open it in a text editor.
 - e. Write the `CustomerValueCount` lines of text to be shown on the display.
 - f. Save and exit the file.
 - g. Continue with step 9.
8. If you want to use `CustomerValueCount` files each of them containing one line of text, perform the following substeps.
 - a. Insert the following line into the `[DisplayAdmin]` section of the `/etc/csxlan.conf` file. `CustomerValueFileType = LINES`
 - b. Insert the following line specifying the files containing one line of text, for example `/tmp/DspCompanyCustomLine*`.
* is automatically replaced by the line numbers 0, 1, 2, 3, 4 etc. Consider that files in

the `/tmp` directory are removed after a reboot of the LAN device.

```
CustomerValueFileName = "/tmp/DspCompanyCustomLine★"
```

c. Save and exit the file.

d. Create the files

- `/tmp/DspCompanyCustomLine0`,
- `/tmp/DspCompanyCustomLine1`,
- `/tmp/DspCompanyCustomLine2`,
- `/tmp/DspCompanyCustomLine3`,
- `/tmp/DspCompanyCustomLine4` etc.,

open them in a text editor, write one line of text into each of them, save them and exit them.

e. Ensure that the number of the created files is equal to the value of the

`CustomerValueCount` variable in the `/etc/csxlan.conf` file. If this variable is not defined, three files must have been created.

f. Continue with step 9.

9. Open the `/etc/dspd_idle_window.conf` file in a text editor.

10. Insert the lines according to the following example into of this file where ever you want to add the customer-specific screens.

```
,CUSTOMER_VALUE.LINE0  
,CUSTOMER_VALUE.LINE1  
,CUSTOMER_VALUE.LINE2  
,CUSTOMER_VALUE.LINE3  
,CUSTOMER_VALUE.LINE4
```

Ensure that the number of created lines are equal to the value of the

`CustomerValueCount` variable in the `/etc/csxlan.conf` file. If this variable is not defined, three lines must have been created.

11. Save and exit this file.

12. To apply the changes, restart the csxlan daemon by performing the following command.

```
/etc/init.d/cs2 restart
```

13. Close your SSH client.

14. Watch the display on the front panel without pressing any menu control button. After some seconds the customer-specific screen(s) are shown.

6.8 Setting up Static Routing

In this chapter we will show you how to set up static routing on the `eth0` and `eth1` Ethernet connections of the LAN device.

To enable static routing to be set up, you must configure an IP address and a default gateway address for the LAN device.



The Internet Protocols IPv4 and IPv6 are supported.

In the example below we use this default gateway address for `eth0`:

```
192.168.0.1 ffde::1
```

For `eth1` we use this gateway address:

```
172.16.1.255
```

Static routing is to be set up for the following networks:

- for `eth0 10.10.10.0/24` (IPv4)
- for `eth0 ffde::effe` (IPv6)
- for `eth1 10.101.0.0/16`

To set up the static routing on the LAN device by using a display and a keyboard connected to the LAN device, proceed as follows:

1. Log in to the LAN device as root with the corresponding password.
2. Create the `route.conf` configuration file by using the UNIX vi editor:

```
vi /etc/route.conf
```



The `/etc/route.conf` configuration file is not available per default in the LAN device, and must be created manually.

3. Configure the desired static routes in the configuration file `/etc/route.conf` by adding the following data for every route in a separate line, and in the given order:

```
<Network address> <Default Gateway address> <Netmask> <Device address>
```

To set up the corresponding static route, the network `init script /etc/init.d/network` reads each line in the `/etc/route.conf` file.

Example

#net	gateway	mask	dev
10.10.10.0	192.168.0.1	24	eth0
10.101.0.0	172.16.1.255	16	eth1
ffde::effe	ffde::1	64	eth0

4. Execute the following command to bring the configured static routing into use:

```
/etc/init.d/network restart
```

6.9 Setting up fcron Jobs

The fcron daemon is a command scheduler periodically starting jobs. These jobs are stored in a configuration file in binary format. See <http://fcron.free.fr> for details.

Perform the following steps to set up fcron jobs.

1. Log in remotely to the LAN device.
2. To show the configuration, perform the `fcrontab -l` command.

Example Output

```
# call logrotate every day at 6:25AM
25 6 * * * /usr/sbin/logrotate /etc/logrotate.conf
# clean /tmp
47 6 * * 7 /bin/find /tmp -mtime +6 -exec rm -rf {} \; &>/dev/null
```

3. Perform the `fcrontab -e` command. This opens an editor (default: vi), which can be used to add or delete rules.
4. Enter the fcron job command, e.g.: `* 1 * * * touch /tmp/tobedeleted.txt`
Consider the following:

- The first 5 entries separated by spaces indicate the time schedule when the command is performed. The rest of the line is the command.
- Time schedule.

<i>Minute</i>	<i>hour</i>	<i>Day of month</i>	<i>Month</i>	<i>Day of week</i>
0 – 59	0 – 23	0 – 31	1 – 12 (or English month names)	0 – 7 (0 = 7 = Sunday)

Examples:

- `* * * * *` - Each minute, each hour, 7 days a week
- `0 0 * * *` - Each day at midnight
- `59 23 * * 0` - Each Sunday at 11:59 PM
- `20,30 1 * * 1-5` - Monday to Friday at 01:20 AM and at 01:30 AM
- `@ 5` - Every 5 minutes
- Complete examples:
 - `25 6 * * * /usr/sbin/logrotate /etc/logrotate.conf`
This starts logrotate at 6:25 AM every day.
 - `@ 5 /usr/sbin/logrotate /etc/logrotate.conf`
This starts logrotate every 5 minutes.



It is highly recommended to start logrotate every 5 minutes, if the `LogLevel` parameter in the `[Csxlan]`, the `[DisplayAdmin]` or the `[NTPClient]` section of the `/etc/csxlan.conf` file has been set to `DEBUG` or `INFO`. Otherwise, the hard disk may be full after a short period of time leading to a non-operational LAN device.

- `47 6 * * 7 /bin/find /tmp -mtime +6 -exec rm -rf {} \ ; &>/dev/null`
This searches for files in the `/tmp` directory with a modification time older than 6 days and removes them.
 - Do not edit the system-wide `/etc/fcrontab.*` files. Always use the `fcrontab -e` command instead.
 - You may use the `fcrontab -e` command with a file but do not use a user column and do not store it as the `/etc/fcrontab` file.
5. Exit the `fcrontab -e` command by entering `:wq`. This automatically updates the configuration.

7 SNMP Objects and SNMP Traps

In the following tables you can see which OIDs and Traps CryptoServer LAN can output, and what information they can provide you with. They are defined in the UTIMACO-CSLAN-MIB.txt and configured in the `cslan_mib.conf` file.

7.1 SNMP Objects

The `snmpget v2c` examples in the following subsections, e.g.,

```
snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-
MIB::cslVersion.0
```

apply with some changes as well to SNMPv3.

```
snmpget -v 3 -u <UserName> -l authPriv -a SHA -A <AuthPassword> -x AES -X
<EncryptPassword> -Oqv <IpAddr> <OID>
```

Parameter	Description
v	SNMP version. It is 3.
u	SNMPv3 user created in Enabling SNMPv3 and SNMPv3 Traps for IPv4 (p. 51)
l	Security level noAuthNoPriv No authentication method (parameters <code>-a</code> and <code>-A</code>) and no encryption algorithm (privacy; parameters <code>-x</code> and <code>-X</code>) are used. Do not use <code>noAuthNoPriv</code> because <code>authPriv</code> has a better security quality. authNoPriv An authentication method is used but no encryption algorithm is used. Do not use <code>AuthNoPriv</code> because <code>authPriv</code> has a better security quality. authPriv An authentication method and an encryption algorithm are used.
a	Authentication method (cryptographic hash function), either MD5 or SHA . Do not use MD5 because it has only poor security quality.
A	Password for the authentication method
x	Encryption algorithm, either DES or AES . Do not use DES because it has only poor security quality.
X	Password for the encryption algorithm
Oqv	Output option. Only the value of the attribute is returned.

Parameter	Description
<IpAddr>	IP address of the CryptoServer LAN. IPv4 and IPv6 are supported.
<OID>	Object identifier. Identifier for an object in the MIB (Management information base). Example: <code>UTIMACO-CSLAN-MIB::cslVersion.0</code>

Table 22: Parameters for the `snmpget v3` command

This applies in an analog way to the `snmpwalk` and `snmptable` commands.

7.1.1 CryptoServer LAN

Object name	<code>cslVersion</code>
Description	CryptoServer LAN version
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.1.1.0 (UTIMACO-CSLAN-MIB::cslVersion)
Example	<code>snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslVersion.0</code> <code>snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.1.0</code>
Example output	CSLAN 5.1.0

Object name	<code>cslSerialNumber</code>
Description	CryptoServer LAN serial number
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.1.2.0 (UTIMACO-CSLAN-MIB::cslSerialNumber)
Example	<code>snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslSerialNumber.0</code> <code>snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.2.0</code>
Example output	MD2000609

Object name	<code>cslBatteryState</code>
Description	State of the external battery in the CryptoServer LAN (OK, LOW or ABSENCE)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.1.3.0 (UTIMACO-CSLAN-MIB::cslBatteryState)

Example	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslBatteryState.0 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.3.0
Example output	OK

Object name	cslDateTime
Description	CryptoServer LAN date and time (YYYYMMDD hhmmss, UTC)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.1.4.0 (UTIMACO-CSLAN-MIB::cslDateTime)
Example	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslDateTime.0 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.4.0
Example output	20150605 092900

Object name	cslLoad
Description	Workload average of the CryptoServer PCIe card in %. The workload is the ratio of the time that requests/commands spend in the CryptoServer PCIe card to the total time. This workload average corresponds to the result of the csadm CSLGetLoad command. For details about this command, see CryptoServer – csadm Manual (p. 240) .
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.1.5.0 (UTIMACO-CSLAN-MIB::cslLoad)
Example	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslLoad.0 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.5.0
Example output	0



The information of the workload of the CryptoServer is read from the display module of the CryptoServer LAN. If the display module is busy (i.e. an operator is working at the display) this information is not available and the cslLoad value does not represent any value.



The cslLoad value is not the workload at that time. It is an average value of the last 64 measurements. The value is continuously recalculated. If no packets arrive, it is recalculated once per second. If more packets arrive, it is recalculated more often, up to once per every few milliseconds.

Object name	cslClients
Description	CryptoServer LAN number of client connections
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.1.6.0 (UTIMACO-CSLAN-MIB::cslClients)
Example	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslClients.0 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.6.0
Example output	1

Object name	cslClientsLoad
Description	CryptoServer LAN client connection load in % (0...100). The client connection load is the relation of the number of current client connections to the permitted maximum value of client connections configured as the MaxConnections parameter in the csxlan.conf file. Example: Number of current client connections: 40, MaxConnections: 400 ==> cslClientsLoad: 10%
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.1.7.0 (UTIMACO-CSLAN-MIB::cslClientsLoad)
Example	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslClientsLoad.0 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.7.0
Example output	0

7.1.2 Fan Table

Object name	cslFanTable
Description	CryptoServer LAN fan table (information about all CryptoServer LAN fans)
Type	Table
OID (Name)	1.3.6.1.4.1.3159.1.1.8 (UTIMACO-CSLAN-MIB::cslFanTable)

Example	snmptable -v 2c -c CryptoServer -Cw 70 111.166.1.200 UTIMACO-CSLAN-MIB::cslFanTable snmptable -v 2c -c CryptoServer -Cw 70 111.166.1.200 1.3.6.1.4.1.3159.1.1.8	
Example output	SNMP table: UTIMACO-CSLAN-MIB::cslFanTable	
	cslFanIndex	cslFanSpeed
	1	3600
	2	3650
	3	3700
	4	3620
	5	3680
	6	3670

Object name	cslFanIndex.x
Description	Fan index for identification. A CryptoServer LAN V5 has 6 fans in 3 fan modules and no CPU fan. Fan modules are exachangeable but fans are not. The fan indexes 1 and 2 indicate fans in the right fan module (fan module f12 in the figure below), 3 and 4 indicate fans in the middle module (f11), and 5 and 6 indicate fans in the left module (f10).
Type	Integer (1...6)
OID (Name)	1.3.6.1.4.1.3159.1.1.8.1.1.x (UTIMACO-CSLAN-MIB:: cslFanIndex.x)
Example (Fan 1)	<pre>snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN- MIB:: cslFanIndex.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.8.1.1.1</pre>
Example output	1



Figure 39 : Front panel with removed fan compartment grill

Object name	cslFanSpeed.x
--------------------	---------------

Description	Fan speed of CryptoServer LAN fan x in rpm. A value of 0 for the fan speed indicates a broken fan. In this case, create an RMA (Return Merchandise Authorization) according to Contact Address for Support Queries (p. 239) .
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.1.8.1.2.x (UTIMACO-CSLAN-MIB::cslFanSpeed.x)
Example (fan 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslFanSpeed.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.8.1.2.1
Example output	3600

Object name	cslFanSpeed
Description	Fan speed of all CryptoServer LAN fans in rpm. A value of 0 for the fan speed indicates a broken fan. In this case, create an RMA (Return Merchandise Authorization) according to Contact Address for Support Queries (p. 239) .
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.1.8.1.2 (UTIMACO-CSLAN-MIB::cslFanSpeed)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cslFanSpeed snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.1.8.1.2
Example output	cslFanSpeed.1 = INTEGER: 3600 cslFanSpeed.2 = INTEGER: 3650 cslFanSpeed.3 = INTEGER: 3700 cslFanSpeed.4 = INTEGER: 3620 cslFanSpeed.5 = INTEGER: 3680 cslFanSpeed.6 = INTEGER: 3670

7.1.3 Power Supply and Temperature

Object name	cslPowerSupply
Description	CryptoServer LAN status of the redundant power supply modules (OK or Failed). If the status of a power supply module is failed, the power supply status of the entire CryptoServer LAN is failed, Only if the status of all power supply modules is OK, the power supply status of the entire CryptoServer LAN is OK.
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.1.9.0 (UTIMACO-CSLAN-MIB::cslPowerSupply)

Example	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslPowerSupply.0 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.9.0
Example output	OK

Object name	cslCPUTemperature
Description	CryptoServer LAN CPU temperature in °C
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.1.10.0 (UTIMACO-CSLAN-MIB::cslCPUTemperature)
Example	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslCPUTemperature snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.10.0
Example output	35

Object name	cslCPUTemperatureAsString
Description	CryptoServer LAN CPU temperature in °C as String with 1 decimal place
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.1.11.0 (UTIMACO-CSLAN-MIB::cslCPUTemperatureAsString)
Example	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslCPUTemperatureAsString snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.11.0
Example output	35.5

7.1.4 Power SupplyTable

Object name	cslPowerSupplyTable
Description	The table holding information about all power supply modules within the CryptoServer LAN
Type	Table
OID (Name)	1.3.6.1.4.1.3159.1.1.12 (UTIMACO-CSLAN-MIB::cslPowerSupplyTable)
Example	snmptable -v 2c -c CryptoServer -Cw 70 111.166.1.200 UTIMACO-CSLAN-MIB::cslPowerSupplyTable snmptable -v 2c -c CryptoServer -Cw 70 111.166.1.200 1.3.6.1.4.1.3159.1.1.12

Example output	SNMP table: UTIMACO-CSLAN-MIB::cslPowerSupplyTable		
	csPowerSupplyIndex	cslPowerSupplyStatus	cslPowerSupplyStatusAsString
	1	1	presence detected
	2	1	presence detected

Object name	cslPowerSupplyIndex.x
Description	CryptoServer LAN power supply index for identification CryptoServer LAN power supply index for identification. Power supply module no. 1 (right one in Figure 7, "Rear view of CryptoServer LAN V5") is identical to cslPowerSupplyIndex=1 and power supply module no. 2 (left one in Figure 7) is identical to cslPowerSupplyIndex=2.
Type	Integer (1...2)
OID (Name)	1.3.6.1.4.1.3159.1.1.12.1.1.x (UTIMACO-CSLAN-MIB::cslPowerSupplyIndex.x)
Example (Power Supply 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslPowerSupplyIndex.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.12.1.1.1
Example output	1

Object name	cslPowerSupplyStatus.x
Description	Status of power supply x in the CryptoServer LAN
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.1.12.1.2.x (UTIMACO-CSLAN-MIB::cslPowerSupplyStatus.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslPowerSupplyStatus.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.12.1.2.1
Example output	1

Object name	cslPowerSupplyStatus
Description	States of all power supplies in the CryptoServer LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.1.12.1.2 (UTIMACO-CSLAN-MIB::cslPowerSupplyStatus)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cslPowerSupplyStatus snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.1.12.1.2
Example output	cslPowerSupplyStatus.1 = INTEGER: 1 cslPowerSupplyStatus.2 = INTEGER: 1

Object name	cslPowerSupplyStatusAsString.x
Description	Status of power supply x in the CryptoServer LAN as a string
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.1.12.1.3.x (UTIMACO-CSLAN-MIB::cslPowerSupplyStatusAsString.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslPowerSupplyStatusAsString.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.12.1.3.1
Example output	presence detected

Object name	cslPowerSupplyStatusAsString
Description	Strings of all power supply states mounted in the CryptoServer LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.1.12.1.3 (UTIMACO-CSLAN-MIB::cslPowerSupplyStatusAsString)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cslPowerSupplyStatusAsString snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.1.12.1.3
Example output	cslPowerSupplyStatusAsString.1 = STRING: presence detected cslPowerSupplyStatusAsString.2 = STRING: presence detected

7.1.5 CryptoServer Table

Object name	csTable
Description	The table holding information about all CryptoServers within the CryptoServer LAN
Type	Table
OID (Name)	1.3.6.1.4.1.3159.1.2 (UTIMACO-CSLAN-MIB::csTable)
Example	snmptable -v 2c -c CryptoServer -Cw 70 111.166.1.200 UTIMACO-CSLAN-MIB::csTable snmptable -v 2c -c CryptoServer -Cw 70 111.166.1.200 1.3.6.1.4.1.3159.1.2

Example output	SNMP table: UTIMACO-CSLAN-MIB::csTable				
	csIndex	csDevice	csMode	csState	csTemperature
	1	288@localhost	OPERATIONAL	INITIALIZED	41
	SNMP table: UTIMACO-CSLAN3-MIB::csTable, part 2				
	csTemperatureAsString	csAlarm	csVersion	csSerialNumber	csBatteryState
	41.3	0	3.00.3.0	CS411957	OK
	SNMP table: UTIMACO-CSLAN-MIB::csTable, part 3				
	csDateTime	csModuleState	csTransactionsPerMinute		
	20150605 093858	OK	7		

Object name	csIndex.x
Description	CryptoServer x device index for identification
Type	Integer (1...4)
OID (Name)	1.3.6.1.4.1.3159.1.2.1.1.x (UTIMACO-CSLAN-MIB::csIndex.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csIndex.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.1.1
Example output	1

Object name	csDevice.x
Description	CryptoServer x device in the CryptoServer LAN
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.2.1.2.x (UTIMACO-CSLAN-MIB::csDevice.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csDevice.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.2.1
Example output	288@localhost

Object name	csDevice
Description	All CryptoServer devices in the CryptoServer LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.2 (UTIMACO-CSLAN-MIB::csDevice)

Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csDevice snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.2
Example output	csDevice.1 = STRING: 288@localhost csDevice.2 = STRING: 288@localhost

Object name	csMode.x
Description	Operating mode of CryptoServer x in the CryptoServer LAN (supported values: BOOTLOADER, OPERATIONAL, MAINTENANCE, ALARM or POWERDOWN)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.2.1.3.x (UTIMACO-CSLAN-MIB::csMode.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csMode.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.3.1
Example output	OPERATIONAL

Object name	csMode
Description	Operating mode of all CryptoServer devices mounted in the CryptoServer LAN (supported values: BOOTLOADER, OPERATIONAL, MAINTENANCE, ALARM or POWERDOWN)
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.3 (UTIMACO-CSLAN-MIB::csMode)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csMode snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.3
Example output	csMode.1 = STRING: OPERATIONAL csMode.2 = STRING: OPERATIONAL

Object name	csState.x
Description	Operational state of CryptoServer x device mounted in the CryptoServer LAN (supported values: BLANK, DEFECT, MANUFACTURED, PRODUCED, INITIALIZED or UNKNOWN)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.2.1.4.x (UTIMACO-CSLAN-MIB::csState.x)

Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO- CSLAN-MIB::csState.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.4.1
Example output	INITIALIZED

Object name	csState
Description	Operational state of all CryptoServer devices mounted in the CryptoServer LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.4 (UTIMACO-CSLAN-MIB::csState)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO- CSLAN-MIB::csState snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.4
Example output	csState.1 = STRING: INITIALIZED csState.2 = STRING: INITIALIZED

Object name	csTemperature.x
Description	Temperature of CryptoServer x in °C
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.2.1.5.x (UTIMACO-CSLAN-MIB::csTemperature.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO- CSLAN-MIB::csTemperature.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.5.1
Example output	41

Object name	csTemperature
Description	Temperature in °C of all CryptoServer devices mounted in the CryptoServer LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.5 (UTIMACO-CSLAN-MIB::csTemperature)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO- CSLAN-MIB::csTemperature snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.5
Example output	csTemperature.1 = INTEGER: 41 csTemperature.2 = INTEGER: 40

Object name	csTemperatureAsString.x
--------------------	-------------------------

Description	Temperature (in °C as string with 1 decimal place) of a CryptoServer x device mounted in the CryptoServer LAN
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.2.1.6.x (UTIMACO-CSLAN-MIB::csTemperatureAsString.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csTemperatureAsString.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.6.1
Example output	41.3

Object name	csTemperatureAsString
Description	Temperature (in °C as string with 1 decimal place) of all CryptoServer devices mounted in the CryptoServer LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.6 (UTIMACO-CSLAN-MIB::csTemperatureAsString)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csTemperatureAsString snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.6
Example output	csTemperatureAsString.1 = STRING: 41.1 csTemperatureAsString.2 = STRING: 40.5

Object name	csAlarm.x
Description	Alarm register of CryptoServer x device mounted in CryptoServer LAN (0 = alarm OFF, 1 or higher = value of the alarm register)
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.2.1.7.x (UTIMACO-CSLAN-MIB::csAlarm.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csAlarm.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.7.1
Example output	0

Object name	csAlarm
Description	Alarm register of all CryptoServer devices mounted in the CryptoServer LAN (0 = alarm OFF, 1 or higher = value of the alarm register)
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.7 (UTIMACO-CSLAN-MIB::csAlarm)

Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csAlarm snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.7
Example output	csAlarm.1 = INTEGER: 0 csAlarm.2 = INTEGER: 639

Object name	csVersion.x
Description	Bootloader version of CryptoServer x device in the CryptoServer LAN
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.2.1.8.x (UTIMACO-CSLAN-MIB::csVersion.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csVersion.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.8.1
Example output	3.00.3.0

Object name	csVersion
Description	Bootloader version of all CryptoServers
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.8 (UTIMACO-CSLAN-MIB::csVersion)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csVersion snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.8
Example output	csVersion.1 = STRING: 3.00.3.0 csVersion.2 = STRING: 3.00.2.0

Object name	csSerialNumber.x
Description	Serial number of CryptoServer x (CSxxxxxx)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.2.1.9.x (UTIMACO-CSLAN-MIB::csSerialNumber.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csSerialNumber.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.9.1
Example output	CS411957

Object name	csSerialNumber
--------------------	----------------

Description	Serial number of all CryptoServer devices mounted in the CryptoServer LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.9 (UTIMACO-CSLAN-MIB::csSerialNumber)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csSerialNumber snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.9
Example output	csSerialNumber.1 = STRING: CS411957 csSerialNumber.2 = STRING: CS888022

Object name	csBatteryState.x
Description	State of the carrier battery in the CryptoServer x device (OK, LOW or ABSENCE)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.2.1.10.x (UTIMACO-CSLAN-MIB::csBatteryState.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csBatteryState.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.10.1
Example output	OK

Object name	csBatteryState
Description	State of the carrier batteries in all (1...4) CryptoServers mounted in the CryptoServer LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.10 (UTIMACO-CSLAN-MIB::csBatteryState)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csBatteryState snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.10
Example output	csBatteryState.1 = STRING: OK csBatteryState.2 = STRING: OK

Object name	csDateTime.x
Description	Date and time of CryptoServer x device mounted in the CryptoServer LAN (YYYYMMDD hhmmss, UTC)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.2.1.11.x (UTIMACO-CSLAN-MIB::csDateTime.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csDateTime.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.11.1

Example output	20150605 111321
-----------------------	-----------------

Object name	csDateTime
Description	Date and time of all CryptoServer in the CryptoServer LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.11 (UTIMACO-CSLAN-MIB::csDateTime)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csDateTime snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.11
Example output	csDateTime.1 = STRING: 20150605 111321 csDateTime.2 = STRING: 20150605 111325

Object name	csModuleState.x
Description	Module initialization state of CryptoServer x device mounted in the CryptoServer LAN (OK or Failed if at least one module failed to initialize)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.2.1.12.x (UTIMACO-CSLAN-MIB::csModuleState.x)
Example (CryptoServer 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csModuleState.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.12.1
Example output	OK

Object name	csModuleState
Description	Module initialization state of all (1...4) CryptoServer devices mounted in the CryptoServer LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.12 (UTIMACO-CSLAN-MIB::csModuleState)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csModuleState snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.12
Example output	csModuleState.1 = STRING: OK csModuleState.2 = STRING: OK

Object name	csTransactionsPerMinute.x
--------------------	---------------------------

Description	<p>Transactions per minute of CryptoServer x device mounted in the CryptoServer LAN.</p> <p>This value is shown on the display on the front panel when you switch on the CryptoServer LAN.</p> <p>This value shows a time-averaged value of how many requests the HSM received in a time interval of 60 seconds. This includes internal requests as well as external requests. So even if no external requests are pending, the value for transactions per minute may be greater than zero.</p> <p>Internal requests can come from the display daemon, which periodically requests statistical values and from snmp when corresponding requests are received. External requests are the typical requests from remote hosts to the HSM.</p> <p>The transactions are calculated over a period of 25 seconds and then extrapolated to transactions per minute (tpm).</p>
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.2.1.13.x (UTIMACO-CSLAN-MIB:: csTransactionsPerMinute.x)
Example (CryptoServer 1)	<pre>snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB:: csTransactionsPerMinute.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.13.1</pre>
Example output	7

```

- CryptoServer LAN -
HSM Model:
  SecurityServer
  Se1500 CS132456

- CryptoServer LAN -
HSM Status (1/2)
Mode:      Operational
Admin Mode:      no

- CryptoServer LAN -
HSM Status (2/2)
Temperature: 30.0 °C
Load:        0.0 %

- CryptoServer LAN -
HSM Battery
Voltage:      3.045 V
              OK

- CryptoServer LAN -
CSLAN Status
Connections:      2
Trans./min.:      7 TPM

- CryptoServer LAN -
CSLAN Battery
Voltage:      3.066 V
              OK

- CryptoServer LAN -
Time (local/UTC)
2018-09-20 13:00:33
2018-09-20 12:00:33

- CryptoServer LAN -
Fan speed
F:  6100  6100  6200
B:  5300  5200  5200

```

Figure 40 : Idle Screens

Object name	csTransactionsPerMinute
--------------------	-------------------------

Description	<p>Transactions per minute of all CryptoServer devices mounted in the CryptoServer LAN.</p> <p>This value shows a time-averaged value of how many requests all HSMs received in a time interval of 60 seconds. This includes internal requests as well as external requests. So even if no external requests are pending, the value for transactions per minute may be greater than zero.</p> <p>Internal requests can come from the display daemon, which periodically requests statistical values and from snmp when corresponding requests are received. External requests are the typical requests from remote hosts to the HSMs.</p> <p>The transactions are calculated over a period of 25 seconds and then extrapolated to transactions per minute (tpm).</p>
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.2.1.12 (UTIMACO-CSLAN-MIB:: csTransactionsPerMinute)
Example	<pre>snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB:: csTransactionsPerMinute</pre> <pre>snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.2.1.13</pre>
Example output	<pre>csTransactionsPerMinute.1 = INTEGER: 4</pre> <pre>csTransactionsPerMinute.2 = INTEGER: 3</pre>

7.2 SNMP Traps

For information about how to configure SNMP traps, see [Configuring SNMP Traps \(p. 56\)](#).

Error Trap

Trap name	notifyError
Description	Error notification
Severity	Major
OID (Name)	1.3.6.1.4.1.3159.1.3.0.1 (UTIMACO-CSLAN-MIB::notifyError)
Variables	Error code (Integer; 1.3.6.1.4.1.3159.1.3.1.2.0)

Mode Change Trap

Trap name	notifyCsModeChange
Description	<p>CryptoServer operating mode change notification</p> <p>Notification that the operating mode of a CryptoServer in the CryptoServer LAN has changed (supported values: BOOTLOADER, OPERATIONAL, MAINTENANCE, ALARM or POWERDOWN)</p>
Severity	Normal

OID (Name)	1.3.6.1.4.1.3159.1.3.0.2 (UTIMACO-CSLAN-MIB::notifyCsModeChange)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0) Old mode (String; 1.3.6.1.4.1.3159.1.3.1.3.0) New mode (String; 1.3.6.1.4.1.3159.1.3.1.4.0)

Alarm Trap

Trap name	notifyCsAlarmTemperatureLow
Description	CryptoServer alarm notification that the temperature is too low
Severity	Critical
OID (Name)	1.3.6.1.4.1.3159.1.3.0.3 (UTIMACO-CSLAN-MIB::notifyCsAlarmTemperatureLow)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

Trap name	notifyCsAlarmTemperatureHigh
Description	CryptoServer alarm notification that the temperature is too high
Severity	Critical
OID (Name)	1.3.6.1.4.1.3159.1.3.0.4 (UTIMACO-CSLAN-MIB::notifyCsAlarmTemperatureHigh)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

Trap name	notifyCsAlarmInnerFoil
Description	CryptoServer alarm notification that the inner foil is broken
Severity	Critical
OID (Name)	1.3.6.1.4.1.3159.1.3.0.5 (UTIMACO-CSLAN-MIB::notifyCsAlarmInnerFoil)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

Trap name	notifyCsAlarmOuterFoil
Description	CryptoServer alarm notification that the outer foil is broken
Severity	Critical
OID (Name)	1.3.6.1.4.1.3159.1.3.0.6 (UTIMACO-CSLAN-MIB::notifyCsAlarmOuterFoil)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

Trap name	notifyCsAlarmPowerFailed
Description	CryptoServer alarm notification of power failure
Severity	Critical
OID (Name)	1.3.6.1.4.1.3159.1.3.0.7 (UTIMACO-CSLAN-MIB::notifyCsAlarmPowerFailed)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

Trap name	notifyCsAlarmPowerLow
Description	CryptoServer alarm notification that the power is too low
Severity	Critical
OID (Name)	1.3.6.1.4.1.3159.1.3.0.8 (UTIMACO-CSLAN-MIB::notifyCsAlarmPowerLow)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

Trap name	notifyCsAlarmPowerHigh
Description	CryptoServer alarm notification that the power is too high
Severity	Critical
OID (Name)	1.3.6.1.4.1.3159.1.3.0.9 (UTIMACO-CSLAN-MIB::notifyCsAlarmPowerHigh)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

Trap name	notifyCsAlarmInvalidMasterKey
Description	CryptoServer alarm notification that the Master Key is invalid
Severity	Critical
OID (Name)	1.3.6.1.4.1.3159.1.3.0.10 (UTIMACO-CSLAN-MIB::notifyCsAlarmInvalidMasterKey)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

Trap name	notifyCsAlarmExternalErase
Description	CryptoServer alarm notification that an External Erase has been performed
Severity	Critical
OID (Name)	1.3.6.1.4.1.3159.1.3.0.11 (UTIMACO-CSLAN-MIB::notifyCsAlarmExternalErase)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

High Temperature Traps

Trap name	notifyCsTemperatureHigh
Description	CryptoServer notification that the temperature has risen above the threshold
Severity	Major
OID (Name)	1.3.6.1.4.1.3159.1.3.0.12 (UTIMACO-CSLAN-MIB::notifyCsTemperatureHigh)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0) Temperature (Integer; 1.3.6.1.4.1.3159.1.3.1.5.0) Temperature with 1 decimal (String; 1.3.6.1.4.1.3159.1.3.1.6.0)

Trap name	notifyCsTemperatureHighBack
Description	CryptoServer notification that the temperature has fallen back to or below the threshold
Severity	Normal
OID (Name)	1.3.6.1.4.1.3159.1.3.0.13 (UTIMACO-CSLAN-MIB::notifyCsTemperatureHighBack)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0) Temperature (Integer; 1.3.6.1.4.1.3159.1.3.1.5.0) Temperature with 1 decimal (String; 1.3.6.1.4.1.3159.1.3.1.6.0)

Low Temperature Traps

Trap name	notifyCsTemperatureLow
Description	CryptoServer notification that the temperature has fallen below the threshold
Severity	Major
OID (Name)	1.3.6.1.4.1.3159.1.3.0.14 (UTIMACO-CSLAN-MIB::notifyCsTemperatureLow)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0) Temperature (Integer; 1.3.6.1.4.1.3159.1.3.1.5.0) Temperature with 1 decimal (String; 1.3.6.1.4.1.3159.1.3.1.6.0)

Trap name	notifyCsTemperatureLowBack
Description	CryptoServer notification that the temperature has risen back to or above the threshold
Severity	Normal
OID (Name)	1.3.6.1.4.1.3159.1.3.0.15 (UTIMACO-CSLAN-MIB::notifyCsTemperatureLowBack)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0) Temperature (Integer; 1.3.6.1.4.1.3159.1.3.1.5.0) Temperature with 1 decimal (String; 1.3.6.1.4.1.3159.1.3.1.6.0)

Battery Traps

Trap name	notifyCsBatteryLow
Description	CryptoServer notification that the CryptoServer onboard battery (carrier battery) voltage level is too low
Severity	Major
OID (Name)	1.3.6.1.4.1.3159.1.3.0.16 (UTIMACO-CSLAN-MIB::notifyCsBatteryLow)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

Trap name	notifyCsIbBatteryLow
Description	CryptoServer LAN notification that the CryptoServer LAN backup battery (external battery) voltage level is too low

Severity	Major
OID (Name)	1.3.6.1.4.1.3159.1.3.0.17 (UTIMACO-CSLAN-MIB::notifyCslBatteryLow)
Variables	-

Load Traps

Trap name	notifyCslLoadHigh
Description	CryptoServer LAN notification that the workload of the CryptoServer PCIe card has risen above the threshold. The workload is the ratio of the time that requests/commands spend in the CryptoServer PCIe card to the total time. The workload average is represented by the cslLoad object and it corresponds to the result of the csadm CSLGetLoad command. For details about this command, see CryptoServer – csadm Manual (p. 240) .
Severity	Major
OID (Name)	1.3.6.1.4.1.3159.1.3.0.18 (UTIMACO-CSLAN-MIB::notifyCslLoadHigh)
Variables	Workload of the CryptoServer PCIe card in % (Integer; 1.3.6.1.4.1.3159.1.3.1.7.0)

Trap name	notifyCslLoadHighBack
Description	CryptoServer LAN notification that the workload of the CryptoServer PCIe card has fallen back to or below the threshold. The workload is the ratio of the time that requests/commands spend in the CryptoServer PCIe card to the total time. The workload average is represented by the cslLoad object and it corresponds to the result of the csadm CSLGetLoad command. For details about this command, see CryptoServer – csadm Manual (p. 240) .
Severity	Normal
OID (Name)	1.3.6.1.4.1.3159.1.3.0.19 (UTIMACO-CSLAN-MIB::notifyCslLoadHighBack)
Variables	Workload of the CryptoServer PCIe card in % (Integer; 1.3.6.1.4.1.3159.1.3.1.7.0)

Client Traps

Trap name	notifyCslClientsHigh
Description	CryptoServer LAN notification that the client connection load has risen above the threshold
Severity	Major
OID (Name)	1.3.6.1.4.1.3159.1.3.0.20 (UTIMACO-CSLAN-MIB::notifyCslClientsHigh)
Variables	Client connection load in % (Integer; 1.3.6.1.4.1.3159.1.3.1.8.0)

Trap name	notifyCslClientsHighBack
Description	CryptoServer LAN notification that the client connection load has fallen back to or below the threshold
Severity	Normal
OID (Name)	1.3.6.1.4.1.3159.1.3.0.21 (UTIMACO-CSLAN-MIB::notifyCslClientsHighBack)
Variables	Client connection load in % (Integer; 1.3.6.1.4.1.3159.1.3.1.8.0)

Boot Trap

Trap name	notifyCslBoot
Description	CryptoServer LAN notification that the CryptoServer LAN has booted
Severity	Normal
OID (Name)	1.3.6.1.4.1.3159.1.3.0.22 (UTIMACO-CSLAN-MIB::notifyCslBoot)
Variables	-

Shutdown Trap

Trap name	notifyCslShutDown
Description	CryptoServer LAN notification that the CryptoServer LAN is shutting down
Severity	Normal
OID (Name)	1.3.6.1.4.1.3159.1.3.0.23 (UTIMACO-CSLAN-MIB::notifyCslShutDown)
Variables	-

Low Fan Speed Traps

By default, a trap is sent if the fan speed falls below a certain threshold or exceeds this threshold again. For more information about this threshold, see [\[FanSpeedTraps\]](#) in [Configuring SNMP Traps \(p. 56\)](#).

Trap name	notifyCslFanSpeedLow
Description	CryptoServer LAN notification that the CryptoServer LAN fan speed has fallen below the threshold
Severity	Major
OID (Name)	1.3.6.1.4.1.3159.1.3.0.24 (UTIMACO-CSLAN-MIB::notifyCslFanSpeedLow)
Variables	Fan index (Integer; 1.3.6.1.4.1.3159.1.3.1.9.0) Fan speed in rpm (Integer; 1.3.6.1.4.1.3159.1.3.1.10.0)

Trap name	notifyCslFanSpeedLowBack
------------------	--------------------------

Description	CryptoServer LAN notification that the CryptoServer LAN fan speed has risen back to or above the threshold
Severity	Normal
OID (Name)	1.3.6.1.4.1.3159.1.3.0.25 (UTIMACO-CSLAN-MIB::notifyCslFanSpeedLowBack)
Variables	Fan index (Integer; 1.3.6.1.4.1.3159.1.3.1.9.0) Fan speed in rpm (Integer; 1.3.6.1.4.1.3159.1.3.1.10.0)

Power Supply Trap

Trap name	notifyCslPowerSupplyFailure
Description	CryptoServer LAN notification that the CryptoServer LAN redundant power supply has failed
Severity	Major
OID (Name)	1.3.6.1.4.1.3159.1.3.0.26 (UTIMACO-CSLAN-MIB::notifyCslPowerSupplyFailure)
Variables	-

IPMI Link Trap

Trap name	notifyCslIPMILink
Description	CryptoServer LAN notification that the CryptoServer LAN dedicated IPMI interface has a link
Severity	Warning
OID (Name)	1.3.6.1.4.1.3159.1.3.0.27 (UTIMACO-CSLAN-MIB::notifyCslIPMILink)
Variables	-

8 Contact Address for Support Queries

If an error occurs while operating the CryptoServer, read [CryptoServer Troubleshooting \(p. 240\)](#) to solve it.

If the error still occurs, prepare diagnostic information in a .txt file on your computer as described in [CryptoServer Troubleshooting \(p. 240\)](#).

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>

9 References

<i>Title/Company</i>	<i>Doc.-No.</i>	<i>Location</i>
CryptoServer – csadm Manual / Utimaco IS GmbH.	2009-0003	Product Bundle ...Documentation\Administration Guides
CryptoServer – Administration Manual / Utimaco IS GmbH.	M010-0001-en	Product Bundle ...Documentation\Administration Guides
CryptoServer LAN V5 Operating Manual / Utimaco IS GmbH.	2018-0004	Product Bundle ...Documentation\Operating Manuals\English
CryptoServer LAN V5 Betriebsanleitung / Utimaco IS GmbH.	2018-0009	Product Bundle ...Documentation\Operating Manuals\Deutsch
CryptoServer Troubleshooting / Utimaco IS GmbH.	M011-0008-en	Product Bundle ...Documentation\Administration Guides
CryptoServer Se-Series Gen2 CP5 – Administration Manual / Utimaco IS GmbH	2017-0008	Product Bundle ...Documentation\Administration Guides