

u.trust Anchor LAN V5

Administration Manual



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	1.2.10
Product Version	6.0.0
Date	2024-10-25
Document No.	2021-0006
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	7
1.1	About this Manual	7
1.1.1	Target Audience for this Manual	7
1.1.2	Document Conventions	7
2	The u.trust Anchor LAN - Overview	9
2.1	Administration	10
2.2	u.trust Anchor LAN System Users	11
2.3	Transferring Files to or from the u.trust Anchor LAN	11
2.4	Authenticating Commands	12
2.5	Boot Partitions in the u.trust Anchor LAN	13
2.6	The Simple Network Manager Protocol (SNMP)	14
2.7	The Internet Protocol Version 6 (IPv6)	15
2.8	The Intelligent Platform Management Interface (IPMI)	15
3	Bringing the u.trust Anchor LAN into Operation	16
3.1	Menu Options on the Front Panel of the u.trust Anchor LAN	16
3.2	Switching on the u.trust Anchor LAN	19
3.3	Changing the Default Password of the System Users	21
3.3.1	Changing the Default Password via an SSH Connection	21
3.3.2	Changing the Default Password via a Terminal	22
3.4	Setting up the IP Configuration	22
3.4.1	Setting up Static IP Addresses	26
3.4.1.1	Entering a static IPv4 Address With the Front Panel	26
3.4.1.2	Entering the IPv4 Default Gateway With the Front Panel	27
3.4.2	Setting up Dynamic IPv4 Addresses With the Front Panel	28
3.4.3	Setting up the IPv4 Configuration With a Command-Line	29
3.4.4	Setting up the IPv6 Configuration With a Command-Line	31
4	Administering the u.trust Anchor LAN	35
4.1	Enabling/Disabling the SSH Daemon	35
4.2	Logging in Remotely to the u.trust Anchor LAN	37
4.3	Setting up SNMP	38
4.3.1	Enabling SNMPv2c and SNMPv2c Traps for IPv4	38
4.3.2	Enabling SNMPv3 and SNMPv3 Traps for IPv4	40
4.3.3	Enabling SNMP and SNMP Traps for IPv6	44

4.3.4	Configuring SNMP Traps	46
4.3.5	Configuring Multiple SNMP Trap Destinations	55
4.3.6	Setting the Date and Time on the CryptoServer LAN.....	58
4.3.7	Specifying the Keyboard Layout.....	59
4.4	Showing u.trust Anchor LAN Information.....	60
4.4.1	Showing the u.trust Anchor LAN Version and Serial Number	60
4.4.2	Showing the Network State	61
4.4.3	Showing the Services on the u.trust Anchor LAN.....	62
4.4.4	Showing the Date and Time on the u.trust Anchor LAN	62
4.4.5	Showing the Partitions	63
4.4.6	Showing the Fan Speed	63
4.4.7	Showing the PCIe Clock Card Information.....	64
4.5	Changing the Default Hostname of the u.trust Anchor LAN	65
4.6	Update and Maintenance.....	66
4.6.1	Updating the Operating System.....	66
4.6.1.1	Performing a Local Update.....	68
4.6.1.2	Performing a Remote Update	70
4.6.2	Selecting a Boot Partition.....	72
4.6.3	Reverting the Configuration of the u.trust Anchor LAN.....	73
4.6.4	Verifying the Reachability in the Network (ping)	73
4.7	Rebooting the u.trust Anchor LAN.....	74
4.8	Shutting down the u.trust Anchor LAN.....	75
4.9	Setting up PCIe Clock Cards	76
4.10	Setting up NTP	80
4.10.1	Preparations	80
4.10.2	Setting up NTP Primarily Using the Front Panel.....	82
4.10.3	Setting up NTP Primarily Using Scripts.....	83
4.10.4	Configuring Time Synchronization between the u.trust Anchor LAN and the u.trust Anchor PCIe Card	85
4.11	Viewing NTP Log Entries	87
4.12	Changing the Time Zone for the u.trust Anchor LAN.....	88
4.13	Setting up Bonding	88
4.14	Using IPMI	91
4.14.1	Accessing the CryptoServer LAN.....	91

4.14.2	Showing Sensor Values	92
4.14.3	Showing Chassis Information.....	96
4.14.4	Showing System Event Log Information	96
4.14.5	Showing LAN Information	97
4.14.6	Showing User Information.....	99
4.14.7	Default IPMI Interface Configuration.....	100
4.14.8	Changing the Default IPMI Interface Configuration.....	101
4.14.8.1	Setting up IP Reachability	101
4.14.8.2	Setting up the IPMI Web Server.....	103
4.15	Changing the SSH Login Banner.....	104
5	Administering the u.trust Anchor	106
5.1	Showing u.trust Anchor Information	106
5.1.1	Symbols on the display	106
5.1.2	Showing the Version.....	106
5.1.3	Showing the u.trust Anchor Status	107
5.1.4	Showing the Battery State.....	108
5.1.5	Showing the Date and Time on the u.trust Anchor	109
6	Advanced Administration on the u.trust Anchor LAN	110
6.1	Configuring the Transfer Speed for Ethernet.....	110
6.2	TLS for u.trust Anchor LAN	112
6.2.1	Configure TLS for u.trust Anchor LAN	114
6.2.1.1	Variables in the global section [Csxlan].....	114
6.2.1.2	Variables in the [Listener] section	115
6.2.1.3	Environment variables on client side.....	116
6.2.2	How to configure TLS.....	118
6.2.2.1	Install OpenSSL >3.0	118
6.2.2.2	Create HSM's Certificates and keys.....	120
6.2.2.3	Create HOST's Certificate and keys	120
6.2.2.4	Update CSXLAN.CONF in section [csxlan]	121
6.2.2.5	Host Side configuration.....	121
6.2.2.6	Test with csadm	121
6.3	The Configuration File csxlan.conf	122
6.4	Restricting the Network Access on the CryptoServer LAN	133
6.4.1	iptables for IPv4	133
6.4.2	iptables for IPv6	137
6.5	Setting up Remote Logging	137

6.5.1	Configuring the csxlan.conf File.....	138
6.5.2	Configuring the syslog.conf File.....	139
6.5.3	Configuring the Remote Syslog Daemon.....	140
6.5.4	Configuring logrotate	140
6.6	Adjusting the Menu Structure for the Menu Options	141
6.7	Adding a Standard Screen to the Idle Screens	144
6.8	Adding a Customer-Specific Screen to the Idle Screens	151
6.9	Setting up Static Routing	154
6.10	Setting up fcron Jobs	155
7	SNMP Objects and SNMP Traps	157
7.1	SNMP Objects.....	157
7.1.1	u.trust Anchor LAN	158
7.1.2	Fan Table.....	160
7.1.3	Power Supply and Temperature	162
7.1.4	Power SupplyTable.....	163
7.1.5	CryptoServer Table.....	165
7.1.6	CSAR Table.....	175
7.1.7	cHSM Table	182
7.2	SNMP Traps.....	190
8	Contact Address for Support Queries	198
9	References	199

1 Introduction

Thank you for purchasing our u.trust Anchor LAN V5 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 u.trust Anchor LAN V5.

You will find the license conditions for this software in the document `ustrust_Anchor_Se_Licenses.pdf` on the delivered SecurityServer bundle in the directory `Documentation\Administration Guides\Licenses`.

1.1 About this Manual

This manual describes how to configure the u.trust Anchor LAN V5, 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.



Please note that the administration tool CAT is not available for the u.trust Anchor Se at this point. It is still mentioned in this manual and will become available at a later version.

1.1.1 Target Audience for this Manual

This manual is primarily designed to be used by OPERATORS who are responsible for the u.trust Anchor LAN V5.

1.1.2 Document Conventions

We use the following document conventions:

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

Table 1: Document conventions

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



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



Here, you find additional notes or supplementary information.



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

2 The u.trust Anchor LAN - Overview

The u.trust Anchor LAN V5 is a 19-inch appliance in which a u.trust Anchor PCIe card is mounted. It can easily be mounted in a 19-inch cabinet and integrated into a network.

The environment in which a u.trust Anchor LAN V5 can be implemented looks like this:

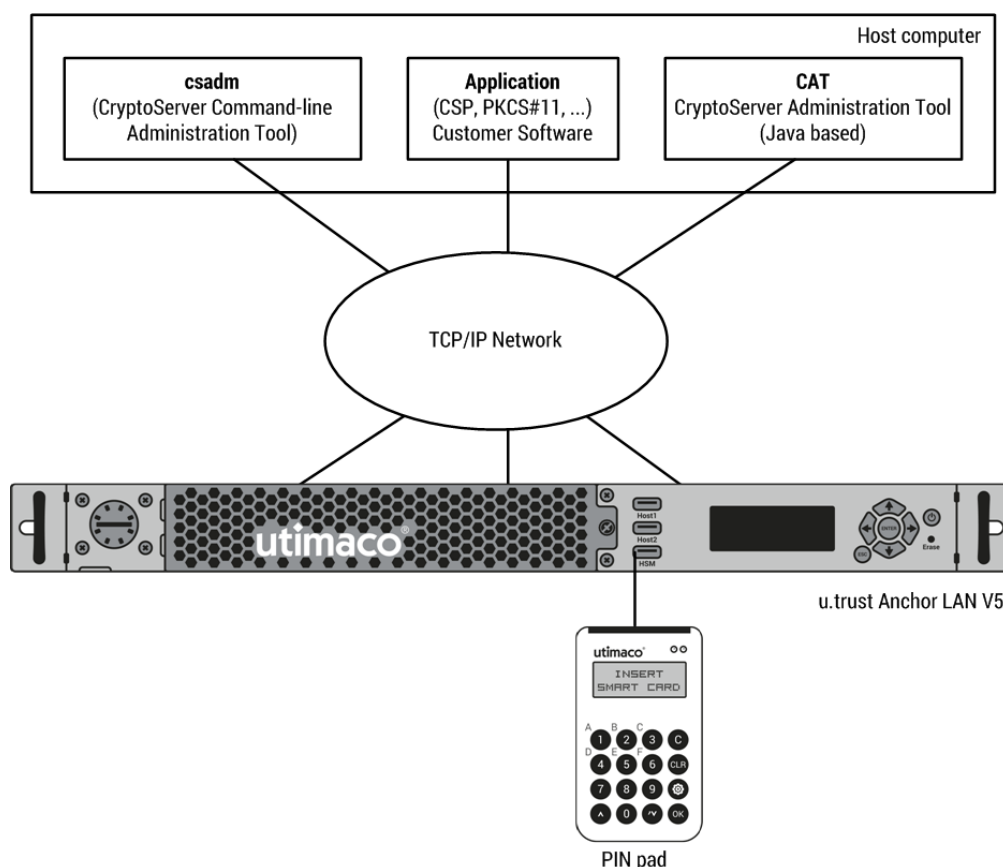


Figure 1 : Example for a u.trust Anchor LAN implementation environment

The u.trust Anchor LAN V5 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](#) in the product bundle in the directory `\Documentation\Product Details`.

2.1 Administration

You can choose between administering the u.trust Anchor LAN or the u.trust Anchor PCIe card.



Please note that CAT is not available at this time for the current version of the product.

Methods to administer the u.trust Anchor LAN:

- **Local administration via the u.trust Anchor LAN menu options**
On the front panel of the u.trust Anchor 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**
The devices need to be directly connected to the u.trust Anchor LAN.
- **Remote administration via an SSH connection**
For example under Windows with PuTTY, see [Logging in Remotely to the u.trust Anchor LAN](#).
- **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.

Methods to administer the u.trust Anchor PCIe card in the u.trust Anchor LAN:

- **Remote administration with the CryptoServer Administration Tool (CAT)**
The CAT is a Java application installed on the host computer that can only be used to administer the u.trust Anchor PCIe card. It is provided in the product bundle and is installed automatically if you select *Default installation* as the Installation type when installing the CryptoServer, see the [CryptoServer - Administration Manual](#). For a description of the CAT, see the [CryptoServer - CAT Manual](#).
- **Remote administration with the command-line Administration tool (csadm)**
Installed on a host computer.

- **Local administration via the u.trust Anchor LAN menu options mentioned above**
To enable this, a PIN pad and smartcards are included in the u.trust Anchor LAN deliverables, see 2021-0006 Connecting the PIN Pad for details on how to connect the PIN pad depending on your u.trust Anchor LAN hardware version, PIN pad model and administration task to be performed.

2.2 u.trust Anchor LAN System Users

There are two system user: user `root` , who has access to all administrative functions and a user, `csagent` , who has no privileges but is used to avoid direct SSH login as `root` . It can be used for monitoring purposes, but cannot perform administrative functions.

2.3 Transferring Files to or from the u.trust Anchor LAN

You may sometimes need to transfer files to the u.trust Anchor LAN, for example to update the CSLAN operating system (also referred to as CSLANOS below) in all or only a single u.trust Anchor 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 u.trust Anchor LAN which has no access to the mounted u.trust Anchor. Connect the USB flash drive to the Host1 or Host2 USB port (f4) on the front panel of the u.trust Anchor 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 u.trust Anchor LAN and can be selected for upload.



u.trust Anchor 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 u.trust Anchor LAN, the USB device that has been inserted as first gets connected with the u.trust Anchor 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 u.trust Anchor LAN.

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

The u.trust Anchor 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.

2.4 Authenticating Commands

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



If you have changed this user authentication key in the u.trust Anchor, 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 u.trust Anchor LAN or to the USB port on the u.trust Anchor PCIe card (a10) on the rear side of the u.trust Anchor LAN.



Figure 3 : Front view of the device

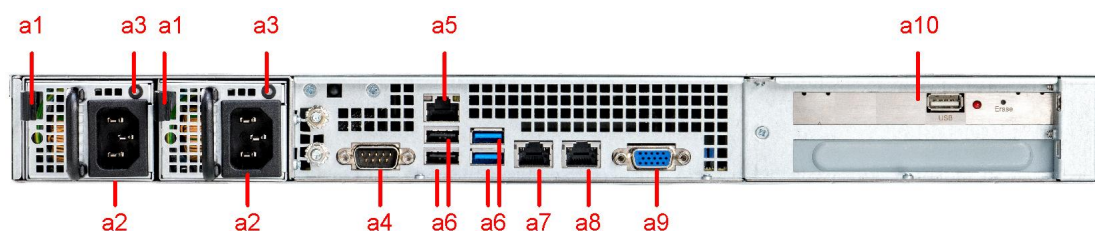


Figure 4 : Rear View

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

2.5 Boot Partitions in the u.trust Anchor LAN

The u.trust Anchor LAN has three boot partitions:

- factory
- user1
- user2

The boot partition user1 is started when the u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor LAN, please read section [Updating the Operating System](#).

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.

So called *Agents* (programs) are used to monitor the devices they are running on. 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.

u.trust Anchor LAN supports SNMPv2c and v3. In the u.trust Anchor LAN, SNMP is disabled by default.

2.7 The Internet Protocol Version 6 (IPv6)

You can assign an IPv4 and an IPv6 address for every network connection of the u.trust Anchor 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 u.trust Anchor V5's IPMI port.

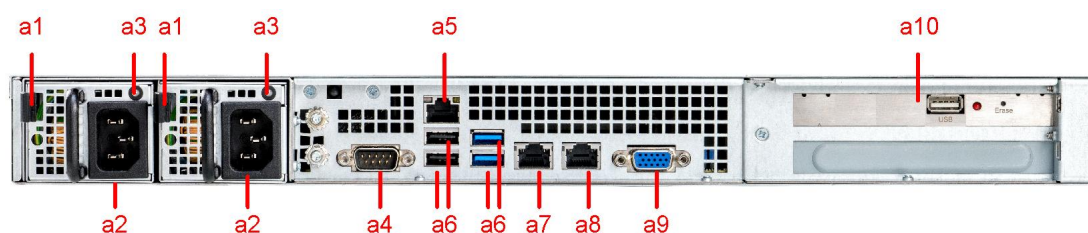


Figure 5 : Rear View

3 Bringing the u.trust Anchor LAN into Operation

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

The accompanying operating guidelines tell you how to integrate u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor into operation by using the menu options on the front panel of the u.trust Anchor LAN.

3.1 Menu Options on the Front Panel of the u.trust Anchor LAN

For administrating the u.trust Anchor LAN a display (4 x 20 characters) and six buttons are available on the front panel of the u.trust Anchor LAN. You can use the buttons to access the u.trust Anchor LAN 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 u.trust Anchor LAN are organized in the following structure.

Menu Item	Description
CSLAN admin	Administration of the u.trust Anchor LAN (host)
_ Configuration	Configuration of the u.trust Anchor LAN (host)
_ Network IP4	IP v4 network configuration
_ eth0	Configuration of the eth0 interface
_ DHCP	Setting up Dynamic IPv4 Addresses With the Front Panel
_ Address	Entering a static IPv4 Address With the Front Panel
_ eth1	Configuration of the eth1 interface
_ DHCP	Setting up Dynamic IPv4 Addresses With the Front Panel
_ Address	Entering a static IPv4 Address With the Front Panel
_ eth2	Optional: Configuration of the eth2 interface
_ DHCP	Setting up Dynamic IPv4 Addresses With the Front Panel
_ Address	Entering a static IPv4 Address With the Front Panel
_ eth3	Optional: Configuration of the eth3 interface
_ DHCP	Setting up Dynamic IPv4 Addresses With the Front Panel
_ Address	Entering the IPv4 Default Gateway With the Front Panel
_ Default gateway	Entering the IPv4 Default Gateway With the Front Panel
_ Services	Services running on the u.trust Anchor LAN
_ SSH	Enabling/Disabling the SSH Daemon
_ SNMP	Enabling SNMPv2c and SNMPv2c Traps for IPv4
_ IPTABLES	Restricting the Network Access on the CryptoServer LAN
_ NTP	Setting up NTP Primarily Using the Front Panel
_ NTP server IP addr.	Setting up NTP Primarily Using the Front Panel 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, see chapter Setting up PCIe Clock Cards for details.
_ CSLAN	u.trust Anchor LAN (host)

Menu Item	Description
_ Set time	See chapter Setting the Date and Time on the CryptoServer LAN . 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, see chapter Setting up PCIe Clock Cards for details.
_ Keyboard	Specifying the Keyboard Layout
_ CSLAN Info	Showing u.trust Anchor LAN Information
_ Show version	Showing the u.trust Anchor LAN Version and Serial Number
_ Show network state	Showing the Network State eth2 and eth3 are optional.
_ eth0	
_ eth1	
_ eth2	
_ eth3	
_ Routing	
_ Show services info	Showing the Services on the u.trust Anchor LAN
_ Show time info	Showing the Date and Time on the u.trust Anchor LAN
_ Show partition info	Showing the Partitions
_ Show fan info	Showing the Fan Speed
_ Show time source	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 and Setting up PCIe Clock Cards
_ Update & Maint.	Update and Maintenance
_ Update	Performing a Local Update
_ Set boot partition	Selecting a Boot Partition
_ Revert configuration	Reverting the Configuration of the u.trust Anchor LAN
_ Ping IP4 address	Verifying the Reachability in the Network (ping)
_ Reboot	Rebooting the u.trust Anchor LAN
_ Shutdown	Shutting down the u.trust Anchor LAN
HSM admin.	Administering the u.trust Anchor LAN
_ HSM Info	Showing u.trust Anchor Information
_ Version	Showing the Version
_ State	Showing the u.trust Anchor Status
_ Battery state	Showing the Battery State
_ Show time info	Showing the Date and Time on the u.trust Anchor

Table 3: Display menu structure

3.2 Switching on the u.trust Anchor LAN



Figure 7 : u.trust Anchor LAN V5 Front View

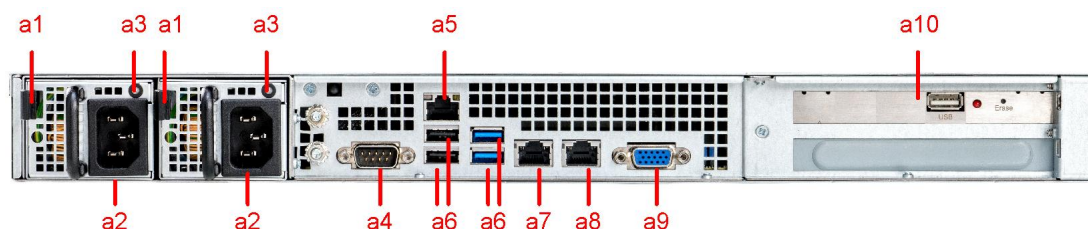


Figure 8 : Rear View



Pressing the u.trust Anchor LAN power switch is only necessary if automatic power on has been disabled in the BIOS.

1. Connect the power supply sockets on the rear side of u.trust Anchor LAN to a power supply using the cables supplied with the device.
2. Connect the **eth0** (a7) ethernet port on the rear side to your network with a twisted pair cable (RJ45).
3. Press the on/off switch on the front panel.
After a few seconds you will hear a short signal tone and the first messages are displayed. After approximately 90 seconds, the u.trust Anchor LAN is ready for use and alternating status information is displayed:

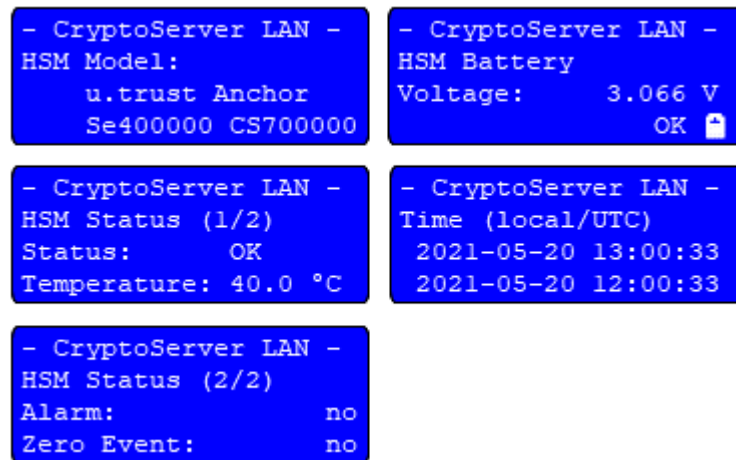


Figure 9 : Idle Screens

HSM Model: The u.trust Anchor model and the unique serial number of the u.trust Anchor PCIe card.

Temperature: The current temperature of the u.trust Anchor in °C.

HSM Battery: The voltage and the status of the carrier battery.

Time (local/UTC): The local time and the UTC (Coordinated Universal Time) of the u.trust Anchor LAN (not of the u.trust Anchor PCIe card).

4. Make sure that the second display shows **Status: OK**.



The u.trust Anchor LAN is switched on and ready for setup.



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

As of CSLANOS v5.1, pressing the ESC button let 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, see 2021-0006 Adding a Customer-Specific Screen to the Idle Screens.

3.3 Changing the Default Password of the System Users

Utimaco has already set the password for accessing the operating system CSLANOS as user `root` and user `csagent`.



We strongly recommend that you change the default password as soon as possible.

User = `root`, `csagent`

Password = `utimaco`

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

3.3.1 Changing the Default Password via an SSH Connection

To change the password for the user `root` user and the user `csagent` via an SSH connection from your administration computer, do as follows:

1. Log in remotely to the u.trust Anchor LAN, see [Logging in Remotely to the u.trust Anchor LAN](#).
2. To change the password for the user `root`, enter `passwd` and press **Enter**.
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.

3.3.2 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 u.trust Anchor LAN, proceed as follows:

1. Connect a keyboard to the **Host1** or **Host2** USB port on the front panel of the u.trust Anchor LAN.
2. Connect a monitor to the VGA connector on the rear side of the u.trust Anchor LAN.
3. Log in to the u.trust Anchor LAN:
 - a. Enter `csagent` as the **CryptoServer login** and press **Enter**.
 - b. As **Password**, enter `utimaco` and press **Enter**.
4. To change the password for the `root` or `csagent` user, enter `passwd` and press **Enter**.
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 u.trust Anchor LAN with the `exit` command.
8. Perform the exit command once more.
9. Disconnect the monitor and the keyboard from u.trust Anchor LAN.



The password has successfully been changed.

3.4 Setting up the IP Configuration

The u.trust Anchor LAN supports several networking features like IPv6 and bonding of network interfaces.

The u.trust Anchor 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.

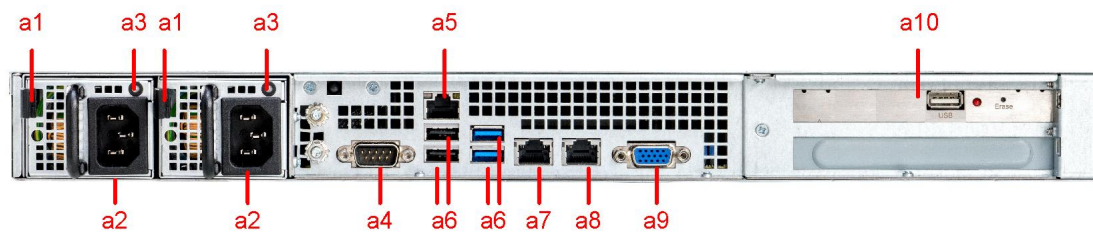


Figure 10 : Rear View

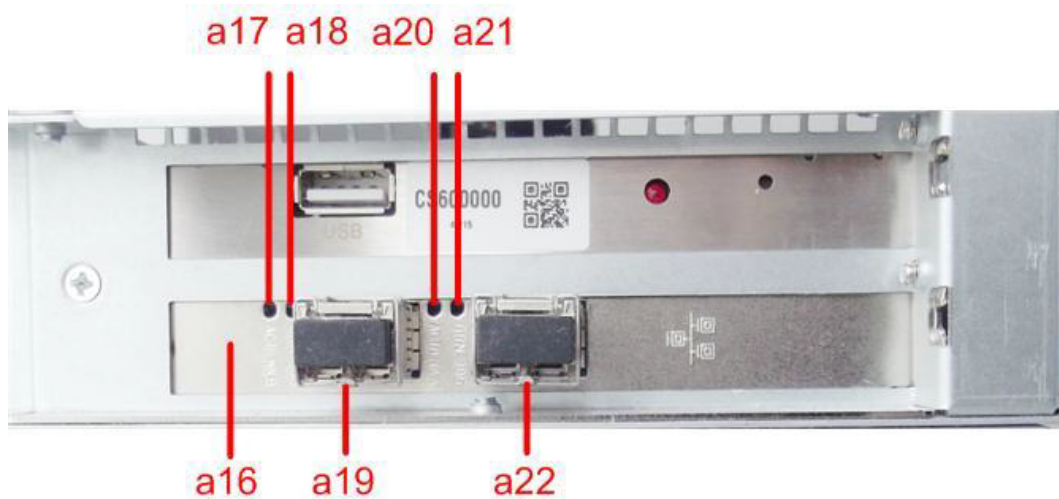


Figure 11 : Optional optical fiber network interface card on the rear side



Figure 12 : 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

Parameter	Description
DHCP_<x>	<p>DHCP for IPv4 addresses for eth<x>.</p> <ul style="list-style-type: none"> yes DHCP for IPv4 addresses is enabled for eth<x>. This assignment overrides any assignment for IP_ADDR_<x>. no DHCP for IPv4 addresses is disabled for eth<x>. This is the default value. It is used if DHCP_<x> is not configured.
DHCP_v6_<x>	<p>DHCP for IPv6 addresses for eth<x>.</p> <ul style="list-style-type: none"> yes DHCP for IPv6 addresses is enabled for eth<x>. This assignment overrides any assignment for IP_ADDR_v6_<x>. no DHCP for IPv6 addresses is disabled for eth<x>. This is the default value. It is used if DHCP_v6_<x> is not configured.
IP_ADDR_<x>	IPv4 address and prefix for eth<x>, for example, 192.168.1.111/24
IP_ADDR_v6_<x>	IPv6 address and prefix for eth<x>, for example, 2002::2/64
GATEWAY	IPv4 default gateway, for example, 192.168.1.1 Only one default gateway per protocol is supported.
GATEWAY_v6	IPv6 default gateway, for example, 2001::1 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 u.trust Anchor 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.


3.4.1 Setting up Static IP Addresses

3.4.1.1 Entering a static IPv4 Address With the Front Panel

You must assign an IP address to the u.trust Anchor LAN to ensure it can be accessed over the network. You must use the menu options on the u.trust Anchor 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 u.trust Anchor.
- Attach a monitor to the VGA port (a9 in Figure 15) of the u.trust Anchor LAN on the rear side.

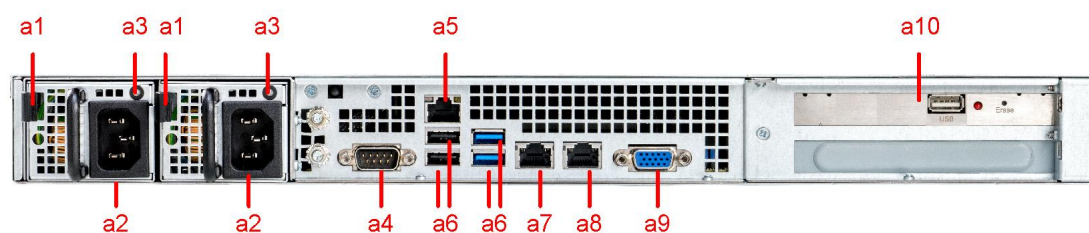


Figure 13 : Rear View

1. Switch on the CryptoServer LAN (f8).



Figure 14 : 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 u.trust Anchor LAN according to chapter [Logging in Remotely to the u.trust Anchor LAN](#).
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. See [Setting up the IP Configuration](#) for details.

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. See chapter [Setting up Bonding](#) for details.



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 u.trust Anchor LAN using a static IPv6 address or DHCPv6.

Step 1 to 8 are mandatory, the rest is optional

1. Switch on the u.trust Anchor LAN (f8).



Figure 15 : Front view of the device

2. Log in remotely to the u.trust Anchor LAN according to chapter [Logging in Remotely to the u.trust Anchor LAN](#).

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 `iptables` to limit access to all IPv6 services on the u.trust Anchor LAN by performing the instructions in chapter [iptables for IPv4](#) and [iptables for IPv6](#). Especially copy the `/etc/iptables.conf.example` file to the `/etc/iptables.conf` file and make it executable (`chmod +x /etc/iptables.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. See [Setting up Static IP Addresses](#) for details. 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/csxlان.conf` file according to your specific IPv6 configuration. You may set `IPv6_disable=0` or omit this option. See chapter [Configuring the csxlان.conf File](#) for details.
 15. To apply the changes, restart the csxlان 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 chapter [Setting up SNMP](#), especially in chapter [Enabling SNMP and SNMP Traps for IPv6](#).
 22. Follow the steps in chapter [Setting up NTP](#). Especially set the IPv6 address of the NTP server in the `/etc/ntp.conf` file.
 23. Reboot the u.trust Anchor LAN according to chapter [Rebooting the u.trust Anchor LAN](#) to ensure a correct boot process.



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

4 Administering the u.trust Anchor LAN

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

4.1 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.

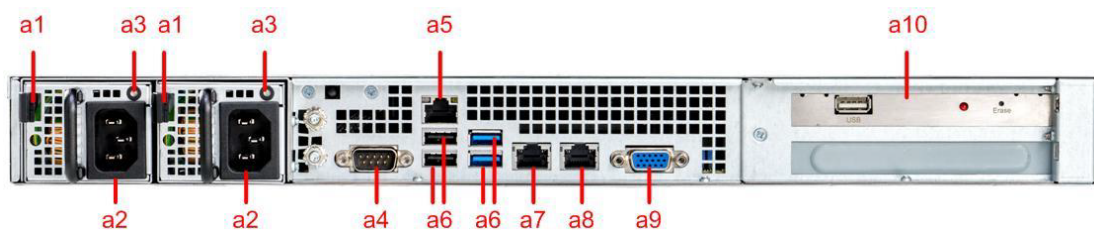


Figure 16 : Rear view of the device

3. Switch on the device (f8).



Figure 17 : 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.`

4.2 Logging in Remotely to the u.trust Anchor LAN

To log in remotely to the u.trust Anchor LAN. Perform the following steps to do so.



The Internet Protocols IPv4 and IPv6 are supported.

Prerequisites

- An IP address must have been assigned to the u.trust Anchor, see [Setting up the IP Configuration](#).
- The SSH daemon is enabled by default. If it has been disabled, enable it, see [Enabling/Disabling the SSH Daemon](#).

1. Start your SSH client (for example, PuTTY on Windows or ssh on Linux).
2. Log in to your u.trust Anchor LAN via SSH, for example, with the following access data:

Host name = <computer name/IP address of the u.trust Anchor LAN>

Port number = 22

User name = cslagent

Password = utimaco

3. Perform the following command to log in as the user `root`:

`su -`

4. Press the Enter key.
5. As **Password**, enter `utimaco` and confirm by pressing **Enter**.



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

4.3 Setting up SNMP

u.trust Anchor supports SNMPv2c and v3 (Simple Network Management Protocol).

4.3.1 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 u.trust Anchor, alarm status and other.



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

To enable SNMPv2c, follow these steps:

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 **↓** key to select **Services** and then press **ENTER**.
5. Use the **↓** Key to select **SNMP** and then press **ENTER**.
The currently applied setting (**disabled** or **enabled**) is indicated by a full circle.
6. Use the **↓** key to select **enabled** and press **ENTER**.
7. Use the **←** or the **→** key to insert the **x** in the **[x] Yes** brackets and press **ENTER** to confirm.



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

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 u.trust Anchor LAN according to chapter [Logging in Remotely to the u.trust Anchor LAN](#).
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 as well chapter [Configuring Multiple SNMP Trap Destinations](#).
5. Save the file after you have finished editing it.
6. Go to the `/etc/snmp` directory.
7. So that the u.trust Anchor 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.

See chapter [Configuring SNMP Traps](#) for important details about using the `[AllTraps]` trap and its influence on specific traps.

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 cronstab 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).

4.3.2 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 u.trust Anchor, alarm status and other.



Enabling SNMPv3 or SNMPv3 traps cannot be done by using the front panel of the u.trust Anchor LAN.

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

1. Log in remotely to the device according to chapter [Logging in Remotely to the u.trust Anchor LAN](#).
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
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 u.trust Anchor LAN, we highly recommend performing the changing and saving operations on the u.trust Anchor LAN itself. Do not perform the changes on a Windows computer and copy the changed file onto the u.trust Anchor 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
```

7. 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>EngineId 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.</p> <p>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 <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>

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
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). It is possible to configure multiple IP addresses. See chapter Configuring Multiple SNMP Trap Destinations for details.

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 u.trust Anchor sends the SNMP traps, a specific configuration file, `/etc/snmp/cslan_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.

See section [Configuring SNMP Traps](#) for details, especially for important details about using the `[AllTraps]` trap and its influence on specific traps.

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.

4.3.3 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 u.trust Anchor LAN according to chapter [Logging in Remotely to the u.trust Anchor LAN](#)
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/snmp.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 as well chapter [Configuring Multiple SNMP Trap Destinations..](#)
`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.

4.3.4 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 u.trust Anchor LAN according to chapter [Logging in Remotely to the u.trust Anchor LAN](#).
2. Open the configuration file specified above in a text editor
The configuration options for each individual u.trust Anchor trap are described in the following table:

<i>SNMP Trap name / Section</i>	<i>Parameter/Description</i>
[StateDevice]	device IP address of the u.trust Anchor 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>enable = 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>

SNMP Trap name / Section	Parameter/Description
[ModeChangeTrap]	<p>enabled This is where you enable or disable messages about a change of the operating mode of a u.trust Anchor in the u.trust Anchor 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"> • [AllTraps] enabled = yes has been set or • [AllTraps] enabled = configured and the default setting for HighTempTraps have been set, <p>messages about the temperature being too high are enabled. You can also configure the following parameter: threshold - u.trust Anchor high temperature threshold value Valid range: threshold: [-30, 100] and > [LowTempTraps] threshold Default: threshold = 50 delta - a value in °C for repeating the message Default: delta = 0 Setting delta = 0 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: threshold = 50, delta = 0 A single notifyCsTemperatureHigh trap is sent when the temperature rises to > 50°C. A single notifyCsTemperatureHighBack trap be sent when the temperature falls back to <= 50°C. Example 2: threshold = 50, delta = 5 The notifyCsTemperatureHigh trap is sent when the temperature rises to > 50°C, > 55°C, > 60°C, etc. The notifyCsTemperatureHighBack trap will be sent when the temperature falls back to <= 55°C, <= 50°C, <= 45°C.</p>

SNMP Trap name / Section	Parameter/Description
[LowTempTraps]	<p>enabled This is where you enable or disable messages about the temperature being too low.</p> <p><code>no</code> - LowTempTraps disabled <code>yes</code> (default) - LowTempTraps enabled</p> <p>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>LowTempTraps</code> have been set, <p>messages about the temperature being too low are enabled.</p> <p>You can also configure the following parameter:</p> <p><code>threshold</code> - u.trust Anchor low temperature threshold value Valid range: <code>threshold: [-30, 100]</code> and <code>></code></p> <p><code>[HighTempTraps] threshold</code> Default: <code>threshold = 10</code></p> <p><code>delta</code> - a value in °C for repeating the message Default: <code>delta = 0</code></p> <p>Setting <code>delta = 0</code> 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.</p> <p>Example 1: <code>threshold = 10, delta = 0</code> A single <code>notifyCsTemperatureLow</code> trap is sent when the temperature falls to <code>< 10°C</code>. A single <code>notifyCsTemperatureLowBack</code> trap is sent when the temperature rises back to <code>>= 10°C</code>.</p> <p>Example 2: <code>threshold = 10, delta = 5</code> The <code>notifyCsTemperatureLow</code> trap is sent when the temperature falls to <code>< 10°C, < 5°C, < 0°C</code>, etc. The <code>notifyCsTemperatureLowBack</code> trap is sent when the temperature rises back to <code>>= 5°C, >= 10°C, >= 15°C</code>.</p>

<i>SNMP Trap name / Section</i>	<i>Parameter/Description</i>
[BatteryTraps]	<p>enabled This is where you enable or disable messages about the battery status of the u.trust Anchor and u.trust Anchor 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 u.trust Anchor and u.trust Anchor LAN are enabled. If the BatteryTraps are enabled a BatteryTrap is generated and sent every time the status of the u.trust Anchor or u.trust Anchor 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 u.trust Anchor PCIe card. The workload is the ratio of the time that requests/commands spend in the u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor LAN connections. no - ClientsTraps disabled yes (default) - ClientsTraps enabled 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 u.trust Anchor LAN connections are enabled. 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. Example 1: <code>threshold = 75, delta = 0</code>: A single <code>notifyCslClientsHigh</code> trap is sent when the client connection load rises to > 75%. A single <code>notifyCslClientsHighBack</code> trap is sent when the client connection load falls back to <= 75%. 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 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>

SNMP Trap name / Section	Parameter/Description
[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, <p>messages about the speed of the cooler fan are enabled. 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</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 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.

4.3.5 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 u.trust Anchor LAN according to chapter [Logging in Remotely to the u.trust Anchor LAN](#).
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 user 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.

4.3.6 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 u.trust Anchor LAN.



If a PCIe clock card is mounted on the u.trust Anchor LAN (see chapter [Setting up PCIe Clock Cards](#)), the date and the time are set automatically and cannot be set manually.

1. On the front panel of the u.trust Anchor LAN, press **ENTER**.
2. Press **ENTER** to open the **CSLAN admin.** menu item.
3. Press **ENTER** to open the **Configuration** menu item.
4. Use the **↓** key to select **CSLAN** and press **ENTER**.
5. Press **ENTER** to open the **Set Time** menu item.
 On the display of the u.trust Anchor LAN, the local date and time of the u.trust Anchor LAN is displayed 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 **↓** keys. Press the **→** key to move the cursor to the next number.
 Only values up to December 31, 2037 can be set.
6. Press the **↑** / **↓** and **→** keys to set the new date and time and then press **ENTER**.
7. Use the **←** or the **→** key to move the **x** into the square brackets **[x] Yes** and confirm by pressing **ENTER**.



A message confirming that you have successfully configured the local time is displayed.

4.3.7 Specifying the Keyboard Layout

If you want to use a keyboard and a monitor to configure the u.trust Anchor LAN, you can specify the layout (language) of the keyboard you are going to connect. To change the keyboard layout do the following:

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



A message confirming that you have successfully configured the keyboard layout is displayed.

2. If you want to use a remote login, perform the following steps.
 - a. Log in remotely to the u.trust Anchor LAN, see [Logging in Remotely to the u.trust Anchor LAN](#).
 - b. Execute the following command to show the available keyboard layouts.

Example Output

```
# Begin /etc/keymap.lst
Belgium      /usr/share/keymaps/i386/azerty/be-latin1.map.gz
Bulgaria     /usr/share/keymaps/i386/qwerty/bg-cp855.map.gz
Finland      /usr/share/keymaps/i386/qwerty/fi.map.gz
```

```

France      /usr/share/keymaps/i386/azerty/fr-latin1.map.gz
Germany     /usr/share/keymaps/i386/qwertz/de-latin1-
nodeadkeys.map.gz
Italy       /usr/share/keymaps/i386/qwerty/it.map.gz
Netherlands /usr/share/keymaps/i386/qwerty/nl.map.gz
Norway      /usr/share/keymaps/i386/qwerty/no-latin1.map.gz
Portugal    /usr/share/keymaps/i386/qwerty/pt-latin1.map.gz
UK          /usr/share/keymaps/i386/qwerty/uk.map.gz
USA         /usr/share/keymaps/i386/qwerty/us.map.gz
# 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
```



A message confirming that you have successfully configured the keyboard layout is displayed. 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.

4.4 Showing u.trust Anchor LAN Information

You can show the version of the u.trust Anchor LAN software.

4.4.1 Showing the u.trust Anchor 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.

4.4.2 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.

4.4.3 Showing the Services on the u.trust Anchor 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.

4.4.4 Showing the Date and Time on the u.trust Anchor 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.

4.4.5 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.

4.4.6 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 18 : Front panel with removed fan compartment grill

4.4.7 Showing the PCIe Clock Card Information

You can display information about the PCIe clock card. See chapter [Setting up PCIe Clock Cards](#) for details about PCIe clock cards.



This menu item is only available if a PCIe clock card is mounted.

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 source** and press **ENTER** to open the menu item.

Example output:

```
Card:PZF180PEX DCF77
```

```
Clock: Synchronized
```

```
Signal: 100 %
```



The PCIe clock card information is displayed.

4.5 Changing the Default Hostname of the u.trust Anchor 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.

4.6 Update and Maintenance

4.6.1 Updating the Operating System

Utimaco IS GmbH supplies updates for the operating system of the u.trust Anchor LAN 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 u.trust Anchor LAN operating system. `cslan-x.y.z.tar.gz` can be imported into the u.trust Anchor LAN from a USB flash drive directly connected to the u.trust Anchor LAN ([Performing a Local Update](#)) or remotely via SSH connection ([Performing a Remote Update](#)). After the import, `cslan-x.y.z.tar.gz` is automatically unpacked and saved in the u.trust Anchor LAN.

An update can only be performed from one boot partition to one of the others. For further details about the boot partitions of the u.trust Anchor LAN please read [Boot Partitions in the u.trust Anchor LAN](#).



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.

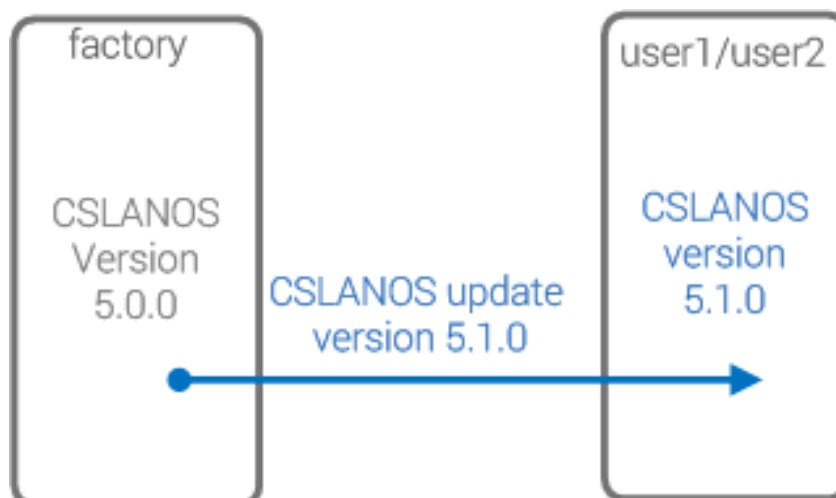


Figure 19 : Updating the operating system CSLANOS in user1 or user2 from the factory boot partition

- 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.

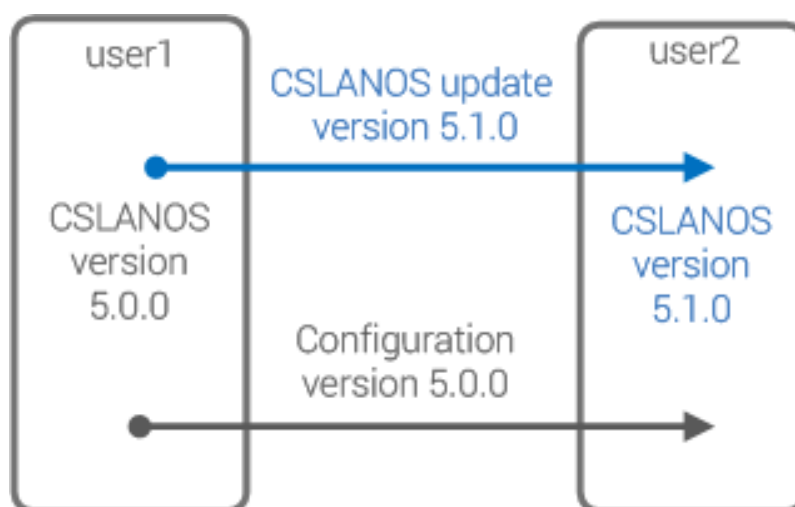


Figure 20 : Updating the operating system CSLANOS in boot partition user2

- 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.

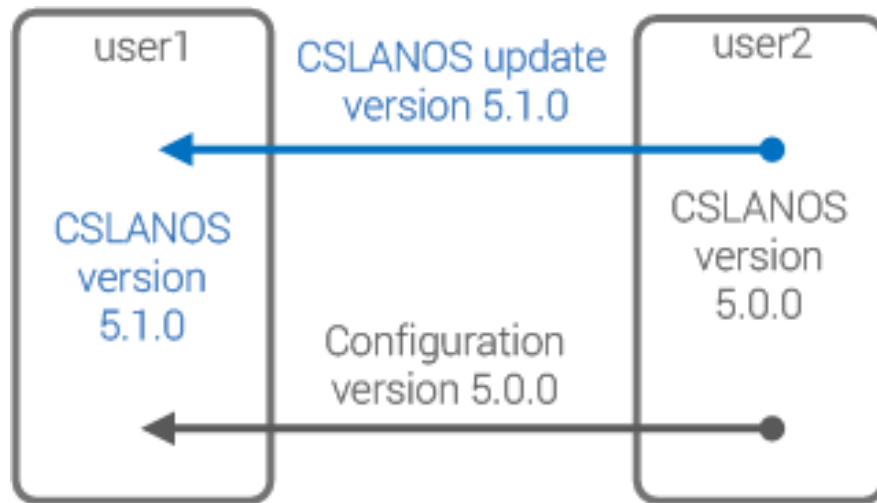


Figure 21 : Updating the operating system CSLANOS in boot partition user1

4.6.1.1 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 `cs1an-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.

- Use the ↑ and ↓ keys to move to the boot partition you want to use after a restart and confirm your selection by pressing **ENTER**.
 - Press **ESC** twice to get to the **CSLAN admin.** menu.
- Remove the USB flash drive from the **Host1** or **Host2 USB** port on the front panel of your device.
 - Reboot the device so you can start using the selected boot partition.
 - Use the ↓ key to select **Reboot** and press **ENTER** to open the menu item.
 - 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.
 - 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.

4.6.1.2 Performing a Remote Update

If you do not have a direct/local access to the device, you can also update the operating system of the device 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 bundle or boot stick).

- You have enabled the SSH daemon locally by using the control menu buttons of the device as described in section [Setting up Dynamic IPv4 Addresses With the Front Panel](#).
- You have booted the appropriate boot partition of the device locally as explained in section [Selecting a Boot Partition](#) or remote by using SSH access and command line `set_boot.sh <boot partition>` and rebooting the device 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 device remotely, proceed as follows:

1. Log in remotely to the device according to section [Logging in Remotely to the u.trust Anchor LAN](#).
2. Copy the `cslan-x.y.z.tar.gz` to the device 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 device:
`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 device has been installed.



The remote update has been performed successfully.

4.6.2 Selecting a Boot Partition

This section describes how to use the menu options to select the u.trust Anchor's boot partition, see [Boot Partitions in the u.trust Anchor LAN](#) for details.



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

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 **Update & Maint.** and press **ENTER**.
4. Use the **↓** key to select **Set boot partition** and press **ENTER**.
The currently applied setting (**factory**, **user1** or **user2**) is indicated by a full circle.
5. Use the **↓** key to select the desired entry and press **ENTER**.
6. Use the **←** or the **→** key to insert the **x** in the brackets **[x] Yes** and press **ENTER**.
7. Press **ESC** to leave the **Update & Maint.** menu and go to the **CSLAN admin.** menu.
8. Reboot the device in order to start using the selected boot partition.
 - a. Use the **↓** key to select **Reboot** and press **ENTER**.
 - b. Use the **←** or the **→** key to insert the **x** in the brackets **[x] Yes** and press **ENTER**.
 - c. The device restarts and boots from the boot partition you have just selected.



The boot partition has been selected and applied successfully.

4.6.3 Reverting the Configuration of the u.trust Anchor LAN

Resetting the configuration of the u.trust Anchor LAN means to reset the entire configuration in a particular boot partition. All settings you have made in this boot partition will be deleted.

Prerequisites

Before you can reset the u.trust Anchor LAN configuration in a particular boot partition you may need to select the boot partition you require, see [Selecting a Boot Partition](#).

To reset the configuration of the u.trust Anchor LAN in a specific boot partition, follow these steps:

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 **Update & Maint.** and press **ENTER** to open the menu item.
4. Use the **↓** key to select **Revert configuration** and press **ENTER**.
5. Respond to the prompt **Really revert 'factory' | 'user1' | 'user2'** by pressing the **←** or the **→** key to insert the **x** in the brackets **[x] Yes** and then press **ENTER**.
6. Reboot the device, see [Rebooting the u.trust Anchor LAN](#), to reset the configuration.



The u.trust Anchor LAN was reset to the standard configuration upon delivery by Utimaco.



Change the default password for the root user according to chapter [Changing the Default Password of the System Users](#).

Make sure that you have booted the same boot partition as the one you have reverted to default configuration.

4.6.4 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.

4.7 Rebooting the u.trust Anchor LAN

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

There are the following options to reboot the u.trust Anchor LAN:

- **Local command-line**

Execute the reboot command, see *Restarting the Device (device-restart)* in the *u.trust Anchor - Administration Manual*.

- **Remote command-line**

- a. Log in remotely to the u.trust Anchor LAN, see [Logging in Remotely to the u.trust Anchor LAN](#).
- b. Execute the reboot command.

- **Front panel**

- a. On the front panel of the device, press **ENTER**.
- b. Press **ENTER** to open the **CSLAN admin.** menu item.
- c. Use the ↓ key to select **Reboot** and press **ENTER**.
- d. Use the ← or the → key to insert the **x** in the brackets **[x] Yes** and press **ENTER**.



The device is rebooted.

4.8 Shutting down the u.trust Anchor LAN

There are the following options to shut down the u.trust Anchor LAN:

- **Local command-line**

Perform the following command.

```
shutdown -h now
```

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

- **Remote command-line**

- a. Log in remotely to the device, see [Logging in Remotely to the u.trust Anchor LAN](#)
- b. Execute the following command.

```
shutdown -h now
```

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

- **Front panel**

- a. On the front panel of the device, press **ENTER**.
- b. Press **ENTER** to open the **CSLAN admin.** menu item.
- c. Use the ↓ key to select **Shutdown** and press the → key to open the menu item.

- d. Use the ← or the → key to insert the **x** in the brackets **[x] Yes** and press **ENTER**.



The device shuts down after a few seconds.



The u.trust Anchor 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 depleted. After a while this can result in the u.trust Anchor 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.

4.9 Setting up PCIe Clock Cards

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



The u.trust Anchor 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 u.trust Anchor LAN manually and if this causes the time difference between the time on the u.trust Anchor 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 u.trust Anchor will not be set.

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

1. Switch off the device by pressing the f8 button.



Figure 22 : 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.

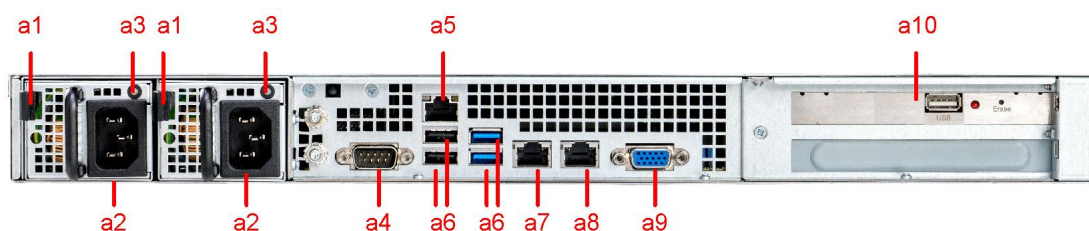


Figure 23 : Rear View



Figure 24 : PCIe Clock Card



Figure 25 : Sample for a DCF77 antenna with cable

3. Switch on the device 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 chapter [Showing the PCIe Clock Card Information](#).
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 chapter [Setting up NTP](#). Consider the differences described below.

The differences between a u.trust Anchor 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 chapter [Showing the PCIe Clock Card Information](#)

- **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 u.trust Anchor 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 u.trust Anchor LAN. To do so, first log in remotely to the u.trust Anchor LAN according to chapter [Logging in Remotely to the u.trust Anchor LAN](#). 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 u.trust Anchor LAN with PCIe clock card support, the NTP daemon is enabled by default. In contrast to the u.trust Anchor LAN versions without a PCIe clock card, ntpdate is not executed at the ntpd start because the given server IP address for the PCIe clock card is not accessible by ntpdate. 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
```

4.10 Setting up NTP

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

The following subchapters describe how to set up NTP for the u.trust Anchor.

4.10.1 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.

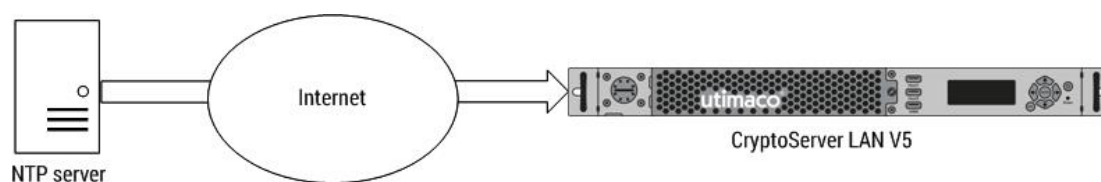


Figure 26 : Automatic time synchronization from an NTP server to the CryptoServer LAN



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 a 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 `ntdate`. Perform the `ntpcclient -h` command for the online help.

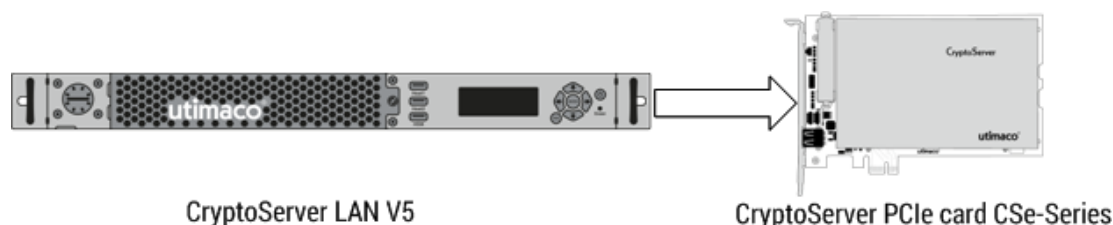


Figure 27 : Automatic time synchronization from the CryptoServer LAN to the CryptoServer PCIe card

The NTP client is configured in the `[NTPClient]` section in the `/etc/csylan.conf` file.

Prerequisites

- Unless you use a local command line on the u.trust Anchor, make sure that the SSH daemon has been enabled according to chapter [Enabling/Disabling the SSH Daemon](#). By default, the SSH daemon is enabled. A remote or local command line is needed in any case for performing certain commands on the u.trust Anchor LAN.
- Clarify whether you perform some steps with physical local access to the u.trust Anchor LAN by using the front panel of the u.trust Anchor LAN or whether you mainly use scripts. In the first case, continue with the instructions in chapter [Setting up NTP Primarily Using](#)

[the Front Panel](#). In the latter case, continue with chapter [Setting up NTP Primarily Using Scripts](#). The effect of the instructions in these chapters is identical.

4.10.2 Setting up NTP Primarily Using the Front Panel

To set up NTP, perform the following steps.



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

1. PCIe clock cards providing a high-precision time signal received by radio are supported. See chapter [Setting up PCIe Clock Cards](#) for details. If no PCIe clock card is mounted, continue with step 2. To verify whether a PCIe clock card is mounted, go to **CSLAN admin. > CSLAN Info > Show services info > NTP IPv4** on the display of the front panel. If it shows `127.127.28.0`, a PCIe clock card is mounted. As an alternative, log in remotely to the u.trust Anchor LAN according to chapter [Logging in Remotely to the u.trust Anchor LAN](#) and verify whether the following line is included in the `/etc/ntp.conf` file:


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

 If it is, a PCIe clock card is mounted.
2. Configuring the NTP server's IP address
 - a. Press **ENTER** on the front panel of the device.
 - b. Press **ENTER** to select **CSLAN admin..**
 - c. Press **ENTER** to select **Configuration**.
 - d. Press the **↓** key to select **Services** and confirm by pressing **ENTER**.
 - e. Press the **↓** key 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 **ENTER**.
 - g. If you have assigned a valid IP address, respond to the prompt that follows with Yes, by pressing the ← or → key to insert the **x** in the 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**.
3. Starting the NTP daemon
- a. Press the **ENTER** button on the front panel of the u.trust Anchor LAN.
 - b. Press the **ENTER** button to select **CSLAN admin..**
 - c. Press the **ENTER** button to select **Configuration**.
 - d. Press the ↓ key to select **Services** and press **ENTER**.
 - e. Press the ↓ key to select **NTP** and press **ENTER**.
The currently applied setting (**disabled** or **enabled**) is indicated by a full circle.
 - f. Use the → key to select clock card and press **ENTER** to open the menu item.
 - g. Use the ← or the → key to move the **x** into the square brackets **[x] Yes** and press **ENTER**.
 - h. You see a system message that you have performed the configuration successfully. Confirm by pressing **ENTER**.



The NTP was successfully set up.

4.10.3 Setting up NTP Primarily Using Scripts

To set up NTP, perform the following steps.



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

1. The PCIe clock cards providing a high-precision time signal received by radio are supported. See Section [Setting up PCIe Clock Cards](#) for details.
If no PCIe clock card is mounted, continue with step 2.
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 u.trust Anchor LAN according to [Logging in Remotely to the u.trust Anchor LAN](#), 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.
2. 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. 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.
3. 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.



The NTP has been successfully set up.

4.10.4 Configuring Time Synchronization between the u.trust Anchor LAN and the u.trust Anchor PCIe Card

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

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 u.trust Anchor LAN. It is configured in the `/etc/csxlan.conf` file on the u.trust Anchor LAN. See the steps below to perform this configuration.

- `Deviation`

Time deviation in milliseconds between the u.trust Anchor LAN and the u.trust Anchor PCIe card for which the time on the u.trust Anchor PCIe card 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.

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

- `max_delta_per_op`

`max_delta_per_op` (maximum delta time per operation) specifies the maximum value in milliseconds permitted for the `Deviation` parameter. If the time difference between the time on the u.trust Anchor LAN and the time on the u.trust Anchor PCIe card is greater than `max_delta_per_op`, the time on the u.trust Anchor LAN is not transferred to the u.trust Anchor PCIe card but the time on the u.trust Anchor PCIe card is changed by `max_delta_per_op` milliseconds.

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

value.

`max_delta_per_op` is a parameter of the NTP firmware module on the u.trust Anchor PCIe card. It can only be configured by using the `gladm system-set-ntp-config` command.

- `max_delta_per_day`

If the per day accumulated time by which the u.trust Anchor PCIe card time has been corrected, is greater than `max_delta_per_day`, the time on the u.trust Anchor LAN is not transferred to the u.trust Anchor PCIe card but the time on the u.trust Anchor PCIe card is changed by `max_delta_per_day` milliseconds.

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

`max_delta_per_day` is a parameter of the NTP firmware module on the u.trust Anchor PCIe card. It can only be configured by using the `gladm system-set-ntp-config` command.

- `ntp_enabled`

`ntp_enabled` activates or deactivates the NTP configuration of the NTP firmware module on the u.trust Anchor PCIe card. `ntp_enabled` can be configured by using the `gladm system-set-ntp-config` command. As an alternative, the `gladm system-activate-ntp` command can be used.

The default value is `true` (1). The other permitted value is `false` (0).

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

1. Log in remotely to the u.trust Anchor LAN, see *Logging in Remotely to the u.trust Anchor LAN* in the *u.trust Anchor LAN V5 - Administration Manual*.
2. Go 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 remote access to the u.trust Anchor 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.

4.11 Viewing NTP Log Entries

All log entries or error messages relating to the NTP daemon 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 device according to chapter [Logging in Remotely to the u.trust Anchor LAN](#).
2. Go to the `/var/log` directory and open the `syslog` file in a text editor.
3. Look for these entry: `ntpd`
4. Close the `syslog` file and shut down your SSH client.



The NTP log entries are being displayed.

4.12 Changing the Time Zone for the u.trust Anchor LAN

Perform the following steps to change the time zone:

1. Log in remotely to the u.trust Anchor LAN according to section [Logging in Remotely to the u.trust Anchor LAN](#).
2. Getting the time on the u.trust Anchor LAN (optional).
Perform the `date` command in the command line.
3. Enter the `tzconfig` command in your 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.

4.13 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 " .

<i>Parameter</i>	<i>Description</i>
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"
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.

4.14 Using IPMI

4.14.1 Accessing the CryptoServer LAN

1. Log in remotely to the CryptoServer LAN, see [Logging in Remotely to the u.trust Anchor LAN](#).

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
```

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

Commands:

<code>raw</code>	Send a RAW IPMI request and print response
<code>i2c</code>	Send an I2C Master Write-Read command and print response
<code>spd</code>	Print SPD info from remote I2C device
<code>lan</code>	Configure LAN Channels chassis Get chassis status and set power
<code>state</code>	
<code>power</code>	Shortcut to chassis power commands event Send pre-defined events
<code>to MC</code>	
<code>mc</code>	Management Controller status and global enables
<code>sdr</code>	Print Sensor Data Repository entries and readings
<code>sensor</code>	Print detailed sensor information
<code>fru</code>	Print built-in FRU and scan SDR for FRU locators
<code>gendev</code>	Read/Write Device associated with Generic Device locators sdr
<code>sel</code>	Print System Event Log (SEL) pef Configure Platform Event
Filtering (PEF)	
<code>sol</code>	Configure and connect IPMIv2.0 Serial-over-LAN
<code>tsol</code>	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
kontronoe	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

4.14.2 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
PW Consumption	5.000	Watts	ok	na	na	na	na	na

4.14.3 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
```

4.14.4 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

```

4.14.5 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

```

4.14.6 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.

4.14.7 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.

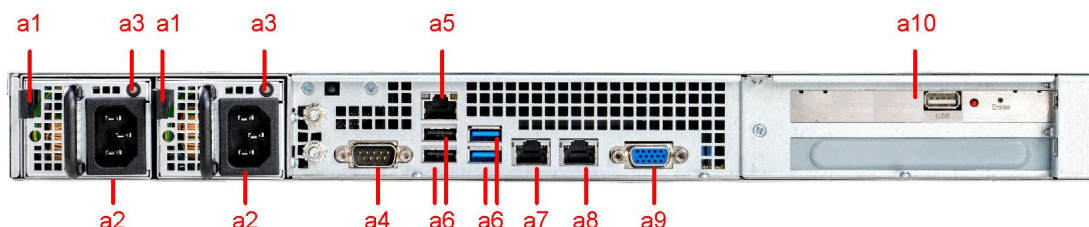


Figure 28 : Rear View

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.

4.14.8 Changing the Default IPMI Interface Configuration

4.14.8.1 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.

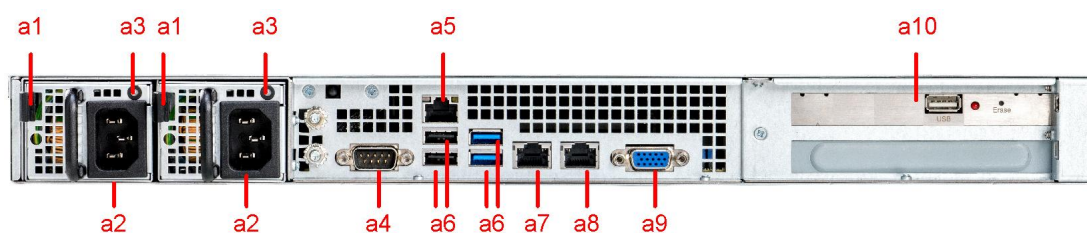


Figure 29 : Rear View

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 [Logging in Remotely to the u.trust Anchor LAN](#).

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
```

4. Verify the current interface configuration by performing the `ipmitool lan print` command. For details, see [Showing LAN Information](#).
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.

4.14.8.2 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 u.trust Anchor LAN since it may conflict with the internal use of IPMI for the u.trust Anchor 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](#) 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 u.trust Anchor 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.

4.15 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 u.trust Anchor

You can use the menu options on the front panel of the u.trust Anchor LAN to administrate the u.trust Anchor (PCIe card) mounted within the u.trust Anchor LAN. The available administration options are described here.

5.1 Showing u.trust Anchor Information

5.1.1 Symbols on the display

The following symbols are used on the display of the u.trust Anchor LAN.

<i>Symbol</i>	<i>Description</i>
Full battery	Sufficient voltage in the external battery
Low battery	Low voltage in the external battery. Exchange it according to the Chapter “ <i>Replacing the External Battery</i> ” in [CSLAN5-OM] . See Chapter “ <i>Power Supply Monitoring</i> ” in [CSMSADM] for details about voltage threshold values.
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 10: Symbols on the display

5.1.2 Showing the Version

1. On the front panel of the u.trust Anchor LAN, 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 **Version** and press **ENTER**.



Version information of the built-in PCIe card is displayed,

Example Output

```
HSM Model:
  u.trust Anchor
  Se40000
Serial Number:
  CS700000
SW Version:
  1.16
```

The HSM model number differs from this example, based on the model you purchased. The display can only show three lines at a time. Use the ↑ and the ↓ keys to scroll up and down.

5.1.3 Showing the u.trust Anchor Status

1. On the front panel of the u.trust Anchor LAN, 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 **State** and press **ENTER**.



Status information of the built-in PCIe card is displayed,

Example Output

```
Status:      OK
Alarm:       no      clarification of terms (not part of the displayed text)
Zero Event:  no -> Zero Event - gladm System Clear or External Erase
Glad State:  OK -> Global administration application
CM State:    OK -> Container Manager
UDS State:   OK -> Update Service
TRNG State:  OK -> True Random Number Generator
XRS State:   OK -> Crypto Acceleration service
Temperature: 44.5 C
```

The display can only show three lines at a time. Use the ↑ and the ↓ keys to scroll up and down.

5.1.4 Showing the Battery State

1. On the front panel of the u.trust Anchor LAN, 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 **Battery state** and press **ENTER**.

Example Output

```
Carrier battery:
  State   = OK [battery symbol]
  voltage = 2.920 V
External battery:
  State   = OK [battery symbol]
  Voltage = 3.220 V
```

The display can only show three lines at a time. Use the ↑ and the ↓ keys to scroll up and down.

Status and voltage (in V) of the carrier battery and the external battery are displayed. The carrier battery is mounted on the u.trust Anchor PCIe card. The external battery is mounted in the u.trust Anchor LAN. Both batteries supply power to the u.trust Anchor PCIe card in the u.trust Anchor LAN.



If the system cannot determine the battery status, because the u.trust Anchor register is currently being accessed by another process, you should try to determine the battery state again after a few minutes.



The battery power level shown on the display of the u.trust Anchor LAN is not updated very frequently. Therefore, after replacing the External Battery we recommend to wait for at least three minutes before checking the battery state.

5.1.5 Showing the Date and Time on the u.trust Anchor

To display the u.trust Anchor's date and time on the u.trust Anchor LAN display:

1. On the front panel of the u.trust Anchor LAN, 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 time info** and press **ENTER**.



UTC date and time and the local time zone with date and time are displayed.

Example Output

```
Date(UTC): 2021-03-15
Time(UTC): 13:20:32
Timezone : +0100
Date(Loc): 2021-03-15
Time(Loc): 14:20:38
```

The display can only show three lines at a time. Use the ↑ and the ↓ keys to scroll up and down.

6 Advanced Administration on the u.trust Anchor LAN

This chapter describes advanced administration functions for the u.trust Anchor LAN. None of the administration tasks detailed in this chapter can be performed using the menu options on the u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor 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 enter the current password.



If you want to change and save a configuration file on the remote u.trust Anchor LAN, we highly recommend to perform the changing and saving operations on the u.trust Anchor LAN itself. Do not perform the changes on a Windows computer and copy the changed file onto the u.trust Anchor 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:

Parameter	Description
Speed	Possible values: [10, 100, 1000] Sets the network interface speed in MBit/s.

<i>Parameter</i>	<i>Description</i>
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 11: 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 TLS for u.trust Anchor LAN

- TLS peers: client tools and u.trust Anchor LAN daemon
- Only TLS 1.3 is supported
- Certificates and keys in PEM format
- Client configuration with environment variables
- Client uses `TLS` specifier instead of `TCP`



TLS is only supported for Linux Clients.

The TLS implementation for u.trust Anchor LAN allows the client tool `csadm` to connect to u.trust Anchor LAN over TLS and access the cHSM instances.

Only TLS 1.3 is supported. All other connection attempts will be rejected.

On client and server side certificates and keys in PEM format are used.

To use TLS, configuration on the server (u.trust Anchor LAN) and client-side is necessary:

- On the server side, the TLS-specific variables must be added to the configuration file `csxlan.conf`, see 2021-0006 The Configuration File `csxlan.conf`. The file can be found in `/etc/csxlan.conf`.
- On the client side, certain environment variables must be set in the command shell in which the client tool is executed, to use the desired certificates and keys to connect, see [Environment variables on client side](#).

Selecting TLS is done by extending commands with a `TLS` specifier on the client side, see *TLS connection to u.trust Anchor LAN* in the *u.trust Anchor - csadm Manual*.

csadm example

```
csadm dev=TLS:4001@192.168.1.1 GetState
```


For an example of configuring TLS, see [How to configure TLS](#).

6.2.1 Configure TLS for u.trust Anchor LAN

You need to do the configuration in the file `/etc/csxlan.conf`, see 2021-0006 The Configuration File `csxlan.conf`.

The easiest way to configure TLS on the server side for the connection between client tools and u.trust Anchor LAN is to specify the necessary setting in the global section `[Csxlan]` of the configuration file `csxlan.conf`. This configuration is then used by all listeners/servers.



If you set TLS in the global sections `[Csxlan]`, TLS will be used for communication with all cHSMs (endpoints in appliance daemon).

If you add a specific listener configuration for a port in the `[Listener]` section, it takes precedence over the global configuration.

For example, you can set TLS in the global section and set "an exception" for port 4004 by specifying `ConnectionType = TCP` in its listener section.

TCP must then be used for port 4004 and TLS for all others.

The communication modes can be chosen as needed, for example, one listener can use TLS and another can use TCP.


6.2.1.1 Variables in the global section `[Csxlan]`

Variables	Description
ListenerConnType	<p>Defines cHSM listener/server connection types valid for all <code>[Listener]</code> sections that don't have their own connection type defined. The default - if not set - is TCP to be compatible with older versions. Possible values are:</p> <ul style="list-style-type: none"> ▪ TCP ▪ TLS <p>Example: <code>ListenerConnType = TLS</code></p>
TLSCaFile	<p>Defines path and filename to the bundle file which includes a CA (public) certificate chain. It is used when the listeners connection mode is TLS. Example: <code>TLSCaFile = /etc/CACert.pem</code></p>
TLSCertFile	<p>Defines path and filename to the listener/server certificate file. It is used when the listeners connection mode is TLS. Example: <code>TLSCertFile = /etc/HSMCert.pem</code></p>

Variables	Description
TLSKeyFile	Defines path and filename to the file that holds the listener/servers private key. It is used when the listeners connection mode is TLS: Example: <code>TLSKeyFile = /etc/HSMPrivkey.pem</code>
TLSPathLength	Defines the maximum path length (CA certificates and intermediate certificates) of a certificate verification chain for TLS according to the OpenSSL function <code>SSL_CTX_set_verify_depth(x)</code> . <i>The default is 5.</i> It determines the maximum number of certificates that can be between the end-entity and trust-anchor certificates, Example: <code>TLSPathLength = 10</code>

6.2.1.2 Variables in the [Listener] section


If you add a specific configuration for a port in the [Listener] section, it takes precedence over the global configuration.

Variables	Description
ConnectionType	<p>Defines cHSM listener connection type. The default - if not set - is TCP.</p> <hr/> <p> To use TCP, you must set it explicitly.</p> <hr/> <p>Possible values are:</p> <ul style="list-style-type: none"> ▪ TCP ▪ TLS <p>This overrides the global <code>ListenerConnType</code> setting for this listener. Example: <code>ConnectionType = TLS</code></p>
TLSCaFile	<p>Defines path and filename to the bundle file which includes a CA (public) certificate chain. It is used when the listeners connection mode is TLS. Example: <code>TLSCaFile = /etc/CACert.pem</code></p>
TLSCertFile	<p>Defines path and filename of the server certificate file. It is used when the listeners connection mode is TLS. Example: <code>TLSCertFile = /etc/HSMCert.pem</code></p>
TLSKeyFile	<p>Defines path and filename to the file that holds the servers private key. It is used when the listeners connection mode is TLS. Example: <code>TLSKeyFile = /etc/HSMPrivkey.pem</code></p>



You can also find a description of the variables in the `csxlan.examples` file on your u.trust Anchor LAN (`/etc/csxlan.example`).

6.2.1.3 Environment variables on client side

Variable	Description
TLS_CLIENT_CERT	Path to the file that holds the client certificate. Example: <code>export TLS_CLIENT_CERT=/UTI/SE5K/MTLS/HostCert.pem</code>
TLS_CLIENT_PWD	Optional password for encrypted client certificate. Example: <code>export TLS_CLIENT_PWD=my_password</code>
TLS_CLIENT_KEY	Path to the file which holds the client private key. Example: <code>export TLS_CLIENT_KEY=/UTI/SE5K/MTLS/HostPrivkey.pem</code>
TLS_CA_BUNDLE	Path to the file which holds the CA certificate chain. Example: <code>export TLS_CA_BUNDLE=/UTI/SE5K/MTLS/CACert.pem</code>
TLS_SKIP_DN_VERIFY	<p>If set it skips the domain name verification. The domain name of the server is compared to the DN or alternative subject name in the server certificate. Example: <code>export TLS_SKIP_DN_VERIFY=1</code></p> <div>  <p>Only use this functionality for a limited time for testing purposes or for troubleshooting.</p> </div>
TLS_VERBOSE	Show more output in case of errors. Example: <code>export TLS_VERBOSE=1</code>
TLS_DEBUG	Show maximum output for problem analysis. Example: <code>export TLS_DEBUG=1</code>



`TLS_VERBOSE` and `TLS_DEBUG` are only available on the client side. `TLS_VERBOSE` provides the ability to better see errors on the client side. With `TLS_DEBUG` you can analyze problems even more precisely.

These options are not available on the u.trust Anchor LAN side. There errors are always written to the `csxlan.log` file.

6.2.2 How to configure TLS

The following chapter uses an example with OpenSSL to show all the steps necessary for configuring TLS from generating the required keys to adjusting the configuration files and testing the connection.

6.2.2.1 Install OpenSSL >3.0

```
sudo apt install build-essential checkinstall zlib1g-dev -y
```

```
sudo wget https://github.com/openssl/openssl/releases/download/openssl-3.0.8/openssl-3.0.8.tar.gz
```

```
sudo tar xvf openssl-3.0.8.tar.gz
```

```
cd openssl-3.0*/
```

```
./config
```

Output

```
*****
***                                     ***
***  OpenSSL has been successfully configured                                     ***
***                                     ***
***  If you encounter a problem while building, please open an                 ***
***  issue on GitHub <https://github.com/openssl/openssl/issues>               ***
***  and include the output from the following command:                         ***
***                                     ***
***      perl configdata.pm --dump                                              ***
***                                     ***
***  (If you are new to OpenSSL, you might want to consult the                 ***
***  'Troubleshooting' section in the INSTALL.md file first)                   ***
***                                     ***
*****
```

Build the package

```
make
```

Run tests

```
make test
```

Install OpenSSL

```
make install
```

Update links and caches

```
ldconfig
```

Update links and caches

```
ldconfig /usr/local/lib64/
```

Create a file (or alternatively update PATH in your .bashrc)

```
tee /etc/profile.d/openssl.sh<<EOF
export PATH=/usr/local/openssl/bin:SPATH
export LD_LIBRARY_PATH=/usr/local/openssl/lib:SLD_LIBRARY_PATH
EOF
```

Reload your shell

```
source /etc/profile.d/openssl.sh
```

Check your version

```
openssl version
OpenSSL 3.0.8 7 Feb 2023 (Library: OpenSSL 3.0.8 7 Feb 2023)
```

Ouput

```
OpenSSL 3.0.8 7 Feb 2023 (Library: OpenSSL 3.0.8 7 Feb 2023)
```

Create a CA

Generate a CA private key

```
openssl.exe genrsa -out CAPrivkey.pem 2048
```

Generate a CSR from your private key

```
openssl req -key CAPrivkey.pem -new -sha256 -out CAcsr.pem
```

Generate SelfSigned CA from private key

```
openssl req -x509 -sha256 -new -nodes -key CAPrivkey.pem -days 3650 -out  
CACert.pem
```

6.2.2.2 Create HSM's Certificates and keys

Generate a HSM private key

```
openssl genrsa -out HSMPrivkey.pem 2048
```

Generate a CSR from your HSM private key

```
openssl req -key HSMPrivkey.pem -new -sha256 -out HSMcsr.pem
```

Sign your certificate with CA

```
openssl x509 -req -in HSMcsr.pem -CA CACert.pem -CAkey CAPrivkey.pem -  
set_serial 01 -days 30 -outform pem -out HSMCert.pem
```

6.2.2.3 Create HOST's Certificate and keys

Generate a Host private key

```
openssl genrsa -out HostPrivkey.pem 2048
```


Generate a csr from your HSM private key

```
openssl req -key HostPrivkey.pem -new -sha256 -out Hostcsr.pem
```

Sign your certificate with CA

```
openssl x509 -req -in Hostcsr.pem -CA CACert.pem -CAkey CAPrivkey.pem -  
set_serial 01 -days 30 -outform pem -out HostCert.pem
```

6.2.2.4 Update CSXLAN.CONF in section [csxlan]

```
ListenerConnType = TLS  
TLSCaFile = /etc/CACert.pem  
TLSCertFile = /etc/HSMCert.pem  
TLSKeyFile = /etc/HSMPrivkey.pem  
TLSPathLength = 10
```

Reboot the appliance

6.2.2.5 Host Side configuration

Add these lines into you /home directory in .bashrc

```
export TLS_CLIENT_CERT=/UTI/SE5K/MTLS/HostCert.pem  
export TLS_CLIENT_KEY=/UTI/SE5K/MTLS/HostPrivkey.pem  
export TLS_CA_BUNDLE=/UTI/SE5K/MTLS/CACert.pem  
export TLS_SKIP_DN_VERIFY=1  
export TLS_VERBOSE=1  
export TLS_DEBUG=1
```

Reload your shell

```
source /root/.bashrc
```

6.2.2.6 Test with csadm

```
csadm dev=4001@192.168.1.10 GetState  
  
Error B9010007  
CryptoServer API LINUX
```

```
timeout occurred
```

With TLS spezifier

```
csadm dev=TLS:4001@192.168.1.10 GetState
```

```
mode      = Operational Mode
state     = INITIALIZED (0x00100004)
temp      = ---
alarm     = OFF
bl_ver    = 7.00.0.0          (Model: u.trust Anchor cHSM)
hw_ver    = 7.00.0.0
uid       = 0b860301 b95f0443 |      _ C      |
adm1      = 5365356b 20202020 43533834 30303731 |Se5k   CS840071|
adm2      = 53656375 72697479 53657276 65720000 |SecurityServer |
adm3      = 342e3730 2e302e30 00000000 00000000 |4.70.0.0      |
```

6.3 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 u.trust Anchor LAN.

This configuration file is split into the sections `[Csxlan]`, `[CryptoServerGlad]`, `[ListenerGlad]`, `[CryptoServer]`, `[Listener]` and `[DisplayAdmin]`. Each section 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 sections 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, 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 step 4. <hr/> <p>All values but the <code>OFF</code> value can be overwritten until the next (re)start of the u.trust Anchor LAN using the <code>csadm CSLSetTraceLevel</code> command. See [ANCHOR_CSADM] for details about the <code>csadm CSLSetTraceLevel</code> command.</p> <p>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 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 u.trust Anchor 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 u.trust Anchor 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 enabled. 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.

Parameter	Description
AuthReset	Shows whether the <code>csadm Reset</code> , <code>csadm ResetToBL</code> and <code>csadm Restart</code> commands must be authenticated by the u.trust Anchor LAN root user. See [ANCHOR_CSADM] for details. No authentication is necessary if the commands were input using the menu options on the u.trust Anchor LAN. Example: <ul style="list-style-type: none"> <code>AuthReset = 0</code> No authentication <code>AuthReset = 1</code> Authentication required
MaxConnections	Number of concurrent cHSM connections. Default: 256 Example: <code>MaxConnections = 3000</code>
MaxConnectionsGlad	Number of concurrent glad connections (from gladm tool to typically port 4000). Default: 64 Example: <code>MaxConnectionsGlad = 3000</code>
MaxDataSizeGlad	Maximum payload (memory usage) for all gladm commands. Default: 157286400 (150 Mb) Example: <code>MaxDataSizeGlad = 157286400</code>
CryptoServerThreadClones	Number of worker threads to create per cHSM. This many requests will be submitted/queued to the device concurrently per cHSM. The maximum value is 3. Example: <code>CryptoServerThreadClones = 3</code>

Table 12: Variables in the [Csxlan] section of csxlan.conf

Variables for the [CryptoServerGlad] section

The `[CryptoServerGlad]` section defines a CryptoServerGlad instance (management instance) on a u.trust Anchor PCIe card.

Parameter	Description
Label	Label is used to connect an IP port to a CryptoServerGlad Example: Label = GladCS1
Device	Device node of a CryptoServer Example: Device = /dev/cs2.0.0
Timeout	Timeout in ms of the CryptoServer driver Example: Timeout = 30000

Table 13: Variables in the [CryptoServerGlad] section of csxlan.conf

Variables for the [ListenerGlad] section

The `[ListenerGlad]` section defines the listening sockets of the CSARD (CSAR daemon). Only one `[ListenerGlad]` section can be routed to one `[CryptoServerGlad]` section.

Parameter	Description
Address	IPv4 or IPv6 address of glad listening socket. Default: any device Example: Address = 1.2.3.4
Port	Number of listening port Example: Port = 4000
Keepalive	Enables or disables TCP keepalive data packets that search for interrupted connections. Keepalive = 0 means that TCP keepalive data packets are disabled Keepalive = 1 means TCP keepalive data packets are enabled.
Route_to	This mandatory option assigns the <code>[ListenerGlad]</code> section to the <code>[CryptoServerGlad]</code> section. The data you input here is the same as you input in the <code>[CryptoServerGlad]</code> section as the Label. Example: Route_to = GladCS1

Table 14: Variables in the [ListenerGlad] section of csxlan.conf

Variables for the [CryptoServer] section

The `[CryptoServer]` section defines a CryptoServer (cHSM) instance on a u.trust Anchor PCIe card.

Parameter	Description
Label	Unique ID for a cHSM in the u.trust Anchor LAN. <code>Label</code> is used to connect an IP port (<code>[Listener]</code> section) to a cHSM (<code>[CryptoServer]</code> section). Values: For example, <code>CSm</code> where $m=\{1, 2, 3, \dots, 32\}$. Example: <code>Label = CS1</code>
Device	device node of a CryptoServer (cHSM) (for example <code>/dev/cs2.0.m</code> where $m=\{1, 2, 3, \dots, 32\}$). Example: <code>Device = /dev/cs2.0.1</code>
Timeout	Timeout in ms of the CryptoServer driver Example: <code>Timeout = 30000</code>

Table 15: Variables in the `[CryptoServer]` section of `csxlan.conf`

Examples for [CryptoServer] sections in a csxlan.conf file

```
[CryptoServer]
Label = CS1
Timeout = 30000
Device = /dev/cs2.0.1
```

```
[CryptoServer]
Label = CS2
Timeout = 30000
Device = /dev/cs2.0.2
```

```
[CryptoServer]
Label = CS3
Timeout = 30000
Device = /dev/cs2.0.3
```

```
# ...
```

```
[CryptoServer]
Label = CS32
Timeout = 30000
Device = /dev/cs2.0.32
```

Variables for the [Listener] section

The [Listener] section defines the listening sockets for cHSMs or the control module. Add an additional localhost [Listener] section when the Address variable is set to a specific address.

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 IPv6_disable variable or the IPv4_disable variable in the [Csxlan] section has been set to 1, the IP_version variable in any [Listener] section becomes overridden.</p>
Address	<p>IPv4 or IPv6 address of cHSM listening socket. Default: Any device</p> <p>Example: 1.2.3.4</p>
Port	<p>Port name/number of the listening socket. If the value is CSL_CONTROL_PORT (port number = 288), this port is used for csadm CSL* commands, for example, csadm CSLGetVersion. In this case, the value of Route_to must be CSL.</p> <p>Examples:</p> <ul style="list-style-type: none"> Port = CSL_CONTROL_PORT Port = 4001 Port = 4002 Port = 4003
Keepalive	<p>Enables or disables TCP keepalive data packets that search for interrupted connections.</p> <p>Keepalive = 0 means that TCP keepalive data packets are disabled</p> <p>Keepalive = 1 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>

Parameter	Description
Route_to	<p>This mandatory option assigns the [Listener] section to a specific [CryptoServer] section. The data you input here is the same as you input in the [CryptoServer] section as the Label.</p> <p>However, if the value of Route_to is CSL, the endpoint is the control module of the u.trust Anchor LAN. In this case, the value of Port must be CSL_CONTROL_PORT.</p> <p>Examples:</p> <ul style="list-style-type: none"> ▪ Port = CSL ▪ Port = CS1 ▪ Port = CS2 ▪ Port = CS3

Table 16: Variables in the [Listener] section of csxlan.conf

Examples for [Listener] sections in a csxlan.conf file

```
[Listener]
# port of listening socket; used for csadm csl* requests (CSL_CONTROL_PORT = 288)
Port = CSL_CONTROL_PORT
Keepalive = 1
# label to endpoint; CSL is the control module of the u.trust Anchor LAN
Route_to = CSL
```

```
[Listener]
Port = 4001
Keepalive = 1
Route_to = CS1
```


```
[Listener]
Port = 4002
Keepalive = 1
Route_to = CS2
```

```
[Listener]
Port = 4003
Keepalive = 1
Route_to = CS3
```

```
# ...
```

```
[Listener]
Port = 4032
Keepalive = 1
Route_to = CS32
```

Variables for the [DisplayAdmin] section

<i>Parameter</i>	<i>Description</i>
LogLevel	<p>The log level supports the following values:</p> <ul style="list-style-type: none"> ▪ <code>OFF</code> – Stop producing messages, useful for benchmarks ▪ <code>ERROR</code> – Error conditions ▪ <code>WARNING</code> – Warning conditions ▪ <code>NOTICE</code> – Normal but significant condition. Default value. ▪ <code>INFO</code> – Informational ▪ <code>DEBUG</code> – 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. <p>For details, see Setting up fcron Jobs, step 4.</p> <hr/> <p>See Configuring the csxlan.conf File for how to use it.</p>

Parameter	Description
LogFacility	<p>The log facility supports the following values:</p> <ul style="list-style-type: none"> <code>local0</code> – Reserved for local use. <code>local1</code> – Reserved for local use. <code>local2</code> – Reserved for local use. <code>local3</code> – Reserved for local use. <code>local4</code> – Reserved for local use. <code>local5</code> – Reserved for local use. <code>local6</code> – Reserved for local use. <code>local7</code> – Reserved for local use. Default value. <p>See Configuring the csxlan.conf File for how to use it.</p>
Device	<p>Device name that is used for the communication between the display on the front panel of the u.trust Anchor LAN and the u.trust Anchor PCIe card.</p> <p>Value: <code>localhost</code></p>
Display	<p><code>Display</code> defines the display port of the u.trust Anchor LAN</p> <p>Example:</p> <pre>Display = /dev/ttyS0</pre>
PINPad	<p><code>PINPad</code> specifies which PIN pad is connected. <code>PINPad</code> is deprecated. The name has this format:</p> <pre>:<smartcard ID>:<PIN pad ID>:USB0</pre> <p>Example:</p> <pre>:cs2:auto:USB0</pre> <p>See "Storage and Specification of RSA and ECDSA Keys for Authentication" in [ANCHOR_CSADM] for details.</p>
OSUpdateDevice	<p><code>OSUpdateDevice</code> defines the device for firmware updates.</p> <p>Example:</p> <pre>OSUpdateDevice = /dev/sdb1</pre>
IdleWindowTitle	<p><code>IdleWindowTitle</code> defines the title line of all idle screens.</p> <p>Example:</p> <pre>IdleWindowTitle = "CryptoServer LAN"</pre> <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> <pre>MenuWindowTitle = "CSLAN menu"</pre> <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>See Adding a Customer-Specific Screen to the Idle Screens for details.</p> <p>The number of new lines of text is defined by the <code>CustomerValueCount</code> variable (default value: 3).</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"> ▪ <code>CustomerValueFileName = "/tmp/dspd_customer.val"</code> The file contains three (default value of the <code>CustomerValueCount</code> variable) lines of text to be shown on the display. ▪ <code>CustomerValueFileName = "/tmp/DspCompanyCustomLine*"</code> 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>Consider that files in the <code>/tmp</code> directory are removed after a reboot of the u.trust Anchor LAN.</p> <p>See Adding a Customer-Specific Screen to the Idle Screens for details.</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 3, and its maximum value is 6.</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>See Adding a Customer-Specific Screen to the Idle Screens for details.</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 u.trust Anchor 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 17: Variables in the [DisplayAdmin] 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.

6.4 Restricting the Network Access on the CryptoServer LAN

If you want to restrict the network access to the u.trust Anchor LAN and only want to permit specific network services (SSH etc.) to connect to the u.trust Anchor LAN, you shall use iptables.

6.4.1 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          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 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          icmp type 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
```


6.4.2 iptables for IPv6

Chapter [iptables for IPv4](#) 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 according to chapter [Setting up the IPv6 Configuration With a Command-Line](#), 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 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**.

- 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`

6.5 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`

6.5.1 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.

6.5.2 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/csxlان.log`.

Example:

```
local7.* -/var/log/csxlان.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).

6.5.3 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.

6.5.4 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/csxlان.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.

6.6 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.

6.7 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 30 : 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
<code>CSLAN.DATE_TIME_UTC</code>	Date and time of the UTC time on the u.trust Anchor LAN (not on the u.trust Anchor LAN card)
<code>CSLAN.DATE_UTC</code>	Date of the UTC time on the u.trust Anchor LAN (not on the u.trust Anchor LAN PCIe card)
<code>CSLAN.TIME_UTC</code>	UTC time on the u.trust Anchor LAN (not on the u.trust Anchor LAN PCIe card)
<code>CSLAN.TIMEZONE_OFS</code>	Timezone offset of the local time on the u.trust Anchor LAN (not on the u.trust Anchor LAN PCIe card) to UTC
<code>CSLAN.DATE_TIME_LOCAL</code>	Date and time of the UTC time on the u.trust Anchor LAN (not on the u.trust Anchor LAN PCIe card)
<code>CSLAN.DATE_LOCAL</code>	Date of the local time on the u.trust Anchor LAN (not on the u.trust Anchor LAN PCIe card)
<code>CSLAN.TIME_LOCAL</code>	Local time on the u.trust Anchor LAN (not on the u.trust Anchor LAN PCIe card)
<code>HSM.DATE_TIME_UTC</code>	Date and time of the UTC time on the u.trust Anchor LAN PCIe card
<code>HSM.DATE_UTC</code>	Date of the UTC time on the u.trust Anchor LAN PCIe card
<code>HSM.TIME_UTC</code>	UTC time on the u.trust Anchor LAN PCIe card
<code>HSM.DATE_TIME_LOCAL</code>	Date and time of the UTC time on the u.trust Anchor LAN PCIe card
<code>HSM.DATE_LOCAL</code>	Date of the local time on the u.trust Anchor LAN PCIe card
<code>HSM.TIME_DIFF</code>	Difference between the time on the u.trust Anchor LAN and the time on the u.trust Anchor LAN PCIe card
<code>HSM.LOAD_PER_CENT</code>	u.trust Anchor LAN load for the last 60 seconds in %
<code>HSM.TRANS_PER_MINUTE</code>	The number of transactions number per minute
<code>HSM.NO_OF_CONNECTIONS</code>	The number of IP client connections to the u.trust Anchor LAN. If, for example, a <code>csadm GetState</code> command is performed, which takes a fraction of a second, Connections is increased by 1 for this period of time.

Variable	Description
CSLAN.SSH_ENABLED	Indication whether the SSH daemon is enabled or disabled. See chapter Enabling/Disabling the SSH Daemon .
CSLAN.SNMP_ENABLED	Indication whether the SNMP daemon is enabled or disabled. See chapter Setting up SNMP .
CSLAN.IPTABLES_ENABLED	Indication whether IPTABLES is enabled or disabled. See chapter Restricting the Network Access on the CryptoServer LAN .
CSLAN.NTP_ENABLED	Indication whether the NTP daemon on the u.trust Anchor LAN is enabled or disabled. See chapter Setting up NTP .
CSLAN.NTP_SERVER_IP4	IPv4 address of the NTP server
HSM.NTP_MDL_STATE	Indication whether the NTP firmware module on the u.trust Anchor LAN PCIe card is active or not active
CSLAN.BOOT_PARTITION	Name of the partition to boot from, for example, user2
CSLAN.RUN_PARTITION	Name of the running partition
NETWORK.IP4_STATE_DEFAULT_GATEWAY	IP address of the IPv4 default gateway
NETWORK.IP6_STATE_DEFAULT_GATEWAY_UPPER	First half of the IPv6 default gateway. The IPv6 gateway value is split into two halves, ..._UPPER and ..._LOWER, because the unsplit value is too long for one line of the display.
NETWORK.IP6_STATE_DEFAULT_GATEWAY_LOWER	Second half of the IPv6 default gateway
NETWORK.ETH0.IP4_STATE_ADDRESS	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.
NETWORK.ETH0.IP4_STATE_NETMASK	Network mask of the eth0 port
NETWORK.ETH0.IP4_STATE_MAC	MAC Address of the eth0 port
NETWORK.ETH0.IP4_STATE_MTU	Maximum transmission unit of the eth0 port in byte, for example, 1500
NETWORK.ETH0.IP4_STATE_LINK_UP	Indicator whether the link of the eth0 port is up and running. Example value: yes. ..._LINK_UP represents the hardware connection to the network. If, for example, the network cable has been disconnected from the network interface card, ..._LINK_UP is no and ..._LINK_SPEED is 0Mb/s. In contrast to ..._LINK_UP, ..._IF_UP (interface up) represents the addressability of the network port by the software.
NETWORK.ETH0.IP4_STATE_LINK_SPEED	Transmission rate via the eth0 port, for example, 1000Mb/s. 1000Mb/s corresponds to an orange control light in the upper left corner of the eth0 port. 10/100Mb/s corresponds to a green control light.

Variable	Description
<code>NETWORK.ETH0.IP4_STATE_DUPLEX_MODE</code>	Duplex mode of the eth0 port, for example, <code>full duplex</code>
<code>NETWORK.ETH0.IP4_STATE_IF_UP</code>	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.
<code>NETWORK.ETH0.IP6_STATE_ADDRESS_0_UPPER</code>	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.
<code>NETWORK.ETH0.IP6_STATE_ADDRESS_0_LOWER</code>	Second half of the first IPv6 address
<code>NETWORK.ETH0.IP6_STATE_PREFIX_0</code>	Prefix length of the first IPv6 address
<code>NETWORK.ETH0.IP6_STATE_ADDRESS_1_UPPER</code>	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.
<code>NETWORK.ETH0.IP6_STATE_ADDRESS_1_LOWER</code>	Second half of the second IPv6 address
<code>NETWORK.ETH0.IP6_STATE_PREFIX_1</code>	Prefix length of the second IPv6 address
<code>CSLAN.FAN1_SPEED</code>	Fan speed in revolutions per minute, for example, <code>6100</code> . A u.trust Anchor 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 2018-0006 Contact Address for Support Queries .
<code>CSLAN.FAN2_SPEED</code>	
<code>CSLAN.FAN3_SPEED</code>	
<code>CSLAN.FAN4_SPEED</code>	
<code>CSLAN.FAN5_SPEED</code>	
<code>CSLAN.FAN6_SPEED</code>	
<code>TIME_SOURCE.CARD_TYPE</code>	Type of the optional PCIe clock card, for example, <code>PZF180PEX DCF77</code> . See chapter Setting up PCIe Clock Cards for details about PCIe clock cards.
<code>TIME_SOURCE.CLOCK_STATE</code>	State of the PCIe clock card, <code>Synchronized</code> or <code>no synch</code>

Variable	Description
TIME_SOURCE.ANTENNA_SIGNAL	Strength of the signal coming from the antenna to the PCIe clock card in percent, for example, 77 % or Error.

Table 18: Examples of idle screen configurations



Figure 31 : 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 u.trust Anchor LAN according to chapter [Logging in Remotely to the u.trust Anchor LAN](#).
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.

6.8 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.

6.9 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

- Execute the following command to bring the configured static routing into use:

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

6.10 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.

- Log in remotely to the LAN device.
- 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
```

- Perform the `fcrontab -e` command. This opens an editor (default: vi), which can be used to add or delete rules.
- 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 u.trust Anchor LAN can output, and the information they provide. They are defined in the `UTIMACO-CSLAN-MIB.txt` file 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 chapter Enabling SNMPv3 and SNMPv3 Traps for IPv4
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 u.trust Anchor 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 19: Parameters for the snmpget v3 command

This applies in an analog way to the `snmpwalk` and `snmptable` commands.

7.1.1 u.trust Anchor LAN

Object name	cslVersion
Description	u.trust Anchor LAN version
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.1.1.0 (UTIMACO-CSLAN-MIB::cslVersion)
Example	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslVersion.0 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.1.0
Example output	CSLAN 5.1.0

Object name	cslSerialNumber
Description	u.trust Anchor LAN serial number
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.1.2.0 (UTIMACO-CSLAN-MIB::cslSerialNumber)
Example	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cslSerialNumber.0 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.1.2.0
Example output	MD2000609

Object name	cslBatteryState
Description	State of the external battery in the u.trust Anchor 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	u.trust Anchor 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	All cHSMs in the u.trust Anchor LAN have a workload average in %. The workload is the ratio of the time that requests/commands spend in the cHSM to the total time. cslLoad is the maximum value of the workload average values of all cHSMs. This workload average maximum corresponds to the result of the csadm CSLGetLoad command. See [ANCHOR_CSADM] for details about this command.
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 u.trust Anchor is read from the display module of the u.trust Anchor 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	u.trust Anchor 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	Load of all client connections of all cHSMs in the u.trust Anchor LAN 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	u.trust Anchor LAN fan table (information about all u.trust Anchor 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 <table> <tr> <th>cslFanIndex</th><th>cslFanSpeed</th></tr> <tr><td>1</td><td>3600</td></tr> <tr><td>2</td><td>3650</td></tr> <tr><td>3</td><td>3700</td></tr> <tr><td>4</td><td>3620</td></tr> <tr><td>5</td><td>3680</td></tr> <tr><td>6</td><td>3670</td></tr> </table>	cslFanIndex	cslFanSpeed	1	3600	2	3650	3	3700	4	3620	5	3680	6	3670
cslFanIndex	cslFanSpeed														
1	3600														
2	3650														
3	3700														
4	3620														
5	3680														
6	3670														

Object name	cslFanIndex.x
Description	Fan index for identification. A u.trust Anchor 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)	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
Example output	1



Figure 32 : Front panel with removed fan compartment grill

Object name	cslFanSpeed.x
--------------------	---------------

Description	Fan speed of u.trust Anchor 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 2018-0006 Contact Address for Support Queries .
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 u.trust Anchor 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 2018-0006 Contact Address for Support Queries .
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	u.trust Anchor 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 u.trust Anchor LAN is failed, Only if the status of all power supply modules is OK, the power supply status of the entire u.trust Anchor 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	u.trust Anchor 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	u.trust Anchor 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 u.trust Anchor 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	u.trust Anchor LAN power supply index for identification u.trust Anchor LAN power supply index for identification. Power supply module no. 1 (on the right) is identical to cslPowerSupplyIndex=1 and power supply module no. 2 (on the left) 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 u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor 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

The csTable is empty for any u.trust Anchor LAN device. Use the csarTable instead.

Object name	csTable
Description	The table holding information about all u.trust Anchors within the u.trust Anchor 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-CSLAN-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	u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor devices in the u.trust Anchor 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 u.trust Anchor x in the u.trust Anchor 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 u.trust Anchor devices mounted in the u.trust Anchor 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 u.trust Anchor x device mounted in the u.trust Anchor 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 u.trust Anchor devices mounted in the u.trust Anchor 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 u.trust Anchor 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 u.trust Anchor devices mounted in the u.trust Anchor 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 u.trust Anchor x device mounted in the u.trust Anchor 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 u.trust Anchor devices mounted in the u.trust Anchor 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 u.trust Anchor x device mounted in u.trust Anchor 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 u.trust Anchor devices mounted in the u.trust Anchor 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 u.trust Anchor x device in the u.trust Anchor 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 u.trust Anchor
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 u.trust Anchor 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 u.trust Anchor devices mounted in the u.trust Anchor 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 u.trust Anchor 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) u.trust Anchors mounted in the u.trust Anchor 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 u.trust Anchor x device mounted in the u.trust Anchor 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 u.trust Anchor in the u.trust Anchor 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 u.trust Anchor x device mounted in the u.trust Anchor 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) u.trust Anchor devices mounted in the u.trust Anchor 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 u.trust Anchor x device mounted in the u.trust Anchor 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 33 : Idle Screens

Object name	csTransactionsPerMinute
--------------------	-------------------------

Description	<p>Transactions per minute of all u.trust Anchor devices mounted in the u.trust Anchor 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 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 csTransactionsPerMinute.2 = INTEGER: 3</pre>

7.1.6 CSAR Table

The csarTable is used for any u.trust Anchor LAN device instead of the csTable.

Object name	csarTable
Description	The table holding information about the u.trust Anchor PCIe card within the u.trust Anchor LAN
Type	Table
OID (Name)	1.3.6.1.4.1.3159.1.5 (UTIMACO-CSLAN-MIB::csarTable)
Example	<pre>snmptable -v 2c -c CryptoServer -Cw 70 111.166.1.200 UTIMACO-CSLAN-MIB::csarTable snmptable -v 2c -c CryptoServer -Cw 70 111.166.1.200 1.3.6.1.4.1.3159.1.5</pre>

Example output	SNMP table: UTIMACO-CSLAN-MIB::csarTable				
	csarIndex	csarDevice	csarState	csarTemperature	csarTemperatureAsString
	1	4000@localhost	OK	41	41.3
	SNMP table: UTIMACO-CSLAN-MIB::csarTable, part 2				
	csarAlarm	csarZeroEvent	csarVersion	csarSerialNumber	csarBatteryState
	0	0	1.15	CS411957	OK
	SNMP table: UTIMACO-CSLAN-MIB::csarTable, part 3				
	csarDateTime		csarMemory		csarDisk
	20210605 093858		70		70

Object name	csarIndex.x
Description	u.trust Anchor x device index for identification
Type	Integer (1...4)
OID (Name)	1.3.6.1.4.1.3159.1.5.1.1.x (UTIMACO-CSLAN-MIB::csarIndex.x)
Example (u.trust Anchor PCIe card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarIndex.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.1.1
Example output	1

Object name	csarDevice.x
Description	u.trust Anchor x device in the u.trust Anchor LAN
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.5.1.2.x (UTIMACO-CSLAN-MIB::csarDevice.x)
Example (u.trust Anchor PCIe card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarDevice.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.2.1
Example output	4000@localhost

Object name	csarDevice
Description	All u.trust Anchor devices in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.5.1.2 (UTIMACO-CSLAN-MIB::csarDevice)

Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarDevice snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.2
Example output	csarDevice.1 = STRING: 4000@localhost csarDevice.2 = STRING: 4001@localhost

Object name	csarState.x
Description	State of services and TRNG on the u.trust Anchor x device mounted in the u.trust Anchor LAN (supported values: OK, Failed)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.5.1.3.x (UTIMACO-CSLAN-MIB::csarState.x)
Example (u.trust Anchor PCIe card1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarState.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.3.1
Example output	OK

Object name	csarState
Description	State of services and TRNG of all u.trust Anchor devices mounted in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.5.1.3 (UTIMACO-CSLAN-MIB::csState)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarState snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.3
Example output	csarState.1 = STRING: OK csarState.2 = STRING: OK

Object name	csarTemperature.x
Description	Temperature of u.trust Anchor x in °C
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.5.1.4.x (UTIMACO-CSLAN-MIB::csarTemperature.x)
Example (u.trust Anchor PCIe card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarTemperature.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.4.1
Example output	41

Object name	csarTemperature
Description	Temperature in °C of all u.trust Anchor devices mounted in the u.trust Anchor LAN
Type	List

OID (Name)	1.3.6.1.4.1.3159.1.5.1.4 (UTIMACO-CSLAN-MIB::csarTemperature)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarTemperature snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.4
Example output	csarTemperature.1 = INTEGER: 41 csarTemperature.2 = INTEGER: 40

Object name	csarTemperatureAsString.x
Description	Temperature (in °C as string with 1 decimal place) of a u.trust Anchor x device mounted in the u.trust Anchor LAN
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.5.1.5.x (UTIMACO-CSLAN-MIB::csarTemperatureAsString.x)
Example (u.trust Anchor PCIe card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarTemperatureAsString.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.5.1
Example output	41.3

Object name	csarTemperatureAsString
Description	Temperature (in °C as string with 1 decimal place) of all u.trust Anchor devices mounted in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.5.1.5 (UTIMACO-CSLAN-MIB::csarTemperatureAsString)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarTemperatureAsString snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.5
Example output	csarTemperatureAsString.1 = STRING: 41.1 csarTemperatureAsString.2 = STRING: 40.5

Object name	csarAlarm.x
Description	Alarm register of u.trust Anchor x device mounted in u.trust Anchor LAN (0 = alarm OFF, value unequal to 0 = alarm ON)
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.5.1.6.x (UTIMACO-CSLAN-MIB::csarAlarm.x)
Example (u.trust Anchor PCIe card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarAlarm.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.6.1
Example output	0

Object name	csAlarm
--------------------	---------

Description	Alarm register of all u.trust Anchor devices mounted in the u.trust Anchor LAN (0 = alarm OFF, value unequal to 0 = alarm ON)
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.5.1.6 (UTIMACO-CSLAN-MIB::csarAlarm)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarAlarm snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.6
Example output	csarAlarm.1 = INTEGER: 0 csarAlarm.2 = INTEGER: 1

Object name	csarZeroEvent.x
Description	Zeroization event on a u.trust Anchor x device mounted in u.trust Anchor LAN (0 = no zeroization event, 1 = zeroization event)
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.5.1.7.x (UTIMACO-CSLAN-MIB::csarZeroEvent.x)
Example (u.trust Anchor PCle card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarZeroEvent.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.7.1
Example output	0

Object name	csarZeroEvent
Description	Zeroization events of all u.trust Anchor devices mounted in the u.trust Anchor LAN (0 = no zeroization event, 1 = zeroization event)
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.5.1.7 (UTIMACO-CSLAN-MIB::csarZeroEvent)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarZeroEvent snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.7
Example output	csarZeroEvent.1 = INTEGER: 0 csarZeroEvent.2 = INTEGER: 1

Object name	csarVersion.x
Description	Device system version of u.trust Anchor x device in the u.trust Anchor LAN
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.5.1.8.x (UTIMACO-CSLAN-MIB::csarVersion.x)
Example (u.trust Anchor PCle card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarVersion.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.8.1
Example output	1.15

Object name	csarVersion
Description	Device system version of all u.trust Anchor
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.5.1.8 (UTIMACO-CSLAN-MIB::csarVersion)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarVersion snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.8
Example output	csarVersion.1 = STRING: 1.15 csarVersion.2 = STRING: 1.15

Object name	csarSerialNumber.x
Description	Serial number of u.trust Anchor x (CSxxxxxx)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.5.1.9.x (UTIMACO-CSLAN-MIB::csarSerialNumber.x)
Example (u.trust Anchor PCle card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarSerialNumber.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.9.1
Example output	CS411957

Object name	csarSerialNumber
Description	Serial number of all u.trust Anchor devices mounted in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.5.1.9 (UTIMACO-CSLAN-MIB::csarSerialNumber)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarSerialNumber snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.9
Example output	csarSerialNumber.1 = STRING: CS411957 csarSerialNumber.2 = STRING: CS888022

Object name	csarBatteryState.x
Description	State of the carrier battery in the u.trust Anchor x device (OK, LOW or ABSENCE)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.5.1.10.x (UTIMACO-CSLAN-MIB::csarBatteryState.x)
Example (u.trust Anchor PCle card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarBatteryState.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.10.1
Example output	OK

Object name	csarBatteryState
Description	State of the carrier batteries in all u.trust Anchors mounted in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.5.1.10 (UTIMACO-CSLAN-MIB::csarBatteryState)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarBatteryState snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.10
Example output	csarBatteryState.1 = STRING: OK csarBatteryState.2 = STRING: OK

Object name	csarDateTime.x
Description	Date and time of u.trust Anchor x device mounted in the u.trust Anchor LAN (YYYYMMDD hhmmss, UTC)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.5.1.11.x (UTIMACO-CSLAN-MIB::csarDateTime.x)
Example (u.trust Anchor PCIe card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarDateTime.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.11.1
Example output	20150605 111321

Object name	csarDateTime
Description	Date and time of all u.trust Anchor in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.5.1.11 (UTIMACO-CSLAN-MIB::csarDateTime)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarDateTime snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.11
Example output	csarDateTime.1 = STRING: 20150605 111321 csarDateTime.2 = STRING: 20150605 111321

Object name	csarMemory.x
Description	Available/total memory in percent of u.trust Anchor x device mounted in the u.trust Anchor LAN
Type	Integer (0...100)
OID (Name)	1.3.6.1.4.1.3159.1.5.1.12.x (UTIMACO-CSLAN-MIB::csarMemory.x)
Example (u.trust Anchor PCIe card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarMemory.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.12.1
Example output	80

Object name	csarMemory
Description	Available/total memory in percent of all u.trust Anchor devices mounted in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.5.1.12 (UTIMACO-CSLAN-MIB::csarMemory)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarMemory snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.12
Example output	csarMemory.1 = INTEGER: 80 csarMemory.2 = INTEGER: 70

Object name	csarDisk.x
Description	Available/total disk space in percent of u.trust Anchor x device mounted in the u.trust Anchor LAN
Type	Integer (0...100)
OID (Name)	1.3.6.1.4.1.3159.1.5.1.13.x (UTIMACO-CSLAN-MIB::csarDisk.x)
Example (u.trust Anchor PCIe card 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::csarDisk.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.13.1
Example output	80

Object name	csarDisk
Description	Available/total disk space in percent of all u.trust Anchor devices mounted in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.5.1.13 (UTIMACO-CSLAN-MIB::csarDisk)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::csarDisk snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.5.1.13
Example output	csarDisk.1 = INTEGER: 80 csarDisk.2 = INTEGER: 70

7.1.7 cHSM Table

Object name	cHSMTTable
Description	The table holding information about all cHSMs within the u.trust Anchor LAN
Type	Table
OID (Name)	1.3.6.1.4.1.3159.1.6 (UTIMACO-CSLAN-MIB::cHSMTTable)

Example	snmptable -v 2c -c CryptoServer -Cw 70 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMTTable snmptable -v 2c -c CryptoServer -Cw 70 111.166.1.200 1.3.6.1.4.1.3159.1.6				
Example output	SNMP table: UTIMACO-CSLAN-MIB::cHSMTTable				
	cHSMIndex	cHSMValid	cHSMDevice	cHSMParentDeviceIndex	cHSMModule
	1	1	4001@local host	1	OPERATIONAL
	SNMP table: UTIMACO-CSLAN-MIB::cHSMTTable, part 2				
	cHSMState	cHSMTemplate	cHSMModuleState	cHSMDisk	cHSMLoad
	INITIALIZED	SecurityServer	OK	80	47
	SNMP table: UTIMACO-CSLAN-MIB::cHSMTTable, part 3				
	cHSMTransactionsPerMinute		cHSMConnections		
	7		1		

Object name	cHSMIndex.x
Description	cHSM index for identification
Type	Integer (1...128)
OID (Name)	1.3.6.1.4.1.3159.1.6.1.1.x (UTIMACO-CSLAN-MIB::cHSMIndex.x)
Example (cHSM 1)	<pre>snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO- CSLAN-MIB::cHSMIndex.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.1.1</pre>
Example output	1

Object name	cHSMValid.x
Description	Flag to identify active (1) or inactive (0) cHSM in the u.trust Anchor LAN. If zero, all other values are dummy values.
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.6.1.2.x (UTIMACO-CSLAN-MIB::cHSMValid.x)
Example (cHSM 1)	<pre>snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO- CSLAN-MIB::cHSMValid.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.2.1</pre>
Example output	1

Object name	cHSMValid
Description	Flag to identify all active or inactive cHSM in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.6.1.2 (UTIMACO-CSLAN-MIB::cHSMValid)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMValid snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.2
Example output	cHSMValid.1 = INTEGER: 1 cHSMValid.2 = INTEGER: 1 ... cHSMValid.32 = INTEGER: 0

Object name	cHSMDevice.x
Description	cHSM x device in the u.trust Anchor LAN. The device is reachable at e.g., 4001@localhost.
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.6.1.3.x (UTIMACO-CSLAN-MIB::cHSMDevice.x)
Example (cHSM 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMDevice.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.3.1
Example output	4001@localhost

Object name	cHSMDevice
Description	All cHSM devices in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.6.1.3 (UTIMACO-CSLAN-MIB::cHSMDevice)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMDevice snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.3
Example output	cHSMDevice.1 = STRING: 4001@localhost cHSMDevice.2 = STRING: 4002@localhost ... cHSMDevice.32 = STRING: 4032@localhost

Object name	cHSMParentDeviceIndex.x
--------------------	-------------------------

Description	csarIndex value of the u.trust Anchor PCIe card this cHSM is running on. csarIndex is the index of the csarTable.
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.6.1.4.x (UTIMACO-CSLAN-MIB::cHSMParentDeviceIndex.x)
Example (cHSM 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMParentDeviceIndex.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.4.1
Example output	1

Object name	cHSMParentDeviceIndex
Description	csarIndex values of all u.trust Anchor PCIe devices mounted in the u.trust Anchor LAN and containing cHSMs
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.6.1.4 (UTIMACO-CSLAN-MIB::cHSMParentDeviceIndex)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMParentDeviceIndex snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.4
Example output	cHSMParentDeviceIndex.1 = INTEGER: 1 cHSMParentDeviceIndex.2 = INTEGER: 1 ... cHSMParentDeviceIndex.32 = INTEGER: 1

Object name	cHSMMode.x
Description	Operating mode of cHSM x in the u.trust Anchor LAN (supported value: OPERATIONAL)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.6.1.5.x (UTIMACO-CSLAN-MIB::cHSMMode.x)
Example (cHSM 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMMode.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.5.1
Example output	OPERATIONAL

Object name	cHSMMode
Description	Operating mode of all cHSMs in the u.trust Anchor LAN (supported value: OPERATIONAL)
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.6.1.5 (UTIMACO-CSLAN-MIB::cHSMMode)

Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO- CSLAN-MIB::cHSMMode snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.5
Example output	cHSMMode.1 = STRING: OPERATIONAL cHSMMode.2 = STRING: OPERATIONAL ... cHSMMode.32 = STRING: BOOTLOADER

Object name	cHSMState.x
Description	Operational state of cHSM x device in the u.trust Anchor LAN (supported value: INITIALIZED)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.6.1.6.x (UTIMACO-CSLAN-MIB::cHSMState.x)
Example (cHSM 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO- CSLAN-MIB::cHSMState.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.6.1
Example output	INITIALIZED

Object name	cHSMState
Description	Operational state of all cHSM devices in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.6.1.6 (UTIMACO-CSLAN-MIB::cHSMState)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO- CSLAN-MIB::cHSMState snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.6
Example output	cHSMState.1 = STRING: INITIALIZED cHSMState.2 = STRING: INITIALIZED ... cHSMState.32 = STRING: UNKNOWN

Object name	cHSMTemplate.x
Description	Template used for the cHSM x device in the u.trust Anchor LAN. (supported value: SecurityServer) It is part of the adm2 field. This field is part of the output when showing the State menu item on the display or when performing the <code>csadm GetState</code> command.
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.6.1.7.x (UTIMACO-CSLAN-MIB::cHSMTemplate.x)

Example (cHSM 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMTemplate.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.7.1
Example output	SecurityServer

Object name	cHSMTemplate
Description	Templates of all cHSM devices in the u.trust Anchor LAN. (supported value: SecurityServer) It is part of the adm2 field. This field is part of the output when showing the State menu item on the display or when performing the <code>csadm GetState</code> command.
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.6.1.7 (UTIMACO-CSLAN-MIB::cHSMTemplate)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMTemplate snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.7
Example output	cHSMTemplate.1 = STRING: SecurityServer cHSMTemplate.2 = STRING: SecurityServer ... cHSMTemplate.32 = STRING: UNKNOWN

Object name	cHSModuleState.x
Description	Module initialization state of cHSM x device in the u.trust Anchor LAN (OK or FAILED if at least one module failed to initialize)
Type	String
OID (Name)	1.3.6.1.4.1.3159.1.6.1.8.x (UTIMACO-CSLAN-MIB::cHSModuleState.x)
Example (cHSM 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cHSModuleState.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.8.1
Example output	OK

Object name	cHSModuleState
Description	Module initialization state of all cHSM devices in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.6.1.8 (UTIMACO-CSLAN-MIB::cHSModuleState)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cHSModuleState snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.8

Example output	cHSModuleState.1 = STRING: OK cHSModuleState.2 = STRING: OK ... cHSModuleState.32 = STRING: FAILED
Object name	cHSMDisk.x
Description	Available/total disk space used by cHSM in percent
Type	Integer (0...100)
OID (Name)	1.3.6.1.4.1.3159.1.6.1.9.x (UTIMACO-CSLAN-MIB::cHSMDisk.x)
Example (cHSM 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMDisk.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.9.1
Example output	80
Object name	cHSMDisk
Description	Available/total disk space used by cHSMs in percent of all cHSMs in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.6.1.9 (UTIMACO-CSLAN-MIB::cHSMDisk)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMDisk snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.9
Example output	cHSMDisk.1 = INTEGER: 80 cHSMDisk.2 = INTEGER: 70 ... cHSMDisk.32 = INTEGER: 0
Object name	cHSMLoad.x
Description	Workload average of the cHSM x device in the u.trust Anchor LAN in %. The workload is the ratio of the time that requests/commands spend in the cHSM to the total time.
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.6.1.10.x (UTIMACO-CSLAN-MIB::cHSMLoad.x)
Example (cHSM 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMLoad.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.10.1
Example output	47

Object name	cHSMLoad
Description	Workload average of all cHSMs in the u.trust Anchor LAN in %. The workload is the ratio of the time that requests/commands spend in the cHSM to the total time.
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.6.1.10 (UTIMACO-CSLAN-MIB:: cHSMLoad)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMLoad snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.10
Example output	cHSMLoad.1 = INTEGER: 47 cHSMLoad.2 = INTEGER: 38 ... cHSMLoad.32 = INTEGER: 0

Object name	cHSMTransactionsPerMinute.x
Description	Transactions per minute of cHSM x device in the u.trust Anchor LAN. 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. 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. The transactions are calculated over a period of 25 seconds and then extrapolated to transactions per minute (tpm).
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.6.1.11.x (UTIMACO-CSLAN-MIB:: cHSMTransactionsPerMinute.x)
Example (cHSM 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMTransactionsPerMinute.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.11.1
Example output	7

Object name	cHSMTransactionsPerMinute
Description	Transactions per minute of all cHSMs in the u.trust Anchor LAN. This value shows a time-averaged value of how many requests all cHSMs 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. 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 cHSMs. The transactions are calculated over a period of 25 seconds and then extrapolated to transactions per minute (tpm).
Type	List

OID (Name)	1.3.6.1.4.1.3159.1.6.1.11 (UTIMACO-CSLAN-MIB:: cHSMTransactionsPerMinute)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMTransactionsPerMinute snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.11
Example output	cHSMTransactionsPerMinute.1 = INTEGER: 4 cHSMTransactionsPerMinute.2 = INTEGER: 3 ... cHSMTransactionsPerMinute.32 = INTEGER: 0

Object name	cHSMConnections.x
Description	Number of client connections of cHSM x device in the u.trust Anchor LAN (analog to cslClients but for a specific cHSM)
Type	Integer
OID (Name)	1.3.6.1.4.1.3159.1.6.1.12.x (UTIMACO-CSLAN-MIB:: cHSMConnections.x)
Example (cHSM 1)	snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMConnections.1 snmpget -v 2c -c CryptoServer -Oqv 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.12.1
Example output	1

Object name	cHSMConnections
Description	Number of client connections of all cHSMs in the u.trust Anchor LAN
Type	List
OID (Name)	1.3.6.1.4.1.3159.1.6.1.12 (UTIMACO-CSLAN-MIB::cHSMConnections)
Example	snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 UTIMACO-CSLAN-MIB::cHSMConnections snmpwalk -v 2c -c CryptoServer -Os 111.166.1.200 1.3.6.1.4.1.3159.1.6.1.12
Example output	cHSMConnections.1 = INTEGER: 1 cHSMConnections.2 = INTEGER: 1 ... cHSMConnections.32 = INTEGER: 0

7.2 SNMP Traps

See chapter [Configuring SNMP Traps](#) for information about how to configure SNMP traps.

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	cHSM operating mode change notification Notification that the operating mode of a cHSM in the u.trust Anchor LAN has changed (supported values: OPERATIONAL)
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	u.trust Anchor 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	u.trust Anchor 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	u.trust Anchor alarm notification that the inner foil is broken The notifyCsAlarmInnerFoil trap is not used in u.trust Anchor LAN
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	u.trust Anchor alarm notification that the outer foil is broken The notifyCsAlarmOuterFoil trap is not used in u.trust Anchor LAN
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	u.trust Anchor 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	u.trust Anchor 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	u.trust Anchor 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	u.trust Anchor alarm notification that the Master Key is invalid The notifyCsAlarmInvalidMasterKey trap is not used in u.trust Anchor LAN
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	u.trust Anchor 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	u.trust Anchor 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	u.trust Anchor 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	u.trust Anchor 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	u.trust Anchor 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)

Trap name	<i>notifyCsTemperatureLowBack</i>
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	u.trust Anchor 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	notifyCslBatteryLow
Description	u.trust Anchor LAN notification that the u.trust Anchor 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	u.trust Anchor LAN notification that the workload of the u.trust Anchor PCIe card has risen above the threshold. The workload is the ratio of the time that requests/commands spend in the u.trust Anchor 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. See [ANCHOR_CSADM] for details about this command.
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	u.trust Anchor LAN notification that the workload of the u.trust Anchor PCIe card has fallen back to or below the threshold. The workload is the ratio of the time that requests/commands spend in the u.trust Anchor 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. See [ANCHOR_CSADM] for details about this command.
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	u.trust Anchor 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	u.trust Anchor 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	u.trust Anchor LAN notification that the u.trust Anchor 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	u.trust Anchor LAN notification that the u.trust Anchor 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. See [\[FanSpeedTraps\]](#) in chapter [Configuring SNMP Traps](#) for more information about this threshold.

Trap name	notifyCslFanSpeedLow
Description	u.trust Anchor LAN notification that the u.trust Anchor 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	u.trust Anchor LAN notification that the u.trust Anchor 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	u.trust Anchor LAN notification that the u.trust Anchor 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	notifyCsIPMILink
Description	u.trust Anchor LAN notification that the u.trust Anchor 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::notifyCsIPMILink)
Variables	-

Tamper Wire Trap

Trap name	notifyCsAlarmTamperWire
Description	u.trust Anchor notification that the tamper wire has been destroyed
Severity	Critical
OID (Name)	1.3.6.1.4.1.3159.1.3.0.28 (UTIMACO-CSLAN-MIB::notifyCsTamperWire)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

Zero Event Trap

Trap name	notifyCsZeroEvent
Description	u.trust Anchor notification that a zeroization event has occurred
Severity	Major
OID (Name)	1.3.6.1.4.1.3159.1.3.0.29 (UTIMACO-CSLAN-MIB::notifyCsSensoryController)
Variables	CryptoServer device (String; 1.3.6.1.4.1.3159.1.3.1.1.0)

8 Contact Address for Support Queries

If an error occurs while operating the u.trust Anchor, prepare diagnostic information in a .txt file on your computer via the `csadm GetState` command.

If you have any further questions on u.trust Anchor, 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.com
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.

9 References

Reference	Title/Company	Doc.-No
[ANCHOR_CSADM]	u.trust Anchor – csadm Manual / Utimaco IS GmbH.	2020-0037
[CSLAN5-OM]	u.trust Anchor LAN V5 - Operating Manual / Utimaco IS GmbH.	2021-0039
[CSMSADM]	u.trust Anchor - Containerized Hardware Security Module (cHSM) - Administration Manual / Utimaco IS GmbH	2020-0040
	CryptoServer - Administration Manual / Utimaco IS GmbH	M010-0001-en
	CryptoServer - CAT Manual / Utimaco IS GmbH	2021-0055
	u.trust Anchor - Administration Manual / Utimaco IS GmbH.	2020-0035