

Manufacturer & Contact

SEH Computertechnik GmbH
Suedring 11
33647 Bielefeld
Germany
Phone: +49 (0)521 94226-29
Fax: +49 (0)521 94226-99
Support: +49 (0)521 94226-44
Email: info@seh.de
Web: <https://www.seh-technology.com>



Document

Type: User Manual
Title: INU User Manual Linux
Version: 1.3 | 2022-12

Legal Information

SEH Computertechnik GmbH has endeavored to ensure that the information in this documentation is correct. If you detect any inaccuracies please inform us at the address indicated above. SEH Computertechnik GmbH will not accept any liability for any error or omission. The information in this manual is subject to change without notification.

The original manual is the German version of this document and shall govern. All non-German versions of this document are translation of the original manual.

All rights are reserved. Copying, other reproduction, or translation without the prior written consent from SEH Computertechnik GmbH is prohibited.

© 2022 SEH Computertechnik GmbH

All trademarks, registered trademarks, logos and product names are property of their respective owners.

Inhalt

1	General Information	1
1.1	Product	2
1.2	Documentation	5
1.3	Support and Service.....	7
1.4	Your Safety	8
1.5	First Steps	9
2	Administration Methods.....	10
2.1	Administration via INU Control Center	11
2.2	Administration via the SEH UTN Manager	13
2.3	Administration via Email	19
3	Working with the SEH UTN Manager	21
3.1	How to Find INU Servers/USB Devices in the Network	22
3.2	How to Establish a Connection to a USB Device	24
3.3	How to End the Connection between the USB Device and the Client.....	25
3.4	How to Request an Occupied USB Device.....	26
3.5	How to Automate USB Device Connections and Program Starts	27
3.6	How to Find Status Information on USB Ports and USB Devices.....	29
3.7	How to Use the Selection List and Manage User Access Rights with It.....	31
3.8	How to Use the SEH UTN Manager without Graphical User Interface (utnm).....	34
4	Network Settings	39
4.1	How to Configure IPv4 Parameters	40
4.2	How to Configure IPv6 Parameters	42
4.3	How to Use the INU Server in VLAN Environments	43
4.4	How to Configure the DNS.....	45
4.5	How to Configure Email (POP3 and SMTP).....	46
4.6	How to Configure Bonjour	48
4.7	How to Configure Server Services	49
5	Device Settings	51
5.1	How to Assign a Description.....	52
5.2	How to Configure the Device Time.....	53
5.3	How to Configure the (Encrypted) UTN Port	54
5.4	How to Write a Description for a USB port	55
5.5	How to Get Messages.....	56
5.6	How to Monitor the INU Server	58
5.7	How to Use the Relay	62
6	Security.....	64
6.1	How to Define the Encryption Strength for SSL/TLS Connections.....	65
6.2	How to Encrypt the Connection to the INU Control Center.....	67
6.3	How to Protect Access to the INU Control Center(User Accounts).....	68
6.4	How to Configure SNMP	69
6.5	How to Block INU Server Ports (TCP Port Access Control)	70
6.6	How to Use Certificates	71
6.7	How to Configure Network Authentication (IEEE 802.1X)	76

6.8	How to Assign a Name to a USB Port.....	79
6.9	How to Control Access to USB Devices.....	80
6.10	How to hide protected USB devices in the SEH UTN Manager selection list?	83
6.11	How to Block USB Device Types	84
6.12	How to Disable a USB Port.....	85
6.13	How to Encrypt the USB Connection.....	86
7	Maintance.....	87
7.1	How to Backup Your Configuration	88
7.2	How to Reset Parameters to their Default Values.....	91
7.3	How to Perform a Device Software Update	92
7.4	How to Restart the INU Server	93
8	Appendix	94
8.1	Glossary	95
8.2	Troubleshooting	96
8.3	Parameter lists.....	98
8.4	SEH UTN Manager – Feature Overview.....	119
8.5	Index.....	121

1 General Information

- Product ⇨ 2
- Documentation ⇨ 5
- Support and Service ⇨ 7
- Your Safety ⇨ 8
- First Steps ⇨ 9

1.1 Product

Purpose

INU servers integrate non-network-ready USB devices (e.g. USB sensors, USB cameras, etc.) into an industrial environment via TCP/IP network. For this purpose, the USB devices will be connected to the USB ports of the INU server. Then the UTN (UTN = USB to Network) functionality and the corresponding software tool 'SEH UTN Manager' establish a virtual USB connection between USB device and client. The USB device can be used as if it were connected locally.

In addition, a load can be connected to and then used via the relay of the INU server. By default, predefined events and errors switch the relay. For example, an active connection to a USB device can be visualized by a lamp or the loss of a power supply by an acoustic alarm signal. Alternatively, the relay can be switched manually or via SNMP. Thus diverse, individually adapted relay scenarios can be set up in your environment.

System Requirements

The INU server has been designed for use in TCP/IP networks.

The SEH UTN Manager can be used in the following systems:

- For Windows 10 or later, Windows Server 2012 or later
- For macOS with SEH UTN Manager Version 3.3.x
 - 10.15 (Catalina)
 - 11 (Big Sur)¹
- For macOS with SEH UTN Manager Version 3.4.x
 - 12 (Monterey)²
- For Linux (Ubuntu 18.04/20.0.4, Debian 9/10/11, CentOS 7/8, CentOS Stream 8, Oracle 7/8, RHEL 7.4/8.4, OpenSUSE Leap 15.3, SUSE Linux Enterprise Server 15)³
- IPv4 TCP/IP network
- IPv6 TCP/IP network




Important:

The support of isochronous USB devices (e.g. cameras, microphones, speakers, etc.) depends on

- the operating system:
 - Windows
 - macOS
 - Linux
- the software version:
 - firmware/software for INU servers: 20.1.16 or later
 - SEH UTN Manager: 3.3.5 or later

1. macOS 11.x (Big Sur) only limited USB device support.
2. Installer supports only „complete version“. More details can be found in chapter 'Administration via the SEH UTN Manager' ⇒ 13.
3. A successful installation cannot be guaranteed due to the variety of Linux systems! The installation must be carried out under your own responsibility.

This document describes the usage in Linux environments. Information about the usage in other environments can be found in the relevant system-specific User Manual. More details can be found in chapter 'Documentation' ⇒ 5.

Combination with Associated Products

You can combine the INU server with additional SEH Computertechnik GmbH products to ideally adapt the use of your devices to your environment!

Industrial Solution 'IH-304 USB Hub'

The industrial solution IH-304 is a USB hub with four USB 3.0 ports. If it is connected to the INU server, up to four USB devices can be used per INU server USB port. This is a most efficient solution for control cabinets with little space.

The IH-304 must be purchased separately. Detailed information:

<https://www.seh-technology.com/products/industrial-solutions/ih-304.html>



Industrial Solution 'SU-302 Serial to USB Converter'

The industrial solution SU-302 is a serial to USB converter. It can be connected to the INU server via USB and allows for the use of two serial devices via its interfaces RS-232 (for plug type D-Sub, DE-9) and RS-485 (also known as EIA-485; compatible with RS-422/EIA-422).

By combining the INU server and SU-302 you make your serial devices available via network (TCP/IP, Internet)!

<https://www.seh-technology.com/products/industrial-solutions/su-302.html>



Industrial Solutions 'Top-Hat Rail Power Supplies'

All Industrial Solutions are mounted on a top-hat rail in a control cabinet. The USB Deviceserver INU-100 and the USB Hub IH-304 are to be connected to a power supply. You either use your existing power supply or—if there is none or no vacancy—you can buy a new one.

Spare yourself the search and use the top-hat rail power supplies DRP-20 and DRP-75 which are specifically selected to perfectly match the industrial solutions!

<https://www.seh-technology.com/products/industrial-solutions/accessories.html>



1.2 Documentation



Please load all current documents from our Website:
<https://www.seh-technology.com>

Further applicable documents

The INU documentation consists of the following documents:

Hardware Installation Guide	Print, PDF	Information on safety, technical data, hardware installation and declarations of conformity
Quick Installation Guide	Print, PDF	Description of initial setup
User Manual	PDF	Detailed description of the INU server configuration, administration and maintenance. System-specific instructions for the following systems: - Windows - macOS - Linux
Online help	HTML	Information on how to use the web interface 'INU Control Center'. (Embedded into web interface; no download.)
Product information	print, PDF	Features and technical data
Brochures	print, PDF	
Open Source Licenses	online	https://www.seh-technology.com/services/licenses.html

Symbols and Legend

A variety of symbols and mark-ups are used within this document.



WARNING

Warning

A warning contains important information that must be heeded. Non-observance may lead to malfunctions.



Important:

Important information

These notes contain crucial information for failure-free operation.

✓ Requirement

Requirements that must be met before you can begin the action.

• Numeration

Listing

1. Numeration

Step-by-step instructions

↳ Result

Outcome of a performed action



Recommendations and beneficial advice



Reference (Within the document you can use hyperlinks.)

Bold

Established terms (e.g. of buttons, menu items, or selection lists)

Courier

Code (e.g. for command lines or scripts), Paths

'Proper names'

Single quotation marks identify proper names

1.3 Support and Service

SEH Computertechnik GmbH offers extensive Support. If you have any questions, please contact us.



Monday through Thursday

8:00 a.m. to 4:45 p.m.

Friday

8:00 a.m. to 15:15 p.m.



+49 (0)521 94226-44



support@seh.de

Customers from the United States of America (USA) and Canada please contact North American Support:



Monday – Friday

9:00 am – 5:00 pm (EST/EDT)



+1-610-933-2088



support@sehtechnology.com

All information and downloads regarding your product are available on our website:



<https://www.seh-technology.com>



1.4 Your Safety

Read and observe all safety regulations and warnings found in the documentation, on the device and on the packaging. This will avoid potential misuse and prevent damages to people and devices.

Intended Use

The INU server is used in TCP/IP networks and has been designed for use in industrial environments. It allows network users to access non-network-ready USB devices. In addition, a load can be connected to and then used via the relay of the INU server.

Improper Use

All uses of the device that do not comply with the functionalities described in the INU documentation are regarded as improper uses.

Safety Regulations

Before starting the initial setup of the INU server, read and observe the safety regulations in the 'Hardware Installation Guide'. This document is enclosed in the packaging in printed form.

Warnings

Read and observe all warnings mentioned in this document. Warnings are found before any instructions known to be dangerous. They are presented as follows:






Liability and Guarantee

SEH Computertechnik GmbH will not accept any liability for personal injuries, property damages and consequential damages resulting from the non-observance of the mentioned safety regulations and warnings. Non-observance will also result in any guarantee claims becoming void.

Modifications to the Device and Repairs

It is not allowed to make modifications to the hardware and software or to try to repair the device. If your device needs to be repaired, contact our support ⇒ [7](#).

1.5 First Steps

1. Read and observe the security regulations in order to avoid damages to people and devices ⇒ 8.
2. Install the hardware. The hardware installation includes connecting the INU server to the network, USB devices, and power grid ⇒  'Hardware Installation Guide'.
3. Install the software. The software installation includes installing the required software tool 'SEH UTN Manager' on your client and assigning an IP address ⇒  'Software Installation Guide'.
4. Configure the INU server so that it is optimally embedded into your network and sufficiently protected. All information on how to do this you will find in this document.
5. Use the SEH UTN Manager to establish and manage connections to the USB devices which are connected to the INU server.



You can find information on the INU documentation in chapter Documentation ⇒

5

2 Administration Methods

You can administer, configure and maintain the INU server in a number of ways:

- Administration via INU Control Center ⇒ 11
- Administration via the SEH UTN Manager ⇒ 13
- Administration via Email ⇒ 19

2.1 Administration via INU Control Center

The INU server has a user interface, the INU Control Center which can be opened in an Internet browser (e.g. Mozilla Firefox).

The INU server can be configured, monitored and maintained via the INU Control Center.

- Open INU Control Center in Browser ⇒ 11
- INU Open Control Center via SEH UTN Manager ⇒ 11
- Controls ⇒ 12

Open INU Control Center in Browser

- ✓ The INU server is connected to the network and the power grid.
 - ✓ The INU server has a valid IP address ⇒ 40.
1. Open your browser.
 2. Enter the IP address of the INU server as the URL.
- ↳ The INU Control Center is displayed in the browser.



Important:

If the INU Control Center is not displayed, check if a gateway is configured (⇒ 40) and the proxy settings of your browser.

INU Open Control Center via SEH UTN Manager

- ✓ The INU server is connected to the network and the power grid.
 - ✓ The INU server has a valid IP address ⇒ 40.
 - ✓ The SEH UTN Manager is installed on the client ⇒ 13.
1. Start the SEH UTN Manager.
 2. In the selection list, select the INU server.
 3. In the menu bar, select **UTN Server-Configure**.
- ↳ Your browser opens and the INU Control Center is displayed.

Controls

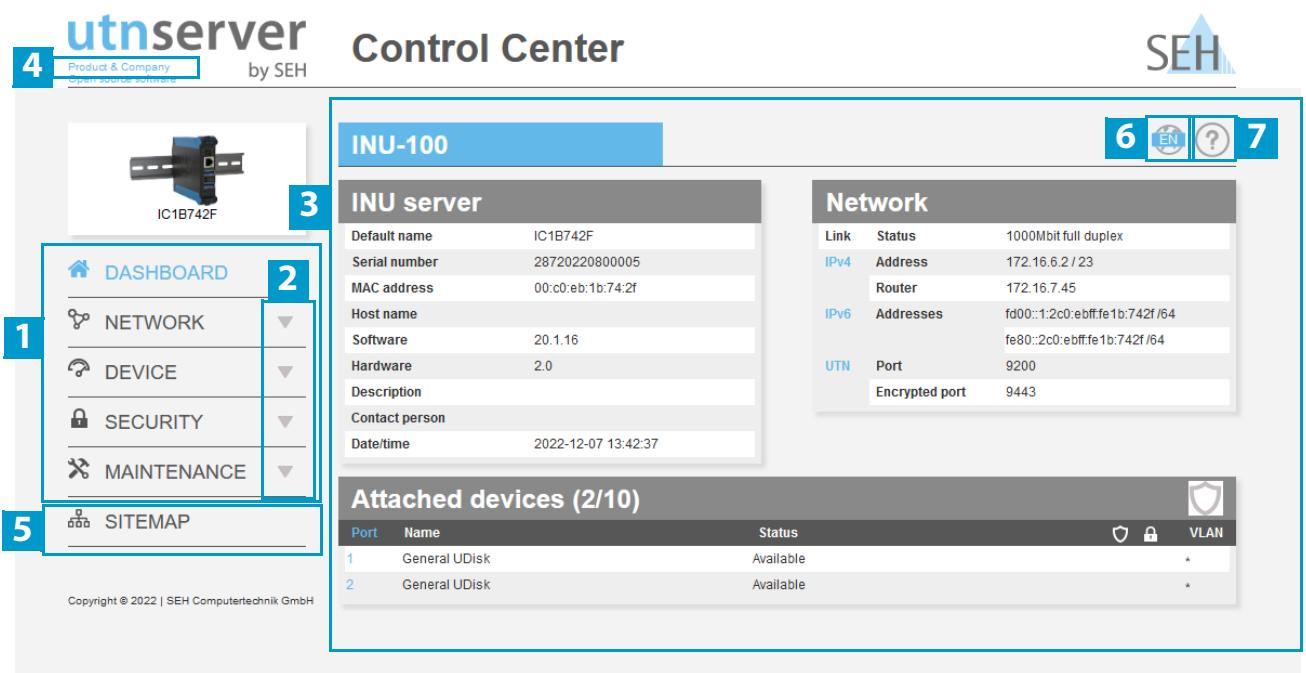


Figure 2.1-1: INU Control Center

- | | | |
|---|-------------------|--|
| 1 | Menu item | After selecting a menu item (simple mouse click), the available submenu items are displayed to the left. |
| 2 | Submenu items | After selecting a submenu item, the corresponding page with its content is displayed. |
| 3 | Page | Menu content |
| 4 | Product & Company | Manufacturer's contact details and additional product information. |
| 5 | Sitemap | Overview of and direct access to all pages of the INU Control Center. |
| 6 | Flags | Language selection |
| 7 | ? icon | Online help |

2.2 Administration via the SEH UTN Manager

The 'SEH UTN Manager' is a software tool developed by SEH Computertechnik GmbH. The SEH UTN Manager is used to establish and manage connections to the USB devices connected to the INU servers.

- Features ⇨ 13
- Versions ⇨ 14
- Installation ⇨ 15
- Program Start ⇨ 18

Features

The software is installed on all clients that are meant to access a USB device in the network. After the SEH UTN Manager is started, the network is scanned for connected INU servers. All INU servers found and their connected USB devices are displayed in the 'network list'. To use the USB devices connected to the INU server, you have to add the INU server to the 'selection list'. The devices shown in the selection list can be administrated and the connected USB devices can be used. Working with the SEH UTN Manager is described in detail in the chapter 'Working with the SEH UTN Manager' ⇨ 21.



Important:

The SEH UTN Manager can be used in IPv4 and IPv6 environments. The selection determines which IP version is used in the software.

"IPv4" is default. Selecting "IPv6" is only suitable for IPv6 networks. If you are not sure about your network, select "IPv4 and IPv6".

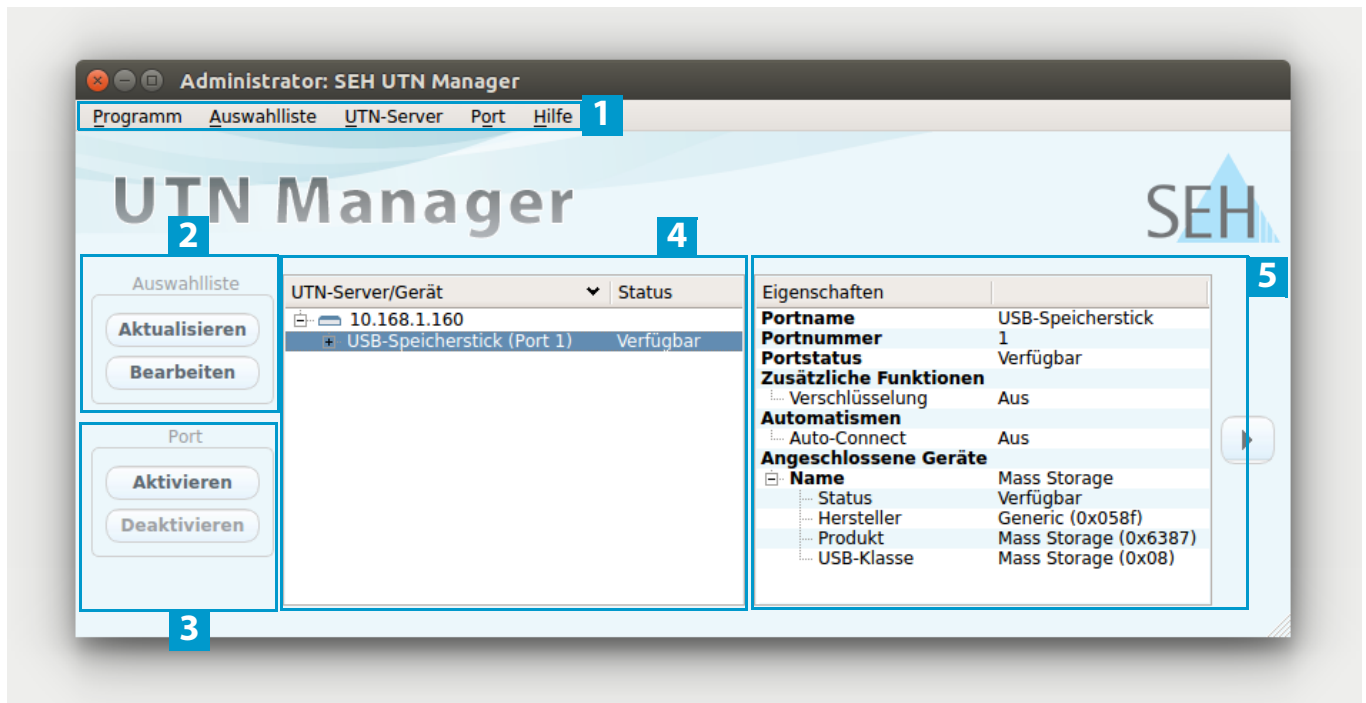


Figure 2.2-2: SEH UTN Manager

1	Menu bar	Available menu items
2	Buttons for editing the selection list	Opens the dialog for searching INU servers in the network and for selecting the desired devices ⇒ 122 .
3	Buttons for managing the port connection	Establishes a connection to the USB device connected to the USB port (⇒ 124) or interrupts the connection (⇒ 125).
4	Selection list	Shows the selected INU servers and the connected USB devices.
5	Display area for the properties	Shows information on the selected INU server or USB device ⇒ 129 .

Detailed information on how to use the SEH UTN Manager can be found in the ⇒ [129](#) 'SEH UTN Manager Online Help'. To start the online help, go to the SEH UTN Manager menu bar and select **Help – Online Help**.



Important:

Some SEH UTN Manager features might not be displayed or are displayed as inactive. This depends on

- the type and location of the selection list
- the user's rights and the group memberships on the client
- the client operating system
- the settings of the product-specific security mechanisms
- the status of the INU server and respective USB port

More details can be found in chapter 'SEH UTN Manager – Feature Overview' ⇒ [119](#).

Versions

The SEH UTN Manager is available in two versions:

- Complete Version:
SEH UTN Manager with graphical user interface (⇒ [Figure 2.2-2 113](#)) and additional features.
- Minimal version (without graphical user interface):
Usage only via command line ('utnm' ⇒ [134](#)).



Important:

The complete version is recommended for general use.
The minimal version is to be used by experts only!

In both versions the 'SEH UTN Service' (Daemon) works in the background and is automatically active after the system start.

Additionally, the following user groups are distinguished:

- users with administrative rights (administrator)
- users without administrative rights (standard user)



Important:

Some features can only be configured by administrators. More details can be found in chapter 'SEH UTN Manager – Feature Overview' ⇒ [119](#).

Installation

In order to use the SEH UTN Manager, the program must be installed on a computer with a Linux operating system. The SEH UTN Manager installation file can be found on the SEH Computertechnik GmbH website:

<https://www.seh-technology.com/us/services/downloads/industrial/inu-100.html>



There are four installation packages:

- 1) driver
- 2) service (SEH UTN service/daemon)
- 3) clitool (command line interface tool 'utnm')
- 4) manager (graphical user interface)

The number of installed packages determines the version of the SEH UTN Manager:

package 1)-3): minimal version

package 1)–4): complete version

**Important:**

Install the packages in the order given above to comply with their dependencies.

The installation of the files depends on the distribution. For more information, refer to the documentation of your operating system.

**Important:**

Installation must only be carried out by experienced users.

Some installation examples are given below.

- 'Installing the SEH UTN Manager in Ubuntu 20.0.4 (64-Bit) via Software Management' ⇒ 16
- 'Installing the SEH UTN Manager in Ubuntu 20.0.4 (64-Bit) via Terminal' ⇒ 16
- 'Installing the SEH UTN Manager in Red Hat Enterprise Linux Server (8)' ⇒ 17



Important:

Knowledge Base articles with further installation information for Linux (e.g. installation of DKMS and the UEFI Secure Boot problem) are available at the SEH Computertechnik GmbH website:

<https://www.seh-technology.com/services/knowledgebase.html>



Installing the SEH UTN Manager in Ubuntu 20.0.4 (64-Bit) via Software Management

- ✓ Linux kernel 2.6.32 or later
 - ✓ glibc 2.15 or later
 - ✓ OpenSSL 1.0.1 or later
 - ✓ DKMS (Dynamic Kernel Module Support) is installed on the client.
 - ✓ The user used can gain root privileges via the command `sudo`.
1. Start installation package no. 1.
The **Ubuntu Software** appears.
 2. Click **Install**.
A password prompt appears.
 3. Authenticate yourself with your password.
The package will be installed on your client.
 4. Repeat steps 1 through 3 with the remaining packages.
 5. Add all users that are to administrate the SEH UTN Manager on the client to the user group 'utnusers'. To do this, open a **Terminal** and enter the command:

```
sudo usermod -aG utnusers <username>
```
 6. Logout and login again so that the group changes take effect.
↳ The SEH UTN Manager is installed on your client. Check the installation by starting the SEH UTN Manager (⇒ 18) and activating a connection to the USB port including the connected USB device. All information on this can be found in chapter 'Working with the SEH UTN Manager' ⇒ 21.

Installing the SEH UTN Manager in Ubuntu 20.0.4 (64-Bit) via Terminal

- ✓ Linux kernel 2.6.32 or later
 - ✓ glibc 2.15 or later
 - ✓ OpenSSL 1.0.1 or later
 - ✓ DKMS (Dynamic Kernel Module Support) is installed on the client.
 - ✓ The user used can gain root privileges via the command `sudo`.
1. Open a **Terminal**.
 2. Install the headers for your kernel:

```
sudo apt-get install linux-headers-`uname -r`
```

3. Verify, that the version numbers of kernel and headers match exactly:

Kernel: `uname -r`

Header: `sudo apt list --installed | grep linux-headers`



WARNING

The version numbers must be identical. Otherwise, the SEH UTN Manager packages cannot be installed correctly.

If kernel and headers do not match, you must create a match on your own.

4. Change to the directory containing the SEH UTN Manager packages:

`cd <directory>`

5. Install the desired SEH UTN Manager packages:

`sudo dpkg -i <full package name>`

6. Add all users that are to administrate the SEH UTN Manager on the client to the user group 'utnusers'. To do this, open a **Terminal** and enter the command:

`sudo usermod -aG utnusers <username>`

7. Logout and login again so that the group changes take effect.

↳ The SEH UTN Manager is installed on your client. Check the installation by starting the SEH UTN Manager (⇒ 18) and activating a connection to the USB port including the connected USB device. All information on this can be found in chapter 'Working with the SEH UTN Manager' ⇒ 21.

Installing the SEH UTN Manager in Red Hat Enterprise Linux Server (8)

- ✓ Linux kernel 2.6.32 or later
- ✓ glibc 2.12 or later
- ✓ OpenSSL 1.0.1 or later
- ✓ DKMS (Dynamic Kernel Module Support) is installed on the client.
- ✓ The user used can gain root privileges via the command `sudo`.

1. Open a **Terminal**.

2. Install the headers for your kernel:

`sudo yum install kernel-devel-`uname -r``

3. Verify, that the version numbers of kernel and headers match exactly:

Kernel: `uname -r`

Header: `sudo yum list | grep kernel-headers`



WARNING

The version numbers must be identical. Otherwise, the SEH UTN Manager packages cannot be installed.

If kernel and headers do not match, you must create a match on your own.

4. Change to the directory containing the SEH UTN Manager packages:

`cd <directory>`

5. Install the desired SEH UTN Manager packages:

`sudo yum install <full package name>`

6. Add all users that are to administrate the SEH UTN Manager on the client to the user group 'utnusers'. To do this, open a **Terminal** and enter the command:

`sudo usermod -aG utnusers <username>`


7. Logout and login again so that the group changes take effect.

↳ The SEH UTN Manager is installed on your client. Check the installation by starting the SEH UTN Manager (⇒ 18) and activating a connection to the USB port including the connected USB device. All information on this can be found in chapter 'Working with the SEH UTN Manager' ⇒ 21.

Program Start

To start the SEH UTN Manager, go to the launcher and call 'UTN Manager' via Dash (search) or go to **Terminal** and run the command `utnmanager`.

Update

You can check for program updated manually and automatically. More information can be found in the ⇒  'SEH UTN Manager Online Help'.

2.3 Administration via Email

You can administrate the INU server via email and thus from any computer Internet access (remote access):

- Get INU server status
- Set INU server parameters
- INU server update

To do so, you write commands into the email message header ⇒ Table 2.3-1 ¶19.

Table 2.3-1: Commands and comment:

Commands	Option	Description
<Command>	get status	You get the INU server status page.
	get parameters	You get the INU server parameter list.
	set parameters	Sends one or more parameters to the INU server which will then be adopted by the INU server. Write the parameters and their values into the email message body: <parameter> = <value>
		The syntax and values can be found in the parameter lists .
	update utn	Carries out an automatic update using the software that is attached to the mail.
	help	You get a page with information on remote maintenance.
[<Comment>]		Freely definable text for descriptions.

The following applies to the instructions:

- not case-sensitive
- one or more space characters are allowed
- max. length is 128 byte
- only the ASCII format can be read.

In addition, a TAN is needed to execute updates or parameter changes. To begin with, you have to get a status page via email (⇒ Table 2.3-1 ¶19) because it contains the TAN. You enter the received TAN into the email message body. A space character must follow.

- ✓ An email user account for the INU server is set up on a POP3 server.
- ✓ An email user account for the INU server is set up on an SMTP server.
- ✓ A DNS server is configured on the INU server ⇒ ¶40.
- ✓ POP3 and SMTP parameters have been configured on the INU server ⇒ ¶46.

1. Open an email program.
 2. Write a new email:
 - As recipient enter the INU server address.
 - Enter a command in the subject line: cmd: <command> [<comment>]
Commands and comments: ⇒ Table 2.3-1 ¶19.
 - Into the email message body enter a TAN, if applicable.
 3. Send the email.
- ↳ The INU server receives the email and carries out the instruction.

Examples

You want to get the INU server parameter list:

To: INUserver@company.com

Subject: cmd: get parameters

You want to set the 'configuration' parameter:

To: INUserver@company.com

Subject: cmd: set parameters

Email message body: TAN = nUn47ir79Ajs7QKE
sys_descr = <your description>

3 Working with the SEH UTN Manager

The 'SEH UTN Manager' is a software tool developed by SEH Computertechnik GmbH. The SEH UTN Manager is used to establish and manage connections to the USB devices connected to the INU servers..

- How to Find INU Servers/USB Devices in the Network ⇒ 22
- How to Establish a Connection to a USB Device ⇒ 24
- How to End the Connection between the USB Device and the Client ⇒ 25
- How to Request an Occupied USB Device ⇒ 26
- How to Automate USB Device Connections and Program Starts ⇒ 27
- How to Find Status Information on USB Ports and USB Devices ⇒ 29
- How to Use the Selection List and Manage User Access Rights with It ⇒ 31
- How to Use the SEH UTN Manager without Graphical User Interface (utnm) ⇒ 34

3.1 How to Find INU Servers/USB Devices in the Network

The software tool SEH UTN Manager is used to establish and manage connections to the USB devices connected to the INU servers.

After the SEH UTN Manager is started, the network has to be scanned for connected INU servers. The network range to be scanned is freely definable; the search can be effected via multicast and/or in definable IP ranges. The default setting is multicast search in the local network segment.

All INU servers found and their connected USB devices are displayed in the 'network list'. To use the USB devices connected to the INU server, you have to add the INU server to the 'selection list'.

You can also directly add an INU server to the selection list. To do this, you need to know its IP address.

- Defining Search Parameters ⇨ 22
- Scanning the Network ⇨ 22
- Adding the INU Server to the Selection List ⇨ 22
- Adding a INU Server via IP Address ⇨ 23

Defining Search Parameters

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 13.

1. Start the SEH UTN Manager.
2. In the menu bar, select **Program – Options**.
The **Options** dialog appears.
3. Select the **Network Scan** tab.
4. Tick **IP Range Search** and define one or more network ranges.
5. Click **OK**.
↳ The settings will be saved.

Scanning the Network

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 13.

1. Start the SEH UTN Manager.
2. In the menu bar, select **Selection List – Edit**.
The **Edit Selection List** dialog appears.
3. Click **Scan**.
4. The network is scanned. The INU servers and USB devices found are displayed in the network list.

Adding the INU Server to the Selection List

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 13.

✓ The INU server was found via the network scan and is displayed in the network list.

1. Start the SEH UTN Manager.
2. In the menu bar, select **Selection List – Edit**.
The **Edit Selection List** dialog appears.
3. In the network list, select the INU server to be used.
4. Click **Add**.
(Repeat steps 2 and 3, if necessary.)
5. Click **OK**.
↳ The INU servers and the connected USB devices are shown in the selection list.



Figure 3.1-1: SEH UTN Manager – Edit Selection List

Adding a INU Server via IP Address

- ✓ The SEH UTN Manager (complete version) is installed on the client ⇒ 13.
 - ✓ You know the IP address of the INU server.
1. Start the SEH UTN Manager.
 2. Select **UTN server – Add**.
The **Add server** dialog appears.
 3. In the **Host name or IP address** box, enter the IP address of the INU server.
 4. If you changed the UTN port or encrypted UTN port (⇒ 54), define the respective port number in the **UTN Port** and **Encrypted UTN Port** boxes.
 5. Click **OK**.
↳ The INU server and the connected USB devices is shown in the selection list.

3.2 How to Establish a Connection to a USB Device

To connect a USB device to the client, a point-to-point-connection is established between the client and the USB port of the INU server to which the USB device is connected. The USB device can then be used as if it were directly connected to the client. As long as the connection is established, other users cannot connect the USB device to their client and thus cannot use it.



Important:

Special case of compound USB devices

When connecting certain USB devices to a USB port of the INU server, the selection list displays several USB devices on this port. These are compound USB devices. They consist of a hub and one or more USB devices that are all integrated into a single housing.

If the connection is established to a port with a connected compound USB device, all USB devices shown will be connected to the user's client. In this case, each integrated USB device occupies a virtual USB port of the INU server. If the limit is reached, no further USB devices can be used on this INU server.

INU server	Number of physical USB ports	Number of virtual USB ports
INU-100	2	10

- ✓ The SEH UTN Manager (complete version) is installed on the client ⇒ 13.
 - ✓ The USB port is shown in the selection list ⇒ Figure 3.1 22.
 - ✓ All provisions (driver installation, etc.) necessary to operate the USB device locally (i.e. connected directly to the client) have been met on the client. Ideally, the USB device has been connected and operated on the client locally according to the instructions of the manufacturer.
 - ✓ The USB port is not connected to another client.
1. Start the SEH UTN Manager. In the selection list, select the port.
 2. In the menu bar, select **Port – Activate**.
- ↳ The connection between the USB device and client is established.

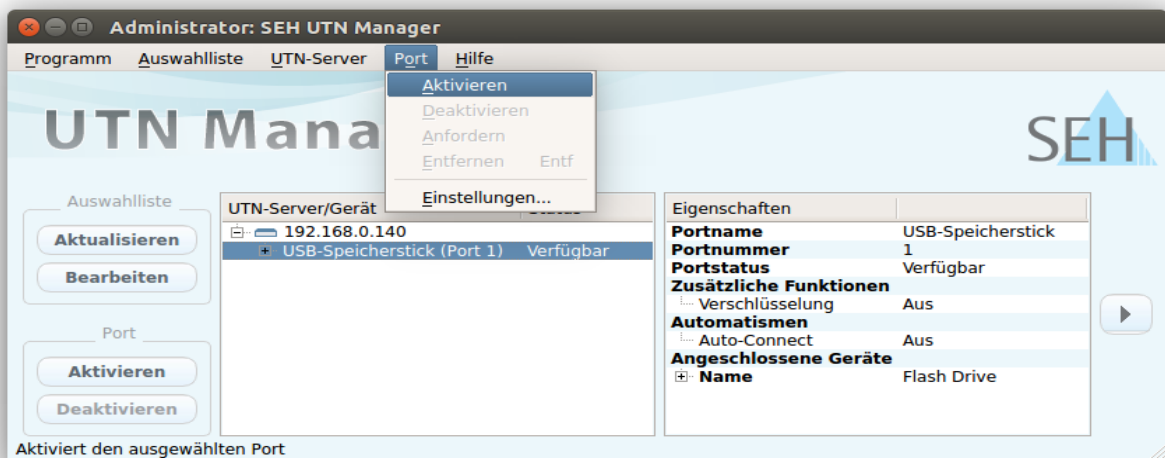


Figure 3.2-2: SEH UTN Manager – USB port activation

3.3 How to End the Connection between the USB Device and the Client

If a USB device is connected to a client, the connection is of a point-to-point type. As long as the connection is established, other users cannot connect the USB device to their client and thus cannot use it. For this reason, you have to end the connection once you are no longer using the USB device.

To end the connection between USB device and client, deactivate the connection between the client and the USB port of the INU server to which the USB device is connected.


- Usually the connection is cut by the user via the SEH UTN Manager ⇒ 13.
- The administrator can also end the connection from the INU Control Center ⇒ 25.
- You can also set up an automatic deactivation (Auto Disconnect) .

Disconnecting the Device Using the SEH UTN Manager

- ✓ The SEH UTN Manager (complete version) is installed on the client ⇒ 13.
- ✓ The USB port is shown in the selection list ⇒ 22.
- ✓ The USB port is connected to your client ⇒ 24.

1. Start the SEH UTN Manager.
2. In the selection list, select the port.
3. Select **Port – Deactivate** from the menu bar.
↳ The connection will be deactivated.

Disconnecting the Device Using the INU Control Center

- ✓ A USB port is connected to your client ⇒ 24.
1. Start the INU Control Center.
 2. Select **DASHBOARD**.
 3. Choose the active connection from the **Attached devices** list and click the  icon.
 4. Confirm the security query.
↳ The connection will be deactivated.

3.4 How to Request an Occupied USB Device

If a USB device is connected to a client, the connection is of a point-to-point type. As long as the connection is established, other users cannot connect the USB device to their client and thus cannot use it.

If you want to use an occupied USB device, you can request it. The other user will receive a release request in form of a pop up. If the user follows your request and releases the USB device by deactivating the connection to the USB device, the connection between the USB device and your client will automatically be activated.

- ✓ The SEH UTN Manager (complete version) is installed on the client ⇒ 13.
 - ✓ The SEH UTN Manager (complete version) is installed on the client of the user who uses the USB device ⇒ 13.
 - ✓ The SEH UTN Manager (complete version) is executed with graphical user interface on both clients.
 - ✓ The USB port is shown in the selection list ⇒ 22.
 - ✓ The USB port is connected to another client ⇒ 24 (but not via Auto-Connect).
5. In the selection list, select the port.
 6. In the menu bar, select **Port – Request**.
 - ↳ The release request will be sent.

3.5 How to Automate USB Device Connections and Program Starts

Connections to USB ports of the INU server and the connected USB devices can be automated. Simple to complex processes can be implemented.

- Automatic Connection If a USB Device Is Connected (Auto-Connect) ⇒ 27
- Automatic Deactivation of the Connection after a Time Defined (Auto-Disconnect) ⇒ 28



This chapter describes features of the SEH UTN Manager with which automa-tisms are set up. Users who have expert knowledge in scripting should use the command line tool 'utnm' ⇒ 34.

Automatic Connection If a USB Device Is Connected (Auto-Connect)

Auto-Connect automatically establishes a connection to a USB port and the connected USB device as soon as a USB device is connected to the USB port. Auto-Connect must be activated for each USB port and works for all USB devices which are connected to the USB port.

- ✓ The SEH UTN Manager (complete version) is installed on the client ⇒ 13.
 - ✓ The USB port is shown in the selection list ⇒ 22.
 - ✓ You are logged on to the client as administrator.
1. Start the SEH UTN Manager.
 2. Select the INU server from the selection list.
 3. In the menu bar, select **UTN server – Activate Auto-Connect**.
The dialog **Activate Auto-Connect** appears.
 4. Tick the option for the desired USB ports.
 5. Click **OK**.
- ↳ The setting will be saved. The connection to the USB port and the connected USB device is automatically and immediately activated. If you disconnect the USB device and reconnect it, the connection is again automatically established.



Important:

If you manually deactivate an active USB port connection that was established via Auto-Connect, Auto-Connect will be switched off. If you want to use Auto-Connect again, you will need to reconfigure it later.

Automatic Deactivation of the Connection after a Time Defined (Auto-Disconnect)

Auto-Disconnect deactivates the connection to a USB port and the connected USB device after a previously defined time. 2 minutes before time runs out, the user will receive a notification and is asked to deactivate their connection in order to prevent data loss and error states. Optionally, a one-off prolongation of the connection by the duration of the defined time can be activated. In this case, the user can choose to prolong the connection or decline it when the notification pops up. Auto-Disconnect allows a large number of network participants to access a small number of devices and avoids idle times.



Important:

With RHEL and Oracle 8, the auto-disconnect only works when the firewall is disabled or with a suitable firewall configuration.

The following ports must be enabled for this purpose:

- UDP port 427 (SLP multicast)
- TCP/IP port 9300 and 9301 (internal communication between SEH UTN Manager and SEH UTN Service)
- TCP/IP port 9310 (device request in the SEH UTN Manager)
- TCP/IP-Port 9200/9443 (data transfer between the SEH UTN Manager and the UTN server)

Please also refer to the documentation of Oracle:

<https://docs.oracle.com/en/operating-systems/oracle-linux/8/firewall/F20786.pdf>

All adjustments to the firewall must be made on your own responsibility.



You can be notified about the free port if a connection is automatically disconnected. For this purpose, set up a notification if the USB port is available ⇨ 56.

- ✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 13.
 - ✓ The INU server is displayed in the 'Automatic Device Disconnect' area ⇨ 22.
 - ✓ You are logged on to the client as administrator.
1. Start the SEH UTN Manager.
 2. Select the INU server in the selection list.
 3. In the UTN Server menu, select the command "Activate Auto Disconnect".
The Activate **Auto Disconnect** dialog appears.
 4. Activate the option for the desired USB ports.
 5. Define the desired time period (10-9999 minutes).
 6. Activate the **Extension** option if required.
 7. Select the **OK** button.
- ↳ The setting is saved

3.6 How to Find Status Information on USB Ports and USB Devices

You can check the status of USB ports and USB devices at any given time. You can also configure automatic messages. You can use automatic messages to be notified when a USB port becomes available or to receive information about the connection duration.



Important:

Automatic messages might not appear.

Messages depend on the system's window manager. Due to the multitude of Linux varieties (and window managers) notification via message might not be supported.

- Displaying Status Information ⇒ 29
- Notification If a USB Port Becomes Available ⇒ 29
- Message about the Duration of a Connection ⇒ 29

Displaying Status Information

- ✓ The SEH UTN Manager (complete version) is installed on the client .
 - ✓ The USB port is shown in the selection list ⇒ 22.
1. Start the SEH UTN Manager.
 2. Select the USB port from the selection list.
- ↳ The status information is displayed in the **Properties** area.

Notification If a USB Port Becomes Available

You will receive a message once a network participant deactivates the connection to a USB port and the connected USB device.



Important:

With Gnome Shell 3.32 (primarily with RHEL8 and Oracle 8) the system tray is missing.

Notifications work only when the system tray of the Linux system is restored.

Use for example the extension „TopIcons Plus“

<https://www.maketecheasier.com/restore-legacy-system-tray-gnome-shell/>

All adjustments must be made on your own responsibility.

- ✓ The SEH UTN Manager (complete version) is installed on the client ⇒ 13.
 - ✓ The USB port is shown in the selection list ⇒ 22.
1. In the selection list, select the port.
 2. In the menu bar, select **Port – Settings**.
The **Port Settings** dialog appears.
 3. Tick the option under **Messages**.
 4. Click **OK**.
- ↳ The setting will be saved.

Message about the Duration of a Connection

You will receive a message if one of your connections to a USB port and the connected USB device exceeds a defined time period.

- ✓ The SEH UTN Manager (complete version) is installed on the client ⇒ 54.

1. In the menu bar, select **Program – Options**.
The **Options** dialog appears.
2. Select the **Program** tab.
3. In the **Messages** area, tick the option.
4. Define the desired duration.
5. Click **OK**.
↳ The setting will be saved.

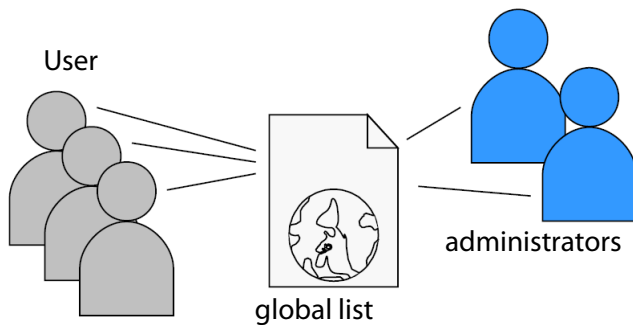
3.7 How to Use the Selection List and Manage User Access Rights with It

The selection list is the main element in the SEH UTN Manager and shows all embedded INU servers. USB devices can only be used if the INU server to which they are connected is on the list (⇒ 22). By controlling the selection list you consequently control the user's access to INU servers and the connected USB devices.

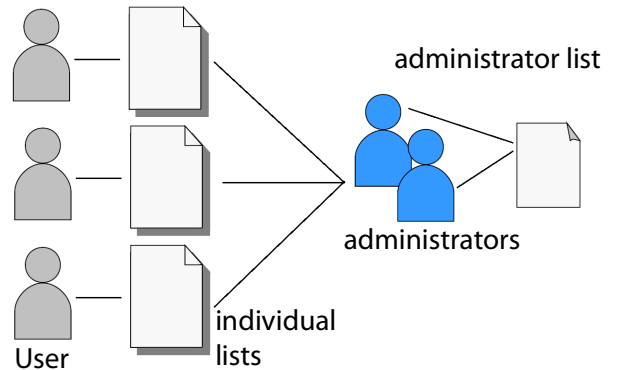
By default, all client users use the global selection list in the SEH UTN Manager. However, you can set a user selection list for the client users. This list can be compiled by the users themselves. Alternatively, you as client administrator restrict user rights and provide a list with which only the INU servers you define can be used.

Table 3.7-1: Differences in global and user selection list

Global Selection List



User Selection List



- All users of a client use the same selection list.
- The users can access all devices listed in the selection list. (Provided that no security mechanisms have been specified via the INU Control Center.)
- List is stored at: /etc
- The selection list can be edited by administrators.
- Each user has their own selection list. All administrators have the same selection list.
- The users can access all devices listed in the selection list. (Provided that no security mechanisms have been specified via the INU Control Center.)
- List ('ini'-file) is stored at:


```
$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini
```

 (\$HOME is an environment variable for the user folder in Linux ; the path for the current user can be determined as follows from the command line: `echo $HOME`)

Example Ubuntu 14.04.01 LTS:

```
echo $HOME yields /Usershome/User name +
.config/SEH Computertechnik GmbH/SEH UTN Manager.ini
```

 Complete path to the ini file:


```
/Usershome/User name/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini
```
- The selection list can be edited by administrators or by users with write access to the ini-file. Users with read-only access to the ini-file cannot edit the selection list and have limited access to SEH UTN Managers functions.



Which functions (selection list editing etc.) can be used in the SEH UTN Manager depends on the selection list type (global/user) and user account type on the client (administrator/user; user with/without write access to ini-file). For a detailed breakdown see ⇒ Figure 8.4 119.

- Setting Up the Global Selection List for All Users ⇒ 32
- Providing User Selection Lists ⇒ 32
- Restrict Write Access to the 'SEH UTN Manager.ini'-file ⇒ 33

Setting Up the Global Selection List for All Users

The global selection list is used by default.

- ✓ The SEH UTN Manager (complete version) is installed on the client .
 - ✓ You are logged on to the system as administrator.
1. Start the SEH UTN Manager.
 2. Compose the selection list ⇒ 22.
 3. In the menu bar, select **Program – Options**.
The **Options** dialog appears.
 4. Select the tab **Selection List**.
 5. Tick **Global selection list**.
 6. Click **OK**.
- ↳ The setting will be saved. All users of a client use the same selection list.

Providing User Selection Lists

- ✓ The SEH UTN Manager (complete version) is installed on the client ⇒ 13.
 - ✓ You are logged on to the system as administrator.
1. Start the SEH UTN Manager.
 2. In the menu bar, select **Program – Options**.
The **Options** dialog appears.
 3. Select the tab **Selection List**.
 4. Tick **User selection list**.
 5. Click **OK**.

Optional: With the following steps you provide a predefined selection list.

6. Create a selection list with the desired devices ⇒ 22.
 7. In the menu bar, select **Selection List–Export**.
The **Export to** dialog appears.
 8. Save the file 'SEH UTN Manager.ini' to the user directories:
\$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini (⇒ Table 3.7-1 31)
- ↳ The setting will be saved. Each user uses their individual (predefined) selection list. The administrators share one selection list.

Restrict Write Access to the 'SEH UTN Manager.ini'-file

User selection lists can be set up and edited by the users themselves.

In order to restrict users to just the INU servers you want them to have access to, you can provide a list to users. To do so, you as administrator store a predefined list for the user (⇒ 32) and limit the user to read-only access to the 'SEH UTN Manager.ini'-file. By limiting the user to read-only access, all SEH UTN Manager functions concerning the selection list are disabled for the user.

Use the usual methods of your operating system to turn the ini-files into read-only files. For more information, read the documentation of your operating system.

3.8 How to Use the SEH UTN Manager without Graphical User Interface (utnm)

The SEH UTN Manager is available in two versions ⇒ 13. It can be used without graphical user interface in the minimal version. To do so, the tool 'utnm' is utilized to use UTN features via the console of the operating system:

- directly, by entering commands in a certain syntax and executing them
- via scripts which contain commands in a certain syntax that will be executed automatically and step by step by the command line interpreter



Use scripts to automate frequently recurring command sequences such as port activations.



The execution of scripts can be automated as well, e.g. by means of login scripts.

- Syntax ⇒ 34
- Commands ⇒ 34
- Return ⇒ 37
- Using utnm via Console ⇒ 37
- Creating a utnm Script ⇒ 38

Syntax



```
utnm -c "command string" [-<command>]
```


The executable file 'utnm' can be found in `/usr/bin/`.

Commands

Rules for commands:

- Underlined elements are to be replaced by the appropriate values (e.g. server = IP address or host name of a INU server)
- elements in square brackets are optional.
- not case-sensitive
- only the ASCII format can be read.

Command	Description
<p><code>-c "<u>command string</u>"</code></p> <p>or</p> <p><code>--command "<u>command string</u>"</code></p>	<p>Runs a command. The command is specified in greater detail by the command string. Command strings:</p> <ul style="list-style-type: none"> • activate <u>server port number</u> activates the connection to a USB port and the connected USB device. • activate <u>server vendor ID (VID) product ID (PID)</u> activates the connection to a USB port and the first free connected USB device with the defined IDs, if several identical USB devices are connected to the INU server. • deactivate <u>server port number</u> deactivates the connection to a USB port and the connected USB device. • set autoconnect=true false <u>server port number</u> activates/deactivates Auto-Connect (⇒ 26) for the USB port. • set userportkey=port key <u>server port number</u> stores a USB port key (⇒ 80) locally on the system for the current user account. This way, the USB port key is always automatically sent and does not need to be specified each time with the command <code>-k <u>USB port key</u></code> or <code>--key <u>USB port key</u></code> (see below). (To remove the USB port key use the command string <code>set userportkey= <u>server port number</u></code>) <p> Important: The command only sets the key permanently to make the USB device available. The USB port key configuration is done via the INU Control Center ⇒ 80.</p> <ul style="list-style-type: none"> • set autoconnectportkey=port key <u>server port number</u> stores a USB port key (⇒ 80) locally and system-wide for the Auto-Connect function (⇒ 26). This way, the USB port key is always automatically sent and does not need to be specified each time with the command <code>-k <u>USB port key</u></code> or <code>--key <u>USB port key</u></code> (see below). (To remove the USB port key use the command string <code>set autoconnectportkey= <u>server port number</u></code>) <p> Important: The command only sets the key permanently to make the USB device available. The USB port key configuration is done via the INU Control Center ⇒ 80.</p> <ul style="list-style-type: none"> • find [IP address-IP address] searches for all INU servers in the network segment and shows the INU servers found with IP address, MAC address, model and software version. IP address ranges can also be searched. • find6 Searches for all INU servers in the network segment via IPv6 and shows the servers found with IP address, MAC address, model and software version.

Command	Description
	<ul style="list-style-type: none"> • <code>state <u>server</u> <u>port</u> <u>number</u></code> displays the status of the USB device connected to the USB port. • <code>getlist <u>server</u></code> shows an overview of the USB devices connected to the INU server (including port number, vendor ID, product ID, vendor name, product name, device class, and status).
-h or --help	Shows the help page.
-k <u>USB port key</u> or --key <u>USB port key</u>	Specifies a USB port key ⇒ 80.  Important: The command only enters the key to make the USB device available. Use the command <code>-c "<u>command string</u>"</code> or <code>--command "<u>command string</u>"</code> to permanently store a USB port key on the system so that it is sent automatically each time (see above). The USB port key configuration is done via the INU Control Center ⇒ 80.
-mr or --machine readable	Separates the output of the command string <code>getlist</code> with tabulators and the output of <code>find</code> with commas.
-nw or --no-warnings	Suppresses warning messages.
-o or --output	Shows the output in the command line.
-p <u>port number</u> or --port <u>port number</u>	Uses an alternative UTN port. Use this command if the UTN port number was changed (⇒ 54).
-q or --quiet	Suppresses the output.
-sp <u>port number</u> or --ssl-port <u>port number</u>	Uses an alternative UTN port with SSL/TLS encryption. Use this command if the UTN SSL port number was changed (⇒ 54).
-t <u>seconds</u> or timeout <u>seconds</u>	Specifies a timeout for the command strings <code>activate</code> and <code>deactivate</code> .
-v or --version	Shows version information about <code>utnm</code> .

Return

After a command is executed, a return indicates success or failure of the process. The returned information is a status combined with a return value (return code). If the output is suppressed ('--quiet' ⇒ 136), only the value is returned.

The return can be used to determine how the process proceeds, e.g. in a script.

Return Value	Description
0	The command was executed successfully.
20	Activation failed.
21	Deactivation failed.
23	Is already activated.
24	Is already deactivated or not available.
25	Activation failed: Another user has activated the USB port incl. device.
26	Not found: There is no device connected to the USB port or the USB port key (⇒ 180) is missing or wrong.
29	Not found: No USB device with this VID and PID connected.
30	Isochronous USB devices are not supported.
31	UTN driver error. Contact the SEH Computertechnik GmbH support ⇒ 17.
40	No network connection to the INU server.
41	An encrypted connection to INU server cannot be established.
42	No connection to UTN service.
43	The DNS resolution failed.
44	Insufficient rights (administrative rights required).
47	This feature is not supported.
200	Error (with error code).

Using utnm via Console

- ✓ The SEH UTN Manager is installed on the client ⇒ 13.
- ✓ The IP address or host name of a INU server is known.

1. Open a **Console**.
2. Enter the sequence of commands; see 'Syntax' ⇒ 134 and 'Commands' ⇒ 134.
3. Confirm your entry.
 - ↳ The sequence of commands will be run.

Example: Activating a USB device on port 3 of the INU server with the IP address 10.168.1.167

```
utnm -c "activate 10.168.1.167 3"
```

Creating a utnm Script


- ✓ The SEH UTN Manager is installed on the client ⇒ 13.
 - ✓ The IP address or host name of a INU server is known.
 - ✓ You know how to create and use scripts in your operating system. If needed, refer to the documentation of your operating system.
1. Open a text editor.
 2. Enter the sequence of commands; see 'Syntax' ⇒ 34, 'Commands' ⇒ 34, and 'Return' ⇒ 37.
 3. Save the file as executable script on your client.
- ↳ The script is saved and can be used.

4 Network Settings

To optimally embed your INU server into your network, you can configure the following settings:


- [How to Configure IPv4 Parameters](#) ⇨ 40
- [How to Configure IPv6 Parameters](#) ⇨ 42
- [How to Use the INU Server in VLAN Environments](#) ⇨ 43
- [How to Configure the DNS](#) ⇨ 45
- [How to Configure Email \(POP3 and SMTP\)](#) ⇨ 46
- [How to Configure Bonjour](#) ⇨ 48
- [How to Configure Server Services](#) ⇨ 49


4.1 How to Configure IPv4 Parameters




In the hardware installation (⇒  'Hardware Installation Guide') the INU server is connected to the network. The INU server then checks if it receives an IPv4 network configuration (IP address, subnet mask, gateway, DNS - Domain Name Service) dynamically over DHCP (Dynamic Host Configuration Protocol). If this is not the case, the INU server assigns itself an IP address via Zeroconf from the address range which is reserved for Zeroconf (169.254.0.0/16).



Important:

If the INU server is connected to an IPv6 network, it will automatically receive an additional IPv6 address ⇒ 42.

The IPv4 address assigned to the INU servers can be found via the SEH UTN Manager software tool. This step usually is carried out during the initial set up (⇒  'Quick Installation Guide'). As an alternative to automatic configuration via DHCP or Zeroconf, you can assign a manual (static) IPv4 network configuration to the INU server.

- Assigning an IPv4 network configuration using the INU Control Center ⇒ 40
- Assigning an IPv4 Network Configuration using the SEH UTN Manager ⇒ 41
- Determining the IPv4 Address using the SEH UTN Manager and Assigning an IPv4 Network Configuration ⇒ 41

Assigning an IPv4 network configuration using the INU Control Center




- ✓ For DHCP: Your network has a DHCP server.
 - ✓ For DNS: Your network has a DNS server.
1. Start the INU Control Center.
 2. Select **NETWORK – IPv4**.
 3. Configure the IPv4 parameters; ⇒ Table 4.1-1 40.
 4. Click **Save & Restart** to confirm.
 - ↳ The settings will be saved.

Table 4.1-1: IPv4 parameters

Parameters	Description
DHCP	<p>Enables/disables the DHCP protocol.</p> <p>If DHCP is enabled in your network, IPv4 network configuration (IP address, subnet mask, gateway, DNS) is automatic.</p> <div style="text-align: right;">  <i>We recommend disabling this option once an IP address has been assigned to the INU server.</i> </div>
ARP/PING	<p>Enables/disables the ARP/PING protocol.</p> <p>You can use the commands ARP and PING to change an IP address. The implementation depends on your system; read the documentation of your operating system.</p> <div style="text-align: right;">  <i>We recommend disabling this option once an IP address has been assigned to the INU server.</i> </div>
IP Address	IP address of the INU server.

Parameters	Description
Prefix length	The IP address and the prefix length defines the network mask of the INU server. Subnet masks are used to logically partition big networks into subnetworks. If you are using the INU server in a subnetwork, it requires the subnet mask of the subnetwork.
Router	Router address (Gateway) of the INU server IP addresses in another network are addressed via the router address.

Assigning an IPv4 Network Configuration using the SEH UTN Manager

- ✓ The SEH UTN Manager (complete version) is installed on the client ⇒ 13.
 - ✓ The INU server is shown in the selection list ⇒ 22.
1. Start the SEH UTN Manager.
 2. In the selection list, select the INU server.
 3. In the menu bar, select **UTN Server–Set IP Address**.
The **Set IP Address dialog** appears.
 4. Enter the relevant TCP/IP parameters.
 5. Click **OK**.
↳ The settings will be saved.

Determining the IPv4 Address using the SEH UTN Manager and Assigning an IPv4 Network Configuration

The SEH UTN Manager searches the network for connected INU servers.

- ✓ The SEH UTN Manager (complete version) is installed on the client ⇒ 13.
1. Start the SEH UTN Manager.
 2. Confirm the note dialog **Your Selection List seems to be empty** with **Yes**.
If no note dialog is available and the main dialog appears, select **Selection List–Edit** in the menu bar.
The **Edit Selection List** dialog appears.
 3. In the network list, select the INU server.



If you are using several INU servers of the same model, you can identify a specific device by its default name (⇒ 40) or the connected USB devices.

4. In the shortcut menu, select **Set IP Address**.
The **Set IP Address** dialog appears.
5. Enter the relevant TCP/IP parameters.
6. Click **OK**.
↳ The settings will be saved.

4.2 How to Configure IPv6 Parameters

IPv6 (Internet Protocol Version 6) is the successor of the still predominantly used IPv4 (Internet Protocol Version 4). IPv6 offers the same basic functions but has many advantages such as the increased address space of 2^{128} (IPv6) instead of 2^{32} (IPv4) IP addresses and auto configuration.



Important:

IPv6 address notation differs from IPv4: An IPv6 address consists of 128 bits. The normal format of an IPv6 address is eight fields. Each field contains four hexadecimal digits representing 16 bits.

Example: `2001:db8:4:0:2c0:ebff:fe0f:3b6b`

As a URL in a Web browser, an IPv6 address must be enclosed in square brackets. This prevents port numbers from being mistakenly regarded as part of an IPv6 address.

Example: `http://[2001:db8:4:0:2c0:ebff:fe0f:3b6b]:443`

The URL will only be accepted by browsers that support IPv6.

You can embed the INU server into an IPv6 network.

The INU server will automatically receive one or more IPv6 addresses in addition to its IPv4 address. To optimally embed the INU into your network, you can configure IPv6 parameters.

1. Start the INU Control Center.
2. Select **NETWORK – IPv6**.
3. Configure the IPv6 parameters; ⇒ Table 4.2-2 42.
4. Click **Save & Restart** to confirm.
 - ↳ The settings will be saved.

Table 4.2-2: IPv6 parameters

Parameters	Description
IPv6	Enables/disables the IPv6 functionality of the INU server.
Automatic configuration	Enables/disables the automatic assignment of the IPv6 address to the INU server.
IPv6 address	<p>Defines an IPv6 unicast address in the format <code>n:n:n:n:n:n:n</code> which is manually assigned to the INU server.</p> <ul style="list-style-type: none"> • Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. • Leading zeros can be omitted. • An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.
Router	Manually defines a static router to which the INU server sends its requests.
Prefix length	<p>Defines the length of the subnet prefix for the IPv6 address. The value 64 is pre-set.</p> <p>Address ranges (e.g. your network) are specified with prefixes. To do this, the prefix length (number of bits used) is added to the IPv6 address as a decimal number and the decimal number is preceded by '/'.</p>

4.3 How to Use the INU Server in VLAN Environments

The INU server supports VLAN (Virtual Local Area Network) according to 802.1Q.

A VLAN divides a physical network into logical subnetworks. Each subnetwork is its own broadcast domain, so data packets cannot be exchanged between subnetworks. VLANs are used to structure networks and, above all, to secure them.

Each USB device can be assigned to a VLAN. To transfer VLAN data via the USB ports, you must first enter the VLANs on the INU server. After this, the USB ports used for forwarding data must be linked to the specified VLANs.



The access to USB devices can be regulated particularly well with VLAN: a defined group of network users may use certain USB devices.

Inform yourself on how to implement VLAN in your environment and then set up the INU server for it.



Important:

SNMP works only over LAN and the VLAN specified in the selection menu.

- Configure IP management VLAN ⇒ 43
- Define a IP Client VLAN ⇒ 44
- Allocating a IP Client VLAN to a USB Port ⇒ 44

Configure IP management VLAN

1. Start the INU Control Center.
2. Select **NETWORK – IP VLAN**.
3. Configure the IP VLAN parameters; ⇒ Table 4.3-3 43.
4. To confirm, click **Save**.
5. The settings will be saved.

Table 4.3-3: IP management VLAN parameters

Parameters	Description
IP management VLAN	Enables/disables the forwarding of IP management VLAN data. If this option is enabled, SNMP is only available in the IP management VLAN.
Management VLAN selection menu	Sets the management VLAN in the network. Note: From the configured Client VLANs (⇒ Table 4.3-4 44), you can select a specific one or each as a management VLAN.
TCP Access via LAN (untagged)	Enables/disables the web access INU Control Center to the INU server via IP packets without tag. If this option is disabled, the INU server can only be administrated via VLANs. Note: The SNMP works exclusively via LAN and the VLAN specified in the selection menu.

Define a IP Client VLAN

1. Start the INU Control Center.
2. Select **NETWORK – IP VLAN**.
3. Configure the IP VLAN parameters; ⇨ Table 4.3-4 44.
4. To confirm, click **Save**.
 - ↳ The settings will be saved.

Table 4.3-4: IP client VLAN parameters

Parameters	Description
VLAN	Enables/disables the forwarding of IP client VLAN data.
IP Address	IP address of the INU server within the IP client VLAN.
Prefix length	The IP address and the prefix length defines the network mask of the INU server.
Router	Router address of the IP client VLAN.
VLAN ID	ID for the identification of the IP client VLAN (0–4096).





Use **Auto-fill** to automatically fill **VLAN**, **IP address** and **Subnetmask** with the values from line 1. **VLAN ID** will automatically be counted up by '1'.

Allocating a IP Client VLAN to a USB Port

1. Start the INU Control Center.
2. Select **SECURITY – USB**.
3. Select the appropriate VLAN assignment from the **VLAN** drop-down list.
4. To confirm, click **Save**.
 - ↳ The settings will be saved.

4.4 How to Configure the DNS

The DNS - Domain Name Service is responsible for resolving IP addresses and domain name addresses in a network. The INU server dynamically configures the DNS using the protocol DHCP (Dynamic Host Configuration Protocol). during the IP network configuration. This step usually is carried out during the initial set up (⇒  'Quick Installation Guide') of the INU server during the hardware installation (⇒  'Hardware Installation Guide').

As an alternative to automatic configuration via DHCP or Zeroconf, you can assign a manual (static) IPv4 network configuration to the INU server.

Configure DNS via utnserver Control Center ⇒  **45 Configure DNS via utnserver Control Center**




- ✓ For DHCP: Your network has a DHCP server.
 - ✓ For DNS: Your network has a DNS server.
1. Start the INU Control Center.
 2. Select **NETWORK – DNS**.
 3. Configure the DNS parameters; ⇒ Table 4.4-5 .
 4. Click **Save & Restart** to confirm.
- ↳ The settings will be saved.

Table 4.4-5: DNS parameters

Parameters	Description
DNS	<p>Enables/disables the name resolution via a DNS server.</p> <div style="border-left: 2px solid #00a0e3; padding-left: 10px; margin-top: 10px;">  <p>Important: Only DNS allows you to use host names instead of IP addresses if you define servers such as e.g. a time server on the INU server. Example: Time server configuration (⇒  53) with <code>ntp.server.de</code> instead of <code>10.168.0.140</code>.</p> </div>
Primary DNS server	Defines the IP address of the primary DNS server.
Secondary DNS server	<p>Defines the IP address of the secondary DNS server.</p> <p>The secondary DNS server is used if the first one is not available.</p>
Domain name (suffix)	Defines the domain name of an existing DNS server.
Preferred address type	Specifies which address type is used after the IP address is returned from the DNS server. (This option is only relevant if „IPv4 and IPv6“ is enabled.)

4.5 How to Configure Email (POP3 and SMTP)

The INU server uses email for a range of functions:

- The INU server can be administered using email ⇒ 19.

The notification service will send you status and error messages over email ⇒ 56. To use these features, the 'POP3' and 'SMTP' email protocols must be configured on the INU server.

- POP3 (Post Office Protocol Version 3), to allow the INU server to retrieve email from an email server.
- Simple Mail Transfer Protocol (SMTP) to send email.

For this, the INU server (client) needs an email user account on an email server.

- Configuring POP3 ⇒ 46
- Configuring SMTP ⇒ 47

Configuring POP3

✓ An email user account for the INU server is set up on a POP3 server.

1. Start the INU Control Center.
2. Select **NETWORK – Email**.
3. Configure the POP3 parameters; ⇒ Table 4.5-6 46.
4. To confirm, click **Save**.
↳ The settings will be saved.

Table 4.5-6: POP3 parameters

Parameters	Description
POP3	Enables/disables the POP3 functionality.
POP3 – Server Address	Defines the POP3 server via its IP address or host name. A host name can only be used if a DNS server (⇒ 40) was configured beforehand.
POP3 – Server Port	Defines the port which the INU server uses to receive emails. The default port number for POP3 is 110. The default port number for SSL/TLS (parameter 'POP3 – Security' ⇒ 46) is 995. If required, read the documentation of your POP3 server.
POP3 – Security	Defines the authentication method to be used: <ul style="list-style-type: none"> • APOP: encrypts the password when logging on to the POP3 server. • SSL/TLS: encrypts the entire communication with the POP3 server. The encryption strength is defined via the encryption protocol and level ⇒ 65.
POP3 – Check mail every	Defines the time interval (in minutes) which with the POP3 server is checked for emails.
POP3 – Ignore mail exceeding	Defines the maximum email size (in Kbyte) to be accepted by the INU server. (0 = unlimited)
POP3 – User name	Defines the user name used by the INU server to log on to the POP3 server.
POP3 – Password	Defines the user password used by the INU server to log on to the POP3 server.

Configuring SMTP

- ✓ An email user account for the INU server is set up on an SMTP server.
- 1. Start the INU Control Center.
- 2. Select **NETWORK – Email**.
- 3. Configure the SMTP parameters; ⇨ Table 4.5-7 ¶47.
- 4. To confirm, click **Save**.
 - ↳ The settings will be saved.

Table 4.5-7: SMTP Parameters

Parameters	Description
SMTP – Server Address	Defines the SMTP server via its IP address or host name. A host name can only be used if a DNS server (⇨ ¶40) was configured beforehand.
SMTP – Server Port	Defines the port which the INU server and SMTP server use to communicate. The default port number for SMTP is 25. For SSL/TLS (parameter 'SMTP – SSL/TLS' ⇨ ¶47), SMTP servers use by default port 587 (STARTSSL/STARTTLS) or the old port 465 (SMTPS). If required, read the documentation of your SMTP server.
SMTP – SSL/TLS	Enables/disables SSL/TLS. SSL/TLS encrypts the communication from the INU to the SMTP server. The encryption strength is defined via the encryption protocol and level ⇨ ¶65.
SMTP – Sender name	Defines the email address used by the INU server to send emails. Very often the name of the sender and the email account user name are identical.
SMTP – Login	Enables/disables SMTP authentication. To send emails, the INU sends its user name and password to the SMTP server to authenticate itself. Enter user name (parameter 'SMTP – User name' ⇨ ¶47) and password (parameter 'SMTP – Password' ⇨ ¶47). Some SMTP servers require SMTP authentication to prevent fraudulent use (spam).
SMTP – User name	Defines the user name used by the INU server to log on to the SMTP server.
SMTP – Password	Defines the password used by the INU server to log on to the SMTP server.
SMTP – Security (S/MIME)	Enables/disables signing email using S/MIME (Secure/Multipurpose Internet Mail Extensions). A signature created by the sender allows the recipient to verify the identity of the sender and to make sure that the email was not modified. All S/MIME security features require an S/MIME certificate ⇨ ¶71.
SMTP – Attach public key	Sends the public key together with the email. Many email clients require the public key to be attached in order to view the emails.
SMTP – Encrypt	Enables the encryption of emails. Only the intended recipient can open and read the encrypted email.

4.6 How to Configure Bonjour

Bonjour is a technology which automatically detects devices and services in TCP/IP networks.

The INU server uses Bonjour to

- verify IP addresses
 - announce and find network services
 - match host names and IP addresses
1. Start the INU Control Center.
 2. Select **NETWORK – Bonjour**.
 3. Configure the Bonjour parameters; ⇨ Table 4.6-8 48.
 4. To confirm, click **Save**.
 - ↳ The settings will be saved.

Table 4.6-8: Bonjour parameters

Parameters	Description
Bonjour	Enables/disables Bonjour.
Bonjour name	Defines the Bonjour name of the INU server. The INU server uses this name to announce its Bonjour services. If no Bonjour name is entered, a default name will be used (device name@ICxxxxxx).

4.7 How to Configure Server Services

Some features of the INU server are based on services running on external servers:

- Monitoring (⇒ 58): Export the collected values to a WebDAV and/or syslog-ng server.
- Backup (⇒ 88): Save a system backup to a WebDAV server.

To use these features, you must first implement the corresponding server service on your network. Then configure the basic server service settings and functionality on the INU server.

- 'WebDAV Server Configuration' ⇒ 49
- " ⇒ 49

WebDAV Server Configuration

The WebDAV (Web-based Distributed Authoring and Versioning) protocol allows you to transfer files and directories over HTTP. The protocol also has a versioning mechanism.

How you implement WebDAV in your network depends on your network environment. You must handle this implementation yourself.

- ✓ Your network has a WebDAV server.
 1. Start the INU Control Center.
 2. Select **NETWORK – Server**.
 3. Tick the **WebDAV** option.
 4. Configure the WebDAV parameters; ⇒ Table 4.7-1 49.
 5. To confirm, click **Save**.
 - ↳ The settings will be saved.

Table 4.7-1: WebDAV parameters

Parameters	Description
Server address	Defines a WebDAV server by its IP address or host name. A host name can only be used if a DNS server (⇒ 40) was configured beforehand.
User name	Defines the user name used by the INU server to log on to the WebDAV server.
Password	Defines the password used by the INU server to log on to the WebDAV server.
SSL/TLS	Enables/disables SSL/TLS encryption of communication between the INU server and WebDAV server. The encryption strength is defined via the encryption protocol and level ⇒ 65.

syslog-ng Server Configuration

The syslog-ng protocol allows you to transmit log messages (monitoring data in this case) to a syslog-ng server over the network. The received data can be written to a database or forwarded to other servers, for example.

How you implement syslog-ng in your network depends on your network environment. You must handle this implementation yourself.

- ✓ Your network has a syslog-ng server.
- 1. Start the INU Control Center.
- 2. Select **NETWORK – Server**.
- 3. Tick the **syslog-ng** option.
- 4. Configure the syslog-ng parameters; ⇒ Table 4.7-2 ¶50.
↳ To confirm, click **Save**.

Table 4.7-2: syslog-ng parameters

Parameters	Description
Server address	Defines a syslog-ng server by its IP address or host name. A host name can only be used if a DNS server (⇒ ¶40) was configured beforehand.
Server port	Defines the port number used by the INU server to communicate with the syslog-ng server. The port number 514 is preset.
SSL/TLS	Enables/disables SSL/TLS encryption of communication between the INU server and syslog-ng server. The encryption strength is defined via the encryption protocol and level ⇒ ¶65.

5 Device Settings

- How to Assign a Description ⇨ 52
- How to Configure the Device Time ⇨ 53
- How to Configure the (Encrypted) UTN Port ⇨ 54
- How to Write a Description for a USB port ⇨ 55
- How to Get Messages ⇨ 56
- How to Monitor the INU Server ⇨ 58
- How to Use the Relay ⇨ 62

5.1 How to Assign a Description

You can assign freely definable descriptions to the INU server. This gives you a better overview of the devices in the network.



You can also assign names to USB ports to distinguish them ⇔ 79.

1. Start the INU Control Center.
2. Select **DEVICE – Description**.
3. Enter freely definable names for **Host name**, **Description**, and **Contact person**.
4. To confirm, click **Save**.
 - ↳ The settings will be saved.

Table 5.1-1: Description

Parameters	Description
Host name	Device name as alternative to IP address. With a name you can identify the INU server more easily in the network, e.g. if you are using several INU servers. Is displayed in the INU and SEH UTN Manager.
Description	Device description, e.g. location or department. Is displayed in the INU and SEH UTN Manager.
Contact person	Contact person, e.g. device administrator. Is displayed in the INU Control Center.

5.2 How to Configure the Device Time

The INU server has a device time. Correct time information is required for some network mechanisms, such as authentication for example. Device monitoring (⇒ 58) also uses the device time as the timestamp.

The device time of the INU server can be set via an SNTP time server (Simple Network Time Protocol) in the network. A time server synchronizes the time of devices within a network.



We recommend the use of a time server for regular operation, and use of the device clock only for special cases such as the initial installation. This is because a time server guarantees an accurate and synchronous time for all network participants.

In general, today's primary time standard 'UTC' (Universal Time Coordinated) is used. The time zone compensates for location.



Important:

If your network is configured accordingly, the INU server receives the time server settings automatically via DHCP (⇒ 40). A time server assigned in such a manner always takes precedence over a manually set time server and the device clock.

- Time zone configuration ⇒ 53
- Device time configuration via time server ⇒ 53

Time zone configuration

The time zone adjusts the device time (set using the device clock or received from a time server) to your local zone time including country-specific features such as daylight saving time.

1. Start the INU Control Center.
 2. Select **DEVICE – Date/Time**.
 3. From the **Time zone** list, select the code for your local time zone.
 4. To confirm, click **Save**.
- ↳ The settings will be saved.

Device time configuration via time server

- ✓ The network has a time server.
1. Start the INU Control Center.
 2. Select **DEVICE – Date/Time**.
 3. Tick the **Time Server** option.
 4. Enter the IP address or the host name of the time server in the **Server Address** field.
(The host name can only be used if a DNS server was configured beforehand ⇒ 40.)
 5. To confirm, click **Save**.
- ↳ The settings will be saved

5.3 How to Configure the (Encrypted) UTN Port

A shared port is used for the data transfer between the INU server (including connected USB devices) and the client. It depends on the connection type:

- unencrypted connection: UTN port (default = 9200)
- encrypted connection (⇒ ⓘ86): encrypted UTN port (default = 9443)



WARNING


The UTN port or encrypted UTN port must not be blocked by security software (firewall).

You can change the port number, e.g. if the port number is already used for another application in your network. The change is made on the INU server and is relayed to the SEH UTN Manager installed on the clients via SNMPv1.

- ✓ SNMPv1 is enabled ⇒ ⓘ69.
1. Start the INU Control Center.
 2. Select **Device – UTN port**.
 3. Enter the port number into the **UTN port** or **Encrypted UTN port** box.
 4. To confirm, click **Save**.
- ↳ The settings will be saved.

5.4 How to Write a Description for a USB port

Each USB port can be labeled with additional information. This information is displayed next to the corresponding USB port in the SEH UTN manager.

1. Start the INU Control Center.
2. Select **SECURITY – USB**.
3. In the USB port table for the desired USB port, click the **Change**  icon.
The **USB Port** page appears.
4. Type the information in the **Description** field (maximum length 128byte = 128 ASCII characters).



*With the input
 you create a line break.*

5. To confirm, click **Save**.
↳ Your entry will be saved as a description of the USB port and displayed in the SEH UTN manager.

5.5 How to Get Messages

The INU server can send you different messages:

- Status email: Periodically sent email containing the status of the INU server and of the connected USB devices.
- Event notification via email or SNMP trap:
 - System information (restart, network connections, power supply, temperature warnings, etc.)
 - USB port and USB device information (enabling or disabling a USB port, connecting or disconnecting a USB device, etc.)

You can customize the content of the e-mail subject line.

- Configuring the sending of status emails ⇒ 56
- Configuring event and system notifications via email ⇒ 56
- Customizing the email subject ⇒ 57
- Configuring event and system notifications via SNMP traps ⇒ 57

Configuring the sending of status emails

The status email can be sent to up to two recipients.

- ✓ SMTP is set up ⇒ 46.
 - ✓ DNS is set up ⇒ 40.
1. Start the INU Control Center.
 2. Select **DEVICE – Notification**.
 3. Enter the recipient into the **Email address** box.
 4. Tick the desired recipient(s) in the **Status email** area.
 5. Define the interval.
 6. To confirm, click **Save**.
- ↳ The settings will be saved.

Configuring event and system notifications via email

The event emails can be sent to up to two recipients.

- ✓ SMTP is set up ⇒ 46.
 - ✓ DNS is set up ⇒ 40.
1. Start the INU Control Center.
 2. Select **DEVICE – Notification**.
 3. Enter the recipient into the **Email address** box.
 4. Tick the options with the desired messages.
 5. To confirm, click **Save**.
- ↳ The settings will be saved.

Customizing the email subject

You can specify the content of the email subject line with a–z, A–Z, 0–9 and using variables:

%P = product type %p = model %N = default name %H = host name
%I = IP address %M = MAC address %E = event %D = date %t = time

1. Start the INU Control Center.
2. Select **DEVICE – Notification**.
3. Enter the desired variables in the **Email Subject** box.
4. To confirm, click **Save**.
↳ The settings will be saved.

Configuring event and system notifications via SNMP traps

The event SNMP traps can be sent to up to two recipients.

✓ SNMPv1 or/and SNMPv3 is set up ⇨ 69.

1. Start the INU Control Center.
2. Select **DEVICE – Notification**.
3. Enter the IP address of the recipient in the **Address** box.
4. Enter the community of the recipient in the **Community** box.
5. Select the SNMP protocol version from the **SNMP Version** list.
6. Enable the desired messages in the **Content** area.
7. To confirm, click **Save**.
↳ The settings will be saved.

5.6 How to Monitor the INU Server

The INU server has a monitoring function (logging) that collects various values:

- Error (e.g. missing certificates)
- System status (e.g. restarts)
- Parameter Changes
- USB ports and attached devices (e.g. enable or disable a USB port)
- Device access (e.g. logins)

The collected data is stored on the INU server and can be viewed and deleted directly. You can also export the monitoring logs as a backup

- to your local client
- via WebDAV
- via Email
- via syslog-ng

With syslog-ng the data is continuously exported. With WebDAV and e-mail you can choose between different time intervals:

- Continuous backup: On the INU server, the monitoring logs are divided into 2 MB files. Once this size is reached, the file is transferred.
- Daily backup: Transmits the monitoring logs daily at a defined time.
- Manual backup: Transmits the monitoring logs immediately.

This allows you to integrate monitoring of the INU server appropriately into your network environment and to capture, archive and evaluate the collected data as desired.

- Configuring Monitoring ⇒ [58](#)
- Viewing the Monitoring Log ⇒ [59](#)
- Continuously Exporting Monitoring Logs via WebDAV ⇒ [59](#)
- Saving the Monitoring Log Locally ⇒ [59](#)
- Continuously Exporting Monitoring Logs via WebDAV ⇒ [59](#)
- Exporting Monitoring Logs Daily via WebDAV ⇒ [59](#)
- Immediately Exporting Monitoring Logs via WebDAV ⇒ [60](#)
- Continuously Exporting Monitoring Logs via Email ⇒ [60](#)
- Exporting Monitoring Logs Daily via Email ⇒ [61](#)
- Immediately Exporting Monitoring Logs via Email ⇒ [61](#)
- Exporting Monitoring Logs via syslog-ng ⇒ [61](#)

Configuring Monitoring

1. Start the INU Control Center.
 2. Select **DEVICE – Monitoring**.
 3. In the **Values** area, activate the desired option.
 4. To confirm, click **Save**.
- ↳ The settings will be saved.

Deleting the Monitoring Log

1. Start the INU Control Center.
2. Select **DEVICE – Monitoring**.
3. In the **Monitoring** area, click the **Delete** button.
4. Confirm the security query by clicking **OK**.
 - ↳ The monitoring log is deleted.

Viewing the Monitoring Log

1. Start the INU Control Center.
2. Select **DEVICE – Monitoring**.
3. In the **Monitoring** area, click the **Show log** button.
 - ↳ The log file is displayed on a separate tab.

Saving the Monitoring Log Locally

1. Start the INU Control Center.
2. Select **DEVICE – Monitoring**.
3. In the **Monitoring** area, click the **Export** button.
4. Save the '<default-name>_monitor.txt' file to your client using your browser.
 - ↳ The monitoring log is saved.

Continuously Exporting Monitoring Logs via WebDAV

- ✓ Your network has a WebDAV server.
 - ✓ WebDAV is configured on the INU server ⇒ 49.
 - ✓ Monitoring is enabled ⇒ 58.
1. Start the INU Control Center.
 2. Select **DEVICE – Monitoring**.
 3. In the **WebDAV – Server** area, enter the directory on the WebDAV server where the monitoring logs are to be stored in the **Directory** box.
 4. Optional: If you want to save the monitoring logs for a single day to subfolders, enable the **Create individual directories for days** option.



Important:

The FIFO principle (first-in, first-out) is applied after one year. For example, January 01 of last year is overwritten with the files of the current year January 01.

5. In the **WebDAV – Backup** area, enable the **Continuous Backup** option.
 - ↳ The settings will be saved.

Exporting Monitoring Logs Daily via WebDAV

- ✓ Your network has a WebDAV server.
 - ✓ WebDAV is configured on the INU server ⇒ 49.
 - ✓ Monitoring is enabled ⇒ 58.
1. Start the INU Control Center.
 2. Select **DEVICE – Monitoring**.
 3. In the **WebDAV – Server** area, enter the directory on the WebDAV server where the monitoring logs are to be stored in the **Directory** box.

- Optional: If you want to save the monitoring logs for a single day to subfolders, enable the **Create individual directories for days** option.



Important:

The FIFO principle (first-in, first-out) is applied after one year. For example, 1 January of last year will be overwritten with files from 1 January of the current year.

- In the **WebDAV – Backup** area, enable the **Daily backup at** option.
- From the list, select the hour at which the backup will be transferred.
- To confirm, click **Save**.
 - ↳ The settings will be saved.

Immediately Exporting Monitoring Logs via WebDAV

- ✓ Your network has a WebDAV server.
 - ✓ WebDAV is configured on the INU server ⇒ 49.
 - ✓ Monitoring is enabled ⇒ 58.
- Start the INU Control Center.
 - Select **DEVICE – Monitoring**.
 - In the **WebDAV – Server** area, enter the directory on the WebDAV server where the monitoring logs are to be stored in the **Directory** box.
 - Optional: If you want to save the monitoring logs for a single day to subfolders, enable the **Create individual directories for days** option.



Important:

The FIFO principle (first-in, first-out) is applied after one year. For example, January 01 of last year is overwritten with the files of the current January 01.

- Click the **Export manually now** button.
 - ↳ The monitoring logs are stored on the WebDAV server.

Continuously Exporting Monitoring Logs via Email

- ✓ SMTP is configured on the INU server ⇒ 46.
 - ✓ Monitoring is enabled ⇒ 58.
- Start the INU Control Center.
 - Select **DEVICE – Monitoring**.
 - In the **Email – Recipient** area, enter the email address of the recipient where the monitoring logs will be sent in the **Email Address** box.
 - In the **Email – Recipient** area, enter the content of the email subject line for monitoring log emails in the **Email Subject** box.

(You can specify the content of the email subject line with a–z, A–Z, 0–9 and using variables:

%P = product type	%p = model	%N = default name	%H = host name
%l = IP address	%M = MAC address	%E = event	%D = date
			%t = time)

- In the **Email – Backup** area, enable the **Continuous Backup** option.
- To confirm, click **Save**.
 - ↳ The settings will be saved.

Exporting Monitoring Logs Daily via Email

- ✓ SMTP is configured on the INU server ⇒ 46.
 - ✓ Monitoring is enabled ⇒ 58.
1. Start the INU Control Center.
 2. Select **DEVICE – Monitoring**.
 3. In the **Email – Recipient** area, enter the email address of the recipient where the monitoring logs will be sent in the **Email Address** box.
 4. In the **Email – Recipient** area, enter the content of the email subject line for monitoring log emails in the **Email Subject** box.
(You can specify the content of the email subject line with a–z, A–Z, 0–9 and using variables:

%P = product type	%p = model	%N = default name	%H = host name
%l = IP address	%M = MAC address	%E = event	%D = date
			%t = time)
 5. In the **Email – Backup** area, enable the **Daily backup at** option.
 6. From the list, select the hour at which the backup will be transferred.
 7. To confirm, click **Save**.
- ↳ The settings will be saved.

Immediately Exporting Monitoring Logs via Email

- ✓ SMTP is configured on the INU server ⇒ 46.
 - ✓ Monitoring is enabled ⇒ 58.
1. Start the INU Control Center.
 2. Select **DEVICE – Monitoring**.
 3. In the **Email – Recipient** area, enter the email address of the recipient where the monitoring logs will be sent in the **Email Address** box.
 4. In the **Email – Recipient** area, enter the content of the email subject line for monitoring log emails in the **Email Subject** box.
(You can specify the content of the email subject line with a–z, A–Z, 0–9 and using variables:

%P = product type	%p = model	%N = default name	%H = host name
%l = IP address	%M = MAC address	%E = event	%D = date
			%t = time)
 5. Click the **Export manually now** button.
↳ The monitoring logs will be sent by email.

Exporting Monitoring Logs via syslog-ng

- ✓ Your network has a syslog-ng server.
 - ✓ syslog-ng is configured on the INU server ⇒ 49.
 - ✓ Monitoring is enabled ⇒ 58.
1. Start the INU Control Center.
 2. Select **DEVICE – Monitoring**.
 3. Tick the **syslog-ng export option**.
 4. In the **syslog-ng export** area, select the desired **Format**.
(IETF = RFC 5424 or Legacy = RFC 3164/BSD)
- ↳ The settings will be saved.

5.7 How to Use the Relay

A device can be connected to the Change Over (CO) relay which is integrated into the INU server. The relay can

- be fixed in a position of your choice:
You switch the relay to the desired position (open or closed). The relay stays in the selected position until you manually switch it again.
- display a status:
By default, the relay is in open position. As soon as one chosen device status occurs, the relay switches to closed position. As soon as the status changes back, the relay automatically returns to open position.
 - USB device connected (any or on a certain port)
 - USB device disconnected (any or on a certain port)
 - USB device activated (any or on a certain port)
 - USB device deactivated (any or a certain port)
 - interrupted network connection
 - network connection established
- Showing events:
The relay switches to closed position as soon as one of the chosen events occurs. After that, the relay will not switch automatically anymore; you first have to manually clear the event / reset the relay.
 - USB device connected (any or on a certain port)
 - USB device disconnected (any or on a certain port)
 - USB device activated (any or on a certain port)
 - USB device deactivated (any or a certain port)
 - SD card connected
 - SD card disconnected
 - SC card cannot be used
 - interrupted network connection
 - network connection established
 - INU server restart
 - interrupted power supply
 - power supply established



The relay can also be switched with a SNMP management tool and the SEH private MIB (download at the website ⇒ 7). Switching via SNMP is not described here and must be implemented self-dependently.

The relay position and events or status which changed it are displayed in the INU Control Center under **DEVICE – Relay** in the **Relay status** table.

Application Scenarios

Fixed position: This is a simple way to switch the relay and therefore the connected device through remote access (HTTP).

Example: The INU server is installed in a production environment. The relay is switched as required by a technician in the control center. Scenarios include a simple connection/disconnection (e.g. diagnosis tool) or an emergency shutdown (e.g. if a sensor warns about overheating).

Displaying a status: The status display is especially useful in production environments.

Example: The quality is checked regularly in a manufacturing process. To do this, a USB analysis device is connected to the INU server and automatically activated via Auto-Connect (⇒ 27). The activation triggers the relay and a connected light bulb switches on to signal the ongoing check. The employees in the manufacturing environment know about it. As soon as the check is completed and the data transferred over the network to the client with the analysis software, the connection to the USB device is deactivated and it is removed from the INU server. The relay switches and the light bulb goes out. The employees know that the quality check is completed.

Showing events: Event display is most suitable for error warnings, as a manual reset of the relay is required.

Example: An interrupted network connection is indicated visually through a red lamp or acoustically with an audio alert. As the reset is to be done manually, the error is displayed permanently by the changed relay position. That remains the case even if the error is removed (maybe of its own volition), e.g. if the network connection is re-

established after a sever error. This error history can give you valuable information on basic problems in your environment. As soon as the technician has analyzed and removed the error, the relay is returned to its default position so that the next error (e.g. an interrupted power supply) is indicated as well.

- Switch relay to fixed position (or switch manually) ⇒ 63
- Switch Relay activation event driven ⇒ 63
- Switch Relay activation state driven ⇒ 63
- Set Relay to Default Position ⇒ 63

Switch relay to fixed position (or switch manually)

Manually switches the relay to the desired position (open or closed). The relay remains in the selected switching state.

1. Start the INU Control Center.
 2. Select **DEVICE – Relay**.
 3. Activate the option **user driven** for **Relay activation**.
 4. From the list, select **Open** or **Closed**.
 5. To confirm, click **Save**.
- ↳ The relay stays in the selected position.

Switch Relay activation event driven

The relay is open by default and automatically switches to the closed position as soon as a predefined event occurs. The device does not automatically switch back to the open position after the event. For this, all events must be deleted and the relay reset.

1. Start the INU Control Center.
 2. Select **DEVICE – Relay**.
 3. Activate the option **event driven** for **Relay activation**.
 4. Configure the events at which the relay is to switch.
 5. To confirm, click **Save**.
- ↳ The settings will be saved.

Switch Relay activation state driven

The relay is open by default and automatically switches to the closed position as soon as a predefined device status occurs. If the device status changes, the relay automatically switches back to the open position.

1. Start the INU Control Center.
 2. Select **DEVICE – Relay**.
 3. Activate the option **state driven** for **Relay activation**.
 4. Configure the states in which the relay is closed.
 5. To confirm, click **Save**.
- ↳ The settings will be saved.

Set Relay to Default Position

✓ 'Show event' is activated ⇒ 67.

1. Start the INU Control Center.
 2. Select **DEVICE – Relay**.
 3. In the table **Relay status**, click **Clear all events / reset relay**.
- ↳ The relay is reset.

6 Security

The INU server can be protected with various security mechanisms. These mechanisms secure the INU server itself as well as the connected USB devices. In addition, you can integrate the INU into the protection mechanisms implemented in your network.

- How to Define the Encryption Strength for SSL/TLS Connections ⇒ 65
- How to Encrypt the Connection to the INU Control Center ⇒ 67
- How to Protect Access to the INU Control Center (User Accounts) ⇒ 68
- How to Configure SNMP ⇒ 69
- How to Block INU Server Ports (TCP Port Access Control) ⇒ 70
- How to Use Certificates ⇒ 71
- How to Configure Network Authentication (IEEE 802.1X) ⇒ 76
- How to Assign a Name to a USB Port ⇒ 79
- How to Control Access to USB Devices ⇒ 80
- How to hide protected USB devices in the SEH UTN Manager selection list? ⇒ 83
- How to Block USB Device Types ⇒ 84
- How to Disable a USB Port ⇒ 85
- How to Encrypt the USB Connection ⇒ 86

**Important:**

Protect access to the INU Control Center with user accounts so that security related settings cannot be modified by unauthorized persons.



•SNMP and VLAN are also security concepts that you can use 6 ⇒ 43; 69

6.1 How to Define the Encryption Strength for SSL/TLS Connections

Some connections to and from the INU server can be encrypted with the protocol SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security):

- Web access to the INU Control Center: HTTPS (⇒ 67)
- USB connection: Data transfer between the clients and the INU server and the connected USB devices (⇒ 65)
- Email: POP3 (⇒ 46)
- Email: SMTP (⇒ 46)

The encryption strength and thus the safety of the connection is defined via the encryption protocol and level. You can choose both.

Each encryption level is a collection of what is called cipher suites. A cipher suite in turn is a standardized sequence of four cryptographic algorithms that are used to establish a secure connection. Based on their encryption strength they are grouped to encryption levels. Which cipher suites are supported by the INU server, i.e. are part of an encryption level, depends on the chosen encryption protocol. You can choose between two encryption levels:

- Any: The encryption is automatically negotiated by both communicating parties. The strongest encryption supported by both parties will always be chosen.
- Low: Only cipher suites with a low encryption are used. (Fast data transfer)
- Medium
- High: Only cipher suites with a strong encryption are used. (Slow data transfer)

When a secure connection is established, the protocol to be used and a list of supported cipher suites are sent to the communication partner. A cipher suite is agreed upon that will be used later on. The strongest cipher suite that is supported by both parties will be used by default.



WARNING

If the communication partner of the INU server does not support the protocol selected and/or if there is no cipher suite that is supported by both parties, the SSL/TLS connection will not be established.

If problems occur, select different settings or reset the parameters of the INU server ⇒ 91.



*If you want the INU server and its communication partner to automatically negotiate the settings, set both options to **Any**. With these settings, the chances that a secure connection can be established are the highest.*

1. Start the INU Control Center.
2. Select **SECURITY – SSL/TLS**.
3. In the **Encryption protocol** area, select the desired protocol.



WARNING

Current browsers do not support **SSL**. If you use an up-to-date browser and set the combination **SSL** and **HTTPS only** to access the INU Control Center (⇒ 67), a connection cannot be established.

Use TLS (and not SSL).

4. In the **Encryption level** area, select the desired level.

**WARNING**

Current browsers do not support cipher suites from the **Low** level. If you use an up-to-date browser and set the combination **Low** and **HTTPS only** to access the INU Control Center (⇒ 67), a connection cannot be established.

Use an encryption level as high as possible.

**WARNING**

The SEH UTN Manager does not support the encryption level **Low**. If you set up **Low** in combination with an encrypted USB connection (⇒ 86), a connection cannot be established.

Use an encryption level as high as possible.

5. To confirm, click **Save**.

↳ The setting will be saved.



*Detailed information about the individual SSL/TLS connections (e.g. supported cipher suites) can be found on the details page under **Security – SSL/TLS – Details**.*

6.2 How to Encrypt the Connection to the INU Control Center

You can protect the connection to the INU Control Center by encrypting it with the SSL (Secure Sockets Layer) protocol and its successor TLS (Transport Layer Security).

- HTTP: unencrypted connection
- HTTPS: encrypted connection

The encryption strength is defined via the encryption protocol and level ⇒ 65. When an encrypted connection is to be established, the client asks for a certificate via a browser (⇒ 71). This certificate must be accepted by the browser; read the documentation of your browser software.



WARNING

Current browsers do not support low security settings. With them a connection cannot be established.

Do not use the following combination: Encryption protocol **HTTPS** and encryption level **Low**.

1. Start the INU Control Center.
 2. Select **SECURITY – Control Center**.
 3. In the **Connection** area, tick **HTTP/HTTPS** or **HTTPS only**.
 4. To confirm, click **Save**.
- ↳ The setting will be saved.

6.3 How to Protect Access to the INU Control Center (User Accounts)

By default, anyone who can find the INU server on the network can access the INU Control Center. To protect the INU from unwanted configuration changes, you can set up two user accounts:

- Administrator: Complete access to the INU Control Center. The user can see all pages and change settings.
- USB Manager: Restricted access to the Control Center. The USB Manager can see the start page and there deactivate activated USB devices. Furthermore he has access to the USB subpage and can administrate and configure it.
- Read-only user: Very restricted access to the INU Control Center. The user can only see the 'DASHBOARD' page.

If you have set up user accounts, a login screen is displayed when the INU Control Center is started. You can choose between two login screens:

- Neutral screen: Login screen in which user name and password are to be entered. (better protection)
- List of users: User names are displayed. Only the password has to be entered.

A user account allows for multiple logins, i.e. the account can be used by a single user or by a group of users. Up to 16 users can be logged in at the same time.



Important:

The user accounts for INU Control Center access are also used for SNMP ⇒ 69. Consider this when setting up user accounts.

For stronger security, you can use a session timeout. If there is no activity within a defined timeout, the user will automatically be logged out.

1. Start the INU Control Center.
2. Select **SECURITY – Control Center**.
3. Define the two user accounts. To do this, in the area **User accounts** enter a **User name** and **Password** respectively.



You can show the typing if you want to make sure that there are no typing errors in the password.

4. Tick **Restrict Control Center access**.
5. Under **Login window shows**, select the type of login screen: **Neutral screen** or **List of users**.
6. Tick the **Session timeout** option and enter in the box the time in minutes after which the an inactive user should be automatically logged out.
7. To confirm, click **Save**.
 - ↳ The settings will be saved.

6.4 How to Configure SNMP

SNMP (Simple Network Management Protocol) is protocol for configuring and monitoring network elements. The protocol controls communication between the monitored devices and the monitoring station (SNMP management tool). Information can be read and changed.

SNMP exists in 3 versions, the INU supports version 1 and 2.

SNMPv1

SNMPv1 is the first and most simple SNMP version. A disadvantage is the insecure access control which is the community: a community groups monitoring station and monitored devices. This makes their administration easier. There are two types of communities, read-only and read/write. For both the community name is also the password used between the monitoring station and the monitored devices. As it is transmitted as clear text, it does not offer sufficient protection.

SNMPv3

SNMPv3 is the newest SNMP version. It contains enhancements and a new security concept which includes, amongst other things, encryption and authentication. Therefore, a SNMP user with name and password must be created in the monitoring station. This user must then be specified in the INU server.



Important:

The user accounts are also used to access the INU Control Center and thus are to be defined under **SECURITY - Control Center**, see 'How to Protect Access to the INU Control Center (User Accounts)' ⇒ 68.

- ✓ SNMPv3 users are created in the monitoring station. (Only for SNMPv3.)
 - ✓ The SNMPv3 users from the monitoring station are specified on the INU server ⇒ 68. (Only for SNMPv3.)
1. Start the INU Control Center.
 2. Select **SECURITY – SNMP**.
 3. Configure the SNMP parameters; ⇒ Table 6.4-1 69.
 4. To confirm, click **Save**.
 - ↳ The settings will be saved.

Table 6.4-1: SNMP Parameters

Parameters	Description
SNMPv1	Enables/disables SNMPv1.
Read-only	Enables/disables the write protection for the community.
Community	SNMP community name Enter the name as it is defined in the monitoring station.
	<p>Important: The default name is 'public'. This name is commonly used for read/write communities. We recommend to change it as soon as possible to increase security.</p>
SNMPv3	Enables/disables SNMPv3.
Hash	Defines the hash algorithm.
Access rights	Defines the access rights of the SNMP user.
encryption	Defines the encryption method.

6.5 How to Block INU Server Ports (TCP Port Access Control)

You can restrict access to the INU server by blocking ports using 'TCP port access control'. If a port is blocked, the protocols and/or services using this port cannot establish a connection with the INU server. Thus attackers have less room for attack.

The security level defines which port types are blocked:

- UTN access (blocks UTN ports)
- TCP access (blocks TCP ports: HTTP/HTTPS/UTN)
- All ports (blocks IP ports)

You have to define exceptions so that your desired network elements, e.g. clients or DNS servers, can establish a connection with the INU server.



WARNING

The 'test mode' is active by default so that you can test your settings without locking yourself out. Your settings will be active until the INU is restarted, afterwards access is no longer restricted.

After you have successfully tested your settings, you have to deactivate the test mode so that access control is permanent.

1. Start the INU Control Center.
2. Select **SECURITY – TCP port access**.
3. Click **Port access control**.
4. In the **Security level** area, select the desired protection
5. In the **Exceptions** area, define the network elements that are to have access to the INU server. To do this, enter the IP or MAC (hardware) addresses and tick the options.



Important:

MAC addresses are not delivered through routers!



The prefix notation "<IP address>/<prefix length>" can be used to freely define IPv4 and IPv6 subnets.

6. Make sure that the **Test mode** is enabled.
7. Click **Save & Restart** to confirm.
The settings will be saved.
The port access control is activated until the device is restarted.
8. Check the port access and if it is possible to reach the INU Control Center.



Important:

If it is not possible to reach the INU Control Center, restart the INU server ⇒ 93.

9. Deactivate the **Test mode**.
10. Click **Save & Restart** to confirm.
↳ The settings will be saved.

6.6 How to Use Certificates

The INU server has its own certificate management. Digital certificates are data sets, which confirm the identity of a person, object, or organization. In TCP/IP networks they are used to encrypt data and to authenticate communication partners.

The INU needs a certificate for:

- participating in the authentication mechanisms EAP-TLS, EAP-TTLS and PEAP ⇒ 76
- protecting email communication (POP3/SMTP via SSL/TLS) ⇒ 46
- protecting the connection between the clients and the connected USB devices ⇒ 86
- protecting the connection to the INU Control Center (with HTTPS) ⇒ 67

The following certificates can be used in the INU server:

- 1 self-signed certificate
Certificate generated by the INU server and signed by the INU server itself. The certificate confirms the INU server's identity.
- 1 client certificate, i.e. 1 requested certificate or 1 PKCS#12 certificate
The client certificate confirms the identity of the INU server with the help of an additional trustworthy authority which is the certification authority (short CA).
 - Requested certificate: As first step, a certificate request is generated on the INU server and then the request is sent to a certification authority. In the second step, the certification authority creates a certificate based on the request for the INU server and signs it.
 - PKCS#12 certificate Exchange format for certificates. You have a certification authority generate a certificate which is stored in password-protected PKCS#12 format for the INU server. Then you transport the PKCS#12 file to the INU server and install it (and thus the certificate in it).
- 1 S/MIME certificate
The INU server uses the S/MIME Certificate to sign and encrypt emails which is sends. The corresponding private key (PKCS#12 format) has to be installed as certificate of it's own in the email program (Mozilla Thunderbird etc.) so that emails can be verified and, if necessary, decrypted.
- 1–32 CA certificates, also known as root CA certificates.
Certificates which are issued for a certification authority and confirm its identity. They are used for verifying certificates that have been issued by the respective certification authority. In case of the INU server these are the certificates of communication partners to verify their identity (chain of trust). Thus multi-level public key infrastructures (PKIs) are supported.




Important:


Upon delivery, a default certificate is stored in the INU server. This certificate is issued by SEH Computertechnik GmbH for each device specifically.

- Having a Look at Certificates ⇒ 72
- Saving a Certificate Locally ⇒ 72
- Creating a Self-Signed Certificate ⇒ 72
- Request and Install Certificate (Requested Certificate) ⇒ 73
- Installing a PKCS#12 Certificate ⇒ 74
- Installing an S/MIME Certificate myUTN-2500 ⇒ 74
- Installing a CA Certificate ⇒ 74
- Deleting Certificates ⇒ 75

Having a Look at Certificates

- ✓ A certificate is installed on the INU server.
- 1. Start the INU Control Center.
- 2. Select **SECURITY – Certificates**.
- 3. Select the certificate via the icon .
- ↳ The certificate is displayed.

Saving a Certificate Locally

- ✓ A certificate is installed on the INU server.
- 1. Start the INU Control Center.
- 2. Select **SECURITY – Certificates**.
- 3. Save the certificate using the icon .
- ↳ The certificate is stored on your local client.

Creating a Self-Signed Certificate




Important:

Only one self-signed certificate can be installed on the INU server.
 To create a new certificate, you must first delete the existing certificate ⇒ [75](#).

- 1. Start the INU Control Center.
- 2. Select **SECURITY – Certificates**.
- 3. Click **Self-signed certificate**.
- 4. Enter the relevant parameters; ⇒ [Table 6.6-2](#) [72](#).
- 5. Click **Create/Install**.
- ↳ The certificate will be created and installed. This may take a few minutes.

Table 6.6-2: Parameters for the Creation of Certificates

Parameters	Description
Common name	Freely definable certificate name. (max. 64 characters)
	 <i>Use the IP address or host name of the INU server, so that you can clearly match device and certificate.</i>
Email address	Email address of the person responsible for the INU server. (max. 40 characters; optional)
Organization name	Name of the company which uses the INU server. (max. 64 characters)
Organizational unit	Name of a department or subsection in the company. (max. 64 characters; optional)
Location	Location of the company. (max. 64 characters)
State name	State where the company is based. (max. 64 characters)

Parameters	Description
Domain component	Allows you to enter additional attributes. (Optional entry)
SAN (multi-domain)	Allows you to enter Subject Alternative Names (SAN). Used to specify additional host names (e.g. domains). (Optional entry, max. 255 characters)
Country	Country where the company is based. Enter the two-digit country code according to ISO 3166. Examples: DE = Germany, GB = Great Britain, US = USA
Issued on	Date from which on the certificate is valid.
Expires on	Date from which on the certificate becomes invalid.
RSA key length	Defines the length of the RSA key used: <ul style="list-style-type: none"> • 512 bit (fast encryption and decryption) • 768 bit • 1024 bit • 2048 bit (standard encryption and decryption) • 4096 bit (slow encryption and decryption)

Request and Install Certificate (Requested Certificate)

A certificate that has been issued by a certification authority for the INU server can be used in the INU server. To do this, your first create a certificate request and then send it to the certification authority. Based on the request, the certification authority then creates a certificate specifically for the INU server. You install this certificate in the INU server.



Important:

You can only install a requested certificate that has been issued based on the certificate request created on the INU server.

If the files do not match, you have to request a new certificate which is based on the current certificate request. If you want to start over, you must delete the certificate request ⇒ ¶75.

1. Start the INU Control Center.
2. Select **SECURITY – Certificates**.
3. Click **Certificate request**.
4. Enter the required parameters; ⇒ Table 6.6-2 ¶72.
5. Click **Create a request**.
The certificate request will be created. This may take a few minutes.
6. Select **Upload** and save the requests in a text file.
7. Click **OK**.
8. Send the text file as certificate request to a certification authority. The certification authority creates the certificate and gives it to you.



Important:

The certificate must be in 'base64' format.

9. Click **Requested certificate**.
 10. Enter the password into the **Password** box.
 11. Click **Install**.
- ↳ The requested certificate is installed in the INU server.

Installing a PKCS#12 Certificate



Important:

If a PKCS#12 certificate has already been installed in the INU server, you must first delete the certificate ⇒ 75.

- ✓ The certificate has 'base64' format.
1. Start the INU Control Center.
 2. Select **SECURITY – Certificates**.
 3. Click **PKCS#12 certificate**.
 4. Specify the PKCS#12 certificate in the **Certificate file** box.
 5. Enter the password.
 6. Click **Install**.
- ↳ The PKCS#12 certificate will be installed in the INU server.

Installing an S/MIME Certificate myUTN-2500



Important:

If an S/MIME certificate has already been installed in the INU server, you must first delete the certificate ⇒ 75.

- ✓ The certificate has 'pem' format.
1. Start the INU Control Center.
 2. Select **SECURITY – Certificates**.
 3. Click **S/MIME certificate**.
 4. Specify the S/MIME certificate in the **Certificate file** box.
 5. Click **Install**.
- ↳ The S/MIME certificate is installed in the INU server.

Installing a CA Certificate

- ✓ The certificate has 'base64' format.
1. Start the INU Control Center.
 2. Select **SECURITY – Certificates**.
 3. Click **CA certificate**.
 4. Specify the CA certificate in the **Certificate file** box.
 5. Click **Install**.
- ↳ The CA certificate is installed in the INU server.


Deleting Certificates



WARNING

To establish an encrypted (HTTPS ⇒ 67) connection to the INU Control Center, a certificate (self-signed/CA/PKCS#12) is required. If you delete the corresponding certificate, the INU Control Center can no longer be reached.

In this case restart the INU server ⇒ 93. The INU server then generates a new self-signed certificate with which a secured connection can be established.

- ✓ A certificate is installed on the INU server.
- 1. Start the INU Control Center.
- 2. Select **SECURITY – Certificates**.
- 3. Delete the certificate using the icon .
- ↳ The certificate is deleted.

6.7 How to Configure Network Authentication (IEEE 802.1X)

Authentication is the proof and verification of an identity. With it your network is protected from abuse, because only authorized devices have access.

The INU supports authentication according to the IEEE 802.1X standard which is based on EAP (Extensible Authentication Protocol).

If you use authentication according to IEEE 802.1X in your network, the INU server can participate:

- Configuring EAP-MD5 ⇒ 76
- Configuring EAP-TLS ⇒ 76
- Configuring EAP-TTLS ⇒ 77
- Configuring PEAP ⇒ 77
- Configuring EAP-FAST ⇒ 78

Configuring EAP-MD5

EAP-MD5 (Message Digest #5) is a user-based authentication via a RADIUS server. First, you have to create a user (user name and password) on the RADIUS server for the INU server. Afterwards you set up EAP-MD5 on the INU server.

- ✓ A user account for the INU server is set up on the RADIUS server.
1. Start the INU Control Center.
 2. Select **SECURITY – Authentication**.
 3. From the **Authentication method** list, select **MD5**.
 4. Enter the user name and the password of the user account that is set up for the INU server on the RADIUS server.
 5. Click **Save & Restart** to confirm.
- ↳ The settings will be saved.

Configuring EAP-TLS

EAP-TLS (Transport Layer Security) is a mutual, certificate based authentication via a RADIUS server. In this method, INU server and RADIUS server exchange certificates through an encrypted TLS connection.

Both RADIUS and INU server require a valid, digital certificate signed by a CA. This requires a PKI (Public Key Infrastructure).



WARNING

Follow the instructions below in the given order. If you do not follow the order, the INU server might not be reachable in the network.

In this case, reset the parameters of the INU server ⇒ 91.

1. Create a certificate request on the INU server ⇒ 71.
 2. Create a certificate using the certificate request and the authentication server.
 3. Install the requested certificate on the INU server ⇒ 71.
 4. Install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) is installed in the INU server ⇒ 71.
 5. Start the INU Control Center.
 6. Select **SECURITY – Authentication**.
 7. Select **TLS** from the **Authentication method** list.
 8. From the **EAP root certificate** list, select the root CA certificate.
 9. Click **Save & Restart** to confirm.
- ↳ The settings will be saved.

Configuring EAP-TTLS

In EAP-TTLS (Tunneled Transport Layer Security), a TLS-protected tunnel is used for exchanging secrets. The method consists of two phases:

1. Outer authentication: An encrypted TLS (Transport Layer Security) tunnel is created between INU server and RADIUS server. To do this, the RADIUS server authenticates itself to the INU server using a certificate that was signed by a CA.
 2. Inner authentication: In the tunnel the authentication (via CHAP, PAP, MS-CHAP, or MS-CHAPv2) takes place.
- ✓ A user account for the INU server is set up on the RADIUS server.
 - ✓ For increased security during connection establishment (optional): The root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) is installed in the INU server ⇒ [71](#).
1. Start the INU Control Center.
 2. Select **SECURITY – Authentication**.
 3. Select **TTLS** from the **Authentication method** list.
 4. Enter the user name and the password of the user account that is set up for the INU server on the RADIUS server.
 5. Select the settings which secure the communication in the TLS channel.
 6. Increase the security during connection establishment (optional):
From the list **EAP root certificate**, select the root CA certificate.
 7. Click **Save & Restart** to confirm.
- ↳ The settings will be saved.

Configuring PEAP

With PEAP (Protected Extensible Authentication Protocol), an encrypted TLS (Transport Layer Security) tunnel is established between the INU server and the RADIUS server. To do this, the RADIUS server authenticates itself to the INU server using a certificate that was signed by a CA. The TLS channel is then used to establish another connection that can be protected by means of additional EAP authentication methods (e.g. MSCHAPv2).

The method is very similar to EAP-TTLS (⇒ [77](#)), but other methods are used to authenticate the INU server.

- ✓ A user account for the INU server is set up on the RADIUS server.
 - ✓ For increased security during connection establishment (optional): The root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) is installed in the INU server ⇒ [71](#).
1. Start the INU Control Center.
 2. Select **SECURITY – Authentication**.
 3. Select **PEAP** from the **Authentication method** list.
 4. Enter the user name and the password of the user account that is set up for the INU server on the RADIUS server.
 5. Select the settings which secure the communication in the TLS channel.
 6. Increase the security during connection establishment (optional):
From the list **EAP root certificate**, select the root CA certificate.
 7. Click **Save & Restart** to confirm.
- ↳ The settings will be saved.

Configuring EAP-FAST

EAP-FAST (Flexible Authentication via Secure Tunneling) is a specific EAP method developed by the company Cisco.

As with EAP-TTLS (⇒ 77) and PEAP (⇒ 77) a secure tunnel protects data transmission. However, the server does not authenticate itself with a certificate. Instead it uses PACs (Protected Access Credentials).

✓ A user account for the INU server is set up on the RADIUS server.

1. Start the INU Control Center.
2. Select **SECURITY – Authentication**.
3. Select **FAST** from the **Authentication method** list.
4. Enter the user name and the password of the user account that is set up for the INU server on the RADIUS server.
5. Select the settings intended to secure the communication in the channel.
6. Click **Save & Restart** to confirm.
 - ↳ The settings will be saved.

6.8 How to Assign a Name to a USB Port

By default, the names of the connected USB devices are displayed on the USB ports in the INU Control Center and SEH UTN Manager. These names are specified by the device manufacturers and might be ambiguous or inaccurate.

That is why you can assign freely definable names to the USB ports, e.g. the name of a corresponding software. This gives you a better overview of the USB devices available in the network.

1. Start the INU Control Center.
2. Select **SECURITY – USB**.
3. Enter a name for the desired USB port in the **Name** box.
4. To confirm, click **Save**.
 - ↳ The settings will be saved.

6.9 How to Control Access to USB Devices

You can restrict the access to the USB ports and the connected USB devices:

- **USB port key control:** Up to two keys are defined for the USB port. Each key can be assigned a validity period (always, expiration date, weekly period). The USB port and the connected USB device are shown in the SEH UTN Manager greyed out, i.e. the connection cannot be established. As soon as the key for the USB port is entered in the SEH UTN Manager, the USB port and the connected USB device appear and can be used.
- **USB port device assignment:** A certain USB device is assigned to a USB port. This is achieved by linking the USB port and USB device through the vendor ID (short VID) and product ID (short PID) of the USB device. The combination of VID and PID is specific to a certain USB device model which means that only USB devices of this specific model can be used on the USB port. This way you can assure, that (security) settings cannot be circumvented by connecting USB devices to other ports.




Power off unused ports to increase security ⇒ 85.

You can either use one of the two security methods, or both in combination.

- Setting Up USB Port Keys ⇒ 80
- Entering a USB Port Key (Unlocking a USB Device) ⇒ 81
- Configuring USB Port Device Mapping ⇒ 81
- Configuring USB Port Keys in Combination with USB Port Device Mapping ⇒ 81

Setting Up USB Port Keys

The USB port keys are defined in the INU Control Center.

1. Start the INU Control Center.
 2. Select **SECURITY – USB**.
 3. In the USB port table for the desired USB port, click the **Change**  icon. The **USB Port** page appears.
 4. Go to the **Method** list and click **Port key control**.
 5. For **Key 1**, click the **Generate** button, or enter a freely definable key in the box (max. 64 ASCII characters).
 6. Select a period from the **Validity** list and define the time window if necessary:
 - off (always invalid, use 'off' if you want to keep the key but temporarily disable it)
 - always (permanently valid)
 - expires on (valid until hour X on day Z)
 - weekly (valid on X days from hour Y to Z)
 7. Optional: For **Key 2**, repeat steps 5. and 6.
 8. To confirm, click **Save**.
- ↳ The settings will be saved. Access to the USB device is protected.



*To deactivate the feature, go to the **Method** list and select ---.*

Entering a USB Port Key (Unlocking a USB Device)

When USB port key control is enabled in the SEH UTN Manager, neither the USB port nor the connected USB device are shown, which means the connection cannot be established.

To gain access to the protected USB device, the key must be entered on the client in the SEH UTN Manager. Since the port key applies only to the user account currently in use on the client, you must enter it into each client user account that should have access to the USB device (user port key). The USB port and the connected USB device will then appear and can be used.

1. Start the SEH UTN Manager.
 2. In the selection list, select the INU server.
 3. In the menu bar, select **UTN Server – Set User Port Keys**.
The **Enter User Port Key** dialog appears.
 4. Enter the key for the relevant USB port.
 5. Click **OK**.
- ↳ Access is granted.




Important:

If you are using Auto-Connect () in combination with USB port keys, you must enter the key separately as the Auto-Connect port key. These apply system-wide.

In the menu bar, select **UTN Server – Enter Auto-Connect Port Key**.

Configuring USB Port Device Mapping

1. Start the INU Control Center.
 2. Select **SECURITY – USB**.
 3. In the USB port table for the desired USB port, click the **Change**  icon.
The **USB Port** page appears.
 4. Go to the **Method** list and click **Device Assignment**.
 5. Click **Assign device**.
The **USB device** box shows the VID and PID of the USB device.
 6. To confirm, click **Save**.
- ↳ The settings will be saved. Only the assigned USB device model can be operated on the USB port.




*To deactivate the feature, go to the **Method** list and select ---.*

To assign a different USB device to the USB port, connect the USB device to the USB port and repeat the USB port device mapping.

Configuring USB Port Keys in Combination with USB Port Device Mapping

Combine the USB port key control and USB port device mapping security methods to use only the USB devices of the assigned USB device model on the USB port and further restrict access to them (over time periods).

1. Start the INU Control Center.
2. Select **SECURITY – USB**.
3. In the USB port table for the desired USB port, click the **Change**  icon.
The **USB Port** page appears.
4. Go to the **Method** list and click **Port key control/Device mapping**.
5. For **Key 1**, click the **Generate** button, or enter a freely definable key in the box (max. 64 ASCII characters).

6. Select a period from the **Validity** list and define the time window if necessary:
 - off (always invalid, use 'off' if you want to keep the key but temporarily disable it)
 - always (permanently valid)
 - expires on (valid until hour X on day Z)
 - weekly (valid on X days from hour Y to Z)
7. Optional: For **Key 2**, repeat steps 5. and 6.
8. Click **Assign device**.
The **USB device** box shows the VID and PID of the USB device.
9. To confirm, click **Save**.
↳ The settings will be saved.



*To deactivate the feature, go to the **Method** list and select ---.*

6.10 How to hide protected USB devices in the SEH UTN Manager selection list?

You can restrict the access to the USB ports and the connected USB devices with the USB port key control, see 'How to Control Access to USB Devices' ⇒ 80. By default, USB devices that are protected by a port key are displayed in the selection list of the SEH UTN Manager without being accessible.

In addition, you can hide the protected USB devices so that they are not displayed in the selection list of the SEH UTN Manager. Proceed as follows:

1. Start the INU Control Center.
2. Select **SECURITY – USB**.
3. Click **Hide protected USB devices**.
4. Click **Save** to confirm.
↳ The settings will be saved.

6.11 How to Block USB Device Types

USB devices are grouped into classes according to their function. For example, input devices such as keyboards belong to the group 'Human Interface Device' (HID).

USB devices may present themselves as HID class USB devices while they are actually used for abuse (known as 'BadUSB').

In order to protect the INU server, you can block input devices of the HID class.

1. Start the INU Control Center.
2. Select **SECURITY – USB**.
3. Click/clear **Disable input devices (HID class)**.
4. To confirm, click **Save**.
↳ The setting will be saved.

Additionally, there is a selection that enables or disables all input devices (HID class) on the ports.

1. Start the INU Control Center.
2. Select **SECURITY – USB**.
3. Select **Disable input devices (HID class) for all ports** or **Enable input devices (HID class) for all ports**.
4. To confirm, click **Save**.
↳ The setting will be saved.

6.12 How to Disable a USB Port

By default all USB ports are active. You can deactivate (and re-activate) the USB port by interrupting or restoring the power supply.

Deactivate

- unused USB ports to ensure that unwanted USB devices cannot be connected to the network. (Deactivated USB ports cannot be seen in the SEH UTN Manager.)
 - a USB port and re-activate it to restart the connected USB device if it is in an undefinable condition. (The USB device does not need to be removed and reconnected manually.)
1. Start the INU Control Center.
 2. Select **SECURITY – USB**.
 3. For the desired USB port, enable/disable the option in the column.
 4. To confirm, click **Save**.
- ↳ The USB port is disabled/enabled.

6.13 How to Encrypt the USB Connection

To secure the USB connections, encrypt the entire data transfer (user data, control data and protocol data) between the clients and the USB devices connected to the INU server.

The protocols SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) are used for encryption. The encryption strength is defined via the encryption protocol and level ⇒ 65.



WARNING

The SEH UTN Manager does not support the encryption level **Low**. If you set up **Low** in combination with an encrypted USB connection, a connection cannot be established.

Use an encryption level as high as possible.

If connections are encrypted, client and INU server communicate over the encrypted UTN port. By default, that is port 9443. If the port is already in use on your network, e.g. for another application, you can change the port number ⇒ 54.

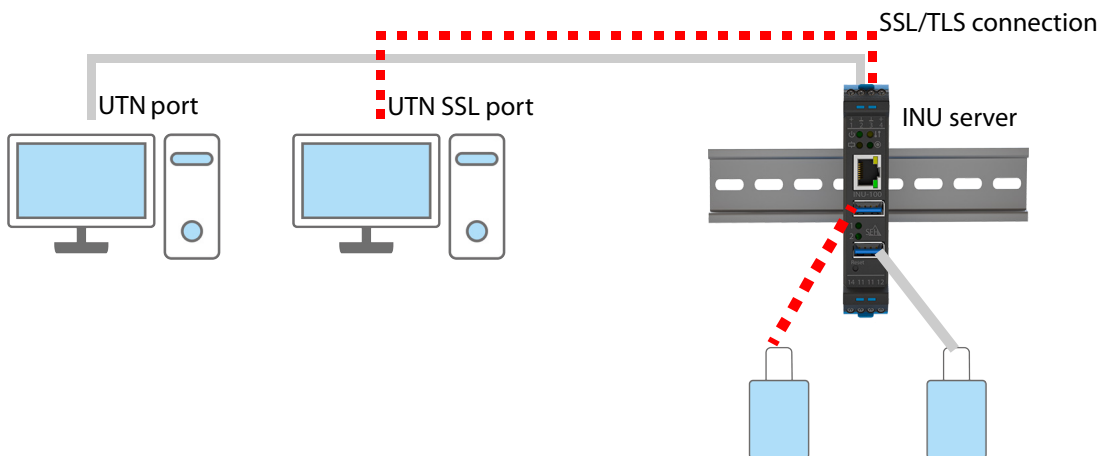


Figure 6.13-1: INU server – SSL/TLS connection in the network

1. Start the INU Control Center.
 2. Select **SECURITY – USB**.
 3. Enable the **Encrypt USB communication (SSL/TLS)** option.
 4. To confirm, click **Save**.
- ↳ The data transfer between the clients and the USB devices will be encrypted.

7 Maintenance

You can maintain the INU server in the following ways:

- [How to Backup Your Configuration](#) ⇒ [88](#)
- [How to Reset Parameters to their Default Values](#) ⇒ [91](#)
- [How to Perform a Device Software Update](#) ⇒ [92](#)
- [How to Restart the INU Server](#) ⇒ [93](#)

7.1 How to Backup Your Configuration

The INU server includes a backup function that allows you to access a fixed configuration state at any time. All parameters are saved in the '<default-name>_parameters.txt' parameter file (exception: passwords). You can view this file on the INU server and save it to your local client for backup. You can edit the parameter values in the backed up file using a text editor. Afterwards, the edited file can be loaded onto one or more INU servers. The device(s) will then adopt the parameter values of the file. This allows you to quickly configure a large number of INU servers. You can find a detailed description of the parameters in the 'Parameter lists' ⇒ 98.

1. Parameter file:
All parameters are saved in the '<default-name>_parameters.txt' file (exception: passwords). You can view this file on the INU server and save it to your local client for backup. You can edit the parameter values in the backed up file using a text editor. Afterwards, the edited file can be loaded onto one or more INU servers. The device(s) will then adopt the parameter values of the file. This allows you to quickly configure a large number of INU servers. You can find a detailed description of the parameters in the 'Parameter lists' ⇒ 100.
2. System backup: The entire system (settings, certificates, passwords, etc.) are saved to the SD card. By inserting the SD card in another INU server, you can transfer the system backup to this device. The system backup is automatically updated after a change to the configuration.



WARNING

If the SD card is lost or stolen, your environment becomes vulnerable (certificates, passwords).

Therefore, you have to take all necessary precautions to protect the INU server if you use the automatic backup.

- See Parameter Values ⇒ 88
- Exporting the Parameter File via INU Control Center ⇒ 88
- Exporting the Parameter File via SEH Product Manager ⇒ 88
- Loading the Parameter File INU Control Center onto a INU Server ⇒ 89
- Loading the Parameter File via SEH Product Manager onto a INU Server ⇒ 89

See Parameter Values

1. Start the INU Control Center.
2. Select **MAINTENANCE – Backup**.
3. In the **Parameter File – Content** area, click the **View** button.
↳ The current parameter values are displayed.

Exporting the Parameter File via INU Control Center

1. Start the INU Control Center.
2. Select **MAINTENANCE – Backup**.
3. In the **Parameter file – Backup** area, click the **Export** button.
4. Save the '<default-name>_parameters.txt' file to your client using your browser.
↳ The parameters file is backed up.

Exporting the Parameter File via SEH Product Manager

You can save the parameter file from one or more INU servers to your local client.

- ✓ The SEH Product Manager is installed on the client.
 - ✓ The device is shown in the device list.
1. Start the SEH Product Manager.

The device list is displayed.

2. Select the INU server(s) in the device list.
3. In the menu bar, select **Device – Backup**.
The **Parameter backup** dialog appears.
4. Follow the instructions in the dialog.
↳ The parameters are saved.

Loading the Parameter File INU Control Center onto a INU Server

1. Start the INU Control Center.
2. Select **MAINTENANCE – Backup**.
3. In the **Parameter file – Restore** area, specify the '<default name>_parameters.txt' file in the **Parameter file** box.
4. Click **Import**.
↳ The INU server adopts the parameter values from the file.

Loading the Parameter File via SEH Product Manager onto a INU Server

You can load the parameter file onto one or more INU servers.



WARNING

Some parameters (e.g. a static IPv4 network configuration) must be assigned individually. Conflicts can occur if you load the parameter file on multiple INU servers at the same time.

Only upload parameter files to multiple INU servers at the same time if the settings are universal.

- ✓ The SEH Product Manager is installed on the client .
 - ✓ The device is shown in the device list .
1. Start the SEH Product Manager.
The device list is displayed.
 2. Select the INU server(s) in the device list.
 3. In the menu bar, select **Device – Load parameter**.
The **Load parameter** dialog appears.
 4. Follow the instructions in the dialog.
↳ The INU server adopts the parameter values from the file.

Automatic WebDAV System Backup

System backup to a WebDAV server stores the INU server system in a directory on the WebDAV server. The system backup is automatically updated when you make changes to the system. To increase clarity on the WebDAV server, you can automatically create individual directories for days. All change backups from a single day are then stored in a subdirectory of the backup directory.

In addition to the change backup, you can also save an additional daily system backup. This single backup is stored on the WebDAV server every day at a time you specify.

- ✓ A WebDAV server is available on your network.
 - ✓ A directory for system backup has been created on the WebDAV server.
1. Start the INU Control Center.
 2. Select **MAINTENANCE – Backup**.
 3. In the **System Backup – WebDAV** area, enable the **Change Backup** option.
 4. In the **System Backup – WebDAV** area, enter the directory on the WebDAV server where the backup files are to be stored in the **Server Directory** box.
(Also defines the WebDAV server directory for manual system backup ⇒ 90.)
 5. Optional: In the **System Backup – WebDAV** area, enable the **Individual Directories for Days** option.
 6. Optional: In the **System Backup – WebDAV** area, enable the **Additional Individual Backups** option and specify the desired time.
 7. To confirm, click **Save**.
↳ The setting will be saved.

Manual WebDAV System Backup

You can manually backup the current system state to the WebDAV server.

1. Start the INU Control Center.
2. Select **MAINTENANCE – Backup**.
3. In the **System Backup – WebDAV** area, enter the directory on the WebDAV server where the backup file is to be stored in the **Server Directory** box.
(Also defines the WebDAV server directory for automatic system backup ⇒ 98.)
4. In the **System Backup – WebDAV** area, click the **Create manual backup now** button.
↳ The system backup is saved to the WebDAV server.

Automatic Backup

- ✓ An SD card is connected to the INU server.
- ✓ The SD card has the file system FAT12, FAT16 or FAT32.
- ✓ 1 MB of free space is available on the SD card.

(These requirements are fulfilled ex factory.)

1. Start the INU Control Center.
2. Select **MAINTENANCE – Backup**.
3. In the **System Backup – SD Card** area, enable the **Parameter Backup** option.
4. Click **Save**.
↳ The settings will be saved.

7.2 How to Reset Parameters to their Default Values

You can reset the INU to its default values, e.g. if you want to install the INU server in a different network. All settings will be set to factory settings. Installed certificates will not be deleted.



Important:

The connection to the INU Control Center may be interrupted if the IP address of the INU server changes with the reset.

If required, determine the new IP address ⇒ 40.

You can change the settings either via remote access (INU Control Center and SEH Product Manager) or using the Reset button on the INU server.



If you lost the password for the INU Control Center, you can reset the INU server using the reset button. You do not need a password to do so.



WARNING

Remove the SD card from the INU server before resetting the parameters. Otherwise, the INU server will adopt the parameter values stored on it (automatic backup ⇒ 88).

- Resetting Parameters from the INU Control Center ⇒ 91
- Resetting Parameters via Reset Button ⇒ 91

Resetting Parameters from the INU Control Center

1. Start the INU Control Center.
2. Select **MAINTENANCE – Default settings**.
3. Click **Reset device**.
A security query appears.
4. Confirm the security query.
↳ The parameters are reset.

Resetting Parameters via Reset Button

With the reset button you can reset the INU server's parameter values to their default settings.

1. Press the reset button for 5 seconds.
The INU server restarts.
↳ The parameters are reset.

7.3 How to Perform a Device Software Update

You can update your INU server with a software update. Software updates include new features and/or bug fixes. You can find the version number of the software currently installed on the INU server on the start page of the INU Control Center or in the device list in the SEH Product Manager.

Visit the SEH Computertechnik GmbH website for current software files:

<https://www.seh-technology.com/us/services/downloads/industrial/inu-100.html>

**Important:**

Save your current settings with a parameter backup before you upgrade. A backup is the best way to preserve all configuration settings in the event of a downgrade.

Only the software in use is updated; settings will remain preserved.

**Important:**

Every update file comes with a 'readme' file. Read the 'readme' file and follow its instructions.

2. Start the INU Control Center.
 3. Select **MAINTENANCE – Update**.
 4. Specify the update file in the **Update file** box.
 5. Click **Install**.
- ↳ The update is executed. Afterwards, the INU server restarts.

7.4 How to Restart the INU Server

After some parameter changes or after an update, the INU server restarts automatically. If the INU server is in an undefined state, you can also restart the INU server manually.

- Restarting the INU Server from the INU Control Center ⇒ 93
- Restarting the INU Server via Reset Button ⇒ 93

Restarting the INU Server from the INU Control Center

1. Start the INU Control Center.
 2. Select **MAINTENANCE – Restart**.
 3. Click **Restart device**.
- ↳ The INU server restarts.

Restarting the INU Server via Reset Button

1. Press the restart button of the device for a short time.
- ↳ The INU server restarts.

8 Appendix

The appendix contains a glossary, a troubleshooting guide and the lists of this document.

- Glossary ⇒ 95
- Troubleshooting ⇒ 96
- Parameter lists ⇒ 98
- SEH UTN Manager – Feature Overview ⇒ 119
- Index ⇒ 121

8.1 Glossary

Compound USB device

A compound USB device consists of a hub and one or more USB devices that are all integrated into a single housing. Dongles are often compound USB devices.

If a compound USB device is connected to a USB port of the INU server, all integrated USB devices will be shown in the INU Control Center and in the selection list of the SEH UTN Manager. When the port connection is activated, all displayed USB devices will be connected to the user's client. It is not possible to activate a port connection to only one of the USB devices.

Default name

Device name which is assigned by the manufacturer and cannot be changed. If you are using several identical INU servers, you can identify a certain device with it.

The default name of the INU server is made up of the two letters 'IC' and the device number. The device number consists of the last six numbers of the MAC address.

You can read the default name in the INU Control Center or SEH Product Manager.

INU Control Center

The INU Control Center is the UI of the INU server. The INU server can be configured, monitored and maintained using the INU Control Center.

You can access the INU Control Center with an Internet browser (e.g. Mozilla Firefox).

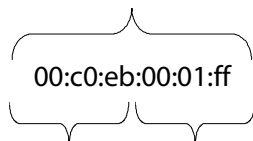
More information ⇒ [11](#).

MAC address

The MAC address (often also Ethernet address, physical or hardware address) is a globally unique identifier of a network adapter. If you are using several identical INU servers, you can identify a certain device with it.

The manufacturer defines the MAC address in the hardware of the device. It consists of 12 hexadecimal numbers. The first six numbers represent the manufacturer, while the last six numbers identify the individual device. The characters for separating the numbers depend on the platform. Under Linux, ':' are used.

MAC address



Manufacturer ID Device number

You can read the MAC address on the type plate on the housing, in the SEH UTN Manager.

SEH UTN Manager

The 'SEH UTN Manager' is a software tool developed by SEH Computertechnik GmbH. The SEH UTN Manager is used to establish and manage connections to the USB devices connected to the INU servers.



More information ⇒ [13](#).

8.2 Troubleshooting



The SEH Computertechnik GmbH website contains our Knowledge Base articles that provide solutions and detailed background knowledge addressing specific problems and questions.

<https://www.seh-technology.com/services/knowledgebase.html>

Fault	Cause	Fix
Lost password and/or user name for the user accounts.	—	Reset the INU server parameter values to the default ⇒ ¶91.  WARNING Resetting the device causes all settings to be lost.
INU Control Center can not be reached.	<ul style="list-style-type: none"> • Faulty cable connections • Wrong IP address used • Browser proxy settings • Access is protected via SSL/TLS (HTTPS) and the security settings are not supported ⇒ ¶67 • TCP port access control is enabled (ports are blocked) ⇒ ¶70 	<ul style="list-style-type: none"> • Check the <ul style="list-style-type: none"> - Cabling - Settings • Reset the INU server parameter values to the default ⇒ ¶91.  WARNING Resetting the device causes all settings to be lost.
Functions are grayed out or unavailable in the SEH UTN Manager.	Which features are inactive (grayed out) in the SEH UTN Manager depends on different factors: <ul style="list-style-type: none"> • Selection list mode <ul style="list-style-type: none"> - global - user • Client user account <ul style="list-style-type: none"> - administrator or group members of 'utnusers' - standard user or users which are not members of the group 'utnusers' • Write access to the *.ini file (selection list) • The connected USB device does not support the function • Security measures have been implemented 	<ul style="list-style-type: none"> • Consult your administrator. • Start the SEH UTN Manager with a different user account. • Check the configured security measures.

Fault	Cause	Fix
USB devices are not shown in the SEH UTN Manager	<ul style="list-style-type: none"> • The USB device is no longer connected to the INU server. • The SEH UTN Manager and the INU server firmware/software are incompatible. • The USB port is deactivated. • Too many compound USB devices are connected to the INU server. The number of virtual ports has been exceeded ⇒ 24. 	<ul style="list-style-type: none"> • Check if the USB device is connected. • Update the SEH UTN Manager (92) and the software (⇒ 92). • Switch on the USB port power supply ⇒ 85. • Remove compound USB devices to free up virtual ports.
The SEH UTN Manager displays several USB devices on one USB port.	<p>The USB device is a compound USB device. It consists of a hub and one or more USB devices that are all integrated into a single housing. When the connection to the port is established, all the displayed USB devices are connected.</p>	—
The connection to the USB port (and the connected USB device) cannot be established in the SEH UTN Manager.	<ul style="list-style-type: none"> • The USB port is already connected to another client (in use by another user). • The driver software for the USB device is not installed on the client. • Access to USB devices is restricted. 	<ul style="list-style-type: none"> • Wait until the USB device is available or request the used USB device. • Install the USB device driver on the client, e.g. by connecting the USB device directly to the client. • Check the access settings for USB devices ⇒ 80.
<p>The connection between the SEH UTN Manager and the INU server cannot be established:</p> <ul style="list-style-type: none"> • The INU server does not appear in the SEH UTN Manager. • The INU server is grayed out in the SEH UTN Manager. 	<ul style="list-style-type: none"> • The UTN port is blocked, e.g. by security software (firewall). • The UTN port is not identical (you changed the port number). 	<ul style="list-style-type: none"> • Enable communication through the UTN port on your network. • SNMPv1, which is required to forward the port change to the clients, is disabled. Enable SNMPv1 ⇒ 69.

8.3 Parameter lists

The INU servers stores its configuration as parameters. You directly use parameters for:

- Administration via email ⇒ 19
- Configuration backup (viewing, editing and loading parameters onto other devices) ⇒ 88

The following tables list all parameters and their values so that you can use them in the actions named above.

- Table 8.3-1 'Parameter list – IPv4' ⇒ 99
- Table 8.3-2 'Parameter list – IPv6' ⇒ 99
- Table 8.3-3 'Parameter list – IP-VLAN' ⇒ 100
- Table 8.3-5 'Parameter list – POP3' ⇒ 101
- Table 8.3-6 'Parameter list – SMTP' ⇒ 102
- Table 8.3-7 'Parameter list – Bonjour' ⇒ 104
- Table 8.3-8 'Parameter list – Server services' ⇒ 104
- Table 8.3-9 'Parameter list – Description' ⇒ 105
- Table 8.3-10 'Parameter list – Date/Time' ⇒ 105
- Table 8.3-11 'Parameter list – UTN port' ⇒ 105
- Table 8.3-12 'Parameter list – Notification' ⇒ 106
- Table 8.3-13 'Parameter list – Monitoring' ⇒ 108
- Table 8.3-14 'Parameter list – SSL/TLS' ⇒ 109
- Table 8.3-15 'Parameter list – Control Center' ⇒ 110
- Table 8.3-16 'Parameter list – SNMP' ⇒ 112
- Table 8.3-17 'Parameter list – TCP port access' ⇒ 113
- Table 8.3-18 'Parameter list – Authentication' ⇒ 114
- Table 8.3-19 'Parameter list – USB' ⇒ 115
- Table 8.3-20 'Parameter list – USB device access control' ⇒ 116
- Table 8.3-21 'Parameter list – Backup' ⇒ 117
- Table 8.3-22 'Parameter list – Miscellaneous' ⇒ 118

Table 8.3-1: Parameter list – IPv4

Parameters	Value	Default	Description
ip_addr [IP address]	valid IP address	169.254.0.0/ 16	IP address of the INU server.
ip_pfxlen (Prefix length)	valid IP address	255.255.0.0	The IP address and the prefix length defines the network mask of the INU server. Subnet masks are used to logically partition big networks into subnetworks. If you are using the INU server in a subnetwork, it requires the subnet mask of the subnetwork.
ip_router [Router]	valid IP address	0.0.0.0	IP address of the network's standard router which the INU server uses. With a router, you can address IP addresses from other networks.
ip_dhcp [DHCP]	on/off	on	Enables/disables the DHCP protocol. If DHCP is enabled in your network, IPv4 network configuration (IP address, subnet mask, gateway, DNS) is automatic.
ip_auto [ARP/PING]	on/off	on	Enables/disables the ARP/PING protocol. You can use the commands ARP and PING to change an IP address. The implementation depends on your system; read the documentation of your operating system.



*We recommend deactivating **DHCP**, **BOOTP** and **ARP/PING** as soon as the INU server has been assigned with an IP address.*

Table 8.3-2: Parameter list – IPv6

Parameters	Value	Default	Description
ipv6 [IPv6]	on/off	on	Enables/disables the IPv6 functionality of the INU server.
ipv6_auto [Automatic configuration]	on/off	on	Enables/disables the automatic assignment of the IPv6 address to the INU server.
ipv6_addr [IPv6 address]	n:n:n:n:n:n	::	Defines an IPv6 unicast address in the format n:n:n:n:n:n which is manually assigned to the INU server. <ul style="list-style-type: none"> • Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. • Leading zeros can be omitted. • An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.

Parameters	Value	Default	Description
ipv6_router [Router]	n:n:n:n:n:n	::	Manually defines a static router to which the INU server sends its requests.
ipv6_pfxlen [Prefix length]	0-64 [1–2 characters; 0–9]	64	Defines the length of the subnet prefix for the IPv6 address. The value 64 is preset. Address ranges (e.g. your network) are specified with prefixes. To do this, the prefix length (number of bits used) is added to the IPv6 address as a decimal number and the decimal number is preceded by '/'.

Table 8.3-3: Parameter list – IP-VLAN

Parameters	Value	Default	Description
iplan_mgmt [IP management VLAN]	on/off	off	Enables/disables the forwarding of IP management VLAN data. If this option is enabled, SNMP is only available in the IP management VLAN.
ipvlan_mgmt_idx [VLAN-ID]	0-4096 [1–4 characters; 0–9]	0	ID for the identification of the IP management VLAN.
ipvlan_mgmt_any [Access from any VLAN]	on/off	off	Enables/disables the administrative access (web) to the INU server via IPv4 client VLANs. If this option is enabled, the INU server can be administrated via all VLANs.
ipvlan_mgmt_untag [Access via LAN (untagged)]	on/off	on	Enables/disables the administrative access to the INU server via IP packets without tag. If this option is disabled, the INU server can only be administrated via VLANs.
ipvlan_on_1 ~ ipvlan_on_20 [VLAN]	on/off	off	Enables/disables the forwarding of IP client VLAN data.
ipvlan_addr_1 ~ ipvlan_addr_20 [IP address]	valid IP address	192.168.0.0	IP address of the INU server within the IP client VLAN.
ipvlan_mask_1 ~ ipvlan_mask_20 [Prefix length]	valid IP address	255.255.255.0	Subnet mask of the INU server within the IP client VLAN.

Parameters	Value	Default	Description
ipvlan_router_1 ~ ipvlan_router_20 [Router]	valid IP address	0.0.0.0	IP router address in the IP management VLAN. With a router, you can address IP addresses from other networks.
ipvlan_id_1 ~ ipvlan_id_20 [VLAN-ID]	0-4096 [1-4 characters; 0-9]	0	ID for the identification of the IP client VLAN.
utn_2vlan_1 ~ utn_2vlan_20 [Allocate VLAN]	0-9 [1 character; 0-9]	0	Allocates a VLAN to the USB port. 0 = any 1 = VLAN 1 2 = VLAN 2 usw. 9 = none

Table 8.3-4: Parameter list – DNS

Parameters	Value	Default	Description
dns [DNS]	on/off	on	Enables/disables the name resolution via a DNS server.
dns_domain [Domain name]	max. 255 characters [a-z, A-Z, 0-9]	[blank]	Defines the IP address of the primary DNS server.
dns_primary [Primary DNS server]	valid IP address	0.0.0.0	Defines the IP address of the secondary DNS server. The secondary DNS server is used if the first one is not available.
dns_secondary [Secondary DNS server]	valid IP address	0.0.0.0	Defines the domain name of an existing DNS server.
dns_1st4 [Preferred address typ]	on/off	on	Specifies which address type is used after the IP address is returned from the DNS server. (This option is only relevant if „IPv4 and IPv6“ is enabled.) on = IPv4 is preferred off = IPv6 is preferred

Table 8.3-5: Parameter list – POP3

Parameters	Value	Default	Description
pop3 [POP3]	on/off	off	Enables/disables the POP3 functionality.

Parameters	Value	Default	Description
pop3_srv [Server address]	max. 128 characters	[blank]	Defines the POP3 server via its IP address or host name. A host name can only be used if a DNS server (⇒ 40) was configured beforehand.
pop3_port [Server port]	1-65535 [1–5 characters; 0–9]	110	Defines the port which the INU server uses to receive emails. The default port number for POP3 is 110. The default port number for SSL/TLS (parameter 'POP3 – Security' ⇒ 46) is 995. If required, read the documentation of your POP3 server.
pop3_sec [Security]	0-2 [1 character; 0–2]	0	Defines the authentication method to be used: <ul style="list-style-type: none"> • APOP: encrypts the password when logging on to the POP3 server. • SSL/TLS: encrypts the entire communication with the POP3 server. The encryption strength is defined via the encryption protocol and level ⇒ 65. 0 = no security 1 = APOP 2 = SSL/TLS
pop3_poll [Check mail every]	1-10080 [1–5 characters; 0–9]	2	Defines the time interval (in minutes) which with the POP3 server is checked for emails.
pop3_limit [Ignore mail exceeding]	0-4096 [1–4 characters; 0–9]	4096	Defines the maximum email size (in Kbyte) to be accepted by the INU server. 0 = unlimited
pop3_usr [User name]	max. 128 characters	[blank]	Defines the user name used by the INU server to log on to the POP3 server.
pop3_pwd [Password]	max. 128 characters	[blank]	Defines the user password used by the INU server to log on to the POP3 server.

Table 8.3-6: Parameter list – SMTP

Parameters	Value	Default	Description
smtp_srv [Server address]	max. 128 characters	[blank]	Defines the SMTP server via its IP address or host name. A host name can only be used if a DNS server (⇒ 40) was configured beforehand.

Parameters	Value	Default	Description
smtp_port [Server port]	1-65535 [1–5 characters; 0–9]	25	<p>Defines the port which the INU server and SMTP server use to communicate.</p> <p>The default port number for SMTP is 25. For SSL/TLS (parameter 'SMTP – SSL/TLS' ⇨ 47), SMTP servers use by default port 587 (STARTSSL/STARTTLS) or the old port 465 (SMTPS). If required, read the documentation of your SMTP server.</p>
smtp_ssl [SSL/TLS]	on/off	off	<p>Enables/disables SSL/TLS.</p> <p>SSL/TLS encrypts the communication from the INU to the SMTP server. The encryption strength is defined via the encryption protocol and level ⇨ 65.</p>
smtp_sender [Sender name]	max. 128 characters	[blank]	<p>Defines the email address used by the INU server to send emails.</p> <p>Very often the name of the sender and the email account user name are identical.</p>
smtp_auth [Login]	on/off	off	<p>Enables/disables SMTP authentication. To send emails, the INU sends its user name and password to the SMTP server to authenticate itself. Enter user name (parameter 'SMTP – User name' ⇨ 47) and password (parameter 'SMTP – Password' ⇨ 47).</p> <p>Some SMTP servers require SMTP authentication to prevent fraudulent use (spam).</p>
smtp_usr [User name]	max. 128 characters	[blank]	<p>Defines the user name used by the INU server to log on to the SMTP server.</p>
smtp_pwd [Password]	max. 128 characters	[blank]	<p>Defines the password used by the INU server to log on to the SMTP server.</p>
smtp_sign [Security (S/MIME)]	on/off	off	<p>Enables/disables signing email using S/MIME (Secure/Multipurpose Internet Mail Extensions). A signature created by the sender allows the recipient to verify the identity of the sender and to make sure that the email was not modified. All S/MIME security features require an S/MIME certificate ⇨ 71.</p>
smtp_attpkey [Attach public key]	on/off	on	<p>Sends the public key together with the email.</p> <p>Many email clients require the key to display the email.</p>
smtp_encrypt [Encrypt]	on/off	off	<p>Enables the encryption of emails. Only the intended recipient can open and read the encrypted email.</p>

Table 8.3-7: Parameter list – Bonjour

Parameters	Value	Default	Description
bonjour [Bonjour]	on/off	on	Enables/disables Bonjour.
bonjour_name [Bonjour name]	max. 64 characters [a-z, A-Z, 0-9]	[Default name]	Defines the Bonjour name of the INU server. The INU server uses this name to announce its Bonjour services. If no Bonjour name is entered, a default name will be used (device name@lCxxxxxx).

Table 8.3-8: Parameter list – Server services


Parameters	Value	Default	Description
wdav_on [WebDAV]	on/off	off	Enables/disables the WebDAV functionality of the INU server
wdav_url [Server address]	max. 128 characters	[blank]	Defines a WebDAV server by its IP address or host name. A host name can only be used if a DNS server (⇒ 40) was configured beforehand.
wdav_usr [User name]	max. 128 characters	[blank]	Defines the user name used by the INU server to log on to the WebDAV server.
wdav_pwd [Password]	max. 128 characters	[blank]	Defines the password used by the INU server to log on to the WebDAV server.
wdav_ssl [SSL/TLS]	on/off	off	Enables/disables SSL/TLS encryption of communication between the INU server and WebDAV server. The encryption strength is defined via the encryption protocol and level ⇒ 65.
syslogng [Syslog-ng]	on/off	off	Enables/disables the syslog-ng functionality of the INU server.
syslogng_srv [Server address]	max. 64 characters	[blank]	Defines a syslog-ng server by its IP address or host name. A host name can only be used if a DNS server (⇒ 40) was configured beforehand.
syslogng_port [Server port]	1-65535 [1-5 characters; 0-9]	514	Defines the port number used by the INU server to communicate with the syslog-ng server. The port number 514 is preset.
syslogng_ssl [SSL/TLS]	on/off	off	Enables/disables SSL/TLS encryption of communication between the INU server and syslog-ng server. The encryption strength is defined via the encryption protocol and level ⇒ 65.

Table 8.3-9: Parameter list – Description

Parameters	Value	Default	Description
sys_name [Host name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Device name as alternative to IP address. With a name you can identify the INU server more easily in the network, e.g. if you are using several INU servers. Displayed in the INU Control Center, the SEH UTN Manager.
sys_descr [Description]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Device description, e.g. location or department. Displayed in the INU Control Center, the SEH UTN Manager.
sys_contact [Contact person]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Contact person, e.g. device administrator. Is displayed in the INU Control Center.

Table 8.3-10: Parameter list – Date/Time


Parameters	Value	Default	Description
ntp [Date/Time]	on/off	on	Enables/disables the use of a time server (SNTP).
ntp_server [Time server]	max. 64 characters [a-z, A-Z, 0-9]	pool.ntp.org	Defines a time server by its IP address or host name. A host name can only be used if a DNS server (⇒ 40) was configured beforehand.
ntp_tzone [Time zone]	UTC, GMT, EST, EDT, CST, CDT, MST, MDT, PST, PDT, etc.	CET/CEST (EU)	Compensates Coordinated Universal Time (UTC) for location and national particularities (day-light saving time etc.).



Important:
If your network is configured accordingly, the INU server receives the time server settings automatically via DHCP. A time server assigned in such a manner always takes precedence over manual settings.

Table 8.3-11: Parameter list – UTN port

Parameters	Value	Default	Description
utn_port [UTN port]	1-9200 [1-4 characters; 0-9]	9200	Defines the number of the UTN port for unencrypted connections.



WARNING
The UTN port must not be blocked by security software (firewall).


Parameters	Value	Default	Description
utn_sslport [Encrypted UTN port]	1-9443 [1–4 characters; 0–9]	9443	<p>Defines the number of the UTN port for encrypted connections.</p> <div style="display: flex; align-items: center;">  <div> <p>WARNING</p> <p>The encrypted UTN port must not be blocked by security software (firewall).</p> </div> </div>

Table 8.3-12: Parameter list – Notification

Parameters	Value	Default	Description
mailto_1 mailto_2 [Email address]	valid email address [max. 64 characters]	[blank]	Email address of the recipient for notifications.
mailsub [Subject]	max. 64 characters [a–z, A–Z, 0–9, %P, %p, &%N, %H, %l, %M, %E, %D, %t]	%p %N: %E	<p>Defines the content of the email subject line for notification and status emails.</p> <p>%P = Product type %p = Model %N = Default name %H = Host name %l = IP address %M = MAC address %E = Event %D = Date %t = Time</p>
noti_stat_1 noti_stat_2 [Status email]	on/off	off	Enables/disables the periodical sending of a status email to recipient 1 or 2.
notistat_d [Interval]	al su mo tu we th fr sa	al	<p>Defines the day (the interval) on which a status email is sent.</p> <p>al = daily su = Sunday mo = Monday tu = Tuesday we = Wednesday th = Thursday fr = Friday sa = Saturday</p>
notistat_h [hh]	0-23 [1–2 characters; 0–9]	0	<p>Specifies the time (hour) at which a status email is sent.</p> <p>1 = 1. hour 2 = 2. hour 3 = 3. hour etc.</p>

Parameters	Value	Default	Description
notistat_tm [mm]	0-5 [1 character; 0-5]	0	Specifies the time (minute) at which a status email is sent. 0 = 00 min 1 = 10 min 2 = 20 min 3 = 30 min 4 = 40 min 5 = 50 min
notisys_1 notisys_2 [Send system information]	on/off	off	Enables/disables sending emails with system information (reboot, network connections, power supply, temperature warnings, etc.).
notiusb_1 notiusb_2 [Send USB port and USB device information]	on/off	off	Enables/disables sending emails with information about the USB port and connected USB devices (enable or disable a USB port, connect or remove a USB device, etc.)
notisdcard_1 notisdcard_2 [Send SD card information]	on/off	off	Enables/disables sending emails with SD card information (connect or remove an SD card, unusable SD card, etc.).
trapto_1 trapto_2 [Address]	valid IP address	0.0.0.0	SNMP trap address of the recipient.
trapcommu_1 trapcommu_2 [Community]	max. 64 characters [a-z, A-Z, 0-9]	public	SNMP trap community of the recipient.
trapversion_1 trapversion_2 [SNMP version]	--- v1 v3		Defines the SNMP protocol version for SNMP trap sending. --- = none v1 = SNMPv1 v3 = SNMPv3
trapsys [Send system information]	on/off	off	Enables/disables sending SNMP traps with system information (reboot, network connections, power supply, temperature warnings, etc.).
trapusb [Send USB port and USB device information]	on/off	off	Enables/disables sending SNMP traps with information about the USB port and connected USB devices (enable or disable a USB port, connect or remove a USB device, etc.)
trap_sdcard [Send SD card information]	on/off	off	Enables/disables sending SNMP traps with SD card information (connect or remove an SD card, unusable SD card, etc.).

Table 8.3-13: Parameter list – Monitoring

Parameters	Value	Default	Description
monitoring [Monitoring]	on/off	off	Enables/disables the monitoring of system values, events and errors.
wdav_monidir [Directory]	max. 128 characters	[blank]	Defines the directory on the WebDAV server where the monitoring logs are stored.
wdav_monimdir [Create individual directories for days]	on/off	on	Enables/disables the creation of subdirectories to store monitoring logs for a single day. <div style="display: flex; align-items: center;"> <div> <p>Important:</p> <p>The FIFO principle (first-in, first-out) is applied after one year. For example, 1 January of last year will be overwritten with files from 1 January of the current year.</p> </div> </div>
wdav_monion [Continuous backup]	on/off	off	Enables/disables the regular backup of monitoring logs to the WebDAV server. <div style="display: flex; align-items: center;"> <div> <p>Important:</p> <p>The monitoring logs are divided into 2 MB files on the INU server. Once this size is reached, the file is stored on the WebDAV server.</p> </div> </div>
wdav_monidaily [Daily backup at]	on/off	off	Enables/disables daily storage of the monitoring logs on the WebDAV server.
wdav_monihh [Daily backup at]	0-23	0	Defines the time at which the monitoring logs are stored daily on the WebDAV server.
monimailto [Email address]	valid email address [max. 64 characters]	[blank]	Defines the email address of the recipient for sending monitoring logs.
monimailsub [Email subject]	max. 64 characters [a-z, A-Z, 0-9, %P, %p, &%N, %H, %l, %M, %E, %D, %t]	%p: %N %E	Defines the content of the email subject line for monitoring log emails. %P = Product type %p = Model %N = Default name %H = Host name %l = IP address %M = MAC address %E = Event %D = Date %t = Time



Parameters	Value	Default	Description
monimail [Continuous backup]	on/off	off	Enables/disables the regular sending of monitoring logs as email.
			 Important: The monitoring logs are divided into 2 MB files on the INU server. Once this size is reached, the file is sent as an email attachment.
monimaildaily [Daily backup at]	on/off	off	Enables/disables the daily sending of the monitoring logs as email.
monimailhh [Daily backup at]	0-23	0	Defines the time at which the monitoring logs are sent daily by email.
syslogngdbg [Syslog-ng export]	on/off	off	Enables/disables the sending of monitoring information to a syslog-ng server.
syslogng_ietf [Format]	on/off	on	Defines the format for monitoring information sent by the INU server to the syslog-ng server: IETF (RFC 5424) or Legacy (RFC 3164/BSD). on = IETF (RFC 5424) off = Legacy (RFC 3164/BSD)






Table 8.3-14: Parameter list – SSL/TLS

Parameters	Value	Default	Description
sslmethod [Encryption protocol]	any tls10 tls11 tls12 tls13	any	Defines the encryption protocol for SSL/TLS connections. any = at will (automatic negotiation) tls10 = TLS 1.0 tls11 = TLS 1.1 tls12 = TLS 1.2 tls13 = TLS 1.3
			 WARNING Current browsers do not support SSL. If you use SSL with a current browser and the setting HTTPS only for access to the INU Control Center (⇒ 67), a connection cannot be established. Use TLS (and <u>not</u> SSL).

Parameters	Value	Default	Description
security [Encryption level]	1-4 [1 character; 1-4]	4	<p>Defines the encryption level for SSL/TLS connections.</p> <p>1 = low 2 = medium 3 = high 4 = any (automatic negotiation)</p> <div style="border-left: 2px solid red; padding-left: 10px;"> <p>WARNING</p> <p>Current browsers do not support cipher suites from the Low level. If you use Low with a current browser and the setting HTTPS only for access to the INU Control Center (⇒ ¶67), a connection cannot be established.</p> <p>Use an encryption level as high as possible.</p> </div>


Table 8.3-15: Parameter list – Control Center

Parameters	Value	Default	Description
http_allowed [Connection]	on/off	on	<p>Defines the connection type (HTTP/HTTPS) to be used for connecting to the INU Control Center.</p> <p>on = HTTP/HTTPS off = HTTPS only</p> <p>The encryption strength is defined via the encryption protocol and level ⇒ ¶65.</p> <div style="border-left: 2px solid red; padding-left: 10px;"> <p>WARNING</p> <p>Current browsers do not support low security settings. With them a connection cannot be established.</p> <p>Do <u>not</u> use the following combination: Encryption protocol HTTPS and encryption level Low.</p> <p>When the connection is established, the identity of the INU server is verified. For that, the client asks for the certificate via the browser (⇒ ¶71). This certificate must be accepted by the browser; read the documentation of your browser software.</p> </div>

Parameters	Value	Default	Description
sessKeys [Restrict Control Center access]	on/off	off	Enables/disables the INU Control Center Control Center user accounts. If they are enabled, a login screen is displayed when opening the INU Control Center.  Important: Define user accounts (user names and passwords).
admin_name [Administrator – User name]	max. 64 characters [a–z, A–Z, 0–9]	admin	Defines the user name for the administrator user account.  Important: Also, this is the user name of the SNMPv3 admin account ⇒ 69.
admin_pwd [Administrator – Password]	8–64 characters [a–z, A–Z, 0–9]	administrator	Defines the password for the administrator user account.  Important: Also, this is the password of the SNMPv3 admin account ⇒ 69.
any_name [Read-only user – User name]	max. 64 characters [a–z, A–Z, 0–9]	anonymous	Defines the user name for the read-only user account.  Important: Also, this is the user name of the SNMPv3 user account ⇒ 69.
any_pwd [Read-only user – Password]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the password for the read-only user account.  Important: Also, this is the password of the SNMPv3 user account ⇒ 69.
usb_Mg_name [USB Manager – User name]	max. 64 characters [a–z, A–Z, 0–9]	USB Manager	Defines the user name for the USB Manager account.
usb_Mg_pwd [USB Manager – Password]	8–64 characters [a–z, A–Z, 0–9]	[blank]	Defines the user password for the read-only user account.
sessKeyUList [Login screen displays]	on/off	on	Defines the type of login screen. on = shows a user list, only password must be entered off = neutral login screen, user name and password must be entered
sessKeyTimer [Session timeout]	on/off	on	Enables/disables the session timeout.

Parameters	Value	Default	Description
sessKeyTimeout [Session timeout]	120-3600 [3-4 characters; 0-9]	600	Time in seconds after which the timeout is to be effective.

Table 8.3-16: Parameter list – SNMP



Parameters	Value	Default	Description
snmpv1 [SNMPv1]	on/off	on	Enables/disables SNMPv1.
snmpv1_ronly [Read-only]	on/off	off	Enables/disables the write protection for the community.
snmpv1_community [Community]	max. 64 characters [a-z, A-Z, 0-9]	public	SNMP community name Enter the name as it is defined in the monitoring station.
<div style="display: flex; align-items: center;">  <div> <p>Important:</p> <p>The default name is 'public'. This name is commonly used for read/write communities. We recommend to change it as soon as possible to increase security.</p> </div> </div>			
snmpv3 [SNMPv3]	on/off	on	Enables/disables SNMPv3.
any_hash [Hash]	md5 sha	md5	Specifies the hash algorithm for SNMP user group 1.
any_rights [Access rights]	--- readonly readwrite	readonly	Defines the access rights of the SNMP user group 1. --- = none
any_cipher [Encryption]	--- aes des	---	Defines the encryption method of the SNMP user group 1. --- = none
admin_hash [Hash]	md5 sha	md5	Specifies the hash algorithm for SNMP user group 2.
admin_rights [Access rights]	--- readonly readwrite	readwrite	Defines the access rights of the SNMP user group 2. --- = none
admin_cipher [Encryption]	--- aes des	---	Defines the encryption method of the SNMP user group 2.



Important:

The administrator user account and the read access user account are also used as SNMP user accounts (⇒ 69). Consider this when setting up user accounts.

Table 8.3-17: Parameter list – TCP port access

Parameters	Value	Default	Description
protection [Port access control]	on/off	off	Enables/disables the blocking of selected ports and thus connections to the INU server.
protection_level [Security level]	protec_utn protec_tcp protec_all	protec_utn	Specifies the port types to be blocked. protec_utn= UTN access (UTN ports) protec_tcp= TCP access (TCP ports: HTTP/HTTPS, UTN) protec_all= all ports (IP ports)
ip_filter_on_1 ~ ip_filter_on_(max. Ports) [IP address]	on/off	off	Enables/disables an exception from port blocking.
ip_filter_1 ~ ip_filter_(max. Ports) [IP address]	valid IP address	[blank]	Defines networks elements that are excluded from port blocking by their IP address.  The prefix notation "<IP address>/<prefix length>" can be used to freely define IPv4 and IPv6 subnets.
hw_filter_on_1 ~ hw_filter_on_8 [MAC address]	on/off	off	Enables/disables an exception from port blocking.
hw_filter_1 ~ hw_filter_8 [MAC address]	Valid MAC address	00:00:00:00:0 0:00	Defines elements that are excluded from port blocking by their MAC address (MAC address).  Important: MAC addresses are not delivered through routers!


Parameters	Value	Default	Description
protection_test [Test mode]	on/off	on	Enables/disables the test mode.  WARNING The test mode is active by default so that you can test your settings without locking yourself out. Your settings will be active until the INU is restarted, afterwards access is no longer restricted. After you have successfully tested your settings, you have to deactivate the test mode so that access control is permanent.

Table 8.3-18: Parameter list – Authentication

Parameters	Value	Default	Description
auth_typ [Authentication method]	--- MD5 TLS TTLS PEAP FAST	---	Defines an authentication method (according to IEEE 802.1X). If you use an authentication method in your network, the INU server can participate. --- =none MD5 =EAP-MD5 TLS =EAP-TLS TTLS =EAP-TTLS PEAP=PEAP FAST =EAP-FAST
auth_name [User name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the username of the INU server, as it is configured on the authentication server (RADIUS) for the EAP authentication methods MD5, TTLS, PEAP and FAST.
auth_pwd [Password]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the password with which the INU server is set up on the RADIUS server for the EAP authentication methods MD5, TTLS, PEAP, and FAST.
auth_intern [Inner authentication]	--- PAP CHAP MSCHAP2 EMD5 ETLS	---	Defines the kind of inner authentication for the EAP authentication methods TTLS, PEAP, and FAST. --- = none PAP =PAP CHAP=CHAP MSCHAP2=MS-CHAPv2 EMD5=EAP-MD5 ETLS =EAP-TLS

Parameters	Value	Default	Description
auth_extern [PEAP/EAP-FAST options]	--- PLABEL0 PLABEL PVER0 PVER1 FPROV1	---	Defines the kind of external authentication for the EAP authentication methods TTLS, PEAP, and FAST. --- =none PLABEL0=PEAPLABEL0 PLABEL1=PEAPLABEL1 PVER0=PEAPVER0 PVER1=PEAPVER1 FPROV1=FASTPROV1
auth_ano_name [Anonymous name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the anonymous name for the unencrypted part of the EAP authentication methods TTLS, PEAP, and FAST.
auth_wpa_addon [WPA Add on]	max. 255 characters [a-z, A-Z, 0-9]	[blank]	Defines an optional WPA expansion for the EAP authentication methods TTLS, PEAP, and FAST.

Table 8.3-19: Parameter list – USB


Parameters	Value	Default	Description
utn_sec [Encrypt USB communication (SSL/TLS)]	on/off	off	Enables/disables SSL/TLS encryption of all USB and UTN communication. The encryption strength is defined via the encryption protocol and level ⇨ 65.
utn_hide [Hide port key protected USB ports]	on/off	off	Disables/enables the display of USB devices in the selection list of the UTN Manager. Applies to USB devices protected by the "Port Key Control" security mechanism.
utn_hid [Disable input devices (HID class)]	on/off	on	Enables/disables the blocking of input devices (HID – human interface devices). on = no blocking off = blocking
utn_tag_1 ~ utn_tag_20 [Port name]	max. 32 characters [a-z, A-Z, 0-9]	[blank]	Freely definable name of the USB port.
utn_ppwr_1 ~ utn_ppwr_20 	on/off	on	Disables/enables the power supply for the USB port (i.e. the USB device connected to the port).

Table 8.3-20: Parameter list – USB device access control



Important:

Some parameters can be assigned to a USB port twice, e.g. two USB port keys per USB port.

These parameters are assigned to the USB ports as follows:

USB port 01 = Parameter number '_01' and '_21'.

USB port 02 = Parameter number '_02' and '_22'.

...

USB port 10 = Parameter number '_10' and '_30'.

USB port 11 = Parameter number '_11' and '_31'.

...

USB port 19 = Parameter number '_19' and '_39'.

USB port 20 = Parameter number '_20' and '_40'.

Parameters	Value	Default	Description
utn_dscr_1 ~ utn_dscr_20 [Descripton]	max. 128 characters [a-z, A-Z, 0-9]	[blank]	Allows a description of the USB port. The written information is displayed on the properties page of the SEH UTN manager for the corresponding USB port. (A line break can be created with .)
utn_acctr_1 ~ utn_acctr_20 [Method]	--- ids key keyids	---	Defines the method(s) for limiting the access and use of the USB port and the connected USB device. --- =no protection ids =device assignment key =port key control keyids=device assignment and port key control
utn_pkkey_1 ~ utn_pkkey_40 [Key]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the key for the USB port and the connected USB device when port key control is used.
utn_pkvalid_1 ~ utn_pkvalid_40 [Validity]	off ever week date	off	Defines the validity of a port key. Validity allows you to specify when users can use a USB port and the USB device connected to it. off = off ever = always (permanently valid) date = expires on week = weekly






Parameters	Value	Default	Description
utn_pkalive_40 ~ utn_pkalive_40 [Validity]	sMtWTFs:hh:hh:JJ: MM:DD:HH [max. 64 characters]	sMtWTFs:00: 23:19:12:31:2 3	<p>Defines the validity of a port key. Validity allows you to specify when users can use a USB port and the USB device connected to it.</p> <p>sMtWTFs:hh:hh:JJ:MM:DD:HH = Days (for weekly) : hour (for weekly) : hour (for weekly) : year (for expires on) : month (for expires on) : day (for expires on) : hour (for expires on)</p> <p>s= valid on Sunday M= valid on Monday t= valid on Tuesday W= valid on Wednesday T= valid on Thursday F= valid on Friday S= valid on Saturday</p> <p>To exclude a day, the letter of the day must be replaced by an underscore (_).</p>
utn_vendprodIDs_1 ~ utn_vendprodIDs_40 [USB device]	max. 161 characters	[blank]	<p>Defines the VID (Vendor ID) and PID (Product ID) of the USB device that is assigned to the USB port via the device assignment.</p> <p> Often VID and PID of a USB device are unknown. We recommend configuration via the INU Control Center because VID and PID will be automatically determined and entered with this method.</p>

Table 8.3-21: Parameter list – Backup

Parameters	Value	Default	Description
wdav_bupdir [Server directory]	max. 128 characters	[blank]	Defines the directory on the WebDAV server where system backups are stored.
wdav_bupmdir [Create individual directories for days]	on/off	on	<p>Enables/disables the creation of subdirectories to store system backups for a single day.</p> <p> Important: The FIFO principle (first-in, first-out) is applied after one year. For example, 1 January of last year will be overwritten with files from 1 January of the current year.</p>
wdav_bupauto [Change backup]	on/off	off	Enables/disables saving a system backup to a WebDAV server as soon as the device configuration has been changed.

Parameters	Value	Default	Description
wdav_bupday [Daily backup at]	on/off	off	Enables/disables saving a daily system backup to the WebDAV server.
wdav_buph [Daily backup at]	0-23	0	Defines the time at which the daily system backup is stored on the WebDAV server.
autoSync [Parameter backup]	on/off	on	Enables/disables saving a system backup on the SD card as soon as the device configuration has been changed.

Table 8.3-22: Parameter list – Miscellaneous

Parameters	Value	Default	Description
utn_heartbeat	1-1800 [1–4 characters; 0–9]	180	 WARNING This parameter can only be used after consultation with the SEH support team.
utn_poffdura_1 ~ utn_poffdura_20	0-100 [1–3 characters; 0–9]	0	 WARNING This parameter can only be used after consultation with the SEH support team.
utn_prereset_1 ~ utn_prereset_20	on/off	off	 WARNING This parameter can only be used after consultation with the SEH support team.
dailyrestart	0-23	24	Defines the time (full hour) at which a restart is performed. The default value "24" disables the function.
snmprestart	0-23	24	Defines the time (full hour) at which the SNMP services are restarted. The default value "24" disables the function.

8.4 SEH UTN Manager – Feature Overview

Which features are inactive (grayed out) in the SEH UTN Manager depends on different factors:

- Selection list mode
 - global
 - user
- Client operating system (Windows, macOS, Linux)
- Client user account
 - administrator or group members of 'utnusers'
 - standard user or users which are not members of the group 'utnusers'
- Write access to the *.ini file (selection list)



The administrator can use these factors to provide users with individual functions.

The following table gives an overview. It shows the features that are basically available. In addition, individual features will not be displayed or will be displayed as inactive because

- the INU server model does not support them
- the USB device connected does not support them
- security measures have been implemented

Table 8.4-23: SEH UTN Manager – Feature Overview Linux

	Global selection list		User selection list		
	Adminis- trator	User	Adminis- trator	User (read/ write *.ini)	User (no read/ write *.ini)
Menu					
Selection List – Edit	✓	✗	✓	✓	✗
Selection List – Export	✓	✗	✓	✗	✗
Selection List – Refresh	✓	✓	✓	✓	✓
UTN Server – Configure	✓	✓	✓	✓	✓
UTN Server – Set IP Address	✓	✓	✓	✓	✓
UTN-Server – Activate Auto-Connect	✓	✗	✓	✗	✗
UTN Server – Set User Port Keys	✓	✗	✓	✓	✗
UTN Server – Set Auto-Connect Port Keys	✓	✗	✓	✓	✗
UTN Server – Add	✓	✗	✓	✓	✗
UTN Server – Remove	✓	✗	✓	✓	✗
UTN Server – Refresh	✓	✓	✓	✓	✓
Port – Activate	✓	✓	✓	✓	✓
Port – Deactivate	✓	✓	✓	✓	✓
Port – Request	✓	✓	✓	✓	✓
Port – Remove	✓	✗	✓	✗	✗

	Global selection list		User selection list		
	Adminis- trator	User	Adminis- trator	User (read/ write *.ini)	User (no read/ write *.ini)
Port – Settings	✓	✓	✓	✓	✓
Buttons					
Selection List – Refresh	✓	✓	✓	✓	✓
Selection List – Edit	✓	x	✓	✓	x
Port – Activate	✓	✓	✓	✓	✓
Port – Deactivate	✓	✓	✓	✓	✓
'Program – Options' dialog					
Network Scan – Multicast Search	✓	x	✓	x	x
Network Scan – IP Range Search	✓	x	✓	x	x
Program – Program Messages	✓	x	✓	x	x
Program – Program Update	✓	x	✓	x	x
Automatisms – Auto-Disconnect	✓	x	✓	x	x
Selection List – Selection List Mode	✓	x	✓	x	x
Selection List – Automatic Refresh	✓	x	✓	x	x
'Port Settings' dialog					
Messages	✓	✓	✓	✓	✓

8.5 Index

A

Administration

- email 19
- INU Control Center 11
- remote access 19
- SEH UTN Manager 13

Administrator 68

authentication 76

Auto-Connect 27

Auto-Disconnect 28

Automatic connection 27

Automatisms

- Auto-Connect 27
- Auto-Disconnect 28

B

Backup 88

BadUSB 84

Bonjour 48

Brochures 5

Browser 11

Button 91

- restart 93

C

CA (certification authority) 71

CA certificate 71

Certificate 71

- CA 71
- client 71
- create 72
- default 71
- delete 75
- management 71
- request 73
- requested 71
- S/MIME 71
- self-signed 71
- view 72

certificate

- PKCS#12 71

Certification authority 71

Cipher Suite 65

Client certificate 71

Complete version 14

Compound USB device 24, 95

Configuration backup 88

Connection

- encryption 67
- INU Control Center 67
- myUTN Control Center 67

Console 34

Contact 7

Contact person 52

D

Default certificate 71

Default name 95

Description 52

Device

- contact person 52
- description 52
- name 52, 95
- number 95
- time 53

Device number 95

Device time 53

DHCP (Dynamic Host Configuration Protocol) 40, 45

Documentation

- further applicable documents 5
- mark-ups 6
- symbols 6

Dokumentation 5

Downloads 7

E

EAP (Extensible Authentication Protocol) 76

- FAST (Flexible Authentication via Secure Tunneling) 78

MD5 (Message Digest #5) 76

- PEAP (Protected Extensible Authentication Protocol) 77

TLS (Transport Layer Security) 76

TTLS (Tunneled Transport Layer Security) 77

Email 56

- Administration 19
- event 56
- notifications 56
- POP3 46
- SMTP 46

- status 56
- Encrypted UTN port 86
- Encryption
 - cipher suite 65
 - email 65
 - HTTP 65
 - level 65
 - POP3 65
 - protocol 65
 - SMTP 65
 - SSL/TLS 86
 - strength 65
 - USB connection 65
 - web access 65
- encryption 86
- Ethernet address 95
- Event notification 56
- F**
- Factory default settings 91
- File '<Default-Name_parameter.txt>' 88
- Further applicable documents 5
- G**
- Global selection list 31
- Guarantee 8
- H**
- Hardware Installation Guide 5
- HID (Human Interface Device) 84
 - blocking 84
- Host name 52
- Hostname 105
- HTTP/HTTPS 67
- I**
- IEEE 802.1X 76
- Improper use 8
- ini-file 31
 - Wwrite access 31
- Intended use 8
- INU Control Center 11, 95
 - controls 12
 - encrypted connection 67
- IP address
 - dynamic 40
 - IPv4 40
 - IPv6 42
 - static 40, 45
- IP ports 70
- IPv6 42
- L**
- Liability 8
- Licenses 5
- Login 68
- Login screen 68
- M**
- MAC address 95
- Maintenance 87
- Markups 6
- Minimal version 14
- Monitoring 69
- Multicast search 22
- myUTN Control Center
 - encrypted connection 67
 - user accounts 68
- N**
- Network list 22
- Notification service 56
- Notifications 56
- O**
- Online help 5
- Open source licenses 5
- P**
- Parameters 98
 - backup 88
 - default values 91
 - edit 88
 - lists 98
 - load 89
- Password 68
 - lost 91
- Physical address 95
- PKCS#12 certificate 71
- PKI (public key infrastructures) 71
- Point-to-point connection 24
- POP3 (Post Office Protocol Version 3) 46

- Port blocking 70
- Port connection 13
 - activate 24
 - deactivate 25
- Product information 5, 7
- Protection mechanisms 64
- Q**
- Quick Installation Guide 5
- R**
- Read-only user 68
- Release request 26
- Remote access 19
- Repairs 8
- Requested certificate 71
- Reset 91
 - button 91
 - remote access 91
- reset button 91
- Restart 93
- S**
- S/MIME certificate 71
- Safety regulations 8
- Script 34
- Security level 70
- Security mechanisms 64
- SEH UTN Manager 13, 21, 95
 - complete version 14
 - feature overview 119
 - features 13
 - Funktionsübersicht 119
 - install 15
 - minimal version 14
 - selection list 31
 - start 18
 - versions 14
 - without graphical user interface 34
- SEH UTN Service 14
- Selection list 22, 31
 - global 31
 - user 31
- Self-signed certificate 71
- Session timeout 68
- SMTP (Simple Mail Transfer Protocol) 46
- SNMP
 - Community 69
- SNMP (Simple Network Management Protocol) 69
 - password 69
 - SNMPv1 69
 - SNMPv3 69
 - trap 56
 - user 69
- SNTP (Simple Network Time Protocol) 53
- Software 92
- SSL (Secure Sockets Layer) 65, 67, 86
- SSL/TLS connection 65
- Status email 56
- Symbols 6
- System requirements 2
- T**
- TCP access 70
- TCP port access control 70
 - exception 70
 - test mode 70
- Test mode 70
- Time server 53
- Time zone 53
- Timeout 68
- TLS (Transport Layer Security) 65, 67, 86
- Trap 56
- U**
- Update 92
- USB connection
 - automate 27
 - automatic 27
 - automatic disconnect 28
 - disconnect 25
 - encryption 24, 54, 86
 - point-to-point 24
 - unencrypted 54
- USB data transfer
 - encryption 86
- USB device
 - access 80, 83
 - automatic connection 27
 - automatic disconnect 28

- automatisms 27
 - compound 24, 95
 - connect 21, 24
 - disconnect 25
 - find 22
 - HID (Human Interface Device) 84
 - notifications 29
 - request 26
 - status information 29
 - user access 31
- USB device access 80
- USB port 79, 85
- access 80, 83
 - activate 24
 - automatic connection 27
 - automatic disconnect 28
 - connect 24
 - deactivate 25
 - device assignment 80
 - disable 85
 - disconnect 25
 - enable 85
 - encryption 86
 - key control 80, 83
 - name 79
 - notifications 29
 - power supply 85
 - status information 29
 - virtual 24
- User account 68
- administrator 68
 - read-only user 68
- User name 68
- User selection list 31
- UTC 53
- UTN access 70
- UTN port 54, 70
- encrypt 54
 - SSL port 54
 - unencrypted 54
- utnm 34
- commands 34
 - return value 37
 - syntax 34
- V**
- Version number 92
- Viewing Parameters 88
- Virtual USB ports 24
- VLAN (Virtual Local Area Network) 43
- IP client VLAN 44
 - USB ports 43
- W**
- Warnings 8
- Website 7
- Z**
- Zeroconf 40