Industrial Network Unit

INU User Manual Windows

USB Deviceserver INU-100

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: http://www.seh-technology.com

Document

Type: User Manual
Title: INU User Manual Windows
Version: 1.0 | 2017-12

Legal Information

Contents

1 General Information

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 the use in TCP/IP-based networks.

The SEH UTN Manager has been designed for the use in the following systems:

- Windows XP or later except for Windows Vista and Windows Server 2008
  (For Windows 7 and Windows Server 2008 R2 KB3033929 https://technet.microsoft.com/en-us/library/security/3033929 must be installed.)
- OS X 10.8.x, OS X 10.9.x, OS X 10.10.x, OS X 10.11.2 and later, macOS 10.12.x and later
  (OS X 10.11.2 and later: limited USB device support. macOS 10.12.x and later: limited USB device support.)
- Debian: Ubuntu 12.04.x LTS (64-Bit), Ubuntu 14.04.x LTS (64-Bit), Ubuntu 16.04.x LTS (64-Bit);
  Red Hat: Oracle Linux 6.x (64-bit), Oracle Linux 7.x (64-bit)
  (Installation in other, not officially supported systems can be tried at own responsibility. Further information can be found in chapter 'Administration via the SEH UTN Manager' ⇨ 🗎7.)
- IPv4 TCP/IP network

This document describes the usage in Windows 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' ⇨ 🗎2.

1.2 Documentation

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

Further applicable documents

Thee 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 - Mac - 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
Tip	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

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

http://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 INUdocumentation 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:

WARNING
Warning!

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 ⇨ 🗎3.

1.5 First Steps

1. Read and observe the security regulations in order to avoid damages to people and devices ⇨ 🗎3.
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 it 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' ⇨ 🗎2.

2 Administration Methods

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

- Administration via INU Control Center ⇨ 🗎5
- Administration via the SEH UTN Manager ⇨ 🗎7
- Administration via InterCon-NetTool ⇨ 🗎11
- Administration via Email ⇨ 🗎13

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. Mircosoft Edge).

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

- Open INU Control Center in Browser ⇨ 🗎5
- INU Open Control Center via SEH UTN Manager ⇨ 🗎5
- INU Open Control Center via InterCon-NetTool ⇨ 🗎5
- Controls ⇨ 🗎6

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 ⇨ 🗎15.

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 (⇨ 🗎15) 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 ⇨ 🗎15.
✓ The SEH UTN Manager is installed on the client ⇨ 🗎7.

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.

INU Open Control Center via InterCon-NetTool

1. Start the InterCon-NetTool.
2. In the device list, select the INU server.
3. In the menu bar, select **Actions** – **Launch Browser**.

↳ Your browser opens and the INU Control Center is displayed.

Controls

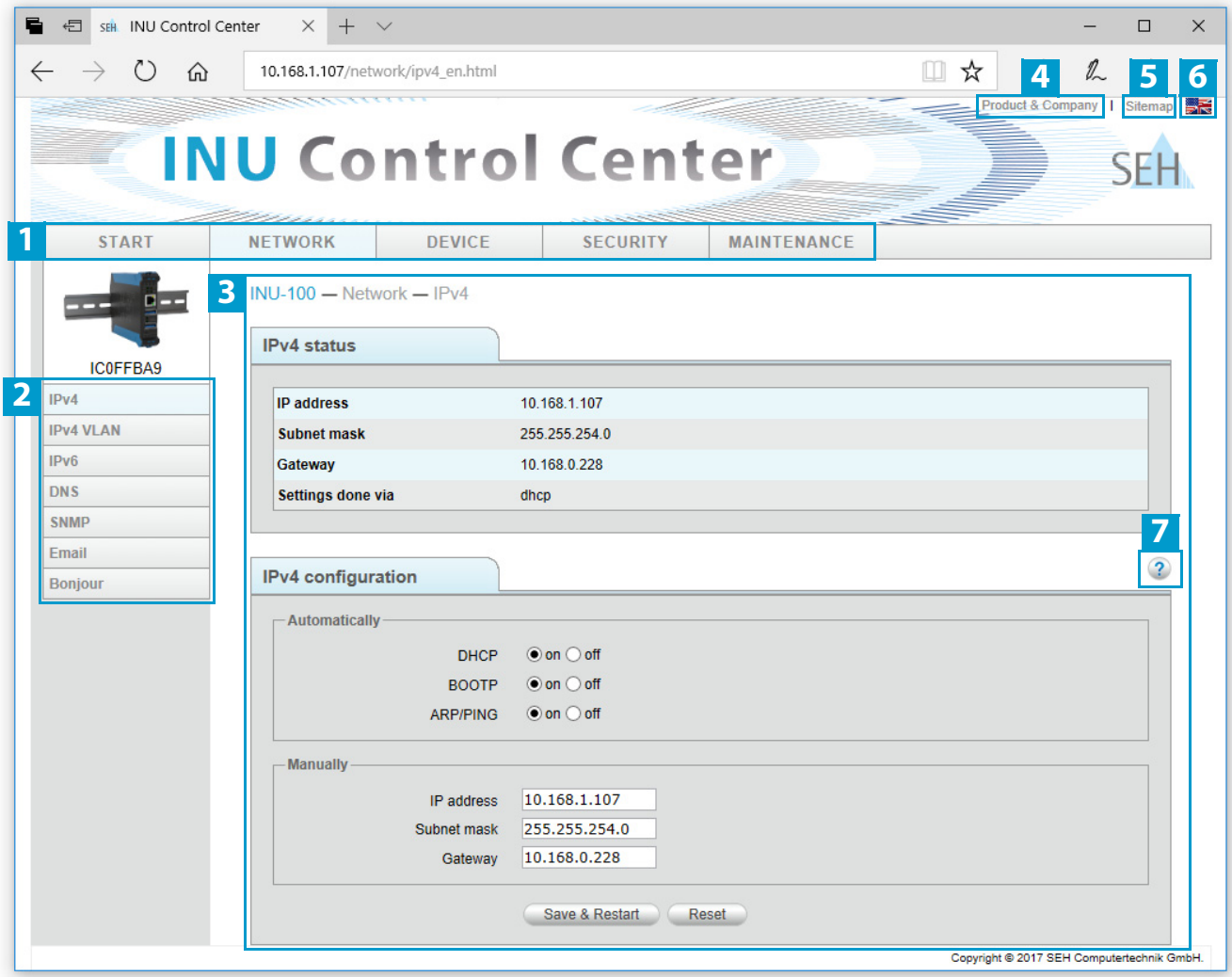


Figure 1: INU Control Center

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

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 working with the SEH UTN Manager is described in detail in the chapter 'Working with the SEH UTN Manager' ⇨ 🗎30.

WARNING

UTN (⇨ 🗎1) and the corresponding SEH UTN Manager only work in IPv4 networks.

In IPv6 networks only the INU Control Center (⇨ 🗎5) can be accessed to administrate the INU server.

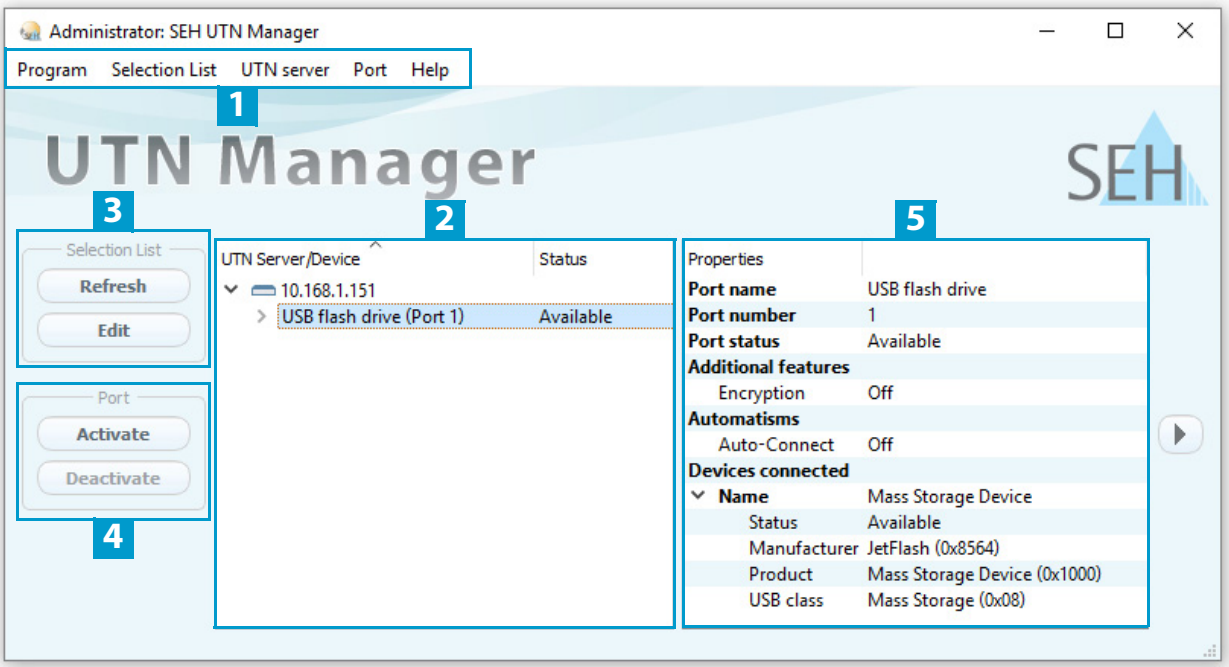


Figure 2: SEH UTN Manager

1	Menu bar	Available menu items
2	Selection list	Shows the selected INU servers and the connected USB devices ⇨ 🗎30.
3	Buttons for editing the selection list	Opens the dialog for searching INU servers in the network and for selecting the desired devices ⇨ 🗎30.
4	Buttons for managing the port connection	Establishes a connection to the USB device connected to the USB port (⇨ 🗎32) or interrupts the connection (⇨ 🗎33).
5	Display area for the properties	Shows information on the selected INU server or USB device ⇨ 🗎37.

Detailed information on how to use the SEH UTN Manager can be found in the ⇨ 🕮 '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 settings of the product-specific security mechanisms
- the client operating system

More details can be found in chapter 'SEH UTN Manager – Feature Overview' ⇨ 🗎85.

Versions

The SEH UTN Manager is available in two versions:

- Complete Version:
  SEH UTN Manager with graphical user interface (⇨Figure 2 🗎7) and additional features.
- Minimal version (without graphical user interface):
  Usage only via command line ('utnm' ⇨ 🗎40) and automated programs ('UTN Actions' ⇨ 🗎34).

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' works in the background and is automatically active after the system start. The service can be controlled by means of the usual administration methods.

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: 'Auto-Connect', 'Auto-Disconnect' and 'Print-On-Demand'. More details can be found in chapter 'SEH UTN Manager – Feature Overview' ⇨ 🗎85.

Installation

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

https://www.seh-technology.com/services/downloads.html

The installation file is available as '*.exe' for Windows systems. The file contains both versions of the SEH UTN Manager. Instead of the standard installation, an unattended installation may be carried out.

- 'Standard Installation' ⇨ 9
- 'Unattended Installation' ⇨ 9

Standard Installation

✓ The SEH UTN Managers installation is suited for Windows XP or later except for Windows Vista and Windows Server 2008.
(For Windows 7 and Windows Server 2008 R2 KB3033929 must be installed https://technet.microsoft.com/en-us/library/security/3033929 installiert.)

✓ The installation can only be carried out by users with administrative rights.

1. Start the SEH UTN Manager installation file.
2. Follow the installation routine.

↳ The SEH UTN Manager is installed on your client.

If used in server-based environments (Citrix XenApp, Microsoft Remote Desktop Services/Terminal Services) and virtualized environments (VMware, Citrix XenDesktop, Microsoft HyperV, etc.) the Windows system may lack required drivers. The installation routine checks the available drivers during the installation process. If drivers are missing, another installer ('USB driver for SEH UTN Manager'). This installer will prepare the installation of the required drivers.

Unattended Installation

An unattended installation takes place without any time-consuming user input. In addition, the SEH UTN Manager UTN Manager can be automatically installed on a large number of clients via login scripts. For more information, refer to the documentation of your operating system.

Default settings used:

- Complete version
- Installation for all users of the client
- Target directory: `%PROGRAMFILES%\SEH Computertechnik GmbH\SEH UTN Manager`
  (Where `%PROGRAMFILES%` is a Windows environment variable for the 'Programs' folder. By means of the command line, the path can be determined as follows: `echo %PROGRAMFILES%`)
- Start menu folder: `SEH Computertechnik GmbH\SEH UTN Manager`
- A desktop shortcut will be created.
- SEH UTN Manager will start automatically after the installation.

✓ The SEH UTN Managers installation is suited for Windows XP or later except for Windows Vista and Windows Server 2008.
(For Windows 7 and Windows Server 2008 R2 the following must be installed: KB3033929 https://technet.microsoft.com/en-us/library/security/3033929 and Hotfix 2921916 https://support.microsoft.com/en-us/help/2921916/the-untrusted-publisher-dialog-box-appears-when-you-install-a-driver-i)

✓ The installation can only be carried out by users with administrative rights.

Important:

By installing the SEH UTN Manager, you automatically accept the SEH Computertechnik GmbH agreement concerning the license and the use of the software. The agreement can be found on the website of SEH Computertechnik GmbH:

https://www.seh-technology.com/services/licenses.html

1. Open the command-line interface.
2. Change to the directory containing the SEH UTN Manager installation file.
3. Enter the command sequence: `"sehutnmanager-win-X.X.X.exe" /S [<command>]`
   Commands: ⇨Table 1 🗎10.
4. Confirm your entry.

↳ The sequence of commands will be run.

Table 1: Installation commands

Command	Description
`/A`	Installs SEH UTN Manager for all users.
`/C`	Installs SEH UTN Manager for the current user only.
`/D=<path>`	Overrides the default installation directory. An absolute path must be specified. It has to be the last parameter used in the command line and must not contain any quotes, even if the path contains spaces.
`/F=<folder name>`	Overrides the default folder name of the Start menu folder. Subfolders can be specified wih '/'.
`/G`	Installs the complete version (⇨ 🗎9) of SEH UTN Manager. Recommended for general use.
`/K`	Does not create a desktop shortcut.
`/M`	Installs the minimal version (⇨ 🗎9) of SEH UTN Manager. Expert use only!
`/R`	Runs SEH UTN Manager after the installation is complete.
`/S`	Instructs the installation to be silent. There is no user interaction and the user cannot cancel the installation.
`/U`	Updates an existing SEH UTN Manager. (If no SEH UTN Manager is installed, it will be installed using the default installation settings.)
`/V1`	Enables command line logging to troubleshoot installation problems.
`/V2`	Creates a log file in the installation folder. The file contains information to troubleshoot installation problems.
`/V3`	Enables command line logging and creates a log file in the installation directory. Both provide information to help troubleshoot installation issues.
`/?`	Shows the help page.

Program Start

You recognize the SEH UTN Manager by its icon: . The program is started with the usual methods of your operating system.

Update

The SEH UTN Manager can notify you about program updates.
If an update is available, the installation file can be loaded and the program updated. Settings are adopted.
You find information on update notifications in the ⇨ 🕮 'SEH UTN Manager Online Help'.

2.3 Administration via InterCon-NetTool

The InterCon-NetTool is a software tool developed by SEH Computertechnik GmbH for the administration of SEH network devices (print servers, TPG, INU servers and so on). Depending on the network device you can perform different actions with the InterCon-NetTool.

- Function ⇨ 🗎11
- Installation ⇨ 🗎12
- Program Start ⇨ 🗎12

Function

After the InterCon-NetToolhas been started, the network will be scanned for connected network devices. The network range to be scanned is freely definable. All network devices found will be displayed in the 'device list'. You can select and configure the devices in the device list.

WARNING
The InterCon-NetTool only works in IPv4 networks.
In IPv6 networks only the INU Control Center (⇨ 🗎5) can be accessed to administrate the INU server.

If you can perform a task with the InterCon-NetTool it is described in the corresponding chapter.

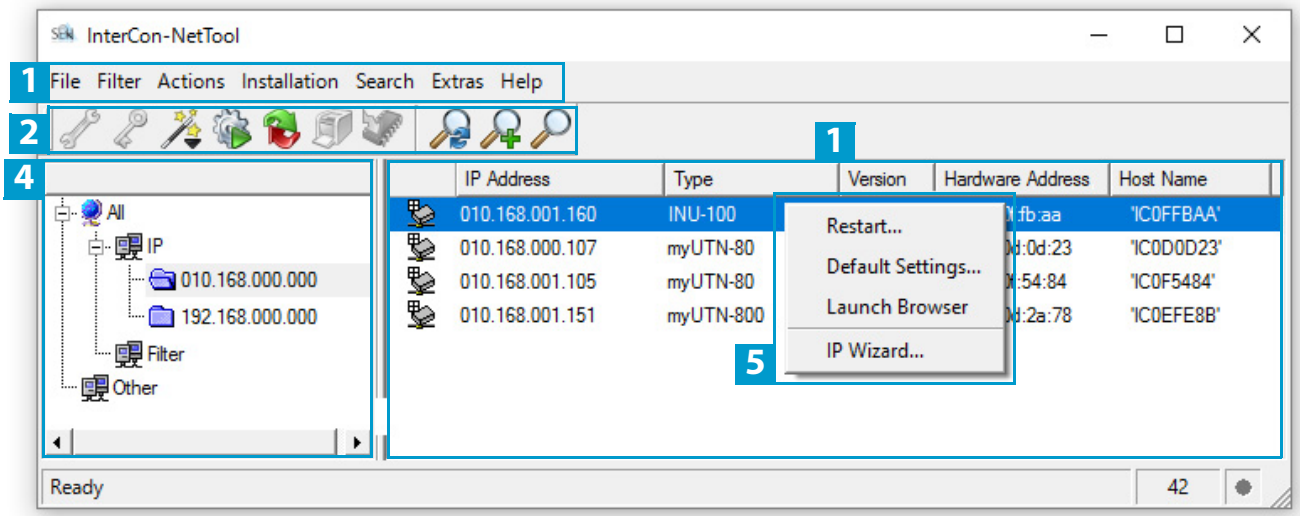


Figure 3: InterCon-NetTool

1	Menu bar	Available menu items
2	Toolbar	Available actions
3	Device list	Shows devices available in the network and device information.
4	Filters for the device list	Filters determine which devices are shown in the device list.
5	Shortcut menu	Available device actions

Detailed information on how to use the InterCon-NetTool can be found in the ⇨ 🕮 'InterCon-NetTool Online Help'. In the menu bar, select **Help**–**Online Help** to start the online help.

Installation

In order to use the InterCon-NetTool, the program must be installed on a computer with Windows operating system. The installation file of the InterCon-NetTool can be found on the SEH Computertechnik GmbH homepage:

http://www.seh-technology.com/services/downloads.html

The installation file is available as '*.exe' for Windows systems.

1. Start the InterCon-NetTool installation file.
2. Select the desired language.
3. Follow the installation routine.

↳ The InterCon-NetTool will be installed on your client.

Program Start

You can identify the InterCon-NetTool by its icon: . Start it with the usual methods of your operating system.

2.4 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 🗎13.

Table 2: 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 ⇨ 🗎65.
	`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 🗎13) because it contains the TAN. You enter the received TAN into the email message body. A space character must follow.

✓ A DNS server is configured on the INU server ⇨ 🗎18.
✓ In order to receive emails, the INU server must be set up as user with its own email address on a POP3 server.
✓ POP3 and SMTP parameters have been configured on the INU server ⇨ 🗎21.

1. Open an email program.
2. Write a new email:
   - As recipient enter the INU server address.
   - Into the subject line enter an instruction. `cmd: <command> [<comment>]`
     Commands and comment: ⇨Table 2 🗎13.
   - 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 Network Settings

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

3.1 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 gets IP address dynamically via the boot protocols BOOTP (Bootstrap Protocol) or 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 ⇨ 🗎17.

The IPv4 address assigned to the INU server can be found via the software tools 'SEH UTN Manager' and 'InterCon-NetTool'. This step usually is carried out during the initial set up (⇨ 🕮 'Quick Installation Guide').

To optimally embed the INU server into a TCP/IP network, you can configure different IPv4 parameters and/or manually assign a static IP address to it.

Configuring IPv4 Parameters via the INU Control Center

1. Start the INU Control Center.
2. Select **NETWORK** – **IPv4**.
3. Configure the IPv4 parameters; ⇨Table 3 🗎16.
4. Click **Save & Restart** to confirm.

↳ The settings will be saved.

Table 3: IPv4 parameters

Parameters	Description
DHCP BOOTP ARP/PING	Enables or disables the protocols DHCP, BOOTP, and ARP/PING. The IP address assignment via DHCP and BOOTP is automatic if one of these protocols is implemented in your network. You can use the commands ARP and PING to change an IP address which was assigned via Zeroconf. The implementation depends on your system; read the documentation of your operating system. *We recommend disabling these options once an IP address has been assigned to the INU server.*
IP address	IP address of the INU server.
Subnet mask	Subnet 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.
Gateway	IP address of the network's standard gateway which the INU server uses. With a gateway, you can address IP addresses from other networks.

Configuring IPv4 Parameters via SEH UTN Manager

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.
✓ The INU server is shown in the selection list ⇨ 🗎30.

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 via SEH UTN Manager and Configuring IPv4 Parameters

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

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.

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 , you can identify a specific device by its default name (⇨ 🗎64) 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.

Determining the IPv4 Address via InterCon-NetTooland/or Configuring IPv4 Parameters

✓ The InterCon-NetTool is installed on the client ⇨ 🗎11.
✓ The network scan via multicast is enabled in the InterCon-NetTool.

1. Start the InterCon-NetTool.
2. In the device list, select the INU server.

If you do not know the IP address, you can identify the INU server in several ways:
- by its type
- if your are using several INU servers of the same model, by its hardware address (which can be found in the type plate at the device bottom)
- if the INU server received its address via Zeroconf, it will appear under the filter 'Zeroconf'

3. In the menu, select **Installation**–**IP Wizard**.
   Der **IP Wizard**is started.
4. Follow the instructions of the wizard.

↳ The settings will be saved.

3.2 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.

WARNING

UTN (⇨ 🗎1) and the corresponding SEH UTN Manager only work in IPv4 networks. The InterCon-NetTool also only works in IPv4 networks.

In IPv6 networks only the INU Control Center (⇨ 🗎5) can be accessed to administrate the INU server.

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 🗎18.
4. Click **Save & Restart** to confirm.

↳ The settings will be saved.

Table 4: 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	Defines an IPv6 unicast address in the format n:n:n:n:n:n:n:n which is manually assigned to the INU server. • 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	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 '/'.

3.3 How to Configure the DNS

DNS is a service to translate domain names into IP addresses and vice versa. Enable DNS so that you can enter host names instead of IP addresses when you define servers.

Example: Time server configuration (⇨ 🗎25) with `ntp.server.de` instead of `10.168.0.140`.

Important:

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

✓ Your network has a DNS server.

1. Start the INU Control Center.
2. Select **NETWORK** – **DNS**.
3. Configure the DNS parameters; ⇨Table 5 🗎18.
4. To confirm, click **Save**.

↳ The settings will be saved.

Table 5: DNS parameters

Parameters	Description
DNS	Enables/disables the name resolution via a DNS server.
Primary DNS server	Defines the IP address of the primary DNS server.
Secondary DNS server	Defines the IP address of the secondary DNS server. The secondary DNS server is used if the first one is not available.
Domain name (suffix)	Defines the domain name of an existing DNS server.

3.4 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 thins, 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** - **Device access** 'How to Protect Access to the INU Control Center (User Accounts)' ⇨ 🗎48.

✓ SNMPv3 users are created in the monitoring station. (Only for SNMPv3.)
✓ The SNMPv3 users from the monitoring station are specified on the INU server ⇨ 🗎48. (Only for SNMPv3.)

1. Start the INU Control Center.
2. Select **NETWORK** – **SNMP**.
3. Configure the SNMP parameters; ⇨Table 6 🗎19.
4. To confirm, click **Save**.

↳ The settings will be saved.

Table 6: 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. **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.
SNMPv3	Enables/disables SNMPv3.
Hash	Defines the hash algorithm.
Access rights	Defines the access rights of the SNMP user.
Encryption	Defines the encryption method.

3.5 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 7 🗎20.
4. To confirm, click **Save**.

↳ The settings will be saved.

Table 7: 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).

3.6 How to Configure Email (POP3 and SMTP)

The INU server can be administered via email (⇨ 🗎13) and offers a notification service (⇨ 🗎27) which sends you status and error messages via email. To use these features, the email protocols 'POP3' and 'SMTP' must be set up on the INU server.

A client, e.g. the INU server, uses POP3 (Post Office Protocol Version 3) to fetch emails from a mail server. POP3 must be set up on the INU server so that it can be administered via email.

SMTP (Simple Mail Transfer Protocol) is used to send and forward emails. The INU server needs SMTP for the administration via email and the notification service.

- Configuring POP3 ⇨ 🗎21
- Configuring SMTP ⇨ 🗎22

Configuring POP3

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

1. Start the INU Control Center.
2. Select **NETWORK** – **Email**.
3. Configure the POP3 parameters; ⇨Table 8 🗎21.
4. To confirm, click **Save**.

↳ The settings will be saved.

Table 8: POP3 parameters

Parameters	Description
POP3	Enables/disables the POP3 functionality.
POP3 – Server name	Defines the POP3 server via its IP address or host name. A host name can only be used if a DNS server 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' ⇨ 🗎21) is 995. If required, read the documentation of your POP3 server.
POP3 – Security	Defines the authentication method to be used: • 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 ⇨ 🗎46.
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 the SMTP server.

1. Start the INU Control Center.
2. Select **NETWORK** – **Email**.
3. Configure the SMTP parameters; ⇨Table 9 🗎22.
4. To confirm, click **Save**.

↳ The settings will be saved.

Table 9: SMTP Parameters

Parameters	Description
SMTP - Server name	Defines the SMTP server via the IP address or the host name. A host name can only be used if a DNS server 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' ⇨ 🗎22), 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 ⇨ 🗎46.
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 SNMP 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' ⇨ 🗎22) and password (parameter 'SMTP – Password' ⇨ 🗎22). 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 the email security standard S/MIME (Secure/Multipurpose Internet Mail Extensions). S/MIME is used to sign ('SMTP – Signing emails' ⇨ 🗎22) or encrypt ('SMTP – Full encryption' ⇨ 🗎22) emails.Enable the desired features (if desired with 'SMTP – Attach public key' ⇨ 🗎22).
SMTP – Signing emails	Enables the signing of emails. The recipient can use the signature to check the sender's identity. This proves, that the email has not been altered. An S/MIME certificate is required for the signing of emails ⇨ 🗎52.
SMTP – Full encryption	Enables the encryption of emails. Only the intended recipient can open and read the encrypted email. An S/MIME certificate is required for the encryption ⇨ 🗎52.
SMTP – Attach public key	Sends the public key together with the email. Many email clients require the key to display the email.

3.7 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.

- Define a IPv4 Management VLAN ⇨ 🗎23
- Define a IPv4 Client VLAN ⇨ 🗎23
- Allocating a IPv4 Client VLAN to a USB Port ⇨ 🗎24

Define a IPv4 Management VLAN

1. Start the INU Control Center.
2. Select **NETWORK** – **IPv4 VLAN**.
3. Configure the IPv4 VLAN parameters; ⇨Table 10 🗎23.
4. To confirm, click **Save**.
5. The settings will be saved.

Table 10: IPv4 management VLAN parameters

Parameters	Description
IPv4 management VLAN	Enables/disables the forwarding of IPv4 management VLAN data. If this option is enabled, SNMP is only available in the IPv4 management VLAN.
VLAN ID	ID for the identification of the IPv4 management VLAN (0–4096).
IP address	IP address of the INU server ⇨ 🗎15.
Subnet mask	Subnet mask of the INU server ⇨ 🗎15.
Gateway	IP address of the network's standard gateway which the INU server uses ⇨ 🗎15. With a gateway, you can address IP addresses from other networks.
Access from any VLAN	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.
Access via LAN (untagged)	Enables/disables the administrative access to the INU server via IPv4 packets without tag. If this option is disabled, the INU server can only be administrated via VLANs.

Define a IPv4 Client VLAN

1. Start the INU Control Center.
2. Select **NETWORK** – **IPv4 VLAN**.
3. Configure the IPv4 VLAN parameters; ⇨Table 11 🗎24.
4. To confirm, click **Save**.

↳ The settings will be saved.

Table 11: IPv4 client VLAN parameters

Parameters	Description
VLAN	Enables/disables the forwarding of IPv4 client VLAN data.
IP address	IP address of the INU server within the IPv4 client VLAN.
Subnet mask	Subnet mask of the INU server within the IPv4 client VLAN.
Gateway	Gateway address of the IPv4 client VLAN.
VLAN ID	ID for the identification of the IPv4 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 IPv4 Client VLAN to a USB Port

1. Start the INU Control Center.
2. Select **SECURITY** – **USB port access**.
3. Allocate a VLAN to the USB port via the **Allocate VLAN** list.
4. To confirm, click **Save**.

↳ The settings will be saved.

4 Device Settings

4.1 How to Configure the Device Time

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.

Today's primary time standard 'UTC' (Universal Time Coordinated) is used. The time zone compensates for location.

Important:

If your network in 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 a manually set time server.

✓ The network has a time server.

1. Start the INU Control Center.
2. Select **DEVICE** – **Date/Time**.
3. Tick **Date/Time**.
4. Into the **Time server** box, enter the IP address or the host name of the time server.
   (The host name can only be used if a DNS server was configured beforehand ⇨ 🗎18.)
5. From the **Time zone** list, select the code for your local time zone.
6. To confirm, click **Save**.

↳ The settings will be saved.

4.2 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 ⇨ 🗎26.

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 12: 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 Control Center, SEH UTN Manager and InterCon-NetTool.
Description	Device description, e.g. location or department. Is displayed in the INU Control Center, SEH UTN Manager and InterCon-NetTool.
Contact person	Contact person, e.g. device administrator. Is displayed in the INU Control Center.

4.3 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 **Device** – **USB port**.
3. Enter the preferred name into the **Port name** field.
4. To confirm, click **Save**.

↳ The settings will be saved.

4.4 How to Disable a USB Port

By default all USB ports are active. You can deactivate (and re-activate) the USB port by interrupting respectively re-establishing 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 **Device** – **USB port**.
3. Tick/clear the option in front of the **USB port**.
4. To confirm, click **Save**.

↳ The USB port is disabled/enabled.

4.5 How to Configure the UTN (SSL) 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 USB connection: UTN port (default = 9200)
- encrypted USB connection (⇨ 🗎45): UTN SSL port (default = 9443)

WARNING

The UTN port respectively UTN SSL port must not be blocked by security measures (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 ⇨ 🗎19.

1. Start the INU Control Center.
2. Select **Device** – **UTN port**.
3. Enter the port number into the **UTN port** or **UTN SSL port** box.
4. To confirm, click **Save**.

↳ The settings will be saved.

4.6 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 notifications via email or SNMP trap:
  - USB device is connected to the INUserver / disconnected from the INU server
  - USB port (i.e. connection to the connected USB device) is activated/deactivated
  - INU server restart

- Configuring the sending of status emails ⇨ 🗎27
- Configuring event notifications via email ⇨ 🗎28
- Configuring event notifications via SNMP traps ⇨ 🗎28

Configuring the sending of status emails

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

✓ SMTP is set up ⇨ 🗎21.
✓ DNS is set up ⇨ 🗎18.

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 notifications via email

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

✓ SMTP is set up ⇨ 🗎21.
✓ DNS is set up ⇨ 🗎18.

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

↳ The settings will be saved.

Configuring event notifications via SNMP traps

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

✓ SNMPv1 or/and SNMPv3 is set up ⇨ 🗎19.

1. Start the INU Control Center.
2. Select **DEVICE** – **Notification**.
3. In the **SNMP traps** area, define the recipients via the IP address and the community.
4. Tick the options with the desired message types.
5. To confirm, click **Save**.

↳ The settings will be saved.

4.7 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 switched manually or, in case of an event, automatically.

If the relay is switched manually, it remains in the chosen position. Usually manual switching is done via the INU Control Center and is described in this chapter. However, it can also be switched via SNMP management tool and SEH private MIB (download at the website ⇨ 🗎3). Switching via SNMP is not described here.

Manual switching is especially suitable for controlling devices through remote access. Example: The INU server is installed in a production environment. The relay is switched as required by an 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).

With automatic relay switching the relay changes position from open to closed if a predefined event occurs. Events which trigger switching:

- INU server restart
- interrupted power supply
- power supply established
- interrupted network connection
- network connection established
- SD card connected
- SD card disconnected
- SC card cannot be used
- 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)

All existing events are displayed in the INU Control Center in the table **Relay status** under **DEVICE** – **Relay**.

After switching has been triggered automatically, the relay must be returned to its default position 'open' manu-

ally before it can switch again.

The automatic control is most suitable for error warnings.
Example: An interrupted network connection is indicated visually through a red lamp or acoustically with an audio alert. As soon as the technician has 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.

Switching the Relay Manually or Setting it to a Fixed Position

1. Start the INU Control Center.
2. Select **DEVICE** – **Relay**.
3. Tick **Fixed position**.
4. From the list **Fixed position**, select **Open** or **Closed**.
5. To confirm, click **Save**.

↳ The relay stays in the selected position.

Relay Position Change Upon Event

1. Start the INU Control Center.
2. Select **DEVICE** – **Relay**.
3. Tick **Change state from open to closed if**.
4. From the list, select the desired events.
5. To confirm, click **Save**.

↳ The settings will be saved.

Set Relay to Default Position

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.

5 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 which are connected to the INU servers.

5.1 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 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

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.

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 ⇨ 🗎7.

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 ⇨ 🗎7.
✓ 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.

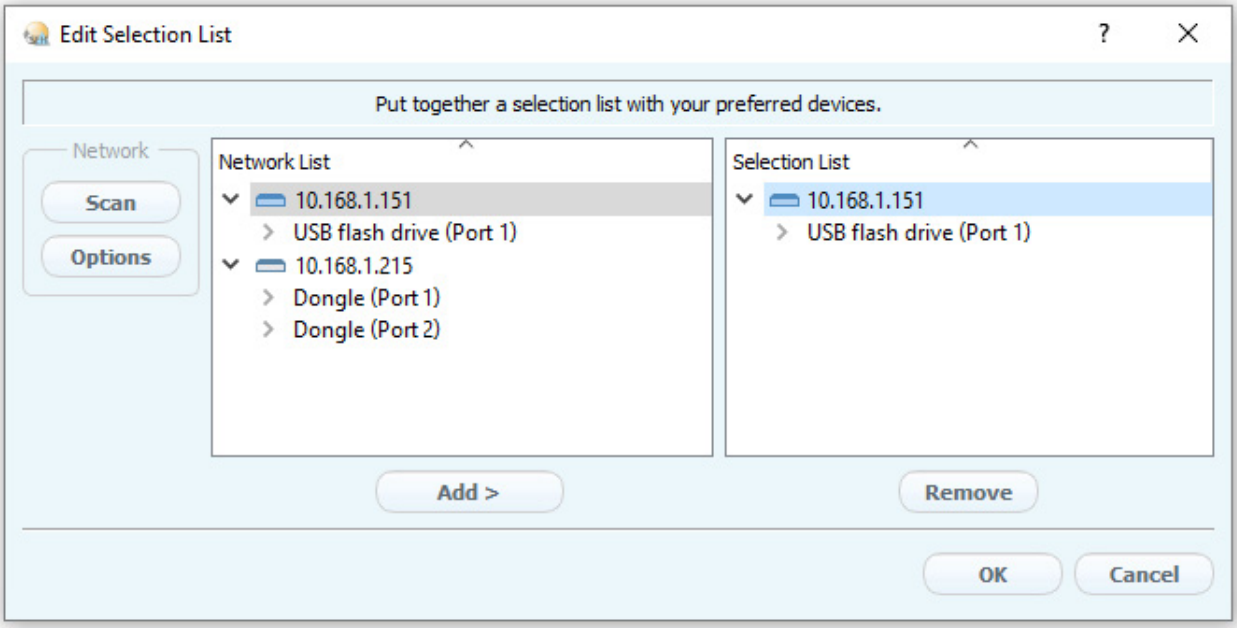


Figure 4: SEH UTN Manager – Edit Selection List

Adding a INU Server via IP Address

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.
✓ 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 UTN SSL port (⇨ 🗎27), define the respective port numbers in the **UTN-Port** and **UTN-SSL-Port** box.
5. Click **OK**.

↳ The INU server and the connected USB devices is shown in the selection list.

5.2 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.

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. The INU server is limited in its number of USB ports: 10. If the limit is reached, no further USB devices can be used on this INU server.

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.
✓ The USB port is shown in the selection list ⇨ 🗎30.
✓ All provisions (driver installation, etc.) necessary to operate the USB device locally (i.e. connected directly to the client) should 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.
2. Select the port from the selection list.
3. From the menu bar, select **Port** – **Activate**.

↳ The connection between the USB device and client is established.

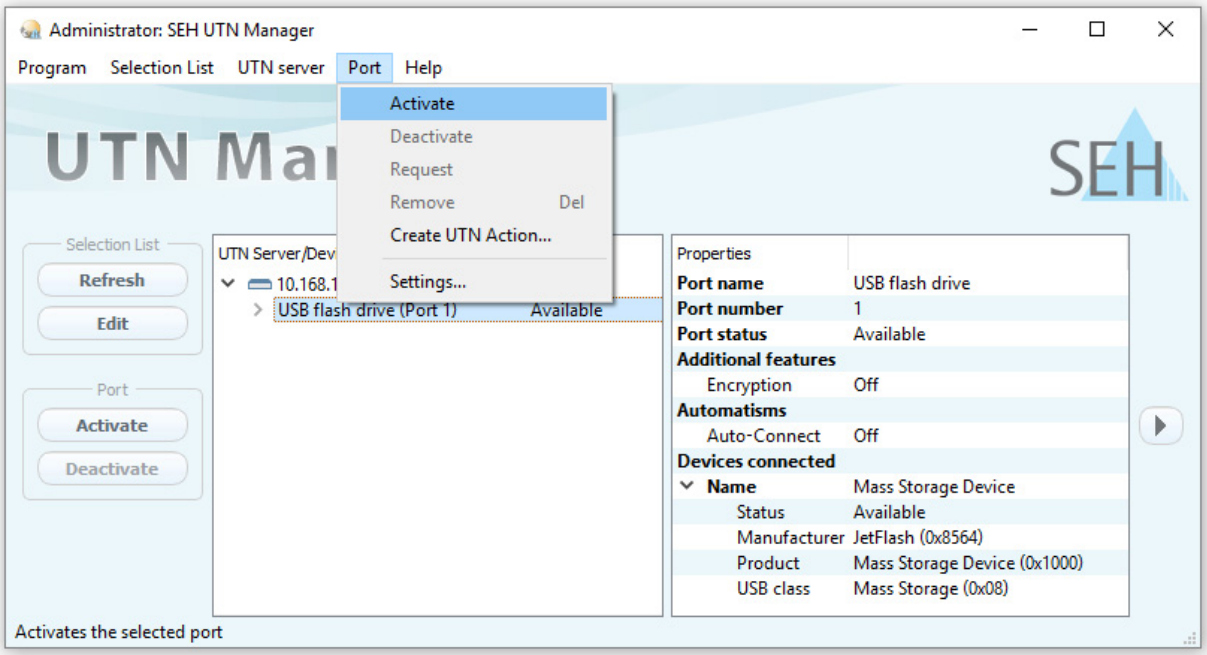


Figure 5: SEH UTN Manager – USB port activation

5.3 How to Cut 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 cut the connection once you do not use the USB device any longer.

To cut the connection between USB device and client, you 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 ⇨ 🗎33.
- In addition, the administrator can deactivate the connection via the INU Control Center ⇨ 🗎33.
- You can also set up an automatic deactivation (Auto Disconnect) ⇨ 🗎34.

Cutting the Device Connection via the SEH UTN Manager

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.
✓ The USB port is shown in the selection list ⇨ 🗎30.
✓ The USB port is connected to your client ⇨ 🗎32.

1. Start the SEH UTN Manager.
2. Select the port from the selection list.
3. Select **Port** – **Deactivate** from the menu bar.

↳ The connection will be deactivated.

Cutting the Device Connection via the INU Control Center

✓ A USB port is connected to your client ⇨ 🗎32.

1. Start the INU Control Center.
2. Select **START**.
3. Choose the active connection from the **Attached devices** list and click the ⊗ icon.
4. Confirm the security query.

↳ The connection will be deactivated.

5.4 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 ⇨ 🗎7.
✓ The SEH UTN Manager (complete version) is installed on the client of the user who uses the USB device ⇨ 🗎7.
✓ The SEH UTN Manager (complete version) is executed on both clients.
✓ The USB port is shown in the selection list ⇨ 🗎30.
✓ The USB port is connected to another client ⇨ 🗎32.

5. Select the port from the selection list.
6. Select **Port** – **Request** from the menu bar.

↳ The release request will be sent.

5.5 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.

- Permanent Connection after Operating System Start (Auto-Connect) ⇨ 🗎34
- Automatic Deactivation of the Connection after a Time Defined (Auto-Disconnect) ⇨ 🗎34
- Automatic Connection between a USB Device and Client When a Print Job Is Received (Print-On-Demand) ⇨ 🗎35
- Creating a UTN Action: Automated Connections and Program Starts without the SEH UTN Manager Interface ⇨ 🗎35

This chapter describes features of the SEH UTN Manager with which automatisms are set up. Users who have expert knowledge in scripting should use the command line tool 'utnm' ⇨ 🗎40.

Permanent Connection after Operating System Start (Auto-Connect)

Auto-Connect automatically establishes a permanent connection to a USB port and the connected USB device without the need for a user to log on to the client. The connection will be

- activated when the operating system is started,
- deactivated when the operating system is shut down,
- automatically re-established when the system restarts.

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.
✓ The USB port is shown in the selection list ⇨ 🗎30.
✓ You are logged on to the client as administrator.

1. Start the SEH UTN Manager.
2. Select the port from the selection list.
3. From the menu bar, select **Port** – **Settings**.
   The **Port Settings** dialog appears.
4. Tick **Activates the device automatically after the SEH UTN Manager program start. (Auto-Connect)**.
5. Click **OK**.

↳ The setting will be saved.

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.

You can be notified if a connection is automatically disconnected and the port thus is free. For this purpose, set up a notification if the USB port is available ⇨ 🗎37.

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.
✓ The INU server is displayed in the 'Automatic Device Disconnect' area ⇨ 🗎30.
✓ You are logged on to the client as administrator.

1. Start the SEH UTN Manager.

2. In the menu bar, select **Program**–**Options**.
   The **Options** dialog appears.
3. Select the **Automatisms** tab.
4. In the **Auto-Disconnect** area, tick **Status** for the relevant INU server.
5. Define the desired time range (10–525 minutes).
6. Is desired, tick **Prolongation**.
7. Click **OK**.

↳ The setting will be saved.

Automatic Connection between a USB Device and Client When a Print Job Is Received (Print-On-Demand)

Print-On-Demand automatically establishes a connection between the client and the USB port to which the USB device (printer or multifunction device) is connected when a print job is received.

After completion of the print job, the connection will be automatically disabled.

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.
✓ The USB port is shown in the selection list ⇨ 🗎30.
✓ The USB port is not connected to another client.
✓ You are logged on to the client as administrator.

1. Start the SEH UTN Manager.
2. Select the port from the selection list.
3. From the menu bar, select **Port** – **Activate**.
   The connection will be established. The device is installed. A printer object is created on the client.
4. From the menu bar, select **Port** – **Settings**.
   The **Port Settings** dialog appears.
5. In the **Automatic device connection** area, tick **Print-On-Demand**.
6. Click **OK**.
   The setting will be saved.
7. Select **Port** – **Deactivate** from the menu bar.
   The connection will be deactivated.

↳ Print-On-Demand is set up.

Creating a UTN Action: Automated Connections and Program Starts without the SEH UTN Manager Interface

UTN Actions are small files which contain a script that automates the connections to USB ports including connected USB devices. The process defined in the script runs automatically when the file is executed. Since the 'SEH UTN Service' is active in the background, the user does not have to start the SEH UTN Manager interface. I.e., UTN Actions can be used with the complete (⇨ 🗎8) and minimal version (⇨ 🗎8).

UTN Actions are for realizing simple scenarios, such as activating a connection, as well as complex procedures, such as activating a connection and starting an application with time delay. You can create the UTN action with a wizard. The wizard is only available in the complete version (⇨ 🗎8) of the SEH UTN Manager. You can create the following UTN Actions:

- UTN Actions which activate and deactivate the device
  The wizard will automatically create one UTN Action for the activation and one UTN Action for the deactivation of the USB port and the connected USB device. Both UTN Actions will be saved to the desktop.
- UTN Action which starts an application and activates the device
  After the selection of an application by the user, the wizard will automatically create a UTN Action which starts an application and activates the USB port and the connected USB device. Additionally, you can define a port deactivation after the closing of the application.
- Custom UTN Action (Experts only)
  With the help of the wizard, a custom UTN Action can be created. You can create:

- UTN Actions for the activation and deactivation of the USB port and the connected USB device. You can define additional options.
- A script for starting the application and activating the USB port and the connected USB device. Additionally, you can define a delay for the start of the application, the deactivation of the USB port after the closing of the application and additional options. Finally, the complete UTN Action will be created automatically by the SEH UTN Manager and saved by the user.

UTN Actions are based on the command line tool 'utnm'. We recommend experts to use this tool, if they want to create very complex scripts without restraints ⇨ 🗎40.

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.
✓ The USB port is shown in the selection list ⇨ 🗎30.

1. Start the SEH UTN Manager.
2. Select a port from the selection list.
3. From the menu bar, select **Port** – **Create UTN Action**.
   The dialog **Create UTN Action** appears.
4. Follow the instructions of the wizard.

↳ A UTN Action will be created. The UTN Action is run by double-clicking the file.

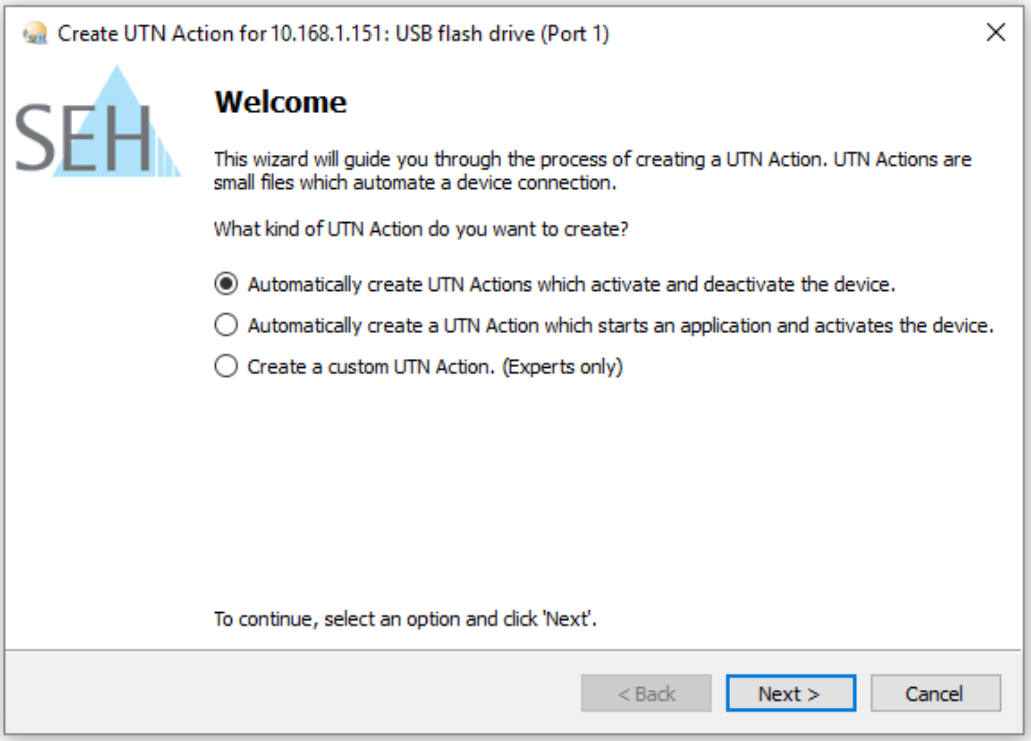


Figure 6: Create UTN Action dialog

Shortcuts can be moved to any place and renamed after they have been saved.

(Experts only) Custom UTN Actions which activate or deactivate USB devices can be edited after their creation. To do this, edit the command line in the shortcut target.

Expert mode (script): You can also edit the script after its creation using a simple text editor.

5.6 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 will be notified when a USB port and the connected USB device become available after they have been occupied.

- Displaying Status Information ⇨ 🗎37
- Configuring Messages ⇨ 🗎37

Displaying Status Information

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.
✓ The USB port is shown in the selection list ⇨ 🗎30.

1. Start the SEH UTN Manager.
2. Select the USB port from the selection list.

↳ The status information is displayed in the **Properties** area.

Configuring Messages

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ 🗎7.
✓ The USB port is shown in the selection list ⇨ 🗎30.

1. Start the SEH UTN Manager.
2. Select the port from the selection list.
3. From the menu bar, select **Port** – **Settings**.
   The **Port Settings** dialog appears.
4. Tick the option under **Messages**.
5. Click **OK**.

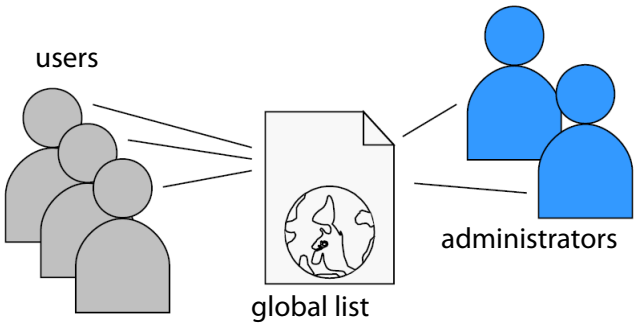
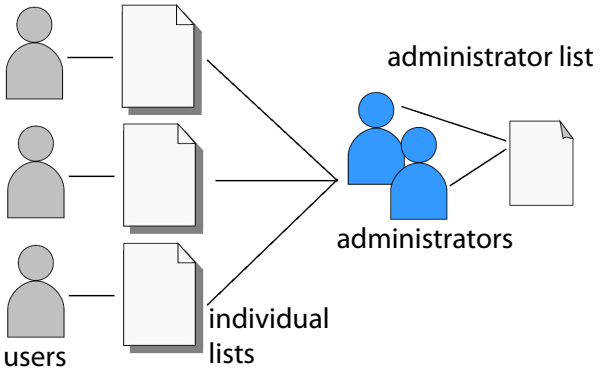
↳ The setting will be saved.
As soon as a network participant disables the connection to the USB port and the connected USB device, a ?desktop alert?will be generated.

5.7 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 (⇨ 🗎30). 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 13: Differences in global and user selection list

Global Selection List	User Selection List
	
• All users of a client use the same selection list.	• 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.)	• 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: Registry	• List ('ini'-file) is stored at:
	`%APPDATA%\SEH Computertechnik GmbH\SEH UTN Manager.ini`
	(`%APPDATA%` is an environment variable for a Windows user; the path for the current user can be determined with using command line: echo `%APPDATA%`
	Example Windows 10:
	`echo %APPDATA% yields C:\Users\Benutzername\AppData\Roaming + \SEH Computertechnik GmbH\SEH UTN Manager.ini`
	Complete path to the ini file:
	`C:\Users\User name\AppData\Roaming\SEH Computertechnik GmbH\SEH UTN Manager.ini`)

• The selection list can be edited by administrators.	• 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 'SEH UTN Manager – Feature Overview' ⇨ 🗎85.

- Setting Up the Global Selection List for All Users ⇨ 🗎39
- Providing User Selection Lists ⇨ 🗎39
- Restrict Write Access to the 'SEH UTN Manager.ini'-file ⇨ 🗎39

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 ⇨ 🗎7.
✓ You are logged on to the system as administrator.

1. Start the SEH UTN Manager.
   Compose the selection list ⇨ 🗎30.
2. In the menu bar, select **Program**–**Options**.
   The **Options** dialog appears.
3. Select the tab **Selection List**.
4. Tick **Global selection list**.
5. 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 ⇨ 🗎7.
✓ 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 ⇨ 🗎30.
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:
   %APPDATA%\SEH Computertechnik GmbH\SEH UTN Manager.ini
   (⇨Table 13 🗎38)

↳ 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 (⇨ 🗎39) 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.

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

The SEH UTN Manager is available in two versions ⇨ 🗎7. 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 command line 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

```
"<path utnm.exe>" /c "command string" [/<command>]
```

The file 'utnm.exe' can be found in the program folder of the SEH UTN Manager.

Commands

Rules for commands:

- Underlined elements are to be replaced by the appropriate values (e.g. `INU 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

`/c "command string"`
 	
or
 	
`/command "command string"`
	Runs a command. The command is specified in greater detail by the command string.
	• `Activate INU server port number`
	Activates the connection to a USB port and the connected USB device.
	• `Deactivate INU server port number`
	Deactivates the connection to a USB port and the connected USB device. If a USB mass storage device is connected to the USB port, the command string `eject` will be used. For all other USB devices the command string `plugout` will be used.
	• `Plugin INU server port number`
	Activates the connection to a USB port and the connected USB device.
	• `Plugout INU server port number`
	Deactivates the connection to a USB port and the connected USB device. (Corresponds to "unplugging" the device.)
	Better use the command string `deactivate`.
	• `eject INU server port number`
	(for USB mass storage devices) Ejects the USB device connected to the USB port. The port connection will only be deactivated if the communication has been terminated properly.
	Better use the command string `deactivate`.
	• `set autoconnect = true|false INU server port number`
	Automatically activates the port connection if the USB device is connected to the USB port but not in use.
	• `find`
	Searches for all INU servers in the network segment and shows the INU servers found with IP address, MAC address, model and software version.
	• `Getlist INU server`
	Shows an overview of the USB devices connected to the INU server (including port number, vendor ID, product ID, manufacturer name, product name, device class, and status).
	• `State INU server port number`
	Displays the status of the USB device connected to the USB port.

`/h`
or
`/help`
	Shows the help page.

`/k USB port key`
or
`/key USB port key`
	Specifies a USB port key ⇨ 📄50.
	Important:
	The command only enters the key to make the USB device available.
	The key itself is set up in the INU Control Center.

Command	Description
/mr or /machine readable	Separates the output of the command string getlist with tabulators and the output of find with commas.
/nw or /no-warnings	Suppresses warning messages.
/o or /output	Shows the output in the command line.
/p port number or /port port number	Uses an alternative UTN port. Use this command if you have changed the UTN port number (⇨ 27).
/q or /quiet	Suppresses the output.
/sp port number or /ssl-port port number	Uses an alternative UTN port with SSL/TLS encryption. Use this command if you have changed the UTN SSL port number (⇨ 27).
/t seconds or /timeout seconds	Specifies a timeout for the command strings activate, deactivate, plugin, plugout, and eject.
/v or /version	Shows version information about utnm.

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' ⇨ 42), 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 USB port including the connected USB device is free for use.
20	The USB device connected to the USB port could not be plugged in.
21	The USB device connected to the USB port could not be plugged out.
22	The USB device connected to the USB port could not be ejected.
23	The USB device connected to the USB port is already plugged in.
24	The USB device connected to the USB port is already plugged out.
25	The USB port including the connected USB device is connected to another user.
26	The USB port including the connected USB device is unreachable.
27	The USB device state is unknown.
100	Unknown command.
101	INU server not found. Either the INU server does not exist or the DNS resolution failed.
103	The port key is too long.

Using utmn via Command Line

✓ The SEH UTN Manager is installed on the client ⇨ 🗎7.
✓ You know the INU server's IP address or host name.

1. Open the command-line interface.
2. Enter the sequence of commands; see 'Syntax' ⇨ 🗎40 and 'Commands' ⇨ 🗎40.
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

```
"C:\Program Files\SEH Computertechnik GmbH\SEH UTN Manager\utnm.exe" /
c "activate 10.168.1.167 3"
```

Creating a utnm Script

✓ The SEH UTN Manager is installed on the client ⇨ 🗎7.
✓ You know the INU server's IP address or host name.
✓ 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' ⇨ 🗎40, 'Commands' ⇨ 🗎40, and 'Return' ⇨ 🗎42.
3. Save the file as executable script on your client.

↳ The script is saved and can be used.

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.

Important:

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

You can also use SNMP and VLAN for security:

- *'How to Configure SNMP'* ⇨ 🗎*19*
- *'How to Use the INU Server in VLAN Environments'* ⇨ 🗎*23*

6.1 How to Encrypt the USB Connection

To secure the USB connections, you encrypt the data transfer between the clients and the USB devices connected to the INU server. The encryption has to be activated individually for each connection, i.e. for each USB port.

For encryption the protocols SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) are used. The encryption strength is defined via the encryption protocol and level ⇨ 🗎46.

Important:

Only payload will be encrypted. Control and log data will be transmitted without encryption.

If connections are encrypted, client and INU server communicate via the UTN SSL port. By default, that is port 9443. If the port is already used in your network, e.g. for another application, you can change the port number ⇨ 🗎27.

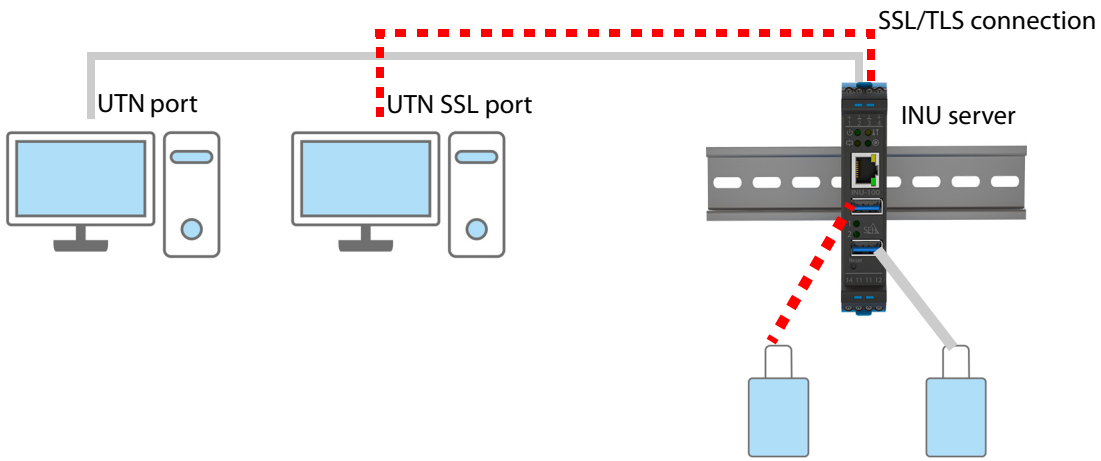


Figure 7: INU Server – SSL/TLS connection in the network

1. Start the INU Control Center.
2. Select **SECURITY** – **Encryption**.
3. Enable the encryption for the USB port.
4. To confirm, click **Save**.

↳ The data transfer between the clients and the USB device will be encrypted.

*The encrypted connection will be displayed client-side in the SEH UTN Manager under **Properties**.*

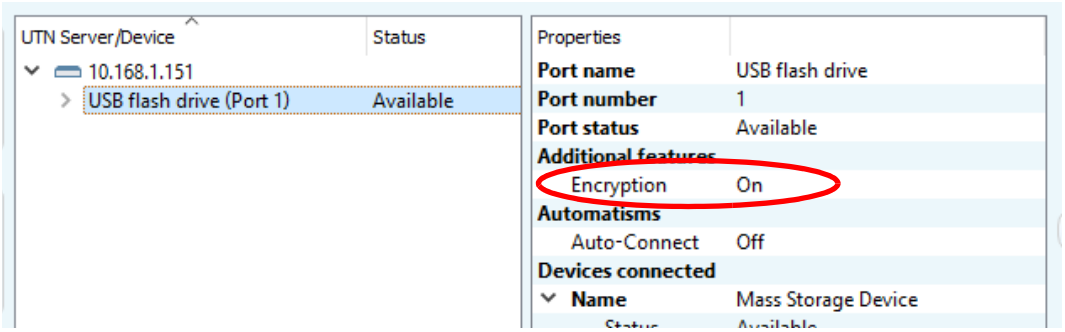


Figure 8:SEH UTN Manager – encryption

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 protocol SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security).

- HTTP: unencrypted connection
- HTTPS: encrypted connection
  The encryption strength is defined via the encryption protocol and level ⇨ 🗎46. When an encrypted connection is to be established, the client asks for a certificate via a browser (⇨ 🗎52). 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** – **Device access**.
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 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):

- Email: POP3 (⇨ 🗎21)
- Email: SMTP (⇨ 🗎21)
- Web access to the INU Control Center: HTTPS (⇨ 🗎46)
- Data transfer between the clients and the INU server (and the connected USB devices): USB connection (⇨ 🗎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 an 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 ⇨ 🗎61.

*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 connections**.
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** for accessing the INU Control Center (⇨ 🗎46), 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** for accessing the INU Control Center (⇨ 🗎46), 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 on the individual SSL/TLS connections (e.g. supported cipher suites) can be found on the details page **SSL connection status** – **Details**.*

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

By default, everyone who can find the INU in the network can access its 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.
- Read-only user: Very restricted access to the INU Control Center. The user can only see the 'START' 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:

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

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 ⇨ 🗎19. 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** – **Device access**.
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. Choose the login screen type: **list of users** or **name and password**.
6. Tick **Session timeout** and into the **Session duration box** enter the time in Minutes after which the timeout is to be effective.
7. To confirm, click **Save**.

↳ The settings will be saved.

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

You can restrict access to the INU server by blocking ports with the 'TCP port access control'. If a port is blocked, the protocols respectively 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. Tick **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 use of wildcards (*) allows you to define subnetworks.

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 the INU Control Center can be reached.

Important:

If the INU Control Center cannot be reached, restart the INU server ⇨ 59.

9. Deactivate the **Test mode**.
10. Click **Save & Restart** to confirm.

↳ The settings will be saved.

6.6 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 A key is defined for the USB port. Neither the USB port nor the connected USB device are shown in the SEH UTN Manager, i.e. the USB device cannot be used. Only if the key for the USB port is entered in the SEH UTN Manager, the USB port and the connected USB device appear.
- 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 ⇨ 🗎26.

- Setting Up USB Port Keys ⇨ 🗎50
- Entering a USB Port Key (Unlocking a USB Device) ⇨ 🗎50
- Setting up USB Port Device Assignment ⇨ 🗎50

Setting Up USB Port Keys

A key for a USB port is defined in the INU Control Center.

1. Start the INU Control Center.
2. Select **SECURITY** – **USB port access**.
3. For the desired USB port, go to the **Method** list and select **Port key control**.
4. Click **Generate key** or enter a freely definable key (max. 64 ASCII characters) into the **Key** box.
5. 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)

To gain access to a USB device that is protected with the USB port key control, the corresponding key must be entered in the SEH UTN Manager on the client.

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

↳ Access is granted. The USB port and the connected USB device are shown in the selection list and can be used.

Setting up USB Port Device Assignment

1. Start the INU Control Center.
2. Select **SECURITY** – **USB port access**.
3. For the desired USB port, go to the **Method** list and select **Device assignment**.
4. Click **Reallocate device**.
   The **USB device** box shows the VID and PID of the USB device.

5. 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 **---**.*

6.7 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** – **Device access**.
3. Tick/clear **Disable input devices (HID class)** in the **USB devices** area.
4. To confirm, click **Save**.

↳ The setting will be saved.

6.8 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 ⇨ 🗎56
- protecting email communication (POP3/SMTP via SSL/TLS) ⇨ 🗎21
- protecting the connection between the clients and the connected USB devices ⇨ 🗎45
- protecting the connection to the INU Control Center (with HTTPS) ⇨ 🗎46

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 (Microsoft Outlook 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 ⇨ 🗎53
- Creating a Self-Signed Certificate ⇨ 🗎53
- Request and Install Certificate (Requested Certificate) ⇨ 🗎54
- Installing a PKCS#12 Certificate ⇨ 🗎54
- Installing an S/MIME Certificate ⇨ 🗎55
- Installing a CA Certificate ⇨ 🗎55
- Deleting Certificates ⇨ 🗎55

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.

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 ⇨ 🖹55.

1. Start the INU Control Center.
2. Select **SECURITY** – **Certificates**.
3. Click **Self-signed certificate**.
4. Enter the relevant parameters; ⇨Table 14 🖹53.
5. Click **Create/Install**.

↳ The certificate will be created and installed. This may take a few minutes.

Table 14: Parameters for the Creation of Certificates

Parameters	Description
Common name	Freely definable certificate name. (max. 64 characters) *Use the IP address or host name of the INU server, so that you can clearly match device and certificate.*
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)
Domain component	Allows you to enter additional attributes. (Optional entry)
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.

Parameters	Description
RSA key length	Defines the length of the RSA key used: - 512 bit (fast encryption and decryption) - 768 bit - 1024 bit (standard encryption and decryption) - 2048 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 ⇨ 🗎55.

1. Start the INU Control Center.
2. Select **SECURITY** – **Certificates**.
3. Click **Certificate request**.
4. Enter the required parameters; ⇨Table 14 🗎53.
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 ⇨ 🗎55.

✓ 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

Important:

If an S/MIME certificate has already been installed in the INU server, you must first delete the certificate ⇨ 🗎55.

✓ 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 ⇨ 🗎46) 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 ⇨ 🗎59. 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. Select the certificate to be deleted via the icon  .
   The certificate is displayed.
4. Click **Delete**.

↳ The certificate is deleted.

6.9 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 ⇨ 🗎56
- Configuring EAP-TLS ⇨ 🗎56
- Configuring EAP-TTLS ⇨ 🗎57
- Configuring PEAP ⇨ 🗎57
- Configuring EAP-FAST ⇨ 🗎57

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 ⇨ 🗎61.

1. Create a certificate request on the INU server ⇨ 🗎54.
2. Create a certificate using the certificate request and the authentication server.
3. Install the requested certificate on the INU server ⇨ 🗎54.
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 ⇨ 🗎55.
5. Start the INU Control Center.
6. Select **SECURITY** – **Authentication**.
7. Select **TLS** from the **Authentication method** list.
8. From the list **EAP root certificate**, 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 ⇨ 🗎55.

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 (⇨ 🗎57), 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 ⇨ 🗎55.

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 (⇨ 🗎57) and PEAP (⇨ 🗎57) 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.

7 Maintenance

You can maintain the INU server in the following ways:

- How to Restart the INU Server ⇨ 🗎59
- How to Update ⇨ 🗎59
- How to Backup Your Configuration ⇨ 🗎60
- How to Reset Parameters to their Default Values ⇨ 🗎61

7.1 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 via the INU Control Center ⇨ 🗎59
- Restarting the INU-Server via InterCon-NetTool ⇨ 🗎59

Restarting the INU Server via the INU Control Center

1. Start the INU Control Center.
2. Select **MAINTENANCE** – **Restart**.
3. Click **Restart**.

↳ The INU server restarts.

Restarting the INU-Server via InterCon-NetTool

1. Start the InterCon-NetTool.
2. In the device list, select the INU server.
3. From the menu bar, select **Actions** – **Restart**.
4. Click **Finish**.

↳ The INU server restarts.

7.2 How to Update

You can update your INU server with a soft- and firmware update. New firmware/software contains new features and/or error fixes.

You can find the version number of the firmware/software installed on the INU server on the start page of the INU Control Center or in the device list in the InterCon-NetTool.

For current firmware/software files go to the SEH Computertechnik GmbH website:

https://www.seh-technology.com/services/downloads.html

Only the existing firmware/software is updated; settings will be preserved.

Important:

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

1. Start the INU Control Center.
2. Select **MAINTENANCE** – **Update**.
3. Specify the update file in the **Update file** box.
4. Click **Install**.

↳ The update is executed. Afterwards, the INU server restarts.

7.3 How to Backup Your Configuration

All settings of the INU server (exception: passwords) are saved in the file '<Default-Name>_parameters.txt'.

You can save this parameters file as backup copy to your local client. This way you can return to a stable configuration status at any time.

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.

You can find a detailed description of the parameters in the Parameter Lists ⇨ 🗎65.

The INU-Server also has an automatic backup feature. It saves the parameter values, passwords and certificates installed on the INU server automatically to a connected SD card. After a parameter or certificate change, the backup will be updated automatically. To transfer the settings to another INU server, you simply insert the SD card into the other device. After a cold boot (interruption and re-establishment of the power supply), the settings will be loaded automatically.

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 INUserver if you use the automatic backup.

See Parameter Values

1. Start the INU Control Center.
2. Select **MAINTENANCE** – **Parameter backup**.
3. Click the icon .

↳ The current parameter values are displayed.

Saving the Parameter File

1. Start the INU Control Center.
2. Select **MAINTENANCE** – **Parameter backup**.
3. Click the icon .
4. Save the '<default name>_parameters.txt' file to a local system using your browser.

↳ The parameters file is backed up.

Loading the Parameters File onto a INU Server

1. Start the INU Control Center.
2. Select **MAINTENANCE** – **Parameter backup**.

3. In the **Parameter file** box, specify the '<default name>_parameters.txt' file.
4. Click **Import**.

↳ The INU server adopts the parameter values from the file.

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** – **SD card**.
3. Tick **Parameter backup**.
4. Click **Save**.

↳ The settings will be saved.

7.4 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 my be interrupted if the IP address of the INU server changes with the reset.

If required, determine the new IP address ⇨ 🗎15.

You can change the settings either via remote access (INU Control Center and InterCon-NetTool) or via the reset button on the INU server.

If you lost the password for the INU Control Center, you can reset the INU server via 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 ⇨ 🗎60).

- Resetting Parameters via INU Control Center ⇨ 🗎61
- Resetting Parameters via InterCon-NetTool ⇨ 🗎62
- Resetting Parameters via Reset Button ⇨ 🗎62

Resetting Parameters via INU Control Center

1. Start the INU Control Center.
2. Select **MAINTENANCE** – **Default settings**.
3. Click **Default settings**.
   A security query appears.
4. Confirm the security query.

↳ The parameters are reset.

Resetting Parameters via InterCon-NetTool

1. Start the InterCon-NetTool.
2. In the device list, select the INU server.
3. From the menu bar, select **Actions** – **Default Settings**.
4. Click **Finish**.

↳ 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.

8 Appendix

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

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.

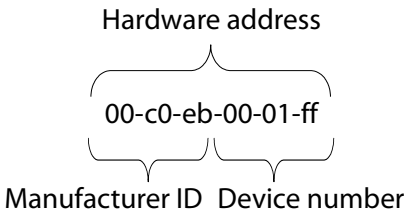
The default name of the INU server is made up of the two letters 'IC' and the device number. The device number consists of the last six numbers of the hardware address.

You can see the default name in the INU Control Center or InterCon-NetTool.

Hardware address

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

The manufacturer has defines the 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. In Windows '-' are used.



You can see the hardware address on the housing, in the SEH UTN Manager or in the InterCon-NetTool.

INU Control Center

The INU Control Center is the user interface of the INU server. The INU server can be configured and monitored via the INU Control Center.

You access the INU Control Center with an Internet browser (e.g. Microsoft Edge).

More information ⇨ 🗎5.

InterCon-NetTool

The InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices. Depending on the network device, different actions can be performed.

More information ⇨ 🗎11.

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 ⇨ 🗎7.

8.2 Parameter Lists

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

- Administration via email ⇨ 🗎13
- Configuration backup (viewing, editing and loading parameters onto other devices) ⇨ 🗎60

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

Table 15: 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_mask [Subnet mask]	valid IP address	255.255.0.0	Subnet 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_gate [Gateway]	valid IP address	0.0.0.0	IP address of the network's standard gateway which the INU server uses. With a gateway, 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, IP address assignment is automatic.
ip_bootp [BOOTP]	on/off	on	Enables/disables the BOOTP protocol. If BOOTP is enabled in your network, IP address assignment 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 which was assigned via Zeroconf. The implementation depends on your system; read the documentation of your operating system.

*We recommend that you deactivate **DHCP**, **BOOTP** and **ARP/PING** as soon as the INU server has received its IP address.*

Table 16: 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:n:n	: :	Defines an IPv6 unicast address in the format n:n:n:n:n:n:n:n which is manually assigned to the INU server. • 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.
ipv6_gate [Router]	n:n:n:n:n:n:n:n	: :	Manually defines a static router to which the INU server sends its requests.
ipv6_plen [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 17: 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.

Table 18: 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. **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.
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 INU server user accounts are also used as SNMP user accounts ⇨ 19. Consider this when setting up user accounts.

Table 19: 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@ICxxxxxx).

Table 20: Parameter list – POP3

Parameters	Value	Default	Description
pop3 [POP3]	on/off	off	Enables/disables the POP3 functionality.
pop3_srv [Server name]	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 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_sec' ⇨ 🗎69) 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: • 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 ⇨ 🗎46. 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 21: Parameter list – POP3

Parameters	Value	Default	Description
smtp_srv [Server name]	max. 128 characters	[blank]	Defines the SMTP server via the IP address or the host name. A host name can only be used if a DNS server was configured beforehand.
smtp_port [Server port]	1–65535 [1–5 characters; 0–9]	25	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' ⇨ 🗎70), 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 [SSL/TLS]	on/off	off	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 ⇨ 🗎46.
smtp_sender [Sender name]	max. 128 characters	[blank]	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_auth [Login]	on/off	off	Enables/disables SNMP authentication (SMTP AUTH). To send emails, the INU sends its user name and password to the SMTP server to authenticate itself. Enter user name (parameter 'smtp_usr' ⇨ 🗎70) and password (parameter 'smtp_pwd' ⇨ 🗎70). Some SMTP servers require SMTP authentication to prevent fraudulent use (spam).
smtp_usr [User name]	max. 128 characters	[blank]	Defines the user name used by the INU server to log on to the SMTP server.
smtp_pwd [Password]	max. 128 characters	[blank]	Defines the password used by the INU server to log on to the SMTP server.
smtp_sign [Security (S/MIME)]	on/off	off	Enables/disables the email security standard S/MIME (Secure/Multipurpose Internet Mail Extensions). S/MIME is used to sign (parameter 'smtp_sign' ⇨ 🗎70) or encrypt (parameter 'smtp_encrypt' ⇨ 🗎71) emails. Enable the desired feature (if desired with 'smtp_attpkey' ⇨ 🗎70).
smtp_attpkey [Attach public key]	on/off	on	Sends the public key together with the email. Many email clients require the key to display the email.

Parameters	Value	Default	Description
smtp_encrypt [Full encryption] [Signing emails]	on/off	off	on = Activates the encryption of emails. Only the intended recipient can open and read the encrypted email. An S/MIME certificate is required for the encryption ⇨ 52. off = Activates the signing of emails. The recipient can use the signature to check the sender's identity. This proves, that the email has not been altered. An S/MIME certificate is required for the signing of emails ⇨ 52.

Table 22: Parameter list – IPv4-VLAN

Parameters	Value	Default	Description
ip4vlan_mgmt [IPv4 management VLAN]	on/off	off	Enables/disables the forwarding of IPv4 management VLAN data. If this option is enabled, SNMP is only available in the IPv4 management VLAN.
ip4vlan_mgmt_id [VLAN-ID]	0–4096 [1–4 characters; 0–9]	0	ID for the identification of the IPv4 management VLAN.
ip4vlan_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.
ip4vlan_mgmt_untag [Access via LAN (untagged)]	on/off	on	Enables/disables the administrative access to the INU server via IPv4 packets without tag. If this option is disabled, the INU server can only be administrated via VLANs.
ipv4vlan_on_1 ~ ipv4vlan_on_20 [VLAN]	on/off	off	Enables/disables the forwarding of IPv4 client VLAN data.
ipv4vlan_addr_1 ~ ipv4vlan_addr_20 [IP address]	valid IP address	192.168.0.0	IP address of the INU server within the IPv4 client VLAN.
ipv4vlan_mask_1 ~ ipv4vlan_mask_20 [Subnet mask]	valid IP address	255.255.255.0	Subnet mask of the INU server within the IPv4 client VLAN.
ip4vlan_gate_1 ~ ip4vlan_gate_20 [Gateway]	valid IP address	0.0.0.0	IP gateway address in the IPv4 management VLAN. With a gateway, you can address IP addresses from other networks.
ipv4vlan_id_1 ~ ipv4vlan_id_20 [VLAN-ID]	0–4096 [1–4 characters; 0–9]	0	ID for the identification of the IPv4 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 = every 1 = VLAN 1 2 = VLAN 2 etc. 9 = none

Table 23: 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 via the IP address or the host name. The host name can only be used if a DNS server was configured beforehand. **Important:** If your network in 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.
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 (daylight saving time etc.).

Table 24: 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. Is displayed in the INU Control Center, SEH UTN Manager and InterCon-NetTool.
sys_descr [Description]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Device description, e.g. location or department. Is displayed in the INU Control Center, SEH UTN Manager and InterCon-NetTool.
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 25: Parameter list – USB port

Parameters	Value	Default	Description
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_poff_1 ~ utn_poff_20 [Port]	on/off	off	Disables/enables the power supply for the USB port (i.e. the USB device connected to the port). off = power on on = power off

Table 26: 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).
utn_sslport [UTN SSL port]	1–9443 [1–4 characters; 0–9]	9443	Defines the number of the UTN SSL port (for encrypted connections). **WARNING** The UTN SSL port must not be blocked by security software (firewall).

Table 27: 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.
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	Defines the day (the interval) on which a status email is sent. al = daily su= Sunday mo= Monday tu= Tuesday we= Wednesday th= Thursday fr = Friday sa= Saturday
notistat_h [hh]	0–23 [1–2 characters; 0–9]	0	Specifies the time (hour) at which a status email is sent. 1 = 1. hour 2 = 2. hour 3 = 3. hour etc.
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
noti_dev_1 noti_dev_2 [Send email if USB devices are connected or disconnected]	on/off	off	Enables/disables the sending of emails after a USB device was connected to/removed from the INU server.
noti_act_1 noti_act_2 [Send email if USB port is activated or deactivated]	on/off	off	Enables/disables the sending of emails after a USB port (i.e. the connection to the connected USB device) was activated/deactivated.

Parameters	Value	Default	Description
noti_pup_1 noti_pup_2 [Send email if INU server is restarted]	on/off	off	Enables/disables the sending of emails when the INU server restarts.
noti_pwr_1 noti_pwr_2 [Send email if power supply is interrupted or established]	on/off	off	Enables/disables the sending of emails when one of the two power supplies of the INU server is interrupted or established.
noti_lnk_1 noti_lnk_2 [Send email if network connection is interrupted or established]	on/off	off	Enables/disables the sending of emails when one of the two network connection of the INU server is interrupted or established.
noti_sdinout_1 noti_sdinout_2 [Send email if SD card is connected or disconnected]	on/off	off	Enables/disables the sending of emails after an SD card was connected to/removed from the INU server.
noti_sdunusable_1 noti_sdunusable_2 [Send email if SD card cannot be used]	on/off	off	Enables/disables the sending of emails if the SD card is unusable.
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.
trapdev [Send trap if USB devices are connected or disconnected]	on/off	off	Enables/disables the sending of SNMP traps after a USB device was connected to/removed from the INU server.
trapact [Send trap if USB ports are activated or deactivated]	on/off	off	Enables/disables the sending of SNMP traps after a USB port (i.e. the connection to the connected USB device) was activated/deactivated.
trappup [Send trap if INU server is restarted]	on/off	off	Enables/disables the sending of SNMP traps when the INU server is restarted.

Parameters	Value	Default	Description
trap_pwr [Send trap if power supply is interrupted or established]	on/off	off	Enables/disables the sending of SNMP traps when one of the two power supplies of the INU server is interrupted or established.
trap_lnk [Send trap if network connection is interrupted or established]	on/off	off	Enables/disables the sending of SNMP traps when one of the two network connections of the INU server is interrupted or established.
trap_sdinout [Send trap if SD card is connected or disconnected]	on/off	off	Enables/disables the sending of SNMP traps after an SD card was connected to/removed from the INU server.
trap_sdunusable [Send trap if SD card cannot be used]	on/off	off	Enables/disables the sending of SNMP traps if the SD card is unusable.

Table 28: Parameter list – SSL/TLS connections

Parameters	Value	Default	Description
sslmethod [Encryption protocol]	any sslv3 tls10 tls11 tls12	any	Defines the encryption protocol for SSL/TLS connections. any = at will (automatic negotiation) sslv3 = SSL 3.0 tls10 = TLS 1.0 tls11 = TLS 1.1 tls12 = TLS 1.2  **WARNING** Current browsers do not support low security settings. If you use SSL with a current browser and the setting **HTTPS only** for access to the INU Control Center (⇨ 🗎46), a connection cannot be established. Use TLS (and not SSL).
security [Encryption level]	1–4 [1 character; 1–4]	4	Defines the encryption level for SSL/TLS connections. 1 = low 2 = medium 3 = high 4 = any (automatic negotiation)  **WARNING** 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 (⇨ 🗎46), a connection cannot be established. Use an encryption level as high as possible.

Table 29: Parameter list – INU Control Center security

Parameters	Value	Default	Description
http_allowed [Connection]	on/off	on	Defines the connection type (HTTP/HTTPS) to be used for connecting to the INU Control Center. on = HTTP/HTTPS off = HTTPS only The encryption strength is defined via the encryption protocol and level ⇨ 🗎46.  **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**. When the connection is established, the identity of the INU server is verified. For that, the client asks for the certificate via the browser (⇨ 🗎52). This certificate must be accepted by the browser; read the documentation of your browser software.
sessKeys [Restrict Control Center access]	on/off	off	Enables/disables the INU 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 is the user name of the SNMPv3 admin account ⇨ 🗎19.
admin_pwd [Administrator – Password]	8–64 characters [a–z, A–Z, 0–9]	administrator	Defines the password for the administrator user account.  **Important:** Also is the password of the SNMPv3 admin account ⇨ 🗎19.
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 is the user name of the SNMPv3 user account ⇨ 🗎19.

Parameters	Value	Default	Description
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 is the password of the SNMPv3 user account ⇨ 19.
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 mask, user name and password must be entered
sessKeyTimer [Session timeout]	on/off	on	Enables/disables the session timeout.
sessKeyTimeout [Session timeout]	120–3600 [3–4 characters; 0–9]	600	Time in seconds after which the timeout is to be effective.

Table 30: 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_8 [IP address]	on/off	off	Enables/disables an exception from the port locking.
ip_filter_1 ~ ip_filter_8 [IP address]	valid IP address	[blank]	Defines networks elements that are excluded from port blocking via their IP address. **Important:** The use of wildcards (*) allows you to define subnetworks.
hw_filter_on_1 ~ hw_filter_on_8 [MAC address]	on/off	off	Enables/disables an exception from the port locking.

Parameters	Value	Default	Description
hw_filter_1 ~ hw_filter_8 [MAC address]	valid hardware address	00:00:00:00:00:00	Defines elements that are excluded from port locking using the MAC address (hardware address).  **Important:** MAC addresses are not delivered through routers!
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 31: Parameter list – USB connection encryption

Parameters	Value	Default	Description
utn_sec_1 ~ utn_sec_20 [USB port]	on/off	off	Enables/disables the SSL/TLS encryption for the connection between USB port (i.e. USB device) and client.  **Important:** Only payload will be encrypted. Control and log data will be transmitted without encryption.

Table 32: Parameter list – USB device type blocking

Parameters	Value	Default	Description
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

Table 33: Parameter list – IPv4-VLAN

Parameters	Value	Default	Description
utn_accctrt_1 ~ utn_accctrt_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 key control
utn_keyval_1 ~ utn_keyval_20 [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_vendprodIDs_1 ~ utn_vendprodIDs_20 [USB device]			Defines the VID (Vendor ID) and PID (Product ID) of the USB device that is assigned to the USB port via the device assignment. *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.*

Table 34: Parameter list – Authentication

Parameters	Value	Default	Description
auth_typ [Authentication method]	--- MD5 TLS TTLS PEAP FAST	---	Defines the authentication method used in your network in which the INU server is to 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 user name with which the INU server is set up on the RADIUS server 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
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 35: Parameter list – Backup

Parameters	Value	Default	Description
autoSync [Parameter backup]	on/off	on	Enables/disables the automatic backup of parameter values, passwords, and certificates to a connected SD card.

Table 36: 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.

8.3 SEH UTN Manager – Feature Overview

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

- Selection list mode
  - global
  - user
- Client operating system (Windows, OS X/macOS, Linux)
- Client user account
  - administrator
  - standard user
- 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 USB device connected does not support them
- security measures have been implemented

Table 37: SEH UTN Manager – Feature Overview Windows

	Global Selection List		User Selection List		
	Administrator	User	Administrator	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	✓	✓	✓	✓	✓
USB Server – Set USB Port Keys	✓	×	✓	✓	×
UTN Server – Add	✓	×	✓	✓	×
UTN Server – Remove	✓	×	✓	✓	×
UTN Server – Refresh	✓	✓	✓	✓	✓
Port – Activate	✓	✓	✓	✓	✓
Port – Deactivate	✓	✓	✓	✓	✓
Port – Request	✓	✓	✓	✓	✓
Port – Remove	✓	×	✓	×	×
Port – Create UTN Action	✓	✓	✓	✓	✓
Port – Settings	✓	✓	✓	✓	✓

	Global Selection List		User Selection List		
	Administrator	User	Administrator	User (read/ write *.ini)	User (no read/ write *.ini)
Buttons					
Selection List – Refresh	✓	✓	✓	✓	✓
Selection List – Edit	✓	×	✓	✓	×
Port – Activate	✓	✓	✓	✓	✓
Port – Deactivate	✓	✓	✓	✓	✓
'Program – Options' dialog					
Network Scan – Multicast Search	✓	×	✓	×	×
Network Scan – IP Range Search	✓	×	✓	×	×
Program – Program Language	✓	✓	✓	✓	✓
Program – Program Messages	✓	×	✓	×	×
Program – Program Update	✓	×	✓	×	×
Automatisms – Program Start (Autostart)	✓	✓	✓	✓	✓
Automatisms – Auto-Disconnect	✓	×	✓	×	×
Selection List – Selection List Mode	✓	×	✓	×	×
Selection List – Automatic Refresh	✓	×	✓	×	×
'Port Settings' dialog					
Automatic device connection – Auto-Connect	✓	×	✓	×	×
Automatic device connection – Print-On-Demand	✓	×	✓	×	×
Plugin mode	✓	×	✓	×	×
Messages	✓	✓	✓	✓	✓

8.4 Index