USB Deviceservers & USB Dongleservers

myUTN User Manual
Windows

USB Deviceservers
myUTN-50a, myUTN-55, myUTN-2500

USB Dongleservers
myUTN-80, myUTN-800
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: myUTN User Manual Windows
Version: 4.0 | 2018-06

Legal Information

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

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

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

© 2018 SEH Computertechnik GmbH

All trademarks, registered trademarks, logos and product names are property of their respective owners.
# myUTN User Manual Windows

6.8 How to Use Certificates .......................................................................................................................... 56
6.9 How to Configure Network Authentication (IEEE 802.1X) ..................................................................... 60

## 7 Maintenance ......................................................................................................................................... 63
7.1 How to Restart the UTN Server ........................................................................................... 64
7.2 How to Update......................................................................................................................................... 64
7.3 How to Backup Your Configuration ............................................................................................ 65
7.4 How to Reset Parameters to their Default Values ........................................................................... 66

## 8 Appendix ........................................................................................................................................... 68
8.1 Glossary ............................................................................................................................................... 69
8.2 Troubleshooting ............................................................................................................................ 70
8.3 Parameter Lists .................................................................................................................................. 73
8.4 SEH UTN Manager – Feature Overview.......................................................................................... 97
8.1 Index.................................................................................................................................................. 99
1 General Information

- Product
- Documentation
- Support and Service
- Your Safety
- First Steps

1.1 Product

Purpose
UTN servers comprise USB Deviceservers and USB Dongleservers. As USB Deviceservers they make non-network-ready USB devices (e.g. USB hard disk drives, USB printers, etc.) and as USB Dongleservers non-network-ready USB dongles accessible via TCP/IP network. For this purpose, the USB devices respectively USB dongles will be connected to the USB ports of the UTN 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 respectively USB dongle and client. The USB device respectively USB dongle can be used as if it were connected locally.

Important:
The Dongleservers myUTN-80 and myUTN-800 are exclusively designed for the deployment of USB dongles.

Important:
Hereinafter USB dongles and USB devices are referred to as 'USB devices'.

System Requirements
The UTN server has been designed for the use in TCP/IP networks.

The SEH UTN Manager runs on the following systems:
- Windows XP or later except for Windows Vista and Windows Server 2008
  (For Windows 7 and Windows Server 2008 R2 KB3033929 http://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: operating system induced limited USB device support. macOS 10.12.x and later: operating system induced limited USB device support.)
- Linux: *.deb (for Debian-based systems) and *.rpm (for Red Hat-based systems) installation packages are available for 64-bit systems. A successful installation cannot be guaranteed due to the multitude of Linux varieties! The installation must be carried out on your own.
  In the following 64-bit systems the installation was tested successfully:
  Debian: Debian 8.10, Debian 9, Ubuntu 14.04, Ubuntu 16.04
  Red Hat: CentOS 6.9, CentOS 7.4, Fedora 25, Fedora 26, openSUSE Leap 42.3, Oracle 6.9, Oracle 7.4, Red Hat Enterprise Linux 7.4, SUSE Linux Enterprise 12.3
- IPv4 TCP/IP network
Important:
The support of isochronous USB devices (e.g. cameras, microphones, speakers, etc.)
depends on
- the operating system:
  - Windows
  - Linux
- the UTN server model
  (information can be found in the respective product information)
- the software version:
  - firmware/software for UTN servers: 14.5.5 or later
  - SEH UTN Manager: 3.1.4 or later

This document describes the usage in Windows environments. Information about the usage in other environ-
ments can be found in the relevant system-specific User Manual. More details can be found in chapter ‘Documen-
tation’ ⇒ ③.

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

Serviceplus
For the Dongleservers myUTN-80 and myUTN-800 service contracts, the Serviceplus packages, are available. The
Serviceplus package extends the manufacturer's guarantee of a Dongleserver from 36 to 60 months. In addition,
you will receive quickly and easily an advance replacement device in case of a defect. Serviceplus packages must
be purchased separately.
Detailed information:

https://www.seh-technology.com/services/service-packages.html

Rack Mount Kits
For a perfect and safe storage of your Dongleserver we recommend the 'Rack Mount Kits' (RMK). With the instal-
lation kits, you can install the Dongleservers in 19" server racks.
Detailed information:

1.2 Documentation

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

Further applicable documents
Thee UTN documentation consists of the following documents:

Quick Installation Guide Print, PDF
Information on safety, technical data, instructions for hardware installation and initial setup, and declarations of conformity.

User Manual PDF
Detailed description of the UTN server configuration and administration. System-specific instructions for the following systems:
- Windows
- OS X/macOS
- Linux

Online help HTML
Information on how to use the web interface 'myUTN Control Center'.
(Embedded into web interface; no download.)

Product information Print, PDF
Features and technical data

Brochures Print, PDF

Open source licenses online
http://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

1. Numeration

→ Result

Tip
Step-by-step instructions
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 UTN server is used in TCP/IP networks and has been designed for use in office environments. It allows network users to access non-network-ready USB devices.

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

Safety Regulations
Before starting the initial setup of the UTN server, read and observe the safety regulations in the 'Quick 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 ⇒ 4.

1.5 First Steps

1. Read and observe the security regulations in order to avoid damages to people and devices ⇒ 4.
2. Install the hardware. The hardware installation includes connecting the UTN server to the network, USB devices, and power grid ‘⇒ Quick 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 ‘⇒ Quick Installation Guide’.
4. Configure the UTN 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 UTN server ⇒ 35.

You can find information on the UTN documentation in chapter ‘Documentation’ ⇒ 3.
2 Administration Methods

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

- Administration via myUTN Control Center  
- Administration via the SEH UTN Manager  
- Administration via InterCon-NetTool  
- Administration via Email

2.1 Administration via myUTN Control Center

The UTN server has a user interface, the myUTN Control Center which can be opened in an Internet browser (e.g. Microsoft Edge).

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

- Open myUTN Control Center in Browser
- myUTN Open Control Center via SEH UTN Manager
- myUTN Open Control Center via InterCon-NetTool
- Controls

Open myUTN Control Center in Browser

- The UTN server is connected to the network and the power grid.
- The UTN server has a valid IP address

1. Open your browser.
2. Enter the IP address of the UTN server as the URL.
3. The myUTN Control Center is displayed in the browser.

**Important:**
If the myUTN Control Center is not displayed, check if a gateway is configured (and the proxy settings of your browser).

myUTN Open Control Center via SEH UTN Manager

- The UTN server is connected to the network and the power grid.
- The UTN server has a valid IP address
- The SEH UTN Manager is installed on the client

1. Start the SEH UTN Manager.
2. In the selection list, select the UTN server.
3. In the menu bar, select **UTN Server – Configure**.
   - Your browser opens and the myUTN Control Center is displayed.

myUTN Open Control Center via InterCon-NetTool

1. Start the InterCon-NetTool.
2. In the device list, select the UTN server.
3. In the menu bar, select **Actions – Launch Browser**.
   - Your browser opens and the myUTN Control Center is displayed.
Controls

Figure 1: myUTN 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 myUTN 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 UTN servers.

- Features
- Versions
- Installation
- Program Start

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 UTN servers. All UTN servers found and their connected USB devices are displayed in the 'network list'. To use the USB devices connected to the UTN server, you have to add the UTN server to the 'selection list'. The devices shown in the selection list can be administrated and the connected USB devices can be used. Working with the SEH UTN Manager is described in detail in the chapter 'Working with the SEH UTN Manager'.

WARNING

UTN and the corresponding SEH UTN Manager only work in IPv4 networks. In IPv6-only networks only the myUTN Control Center can be accessed to administrate the UTN server.

Figure 2: SEH UTN Manager
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 client operating system
- the settings of the product-specific security mechanisms
- the status of the UTN server and respective USB port

More details can be found in chapter ‘SEH UTN Manager – Feature Overview’.

Versions
The SEH UTN Manager is available in two versions:

- **Complete Version:**
  SEH UTN Manager with graphical user interface (Figure 2) and additional features.

- **Minimal version (without graphical user interface):**
  Usage only via command line ('utnm' and automated programs ('UTN Actions').

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. More details can be found in chapter ‘SEH UTN Manager – Feature Overview’.
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:

http://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’ ⇒ 10
- ‘Unattended Installation’ ⇒ 10

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 http://technet.microsoft.com/en-us/library/security/3033929.)

☑ 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.

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:

http://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: "se hutnmanager-win-X.X.X.exe" /S [command]

Commands: Table 1

4. Confirm your entry.
   The sequence of commands will be run.

Table 1: Installation commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/A</td>
<td>Installs SEH UTN Manager for all users.</td>
</tr>
<tr>
<td>/C</td>
<td>Installs SEH UTN Manager for the current user only.</td>
</tr>
<tr>
<td>/F=&lt;folder name&gt;</td>
<td>Overrides the default folder name of the Start menu folder. Subfolders can be specified with '/'.</td>
</tr>
<tr>
<td>/G</td>
<td>Installs the complete version (10) of SEH UTN Manager. Recommended for general use.</td>
</tr>
<tr>
<td>/I=&lt;path&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>/K</td>
<td>Does not create a desktop shortcut.</td>
</tr>
<tr>
<td>/M</td>
<td>Installs the minimal version (10) of SEH UTN Manager. Expert use only!</td>
</tr>
<tr>
<td>/R</td>
<td>Runs SEH UTN Manager after the installation is complete.</td>
</tr>
<tr>
<td>/S</td>
<td>Instructs the installation to be silent. There is no user interaction and the user cannot cancel the installation.</td>
</tr>
<tr>
<td>/U</td>
<td>Updates an existing SEH UTN Manager. (If no SEH UTN Manager is installed, it will be installed using the default installation settings.)</td>
</tr>
<tr>
<td>/V1</td>
<td>Enables command line logging to troubleshoot installation problems.</td>
</tr>
<tr>
<td>/V2</td>
<td>Creates a log file in the installation folder. The file contains information to troubleshoot installation problems.</td>
</tr>
<tr>
<td>/V3</td>
<td>Enables command line logging and creates a log file in the installation directory. Both provide information to help troubleshoot installation issues.</td>
</tr>
<tr>
<td>/?</td>
<td>Shows the help page.</td>
</tr>
</tbody>
</table>
Program Start

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

Update

You can check for program updated manually and automatically. More information can be found in the 📖 'SEH UTN Manager Online Help'.
2.3 Administration via InterCon-NetTool

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

- Function  
- Installation
- Program Start

Function

After the InterCon-NetTool has 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-only networks only the myUTN Control Center can be accessed to administrate the UTN server.

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

![InterCon-NetTool interface](image)

Figure 3: InterCon-NetTool

1. Menu bar
2. Toolbar
3. Device list
4. Filters for the device list
5. Shortcut menu

Detailed information on how to use the InterCon-NetTool can be found in the 'InterCon-NetTool Online Help'. To start the online help, go to the menu bar and select Help – 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 UTN server via email and thus from any computer Internet access (remote access):
- Get UTN server status
- Set UTN server parameters
- UTN server update

To do so, you write commands into the email message header \(\Rightarrow\) Table 2 \(15\).

Table 2: Commands and comment:

<table>
<thead>
<tr>
<th>Commands</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Command&gt;</td>
<td>get status</td>
<td>You get the UTN server status page.</td>
</tr>
<tr>
<td></td>
<td>get parameters</td>
<td>You get the UTN server parameter list.</td>
</tr>
<tr>
<td></td>
<td>set parameters</td>
<td>Sends one or more parameters to the UTN server which will then be adopted by the UTN server. Write the parameters and their values into the email message body: <code>&lt;parameter&gt; = &lt;value&gt;</code></td>
</tr>
<tr>
<td></td>
<td>update utn</td>
<td>Carries out an automatic update using the software that is attached to the mail.</td>
</tr>
<tr>
<td></td>
<td>help</td>
<td>You get a page with information on remote maintenance.</td>
</tr>
</tbody>
</table>

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 \(\Rightarrow\) Table 2 \(15\) 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 UTN server \(\Rightarrow\) \(23\).
- In order to receive emails, the UTN 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 UTN server \(\Rightarrow\) \(25\).

1. Open an email program.
2. Write a new email:
   - As recipient enter the UTN server address.
   - Into the subject line enter an instruction. cmd: `<command> [<comment>]` Commands and comment: \(\Rightarrow\) Table 2 \(15\).
   - Into the email message body enter a TAN, if applicable.
3. Send the email.

\(\Rightarrow\) The UTN server receives the email and carries out the instruction.
Examples

You want to get the UTN server parameter list:
To: UTNserver@company.com
Subject: cmd: get parameters

You want to set the 'configuration' parameter:
To: UTNserver@company.com
Subject: cmd: set parameters
Email message body: TAN = nUn47ir79Ajs7QKE
                     sys_descr = <Your description>
3 Network Settings

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

- How to Configure IPv4 Parameters ➔ 18
- How to Configure IPv6 Parameters ➔ 20
- How to Configure WLAN ➔ 21
- How to Configure the DNS ➔ 23
- How to Configure SNMP ➔ 23
- How to Configure Bonjour ➔ 24
- How to Configure Email (POP3 and SMTP) ➔ 25
- How to Use the UTN Server in VLAN Environments (only myUTN-80 and later) ➔ 27
3.1 How to Configure IPv4 Parameters

In the hardware installation ('Hardware Installation Guide') the UTN server is connected to the network. The UTN 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 UTN server is connected to an IPv6 network, it will automatically receive an additional IPv6 address ⇒ 20.

The IPv4 address assigned to the UTN 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 UTN server into a TCP/IP network, you can configure different IPv4 parameters and/or manually assign a static IP address to the UTN server.

- Configuring IPv4 Parameters via the myUTN Control Center ⇒ 18
- Configuring IPv4 Parameters via SEH UTN Manager ⇒ 19
- Determining the IPv4 Address via SEH UTN Manager and Configuring IPv4 Parameters ⇒ 19
- Determining the IPv4 Address via InterCon-NetTool and/or Configuring IPv4 Parameters ⇒ 19

Configuring IPv4 Parameters via the myUTN Control Center

1. Start the myUTN Control Center.
3. Configure the IPv4 parameters; ⇒ Table 3 18.
4. Click Save & Restart to confirm.
   ⇒ The settings will be saved.

Table 3: IPv4 parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Enables or disables the protocols DHCP, BOOTP, and ARP/PING.</td>
</tr>
<tr>
<td>BOOTP</td>
<td>The IP address assignment via DHCP and BOOTP is automatic if one of these</td>
</tr>
<tr>
<td></td>
<td>protocols is implemented in your network.</td>
</tr>
<tr>
<td>ARP/PING</td>
<td>You can use the commands ARP and PING to change an IP address which was</td>
</tr>
<tr>
<td></td>
<td>assigned via Zeroconf. The implementation depends on your system; read the</td>
</tr>
<tr>
<td></td>
<td>documentation of your operating system.</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the UTN server.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Subnet mask of the UTN server.</td>
</tr>
<tr>
<td></td>
<td>Subnet masks are used to logically partition big networks into subnetworks.</td>
</tr>
<tr>
<td></td>
<td>If you are using the UTN server in a subnetwork, it requires the subnet mask</td>
</tr>
<tr>
<td></td>
<td>of the subnetwork.</td>
</tr>
<tr>
<td>Gateway</td>
<td>IP address of the network's standard gateway which the UTN server uses.</td>
</tr>
<tr>
<td></td>
<td>With a gateway, you can address IP addresses from other networks.</td>
</tr>
</tbody>
</table>

Important:
We recommend disabling these options once an IP address has been assigned to the UTN server.
Configuring IPv4 Parameters via SEH UTN Manager

✓ The SEH UTN Manager (complete version) is installed on the client ⇒ §8.
✓ The UTN server is shown in the selection list ⇒ §35.

1. Start the SEH UTN Manager.
2. In the selection list, select the UTN 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 ⇒ §8.

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 UTN servers of the same model, you can identify a specific device by its default name (⇒ §69) 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-NetTool and/or Configuring IPv4 Parameters

✓ The InterCon-NetTool is installed on the client ⇒ §13.
✓ The network scan via multicast is enabled in the InterCon-NetTool.

1. Start the InterCon-NetTool.
2. In the device list, select the UTN server.
   If you do not know the IP address, you can identify the UTN server in several ways:
   - by its type
   - if you are using several UTN servers of the same model, by its hardware address (which can be found in the type plate at the device bottom)
   - if the UTN server received its address via Zeroconf, it will appear under the filter ‘Zeroconf’
3. In the menu, select Installation → IP Wizard.
   The 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:fe00:3b6b

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:fe00:3b6b]:443

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

You can embed the UTN server into an IPv6 network.

**WARNING**
UTN (⇒ 21) and the corresponding SEH UTN Manager only work in IPv4 networks. The InterCon-NetTool also only works in IPv4 networks.

In IPv6-only networks only the myUTN Control Center (⇒ 26) can be accessed to administrate the UTN server.

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

1. Start the myUTN Control Center.
3. Configure the IPv6 parameters; ⇒ Table 4 ⇒20.
4. Click Save & Restart to confirm.

⇒ The settings will be saved.

**Table 4: IPv6 parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6</td>
<td>Enables/disables the IPv6 functionality of the UTN server.</td>
</tr>
<tr>
<td>Automatic config</td>
<td>Enables/disables the automatic assignment of the IPv6 address to the UTN server.</td>
</tr>
<tr>
<td>IPv6 address</td>
<td>Defines an IPv6 unicast address in the format n:n:n:n:n:n:n:n which is manually assigned to the UTN server.</td>
</tr>
<tr>
<td></td>
<td>• Every ‘n’ represents the hexadecimal value of one of the eight 16 bit elements of the address.</td>
</tr>
<tr>
<td></td>
<td>• Leading zeros can be omitted.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Router</td>
<td>Manually defines a static router to which the UTN server sends its requests.</td>
</tr>
</tbody>
</table>
3.3 How to Configure WLAN

The 'myUTN-55' is a WLAN device (Wireless Local Area Network) and supports the following standards:

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

You can view the current WLAN settings in the myUTN Control Center under NETWORK – WLAN.

To optimally integrate the UTN server into your network, configure the WLAN parameters to match your WLAN settings (network name, encryption, etc.). For this purpose, the UTN server must already be embedded into your WLAN and be addressable. The initial setup is described in your product's 'Quick Installation Guide'.

✓ You know the settings of the WLAN.
✓ The UTN server is within the WLAN range.

Important:
If the UTN server changes the network, it may receive a new IP configuration. If this is the case, the connection to the myUTN Control Center is interrupted.

1. Start the myUTN Control Center.
2. Select NETWORK – WLAN.
3. Configure the WLAN parameters; ⇒ Table 5 ⇐ 21.
4. Click Save & Restart to confirm.
   ⇐ The settings will be saved.

Table 5: WLAN parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix length</td>
<td>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 '/'.</td>
</tr>
<tr>
<td>Network name (SSID)</td>
<td>Enter your WLAN’s network name, also known as SSID (Service Set Identifier).</td>
</tr>
</tbody>
</table>
## Parameters | Description
---|---
Roaming | Enables/disables roaming (switching from one access point/router to another): If your WLAN covers a widespread area with several access points/routers (with identical settings) and the UTN server changes position, the UTN server will automatically switch to the better signal without loss of connection if roaming is activated. (Infrastructure mode only)

Channel | Enter your WLAN's channel (frequency range). (Ad hoc mode only)

⚠️ **WARNING**
Only use WLAN channels authorized for your country!
The UTN is an international product which supports a number of channels. Channels are statutorily regulated by national authorities. So the UTN server might support channels which are forbidden to use in your country. Inform yourself about national regulations.

Encryption method | Select the encryption method that protects your WLAN.

**Important:**
We recommend to use hexadecimal keys for WEP. Some access points/routers convert WEP keys in ASCII format to hexadecimal format. In this case, the ASCII key on the UTN server and the hexadecimal key on the access point/router do not match.

Use WEP key | Defines the WEP key to be used.

Key 1–4 | Defines the WEP keys. Four WEP keys are available. The key type defines the max. number of characters as well as the permitted character set for the WEP keys.

**Important:**
If your access point supports multiple WEP keys, make sure that the key numbers on access point and UTN server are identical. Example: The ABCDE must have the number 2 on both devices (and not 1 on the access point and 2 on the UTN server).

PSK | Defines the Pre Shared Key (PSK) for Wi-Fi Protected Access (WPA).

Authentication method | Choose the authentication mechanism which is used in your WLAN. For further information see 'How to Configure Network Authentication (IEEE 802.1X)' 📝 60.
3.4 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 (⇒ 29) with \texttt{ntp.server.de} instead of 10.168.0.140.

- Your network has a DNS server.
- 1. Start the myUTN Control Center.
- 2. Select \texttt{NETWORK – DNS}.
- 3. Configure the DNS parameters; ⇒ Table 6 23.
- 4. To confirm, click \texttt{Save}.

Table 6: DNS parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Enables/disables the name resolution via a DNS server.</td>
</tr>
<tr>
<td>Primary DNS server</td>
<td>Defines the IP address of the primary DNS server.</td>
</tr>
<tr>
<td>Secondary DNS server</td>
<td>Defines the IP address of the secondary DNS server.</td>
</tr>
<tr>
<td>Domain name (suffix)</td>
<td>Defines the domain name of an existing DNS server.</td>
</tr>
</tbody>
</table>

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

3.5 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 UTN supports version 1 and 2.

SNMPv1

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

SNMPv3

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

Important:
The user accounts are also used to access the myUTN Control Center and thus are to be defined under \texttt{SECURITY - Device access} ‘How to Protect Access to the myUTN Control Center (User Accounts)’ ⇒ 53.
SNMPv3 users are created in the monitoring station. (Only for SNMPv3.)

The SNMPv3 users from the monitoring station are specified on the UTN server. (Only for SNMPv3.)

1. Start the myUTN Control Center.
2. Select NETWORK – SNMP.
3. Configure the SNMP parameters; Table 7 24.
4. To confirm, click Save.

The settings will be saved.

Table 7: SNMP Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv1</td>
<td>Enables/disables SNMPv1.</td>
</tr>
<tr>
<td>Read-only</td>
<td>Enables/disables the write protection for the community.</td>
</tr>
<tr>
<td>Community</td>
<td>SNMP community name Enter the name as it is defined in the monitoring station.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv3</td>
<td>Enables/disables SNMPv3.</td>
</tr>
<tr>
<td>Hash</td>
<td>Defines the hash algorithm.</td>
</tr>
<tr>
<td>Access rights</td>
<td>Defines the access rights of the SNMP user.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Defines the encryption method.</td>
</tr>
</tbody>
</table>

3.6 How to Configure Bonjour

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

The UTN server uses Bonjour to

- verify IP addresses
- announce and find network services
- match host names and IP addresses

1. Start the myUTN Control Center.
2. Select NETWORK – Bonjour.
3. Configure the Bonjour parameters; Table 8 24.
4. To confirm, click Save.

The settings will be saved.

Table 8: Bonjour parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bonjour</td>
<td>Enables/disables Bonjour.</td>
</tr>
<tr>
<td>Bonjour name</td>
<td>Defines the Bonjour name of the UTN server.</td>
</tr>
</tbody>
</table>

The UTN server uses this name to announce its Bonjour services. If no Bonjour name is entered, a default name will be used (device name@ICxxxxxx).
3.7 How to Configure Email (POP3 and SMTP)

The UTN server can be administered via email (⇒ 315) and offers a notification service (⇒ 331) 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 UTN server.

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

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

- Configuring POP3 ⇒ 25
- Configuring SMTP ⇒ 25

Configuring POP3

- An email user account for the UTN server is set up on the POP3 server.

1. Start the myUTN Control Center.
2. Select NETWORK – Email.
3. Configure the POP3 parameters; ⇒ Table 9 ⇒ 25.
4. To confirm, click Save.
   ⇔ The settings will be saved.

Table 9: POP3 parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POP3</td>
<td>Enables/disables the POP3 functionality.</td>
</tr>
<tr>
<td>POP3 – Server name</td>
<td>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.</td>
</tr>
<tr>
<td>POP3 – Server port</td>
<td>Defines the port which the UTN server uses to receive emails. The default port number for POP3 is 110. The default port number for SSL/TLS (parameter 'POP3 – Security' ⇒ 25) is 995. If required, read the documentation of your POP3 server.</td>
</tr>
<tr>
<td>POP3 – Security</td>
<td>Defines the authentication method to be used:</td>
</tr>
<tr>
<td></td>
<td>• APOP: encrypts the password when logging on to the POP3 server.</td>
</tr>
<tr>
<td></td>
<td>• SSL/TLS: encrypts the entire communication with the POP3 server. The encryption strength is defined via the encryption protocol and level ⇒ 51.</td>
</tr>
<tr>
<td>POP3 – Check mail every</td>
<td>Defines the time interval (in minutes) which with the POP3 server is checked for emails.</td>
</tr>
<tr>
<td>POP3 – Ignore mail exceeding</td>
<td>Defines the maximum email size (in Kbyte) to be accepted by the UTN server. (0 = unlimited)</td>
</tr>
<tr>
<td>POP3 – User name</td>
<td>Defines the user name used by the UTN server to log on to the POP3 server.</td>
</tr>
<tr>
<td>POP3 – Password</td>
<td>Defines the user password used by the UTN server to log on to the POP3 server.</td>
</tr>
</tbody>
</table>

Configuring SMTP

- An email user account for the UTN server is set up on the SMTP server.

1. Start the myUTN Control Center.
2. Select NETWORK – Email.
3. Configure the SMTP parameters; ⇒ Table 10 ⇒ 26.
4. To confirm, click **Save**.  
   ⇒ The settings will be saved.

**Table 10: SMTP Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP - Server name</td>
<td>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.</td>
</tr>
<tr>
<td>SMTP – Server port</td>
<td>Defines the port which the UTN server and SMTP server use to communicate. The default port number for SMTP is 25. For SSL/TLS (parameter ‘SMTP – SSL/TLS’ ⇒ 51), SMTP servers use by default port 587 (STARTSSL/STARTTLS) or the old port 465 (SMTPS). If required, read the documentation of your SMTP server.</td>
</tr>
<tr>
<td>SMTP – SSL/TLS</td>
<td>Enables/disables SSL/TLS. SSL/TLS encrypts the communication from the UTN to the SMTP server. The encryption strength is defined via the encryption protocol and level ⇒ 51.</td>
</tr>
<tr>
<td>SMTP – Sender name</td>
<td>Defines the email address used by the UTN server to send emails. Very often the name of the sender and the email account user name are identical.</td>
</tr>
<tr>
<td>SMTP – Login</td>
<td>Enables/disables SNMP authentication. To send emails, the UTN sends its user name and password to the SMTP server to authenticate itself. Enter user name (parameter ‘SMTP – User name’ ⇒ 26) and password (parameter ‘SMTP – Password’ ⇒ 26). Some SMTP servers require SMTP authentication to prevent fraudulent use (spam).</td>
</tr>
<tr>
<td>SMTP – User name</td>
<td>Defines the user name used by the UTN server to log on to the SMTP server.</td>
</tr>
<tr>
<td>SMTP – Password</td>
<td>Defines the password used by the UTN server to log on to the SMTP server.</td>
</tr>
<tr>
<td>SMTP – Security (S/MIME)</td>
<td>Enables/disables the email security standard S/MIME (Secure/Multipurpose Internet Mail Extensions). S/MIME is used to sign (‘SMTP – Signing emails’ ⇒ 26) or encrypt (‘SMTP – Full encryption’ ⇒ 26) emails. Enable the desired features (if desired with ‘SMTP – Attach public key’ ⇒ 26).</td>
</tr>
<tr>
<td>SMTP – Signing emails</td>
<td>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 ⇒ 56.</td>
</tr>
<tr>
<td>SMTP – Full encryption</td>
<td>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 ⇒ 56.</td>
</tr>
<tr>
<td>SMTP – Attach public key</td>
<td>Sends the public key together with the email. Many email clients require the key to display the email.</td>
</tr>
</tbody>
</table>
3.8 How to Use the UTN Server in VLAN Environments (only myUTN-80 and later)

The UTN 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 UTN 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 UTN server for it.]

- Define a IPv4 Management VLAN
- Define a IPv4 Client VLAN
- Allocating a IPv4 Client VLAN to a USB Port

Define a IPv4 Management VLAN

1. Start the myUTN Control Center.
2. Select NETWORK – IPv4 VLAN.
3. Configure the IPv4 VLAN parameters; Table 11 27.
4. To confirm, click Save.
5. The settings will be saved.

Table 11: IPv4 management VLAN parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 management VLAN</td>
<td>Enables/disables the forwarding of IPv4 management VLAN data. If this option is enabled, SNMP is only available in the IPv4 management VLAN.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>ID for the identification of the IPv4 management VLAN (0–4096).</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the UTN server  18.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Subnet mask of the UTN server  18.</td>
</tr>
<tr>
<td>Gateway</td>
<td>IP address of the network's standard gateway which the UTN server uses  18. With a gateway, you can address IP addresses from other networks.</td>
</tr>
<tr>
<td>Access from any VLAN</td>
<td>Enables/disables the administrative access (web) to the UTN server via IPv4 client VLANs. If this option is enabled, the UTN server can be administrated via all VLANs.</td>
</tr>
<tr>
<td>Access via LAN (untagged)</td>
<td>Enables/disables the administrative access to the UTN server via IPv4 packets without tag. If this option is disabled, the UTN server can only be administrated via VLANs.</td>
</tr>
</tbody>
</table>

Define a IPv4 Client VLAN

1. Start the myUTN Control Center.
2. Select NETWORK – IPv4 VLAN.
3. Configure the IPv4 VLAN parameters; Table 12 28.
4. To confirm, click Save.
   The settings will be saved.

Table 12: IPv4 client VLAN parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Enables/disables the forwarding of IPv4 client VLAN data.</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the UTN server within the IPv4 client VLAN.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Subnet mask of the UTN server within the IPv4 client VLAN.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Gateway address of the IPv4 client VLAN.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>ID for the identification of the IPv4 client VLAN (0–4096).</td>
</tr>
</tbody>
</table>

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 myUTN 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

- How to Configure the Device Time ⇒ 29
- How to Assign a Description ⇒ 29
- How to Assign a Name to a USB Port ⇒ 30
- How to Disable a USB Port (only myUTN-80 and later) ⇒ 30
- How to Configure the UTN (SSL) Port ⇒ 31
- How to Get Messages (only myUTN-80 and later) ⇒ 31
- How to Configure Acoustic Signals (myUTN-800 only) ⇒ 32
- How Do I Determine What is Shown in the Display? (myUTN-800 only) ⇒ 33

4.1 How to Configure the Device Time

The device time of the UTN 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 UTN 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 myUTN 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 ⇒ 23.)
  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 UTN server. This gives you a better overview of the devices in the network.

You can also assign names to USB ports to distinguish them ⇒ 30.

1. Start the myUTN 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.
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 myUTN 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 myUTN 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 (only myUTN-80 and later)

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 myUTN 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 UTN server (including connected USB devices) and the client. It depends on the connection type:

- **unencrypted** USB connection: UTN port (default = 9200)
- **encrypted** USB connection (⇒ 49): 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 UTN server and is relayed to the SEH UTN Manager installed on the clients via SNMPv1.

- SNMPv1 is enabled ⇒ 23.

1. Start the myUTN 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 (only myUTN-80 and later)

The UTN server can send you different messages:

- Status email: Periodically sent email containing the status of the UTN server and of the connected USB devices.
- Event notification via email or SNMP trap:
  - USB device is connected to the UTN server / disconnected from the UTN server
  - USB port (i.e. connection to the connected USB device) is activated/deactivated
  - UTN server restart
  - power supply is interrupted/established (myUTN-800 only)
  - network connection is interrupted/established (myUTN-800 only)
  - SD card is inserted into the UTN server / removed from the UTN server (myUTN-800 only)
  - SC card cannot be used (myUTN-800only)

- Configuring the sending of status emails ⇒ 31
- Configuring event notifications via email ⇒ 32
- Configuring event notifications via SNMP traps ⇒ 32

Configuring the sending of status emails

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

- SMTP is set up ⇒ 25.
- DNS is set up ⇒ 23.

1. Start the myUTN 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 ⇒ 25.
✓ DNS is set up ⇒ 23.
1. Start the myUTN 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 ⇒ 23.
1. Start the myUTN 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 Configure Acoustic Signals (myUTN-800 only)
The myUTN-800 Dongleserver gives acoustic feedback if:
   • a USB dongle is connected
   • the Dongleserver restarts
   • the parameters are reset
These acoustic signals cannot be turned off.
Optionally, you can configure additional acoustic feedback for the following events:
   • only one power supply works
   • SD card errors (read and write errors, no SD card)
   • only one network connection is established

   ![Tips]
   **These optional acoustic signals ideally complement the error messages in the display panel ⇒ 33.**

1. Start the myUTN Control Center.
2. Select **DEVICE – Notification**.
3. In the **Acoustic signal** area, tick the options with the desired message types.
4. To confirm, click **Save**.
   ← The settings will be saved.
4.8 How Do I Determine What is Shown in the Display? (myUTN-800 only)

The Dongleserver myUTN-800 has a display panel at its front side. The following information can be displayed:

- Identifier Freely definable name which will be displayed as default. (Default: DS)
- Error states: Optional notifications which can be displayed if these events occur:
  - only one power supply works
  - SD card errors (read and write errors, no SD card)
  - only one network connection is established

The Errors are displayed in codes.

Table 14: Error codes

<table>
<thead>
<tr>
<th>Text</th>
<th>Description</th>
<th>Troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS</td>
<td>The Dongleserver is operational.</td>
<td>–</td>
</tr>
<tr>
<td>RS</td>
<td>The Dongleserver is restarting.</td>
<td>–</td>
</tr>
<tr>
<td>DL</td>
<td>Firmware/software is loaded onto the Dongleserver. Afterwards the Dongleserver is updated.</td>
<td>–</td>
</tr>
<tr>
<td>E1</td>
<td>One of the two power supplies is not working.</td>
<td>Check the cabling connections and voltage source.</td>
</tr>
<tr>
<td></td>
<td>Which connection is not working is indicated by a glowing dot (left dot, left power supply; right dot, right power supply).</td>
<td></td>
</tr>
<tr>
<td>E2</td>
<td>The SD card is formatted with an unsupported file system respectively cannot be read and be written to.</td>
<td>• Format the SD card in the file format FAT32, FAT16 or FAT12.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check if the SD card functions properly.</td>
</tr>
<tr>
<td>E3</td>
<td>The SD card is read-only.</td>
<td>Remove the write protection from the SD card.</td>
</tr>
<tr>
<td>E4</td>
<td>No SD card is available in the card reader.</td>
<td>Insert an SD card into the SD card reader:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: SD or SDHC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• File system: FAT32, FAT16, or FAT12</td>
</tr>
<tr>
<td>E5</td>
<td>One or both network connections have no link.</td>
<td>Check the cable connections and your network.</td>
</tr>
</tbody>
</table>

- Configuring the Identifier ➔ 33
- Enable Error Notifications ➔ 34

Configuring the Identifier

Use the identifier to identify devices if you have installed several myUTN-800 in a server rack or at the same location.

1. Start the myUTN Control Center.
2. Select DEVICE – Description.
3. Enter a freely definable description into the Identifier (display panel) box.
4. To confirm, click **Save**.  
   ➙ The settings will be saved.

Figure 4: Display panel myUTN-800

**Enable Error Notifications**

1. Start the myUTN Control Center.
2. Select **DEVICE – Notification**.
3. In the **Display panel** area, tick the options with the desired message types.
4. To confirm, click **Save**.  
   ➙ The settings will be saved.

*The optional acoustic signals ideally complement the error messages in the display panel ➙ 32.*
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 connected to the UTN servers.

- How to Find UTN Servers/USB Devices in the Network ➔ 35
- How to Establish a Connection to a USB Device ➔ 37
- How to Cut the Connection between the USB Device and the Client ➔ 38
- How to Request an Occupied USB Device ➔ 38
- How to Automate USB Device Connections and Program Starts ➔ 39
- How to Find Status Information on USB Ports and USB Devices ➔ 42
- How to Use the Selection List and Manage User Access Rights with It ➔ 42
- How to Use the SEH UTN Manager without Graphical User Interface (utnm) ➔ 45

5.1 How to Find UTN 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 UTN servers.

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

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

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

- Defining Search Parameters ➔ 35
- Scanning the Network ➔ 35
- Adding the UTN Server to the Selection List ➔ 36
- Adding a UTN Server via IP Address ➔ 36

Defining Search Parameters

✓ The SEH UTN Manager (complete version) is installed on the client ➔ 8.

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 ➔ 8.

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 UTN servers and USB devices found are displayed in the network list.
Adding the UTN Server to the Selection List
- The SEH UTN Manager (complete version) is installed on the client.
- The UTN 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 UTN server to be used.
4. Click **Add.**
   - (Repeat steps 2 and 3, if necessary.)
5. Click **OK.**
   - The UTN servers and the connected USB devices are shown in the selection list.

![Edit Selection List](image)

**Figure 5:** SEH UTN Manager – Edit Selection List

Adding a UTN Server via IP Address
- The SEH UTN Manager (complete version) is installed on the client.
- You know the IP address of the UTN 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 UTN server.
4. If you changed the UTN port or UTN SSL port, define the respective port numbers in the **UTN-Port** and **UTN-SSL-Port** box.
5. Click **OK.**
   - The UTN 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 UTN 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 UTN 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 UTN server. The number of these virtual USB ports is limited depending on the UTN server model. If the limit is reached, no further USB devices can be used on this UTN server.

---

<table>
<thead>
<tr>
<th>UTN server</th>
<th>Number of virtual USB ports</th>
<th>Number of virtual USB ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>myUTN-50a</td>
<td>6</td>
<td>myUTN-800</td>
</tr>
<tr>
<td>myUTN-55</td>
<td>6</td>
<td>myUTN-2500</td>
</tr>
<tr>
<td>myUTN-80</td>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>

- The SEH UTN Manager (complete version) is installed on the client ⇒ §8.
- The USB port is shown in the selection list ⇒ §35.
- All provisions (driver installation, etc.) necessary to operate the USB device locally (i.e. connected directly to the client) have been met on the client. Ideally, the USB device has been connected and operated on the client locally according to the instructions of the manufacturer.
- The USB port is not connected to another client.

1. Start the SEH UTN Manager.
2. In the selection list, select the port.
3. In the menu bar, select Port – Activate.

The connection between the USB device and client is established.
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 UTN server to which the USB device is connected.

- Usually the connection is cut by the user via the SEH UTN Manager ⇨ §38.
- In addition, the administrator can deactivate the connection via the myUTN Control Center ⇨ §38.
- You can also set up an automatic deactivation (Auto Disconnect) ⇨ §39.

Cutting the Device Connection via the SEH UTN Manager

✓ The SEH UTN Manager (complete version) is installed on the client ⇨ §8.
✓ The USB port is shown in the selection list ⇨ §35.
✓ The USB port is connected to your client ⇨ §37.

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

Cutting the Device Connection via the myUTN Control Center

✓ A USB port is connected to your client ⇨ §37.

1. Start the myUTN Control Center.
2. Select **START**.
3. Choose the active connection from the **Attached devices** list and click the [x] 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 ⇨ §8.
✓ The SEH UTN Manager (complete version) is installed on the client of the user who uses the USB device ⇨ §8.
✓ The SEH UTN Manager (complete version) is executed with graphical user interface on both clients.
✓ The USB port is shown in the selection list ⇨ §35.
✓ The USB port is connected to another client ⇨ §37 (but not via Auto-Connect).

1. In the selection list, select the port.
2. In the menu bar, select **Port – Request**.
   ⇨ The release request will be sent.
5.5 How to Automate USB Device Connections and Program Starts

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

- **Automatic Connection If a USB Device Is Connected (Auto-Connect)**
- **Automatic Deactivation of the Connection after a Time Defined (Auto-Disconnect)**
- **Automatic Connection between a USB Device and Client When a Print Job Is Received (Print-On-Demand)**
- **Creating a UTN Action: Automated Connections and Program Starts without the SEH UTN Manager Interface**

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'.

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

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

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

1. Start the SEH UTN Manager.
2. Select the UTN server from the selection list.
3. In the menu bar, select **UTN server – Activate Auto-Connect**. The dialog **Activate Auto-Connect** appears.
4. Tick the option for the desired USB ports.
5. Click OK.

The setting will be saved. The connection to the USB port and the connected USB device is automatically and immediately activated. If you disconnect the USB device and reconnect it, the connection is again automatically established.

**Important:**

If you manually deactivate an established USB port connection that was activated by Auto-Connect, the Auto-Connect setting will be deactivated as well. If you want to use Auto-Connect again, you will have to configure it anew later on.

**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.
The SEH UTN Manager (complete version) is installed on the client.
The UTN server is displayed in the 'Automatic Device Disconnect' area.
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 UTN server.
5. Define the desired time range (10-9999 minutes).
6. If 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.

1. Start the SEH UTN Manager.
2. In the selection list, select the port.
3. In the menu bar, select **Port – Activate**.
The connection will be established. The device is installed. A printer object is created on the client.
4. In 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 ac-
tivates 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.

- The SEH UTN Manager (complete version) is installed on the client.
- The USB port is shown in the selection list.

1. Start the SEH UTN Manager.
2. Select a port from the selection list.
3. In 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 7: 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 can use automatic messages to be notified when a USB port becomes available or to receive information about the connection duration.

- Displaying Status Information ➝ 42
- Notification If a USB Port Becomes Available ➝ 42
- Message about the Duration of a Connection ➝ 42

Displaying Status Information
✓ The SEH UTN Manager (complete version) is installed on the client ➝ 8.
✓ The USB port is shown in the selection list ➝ 35.

1. Start the SEH UTN Manager.
2. Select the USB port from the selection list.
   ↯ The status information is displayed in the Properties area.

Notification If a USB Port Becomes Available
You will receive a message once a network participant deactivates the connection to a USB port and the connected USB device.
✓ The SEH UTN Manager (complete version) is installed on the client ➝ 8.
✓ The USB port is shown in the selection list ➝ 35.

1. In the selection list, select the port.
2. In the menu bar, select Port – Settings.
   The Port Settings dialog appears.
3. Tick the option under Messages.
4. Click OK.
   ↯ The setting will be saved.

Message about the Duration of a Connection
You will receive a message if one of your connections to a USB port and the connected USB device exceeds a defined time period.
✓ The SEH UTN Manager (complete version) is installed on the client ➝ 8.

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

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 UTN servers. USB devices can only be used if the UTN server to which they are connected is on the list (➔ 35). By controlling the selection list you consequently control the user’s access to UTN 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 UTN servers you define can be used.
Table 15: Differences in global and user selection list

<table>
<thead>
<tr>
<th>Global Selection List</th>
<th>User Selection List</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All users of a client use the same selection list.</td>
<td>• Each user has their own selection list. All administrators have the same selection list.</td>
</tr>
<tr>
<td>• The users can access all devices listed in the selection list. (Provided that no security mechanisms have been specified via the myUTN Control Center.)</td>
<td>• The users can access all devices listed in the selection list. (Provided that no security mechanisms have been specified via the myUTN Control Center.)</td>
</tr>
</tbody>
</table>
| • List is stored at: Registry | • List (‘ini’-file) is stored at: `\%APPDATA\%\SEH Computertechnik GmbH\SEH UTN Manager.ini`
\(\%\text{APPDATA}\) 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\Username\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’ ☞ 97.

- Setting Up the Global Selection List for All Users ☞ 44
- Providing User Selection Lists ☞ 44
- Restrict Write Access to the ‘SEH UTN Manager.ini’-file ☞ 44
Setting Up the Global Selection List for All Users

The global selection list is used by default.

- The SEH UTN Manager (complete version) is installed on the client.
- You are logged on to the system as administrator.

1. Start the SEH UTN Manager.
2. Compose the selection list.
3. In the menu bar, select **Program–Options**.
4. Select the tab **Selection List**.
5. Tick **Global selection list**.
6. Click **OK**.

   The setting will be saved. All users of a client use the same selection list.

Providing User Selection Lists

- The SEH UTN Manager (complete version) is installed on the client.
- You are logged on to the system as administrator.

1. Start the SEH UTN Manager.
2. In the menu bar, select **Program–Options**.
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.
7. In the menu bar, select **Selection List–Export**.
8. Save the file 'SEH UTN Manager.ini' to the user directories:
   - \%APPDATA\SEH Computertechnik GmbH\SEH UTN Manager.ini
     (⇒Table 15

   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 UTN 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 (⇒ Table 15) 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. 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
- Commands
- Return
- Using utnm via Command Line
- Creating a utnm Script

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. server = IP address or host name of a UTN server)
- elements in square brackets are optional.
- not case-sensitive
- only the ASCII format can be read.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/c &quot;command string&quot;</td>
<td>Runs a command. The command is specified in greater detail by the command string. Command strings:</td>
</tr>
</tbody>
</table>
|                     | - activate server port number  
                     |   Activates the connection to a USB port and the connected USB device.                                                                     |
|                     | - activate server vendor ID (VID) product ID (PID)  
                     |   Activates the connection to a USB port and the first free connected USB device with the defined IDs, if several identical USB devices are connected to the UTN server. |
|                     | - deactivate server port number  
                     |   Deactivates the connection to a USB port and the connected USB device.                                                                  |
|                     | - set autoconnect = true|false server port number  
                     |   Enables/disables Auto-Connect (☞ 39) for the USB port.                                                                                  |
|                     | - set portkey='port key' server port number  
                     |   Stores a USB port key (☞ 55) locally on the system. This way, the USB port key is always automatically sent and must not be specified each time with the command /k USB port key respectively /key USB port key (see below). |
|                     |   (To remove the USB port key use the command string set portkey= server port number)                                                     |
|                     | Important:                                                                                                                                   |
|                     |   The command only sets the key permanently to make the USB device available.                                                               |
|                     |   The USB port key configuration is done via the myUTN Control Center ☞ 55.                                                                |
|                     | - find  
                     |   Searches for all UTN servers in the network segment and shows the UTN servers found with IP address, MAC address, model and software version. |
|                     | - getlist server  
                     |   Shows an overview of the USB devices connected to the UTN server (including port number, vendor ID, product ID, vendor name, product name, device class, and status). |
|                     | - state server port number  
                     |   Displays the status of the USB device connected to the USB port.                                                                       |
| /h                  | Shows the help page.                                                                                                                          |
| or                  |                                                                                                                                             |
| /help               |                                                                                                                                             |
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' ⇒ § 47), only the value is returned.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/k USB port key or /key USB port key</td>
<td>Specifies a USB port key ⇒ § 55.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td>The command only enters the key to make the USB device available.</td>
</tr>
<tr>
<td></td>
<td><strong>Use the command /c &quot;command string&quot; respectively /command &quot;command string&quot; to permanently store a USB port key on the system so that it is sent automatically each time (see above).</strong></td>
</tr>
<tr>
<td></td>
<td>The USB port key configuration is done via the myUTN Control Center ⇒ § 55.</td>
</tr>
<tr>
<td>/mr or /machine readable</td>
<td>Separates the output of the command string getlist with tabulators and the output of find with commas.</td>
</tr>
<tr>
<td>/nw or /no-warnings</td>
<td>Suppresses warning messages.</td>
</tr>
<tr>
<td>/o or /output</td>
<td>Shows the output in the command line.</td>
</tr>
<tr>
<td>/p port number or /port port number</td>
<td>Uses an alternative UTN port.</td>
</tr>
<tr>
<td></td>
<td>Use this command if you have changed the UTN port number (⇒ § 31).</td>
</tr>
<tr>
<td>/q or /quiet</td>
<td>Suppresses the output.</td>
</tr>
<tr>
<td>/sp port number or /ssl-port port number</td>
<td>Uses an alternative UTN port with SSL/TLS encryption.</td>
</tr>
<tr>
<td></td>
<td>Use this command if you have changed the UTN SSL port number (⇒ § 31).</td>
</tr>
<tr>
<td>/t seconds or /timeout seconds</td>
<td>Specifies a timeout for the command strings activate and deactivate.</td>
</tr>
<tr>
<td>/v or /version</td>
<td>Shows version information about utnm.</td>
</tr>
</tbody>
</table>
The return can be used to determine how the process proceeds, e.g. in a script.

<table>
<thead>
<tr>
<th>Return Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The command was executed successfully.</td>
</tr>
<tr>
<td>20</td>
<td>Activation failed.</td>
</tr>
<tr>
<td>21</td>
<td>Deactivation failed.</td>
</tr>
<tr>
<td>23</td>
<td>Is already activated.</td>
</tr>
<tr>
<td>24</td>
<td>Is already deactivated or not available.</td>
</tr>
<tr>
<td>25</td>
<td>Activation failed: Another user has activated the USB port incl. device.</td>
</tr>
<tr>
<td>26</td>
<td>Not found: There is no device connected to the USB port or the USB port key (\55) is missing respectively wrong.</td>
</tr>
<tr>
<td>29</td>
<td>Not found: No USB device with this VID and PID connected.</td>
</tr>
<tr>
<td>30</td>
<td>Isochronous USB devices are not supported.</td>
</tr>
<tr>
<td>31</td>
<td>UTN driver error. Contact the SEH Computertechnik GmbH support ⇒ 24.</td>
</tr>
<tr>
<td>40</td>
<td>No network connection to the UTN server.</td>
</tr>
<tr>
<td>41</td>
<td>An encrypted connection to UTN server cannot be established.</td>
</tr>
<tr>
<td>42</td>
<td>No connection to UTN service.</td>
</tr>
<tr>
<td>43</td>
<td>The DNS resolution failed.</td>
</tr>
<tr>
<td>44</td>
<td>Insufficient rights (administrative rights required).</td>
</tr>
<tr>
<td>47</td>
<td>This feature is not supported.</td>
</tr>
<tr>
<td>200</td>
<td>Error (with error code).</td>
</tr>
</tbody>
</table>

Using utmn via Command Line

✓ The SEH UTN Manager is installed on the client ⇒ 28.
✓ You know the UTN server’s IP address or host name.

1. Open the command-line interface.
2. Enter the sequence of commands; see ‘Syntax’ ⇒ 45 and ‘Commands’ ⇒ 45.
3. Confirm your entry.
   ⇔ The sequence of commands will be run.

Example: Activating a USB device on port 3 of the UTN 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 ⇒ 28.
✓ You know the UTN 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’ ⇒ 45, ‘Commands’ ⇒ 45, and ‘Return’ ⇒ 47.
3. Save the file as executable script on your client.
   ⇔ The script is saved and can be used.
6 Security

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

- How to Encrypt the USB Connection ⇒ 49
- How to Encrypt the Connection to the myUTN Control Center ⇒ 51
- How to Define the Encryption Strength for SSL/TLS Connections ⇒ 51
- How to Protect Access to the myUTN Control Center (User Accounts) ⇒ 53
- How to Block Ports of the UTN Server (TCP Port Access Control) ⇒ 54
- How to Control Access to USB Devices (only myUTN-80 and later) ⇒ 55
- How to Block USB Device Types ⇒ 56
- How to Use Certificates ⇒ 56
- How to Configure Network Authentication (IEEE 802.1X) ⇒ 60

**Important:**
Protect the access to the myUTN 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’ ⇒ 23
- ‘How to Use the UTN Server in VLAN Environments (only myUTN-80 and later)’ ⇒ 27

### 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 UTN server. The encryption has to be activated individually for each connection, i.e. for each USB port.

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

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 ⇒ 51.

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

Use an encryption level as high as possible.

If connections are encrypted, client and UTN 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 ⇒ 31.
1. Start the myUTN 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:** UTN server – SSL/TLS connection in the network

**Figure 9:** SEH UTN Manager – encryption
6.2 How to Encrypt the Connection to the myUTN Control Center

You can protect the connection to the myUTN 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 ≥ 51. When an encrypted connection is to be established, the client asks for a certificate via a browser (≥ 56). 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 myUTN 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 UTN server can be encrypted with the protocol SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security):

- Email: POP3 (≥ 25)
- Email: SMTP (≥ 25)
- Web access to the myUTN Control Center: HTTPS (≥ 51)
- Data transfer between the clients and the UTN server (and the connected USB devices): USB connection (≥ 51)

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 UTN server, i.e. are part of an encryption level, depends on the chosen encryption protocol. You can choose between two encryption levels:

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

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

**WARNING**

If the communication partner of the UTN 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 UTN server ⇒ 66.

*If you want the UTN 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 myUTN 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 myUTN Control Center (⇒ 51), a connection cannot be established.

Use TLS (and **not** SSL).

**Important:**

Which protocols are supported by the UTN server depends on the product hardware and the installed firmware/software.

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 myUTN Control Center (⇒ 51), a connection cannot be established.

Use an encryption level as high as possible.

**WARNING**

The SEH UTN Manager does not support the encryption level **Low**. If you set up **Low** in combination with an encrypted USB connection (⇒ 49), a connection cannot be established.

Use an encryption level as high as possible.

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

   The setting will be saved.

*Detailed information about the individual SSL/TLS connections (e.g. supported cipher suites) can be found on the details page **SSL connection status – Details**.*
6.4 How to Protect Access to the myUTN Control Center (User Accounts)

By default, everyone who can find the UTN in the network can access its myUTN Control Center. To protect the UTN from unwanted configuration changes, you can set up two user accounts:

- **Administrator:** Complete access to the myUTN Control Center. The user can see all pages and change settings.
- **Read-only user:** Very restricted access to the myUTN Control Center. The user can only see the 'START' page.

If you have set up user accounts, a login screen is displayed when the myUTN 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 myUTN Control Center access are also used for SNMP ⇒ 23. 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 myUTN 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 UTN Server (TCP Port Access Control)

You can restrict access to the UTN 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 UTN 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 UTN server.

1. Start the myUTN 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 UTN 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 myUTN Control Center can be reached.

**Important:**
If the myUTN Control Center cannot be reached, restart the UTN server ⇒ 64.

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 (only myUTN-80 and later)

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 ⇒ 30.**

- Setting Up USB Port Keys ⇒ 55
- Entering a USB Port Key (Unlocking a USB Device) ⇒ 55
- Setting up USB Port Device Assignment ⇒ 55

### Setting Up USB Port Keys

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

1. Start the myUTN 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 UTN server.
3. In 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 myUTN 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.

   ![](image)

   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 UTN server, you can block input devices of the HID class.

1. Start the myUTN 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 UTN 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 UTN needs a certificate for:

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

The following certificates can be used in the UTN server:

- **1 self-signed certificate**
  Certificate generated by the UTN server and signed by the UTN server itself. The certificate confirms the UTN server's identity.

- **1 client certificate, i.e. 1 requested certificate or 1 PKCS#12 certificate**
  The client certificate confirms the identity of the UTN 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 UTN 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 UTN 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 UTN server. Then you transport the PKCS#12 file to the UTN server and install it (and thus the certificate in it).

- **1 S/MIME certificate**
  The UTN 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.

(only myUTN-80 and later)

- **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 UTN 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 UTN server. This certificate is issued by SEH Computertechnik GmbH for each device specifically.

- Having a Look at Certificates ⇒ 57
- Creating a Self-Signed Certificate ⇒ 57
- Request and Install Certificate (Requested Certificate) ⇒ 58
- Installing a PKCS#12 Certificate ⇒ 59
- Installing an S/MIME certificate (only myUTN-80 and later) ⇒ 59
- Installing a CA Certificate ⇒ 59
- Deleting Certificates ⇒ 60

**Having a Look at Certificates**

✓ A certificate is installed on the UTN server.

1. Start the myUTN Control Center.
2. Select **SECURITY – Certificates**.
3. Select the certificate via the icon 🔍.
4. The certificate is displayed.

**Creating a Self-Signed Certificate**

**Important:**
Only one self-signed certificate can be installed on the UTN server. To create a new certificate, you must first delete the existing certificate ⇒ 60.

1. Start the myUTN Control Center.
2. Select **SECURITY – Certificates**.
3. Click **Self-signed certificate**.
4. Enter the relevant parameters; ⇒ Table 16 ⇒ 57.
5. Click **Create/Install**.
6. The certificate will be created and installed. This may take a few minutes.

**Table 16: Parameters for the Creation of Certificates**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common name</td>
<td>Freely definable certificate name. (max. 64 characters)</td>
</tr>
<tr>
<td>Email address</td>
<td>Email address of the person responsible for the UTN server. (max. 40 characters; optional)</td>
</tr>
</tbody>
</table>
Request and Install Certificate (Requested Certificate)

A certificate that has been issued by a certification authority for the UTN server can be used in the UTN 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 UTN server. You install this certificate in the UTN server.

Important:
You can only install a requested certificate that has been issued based on the certificate request created on the UTN 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.

1. Start the myUTN Control Center.
2. Select SECURITY – Certificates.
3. Click Certificate request.
4. Enter the required parameters; ⇒ Table 16 §57.
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.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization name</td>
<td>Name of the company which uses the UTN server. (max. 64 characters)</td>
</tr>
<tr>
<td>Organizational unit</td>
<td>Name of a department or subsection in the company. (max. 64 characters; optional)</td>
</tr>
<tr>
<td>Location</td>
<td>Location of the company. (max. 64 characters)</td>
</tr>
<tr>
<td>State name</td>
<td>State where the company is based. (max. 64 characters)</td>
</tr>
<tr>
<td>Domain component</td>
<td>Allows you to enter additional attributes. (Optional entry)</td>
</tr>
<tr>
<td>SAN (multi-domain)</td>
<td>Allows you to enter Subject Alternative Names (SAN). Is used to enter additional host names (e.g. domains). (Optional entry, max. 255 characters)</td>
</tr>
<tr>
<td>Country</td>
<td>Country where the company is based. Enter the two-digit country code according to ISO 3166. Examples: DE = Germany, GB = Great Britain, US = USA</td>
</tr>
<tr>
<td>Issued on</td>
<td>Date from which on the certificate is valid.</td>
</tr>
<tr>
<td>Expires on</td>
<td>Date from which on the certificate becomes invalid.</td>
</tr>
<tr>
<td>RSA key length</td>
<td>Defines the length of the RSA key used:</td>
</tr>
<tr>
<td></td>
<td>- 512 bit (fast encryption and decryption)</td>
</tr>
<tr>
<td></td>
<td>- 768 bit</td>
</tr>
<tr>
<td></td>
<td>- 1024 bit (standard encryption and decryption)</td>
</tr>
<tr>
<td></td>
<td>- 2048 bit (slow encryption and decryption)</td>
</tr>
</tbody>
</table>
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 UTN server.

**Installing a PKCS#12 Certificate**

![Important:]
If a PKCS#12 certificate has already been installed in the UTN server, you must first delete the certificate ⇒ 60.

✓ The certificate has 'base64' format.

1. Start the myUTN 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 UTN server.

**Installing an S/MIME certificate (only myUTN-80 and later)**

![Important:]
If an S/MIME certificate has already been installed in the UTN server, you must first delete the certificate ⇒ 60.

✓ The certificate has 'pem' format.

1. Start the myUTN 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 UTN server.

**Installing a CA Certificate**

✓ The certificate has 'base64' format.

1. Start the myUTN 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 UTN server.
Deleting Certificates

**WARNING**
To establish an encrypted (HTTPS) connection to the myUTN Control Center, a certificate (self-signed/CA/PKCS#12) is required. If you delete the corresponding certificate, the myUTN Control Center can no longer be reached. In this case restart the UTN server. The UTN server then generates a new self-signed certificate with which a secured connection can be established.

• A certificate is installed on the UTN server.
1. Start the myUTN 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 UTN 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 UTN server can participate:
- Configuring EAP-MD5
- Configuring EAP-TLS
- Configuring EAP-TTLS
- Configuring PEAP
- Configuring EAP-FAST

#### 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 UTN server. Afterwards you set up EAP-MD5 on the UTN server.

• A user account for the UTN server is set up on the RADIUS server.
1. Start the myUTN 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 UTN 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, UTN server and RADIUS server exchange certificates through an encrypted TLS connection.

Both RADIUS and UTN server require a valid, digital certificate signed by a CA. This requires a PKI (Public Key Infrastructure).
1. Create a certificate request on the UTN server ⇒ 58.
2. Create a certificate using the certificate request and the authentication server.
3. Install the requested certificate on the UTN server ⇒ 58.
4. Install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) is installed in the UTN server ⇒ 59.
5. Start the myUTN Control Center.
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 UTN server and RADIUS server. To do this, the RADIUS server authenticates itself to the UTN 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 UTN 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 UTN server ⇒ 59.

1. Start the myUTN 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 UTN 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 UTN server and the RADIUS server. To do this, the RADIUS server authenticates itself to the UTN 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 (⇒ 61), but other methods are used to authenticate the UTN server.

✔ A user account for the UTN 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 UTN server ⇒ 59.
1. Start the myUTN 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 UTN 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 (⇒ 61) and PEAP (⇒ 61) 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 UTN server is set up on the RADIUS server.

1. Start the UTN 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 UTN 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 UTN server in the following ways:

- How to Restart the UTN Server ⇒ 64
- How to Update ⇒ 64
- How to Backup Your Configuration ⇒ 65
- How to Reset Parameters to their Default Values ⇒ 66
7.1 How to Restart the UTN Server

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

- Restarting the UTN Server via the myUTN Control Center ⇒ 64
- Restarting the UTN-Server via InterCon-NetTool ⇒ 64
- Restarting the UTN Server via Reset Button ⇒ 64

Restarting the UTN Server via the myUTN Control Center

1. Start the myUTN Control Center.
2. Select MAINTENANCE – Restart.
3. Click Restart.
   ↳ The UTN server restarts.

Restarting the UTN-Server via InterCon-NetTool

1. Start the InterCon-NetTool.
2. In the device list, select the UTN server.
3. In the menu bar, select Actions – Restart.
4. Click Finish.
   ↳ The UTN server restarts.

Restarting the UTN Server via Reset Button

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

7.2 How to Update

You can update your UTN 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 UTN server on the start page of the myUTN Control Center or in the device list in the InterCon-NetTool.

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

http://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 myUTN 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 UTN server restarts.
7.3 How to Backup Your Configuration

All settings of the UTN 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 UTN 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' ⇒ 73.

The Dongleserver myUTN-800 also has an automatic backup feature. It saves the parameter values, passwords and certificates installed on the UTN 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 UTN 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 UTN server if you use the automatic backup.

- See Parameter Values ⇒ 65
- Saving the Parameter File ⇒ 65
- Loading the Parameters File onto a UTN Server ⇒ 65
- Automatic Backup (myUTN-800 only) ⇒ 65

See Parameter Values
1. Start the myUTN Control Center.
2. Select MAINTENANCE – Parameter backup.
3. Click the icon .
   ↩ The current parameter values are displayed.

Saving the Parameter File
1. Start the myUTN 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 UTN Server
1. Start the myUTN Control Center.
2. Select MAINTENANCE – Parameter backup.
3. In the Parameter file box, specify the '<default name>_parameters.txt' file.
4. Click Import.
   ↩ The UTN server adopts the parameter values from the file.

Automatic Backup (myUTN-800 only)
✓ An SD card is connected to the UTN server.
1. Start the myUTN 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 UTN to its default values, e.g. if you want to install the UTN server in a different network. All settings will be set to factory settings. Installed certificates will not be deleted.

**Important:**
The connection to the myUTN Control Center may be interrupted if the IP address of the UTN server changes with the reset.

If required, determine the new IP address [18].

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

- **If you lost the password for the UTN Control Center, you can reset the UTN server via the reset button. You do not need a password to do so.**

**WARNING**
myUTN-800: Remove the SD card from the UTN server before resetting the parameters. Otherwise, the UTN server will adopt the parameter values stored on it (automatic backup [65]).

- Resetting Parameters via myUTN Control Center [66]
- Resetting Parameters via InterCon-NetTool [66]
- Resetting Parameters via Reset Button [67]

**Resetting Parameters via myUTN Control Center**
1. Start the myUTN 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 UTN server.
3. In 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 UTN server’s parameter values to their default settings.

1. Press the reset button for 5 seconds.
   The UTN server restarts.
   (The Dongleserver myUTN-800 beeps when it restarts.)
→ The parameters are reset.
8 Appendix

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

- Glossary ⇒ 69
- Troubleshooting ⇒ 70
- Parameter Lists ⇒ 73
- SEH UTN Manager – Feature Overview ⇒ 97
- Index ⇒ 99
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 UTN server, all integrated USB devices will be shown in the myUTN 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 UTN servers, you can identify a certain device with it.

The default name of the UTN 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 myUTN 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 UTN 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.

```
00-c0-eb-00-01-ff
```

Manufacturer ID  Device number

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

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

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

More information ⇒ 6.

**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 ⇒ 13.

**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 UTN servers.

More information ⇒ 8.
8.2 Troubleshooting

In this chapter, a few problems are described, explained and fixed.

Problem

- UTN Server: BIOS Mode ⇒ 870
- UTN Server: Connection Cannot Be Established ⇒ 870
- myUTN Control Center: Connection Cannot Be Established ⇒ 871
- myUTN Control Center: You Lost User Name and/or Password ⇒ 871
- SEH UTN Manager: A Connection to the USB device Cannot Be Established ⇒ 871
- SEH UTN Manager: USB Devices Are Not Shown ⇒ 871
- SEH UTN Manager: A USB Device Is Connected to the USB Port, but several USB Devices Are Displayed ⇒ 872
- SEH UTN Manager: Features Are Not Available or Deactivated ⇒ 872

Fix

**UTN Server: BIOS Mode**

The UTN server switches to the BIOS mode if the firmware works but the software is faulty. This may happen in the case of an incorrect software update, for example.

- The LEDs indicate the BIOS mode:
  - Status LED is off
  - Activity LED blinks periodically
- In addition, the UTN server can be found in the **BIOS Mode** filter in the InterCon-Net-Tool.

**WARNING**

The UTN server is not operational if it is in BIOS mode.

Follow the instructions below to remove the error.

To switch the UTN server from BIOS to normal mode, you have to first assign a temporary IP address to the device and then load software onto it. After the software update the UTN server switches to normal mode and will be assigned a new, permanent IP address.

1. Start the InterCon-NetTool
2. In the device list, select the UTN server.
   (You find the UTN-Server under the filter **BIOS Mode**.)
3. In the menu, select **Installation–IP Wizard**.
   Der IP Wizard is started.
4. Follow the instructions of the wizard in order to assign an IP address to the UTN server.
   The IP address is saved.
5. Update the UTN server’s software ⇒ 864.
   The software is saved in the UTN server.
   ⇣ The UTN server switches to normal mode.

**UTN Server: Connection Cannot Be Established**

You find the UTN server in the network and can reach it via TCP/IP connection. However, a connection via the SEH UTN Manager cannot be established.

Possible causes:
A firewall or some other security software blocks communication.
Add the UTN port respectively UTN SSL port as exception to your firewall or security software. Refer to the document-
ation of your firewall or security software on how to do this.

The port numbers in the SEH UTN Manager and on the UTN server are not identical: You changed the port number while SNMPv1 is deactivated, so that the change cannot be communicated to the SEH UTN Manager ⇒ 31.

**myUTN Control Center: Connection Cannot Be Established**

Eliminate possible error sources. Check:
- the cabling connections,
- the IP address of the UTN server ⇒ 18
- the proxy settings of your browser (refer to the documentation of your browser for more information)

If you still cannot establish any connection, the following safety mechanisms might be the cause:
- Access is protected via SSL/TLS (HTTPS) ⇒ 51.
- Access is protected via SSL/TLS (HTTPS) and you deleted the certificate (self-signed/CA/PKCS#12) ⇒ 56. Reset the UTN server to its default parameter values ⇒ 66. In the process, new certificates will be created.

**WARNING**

If you reset the device, all settings are lost and the IP address might change.
If required, determine the new IP address ⇒ 18.

- TCP port access control is enabled ⇒ 54.
- The cipher suites of the encryption level are not supported by the browser ⇒ 51.

**myUTN Control Center: You Lost User Name and/or Password**

If the access to the myUTN Control Center is protected but you have lost the access credentials, you can reset the UTN server to its default values. After the reset you can access the myUTN Control Center again, as it is not pro-
tected by default.

**WARNING**

If you reset the device, all settings are lost and the IP address might change.
If required, determine the new IP address ⇒ 18.

**SEH UTN Manager: A Connection to the USB device Cannot Be Established**

Possible causes:
- The USB port is already connected to another client.
  Wait until the other user terminates the connection or request the device ⇒ 38.
- The driver software for the USB device is not installed on the client.
  Install the driver software for your USB device. Refer to the documentation of your USB device on how to do this.

**SEH UTN Manager: USB Devices Are Not Shown**

Eliminate possible error sources: Check if the USB device is connected to the UTN server.
If the USB device is still not displayed, the following issues might be the cause:
- Several compound USB devices (⇒ 69) are connected to the UTN server. Each integrated USB device occu-
pies a virtual USB port of the UTN server. The number of these virtual USB ports is limited. If the limit is reached, no further USB devices can be used on this UTN server (⇒ 37).
• The USB port is deactivated ⇒ §30.
• The USB port key control is activated for the USB device ⇒ §55. Only once the key for the USB port is entered in the SEH UTN Manager, the USB port and the connected USB device appear.

SEH UTN Manager: A USB Device Is Connected to the USB Port, but several USB Devices Are Displayed
Possible causes:
• A USB hub is connected to the USB port of the UTN server.
• The connected USB device is a compound USB device (⇒ §69). It consists of a hub and one or more USB devices that are all integrated into a single housing. When the connection to the USB port is established, all displayed USB devices will be connected to the user’s client and can be used.

SEH UTN Manager: Features Are Not Available or Deactivated
Possible causes:
• Your client user account does not have the required administrative rights. This restricts user rights in the SEH UTN Manager as well. More details can be found in chapter ‘SEH UTN Manager – Feature Overview’ ⇒ §97. Start the SEH UTN Manager as administrator. Refer to the documentation of your operating system on how to do this.
• A function is not supported by the connected USB device (e.g. the ‘Print-On-Demand’ feature is not supported by a hard disk).
8.3 Parameter Lists

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

- Administration via email ⇞ 15
- Configuration backup (viewing, editing and loading parameters onto other devices) ⇞ 65

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

- Table 17 ‘Parameter list – IPv4’ ⇞ 74
- Table 18 ‘Parameter list – IPv6’ ⇞ 75
- Table 19 ‘Parameter list – DNS’ ⇞ 75
- Table 20 ‘Parameter list – SNMP’ ⇞ 76
- Table 21 ‘Parameter list – Bonjour’ ⇞ 77
- Table 22 ‘Parameter list – POP3 (only myUTN-80 and later)’ ⇞ 78
- Table 23 ‘Parameter list – POP3 (only myUTN-80 and later)’ ⇞ 79
- Table 24 ‘Parameter list – IPv4-VLAN (only myUTN-80 and later)’ ⇞ 81
- Table 25 ‘Parameter list – WLAN (myUTN-55 only)’ ⇞ 82
- Table 26 ‘Parameter list – Date/Time’ ⇞ 84
- Table 27 ‘Parameter list – Description’ ⇞ 84
- Table 28 ‘Parameter list – USB port’ ⇞ 84
- Table 29 ‘Parameter list – UTN port’ ⇞ 85
- Table 30 ‘Parameter list – Notification (only myUTN-80 and later)’ ⇞ 86
- Table 31 ‘Parameter list – Display (myUTN-800 only)’ ⇞ 89
- Table 32 ‘Parameter list – Acoustic signals (myUTN-800 only)’ ⇞ 89
- Table 33 ‘Parameter list – SSL/TLS connections’ ⇞ 90
- Table 34 ‘Parameter list – myUTN Control Center security’ ⇞ 91
- Table 35 ‘Parameter list – TCP port access’ ⇞ 93
- Table 36 ‘Parameter list – USB connection encryption’ ⇞ 94
- Table 37 ‘Parameter list – USB device type blocking’ ⇞ 94
- Table 38 ‘Parameter list – IPv4-VLAN (only myUTN-80 and later)’ ⇞ 94
- Table 39 ‘Parameter list – Authentication’ ⇞ 95
- Table 40 ‘Parameter list – Backup (myUTN-800 only)’ ⇞ 96
- Table 41 ‘Parameter list – Miscellaneous’ ⇞ 96
We recommend that you deactivate DHCP, BOOTP and ARP/PING as soon as the UTN server has received its IP address.
Table 18: Parameter list – IPv6

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the IPv6 functionality of the UTN server.</td>
</tr>
<tr>
<td>[IPv6]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv6_auto</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the automatic assignment of the IPv6 address to the UTN server.</td>
</tr>
<tr>
<td>[Automatic configuration]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[IPv6 address]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Every ‘n’ represents the hexadecimal value of one of the eight 16 bit elements of the address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Leading zeros can be omitted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>[Router]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv6_plen</td>
<td>0–64</td>
<td>64</td>
<td>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 '/'.</td>
</tr>
<tr>
<td>[Prefix length]</td>
<td>[1–2 characters; 0–9]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 19: Parameter list – DNS

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the name resolution via a DNS server.</td>
</tr>
<tr>
<td>[DNS]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dns_domain</td>
<td>max. 255 characters</td>
<td>[blank]</td>
<td>Defines the IP address of the primary DNS server.</td>
</tr>
<tr>
<td>[Domain name]</td>
<td>[a–z, A–Z, 0–9]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dns_primary</td>
<td>valid IP address</td>
<td>0.0.0.0</td>
<td>Defines the IP address of the secondary DNS server. The secondary DNS server is used if the first one is not available.</td>
</tr>
<tr>
<td>[Primary DNS server]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dns_secondary</td>
<td>valid IP address</td>
<td>0.0.0.0</td>
<td>Defines the domain name of an existing DNS server.</td>
</tr>
<tr>
<td>[Secondary DNS server]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Value</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>snmpv1 [SNMPv1]</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables SNMPv1.</td>
</tr>
<tr>
<td>snmpv1_ronly [Read-only]</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the write protection for the community.</td>
</tr>
<tr>
<td>snmpv1_community [Community]</td>
<td>max. 64 characters</td>
<td>public</td>
<td>SNMP community name Enter the name as it is defined in the monitoring station.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Important:</strong> 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.</td>
</tr>
<tr>
<td>snmpv3 [SNMPv3]</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables SNMPv3.</td>
</tr>
<tr>
<td>any_hash [Hash]</td>
<td>md5</td>
<td>md5</td>
<td>Specifies the hash algorithm for SNMP user group 1.</td>
</tr>
<tr>
<td>any_rights [Access rights]</td>
<td>readonly</td>
<td>readonly</td>
<td>Defines the access rights of the SNMP user group 1.</td>
</tr>
<tr>
<td>any_cipher [Encryption]</td>
<td>aes</td>
<td>aes</td>
<td>Defines the encryption method of the SNMP user group 1.</td>
</tr>
<tr>
<td>admin_hash [Hash]</td>
<td>md5</td>
<td>md5</td>
<td>Specifies the hash algorithm for SNMP user group 2.</td>
</tr>
<tr>
<td>admin_rights [Access rights]</td>
<td>readwrite</td>
<td>readwrite</td>
<td>Defines the access rights of the SNMP user group 2.</td>
</tr>
<tr>
<td>admin_cipher [Encryption]</td>
<td>aes</td>
<td>aes</td>
<td>Defines the encryption method of the SNMP user group 2.</td>
</tr>
</tbody>
</table>

**Important:**
The UTN server user accounts are also used as SNMP user accounts 23. Consider this when setting up user accounts.
### Table 21: Parameter list – Bonjour

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bonjour [Bonjour]</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables Bonjour.</td>
</tr>
<tr>
<td>bonjour_name [Bonjour name]</td>
<td>max. 64 characters [a–z, A–Z, 0–9]</td>
<td>[Default name]</td>
<td>Defines the Bonjour name of the myUTN server. The myUTN server uses this name to announce its Bonjour services. If no Bonjour name is entered, a default name will be used (device name@ICxxxxxx).</td>
</tr>
</tbody>
</table>
### Table 22: Parameter list – POP3 (only myUTN-80 and later)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pop3</code></td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the POP3 functionality.</td>
</tr>
<tr>
<td><code>pop3_srv</code></td>
<td>max. 128 characters</td>
<td>[blank]</td>
<td>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.</td>
</tr>
<tr>
<td><code>pop3_port</code></td>
<td>1–65535 [1–5 characters; 0–9]</td>
<td>110</td>
<td>Defines the port which the UTN server uses to receive emails. The default port number for POP3 is 110. The default port number for SSL/TLS (parameter 'POP3 – Security') is 995. If required, read the documentation of your POP3 server.</td>
</tr>
<tr>
<td><code>pop3_sec</code></td>
<td>0–2 [1 character; 0–2]</td>
<td>0</td>
<td>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. 0 = no security 1 = APOP 2 = SSL/TLS</td>
</tr>
<tr>
<td><code>pop3_poll</code></td>
<td>1–10080 [1–5 characters; 0–9]</td>
<td>2</td>
<td>Defines the time interval (in minutes) which with the POP3 server is checked for emails.</td>
</tr>
<tr>
<td><code>pop3_limit</code></td>
<td>0–4096 [1–4 characters; 0–9]</td>
<td>4096</td>
<td>Defines the maximum email size (in Kbyte) to be accepted by the UTN server. 0 = unlimited</td>
</tr>
<tr>
<td><code>pop3_usr</code></td>
<td>max. 128 characters</td>
<td>[blank]</td>
<td>Defines the user name used by the UTN server to log on to the POP3 server.</td>
</tr>
<tr>
<td><code>pop3_pwd</code></td>
<td>max. 128 characters</td>
<td>[blank]</td>
<td>Defines the user password used by the UTN server to log on to the POP3 server.</td>
</tr>
</tbody>
</table>
Table 23: Parameter list – POP3 (only myUTN-80 and later)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>smtp_srv [Server name]</td>
<td>max. 128 characters</td>
<td>[blank]</td>
<td>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.</td>
</tr>
<tr>
<td>smtp_port [Server port]</td>
<td>1–65535 1–5 characters; 0–9</td>
<td>25</td>
<td>Defines the port which the UTN server and SMTP server use to communicate. The default port number for SMTP is 25.</td>
</tr>
<tr>
<td>smtp_ssl [SSL/TLS]</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables SSL/TLS. SSL/TLS encrypts the communication from the UTN to the SMTP server. The encryption strength is defined via the encryption protocol and level.</td>
</tr>
<tr>
<td>smtp_sender [Sender name]</td>
<td>max. 128 characters</td>
<td>[blank]</td>
<td>Defines the email address used by the UTN server to send emails. Very often the name of the sender and the email account user name are identical.</td>
</tr>
<tr>
<td>smtp_auth [Login]</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables SNMP authentication (SMTP AUTH). To send emails, the UTN sends its user name and password to the SMTP server to authenticate itself. Enter user name (parameter SMTP – User name) and password (parameter SMTP – Password). Some SMTP servers require SMTP authentication to prevent fraudulent use (spam).</td>
</tr>
<tr>
<td>smtp_usr [User name]</td>
<td>max. 128 characters</td>
<td>[blank]</td>
<td>Defines the user name used by the UTN server to log on to the SMTP server.</td>
</tr>
<tr>
<td>smtp_pwd [Password]</td>
<td>max. 128 characters</td>
<td>[blank]</td>
<td>Defines the password used by the UTN server to log on to the SMTP server.</td>
</tr>
<tr>
<td>smtp_sign [Security (S/MIME)]</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the email security standard S/MIME (Secure/Multipurpose Internet Mail Extensions). S/MIME is used to sign (parameter SMTP – Signing emails) or encrypt (parameter SMTP – Full encryption) emails. Enable the desired feature (if desired with SMTP – Attach public key).</td>
</tr>
<tr>
<td>smtp_attpkey [Attach public key]</td>
<td>on/off</td>
<td>on</td>
<td>Sends the public key together with the email. Many email clients require the key to display the email.</td>
</tr>
</tbody>
</table>
### smtp_encrypt

**Value**  
on/off

**Default**  
off

**Description**  

- **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.

- **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.
### Table 24: Parameter list – IPv4-VLAN (only myUTN-80 and later)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip4vlan_mgmt</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the forwarding of IPv4 management VLAN data. If this option</td>
</tr>
<tr>
<td>[IPv4 management VLAN]</td>
<td></td>
<td></td>
<td>is enabled, SNMP is only available in the IPv4 management VLAN.</td>
</tr>
<tr>
<td>ip4vlan_mgmt_id</td>
<td>0–4096</td>
<td>0</td>
<td>ID for the identification of the IPv4 management VLAN.</td>
</tr>
<tr>
<td>[VLAN-ID]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip4vlan_mgmt_any</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the administrative access (web) to the UTN server via IPv4</td>
</tr>
<tr>
<td>[Access from any VLAN]</td>
<td></td>
<td></td>
<td>client VLANs. If this option is enabled, the UTN server can be administrated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>via all VLANs.</td>
</tr>
<tr>
<td>ip4vlan_mgmt_untag</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the administrative access to the UTN server via IPv4 packets</td>
</tr>
<tr>
<td>[Access via LAN (untagged)]</td>
<td></td>
<td></td>
<td>without tag. If this option is disabled, the UTN server can only be adminis-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>trated via VLANs.</td>
</tr>
<tr>
<td>ipv4vlan_on_1</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the forwarding of IPv4 client VLAN data.</td>
</tr>
<tr>
<td>~</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv4vlan_on_20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[VLAN]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv4vlan_addr_1</td>
<td>valid IP address</td>
<td>192.168.0.0</td>
<td>IP address of the UTN server within the IPv4 client VLAN.</td>
</tr>
<tr>
<td>~</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv4vlan_addr_20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[IP address]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv4vlan_mask_1</td>
<td>valid IP address</td>
<td>255.255.255.0</td>
<td>Subnet mask of the UTN server within the IPv4 client VLAN.</td>
</tr>
<tr>
<td>~</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv4vlan_mask_20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Subnet mask]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip4vlan_gate_1</td>
<td>valid IP address</td>
<td>0.0.0.0</td>
<td>IP gateway address in the IPv4 management VLAN. With a gateway, you can ad-</td>
</tr>
<tr>
<td>~</td>
<td></td>
<td></td>
<td>dress IP addresses from other networks.</td>
</tr>
<tr>
<td>ip4vlan_gate_20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Gateway]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv4vlan_id_1</td>
<td>0–4096</td>
<td>0</td>
<td>ID for the identification of the IPv4 client VLAN.</td>
</tr>
<tr>
<td>~</td>
<td>[1–4 characters; 0–9]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv4vlan_id_20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[VLAN-ID]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_2vlan_1</td>
<td>0–9</td>
<td>0</td>
<td>Allocates a VLAN to the USB port.</td>
</tr>
<tr>
<td>~</td>
<td>[1 character; 0–9]</td>
<td></td>
<td>0 = every 1 = VLAN 1 2 = VLAN 2  etc. 9 = none</td>
</tr>
<tr>
<td>utn_2vlan_20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Allocate VLAN]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 25: Parameter list – WLAN (myUTN-55 only)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wifi_mode</td>
<td>adhoc</td>
<td>infra</td>
<td>Defines the communication mode (network infrastructure):</td>
</tr>
<tr>
<td>[Mode]</td>
<td></td>
<td></td>
<td>• Ad hoc: Your WLAN is a decentralized ad-hoc-network in which devices communicate directly with each other (peer-to-peer).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Infrastructure: Your WLAN is an infrastructure network with an access point/router as central communication hub. The access point is connected</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>to the fixed network with a cable.</td>
</tr>
<tr>
<td></td>
<td>infra</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wifi_name</td>
<td>max. 64 characters</td>
<td>SEH</td>
<td>Enter your WLAN’s network name, also known as SSID (Service Set Identifier).</td>
</tr>
<tr>
<td>[Network name (SSID)]</td>
<td>a–z, A–Z, 0–9, _, -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wifi_channel</td>
<td>1–14</td>
<td>3</td>
<td>Enter your WLAN’s channel (frequency range). (Ad hoc mode only)</td>
</tr>
<tr>
<td></td>
<td>[1–2 characters; 0–9]</td>
<td></td>
<td>WARNING</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Only use WLAN channels authorized for your country!</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The UTN is an international product which supports a number of channels. Channels are statutorily regulated by national authorities. So the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UTN server might support channels which are forbidden to use in your country.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Inform yourself about national regulations.</td>
</tr>
<tr>
<td>wifi_encrypt</td>
<td>WepOpen</td>
<td>---</td>
<td>Select the encryption method that protects your WLAN.</td>
</tr>
<tr>
<td></td>
<td>TKIP</td>
<td></td>
<td>WepOpen = WEP (Open System)</td>
</tr>
<tr>
<td></td>
<td>AES</td>
<td></td>
<td>WepShared = WEP (Shared Key)</td>
</tr>
<tr>
<td></td>
<td>TKIP2</td>
<td></td>
<td>TKIP = WPA (TKIP)</td>
</tr>
<tr>
<td></td>
<td>AES2</td>
<td></td>
<td>AES = WPA (AES)</td>
</tr>
<tr>
<td></td>
<td>AESTKIP</td>
<td></td>
<td>TKIP2 = WPA2 (TKIP)</td>
</tr>
<tr>
<td></td>
<td>AESTKIP2</td>
<td></td>
<td>AES2 = WPA2 (AES)</td>
</tr>
<tr>
<td></td>
<td>Auto</td>
<td></td>
<td>AESTKIP = WPA (AES/TKIP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AESTKIP2 = WPA2 (AES/TKIP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Auto = WPA (automatic)</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>wifi_keyid</code></td>
<td>0–4</td>
<td>0</td>
<td>Defines the WEP key to be used.</td>
</tr>
<tr>
<td>[Use WEP key]</td>
<td>[1 character; 0–4]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 0 = no key
- 1 = key 1
- 2 = key 2
- 3 = key 3
- 4 = key 4

| `wifi_wkey1` | Depends on the key type. | [blank] | Defines the WEP keys. Four WEP keys are available. |
| `wifi_wkey4` | Number of characters: | | |
| [Key 1–4] | 64 ASCII | 5 |
| | 64 HEX | 10 |
| | 128 ASCII | 13 |
| | 128 HEX | 26 |

- Character set:
  - HEX = 0–9, a–f, A–F
  - ASCII = 0–9, a–z, A–Z

| `wifi_psk` | 8–63 characters | [blank] | Defines the Pre Shared Key (PSK) for Wi-Fi Protected Access (WPA). |
| [PSK] | | |

| `wifi_roaming` | on/off | off | Enables/disables roaming (switching from one access point/router to another): If your WLAN covers a widespread area with several access points/routers (with identical settings) and the UTN server changes position, the UTN server will automatically switch to the better signal without loss of connection if roaming is activated. (Infrastructure mode only) |
| [Roaming] | | | |

**Important:**

We recommend to use hexadecimal keys for WEP.

Some access points/routers convert WEP keys in ASCII format to hexadecimal format. In this case, the ASCII key on the UTN server and the hexadecimal key on the access point/router do not match.
### Table 26: Parameter list – Date/Time

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntp</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the use of a time server (SNTP).</td>
</tr>
<tr>
<td>Date/Time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ntp_server</td>
<td>max. 64 characters [a–z, A–Z, 0–9]</td>
<td>pool.ntp.org</td>
<td>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.</td>
</tr>
<tr>
<td>Time server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ntp_tzone</td>
<td>UTC, GMT, EST, EDT, CST, CDT, MST, MDT, PST, PDT, etc.</td>
<td>CET/CEST (EU)</td>
<td>Compensates Coordinated Universal Time (UTC) for location and national particularities (daylight saving time etc.).</td>
</tr>
<tr>
<td>Time zone</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Important:

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

### Table 27: Parameter list – Description

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys_name</td>
<td>max. 64 characters [a–z, A–Z, 0–9]</td>
<td>[blank]</td>
<td>Device name as alternative to IP address. With a name you can identify the UTN server more easily in the network, e.g. if you are using several UTN servers. Is displayed in the myUTN Control Center, SEH UTN Manager and InterCon-NetTool.</td>
</tr>
<tr>
<td>[Host name]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sys_descr</td>
<td>max. 64 characters [a–z, A–Z, 0–9]</td>
<td>[blank]</td>
<td>Device description, e.g. location or department. Is displayed in the myUTN Control Center, SEH UTN Manager and InterCon-NetTool.</td>
</tr>
<tr>
<td>[Description]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sys_contact</td>
<td>max. 64 characters [a–z, A–Z, 0–9]</td>
<td>[blank]</td>
<td>Contact person, e.g. device administrator. Is displayed in the myUTN Control Center.</td>
</tr>
<tr>
<td>[Contact person]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 28: Parameter list – USB port

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>utn_tag_1</td>
<td>max. 32 characters [a–z, A–Z, 0–9]</td>
<td>[blank]</td>
<td>Freely definable name of the USB port.</td>
</tr>
<tr>
<td>~</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_tag_20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Port name]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_poff_1</td>
<td>on/off</td>
<td>off</td>
<td>Disables/enables the power supply for the USB port (i.e. the USB device connected to the port). off = power on on = power off</td>
</tr>
<tr>
<td>~</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_poff_20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Port]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 29: Parameter list – UTN port

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>utn_port</td>
<td>1–9200</td>
<td>9200</td>
<td>Defines the number of the UTN port (for unencrypted connections).</td>
</tr>
<tr>
<td>[UTN port]</td>
<td>[1–4 characters; 0–9]</td>
<td></td>
<td><strong>WARNING</strong> The UTN port must not be blocked by security software (firewall).</td>
</tr>
<tr>
<td>utn_sslport</td>
<td>1–9443</td>
<td>9443</td>
<td>Defines the number of the UTN SSL port (for encrypted connections).</td>
</tr>
<tr>
<td>[UTN SSL port]</td>
<td>[1–4 characters; 0–9]</td>
<td></td>
<td><strong>WARNING</strong> The UTN SSL port must not be blocked by security software (firewall).</td>
</tr>
</tbody>
</table>
### Table 30: Parameter list – Notification (only myUTN-80 and later)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mailto_1</td>
<td>valid email address</td>
<td>[blank]</td>
<td>Email address of the recipient for notifications.</td>
</tr>
<tr>
<td>mailto_2</td>
<td>[Email address]</td>
<td>[max. 64 characters]</td>
<td></td>
</tr>
<tr>
<td>noti_stat_1</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the periodical sending of a status email to recipient 1 or 2.</td>
</tr>
<tr>
<td>noti_stat_2</td>
<td>[Status email]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>notistat_d</td>
<td>al</td>
<td>al</td>
<td>Defines the day (the interval) on which a status email is sent.</td>
</tr>
<tr>
<td>notistat_h</td>
<td>0–23</td>
<td>0</td>
<td>Specifies the time (hour) at which a status email is sent.</td>
</tr>
<tr>
<td>notistat_tm</td>
<td>0–5</td>
<td>0</td>
<td>Specifies the time (minute) at which a status email is sent.</td>
</tr>
<tr>
<td>noti_dev_1</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of emails after a USB device was connected/to.</td>
</tr>
<tr>
<td>noti_dev_2</td>
<td>[Send email if USB devices are connected or disconnected]</td>
<td></td>
<td>removed from the UTN server.</td>
</tr>
<tr>
<td>noti_act_1</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of emails after a USB port was activated/deactivated.</td>
</tr>
<tr>
<td>noti_act_2</td>
<td>[Send email if USB port is activated or deactivated]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Value</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>noti_pup_1</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of emails when the UTN server restarts.</td>
</tr>
<tr>
<td>noti_pup_2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Send email if UTN server is restarted]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>noti_pwr_1</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of emails when one of the two power supplies of the UTN server is interrupted or established. (myUTN-800 only)</td>
</tr>
<tr>
<td>noti_pwr_2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Send email if power supply is interrupted or established]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>noti_lnk_1</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of emails when one of the two network connection of the UTN server is interrupted or established. (myUTN-800 only)</td>
</tr>
<tr>
<td>noti_lnk_2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Send email if network connection is interrupted or established]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>noti_sdinout_1</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of emails after an SD card was connected to/removed from the UTN server. (myUTN-800 only)</td>
</tr>
<tr>
<td>noti_sdinout_2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Send email if SD card is connected or disconnected]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>noti_sdunusable_1</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of emails if the SD card is unusable. (myUTN-800 only)</td>
</tr>
<tr>
<td>noti_sdunusable_2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Send email if SD card cannot be used]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trapto_1</td>
<td>valid IP address</td>
<td>0.0.0.0</td>
<td>SNMP trap address of the recipient.</td>
</tr>
<tr>
<td>trapto_2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Address]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trapcommu_1</td>
<td>max. 64 characters</td>
<td>public</td>
<td>SNMP trap community of the recipient.</td>
</tr>
<tr>
<td>trapcommu_2</td>
<td>[a–z, A–Z, 0–9]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Community]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trapdev</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of SNMP traps after a USB device was connected to/removed from the UTN server.</td>
</tr>
<tr>
<td>[Send trap if USB devices are connected or disconnected]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trapact</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of SNMP traps after a USB port (i.e. the connection to the connected USB device) was activated/deactivated.</td>
</tr>
<tr>
<td>[Send trap if USB ports are activated or deactivated]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trappup</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of SNMP traps when the UTN server is restarted.</td>
</tr>
<tr>
<td>[Send trap if UTN server is restarted]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Value</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>trap_pwr</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of SNMP traps when one of the two power supplies of the UTN server is interrupted or established. (myUTN-800 only)</td>
</tr>
<tr>
<td>[Send trap if power supply is interrupted or established]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trap_lnk</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of SNMP traps when one of the two network connections of the UTN server is interrupted or established. (myUTN-800 only)</td>
</tr>
<tr>
<td>[Send trap if network connection is interrupted or established]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trap_sdinout</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of SNMP traps after an SD card was connected to/removed from the UTN server. (myUTN-800 only)</td>
</tr>
<tr>
<td>[Send trap if SD card is connected or disconnected]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trap_sdunusable</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the sending of SNMP traps if the SD card is unusable. (myUTN-800 only)</td>
</tr>
<tr>
<td>[Send trap if SD card cannot be used]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 31: Parameter list – Display (myUTN-800 only)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dis_def</td>
<td>1–2 characters</td>
<td>SD</td>
<td>Defines the name (ID) shown in the display panel on the front side of the UTN server.</td>
</tr>
<tr>
<td></td>
<td>[Identifier (display panel)]</td>
<td></td>
<td>[A–Z, 0–9; E+digit is not permitted because this combination is used for errors ⇒ §33.]</td>
</tr>
<tr>
<td>dis_pwr</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the display of error in the display panel if the UTN server only is supplied by one of the two power supplies. Errors are displayed in codes ⇒ §33.</td>
</tr>
<tr>
<td>disp_sdc</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the display of error messages in the display panel if no SD card is inserted into the UTN server or if the SD card cannot be used. Errors are displayed in codes ⇒ §33.</td>
</tr>
<tr>
<td>disp_lnk</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the display of error messages in the display panel if only one of the two network connections of the UTN server is established. Errors are displayed in codes ⇒ §33.</td>
</tr>
</tbody>
</table>

Table 32: Parameter list – Acoustic signals (myUTN-800 only)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>beepPwr</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the acoustic signal that sounds if the UTN server only is supplied by one of the two power supply.</td>
</tr>
<tr>
<td>beepSDc</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the acoustic signal that sounds if no SD card is inserted into the UTN server or if the SD card cannot be used.</td>
</tr>
<tr>
<td>beepLnk</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the acoustic signal that sounds if only one of the two network connections of the UTN server is established.</td>
</tr>
</tbody>
</table>
Table 33: Parameter list – SSL/TLS connections

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sslmethod</td>
<td>any</td>
<td>any</td>
<td>Defines the encryption protocol for SSL/TLS connections.</td>
</tr>
<tr>
<td>[Encryption protocol]</td>
<td>sslv3</td>
<td></td>
<td>any = at will (automatic negotiation)</td>
</tr>
<tr>
<td></td>
<td>tls10</td>
<td></td>
<td>ss lv3 = SSL 3.0</td>
</tr>
<tr>
<td></td>
<td>tls11</td>
<td></td>
<td>tls10 = TLS 1.0</td>
</tr>
<tr>
<td></td>
<td>tls12</td>
<td></td>
<td>tls11 = TLS 1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>tls12 = TLS 1.2</td>
</tr>
</tbody>
</table>

**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 myUTN Control Center (中国大陆), a connection cannot be established. Use TLS (and not SSL).

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>security</td>
<td>1–4</td>
<td>4</td>
<td>Defines the encryption level for SSL/TLS connections.</td>
</tr>
<tr>
<td>[Encryption level]</td>
<td>[1 character; 1–4]</td>
<td></td>
<td>1 = low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 = medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 = high</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 = any (automatic negotiation)</td>
</tr>
</tbody>
</table>

**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 myUTN Control Center (中国大陆), a connection cannot be established. Use an encryption level as high as possible.

**WARNING**

The SEH UTN Manager does not support the encryption level Low. If you set up Low in combination with an encrypted USB connection, a connection cannot be established. Use an encryption level as high as possible.
### Table 34: Parameter list – myUTN Control Center security

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| http_allowed             | on/off                                      | on      | Defines the connection type (HTTP/HTTPS) to be used for connecting to the myUTN Control Center.:
|                          |                                            |         | on = HTTP/HTTPS
|                          |                                            |         | off = HTTPS only
<p>|                          |                                            |         | The encryption strength is defined via the encryption protocol and level $\Rightarrow $51.                                                                                                                   |
| sessKeys                 | on/off                                      | off     | Enables/disables the myUTN Control Center user accounts. If they are enabled, a login screen is displayed when opening the myUTN Control Center.                                                                 |
| admin_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 $\Rightarrow $23.                                                                                                                               |
| admin_pwd                | 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 $\Rightarrow $23.                                                                                                                               |
| any_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 $\Rightarrow $23.                                                                                                                                   |</p>
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any_pwd</td>
<td>max. 64 characters</td>
<td>[blank]</td>
<td>Defines the password for the read-only user account.</td>
</tr>
<tr>
<td>[Read-only user – Password]</td>
<td></td>
<td></td>
<td>Important: Also is the password of the SNMPv3 user account ⇐ 23.</td>
</tr>
<tr>
<td>sessKeyULList</td>
<td>on/off</td>
<td>on</td>
<td>Defines the type of login screen.</td>
</tr>
<tr>
<td>[Login screen displays]</td>
<td></td>
<td></td>
<td>on= Shows a user list, only password must be entered</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>off= neutral login mask, user name and password must be entered</td>
</tr>
<tr>
<td>sessKeyTimer</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the session timeout.</td>
</tr>
<tr>
<td>[Session timeout]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sessKeyTimeout</td>
<td>120–3600</td>
<td>600</td>
<td>Time in seconds after which the timeout is to be effective.</td>
</tr>
<tr>
<td>[Session timeout]</td>
<td>[3–4 characters; 0–9]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 35: Parameter list – TCP port access

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protection [Port access control]</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables the blocking of selected ports and thus connections to the UTN server.</td>
</tr>
<tr>
<td>protection_level [Security level]</td>
<td>protec_utn</td>
<td>protec_utn</td>
<td>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)</td>
</tr>
<tr>
<td>ip_filter_on_1 ~ ip_filter_on_8</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables an exception from the port locking.</td>
</tr>
<tr>
<td>ip_filter_1 ~ ip_filter_8 [IP address]</td>
<td>valid IP address</td>
<td>[blank]</td>
<td>Defines networks elements that are excluded from port blocking via their IP address.</td>
</tr>
<tr>
<td>hw_filter_on_1 ~ hw_filter_on_8</td>
<td>on/off</td>
<td>off</td>
<td>Enables/disables an exception from the port locking.</td>
</tr>
<tr>
<td>hw_filter_1 ~ hw_filter_8 [MAC address]</td>
<td>valid hardware address</td>
<td>00:00:00:00:00</td>
<td>Defines elements that are excluded from port locking using the MAC address (hardware address).</td>
</tr>
<tr>
<td>protection_test [Test mode]</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the test mode.</td>
</tr>
</tbody>
</table>

**Important:**
The use of wildcards (*) allows you to define subnetworks.

**Important:**
MAC addresses are not delivered through routers!

**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 UTN 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 36: Parameter list – USB connection encryption

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

### Table 37: Parameter list – USB device type blocking

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>utn_hid</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the blocking of input devices (HID – human interface devices). on = no blocking off = blocking</td>
</tr>
<tr>
<td>[Disable input devices (HID class)]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 38: Parameter list – IPv4-VLAN (only myUTN-80 and later)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>utn_accctrt_1</td>
<td>---</td>
<td>---</td>
<td>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</td>
</tr>
<tr>
<td>~</td>
<td>ids</td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_accctrt_20</td>
<td>key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Method]</td>
<td>keyids</td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_keyval_1</td>
<td>max. 64 characters</td>
<td>[blank]</td>
<td>Defines the key for the USB port and the connected USB device when port key control is used.</td>
</tr>
<tr>
<td>~</td>
<td>[a–z, A–Z, 0–9]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_keyval_20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Key]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_vendprodIDs_1</td>
<td></td>
<td></td>
<td>Defines the VID (Vendor ID) and PID (Product ID) of the USB device that is assigned to the USB port via the device assignment.</td>
</tr>
<tr>
<td>~</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_vendprodIDs_20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[USB device]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Often VID and PID of a USB device are unknown. We recommend configuration via the myUTN Control Center because VID and PID will be automatically determined and entered with this method.*
Table 39: Parameter list – Authentication

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth_typ [Authentication method]</td>
<td>---</td>
<td>---</td>
<td>Defines the authentication method used in your network in which the UTN server is to participate.</td>
</tr>
<tr>
<td></td>
<td>MD5</td>
<td></td>
<td>--- = none</td>
</tr>
<tr>
<td></td>
<td>TLS</td>
<td></td>
<td>MD5 = EAP-MD5</td>
</tr>
<tr>
<td></td>
<td>TTLS</td>
<td></td>
<td>TLS = EAP-TLS</td>
</tr>
<tr>
<td></td>
<td>PEAP</td>
<td></td>
<td>TTLS = EAP-TTLS</td>
</tr>
<tr>
<td></td>
<td>FAST</td>
<td></td>
<td>PEAP = PEAP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FAST = EAP-FAST</td>
</tr>
<tr>
<td>auth_name [User name]</td>
<td>max. 64 characters</td>
<td>[blank]</td>
<td>Defines the user name with which the UTN server is set up on the RADIUS server for the EAP authentication methods MD5, TTLS, PEAP, and FAST.</td>
</tr>
<tr>
<td></td>
<td>[a–z, A–Z, 0–9]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>auth_pwd [Password]</td>
<td>max. 64 characters</td>
<td>[blank]</td>
<td>Defines the password with which the UTN server is set up on the RADIUS server for the EAP authentication methods MD5, TTLS, PEAP, and FAST.</td>
</tr>
<tr>
<td></td>
<td>[a–z, A–Z, 0–9]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>auth_intern [Inner authentication]</td>
<td>---</td>
<td>---</td>
<td>Defines the kind of inner authentication for the EAP authentication methods TTLS, PEAP, and FAST.</td>
</tr>
<tr>
<td></td>
<td>PAP</td>
<td></td>
<td>--- = none</td>
</tr>
<tr>
<td></td>
<td>CHAP</td>
<td></td>
<td>PAP = PAP</td>
</tr>
<tr>
<td></td>
<td>MSCHAP2</td>
<td></td>
<td>CHAP = CHAP</td>
</tr>
<tr>
<td></td>
<td>EMD5</td>
<td></td>
<td>MSCHAP2 = MS-CHAPv2</td>
</tr>
<tr>
<td></td>
<td>ETLS</td>
<td></td>
<td>EMD5 = EAP-MD5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ETLS = EAP-TLS</td>
</tr>
<tr>
<td>authExtern [PEAP/EAP-FAST options]</td>
<td>---</td>
<td>---</td>
<td>Defines the kind of external authentication for the EAP authentication methods TTLS, PEAP, and FAST.</td>
</tr>
<tr>
<td></td>
<td>PLABEL0</td>
<td></td>
<td>--- = none</td>
</tr>
<tr>
<td></td>
<td>PLABEL</td>
<td></td>
<td>PLABEL0 = PEAPLABEL0</td>
</tr>
<tr>
<td></td>
<td>PVER0</td>
<td></td>
<td>PLABEL1 = PEAPLABEL1</td>
</tr>
<tr>
<td></td>
<td>PVER1</td>
<td></td>
<td>PVER0 = PEAPVER0</td>
</tr>
<tr>
<td></td>
<td>FPROV1</td>
<td></td>
<td>PVER1 = PEAPVER1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FPROV1 = FASTPROV1</td>
</tr>
<tr>
<td>auth_ano_name [Anonymous name]</td>
<td>max. 64 characters</td>
<td>[blank]</td>
<td>Defines the anonymous name for the unencrypted part of the EAP authentication methods TTLS, PEAP, and FAST.</td>
</tr>
<tr>
<td></td>
<td>[a–z, A–Z, 0–9]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>auth_wpa_addon [WPA Add on]</td>
<td>max. 255 characters</td>
<td>[blank]</td>
<td>Defines an optional WPA expansion for the EAP authentication methods TTLS, PEAP, and FAST.</td>
</tr>
<tr>
<td></td>
<td>[a–z, A–Z, 0–9]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 40: Parameter list – Backup (myUTN-800 only)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoSync</td>
<td>on/off</td>
<td>on</td>
<td>Enables/disables the automatic backup of parameter values, passwords, and certificates to a connected SD card.</td>
</tr>
</tbody>
</table>

### Table 41: Parameter list – Miscellaneous

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>utn_heartbeat</td>
<td>1–1800</td>
<td>180</td>
<td><strong>WARNING</strong> This parameter can only be used after consultation with the SEH support team.</td>
</tr>
<tr>
<td>~</td>
<td>[1–4 characters; 0–9]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_poffdura_1</td>
<td>0–100</td>
<td>0</td>
<td><strong>WARNING</strong> This parameter can only be used after consultation with the SEH support team.</td>
</tr>
<tr>
<td>~</td>
<td>[1–3 characters; 0–9]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_prerest_1</td>
<td>on/off</td>
<td>off</td>
<td><strong>WARNING</strong> This parameter can only be used after consultation with the SEH support team.</td>
</tr>
<tr>
<td>~</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>utn_prerest_20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
8.4 SEH UTN Manager – Feature Overview

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

- Selection list mode
  - global
  - user
- Client operating system (Windows, 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 UTN server model does not support them
- the USB device connected does not support them
- security measures have been implemented

Table 42: SEH UTN Manager – Feature overview Windows

<table>
<thead>
<tr>
<th>Menu</th>
<th>Global Selection List</th>
<th>User Selection List</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Administrator</td>
<td>User</td>
</tr>
<tr>
<td>Selection List – Edit</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Selection List – Export</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Selection List – Refresh</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UTN Server – Configure</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UTN Server – Set IP Address</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UTN-Server – Activate Auto-Connect</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>USB Server – Set USB Port Keys</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>UTN Server – Add</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>UTN Server – Remove</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>UTN Server – Refresh</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Port – Activate</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Port – Deactivate</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Port – Request</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Port – Remove</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Port – Create UTN Action</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Port – Settings</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### Buttons

<table>
<thead>
<tr>
<th>Buttons</th>
<th>Administrator</th>
<th>User</th>
<th>Administrator</th>
<th>User (read/write *.ini)</th>
<th>User (no read/write *.ini)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection List – Refresh</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Selection List – Edit</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Port – Activate</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Port – Deactivate</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

### 'Program – Options' dialog

<table>
<thead>
<tr>
<th>'Program – Options' dialog</th>
<th>Administrator</th>
<th>User</th>
<th>Administrator</th>
<th>User (read/write *.ini)</th>
<th>User (no read/write *.ini)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Scan – Multicast Search</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Network Scan – IP Range Search</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Program – Program Language</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Program – Program Messages</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Program – Program Update</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Automatisms – Program Start (Autostart)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Automatisms – Auto-Disconnect</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Selection List – Selection List Mode</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Selection List – Automatic Refresh</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

### 'Port Settings' dialog

<table>
<thead>
<tr>
<th>'Port Settings' dialog</th>
<th>Administrator</th>
<th>User</th>
<th>Administrator</th>
<th>User (read/write *.ini)</th>
<th>User (no read/write *.ini)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic device connection – Print-On-Demand</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Plugin mode</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Messages</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
8.1 Index

A
Acoustic Signals 32
Ad hoc mode 21, 82
Administration
  email 15
  InterCon-NetTool 13
  myUTN Control Center 6
  remote access 15
  SEH UTN Manager 8
Administrator 53
Authentication 60
Auto-Connect 39
Auto-Disconnect 39
Automatic connection 39
Automatism
  Print-On-Demand 40
Automatisms
  Auto-Connect 39
  Auto-Disconnect 39
  UTN Action 40

B
Backup 65
BadUSB 56
Bonjour 24
BOOTP (Bootstrap Protocol) 18
Brochures 3
Browser 6
Button 66
  restart 64

C
CA (certification authority) 56
CA certificate 56
Certificate 56
  CA 56
  client 56
  create 57
  default 57
  delete 60
  management 56
  request 58
requested 56
S/MIME 56
self-signed 56
view 57
Certificate
  PKCS#12 56
Certification authority 56
Cipher Suite 51
Client certificate 56
Command-line interface 45
Communication mode 21, 82
Complete version 9
Compound USB device 37, 69
Configuration backup 65
Connection
  encryption 51
  myUTN Control Center 51
Contact 4
Contact person 30

D
Default certificate 57
Default name 69
Description 29
Device
  contact person 30
  description 30
  name 30, 69
  number 69
  time 29
Device number 69
DHCP (Dynamic Host Configuration Protocol) 18
Display Panel 33
Display panel
  error codes 33
  Identifier 33
Display. See display panel.
DNS (Domain Name Service) 23
Documentation 3
  further applicable documents 3
  mark-ups 3
  symbols 3
Downloads 4
myUTN User Manual Windows

E
EAP (Extensible Authentication Protocol) 60
FAST (Flexible Authentication via Secure Tunneling) 62
MD5 (Message Digest #5) 60
PEAP (Protected Extensible Authentication Protocol) 61
TLS (Transport Layer Security) 60
TTLS (Tunneled Transport Layer Security) 61

Email 31
Administration 15
event 31
notifications 31
POP3 25
SMTP 25
status 31

Encryption 49
cipher suite 51
email 51
HTTP 51
level 51
POP3 51
protocol 51
SMTP 51
SSL/TLS 49
strength 51
USB connection 51
web access 51

Error codes 33
Error states 33
Ethernet address 69
Event notification 31

F
Factory default settings 66
Feedback
acoustic 32
visual 33

File `<Default-Name_parameter.txt>` 65
Firmware/software 64
Frequency range 22, 82
Further applicable documents 3

G
Gateway 18
Global selection list 43
myUTN User Manual Windows

Monitoring 23
Multicast search 35
myUTN Control Center 6
  Controls 7
    encrypted connection 51
    user accounts 53

N
Network list 35
Notification service 31
Notifications 31

O
Online help 3
Open 3
Open source licenses 3

P
Parameters 73
  backup 65
  default values 66
  edit 65
  file 65
  lists 73
  load 65
  see 65
Password 53
  lost 66
Physical address 69
PKCS#12 certificate 56
PKI (public key infrastructures) 57
Point-to-point connection 37
POP3 (Post Office Protocol Version 3) 25
Port blocking 54
Port connection 8
  activate 37
  deactivate 38
Print job 40
Print-On-Demand 40
Product information 3, 4
Protection mechanisms 49

Q
Quick Installation Guide 3

R
Read-only user 53
Release request 38
Remote access 15
Repairs 5
Requested certificate 56
Reset 66
  button 66
  remote access 66
reset button 66
Restart 64

S
S/MIME certificate 56
Safety regulations 4
Script 40, 45
SD card 65
  automatic backup 65
  transfer settings 65
Security level 54
Security mechanisms 49
SEH UTN Manager 8, 35, 69
  complete version 9
  feature overview 97
  features 8
  install 10
  minimal version 9
  selection list 42
  start 12
  versions 9
  without graphical user interface 45
SEH UTN Service 9
Selection List 35, 42
Selection list
  global 42
  user 42
Self-signed certificate 56
Session timeout 53
Settings
  backup 65
  transfer 65
SMTP (Simple Mail Transfer Protocol) 25
SNMP
  Community 23
  SNMP (Simple Network Management Protocol) 23
Virtual USB ports 37
VLAN (Virtual Local Area Network) 27
  IPv4 client VLAN 27
  IPv4 management VLAN 27
  USB ports 27

W
  Warnings 4
  Website 4

WLAN 21
  authentication method 22
  channel 22
  encryption method 22
  mode 21
  Network name 21
  roaming 22
  SSID 21
  standards 21

Z
  Zeroconf 18