USB Device Server

myUTN-50a
myUTN-55
myUTN-250
Dongleserver myUTN-80
Dongleserver myUTN-800





User Manual Linux

Manufacturer:
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.de

Scan this QR code (meCard) using your smart phone.

Document:
Type: User Manual Linux
Title: USB Device Server
Version: 3.5

Online Links to Important Websites:

Free Guarantee Extension:	http://www.seh-technology.com/guarantee
Support Contacts & Information:	http://www.seh-technology.com/support
Sales Contacts & Information:	http://www.seh-technology.com/sales
Downloads:	http://www.seh-technology.com/services/downloads.html

Table of Contents

1 General Information

This chapter contains information concerning the device and the documentation as well as notes about your safety.
You will learn how to benefit from your UTN server and how to operate the device properly.

What Information Do You Need?

1.1 myUTN

Purpose

myUTN (myUSB to Network) allows you to access non-network-ready USB devices (e.g. hard disks, printers, etc.) in the network. The USB devices will be connected to the USB port of the UTN server.

The 'Dongleservers' (myUTN-80 and myUTN-800) are exclusively designed for the deployment of USB dongles.

The software tool 'SEH UTN Manager' handles the access of the USB devices. The software is installed on all clients that are meant to access a USB device in the network. The SEH UTN Manager shows the availability of all UTN servers in the network and establishes a connection between the client and the USB port including the connected USB device.

System Requirements

myUTN has been designed for the use in TCP/IP-based networks. The SEH UTN Manager has been designed for the use in the following systems:

- Windows XP or later
- OS X 10.8.x or later
- Ubuntu 12.04.x LTS (64-bit), Ubuntu 14.04.x LTS (64-bit) or Oracle (64-bit) Linux 6.5 with Linux kernel 2.6.32 or higher, glibc 2.11.1 or higher and OpenSSL 1.0.1 or higher

This document describes the usage in Linux environments. Information about the usage in other environments can be found in the relevant system-specific User Manual. For further information; see: 'Documentation' ⇨🗎8.

Procedure and Basic Functions

After the SEH UTN Manager is started, the network will be scanned for connected UTN servers. The network range to be scanned is freely definable.

All UTN servers found will be shown in the 'network list' together with the connected USB devices. The required UTN servers will be selected and added to the 'selection list'. The UTN servers listed in the selection list can then be used by the user. To use a USB device, the user establishes a connection between the client and the USB port of the UTN server to which the USB device is connected.

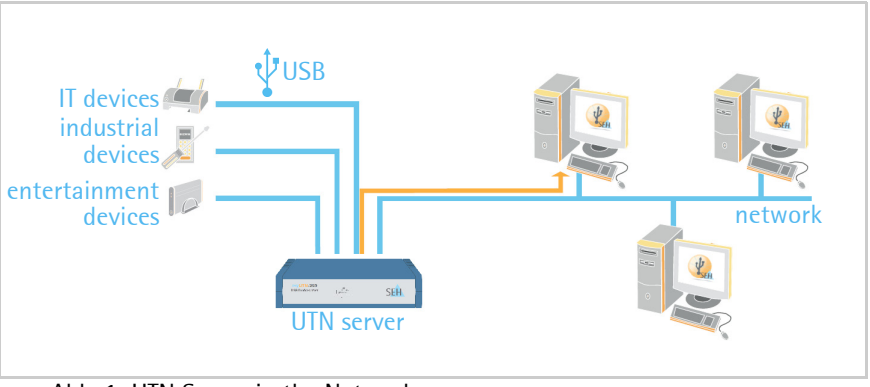


Abb. 1: UTN Server in the Network

Types and number of the USB devices to be connected can be found in the respective 'Quick Installation Guide'.

1.2 Documentation

Scope and Content

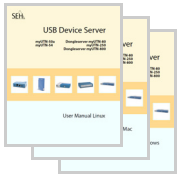
This documentation describes several versions of the USB Deviceserver as well as the Dongleservers. This means that functions will be described that may not be applicable to your product. Some illustrations may differ from your device.

Refer to the data sheet of your UTN server model for information about the functional range of your product. Please note the following names of the product categories in this documentation:

- USB Deviceserver → UTN server
- Dongleserver → UTN server
- dongle → USB device

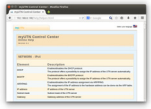
Structure of the Documentation

The myUTN documentation consists of the following documents:



User Manual
Detailed description of the myUTN configuration and administration. System-specific instructions for the following systems:
- Windows
- Mac
- Linux

Quick Installation Guide
Information about security, hardware installation, and the initial operation procedure.



Online Help (myUTN Control Center)
The Online Help contains detailed information about how to use the 'myUTN Control Center'.

Online Help (SEH UTN Manager)
The Online Help contains detailed information about how to use the software tool 'SEH UTN Manager'.

Document Features

This documentation has been designed as an electronic document for screen use. Many programs (e.g. Adobe® Reader®) offer a book-

mark navigation feature that allows you to view the entire document structure.

This document contains hyperlinks to the associated information units. If you want to print this documentation, we recommend using the printer setting 'Duplex' or 'Booklet'.

Terminology Used in this Document

The explanation of technical terms used in this document is summarized in a glossary. The glossary provides a quick overview of technical matters and background information; see: ⇨118.

Symbols and Conventions

A variety of symbols are used within this document. Their meaning is listed in the following table:

Table 1: Conventions within the documentation

Symbol / Convention	Description
 **Warning**	A warning contains important information that must be heeded. Non-observance may lead to malfunctions.
 Note	A notice contains information that should be heeded.
 Proceed as follows: 1. *Mark...*	The 'hand' symbol marks the beginning of instructions. Individual instructions are set in italics.
 Confirmation	The arrow confirms the consequence of an action.
☑ Requirements	Hooks mark requirements that must be met before you can begin the action.
☐ Option	A square marks procedures and options that you can choose.
•	Eye-catchers mark lists.
	This sign indicates the summary of a chapter.
⇨ 	The arrow marks a reference to a page within this document. In the PDF file, you can jump to this page by clicking the symbol.
Bold	Established terms (of buttons or menu items, for example) are set in bold.
`Courier`	Command lines are set in Courier font.
'Proper names'	Proper names are put in inverted commas

1.3 Support and Service

Support

If questions remain, please contact our hotline. SEH Computertechnik GmbH offers extensive support.

Monday through Thursday Friday	from 8:00 a.m. to 4:45 p.m. and from 8:00 a.m. to 3:15 p.m. (CET)
+49 (0)521 94226-44	
support@seh.de	

Current Services

The following services can be found on the homepage of SEH Computertechnik GmbH http://www.seh-technology.com :

- current firmware/software
- current tools
- current documentation
- current product information
- product data sheets
- and much more

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.

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. SEH Computertechnik GmbH will not accept any liability for loss of data, property damages and consequential damages resulting from the non-observance of the mentioned safety regulations and warnings.

Intended Use

The UTN serveris used in TCP/IP networks. myUTN allows you to access non-network-ready USB devices in the network. The UTN server has been designed for use in office environments.

Improper Use

All uses of the device that do not comply with the myUTN functionalities described in the documentation are regarded as improper uses. It is not allowed to make modifications to the hardware and software or to try to repair the device.

Safety Regulations

Before starting the initial operation procedure of the UTN server, please note the safety regulations in the 'Quick Installation Guide'. The Quick Installation Guide is enclosed in the packaging.

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!

1.5 First Steps

This section provides all the information that you need for a fast operational readiness.

Proceed as follows:

1. *Read and observe the security regulations in order to avoid damages to people and devices; see: ⇨🗎**12**.*
2. *Carry out the hardware installation. The hardware installation comprises the connection of the UTN server to the network, the USB device and the power supply; see: 'Quick Installation Guide'.*
3. *Make sure that an IP address is stored in the UTN server; see: ⇨🗎**14**.*
4. *Install and start the software tool 'SEH UTN Manager' on your Windows client; see: ⇨🗎**21**.*
5. *Add the UTN servers that you want to use to the selection list; see: ⇨🗎**62**.*
6. *Activate the connection between your client and the USB port to which the USB device is connected; see: ⇨🗎**63**.*

The connection will be established. The USB device can be used by the client.

1.6 Saving the IP Address in the UTN Server

Why IP Addresses?

An IP address is used to address network devices in an IP network. TCP/IP network protocols require the storing of the IP address in the UTN server so that the device can be addressed within the network.

How Does the UTN Server Obtain IP Addresses?

The UTN server is able to assign itself an IP address during the initial installation. Boot protocols are used to assign an IP address automatically to the UTN server. Upon delivery, the boot protocols 'BOOTP' and 'DHCP' are enabled.

Once the UTN server is connected to the network, it checks whether an IP address can be obtained from the boot protocols BOOTP or DHCP. If this is not the case, the UTN server assigns itself an IP address from the address range (169.254.0.0/16) which is reserved for ZeroConf.

Once the UTN server has automatically received an IP address via a boot protocol, you can save a freely definable IP address in the UTN server. The UTN server's assigned IP address can be determined and changed using the software tool 'SEH UTN Manager'; see: ⇨🗎18.

Different methods for the assignment of the IP address are described in the following.

Automatic Methods of IP Address Assignments

- 'ZeroConf' ⇨🗎15
- 'BOOTP' ⇨🗎15
- 'DHCP' ⇨🗎15
- 'Auto Configuration (IPv6 Standard)' ⇨🗎16

Manual Methods of IP Address Assignments

- 'SEH UTN Manager' ⇨🗎16
- 'myUTN Control Center' ⇨🗎16
- 'ARP/PING' ⇨🗎17

ZeroConf

If no IP address can be assigned via boot protocols, the UTN server assigns itself an IP address via ZeroConf. For this purpose, the UTN server picks an IP address at random from the address range (169.254.0.0/16) which is reserved for ZeroConf.

You can use the domain name service of Bonjour for the name resolution of the IP address; see: ⇨🗎39.

BOOTP

The UTN server supports BOOTP, which means that the IP address of the UTN server can be assigned via a BOOTP server.

Requirements

☑ The 'BOOTP' parameter has been enabled, see: ⇨🗎33.

☑ A BOOTP server is available in the network.

If the UTN server is connected, it asks the BOOTP host for the IP address and the host name. The BOOTP host answers and sends a data packet containing the IP address. The IP address is saved in the UTN server.

DHCP

The UTN server supports DHCP, which means that the IP address of the UTN server can be assigned dynamically via a DHCP server.

Requirements

☑ The 'DHCP' parameter has been enabled, see: ⇨🗎33.

☑ A DHCP server is available in the network.

After the hardware installation, the UTN server asks a DHCP server for an IP address by means of a broadcast query. The DHCP server identifies the UTN server on the basis of its hardware address and sends a data packet to the UTN server.

This data packet contains, among others, the IP address of the UTN server, the default gateway, and the IP address of the DNS server. The data is saved in the UTN server.

Auto Configuration (IPv6 Standard)

The UTN server can have an IPv4 address and several IPv6 addresses at the same time. The IPv6 standard is used to automatically assign IP addresses in IPv6 networks. When connected to an IPv6 network, the UTN server will automatically obtain an additional 'link-local' IP address from the IPv6 address range.

The UTN server uses the 'link-local' IP address to search for a router. The UTN server sends so-called 'router solicitations' (RS) to the special multicast address FF02::2. The available router will then return a 'Router Advertisement' (RA) containing the required information.

With a prefix from the range of the global unicast addresses, the UTN server can compose its own address. It simply replaces the first 64 bits (prefix FE80::) with the prefix that was sent in the RA.

Requirements

☑ The 'IPv6' parameter has been activated.

☑ The 'Automatic configuration' parameter has been activated.

To configure the assignment of IPv6 addresses, see: ⇨🗎35.

SEH UTN Manager

You can manually enter the desired IPv4 address and save it in the UTN server using the SEH UTN Manager. To configure an IPv4 address via the SEH UTN Manager, see: ⇨🗎34.

myUTN Control Center

You can manually enter the desired IP address and save it in the UTN server using the myUTN Control Center.

- To configure an **IPv4** address via the myUTN Control Center, see: ⇨🗎33.
- To configure an **IPv6** address via the myUTN Control Center, see: ⇨🗎35.

ARP/PING

The assignment of the IP address to the hardware address can be done via the ARP table. The ARP table is an internal system file in which the assignment is temporarily saved (about 15 min). This table is administered by the ARP protocol.

By means of the 'arp' and 'ping' commands, you can save the IP address in the UTN server. If the UTN server already has an IP address, the 'arp' and 'ping' commands cannot be used to save a new IP address.

However, an IP address from the address range (169.254.0.0/16) which is reserved for ZeroConf can be overwritten by means of the 'arp' and 'ping' commands.

The 'arp' command is used for editing the ARP table. The 'ping' command transfers a data packet containing the IP address to the hardware address of the UTN server. If the data packet has been successfully sent and received, the UTN server permanently saves the IP address.

The implementation of the 'arp' and 'ping' command depends on the system used. Read the documentation for your operating system.

Requirements

☑ The 'ARP/PING' parameter has been enabled, see: ⇨📄34.

Edit the ARP table:
Syntax: `arp -s <IP address> <hardware address>`
Example: `arp -s 192.168.0.123 00:c0:eb:00:01:ff`

Assign a new IP address to the UTN server:
Syntax: `ping <IP address>`
Example: `ping 192.168.0.123`

2 Administration Methods

You can administer and configure the UTN server in a number of ways. The following chapter gives you an overview of the various administration options.

You will get information on when to use these methods and which functions these methods support.

What Information Do You Need?

- 'Administration via myUTN Control Center' ⇨19
- 'Administration via the SEH UTN Manager' ⇨21
- 'Administration via E-Mail (only myUTN-80 and later)' ⇨30

2.1 Administration via myUTN Control Center

Which Functions Are Supported?

The myUTN Control Center includes all features for the administration and monitoring of the UTN server.

The myUTN Control Center is stored in the UTN server and can be displayed by means of a browser software (e.g. Mozilla Firefox).

Requirements

☑ The UTN server is connected to the network and the mains voltage.

☑ The UTN server has a valid IP address.

Starting the myUTN Control Center

Proceed as follows:

1. *Open your browser.*
2. *Enter the IP address of the UTN server as the URL.*

↳ The **myUTN Control Center** appears.

If the myUTN Control Center is not displayed, check the proxy settings of your browser.

You can also start the myUTN Control Center via the software tool 'SEH UTN Manager': Mark the UTN server in the selection list and select **UTN server –Configure** from the menu bar.

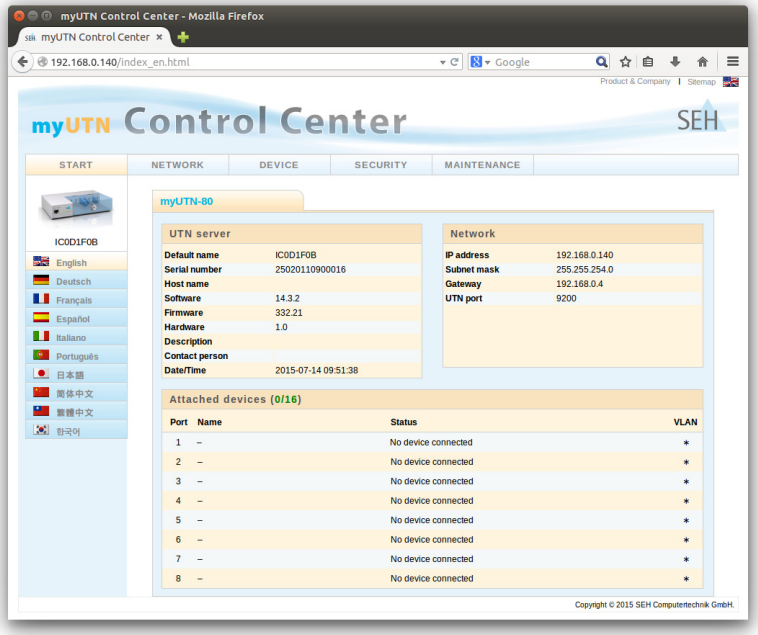


Abb. 2: myUTN Control Center - START

Structure of the myUTN Control Center

The available menu items are located in the navigation bar (top). After selecting a menu item (simple mouse click), the available submenu items are displayed at the left. After selecting a submenu item, the corresponding page with its content is displayed (at the right).

You can set the language via the menu item **START**. Simply select the relevant flag.

The manufacturer's contact details and additional information regarding the product are displayed under **Product & Company** The **Sitemap** provides an overview of and direct access to all pages of the myUTN Control Center.

All other menu items refer to the UTN server's configuration. They are described in the Online Help of the myUTN Control Center. To start the Online Help, click the ? icon.

2.2 Administration via the SEH UTN Manager

Area of Application

The software tool 'SEH UTN Manager' handles the access of the USB devices. The SEH UTN Manager shows the availability of all UTN servers and USB devices that exist in the network and establishes a connection between the client and the USB port of the UTN server to which the USB device is connected. The software is installed on all clients that are meant to access a USB device in the network.

Mode of Operation

After the SEH UTN Manager is started, the network will be scanned for connected UTN servers. The network range to be scanned is freely definable.

After the network scan all UTN servers found – together with the connected USB devices – will be shown in the 'network list'. The required UTN servers will be selected and added to the 'selection list'. The devices in the selection list can be configured or connected to the client.

What Information Do You Need?

- 'Automatisms' ⇨🗎21
- 'SEH UTN Manager Versions' ⇨🗎22
- 'Installation' ⇨🗎23
- 'Programm Start' ⇨🗎27
- 'Changing Versions' ⇨🗎27
- 'Update' ⇨🗎27
- 'Program Structure' ⇨🗎28
- 'Functions' ⇨🗎28

Automatisms

The SEH UTN Manager supports, among other things, the following automatisms:

- **Auto-Connect**: This function enables the automatic activation of a permanent connection to a port and the connected USB device when you start the operating system.

- **Auto-Disconnect**: This functionality allows for the automatic deactivation of a USB port and the connected USB device after a time defined.
- **Additional Tool 'utnm'**: This tool is used for the activation and deactivation of port connections. To this purpose, commands are entered and run in the command-line interface of the operating system. As an alternative, a script will be written.

SEH UTN Manager Versions

The SEH UTN Manager is available in two versions:

- **Complete version**
- **Minimal version** (without graphical user interface)

What Are the Differences Between the Versions?

The decisive difference in the complete version is the graphical user interface. It shows you the program in form of graphic images and offers additional features: searching for and administrating UTN servers, simplified use of USB devices, and much more.

The minimal version of the SEH UTN Manager can only be used via the command-line interface. The minimal version can for example be used to automate the activation/deactivation of port connections (with scripts); see: 'Zusatztool 'utnm'' ⇨🗎150.

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

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

Additionally, the following user groups are distinguished:

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

The functions **Auto-Connect** and **Auto-Disconnect** can only be configured by users with administrative rights.

Installation

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

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

For Linux systems (64-bit), the installation packages are available as '*.deb' and '*rpm' files. There are four packages, respectively:

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

'*.tgz' installation packages for other Linux systems (32- and 64-bit) are also available. Minimum requirements: Linux kernel 2.6.32 and glibc 2.11.1.
Due to the multitude of Linux varieties, a successful installation can however not be guaranteed!

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

- package 1)–3): minimal version
- package 1)–4): complete version

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

The installation of the files depends on the distribution. For more information, refer to the documentation of your operating system. Some installation procedures are described exemplarily.

What Do You Want To Do?

- 'Installting the SEH UTN Manager via the Ubuntu Software Center' ⇨📄24
- 'Installing the SEH UTN Manager via Ubuntu terminal' ⇨📄25
- 'Installing theSEH UTN Manager via the Oracle Terminal' ⇨📄25
- Installing Dynamic Kernel Module Support (DKMS)

Installting the SEH UTN Manager via the Ubuntu Software Center

System Requirements

☑ Ubuntu 12.4.x LTS (64-bit), Ubuntu 14.04.x LTS (64-bit) with Linux kernel 2.6.32 or higher, glibc 2.11.1 or higher and OpenSSL 1.0.1 or higher

☑ The user used can gain root privileges via the command 'sudo'.

Proceed as follows:

1. Start the installation package no. 1.
   The Ubuntu Software Center appears.
2. *Click* **Install**.
   A password prompt appears.
3. *Authenticate yourself with your password.*
   The package will be installed on your client.
4. *Repeat steps 1 through 3 with the remaining packages.*
5. *Add all users that are to administrate the SEH UTN Manager on the client to the user group 'utnusers': To do this, open the console 'Terminal' and enter the command:*
   `sudo usermod -aG utnusers <user name>`
6. *Logout and login again so that the group changes take effect.*

↳ The SEH UTN Manager is installed on your client.

Installing the SEH UTN Manager via Ubuntu terminal

System Requirements

- ☑ Ubuntu 12.04.x LTS (64-bit), Ubuntu 14.04.x LTS (64-bit) with Linux kernel 2.6.32 or higher, glibc 2.11.1 or higher and OpenSSL 1.0.1 or higher
- ☑ The user used can gain root privileges via the command 'sudo'.
- ☑ DKMS (Dynamic Kernel Module Support) is installed on the client see: ⇨🗎26.

Proceed as follows:

1. *Open the console* **Terminal**.
2. *Install the desired SEH UTN Manager packages:*
   `sudo dpkg -i <full package name>`
3. *Add all users that are to administrate the SEH UTN Manager on the client to the user group 'utnusers':*
   `sudo usermod -aG utnusers <user name>`
4. *Logout and login again so that the group changes take effect.*

↳ The SEH UTN Manager is installed on your client.

Installing theSEH UTN Manager via the Oracle Terminal

System Requirements

- ☑ Oracle Linux 6.5 (64-bit) with Linux kernel 2.6.32 or higher, glibc 2.11.1 or higher and OpenSSL 1.0.1 or higher
- ☑ DKMS (Dynamic Kernel Module Support) is installed on the client see: ⇨🗎26.
- ☑ The user used can gain root privileges via the command 'sudo'.

Proceed as follows:

1. *Open the console* **Terminal**.
2. *Install the desired SEH UTN Manager packages:*
   `sudo rpm -i <full package name>`.
3. *Add all users that are to administrate the SEH UTN Manager on the client to the user group 'utnusers':*
   `sudo usermod -aG utnusers <user name>`
4. *Logout and login again so that the group changes take effect.*

↳ The SEH UTN Manager is installed on your client.

Installing Dynamic Kernel Module Support (DKMS)

In order to install the SEH UTN Manager, Dynamic Kernel Module Support (DKMS) must be installed on the system. Some distributions (like Oracle Linux 6.5) do not contain DKMS by default.

As an example the installation procedure in Oracle Linux 6.5 is described.

System Requirements

☑ The user used can gain root privileges via the command 'sudo'.

Proceed as follows:

1. *Open the console* **Terminal**.
2. *Run the command:*
   ```
   sudo wget http://pkgs.repoforge.org/rpm-forge-release/ rpm-forge-release-0.5.3-1.el5.rf.x86_64.rpm
   ```
3. *Run the command:*
   ```
   sudo rpm --import http://apt.sw.be/RPM-GPG-KEY.dag.txt
   ```
4. *Run the command:*
   ```
   sudo rpm -K rpmforge-release-0.5.3-1.el5.rf.*.rpm
   ```
5. *Run the command:*
   ```
   sudo rpm -i rpmforge-release-0.5.3-1.el5.rf.*.rpm
   ```
6. *Install DKMS:*
   ```
   sudo yum install dkms
   ```
7. *Run the command:*
   ```
   sudo yum install chrpath tkcvs rpm-build rpmlint php php-mysql
   ```
   A security query appears.
8. *Confirm the security query.*
   ```
   y
   ```
9. *Determine the current kernel and note down the result.*
   ```
   uname -r
   ```
10. *Run the command:*
    ```
    gpk-application
    ```
    A security query appears.
11. *Confirm the security query by clicking* **Continue anyway**.
    The **Add/Remove Software** *dialog appears.*
12. *Enter* **building kernel** *in the search box.*

13. *Click Find.*
    The search results are displayed.
14. *In the list look for* **Development package for building kernel modules to match the kernel** *for the previously determined kernel.*
15. *Check if the* **Development package for building kernel modules to match the kernel** *for your kernel is installed. If not, install the package.*

↳ DKMS is installed on the client.

Programm Start

Ubuntu

To start the SEH UTN Managers, in the launcher call 'UTN Manager' via Dash (search) or type `utnmanager` in the command line interface 'Terminal'.

Oracle

The SEH can be started in several ways:

- Under **Applications – System Tools** select **UTN Manager** .
- In the console 'Terminal' run the command `utnmanager`.
- Using **Alt+F2**, call the dialog **Run Application**. In the box enter 'utnmanager' and click **Run**.

Changing Versions

If the minimal oder complete version of the SEH UTN Manager is already installed on your system and you want to change to the other version, you must first uninstall the existing version.

Update

You can get information about the update status of the SEH UTN Manager. If an update is available, the installation file can be copied to the computer and the program can be installed. In the case of

updates, the default settings are modified according to the existing version.

Program Structure

After the program start you will see the main dialog with the following elements. The dialog may vary, depending on which elements you have chosen to be shown or hidden.

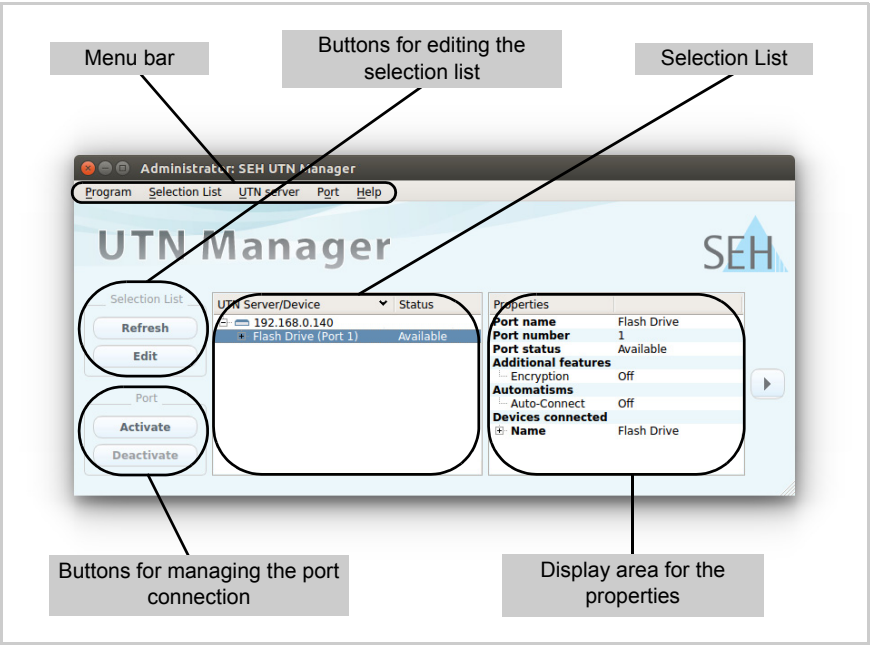


Abb. 3: SEH UTN Manager - Main Dialog

Functions

The SEH UTN Manager offers the following features:

- 'Adding UTN Servers to the Selection List' ⇨🗎62
- 'Connecting the USB Port to the Client' ⇨🗎63
- 'Disconnecting the USB Port from the Client' ⇨🗎65
- 'Requesting Occupied USB Ports' ⇨🗎66
- 'Automating Port Connections and Program Starts' ⇨🗎67
- 'Assigning an IPv4 Address to UTN Servers' ⇨🗎34

- Starting the myUTN Control Center ⇨19
- 'Granting Access to Locked USB Ports' ⇨83
- 'Managing Selection Lists for Several Participants' ⇨70

Detailed information on how to use the SEH UTN Manager can be found in the Online Help. To start the Online Help, select **Help – Online Help** from the menu bar.

Functions in the SEH UTN Manager can be shown as inactive or not shown at all. This depends on

- the embedded UTN server model
- the type and location of the selection list
- the user's rights and the group memberships on the client
- the settings of the product-specific security mechanisms
- the operating system of the client

For further information; see: 'SEH UTN Manager - Funktionsübersicht' ⇨144.

2.3 Administration via E-Mail (only myUTN-80 and later)

You can administer the UTN server via email and thus via any computer with Internet access.

Functionalities

An email allows you to

- send UTN server status information
- define UTN server parameters or
- perform an update on the UTN server.

Requirements

☑ A DNS server has been configured on the UTN server, see: ⇨📄37.

☑ 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; see: ⇨📄41.

Sending Instructions via Email

If you want to administer the UTN server, you must enter the relevant instructions into the subject line of your email.

Proceed as follows:

1. *Open an email program.*
2. *Write a new email.*
3. *Enter the UTN server address as recipient.*
4. *Enter an instruction into the subject line; see: 'Syntax and Format of an Instruction'* ⇨📄***30***.
5. *Send the email.*

↳ The UTN server receives the email and carries out the instruction.

Syntax and Format of an Instruction

Note the following syntax for instructions in the subject line:

```
cmd: <command> [<comment>]
```

The following commands are supported:

Commands	Option	Description
<command>	get status	Sends the status page of the UTN server.
	get parameters	Sends the parameter list of the UTN server.
	set parameters	Sends parameters to the UTN server. The syntax and values can be obtained from the parameter list, see: ⇨121. Parameter and value must be entered into the email body.
	update utn	Carries out an automatic update using the software that is attached to the mail.
	help	Sends a page containing information about the remote maintenance.
[<comment>]		Freely definable text for descriptions.

The following applies for the instructions:

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

Security with TAN

You will need a TAN for updates or parameter changes on the UTN server. You will get a current TAN from the UTN server via email, e.g. when receiving a status page. Enter the TAN into the first line of the email body. A space character must follow.

Parameter Changes

Parameter changes are integrated into the email body with the following syntax:

```
<parameter> = <value>
```

The syntax and values can be obtained from the parameter list, see: ⇨121.

Example 1

This email causes the UTN server to send the parameter list to the sender of the email.

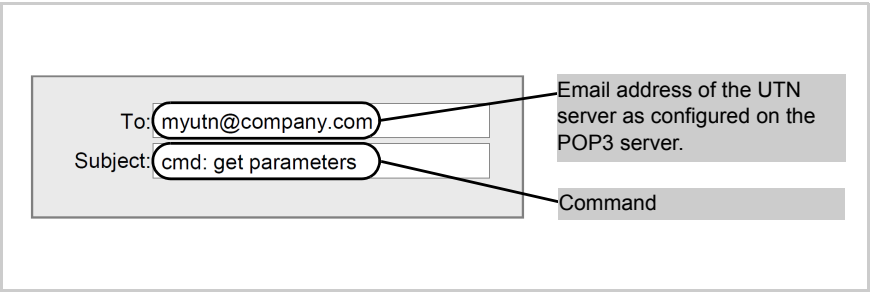


Abb. 4: Administration via Email - Example 1

Example 2

This email configures the parameter 'Description' on the UTN server.

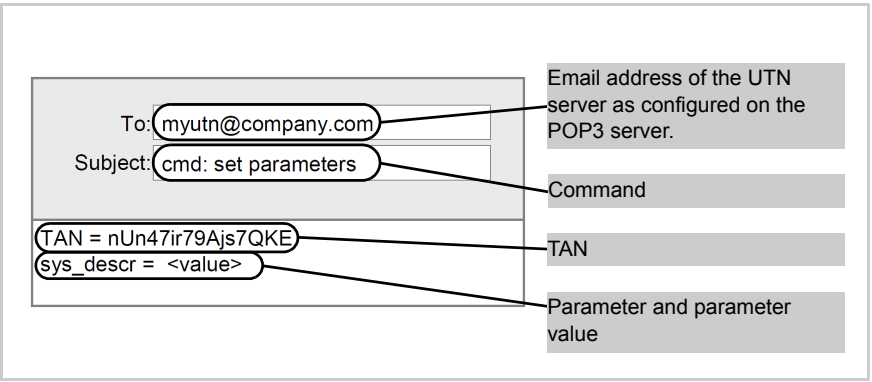


Abb. 5: Administration via Email - Example 2

3 Network Settings

You can define various settings for an ideal integration of the UTN server into a TCP/IP network. This chapter explains which network settings are supported by the UTN server.

What Information Do You Need?

3.1 How to Configure IPv4 Parameters

TCP/IP (Transmission Control Protocol over Internet Protocol) forwards data packets across several connections and establishes a connection between the network participants.

The boot protocols DHCP and BOOTP belong to the TCP/IP protocol family. You can define various IPv4 parameters for an ideal integration of the UTN server into a TCP/IP network. For further information about the assignment of IP addresses, see: ⇨🗎14.

What Do You Want To Do?

Configuring IPv4 Parameters via the myUTN Control Center

Proceed as follows:

1. *Start the myUTN Control Center.*

2. *Select* **NETWORK – IPv4**.
3. *Configure the IPv4 parameters; see: table 2* ⇨🗎*34.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Table 2: IPv4 Parameters

Parameters	Description
DHCP BOOTP ARP/PING	Enables or disables the protocols DHCP, BOOTP, and ARP/PING. *Protocols offer various possibilities to save the IP address in the UTN server.* *(See 'Saving the IP Address in the UTN Server' ⇨🗎14.)* We recommend disabling these options once an IP address has been assigned to the UTN server.
IP Address	IP address of the UTN server
Subnet mask	Subnet mask of the UTN server
Gateway	Gateway address of the UTN server

Configuring IPv4 Parameters via the SEH UTN Manager

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎21.

☑ The UTN server is shown in the selection list; see: ⇨🗎62.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Select the UTN server from the selection list.*
3. *Select* **UTN Server – Set IP Address** *from the menu bar. The* **Set IP Address dialog** *appears.*
4. *Enter the relevant TCP/IP parameters.*
5. *Click* **OK**.

↳ The settings are saved.

3.2 How to Configure IPv6 Parameters

You can integrate the UTN server into an IPv6 network.

What are the Advantages of IPv6?

IPv6 (Internet Protocol version 6) is the successor of the more commonIPv4. Both protocols are standards for the network layer of the OSI model and regulate the addressing and routing of data packets via a network. The introduction of IPv6 has many benefits:

- IPv6 increases the IP address space from 2^{32} (IPv4) to 2^{128} (IPv6) IP addresses
- Auto Configuration and Renumbering
- Efficiency increase during routing due to reduced header information.
- Integrated services such as IPSec, QoS, Multicast
- Mobile IP

What is the Structure of an IPv6 Address?

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.

Each field is separated by a colon (:).
Example: `fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4`

Leading zeros in a field can be omitted.
Example: `fe80 : 0 : 0 : 0 : 0 : 10 : 1000 : 1a4`

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. However, the use of two colons can be used only once in an address.
Example: `fe80 : : 10 : 1000 : 1a4`

As a URL in a Web browser, an IPv6 address must be enclosed in brackets. This prevents port numbers from being mistakenly regarded as part of an IPv6 address.
Example: `http://[2001:608:af:1::100]:443`

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

Which Types of IPv6 Addresses are available?

There are different types of IPv6 addresses. The prefixes of the IPv6 addresses provide information about the IPv6 address types.

- Unicast addresses can be routed globally. These addresses are unique and therefore unambiguous. A packet that is sent to a unicast address will only arrive to the interface that is assigned to this address. Unicast addresses have the prefixes '2' or '3'.
- Anycast addresses are assigned to more than one interface. This means that a data packet that is sent to this address will arrive at various devices. The syntax of anycast addresses is the same as the one of unicast addresses. The difference is that anycast addresses choose one interface out of many.
  A packet that is dedicated to an anycast address arrives at the nearest interface (in line with the router metrics). Anycast addresses are only used by routers.
- Multicast addresses allow you to send data packets to different interfaces at the same time without a proportional increase of the bandwidth. A multicast address can be recognized by the prefix 'ff'.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – IPv6**.
3. *Configure the IPv6 parameters; see: table 3* ⇨📄***36***.
4. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Table 3: IPv6 Parameters

Parameters	Description
IPv6	Enables/disables the IPv6 functionality of the UTN server.
Automatic configuration	Enables/disables the automatic assignment of the IPv6 address for the UTN server.

Parameters	Description
IPv6 address	Defines a UTN server IPv6 unicast address assigned manually in the format n:n:n:n:n:n:n:n. *Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.*
Router	Defines the IPv6 unicast address of the router. The UTN server sends its 'Router Solicitations' (RS) to this router.
Prefix length	Defines the length of the subnet prefix for the IPv6 address. The value 64 is preset. *Address ranges are indicated by prefixes. The prefix length (number of bits used) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/'.*

3.3 How to Configure the DNS

DNS is a service that translates domain names into IP addresses. Using DNS, names can be assigned to IP addresses and vice versa. If a DNS server is available in your network, you can use DNS for your UTN server.

If you use a domain name during the configuration process, you must first enable and configure DNS. DNS is used for the configuration of the time server, for example.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – DNS**.
3. *Configure the DNS parameters; see: table 4* ⇨🗎***38***.
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 4: DNS Parameters

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

3.4 How to Configure SNMP

SNMP (Simple Network Management Protocol) has become the standard protocol for the administration and monitoring of network elements. The protocol controls communication between the monitored devices and the monitoring station.

SNMP allows you to read and edit management information provided by the network elements (e.g. UTN server). The UTN server supports versions 1 and 3 of SNMP.

SNMPv1

The SNMP community is a basic form of access protection. A large number of SNMP managers are grouped together in the community. The community is then assigned (read/write) access rights. The general community string is 'public'.

The community string for SNMPv1 is transferred in plain text and does not provide sufficient protection.

SNMPv3

SNMPv3 is a continuation of the SNMP standard, which provides improved applications and a user-based security model. Distinguishing features of SNMPv3 include its simplicity and security concept.

For SNMPv3 a name and password for the SNMP user have to be defined. The user accounts used for this are those that are used for the myUTN Control Center access; see: ⇨🗎78.

Requirements

☑ Only for SNMPv3: The user accounts have been defined; see: ⇨🗎78.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – SNMP**.
3. *Configure the SNMP parameters; see: table 5* ⇨🗎***39***.
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 5: SNMP parameters

Parameters	Description
SNMPv1	Enables/disables SNMPv1.
Read-only	Enables/disables the write protection for the community.
Community	SNMP community name *The SNMP community is a basic form of access protection in which several participants with the same access rights are grouped together.*
SNMPv3	Enables/disables SNMPv3.
Hash	Defines the hash algorithm.
Access rights	Defines the access rights of the SNMP user.
Encryption	Defines the encryption method.

3.5 How to Configure Bonjour

Bonjour allows the automatic recognition of computers, devices, and network services in TCP/IP-based networks.

The UTN server uses the following Bonjour functions:

- Checking the IP address assigned via ZeroConf
- Assignment of host names to IP addresses

- Location of server services without knowledge of the device's host name or IP address.

When checking the IP address assigned via ZeroConf (see: 'ZeroConf' ⇨15) the UTN server sends a query to the network. If the IP address has already been assigned elsewhere in the network, the UTN server will receive a message. The UTN server then sends another query with a different IP address. If the IP address is available, it is saved in the UTN server.

The domain name service is used for additional Bonjour features. Since there is no central DNS server in Bonjour networks, each device and application has its own small DNS server.

This integrated DNS server (mDNS) collects and administers the information of all participants in the net. In addition to the features of a classical DNS server, the mDNS server also saves the IP address, the service name and the offered services of each participant.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – Bonjour**.
3. *Configure the Bonjour parameters; see: table 6* ⇨***40***.
4. *Click* **Save** *to confirm.*

The settings are saved.

Table 6: Bonjour Parameters

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

3.6 How to Configure POP3 and SMTP (only myUTN-80 and later)

You must configure the protocols POP3 and SMTP on the UTN server so that the notification service (⇨🗎52) and the remote maintenance via email (⇨🗎30) will work.

POP3

'POP3' (Post Office Protocol Version 3) is a transfer protocol that a client can use to fetch emails from a mail server. POP3 is required in the UTN server to administer the UTN server via email.

SMTP

'SMTP' (Simple Mail Transfer Protocol) is a protocol that controls the sending of emails in networks. SMTP is required in the UTN server to administer the UTN server via email and to run the notification service.

What Do You Want To Do?

- ☐ 'Configuring POP3' ⇨🗎41
- ☐ 'Configuring SMTP' ⇨🗎42

Configuring POP3

Requirements

☑ The UTN server is set up as user with its own email address on a POP3 server.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – Email**.
3. *Configure the POP3 parameters; see: table 7* ⇨🗎***41.***
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 7: POP3 Parameters

Parameters	Description
POP3	Enables/disables the POP3 functionality.

Parameters	Description
POP3 - Server name	Defines the POP3 server via the IP address or the host name. *The host name can only be used if a DNS server was configured beforehand.*
POP3 - Server port	Defines the port used by the UTN server for receiving emails. The port number 110 is preset. When using SSL/TLS, enter 995 as port number.
POP3 - Security	Defines the authentication method to be used (APOP/SSL/TLS). When using SSL/TLS, the cipher strength is defined via the encryption level ⇨76.
POP3 - Check mail every	Defines the time interval (in minutes) for retrieving emails from the POP3 server.
POP3 - Ignore mail exceeding	Defines the maximum email size (in Kbyte) to be accepted by the UTN server. *(0 = unlimited)*
POP3 - User name	Defines the user name used by the UTN server to log on to the POP3 server.
POP3 - Password	Defines the password used by the UTN server to log on to the POP3 server.

Configuring SMTP

Requirements

☑ The UTN server is set up as user with its own email address on a SMTP server.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – Email**.
3. *Configure the SMTP parameters; see: table 8* ⇨***43***.
4. *Click* **Save** *to confirm.*

The settings are saved.

Table 8: SMTP Parameters

Parameters	Description
SMTP - Server name	Defines the SMTP server via the IP address or the host name. *The host name can only be used if a DNS server was configured beforehand.*
SMTP - Server port	Defines the port number used by the UTN server to send emails to the SMTP server. The port number 25 is preset.
SMTP - TLS	Enables/disables TLS. *The security protocol TLS (Transport Layer Security) serves to encrypt the transmission between the UTN server and the SMTP server. The cipher strength is defined via the encryption level ⇨🗎76.*
SMTP - Sender name	Defines the email address used by the UTN server to send emails. Note: Very often the name of the sender and the user name are identical.
SMTP - Login	Enables/disables the SMTP authentication for the login.
SMTP - User name	Defines the user name used by the UTN server to log on to the SMTP server.
SMTP - Password	Defines the password used by the UTN server to log on to the SMTP server.
SMTP - Security (S/MIME)	Enables/disables the encryption and signing of emails via S/MIME.
SMTP - Signing emails	Defines the signing of emails. *A signature created by the sender allows the recipient to verify the identity of the sender and to make sure that the email was not modified. An S/MIME certificate is required for the signing of emails ⇨🗎86.*
SMTP - Full encryption	Defines the encryption of emails. *Only the recipient can open and read the encrypted email. An S/MIME certificate is required for the encryption ⇨🗎86.*
SMTP - Attach public key	Sends the public key together with the email. Many email clients require the public key to be attached in order to view the emails.

3.7 How to Configure WLAN (nur myUTN-55)

The UTN server 'myUTN-55' is a WLAN device and is operated wirelessly in the network.

What is WLAN?

WLAN is a radio technology that allows you to establish wireless connections between network components. The WLAN technology is defined as a standard of the IEEE 802.11 family. The myUTN-55 supports the standards IEEE 802.11b, 802.11g and IEEE 802.11n.

The myUTN-55 has additional WLAN parameters; see: table 9 ⇨ 46. You can view the current WLAN settings in the myUTN Control Center under the menu item **NETWORK – WLAN**.

WLAN Security

Make sure that no unauthorized user logs on to the Wireless LAN and that no one has access to the Internet or network resources. Your UTN server offers several security mechanisms.

Default	Mechanism	
	Encryption	Authentication
WEP	WEP (Open System / Shared Key)	---
WEP+EAP	WEP (Open System)	802.1X/EAP
WPA (Personal Mode)	TKIP/MIC	PSK
WPA2 (Personal Mode)	AES-CCMP	PSK
WPA (Enterprise Mode)	TKIP/MIC	802.1X/EAP
WPA2 (Enterprise Mode)	AES-CCMP	802.1X/EAP

WEP

WEP (Wired Equivalent Privacy) is an encryption method according to IEEE 802.11 on the basis of the RC4 encryption algorithm. WEP offers mechanisms for data encryption and authentication. WEP uses a key to encrypt the entire communication. As for encrypted access points, the same WEP key must be used for the access point and the UTN server.

Some access points convert WEP keys that are entered as ASCII text into arbitrary hexadecimal values. In this case, the WEP keys for the

access point and the UTN server do not match. It is therefore recommended to use hexadecimal WEP keys.

WPA/WPA2

In contrast to WEP, WPA (Wi-Fi Protected Access) offers enhanced mechanisms for exchanging keys. The exchange key is only used at the beginning of a session. Afterwards a session key is used. The key is regenerated periodically. The WPA mechanism requires an authentication at the beginning of a connection.

In the 'Personal Mode' authentication is done via the Pre Shared Key (PSK). The PSK is a password with 8–63 alphanumerical characters. The 'Enterprise Mode' uses the EAP authentication method.

An individual 128 bit key is used for data encryption after the authentication. The encryption methods TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) are available for the encryption of data.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – WLAN**.
3. *Configure the WLAN parameters; see: table 9* ⇨🗎***46***.
4. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

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

Tabelle 9: WLAN Parameters

Parameters	Description
Mode Communication mode)	Defines the communication mode. The communication mode defines the network structure in which the UTN server will be installed. Two modes are available: - In the 'Ad-Hoc' mode, the UTN server communicates directly with another WLAN client (peer-to-peer). The 'infrastructure' mode is suitable for setting up large wireless networks with several devices in different rooms. Communication between the devices is done via an access point which is connected to the network. The access point can be protected by encryption or authentication.
Network name (SSID)	Defines the SSID. The ID of a wireless network is referred to as SSID (Service Set Identifier) or network name. Each wireless LAN has a configurable SSID in order to clearly identify the wireless network. The SSID is configured in the access point of a Wireless LAN. Each device (PC, UTN server, etc.) that is intended to have access to the wireless network must be configured using the same SSID.
Roaming	Enables/disables the use of roaming. Roaming refers to the 'moving' of one radio cell to the next. The UTN server will use the access point that has the strongest signal. If the UTN server moves towards the sphere of another access point, the UTN server switches automatically and without loss of connection to the next radio cell. The parameter 'Roaming' can only be configured in the 'Infrastructure' mode.
Roaming level	Defines the transmission power (in -dBm) of the UTN server. The value 65 -dbm is preset. The parameter 'Roaming Level' can only be configured in the 'Infrastructure' mode.
Channel Frequency range)	Defines the channel (frequency range) on which the entire data communication will be transmitted. The product uses the 2.4 GHz ISM band. A channel has a bandwidth of 22 MHz. The distance between two neighboring channels is 5 MHz. Channel 3 is preset. The parameter 'Channel' can only be configured in the 'Ad-Hoc' mode. Neighboring channels overlap, which can lead to interferences. If several WLANs are operated in a small radius, a distance of at least five channels should exist between two channels. ***Keep yourself informed about national provisions regarding the use of WLAN products and only use authorized channels.***

Parameters	Description
Encryption method	see: 'WLAN Security' ⇨ 44
Authentication method	see: 'How to Use Authentication Methods' ⇨ 94

4 Device Settings

You can configure the device time, the UTN port, the notification service, etc. on the UTN server. This chapter describes these device settings.

What Information Do You Need?

4.1 How to Determine a Description

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

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **DEVICE – Description**.
3. *Enter freely definable names for* **Host name, Description** *and* **Contact person**.
4. *Click* **Save** *to confirm.*

↳ The data is saved.

To assign names to USB ports, see: ⇨🗎51.

4.2 How to Assign an Identifier Shown in the Display Panel (myUTN-800 only)

The Dongleserver myUTN-800 can be mounted in a 19" server rack. In order to identify a certain myUTN-800 if several are mounted in a rack, an identifier is shown in the display panel on the front side of the Dongleserver.

By default, the identifier 'DS' is displayed. You can assign a freely definable identifier.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **DEVICE – Description**.
3. *Enter a freely definable description into the* **Identifier (display panel)** *box.*
   (Max. 2 characters; A–Z, 0–9. g75
4. **)**
5. *Click* **Save** *to confirm.*

↳ The data is saved.

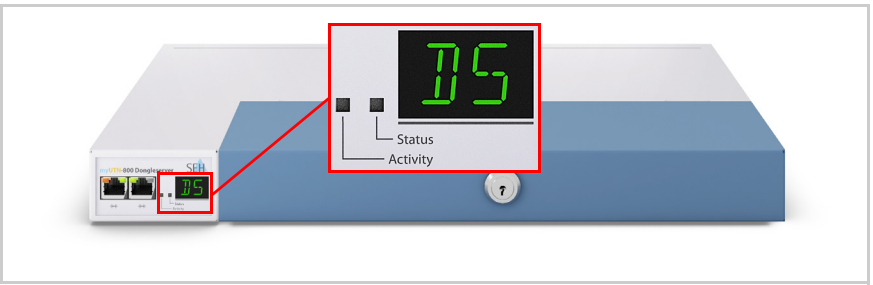


Abb. 6: Display panel myUTN-800

4.3 How to Configure the Device Time

You can control the device time of the UTN server via a time server (SNTP server) in the network. A timeserver is a computer networking device that reads the actual time from a reference clock and distributes this information to its clients. In the UTN server, the time server is defined via the IP address or the host name.

UTC

The UTN server uses 'UTC' (Universal Time Coordinated) as a basis. UTC is a reference time and used as a time standard.

Time Zone

The time received by the time server does not necessarily correspond to your local time zone. Deviations from your location and the resulting time difference (including country-specific particularities such as Daylight Saving Time) can be handled by means of the 'Time zone' parameter.

Requirements

☑ A time server is integrated into the network.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **DEVICE – Date/Time** *an.*
3. *Tick* **Date/Time**.
4. *Enter the IP address or the host name of the time server into the* **Time server** *box.*
   (The host name can only be used if a DNS server was configured beforehand.)
5. *Select the code for your local time zone from the* **Time zone** *list.*
6. *Click* **Save** *to confirm.*

↳ The settings are saved.

4.4 How to Configure the UTN (SSL) Port

A common port will be used for the data transfer between the UTN server and the client. Depending on the type of connection, two port variants are available.

UTN Port

Unencrypted connection means that client and UTN server communicate via the UTN port. The port number 9200 is preset.

UTN SSL Port

Encrypted connection means that client and UTN server communicate via the UTN SSL port. The port number 9443 is preset. In order to use an encrypted connection you must enable the port encryption; see: ⇨ 101.

This UTN port or the UTN SSL port must not be blocked by a firewall.

If required, you can change the port number on the UTN server.

Requirements

☑ In order that the SEH UTN Managers installed on the clients receive the current port number, the 'SNMPv1' parameter must be activated; see ⇨ 38.

Proceed as follows:

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. *Click* **Save** *to confirm.*

↳ The settings are saved.

4.5 How to Assign a Name to a USB Port

You can assign any name to the USB port. This port name will be displayed in the myUTN Control Center and the SEH UTN Manager. If no port name is defined, the name of the USB device connected will be displayed.

Tip

Some USB devices have cryptic or ambiguous names. Assign a clear description, e.g. the name of a corresponding software, to the USB port and thus the USB device. This gives you a better overview of the USB devices available in the network.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **DEVICE – USB port**.
3. *Enter the preferred name into the* **Port name** *field.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

4.6 How to Deactivate a USB Port (only myUTN-80 and later)

You can enable or disable a USB port. This is done by interrupting and re-establishing the power supply.

The power supply for the USB ports is enabled by default.

Benefits and Purpose

Disable unused USB ports in order to ensure that unwanted USB devices cannot be connected to the network. Deactivated USB ports cannot be seen in the SEH UTN Manager.

This function also allows you to turn a USB device off and on again without having to manually remove or reconnect it. USB devices that are in an undefined state, can be restarted by interrupting and re-establishing the power supply of the USB port.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **DEVICE – USB port**.
3. *Tick/clear the option in front of the USB port.*
4. *Click* **Save** *to confirm.*

↳ The power supply of the USB port is established or interrupted.

4.7 How to Use the Notification Service (only myUTN-80 and later)

You can get notifications in the form of emails or SNMP traps from the UTN server. By means of these notifications up to four recipients can be informed about various events irrespective of time and location.

The following message types are possible:

- The status email periodically informs the recipient about the status of the UTN server and the connected USB devices.

- The event notification informs you about a specific event on the UTN server via email or SNMP trap. The event can be:
  - The restart of the UTN server.
  - The connection/disconnection of a USB device to/from the UTN server.
  - The activation/deactivation of a USB port.
  - The interruption or establishment of power supply. (myUTN-800 only)
  - The connection/disconnection of a SD card to/from the UTN server. (myUTN-800 only)
  - The unusability of an SD card. (myUTN-800 only)

What Do You Want To Do?

☐ 'Configuring the sending of status emails' ⇨🗎53

☐ 'Configuring event notifications via email' ⇨🗎54

☐ 'Configuring event notifications via SNMP traps' ⇨🗎54

Configuring the sending of status emails

Requirements

☑ SMTP parameters have been configured on the UTN server, see: ⇨🗎41.

☑ A DNS server has been configured on the UTN server, see: ⇨🗎37.

For the notification service you can specify up to two email recipients.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **Device – Notification**.
3. *Enter the recipient into the* **Email address** *box.*
4. *Tick the desired recipient in the* **Status email** *area.*
5. *Specify the interval.*
6. *Click* **Save** *to confirm.*

↳ The settings are saved.

Configuring event notifications via email

Requirements

☑ SMTP parameters have been configured on the UTN server, see: ⇨📄41.

☑ A DNS server has been configured on the UTN server, see: ⇨📄37.

For the notification service you can specify up to two email recipients and the message types.

Proceed as follows:

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. *Click* **Save** *to confirm.*

↳ The settings are saved.

Configuring event notifications via SNMP traps

For the notification service you can specify up to two SNMP trap recipients and the message types.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **Device – Notification**.
3. *In the* **SNMP traps** *area, specify the recipients via the IP address and the community.*
4. *Tick the options with the desired message types.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

4.8 How to Get Error Messages via the Display Panel (myUTN-800 only)

You can have error states be shown in the panel display on the front side of the Dongleserver myUTN-800.

The following message types are possible:

- only one power supply works
- SD card errors (read and write errors, no SD card)

Errors are displayed in codes. The meaning of the codes you will find in chapter 'Informationen im Anzeigefeld (nur myUTN-800)' ⇨143

Proceed as follows:

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. *Click* **Save** *to confirm.*

The settings are saved.

If there is no error state, i.e. the UTN server is operational, the identifier is displayed ⇨49.

The optional acoustic signals ideally complement the error messages in the display panel. For further information; see: ⇨57.

4.9 How to Configure Acoustic Signals (myUTN-800 only)

The myUTN-800 Dongleserver gives acoustic feedback when:

- a USB dongle is connected to the UTN server
- the UTN server restarts
- the parameters are reset

These acoustic signals cannot be turned off.

Optionally further acoustic signals can be configured for when

- only one power supply works
- an SD card error exists (read and write errors, no SD card)
- only one network connection is established

These optional acoustic signals ideally complement the error messages in the display panel ⇨54.

Proceed as follows:

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. *Click* **Save** *to confirm.*

The settings are saved.

4.10 How to Use the UTN Server in VLAN environments (only myUTN-80 and later)

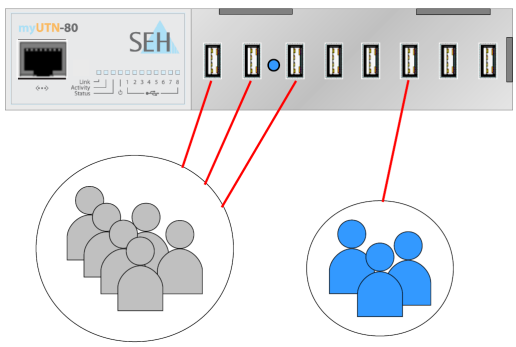
The UTN server supports the use of VLAN (Virtual Local Area Networks). It is useful to divide a physical network into VLANs for performance and security reasons.

If a VLAN spans multiple switches, you can use so-called VLAN trunks (VLT). A VLT is used to forward data from different VLANs via a single connection. Both individual ports and bundled ports can be used.

The UTN server supports the forwarding of VLAN data via its USB ports. To do this, the VLANs must be known to the UTN server. After this, the USB ports used for the forwarding of the data must be linked to the specified VLANs.

Benefits and Purpose

The VLANs can be used to control the access to dongle-protected software (myUTN-80, myUTN-800)or USB devices (myUTN-250). This way, a specified group of network participants can be provided with a certain amount of dongle-protected software licenses or USB devices.



Example

6 engineers have access to 3 dongle-protected CAD software licenses.

3 accountants have access to one dongle-protected accounting software.

The access by a participant to software that is not intended for this participant is excluded.

Note: A USB port can be connected with only one participant at a time.

Abb. 7: USB port based assignment of VLANs

What Do You Want To Do?

- ☐ 'Entering IPv4 Management VLANs' ⇨🗎58
- ☐ 'Entering IPv4 client VLANs' ⇨🗎58
- ☐ 'Allocating an IPv4 client VLAN to a USB port' ⇨🗎59

Entering IPv4 Management VLANs

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – IPv4 VLAN**.
3. *Configure the IPv4 management VLAN parameters; see: table 11* ⇨🗎59.
4. *Click* **Save** *to confirm.*

The settings are saved.

Table 10: IPv4 management VLAN parameters

Parameters	Description
IPv4 management VLAN	Enables/disables the forwarding of IPv4 management VLAN data. *If this option is enabled, SNMP is only available in the IPv4 management VLAN.*
VLAN ID	ID for the identification of the IPv4 management VLAN. (0–4096).
IP Address	IP address of the UTN server ⇨🗎34.
Subnet mask	Subnet mask of the UTN server ⇨🗎34.
Gateway	Gateway address of the IPv4 management VLAN
Access from any VLAN	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.*
Access via LAN (untagged)	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.*

Entering IPv4 client VLANs

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – IPv4 VLAN**.
3. *Configure the IPv4 VLAN parameters; see: table 11* ⇨🗎59.

4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 11: IPv4 client VLAN parameters

Parameters	Description
VLAN	Enables/disables the forwarding of IPv4 client VLAN data.
IP Address	IP address of the UTN server within the IPv4 client VLAN.
Subnet mask	Subnet mask of the UTN server within the IPv4 client VLAN.
Gateway	Gateway address of the IPv4 client VLAN.
VLAN ID	ID for the identification of the IPv4 client VLAN (0–4096).
Auto-fill	All 'VLAN', 'IP address' and 'Subnet mask' fields will be filled with the values from line 1. The 'VLAN ID' will be counted up by '1'.

Allocating an IPv4 client VLAN to a USB port

Proceed as follows:

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. *Click* **Save** *to confirm.*

↳ The settings are saved.

5 Working with the SEH UTN Manager

The software tool SEH UTN Manager handles the access of the USB devices. This chapter will show you how to embed USB devices in the SEH UTN Manager and how to establish connections between the client and the USB port including the connected USB device.

What Information Do You Need?

5.1 How to Find UTN Servers/USB Devices in the Network

In order to display the existing UTN servers and their connected USB devices in the network list, the network needs to be scanned. The network can be scanned via multicast and/or freely definable ranges. The default setting is multicast search in the local network segment.

What Do You Want To Do?

- ☐ 'Defining Search Parameters' ⇨🗎61
- ☐ 'Scanning the Network' ⇨🗎61

Defining Search Parameters

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎21.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Select* **Program – Options** *from the menu bar .*
   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 are saved.

Scanning the Network

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎21.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Select* **Selection List – Edit** *from the menu bar.*
   The **Edit Selection List** *dialog appears.*
3. *Click* **Scan**.

↳ The network is scanned. The UTN servers and USB devices found are displayed in the network list.

5.2 How to Add UTN Servers/USB Devices to the Selection List

The UTN servers found during the network scan will be displayed in the 'network list'. To use the connected USB devices, they must be assigned to the 'selection list' in the SEH UTN Manager together with the UTN server.

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨ 21.

☑ The UTN server was recognized during the network scan and is displayed in the network list.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Select* **Selection List – Edit** *from the menu bar.*
   The **Edit Selection List** *dialog appears.*
3. *Select the UTN server to be used from the network list.*
4. *Click* **Add**.
   (Repeat steps 2 and 3, if necessary.)
5. *Click* **OK**.

↳ The UTN servers and the connected USB devices are displayed in the selection list.

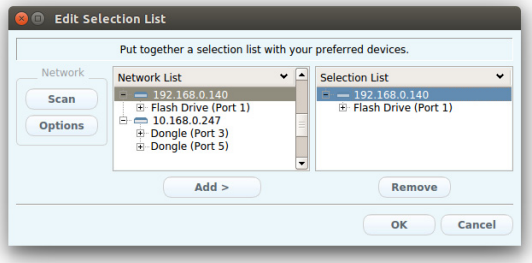


Abb. 8: SEH UTN Manager - Edit Selection List

To directly add a UTN server with a known IP address to the selection list, select **UTN Server – Add** from the menu bar.

5.3 How to Connect a USB Port including USB Device to a Client

A USB device that is connected to the UTN server can be connected to the client. To this purpose, the user establishes a connection 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 by the client as if the USB device was directly connected to the client.

Special Case Compound USB Device

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 so-called 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 12: Virtual USB ports

UTN server	Number of virtual USB ports	UTN server	Number of virtual USB ports
myUTN-50a	6	myUTN-250	12
myUTN-80	16	myUTN-800	40

Requirements

- ☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨ 21.
- ☑ The USB port is shown in the selection list; see: ⇨ 62.
- ☑ All provisions (driver installation, etc.) necessary to operate the USB device locally (i.e. connected directly to the client) should have been met on the client. Ideally, the USB device has been connected and operated on the client locally according to the instructions of the manufacturer.

☑ The USB port is not connected to another client.

Proceed as follows:

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

↳ The connection will be established.

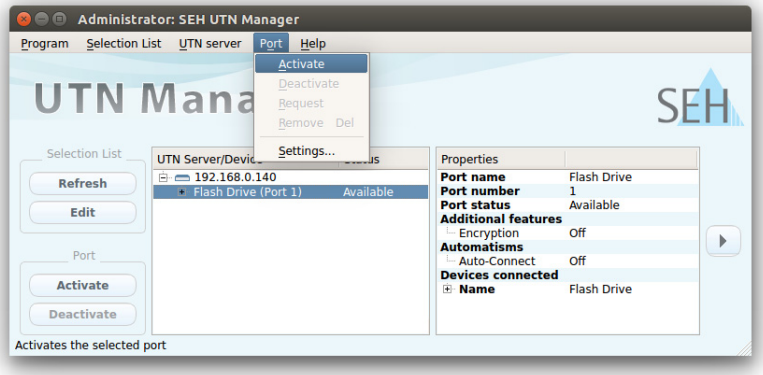


Abb. 9: SEH UTN Manager - Activating the Device

5.4 How to Cut the Connection between the USB Port including USB Device and the Client

Close the connection to the USB port and the connected USB device when the USB device is no longer needed. This allows other network participants to access the USB port and the connected USB device.

Usually the connection is cut by the user via the SEH UTN Manager. The administrator can also cut the connection via the myUTN Control Center. In addition, the connection for some automatisms can be automatically disconnected (⇨📄67).

What Do You Want To Do?

- ☐ 'Cutting the Device Connection via the SEH UTN Manager' ⇨📄65
- ☐ 'Cutting the Device Connection via the myUTN Control Center' ⇨📄65

Cutting the Device Connection via the SEH UTN Manager

Requirements

- ☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨📄21.
- ☑ The USB port is shown in the selection list; see: ⇨📄62.
- ☑ The USB port is connected to your client.

Proceed as follows:

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

↳ The connection will be deactivated.

Cutting the Device Connection via the myUTN Control Center

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **START**.
3. *Choose the active connection from the* **Attached devices** *list and click the* ⊗ *icon.*

4. *Confirm the security query.*

↳ The connection will be deactivated.

5.5 How to Request an Occupied Device

You can request a USB device that is being actively used by another user. To this purpose, send a release request for the USB port to which the USB device is connected.

The other user will be informed about your request via a popup window. The user can then terminate the connection to the USB port. When the USB port is shared, the connection between the USB port and your client will be established automatically.

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨ 21.

☑ The SEH UTN Manager (complete version) is installed on the client of the user who uses the USB device; see: ⇨ 21.

☑ The SEH UTN Manager (complete version) is executed on both clients.

☑ The USB port is shown in the selection list; see: ⇨ 62.

☑ The USB port is connected to another client.

Proceed as follows:

1. *Select the port from the selection list.*
2. *Select* **Port – Request** *from the menu bar.*

↳ The release request will be sent.

5.6 How to Automate Port Connections and Program Starts

You can automate the connections to USB ports (including connected USB devices) and program starts in many ways. This is done by various automatisms.

What Do You Want To Do?

- ☐ 'Permanent Port Connection after Operating System Boot (Auto-Connect)' ⇨📄67
- ☐ 'Automatically Disconnect the Port Connection after the Time Defined (Auto-Disconnect)' ⇨📄68
- ☐ Using the Additional Tool 'utnm' ⇨📄150

Permanent Port Connection after Operating System Boot (Auto-Connect)

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

- activated upon the operating system startup and terminated when the system shuts down
- automatically reestablished when the system restarts.

Requirements

- ☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨📄21.
- ☑ The USB port is shown in the selection list; see: ⇨📄62.
- ☑ You are logged on to the system as administrator.

Proceed as follows:

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

↳ The setting will be saved.

Automatically Disconnect the Port Connection after the Time Defined (Auto-Disconnect)

This function allows you to automatically disconnect the connection to a USB port after the time defined. A one-off prolongation of the connection by the duration of the defined time can be optionally activated. The settings apply to all USB ports on a UTN server.

Two minutes before the expiration of the defined time, the user will receive a message telling them to close the connection to the USB port and the connected USB device in order to avoid data loss and error conditions. If the prolongation is enabled, the note with the possibility to accept or reject the prolongation will appear.

You have the option of being informed about the availability of the port after the automatic disconnection. For this purpose, set up a notification if the USB port is available; see: ⇨ 69.

Auto-Disconnect allows a large number of network participants to access a small amount of USB ports including the connected USB devices and avoids idle times.

Requirements

- ☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨ 21.
- ☑ The UTN server is displayed in the 'Automatic Device Disconnect' area; see: ⇨ 62.
- ☑ You are logged on to the system as administrator.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Select* **Program – Options** *from the menu bar .*
   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 (10-525 minutes).*

6. *Optionally, tick* **Prolongation**.
7. *Click* **OK**.

↳ The setting will be saved.

5.7 How to Get Information about the USB Port and USB Device

You can view the status information of the USB port and the USB device. You can also configure automatic messages. You will be notified when a USB port and the connected USB device become available after they have been in use.

What Do You Want To Do?

- ☐ 'Displaying Status Information' ⇨🗎69
- ☐ 'Configuring Messages' ⇨🗎69

Displaying Status Information

Requirements

- ☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎21.
- ☑ The USB port is shown in the selection list; see: ⇨🗎62.

Proceed as follows:

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

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

Configuring Messages

Requirements

- ☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎21.
- ☑ The USB port is shown in the selection list; see: ⇨🗎62.

Proceed as follows:

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

3. *Select* **Port – Settings** *from the menu bar.*
   The **Port Settings** *dialog appears.*
4. *Tick the option under* **Messages**.
5. *Click* **OK**.

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

5.8 How to Manage Selection Lists for Several Participants

What are Selection Lists?

The selection list is a central element of the SEH UTN Manager. It displays all embedded UTN servers as well as the connected USB devices and shows their status. These USB devices can be connected to the client via the port connection and can then be used. The selection list can be edited and configured according to your needs by adding and deleting the required UTN servers.

Benefits and Purpose

By means of the type and distribution of the selection list in combination with the user management, the administrator can control the access to the UTN servers that are available in the network.

All users will at first use the same global selection list. As an alternative, the administrator can provide users with user-specific selection lists by means of an .ini file.

The access can be controlled by placing predefined selection lists into user-specific directories. Revoking write rights to the .ini file will limit and control the access to functions of the SEH UTN Manager for individual users.

In the following, the selection list types will be described in greater detail.

Global Selection List

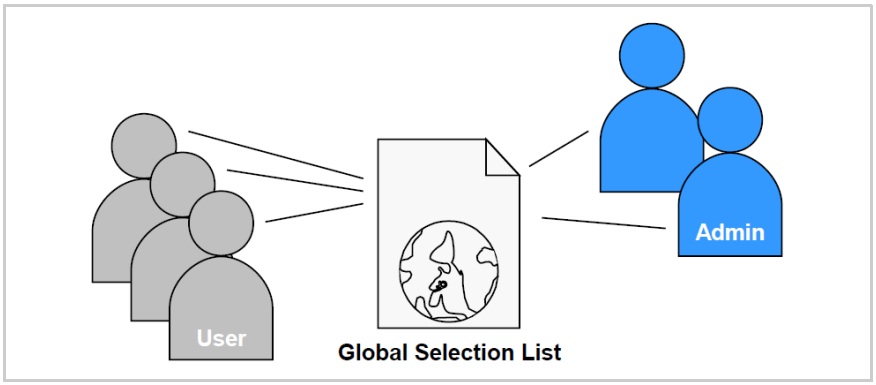


Abb. 10: Global Selection List

Properties of the global selection list:

- All users of a client use the same selection list.
- The users can only access the devices listed in the selection list.
- Unauthorized persons will not be able to access devices that are not listed in the selection list.
- The selection list can only be edited by administrators.

User-Specific Selection List

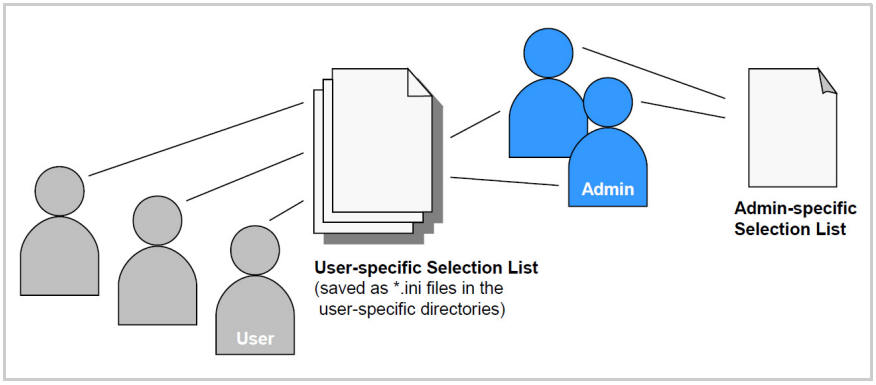


Abb. 11: User-Specific Selection List

Properties of the user-specific selection list:

- Each user has their own selection list.
  All administrators have the same selection list.

- The selection list can be edited by the administrator or by users with write access.
- The users can access all devices listed in the selection list. (Provided that no security mechanisms have been specified via the myUTN Control Center.)
- The selection lists of the users will be saved as .ini files in the following location:
  `$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`

  `$HOME` is an environment variable by Linux for the user folder. By means of the command line the path for the current user can be determined as follows: `echo $HOME`

  Example:

  Ubuntu 14.04.01 LTS:

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

  Complete path to the .ini file:

  `/home/User name/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`

What Do You Want To Do?

- ☐ 'Providing the Global Selection List to All Users' ⇨🗎72
- ☐ 'Providing User-Specific Selection Lists' ⇨🗎73
- ☐ 'Providing Users with a Predefined Selection List' ⇨🗎73
- ☐ 'Protecting the user-specific selection list' ⇨🗎74

Providing the Global Selection List to All Users

Requirements

- ☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎21.
- ☑ You are logged on to the system as administrator.

Proceed as follows:

1. *Start the SEH UTN Manager.*

2. *Compose the selection list; see: 'How to Add UTN Servers/USB Devices to the Selection List'* ⇨🗎62.
3. *Select* **Program – Options** *from the menu bar.*
   The **Options** *dialog appears.*
4. *Select the* **Selection List** *tab.*
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-Specific Selection Lists

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎21.

☑ You are logged on to the system as administrator.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Select* **Program – Options** *from the menu bar.*
   The **Options** *dialog appears.*
3. *Select the* **Selection List** *tab.*
4. *Tick* **User selection list**.
5. *Click* **OK**.

↳ The setting will be saved. Each user uses their own selection list. The selection lists of the users will be saved as .ini files in user-specific directories (see: 'User-Specific Selection List' ⇨🗎71).

The administrators share one selection list.

Providing Users with a Predefined Selection List

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎21.

☑ You are logged on to the system as administrator.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Compose the selection list for the user; see: 'How to Add UTN Servers/USB Devices to the Selection List'* ⇨🗎62.
3. *Select* **Program – Options** *from the menu bar.*
   The **Options** *dialog appears.*
4. *Select the* **Selection List** *tab.*
5. *Tick* **User selection list**.
6. *Click* **OK**.
   The setting will be saved.
7. *Select* **Selection List – Export** *from the menu bar.*
   The **Export to** *dialog appears.*
8. *Save the file 'SEH UTN Manager.ini' using the following path:*
   `$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
   (See: 'User-Specific Selection List' ⇨🗎71.)

↳ Each user has access to their own predefined selection list.

Protecting the user-specific selection list

When using predefined user-specific selection lists we recommend protecting the selection list against modifications by the user.

The selection list of a user is stored as 'SEH UTN Manager.ini' file in the following location:
`$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
(See: 'User-Specific Selection List' ⇨🗎71)

Use the control panel of the operating system to turn .ini files into read-only files. To do this, you need administrative rights on the client.

If an 'SEH UTN Manager.ini' file becomes read-only, all functions of the SEH UTN Manager that relate to the selection list will be disabled.

6 Security

A number of security mechanisms are available to ensure optimum security for the UTN server. This chapter describes how to make use of these security mechanisms.

The following security mechanisms can be configured and activated according to your demands:

What Information Do You Need?

- 'How to Define the Encryption Level for SSL/TLS Connections' ⇨🗎76
- 'How to Encrypt the Connection to the myUTN Control Center' ⇨🗎77
- 'How to Control the Access to the myUTN Control Center (User Accounts)' ⇨🗎78
- 'How to Control Access to the UTN Server (TCP Port Access Control)' ⇨🗎79
- 'How to Control Access to USB Devices (only myUTN-80 and later)' ⇨🗎82
- 'How to Block USB Device Types' ⇨🗎85
- 'How to Use Certificates Correctly' ⇨🗎86
- 'How to Use Authentication Methods' ⇨🗎94
- 'How to Encrypt Data Transfer' ⇨🗎101

The myUTN Control Center can also be protected by the SNMP and/or VLAN security concept. For further information; see:
- 'How to Configure SNMP' ⇨🗎38.
- 'How to Use the UTN Server in VLAN environments (only myUTN-80 and later)' ⇨🗎57

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

The following connections on the UTN server can be encrypted via SSL/TLS:

- Email: POP3 (⇨🗎41)
- Email: SMTP (⇨🗎41)
- Web access to the myUTN Control Center: HTTPS (⇨🗎77)
- Data transfer between the clients and the UTN server (and the connected USB devices): USB port (⇨🗎101)

Encryption Level

The encryption strength and thus the safety of the connection is defined via the encryption level.

Cipher Suite

Each encryption level is a collection of so-called cipher suites. A cipher suite is a standardized sequence of four cryptographic algorithms that are used to establish a secure connection. Depending on their cipher strength (in bit), cipher suites are grouped to form an encryption level. Which cipher suites are supported by the UTN server, i.e. are part of an encryption level, depends on the SSL/TLS protocol used.

Establishing Connections

When establishing a secure connection, a list of supported cipher suites is sent to the communicating party. 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. If there is no cipher suite that is supported by both parties, no SSL/TLS connection will be established.

The communicating parties of the UTN server (e.g. browser) must support the cipher suites of the selected encryption level in order to successfully establish a connection. When problems occur, select a different level or reset the parameters of the UTN server; see: ⇨🗎106.

The following encryption levels can be selected:

- **Compatible:** Cipher suites with an encryption of 40 to 256 bit are used.
- **Low:** Only cipher suites with a low encryption of 56 bit are used. (Fast connection)
- **Medium:** Only cipher suites with an encryption of 128 bit are used.
- **High:** Only cipher suites with a strong encryption of 128 to 256 bit are used. (Slow connection)

Do not use the encryption level 'Low' if only HTTPS is defined as the permitted connection type for the web access to the myUTN Control Center.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – SSL connections**.
3. *Select the desired encryption level from the* **Encryption** *area.*
4. *Click* **Save** *to confirm.*

The setting will be saved.

Detailed information about the individual SSL/TLS connection status (e.g. cipher suites) can be found on the Details page at **SSL connection status - Details**.

6.2 How to Encrypt the Connection to the myUTN Control Center

Types of Connection (HTTP/HTTPS)

The connection to the primos Control Center can be encrypted by selecting the permitted types of connection (HTTP/HTTPS).

If HTTPS is exclusively chosen as the connection type, the connection to the myUTN Control Center is encrypted via SSL/TLS. The cipher strength is defined via the encryption level (⇨76) and must not be 'Low'.

SSL/TLS also requires a certificate (⇨86) to check the identity of the UTN server. During a so-called 'handshake', the client asks for the certificate via a browser. This certificate must be accepted by the browser. Please refer to the documentation of your browser software. URLs that require an SSL/TLS connection start with 'https'.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Device access**.
3. *In the* **Connection** *area, tick* **HTTP/HTTPS** *or* **HTTPS only**.
4. *Click* **Save** *to confirm.*

The setting will be saved.

6.3 How to Control the Access to the myUTN Control Center (User Accounts)

You can limit the access to the myUTN Control Center. This is done with the help of user accounts.

User Accounts

There a two types of user accounts for which a name and password have to be defined. The accounts have different rights.

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

The user accounts are also used for SNMP; see: ⇨38.

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.

Login

If the access control is active, 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 must be entered.)
- name and password request
  (Neutral login screen in which user name and password are to be entered.)

Session Timeout

For stronger security, you can use a session timeout. If there is no activity during the timeout defined, the connection to the myUTN Control Center is terminated automatically.

Proceed as follows:

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. (Optional)*
7. *Click* **Save** *to confirm.*

The settings are saved.

6.4 How to Control Access to the UTN Server (TCP Port Access Control)

TCP Port Access Control

You can control the access to the UTN server. To do so, various TCP port types on the UTN server can be locked. Network elements that have permission to access the UTN server, can be defined as exceptions and excluded from locking. The UTN server only accepts data packets from network elements defined as exceptions.

Security Levels

The port types to be blocked must be defined in the 'Security level' area. The following categorization can be selected:

- Lock UTN access (locks UTN ports)
- Lock TCP access (locks TCP ports: HTTP/HTTPS/UTN)
- Lock all (locks IP ports)

Exceptions

In order to exclude network elements (e.g. clients, DNS server, SNTP server) from port locking, they must be defined as exceptions. To do so, the IP addresses or MAC addresses (hardware addresses) of the network elements with access rights must be entered in the 'Exceptions' area. Please note:

- MAC addresses are not delivered through routers!
- The use of wildcards (*) allows you to define subnetworks.

Test Mode

The 'test mode' allows you to check the configured access protection. If the test mode is activated, access protection remains active until the UTN server is rebooted. After restarting, the protection is no longer effective.

The 'test mode' option is activated by default. After a successful test, you must deactivate the test mode so that access protection remains permanently active.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – TCP port access**.
3. *Tick* **Port access control**.
4. *Select the desired protection in the* **Security level** *area.*
5. *In the* **Exceptions** *area, define the network elements which are excluded from port locking. Enter the IP or MAC addresses and tick the options.*
6. *Make sure that the* **test mode** *is enabled.*

7. *Click* **Save & Restart** *to confirm.*
   The settings are saved.
   The port access control is activated until the device is restarted.
8. *Check the port access and configurability of the UTN server.*

If the UTN server can no longer be reached using the myUTN Control Center, restart the device; see: ⇨ 109.

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

↳ The settings are saved. The port access control is active. Access to the ports is restricted.

6.5 How to Control Access to USB Devices (only myUTN-80 and later)

Via the USB ports you can control the access to the USB devices that are connected to the UTN server. Two security methods are available for each USB port. Both security methods can also be used in combination.

USB Port Key Control

In the course of the key control a key is specified for the USB port via the myUTN Control Center. By setting the key, the USB device that is connected to the USB port is protected against unwanted access.

Neither the USB port nor the connected USB device will be displayed in the SEH UTN Manager. This means that a user will not be able to make changes to the port or to establish a connection between the client and the USB port.

To make the USB port and the connected USB device available, the user must enter the key for the USB port on the client. This is done via the SEH UTN Manager. By changing the key in the myUTN Control Center the user can (once again) lose its permission to access the USB device.

USB Port Device Assignment

Device assignment means that a USB device is permanently assigned to each USB port via the myUTN Control Center. A USB device can then only be operated together with its assigned USB port.

The device assignment makes sure that the (security) settings of the USB port and the USB device are not bypassed. If a device other than the assigned USB device is connected to the USB port, it cannot be operated.

If you want to control the access to the USB devices, it is advisable to restrict the administrative access to the myUTN Control Center so that the settings cannot be changed by unauthorized persons; see: ⇨ 77.

What Do You Want To Do?

Blocking access to USB devices

If you want to control the access to a USB device you must specify a key for the USB port via the myUTN Control Center.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – USB port access**.
3. *Select the entry* **Port key control** *from the* **Method** *list of the relevant USB port.*
4. *Click* **Generate key** *or enter a freely definable key into the* **Key** *box (a maximum of 64 ASCII characters).*
5. *Click* **Save** *to confirm.*

↳ The settings are saved. Access to the USB device is protected.

Unblocking access to USB devices

In order for a user to gain access to a USB device that is protected by means of the USB port key control, an appropriate key must be entered on the client via the SEH UTN Manager.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Select the UTN server from the selection list.*
3. *Select the command* **Set USB Port Keys** *from the* **UTN server** *menu bar.*
   The **Set USB Port Keys** *dialog appears.*
4. *Enter the key for the relevant USB port.*
5. *Click* **OK**.

↳ The access to the USB port is shared. The USB port and the connected USB device are shown in the selection list and can be operated.

Specifying the Device Assignment on the USB Port

To prevent manipulations by switching the USB devices on the UTN server, you can permanently assign USB devices to the USB ports.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – USB port access**.
3. *Select the entry* **Device assignment** *from the* **Method** *list of the relevant USB port.*
4. *Click* **Reallocate device**.
   The **USB device** *box shows the vendor and product ID of the USB device.*
5. *Click* **Save** *to confirm.*

The settings are saved. Only the assigned USB device can be operated on the USB port.

If the USB port is to create an assignment with a newly connected USB device, click 'Reallocate device' again and save your settings.

Disabling the USB Port Access Control

You can disable the access control to the USB ports as well as the connected USB devices.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – USB port access**.
3. *Select the entry* **---** *from the* **Method** *list of the relevant USB port.*
4. *Click* **Save** *to confirm.*

The USB port access control will be disabled.
The connected USB devices can be operated.

6.6 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 but actually are used for abuse (known as 'BadUSB').

In order to protect the UTN server, you can block input devices which belong to the HID class.

Proceed as follows:

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. *Click* **Save** *to confirm.*
5. The setting will be saved.

6.7 How to Use Certificates Correctly

The UTN server has its own certificate management. This section explains how certificates are used and when the use of certificates is recommended.

What are Certificates?

Certificates can be used in TCP/IP-based networks to encrypt data and to authenticate communication partners. Certificates are electronic messages containing a key (public key) and a signature.

Benefits and Purpose

The use of certificates allows for various security mechanisms. Use certificates in your UTN server

- to check the identity of the UTN server in the network; see: 'Configuring EAP-TLS' ⇨🗎95.
- to authenticate the UTN server if the email communication is protected (POP3/SMTP via SSL/TLS) ⇨🗎41.
- to authenticate the UTN server/client if the data transfer between the clients and the UTN server is encrypted via SSL/TLS ⇨🗎101.
- to authenticate the UTN server/client if the administrative access to the myUTN Control Center is protected via HTTPS (SSL/TLS).

If you use certificates, it is advisable to restrict the administrative access to the myUTN Control Center so that the certificate on the UTN server cannot be deleted by unauthorized persons; see: ⇨🗎77.

Which Certificates are Available?

Both self-signed and externally signed certificates can be used with the UTN server. The following certificates can be distinguished:

- Upon delivery, a self-signed certificate (the so-called **default certificate**) is stored in the UTN server. It is recommended that you replace the default certificate by a self-signed certificate or requested certificate as soon as possible.
- **Self-signed certificates** have a digital signature that has been created by the UTN server.
- A **requested certificate** is created by a certification authority (CA) for the UTN server on the basis of a certificate request.

- **CA certificates** are certificates that have been issued for a certification authority (CA). They are used for verifying certificates that have been issued by the respective certification authority.
- **S/MIME certificates** (*.pem file) are used to sign and encrypt the emails that are sent by the UTN server. The corresponding private key must be installed as an own certificate in the PKCS#12 format (as *.p12 file) in the intended email program (Mozilla Thunderbird etc.). Only then can the emails be verified and displayed (in the case of encryption).
  (only myUTN-80 and later)

The following certificates can be installed at the same time in the UTN server:

- 1 self-signed certificate
- 1 client certificate, i.e. 1 requested certificate OR 1 PKCS#12 certificate
- 1–32 CA certifcates
- 1 S/MIME certificate (only myUTN-80 and later)

All certificates can be deleted separately.

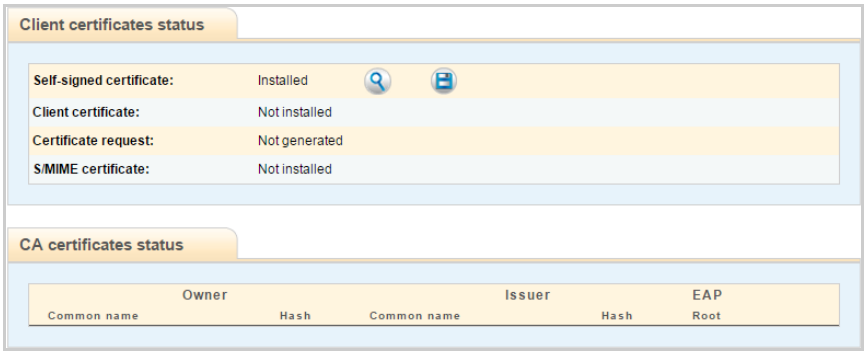


Abb. 12: myUTN Control Center - Certificates

What Do You Want To Do?

Displaying Certificates

Certificates installed on the UTN server and certificate requests can be displayed and viewed.

Requirements

☑ A certificate is installed on the UTN server.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Certificates**.
3. *Select the certificate via the icon* .

↳ The certificate is displayed.

Creating a Self-Signed Certificate

If a self-signed certificate has already been created on the UTN server, you must first delete the certificate; see: ⇨🗎93.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Certificates**.
3. *Click* **Self-signed certificate** *an.*
4. *Enter the relevant parameters; see: table 13* ⇨🗎***89***.

5. *Click* **Create/Install**.

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

Table 13: Parameters for the Creation of Certificates

Parameters	Description
Common name	Is used to clearly identify the certificate. It is advisable to use the IP address or the host name of the UTN server to allow a clear assignment of the certificate to the UTN server. *You can enter a maximum of 64 characters.*
Email address	Specifies an email address. *You can enter a maximum of 40 characters. (Optional entry)*
Organization name	Specifies the company that uses the UTN server. *You can enter a maximum of 64 characters.*
Organizational unit	Specifies the department or subsection of a company. *You can enter a maximum of 64 characters. (Optional entry)*
Location	Specifies the locality where the company is based. *You can enter a maximum of 64 characters.*
State name	Specifies the state in which the company is based. *You can enter a maximum of 64 characters. (Optional entry)*
Domain component	Allows you to enter additional attributes. *(Optional entry)*
Country	Specifies the country in which the company is based. Enter the two-digit country code according to ISO 3166. Examples: DE = Germany, GB = Great Britain, US = USA
Issued on	Specifies the date from which on the certificate is valid.
Expires on	Specifies the date from which on the certificate becomes invalid.
RSA key length	Defines the length of the RSA key used: - 512 bit (fast encryption and decryption) - 768 bit - 1024 bit (standard encryption and decryption) - 2048 bit (slow encryption and decryption)

Creating a Certificate Request for a Requested Certificate

As preparation for using a certificate which is issued by a certification authority for the UTN server, a certificate request can be created in the UTN server. The request must be sent to the certification authority which creates an certificate on the basis of this request. The certificate must be in 'base64' format.

If a certificate request has already been created, you must first delete it; see: ⇨93.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Certificates**.
3. *Click* **Certificate request**.
4. *Enter the required parameters, see: table 13* ⇨***89***.
5. *Click* **Create a request**.
   The creation of the certificate request is in progress. This may take a few minutes.
6. *Select* **Upload** *and save the requests in a text file.*
7. *Click* **OK**.
8. *Send the text file as certificate request to a certification authority.*

When the requested certificate has been received, it must be installed in the UTN server; see: ⇨90.

Installing the Requested Certificate in the UTN Server

Requirements

- ☑ A certificate request has been created at an earlier date; see: ⇨90.
- ☑ The certificate must be in 'base64' format.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Certificates**.
3. *Click* **Requested certificate**.

4. *Click* **Browse**.
5. *Specify the requested certificate.*
6. *Click* **Install**.

↳ The requested certificate will be installed in the UTN server.

Installing the PKCS#12 Certificate in the UTN Server

Certificates with the PKCS#12 format are used to save private keys and their respective certificates and to protect them by means of a password.

If a PKCS#12 certificate has already been installed on the UTN server, you must first delete it; see: ⇨🗎93.

Requirements

☑ The certificate must be in 'base64' format.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Certificates**.
3. *Click* **PKCS#12 certificate**.
4. *Click* **Browse**.
5. *Enter the PKCS#12 certificate.*
6. *Enter the password.*
7. *Click* **Install**.

↳ The PKCS#12 certificate is saved in the UTN server.

Saving S/MIME Certificates in the UTN Server (only myUTN-80 and later)

S/MIME certificates (*.pem file) are used to sign and encrypt the emails that are sent by the UTN server.

If a S/MIME certificate has already been installed on the UTN server, you must first delete it; see: ⇨🗎93.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Certificates**.
3. *Click* **S/MIME certificate**.
4. *Click* **Browse**.
5. *Specify the S/MIME certificate.*
6. *Click* **Install**.

The S/MIME certificate is saved in the UTN server.

Installing the CA Certificate in the UTN Server

In order to check the identity of the communicating parties of the UTN server, it is necessary to validate their certificates. For this, the root CA certificates of the certification authorities that have issued the certificates of said communicating parties are installed on the UTN server.

Up to 32 CA certificates can be installed. Thus multi-level public key infrastructures (PKIs) are supported.

Example: The UTN server offers a number of authentication methods to verify its identity in a network. If you use the authentication method 'EAP-TLS' (⇨95), you must install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the UTN server.

Requirements

☑ The certificate must be in 'base64' format.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Certificates**.
3. *Click* **CA certificate**.
4. *Click* **Browse**.
5. *Specify the CA certificate.*
6. *Click* **Install**.

The CA certificate will be saved in the UTN server.

Deleting Certificates

Do not delete the certificate (CA/self-signed/PKCS#12) if only HTTPS is defined as the permitted connection type for the web access to the myUTN Control Center. If the corresponding certificate is deleted, the myUTN Control Center can no longer be reached. In this case you have to reset the parameters of the UTN server; see: ⇨106.

Requirements

☑ A certificate is installed on the UTN server.

Proceed as follows:

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.

6.8 How to Use Authentication Methods

By means of an authentication, a network can be protected against unauthorized access. The UTN server can participate in various authentication procedures. This section describes which procedures are supported and how these procedures are configured on the UTN server.

What is IEEE 802.1X?

The IEEE 802.1X standard provides a basic structure for various authentication and key management protocols. IEEE 802.1X allows you to control the access to networks. Before users gain access to a network via a network device, they must authenticate themselves in the network. After the authentication was successful, the access to the network will be freed.

What is EAP?

The standard IEEE 802.1X is based upon the EAP (Extensible Authentication Protocol). EAP is a universal protocol for many authentication procedures. EAP allows for a standardized authentication procedure between the network device and an authentication server (RADIUS). First you must define the authentication procedure (TLS, PEAP, TTLS, etc.) to be used and configure it on all network devices involved.

What is RADIUS?

RADIUS (Remote Authentication Dial-In User Service) is an authentication and account management system that validates user login information and grants access to the desired resources.

The UTN server supports various EAP authentication methods in order to authenticate itself in a protected network.

What Do You Want To Do?

- ☐ 'Configuring EAP-MD5' ⇨🗎95
- ☐ 'Configuring EAP-TLS' ⇨🗎95
- ☐ 'Configuring EAP-TTLS' ⇨🗎96
- ☐ 'Configuring PEAP' ⇨🗎98
- ☐ 'Configuring EAP-FAST' ⇨🗎99

Configuring EAP-MD5

Benefits and Purpose

EAP-MD5 validates the identity of devices or users before they gain access to network resources. You can configure the UTN server for the EAP-MD5 network authentication. This ensures that the UTN server gets access to protected networks.

Mode of Operation

EAP-MD5 describes a user-based authentication method via a RADIUS server. The UTN server must be defined as user (with user name and password) on a RADIUS server. The authentication method EAP-MD5 must then be enabled on the UTN server and the user name and password need to be entered.

Requirements

☑ The UTN server is defined as user (with user name and password) on a RADIUS server.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Authentication**.
3. *Select* **MD5** *from the* **Authentication method** *list.*
4. *Enter the user name and the password that are used for the configuration of the UTN server on the RADIUS server.*
5. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Configuring EAP-TLS

Benefits and Purpose

EAP-TLS (Transport Layer Security) validates the identity of devices or users before they gain access to network resources. You can configure the UTN server for the EAP-TLS network authentication. This ensures that the UTN server gets access to protected networks.

Mode of Operation

EAP-TLS describes a certificate-based authentication method via a RADIUS server. For this purpose, certificates are exchanged between the UTN server and the RADIUS server. An encrypted TLS connection between the UTN server and the RADIUS server is established in this process. Both RADIUS server and UTN server need a valid, digital certificate signed by a CA. The RADIUS server and the UTN server must

validate the certificate. After the mutual authentication was successful, the access to the network will be freed.

Since each device needs a certificate, a PKI (Public Key Infrastructure) must be available. User passwords are not necessary.

If you want to use the EAP-TLS authentication, you must observe the instructions below in the indicated order. If this procedure is not adhered to, the UTN server in the network may not be addressable. In this case you have to reset the parameters of the UTN server; see: ⇨🗎106.

Procedure

- Create a certificate request on the UTN server; see: ⇨🗎90.
- Create a certificate using the certificate request and the authentication server.
- Install the requested certificate on the UTN server; see: ⇨🗎90.
- Install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the UTN server; see: 'Installing the CA Certificate in the UTN Server' ⇨🗎92.
- Enable the authentication method 'EAP-TLS' on the UTN server.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Authentication**.
3. *Select* **TLS** *from the* **Authentication method** *list.*
4. *Select the root CA certificate from the list* **EAP root certificate**.
5. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Configuring EAP-TTLS

Benefits and Purpose

EAP-TTLS (Tunneled Transport Layer Security) validates the identity of devices or users before they gain access to network resources. You can configure the UTN server for the EAP-TTLS network authentica-

tion. This ensures that the UTN server gets access to protected networks.

Mode of Operation

EAP-TTLS consists of two phases:

- In phase 1, a TLS-encrypted channel between the UTN server and the RADIUS server will be established. Only the RADIUS server authenticates itself using a certificate that was signed by a CA. This process is also referred to as 'outer authentication'.
- In phase 2, an additional authentication method is used for the communication within the TLS channel. EAP-defined methods and older methods (CHAP, PAP, MS-CHAP and MS-CHAPv2) are supported. This process is also referred to as 'inner authentication'.

The advantage of this procedure is that only the RADIUS server needs a certificate. Therefore no PKI is needed. Moreover, TTLS supports most authentication protocols.

Requirements

☑ The UTN server is defined as user (with user name and password) on a RADIUS server.

Proceed as follows:

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 that are used for the configuration of the UTN server on the RADIUS server.*
5. *Select the settings intended to secure the communication in the TLS channel.*
6. *To make the connection more secure, you can also install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the UTN server; see: 'Installing the CA Certificate in the UTN Server'* ⇨🗎*92*.
   Afterwards, select the root CA certificate from the list **EAP root certificate**.
7. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Configuring PEAP

Benefits and Purpose

PEAP (Protected Extensible Authentication Protocol) validates the identity of devices or users before they gain access to network resources. You can configure the UTN server for the PEAP network authentication. This ensures that the UTN server gets access to protected networks.

Mode of Operation

In the case of PEAP (compare EAP-TTLS, see ⇨🗎96), an encrypted TLS (Transport Layer Security) channel is established between the UTN server and the RADIUS server. Only the RADIUS server authenticates itself 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 advantage of this procedure is that only the RADIUS server needs a certificate. Therefore no PKI is needed. PEAP uses the advantages of TLS and supports various authentication methods, including user passwords and one-time passwords.

Requirements

☑ The UTN server is defined as user (with user name and password) on a RADIUS server.

Proceed as follows:

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 that are used for the configuration of the UTN server on the RADIUS server.*
5. *Select the settings intended to secure the communication in the TLS channel.*
6. *To make the connection more secure, you can also install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the UTN server; see: 'Installing the CA Certificate in the UTN Server'* *⇨🗎92*.
   Afterwards, select the root CA certificate from the list **EAP root certificate**.

7. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Configuring EAP-FAST

Benefits and Purpose

EAP-FAST (Flexible Authentication via Secure Tunneling) validates the identity of devices or users before they gain access to network resources. You can configure the UTN server for the EAP-FAST network authentication. This ensures that the UTN server gets access to protected networks.

Mode of Operation

EAP-FAST uses (as in the case of EAP-TTLS, see ⇨96) a channel in order to protect the data transfer. The main difference is that EAP-FAST does not require certificates for authentication purposes. (The use of certificates is optional).

PACs (Protected Access Credentials) are used to build the channel. PACs are credentials that comprise up to three components.

- A shared secret key that contains the preshared key between the UTN server and the RADIUS server.
- An opaque part that is provided to the UTN server and presented to the RADIUS server when the UTN server wishes to obtain access to network resources.
- Other information that may be useful to the client. (Optional)

EAP-FAST uses two methods to generate PACs:

- The manual delivery mechanism can be every mechanism that the administrator configures and considers to be safe for the network.
- In the case of the automatic delivery, an encrypted channel is established in order to protect the UTN server authentication as well as the delivery of the PACs.

Requirements

☑ The UTN server is defined as user (with user name and password) on a RADIUS server.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Authentication**.
3. *Select* **FAST** *from the* **Authentication method** *list.*
4. *Enter the user name and the password that are used for the configuration of 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 are saved.

6.9 How to Encrypt Data Transfer

You can encrypt the data transfer between the clients and the UTN server (and the connected USB devices).

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

Encrypted connection means that client and UTN server communicate via the UTN SSL port. The port number 9443 is preset. To change the port number, see: ⇨📄50.

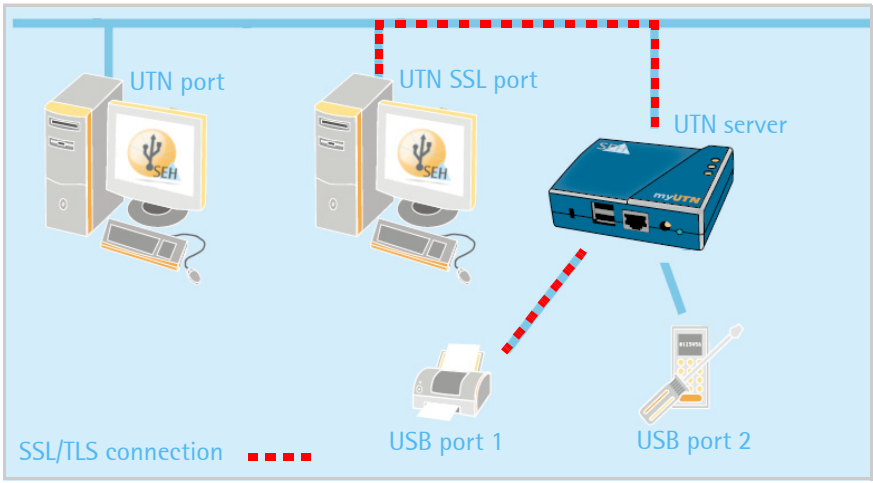


Abb. 13: UTN Server - SSL/TLS Connection in the Network

To use an SSL/TLS connection you must enable the encryption at the relevant USB port. The cipher strength is defined via the encryption level ⇨📄76.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Encryption**.
3. *Enable the encryption at the USB port.*
4. *Click* **Save** *to confirm.*

↳ The data between the clients and the USB device will be transferred in an encrypted way.

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

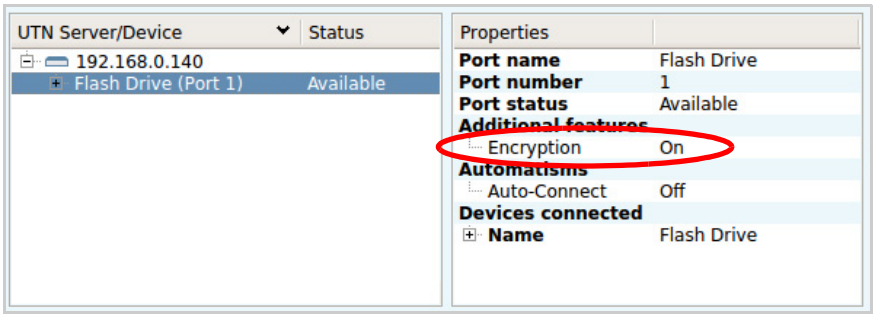


Abb. 14: SEH UTN Manager - Encryption

7 Maintenance

Various maintenance activities can be carried out on the UTN server. This chapter contains information on securing and resetting the parameter values. You will also learn how to carry out a restart and a device update.

What Information Do You Need?

- 'How to Secure UTN Parameters (Backup)' ⇨🗎103
- 'How to Reset the UTN Parameters to their Default Values' ⇨🗎106
- 'How to Perform an Update' ⇨🗎108
- 'How to Restart the UTN Server' ⇨🗎109

7.1 How to Secure UTN Parameters (Backup)

All parameter values of the UTN server (exception: passwords) are saved in the '>default name>_parameters.txt' file.

You can save the parameters file as backup copy on your local client. This allows you to get back to a stable configuration status at any time.

You can edit the parameter values of the copied file using a text editor. Afterwards, the configured file can be downloaded to one or more UTN servers. The parameter values included in the file will be taken over by the device.

Automatic Backup (myUTN-800 Only)

The Dongleserver myUTN-800 additionally has an automatic backup feature. It saves the parameter values (exception: 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.

If the SD card is lost or stolen, your environment becomes vulnerable (certificates, passwords). Therefore, you have to take all necessary precautions for protecting the myUTN-800 if you use the automatic backup.

Upon delivery, the SD card is already inserted into the SD card reader and ready for use (installation or formatting are not required).

By means of the backup, the whole configuration can be quickly and easily loaded to other UTN servers (e.g. when exchanging a UTN server). Parameter values, passwords and certificates will be loaded automatically from the SD card to a Dongleserver myUTN-800 after a cold start of the UTN server.

What Do You Want To Do?

- ☐ 'Displaying Parameter Values' ⇨🗎104
- ☐ 'Saving the Parameter File' ⇨🗎104
- ☐ 'Loading the Parameter file onto the UTN Server' ⇨🗎105
- ☐ 'Automatic backup (myUTN-800 only)' ⇨🗎105

Displaying Parameter Values

Proceed as follows:

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

↳ The current parameter values are displayed.

A detailed description of the parameters can be found in the 'Parameterliste' ⇨🗎121.

Saving the Parameter File

Proceed as follows:

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

3. *Click the icon* .
   The current parameter values are displayed.
4. *Save the '<default name>_parameters.txt' file on a local system with the help of your browser.*

↳ The parameter file is copied and secured.

Loading the Parameter file onto the UTN Server

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **MAINTENANCE – Parameter backup**.
3. *Click* **Browse**.
4. *Specify the '<default name>_parameter.txt' file.*
5. *Click* **Import**.

↳ The parameter values in the file are applied to the UTN server.

myUTN-800: If you want to load the parameter values and certificates from an automatic backup on an SD card, perform a cold start of the UTN server (interrupt and re-establish the power supply).

Automatic backup (myUTN-800 only)

Requirements

☑ An SD card is connected to the UTN server.

☑ The SD card has the file system FAT12, FAT16 or FAT32.

☑ 1 MB of free space is available on the SD card.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **MAINTENANCE – SD card**.
3. *Tick* **Parameter backup**.
4. *Click* **Save**.

↳ The settings are saved.

7.2 How to Reset the UTN Parameters to their Default Values

It is possible to reset the UTN Server's parameters to the default values (factory settings). All previously configured parameter values will be deleted in this process. Installed certificates will not be deleted.

If you reset the parameters, the IP address of the UTN server may change and the connection to the myUTN Control Center may be terminated.

When is Resetting Recommended?

You must reset the parameters, for example, if you have changed the location of the UTN server and if you want to use the UTN server in a different network. Before this change of location, you should reset the parameters to the default settings to install the UTN server in another network.

What Do You Want To Do?

- ☐ 'Resetting the Parameters via the myUTN Control Center' ⇨🗎106
- ☐ 'Resetting the Parameters via the Reset Button' ⇨🗎107

Remove the SD card from the UTN server before resetting the parameters. Otherwise, the UTN server will load the parameter values stored on it (automatic backup ⇨🗎105).

By means of the reset button of the device you can reset the parameters without entering the password.

Resetting the Parameters via the myUTN Control Center

Proceed as follows:

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 the Parameters via the Reset Button

LEDs, the reset button and various ports can be found on the UTN server. These components are described in the 'Quick Installation Guide'.

Using the reset button you can reset the UTN server's parameter values to their default setting.

Proceed as follows:

1. *Press the reset button for 5 seconds.*
   The UTN server restarts.
   (The Dongleserver myUTN-800 beeps when restarting.)

↳ The parameters are reset.

7.3 How to Perform an Update

You can carry out software and firmware updates on the UTN server. Updates allow you to benefit from currently developed features.

What Happens During an Update?

In the course of an update, the old firmware/software will be overwritten and replaced by the new firmware/software. The parameter default settings of the device remain unchanged.

When Is an Update Recommended?

An update should be undertaken if functions do not work properly and if a new software or firmware version with new functions or bug fixes has been released by SEH Computertechnik GmbH.

Check the installed software and firmware version on the UTN server. You will find the version number on the myUTN Control Center.

Where Do I Find the Update Files?

Current firmware and software files can be downloaded from the homepage of SEH Computertechnik GmbH:

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

Every update file has its own 'readme' file. Take note of the information contained in the 'readme' file.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **MAINTENANCE – Update**.
3. *Click* **Browse**.
4. *Select the update file.*
5. *Click* **Install**.

The update is executed. The UTN server will be restarted.

7.4 How to Restart the UTN Server

The UTN server will automatically restart after changes to the parameters or after an update. If the UTN server is in an undefined state, it can also be manually restarted.

What Do You Want To Do?

- ☐ 'Restarting the UTN Server via the myUTN Control Center' ⇨109
- ☐ 'Restarting the UTN server via the restart button (only myUTN-800)' ⇨109

Restarting the UTN Server via the myUTN Control Center

Proceed as follows:

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

The UTN server will be restarted.

Restarting the UTN server via the restart button (only myUTN-800)

Proceed as follows:

1. *Press the restart button of the device for a short time.*

The UTN server will be restarted.

8 Appendix

The appendix contains a glossary, the parameter list of the UTN server, and the index lists.

What Information Do You Need?

8.1 Glossary

The glossary contains information about manufacturer-specific software solutions and terms from the world of network technology.

What Information Do You Need?

Manufacturer-Specific Software Solutions

- 'myUTN Control Center' ⇨🗎111
- 'SEH UTN Manager' ⇨🗎111

Network Technology

- 'Hardware Address' ⇨🗎111
- 'IP Address' ⇨🗎112
- 'Host name' ⇨🗎112
- 'Gateway' ⇨🗎112
- 'Subnet Mask' ⇨🗎112
- 'Default Name' ⇨🗎112

Miscellaneous

- 'Compound USB Device' ⇨🗎113

myUTN Control Center

The UTN server can be configured and monitored via the myUTN Control Center. The myUTN Control Center is stored in the UTN server and can be displayed by means of a browser software (z.B. Mozilla Firefox).

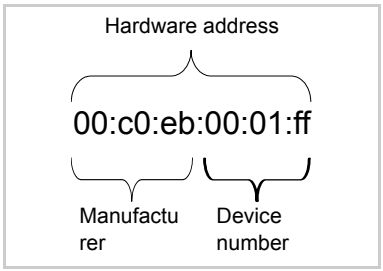
SEH UTN Manager

The software tool SEH UTN Manager handles the access of the USB devices. The software is installed on all clients that are meant to access a USB device in the network. The SEH UTN Manager shows the availability of all UTN servers in the network and establishes a connection between the client and the USB port including the connected USB device.

Hardware Address

The UTN server is addressable by means of its world-wide unique hardware address. This address is commonly referred to as the MAC or Ethernet address. The manufacturer has defined this address in the hardware of the device. The address consists of 12 hexadecimal

numbers. The first six numbers represent the manufacturer, while the last six numbers identify the individual device.



The hardware address can be found on the housing or in the SEH UTN Manager.

The use of separators within the hardware address depends on the platform. In Linux werden ':' are used.

IP Address

The IP address is the unique address of each node in a network, i.e. an IP address may occur only once on a local network. The system administrator usually assigns the IP address. The address must be saved in the UTN server to make sure that it can be addressed within the network.

Host name

The host name is an alias for an IP address. The host name uniquely identifies the UTN server in the network and makes it easier to remember.

Gateway

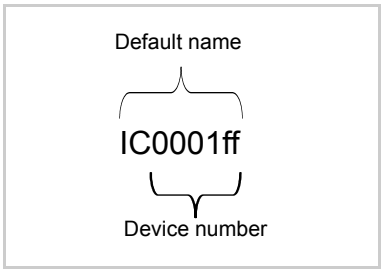
Using a gateway, you can address IP addresses from external networks. If you want to use a gateway, you can configure the relevant parameter in the UTN server via the myUTN Control Center.

Subnet Mask

With the help of the subnet mask, large networks can be split up into subnetworks. In this case, the user IDs of the IP addresses are assigned to the various subnetworks. The UTN server is configured not to use subnetworks by default. If you want to use a subnet mask, you can configure the relevant parameter in the UTN server via the myUTN Control Center.

Default Name

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 its hardware address.



The default name can be found in the myUTN Control Center.

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, in the myUTN Control Center and the selection list of the SEH UTN Manager all integrated USB devices will be displayed on the USB port. 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.

8.2 Parameter List

This chapter gives an overview of all available parameters of the UTN server. The parameter list gives details about the functions and values of the individual parameters.

What Information Do You Need?

To view the current parameter values of your UTN server, see: 'Parameterwerte anzeigen' ⇨🗎108.

Tabelle 14: Parameter List - IPv4

Parameters	Value	Default	Description
ip_addr [IP address]	valid IP address	169.254. 0.0/16	Specifies the IP address of the UTN server.
ip_mask [Subnet mask]	valid IP address	255.255. 0.0	Specifies the subnet mask of the UTN server.
ip_gate [Gateway]	valid IP address	0.0.0.0	Specifies the gateway address of the UTN server.
ip_dhcp [DHCP]	on/off	on	Enables/disables the DHCP protocol.
ip_bootp [BOOTP]	on/off	on	Enables/disables the BOOTP protocol.
ip_auto [ARP/PING]	on/off	on	Enables/disables the IP address assignment via ARP/PING.

Tabelle 15: Parameter List - IPv4-VLAN (only myUTN-80 and later)

Parameters	Value	Default	Description
ip4vlan_mgmt [IPv4 management VLAN]	on/off	off	Enables/disables the forwarding of IPv4 management VLAN data.
ip4vlan_mgmt_id [VLAN ID]	0–4096 [1–4 characters; 0–9]	0	ID for the identification of the IPv4 management VLAN (0–4096).
ip4vlan_mgmt_any [Access from any VLAN]	on/off	off	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.*
ip4vlan_mgmt_untag [Access via LAN (untagged)]	on/off	on	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.*

Parameters	Value	Default	Description
ipv4vlan_on_1 ~ ipv4vlan_on_20 [VLAN]	on/off	off	Enables/disables the forwarding of IPv4 client VLAN data.
ipv4vlan_addr_1 ~ ipv4vlan_addr_20 [IP address]	valid IP address	192.168. 0.0	Specifies the IP address of the UTN server within the IPv4 client VLAN.
ipv4vlan_mask_1 ~ ipv4vlan_mask_20 [Subnet mask]	valid IP address	255.255. 255.0	Specifies the subnet mask of the UTN server within the IPv4 client VLAN.
ip4vlan_gate_1 ~ ip4vlan_gate_20 [Gateway]	valid IP address	0.0.0.0	Gateway address of the IPv4 client VLAN.
ipv4vlan_id_1 ~ ipv4vlan_id_20 [VLAN ID]	0–4096 [1–4 characters; 0–9]	0	Specifies the ID for the identification of the IPv4 client VLAN.

Tabelle 16: Parameterliste - IPv6

Parameters	Value	Default	Description
ipv6 [IPv6]	on/off	on	Enables/disables the IPv6 functionality of the UTN server.
ipv6_addr [IPv6 address]	n:n:n:n:n:n:n:n	: :	Defines a UTN server IPv6 unicast address assigned manually in the format n:n:n:n:n:n:n:n. *Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.*

Parameters	Value	Default	Description
ipv6_gate [Router]	n:n:n:n:n:n:n:n	: :	Defines the IPv6 unicast address of the router. The UTN server sends its 'Router Solicitations' (RS) to this router.
ipv6_plen [Prefix length]	0–64 [1–2 characters; 0–9]	64	Defines the length of the sub-net prefix for the IPv6 address. *Address ranges are indicated by prefixes.* The prefix length (number of bits used) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/'.
ipv6_auto [Automatic configuration]	on/off	on	Enables/disables the automatic assignment of the IPv6 address for the UTN server.

Tabelle 17: Parameter List - Bonjour

Parameters	Value	Default	Description
bonjour [Bonjour]	on/off	on	Enables/disables the Bonjour service.
bonjour_name [Bonjour name]	max. 64 characters [a–z, A–Z, 0–9]	[Default name]	Defines the Bonjour name of the UTN server.

Tabelle 18: Parameter List - SSL Connections

Parameters	Value	Default	Description
security [Encryption]	1–4 [1 characters]	2	Defines the encryption level to be used for SSL/TLS connections. *1 = low (56 bit)* *2 = medium (128 bit)* *3 = high (128 –256 bit)* *4 = compatible (40–256 bit)* **Do not use the encryption level 'Low' if only HTTPS is defined as the permitted connection type for the web access to the myUTN Control Center.**

Tabelle 19: Parameter List - myUTN Control Center security

Parameters	Value	Default	Description
http_allowed [Connection]	on/off	on	Defines the permitted type of connection (HTTP/HTTPS) to the myUTN Control Center. *If HTTPS is exclusively chosen as the connection type [http_allowed = off], the administrative access to the myUTN Control Center is protected via SSL/TLS.*
sessKeys [Restrict Control Center access]	on/off	off	Enables/disables the myUTN Control Center access restriction. If access is restricted, a login screen is displayed when opnening the myUTN Control Center. Note: If access is restricted, user accounts must be defined.
sessKeyUList [Login screen displays]	on/off	on	Defines the type of login screen. on = list of users off = name and password request
sessKeyTimer [Session timeout]	on/off	on	Enables/disables the session timeout.

Parameters	Value	Default	Description
sessKeyTimeout [Session timeout]	120–3600 [3–4 characters; 0–9]	600	Time in seconds after which the timeout is to be effective.
admin_name [Administrator - User name]	max. 64 characters [a–z, A–Z, 0–9]	admin	Defines the user name for the administrator user account. Note: Also is the user name of the SNMP admin account.
admin_pwd [Administrator - Password]	8-64 characters [a–z, A–Z, 0–9]	adminis-trator	Defines the password for the administrator user account. Note: Also is the password of the SNMP admin account.
any_name [Read-only user - User name]	max. 64 characters [a–z, A–Z, 0–9]	anony-mous	Defines the user name for the read-only user account. Note: Also is the user name of the SNMP user account.
any_pwd [Read-only user - Password]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the password for the read-only user account. Note: Also is the password of the SNMP user account.

Tabelle 20: Parameter List – USB device type blocking

Parameters	Value	Default	Description
utn_hid [Disable input devices (HID class)]	on/off	on	De-/activates the blocking of input devices (HID - human interface devices). *on = no blocking* *off = blocking*

Tabelle 21: Parameter List - TCP port access

Parameters	Value	Default	Description
protection [Port access control]	on/off	off	Enables/disables the locking of the selected ports.

Parameters	Value	Default	Description
protection_test [Test mode]	on/off	on	Enables/disables the test mode. *The test mode allows you to test the parameters set using the access control. If the test mode is activated, the access protection remains active until the UTN server is rebooted.*
protection_level [Security level]	protec_utn protec_tcp protec_all	protec_ utn	Specifies the port types to be locked: - UTN ports - TCP ports - all ports (IP ports)
ip_filter_on_1 ~ ip_filter_on_8 [IP address]	on/off	off	Enables/disables an exception from the port locking.
ip_filter_1 ~ ip_filter_8 [IP address]	valid IP address	[blank]	Defines elements that are excluded from port locking, using the IP address.
hw_filter_on_1 ~ hw_filter_on_8 [MAC address]	on/off	off	Enables/disables an exception from the port locking.
hw_filter_1 ~ hw_filter_8 [MAC address]	valid hardware address	00:00:00: 00:00:00	Defines elements that are excluded from port locking, using the hardware address.

Tabelle 22: Parameter List - UTN port

Parameters	Value	Default	Description
utn_port UTN port	1–9200 [1–4 characters; 0–9]	9200	Defines the number of the UTN port.
utn_sslport [UTN SSL port]	1–9443 [1–4 characters; 0–9]	9443	Defines the number of the UTN SSL port.

Tabelle 23: Parameter List - Encryption

Parameters	Value	Default	Description
utn_sec_1 ~ utn_sec_20 [USB port]	on/off	off	Enables/disables the SSL/TLS encryption of the USB port. *If the encryption is enabled, the payload between the clients and the USB devices (that are connected to the USB ports) will be transferred in an encrypted way.*

Tabelle 24: Parameter List - USB port access (only myUTN-80 and later)

Parameters	Value	Default	Description
utn_heartbeat	1–1800 [1–4 characters; 0–9]	180	**This parameter can only be used after consultation with the SEH support team.**
utn_accctrt_1 ~ utn_accctrt_20 [Method]	--- ids key keyids	[---]	Specifies methods for limiting the access and use of the USB port and the connected USB device. *---* = *no protection* *ids* = *device assignment* *key* = *port key control* *keyids* = *device assignment and key control*
utn_keyval_1 ~ utn_keyval_20 [Key]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Specifies the key used to protect the access to the connected USB device.

Parameters	Value	Default	Description
utn_vendprodIDs_1 ~ utn_vendprodIDs_20 [USB device]			Shows the VID (Vendor ID) and PID (Product ID) of the USB device that is assigned to the USB port via the device assignment.
utn_2vlan_1 ~ utn_2vlan_20 [Allocate VLAN]	0–9 [1 character] (see: ⇨ 115)	0	Allocates a VLAN to the USB port. *0 = every* *1 = VLAN 1* *2 = VLAN 2, etc.* *9 = none*

Tabelle 25: Parameter List - USB port

Parameters	Value	Default	Description
utn_tag_1 ~ utn_tag_20 [Port name]	max. 32 characters [a–z, A–Z, 0–9]	[blank]	Freely definable description of the USB port.
utn_poff_1 ~ utn_poff_20 [Port]	on/off	off	Disables/enables the power supply for the USB port (i.e. the USB device connected to the port). *off = power on* *on = power off*
utn_poffdura_1 ~ utn_poffdura_20	0–100 [1–3 characters; 0–9]	0	**This parameter can only be used after consultation with the SEH support team.**
utn_prereset_1 ~ utn_prereset_20	on/off	off	**This parameter can only be used after consultation with the SEH support team.**

Tabelle 26: Parameter List - DNS

Parameters	Value	Default	Description
dns [DNS]	on/off	on	Enables/disables the name resolution via a DNS server.

Parameters	Value	Default	Description
dns_domain [Domain name]	max. 255 characters [a–z, A–Z, 0–9]	[blank]	Defines the domain name of an existing DNS server.
dns_primary [Primary DNS server]	valid IP address	0.0.0.0	Defines the IP address of the primary DNS server.
dns_secondary [Secondary DNS server]	valid IP address	0.0.0.0	Defines the IP address of the secondary DNS server. *The secondary DNS server is used if the primary DNS server is not available.*

Tabelle 27: Parameter List - SNMP

Parameters	Value	Default	Description
snmpv1 [SNMPv1]	on/off	on	Enables/disables SNMPv1.
snmpv1_ronly [Read-only]	on/off	off	Enables/disables the write protection for the community.
snmpv1_community [Community]	max. 64 characters [a–z, A–Z, 0–9]	public	Defines the name of the SNMP community. *The SNMP community is a basic form of access protection in which several participants with the same access rights are grouped together.*
snmpv3 [SNMPv3]	on/off	on	Enables/disables SNMPv3.
any_rights [Access rights]	--- [None] readonly readwrite	readonly	Defines the access rights of the SNMP user group 1.
any_hash [Hash]	md5 sha	md5	Specifies the hash algorithm of the SNMP user group 1.
any_cipher [Encryption]	--- [None] aes des	---	Defines the encryption method of the SNMP user group 1.
admin_rights [Access rights]	--- [None] readonly readwrite	readwrite	Defines the access rights of the SNMP user group 2.

Parameters	Value	Default	Description
admin_hash [Hash]	md5 sha	md5	Specifies the hash algorithm of the SNMP user group 2.
admin_cipher [Encryption]	--- [None] aes des	---	Defines the encryption method of the SNMP user group 2.

For SNMP user accounts see: 'Parameter List - myUTN Control Center security' ⇨🗎118.

Tabelle 28: Parameter List - Date/Time

Parameters	Value	Default	Description
ntp [Date/Time]	on/off	on	Enables/disables the use of a time server (SNTP).
ntp_server [Time server]	max. 64 characters [a–z, A–Z, 0–9]	pool.ntp.org	Defines a time server via the IP address or the host name. *The host name can only be used if a DNS server was configured beforehand.*
ntp_tzone [Time zone]	UTC, GMT, EST, EDT, CST, CDT, MST, MDT, PST, PDT, etc.	CET/CEST (EU)	The time zone is used to equalize the difference between the time received over the time server and the local time.

Tabelle 29: Parameter List - Description

Parameters	Value	Default	Description
sys_name [Host name]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the host name of the UTN server.
sys_descr [Description]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Freely definable description
sys_contact [Contact person]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Freely definable description (of the contact person)

Tabelle 30: Parameter List - Authentication

Parameters	Value	Default	Description
auth_typ [Authentication method]	--- [None] MD5 TLS TTLS PEAP FAST	----	Defines the authentication method that is used to identify devices or users in the network.
auth_name [User name]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the name of the UTN server as saved in the authentication server (RADIUS).
auth_pwd [Password]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the password of the UTN server as saved in the authentication server (RADIUS).
auth_intern [Inner authentication]	--- = none PAP = PAP CHAP = CHAP MSCHAP2 = MS-CHAPv2 EMD5 = EAP-MD5 ETLS = EAP-TLS	---	Defines the kind of inner authentication for the EAP authentication methods TTLS, PEAP, and FAST.
auth_extern [PEAP/EAP-FAST Options]	--- = none PLABEL0 = PEAPLABEL0 PLABEL1 = PEAPLABEL1 PVER0 = PEAPVER0 PVER1 = PEAPVER1 FPROV1 = FAST-PROV1	---	Defines the kind of external authentication for the EAP authentication methods TTLS, PEAP, and FAST.
auth_ano_name [Anonymous name]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the anonymous name for the unencrypted part of the EAP authentication methods TTLS, PEAP, and FAST.
auth_wpa_addon [WPA add-on]	max. 255 characters [a–z, A–Z, 0–9]	[blank]	Specifies an optional WPA expansion.

Tabelle 31: Parameter List - POP3 (only myUTN-80 and later)

Parameters	Value	Default	Description
pop3 [POP3]	on/off	off	Enables/disables the POP3 functionality.
pop3_srv [Server name]	max. 128 characters	[blank]	Defines the POP3 server via the IP address or the host name. *The host name can only be used if a DNS server was configured beforehand.*
pop3_poll [Check mail every]	1–10080 [1–5 characters; 0–9]	2	Defines the time interval (in minutes) for retrieving emails from the POP3 server.
pop3_port [Server port]	1–65535 [1–5 characters; 0–9]	110	Defines the port of the POP3 server used by the UTN server for receiving emails. *When using SSL/TLS, enter 995 as port number.*
pop3_usr [User name]	max. 128 characters	[blank]	Defines the name used by the UTN server to log on to the POP3 server.
pop3_pwd [Password]	max. 128 characters	[blank]	Defines the password used by the UTN server to log on to the POP3 server.
pop3_sec [Security]	0 = --- (no security) 1 = APOP 2 = SSL/TLS	0	Defines an authentication method.
pop3_limit [Ignore mail exceeding]	0–4096 [1–4 characters; 0–9; 0 = unlimited]	4096	Defines the maximum email size (in Kbyte) to be accepted by the UTN server.

Tabelle 32: Parameter List - SMTP (only myUTN-80 and later)

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

Parameters	Value	Default	Description
smtp_port [Server port]	1–65535 [1–5 characters; 0–9]	25	Defines the port number used by the UTN server to send emails to the SMTP server.
smtp_usr [User name]	max. 128 characters	[blank]	Defines the user name used by the UTN server to log on to the SMTP server.
smtp_pwd [Password]	max. 128 characters	[blank]	Defines the password used by the UTN server to log on to the SMTP server.
smtp_sender [Sender name]	max. 128 characters	[blank]	Defines the email address used by the UTN server to send emails. Note: Very often the name of the sender and the user name are identical.
smtp_ssl [TLS]	on/off	off	Enables/disables TLS. *The security protocol TLS (Transport Layer Security) serves to encrypt the transmission between the UTN server and the SMTP server.*
smtp_auth [Login]	on/off	off	Enables/disables the SMTP authentication for the login.
smtp_sign [Security (S/MIME)]	on/off	off	Enables/disables the encryption and signing of emails via S/MIME.
smtp_attpkey [Attach public key]	on/off	on	Enables/disables the attachment of a public key to an email.
smtp_encrypt [Full encryption] [Signing of emails]	on/off	off	Defines the signing and encryption of emails. *off = signing* *on = encrypt*

Tabelle 33: Parameter List - Notification (only myUTN-80 and later)

Parameters	Value	Default	Description
trapto_1 trapto_2 [Address]	valid IP address	0.0.0.0	Defines the SNMP trap address of the recipient.

Parameters	Value	Default	Description
trapcommu_1 trapcommu_2 [Community]	max. 64 characters [a–z, A–Z, 0–9]	public	Defines the SNMP trap community of the recipient.
trapdev [Send trap if USB devices are connected or disconnected]	on/off	off	Enables/disables the sending of SNMP traps after a USB device was connected to/removed from the UTN server.
trappup [Send trap if UTN server is restarted]	on/off	off	Enables/disables the sending of SNMP traps when the UTN server is restarted.
trapact [Send trap if USB ports are activated or deactivated]	on/off	off	Enables/disables the sending of SNMP traps after a USB port was activated/deactivated.
trap_pwr [Send trap if power supply is interrupted or established]	on/off	off	Enables/disables the sending of SNMP traps when one of the power supplies of the UTN server is interrupted or established (myUTN-800 only).
trap_sdinout [Send trap if SD card is connected or disconnected]	on/off	off	Enables/disables the sending of SNMP traps after an SD card was connected to/removed from the UTN server (myUTN-800 only).
trap_sdunusable [Send trap if SD card cannot be used]	on/off	off	Enables/disables the sending of SNMP traps if the SD card is unusable (myUTN-800 only).
mailto_1 mailto_2 [Email address]	valid email address [max. 64 characters]	[blank]	Defines the email address of the recipient for notifications.
noti_dev_1 noti_dev_2 [Send email if USB devices are connected or disconnected]	on/off	off	Enables/disables the sending of emails after a USB device was connected to/removed from the UTN server.

Parameters	Value	Default	Description
noti_act_1 noti_act_2 [Send email if USB port is activated or deactivated]	on/off	off	Enables/disables the sending of emails after a USB port was activated/deactivated.
noti_pwr_1 noti_pwr_2 [Send email if power supply is interrupted or established]	on/off	off	Enables/disables the sending of emails when one of the power supplies of the UTN server is interrupted or established (myUTN-800 only).
noti_sdinout_1 noti_sdinout_2 [Send email if SD card is connected or disconnected]	on/off	off	Enables/disables the sending of emails after an SD card was connected to/removed from the UTN server (only myUTN-800).
noti_sdunusable_1 noti_sdunusable_2 [Send email if SD card cannot be used]	on/off	off	Enables/disables the sending of emails if the SD card is unusable (myUTN-800 only).
noti_stat_1 noti_stat_2 [Status email]	on/off	off	Enables/disables the periodical sending of a status email to recipient 1 or 2.
noti_pup_1 noti_pup_2 [Send email if UTN server is restarted]	on/off	off	Enables/disables the sending of emails when the UTN server is restarted.
notistat_d [Interval]	al = daily su = Sunday mo = Monday tu = Tuesday we = Wednesday th = Thursday fr = Friday sa = Saturday	al	Specifies the interval at which a status email is sent.
notistat_h [hh]	1 = 1. hour 2 = 2. hour 3 = 3. hour etc.	0	Specifies the time at which a status email is sent.

Parameters	Value	Default	Description
notistat_tm [mm]	0 = 00 min 1 = 10 min 2 = 20 min 3 = 30 min 4 = 40 min 5 = 50 min 6 = 00 min	0	Specifies the time at which a status email is sent.

Tabelle 34: Parameter List - Display panel (myUTN-800 only)

Parameters	Value	Default	Description
dis_def [Identifier (display panel)]	1–2 characters [A–Z, 0–9; E+number cannot be used because this combination denotes error codes ⇨132.]	SD	Defines the identifier shown in the display panel on the front side of the Dongleserver.
dis_pwr [Display error if only one power supply provides power]	on/off	on	Enables/disables the display of error messages in the display panel if the UTN server only is supplied by one power supply. *Errors are displayed in codes; see: ⇨132.*
disp_sdc [Display SD card errors]	on/off	on	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; see: ⇨132.*

Tabelle 35: Parameter List - Acoustic signal (only myUTN-800)

Parameters	Value	Default	Description
beepPwr [Only one power supply provides power]	on/off	off	Enables/disables the acoustic signal that sounds if the UTN server only is supplied by one power supply.

Parameters	Value	Default	Description
beepSDc [SD card error]	on/off	off	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.

Tabelle 36: Parameter list - SD card (myUTN-800 only)

Parameters	Value	Default	Description
autoSync [Parameter backup]	on/off	on	Enables/disables the automatic parameter backup to a connected SD card.

8.3 Information shown in the display panel (myUTN-800 only)

The Dongleserver myUTN-800 has a display panel at its front side. It provides status information (error states).

Text	Description	Troubleshooting
DS (identifier ⇨ 51)	The Dongleserver is operational.	-
RS	The Dongleserver is restarting.	-
DL	Firmware/software is loaded onto the Dongleserver. Afterwards the Dongleserver is updated.	-
E1	One of the two power supplies is not working. Which connection is not working is indicated by a glowing dot (left dot, left power supply; right dot, right power supply).	Check the cabling connections and voltage source.
E2	The SD card is formatted with an unsupported file system respectively cannot be read and be written to.	Format the SD card in the file format FAT32, FAT16 or FAT12. Check if the SD card functions properly.
E3	The SD card is read-only.	Remove the write protection from the SD card.
E4	No SD card is available in the card reader.	Insert an SD card into the SD card reader: - Type: SD or SDHC - File system: FAT32, FAT16 or FAT12
E5	One or both network connections have no link.	Check the cabling connections and your network.

8.4 SEH UTN Manager - Function Overview

Functions in the SEH UTN Manager can be shown as inactive (grayed out) or not shown at all. This depends on the following factors:

- Settings of the selection list mode (global list / user list)
- User Groups
  - Users that have administrative rights or are members of the group 'utnusers'
  - Users that do not have administrative rights or that do not belong to the group 'utnusers'
    + Users with write access to the *.ini file (selection list)
    + Users without 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, siehe: Tabelle 37 ⇨🗎134.

The table shows the features that are basically available. In addition, individual features will not be displayed or will be displayed as inactive. This depends on
– the embedded UTN server model
– the settings of the product-specific security mechanisms

Tabelle 37: SEH UTN Manager - Function Overview Linux

	Global Selection List		User-Specific Selection List		
	Administrative rights / 'utn users'	User	Administrative rights / 'utn users'	User (rw) (INI)	User (r) (INI)
Menu					
Selection List – Edit	✓	×	✓	✓	×
Selection List – Export	✓	×	✓	×	×
Selection List – Refresh	✓	✓	✓	✓	✓
UTN server – Configure	✓	✓	✓	✓	✓
UTN server – Set IP Address	✓	✓	✓	✓	✓
UTN server – Set USB Port Keys	✓	×	✓	✓	×
UTN server – Add	✓	×	✓	✓	×
UTN server – Remove	✓	×	✓	✓	×
UTN server – Refresh	✓	✓	✓	✓	✓
Port – Activate	✓	✓	✓	✓	✓
Port – Deactivate	✓	✓	✓	✓	✓
Port – Request	✓	✓	✓	✓	✓
Port – Remove	✓	×	✓	×	×
Port – Settings	✓	✓	✓	✓	✓
Buttons					
Selection List – Refresh	✓	✓	✓	✓	✓
Selection List – Edit	✓	×	✓	✓	×
Port – Activate	✓	✓	✓	✓	×
Port – Deactivate	✓	✓	✓	✓	✓
'Program – Options' dialog					
Network Scan – Multicast Search	✓	×	✓	×	×
Network Scan – IP Range Search	✓	×	✓	×	×
Program – Program Messages	✓	×	✓	×	×
Program – Program Update	✓	×	✓	×	×
Automatisms – Auto-Disconnect	✓	×	✓	×	×
Selection List – Selection List Mode	✓	×	✓	×	×
Selection List – Automatic Refresh	✓	×	✓	×	×
'Port Settings' dialog					
Automatic device connection – Auto-Connect	✓	×	✓	×	×
Messages	✓	✓	✓	✓	✓

✓ = active
× = inactive (grayed out)

r = read-only
rw = read and write
INI = *.ini file (⇨ 73)

8.5 Troubleshooting

This chapter describes some problems and their solutions.

Problem

The UTN server signalizes the BIOS mode

Possible Cause

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

- the activity LED (yellow) blinks periodically and
- the status LED (green) is not active.

The UTN server is not operational in the BIOS mode.

In this case please contact the SEH support team, see: 'Support und Service' ⇨🗎11.

Some functions in the SEH UTN Manager are hidden, enabled or appear dimmed

Possible Cause

- ☐ Your user account does not have the required administrative rights. This leads to restricted user rights in the SEH UTN Manager; see: 'SEH UTN Manager - Function Overview' ⇨🗎133.
- ☐ A function is not supported by the connected USB device.

Start the SEH UTN Manager as administrator. For more information, refer to the documentation of your operating system.

USB devices are not shown in the SEH UTN Manager

Eliminate possible error sources. Check first if the USB device is connected to the UTN server.

Possible Cause

- ☐ The SEH UTN Manager and the firmware/software on the UTN server are incompatible. Update the SEH UTN Manager (⇨🗎28) and the firmware/software (⇨🗎115).
- ☐ Several compound USB devices (⇨🗎113) are connected to the UTN server. 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 (⇨🗎65).
- ☐ The USB port is deactivated (⇨🗎52).

The SEH UTN Manager displays several USB devices at one USB port

Possible Cause

- ☐ The connected USB device is a so-called compound USB device. It consists of a hub and one or more USB devices that are all integrated into a single housing. When the connection to the port is established, all displayed USB devices will be connected to the user's client and can be used.

A connection to the UTN server cannot be established

A common port will be used for the data transfer between the UTN server and the SEH UTN Manager that is installed on the client. ⇨🗎52.

Possible Cause

- ☐ The port numbers are not identical.
  The current port number cannot be transferred to the SEH UTN Managers that are installed on the clients.
  The 'SNMPv1' parameter has been disabled; see: ⇨🗎39.
- ☐ The communication is blocked by a firewall.

A connection to the USB port cannot be established

Possible Cause

- ☐ The access control for USB devices is enabled ⇨🗎86.
- ☐ No driver software for the USB device is installed on the client.
- ☐ The USB port is already connected to another client.

A connection to the myUTN Control Center cannot be established

Eliminate possible error sources. First of all, check:

- the cabling connections
- the IP address of the UTN server ⇨🗎14 as well as
- the proxy settings of your browser

If you still cannot establish any connection, the following safety mechanisms might be the cause:

- ☐ The access is protected via SSL/TLS (HTTPS) ⇨🗎82.
- ☐ The access is protected via SSL/TLS (HTTPS) and you deleted the certificate (CA/self-signed/PKCS#12). Reset the parameter values of the UTN server to their default settings to get access ⇨🗎111. Previous settings will be deleted.
- ☐ The TCP port access control is enabled ⇨🗎83.

- ☐ The cipher suites of the encryption level are not supported by the browser ⇨80.

Password and/or user name is no longer available

Access to the myUTN Control Center can be restricted. If the password and/or user name is no longer available, you can reset the parameter values of the UTN server to their default settings to get access ⇨111. Previous settings will be deleted.

8.6 Additional Tool 'utnm'

utnm

The additional tool 'utnm' has been developed for the myUTN products of SEH Computertechnik GmbH. It is used for the activation and deactivation of USB ports including connected USB devices.

Use

In order to activate or deactivate a USB port with utnm, commands are entered and run in a special syntax in the console of the operating system.

As an alternative, a script will be written for the USB port. The script contains commands in a special syntax. When it is run, the commands will be executed automatically step by step by the command-line interpreter.

Benefits and Purpose

When using utnm, it is not necessary to open and/or install the interface of the SEH UTN Manager (minimal version of the SEH UTN Manager ⇨🗎22).

Frequently recurring command sequences (e.g. a port activation) can be automated by means of scripts. The execution of scripts can be done automatically (e.g. by means of login scripts).

What Do You Want To Do?

☐ 'Using the Console' ⇨🗎139

☐ 'Creating Scripts' ⇨🗎140

Using the Console

Requirements

☑ The SEH UTN Manager is installed on the client; see: ⇨🗎21.

☑ The IP address or host name of a UTN server is known.

Proceed as follows:

1. *Open the console* **Terminal**.
2. *Enter the sequence of commands; see 'Syntax and Commands' ⇨🗎140.*
3. *Confirm your entries.*

↳ The sequence of commands will be run.

Creating Scripts

Requirements

☑ The SEH UTN Manager is installed on the client; see: ⇨📄21.

☑ The IP address or host name of a UTN server is known.

Proceed as follows:

1. *Open a text editor.*
2. *Enter the sequence of commands; see 'Syntax and Commands' ⇨📄140.*
3. *Save the file as executable script; for more information, refer to the documentation of your operating system.*

The script is saved. Information on how to use the script can be found in the documentation of your operating system.

Syntax and Commands

Note the following syntax:

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

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

The following commands are supported:

Command	Description

`-c "command string"`
 	
or
 	
`--command "command string"`
	Runs a command. The command is specified in greater detail by the command string. The following command strings can be used:
	• `activate UTN server port number`
	Activates the connection to a USB port and the connected USB device.
	• `deactivate UTN server port number`
	Deactivates the connection to a USB port and the connected USB device. The command string 'eject' will be used when a USB mass storage device is connected to the USB port. The command string 'plugout' will be used for all other USB devices.
	• `plugin UTN server port number`
	Activates the connection to a USB port and the connected USB device.
	• `plugout UTN server port number`
	Deactivates the connection to a USB port and the connected USB device. (Corresponds to the 'plugging out' of the device.)
	Note: *The command string 'deactivate' is to be preferred.*
	• `eject UTN server port number`
	(for USB mass storage devices) Ejects the USB device connected to the USB port. The port connection will only be deactivated if the communication has been terminated properly.
	Note: *The command string 'deactivate' is to be preferred.*
	• `set autoconnect = true|false UTN server port number`
	Automatically activates the port connection if the USB device is connected to the USB port but not in use.
	• `getlist UTN server`
	Shows an overview of the USB devices (including port number, vendor ID, product ID, manufacturer name, product name, device class and status) that are connected to the UTN server.
	• `state UTN server port number`
	Displays the status of the USB device connected to the USB port.

`-h` *or* `--help`	Shows the help page.

Command	Description

`-k USB port key`
or
`--key USB port key`
	Specifies a USB port key.
	In the course of the port key control a key is specified for the USB port via the myUTN Control Center so that the USB device that is connected to the USB port is protected against unwanted access (⇨86). In order to gain access to this USB device, the appropriate key must be entered.
	Note: The key cannot be configured via this command. Entering the key allows access to the USB device. The key must be entered each time the connection is activated.

`-mr` *or* `--machine readable`	Separates the output of the command string 'getlist' with tabulators.
`-nw` *or* `--no-warnings`	Suppresses warning messages.
`-o` *or* `--output`	Shows the output in the command line.
`-p port number` *or* `--port port number`	Uses an alternative UTN port. *Client and UTN server communicate via the UTN port. If a non-default UTN port has been be defined (⇨52), this command is to be used.*
`-q` *or* `--quiet`	Suppresses the output.
`-sp port number` *or* `--ssl-port port number`	Uses an alternative UTN port with SSL encryption. *Encrypted connection means that client and UTN server communicate via the UTN SSL port. If a non-default UTN SSL port has been be defined (⇨52), this command is to be used.*
`-t seconds` *or* `timeout seconds`	Specifies a timeout for the command strings 'activate', 'deactivate', 'plugin', 'plugout' and 'eject'.
`-v` *or* `--version`	Shows version information about utnm.

The following applies for the commands:

- UTN 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

Return Values

Return Value	Description
0	The USB port including the connected USB device is free for use.
20	The plugin of the USB device connected to the USB port failed.
21	The plugout of the USB device connected to the USB port failed.
22	The ejection of the USB device connected to the USB port failed.
23	The USB device connected to the USB port is already plugged in.
24	The USB device connected to the USB port is already plugged out.
25	The USB port including the connected USB device is connected to another user.
26	The USB port including the connected USB device is unreachable.
27	The USB device state is unknown.
100	Unknown command.
101	UTN server not found. Either the UTN server does not exist or the DNS resolution failed.
103	The port key is too long.

Example

A USB device is to be activated. Commands and syntax:

```
utnm -c "activate UTN server port number"
```

Results in:

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

8.7 List of Figures

8.8 Index