USB Device Server

myUTN-50
myUTN-52
myUTN-54
Dongleserver myUTN-80

SDCardserver myUTN-120
Scannerserver myUTN-130
myUTN-150

User Manual

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 Manuel
Title: USB Device Server
Version: 2.0

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/myutn.html

InterCon is a registered trademark of SEH Computertechnik GmbH.

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

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

Table of Contents

1 General Information. 5

1.1 myUTN 6

1.2 Documentation. 7

1.3 Support and Service 10

1.4 Your Safety 11

1.5 First Steps 12

1.6 Saving the IP Address in the UTN Server 13

2 Administration Methods 17

2.1 Administration via the myUTN Control Center 18

2.2 Administration via the SEH UTN Manager. 20

2.3 Administration via the InterCon-NetTool 28

2.4 Administration via Email (only myUTN-80 and later). 31

2.5 Administration via Reset Button of the Device 34

3 Network Settings 35

3.1 How to Configure IPv4 Parameters 35

3.2 How to Configure IPv6 Parameters 38

3.3 How to Configure the DNS 40

3.4 How to Configure SNMP 41

3.5 How to Configure Bonjour 42

3.6 How to Configure POP3 and SMTP (only myUTN-80 and later) 44

3.7 How to Configure WLAN (myUTN-54 only). 47

4 Device Settings 52

4.1 How to Determine a Description 53

4.2 How to Configure the Device Time 53

4.3 How to Configure the UTN (SSL) Port 54

4.4 How to Assign a Name to a USB Device 55

4.5 How to Control the Power Supply for a USB Port
(only myUTN-80 and later) 55

4.6 How to Compress the Data Stream of the USB Scanner
(myUTN-130 only) 56

4.7 How to Use the Notification Service (only myUTN-80 and later). 57

4.8 How to Control the Access to Dongle-Protected Software (only myUTN-80) or USB Devices (only myUTN-150) via VLAN 59

5 Working with the SEH UTN Manager 61

5.1 How to Find UTN Servers/USB Devices in the Network 61
5.2 How to Add USB Devices to the Selection List 63
5.3 How to Connect a USB Device to a Client 64
5.4 How to Cut the Connection between the USB Device and the Client65
5.5 How to Request an Occupied Device 66
5.6 How to Automate Device Connections and Program Starts 67
5.7 How to Get Information about the USB Device 72
5.8 How to Manage Selection Lists for Several Participants 73

6 Security 79

6.1 How to Define the Encryption Level for SSL/TLS Connections. 80
6.2 How to Control Access to the myUTN Control Center 82
6.3 How to Control Access to the UTN Server (TCP Port Access Control) 84
6.4 How to Control Access to USB Devices (only myUTN-80 and later) . . 86
6.5 How to Use Certificates Correctly 89
6.6 How to Use Authentication Methods 96
6.7 How to Encrypt Data Transfer 103

7 Maintenance 105

7.1 How to Secure UTN Parameters (Backup) 105
7.2 How to Reset the UTN Parameters to their Default Values 107
7.3 How to Perform an Update. 110
7.4 How to Restart the UTN Server 111

8 Appendix. 112

8.1 Glossary 113
8.2 Parameter List 116
8.3 LED Display. 132
8.4 SEH UTN Manager - Function Overview. 133
8.5 Troubleshooting. 136
8.6 Additional Tool 'utnm' 140
8.7 List of Figures. 145
8.8 Index. 146

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?

- 'myUTN' ⇨🗎6
- 'Documentation' ⇨🗎7
- 'Support and Service' ⇨🗎10
- 'Your Safety' ⇨🗎11
- 'First Steps' ⇨🗎12
- 'Saving the IP Address in the UTN Server' ⇨🗎13

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 'dongle server' (myUTN-80) was exclusively designed for the deployment of USB dongles.

The 'Scannerserver' (myUTN-130) was exclusively designed for the deployment of USB scanners.

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 USB devices in the network and establishes a connection between the client and the 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 and later
- Mac OS X 10.6.x, Mac OS X 10.7.x (64-bit), OS X 10.8.x

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 devices. The preferred devices will be selected and added to the selection list. The devices in the selection list can be connected to the client.

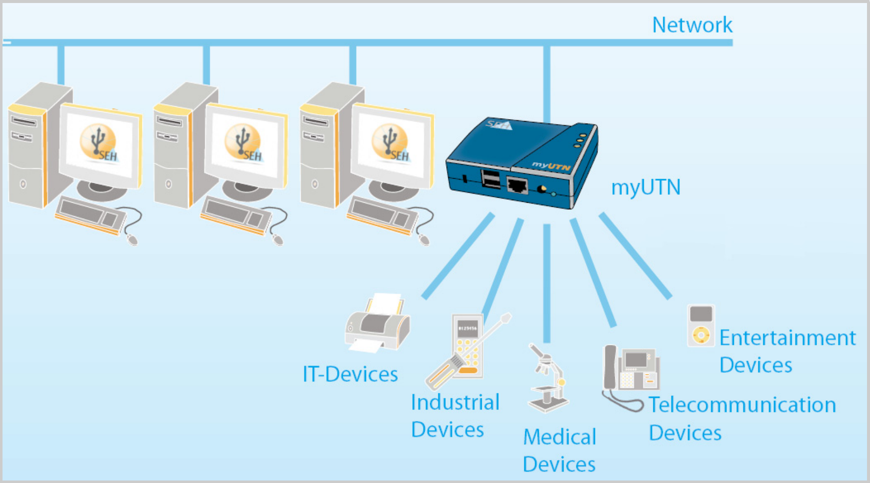


Fig. 1: UTN Server in the Network

1.2 Documentation

Scope and Content

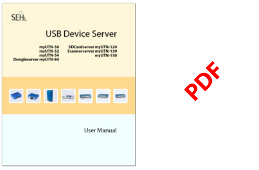
This documentation describes several versions of the USB Deviceserver, the dongle server, the Scannerserver as well as the SDCardserver. This means that functions will be described that may not be applicable to your product. Some illustrations may differ from your device.

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:

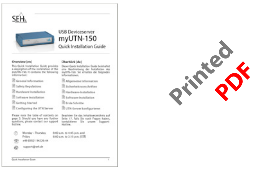
- USB Deviceserver → UTN server
- dongle server → UTN server
- Scannerserver → UTN server
- SDCardserver → UTN server
- dongle → USB device
- SD card reader → USB device
- USB scanner → USB device

Structure of the Documentation

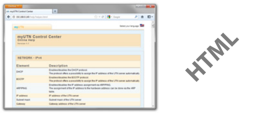
The myUTN documentation consists of the following documents:



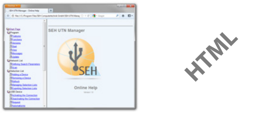
User Documentation
Detailed description of the myUTN configuration and administration.



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 bookmark 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: ⇨🗎113.

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.
ℹ 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

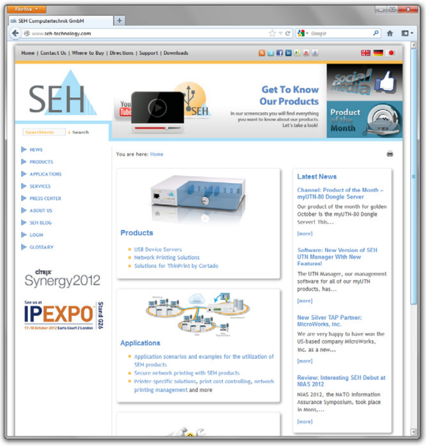
If questions remain, please contact our hotline. SEH Computertechnik GmbH offers extensive support.

🕗	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 SEH Computertechnik GmbH homepage http://www.seh-technology.com/ :



In our screencasts you will find everything you want to know about our products. Let's take a look!

You are here: Home

Products

- USB Device Servers
- Network Printing Solutions
- Solutions for ThinPrint by Cortado

Applications

- Application scenarios and examples for the utilization of SEH products
- Secure network printing with SEH products
- Printer-specific solutions, print cost controlling, network printing management and more

Latest News

Channel: Product of the Month – myUTN-80 Dongle Server
Our product of the month for golden October is the myUTN-80 Dongle Server! This...
[more]

Software: New Version of SEH UTN Manager With New Features!
The UTN Manager, our management software for all of our myUTN products, has...
[more]

New Silver TAP Partner: MicroWorks, Inc.
We are very happy to have won the US-based company MicroWorks, Inc. as a new...
[more]

Review: Interesting SEH Debut at NIAS 2012
NIAS 2012, the NATO Information Assurance Symposium, took place in Mons,...
[more]

- current firmware/software
- current tools
- current documentation
- current product information
- product data sheet
- 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. Non-observance will result in the warranty claims becoming void.

Intended Use

The UTN server is 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: ⇨🗎11.*
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: ⇨🗎13.*
4. *Install and start the software tool 'SEH UTN Manager' on your client; see: ⇨🗎20.*
5. *Add the devices that you want to use to the selection list; see: ⇨🗎63.*
6. *Activate the connection between the client and the USB device; see: ⇨🗎64.*

↳ 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 tools 'SEH UTN Manager' and 'InterCon-NetTool'; see: ⇨🗎17.

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

Automatic Methods of IP Address Assignments

- 'ZeroConf' ⇨🗎14
- 'BOOTP' ⇨🗎14
- 'DHCP' ⇨🗎14
- 'Auto Configuration (IPv6 Standard)' ⇨🗎15

Manual Methods of IP Address Assignments

- 'InterCon-NetTool' ⇨🗎15
- 'SEH UTN Manager' ⇨🗎15
- 'myUTN Control Center' ⇨🗎16
- 'ARP/PING' ⇨🗎16

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: ⇨🗎42.

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: ⇨🗎35.

☑ 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: ⇨🗎35.

☑ 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: ⇨🗎38.

InterCon-NetTool

The InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices. The IP Wizard of the InterCon-NetTool helps you to configure the TCP/IP parameters, e.g. the IP address. You can manually enter the desired IPv4 address and save it in the UTN server using the IP Wizard. To configure an IPv4 address via the InterCon-NetTool, see: ⇨🗎37.

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: ⇨🗎36.

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: ⇨🗎36.
- To configure an **IPv6** address via the myUTN Control Center, see: ⇨🗎38.

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: ⇨🗎36.

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 the myUTN Control Center' ⇨🗎18
- 'Administration via the SEH UTN Manager' ⇨🗎20
- 'Administration via the InterCon-NetTool' ⇨🗎28
- 'Administration via Email (only myUTN-80 and later)' ⇨🗎31
- 'Administration via Reset Button of the Device' ⇨🗎34

2.1 Administration via the 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 (Internet Explorer, Mozilla Firefox, Safari).

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:

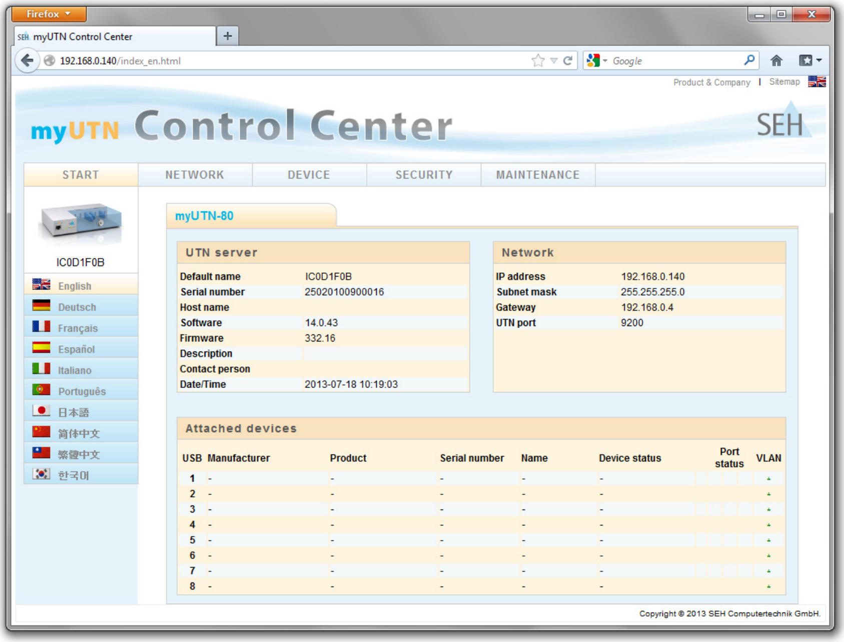
1. *Open your browser.*
2. *Enter the IP address of the UTN server as the URL.*

↳ The **myUTN Control Center** appears.

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

The myUTN Control Center can also be started via the software tools 'SEH UTN Manager' and 'InterCon-NetTool'.

- To start the myUTN Control Center via the InterCon-NetTool, mark the UTN server in the device list and select **Actions – Launch Browser** from the menu bar.
- To start the myUTN Control Center via the SEH UTN Manager, mark the UTN server in the selection list and select **UTN Server – Configure** from the menu bar.



myUTN-80

UTN server

Default name	IC0D1F0B
Serial number	25020100900016
Host name	
Software	14.0.43
Firmware	332.16
Description	
Contact person	
Date/Time	2013-07-18 10:19:03

Network

IP address	192.168.0.140
Subnet mask	255.255.255.0
Gateway	192.168.0.4
UTN port	9200

Attached devices

USB	Manufacturer	Product	Serial number	Name	Device status	Port status	VLAN
1	-	-	-	-	-		+
2	-	-	-	-	-		+
3	-	-	-	-	-		+
4	-	-	-	-	-		+
5	-	-	-	-	-		+
6	-	-	-	-	-		+
7	-	-	-	-	-		+
8	-	-	-	-	-		+

Copyright © 2013 SEH Computertechnik GmbH.

Fig. 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 device. The software is installed on all clients that are meant to access a USB device in the network.

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.

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

Automatisms

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

- **Autostart**: Upon booting the user's computer the SEH UTN Manager is activated.
- **Auto-Connect**: This functionality allows for the automatic activation of a device connection after the launch of the SEH UTN Manager.
- **Auto-Disconnect**: This functionality allows for the automatic deactivation of a device connection after a time defined.
- **Print-On-Demand**: A connection between the USB device (printer or MFP) and the client will be automatically created as soon as a print job is received. After completion of the print job, the connection will be automatically disabled.
- **Creating a UTN Action**: UTN Actions are small programs used for the automatic activation and deactivation of device connections. UTN Actions can also automate the starting and

closing of an application in combination with a device connection.

- **Additional tool 'utnm'**: This tool is used for the activation and deactivation of USB devices. 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 and UTN Actions. The minimal version can be used to

- provide users with only certain devices with simplified activation/deactivation; see: 'Creating a UTN Action: Automated Device Connections and Program Starts without the SEH UTN Manager Interface' ⇨🗎70.
- automate the activation/deactivation of USB devices (with scripts); see: 'Additional Tool 'utnm'' ⇨🗎140.

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

In both versions the service 'SEH UTN Service' works in the background and becomes active after the system start. The service can be controlled by means of the usual administration methods.

Additionally, the following user groups are distinguished:

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

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

Installation and Program Start

In order to use the SEH UTN Manager, the program must be installed on a computer with a Windows or Mac OS X operating system. Different installation files are available, depending on the 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/myutn.html

The installation file contains both versions of the SEH UTN Manager. You can select the preferred version during the installation routine.

In addition, an unattended installation can be carried out in Windows.

Windows

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

System Requirements

☑ The installation of the SEH UTN Manager is suitable for Windows XP and later.

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

Proceed as follows:

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

↳ The SEH UTN Manager is installed on your client.

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

To start the SEH UTN Manager, double-click the SEH UTN Manager icon . The icon is found on the desktop or the Windows start menu.
(Start → All Programs → SEH Computertechnik GmbH → SEH UTN Manager)

In some cases the Windows user account control requires a confirmation if the SEH UTN Manager is to be run.

Mac OS X

The installation file is available as '*.pkg' for Mac systems.

System Requirements

☑ The installation of the SEH UTN Manager is suitable for Mac OS X 10.6.x, Mac OS X 10.7.x (64-bit) and OS X 10.8.x.

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

Proceed as follows:

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

↳ The SEH UTN Manager is installed on your client.

To start the SEH UTN Manager, double-click the 'SEH UTN Manager.app' file .

(Applications → SEH UTN Manager.app)

Unattended Installation (Windows)

An unattended installation takes place without any user input. The following settings are used by default:

- Complete version
- Installation for all users of the client
- Target directory: `%PROGRAMFILES%\SEH Computertechnik GmbH\SEH UTN Manager`
  (Where `%PROGRAMFILES%` **is a Windows environment variable for the 'Programs' folder. By means of the command line, the path can be determined as follows: echo** `%PROGRAMFILES%`**)**

Benefits and Purpose

Unattended installations are less time-consuming. The SEH UTN Manager can be automatically installed on a large number of clients via login scripts. For more information, refer to the documentation of your operating system.

System Requirements

☑ The installation of the SEH UTN Manager is suitable for Windows XP and later.

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

By installing the SEH UTN Manager, you automatically accept the SEH Computertechnik GmbH agreement concerning the license and the use of the software. The agreement can be found on the homepage of SEH Computertechnik GmbH: http://www.seh-technology.com/services/licenses/software-license-agreement.html

Proceed as follows:

1. *Open the command-line interface.*
2. *Change to the directory containing the SEH UTN Manager installation file.*
3. *Enter the sequence of commands; see 'Syntax and Commands' ⇨🗎25.*
4. *Confirm your entries.*

↳ The sequence of commands will be run.

Syntax and Commands

Note the following syntax:

```
"sehutnmanager-win-X.X.X.exe" /S [<command>]
```

The following commands are supported:

Command	Description
`/S`	Runs the silent installation (no screen output).
`/U`	Updates an existing installation.
`/Srv`	Installs the minimal version (without graphical user interface).
`?`	Shows the help page.

The capitalization of the commands is mandatory.

Changing Versions

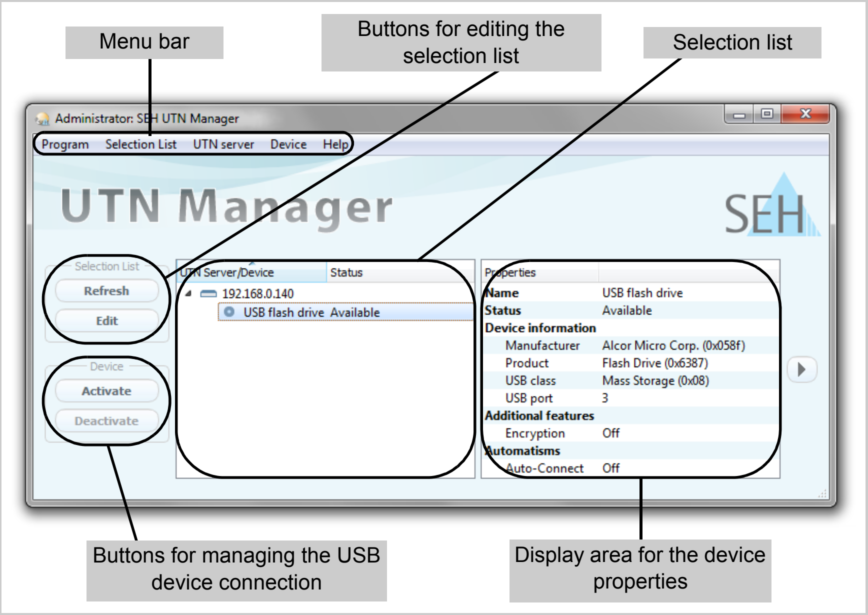
If a version of the SEH UTN Manager is installed on your system and you want to change to a different version, you must first uninstall the existing version.

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.


Menu bar
Buttons for editing the selection list
Selection list
Buttons for managing the USB device connection
Display area for the device properties
Administrator: SEH UTN Manager
Program
Selection List
UTN server
Device
Help
UTN Manager
SEH
Selection List
Refresh
Edit
Device
Activate
Deactivate

UTN Server/Device	Status
192.168.0.140	
USB flash drive	Available

Properties	
Name	USB flash drive
Status	Available
Device information	
Manufacturer	Alcor Micro Corp. (0x058f)
Product	Flash Drive (0x6387)
USB class	Mass Storage (0x08)
USB port	3
Additional features	
Encryption	Off
Automatisms	
Auto-Connect	Off

Fig. 3: SEH UTN Manager - Main Dialog

Which Functions Are Supported?

The SEH UTN Manager offers the following features:

- 'Adding USB Devices to the Selection List' ⇨🖹63
- 'Connecting the USB Device to the Client' ⇨🖹64
- 'Separating USB Device and Client' ⇨🖹65
- 'Requesting occupied USB devices' ⇨🖹66
- 'Automating Device Connections and Program Starts' ⇨🖹67
- 'Assigning an IPv4 Address to UTN Servers' ⇨🖹36
- 'Starting the myUTN Control Center' ⇨🖹18
- 'Granting Access to Locked USB Devices' ⇨🖹87
- 'Managing Selection Lists for Several Participants' ⇨🖹73

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 rights on the client
- the settings of the product-specific security mechanisms

For further information; see: 'SEH UTN Manager - Function Overview' ⇨🗎133.

2.3 Administration via the InterCon-NetTool

The software InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices (print server, TPG, ISD, UTN server, etc.). Depending on the network device you can configure various features via the InterCon-NetTool.

Basic Functions

After the InterCon-NetTool is started, the network will be scanned for connected network devices. The network range to be scanned is freely definable. All network devices found will be displayed in the 'device list'.

You can modify the device list and adopt it to your individual needs. You can mark and configure the devices in the device list.

Installation and Program Start

In order to use the InterCon-NetTool, the program must be installed on a computer with a Windows or Mac OS X operating system. Different installation files are available, depending on the operating system. The installation file of the InterCon-NetTool can be found on the SEH Computertechnik GmbH homepage:

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

Windows

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

📂 Proceed as follows:

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

↳ The InterCon-NetTool is installed on your client.

To start the InterCon-NetTool, double-click the InterCon-NetTool icon SEH. The icon is found on the desktop or the Windows start menu.
(Start → All Programs → SEH Computertechnik GmbH → InterCon-NetTool)

The settings of the InterCon-NetTool are saved in the 'NetTool.ini' file. This file is stored in the respective user folder. This file is stored in the user folder of the user that is currently logged in.

Mac OS X

The installation file is available in the image data format '*.dmg' for Mac systems.

☞ Proceed as follows:

1. *Open the InterCon-NetTool installation file.*
   The content of the file will appear on the screen.
2. *Start the '*.pkg' file.*
3. *Follow the installation routine.*

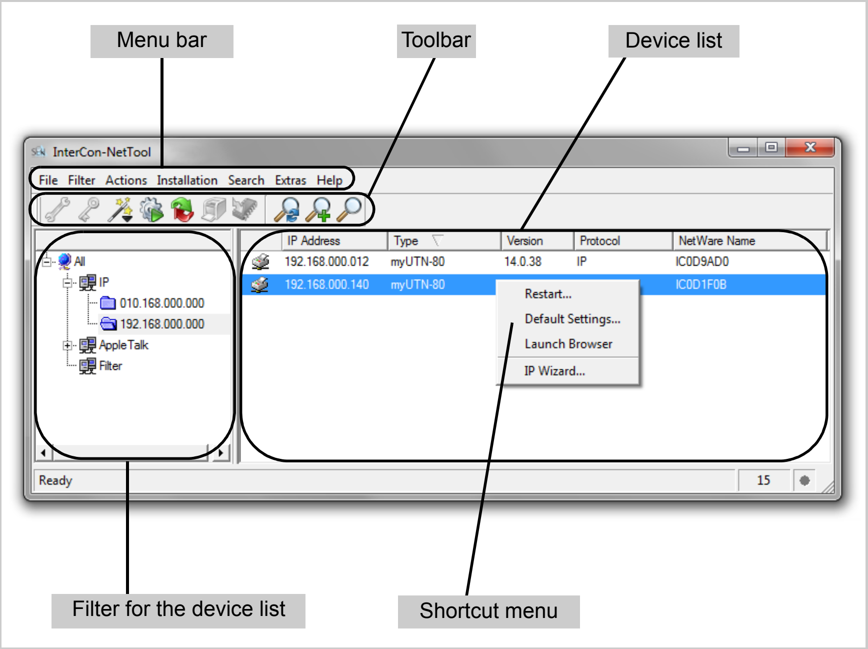
↳ The InterCon-NetTool is installed on the system.

To start the InterCon-NetTool, double-click the 'Intercon-NetTool.app' file .

The program settings are saved in the 'InterCon-NetTool.ini' file. This file can be found in the directory `/Users/<User name>/Library/Preferences/InterCon-NetTool`.

Structure of the InterCon-NetTool

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.



IP Address	Type	Version	Protocol	NetWare Name
192.168.000.012	myUTN-80	14.0.38	IP	IC0D9AD0
192.168.000.140	myUTN-80			IC0D1F0B

Fig. 4: InterCon-NetTool – Main Dialog

Which Functions Are Supported?

The InterCon-NetTool allows you to

- 'assign an IPv4 address to the UTN server' ⇨🗎37
- 'restart the UTN server' ⇨🗎111
- 'reset the UTN server's parameter values to their default settings' ⇨🗎108
- 'start the myUTN Control Center' ⇨🗎18
- 'switch from the BIOS mode to the default mode' ⇨🗎136

Detailed information on how to use the InterCon-NetTool can be found in the Online Help. To start the Online Help, select **Help – Online Help** from the menu bar.

2.4 Administration via Email (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: ⇨🗎40.

☑ 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: ⇨🗎44.

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' ⇨🗎32.*
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: ⇨ 🗎116. 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: ⇨🗎116.

Example 1

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

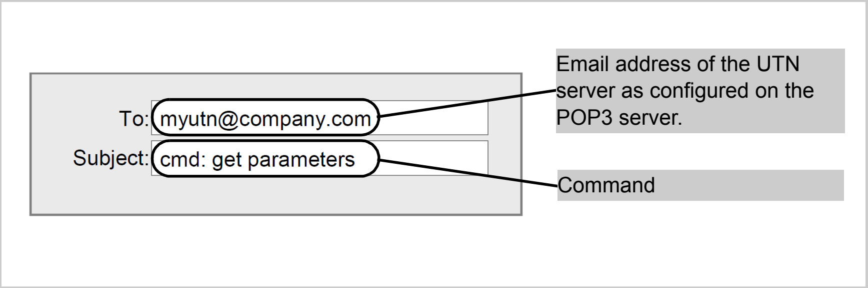

To:
myutn@company.com
Subject:
cmd: get parameters
Email address of the UTN server as configured on the POP3 server.
Command

Fig. 5: Administration via Email - Example 1

Example 2

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

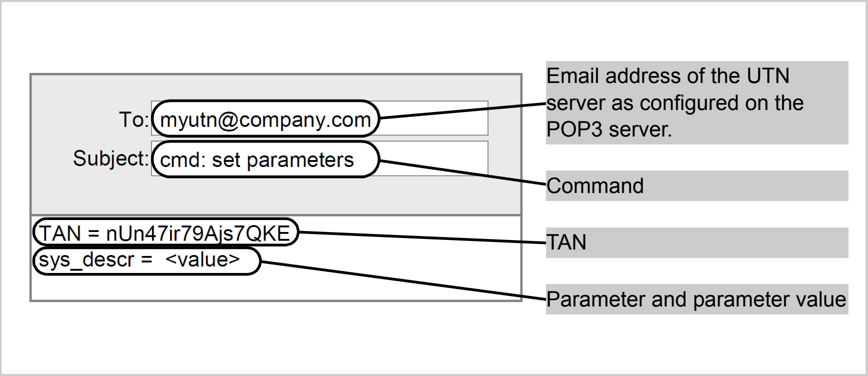


Fig. 6: Administration via Email - Example 2

2.5 Administration via Reset Button of the Device

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; see: ⇨🗎108.

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?

- 'How to Configure IPv4 Parameters' ⇨🗎35
- 'How to Configure IPv6 Parameters' ⇨🗎38
- 'How to Configure the DNS' ⇨🗎40
- 'How to Configure SNMP' ⇨🗎41
- 'How to Configure Bonjour' ⇨🗎42
- 'How to Configure POP3 and SMTP (only myUTN-80 and later)' ⇨🗎44
- 'How to Configure WLAN (myUTN-54 only)' ⇨🗎47

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: ⇨🗎13.

What Do You Want to Do?

□ 'Configuring IPv4 Parameters via the myUTN Control Center' ⇨🗎36

□ 'Configuring IPv4 Parameters via the SEH UTN Manager' ⇨🗎36

□ 'Configuring IPv4 Parameters via the InterCon-NetTool' ⇨🗎37

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 ⇨🗎36.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Table 2: IPv4 Parameters

Parameters	Description
DHCP BOOTP ARP/PING	Enables/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' ⇨🗎13.)* 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: ⇨🗎20.

☑ The UTN server is added to the selection list; see: ⇨🗎63.

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.

Configuring IPv4 Parameters via the InterCon-NetTool

Requirements

☑ The InterCon-NetTool is installed on the client, see: ⇨🗎28.

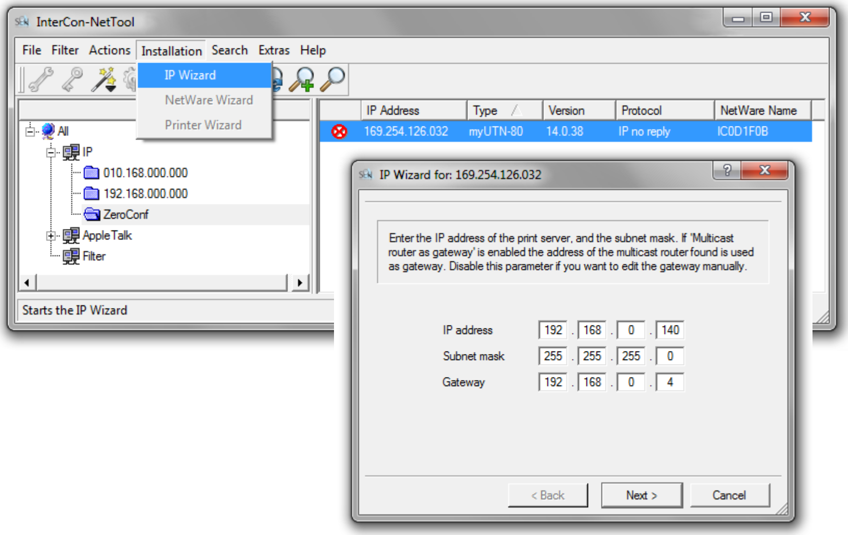
☑ The network scan via Multicast has been enabled in the InterCon-NetTool.

☑ The router in the network forwards multicast requests.

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the UTN server from the device list.*
   The UTN server is displayed in the device list under 'ZeroConf' with an IP address from the address range (169.254.0.0/16) which is reserved for ZeroConf.
3. *Select* **Installation – IP Wizard** *from the menu bar.*
   The IP Wizard is started.
4. *Follow the instructions of the Wizard.*

↳ The settings are saved.



IP Address	Type	Version	Protocol	NetWare Name
169.254.126.032	myUTN-80	14.0.38	IP no reply	IC0D1F0B

Enter the IP address of the print server, and the subnet mask. If 'Multicast router as gateway' is enabled the address of the multicast router found is used as gateway. Disable this parameter if you want to edit the gateway manually.

IP address 192 . 168 . 0 . 140
Subnet mask 255 . 255 . 255 . 0
Gateway 192 . 168 . 0 . 4

Fig. 7: InterCon-NetTool - IP Wizard

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 common IPv4. 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 ⇨🗎40.*
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.
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 ⇨🗎41.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Table 4: DNS Parameters

Parameters	Description
DNS	Enables/disables DNS.
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.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – SNMP***.*
3. *Configure the SNMP parameters; see: Table 5* ⇨🗎*42.*
4. *Click* **Save & Restart** *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.
User name	Defines the name of the SNMP user.
Password	Defines the password of the SNMP user.
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' ⇨🗎14) 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 ⇨🗎43.*
4. *Click* **Save & Restart** *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 (⇨🗎57) and the remote maintenance via email (⇨🗎31) will work properly.

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 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 to administer the UTN server via email and to run the notification service.

What Do You Want to Do?

□ 'Configuring POP3' ⇨🗎44

□ 'Configuring SMTP' ⇨🗎45

Configuring POP3

☞ Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – Email***.*
3. *Configure the POP3 parameters; see: Table 7 ⇨🗎44.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Table 7: POP3 Parameters

Parameters	Description
POP3	Enables/disables the POP3 functionality.
POP3 - Server name	Defines a POP3 server via the IP address or the host name. *The host name can only be used if a DNS server was configured beforehand.*

Parameters	Description
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 ⇨ 🗎80.
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

☞ Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK - Email***.*
3. *Configure the SMTP parameters; see: Table 8 ⇨ 🗎45.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Table 8: SMTP Parameters

Parameters	Description
SMTP - Server name	Defines an 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.

Parameters	Description
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 ⇨ 🗎80.*
SMTP - Sender name	Defines the email address used by the UTN server to send emails. <u>Note:</u> 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* ⇨ 🗎89.
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* ⇨ 🗎89.
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 (myUTN-54 only)

The UTN server model 'myUTN-54' can handle WLAN. This allows you to wirelessly operate the UTN server 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-54 supports the standards IEEE 802.11b, IEEE 802.11g and IEEE 802.11n.

To make use of the radio technology the myUTN-54 has additional parameters ⇨🗎50. You can view the current WLAN settings in the myUTN Control Center under the menu item **NETWORK – WLAN.**

Connection Status

The following icons in the myUTN Control Center indicate the current connection status:

UTN server in the wireless network

UTN server in the wired network

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.

Authentication

You can check the identity of a device or user by means of an authentication method before they gain access to resources in the network. The UTN server offers different variants of EAP (Extensible Authentication Protocol) as authentication method. For further information; see: 'How to Use Authentication Methods' ⇨🗎96.

What Do You Want to Do?

- □ 'Using the UTN Server (myUTN-54) in a Wireless Network' ⇨🗎49
- □ 'Connecting the UTN Server to the Wired Network' ⇨🗎51

Using the UTN Server (myUTN-54) in a Wireless Network

To operate the UTN server in a wireless network, the WLAN and security settings of the UTN server must match those of the wireless network.

In order to configure the UTN server you must first establish a connection to a wired network by means of the network connector RJ-45; see: 'Quick Installation Guide'.

Requirements

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

☑ The UTN server is known to the wired network via its IP address, see: ⇨🗎13.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK – WLAN**.
   The available WLANs are shown in the network list. Decide in which WLAN you want to operate the UTN server.
3. *Configure the WLAN parameters in such a way that they match the parameters of the WLAN to be used; see: Table 9 ⇨🗎50.*
4. *Tick* **WLAN** *to enable the WLAN module in the UTN server.*
5. *Click* **Save & Restart** *to confirm.*
   The settings are saved.
6. *Remove the network cable (RJ-45) from the UTN server.*
   The connection to the wired network will be deactivated.

↳ The UTN server automatically switches to the WLAN mode.
The connection to the WLAN will be established.

If the UTN server gets a new IP address in the course of the network change, the connection to the myUTN Control Center will be interrupted.

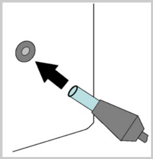
Table 9: WLAN Parameters

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	The transmission power of the UTN server can be defined using the parameter 'Roaming level'. The value 65 -dbm is preset. The parameter 'Roaming level' can only be configured in the 'Infrastructure' mode.

Parameters	Description
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.***
Encryption method	see: ’WLAN Security’ ⇨ 📄47
Authentication method	see: ’Authentication’ ⇨ 📄48

Connecting the UTN Server to the Wired Network

To establish a connection to a wired network, connect the network cable (RJ-45) to the UTN server. The UTN server automatically switches to the wired network.



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?

- 'How to Determine a Description' ⇨🗎53
- 'How to Configure the Device Time' ⇨🗎53
- 'How to Configure the UTN (SSL) Port' ⇨🗎54
- 'How to Assign a Name to a USB Device' ⇨🗎55
- 'How to Control the Power Supply for a USB Port (only myUTN-80 and later)' ⇨🗎55
- 'How to Compress the Data Stream of the USB Scanner (myUTN-130 only)' ⇨🗎56
- 'How to Use the Notification Service (only myUTN-80 and later)' ⇨🗎57
- 'How to Control the Access to Dongle-Protected Software (only myUTN-80) or USB Devices (only myUTN-150) via VLAN' ⇨🗎59

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 & Restart** *to confirm.*

↳ The data is saved.

To assign names to the connected USB devices, see: ⇨🗎55.

4.2 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***.*

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 & Restart** *to confirm.*

↳ The settings are saved.

4.3 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: ⇨🗎103.

ℹ 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 client receive the current port number, the 'SNMPv1' parameter must be activated; see ⇨🗎41.

☞ 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 & Restart** *to confirm.*

↳ The settings are saved.

4.4 How to Assign a Name to a USB Device

You can assign any name to the USB device. 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 – USB port***.*
3. *Enter the preferred name into the* **Name** *field.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

4.5 How to Control the Power Supply for a USB Port (only myUTN-80 and later)

You can enable or disable the power supply of a USB port. This allows you to establish or interrupt the power supply for a USB device.

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

Benefits and Purpose

This function allows you to turn a USB device on or off 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 ports.

Proceed as follows:

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

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

4.6 How to Compress the Data Stream of the USB Scanner (myUTN-130 only)

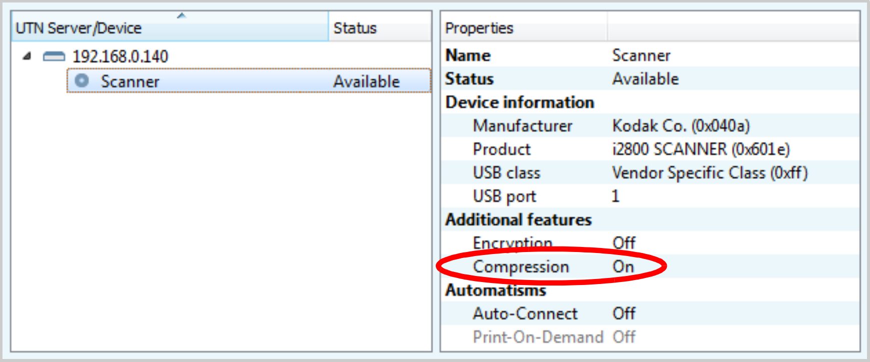
The myUTN-130 has a hardware-based data compression. This allows you to compress the data stream of the USB scanner. The compression process reduces the size of the data stream in order to reduce the transmission volume and the transmission time.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **DEVICE – USB port***.*
3. *Tick* **Compression***.*
4. *Click* **Save** *to confirm.*

↳ The data stream of the USB scanner will be compressed.

The compression will be displayed client-side in the SEH UTN Manager under the device properties.



UTN Server/Device	Status
192.168.0.140	
Scanner	Available

Properties	
Name	Scanner
Status	Available
Device information	
Manufacturer	Kodak Co. (0x040a)
Product	i2800 SCANNER (0x601e)
USB class	Vendor Specific Class (0xff)
USB port	1
Additional features	
Encryption	Off
Compression	On
Automatisms	
Auto-Connect	Off
Print-On-Demand	Off

Fig. 8: SEH UTN Manager - Compression

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 email 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 device.

What Do You Want to Do?

□ 'Configuring the sending of status emails' ⇨🗎57

□ 'Configuring event notifications via email' ⇨🗎58

□ 'Configuring event notifications via SNMP traps' ⇨🗎58

Configuring the sending of status emails

Requirements

☑ SMTP parameters have been configured on the UTN server, see: ⇨🗎44.

☑ A DNS server has been configured on the UTN server, see: ⇨🗎40.

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 & Restart** *to confirm.*

↳ The settings are saved.

Configuring event notifications via email

Requirements

☑ SMTP parameters have been configured on the UTN server, see: ⇨🗎44.

☑ A DNS server has been configured on the UTN server, see: ⇨🗎40.

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 & Restart** *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 & Restart** *to confirm.*

↳ The settings are saved.

4.8 How to Control the Access to Dongle-Protected Software (only myUTN-80) or USB Devices (only myUTN-150) via VLAN

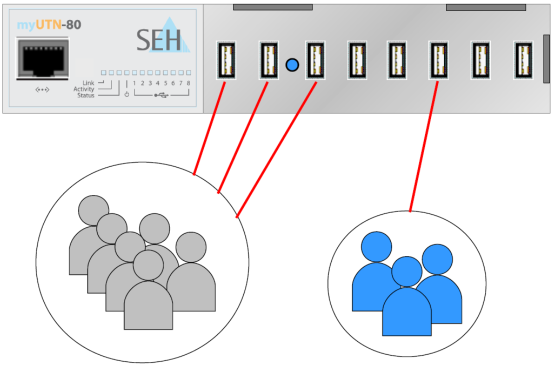
The UTN server supports the use of VLAN (Virtual Local Area Network). It is useful to divide a physical network into VLANs for performance and security reasons.

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) or USB devices (myUTN-150). 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.

Fig. 9: USB port based assignment of VLANs

What Do you Want to Do?

□ 'Entering VLANs' ⇨🗎60

□ 'Allocating VLAN to a USB port' ⇨🗎60

Entering VLANs

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **NETWORK - IPv4 VLAN**.
3. *Configure the VLAN parameters; see: Table 10* ⇨🗎*60.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 10: IPv4 VLANParameters

Parameters	Description
VLAN	Enables/disables the forwarding of VLAN data.
IP address	IP address of the UTN server within the VLAN.
Subnet mask	Subnet mask of the UTN server within the VLAN.
VLAN ID	ID for the identification of the VLAN (0–4096). *0 = untagged multihomed IP addresses*

Allocating 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 device.

What Information Do You Need?

- 'How to Find UTN Servers/USB Devices in the Network' ⇨🗎61
- 'How to Add USB Devices to the Selection List' ⇨🗎63
- 'How to Connect a USB Device to a Client' ⇨🗎64
- 'How to Cut the Connection between the USB Device and the Client' ⇨🗎65
- 'How to Request an Occupied Device' ⇨🗎66
- 'How to Automate Device Connections and Program Starts' ⇨🗎67
- 'How to Get Information about the USB Device' ⇨🗎72
- 'How to Manage Selection Lists for Several Participants' ⇨🗎73

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' ⇨🗎62

□ 'Scanning the Network' ⇨🗎62

Defining Search Parameters

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎20.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Windows: Select* **Program – Options** *from the menu bar.*
   Mac: Select **SEH UTN Manager – Preferences** *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** *to confirm.*

↳ The settings are saved.

Scanning the Network

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎20.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Select* **Selection List – Edit** *from the menu bar.*
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 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

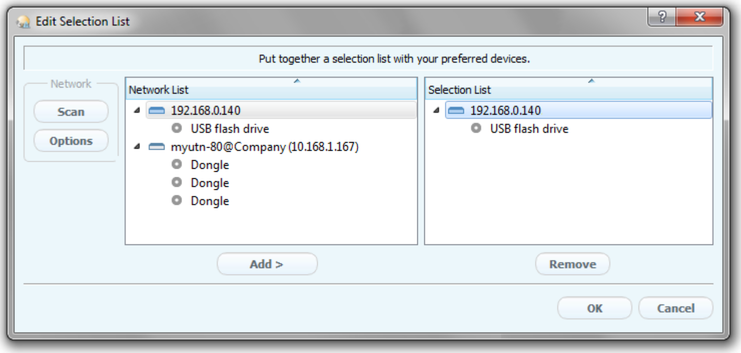
☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎20.

☑ 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 devices are displayed in the selection list.



Put together a selection list with your preferred devices.

Network List:
- 192.168.0.140
  - USB flash drive
- myutn-80@Company (10.168.1.167)
  - Dongle
  - Dongle
  - Dongle

Selection List:
- 192.168.0.140
  - USB flash drive

Fig. 10: 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 Device to a Client

A USB device that is connected to the UTN server can be connected to the client. The USB device can then be used by the client as if the USB device was directly connected to the client.

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎20.

☑ The USB device is shown in the selection list; see: ⇨🗎63.

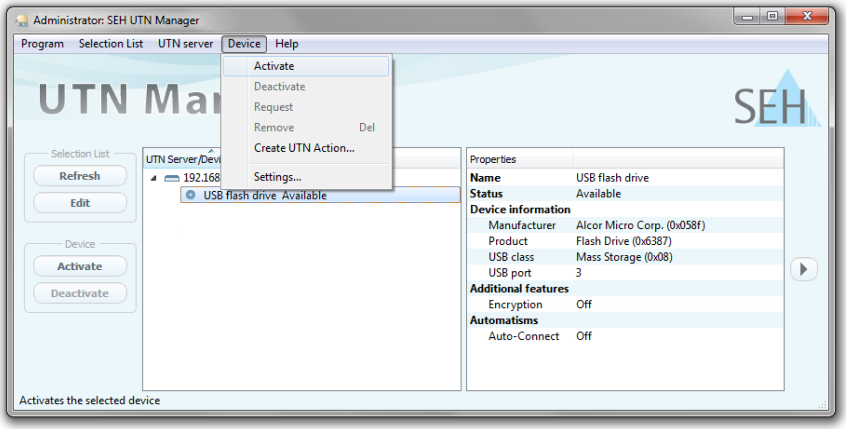
☑ All provisions (driver installation, etc.) necessary to operate the USB device locally (i.e. connected directly to the client) should have been met on the client. Ideally, the USB device has been connected and operated on the client locally according to the instructions of the manufacturer.

☑ The USB device is <u>not</u> connected to another client.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Mark the relevant USB device in the selection list.*
3. *Select* **Device – Activate** *from the menu bar.*

↳ The connection will be established.



Properties	
Name	USB flash drive
Status	Available
Device information	
Manufacturer	Alcor Micro Corp. (0x058f)
Product	Flash Drive (0x6387)
USB class	Mass Storage (0x08)
USB port	3
Additional features	
Encryption	Off
Automatisms	
Auto-Connect	Off

Fig. 11: SEH UTN Manager - Activating the Device

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

Close the connection to the USB device when the device is no longer needed. This allows other network participants to access the 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: ⇨🗎20.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Mark the relevant USB device in the selection list.*
3. *Select* **Device – 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 device that is being actively used by another user.

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

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎20.

☑ The SEH UTN Manager is installed on the client of the user who uses the USB device; see: ⇨🗎20.

☑ The SEH UTN Manager is be executed on both clients.

☑ The USB device is shown in the selection list; see: ⇨🗎63.

Proceed as follows:

1. *Mark the relevant USB device in the selection list.*
2. *Select* **Device – Request** *from the menu bar.*

↳ The device request is sent to the user who uses the device.

5.6 How to Automate Device Connections and Program Starts

You can automate device connections and program starts in many ways. This is done by various automatisms.

What Do You Want to Do?

- □ 'Activating the Device Automatically after the SEH UTN Manager Program Start (Auto-Connect)' ⇨🗎67
- □ 'Automatically disconnect the connection to a device after the time defined (Auto-Disconnect)' ⇨🗎68
- □ 'Automatically Creating a Connection between the USB Device and the Client when a Print Job is Received (Print-On-Demand)' ⇨🗎69
- □ 'Creating a UTN Action: Automated Device Connections and Program Starts without the SEH UTN Manager Interface' ⇨🗎70
- □ 'Using the Additional Tool 'utnm'' ⇨🗎140

Activating the Device Automatically after the SEH UTN Manager Program Start (Auto-Connect)

This functionality allows for the automatic activation of a device connection after the launch of the SEH UTN Manager.

Can only be configured by an administrator.

Requirements

- ☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎20.
- ☑ The USB device is shown in the selection list; see: ⇨🗎63.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Mark the relevant USB device in the selection list.*
3. *Select* **Device – Settings** *from the menu bar.*

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 connection to a device after the time defined (Auto-Disconnect)

This function allows you to automatically disconnect the connection to a USB device 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 devices on a UTN server.

Two minutes before the expiration of the defined time, the user will receive a note 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 device after the automatic disconnection. For this purpose, set up a notification if the device is available; see: ⇨🗎72.

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

Can only be configured by an administrator.

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎20.

☑ The UTN server is displayed in the 'Automatic Device Disconnect' area; see: ⇨🗎63.

Proceed as follows:

1. *Start the SEH UTN Manager.*

2. *Windows: Select* **Program – Options** *from the menu bar.*
   Mac: Select **SEH UTN Manager – Preferences** *from the menu bar.*
   The **Options** *dialog appears.*
3. *Select the* **Automatisms** *tab.*
4. *In the* **Automatic Device 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.

Automatically Creating a Connection between the USB Device and the Client when a Print Job is Received (Print-On-Demand)

A connection between the USB device (printer or MFP) and the client will be automatically created as soon as a print job is received. After completion of the print job, the connection will be automatically disabled.

Can only be configured by an administrator.

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎20.

☑ The USB device is shown in the selection list; see: ⇨🗎63.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Mark the relevant USB device in the selection list.*
3. *Select* **Device – Settings** *from the menu bar.*
4. *Tick* **Print-On-Demand***.*
5. *Click* **OK***.*

↳ The setting will be saved.

In order to use this option, the printer must be set up on this client (driver installation).

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

You can create UTN actions. UTN Actions are small programs used for the automatic activation and deactivation of device connections. UTN Actions can also automate the starting and closing of an application in combination with a device connection.

The process defined in the UTN action will run automatically after the execution of the file. Since the 'SEH UTN Service' is active in the background, the user is not required to start the SEH UTN Manager interface. I.e., UTN Actions can be used with the complete and minimal version.

A wizard within the SEH UTN Manager will guide you through the process of creating a UTN Action. The following UTN Actions can be created:

- **UTN Actions which activate and deactivate the device**
  The wizard will automatically create one UTN Action for the activation and one UTN Action for the deactivation of the device. Both UTN Actions will be saved to the desktop.
- **UTN Action which starts an application and activates the device**
  After the selection of an application by the user, the wizard will automatically create an action which starts an application and activates the device. Additionally, you can specify a device deactivation after the closing of the application.
- **Custom UTN Action (Experts only)**
  With the help of the wizard, a custom UTN Action can be created. You can create:
  - UTN Actions which activate and deactivate the device. You can define additional options.
  - A script for the start of the application and activation of the device. Additionally, you can specify a delay for the start of the application, the deactivation of the device after the closing of the application and additional options. The script will be created automatically and can then be edited. Finally, the complete UTN Action will be created automatically by the SEH UTN Manager and saved by the user.

Requirements

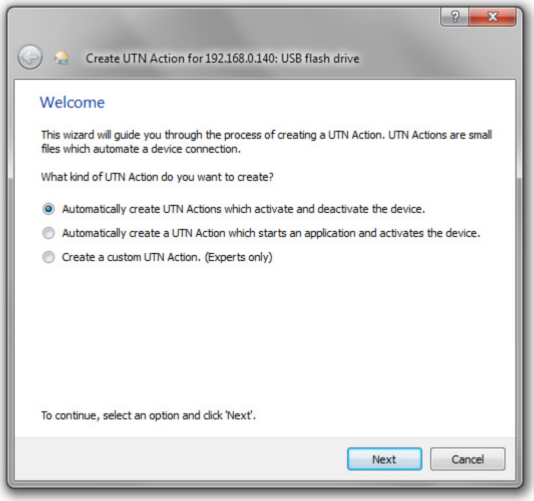
☑ The USB device is shown in the selection list; see: ⇨🗎63.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Mark a USB device in the selection list.*
3. *Select* **Device – Create UTN Action** *from the menu bar.*
   The dialog **Create UTN Action** *will be started.*

4. *Follow the instructions of the Wizard.*

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



Create UTN Action for 192.168.0.140: USB flash drive

Welcome

This wizard will guide you through the process of creating a UTN Action. UTN Actions are small files which automate a device connection.

What kind of UTN Action do you want to create?

● Automatically create UTN Actions which activate and deactivate the device.

○ Automatically create a UTN Action which starts an application and activates the device.

○ Create a custom UTN Action. (Experts only)

To continue, select an option and click 'Next'.

Fig. 12: **Create UTN Action** dialog

Tip 1

After the saving, shortcuts (Windows) respectively apps (Mac) can be moved to any location and renamed.

Tip 2

Experts only (UTN Actions which activate and deactivate the device): In Windows the target of the shortcut contains the command line. The command line can be edited, if required. In Mac the app script can be edited, if required (path: `Contents/Resources/script`).

Tip 3

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

5.7 How to Get Information about the USB Device

You can view the status information of the USB device. You can also configure automatic messages. You will be informed when a USB device becomes available.

What Do You Want to Do?

□ 'Displaying Status Information' ⇨🗎72

□ 'Configuring Messages (only Windows at present)' ⇨🗎72

Displaying Status Information

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎20.

☑ The USB device is shown in the selection list; see: ⇨🗎63.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Mark the relevant USB device in the selection list.*

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

Configuring Messages (only Windows at present)

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎20.

☑ The USB device is shown in the selection list; see: ⇨🗎63.

Proceed as follows:

1. *Start the SEH UTN Manager.*
2. *Mark the relevant USB device in the selection list.*
3. *Select* Device – Settings *from the menu bar.*
   The Device Settings *dialog appears.*
4. *Tick the option under* Messages*.*
5. *Click* OK*.*

↳ The setting will be saved.
If a network participant disables the connection to the USB device a '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. The displayed USB devices can be connected to the client and can be used. The selection list can be edited and configured according to your needs by adding und deleting the required devices.

Selection lists are saved as 'SEH UTN Manager .ini' files.

Two selection list types are available:

- global selection list
- user-specific selection list

Benefits and Purpose

By means of the selection list type 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.

Alternatively, each user can use a user-specific selection list. 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

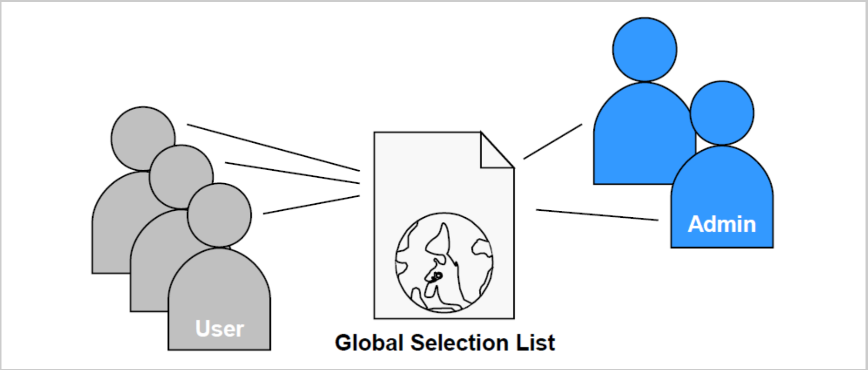


Fig. 13: Global Selection List

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

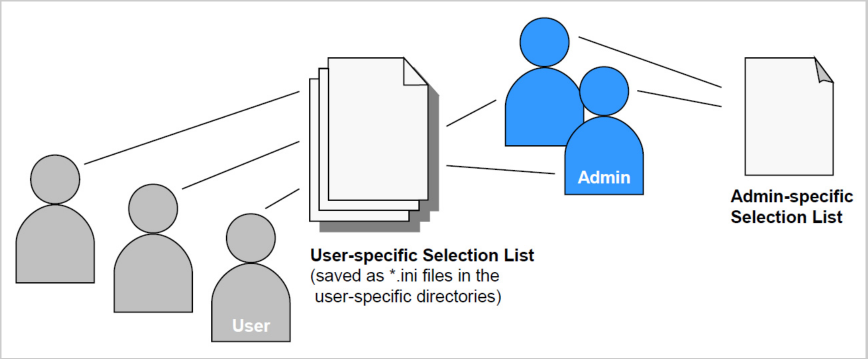

User
User-specific Selection List
(saved as *.ini files in the
user-specific directories)
Admin
Admin-specific
Selection List

Fig. 14: 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:
  Windows: `%APPDATA%\SEH Computertechnik GmbH\SEH UTN Manager.ini`
  Mac: `$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`

Where `%APPDATA%` is an environment variable by Windows for the user. By means of the command line the path for the current user can be determined as follows: `echo %APPDATA%`

Example:

Windows XP:

`echo %APPDATA%` returns `C:\Users\User name\AppData\Roaming`

+

`\SEH Computertechnik GmbH\SEH UTN Manager.ini`

Complete path to the .ini file:

```
C:\Users\User name\AppData\Roaming\SEH Computertechnik
GmbH\SEH UTN Manager.ini
```

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

Example:

Mac OS X 10.7.5 (Lion):

`echo $HOME` returns `/Users/User name`

+

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

Complete path to the .ini file:

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

What Do You Want to Do?

□ 'Providing the Global Selection List to All Users' ⇨🗎76

□ 'Providing User-Specific Selection Lists' ⇨🗎76

□ 'Providing Users with a Predefined Selection List' ⇨🗎77

□ 'Protecting the user-specific selection list' ⇨🗎78

Providing the Global Selection List to All Users

Requirements

☑ The SEH UTN Manager (complete version) is installed on the client; see: ⇨🗎20.

Proceed as follows:

1. *Start the SEH UTN Manager (as administrator).*
2. *Compose the selection list; see: 'How to Add USB Devices to the Selection List' ⇨🗎63.*
3. *Windows: Select* **Program – Options** *from the menu bar.*
   Mac: Select **SEH UTN Manager – Preferences** *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: ⇨🗎20.

Proceed as follows:

1. *Start the SEH UTN Manager (as administrator).*

2. *Windows: Select* **Program – Options** *from the menu bar.*
   Mac: Select **SEH UTN Manager – Preferences** *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' ⇨🗎74).

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: ⇨🗎20.

Proceed as follows:

1. *Start the SEH UTN Manager (as administrator).*
2. *Compose the selection list for the user; see: 'How to Add USB Devices to the Selection List'* ⇨🗎*63.*
3. *Windows: Select* **Program – Options** *from the menu bar.*
   Mac: Select **SEH UTN Manager – Preferences** *from the menu bar.*
   The **Options** *dialog appears.*
4. *Select the* **Selection List** *tab.*
5. *Tick* **User selection list***.*
6. *Click* **OK***.*
   The setting is 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:*
   Windows:`%APPDATA%\SEH Computertechnik GmbH\SEH UTN Manager.ini`
   Mac: `$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
   (See: 'User-Specific Selection List' ⇨🗎*74.*)

↳ 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:

Windows: `%APPDATA%\SEH Computertechnik GmbH\SEH UTN Manager.ini`
Mac: `$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
(See: 'User-Specific Selection List' ⇨🗎74)

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' ⇨🗎80
- 'How to Control Access to the myUTN Control Center' ⇨🗎82
- 'How to Control Access to the UTN Server (TCP Port Access Control)' ⇨🗎84
- 'How to Control Access to USB Devices (only myUTN-80 and later)' ⇨🗎86
- 'How to Use Certificates Correctly' ⇨🗎89
- 'How to Use Authentication Methods' ⇨🗎96
- 'How to Encrypt Data Transfer' ⇨🗎103

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 (⇨🗎44)
- Email: SMTP (⇨🗎44)
- Web access to the myUTN Control Center: HTTPS (⇨🗎82)
- Data transfer between the clients and the UTN server (and the connected USB devices): USB port (⇨🗎103)

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 protocol used (SSLv2, SSLv3, TLSv1).

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: ⇨🗎107.

The following encryption levels can be selected:

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

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 & Restart** *to confirm.*
5. The setting will be saved.

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

6.2 How to Control Access to the myUTN Control Center

You can protect the administrative Web and SNMP access to the myUTN Control Center.

What Do You Want to Do?

- □ 'Specifying the Permitted Web Connection Type' ⇨🗎82
- □ 'Protecting the web access via password' ⇨🗎83
- □ 'Granting/denying the web access via VLAN addresses (only myUTN-80 and myUTN-150)' ⇨🗎83
- □ 'Granting/denying the SNMP access via VLAN addresses (only myUTN-80 and myUTN-150)' ⇨🗎84

The myUTN Control Center can also be protected by the SNMP security concept. The concept includes administration of user groups and access rights. For further information; see: 'How to Configure SNMP' ⇨🗎41.

Specifying the Permitted Web Connection Type

Types of Connection (HTTP/HTTPS)

The web access to the myUTN Control Center can be secured by selecting the permitted types of connection (HTTP/HTTPS).

If HTTPS is exclusively chosen as the connection type, the administrative web access to the myUTN Control Center is protected via SSL/TLS. The cipher strength is defined via the encryption level ⇨🗎80.

SSL/TLS requires a certificate to check the identity of the UTN server. During a so-called 'handshake', the client asks for a 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. *Tick* **HTTP/HTTPS** *or* **HTTPS only** *in the* **Web** *area.*

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

↳ The setting will be saved.

Protecting the web access via password

You can use a password to protect the myUTN Control Center against unauthorized web access. If a password is set, only the start page of the myUTN Control Center can be visited and displayed. If you select a menu item, you will be asked to enter a password.

You will also be asked to enter a non-definable user name. Leave this field blank at the password prompt.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Device access**.
3. *In the* **web** *area, enter a password into the* **Password** *box.*
4. *Repeat the password.*
5. *Click* **Save & Restart** *to confirm.*

↳ The setting will be saved.

Granting/denying the web access via VLAN addresses (only myUTN-80 and myUTN-150)

You can deny the administrative web access to the myUTN Control Center via a VLAN address.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Device access**.
3. *Tick/clear* **VLAN access** *in the* **Web** *area.*
4. *Click* **Save & Restart** *to confirm.*

↳ The setting will be saved.

Granting/denying the SNMP access via VLAN addresses (only myUTN-80 and myUTN-150)

You can deny the administrative SNMP access to the myUTN Control Center via a VLAN address.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Device access**.
3. *Tick/clear* **VLAN access** *in the* **SNMP** *area.*
4. *Click* **Save & Restart** *to confirm.*

↳ The setting will be saved.

6.3 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 locked 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 access-authorized network elements' IP addresses or MAC addresses (hardware addresses) 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 on.*
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: ⇨🗎111.

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.

6.4 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 entering the key, the USB device that is connected to the USB port is protected against unwanted access.

The USB device will no longer be shown in the SEH UTN Manager. This means that a user will not be able to make changes to the USB device or to establish a connection between the client and the USB device.

To make the 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.

What Do You Want to Do?

☐ 'Blocking access to USB devices' ⇨🗎87

☐ 'Unblocking access to USB devices' ⇨🗎87

☐ 'Specifying the Device Assignment on the USB Port' ⇨🗎88

☐ 'Disabling the USB Port Access Control' ⇨🗎88

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 device is shared. The USB device is 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* **Save** *to confirm.*

↳ The settings are saved. Only the USB device that is displayed under 'USB port' 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'.

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.

6.5 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' ⇨🗎98.
- to authenticate the UTN server/client if the administrative access to the myUTN Control Center is protected via HTTPS (SSL/TLS).

If you want to use certificates, it is advisable to protect the administrative access to the myUTN Control Center by a password so that certificates on the UTN server cannot be deleted by unauthorized persons; see: ⇨🗎83.

Which Certificates Are available?

Both self-signed certificates and CA 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 CA certificate as soon as possible.
- **Self-signed certificates** have a digital signature that has been created by the UTN server.
- **CA certificates** are certificates that have been signed by a certification authority (CA).
- The authenticity of the CA certificate can be verified by means of a so-called **root certificate** issued by the certification

authority. The root certificate is stored on an authentication server in the network.

- **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, Microsoft Outlook, 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

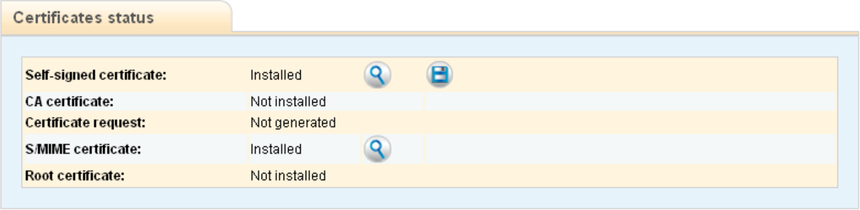
- 1 CA certificate or PKCS#12 certificate

- 1 Root certificate

- 1 S/MIME certificate (only myUTN-80 and later)

You can also generate a certificate request for a CA certificate. All certificates can be deleted separately. Existing certificates will be overridden when installing or generating new certificates.

A PKCS#12 certificate can only be installed if there are currently no certificate requests or CA certificates installed.



Certificates status

Self-signed certificate:	Installed
CA certificate:	Not installed
Certificate request:	Not generated
S/MIME certificate:	Installed
Root certificate:	Not installed

Fig. 15: myUTN Control Center - Certificates

What Do You Want to Do?

□ 'Displaying Certificates' ⇨🗎91

□ 'Creating a Self-Signed Certificate' ⇨🗎91

□ 'Creating a Certificate Request for CA Certificates' ⇨🗎92

- □ 'Saving the CA Certificate in the UTN Server' ⇨🗎93
- □ 'Saving the Root Certificate in the UTN Server' ⇨🗎94
- □ 'Saving the PKCS#12 Certificate in the UTN Server' ⇨🗎94
- □ 'Saving S/MIME Certificates in the UTN Server (only myUTN-80 and later)' ⇨🗎95
- □ 'Deleting Certificates' ⇨🗎96

Displaying Certificates

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

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

ℹ If a self-signed certificate has already been created on the UTN server, you must first delete the certificate; see: ⇨🗎96.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Certificates**.
3. *Click* **Self-signed certificate**.
4. *Enter the relevant parameters, see: Table 11 ⇨🗎92.*
5. *Click* **Install**.

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

Table 11: 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 CA Certificates

As a preparation for the use of a CA certificate, a certificate request that has to be sent to the certification authority can be created in the UTN server. The certification authority will then create a CA certificate on the basis of the certificate request. The certificate must be in base64 format.

If a certificate request has already been created on the UTN server, you must first delete the certificate request; see: ⇨🗎96.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Certificates**.
3. *Click* **Certificate request**.
4. *Enter the required parameters, see: Table 11 ⇨🗎92.*
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 CA certificate has been received, it must be saved in the UTN server; see: ⇨🗎93.

Saving the CA Certificate in the UTN Server

If a CA certificate has already been installed on the UTN server, it will be overwritten.

Requirements

☑ A certificate request has been created at an earlier date; see: ⇨🗎92.

☑ 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 CA certificate.*
6. *Click* **Install***.*

↳ The CA certificate will be saved in the UTN server.

Saving the Root Certificate in the UTN Server

The UTN server offers a number of authentication methods to verify its identity in a network. If you use the authentication method 'EAP-TLS', you must install the root certificate of the authentication server (RADIUS) on the UTN server; see: ⇨🗎98.

If a root certificate has already been installed on the UTN server, it will be overwritten.

Requirements

☑ The certificate must be in base64 format.

Proceed as follows:

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

↳ The root certificate is saved in the UTN server.

Saving 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, it will be overwritten.

Requirements

☑ The certificate must be in base64 format.

☑ No certificate request may exist. To delete the certificate request; see: ⇨🗎96.

☑ No CA certificate may be installed. To delete a CA certificate; see: ⇨🗎96.

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – Certificates**.
3. *Click* **PKCS#12 certificate**.
4. *Click* **Browse**.
5. *Specify 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, it will be overwritten.

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.

Deleting Certificates

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.

6.6 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' ⇨🗎97

□ 'Configuring EAP-TLS' ⇨🗎98

□ 'Configuring EAP-TTLS' ⇨🗎99

□ 'Configuring PEAP' ⇨🗎100

□ 'Configuring EAP-FAST' ⇨🗎101

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.

Basic Functions

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 makes sure that the UTN server gets access to protected networks.

Basic Functions

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.

ℹ

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: ⇨🗎107.

Procedure

- Create a certificate request on the UTN server; see: ⇨🗎92.
- Create a CA certificate using the certificate request and the authentication server.
- Install the CA certificate on the UTN server; see: 'Saving the CA Certificate in the UTN Server' ⇨🗎93.
- Install the root certificate of the authentication server on the UTN server; see: 'Saving the Root Certificate in the UTN Server' ⇨🗎94.
- 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. *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 authentication. This ensures that the UTN server gets access to protected networks.

Basic Functions

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 und 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 certificate of the RADIUS server on the UTN server (⇨🗎94).*
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.

Basic Functions

In the case of PEAP (compare EAP-TTLS, see ⇨🗎99), 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 certificate (⇨🗎94) of the RADIUS server on the UTN server.*
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.

Basic Functions

EAP-FAST uses (as in the case of EAP-TTLS, see ⇨🗎99) 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.

6.7 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: ⇨🗎54.

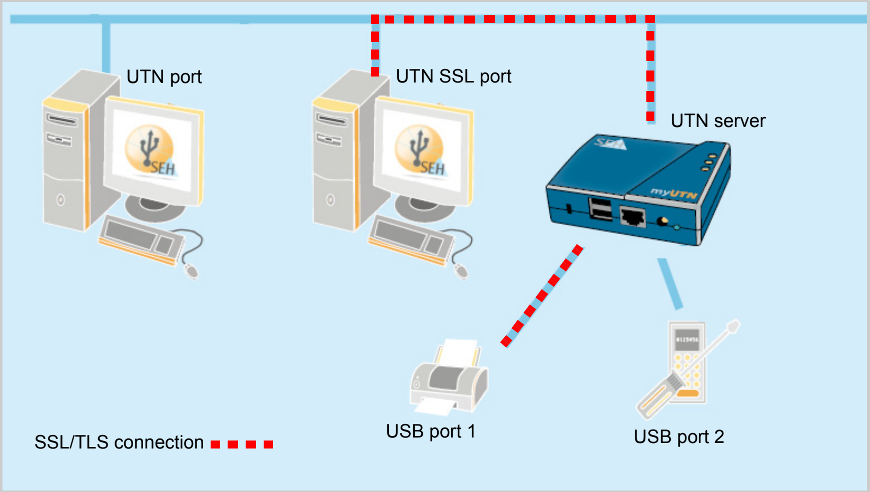


Fig. 16: UTN Server - SSL/TLS Connection in the Network

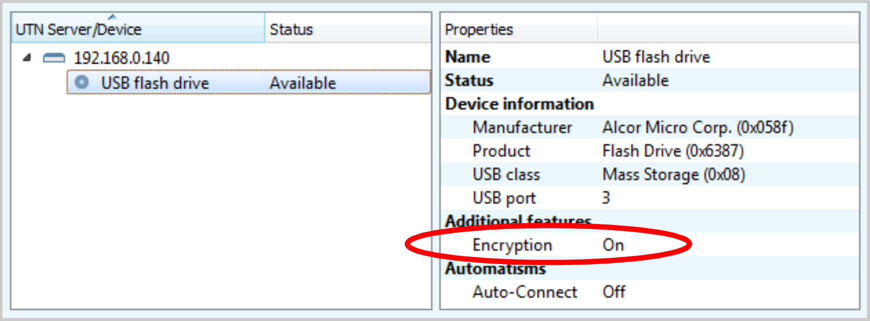
To use an SSL/TLS connection you must enable the encryption at the relevant USB port. The cipher strength is defined via the encryption level ⇨🗎80.

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 the device properties.



UTN Server/Device	Status
192.168.0.140	
USB flash drive	Available

Properties	
Name	USB flash drive
Status	Available
Device information	
Manufacturer	Alcor Micro Corp. (0x058f)
Product	Flash Drive (0x6387)
USB class	Mass Storage (0x08)
USB port	3
Additional features	
Encryption	On
Automatisms	
Auto-Connect	Off

Fig. 17: 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)' ⇨🗎105
- 'How to Reset the UTN Parameters to their Default Values' ⇨🗎107
- 'How to Perform an Update' ⇨🗎110
- 'How to Restart the UTN Server' ⇨🗎111

7.1 How to Secure UTN Parameters (Backup)

All parameter values of the UTN server (exception: passwords) are saved in the parameters file '<Default-name>_parameter.txt'.

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.

What Do You Want to Do?

☐ 'Displaying Parameter Values' ⇨🗎106

☐ 'Saving the Parameter File' ⇨🗎106

☐ 'Loading the Parameter File onto the UTN Server' ⇨🗎106

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 'Parameter List' ⇨🗎116.

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>_parameter.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.

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.

Resetting the parameters may lead to a change in the IP address of the UTN server and the connection to the myUTN Control Center can get lost.

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 Parameters via the myUTN Control Center' ⇨🗎107

□ 'Resetting Parameters via the InterCon-NetTool' ⇨🗎108

□ 'Resetting the Parameters via the Reset Button' ⇨🗎108

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

Resetting Parameters via the myUTN Control Center

Proceed as follows:

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

↳ The parameters are reset.

Resetting Parameters via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the UTN server from the device list.*
3. *Select* **Actions – Default Settings** *from the menu bar.*
4. *Click* **Finish***.*

↳ The parameters are reset.

Resetting the Parameters via the Reset Button

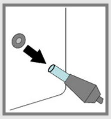
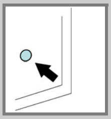
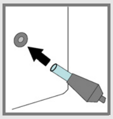
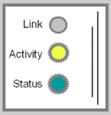
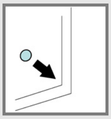
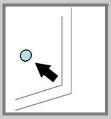
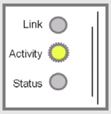
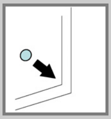
LEDs, the reset button and various ports can be found on the UTN server. These components are described in the 'Quick Installation Guide'.

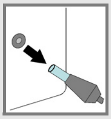
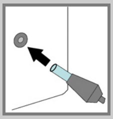
Using the reset button you can reset the UTN server's parameter values to their default setting. The reset process can be divided into two phases:

- During phase 1, the device is forced into the reset mode. During the reset mode, the parameters are reset.
- The second phase describes the restart of the device.

IMPORTANT: The reset mode is indicated by the synchronous blinking of the activity LED (yellow) and the status LED (green) and last for about five intervals.
You must release the reset button within this time frame, otherwise the device switches to the BIOS mode. If this happens, try the reset again.

The phases are described in the following:

[Phase 1] Reset	
	Switch off the UTN server (interrupt the power supply).
	Press and hold the reset button.
	Switch on the UTN server (establish the power supply).
	Wait until the activity LED and status LED blink synchronously. *The reset mode has been activated.*
	Release the reset button for about 2 seconds. *The LEDs blink alternatingly.*
	Press and hold the reset button again. *The LEDs blink synchronously.*
	*After a few seconds, only the activity LED will blink.*
	Release the reset button.

[Phase 2] Restart	
	Switch off the UTN server (interrupt the power supply).
	Switch on the UTN server (establish the power supply).

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 existing firmware/software will be overwritten and replaced by a new version. The parameter default settings of the device remain unchanged.

When Is an Update Recommended?

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

Check the installed software and firmware version on the UTN server. You will find the version number on the myUTN Control Center homepage or in the product list in the InterCon-NetTool.

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/myutn.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' ⇨🗎111

□ 'Restarting the UTN Server via the InterCon-NetTool' ⇨🗎111

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 InterCon-NetTool

☞ Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the UTN server from the device list.*
3. *Select* **Actions – Restart** *from the menu bar.*
4. *Click* **Finish**.

↳ 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?

- 'Glossary' ⇨🗎113
- 'Parameter List' ⇨🗎116
- 'LED Display' ⇨🗎132
- 'SEH UTN Manager - Function Overview' ⇨🗎133
- 'Troubleshooting' ⇨🗎136
- 'Additional Tool 'utnm'' ⇨🗎140
- 'List of Figures' ⇨🗎145
- 'Index' ⇨🗎146

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' ⇨🗎113
- 'InterCon-NetTool' ⇨🗎113
- 'SEH UTN Manager' ⇨🗎113

Network Technology

- 'Hardware Address' ⇨🗎114
- 'IP Address' ⇨🗎114
- 'Host Name' ⇨🗎115
- 'Gateway' ⇨🗎115
- 'Subnet Mask' ⇨🗎115
- 'Default Name' ⇨🗎115

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 (Internet Explorer, Mozilla Firefox, Safari).

InterCon-NetTool

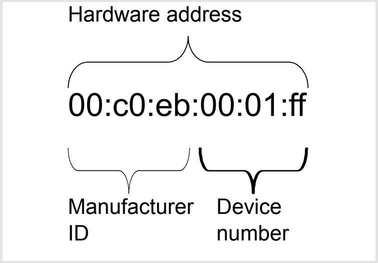
The software InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices within a predefined network.

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 USB devices in the network and establishes a connection between the client and the 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, in the SEH UTN Manager or in the InterCon-NetTool.

The use of separators within the hardware address depends on the platform. Note the following conventions when entering the hardware address:

Operating system	Representation	Example
Windows	Hyphen	00-c0-eb-00-01-ff
UNIX	Colon or period	00:c0:eb:00:01:ff or 00.c0.eb.00.01.ff

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

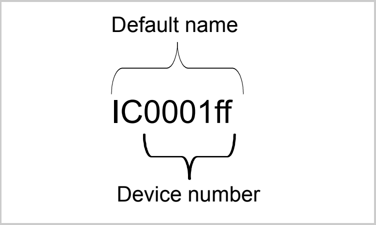
Using a gateway, you can address IP addresses from external networks. If you want to use a gateway, you can configure the relevant parameter in the UTN server via the myUTN Control Center.

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 subnetwork, 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 or in the InterCon-NetTool.

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?

- 'Parameter List - IPv4' ⇨🗎117
- 'Parameter List - IPv4 VLAN (only myUTN-80 and myUTN-150)' ⇨🗎117
- 'Parameter List – IPv6' ⇨🗎118
- 'Parameter List - Bonjour' ⇨🗎119
- 'Parameter List - SSL connections' ⇨🗎119
- 'Parameter List - Web access' ⇨🗎119
- 'Parameter List - TCP port access' ⇨🗎120
- 'Parameter List - UTN port' ⇨🗎120
- 'Parameter List - Encryption' ⇨🗎121
- 'Parameter List - USB port access (only myUTN-80 and later)' ⇨🗎121
- 'Parameter List - USB port' ⇨🗎122
- 'Parameter List - DNS' ⇨🗎122
- 'Parameter List - SNMP' ⇨🗎123
- 'Parameter List - Date/Time' ⇨🗎124
- 'Parameter List - Description' ⇨🗎124
- 'Parameter List - Authentication' ⇨🗎125
- 'Parameter List - POP3 (only myUTN-80 and later)' ⇨🗎126
- 'Parameter List - SMTP (only myUTN-80 and later)' ⇨🗎127
- 'Parameter List – Notification (only myUTN-80 and later)' ⇨🗎128
- 'Parameter List - WLAN (only myUTN-54)' ⇨🗎129

To view the current parameter values of your UTN server, see: 'Displaying Parameter Values' ⇨🗎106.

Table 12: 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.

Table 13: Parameter List - IPv4 VLAN (only myUTN-80 and myUTN-150)

Parameters	Value	Default	Description
ipv4vlan_on_1 ~ ipv4vlan_on_8 [VLAN]	on/off	off	Enables/disables the forwarding of VLAN data.
ipv4vlan_addr_1 ~ ipv4vlan_addr_8 [IP address]	valid IP address	192.168. 0.0	Specifies the IP address of the UTN server within the VLAN.
ipv4vlan_mask_1 ~ ipv4vlan_mask_8 [Subnet mask]	valid IP address	255.255. 255.0	Specifies the subnet mask of the UTN server within the VLAN.
ipv4vlan_id_1 ~ ipv4vlan_id_8 [VLAN ID]	0–4096 [1–4 characters; 0–9]	0	Specifies the ID for the identification of the VLAN. *0 = untagged multihomed IP addresses*
ipv4vlan_web [VLAN access]	on/off	on	Grants/denies the administrative web access to the myUTN Control Center via a VLAN address.

Parameters	Value	Default	Description
ipv4vlan_snmp [VLAN access]	on/off	on	Grants/denies the administrative SNMP access to the myUTN Control Center via a VLAN address.

Table 14: Parameter List – 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.*
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 subnet 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 '/'.*

Parameters	Value	Default	Description
ipv6_auto [Automatic configuration]	on/off	on	Enables/disables the automatic assignment of the IPv6 address for the UTN server.

Table 15: 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 16: Parameter List - SSL connections

Parameter	Value	Default	Description
security [Encryption]	1–4 [1 character]	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)*

Table 17: Parameter List - Web access

Parameters	Value	Default	Description
http_pwd [Password]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the password for the administrative access to the myUTN Control Center.
http_allowed [Permitted 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.*

Table 18: Parameter List – TCP port access

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

Table 19: 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.

Table 20: Parameter List - Encryption

Parameters	Value	Default	Description
utn_sec_1 ~ utn_sec_8 [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.*

Table 21: 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_8 [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 port key control*
utn_keyval_1 ~ utn_keyval_8 [Key]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Specifies the key used to protect the access to the connected USB device.
utn_prodid_1 ~ utn_prodid_8 [USB device]			Shows the Product ID of the USB device that is assigned to the respective USB port.
utn_vendid_1 ~ utn_vendid_8 [USB device]			Shows the Vendor ID of the USB device that is assigned to the respective USB port.

Parameters	Value	Default	Description
utn_2vlan_1 ~ utn_2vlan_8 [Allocate VLAN]	0–9 [1 character] (see: ⇨🗎117)	0	Allocates a VLAN to the USB port. 0 = every 1 = VLAN 1 2 = VLAN 2, etc. 9 = none

Table 22: Parameter List - USB port

Parameters	Value	Default	Description
utn_tag_1 ~ utn_tag_8 [Name]	max. 32 characters [a–z, A–Z, 0–9]	[blank]	Freely definable description of the USB device.
utn_comp_1 [Compression]	on/off	off	Disables/enables the data compression for the USB device that is connected to the USB port (only myUTN-130).
utn_poff_1 ~ utn_poff_8 [Active]	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_postreset_1 ~ utn_postreset_8	on/off	off	**This parameter can only be used after consultation with the SEH support team.**

Table 23: Parameter List - DNS

Parameters	Value	Default	Description
dns [DNS]	on/off	on	Enables/disables the name resolution via a DNS server.
dns_domain [Domain name]	max. 255 characters [a–z, A–Z, 0–9]	[blank]	Defines the 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.

Parameters	Value	Default	Description
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.*

Table 24: 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_name [User name]	max. 64 characters [a–z, A–Z, 0–9]	anonymous	Defines the name of the SNMP user group 1.
any_pwd [Password]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the password of the SNMP user group 1.
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_name [User name]	max. 64 characters [a–z, A–Z, 0–9]	admin	Defines the name of the SNMP user group 2.

Parameters	Value	Default	Description
admin_pwd [Password]	8–64 characters [a–z, A–Z, 0–9]	administrator	Defines the password of the SNMP user group 2.
admin_rights [Access rights]	--- [None] readonly readwrite	readwrite	Defines the access rights of the SNMP user group 2.
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.

Table 25: 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.

Table 26: Parameter List - Description

Parameters	Value	Default	Description
sys_name [Host name]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Specifies 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)

Table 27: Parameter List - Authentication

Parameters	Value	Default	Description
auth_typ [Authentication method]	--- [None] MD5 TLS TTLS PEAP FAST	----	Defines the EAP authentication method that is used by the UTN server to identify itself 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 = FASTPROV1
		---	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.

Table 28: 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 a 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 user 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 [1–5 characters; 0–9; 0 = unlimited]	10	Defines the maximum email size (in Kbyte) to be accepted by the UTN server.

Table 29: Parameter List - SMTP (only myUTN-80 and later)

Parameters	Value	Default	Description
smtp_srv [Server name]	max. 128 characters	[blank]	Defines an 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_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 name used by the UTN server to connect to the SMTP server.
smtp_pwd [Password]	max. 128 characters	[blank]	Defines the password used by the UTN server to connect 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*

Table 30: 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.
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 devices are activated or deactivated]	on/off	off	Enables/disables the sending of SNMP traps after a USB device was activated/deactivated.
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.
noti_act_1 noti_act_2 [Send email if USB devices are activated or deactivated]	on/off	off	Enables/disables the sending of emails after a USB device was activated/deactivated.
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.

Parameters	Value	Default	Description
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.
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.

Table 31: Parameter List - WLAN (only myUTN-54)

Parameters	Value	Default	Description
wifi [WLAN]	on/off	on	Enables/disables the WLAN module of the UTN server.
wifi_mode [Mode]	adhoc infra	adhoc	Defines the communication mode. *The communication mode defines the network structure in which the UTN server will be installed. Two modes are available:* *- Ad-Hoc* *- Infrastructure*

Parameters	Value	Default	Description
wifi_channel [Channel]	1–14 (country-specific)	3	Defines the channel to which the entire data communication will be transmitted. *The channel (frequency range) should be changed if interferences emerge.* **Keep yourself informed about national provisions regarding the use of WLAN products and only use authorized channels.**
wifi_name [Network name (SSID)]	max. 64 characters [a–z, A–Z, 0–9, _, -]	SEH	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.*

wifi_encrypt [Encryption method]	--- [None]
	WepOpen = WEP (Open System)
	WepShared = WEP (Shared Key)
	TKIP = WPA (TKIP)
	AES = WPA (AES)
	TKIP2 = WPA2 (TKIP)
	AES2 = WPA2 (AES)
	AESTKIP = WPA (AES/TKIP)
	AESTKIP2 = WPA2 (AES/TKIP)
	Auto = WPA (Auto)
		---	Defines the encryption method to be used to protect the access to the WLAN.

wifi_keyid [Use WEP key]	1 = key 1 2 = key 2 3 = key 3 4 = key 4	0	Defines the WEP key to be used.

Parameters	Value	Default	Description
wifi_wepkey1 wifi_wepkey2 wifi_wepkey3 wifi_wepkey4 [Key 1-4]	The max. number of characters depends on the selected key type: 64 ASCII = 5 64 HEX = 10 128 ASCII = 13 128 HEX = 26	[blank]	Defines the WEP keys. Four WEP keys are available. *You can enter the following characters:* *- Hexadecimal = 0–9, a–f, A–F* *- ASCII = 0–9, a–z, A-Z*
wifi_psk [PSK]	8–63 characters	[blank]	Defines the Pre Shared Key (PSK) for Wi-Fi Protected Access (WPA).
wifi_roaming [Roaming]	on/off	off	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.*
wifi_dbmroam [Roaming level]	0–100 [1–3 characters; 0–9]	0	Defines the transmission power (in -dBm) of the UTN server.

8.3 LED Display

The UTN server has LEDs. The LEDs of the UTN server provide information about its status.

During the activation procedure, the behavior of the LEDs differs from this description.

LED	Action	Color	Description
Link	permanently on	green	There is a connection to the network.
	permanently off	-	There is no connection to the network.
Activity	blinks at irregular intervals	yellow	Indicates the exchange of network data packets.
Status	permanently off	-	There is no connection to the USB device. CAUTION: If the activity LED blinks periodically at the same time, the BIOS mode is signalized. The UTN server is not operational in the BIOS mode; see: ⇨ 🗎136.
	permanently on	green	Indicates the connection to at least one USB device.
	blinks 3 times	green	Indicates the assignment of a ZeroConfig IP address. NOTE: We recommend using an IP address from outside the ZeroConf range.
	blinks 2 times	green	Indicates the assignment of an IP address that does not correspond to 0.0.0.0 or that comes from outside the ZeroConf range.

The UTN servers 'myUTN-80', 'myUTN-120', 'myUTN-130' and 'myUTN-150' have differnt LEDs. Refer to the relevant Quick Installation Guide for a description of the LEDs.

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 belonging to the group 'Administrator'
  - Users <u>not</u> belonging to the group 'Administrator'

    + Users <u>with</u> write access to the *.ini file (selection list)
    + Users <u>without</u> write access to the *.ini file (selection list)

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

The tables give an overview:

- for Windows see: Table 32 ⇨🗎134
- for Mac see: Table 33 ⇨🗎135

The tables show 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

Table 32: SEH UTN Manager - Function Overview Windows

	Global Selection List		User-Specific Selection List		
	Admin	User	Admin	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	✓	✓	✓	✓	✓
Device – Activate	✓	✓	✓	✓	✓
Device – Deactivate	✓	✓	✓	✓	✓
Device – Request	✓	✓	✓	✓	✓
Device – Remove	✓	×	✓	×	×
Device – Create UTN Action	✓	✓	✓	✓	✓
Device – Settings	✓	✓	✓	✓	✓
Buttons					
Selection List – Refresh	✓	✓	✓	✓	✓
Selection List – Edit	✓	×	✓	✓	×
Device – Activate	✓	✓	✓	✓	✓
Device – Deactivate	✓	✓	✓	✓	✓
'Program – Options' dialog					
Network Scan – Multicast Search	✓	×	✓	×	×
Network Scan – IP Range Search	✓	×	✓	×	×
Program – Program Language	✓	✓	✓	✓	✓
Program – Program Messages	✓	×	✓	×	×
Program – Program Update	✓	×	✓	×	×
Automatisms – Program Start (Autostart)	✓	✓	✓	✓	✓
Automatisms – Automatic Device Disconnect (Auto-Disconnect)	✓	×	✓	×	×
Selection List – Selection List Mode	✓	×	✓	×	×
Selection List – Automatic Refresh	✓	×	✓	×	×
'Device Settings' dialog					
Automatic device connection – Auto-Connect	✓	×	✓	×	×
Automatic device connection – Print-On-Demand	✓	×	✓	×	×
Messages	✓	✓	✓	✓	✓

✓ = active	r = read only
× = inactive (grayed out)	rw = read and write
	INI = *.ini file (⇨ 🗎73)

Table 33: SEH UTN Manager - Function Overview Mac

	Global Selection List		User-Specific Selection List		
	Admin	User	Admin	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	✓	✓	✓	✓	✓
Device – Activate	✓	✓	✓	✓	✓
Device – Deactivate	✓	✓	✓	✓	✓
Device – Request	✓	✓	✓	✓	✓
Device – Remove	✓	×	✓	×	×
Device – Create UTN Action	✓	✓	✓	✓	✓
Device – Settings	✓	✓	✓	✓	✓
Buttons					
Selection List – Refresh	✓	✓	✓	✓	✓
Selection List – Edit	✓	×	✓	✓	×
Device – Activate	✓	✓	✓	✓	✓
Device – Deactivate	✓	✓	✓	✓	✓
'SEH UTN Manager – Preferences' dialog					
Network Scan – Multicast Search	✓	×	✓	×	×
Network Scan – IP Range Search	✓	×	✓	×	×
Program – Program Messages	only functional in Windows				
Program – Program Update	✓	×	✓	×	×
Automatisms – Program Start (Autostart)	✓	✓	✓	✓	✓
Automatisms – Automatic Device Disconnect (Auto-Disconnect)	✓	×	✓	×	×
Selection List – Selection List Mode	✓	×	✓	×	×
Selection List – Automatic Refresh	✓	×	✓	×	×
'Device Settings' dialog					
Automatic device connection – Auto-Connect	✓	×	✓	×	×
Automatic device connection – Print-On-Demand	✓	×	✓	×	×
Messages	only functional in Windows				

✓ = 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' ⇨🗎136
- 'Some functions in the SEH UTN Manager are hidden, enabled or appear dimmed' ⇨🗎138
- 'A connection to the UTN server cannot be established' ⇨🗎138
- 'A connection to the USB device cannot be established' ⇨🗎138
- 'A connection to the myUTN Control Center cannot be established' ⇨🗎139
- 'The password is no longer available' ⇨🗎139

The UTN server signalizes the BIOS mode

Possible Cause

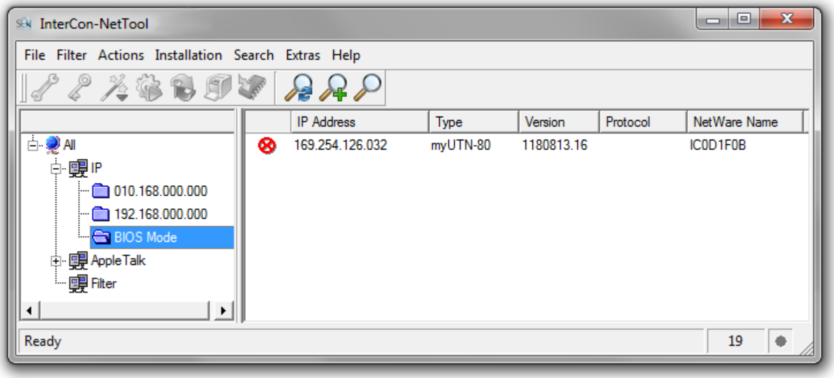
The UTN server switches to the BIOS mode if the firmware functions well but the software is faulty. This may happen in the case of an incorrect software update, for example. The UTN server signalizes the BIOS mode if

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

⚠

The UTN server is not operational in the BIOS mode.

If the UTN server is in the BIOS mode, the filter 'BIOS Mode' will be created automatically in the device list of the InterCon-NetTool. The UTN server will be displayed within this filter.



IP Address	Type	Version	Protocol	NetWare Name
169.254.126.032	myUTN-80	1180813.16		IC0D1F0B

Fig. 18: InterCon-NetTool – UTN Server in BIOS Mode

The software must be loaded on the UTN server so that the UTN server can switch from the BIOS mode to the normal mode.

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the UTN server from the device list.*
   (You will find the UTN server under the filter 'BIOS Mode'.)
3. *Select* **Installation – IP Wizard** *from the menu bar.*
   The IP Wizard is started.
4. *Follow the instructions of the wizard in order to assign an IP address to the UTN server.*
   The IP address is saved.
5. *Carry out a software update on the UTN server; see: ⇨🗎110.*

↳ The software will be saved in the UTN server. The UTN server switches to the normal mode.

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 (e.g. the 'Print-On-Demand' feature is not supported by a hard disk).

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

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. ⇨🗎54.

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: ⇨🗎41.

□ The communication is blocked by a firewall.

A connection to the USB device 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 device 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 ⇨🗎13 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 TCP port access control is enabled ⇨🗎84.

□ The password protection is enabled ⇨🗎83.

□ The cipher suites of the encryption level are not supported by the browser ⇨🗎80.

The password is no longer available

Access to the myUTN Control Center can be protected by a password. If the password is no longer available you can reset the parameter values of the UTN server to their default settings to get access to the myUTN Control Center ⇨🗎107. 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 devices.

Use

In order to activate or deactivate a USB device with utnm, commands are entered and run in a special syntax in the command-line interface of the operating system.

As an alternative, a script will be written for the USB device. 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 ⇨🗎20).

Frequently recurring command sequences (e.g. a device 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 Command-Line Interface' ⇨🗎140

□ 'Creating Scripts' ⇨🗎141

Using the Command-Line Interface

Requirements

☑ The SEH UTN Manager is installed on the client; see: ⇨🗎20.

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

Proceed as follows:

1. *Open the command-line interface.*
2. *Enter the command sequence; see 'Syntax and Commands' ⇨🗎141.*
3. *Confirm your entries.*

↳ The command sequence will be run.

Creating Scripts

Requirements

☑ The SEH UTN Manager is installed on the client; see: ⇨🗎20.

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

Proceed as follows:

1. *Open a text editor.*
2. *Enter the command sequence; see 'Syntax and Commands' ⇨🗎141.*
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:

<u>Windows</u>

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

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

<u>Mac</u>

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

The executable file 'utnm' can be found in the 'SEH UTN Manager.app'. In `/usr/local/bin/` there is a symbolic link to it.

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 vendor ID product ID [port number]`
	Activates the connection to a USB device. If several USB devices with the same product ID and vendor ID are connected to the UTN server, the first available device will be activated if the port has not been specified.
	• `deactivate UTN server vendor ID product ID [port number]`
	Deactivates the connection to a USB device. The command 'eject' will be used when a USB mass storage device is removed. The command 'plugout' will be used for all other devices.
	• `plugin UTN server vendor ID product ID [port number]`
	Activates the connection to a USB device. If several USB devices with the same product ID and vendor ID are connected to the UTN server, the first available device will be activated if the port has not been specified.
	• `plugout UTN server vendor ID product ID [port number]`
	Deactivates the connection to a USB device. (Corresponds to the 'plugging out' of the device.)
	Note: *The command 'deactivate' is to be preferred.*
	• `eject UTN server vendor ID product ID [port number]`
	(for USB mass storage devices) Ejects the USB device. The device connection will only be deactivated if the communication has been terminated properly.
	Note: *The command 'deactivate' is to be preferred.*
	• `state UTN server vendor ID product ID port number`
	Displays the status of the USB device.
	• `getlist UTN server`
	Shows an overview of the USB devices (including port, vendor ID, product ID, manufacturer name, product name, device class and status) that are connected to the UTN server.
	• `set autoconnect = true|false UTN server vendor ID product ID port number`
	Automatically activates the device connection if the USB device is connected and not in use.

Command	Description
`p port number` *or* `port port number`	Uses an alternative USB port on the UTN server.
`sp` *or* `ssl-port`	Uses an alternative USB port on the UTN server with SSL encryption.

`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.

`t seconds` *or* `timeout seconds`	Specifies a timeout for the command strings 'activate', 'deactivate', ’plugin’, 'plugout' and 'eject'.
`nw` *or* `no-warnings`	Suppresses warning messages.
`q` *or* `quiet`	Suppresses the output.
`o` *or* `output`	Shows the output in the command line.
`v` *or* `version`	Shows version information about utnm.
`?` *or* `help`	Shows the help page.

The following applies for the commands:

- UTN server = IP address or host name of a UTN server
- vendor ID = vendor ID of the USB device
- product ID = product ID of the USB device
- Elements in square brackets are optional
- not case-sensitive
- only the ASCII format can be read

Return Values

Return Value	Description
0	The USB device is free for use.
20	The plugin of the USB device failed.
21	The plugout of the USB device failed.
22	The ejection of the USB device failed.
23	The USB device is already plugged in.
24	The USB device is already plugged out.
25	The USB device is plugged in by another user.
26	The 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:

Windows

```
"<path utnm.exe>" /c "activate UTN server vendor ID product ID
[port number]"
```

Results in:

```
"C:\Program Files\SEH Computertechnik GmbH\SEH UTN Manager\
utnm.exe" /c "activate 192.168.0.140 0x0d7d 0x1400 4"
```

Mac

```
utnm -c "activate UTN server vendor ID product ID [port number]"
```

Results in:

```
utnm -c "activate 10.168.1.167 0x058f 0x6387 3"
```

8.7 List of Figures

UTN Server in the Network 7
myUTN Control Center - START 19
SEH UTN Manager - Main Dialog 26
InterCon-NetTool - Main Dialog 30
Administration via Email - Example 1 33
Administration via Email - Example 2 33
InterCon-NetTool - IP Wizard 37
SEH UTN Manager - Compression 56
USB port based assignment of VLANs 59
SEH UTN Manager - Edit Selection List 63
SEH UTN Manager - Activating the Device 64
Create UTN Action dialog 71
Global Selection List 74
User-Specific Selection List 74
myUTN Control Center - Certificates 90
UTN Server - SSL/TLS Connection in the Network 103
SEH UTN Manager - Encryption 104
InterCon-NetTool - UTN Server in BIOS Mode 137

8.8 Index

A

Address
  Hardware address 114
  IP address 114
  MAC address 114
Ad-Hoc mode 50
ARP/PING 16
Authentication 47, 48, 96
Auto-Connect 20, 67
Auto-Disconnect 20, 68
Automatisms 20, 67
  Auto-Connect 20, 67
  Auto-Disconnect 20, 68
  Autostart 20
  Print-On-Demand 20, 69
  UTN Action 20, 70
  utnm 21, 140
Autostart 20

B

Backup 105
Backup copy 105
Bonjour 42
BOOTP 14

C

CA certificate 89
Certificate 89
  Create 91
  Delete 96
  Display 91
  Save 93
Certificate request 92
Channel 51, 130
Cipher suite 80
Communication mode 50
Complete version 21
Connection
  Disable 65
  Enable 64

D

Data compression 56
Default certificate 89
Default name 115
Default settings 107
Descriptions 53
Device number 115
DHCP 14
DNS (Domain Name Service) 40
Documentation 7

E

EAP 96
EAP-FAST 101
EAP-MD5 97
EAP-TLS 98
EAP-TTLS 99
Email 31
Encryption 103
Encryption level 80

F

file
  '<Default-name>_parameter.txt' 105
Frequency range 51

G

Gateway 115
Global selection list 74

H

Hardware address 114
Host name 115
Hotline 10
HTTP/HTTPS 82

I

IEEE 802.1x 96
Improper use 11
Infrastructure mode 50
Intended use 11
InterCon-NetTool 28
  Installation 28
  IP Wizard 15
  Start 28
  Structure 30
Interferences 130
IP address 114
  Save 13
IPv4 35
IPv6 38

L

LEDs 132

M

MAC address 114
Maintenance 105
Minimal version 21
Mode 50
Multicast search 61
myUTN Control Center 18
  Language 19
  Start 18
  Structure 19

N

Network list 61
Network settings 35
Notification service 57
  Email 58
  SNMP trap 58
Notifications 57

P

Parameter list 116
Parameters
  Default settings 107
  Display 106
  Load 106
  Resetting 107
  Save 106
Parameters file 105
Password 83
PEAP 100
PKCS#12 94
POP3 44
Print-On-Demand 20, 69
Protection 79
Protocol
  BOOTP 14
  DHCP 14
  IPv4 35
  IPv6 38
  POP3 44
  SMTP 44
  SNMP 41
  SNTP 53
  SSL/TLS 80
Purpose 6

R

RADIUS 96
Reset 107
Reset button 34, 108
Restart 111
Roaming 50
Roaming level 50
Root certificate 89

S

S/MIME certificate 90
Security 79
Security level 84
SEH UTN Manager
  Function overview 133
  Installation 22
  Start 22

Structure 25
Update 25
Versions 21
Selection list 73
Self-signed certificate 89
SMTP 44
SNMP trap 57
SNMPv1 41
SNMPv3 41
SSID (Service Set Identifier) 50
SSL/TLS connection 80, 103
Subnet mask 115
Support 10
System requirements 6

T

TCP port access control 84
TCP/IP 35
Test mode 85
Time of the device 53
Time server 53
Time zone 53
Types of connection 82
Define 82

U

Update 110
USB Devices
Add 63
Connect 64
Control access 86
Cutting the connection 65
Data compression 56
Names 55
Power supply 55
Request 66
Status information 72
USB port device assignment 86
USB port key control 86
User-specific selection list 74
UTC 53
UTN Action 20, 70
UTN port 54
UTN SSL port 54, 103
utnm 21, 140

V

Version number 110
VLAN 59

W

WEP (Wired Equivalent Privacy) 47
WPA/WPA2 48

Z

ZeroConf 14