myUTN

USB Deviceserver-Benutzerhandbuch Linux

myUTN-2500

Hersteller & Kontakt

SEH Computertechnik GmbH
Südring 11
33647 Bielefeld
Deutschland
Tel.: +49 (0)521 94226-29
Fax: +49 (0)521 94226-99
Support: +49 (0)521 94226-44
E-Mail: info@seh.de
Web: https://www.seh.de

Dokument

Typ: Benutzerhandbuch
Titel: myUTN-Benutzerhandbuch Linux
Version: 4.1 | 2021-07

Rechtliche Hinweise

1 Allgemeine Information

1.1 Produkt

Verwendungszweck

UTN-Server umfassen USB Deviceserver und USB Dongleserver. Als USB Deviceserver stellen sie nicht-netzwerkfähige USB-Geräte (z.B. USB-Festplatten, USB-Drucker usw.) und als USB Dongleserver nicht-netzwerkfähige USB-Dongles via TCP/IP-Netzwerk bereit. Dazu werden die USB-Geräte bzw. USB-Dongles an die USB-Ports des UTN-Servers angeschlossen. Anschließend wird mithilfe der UTN-Funktionalität (UTN = USB to Network) und dem dafür entwickelten Software-Tool 'SEH UTN Manager' eine virtuelle USB-Verbindung zwischen USB-Gerät bzw. USB-Dongle und Client hergestellt. Das USB-Gerät bzw. der USB-Dongle kann wie lokal angeschlossen verwendet werden.

Wichtig:
Nachfolgend werden USB-Geräte und USB-Dongles zusammengefasst als 'USB-Geräte' bezeichnet.

Systemvoraussetzungen

Der UTN-Server ist für den Einsatz in TCP/IP-Netzwerken konzipiert.

Der SEH UTN Manager kann in folgenden Systemen genutzt werden:

- Microsoft Windows (32/64-Bit; Windows 10 oder höher, Server 2012 R2 oder höher)
- macOS 10.9 oder höher [1]
- Linux (Debian 10, Ubuntu 20.0.4, Red Hat Enterprise Linux 8, Oracle 8, CentOS 8, SUSE Linux Enterprise 15.1, openSUSE Leap 15.1) [2]
- IPv4-TCP/IP-Netzwerk

Wichtig:
Die Unterstützung von isochronen USB-Geräten (z.B. Kameras, Mikrofone, Lautsprecher usw.) ist abhängig von

- dem Betriebssystem:
  - Windows
  - macOS
  - Linux
- der Softwareversion:
  - Firmware/Software für UTN-Server: 14.5.5 oder höher
  - SEH UTN Manager: 3.1.4 oder höher

Dieses Dokument beschreibt den Einsatz in Linux-Umgebungen. Für den Einsatz in anderen Umgebungen lesen Sie bitte die jeweilige systemspezifische Benutzerhandbuch. Mehr Informationen finden Sie im Kapitel 'Dokumentation' ⇨ 3.

1. macOS 11.x (Big Sur) nur eingeschränkte USB-Geräte Unterstützung nicht lauffähig auf Apple Silicon (Apple M1 Chip) basierten Macs
2. Eine erfolgreiche Installation kann nicht garantiert werden aufgrund der Vielfalt an Linux-Systemen! Die Installation muss in Eigenverantwortung durchgeführt werden.

1.2 Dokumentation

Die aktuelle Version aller Dokumente laden Sie bitte von unserer Website:
https://www.seh-technology.com/de/service/downloads.html

Mitgeltende Dokumente

Die UTN-Dokumentation besteht aus den folgenden Dokumenten:

Quick Installation Guide	Print, PDF	Informationen zur Sicherheit, technische Daten, Beschreibung der Hardware-Installation und Inbetriebnahme sowie Konformitätserklärungen.
Benutzerhandbuch	PDF	Detaillierte Beschreibung der UTN-Server-Konfiguration und -Administration. Systemspezifische Anleitungen für folgende Systeme: - Windows - macOS - Linux
Online Hilfe	HTML	Informationen zur Bedienung der Weboberfläche 'myUTN Control Center'. (In die Weboberfläche integriert; kein Download.)
Produktinformationen	Print, PDF	Leistungsumfang und technische Daten
Broschüren	Print, PDF	https://www.seh.de
Open Source Lizenzen	online	https://www.seh-technology.com/de/service/lizenzen.html

Symbole und Legende

Innerhalb dieses Dokumentes finden Sie verschiedene Symbole und Auszeichnungen:

WARNUNG Warnhinweis	Ein Warnhinweis enthält wichtige Informationen, die Sie unbedingt beachten müssen. Nichtbeachtung kann zu Fehlfunktionen führen.
Wichtig: Wichtige Information	Dieser Hinweis enthält wichtige Informationen für den störungsfreien Betrieb.
✓ Voraussetzung	Bedingungen, die erfüllt sein müssen, bevor Sie mit einer Handlung beginnen.
• Aufzählung	Liste
1. Nummerierte Aufzählung	Schritt-für-Schritt-Handlungsanweisung
↳ Ergebnis	Auswirkung einer ausgeführten Handlung.
Tipp	Empfehlungen und nützliche Hinweise
⇨	Querverweis (Innerhalb des Dokumentes können Sie Hyperlinks nutzen.)
Fett	Feststehende Bezeichnungen (z.B. von Schaltflächen, Menüpunkten und Auswahllisten)
`Courier`	Code (z.B. für Kommandozeilen und Skripte), Pfade
'Eigennahmen'	Einfache Anführungszeichen kennzeichnen Eigennamen.

1.3 Support und Service

SEH Computertechnik GmbH bietet einen umfassenden Support. Falls Sie Fragen haben, kontaktieren Sie uns:

Montag–Donnerstag	8:00–16:45 Uhr
Freitag	8:00–15:15 Uhr

+49 (0)521 94226-44

support@seh.de

Kunden aus den Vereinigten Staaten von Amerika (USA) und Kanada kontaktieren bitte den nordamerikanischen Support:

Montag–Freitag	9:00–17:00 Uhr (EST/EDT)

+1-610-933-2088

support@sehtechnology.com

Alle Informationen und Downloads rund um Ihr Produkt finden Sie auf unserer Website:

https://www.seh.de/

1.4 Ihre Sicherheit

Lesen und beachten Sie alle in der Dokumentation, auf dem Gerät oder auf der Verpackung dargestellten Sicherheits- und Warnhinweise. Das Beachten der Hinweise vermeidet potentiellen Fehlgebrauch und schützt Personen vor Gefahren und das Gerät vor Schäden.

Bestimmungsgemäße Verwendung

Der UTN-Server wird in TCP/IP-Netzwerken eingesetzt und ist konzipiert für den Einsatz in Büroumgebungen. Er erlaubt das Bereitstellen von nicht-netzwerkfähigen USB-Geräten für mehrere Netzwerkteilnehmer.

Bestimmungswidrige Verwendung

Alle Verwendungen des Gerätes, die den in der myUTN-Dokumentation beschriebenen Funktionalitäten nicht entsprechen, sind bestimmungswidrig.

Sicherheitshinweise

Lesen und beachten Sie vor der Inbetriebnahme des UTN-Servers die Sicherheitshinweise im 'Quick Installation Guide'. Dieses Dokument liegt in gedruckter Form dem Lieferumfang bei.

Warnhinweise

Lesen und beachten Sie alle in diesem Dokument dargestellten Warnhinweise. Die Hinweise sind gefahrenträchtigen Handlungsanleitungen vorangestellt. Sie werden wie folgt dargestellt:

WARNUNG

Dies ist ein Warnhinweis!

Haftung und Garantie

Bei Nichtbeachtung der dargebotenen Sicherheits- und Warnhinweise übernimmt SEH Computertechnik GmbH keine Haftung bei Sach- und Personen- oder Folgeschäden. Zudem entfällt in diesem Fall jeglicher Garantieanspruch.

Konstruktive Veränderungen und Reparatur

Eigenmächtige konstruktive Veränderungen an Hardware oder Software sowie Reparaturversuche am Gerät sind verboten. Falls eine Gerätereparatur erforderlich ist, wenden Sie sich an unseren Support ⇨ 🗎4.

1.5 Erste Schritte

1. Lesen und beachten Sie die Sicherheitsinformationen, um Schaden an Personen und Gerät zu vermeiden ⇨ 🗎5.
2. Führen Sie die Hardware-Installation aus. Die Hardware-Installation beinhaltet das Anschließen des UTN-Servers an Netzwerk, USB-Geräte und Stromnetz ⇨ 🕮 'Quick Installation Guide'.
3. Führen Sie die Software-Installation aus. Die Software-Installation beinhaltet die Installation des benötigten Software-Tools 'SEH UTN Manager' auf Ihrem Client und die Zuweisung einer IP-Adresse ⇨ 🕮 'Quick Installation Guide'.
4. Konfigurieren Sie den UTN-Server, sodass er optimal in Ihr Netzwerk integriert und ausreichend geschützt ist. Alle benötigten Informationen dazu finden Sie in diesem Dokument.
5. Arbeiten Sie mit dem SEH UTN Manager, um Verbindungen zu den USB-Geräten die an den UTN-Server angeschlossen sind herzustellen und zu verwalten ⇨ 🗎40.

Informationen zur UTN-Dokumentation finden Sie im Kapitel 'Dokumentation' ⇨ 🗎3.

2 Administrationsmethoden

Sie können den UTN-Server auf unterschiedliche Weise administrieren, konfigurieren und warten:

- Administration via myUTN Control Center ⇨ 🗎8
- Administration via SEH UTN Manager ⇨ 🗎10
- Administration via E-Mail ⇨ 🗎17

2.1 Administration via myUTN Control Center

Der UTN-Server verfügt über eine Benutzeroberfläche, das myUTN Control Center, welches Sie in einem Internet-Browser (z.B. Mozilla Firefox) aufrufen.

Über das myUTN Control Center kann der UTN-Server konfiguriert, überwacht und gewartet werden.

- myUTN Control Center im Browser öffnen ⇨ 🗎8
- myUTN Control Center via SEH UTN Manager öffnen ⇨ 🗎8
- Bedienung ⇨ 🗎9

myUTN Control Center im Browser öffnen

✓ Der UTN-Server ist an Netzwerk und Netzspannung angeschlossen.
✓ Der UTN-Server hat eine gültige IP-Adresse ⇨ 🗎20.

1. Öffnen Sie Ihren Browser.
2. Geben Sie als URL die IP-Adresse des UTN-Servers ein.

↳ Das myUTN Control Center wird im Browser dargestellt.

Wichtig:

Falls das myUTN Control Center nicht angezeigt wird, überprüfen Sie ob ein Gateway konfiguriert ist (⇨ 🗎20) sowie die Proxy-Einstellungen des Browsers.

myUTN Control Center via SEH UTN Manager öffnen

✓ Der UTN-Server ist an Netzwerk und Netzspannung angeschlossen.
✓ Der UTN-Server hat eine gültige IP-Adresse ⇨ 🗎20.
✓ Der SEH UTN Manager ist auf dem Client installiert ⇨ 🗎9.

1. Starten Sie den SEH UTN Manager.
2. Markieren Sie den UTN-Server in der Auswahlliste.
3. Wählen Sie im Menü **UTN-Server** den Befehl **Konfigurieren**.

↳ Ihr Browser wird geöffnet und das myUTN Control Center dargestellt.

Bedienung

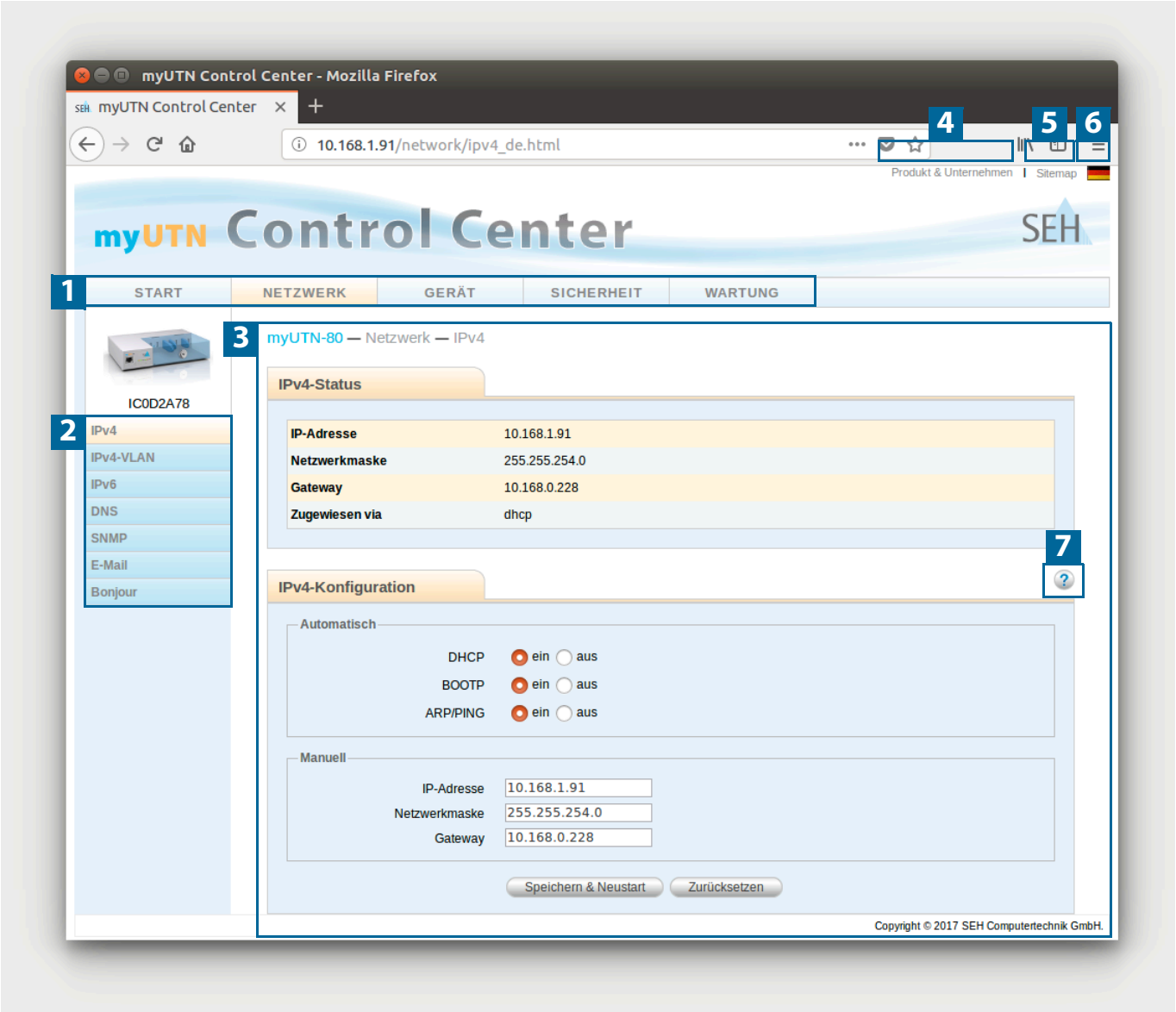


Abbildung 1: myUTN Control Center

1	Menüpunkte	Nach dem Anwählen eines Menüpunkts (einfacher Mausklick) werden links die verfügbaren Untermenüpunkte angezeigt.
2	Untermenüpunkte	Nach dem Anwählen wird die entsprechende Seite mit den Menüinhalten dargestellt.
3	Seite	Menüinhalte
4	Produkt & Unternehmen	Kontaktdaten des Herstellers und weiterführende Informationen zum Produkt.
5	Sitemap	Übersicht über und direkter Zugriff auf alle Seiten des myUTN Control Centers.
6	Flaggen	Sprachwahl
7	? -Symbol	Online Hilfe

2.2 Administration via SEH UTN Manager

Der 'SEH UTN Manager' ist ein von SEH Computertechnik GmbH entwickeltes Software-Tool. Mit dem SEH UTN Manager werden Verbindungen zu den USB-Geräten an UTN-Servern hergestellt und verwaltet.

Funktion

Die Software wird auf allen Clients installiert, die auf ein im Netzwerk bereitgestelltes USB-Gerät zugreifen sollen. Nach dem Start des SEH UTN Managers wird zunächst im Netzwerk nach angeschlossenen UTN-Servern gesucht. Alle gefundenen UTN-Server und deren angeschlossene USB-Geräte werden in der 'Netzwerkliste' angezeigt. Um die an einen UTN-Server angeschlossenen USB-Geräte zu verwenden, müssen Sie den UTN-Server zur 'Auswahlliste' hinzufügen. Die in der Auswahlliste aufgeführten Geräte können administriert und die angeschlossenen USB-Geräte verwendet werden. Das Arbeiten mit dem SEH UTN Manager wird im Kapitel 'Arbeiten mit dem SEH UTN Manager' ⇨ 🗎40 ausführlich beschrieben.

WARNUNG

Die UTN-Funktionalität (⇨ 🗎2) und der zugehörige SEH UTN Manager funktionieren nur in IPv4-Netzwerken.

In reinen IPv6-Netzwerken kann lediglich auf das myUTN Control Center (⇨ 🗎8) zugegriffen werden, um den UTN-Server zu administrieren.

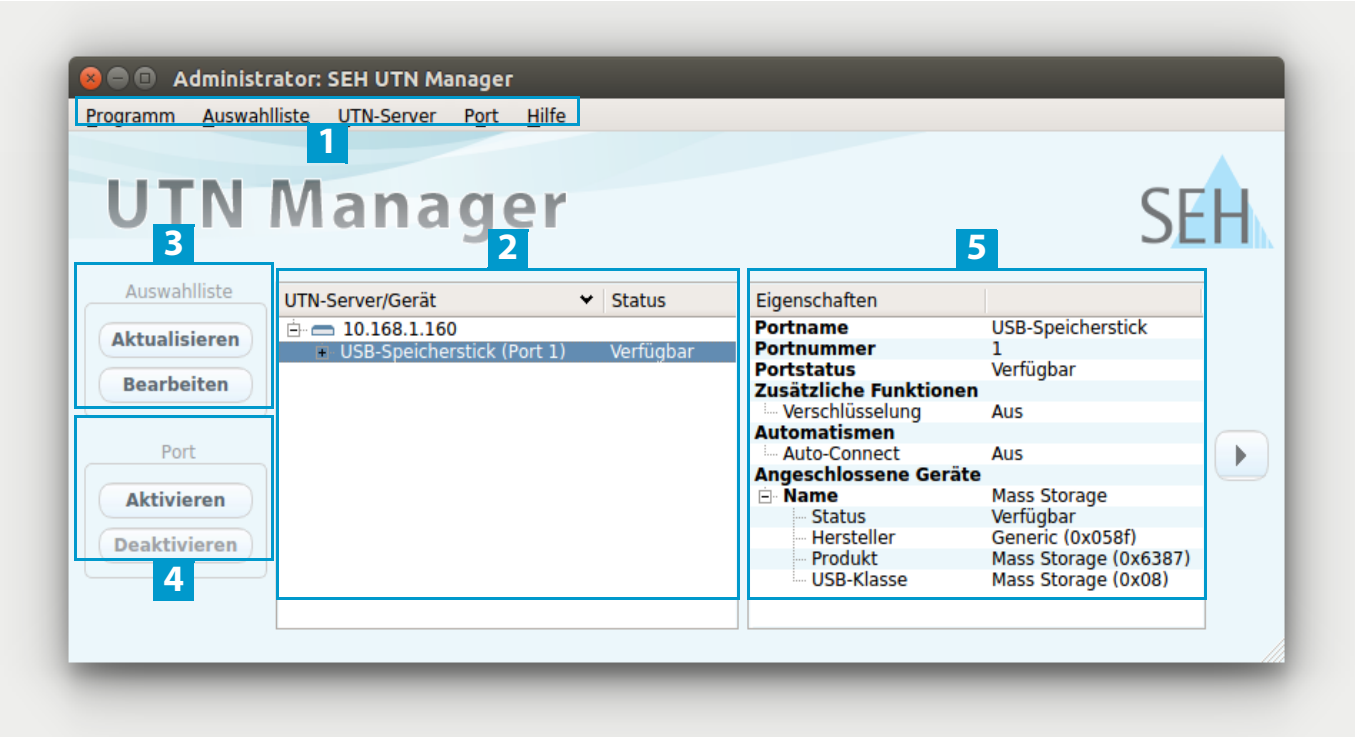


Abbildung 2: SEH UTN Manager

1	Menüleiste	Verfügbare Menüpunkte
2	Auswahlliste	Zeigt die ausgewählten UTN-Server und die daran angeschlossenen USB-Geräte.
3	Schaltflächen zum Bearbeiten der Auswahlliste	Ruft den Dialog zur Netzwerksuche von UTN-Servern und die Auswahl der gewünschten Geräte auf ⇨ 🗎41.
4	Schaltflächen zum Managen der Portverbindung	Stellt eine Verbindung zum an den USB-Port angeschlossenen USB-Gerät her (⇨ 🗎43) oder beendet sie (⇨ 🗎44).
5	Anzeigebereich 'Eigenschaften'	Zeigt Informationen zum ausgewählten UTN-Server oder USB-Gerät ⇨ 🗎48.

Detaillierte Informationen zur Bedienung des SEH UTN Managers entnehmen Sie der ⇨ 🕮 'SEH UTN Manager Online Hilfe'. Um die Online Hilfe zu starten, wählen Sie im SEH UTN Manager im Menü **Hilfe** den Befehl **Online Hilfe**.

Wichtig:

Eventuell werden einige Funktionen im SEH UTN Manager nicht oder inaktiv dargestellt. Dieses steht in Abhängigkeit zu

- dem Typ und dem Speicherort der Auswahlliste
- den Benutzerrechten und der Gruppenzugehörigkeit auf dem Client
- dem Client-Betriebssystem
- den Einstellungen der produkteigenen Sicherheitsmechanismen
- dem Status des UTN-Servers und dem jeweiligen USB-Port

Mehr Informationen finden Sie in der
'SEH UTN Manager – Funktionsübersicht' ⇨ 🗎106.

Varianten

Der SEH UTN Manager ist in zwei Varianten verfügbar:

- Vollständige Variante:
  SEH UTN Manager mit grafischer Bedienoberfläche (⇨Abbildung 2 🗎11) und zusätzlichen Funktionen.
- Minimal-Variante (ohne grafische Bedienoberfläche):
  Bedienung nur über Kommandozeile ('utnm' ⇨ 🗎52) ⇨ 🗎46.

Wichtig:

Für den Standard-Gebrauch wird die vollständige Variante empfohlen.

Die Minimal-Variante ist nur von Experten zu verwenden!

Bei beiden Varianten agiert der Dienst 'SEH UTN Service' (Daemon) im Hintergrund und ist nach Systemstart automatisch aktiv.

Es wird zudem zwischen den folgenden Benutzergruppen unterschieden:

- Benutzer mit administrativen Rechten (Administrator)
- Benutzer ohne administrative Rechte (Standard-Benutzer)

Wichtig:

Einige Funktionen können ausschließlich durch Administratoren konfiguriert werden. Mehr Informationen finden Sie in der 'SEH UTN Manager – Funktionsübersicht' ⇨ 🗎106.

Installation

Um mit dem SEH UTN Manager zu arbeiten, muss das Programm auf einem Rechner mit einem Linux-Betriebssystem installiert werden. Sie finden die SEH UTN Manager-Installationsdatei auf der SEH Computertechnik GmbH-Website:

https://www.seh-technology.com/de/service/downloads.html

Für Linux-Systeme (64-Bit) sind Installationspakete in folgenden Formaten verfügbar:

- *.deb (für 64-Bit-Debian-basierte Systeme)
- *.rpm (für 64-Bit-Red Hat-basierte Systeme)

WARNUNG

Eine erfolgreiche Installation kann nicht garantiert werden aufgrund der Vielfalt an Linux-Systemen!

Die Installation muss in Eigenverantwortung durchgeführt werden.

Auf Anfrage ist kostenpflichtiger Installations-Support durch SEH Computertechnik GmbH möglich ⇨ 🗎4.

Die Installation wurde in folgenden 64-Bit-Systemen erfolgreich getestet:

- Debian: Debian10, Ubuntu 20.0.4
- Red Hat: Red Hat Enterprise Linux 8, Oracle 8, CentOS 8, openSUSE Leap 15.1

Installationsvoraussetzungen:

✓ deb: Linux-Kernel 2.6.32 oder höher, glibc 2.15 oder höher, DKMS (Dynamic Kernel Module Support)

✓ rpm: Kernel 2.6.32 oder höher, glibc 2.12 oder höher, DKMS (Dynamic Kernel Module Support)

Es gibt jeweils vier Installationspakete:

1) driver (Treiber)
2) service (SEH UTN Service/Daemon)
3) clitool (Kommandozeilentool 'utnm')
4) manager (grafische Bedienoberfläche)

Die Anzahl der installierten Pakete entscheidet über die Variante des SEH UTN Managers:

Paket 1)–3): Minimalvariante

Paket 1)–4): vollständige Variante

Wichtig:

Installieren Sie die Pakete aufgrund ihrer Abhängigkeiten in der oben dargestellten Reihenfolge.

Je nach Distribution sind für die Installation der Dateien unterschiedliche Maßnahmen erforderlich. Lesen Sie hierzu die Dokumentation Ihres Betriebssystems.

Wichtig:

Die Installation ist nur durch erfahrene Benutzer vorzunehmen.

Beispielhaft werden nachfolgend einige Installationsverfahren beschrieben:

- 'SEH UTN Manager in Ubuntu 20.0.4.x LTS (64-Bit) via Software-Verwaltung installieren' ⇨ 14
- 'SEH UTN Manager in Ubuntu 20.0.4.x LTS (64-Bit) via Terminal installieren' ⇨ 15
- 'SEH UTN Manager in Red Hat Enterprise Linux Server (8) via Terminal installieren' ⇨ 16

Wichtig:

Auf der SEH Computertechnik GmbH-Webseite finden Sie Knowledge Base-Artikel mit weiterführenden Informationen zur Installation in Linux-Systemen (z.B. zur Installation von DKMS und dem UEFI-Secure-Boot-Problem):

http://www.seh-technology.com/de/service/knowledge-base.html

SEH UTN Manager in Ubuntu 20.0.4.x LTS (64-Bit) via Software-Verwaltung installieren

- ✓ Linux-Kernel 2.6.32 oder höher
- ✓ glibc 2.15 oder höher
- ✓ OpenSSL 1.0.1 oder höher
- ✓ DKMS (Dynamic Kernel Module Support) ist auf dem Client installiert.
- ✓ Der verwendete Benutzer kann über den Befehl `sudo` Rootrechte erlangen.

1. Starten Sie das Installationspaket Nr. 1.
   Der Dialog **Ubuntu Software** erscheint.
2. Wählen Sie die Schaltfläche **Installieren** an.
   Eine Passwort-Abfrage erscheint.
3. Legitimieren Sie sich mit Ihrem Passwort.
   Das Paket wird auf Ihrem Client installiert.
4. Wiederholen Sie Schritte 1. bis 3. mit den restlichen Paketen.
5. Der bei der Installation verwendete Benutzer kann automatisch den SEH UTN Manager auf dem Client nutzen. Sollen weitere Benutzer den SEH UTN Manager nutzen können, müssen Sie diese der Benutzergruppe 'utnusers' hinzufügen. Öffnen Sie hierzu ein **Terminal** und geben den Befehl ein:
   `sudo usermod -aG utnusers <Benutzername>`
6. Melden Sie sich ab und wieder an, damit die Zugehörigkeit zur Gruppe wirksam wird.

↳ Der SEH UTN Manager ist auf Ihrem Client installiert. Überprüfen Sie die Installation, indem Sie den SEH UTN Manager starten (⇨ 🗎10) und eine Verbindung zu einem USB-Port inklusive dem daran angeschlossenen USB-Gerät herstellen. Alle Informationen dazu finden Sie im Kapitel 'Arbeiten mit dem SEH UTN Manager' ⇨ 🗎40.

SEH UTN Manager in Ubuntu 20.0.4.x LTS (64-Bit) via Terminal installieren

- ✓ Linux-Kernel 2.6.32 oder höher
- ✓ glibc 2.15 oder höher
- ✓ OpenSSL 1.0.1 oder höher
- ✓ DKMS (Dynamic Kernel Module Support) ist auf dem Client installiert.
- ✓ Der verwendete Benutzer kann über den Befehl `sudo` Rootrechte erlangen.

1. Öffnen Sie ein **Terminal**.
2. Installieren Sie die Header für Ihren Kernel:
   `sudo apt-get install linux-headers-`uname -r``
3. Überprüfen Sie, ob die Versionsnummer Ihres Kernels und der Header exakt übereinstimmen:
   Kernel: `uname -r`
   Header: `sudo apt list --installed | grep linux-headers`

WARNUNG

Die Versionsnummern müssen exakt übereinstimmen. Sonst können die SEH UTN Manager-Pakete nicht korrekt installiert werden.

Falls Kernel und Header nicht zueinander passen, müssen Sie eigenverantwortlich eine Übereinstimmung herstellen.

4. Wechseln Sie in das Verzeichnis, in dem die SEH UTN Manager-Pakete liegen:
   `cd <Verzeichnis>`
5. Installieren Sie die gewünschten SEH UTN Manager-Pakete:
   `sudo dpkg -i <vollständiger Paketname>`
6. Der bei der Installation verwendete Benutzer kann automatisch den SEH UTN Manager auf dem Client nutzen. Sollen weitere Benutzer den SEH UTN Manager nutzen können, müssen Sie diese der Benutzergruppe 'utnusers' hinzufügen:
   `sudo usermod -aG utnusers <Benutzername>`
7. Melden Sie sich ab und wieder an, damit die Zugehörigkeit zur Gruppe wirksam wird.

↳ Der SEH UTN Manager ist auf Ihrem Client installiert. Überprüfen Sie die Installation, indem Sie den SEH UTN Manager starten (⇨ 🗎10) und eine Verbindung zu einem USB-Port inklusive dem daran angeschlossenen USB-Gerät herstellen. Alle Informationen dazu finden Sie im Kapitel 'Arbeiten mit dem SEH UTN Manager' ⇨ 🗎40.

SEH UTN Manager in Red Hat Enterprise Linux Server (8) via Terminal installieren

- ✓ Linux-Kernel 2.6.32 oder höher
- ✓ glibc 2.12 oder höher
- ✓ OpenSSL 1.0.1 oder höher
- ✓ DKMS (Dynamic Kernel Module Support) ist auf dem Client installiert.
- ✓ Der verwendete Benutzer kann über den Befehl `sudo` Rootrechte erlangen.

1. Öffnen Sie ein **Terminal**.
2. Installieren Sie die Header für Ihren Kernel:
   `sudo yum install kernel-devel-`uname -r``
3. Überprüfen Sie, ob die Versionsnummer Ihres Kernels und der Header exakt übereinstimmen:
   Kernel: `uname -r`
   Header: `sudo yum list | grep kernel-headers`

WARNUNG

Die Versionsnummern müssen exakt übereinstimmen. Sonst können die SEH UTN Manager-Pakete nicht installiert werden.

Falls Kernel und Header nicht zueinander passen, müssen Sie eigenverantwortlich eine Übereinstimmung herstellen.

4. Wechseln Sie in das Verzeichnis, in dem die SEH UTN Manager-Pakete liegen:
   `cd <Verzeichnis>`
5. Installieren Sie die gewünschten SEH UTN Manager-Pakete:
   `sudo yum install <vollständiger Paketname>`
6. Der bei der Installation verwendete Benutzer kann automatisch den SEH UTN Manager auf dem Client nutzen. Sollen weitere Benutzer den SEH UTN Manager nutzen können, müssen Sie diese der Benutzergruppe 'utnusers' hinzufügen:
   `sudo usermod -aG utnusers <Benutzername>`
7. Melden Sie sich ab und wieder an, damit die Zugehörigkeit zur Gruppe wirksam wird.

↳ Der SEH UTN Manager ist auf Ihrem Client installiert. Überprüfen Sie die Installation, indem Sie den SEH UTN Manager starten (⇨ 🗎10) und eine Verbindung zu einem USB-Port inklusive dem daran angeschlossenen USB-Gerät herstellen. Alle Informationen dazu finden Sie im Kapitel 'Suchparameter definieren' ⇨ 🗎41.

Programmstart

Zum Starten des SEH UTN Managers rufen Sie im Startmenü über das Schnellstartmenü (Suchfunktion) 'UTN Manager' auf oder führen im **Terminal** den Befehl `utnmanager` aus.

Update

Sie können entweder manuell oder automatisch prüfen, ob ein Programm-Update verfügbar ist. Mehr Informationen dazu finden Sie in der ⇨ 🕮 'SEH UTN Manager Online Hilfe'.

2.3 Administration via E-Mail

Sie können den UTN-Server über E-Mail und somit von jedem internetfähigen Rechner aus administrieren (Fernwartung):

- UTN-Server-Status erhalten
- UTN-Server-Parameter definieren
- UTN-Server-Update durchführen

Dazu geben Sie in die Betreffzeile einer E-Mail entsprechende Anweisungen ein ⇨Tabelle 1 🗎17.

Tabelle 1: Befehle und Kommentar

Kommandos	Option	Beschreibung
<Befehl>	`get status`	Sie erhalten Statusseite des UTN-Servers.
	`get parameters`	Sie erhalten die Parameterliste des UTN-Servers.
	`set parameters`	Sendet einen oder mehrere Parameter zum UTN-Server, die dann vom UTN-Server übernommen werden. Schreiben Sie Parameter und Werte in den E-Mail-Textkörper: `<Parameter> = <Wert>` Parameter und Wertekonventionen entnehmen Sie den Parameterlisten ⇨ 🗎85.
	`update utn`	Führt automatisch ein Update mit der in der Mail angehängten Software durch.
	`help`	Sie erhalten eine Seite mit Informationen zur Fernwartung.
[<Kommentar>]		Frei definierbarer Text für Beschreibungszwecke.

Für die Anweisungen gilt:

- keine Unterscheidung von großer bzw. kleiner Schreibweise (nicht case-sensitive)
- ein oder mehrere Leerzeichen sind möglich
- maximale Länge beträgt 128 Byte
- nur das ASCII-Format kann interpretiert werden

Bei Updates oder Parameteränderungen ist zudem eine TAN erforderlich. Zunächst müssen Sie sich via E-Mail eine Statusseite schicken lassen (⇨Tabelle 1 🗎17), weil diese die TAN enthält. Die erhaltene TAN geben Sie in die erste Zeile des E-Mail-Textkörpers ein. Anschließend muss ein Leerzeichen folgen.

✓ Auf dem UTN-Server ist ein DNS-Server konfiguriert ⇨ 🗎24.
✓ Damit der UTN-Server E-Mails empfangen kann, muss der UTN-Server als Benutzer mit eigener E-Mail-Adresse auf einem POP3-Server eingerichtet sein.
✓ Am UTN-Server sind POP3- und SMTP-Parameter konfiguriert ⇨ 🗎28.

1. Öffnen Sie ein E-Mail-Programm.
2. Erstellen Sie eine neue E-Mail:
   - Geben Sie als Adressat die UTN-Server-Adresse ein.
   - Geben Sie eine Anweisung in die Betreffzeile ein: `cmd: <Befehl> [<Kommentar>]`
     Befehle und Kommentar: ⇨Tabelle 1 🗎17.
   - Geben Sie ggf. eine TAN in den E-Mail-Textkörper ein.
3. Versenden Sie die E-Mail.

↳ Der UTN-Server erhält die E-Mail und führt die Anweisung aus.

Beispiele

Sie möchten die Parameterliste vom UTN-Server erhalten:

Empfänger: `UTN-Server@Firma.de`

Betreff: `cmd: get parameters`

Sie möchten den Parameter 'Beschreibung' konfigurieren:

Empfänger: `UTN-Server@Firma.de`

Betreff: `cmd: set parameters`

E-Mail-Textkörper:
```
TAN = nUn47ir79Ajs7QKE
sys_descr = <Ihre Beschreibung>
```

3 Netzwerkeinstellungen

Um den UTN-Server optimal in Ihr Netzwerk zu integrieren, können Sie folgende Einstellungen konfigurieren:

3.1 Wie konfiguriere ich IPv4-Parameter?

Bei der Hardware-Installation (⇨ 🕮 'Hardware Installation Guide'), wird der UTN-Server an das Netzwerk angeschlossen. Dann überprüft der UTN-Server, ob er eine IP-Adresse dynamisch über die Bootprotokolle BOOTP (Bootstrap Protocol) oder DHCP (Dynamic Host Configuration Protocol) erhält. Ist das nicht der Fall, gibt sich der INU-Server über Zeroconf selbst eine IP-Adresse aus dem für Zeroconf reservierten Adressbereich (169.254.0.0/16).

Wichtig:
Wird der UTN-Server in einem IPv6-fähigen Netzwerk angeschlossen, erhält er automatisch eine zusätzliche IPv6-Adresse ⇨ 🗎22.

Die zugewiesene IPv4-Adresse des UTN-Servers kann über das Software-Tool 'SEH UTN Manager' ermittelt werden. Dieser Schritt erfolgt üblicherweise bei der Inbetriebnahme (⇨ 🕮 'Quick Installation Guide').

Zur optimalen Integration des UTN-Servers in ein TCP/IP-Netzwerk können Sie verschiedene IPv4-Parameter konfigurieren und/oder ihm manuell eine statische IP-Adresse zuweisen.

- IPv4-Parameter via myUTNControl Center konfigurieren ⇨ 🗎20
- IPv4-Parameter via SEH UTN Manager konfigurieren ⇨ 🗎21
- IPv4-Adresse via SEH UTN Manager ermitteln und IPv4-Parameter konfigurieren ⇨ 🗎21

IPv4-Parameter via myUTNControl Center konfigurieren

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK** – **IPv4** an.
3. Konfigurieren Sie die IPv4-Parameter; ⇨Tabelle 2 🗎20.
4. Bestätigen Sie mit **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

Tabelle 2: IPv4-Parameter

Parameter	Beschreibung
DHCP BOOTP ARP/PING	De-/aktiviert die Protokolle DHCP, BOOTP und ARP/PING. Über DHCP und BOOTP erfolgt die IP-Adresszuweisung automatisch, wenn in Ihrem Netzwerk eines der Protokolle implementiert ist. Mit den Befehlen ARP und PING können Sie eine über Zeroconf zugewiesene IP-Adresse ändern. Die Implementierung der Befehle ist systemabhängig; lesen Sie die Dokumentation zu Ihrem Betriebssystem. *Wir empfehlen diese Optionen zu deaktivieren, sobald der UTN-Server eine IP-Adresse zugewiesen bekommen hat.*
IP-Adresse	IP-Adresse des UTN-Servers.
Netzwerkmaske	Netzwerkmaske des UTN-Servers. Mit Netzwerkmasken (auch Netzmasken oder Subnetzmasken) werden große Netzwerke logisch in Subnetzwerke unterteilt. Falls Sie den UTN-Server in einem Subnetzwerk einsetzen, benötigt er die Netzwerkmaske des jeweiligen Subnetzwerks.
Gateway	IP-Adresse des Standard-Gateways im Netzwerk, das der UTN-Server verwendet. Über das Gateway werden IP-Adressen in einem anderen Netzwerk angesprochen.

IPv4-Parameter via SEH UTN Manager konfigurieren

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.
✓ Der UTN-Server wird in der Auswahlliste angezeigt ⇨ 🗎41.

1. Starten Sie den SEH UTN Manager.
2. Markieren Sie den UTN-Server in der Auswahlliste.
3. Wählen Sie im Menü **UTN-Server** den Befehl **IP-Adresse definieren**.
   Der Dialog **IP-Adresse definieren** erscheint.
4. Geben Sie die entsprechenden TCP/IP-Parameter ein.
5. Wählen Sie die Schaltfläche **OK** an.

↳ Die Einstellungen werden gespeichert.

IPv4-Adresse via SEH UTN Manager ermitteln und IPv4-Parameter konfigurieren

Der SEH UTN Manager durchsucht das Netzwerk nach angeschlossenen INU-Servern.

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.

1. Starten Sie den SEH UTN Manager.
2. Bestätigen Sie den Hinweisdialog **Auswahlliste ist leer** mit **Ja**.
   Falls kein Hinweisdialog vorhanden ist und der Hauptdialog angezeigt wird, wählen Sie im Menü **Auswahlliste** den Befehl **Bearbeiten**.
   Der Dialog **Auswahlliste bearbeiten** erscheint.
3. Markieren Sie den INU-Server in der Netzwerkliste.

Falls Sie mehrere UTN-Server gleichen Modells einsetzen, können Sie ein bestimmtes Gerät anhand des Default-Namens (⇨ 🗎81) oder der angeschlossenen USB-Geräte identifizieren.

4. Wählen Sie im Kontextmenü **IP-Adresse definieren**.
   Der Dialog **IP-Adresse definieren** erscheint.
5. Geben Sie die entsprechenden TCP/IP-Parameter ein.
6. Wählen Sie die Schaltfläche **OK** an.

↳ Die Einstellungen werden gespeichert.

3.2 Wie konfiguriere ich IPv6-Parameter?

IPv6 (Internet Protocol Version 6) ist der Nachfolger des gegenwärtig überwiegend verwendeten Internet-Protokolls in der Version 4 (IPv4). IPv6 hat dieselben Grundfunktionen, hat aber viele Vorteile wie z.B. die Vergrößerung des Adressraums von 2^{32} (IPv4) auf 2^{128} (IPv6) IP-Adressen und die Autokonfiguration.

Wichtig:

Die IPv6-Notation unterscheidet sich von IPv4: IPv6-Adressen sind 128 Bit lang und werden als 8 x 16 Bit hexadezimal dargestellt.
Beispiel: `2001:db8:4:0:2c0:ebff:fe0f:3b6b`

In einer URL, z.B. im Browser, wird eine IPv6-Adresse in eckigen Klammern eingeschlossen. Diese Notation verhindert eine falsche Interpretation von Portnummern als Teil der IPv6-Adresse.
Beispiel: `http://[2001:db8:4:0:2c0:ebff:fe0f:3b6b]:443`

Die URL wird ausschließlich von IPv6-fähigen Browsern akzeptiert.

Sie können den UTN-Server in ein IPv6-Netzwerk einbinden.

WARNUNG

Die UTN-Funktionalität (⇨ 🗎2) und der zugehörige SEH UTN Manager funktionieren nur in IPv4-Netzwerken.

In reinen IPv6-Netzwerken kann lediglich auf das myUTN Control Center (⇨ 🗎8) zugegriffen werden, um den UTN-Server zu administrieren.

Seine IPv6-Adresse(n) erhält der UTN-Server automatisch und zusätzlich zur IPv4-Adresse. Zur optimalen Integration des UTN-Servers in Ihr IPv6-Netzwerk können Sie IPv6-Parameter konfigurieren.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK** – **IPv6** an.
3. Konfigurieren Sie die IPv6-Parameter; ⇨Tabelle 3 🗎22.
4. Bestätigen Sie mit **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

Tabelle 3: IPv6-Parameter

Parameter	Beschreibung
IPv6	De-/aktiviert die IPv6-Funktionalität des UTN-Servers.
Automatische Konfiguration	De-/aktiviert die automatische Vergabe der IPv6-Adressen für den UTN-Server.
IPv6-Adresse	Definiert eine manuell vergebene IPv6-Adresse im Format n:n:n:n:n:n:n:n für den UTN-Server: • Jedes 'n' stellt den hexadezimalen Wert von einem der acht 16-Bit-Elemente der Adresse dar. • Führende Nullen können vernachlässigt werden. • Ein Block aus zusammenhängenden Nullen kann mit zwei aufeinander folgenden Doppelpunkten zusammengefasst werden.
Router	Definiert manuell einen statischen Router, an den der UTN-Server seine Anfragen sendet.

Parameter	Beschreibung
Präfixlänge	Definiert die Länge des Subnetz-Präfixes für die IPv6-Adresse. Der Wert 64 ist voreingestellt. Adressbereiche (z.B. Ihr Netzwerk) werden durch Präfixe angegeben. Dazu wird die Präfixlänge (Anzahl der verwendeten Bits) als Dezimalzahl mit vorangehendem '/' an die IPv6-Adresse angehängt.

3.3 Wie konfiguriere ich den DNS?

DNS (Domain Name Service) erlaubt die gegenseitige Zuordnung von Namen und Adressen. Aktivieren Sie DNS, damit Sie Hostnamen anstelle von IP-Adressen eingeben können, wenn Sie Server definieren.

Beispiel: Konfiguration des Time-Servers (⇨ 🗎34) mit `ntp.server.de` anstelle von `10.168.0.140`

Wichtig:

Ist Ihr Netzwerk entsprechend konfiguriert, erhält der UTN-Server die DNS-Server-Einstellungen automatisch über DHCP. Ein so eingetragener DNS-Server hat immer Vorrang gegenüber manuellen Einstellungen.

✓ Ihr Netzwerk hat einen DNS-Server.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK** – **DNS** an.
3. Konfigurieren Sie die DNS-Parameter; ⇨Tabelle 4 🗎24.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 4: DNS-Parameter

Parameter	Beschreibung
DNS	De-/aktiviert die Namensauflösung über einen DNS-Server.
Erster DNS-Server	Definiert die IP-Adresse des ersten DNS-Servers.
Zweiter DNS-Server	Definiert die IP-Adresse des zweiten DNS-Servers. Der zweite DNS-Server wird benutzt, wenn der erste nicht verfügbar ist.
Domain-Name (Suffix)	Definiert den Domain-Namen eines vorhandenen DNS-Servers.

3.4 Wie konfiguriere ich SNMP?

SNMP (Simple Network Management Protocol) ist ein Protokoll für die Konfiguration und Überwachung von Netzwerkgeräten entwickelt. Das Protokoll regelt die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation (SNMP-Management-Tool). Dabei können Informationen gelesen und verändert werden.

SNMP gibt es in 3 Versionen, der UTN-Server unterstützt Version 1 und 3.

SNMPv1

SNMPv1 ist die erste und einfachere SNMP-Version. Nachteilig ist die unsichere Zugriffskontrolle, die über die sogenannte Community erfolgt: In einer Community werden Überwachungsstation und überwachte Geräte zusammengefasst. So lassen sie sich leichter administrieren. Es gibt dabei zwei Arten von Communities, schreibgeschützte und solche mit Lese-/Schreibzugriff. Bei beiden fungiert der Community-Name als Zugriffspasswort zwischen der Überwachungsstation und den überwachten Geräten in der Community. Da er im Klartext übertragen wird, stellt er keinen ausreichenden Schutz dar.

SNMPv3

SNMPv3 ist die neueste SNMP-Version. Es enthält Erweiterungen und ein neues Sicherheitskonzept, das u.a. Verschlüsselung und Authentifizierung umfasst. Daher müssen für SNMPv3 in der Überwachungsstation Name und Passwort für SNMP-Benutzer angelegt sein, die auf dem UTN-Server eingetragen werden.

Wichtig:

Die Benutzerkonten werden auch für den Zugang zum myUTN Control Center verwendet und daher unter **SICHERHEIT** – **Gerätezugriff** eingetragen, siehe 'Wie schütze ich den Zugriff auf das myUTN Control Center? (Benutzerkonten)' ⇨ 🗎62.

✓ In der Überwachungsstation sind SNMPv3-Benutzer angelegt. (Nur bei SNMPv3.)
✓ Die SNMPv3-Benutzer aus der Überwachungsstation sind auf dem UTN Server eingetragen ⇨ 🗎62. (Nur bei SNMPv3.)

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK** – **SNMP** an.
3. Konfigurieren Sie die SNMP-Parameter; ⇨Tabelle 5 🗎25.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 5: SNMP-Parameter

Parameter	Beschreibung
SNMPv1	De-/aktiviert die SNMPv1-Funktionalität.
Nur Lesen	De-/aktiviert den Schreibschutz für die Community.
Community	Name der SNMP-Community. Tragen Sie den Namen so ein, wie er in der Überwachungsstation definiert ist. **Wichtig:** Der standardmäßig eingetragene Name ist 'public'. Dieser Name wird weitläufig für Communities mit Lese-/Schreibzugriff verwendet. Wir empfehlen diesen sobald wie möglich zu ändern, um die Sicherheit zu erhöhen.
SNMPv3	De-/aktiviert die SNMPv3-Funktionalität.
Hash	Definiert den Hash-Algorithmus.
Zugriffsrechte	Definiert die Zugriffsrechte des SNMP-Benutzers.

Parameter	Beschreibung
Verschlüsselung	Definiert die Verschlüsselungsmethode.

3.5 Wie konfiguriere ich Bonjour?

Bonjour ist eine Technik zur automatischen Erkennung von Geräten und Diensten in TCP/IP-Netzwerken.

Der UTN-Server nutzt Bonjour um

- IP-Adressen zu prüfen
- Netzwerkdienste bekanntzugeben und zu finden
- Hostnamen und IP-Adressen zuzuordnen

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK** – **Bonjour** an.
3. Konfigurieren Sie die Bonjour-Parameter; ⇨Tabelle 6 🗎27.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 6: Bonjour-Parameter

Parameter	Beschreibung
Bonjour	De-/aktiviert Bonjour.
Bonjour-Name	Definiert den Bonjour Namen des UTN-Servers. Der UTN-Server gibt unter diesem Namen seine Bonjour-Dienste bekannt. Wird kein Bonjour-Name eingegeben, wird ein Standardname verwendet (Geräte-name@ICxxxxxx).

3.6 Wie konfiguriere ich E-Mail (POP3 und SMTP)?

Der UTN-Server kann via E-Mail administriert (⇨ 🗎17) werden und verfügt über einen Benachrichtigungsservice (⇨ 🗎39), der Ihnen Status- und Fehlermeldungen via E-Mail schickt. Um diese Funktionen zu nutzen, müssen die E-Mail-Protokolle 'POP3' und 'SMTP' am UTN-Server konfiguriert werden:

Mit POP3 (Post Office Protocol Version 3) ruft ein Client, wie z.B. der UTN-Server, E-Mails von einem E-Mail-Server ab. Am UTN-Server muss POP3 konfiguriert sein, damit er via E-Mail administriert werden kann.

Mit SMTP (Simple Mail Transfer Protocol) werden E-Mails versendet und weitergeleitet. Der UTN-Server benötigt SMTP für die Administration via E-Mail und den Benachrichtigungsservice.

- POP3 konfigurieren ⇨ 🗎28
- SMTP konfigurieren ⇨ 🗎29

POP3 konfigurieren

✓ Auf dem POP3-Server ist ein E-Mail-Benutzerkonto für den UTN-Server angelegt.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK** – **E-Mail** an.
3. Konfigurieren Sie die POP3-Parameter; ⇨Tabelle 7 🗎28.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 7: POP3-Parameter

Parameter	Beschreibung
POP3	De-/aktiviert die POP3-Funktionalität.
POP3 – Servername	Definiert den POP3-Server über die IP-Adresse oder den Hostnamen. Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.
POP3 – Serverport	Definiert den Port, über den der UTN-Server E-Mails empfängt. Die standardmäßig bei POP3 verwendete Portnummer 110 ist voreingestellt. Bei SSL/TLS (Parameter 'POP3 – Sicherheit' ⇨ 🗎28) wird standardmäßig 995 verwendet. Lesen Sie hierzu ggf. die Dokumentation des POP3-Servers.
POP3 – Sicherheit	Definiert das anzuwendende Authentifizierungsverfahren: • APOP: verschlüsselt das Passwort beim Einloggen auf dem POP3-Server • SSL/TLS: verschlüsselt die gesamte Kommunikation mit dem POP3-Server. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨ 🗎60.
POP3 – E-Mails abfragen alle	Definiert das Zeitintervall (in Minuten) mit dem E-Mails vom POP3-Server abgefragt werden.
POP3 – E-Mails ignorieren mit mehr als	Definiert die maximale Größe (in Kbyte) der vom UTN-Server akzeptierten E-Mails. (0 = unbegrenzt)
POP3 – Benutzername	Definiert den Benutzernamen, den der UTN-Server benutzt, um sich am POP3-Server anzumelden.
POP3 – Passwort	Definiert das Benutzerpasswort, das der UTN-Server benutzt, um sich am POP3-Server anzumelden.

SMTP konfigurieren

✓ Auf dem SMTP-Server ist ein E-Mail-Benutzerkonto für den UTN-Server angelegt.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK** – **E-Mail** an.
3. Konfigurieren Sie die SMTP-Parameter; ⇨Tabelle 8 🗎29.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 8: SMTP-Parameter

Parameter	Beschreibung
SMTP – Servername	Definiert den SMTP-Server über die IP-Adresse oder den Hostnamen. Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.
SMTP – Serverport	Definiert den Port, über den der UTN- und SMTP-Server kommunizieren. Die standardmäßig bei SMTP verwendete Portnummer 25 ist voreingestellt. Bei SSL/TLS (Parameter 'SMTP – SSL/TLS' ⇨ 🗎29) verwenden SMTP-Server standardmäßig den Port 587 (STARTSSL/STARTTLS) oder den veralteten Port 465 (SMTPS). Lesen Sie hierzu ggf. die Dokumentation des SMTP-Servers.
SMTP – SSL/TLS	De-/aktiviert die Option SSL/TLS. Mit SSL/TLS wird der Übertragungsweg vom UTN-Server zum SMTP-Server verschlüsselt. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨ 🗎60.
SMTP – Name des Absenders	Definiert die E-Mail-Adresse, die der UTN-Server zum Versenden von E-Mails verwendet. Oft sind der Name des Absenders und der Benutzername des E-Mail-Benutzerkontos identisch.
SMTP – Anmelden	De-/aktiviert die SMTP-Authentifizierung. Beim E-Mail-Versand übermitteltet der UTN-Server Benutzername und Passwort an den SMTP-Server um sich zu authentifizieren. Tragen Sie Benutzername (Parameter 'SMTP – Benutzername' ⇨ 🗎29) und Passwort (Parameter 'SMTP – Passwort' ⇨ 🗎29) ein. Einige SMTP-Server sind für SMTP-Authentifizierung konfiguriert, um Missbrauch (Spam) zu verhindern.
SMTP – Benutzername	Definiert den Benutzernamen, den der UTN-Server benutzt, um sich am SMTP-Server anzumelden.
SMTP – Passwort	Definiert das Passwort, das der UTN-Server benutzt, um sich am SMTP-Server anzumelden.
SMTP – Sicherheit (S/MIME)	De-/aktiviert den E-Mail-Sicherheitsstandard S/MIME (Secure/Multipurpose Internet Mail Extensions). Mit S/MIME können E-Mails signiert ('SMTP – E-Mail signieren' ⇨ 🗎29) oder verschlüsselt ('SMTP – Vollständig verschlüsseln' ⇨ 🗎30) werden. Aktivieren Sie die gewünschte Funktion (ggf. mit 'SMTP – Öffentlichen Schlüssel beifügen' ⇨ 🗎30).
SMTP – E-Mail signieren	Aktiviert das Signieren von E-Mails. Mit der Signatur kann der Empfänger die Identität des Absenders zu prüfen. Dadurch wird gewährleistet, dass die E-Mail nicht verändert wurde. Für das Signieren wird ein S/MIME-Zertifikat benötigt ⇨ 🗎67.

Parameter	Beschreibung
SMTP – Vollständig verschlüsseln	Aktiviert das Verschlüsseln von E-Mails. Eine verschlüsselte E-Mail kann nur vom vorgesehenen Empfänger geöffnet und gelesen werden. Für die Verschlüsselung wird ein S/MIME-Zertifikat benötigt ⇨ 67.
SMTP – Öffentlichen Schlüssel beifügen	Sendet den öffentlichen Schlüssel zusammen mit der E-Mail. Viele E-Mail-Clients benötigen den Schlüssel um die E-Mail anzeigen zu können.

3.7 Wie setze ich den UTN-Server in VLAN-Umgebungen ein?

Der UTN-Server unterstützt die Verwendung von VLAN (Virtual Local Area Network – virtuelle lokale Netzwerke) gemäß 802.1Q.

Ein VLAN trennt ein physisches Netzwerk in mehrere logische Teilnetze auf. Zwischen den Teilnetzen können Datenpakete nicht ausgetauscht werden weil es eine eigene Broadcast-Domäne ist. VLANs werden eingesetzt, um Netzwerke zu organisieren und vor allem abzusichern.

Jedes USB-Gerät kann einem VLAN zugeordnet werden. Damit die VLAN-Daten über die USB-Ports weitergeleitet werden, müssen Sie zunächst die VLANs am UTN-Server eintragen. Anschließend müssen Sie die USB-Ports, über welche die Daten weitergeleitet werden sollen, mit den eingetragenen VLANs verknüpfen.

Mit VLAN kann der Zugriff auf USB-Geräte besonders gut reguliert werden: einer definierten Gruppe von Netzteilnehmern werden bestimmte USB-Geräten zur Verfügung gestellt.
Informieren Sie sich, wie Sie VLAN in Ihrer Umgebung implementieren und konfigurieren Sie anschließend den UTN-Server dafür.

- IPv4-Management-VLAN eintragen ⇨ 🗎31
- IPv4-Client-VLAN eintragen ⇨ 🗎32
- IPv4-Client-VLAN einem USB-Port zuordnen ⇨ 🗎32

IPv4-Management-VLAN eintragen

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK** – **IPv4-VLAN** an.
3. Konfigurieren Sie die IPv4-Management-VLAN-Parameter; ⇨Tabelle 9 🗎31.
4. Bestätigen Sie mit **Speichern**.
5. Die Einstellungen werden gespeichert.

Tabelle 9: IPv4-Management-VLAN-Parameter

Parameter	Beschreibung
IPv4-Management-VLAN	De-/aktiviert die Weiterleitung der IPv4-Management-VLAN-Daten. Ist die Option aktiviert, ist SNMP ist ausschließlich im IPv4-Management-VLAN verfügbar.
VLAN-ID	ID zur Identifizierung des IPv4-Management-VLANs (0–4096).
IP-Adresse	IP-Adresse des UTN-Servers ⇨ 🗎20.
Netzwerkmaske	Netzwerkmaske des UTN-Servers ⇨ 🗎20.
Gateway	IP-Adresse des Standard-Gateways im Netzwerk, das der UTN-Server verwendet ⇨ 🗎20. Über das Gateway werden IP-Adressen in einem anderen Netzwerk angesprochen.
Zugriff über alle VLANs	De-/aktiviert den administrativen Zugang (Web) zum UTN-Server über IPv4-Client-VLAN. Ist die Option aktiviert, kann der UTN-Server aus allen VLANs heraus administriert werden.

Parameter	Beschreibung
Zugriff vom LAN (untagged)	De-/aktiviert den administrativen Zugang zum UTN-Server über IPv4-Pakete ohne VLAN-Tag. Ist die Option deaktiviert, kann der UTN-Server ausschließlich über VLANs administriert werden.

IPv4-Client-VLAN eintragen

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK** – **IPv4-VLAN** an.
3. Konfigurieren Sie die IPv4-VLAN-Parameter; ⇨Tabelle 10 🗎32.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 10: IPv4-Client-VLAN-Parameter

Parameter	Beschreibung
VLAN	De-/aktiviert die Weiterleitung der IPv4-Client-VLAN-Daten.
IP-Adresse	IP-Adresse des UTN-Servers innerhalb des IPv4-Client-VLANs.
Netzwerkmaske	Netzwerkmaske des UTN-Servers innerhalb des IPv4-Client-VLANs.
Gateway	Gateway-Adresse des IPv4-Client-VLANs.
VLAN-ID	ID zur Identifizierung des IPv4-Client-VLANs (0–4096).

*Nutzen Sie die Schaltfläche **Automatisch ausfüllen**, um die Felder **VLAN**, **IP-Adresse** und **Netzwerkmaske** automatisch mit den Werten aus Zeile 1 zu füllen. Die **VLAN ID** wird dabei automatisch um '1' hochgezählt.*

IPv4-Client-VLAN einem USB-Port zuordnen

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **USB-Portzugriff** an.
3. Weisen Sie über die Liste **VLAN zuordnen** dem USB-Port ein VLAN zu.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

4 Geräteeinstellungen

4.1 Wie konfiguriere ich die Gerätezeit?

Die Gerätezeit des UTN-Servers kann über einen SNTP-Zeitserver (Simple Network Time Protocol) im Netzwerk gesteuert werden. Ein Zeit-Server synchronisiert die Zeit mehrerer Geräte innerhalb eines Netzwerkes.

Es wird die heute gültige koordinierte Weltzeit ('UTC' – Universal Time Coordinated) verwendet. Standortabweichungen werden durch die Zeitzone ausgeglichen.

Wichtig:

Ist Ihr Netzwerk entsprechend konfiguriert, erhält der UTN-Server die Zeit-Server-Einstellungen automatisch über DHCP. Ein so eingetragener Zeit-Server hat immer Vorrang gegenüber einem manuell eingetragenen Zeit-Server.

✓ Im Netzwerk wird ein Zeit-Server betrieben.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **GERÄT** – **Datum/Zeit** an.
3. Aktivieren Sie die Option **Datum/Zeit**.
4. Geben Sie im Feld **Time-Server** die IP-Adresse oder den Hostnamen des Zeit-Servers ein.
   (Der Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde ⇨ 24.)
5. Wählen Sie aus der Liste **Zeitzone** das Kürzel für Ihre lokale Zeitzone.
6. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

4.2 Wie lege ich eine Beschreibung fest?

Sie können dem UTN-Server freidefinierbare Beschreibungen zuweisen. Damit haben Sie einen besseren Überblick über die im Netzwerk vorhandenen Geräte.

USB-Ports können Sie zur Unterscheidung ebenfalls Namen zuweisen ⇨ 36.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **GERÄT** – **Beschreibung** an.
3. Geben Sie in die Felder **Hostname**, **Beschreibung** und **Ansprechpartner** freidefinierbare Bezeichnungen ein.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 11: Beschreibung

Parameter	Beschreibung
Hostname	Geräte-Name als Alternative zur IP-Adresse. Mithilfe des Namen können Sie den UTN-Server leichter im Netzwerk identifizieren, z.B. falls Sie mehrere UTN-Server verwenden. Wird im myUTN Control Center und im SEH UTN Manager angezeigt.
Beschreibung	Geräte-Beschreibung, z.B. Aufstellort oder Abteilung. Wird im myUTN Control Center und im SEH UTN Manager angezeigt.
Ansprechpartner	Kontaktperson, z.B. Geräte-Administrator. Wird im myUTN Control Center angezeigt.

4.3 Wie weise ich einem USB-Port einen Namen zu?

Standardmäßig werden im myUTN Control Center und SEH UTN Manager am USB-Port die Namen des angeschlossenen USB-Gerätes angezeigt. Diese Namen werden durch die Gerätehersteller vergeben und sind nicht immer eindeutig oder aussagekräftig.

Deswegen können Sie den USB-Ports beliebige Bezeichnungen zuzuweisen, z.B. den Namen einer zugehörigen Software. Auf diese Weise erhalten Sie einen besseren Überblick über die im Netzwerk vorhandenen USB-Geräte.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **GERÄT** – **USB-Port** an.
3. Geben Sie im Feld **Portname** eine Bezeichnung ein.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

4.4 Wie schalte ich einen USB-Port ab?

Standardmäßig sind alle USB-Ports aktiv. Sie können einen USB-Port ausschalten (und wieder einschalten) indem Sie die Stromzufuhr unterbrechen bzw. wiederherstellen.

Schalten Sie

- unbenutzte USB-Ports ab um sicherzustellen, dass keine ungewünschten USB-Geräte in das Netzwerk eingebunden werden. (Abgeschaltete USB-Ports sind im SEH UTN Manager nicht sichtbar.)
- einen USB-Port aus und wieder ein, um das angeschlossene USB-Gerät neu zu starten, wenn es sich in einem undefinierten Zustand befindet. (Das USB-Gerät muss nicht manuell zu entfernt und erneut angeschlossen werden).

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **GERÄT** – **USB-Port** an.
3. De-/aktivieren Sie die Option vor dem **USB-Port**.
4. Bestätigen Sie mit **Speichern**.

↳ Der USB-Port wird aus- bzw. eingeschaltet.

4.5 Wie konfiguriere ich den UTN-(SSL-)Port?

Für den Datentransfer zwischen Client und UTN-Server inklusive der angeschlossenen USB-Geräte wird ein gemeinsamer Port verwendet. Er unterscheidet sich je nach Verbindungstyp:

- unverschlüsselte USB-Verbindung: UTN-Port (Standard = 9200)
- verschlüsselte USB-Verbindung (⇨ 🗎57): UTN-SSL-Port (Standard = 9443)

WARNUNG

Der UTN-Port bzw. der UTN-SSL-Port darf nicht durch eine Sicherheitssoftware (Firewall) blockiert werden.

Die Portnummer können Sie ändern, z.B. wenn die Portnummer in Ihrem Netzwerk bereits von einer anderen Anwendung genutzt wird. Die Änderung erfolgt am UTN-Server und wird per SNMPv1 an die auf den Clients installierten SEH UTN Manager weitergegeben.

✓ SNMPv1 ist aktiviert ⇨ 🗎25.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **GERÄT** – **UTN-Port** an.
3. Geben Sie im Feld **UTN-Port** bzw. **UTN-SSL-Port** die Portnummer ein.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

4.6 Wie erhalte ich Benachrichtigungen?

Der UTN-Server kann Ihnen verschiedene Benachrichtigungen schicken:

- Status-E-Mail: Regelmäßig versendete E-Mail, die den Status des UTN-Servers inklusive der angeschlossenen USB-Geräte enthält.
- Ereignis-Benachrichtigung via E-Mail oder SNMP-Trap:
  - USB-Gerät an den UTN-Server angeschlossen/ vom UTN-Server entfernt
  - USB-Port (d.h. Verbindung zu dem daran angeschlossenen USB-Gerät) aktiviert/deaktiviert
  - Neustart des UTN-Servers
- Versand von Status-E-Mails konfigurieren ⇨ 🗎39
- Ereignis-Benachrichtigung via E-Mail konfigurieren ⇨ 🗎39
- Ereignis-Benachrichtigung via SNMP-Trap konfigurieren ⇨ 🗎39

Versand von Status-E-Mails konfigurieren

Die Status-E-Mail kann an bis zu zwei Empfänger geschickt werden.

✓ SMTP ist konfiguriert ⇨ 🗎28.
✓ DNS ist konfiguriert ⇨ 🗎24.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **GERÄT** – **Benachrichtigung** an.
3. Geben Sie im Feld **E-Mail-Adresse** den Empfänger ein.
4. Aktivieren Sie im Bereich **Status-E-Mail** den/die Empfänger.
5. Definieren Sie das Sendeintervall.
6. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Ereignis-Benachrichtigung via E-Mail konfigurieren

Die Ereignis-E-Mails können an bis zu zwei Empfänger geschickt werden.

✓ SMTP ist konfiguriert ⇨ 🗎28.
✓ DNS ist konfiguriert ⇨ 🗎24.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **GERÄT** – **Benachrichtigung** an.
3. Geben Sie im Feld **E-Mail-Adresse** den Empfänger ein.
4. Aktivieren Sie die Optionen mit den gewünschten Meldungstypen.
5. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Ereignis-Benachrichtigung via SNMP-Trap konfigurieren

Die Ereignis-SNMP-Traps können an bis zu zwei Empfänger geschickt werden.

✓ SNMPv1 oder/und SNMPv3 ist konfiguriert ⇨ 🗎25.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **GERÄT** – **Benachrichtigung** an.
3. Definieren Sie im Bereich **SNMP-Traps** die Empfänger über die IP-Adresse und die Community.
4. Aktivieren Sie die Optionen mit den gewünschten Meldungstypen.
5. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

5 Arbeiten mit dem SEH UTN Manager

Der 'SEH UTN Manager' ist ein von SEH Computertechnik GmbH entwickeltes Software-Tool. Mit dem SEH UTN Manager werden Verbindungen zu den USB-Geräten an UTN-Servern hergestellt und verwaltet.

5.1 Wie finde ich UTN-Server/USB-Geräte im Netzwerk?

Mit dem Software-Tool 'SEH UTN Manager' werden Verbindungen zu den USB-Geräten an UTN-Servern hergestellt und verwaltet.

Nach dem Start des SEH UTN Managers muss zunächst im Netzwerk nach angeschlossenen UTN-Servern gesucht werden. Der zu scannende Netzwerkbereich ist frei definierbar; es kann über Multicast und/oder in freidefinierbaren IP-Bereichen gesucht werden. Voreingestellt ist die Multicastsuche in dem lokalen Netzwerksegment.

Alle gefundenen UTN-Server und deren angeschlossene USB-Geräte werden in der 'Netzwerkliste' angezeigt. Um die an einen UTN-Server angeschlossenen USB-Geräte zu verwenden, müssen Sie den UTN-Server zur 'Auswahlliste' hinzufügen.

Alternativ können Sie einen UTN-Server direkt zur Auswahlliste hinzufügen. Dafür müssen Sie seine IP-Adresse kennen.

Suchparameter definieren

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.

1. Starten Sie den SEH UTN Manager.
2. Wählen Sie im Menü **Programm** den Befehl **Optionen**.
   Der Dialog **Optionen** erscheint.
3. Wählen Sie die Registerkarte **Netzwerksuche** an.
4. Aktivieren Sie die Option **Netzwerkbereichsuche** und definieren Sie einen oder mehrere Netzwerkbereiche.
5. Wählen Sie die Schaltfläche **OK** an.

↳ Die Einstellungen werden gespeichert.

Netzwerk durchsuchen

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.

1. Starten Sie den SEH UTN Manager.
2. Wählen Sie im Menü **Auswahlliste** den Befehl **Bearbeiten**.
   Der Dialog **Auswahlliste bearbeiten** erscheint.
3. Wählen Sie die Schaltfläche **Suche** an.
4. Das Netzwerk wird durchsucht. Die gefundenen UTN-Server und USB-Geräte werden in der Netzwerkliste angezeigt.

UTN-Server zur 'Auswahlliste' hinzufügen

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.
✓ Der UTN-Server wurde bei der Netzwerksuche gefunden und wird in der Netzwerkliste angezeigt.

1. Starten Sie den SEH UTN Manager.
2. Wählen Sie im Menü **Auswahlliste** den Befehl **Bearbeiten**.
   Der Dialog **Auswahlliste bearbeiten** erscheint.
3. Markieren Sie in der Netzwerkliste den zu verwendenden UTN-Server.
4. Wählen Sie die Schaltfläche **Hinzufügen** an.
   (Wiederholen Sie die Schritte 2-3 nach Bedarf.)
5. Wählen Sie die Schaltfläche **OK** an.

↳ Die UTN-Server mitsamt den angeschlossenen USB-Geräten werden in der Auswahlliste angezeigt.

Abbildung 5: SEH UTN Manager – Auswahlliste bearbeiten

UTN-Server über IP-Adresse hinzufügen

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.
✓ Sie kennen die IP-Adresse des UTN-Servers.

1. Starten Sie den SEH UTN Manager.
2. Wählen Sie im Menü **UTN-Server** den Befehl **Hinzufügen**.
   Der Dialog **Server hinzufügen** erscheint.
3. Geben Sie im Feld **Name oder IP-Adresse** die IP-Adresse des UTN-Servers ein.
4. Sofern Sie den UTN-Port oder den UTN-SSL-Port geändert haben (⇨ 🗎38), geben Sie in den Feldern **UTN-Port** und **UTN-SSL-Port** die jeweiligen Portnummern an.
5. Wählen Sie die Schaltfläche **OK** an.

↳ Der UTN-Server mitsamt den angeschlossenen USB-Geräten wird in der Auswahlliste angezeigt.

5.2 Wie stelle ich eine Verbindung zu einem USB-Gerät her?

Um ein USB-Gerät mit dem Client zu verbinden, wird eine Punkt-zu-Punkt-Verbindung zwischen dem Client und dem USB-Port des UTN-Servers, an den das USB-Gerät angeschlossen ist, hergestellt. Das USB-Gerät kann dann so genutzt werden, als ob es direkt am Client angeschlossen wäre.

Wichtig:

Sonderfall Compound-USB-Gerät

Bei dem Anschluss bestimmter USB-Geräte an einen USB-Port des UTN-Servers werden in der Auswahlliste mehrere USB-Geräte am Port dargestellt. Dabei handelt es sich um sogenannte Compound-USB-Geräte. Sie bestehen aus einem Hub und einem oder mehreren USB-Geräten, die alle in einem einzigen Gehäuse eingebaut sind.

Wenn die Verbindung zu einem Port mit angeschlossenem Compound-USB-Gerät hergestellt wird, werden alle dargestellten USB-Geräte mit dem Client des Benutzers verbunden. Jedes eingebaute USB-Gerät belegt dabei einen virtuellen USB-Port des UTN-Servers. Die Anzahl dieser virtuellen USB-Ports ist abhängig vom UTN-Server-Modell. Wird sie überschritten, können keine weiteren USB-Geräte am UTN-Server verwendet werden.

UTN-Server	Anzahl virtueller USB-Ports
myUTN-2500	12

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.
✓ Der USB-Port wird in der Auswahlliste angezeigt ⇨ 🗎41.
✓ Auf dem Client sind alle Vorbereitungen (Treiberinstallation usw.) getroffen worden, die notwendig wären, um das USB-Gerät lokal (also direkt an dem Client angeschlossen) zu betreiben. Idealerweise ist das USB-Gerät zuvor lokal am Client nach der Anleitung des Herstellers angeschlossen und betrieben worden.
✓ Der USB-Port ist nicht mit einem anderen Client verbunden.

1. Starten Sie den SEH UTN Manager.
2. Markieren Sie den Port in der Auswahlliste.
3. Wählen Sie im Menü **Port** den Befehl **Aktivieren**.

↳ Die Verbindung zwischen USB-Gerät und Client wird hergestellt.

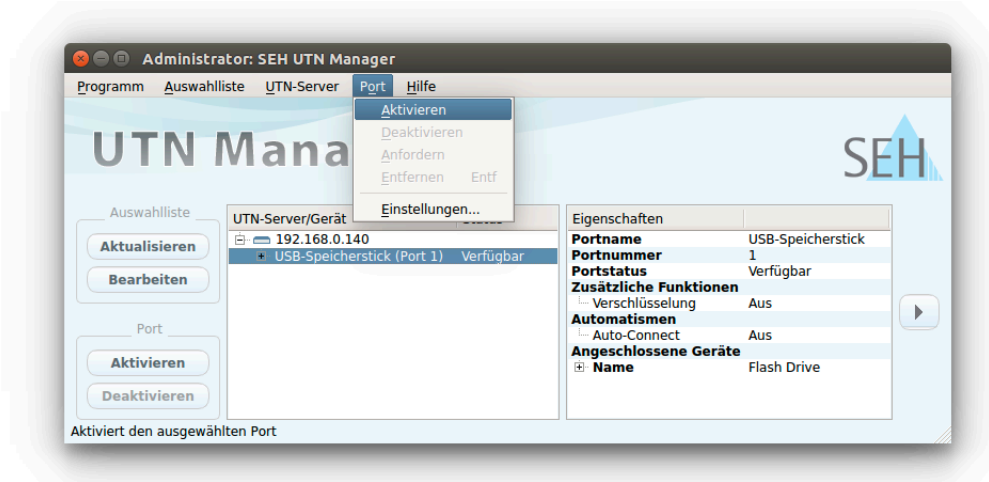


Abbildung 6: SEH UTN Manager – USB-Port aktivieren

5.3 Wie trenne ich die Verbindung zwischen USB-Gerät und Client?

Wenn ein USB-Gerät mit einem Client verbunden ist, besteht eine Punkt-zu-Punkt-Verbindung. Solange diese Verbindung besteht, kann kein anderer Benutzer das USB-Gerät mit seinem Client verbinden und nutzen. Trennen Sie daher die Verbindung, sobald Sie das USB-Gerät nicht mehr benötigen

Um die Verbindung zwischen USB-Gerät vom Client zu trennen, deaktivieren Sie die Verbindung zwischen dem Client und dem USB-Port des UTN-Servers an den das USB-Gerät angeschlossen ist:

- Üblicherweise trennt der Benutzer die Verbindung via SEH UTN Manager ⇨ 🗎44.
- Zudem kann der Administrator die Verbindung über das myUTN Control Center trennen ⇨ 🗎44.
- Auch eine automatische Trennung lässt sich einrichten (Auto Disconnect) ⇨ 🗎46.

Geräteverbindung via SEH UTN Manager trennen

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.
✓ Der USB-Port wird in der Auswahlliste angezeigt ⇨ 🗎41.
✓ Der USB-Port ist mit Ihrem Client verbunden ⇨ 🗎43.

1. Starten Sie den SEH UTN Manager.
2. Markieren Sie den Port in der Auswahlliste.
3. Wählen Sie im Menü **Port** den Befehl **Deaktivieren**.

↳ Die Verbindung wird getrennt.

Geräteverbindung via myUTN Control Center trennen

✓ Ein USB-Port ist mit einem Client verbunden ⇨ 🗎43.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **START** an.
3. Finden Sie in der Liste **Angeschlossene Geräte** die aktive Verbindung und wählen Sie das Symbol  an.
4. Bestätigen Sie die Sicherheitsabfrage.

↳ Die Verbindung wird getrennt.

5.4 Wie fordere ich ein belegtes USB-Gerät an?

Wenn ein USB-Gerät mit einem Client verbunden ist, besteht eine Punkt-zu-Punkt-Verbindung. Solange diese Verbindung besteht, kann kein anderer Benutzer das USB-Gerät mit seinem Client verbinden und nutzen.

Wenn Sie ein belegtes USB-Gerät nutzen möchten, können Sie es anfordern. Der andere Benutzer erhält dann eine Freigabe-Aufforderung in Form eines Popup-Fensters. Wenn er der Aufforderung nachkommt und seine Verbindung zum USB-Gerät beendet, wird die Verbindung zwischen dem USB-Gerät und Ihrem Client automatisch hergestellt.

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.
✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client des Benutzers, der das USB-Gerät verwendet, installiert ⇨ 🗎9.
✓ Der SEH UTN Manager (vollständige Variante) wird mit grafischer Bedienoberfläche auf beiden Clients ausgeführt.
✓ Der USB-Port wird in der Auswahlliste angezeigt ⇨ 🗎41.
✓ Der USB-Port ist mit einem anderen Client verbunden ⇨ 🗎43 (aber nicht via Auto-Connect).

5. Markieren Sie den Port in der Auswahlliste.
6. Wählen Sie im Menü **Port** den Befehl **Anfordern**.

↳ Die Freigabe-Aufforderung wird gesendet.

5.5 Wie automatisiere ich Verbindungen zu USB-Geräten und Programmstarts?

Die Verbindungen zu USB-Ports des UTN-Servers und den daran angeschlossenen USB-Geräten können automatisiert werden. Dabei können einfache bis komplexe Szenarien umgesetzt werden:

- Automatische Verbindung wenn ein USB-Gerät angeschlossen wird (Auto-Connect) ⇨ 🗎46
- Verbindung nach einem definierten Zeitraum automatisch trennen (Auto-Disconnect) ⇨ 🗎46

Dieses Kapitel beschreibt Funktionen des SEH UTN Managers, mit denen Automatismen eingerichtet werden. Benutzern mit Experten-Wissen über Skripte empfehlen wir das Kommandozeilen-Tool 'utnm' ⇨ 🗎52.

Automatische Verbindung wenn ein USB-Gerät angeschlossen wird (Auto-Connect)

Beim Auto-Connect wird automatisch eine Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät hergestellt, sobald ein USB-Gerät am USB-Port angeschlossen wird. Auto-Connect muss für jeden USB-Port einzeln aktiviert werden und gilt für alle USB-Geräte die an den USB-Port angeschlossen werden.

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.
✓ Der USB-Port wird in der Auswahlliste angezeigt ⇨ 🗎41.
✓ Sie sind als Administrator am Client angemeldet.

1. Starten Sie den SEH UTN Manager.
2. Markieren Sie den UTN-Server in der Auswahlliste.
3. Wählen Sie im Menü **UTN-Server** den Befehl **Auto-Connect aktivieren**.
   Der Dialog **Auto-Connect aktivieren** erscheint.
4. Aktivieren Sie die Option für die gewünschten USB-Ports.
5. Wählen Sie die Schaltfläche **OK** an.

↳ Die Einstellung wird gespeichert.

Die Verbindung zum USB-Port und dem daran angeschlossenen USB-Gerät wird sofort automatisch hergestellt. Wenn Sie das USB-Gerät entfernen und wieder anschließen wird die Verbindung erneut automatisch hergestellt.

Wichtig:
Wenn Sie eine aktive USB-Portverbindung die über Auto-Connect hergestellt wurde manuell deaktivieren, wird Auto-Connect ausgeschaltet. Falls Sie Auto-Connect wieder nutzen möchten, müssen Sie es später erneut konfigurieren

Verbindung nach einem definierten Zeitraum automatisch trennen (Auto-Disconnect)

Der Auto-Disconnect trennt die Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät automatisch sobald ein definierter Zeitraum abgelaufen ist. Dabei erhält der Benutzer des USB-Gerätes 2 Minuten vor Ablauf des Zeitraums eine Meldung in der er aufgefordert wird, die Verbindung zu beenden, um Datenverlust und Fehlerzuständen vorzubeugen. Optional kann dem Benutzer eine einmalige Verlängerung der Verbindung um die Dauer des definierten Zeitraums angeboten werden. In diesem Fall hat der Benutzer bei der Meldung die Möglichkeit, die Verlängerung zu aktivieren oder abzulehnen.

Mit Auto-Disconnect ermöglichen Sie einer großen Anzahl von Netzwerkteilnehmern den Zugriff auf eine geringe Anzahl an USB-Geräten und verhindern Geräteleerläufe.

Lassen Sie sich nach dem automatischen Trennen einer Verbindung über die Portverfügbarkeit informieren. Richten Sie hierzu eine Benachrichtigung über die Freigabe eines USB-Ports ein ⇨ 🗎48.

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.

✓ Der UTN-Server wird im Bereich 'Automatische Gerätetrennung' angezeigt ⇨ 🗎41.
✓ Sie sind als Administrator am Client angemeldet.

1. Starten Sie den SEH UTN Manager.
2. Markieren Sie den UTN-Server in der Auswahlliste.
3. Wählen Sie im Menü UTN-Server den Befehl "Auto-Disconnect aktivieren".
   Der Dialog **Auto-Disconnect** aktivieren erscheint.
4. Aktivieren Sie die Option für die gewünschten USB-Ports.
5. Definieren Sie den gewünschten Zeitraum (10–9999 Minuten).
6. Aktivieren Sie bei Bedarf die Option **Verlängerung**.
7. Wählen Sie die Schaltfläche **OK** an.

↳ Die Einstellung wird gespeichert.

5.6 Wo finde ich Statusinformationen von USB-Ports und USB-Geräten?

Sie können jederzeit die Statusinformation von USB-Ports und USB-Geräten einsehen. Zudem können Sie automatische Meldungen konfigurieren. Sie werden dann informiert über die Freigabe eines USB-Ports oder die Dauer einer Verbindung zu einem USB-Port.

Wichtig:

Die Meldungen erscheinen unter Umständen nicht.

Die Meldungsfunktion steht in Abhängigkeit zum Fenstermanager des Systems. Aufgrund der Vielfalt an Linux-Systemen (und Fenstermanagern) kann die Verfügbarkeit der Benachrichtigungsfunktion nicht garantiert werden.

- Statusinformationen anzeigen ⇨ 🗎48
- Benachrichtigung bei Freigabe eines USB-Ports ⇨ 🗎48
- Benachrichtigung über die Dauer einer Verbindung ⇨ 🗎48

Statusinformationen anzeigen

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.
✓ Der USB-Port wird in der Auswahlliste angezeigt ⇨ 🗎41.

1. Starten Sie den SEH UTN Manager.
2. Markieren Sie den USB-Port in der Auswahlliste.

↳ Die Statusinformationen werden in dem Bereich **Eigenschaften** angezeigt.

Benachrichtigung bei Freigabe eines USB-Ports

Sie erhalten eine Meldung, sobald ein Netzteilnehmer die Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät deaktiviert.

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.
✓ Der USB-Port wird in der Auswahlliste angezeigt ⇨ 🗎41.

1. Markieren Sie in der Auswahlliste den Port.
2. Wählen Sie im Menü **Port** den Befehl **Einstellungen**.
   Der Dialog **Porteinstellungen** erscheint.
3. Aktivieren Sie im Bereich **Meldungen** die Option.
4. Wählen Sie die Schaltfläche **OK** an.

↳ Die Einstellung wird gespeichert.

Benachrichtigung über die Dauer einer Verbindung

Sie erhalten eine Meldung, wenn eine Ihrer Verbindungen zu einem USB-Port und dem daran angeschlossenen USB-Gerät eine definierte Dauer überschreitet.

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.

1. Wählen Sie im Menü **Programm** den Befehl **Optionen**.
   Der Dialog **Optionen** erscheint.
2. Wählen Sie die Registerkarte **Programm** an.
3. Aktivieren Sie im Bereich **Programmmeldungen** die Option.
4. Definieren Sie die gewünschte Dauer.
5. Wählen Sie die Schaltfläche **OK** an.

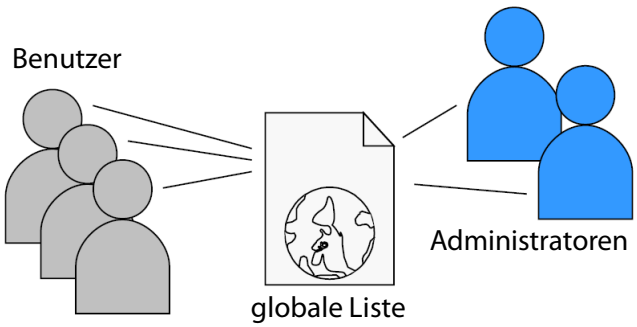
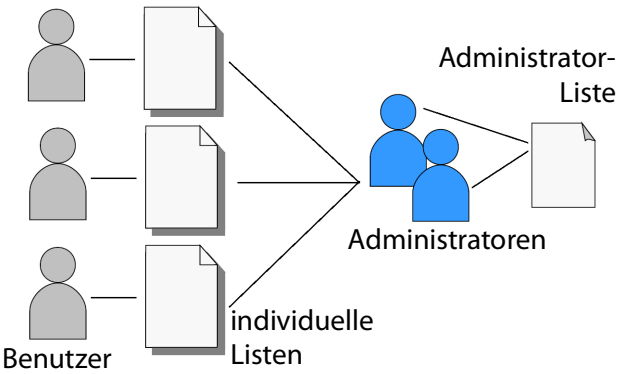
↳ Die Einstellung wird gespeichert.

5.7 Wie verwalte ich die Auswahlliste und damit die Benutzerzugriffsrechte auf USB-Geräte?

Als zentrales Element im SEH UTN Manager zeigt die Auswahlliste alle eingebundenen UTN-Server. Nur wenn sich ein UTN-Server auf der Liste befindet (⇨ 41), können die angeschlossenen USB-Geräte verwendet werden. Wenn Sie die Auswahlliste kontrollieren, können Sie also den Benutzerzugriff auf UTN-Server und die daran angeschlossenen USB-Geräte vorgeben.

Standardmäßig wird im SEH UTN Manager die sogenannte globale Auswahlliste von allen Client-Benutzern verwendet. Allerdings können Sie den Client-Benutzern auch eine benutzerindividuelle Auswahlliste zur Verfügung stellen. Diese Liste können die Benutzer selbst zusammenstellen. Alternativ schränken Sie als Client-Administrator die Rechte der Benutzer ein und geben die Liste vor, damit nur die von Ihnen festgelegten UTN-Server verwendet werden können.

Tabelle 12: Unterschiede globale und benutzerindividuelle Auswahlliste

Globale Auswahlliste	**Benutzerindividuelle Auswahlliste**
	
• Alle Benutzer eines Clients verwenden dieselbe Auswahlliste.	• Jeder Benutzer eines Clients hat seine individuelle Auswahlliste. Alle Administratoren haben dieselbe Auswahlliste.
• Der Benutzer kann auf alle in der Auswahlliste aufgeführten Geräte zugreifen. (Vorausgesetzt es sind keine Schutzmechanismen über das myUTN Control Center definiert.)	• Der Benutzer kann auf alle in der Auswahlliste aufgeführten Geräte zugreifen. (Vorausgesetzt es sind keine Schutzmechanismen über das myUTN Control Center definiert.)

• Speicherort der Liste: /etc	• Speicherort der Liste ('ini'-Datei):
	`$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
	(`$HOME` ist eine Umgebungsvariable von Linux für den Benutzerordner; mithilfe der Kommandozeile kann der Pfad für den aktuellen Benutzer folgendermaßen ermittelt werden:
	`echo $HOME`
	Beispiel Ubuntu 20.0.4 LTS:
	`echo $HOME` ergibt `/Usershome/Benutzername` +
	`.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
	Vollständiger Pfad zur ini-Datei:
	`/Usershome/Benutzername/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`)

- Die Auswahlliste kann durch Administratoren bearbeitet werden.
- Die Auswahlliste kann durch Administratoren oder durch Benutzer mit Schreibrechten für die ini-Datei bearbeitet werden.
  Benutzer ohne Schreibrechte für die ini-Datei können die Auswahlliste nicht bearbeiten und haben nur eingeschränkten Zugriff auf die Funktionen des SEH UTN Managers.

Welche Funktionen (Auswahllisten-Bearbeitung u.v.m.) im SEH UTN Manager genutzt werden können ist abhängig vom Auswahllisten-Typ (global/benutzerindividuell) und dem Benutzerkonto auf dem Client (Administrator/Benutzer; Benutzer mit/ohne Schreibrechte für die ini-Datei). Eine genaue Aufschlüsselung finden Sie in der 'SEH UTN Manager – Funktionsübersicht' ⇨ 🗎106.

- Globale Auswahlliste für alle Benutzer einrichten ⇨ 🗎50
- Benutzerindividuelle Auswahllisten vorgeben ⇨ 🗎50
- Schreibrechte auf die 'SEH UTN Manager.ini'-Datei einschränken ⇨ 🗎51

Globale Auswahlliste für alle Benutzer einrichten

Die globale Auswahlliste wird standardmäßig verwendet.

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.
✓ Sie sind als System-Administrator am Client angemeldet.

1. Starten Sie den SEH UTN Manager.
2. Stellen Sie die Auswahlliste zusammen ⇨ 🗎41.
3. Wählen Sie im Menü **Programm** den Befehl **Optionen**.
   Der Dialog **Optionen** erscheint.
4. Wählen Sie die Registerkarte **Auswahlliste** an.
5. Aktivieren Sie die Option **Globale Auswahlliste**.
6. Wählen Sie die Schaltfläche **OK** an.

↳ Die Einstellung wird gespeichert. Alle Benutzer eines Clients verwenden dieselbe Auswahlliste.

Benutzerindividuelle Auswahllisten vorgeben

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert ⇨ 🗎9.
✓ Sie sind als Administrator am System angemeldet.

1. Starten Sie den SEH UTN Manager.
2. Wählen Sie im Menü **Programm** den Befehl **Optionen**.
   Der Dialog **Optionen** erscheint.
3. Wählen Sie die Registerkarte **Auswahlliste** an.
4. Aktivieren Sie die Option **Benutzerindividuelle Auswahlliste**.
5. Wählen Sie die Schaltfläche **OK** an.

Optional: Die nachfolgenden Schritte geben eine von Ihnen definierte Auswahlliste vor.

6. Stellen Sie eine Auswahlliste mit den von Ihnen gewünschten Geräten zusammen ⇨ 🗎41.
7. Wählen Sie im Menü **Auswahlliste** den Befehl **Exportieren**.
   Der Dialog **Exportieren nach** erscheint.
8. Speichern Sie die Datei 'SEH UTN Manager.ini' in den Verzeichnissen der Benutzer ab:
   $HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini (⇨Tabelle 12 🗎49)

↳ Die Einstellung wird gespeichert. Jeder Benutzer verwendet eine individuelle (ggf. vordefinierte) Auswahlliste. Die Administratoren teilen sich eine Auswahlliste.

Schreibrechte auf die 'SEH UTN Manager.ini'-Datei einschränken

Wenn Sie benutzerindividuelle Auswahllisten verwenden, können Benutzer diese Liste selbst zusammenstellen.

Damit der nur die von Ihnen festgelegten UTN-Server verwendet werden, können Sie den Benutzern die Liste vorgeben. Dazu speichern Sie als Administrator eine vordefinierte Auswahlliste für den Benutzer ab (⇨ 50) und schränken die Schreibrechte der Benutzer auf die 'SEH UTN Manager.ini'-Datei ein. Durch den Schreibschutz sind für den Benutzer im SEH UTN Manager alle Funktionen deaktiviert, die die Auswahlliste betreffen.

Verwenden Sie die üblichen Methoden Ihres Betriebssystems, um ini-Dateien mit einem Schreibschutz zu belegen. Für mehr Informationen lesen Sie die Dokumentation Ihres Betriebssystems.

5.8 Wie nutze ich den SEH UTN Manager ohne grafische Oberfläche? (utnm)

Der SEH UTN Manager ist in zwei Varianten verfügbar ⇨ 🗎9. In der Minimal-Variante kann er ohne grafische Oberfläche verwendet werden. Dazu wird das Tool 'utnm' verwendet, mit dem UTN-Funktionen über die Konsoledes Betriebssystems genutzt werden:

- direkt, indem Befehle in einer speziellen Syntax eingegeben und ausgeführt werden
- über Skripte, die Kommandozeilenbefehle in einer speziellen Skriptsprache enthalten vom Kommandozeileninterpreter Schritt für Schritt automatisch abgearbeitet werden

Nutzen Sie Skripte, um häufig wiederkehrende Kommandofolgen, z.B. eine Portaktivierung, zu automatisieren.

Das Ausführen von Skripten kann auch automatisiert werden, z.B. via Loginskript.

Syntax

```
utnm -c "Befehlsstring" [-<Befehl>]
```

Die ausführbare Datei 'utnm' finden Sie unter `/usr/bin/`.

Befehle

Für die Befehle gilt:

- unterstrichene Elemente sind durch die genannten Werte zu ersetzen (z.B. `Server` = IP-Adresse oder Hostname eines UTN-Servers)
- Elemente in eckigen Klammern sind optional
- keine Unterscheidung von großer bzw. kleiner Schreibweise
- nur das ASCII-Format kann interpretiert werden

Befehl	Beschreibung

`-c "Befehlsstring"`
 	
oder
 	
`--command "Befehlsstring"`
	Führt einen Befehl aus. Der Befehl wird durch den Befehlsstring näher spezifiziert. Folgende Befehlsstrings gibt es:
	• `activate Server Portnummer`
	Aktiviert die Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät.
	• `activate Server Hersteller-ID (VID) Produkt-ID (PID)`
	Aktiviert die Verbindung zu einem USB-Port und dem ersten daran angeschlossenen USB-Gerät, das die definierten IDs hat und verfügbar ist, wenn mehrere identische USB-Geräte an den UTN-Server angeschlossen sind.
	• `deactivate Server Portnummer`
	Deaktiviert die Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät.
	• `set autoconnect = true|false Server Portnummer`
	De-/aktiviert Auto-Connect (⇨ 🗎46) für den USB-Port.
	• `set portkey='Portschlüssel' Server Portnummer`
	Speichert einen USB-Portschlüssel (⇨ 🗎64) lokal auf dem System. Damit wird der USB-Portschlüssel immer automatisch mitgesendet und muss nicht jedes Mal über den Befehl `-k USB-Portschlüssel` bzw. `--key USB-Portschlüssel` (siehe unten) spezifiziert werden.
	(Um den USB-Portschlüssel zu entfernen nutzen Sie den Befehlsstring `set portkey= Server Portnummer`)
	Wichtig:
	Der Befehl ermöglicht nur die dauerhafte Schlüsseleingabe, um das USB-Gerät verfügbar zu machen.
	Die Konfiguration des USB-Portschlüssels erfolgt über das myUTN Control Center ⇨ 🗎64.
	• `find`
	Sucht alle UTN-Server im Netzwerksegment und zeigt die gefundenen UTN-Server mit IP-Adresse, MAC-Adresse, Modell und Softwareversion.
	• `getlist Server`
	Zeigt eine Übersicht der USB-Geräte, die an den UTN-Server angeschlossenen sind (inkl. Portnummer, Hersteller-ID, Produkt-ID, Herstellername, Produktname, Geräteklasse und Status).
	• `state Server Portnummer`
	Zeigt den Status des am USB-Port angeschlossenen USB-Gerätes.

`-h`
oder
`--help`
	Zeigt die Hilfeseite an.

Befehl	Beschreibung

`-k USB-Portschlüssel`
oder
`--key USB-Portschlüssel`
	Spezifiziert einen USB-Portschlüssel ⇨ 🗎64.
	 
	Wichtig:
	Der Befehl ermöglicht nur die Schlüsseleingabe, um das USB-Gerät verfügbar zu machen.
	Über den Befehl `-c "Befehlsstring"` bzw. `--command "Befehlsstring"` können Sie den USB-Portschlüssel dauerhaft auf dem System speichern, sodass er automatisch mitgesendet wird (siehe oben).
	Die Konfiguration des USB-Portschlüssels erfolgt über das myUTN Control Center ⇨ 🗎64.

`-mr`
oder
`--machine readable`
	Trennt die Ausgabe des Befehlsstrings `getlist` durch Tabulatoren und die von `find` durch Kommas.

`-nw`
oder
`--no-warnings`
	Unterdrückt Warnmeldungen.

`-o`
oder
`--output`
	Zeigt die Ausgabe in der Kommandozeile an.

`-p Portnummer`
oder
`--port Portnummer`
	Verwendet einen alternativen UTN-Port.
	Verwenden Sie diesen Befehl, falls die UTN-Portnummer geändert wurde (⇨ 🗎38).

`-q`
oder
`--quiet`
	Unterdrückt die Ausgabe.

`-sp Portnummer`
oder
`--ssl-port Portnummer`
	Verwendet einen alternativen UTN-Port mit SSL-/TLS-Verschlüsselung.
	Verwenden Sie diesen Befehl, falls die UTN-SSL-Portnummer geändert wurde (⇨ 🗎38).

`-t Sekunden`
oder
`timeout Sekunden`
	Spezifiziert ein Timeout für die Befehlsstrings `activate` und `deactivate`.

`-v`
oder
`--version`
	Zeigt die Versionsnummer von utnm an.

Rückgabe

Nach der Ausführung eines Befehls wird zurückgegeben, ob der Prozess korrekt abgelaufen ist oder ein Fehler auftrat. Die Rückgabeinformation besteht aus einem Status und einem Rückgabewert (Return Code). Wird die Ausgabe unterdrückt ('`--quiet`' ⇨ 🗎54), wird nur der Rückgabewert zurückgegeben.

Anhand der Rückgabe kann z.B. in einem Skript entschieden werden, wie der Prozess weiterläuft.

Rückgabewert	Beschreibung
0	Der Befehl wurde erfolgreich ausgeführt.
20	Aktivieren fehlgeschlagen.
21	Deaktivieren fehlgeschlagen.
23	Ist bereits aktiviert.
24	Wurde bereits deaktiviert oder es ist kein USB-Gerät verfügbar.
25	Aktivieren fehlgeschlagen: Der USB-Port und das daran angeschlossene USB-Gerät sind mit einem anderen Benutzer verbunden.
26	Nicht gefunden: Am USB-Port ist kein USB-Gerät angeschlossen oder der USB-Portschlüssel (⇨ 🗎64) fehlt bzw. ist falsch.
29	Nicht gefunden: Am USB-Port ist kein USB-Gerät mit der definierten VID und PID angeschlossen.
30	Isochrone USB-Geräte wird nicht unterstützt.
31	UTN-Treiber-Fehler. Kontaktieren Sie den Support von SEH Computertechnik GmbH ⇨ 🗎4.
40	Keine Netzwerkverbindung zum UTN-Server vorhanden.
41	Verschlüsselte Verbindung (SSL/TLS) zum UTN-Server kann nicht hergestellt werden.
42	Verbindung zum UTN-Dienst kann nicht hergestellt werden.
43	Die DNS-Auflösung ist fehlgeschlagen.
44	Keine ausreichenden Rechte (administrative Rechte erforderlich).
47	Die Funktion wird nicht unterstützt.
200	Fehler (mit Fehlercode).

utnm über Konsole verwenden

✓ Der SEH UTN Manager ist auf dem Client installiert ⇨ 🗎9.
✓ IP-Adresse oder Hostname eines UTN-Servers ist bekannt.

1. Öffnen Sie eine **Konsole**.
2. Geben Sie die Befehlsfolge ein; siehe 'Syntax' ⇨ 🗎52 und 'Befehle' ⇨ 🗎52.
3. Bestätigen Sie die Eingabe.

↳ Die Befehlsfolge wird ausgeführt.

Beispiel: Aktivierung eines USB-Gerätes an Port 3 des UTN-Servers mit der IP-Adresse 10.168.1.167

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

Skript mit utnm erstellen

✓ Der SEH UTN Manager ist auf dem Client installiert ⇨ 🗎9.
✓ IP-Adresse oder Hostname eines UTN-Servers ist bekannt.
✓ Sie kennen sich mit dem Erstellen und Verwenden von Skripten für Ihr Betriebssystem aus. Lesen Sie ggf. die Dokumentation Ihres Betriebssystems

1. Öffnen Sie einen Texteditor.
2. Geben Sie die Befehlsfolge ein; siehe 'Syntax' ⇨ 🗎52, 'Befehle' ⇨ 🗎52 und 'Rückgabe' ⇨ 🗎54.
3. Speichern Sie die Datei als ausführbares Skript.

↳ Das Skript ist gespeichert und kann verwendet werden.

6 Sicherheit

Am UTN-Server können verschiedene Schutzmechanismen konfiguriert werden. Mit den Maßnahmen sichern Sie den UTN-Server selbst und die angeschlossenen USB-Geräte. Außerdem können Sie den UTN-Server in die Sicherheitsmaßnahmen Ihres Netzwerkes integrieren.

- Wie verschlüssele ich die USB-Verbindung? ⇨ 🗎57
- Wie verschlüssele ich die Verbindung zum myUTN Control Center? ⇨ 🗎59
- Wie definiere ich die Verschlüsselungsstärke für SSL-/TLS-Verbindungen? ⇨ 🗎60
- Wie schütze ich den Zugriff auf das myUTN Control Center? (Benutzerkonten) ⇨ 🗎62
- Wie sperre ich Ports am UTN-Server? (TCP-Portzugriffskontrolle) ⇨ 🗎63
- Wie kontrolliere ich den Zugriff auf USB-Geräte? ⇨ 🗎64
- Wie blockiere ich USB-Gerätetypen? ⇨ 🗎66
- Wie nutze ich Zertifikate? ⇨ 🗎67
- Wie konfiguriere ich die Authentifizierung in Netzwerken (IEEE 802.1X)? ⇨ 🗎72

Wichtig:
Schützen Sie den Zugang zu dem myUTN Control Center mithilfe von Benutzerkonten, damit sicherheitsrelevante Einstellungen nicht durch Unbefugte verändert werden können.

Auch SNMP und VLAN sind Sicherheitskonzepte, die Sie verwenden können:

- *'Wie konfiguriere ich SNMP?'* ⇨ 🗎25
- *'Wie setze ich den UTN-Server in VLAN-Umgebungen ein?'* ⇨ 🗎31

6.1 Wie verschlüssele ich die USB-Verbindung?

Um die USB-Verbindungen zu sichern, verschlüsseln Sie die Datenübertragung zwischen den Clients und den USB-Geräten die an den UTN-Server angeschlossen sind. Die Verschlüsselung muss für jede Verbindung, d.h. jeden USB-Port, einzeln aktiviert werden.

Wichtig:

Nur Nutzdaten werden verschlüsselt. Steuer- und Protokolldaten werden unverschlüsselt übertragen.

Zum Verschlüsseln werden die Protokolle SSL (Secure Sockets Layer) und dessen Nachfolger TLS (Transport Layer Security) verwendet. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨ 60.

WARNUNG

Der SEH UTN Manager unterstützt die Verschlüsselungsstufe **Niedrig** nicht. Wenn Sie **Niedrig** in Kombination mit einer verschlüsselten USB-Verbindung einstellen, kann keine Verbindung aufgebaut werden.

Verwenden Sie eine möglichst hohe Verschlüsselungsstufe.

Bei einer verschlüsselten Verbindung kommunizieren der Client und der UTN-Server über den UTN-SSL-Port. Standardmäßig wird der Port 9443 verwendet. Wird der Port in Ihrem Netzwerk bereits genutzt, z.B. von einer anderen Anwendung, können Sie die Portnummer ändern ⇨ 38.

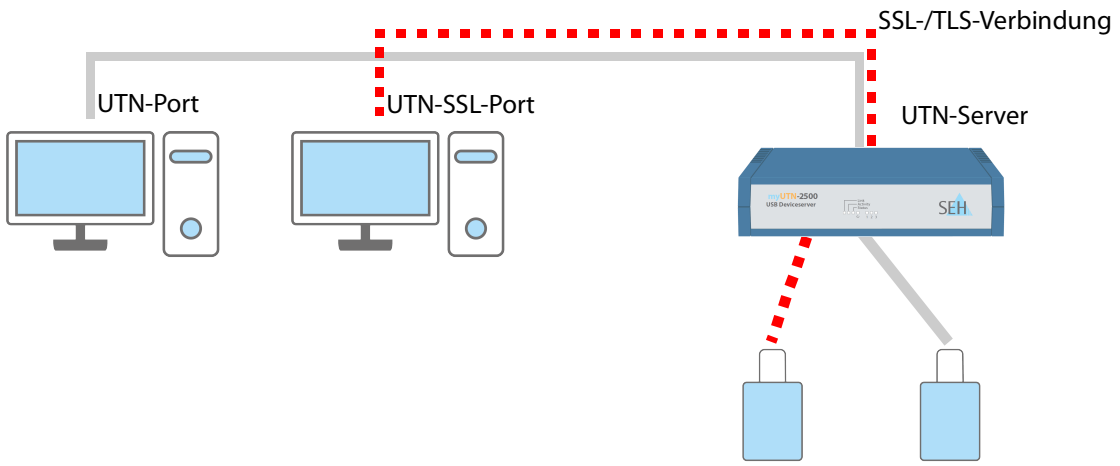


Abbildung 7: UTN-Server – SSL-/TLS-Verbindung im Netzwerk

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Verschlüsselung** an.
3. Aktivieren Sie die Verschlüsselung an dem USB-Port.
4. Bestätigen Sie mit **Speichern**.

↳ Die Daten zwischen den Clients und dem USB-Gerät werden verschlüsselt übermittelt.

*Eine verschlüsselte Verbindung wird clientseitig im SEH UTN Manager unter **Eigenschaften** angezeigt.*

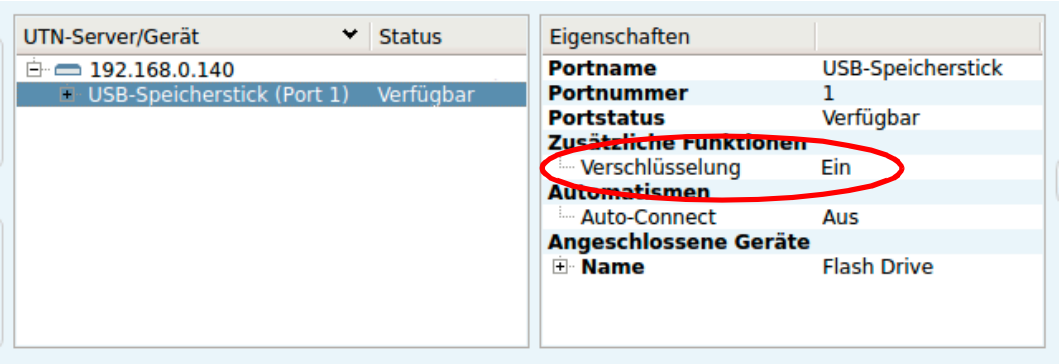


Abbildung 8:SEH UTN Manager – Verschlüsselung

6.2 Wie verschlüssele ich die Verbindung zum myUTN Control Center?

Sie können die Verbindung zum myUTN Control Center schützen, indem Sie sie mit den Protokollen SSL (Secure Sockets Layer) und dessen Nachfolger TLS (Transport Layer Security) verschlüsseln.

- HTTP: unverschlüsselte Verbindung
- HTTPS: verschlüsselte Verbindung
  Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨ 🗎60. Beim Aufbau der verschlüsselten Verbindung fragt der Client via Browser nach einem Zertifikat (⇨ 🗎67). Dieses Zertifikat muss vom Browser akzeptiert werden; lesen Sie hierzu die Dokumentation Ihrer Browsersoftware.

WARNUNG

Aktuelle Browser unterstützen niedrige Sicherheitseinstellungen nicht. Mit ihnen kann keine Verbindung aufgebaut werden.

Verwenden Sie nicht die folgende Kombination: Verschlüsselungsprotokoll **HTTPS** und Verschlüsselungsstufe **Niedrig**.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Gerätezugriff** an.
3. Aktivieren Sie im Bereich **Verbindung** die Option **HTTP/HTTPS** bzw. **Nur HTTPS**.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellung wird gespeichert.

6.3 Wie definiere ich die Verschlüsselungsstärke für SSL-/TLS-Verbindungen?

Einige Verbindungen zum und vom UTN-Server können mit den Protokollen SSL (Secure Sockets Layer) und dessen Nachfolger TLS (Transport Layer Security) verschlüsselt werden:

- E-Mail: POP3 (⇨ 🗎28)
- E-Mail: SMTP (⇨ 🗎28)
- Webzugang zum myUTN Control Center: HTTPS (⇨ 🗎59)
- Datenübertragung zwischen den Clients und dem UTN-Server (bzw. den angeschlossenen USB-Geräten): USB-Verbindung (⇨ 🗎60)

Die Stärke der Verschlüsselung und damit die Sicherheit der Verbindung wird über das Verschlüsselungsprotokoll und die Verschlüsselungsstufe definiert. Beides können Sie auswählen.

Jede Verschlüsselungsstufe ist eine Sammlung sog. Cipher Suites. Eine Cipher Suite ist wiederum eine standardisierte Folge aus vier kryptografischen Algorithmen, die zum Aufbau einer sicheren Verbindung verwendet werden. Gemäß ihrer Verschlüsselungsstärke werden sie zu einer Verschlüsselungsstufe zusammengefasst. Welche Cipher Suites vom UTN-Server unterstützt werden, also Teil einer Verschlüsselungsstufe sind, hängt vom ausgewählten Verschlüsselungsprotokoll ab. Sie können zwischen folgen Verschlüsselungsstufen wählen:

- Beliebig: Die Verschlüsselung wird zwischen beiden Parteien automatisch ausgehandelt. Dabei wird immer die stärkste Verschlüsselung gewählt, die beide Parteien unterstützen.
- Niedrig: Es werden nur Cipher Suites mit einer schwachen Verschlüsselung verwendet. (Schnelle Übertragung)
- Mittel
- Hoch: Es werden nur Cipher Suites mit einer starken Verschlüsselung verwendet. (Langsame Übertragung)

Beim Aufbau einer sicheren Verbindung wird das zu verwendende Verschlüsselungsprotokoll sowie eine Liste von unterstützten Cipher Suites an den Kommunikationspartner gesendet. Es wird eine Cipher Suite ausgehandelt, die im Weiteren verwendet wird.

Standardmäßig handelt es sich um die stärkste von beiden Parteien unterstützte Cipher Suite.

WARNUNG

Unterstützt der Kommunikationspartner des UTN-Servers (z.B. der Browser) das gewählte Protokoll nicht und/oder gibt es keine von beiden Seiten unterstützte Cipher Suite, wird keine SSL-/TLS-Verbindung aufgebaut.

Bei Problemen wählen Sie andere Einstellungen oder setzen die UTN-Server-Parameter zurück ⇨ 🗎79.

*Wenn Sie möchten, dass der UTN-Server und sein Kommunikationspartner die Einstellungen automatisch aushandeln, wählen Sie für beide Einstellungen die Option **Beliebig**. Mit diesen Einstellungen sind die Chancen für einen erfolgreichen Verbindungsaufbau am größten.*

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **SSL-Verbindungen** an.

3. Wählen Sie im Bereich **Verschlüsselungsprotokoll** das gewünschte Protokoll.

WARNUNG

Aktuelle Browser unterstützen **SSL** nicht. Wenn Sie einen aktuellen Browser verwenden und für den Webzugang zum myUTN Control Center (⇨ 🗎59) **SSL** in Kombination mit **Nur HTTPS** einstellen, kann keine Verbindung aufgebaut werden.

Verwenden Sie TLS (und nicht SSL).

Wichtig:

Welche Protokolle vom UTN-Server unterstützt und anbietet, hängt von der Produkt-Hardware und der installierten Firmware/Software ab.

4. Wählen Sie im Bereich **Verschlüsselungsstufe** die gewünschte Verschlüsselungsstufe.

WARNUNG

Aktuelle Browser unterstützen Cipher Suites der Stufe **Niedrig** nicht. Wenn Sie einen aktuellen Browser verwenden und für den Webzugang zum myUTN Control Center (⇨ 🗎59) **Niedrig** in Kombination mit **Nur HTTPS** einstellen, kann keine Verbindung aufgebaut werden.

Verwenden Sie eine möglichst hohe Verschlüsselungsstufe.

WARNUNG

Der SEH UTN Manager unterstützt die Verschlüsselungsstufe **Niedrig** nicht. Wenn Sie **Niedrig** in Kombination mit einer verschlüsselten USB-Verbindung (⇨ 🗎57) einstellen, kann keine Verbindung aufgebaut werden.

Verwenden Sie eine möglichst hohe Verschlüsselungsstufe.

5. Bestätigen Sie mit **Speichern**.

↳ Die Einstellung wird gespeichert.

*Detaillierte Informationen zu den einzelnen SSL-/TLS-Verbindungen (z.B. unterstützte Cipher Suites) entnehmen Sie der Detailseite unter **Status der SSL-Verbindung – Details**.*

6.4 Wie schütze ich den Zugriff auf das myUTN Control Center? (Benutzerkonten)

Standardmäßig kann jeder auf das myUTN Control Center zugreifen sofern er den UTN-Server im Netzwerk findet. Um den UTN-Server vor ungewollten Änderungen seiner Konfiguration zu schützen, können Sie zwei Benutzerkonten einrichten:

- Administrator: Vollständiger Zugriff auf das myUTN Control Center. Der Benutzer kann alle Seiten einsehen und Einstellungen vornehmen.
- Lesezugriff-Benutzer: Stark eingeschränkter Zugang zum myUTN Control Center. Der Benutzer kann nur die Seite 'START' ansehen.

Haben Sie die Benutzerkonten eingerichtet, erscheint beim Aufrufen des myUTN Control Centers ein Anmeldefenster. Sie können zwischen zwei Login-Masken wählen:

- Liste der Benutzer: Benutzernamen werden angezeigt. Nur das Passwort muss eingegeben werden.
- Dialog Name und Passwort: Neutrale Anmeldemaske, in die Benutzername und Passwort eingegeben werden. (stärkerer Schutz)

Über ein Benutzerkonto sind Mehrfach-Logins möglich, d.h. das Konto kann von einem einzelnen Benutzer oder einer Gruppe von Benutzern verwendet werden. Maximal 16 Benutzer können zeitgleich angemeldet sein.

Wichtig:

Die Benutzerkonten für den Zugang zum myUTN Control Center werden auch für SNMP verwendet ⇨ 25. Berücksichtigen Sie dies bei Ihren Einstellungen.

Als zusätzliche Sicherheitsmaßnahme können Sie ein Sitzungs-Timeout nutzen. Wenn innerhalb des definierten Timeouts keine Aktivität stattfindet, wird der Benutzer automatisch ausgeloggt.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Gerätezugriff** an.
3. Definieren Sie die zwei Benutzerkonten. Geben Sie hierzu im Bereich **Benutzerkonten** jeweils **Benutzername** und **Passwort** ein.

Um sicherzustellen, dass Sie sich beim Passwort nicht vertippen, können Sie den Klartext einblenden.

4. Aktivieren Sie die Option **Control Center-Zugriff einschränken**.
5. Wählen Sie für das Anmeldefenster die Art der Login-Maske: **Liste der Benutzer** oder **Name und Passwort**.
6. Aktivieren Sie bei Bedarf die Option **Sitzungs-Timeout** und geben Sie im Feld **Sitzungsdauer** den Zeitraum in Minuten ein, nach dem ein inaktiver Benutzer automatisch ausgeloggt werden soll.
7. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

6.5 Wie sperre ich Ports am UTN-Server? (TCP-Portzugriffskontrolle)

Sie können den Zugriff auf den UTN-Server einschränken, indem Sie mit der 'TCP-Portzugriffskontrolle' Ports sperren. Wenn ein Port gesperrt ist, können darüber laufende Protokolle bzw. Dienste keine Verbindung zum UTN-Server aufbauen. Dadurch werden Angreifern weniger Möglichkeiten geboten.

Über die Sicherheitsstufe wählen Sie, welche Porttypen gesperrt werden:

- UTN-Zugriff (sperrt UTN-Ports)
- TCP-Zugriff (sperrt TCP-Ports: HTTP/HTTPS/UTN)
- Alle Ports (sperrt IP-Ports)

Damit die von Ihnen gewünschten Netzwerkelemente, z.B. Clients oder DNS-Server, eine Verbindung zum UTN-Server herstellen können, müssen Sie diese als Ausnahme definieren.

WARNUNG

Der 'Testmodus' ist standardmäßig aktiv, damit Sie Ihre Einstellungen prüfen können ohne sich auszusperren. Ihre Einstellungen bleiben bis zu einem Neustart des UTN-Servers aktiv, danach ist der Zugriffsschutz nicht mehr wirksam.

Deaktivieren Sie den Testmodus nachdem Sie Ihre Einstellungen erfolgreich getestet haben, damit der Zugriffsschutz dauerhaft aktiv bleibt.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **TCP-Portzugriff** an.
3. Aktivieren Sie die Option **Portzugriff kontrollieren**.
4. Wählen Sie im Bereich **Sicherheitsstufe** den gewünschten Schutz.
5. Definieren Sie im Bereich **Ausnahmen** die Netzwerkelemente, die Zugriff auf den UTN-Server haben sollen. Geben Sie hierzu die IP-Adressen oder MAC-Adressen (Hardwareadressen) ein und aktivieren Sie die Optionen.

Wichtig:

- MAC-Adressen werden nicht über Router weitergeleitet.
- Mit dem Einsatz von Wildcards (*) können Subnetzwerke definiert werden.

6. Stellen Sie sicher, dass der **Testmodus** aktiviert ist.
7. Bestätigen Sie mit **Speichern & Neustart**.
   Die Einstellungen werden gespeichert.
   Die Portzugriffskontrolle ist bis zum Geräte-Neustart aktiv.
8. Überprüfen Sie den Portzugriff und ob das myUTN Control Center erreicht werden kann.

Wichtig:

Kann das myUTN Control Center nicht mehr erreicht werden, starten Sie den UTN-Server neu ⇨ 🗎76.

9. Deaktivieren Sie den **Testmodus**.
10. Bestätigen Sie mit **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

6.6 Wie kontrolliere ich den Zugriff auf USB-Geräte?

Sie können den Zugriff auf USB-Ports und die Nutzung der daran angeschlossenen USB-Geräte einschränken:

- USB-Portschlüsselkontrolle: Für den USB-Port wird ein Schlüssel definiert. Im SEH UTN Manager werden weder der USB-Port noch das daran angeschlossene USB-Gerät werden angezeigt, d.h. das USB-Gerät kann nicht verwendet werden. Erst wenn der Schlüssel für den USB-Port im SEH UTN Manager eingegeben wird, erscheint der USB-Port und das daran angeschlossene USB-Gerät.
- USB-Port-Gerätezuordnung: Dem USB-Port wird ein bestimmtes USB-Gerät fest zugewiesen. Dazu werden USB-Port und USB-Gerät über die Hersteller-ID (engl. Vendor ID – VID) und Produkt-ID (engl. Product ID – PID) des USB-Gerätes miteinander verknüpft. Über die spezifische Kombination von VID und PID verfügt nur ein bestimmtes USB-Gerätemodell, d.h. am USB-Port können nur USB-Geräte eines spezifischen Modells betrieben werden. So stellen Sie sicher, dass (sicherheitsrelevante) Einstellungen durch Umstecken der USB-Geräte nicht umgangen werden.

Schalten Sie ungenutzte Ports zur Sicherheit ab ⇨ 🗎37.

- USB-Portschlüssel konfigurieren ⇨ 🗎64
- USB-Portschlüssel eingeben (USB-Gerät freischalten) ⇨ 🗎64
- USB-Port-Gerätezuordnung einrichten ⇨ 🗎65

USB-Portschlüssel konfigurieren

Der Schlüssel für den USB-Port wird im myUTN Control Center definiert.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **USB-Portzugriff** an.
3. Wählen Sie am entsprechenden USB-Port aus der Liste **Methode** den Eintrag **Portschlüsselkontrolle**.
4. Wählen Sie die Schaltfläche **Schlüssel generieren** an oder geben Sie im Feld **Schlüssel** einen freidefinierbaren Schlüssel ein (max. 64 ASCII-Zeichen).
5. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert. Der Zugriff auf das USB-Gerät ist geschützt.

*Um den Mechanismus zu deaktivieren, wählen aus der Liste **Methode** den Eintrag **---**.*

USB-Portschlüssel eingeben (USB-Gerät freischalten)

Um den Zugriff auf ein durch die USB-Portschlüsselkontrolle geschütztes USB-Gerät freizuschalten, muss auf dem Client im SEH UTN Manager beim entsprechenden USB-Port der zugehörige Schlüssel eingegeben werden.

1. Starten Sie den SEH UTN Manager.
2. Markieren Sie den UTN-Server in der Auswahlliste.
3. Wählen Sie im Menü **UTN-Server** den Befehl **USB-Portschlüssel eingeben**.
   Der Dialog **USB-Portschlüssel eingeben** erscheint.
4. Geben Sie für den entsprechenden USB-Port den Schlüssel ein.
5. Wählen Sie die Schaltfläche **OK** an.

↳ Der Zugriff wird freigegeben. Der USB-Port und das daran angeschlossene USB-Gerät werden in der Auswahlliste angezeigt und können verwendet werden.

USB-Port-Gerätezuordnung einrichten

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **USB-Portzugriff** an.
3. Wählen Sie am entsprechenden USB-Port aus der Liste **Methode** den Eintrag **Gerätezuordnung**.
4. Wählen Sie die Schaltfläche **Gerät neu zuordnen** an.
   Im Feld **USB-Gerät** werden VID und PID des USB-Gerätes angezeigt.
5. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert. Am USB-Port kann ausschließlich das zugewiesene USB-Gerätemodell verwendet werden.

*Um den Mechanismus zu deaktivieren, wählen aus der Liste **Methode** den Eintrag **---**.*

6.7 Wie blockiere ich USB-Gerätetypen?

USB-Geräte werden gemäß ihrer Funktion in Klassen gruppiert. Beispielsweise werden Eingabegeräte, wie z.B. Tastaturen, in der Gruppe 'Human Interface Device' (HID) zusammengefasst.

USB-Geräte können sich als USB-Geräte der Klasse HID ausgeben, werden in Wahrheit aber zum Missbrauch verwendet ('BadUSB'-Schwachstelle).

Um den UTN-Server davor zu schützen, können Sie USB-Geräte der HID-Klasse blockieren.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Gerätezugriff** an.
3. De-/Aktivieren Sie im Bereich **USB-Geräte** die Option **Eingabegeräte deaktivieren (HID-Klasse)**.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellung wird gespeichert.

6.8 Wie nutze ich Zertifikate?

Der UTN-Server verfügt über eine eigene Zertifikatsverwaltung. Digitale Zertifikate sind Datensätze, welche die Identität einer Person, eines Objektes oder einer Organisation bestätigen. In TCP/IP-Netzwerken werden sie verwendet, um Daten zu verschlüsseln und Kommunikationspartner zu authentifizieren.

Bei folgenden Mechanismen benötigt der UTN-Server ein Zertifikat:

- Teilnahme an den Authentifizierungsmethoden EAP-TLS, EAP-TTLS und PEAP ⇨ 🗎72
- E-Mail-Kommunikation schützen (POP3/SMTP via SSL/TLS) ⇨ 🗎28
- USB-Verbindung zwischen den Clients und angeschlossenen USB-Geräten verschlüsseln ⇨ 🗎57
- Verbindung zum myUTN Control Center (mit HTTPS) schützen ⇨ 🗎59

Im UTN-Server können folgenden Zertifikate verwendet werden:

- 1 selbstsigniertes Zertifikat:
  Auf dem UTN-Server generiertes Zertifikat, das vom UTN-Server selbst unterschrieben wird. Mit dem Zertifikat bestätigt der UTN-Server seine Identität.
- 1 Client-Zertifikat, d.h. 1 angefordertes Zertifikat oder 1 PKCS#12-Zertifikat:
  Das Client-Zertifikat bestätigt die Identität des UTN-Servers mithilfe einer weiteren vertrauenswürdigen Instanz, der Zertifizierungsstelle (engl. certification authority, kurz CA).
  - Angefordertes Zertifikat: Zunächst wird auf dem UTN-Server eine Zertifikatsanforderung erstellt, die an eine Zertifizierungsstelle geschickt wird. Anschließend erstellt die Zertifizierungsstelle auf Basis der Anforderung ein Zertifikat für den UTN-Server und unterschreibt es.
  - PKCS#12-Zertifikat: Austauschformat für Zertifikate. Sie erstellen bei einer Zertifizierungsstelle ein Zertifikat für den UTN-Server, das passwortgeschützt im PKCS#12-Format gespeichert wird. Anschließend transportieren Sie die PKCS#12-Datei zum UTN-Server und installieren sie (und damit das enthaltene Zertifikat).
- 1 S/MIME-Zertifikat:
  Mit dem S/MIME-Zertifikat signiert und verschlüsselt der UTN-Server E-Mails, die er versendet. Den zugehörigen privaten Schlüssel (PKCS#12-Format) müssen Sie im E-Mail-Programm (Mozilla Thunderbird usw.) als eigenes Zertifikat installieren, um die E-Mails verifizieren und ggf. entschlüsseln zu können.

- 1–32 CA-Zertifikate, auch als Wurzel-CA-Zertifikate bekannt:
  Zertifikate, die für ein Zertifizierungsstelle ausgestellt wurden und deren Identität bestätigen. Mit ihnen werden Zertifikate überprüft, die von der jeweiligen Zertifizierungsstelle ausgegeben wurden. Im Falle des UTN-Servers handelt es sich um die Zertifikate der Kommunikationspartner, deren Identität somit geprüft wird (Vertrauenskette). Mit diesem Mechanismus werden mehrstufige Public Key Infrastrukturen (PKI) unterstützt.

Wichtig:

Bei Auslieferung ist ein Defaultzertifikat im UTN-Server gespeichert, das von SEH Computertechnik GmbH für das jeweilige Gerät ausgestellt wurde.

- Zertifikat ansehen ⇨ 🗎68
- Selbstsigniertes Zertifikat erstellen ⇨ 🗎68
- Zertifikat anfordern und installieren (angefordertes Zertifikat) ⇨ 🗎69
- PKCS#12-Zertifikat installieren ⇨ 🗎70
- S/MIME-Zertifikat installieren ⇨ 🗎70
- CA-Zertifikat installieren ⇨ 🗎70
- Zertifikat löschen ⇨ 🗎71

Zertifikat ansehen

✓ Auf dem UTN-Server ist ein Zertifikat vorhanden.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Zertifikate** an.
3. Wählen Sie das Zertifikat über das Symbol aus.

↳ Das Zertifikat wird angezeigt.

Selbstsigniertes Zertifikat erstellen

Wichtig:
Es kann nur ein selbstsigniertes Zertifikat auf dem UTN-Server installiert sein.
Um ein neues Zertifikat zu erstellen, löschen Sie zunächst das vorhandene ⇨ 71.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Zertifikate** an.
3. Wählen Sie die Schaltfläche **Selbstsigniertes Zertifikat** an.
4. Geben Sie die entsprechenden Parameter ein; ⇨Tabelle 13 68.
5. Wählen Sie die Schaltfläche **Erstellen/Installieren** an.

↳ Das Zertifikat wird erstellt und installiert. Dieser Vorgang kann einige Minuten dauern.

Tabelle 13: Parameter für die Erstellung von Zertifikaten

Parameter	Beschreibung
Allgemeiner Name	Freidefinierbarer Name des Zertifikats. (Maximal 64 Zeichen) *Verwenden Sie die IP-Adresse oder den Hostnamen des UTN-Servers, damit Sie Gerät und Zertifikat einander eindeutige zuordnen können.*
E-Mail-Adresse	E-Mail-Adresse des Ansprechpartners, der für den UTN-Server zuständig ist. (Maximal 40 Zeichen; optionale Eingabe)
Organisation	Namen der Firma, die den UTN-Server einsetzt. (Maximal 64 Zeichen)
Unternehmensbereich	Name der Abteilung oder Untergruppe der Firma. (Maximal 64 Zeichen; optionale Eingabe)
Ort	Ort, an dem die Firma ansässig ist. (Maximal 64 Zeichen)
Bundesland	Bundeslandes, in dem die Firma ansässig ist. (Maximal 64 Zeichen)
Domain-Komponente	Ermöglicht das Eintragen weiterer Attribute. (Optionale Eingabe)
SAN (multi-domain)	Ermöglicht das Eintragen von Subject Alternative Names (SAN). Dient der Angabe zusätzlicher Hostnamen (z.B. Domänen). (Optionale Eingabe, maximal 255 Zeichen)
Land	Land, in dem die Firma ansässig ist. Geben Sie das zweistellige Länderkürzel gemäß ISO 3166 ein. Beispiele: DE = Deutschland, GB = Großbritannien, US = USA

Parameter	Beschreibung
Ausgestellt am	Datum, ab dem das Zertifikat gültig ist.
Endet am	Datum, an dem das Zertifikat ungültig wird.
RSA-Schlüssellänge	Definiert die Länge des verwendeten RSA-Schlüssels: • 512 Bit (schnelle Ver- und Entschlüsselung) • 768 Bit • 1024 Bit (standardmäßige Ver- und Entschlüsselung) • 2048 Bit • 4096 Bit (langsame Ver- und Entschlüsselung)

Zertifikat anfordern und installieren (angefordertes Zertifikat)

Im UTN-Server kann ein Zertifikat verwendet werden, das von einer Zertifizierungsstelle für den UTN-Server ausgestellt ist.

Dafür erstellen Sie zunächst eine Zertifikatsanforderung und senden diese anschließend an die Zertifizierungsstelle. Die Zertifizierungsstelle erstellt dann anhand der Anforderung ein Zertifikat speziell für den UTN-Server. Dieses Zertifikat installieren Sie auf dem UTN-Server.

Wichtig:

Sie können nur ein angefordertes Zertifikat installieren, das anhand der Zertifikatsanforderung auf dem UTN-Server erstellt wurde.

Passen die beiden Dateien nicht zueinander, müssen Sie ein neues Zertifikat für die aktuell vorliegende Zertifikatsanforderung anfordern. Möchten Sie den gesamt Prozess von vorne beginnen, müssen Sie zunächst die Zertifikatsanforderung löschen ⇨ 🗎71.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Zertifikate** an.
3. Wählen Sie die Schaltfläche **Zertifikatsanforderung** an.
4. Geben Sie die benötigten Parameter ein; ⇨Tabelle 13 🗎68.
5. Wählen Sie die Schaltfläche **Anforderung erstellen** an.
   Die Zertifikatsanforderung wird erstellt. Dieser Vorgang kann einige Minuten dauern.
6. Wählen Sie die Schaltfläche **Upload** an und speichern Sie die Anforderung in einer Textdatei.
7. Wählen Sie die Schaltfläche **OK** an.
8. Senden Sie die Textdatei als Zertifikatsanforderung an eine Zertifizierungsstelle.
   Die Zertifizierungsstelle erstellt das Zertifikat und übergibt es an Sie.

Wichtig:

Das angeforderte Zertifikat muss im 'Base64'-Format vorliegen.

9. Wählen Sie die Schaltfläche **Angefordertes Zertifikat** an.
10. Geben Sie im Feld **Zertifikatsdatei** das erhaltene Zertifikat an.
11. Wählen Sie die Schaltfläche **Installieren** an.

↳ Das angeforderte Zertifikat wird auf dem UTN-Server gespeichert.

PKCS#12-Zertifikat installieren

Wichtig:
Ist bereits ein PKCS#12-Zertifikat auf dem UTN-Server installiert, muss dieses zunächst gelöscht werden ⇨ 🗎71.

✓ Das Zertifikat liegt im 'Base64'-Format vor.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Zertifikate** an.
3. Wählen Sie die Schaltfläche **PKCS#12-Zertifikat** an.
4. Geben Sie im Feld **Zertifikatsdatei** das PKCS#12-Zertifikat an.
5. Geben Sie das Passwort ein.
6. Wählen Sie die Schaltfläche **Installieren** an.

↳ Das PKCS#12-Zertifikat wird auf dem UTN-Server gespeichert.

S/MIME-Zertifikat installieren

Wichtig:
Ist bereits ein S/MIME-Zertifikat auf dem UTN-Server installiert, muss dieses zunächst gelöscht werden ⇨ 🗎71.

✓ Das S/MIME-Zertifikat liegt im 'pem'-Format vor.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Zertifikate** an.
3. Wählen Sie die Schaltfläche **S/MIME-Zertifikat** an.
4. Geben Sie im Feld **Zertifikatsdatei** das S/MIME-Zertifikat an.
5. Wählen Sie die Schaltfläche **Installieren** an.

↳ Das S/MIME-Zertifikat wird auf dem UTN-Server gespeichert.

CA-Zertifikat installieren

✓ Das Zertifikat liegt im 'Base64'-Format vor.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Zertifikate** an.
3. Wählen Sie die Schaltfläche **CA-Zertifikat** an.
4. Geben Sie im Feld **Zertifikatsdatei** das CA-Zertifikat an.
5. Wählen Sie die Schaltfläche **Installieren** an.

↳ Das CA-Zertifikat wird auf dem UTN-Server gespeichert.

Zertifikat löschen

WARNUNG

Um eine verschlüsselte (HTTPS ⇨ 🗎59) Verbindung zum myUTN Control Center aufzubauen, wird zwingend ein Zertifikat (selbstsigniert/CA/PKCS#12) benötigt. Falls Sie das zugehörige Zertifikat löschen, kann das myUTN Control Center nicht mehr erreicht werden.

Starten Sie in diesem Fall den UTN-Server neu ⇨ 🗎76. Dabei generiert der UTN-Server ein neues selbstsigniertes Zertifikat, wodurch wieder eine gesicherte Verbindung aufgebaut werden kann.

✓ Auf dem UTN-Server ist ein Zertifikat installiert.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Zertifikate** an.
3. Wählen Sie das zu löschende Zertifikat über das Symbol aus.
   Das Zertifikat wird angezeigt.
4. Wählen Sie die Schaltfläche **Löschen** an.

↳ Das Zertifikat wird gelöscht.

6.9 Wie konfiguriere ich die Authentifizierung in Netzwerken (IEEE 802.1X)?

Authentifizierung ist der Nachweis und die Prüfung einer Identität. Mit ihr wird ein Netzwerk vor Missbrauch geschützt, weil nur genehmigte Geräte Zugang zum Netzwerk erhalten.

Der UTN-Server unterstützt das Authentifizierungsverfahren nach dem Standard IEEE 802.1X, dessen Kern das EAP (Extensible Authentication Protocol) ist.

Wenn Sie in Ihrem Netzwerk eine Authentifizierungsmethode nach IEEE 802.1X nutzen, kann der UTN-Server daran teilnehmen:

EAP-MD5 konfigurieren

EAP-MD5 (Message Digest #5) ist eine benutzerbasierte Authentifizierung über einen RADIUS-Server. Zuerst müssen Sie auf dem RADIUS-Server einen Benutzer (Benutzernamen und Passwort) für den UTN-Server anlegen. Danach konfigurieren Sie EAP-MD5 auf dem UTN-Server.

✓ Auf dem RADIUS-Server ist ein Benutzer für den UTN-Server angelegt.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Authentifizierung** an.
3. Wählen Sie aus der Liste **Authentifizierungsmethode** den Eintrag **MD5**.
4. Geben Sie Benutzername und Passwort ein, mit denen der UTN-Server auf dem RADIUS-Server eingerichtet ist.
5. Bestätigen Sie mit **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

EAP-TLS konfigurieren

EAP-TLS (Transport Layer Security) ist eine gegenseitige zertifikatbasierte Authentifizierung über einen RADIUS-Server. Hierzu werden zwischen dem UTN-Server und dem RADIUS-Server Zertifikate über eine verschlüsselte TLS-Verbindung ausgetauscht.

Sowohl RADIUS-Server als auch UTN-Server benötigen ein gültiges digitales Zertifikat, das von einer CA unterschrieben ist. Dafür muss eine PKI (Public Key Infrastructure) vorhanden sein.

WARNUNG

Führen Sie die unten aufgeführten Punkte in der angegebenen Reihenfolge aus. Ansonsten kann der UTN-Server im Netzwerk möglicherweise nicht angesprochen werden.

Setzen Sie in diesem Fall die UTN-Server-Parameter zurück ⇨ 🗎79.

1. Erstellen Sie auf dem UTN-Server eine Zertifikatsanforderung ⇨ 🗎69.
2. Erstellen Sie mit der Zertifikatsanforderung und mithilfe Ihres Authentifizierungsservers ein Zertifikat.
3. Installieren Sie das angeforderte Zertifikat auf dem UTN-Server ⇨ 🗎69.
4. Installieren Sie auf dem UTN-Server das Wurzel-CA-Zertifikat der Zertifizierungsstelle, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat ⇨ 🗎70.
5. Starten Sie das myUTN Control Center.
6. Wählen Sie den Menüpunkt **SICHERHEIT** – **Authentifizierung** an.
7. Wählen Sie aus der Liste **Authentifizierungsmethode** den Eintrag **TLS**.

8. Wählen Sie in der Liste **EAP-Wurzelzertifikat** das Wurzel-CA-Zertifikat aus.
9. Bestätigen Sie mit **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

EAP-TTLS konfigurieren

Bei EAP-TTLS (Tunneled Transport Layer Security) wird ein durch TLS geschützter Tunnel zum Geheimnisaustausch genutzt. Das Verfahren besteht aus zwei Phasen:

1. Äußere Authentifizierung: Zwischen UTN-Server und RADIUS-Server wird ein verschlüsselter TLS-Tunnel (Transport Layer Security) aufgebaut. Dazu identifiziert sich nur der RADIUS-Server mit einem von einer CA unterschriebenen Zertifikat beim UTN-Server.
2. Innere Authentifizierung: Im Tunnel findet die Authentifizierung (über CHAP, PAP, MS-CHAP oder MS-CHAPv2) statt.

✓ Auf dem RADIUS-Server ist ein Benutzer für den UTN-Server angelegt.

✓ Für erhöhte Sicherheit beim Verbindungsaufbau (optional): Auf dem UTN-Server ist das Wurzel-CA-Zertifikat der Zertifizierungsstelle, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat, installiert ⇨ 🗎70.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Authentifizierung** an.
3. Wählen Sie aus der Liste **Authentifizierungsmethode** den Eintrag **TTLS**.
4. Geben Sie Benutzername und Passwort ein, mit denen der UTN-Server auf dem RADIUS-Server eingerichtet ist.
5. Wählen Sie die Einstellungen, mit denen die Kommunikation im TLS-Tunnel gesichert werden soll.
6. Erhöhen Sie die Sicherheit beim Verbindungsaufbau (optional):
   Wählen Sie in der Liste **EAP-Wurzelzertifikat** das Wurzel-CA-Zertifikat aus.
7. Bestätigen Sie mit **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

PEAP konfigurieren

Bei PEAP (Protected Extensible Authentication Protocol) wird zunächst ein verschlüsselter TLS-Tunnel (Transport Layer Security) zwischen UTN-Server und RADIUS-Server aufgebaut. Dazu identifiziert sich nur der RADIUS-Server mit einem von einer CA unterschriebenen Zertifikat beim UTN-Server. Der TLS-Tunnel wird anschließend benutzt, um eine weitere Verbindung aufzubauen, wobei diese mit zusätzlichen EAP-Authentifizierungsmethoden (z.B. MSCHAPv2) geschützt werden kann.

Das Verfahren ähnelt EAP-TTLS (⇨ 🗎73) stark, allerdings werden andere Verfahren zur Authentifizierung des UTN-Servers verwendet.

✓ Auf dem RADIUS-Server ist ein Benutzer für den UTN-Server angelegt.

✓ Für erhöhte Sicherheit beim Verbindungsaufbau (optional): Auf dem UTN-Server ist das Wurzel-CA-Zertifikat der Zertifizierungsstelle, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat, installiert ⇨ 🗎70.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Authentifizierung** an.
3. Wählen Sie aus der Liste **Authentifizierungsmethode** den Eintrag **PEAP**.
4. Geben Sie Benutzername und Passwort ein, mit denen der UTN-Server auf dem RADIUS-Server eingerichtet ist.
5. Wählen Sie die Einstellungen, mit denen die Kommunikation im TLS-Tunnel gesichert werden soll.
6. Erhöhen Sie die Sicherheit beim Verbindungsaufbau (optional):
   Wählen Sie in der Liste **EAP-Wurzelzertifikat** das Wurzel-CA-Zertifikat aus.

7. Bestätigen Sie mit **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

EAP-FAST konfigurieren

EAP-FAST (Flexible Authentication via Secure Tunneling) ist ein von der Firma Cisco entwickeltes spezifisches EAP-Verfahren.

Wie bei EAP-TTLS (⇨ 🗎73) und PEAP (⇨ 🗎73) schützt ein Tunnel die Datenübertragung. Allerdings identifiziert sich der Server nicht mit einem Zertifikat sondern mit PACs (Protected Access Credentials).

✓ Auf dem RADIUS-Server ist ein Benutzer für den UTN-Server angelegt.

1. Starten Sie das UTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT** – **Authentifizierung** an.
3. Wählen Sie aus der Liste **Authentifizierungsmethode** den Eintrag **FAST**.
4. Geben Sie Benutzername und Passwort ein, mit denen der UTN-Server auf dem RADIUS-Server eingerichtet ist.
5. Wählen Sie die Einstellungen, mit denen die Kommunikation im Tunnel gesichert werden soll.
6. Bestätigen Sie mit **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

7 Wartung

Sie können am UTN-Server verschiedene Wartungsmaßnahmen durchführen:

- Wie starte ich den UTN-Server neu? ⇨ 76
- Wie führe ich ein Update aus? ⇨ 77
- Wie mache ich ein Konfigurations-Backup? ⇨ 78
- Wie setze ich die Parameter auf die Standardwerte zurück? ⇨ 79

7.1 Wie starte ich den UTN-Server neu?

Nach einigen Parameteränderungen oder nach einem Update wird der UTN-Server automatisch neu gestartet. Falls sich der UTN-Server in einem undefinierten Zustand befindet, können Sie den UTN-Server auch manuell neu starten.

- UTN-Server via myUTN Control Center neu starten ⇨ 🗎76
- UTN-Server über Restart-Taster neu starten ⇨ 🗎76

UTN-Server via myUTN Control Center neu starten

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG** – **Neustart** an.
3. Wählen Sie die Schaltfläche **Neustart** an.

↳ Der UTN-Server wird neu gestartet.

UTN-Server über Restart-Taster neu starten

1. Drücken Sie kurz den Restart-Taster am Gerät.

↳ Der UTN-Server wird neu gestartet.

7.2 Wie führe ich ein Update aus?

Aktualisieren Sie Ihren UTN-Server mit einem Soft- und Firmware-Update. Neue Firm-/Software enthält neue Funktionen und/oder Fehlerbereinigungen.

Die Versionsnummer der aktuell auf dem UTN-Server installieren Firm-/Software finden Sie auf der Startseite des myUTN Control Centers.

Aktuelle Firm-/Software-Dateien finden Sie auf der SEH Computertechnik GmbH-Website:

https://www.seh-technology.com/de/service/downloads.html

Beim Update wird lediglich die vorhandene Firm-/Software aktualisiert; die Einstellungen bleiben erhalten.

Wichtig:

Jede Update-Datei enthält eine 'Readme'-Datei. Lesen und befolgen Sie die Informationen aus der Readme-Datei.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG** – **Update** an.
3. Geben Sie im Feld **Update-Datei** die Update-Datei an.
4. Wählen Sie die Schaltfläche **Installieren** an.

↳ Das Update wird ausgeführt. Anschließend startet der UTN-Server neu.

7.3 Wie mache ich ein Konfigurations-Backup?

Alle Einstellungen des UTN-Servers (Ausnahme: Passwörter) sind in der Datei '<Default-Name>_parameters.txt' gespeichert.

Sie können diese Parameterdatei als Sicherungskopie auf Ihren lokalen Client speichern. Dadurch können Sie jederzeit auf einen festen Konfigurationsstatus zurückgreifen.

Zudem können Sie in der kopierten Datei die Parameterwerte mit einem Texteditor bearbeiten. Die bearbeitete Datei kann anschließend auf einen oder mehrere UTN-Server geladen werden. Die in der Datei enthaltenen Parameterwerte werden dann von dem Gerät bzw. den Geräten übernommen.

Detaillierte Beschreibungen zu den Parametern entnehmen Sie den 'Parameterlisten' ⇨ 🗎85.

- Parameterwerte ansehen ⇨ 🗎78
- Parameterdatei sichern ⇨ 🗎78
- Parameterdatei auf einen UTN-Server laden ⇨ 🗎78

Parameterwerte ansehen

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG** – **Parameter-Backup** an.
3. Wählen Sie das Symbol an.

↳ Die aktuellen Parameterwerte werden angezeigt.

Parameterdatei sichern

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG** – **Parameter-Backup** an.
3. Wählen Sie das Symbol an.
4. Speichern Sie die Datei '<Default-Name>_parameters.txt' mithilfe Ihres Browsers auf ein lokales System.

↳ Die Parameterdatei ist gesichert.

Parameterdatei auf einen UTN-Server laden

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG** – **Parameter-Backup** an.
3. Geben Sie im Feld **Parameterdatei** die Datei '<Default-Name>_parameters.txt' an.
4. Wählen Sie die Schaltfläche **Importieren** an.

↳ Die in der Datei enthaltenen Parameterwerte werden von dem UTN-Server übernommen.

7.4 Wie setze ich die Parameter auf die Standardwerte zurück?

Sie können den UTN-Server auf die Standardwerte zurücksetzen, z.B. wenn Sie den UTN-Server in einem anderen Netzwerk neu installieren möchten. Es werden alle Einstellungen auf die Werkseinstellung zurückgesetzt. Installierte Zertifikate bleiben erhalten.

Wichtig:

Die Verbindung zum myUTN Control Center kann abbrechen, falls sich beim Zurücksetzen die IP-Adresse des UTN-Servers ändert.

Ermitteln Sie ggf. die neue IP-Adresse ⇨ 🗎20.

Sie können die Einstellungen entweder via Fernzugriff (myUTN Control Center) oder über den Reset-Taster am UTN-Server zurücksetzen.

Wenn Sie das Passwort für das UTN Control Center verloren haben, setzen Sie den UTN-Server über den Reset-Taster zurück. Dabei ist keine Passworteingabe erforderlich.

- Parameter via myUTN Control Center zurücksetzen ⇨ 🗎79
- Parameter via Reset-Taster zurücksetzen ⇨ 🗎79

Parameter via myUTN Control Center zurücksetzen

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG** – **Standardeinstellung** an.
3. Wählen Sie die Schaltfläche **Standardeinstellung** an.
   Eine Sicherheitsabfrage erscheint.
4. Bestätigen Sie die Sicherheitsabfrage.

↳ Die Parameter werden zurückgesetzt.

Parameter via Reset-Taster zurücksetzen

Über den Reset-Taster am Gerät können Sie die Parameterwerte des UTN-Servers auf die Standardeinstellung zurücksetzen.

1. Drücken Sie den Reset-Taster für 5 Sekunden.
   Der UTN-Server startet neu.

↳ Die Parameter sind zurückgesetzt.

8 Anhang

Der Anhang enthält ein Glossar, die Problembehandlung und die Listen dieses Dokumentes.

8.1 Glossar

Compound-USB-Gerät

Ein Compound-USB-Gerät besteht aus einem USB-Hub und einem oder mehreren USB-Geräten, die alle in einem einzigen Gehäuse eingebaut sind. Dongles sind oft Compound-USB-Geräte.

Wird ein Compound-USB-Gerät an den USB-Port eines UTN-Server angeschlossen, werden im myUTN Control Center und in der Auswahlliste des SEH UTN Managers alle eingebauten USB-Geräte am USB-Port dargestellt. Beim Aktivieren der Portverbindung, werden alle angezeigten USB-Geräte mit dem Client des Benutzers verbunden. Es ist nicht möglich, die Portverbindung nur zu einem der USB-Geräte herzustellen.

Default-Name

Gerätename, der vom Hersteller vergeben wird und nicht geändert werden kann. Wenn Sie mehrere identische UTN-Server verwenden, können Sie damit ein bestimmtes Gerät identifizieren.

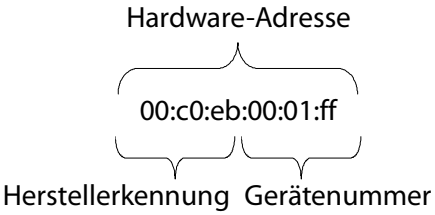
Der Default-Name des UTN-Servers setzt sich aus den zwei Buchstaben 'IC' und der Gerätenummer zusammen. Die Gerätenummer entspricht den sechs letzten Ziffern der Hardware-Adresse.

Sie können den Default-Namen im myUTN Control Center ablesen.

Hardware-Adresse

Die Hardware-Adresse (oft auch Ethernet-Adresse, physikalische oder MAC-Adresse) ist ein weltweit eindeutiger Identifikator eines Netzwerkadapters. Wenn Sie mehrere identische UTN-Server verwenden, können Sie damit ein bestimmtes Gerät identifizieren.

Die Hardware-Adresse wird vom Hersteller in der Hardware des Gerätes festgelegt. Sie besteht aus zwölf hexadezimalen Ziffern: Die ersten sechs Ziffern kennzeichnen den Hersteller, die letzten sechs Ziffern identifizieren das individuelle Gerät. Die zur Trennung der Ziffern verwendeten Zeichen sind plattformabhängig. Unter Linux werden ':' verwendet.



Sie können die Hardware-Adresse am Gehäuse oder im SEH UTN Manager ablesen.

myUTN Control Center

Das myUTN Control Center ist die Benutzeroberfläche des UTN-Servers. Über das myUTN Control Center kann der UTN-Server konfiguriert und überwacht werden.

Sie rufen das myUTN Control Center in einem Internet-Browser (z.B. Mozilla Firefox) auf.

Mehr Informationen ⇨ 8.

SEH UTN Manager

Der 'SEH UTN Manager' ist ein von SEH Computertechnik GmbH entwickeltes Software-Tool. Mit dem SEH UTN Manager werden Verbindungen zu den USB-Geräten an UTN-Servern hergestellt und verwaltet.

Mehr Informationen ⇨ 9.

8.2 Problembehandlung

Dieses Kapitel beschreibt einige Probleme, erklärt ihre Ursachen und gibt erste Lösungshilfen.

Problem

Lösung

UTN-Server: BIOS-Modus

Der UTN-Server fällt in den BIOS-Modus, wenn die Firmware funktioniert, jedoch die Software fehlerhaft ist. Dieses Verhalten tritt z.B. bei einem nicht korrekt durchgeführtem Softwareupdate auf.

Sie erkennen den BIOS-Modus an den LEDs:

- *Status-LED ist aus*
- *Activity-LED blinkt zyklisch*

WARNUNG

Der UTN-Server ist im BIOS-Modus nicht funktionsfähig.

Wenden Sie sich in diesem Fall an unser Support-Team ⇨ 🗎4.

UTN-Server: Verbindung kann nicht hergestellt werden

Sie finden den UTN-Server im Netzwerk und können ihn via TCP/IP-Verbindung erreichen. Über den SEH UTN Manager kann jedoch keine Verbindung hergestellt werden.

Mögliche Ursachen:

- Eine Firewall oder andere Sicherheitssoftware blockiert die Kommunikation.
  Fügen Sie für den UTN-Port bzw. UTN-SSL-Port eine Ausnahme in Ihrer Firewall oder Sicherheitssoftware hinzu. Lesen Sie hierzu die Dokumentation Ihrer Firewall oder Sicherheitssoftware.
- Die Portnummern im SEH UTN Manager und auf dem UTN-Server und sind nicht identisch: Sie haben die Portnummer geändert und SNMPv1 ist deaktiviert, sodass die Änderung nicht an den SEH UTN Manager weitergegeben werden kann ⇨ 🗎38.

myUTN Control Center: Verbindung kann nicht hergestellt werden

Schließen Sie Fehlerquellen aus. Überprüfen Sie dazu:

- die Kabelverbindungen
- die IP-Adresse des UTN-Servers ⇨ 20
- die Proxy-Einstellungen Ihres Browsers (lesen Sie hierzu die Dokumentation Ihres Browsers)

Kann weiterhin keine Verbindung hergestellt werden, können folgende Sicherheitsmechanismen verantwortlich sein:

- Der Zugang ist via SSL/TLS (HTTPS) geschützt ⇨ 59.
- Der Zugang ist via SSL/TLS (HTTPS) geschützt und Sie haben das Zertifikat (selbstsigniert/CA/PKCS#12) gelöscht ⇨ 67.
  Setzen Sie die Parameterwerte UTN-Server auf die Standardwerte zurück ⇨ 79. Dabei werden automatisch neue Zertifikate generiert.

WARNUNG

Beim Zurücksetzen gehen sämtliche Einstellungen verloren und es ändert sich ggf. die IP-Adresse.

Ermitteln Sie ggf. die neue IP-Adresse ⇨ 20.

- Die TCP-Portzugriffskontrolle ist aktiviert ⇨ 63.
- Die Cipher Suites der Verschlüsselungsstufe werden vom Browser nicht unterstützt ⇨ 60.

myUTN Control Center: Benutzername und/oder Passwort verloren

Wenn Sie den Zugriff auf das myUTN Control Center geschützt aber die Zugangsdaten verloren haben, können Sie den UTN-Server auf die Standardwerte zurücksetzen. Sie erhalten dann wieder Zugriff, weil das Zugriff auf das myUTN Control Center standardmäßig nicht geschützt ist.

WARNUNG

Beim Zurücksetzen gehen sämtliche Einstellungen verloren und es ändert sich ggf. die IP-Adresse.

Ermitteln Sie ggf. die neue IP-Adresse ⇨ 20.

SEH UTN Manager: Verbindung zum USB-Gerät kann nicht hergestellt werden

Mögliche Ursachen:

- Der USB-Port ist bereits mit einem anderen Client verbunden.
  Warten Sie bis die Verbindung vom anderen Benutzer getrennt wird oder fordern Sie das USB-Gerät an ⇨ 45.
- Auf dem Client ist keine Treibersoftware für das USB-Gerät installiert.
  Installieren Sie dieTreibersoftware für Ihr USB-Gerät. Lesen Sie dazu die Dokumentation des USB-Gerätes.

SEH UTN Manager: USB-Geräte werden nicht angezeigt

Schließen Sie Fehlerquellen aus: Überprüfen Sie, ob das USB-Gerät am UTN-Server angeschlossen ist.

Wird das USB-Gerät weiterhin nicht angezeigt, kann dies folgende Gründe haben:

- Am UTN-Server sind mehrere Compound-USB-Geräte (⇨ 🗎81) angeschlossen. Jedes darin eingebaute USB-Gerät belegt einen virtuellen USB-Port des UTN-Servers. Die Anzahl dieser virtuellen USB-Ports ist begrenzt. Wird sie überschritten, können keine weiteren USB-Geräte am UTN-Server verwendet werden (⇨ 🗎43).
- Der USB-Port ist abgeschaltet ⇨ 🗎37 .
- Die USB-Portschlüsselkontrolle ist für das USB-Geräte aktiviert ⇨ 🗎64.
  Erst wenn der Schlüssel für den USB-Port im SEH UTN Manager eingegeben wird, erscheint der USB-Port und das daran angeschlossene USB-Gerät.

SEH UTN Manager: Ein USB-Gerät ist am USB-Port angeschlossen, aber es werden mehrere USB-Geräte angezeigt

Mögliche Ursachen:

- Am USB-Port des UTN-Servers ist ein USB-Hub angeschlossen.
- Bei dem angeschlossenen USB-Gerät handelt es sich um ein Compound-USB-Gerät (⇨ 🗎81) . Es besteht aus einem Hub und einem oder mehreren USB-Geräten, die alle in einem einzigen Gehäuse eingebaut sind. Wenn die Verbindung zum USB-Port hergestellt wird, werden alle dargestellten USB-Geräte mit dem Client des Benutzers verbunden und können genutzt werden.

SEH UTN Manager: Funktionen sind nicht verfügbar bzw. deaktiviert

Mögliche Ursachen:

- Ihr Client-Benutzerkonto hat nicht die erforderlichen administrativen Rechte. Hierdurch haben Sie auch im SEH UTN Manager eingeschränkte Benutzerrechte. Mehr Informationen finden Sie im Kapitel 'SEH UTN Manager – Funktionsübersicht' ⇨ 🗎106.
  Starten Sie den SEH UTN Manager als Administrator. Lesen Sie dazu die Dokumentation Ihres Betriebssystems.
- Eine Funktion wird nicht vom angeschlossenen USB-Gerät unterstützt.

8.3 Parameterlisten

Der UTN-Server speichert seine Konfiguration in Form von Parametern. Die Parameter nutzen Sie direkt bei folgenden Aktionen:

- Administration via E-Mail ⇨ 🗎17
- Konfigurations-Backup (Parameter ansehen, bearbeiten und auf andere Geräte laden) ⇨ 🗎78

Die folgenden Tabellen listen alle Parameter und Ihre Werte, damit Sie die Aktionen durchführen können.

Tabelle 14: Parameterliste – IPv4

Parameter	Wertekonvention	Default	Beschreibung
ip_addr [IP-Adresse]	gültige IP-Adresse	169.254.0.0/16	IP-Adresse des UTN-Servers.
ip_mask [Netzwerkmaske]	gültige IP-Adresse	255.255.0.0	Netzwerkmaske des UTN-Servers. Mit Netzwerkmasken (auch Netzmasken oder Subnetzmasken) werden große Netzwerke logisch in Subnetzwerke unterteilt. Falls Sie den UTN-Server in einem Subnetzwerk einsetzen, benötigt er die Netzwerkmaske des jeweiligen Subnetzwerks.
ip_gate [Gateway]	gültige IP-Adresse	0.0.0.0	IP-Adresse des Standard-Gateways im Netzwerk, das der UTN-Server verwendet. Über das Gateway werden IP-Adressen in einem anderen Netzwerk angesprochen.
ip_dhcp [DHCP]	on/off	on	De-/aktiviert das Protokoll DHCP. Über DHCP erfolgt die IP-Adresszuweisung automatisch, wenn das Protokoll in Ihrem Netzwerk implementiert ist.
ip_bootp [BOOTP]	on/off	on	De-/aktiviert das Protokoll BOOTP. Über BOOTP erfolgt die IP-Adresszuweisung automatisch, wenn das Protokoll in Ihrem Netzwerk implementiert ist.
ip_auto [ARP/PING]	on/off	on	De-/aktiviert das Protokoll ARP/PING. Mit den Befehlen ARP und PING können Sie eine über Zeroconf zugewiesene IP-Adresse ändern. Die Implementierung der Befehle ist systemabhängig; lesen Sie die Dokumentation zu Ihrem Betriebssystem.

*Wir empfehlen die Parameter **DHCP**, **BOOTP** und **ARP/PING** zu deaktivieren, sobald der UTN-Server eine IP-Adresse zugewiesen bekommen hat.*

Tabelle 15: Parameterliste – IPv6

Parameter	Wertekonvention	Default	Beschreibung
ipv6 [IPv6]	on/off	on	De-/aktiviert die IPv6-Funktionalität des UTN-Servers.
ipv6_auto [Automatische Konfiguration]	on/off	on	De-/aktiviert die automatische Vergabe der IPv6-Adressen für den UTN-Server.
ipv6_addr [IPv6-Adresse]	n:n:n:n:n:n:n:n	: :	Definiert eine manuell vergebene IPv6-Adresse im Format n:n:n:n:n:n:n:n für den UTN-Server: • Jedes 'n' stellt den hexadezimalen Wert von einem der acht 16-Bit-Elemente der Adresse dar. • Führende Nullen können vernachlässigt werden. • Ein Block aus zusammenhängenden Nullen kann mit zwei aufeinander folgenden Doppelpunkten zusammengefasst werden.
ipv6_gate [Router]	n:n:n:n:n:n:n:n	: :	Definiert manuell einen statischen Router, an den der UTN-Server seine Anfragen sendet.
ipv6_plen [Präfixlänge]	0–64 [1–2 Zeichen; 0–9]	64	Definiert die Länge des Subnetz-Präfixes für die IPv6-Adresse. Der Wert 64 ist voreingestellt. Adressbereiche (z.B. Ihr Netzwerk) werden durch Präfixe angegeben. Dazu wird die Präfixlänge (Anzahl der verwendeten Bits) als Dezimalzahl mit vorangehendem '/' an die IPv6-Adresse angehängt.

Tabelle 16: Parameterliste – DNS

Parameter	Wertekonvention	Default	Beschreibung
dns [DNS]	on/off	on	De-/aktiviert die Namensauflösung über einen DNS-Server.
dns_domain [Domain-Name]	max. 255 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert die IP-Adresse des ersten DNS-Servers.
dns_primary [Erster DNS-Server]	gültige IP-Adresse	0.0.0.0	Definiert die IP-Adresse des zweiten DNS-Servers. Der zweite DNS-Server wird benutzt, wenn der erste nicht verfügbar ist.
dns_secondary [Zweiter DNS-Server]	gültige IP-Adresse	0.0.0.0	Definiert den Domain-Namen eines vorhandenen DNS-Servers.

Tabelle 17: Parameterliste – SNMP

Parameter	Wertekonvention	Default	Beschreibung
snmpv1 [SNMPv1]	on/off	on	De-/aktiviert die SNMPv1-Funktionalität.
snmpv1_ronly [Nur Lesen]	on/off	off	De-/aktiviert den Schreibschutz für die Community.
snmpv1_community [Community]	max. 64 Zeichen [a–z, A–Z, 0–9]	public	Name der SNMP-Community. Tragen Sie den Namen so ein, wie er in der Überwachungsstation definiert ist. **Wichtig:** Der standardmäßig eingetragene Name ist 'public'. Dieser Name wird weitläufig für Communities mit Lese-/Schreibzugriff verwendet. Wir empfehlen diesen sobald wie möglich zu ändern, um die Sicherheit zu erhöhen.
snmpv3 [SNMPv3]	on/off	on	De-/aktiviert die SNMPv3-Funktionalität.
any_hash [Hash]	md5 sha	md5	Definiert den Hash-Algorithmus für die SNMP-Benutzergruppe 1.
any_rights [Zugriffsrechte]	--- readonly readwrite	readonly	Definiert die Zugriffsrechte der SNMP-Benutzergruppe 1. --- = [keine]
any_cipher [Verschlüsselung]	--- aes des	---	Definiert die Verschlüsselungsmethode der SNMP-Benutzergruppe 1. --- = [keine]
admin_hash [Hash]	md5 sha	md5	Definiert den Hash-Algorithmus für die SNMP-Benutzergruppe 2.
admin_rights [Zugriffsrechte]	--- readonly readwrite	readwrite	Definiert die Zugriffsrechte der SNMP-Benutzergruppe 2. --- = [keine]
admin_cipher [Verschlüsselung]	--- aes des	---	Definiert die Verschlüsselungsmethode der SNMP-Benutzergruppe 2.

Wichtig:

Die Benutzerkonten des UTN-Servers werden als SNMP-Benutzerkonten verwendet ⇨ 25. Berücksichtigen Sie dies bei Ihren Einstellungen.

Tabelle 18: Parameterliste – Bonjour

Parameter	Wertekonvention	Default	Beschreibung
bonjour [Bonjour]	on/off	on	De-/aktiviert Bonjour.
bonjour_name [Bonjour-Name]	max. 64 Zeichen [a–z, A–Z, 0–9]	[Standard-name]	Definiert den Bonjour Namen des myUTN-Servers. Der myUTN-Server gibt unter diesem Namen seine Bonjour-Dienste bekannt. Wird kein Bonjour-Name eingegeben, wird ein Standardname verwendet (Gerätename@ICxxxxxx).

Tabelle 19: Parameterliste – POP3

Parameter	Wertekonvention	Default	Beschreibung
pop3 [POP3]	on/off	off	De-/aktiviert die POP3-Funktionalität.
pop3_srv [Servername]	max. 128 Zeichen	[blank]	Definiert den POP3-Server über die IP-Adresse oder den Hostnamen. Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.
pop3_port [Serverport]	1–65535 [1–5 Zeichen; 0–9]	110	Definiert den Port, über den der UTN-Server E-Mails empfängt. Die standardmäßig bei POP3 verwendete Portnummer 110 ist voreingestellt. Bei SSL/TLS (Parameter 'POP3 – Sicherheit' ⇨ 🗎28) wird standardmäßig 995 verwendet. Lesen Sie hierzu ggf. die Dokumentation des POP3-Servers.
pop3_sec [Sicherheit]	0–2 [1 Zeichen; 0–2]	0	Definiert das anzuwendende Authentifizierungsverfahren: • APOP: verschlüsselt das Passwort beim Einloggen auf dem POP3-Server • SSL/TLS: verschlüsselt die gesamte Kommunikation mit dem POP3-Server. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨ 🗎60. 0 = keine Sicherheit 1 = APOP 2 = SSL/TLS
pop3_poll [E-Mails abfragen alle]	1–10080 [1–5 Zeichen; 0–9]	2	Definiert das Zeitintervall (in Minuten) mit dem E-Mails vom POP3-Server abgefragt werden.
pop3_limit [E-Mails ignorieren mit mehr als]	0–4096 [1–4 Zeichen; 0–9]	4096	Definiert die maximale Größe (in Kbyte) der vom UTN-Server akzeptierten E-Mails. 0 = unbegrenzt
pop3_usr [Benutzername]	max. 128 Zeichen	[blank]	Definiert den Benutzernamen, den der UTN-Server benutzt, um sich am POP3-Server anzumelden.
pop3_pwd [Passwort]	max. 128 Zeichen	[blank]	Definiert das Benutzerpasswort, das der UTN-Server benutzt, um sich am POP3-Server anzumelden.

Tabelle 20: Parameterliste – SMTP

Parameter	Wertekonvention	Default	Beschreibung
smtp_srv [Servername]	max. 128 Zeichen	[blank]	Definiert den SMTP-Server über die IP-Adresse oder den Hostnamen. Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.
smtp_port [Serverport]	1–65535 [1–5 Zeichen; 0–9]	25	Definiert den Port, über den der UTN- und SMTP-Server kommunizieren. Die standardmäßig bei SMTP verwendete Portnummer 25 ist voreingestellt. Bei SSL/TLS (Parameter 'SMTP – SSL/TLS' ⇨ 🗎29) verwenden SMTP-Server standardmäßig den Port 587 (STARTSSL/STARTTLS) oder den veralteten Port 465 (SMTPS). Lesen Sie hierzu ggf. die Dokumentation des SMTP-Servers.
smtp_ssl [SSL/TLS]	on/off	off	De-/aktiviert die Option SSL/TLS. Mit SSL/TLS wird der Übertragungsweg vom UTN-Server zum SMTP-Server verschlüsselt. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨ 🗎60.
smtp_sender [Name des Absenders]	max. 128 Zeichen	[blank]	Definiert die E-Mail-Adresse, die der UTN-Server zum Versenden von E-Mails verwendet. Oft sind der Name des Absenders und der Benutzername des E-Mail-Benutzerkontos identisch.
smtp_auth [Anmelden]	on/off	off	De-/aktiviert die SMTP-Authentifizierung (SMTP AUTH). Beim E-Mail-Versand übermitteltet der UTN-Server Benutzername und Passwort an den SMTP-Server um sich zu authentifizieren. Tragen Sie Benutzername (Parameter 'SMTP – Benutzername' ⇨ 🗎29) und Passwort (Parameter 'SMTP – Passwort' ⇨ 🗎29) ein. Einige SMTP-Server sind für SMTP-Authentifizierung konfiguriert, um Missbrauch (Spam) zu verhindern.
smtp_usr [Benutzername]	max. 128 Zeichen	[blank]	Definiert den Benutzernamen, den der UTN-Server benutzt, um sich am SMTP-Server anzumelden.
smtp_pwd [Passwort]	max. 128 Zeichen	[blank]	Definiert das Passwort, das der UTN-Server benutzt, um sich am SMTP-Server anzumelden.

Parameter	Wertekonvention	Default	Beschreibung
smtp_sign [Sicherheit (S/MIME)]	on/off	off	De-/aktiviert den E-Mail-Sicherheitsstandard S/MIME (Secure/Multipurpose Internet Mail Extensions). Mit S/MIME können E-Mails signiert (Parameter 'SMTP – E-Mail signieren' ⇨ 🗎29) oder verschlüsselt (Parameter 'SMTP – Vollständig verschlüsseln' ⇨ 🗎30) werden. Aktivieren Sie die gewünschte Funktion (ggf. mit 'SMTP – Öffentlichen Schlüssel beifügen' ⇨ 🗎30).
smtp_attpkey [Öffentlichen Schlüssel beifügen]	on/off	on	Sendet den öffentlichen Schlüssel zusammen mit der E-Mail. Viele E-Mail-Clients benötigen den Schlüssel um die E-Mail anzeigen zu können.
smtp_encrypt [Vollständig verschlüsseln] [E-Mail signieren]	on/off	off	on = Aktiviert das Verschlüsseln von E-Mails. Eine verschlüsselte E-Mail kann nur vom vorgesehenen Empfänger geöffnet und gelesen werden. Für die Verschlüsselung wird ein S/MIME-Zertifikat benötigt ⇨ 🗎67. off = Aktiviert das Signieren von E-Mails. Mit der Signatur kann der Empfänger die Identität des Absenders zu prüfen. Dadurch wird gewährleistet, dass die E-Mail nicht verändert wurde. Für das Signieren wird ein S/MIME-Zertifikat benötigt ⇨ 🗎67.

Tabelle 21: Parameterliste – IPv4-VLAN

Parameter	Wertekonvention	Default	Beschreibung
ip4vlan_mgmt [IPv4-Management-VLAN]	on/off	off	De-/aktiviert die Weiterleitung der IPv4-Management-VLAN-Daten. Ist die Option aktiviert, ist SNMP ist ausschließlich im IPv4-Management-VLAN verfügbar.
ip4vlan_mgmt_id [VLAN-ID]	0–4096 [1–4 Zeichen; 0–9]	0	ID zur Identifizierung des IPv4-Management-VLANs.
ip4vlan_mgmt_any [Zugriff über alle VLANs]	on/off	off	De-/aktiviert den administrativen Zugang (Web) zum UTN-Server über IPv4-Client-VLAN. Ist die Option aktiviert, kann der UTN-Server aus allen VLANs heraus administriert werden.
ip4vlan_mgmt_untag [Zugriff vom LAN (untagged)]	on/off	on	De-/aktiviert den administrativen Zugang zum UTN-Server über IPv4-Pakete ohne VLAN-Tag. Ist die Option deaktiviert, kann der UTN-Server ausschließlich über VLANs administriert werden.
ipv4vlan_on_1 ~ ipv4vlan_on_20 [VLAN]	on/off	off	De-/aktiviert die Weiterleitung der IPv4-Client-VLAN-Daten.
ipv4vlan_addr_1 ~ ipv4vlan_addr_20 [IP-Adresse]	gültige IP-Adresse	192.168.0.0	IP-Adresse des UTN-Servers innerhalb des IPv4-Client-VLANs.
ipv4vlan_mask_1 ~ ipv4vlan_mask_20 [Netzwerkmaske]	gültige IP-Adresse	255.255.255.0	Netzwerkmaske des UTN-Servers innerhalb des IPv4-Client-VLANs.
ip4vlan_gate_1 ~ ip4vlan_gate_20 [Gateway]	gültige IP-Adresse	0.0.0.0	IP-Adresse des Gateways im IPv4-Management-VLAN. Über das Gateway werden IP-Adressen in einem anderen Netzwerk angesprochen.
ipv4vlan_id_1 ~ ipv4vlan_id_20 [VLAN-ID]	0–4096 [1–4 Zeichen; 0–9]	0	ID zur Identifizierung des IPv4-Client-VLANs.
utn_2vlan_1 ~ utn_2vlan_20 [VLAN zuordnen]	0–9 [1 Zeichen; 0–9]	0	Ordnet dem USB-Port ein VLAN zu. 0 = jedes 1 = VLAN 1 2 = VLAN 2 usw. 9 = keines

Tabelle 22: Parameterliste – Datum/Zeit

Parameter	Wertekonvention	Default	Beschreibung
ntp [Datum/Zeit]	on/off	on	De-/aktiviert die Verwendung eines Zeit-Servers (SNTP).
ntp_server [Time-Server]	max. 64 Zeichen [a–z, A–Z, 0–9]	pool.ntp.org	Definiert einen Zeit-Server über die IP-Adresse oder den Hostnamen. Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde. **Wichtig:** Ist Ihr Netzwerk entsprechend konfiguriert, erhält der UTN-Server die Zeit-Server-Einstellungen automatisch über DHCP. Ein so eingetragener Zeit-Server hat immer Vorrang gegenüber manuellen Einstellungen.
ntp_tzone [Zeitzone]	UTC, GMT, EST, EDT, CST, CDT, MST, MDT, PST, PDT usw.	CET/CEST (EU)	Gleicht Standortabweichungen und länderspezifische Eigenheiten (Sommerzeit usw.) im Verhältnis zur koordinierten Weltzeit (UTC) aus.

Tabelle 23: Parameterliste – Beschreibung

Parameter	Wertekonvention	Default	Beschreibung
sys_name [Hostname]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Geräte-Name als Alternative zur IP-Adresse. Mithilfe des Namen können Sie den UTN-Server leichter im Netzwerk identifizieren, z.B. falls Sie mehrere UTN-Server verwenden. Wird im myUTN Control Center und im SEH UTN Manager angezeigt.
sys_descr [Beschreibung]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Geräte-Beschreibung, z.B. Aufstellort oder Abteilung. Wird im myUTN Control Center und im SEH UTN Manager angezeigt.
sys_contact [Ansprechpartner]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Kontaktperson, z.B. Geräte-Administrator. Wird im myUTN Control Center angezeigt.

Tabelle 24: Parameterliste – USB-Port

Parameter	Wertekonvention	Default	Beschreibung
utn_tag_1 ~ utn_tag_20 [Portname]	max. 32 Zeichen [a–z, A–Z, 0–9]	[blank]	Freidefinierbare Bezeichnung des USB-Ports.
utn_poff_1 ~ utn_poff_20 [Port]	on/off	off	De-/aktiviert die Stromzufuhr für den USB-Port (bzw. das an den Port angeschlossene USB-Gerät). off = Stromzufuhr an on = Stromzufuhr aus

Tabelle 25: Parameterliste – UTN-Port

Parameter	Wertekonvention	Default	Beschreibung
utn_port [UTN-Port]	1–9200 [1–4 Zeichen; 0–9]	9200	Definiert die Nummer des UTN-Ports (für unverschlüsselte Verbindungen).  **WARNUNG** Der UTN-Port darf nicht durch eine Sicherheitssoftware (Firewall) blockiert werden.
utn_sslport [UTN-SSL-Port]	1–9443 [1–4 Zeichen; 0–9]	9443	Definiert die Nummer des UTN-SSL-Ports (für verschlüsselte Verbindungen).  **WARNUNG** Der UTN-SSL-Port darf nicht durch eine Sicherheitssoftware (Firewall) blockiert werden.

Tabelle 26: Parameterliste – Benachrichtigung

Parameter	Wertekonvention	Default	Beschreibung
mailto_1 mailto_2 [E-Mail-Adresse]	gültige E-Mail Adresse [max. 64 Zeichen]	[blank]	E-Mail-Adresse des Empfängers für Benachrichtigungen.
noti_stat_1 noti_stat_2 [Status-E-Mail]	on/off	off	De-/aktiviert den periodischen Versand einer Status-E-Mail an den Empfänger 1 oder 2.
notistat_d [Intervall]	al su mo tu we th fr sa	al	Definiert den Tag (das Intervall) an dem eine Status-E-Mail versendet wird. al = täglich su= Sonntag mo= Montag tu= Dienstag we= Mittwoch th= Donnerstag fr = Freitag sa= Samstag
notistat_h [hh]	0–23 [1–2 Zeichen; 0–9]	0	Definiert die Uhrzeit (Stunde), zu der eine Status-E-Mail versendet wird. 1 = 1. Stunde 2 = 2. Stunde 3 = 3. Stunde usw.
notistat_tm [mm]	0–5 [1 Zeichen; 0–5]	0	Definiert die Uhrzeit (Minute), zu der eine Status-E-Mail versendet wird. 0 = 00 min 1 = 10 min 2 = 20 min 3 = 30 min 4 = 40 min 5 = 50 min
noti_dev_1 noti_dev_2 [Sende E-Mail nach dem Anschließen oder Entfernen eines USB-Gerätes]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch das Anschließen oder Entfernen eines USB-Gerätes am UTN-Server ausgelöst wird.

Parameter	Wertekonvention	Default	Beschreibung
noti_act_1 noti_act_2 [Sende E-Mail nach der Aktivierung oder Deaktivierung eines USB-Ports]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch das Aktivieren oder Deaktivieren eines USB-Ports (d.h. der Verbindung zu dem daran angeschlossenen USB-Gerät) ausgelöst wird.
noti_pup_1 noti_pup_2 [Sende E-Mail nach Neustart des UTN-Servers]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch einen Neustart des UTN-Servers ausgelöst wird.
trapto_1 trapto_2 [Adresse]	gültige IP-Adresse	0.0.0.0	SNMP-Trap-Adresse des Empfängers.
trapcommu_1 trapcommu_2 [Community]	max. 64 Zeichen [a–z, A–Z, 0–9]	public	SNMP-Trap-Community des Empfängers.
trapdev [Sende Trap nach dem Anschließen oder Entfernen eines USB-Gerätes]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch das Anschließen oder Entfernen eines USB-Gerätes am UTN-Server ausgelöst wird.
trapact [Sende Trap nach der Aktivierung oder Deaktivierung eines USB-Ports]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch das Aktivieren oder Deaktivieren eines USB-Ports (d.h. der Verbindung zu dem daran angeschlossenen USB-Gerät) ausgelöst wird.
trappup [Sende Trap nach Neustart des UTN-Servers]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch einen Neustart des UTN-Servers ausgelöst wird.

Tabelle 27: Parameterliste – SSL-/TLS-Verbindungen

Parameter	Wertekonvention	Default	Beschreibung
sslmethod [Verschlüsselungsprotokoll]	any sslv3 tls10 tls11 tls12	any	Definiert das Verschlüsselungsprotokoll für SSL-/TLS-Verbindungen. any = Beliebig (automatisches Aushandeln) sslv3 = SSL 3.0 tls10 = TLS 1.0 tls11 = TLS 1.1 tls12 = TLS 1.2  **WARNUNG** Aktuelle Browser unterstützen SSL nicht. Bei Verwendung von SSL in Kombination mit aktuellen Browsern und der Einstellung **Nur HTTPS** für den Webzugang zum myUTN Control Center (⇨ 🗎59) kann keine Verbindung aufgebaut werden. Verwenden Sie TLS (und nicht SSL).

Parameter	Wertekonvention	Default	Beschreibung
security [Verschlüsselungs-stufe]	1–4 [1 Zeichen; 1–4]	4	Definiert die Verschlüsselungsstufe für SSL-/TLS-Verbindungen. 1 = Niedrig 2 = Mittel 3 = Hoch 4 = Beliebig (automatisches Aushandeln)  **WARNUNG** Aktuelle Browser unterstützen Cipher Suites der Stufe **Niedrig** nicht. Bei Verwendung von **Niedrig** in Kombination mit aktuellen Browsern und der Einstellung **Nur HTTPS** für den Webzugang zum myUTN Control Center (⇨ 🗎59) kann keine Verbindung aufgebaut werden. Verwenden Sie eine möglichst hohe Verschlüsselungsstufe.  **WARNUNG** Der SEH UTN Manager unterstützt die Verschlüsselungsstufe **Niedrig** nicht. Wenn Sie **Niedrig** in Kombination mit einer verschlüsselten USB-Verbindung (⇨ 🗎57) einstellen, kann keine Verbindung aufgebaut werden. Verwenden Sie eine möglichst hohe Verschlüsselungsstufe.

Tabelle 28: Parameterliste – myUTN Control Center Sicherheit

Parameter	Wertekonvention	Default	Beschreibung
http_allowed [Verbindung]	on/off	on	Definiert den erlaubten Verbindungstyp (HTTP/HTTPS) zum myUTN Control Center. on = HTTP/HTTPS off = nur HTTPS Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨ 60.  **WARNUNG** Aktuelle Browser unterstützen niedrige Sicherheitseinstellungen nicht. Mit ihnen kann keine Verbindung aufgebaut werden. Verwenden Sie nicht die folgende Kombination: Verschlüsselungsprotokoll **HTTPS** und Verschlüsselungsstufe **Niedrig**. Beim Verbindungsaufbau wird die Identität des UTN-Servers überprüft. Dazu fragt der Client via Browser nach dem Zertifikat (⇨ 67). Dieses Zertifikat muss vom Browser akzeptiert werden; lesen Sie hierzu die Dokumentation Ihrer Browsersoftware.
sessKeys [Control Center-Zugriff einschränken]	on/off	off	De-/aktiviert die Benutzerkonten des myUTN Control Center. Sind sie aktiviert, erscheint beim Anrufen des myUTN Control Centers eine Login-Maske. **Wichtig:** Definieren Sie die Benutzerkonten (Benutzernamen und Passwörter).
admin_name [Administrator – Benutzername]	max. 64 Zeichen [a–z, A–Z, 0–9]	admin	Definiert den Benutzernamen für das Administrator-Benutzerkonto. **Wichtig:** Ist gleichzeitig der Benutzername für das SNMPv3-Admin-Konto ⇨ 25.
admin_pwd [Administrator – Passwort]	8–64 Zeichen [a–z, A–Z, 0–9]	administrator	Definiert das Passwort für das Administrator-Benutzerkonto. **Wichtig:** Ist gleichzeitig das Passwort für das SNMPv3-Admin-Konto ⇨ 25.

Parameter	Wertekonvention	Default	Beschreibung
any_name [Lesezugriff-Benutzer-Benutzername]	max. 64 Zeichen [a–z, A–Z, 0–9]	anonymous	Definiert den Benutzernamen für das Lesezugriff-Benutze-Benutzerkonto. **Wichtig:** Ist gleichzeitig der Benutzername für das SNMPv3-User-Konto ⇨ 🗎25.
any_pwd [Lesezugriff-Benutzer-Passwort]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert das Passwort für das Lesezugriff-Benutze-Benutzerkonto. **Wichtig:** Ist gleichzeitig das Passwort für das SNMPv3-User-Konto ⇨ 🗎25.
sessKeyUList [Anmeldefenster zeigt]	on/off	on	Definiert das Aussehen der Login-Maske. on= Zeigt eine Liste der Benutzer, nur Passwort-Eingabe off= Neutrale Anmeldemaske, Eingabe von Benutzername und Passwort
sessKeyTimer [Sitzungs-Timeout]	on/off	on	De-/aktiviert das Sitzungs-Timeout.
sessKeyTimeout [Sitzungs-Timeout]	120–3600 [3–4 Zeichen; 0–9]	600	Zeitraum in Sekunden nach dem das Timeout wirksam wird.

Tabelle 29: Parameterliste – TCP-Portzugriff

Parameter	Wertekonvention	Default	Beschreibung
protection [Portzugriff kontrollieren]	on/off	off	De-/aktiviert die Sperrung von ausgewählten Ports und damit von Verbindungen zum UTN-Server.
protection_level [Sicherheitsstufe]	protec_utn protec_tcp protec_all	protec_utn	Definiert die zu sperrenden Porttypen. protec_utn= UTN-Zugriff (UTN-Ports) protec_tcp= TCP-Zugriff (TCP-Ports: HTTP/HTTPS/UTN) protec_all = alle Ports (IP-Ports)
ip_filter_on_1 ~ ip_filter_on_8 [IP-Adresse]	on/off	off	De-/aktiviert eine Ausnahme von der Portsperrung.
ip_filter_1 ~ ip_filter_8 [IP-Adresse]	gültige IP-Adresse	[blank]	Definiert Netzwerkelemente, die von einer Portsperrung ausgenommen sind über die IP-Adresse. **Wichtig:** Mit dem Einsatz von Wildcards (*) können Subnetzwerke definiert werden.
hw_filter_on_1 ~ hw_filter_on_8 [MAC-Adresse]	on/off	off	De-/aktiviert eine Ausnahme von der Portsperrung.
hw_filter_1 ~ hw_filter_8 [MAC-Adresse]	gültige Hardware-Adresse	00:00:00:00:00:00	Definiert Elemente, die von einer Portsperrung ausgenommen sind über die MAC-Adresse (Hardware-Adresse). **Wichtig:** MAC-Adressen werden nicht über Router weitergeleitet.
protection_test [Testmodus]	on/off	on	De-/aktiviert den Testmodus. **WARNUNG** Der Testmodus ist standardmäßig aktiv, damit Sie Ihre Einstellungen prüfen können ohne sich auszusperren. Ihre Einstellungen bleiben bis zu einem Neustart des UTN-Servers aktiv, danach ist der Zugriffsschutz nicht mehr wirksam. Deaktivieren Sie den Testmodus nachdem Sie Ihre Einstellungen erfolgreich getestet haben, damit der Zugriffsschutz dauerhaft aktiv bleibt.

Tabelle 30: Parameterliste – Verschlüsselung der USB-Verbindung

Parameter	Wertekonvention	Default	Beschreibung
utn_sec_1 ~ utn_sec_20 [USB-Port]	on/off	off	De-/aktiviert die SSL-/TLS-Verschlüsselung für Verbindung zwischen USB-Port (d.h. USB-Gerät) und Client. **Wichtig:** Nur Nutzdaten werden verschlüsselt. Steuer- und Protokolldaten werden unverschlüsselt übertragen.

Tabelle 31: Parameterliste – USB-Gerätetypen-Blockierung

Parameter	Wertekonvention	Default	Beschreibung
utn_hid [Eingabegeräte deaktivieren (HID-Klasse)]	on/off	on	De-/aktiviert das Blockieren von Eingabegeräten (HID – human interface devices). on = keine Blockierung off = Blockierung

Tabelle 32: Parameterliste – USB-Geräte-Zugriff

Parameter	Wertekonvention	Default	Beschreibung
utn_accctrt_1 ~ utn_accctrt_20 [Methode]	--- ids key keyids	---	Definiert die Zugriffs- und Nutzungseinschränkung für den USB-Port und das daran angeschlossene USB-Gerät. --- = kein Schutz ids = Gerätezuordnung key = Portschlüsselkontrolle keyids= Gerätezuordnung und Portschlüsselkontrolle
utn_keyval_1 ~ utn_keyval_20 [Schlüssel]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert den Schlüssel für den USB-Port und das daran angeschlossene USB-Gerät für den Schutz bei der Portschlüsselkontrolle.
utn_vendprodIDs_1 ~ utn_vendprodIDs_20 [USB-Gerät]			Definiert die VID (Vendor-ID) und PID (Product-ID) des USB-Gerätes, das dem USB-Port im Rahmen der Gerätezuordnung zugewiesen ist. *VID und PID eines USB-Gerätes sind meist nicht bekannt. Wir empfehlen die Konfiguration über das myUTN Control Center, weil VID und PID dabei automatisch ausgelesen und eingetragen werden.*

Tabelle 33: Parameterliste – Authentifizierung

Parameter	Wertekonvention	Default	Beschreibung
auth_typ [Authentifizierungs-methode]	--- MD5 TLS TTLS PEAP FAST	---	Definiert die Authentifizierungsmethode, die in Ihrem Netzwerk verwendet wird und an der der UTN-Server teilnehmen soll. --- = keine MD5= EAP-MD5 TLS = EAP-TLS TTLS= EAP-TTLS PEAP= PEAP FAST= EAP-FAST
auth_name [Benutzername]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert den Benutzernamen, mit dem der UTN-Server auf dem RADIUS-Server eingerichtet ist für die EAP-Authentifizierungsmethoden MD5, TTLS, PEAP und FAST.
auth_pwd [Passwort]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert das Passwort, mit dem der UTN-Server auf dem RADIUS-Server eingerichtet ist für die EAP-Authentifizierungsmethoden MD5, TTLS, PEAP und FAST.
auth_intern [Innere Authentifizierung]	--- PAP CHAP MSCHAP2 EMD5 ETLS	---	Definiert die Art der inneren Authentifizierung bei den EAP-Authentifizierungsmethoden TTLS, PEAP und FAST. --- = keine PAP = PAP CHAP = CHAP MSCHAP2= MS-CHAPv2 EMD5 = EAP-MD5 ETLS = EAP-TLS
auth_extern [PEAP/EAP-FAST-Optionen]	--- PLABEL0 PLABEL PVER0 PVER1 FPROV1	---	Definiert die Art der äußeren Authentifizierung bei den EAP-Authentifizierungsmethoden TTLS, PEAP und FAST. --- = keine PLABEL0= PEAPLABEL0 PLABEL1= PEAPLABEL1 PVER0 = PEAPVER0 PVER1 = PEAPVER1 FPROV1= FASTPROV1
auth_ano_name [Anonymer Name]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert den anonymen Namen für den unverschlüsselten Teil der EAP-Authentifizierungsmethoden TTLS, PEAP und FAST.
auth_wpa_addon [WPA-Add-on]	max. 255 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert eine optionale WPA-Erweiterung für die EAP-Authentifizierungsmethoden TTLS, PEAP und FAST.

Tabelle 34: Parameterliste – Sonstige

Parameter	Wertekonvention	Default	Beschreibung
utn_heartbeat	1–1800 [1–4 Zeichen; 0–9]	180	 **WARNUNG** Der Parameter ist ausschließlich in Absprache mit dem SEH Support zu verwenden.
utn_poffdura_1 ~ utn_poffdura_20	0–100 [1–3 Zeichen; 0–9]	0	 **WARNUNG** Der Parameter ist ausschließlich in Absprache mit dem SEH Support zu verwenden.
utn_prereset_1 ~ utn_prereset_20	on/off	off	 **WARNUNG** Der Parameter ist ausschließlich in Absprache mit dem SEH Support zu verwenden.

8.4 SEH UTN Manager – Funktionsübersicht

Welche Funktionen im SEH UTN Manager inaktiv (ausgegraut) sind ist abhängig von verschiedenen Faktoren:

- Auswahllisten-Modus
  - global
  - benutzerindividuell
- Client-Betriebssystem (Windows, macOS, Linux)
- Client-Benutzerkonto
  - Administrator oder Mitglieder der Gruppe 'utnusers'
  - Standardbenutzer oder Benutzer ohne Zugehörigkeit zur Gruppe 'utnusers'
- Schreibrecht auf die *.ini-Datei (Auswahlliste)

Ein Administrator kann sich diese Faktoren zu nutze machen, um für Anwender einen individuellen Funktionsumfang zusammenzustellen.

Die nachfolgende Tabelle gibt einen Überblick. Sie zeigt die grundsätzlich vorhandenen Funktionen. Zusätzlich werden einzelne Funktionen eventuell nicht oder inaktiv dargestellt, weil

- das UTN-Server-Modell sie nicht unterstützt
- das angeschlossene USB-Gerät die Funktion nicht unterstützt
- Sicherheitsmechanismen eingerichtet sind

Tabelle 35: SEH UTN Manager – Funktionsübersicht Linux

	Globale Auswahlliste		Benutzerindividuelle Auswahlliste		
	Administrator	Benutzer	Administrator	Benutzer (mit *.ini-Schreibrechten)	Benutzer (ohne *.ini-Schreibrechte)
Menü					
Auswahlliste – Bearbeiten	✓	×	✓	✓	×
Auswahlliste – Exportieren	✓	×	✓	×	×
Auswahlliste – Aktualisieren	✓	✓	✓	✓	✓
UTN-Server – Konfigurieren	✓	✓	✓	✓	✓
UTN-Server – IP-Adresse definieren	✓	✓	✓	✓	✓
UTN-Server – Auto-Connect aktivieren	✓	×	✓	×	×
UTN-Server – USB-Portschlüssel eingeben	✓	×	✓	✓	×
UTN-Server – Hinzufügen	✓	×	✓	✓	×
UTN-Server – Entfernen	✓	×	✓	✓	×
UTN-Server – Aktualisieren	✓	✓	✓	✓	✓
Port – Aktivieren	✓	✓	✓	✓	✓
Port – Deaktivieren	✓	✓	✓	✓	✓
Port – Anfordern	✓	✓	✓	✓	✓
Port – Entfernen	✓	×	✓	×	×
Port – Einstellungen	✓	✓	✓	✓	✓

	Globale Auswahlliste		Benutzerindividuelle Auswahlliste		
	Administrator	Benutzer	Administrator	Benutzer (mit *.ini-Schreibrechten)	Benutzer (ohne *.ini-Schreibrechte)
Schaltflächen					
Auswahlliste – Aktualisieren	✓	✓	✓	✓	✓
Auswahlliste – Bearbeiten	✓	×	✓	✓	×
Port – Aktivieren	✓	✓	✓	✓	✓
Port – Deaktivieren	✓	✓	✓	✓	✓
Dialog 'Programm – Optionen'					
Netzwerksuche – Multicastsuche	✓	×	✓	×	×
Netzwerksuche – Netzwerkbereichsuche	✓	×	✓	×	×
Programm – Programmmeldungen	✓	×	✓	×	×
Programm – Programm-Update	✓	×	✓	×	×
Automatismen – Auto-Disconnect	✓	×	✓	×	×
Auswahlliste – Auswahllisten-Modus	✓	×	✓	×	×
Auswahlliste – Automatische Aktualisierung	✓	×	✓	×	×
Dialog 'Porteinstellungen'					
Meldungen	✓	✓	✓	✓	✓

8.5 Index