SEH

USB Device Server

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

SDCardserver myUTN-120
Scannerserver myUTN-130
myUTN-150

Benutzerdokumentation

Hersteller:
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: http://www.seh.de

Scannen Sie diesen QR-Code (meCard) mit Ihrem Smartphone.

Dokument:
Typ: Benutzerdokumentation
Titel: USB Device Server
Version: 2.0

Online Links zu den wichtigsten Internet-Seiten:

Kostenlose Garantieverlängerung:	http://www.seh.de/guarantee
Support-Kontakte und Informationen:	http://www.seh.de/support
Vertriebskontakte und Informationen:	http://www.seh.de/sales
Downloads:	http://www.seh.de/services/downloads/myutn.html

Inhaltsverzeichnis

1 Allgemeine Information

In diesem Kapitel erhalten Sie Informationen zu Gerät und Dokumentation sowie Hinweise zu Ihrer Sicherheit. Sie erfahren, wie Sie Ihren UTN-Server optimal einsetzen und eine schnelle Funktionsbereitschaft herstellen.

Welche Information benötigen Sie?

1.1 myUTN

Verwendungszweck

myUTN (myUSB to Network) erlaubt das Bereitstellen von nicht-netzwerkfähigen USB-Geräten (z.B. Festplatten, Drucker usw.) für mehrere Netzwerkteilnehmer. Dazu werden die USB-Geräte an den USB-Port des UTN-Servers angeschlossen.

Der 'Dongleserver' (myUTN-80) ist ausschließlich für die Bereitstellung von USB-Dongles konzipiert.

Der 'Scannerserver' (myUTN-130) ist ausschließlich für die Bereitstellung von USB-Scannern konzipiert.

Die Zugriffsverteilung der USB-Geräte erfolgt über das Software-Tool 'SEH UTN Manager'. Die Software wird auf alle Clients installiert, die auf ein im Netzwerk bereitgestelltes USB-Gerät zugreifen sollen. Der SEH UTN Manager zeigt die Verfügbarkeit aller im Netzwerk eingebundenen USB-Geräte an und stellt die Verbindung zwischen Client und USB-Gerät her.

Systemvoraussetzungen

myUTN ist konzipiert für den Einsatz in TCP/IP-basierten Netzwerken. Der SEH UTN Manager ist für den Einsatz in folgenden Systemen konzipiert:

- Windows XP und höher
- Mac OS X 10.6.x, Mac OS X 10.7.x (64-Bit), OS X 10.8.x

Ablauf und Funktionsweise

Nach dem Start des SEH UTN Managers wird das Netzwerk nach angeschlossenen UTN-Servern gescannt. Der zu scannende Netzwerkbereich ist frei definierbar. Nach dem Scannen des Netzwerks werden alle gefundenen UTN-Server und deren angeschlossene Geräte in der 'Netzwerkliste' angezeigt. Die benötigten Geräte werden ausgewählt und der 'Auswahlliste' hinzugefügt. Die in der Auswahlliste aufgeführten Geräte können dann mit dem Client verbunden werden.

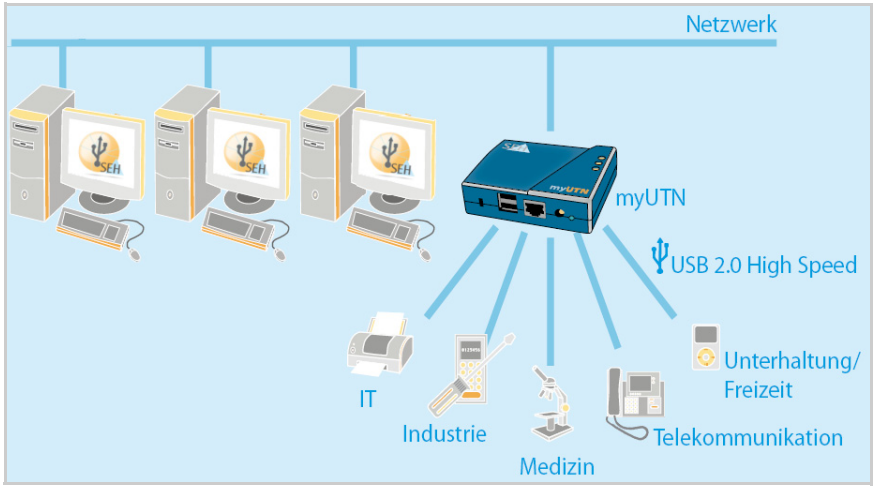


Abb. 1: UTN-Server im Netzwerk

1.2 Dokumentation

Beschreibungsumfang und Inhalte

Diese Dokumentation beschreibt mehrere Varianten des USB Deviceservers, den Dongleserver, den Scannerserver sowie den SDCardserver. Das hat zur Folge, dass zum Teil Funktionen beschrieben werden, die nicht dem Leistungsumfang Ihres Produktes entsprechen. Abbildungen können von Ihrem Gerät abweichen.

Informationen zum Leistungsumfang Ihres Produktes entnehmen Sie dem Datenblatt Ihres UTN-Server-Modells. Bitte beachten Sie die folgenden sprachlichen Einordnungen der Produktbezeichnungen in dieser Dokumentation:

- USB Deviceserver → UTN-Server
- Dongleserver → UTN-Server
- Scannerserver → UTN-Server
- SDCardserver → UTN-Server
- Dongle → USB-Gerät
- SD-Card-Reader → USB-Gerät
- USB-Scanner → USB-Gerät

Aufbau der Dokumentation

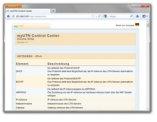
Die myUTN-Dokumentation besteht aus den folgenden Dokumenten:

PDF

Benutzerdokumentation
Detaillierte Beschreibung der myUTN-Konfiguration und -Administration.

Print PDF

Quick Installation Guide
Informationen zur Sicherheit, Hardware-Installation sowie zur Inbetriebnahme.



HTML

Online Hilfe (myUTN Control Center)
Die Online Hilfe enthält detaillierte Informationen zur Bedienung des 'myUTN Control Center'.

HTML

Online Hilfe (SEH UTN Manager)
Die Online Hilfe enthält detaillierte Informationen zur Bedienung des Software-Tools 'SEH UTN Manager'.

Merkmale dieses Dokumentes

Diese Dokumentation ist als elektronisches Dokument für die Betrachtung am Bildschirm konzipiert. Viele Anzeigeprogramme (z.B. Adobe® Reader®) verfügen über eine Lesezeichen-Funktion, in deren Fenster die gesamte inhaltliche Struktur des Dokumentes dargestellt wird.

Dieses Dokument enthält Verknüpfungen (Hyperlinks), über die Sie mit einem Mausklick zusammenhängende Informationseinheiten anzeigen lassen können. Zum Ausdrucken dieser Dokumentation empfehlen wir die Druckereinstellung 'Duplex' oder 'Heft bzw. Buch'.

Fachbegriffe in diesem Dokument

In diesem Dokument sind Erläuterungen von Fachbegriffen in einem Glossar zusammengefasst. Das Glossar bietet einen schnellen Überblick über technische Zusammenhänge und Hintergrundinformationen; siehe: ⇨ 116.

Symbole und Auszeichnungen

Innerhalb dieses Dokumentes finden Sie verschiedene Symbole und Auszeichnungen. Entnehmen Sie deren Bedeutung der Tabelle:

Tabelle 1: Konventionen in der Dokumentation

Symbol / Auszeichnung	Beschreibung
 **Warnung**	Ein Warnhinweis enthält wichtige Informationen, die Sie unbedingt beachten müssen. Nichtbeachtung kann zu Fehlfunktionen führen.
 Hinweis	Ein Hinweis enthält Informationen, die Sie beachten sollten.
 Gehen Sie wie folgt vor: 1. *Markieren Sie ...*	Das Hand-Symbol leitet eine Handlungsanweisung ein. Einzelne Handlungsschritte sind kursiv dargestellt.
 Bestätigung	Der Pfeil bestätigt die Auswirkung einer ausgeführten Handlung.
☑ Voraussetzung	Ein Haken kennzeichnet Bedingungen, die erfüllt sein müssen, bevor Sie mit einer Handlung beginnen.
☐ Option	Ein Quadrat weist Sie auf unterschiedliche Verfahren und Varianten hin, die Sie durchführen können.
•	Blickfangpunkte kennzeichnen Aufzählungen.
	Das Zeichen signalisiert die inhaltliche Zusammenfassung eines Kapitel.
⇨ 	Der Pfeil symbolisiert einen Verweis auf eine Seite innerhalb dieses Dokuments. Im PDF-Dokument kann durch einen einfachen Mausklick auf das Symbol die Seite angesprochen werden.
Fett	Feststehende Bezeichnungen (z.B. von Schaltflächen oder Menüpunkten) sind fett ausgezeichnet.
`Courier`	Kommandozeilen sind im Schrifttyp Courier dargestellt.
'Eigennamen'	Eigennamen sind in Anführungszeichen gesetzt

1.3 Support und Service

Support

Falls Sie noch Fragen haben, kontaktieren Sie unsere Hotline. Die SEH Computertechnik GmbH bietet einen umfassenden Support.

	Montag - Donnerstag Freitag	8:00–16:45 Uhr und 8:00–15:15 Uhr (CET)
	+49 (0)521 94226-44	
	support@seh.de	

Aktuelle Services

Folgende Services finden Sie auf der SEH Computertechnik GmbH-Homepage http://www.seh.de/ :

- aktuelle Firmware/Software
- aktuelle Tools
- aktuelle Dokumentationen
- aktuelle Produktinfomationen
- Produktdatenblätter
- u.v.m.

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.

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

Bestimmungsgemäße Verwendung

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

Bestimmungswidrige Verwendung

Alle Verwendungen des Gerätes, die den in der myUTN-Dokumentation beschriebenen Funktionalitäten nicht entsprechen, sind bestimmungswidrig. Eigenmächtige konstruktive Veränderungen an Hardware oder Software sowie Reparaturversuche am Gerät sind verboten.

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:

Dies ist ein Warnhinweis!

1.5 Erste Schritte

In diesem Abschnitt erhalten Sie alle notwendigen Informationen, um eine schnelle Funktionsbereitschaft herzustellen.

Gehen Sie wie folgt vor:

1. *Lesen und beachten Sie die Sicherheitsinformationen, um Schaden an Personen und Gerät zu vermeiden; siehe:* ⇨ 12.
2. *Führen Sie die Hardware-Installation aus. Die Hardware-Installation beinhaltet das Anschließen des UTN-Servers an Netzwerk, USB-Geräte und Stromnetz; siehe: 'Quick Installation Guide'.*
3. *Stellen Sie sicher, dass eine IP-Adresse im UTN-Server gespeichert ist; siehe:* ⇨ 14.
4. *Installieren und starten Sie das Software-Tool 'SEH UTN Manager' auf Ihrem Client; siehe:* ⇨ 21.
5. *Fügen Sie der Auswahlliste die Geräte hinzu, die Sie nutzen möchten; siehe:* ⇨ 64.
6. *Aktivieren Sie die Verbindung zwischen Client und USB-Gerät; siehe:* ⇨ 65.

Die Verbindung wird hergestellt. Das USB-Gerät kann vom Client genutzt werden.

1.6 Speichern der IP-Adresse im UTN-Server

Wozu eine IP-Adresse?

Eine IP-Adresse dient zur Adressierung von Netzwerkgeräten in einem IP-Netzwerk. Im Rahmen des TCP/IP-Netzwerkprotokolls ist es erforderlich, eine IP-Adresse im UTN-Server zu speichern, damit das Gerät im Netzwerk angesprochen werden kann.

Wie erhält der UTN-Server eine IP-Adresse?

Der UTN-Server ist in der Lage, sich während der Erstinstallation selbst eine IP-Adresse zuzuweisen. Der UTN-Server verfügt über Bootprotokolle zur automatischen IP-Adresszuweisung. Im Auslieferungszustand sind die Bootprotokolle 'BOOTP' und 'DHCP' standardmäßig aktiviert.

Nachdem der UTN-Server an das Netzwerk angeschlossen ist, überprüft der UTN-Server, ob er eine IP-Adresse über die Bootprotokolle BOOTP oder DHCP erhält. Ist das nicht der Fall, gibt sich der UTN-Server selbst eine IP-Adresse aus dem für ZeroConf reservierten Adressbereich (169.254.0.0/16).

Nachdem der UTN-Server eine IP-Adresse automatisch über ein Bootprotokoll erhalten hat, können Sie nachträglich manuell eine freidefinierbare IP-Adresse im UTN-Server speichern. Die zugewiesene IP-Adresse des UTN-Servers kann über die Software-Tools 'SEH UTN Manager' und 'InterCon-NetTool' ermittelt und verändert werden; siehe: ⇨🗎18.

Nachfolgend sind die verschiedenen Methoden zur IP-Adressenvergabe beschrieben.

Automatische Methoden zur IP-Adressenvergabe

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

Manuelle Methoden zur IP-Adressenvergabe

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

ZeroConf

Erhält der UTN-Server keine IP-Adresse über Bootprotokolle, gibt sich der UTN-Server über ZeroConf selbst eine IP-Adresse. Hierzu wählt der UTN-Server zufällig eine IP-Adresse aus dem reservierten Adressbereich (169.254.0.0/16).

Zur Namensauflösung der IP-Adresse kann der Domain Name Service von Bonjour verwendet werden; siehe: ⇨ 43.

BOOTP

Der UTN-Server unterstützt BOOTP, so dass über einen BOOTP-Server die IP-Adresse des UTN-Servers vergeben werden kann.

Voraussetzung

☑ Der Parameter 'BOOTP' ist aktiviert; siehe: ⇨ 36.

☑ Im Netzwerk ist ein BOOTP-Server vorhanden.

Ist der UTN-Server angeschlossen, erfragt der UTN-Server beim BOOTP-Host die IP-Adresse und den Hostnamen. Der BOOTP-Host sendet als Antwort ein Datenpaket mit der IP-Adresse. Die IP-Adresse wird im UTN-Server gespeichert.

DHCP

Der UTN-Server unterstützt DHCP, so dass einfach und bequem über einen DHCP-Server die IP-Adresse des UTN-Servers dynamisch vergeben werden kann.

Voraussetzung

☑ Der Parameter 'DHCP' ist aktiviert; siehe: ⇨ 36.

☑ Im Netzwerk ist ein DHCP-Server vorhanden.

Nach der Hardware-Installation erfragt der UTN-Server per Broadcast-Umfrage, ob ihm ein DHCP-Server eine IP-Adresse zuteilen kann. Der DHCP-Server identifiziert den UTN-Server anhand seiner Hardware-Adresse und sendet ein Datenpaket an den UTN-Server.

Dieses Datenpaket enthält u.a. die IP-Adresse des UTN-Servers, das Standard-Gateway und die IP-Adresse des DNS-Servers. Diese Daten werden im UTN-Server gespeichert.

Autokonfiguration (IPv6-Standard)

Der UTN-Server kann zeitgleich über eine IPv4-Adresse und mehrere IPv6-Adressen verfügen. Der IPv6-Standard sieht eine automatische Vergabe von IP-Adressen in IPv6-Netzwerken vor. Wird der UTN-Server in einem IPv6-fähigen Netzwerk angeschlossen, erhält der UTN-Server automatisch eine zusätzliche 'link-local'-IP-Adresse aus dem IPv6-Adressbereich.

Mit Hilfe der 'link-local'-IP-Adresse hält der UTN-Server Ausschau nach einem Router. Der UTN-Server sendet sogenannte 'Router Solicitations' (RS) an die spezielle Multicast-Adresse FF02::2, worauf ein vorhandener Router ein 'Router Advertisement' (RA) mit den benötigten Informationen zurückschickt.

Mit einem Präfix aus dem Bereich der global eindeutigen Adressen kann sich der UTN-Server seine Adresse selbst zusammensetzen. Er ersetzt einfach die ersten 64 Bit (Präfix FE80::) mit dem im RA verschickten Präfix.

Voraussetzung

☑ Der Parameter 'IPv6' ist aktiviert.

☑ Der Parameter 'Automatische Konfiguration' ist aktiviert.

Um die Vergabe von IPv6-Adressen zu konfigurieren, siehe: ⇨ 39.

InterCon-NetTool

Das InterCon-NetTool ist eine von der SEH Computertechnik GmbH entwickelte Software zur Administration von SEH Netzwerkgeräten. Der IP-Assistent des InterCon-NetTools hilft bei der Konfiguration von TCP/IP-Parametern, wie z.B. der IP-Adresse. Über den IP-Assistenten kann die gewünschte IPv4-Adresse manuell eingegeben und im UTN-Server gespeichert werden. Um eine IPv4-Adresse via InterCon-NetTool zu konfigurieren, siehe: ⇨ 38.

SEH UTN Manager

Über den SEH UTN Manager kann die gewünschte IPv4-Adresse manuell eingegeben und im UTN-Server gespeichert werden. Um eine IPv4-Adresse via SEH UTN Manager zu konfigurieren, siehe: ⇨ 37.

myUTN Control Center

Über das myUTN Control Center kann die gewünschte IP-Adresse manuell eingegeben und im UTN-Server gespeichert werden.

- Um eine **IPv4**-Adresse via myUTN Control Center zu konfigurieren, siehe: ⇨📄37.
- Um eine **IPv6**-Adresse via myUTN Control Center zu konfigurieren, siehe: ⇨📄39.

ARP/PING

Die Zuordnung von der IP-Adresse zur Hardware-Adresse kann über die ARP-Tabelle erfolgen. Die ARP-Tabelle ist eine systeminterne Datei, in der die Zuordnung temporär (ca. 15 Min.) gespeichert wird. Diese Tabelle wird vom ARP-Protokoll verwaltet.

Mit Hilfe der Befehle 'arp' und 'ping' kann die IP-Adresse im UTN-Server gespeichert werden. Verfügt der UTN-Server bereits über eine IP-Adresse, kann mit den Befehlen 'arp' und 'ping' keine neue IP-Adresse gespeichert werden.

Eine IP-Adresse aus dem für ZeroConf reservierten Adressbereich (169.254.0.0/16) kann jedoch mit 'arp' und 'ping' überschrieben werden.

Der Befehl 'arp' dient zum Editieren der ARP-Tabelle. Der Befehl 'ping' versendet ein Datenpaket mit der IP-Adresse an die Hardware-Adresse des UTN-Servers. Bei Empfang des Datenpaketes speichert der UTN-Server seine IP-Adresse dauerhaft ab.

Die Implementierung der Befehle 'arp' und 'ping' ist systemabhängig. Lesen Sie die Dokumentation zu Ihrem Betriebssystem.

Voraussetzung

☑ Der Parameter 'ARP/PING' ist aktiviert; siehe: ⇨📄37.

Ändern Sie die ARP-Tabelle:
Syntax: `arp -s <IP-Adresse><Hardware-Adresse>`
Beispiel: `arp -s 192.168.0.123  00-c0-eb-00-01-ff`

Weisen Sie dem UTN-Server eine neue IP-Adresse zu:
Syntax: `ping <IP-Adresse>`
Beispiel: `ping 192.168.0.123`

2 Administrationsmethoden

Sie können den UTN-Server auf unterschiedliche Weise administrieren und konfigurieren. In diesem Kapitel erhalten Sie eine Übersicht über die verschiedenen Administrationsmöglichkeiten.

Sie erfahren, unter welchen Voraussetzungen die Methoden verwendet werden können und welche Funktionalitäten die jeweilige Methode unterstützt.

Welche Information benötigen Sie?

- 'Administration via myUTN Control Center' ⇨ 19
- 'Administration via SEH UTN Manager' ⇨ 21
- 'Administration via InterCon-NetTool' ⇨ 29
- 'Administration via E-Mail (nur myUTN-80 und höher)' ⇨ 32
- 'Administration via Reset-Taster am Gerät' ⇨ 35

2.1 Administration via myUTN Control Center

Welche Funktionen werden unterstützt?

Das myUTN Control Center umfasst alle Funktionalitäten zur Administration und Überwachung Ihres UTN-Servers.

Das myUTN Control Center ist in dem UTN-Server gespeichert und kann mit einer Browsersoftware (Internet Explorer, Mozilla Firefox, Safari) dargestellt werden.

Voraussetzung

☑ Der UTN-Server ist an Netzwerk und Netzspannung angeschlossen.

☑ Der UTN-Server hat eine gültige IP-Adresse.

myUTN Control Center starten

Gehen Sie wie folgt vor:

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

Das **myUTN Control Center** erscheint.

Falls das myUTN Control Center nicht angezeigt wird, überprüfen Sie die Proxy-Einstellungen des Browsers.

Zusätzlich kann das myUTN Control Center über die Software-Tools 'SEH UTN Manager' und 'InterCon-NetTool' gestartet werden.

- Um das myUTN Control Center über das InterCon-NetTool zu starten, markieren Sie den UTN-Server in der Geräteliste und wählen Sie im Menü **Aktionen** den Befehl **Browser starten**.
- Um das myUTN Control Center über den SEH UTN Manager zu starten, markieren Sie den UTN-Server in der Auswahlliste und wählen Sie im Menü **UTN-Server** den Befehl **Konfigurieren**.

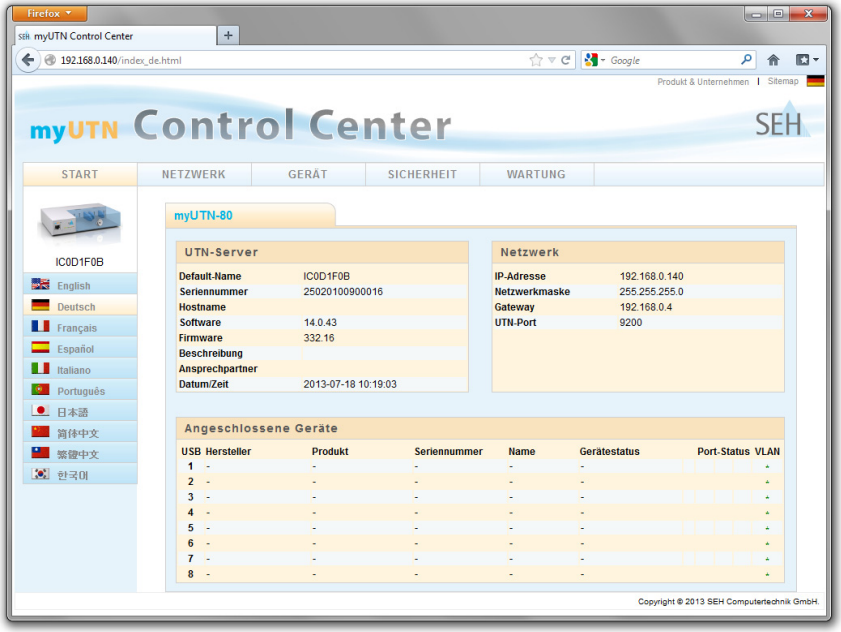


Abb. 2: myUTN Control Center - START

Aufbau des myUTN Control Centers

In der Navigationsleiste (oben) befinden sich die verfügbaren Menüpunkte. Nach dem Anwählen eines Menüpunkts (einfacher Mausklick) werden auf der linken Seite die verfügbaren Untermenüpunkte angezeigt. Nach dem Anwählen eines Untermenüs wird die entsprechende Seite mit den Menüinhalten dargestellt (rechts).

Über den Menüpunkt **START** können Sie die Sprache einstellen. Wählen Sie hierzu das entsprechende Flaggensymbol an.

Über den Punkt **Produkt & Unternehmen** werden die Kontaktdaten des Herstellers sowie weiterführende Informationen zum Produkt angezeigt. Über den Punkt **Sitemap** erhalten Sie eine Übersicht und direkten Zugriff auf alle Seiten des myUTN Control Centers.

Alle anderen Menüpunkte beziehen sich auf die Konfiguration des UTN-Servers. Die Menüpunkte sind in der Online Hilfe des myUTN Control Centers beschrieben. Um die Online Hilfe zu starten, wählen Sie das ? -Symbol an.

2.2 Administration via SEH UTN Manager

Einsatzbereich

Die Zugriffsverteilung der USB-Geräte erfolgt über das Software-Tool 'SEH UTN Manager'. Der SEH UTN Manager zeigt die Verfügbarkeit aller im Netzwerk eingebundenen UTN-Server mitsamt USB-Geräten an und stellt die Verbindung zwischen Client und USB-Gerät her. Die Software wird auf alle Clients installiert, die auf ein im Netzwerk bereitgestelltes USB-Gerät zugreifen sollen.

Funktionsweise

Nach dem Start des SEH UTN Managers wird das Netzwerk nach angeschlossenen UTN-Servern gescannt. Der zu scannende Netzwerkbereich ist frei definierbar.

Nach dem Netzwerkscan werden alle gefundenen UTN-Server und deren angeschlossene Geräte in der 'Netzwerkliste' angezeigt. Die benötigten Geräte werden ausgewählt und der 'Auswahlliste' hinzugefügt. Die in der Auswahlliste aufgeführten Geräte können konfiguriert oder mit dem Client verbunden werden.

Automatismen

Der SEH UTN Manager unterstützt u.a. die folgenden Automatismen:

- **Autostart**: Der SEH UTN Manager startet sofort, wenn der Rechner des Anwenders gestartet wird.
- **Auto-Connect**: Die Funktion ermöglicht das automatische Aktivieren einer Geräteverbindung nach Programmstart des SEH UTN Managers.
- **Auto-Disconnect**: Die Funktion ermöglicht das automatische Trennen einer Geräteverbindung nach einem definierten Zeitraum.
- **Print-On-Demand**: Zwischen USB-Gerät (Drucker oder MFG) und Client wird, sobald ein Druckauftrag anliegt, automatisch eine Verbindung hergestellt. Nach Beendigung des Druckauftrages wird die Verbindung automatisch deaktiviert.
- **UTN Aktion erstellen**: UTN Aktionen sind kleine Programme, die zum automatischen Aktivieren und Deaktivieren von Geräteverbindungen verwendet werden. Auch das Starten und

Beenden einer Applikation in Kombination mit einer Geräteverbindung kann durch eine UTN Aktion automatisiert werden.

- **Zusatztool 'utnm'**: Das Tool wird verwendet zum Aktivieren und Deaktivieren von USB-Geräten. Dies erfolgt über Befehle, die in die Kommandozeile des Betriebssystems eingegeben und ausgeführt werden. Alternativ wird ein Skript geschrieben.

SEH UTN Manager-Varianten

Der SEH UTN Manager ist in zwei Varianten verfügbar:

- **Vollständige Variante**
- **Minimal-Variante** (ohne grafische Bedienoberfläche)

Wodurch unterscheiden sich die Varianten?

Wesentlicher Unterschied der vollständigen Variante ist die grafische Bedienoberfläche. Sie stellt das Programm mittels bildlicher Elemente dar und bietet zusätzliche Funktionen: UTN-Server suchen und verwalten, einfacheres Verwenden von USB-Geräten u.v.m.

In der Minimal-Variante kann der SEH UTN Manager nur über die Kommandozeile und UTN Aktionen verwendet werden. Die Minimal-Variante eignet sich z.B.

- um Benutzern nur bestimmte Geräte mit vereinfachter De-/aktivierung bereitzustellen; siehe: 'UTN Aktion erstellen: Automatisierte Geräteverbindungen und Programmstarts ohne SEH UTN Manager-Oberfläche' ⇨ 72.
- um das De-/aktivieren von USB-Geräten zu automatisieren (mit Skripten); siehe: 'Zusatztool 'utnm'' ⇨ 145.

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' im Hintergrund und ist nach Systemstart automatisch aktiv. Der Dienst kann über die üblichen Administrationsmethoden gesteuert werden.

Es wird zudem zwischen den folgenden Benutzergruppen unterschieden:

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

Die Funktionen **Auto-Connect, Auto-Disconnect** und **Print-On-Demand** können ausschließlich durch Benutzer mit administrativen Rechten konfiguriert werden.

Installation und Programmstart

Um mit dem SEH UTN Manager zu arbeiten, muss das Programm auf einem Rechner mit einem Windows- oder Mac OS X-Betriebssystem installiert werden. Je nach Betriebssystem sind verschiedene Installationsdateien verfügbar. Sie finden die SEH UTN Manager-Installationsdatei auf der SEH Computertechnik GmbH-Homepage:

http://www.seh.de/services/downloads/myutn.html

Die Installationsdatei enthält beide Varianten des SEH UTN Managers. Die bevorzugte Variante kann über die Installationsroutine ausgewählt werden.

Unter Windows kann zudem eine unbeaufsichtigte Installation durchgeführt werden.

Windows

Für Windows-Systeme ist die Installationsdatei in dem Format '*.exe' verfügbar.

Systemvoraussetzung

☑ Die Installation des SEH UTN Managers ist für Windows XP und höher geeignet.

☑ Die Installation kann ausschließlich durch Benutzer mit administrativen Rechten durchgeführt werden.

Gehen Sie wie folgt vor:

1. *Starten Sie die SEH UTN Manager-Installationsdatei.*

2. *Folgen Sie der Installationsroutine.*

↳ Der SEH UTN Manager wird auf Ihrem Client installiert.

Beim Einsatz in serverbasierten Umgebungen (Citrix XenApp, Microsoft Remote Desktop Services/Terminal Services) und virtualisierten Umgebungen (VMware, Citrix XenDesktop, Microsoft HyperV usw.) können dem Windows-System benötigte Treiber fehlen. Die Installationsroutine überprüft während des Installationsvorgang die vorhandenen Treiber. Bei fehlenden Treibern startet ein weiterer Installer ('USB driver for SEH UTN Manager'). Dieser leitet die Installation der benötigten Treiber ein.

Zum Starten des SEH UTN Managers doppelklicken Sie auf das SEH UTN Manager-Symbol . Sie finden das Symbol auf dem Desktop oder im Windows-Startmenü.
(Start → Alle Programme → SEH Computertechnik GmbH → SEH UTN Manager)

In einigen Fällen verlangt die Windows-Benutzerkontensteuerung eine Bestätigung, wenn der SEH UTN Manager ausgeführt werden soll.

Mac OS X

Für Mac-Systeme ist die Installationsdatei in dem Format '*.pkg' verfügbar.

Systemvoraussetzung

☑ Die Installation des SEH UTN Managers ist für Mac OS X 10.6.x, Mac OS X 10.7.x (64-Bit) und OS X 10.8.x geeignet.

☑ Die Installation kann ausschließlich durch Benutzer mit administrativen Rechten durchgeführt werden.

Gehen Sie wie folgt vor:

1. *Starten Sie die SEH UTN Manager-Installationsdatei.*
2. *Folgen Sie der Installationsroutine.*

↳ Der SEH UTN Manager wird auf Ihrem Client installiert.

Zum Starten des SEH UTN Managers doppelklicken Sie auf die Datei 'SEH UTN Manager.app' .
(Programme → SEH UTN Manager.app)

Unbeaufsichtigte Installation (Windows)

Eine unbeaufsichtigte Installation läuft ohne Benutzereingaben ab. Es werden die folgenden Standardeinstellungen verwendet:

- Vollständige Variante
- Installation für alle Benutzer des Clients
- Zielverzeichnis: `%PROGRAMFILES%\SEH Computertechnik GmbH\SEH UTN Manager`
  (Wobei `%PROGRAMFILES%` eine Umgebungsvariable von Windows für den Ordner 'Programme' ist. Mit Hilfe der Kommandozeile kann der Pfad folgendermaßen ermittelt werden: echo `%PROGRAMFILES%`)

Nutzen und Zweck

Unbeaufsichtigte Installationen laufen zeitsparend ab. Via Loginskript kann der SEH UTN Manager auf einer großen Anzahl von Clients automatisch installiert werden; lesen Sie hierzu die Dokumentation Ihres Betriebssystems.

Systemvoraussetzung

☑ Die Installation des SEH UTN Managers ist für Windows XP und höher geeignet.

☑ Die Installation kann ausschließlich durch Benutzer mit administrativen Rechten durchgeführt werden.

Indem Sie den SEH UTN Manager installieren, akzeptieren Sie automatisch die SEH Computertechnik GmbH-Vereinbarung hinsichtlich Lizenz und Nutzung der Software. Sie können die Vereinbarung auf der SEH Computertechnik GmbH-Homepage einsehen:
http://www.seh.de/services/lizenzen/software-lizenzvertrag.html

Gehen Sie wie folgt vor:

1. *Öffnen Sie die Kommandozeile.*
2. *Wechseln Sie in das Verzeichnis mit der SEH UTN Manager-Installationsdatei.*

3. *Geben Sie die Befehlsfolge ein; siehe 'Syntax und Befehle' ⇨ 26.*
4. *Bestätigen Sie die Eingabe.*

↳ Die Befehlsfolge wird ausgeführt.

Syntax und Befehle

Beachten Sie die folgende Syntax.

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

Folgende Befehle werden unterstützt:

Befehl	Beschreibung
`/S`	Führt die Installationsroutine ohne Rückfragen/Meldungen/Hinweise aus (keine Bildschirmausgabe).
`/U`	Aktualisiert eine vorhandene Installation (Update).
`/Srv`	Installiert die Minimal-Variante (ohne grafische Bedienoberfläche).
`/?`	Zeigt die Hilfeseite an.

Die Befehle müssen zwingend großgeschrieben werden.

Variantenwechsel

Ist auf Ihrem System eine Variante des SEH UTN Managers installiert und Sie möchten auf eine andere Variante umsteigen, ist zunächst die vorhandene Variante zu deinstallieren.

Update

Sie haben die Möglichkeit, sich über den Update-Status des SEH UTN Managers informieren zu lassen. Ist ein Update verfügbar, kann die Installationsdatei auf den Rechner kopiert und das Programm installiert werden. Bei Updates werden die Voreinstellungen entsprechend der vorhandenen Variante angepasst.

Programmaufbau

Nach dem Programmstart wird der Hauptdialog mit den folgenden Dialogelementen angezeigt. Die Darstellung kann variieren, da Elemente individuell ein- bzw. ausgeblendet werden können.

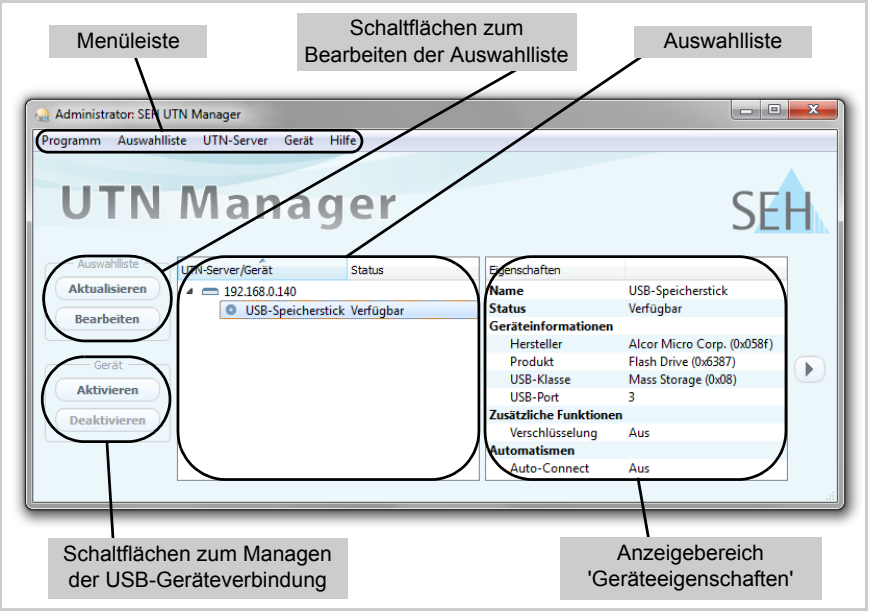


Abb. 3: SEH UTN Manager - Hauptdialog

Welche Funktionen werden unterstützt?

Über den SEH UTN Manager können Sie u.a.

- 'USB-Geräte der Auswahlliste hinzufügen' ⇨ 64
- 'USB-Gerät mit Client verbinden' ⇨ 65
- 'USB-Gerät und Client trennen' ⇨ 66
- 'belegte USB-Geräte anfordern' ⇨ 67
- 'Geräteverbindungen und Programmstars automatisieren' ⇨ 68
- 'UTN-Servern eine IPv4-Adresse zuweisen' ⇨ 37
- 'myUTN Control Center starten' ⇨ 19
- 'Zugriff auf gesperrte USB-Geräte freischalten' ⇨ 89
- 'Auswahllisten für mehrere Teilnehmer verwalten' ⇨ 75

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

Im SEH UTN Manager können Funktionen gar nicht oder als inaktiv dargestellt werden. Dieses steht in Abhängigkeit zu

- dem eingebundenen UTN-Server-Modell
- dem Typ und dem Speicherort der Auswahlliste
- den Benutzerrechten auf dem Client
- den Einstellungen der produkteigenen Sicherheitsmechanismen

Für weitere Informationen, siehe: 'SEH UTN Manager - Funktionsübersicht' ⇨ 138.

2.3 Administration via InterCon-NetTool

Das InterCon-NetTool ist eine von der SEH Computertechnik GmbH entwickelte Software zur Administration von SEH Netzwerkgeräten (Printserver, TPG, ISD, UTN-Server usw.). Über das InterCon-NetTool lassen sich je nach Netzwerkgerät verschiedene Funktionalitäten konfigurieren.

Funktionsweise

Nach dem Start des InterCon-NetTools wird das Netzwerk nach angeschlossenen Netzwerkgeräten gescannt. Der zu scannende Netzwerkbereich ist frei definierbar. Nach dem Scannen werden alle gefundenen Netzwerkgeräte in der 'Geräteliste' angezeigt.

Die Ansicht der Geräteliste kann verändert und so Ihren individuellen Bedürfnissen angepasst werden. Die in der Geräteliste aufgeführten Geräte können markiert und konfiguriert werden.

Installation und Programmstart

Um mit dem InterCon-NetTool zu arbeiten, muss das Programm auf einem Rechner mit einem Windows- oder Mac OS X-Betriebssystem installiert werden. Je nach Betriebssystem sind verschiedene Installationsdateien verfügbar. Sie finden die InterCon-NetTool-Installationsdatei auf der SEH Computertechnik GmbH-Homepage:

http://www.seh.de/services/downloads/myutn.html

Windows

Für Windows-Systeme ist die Installationsdatei in dem Format '*.exe' verfügbar.

Gehen Sie wie folgt vor:

1. *Starten Sie die InterCon-NetTool-Installationsdatei.*
2. *Wählen Sie die gewünschte Sprache.*
3. *Folgen Sie der Installationsroutine.*

↳ Das InterCon-NetTool wird auf Ihrem Client installiert.

Zum Starten des InterCon-NetTools doppelklicken Sie auf das InterCon-NetTool-Symbol  . Sie finden das Symbol auf dem Desktop oder im Windows-Startmenü.
(Start → Alle Programme → SEH Computertechnik GmbH → InterCon-NetTool)

Die InterCon-NetTool-Einstellungen werden in der Datei 'NetTool.ini' gespeichert. Diese ist im Benutzerordner des gerade angemeldeten Benutzers abgelegt.

Mac OS X

Für Mac-Systeme ist die Installationsdatei in dem Image-Datenformat '*.dmg' verfügbar.

Gehen Sie wie folgt vor:

1. *Öffnen Sie die InterCon-NetTool Installationsdatei.*
   Der Dateiinhalt wird angezeigt.
2. *Starten Sie die '*.pkg'-Datei.*
3. *Folgen Sie der Installationsroutine.*

Das InterCon-NetTool wird auf dem System installiert.

Zum Starten des InterCon-NetTools doppelklicken Sie auf die Datei 'Intercon-nettool.app'  .

Die Programmeinstellungen werden in der Datei 'InterCon-NetTool.ini' gespeichert. Diese ist im Verzeichnis `/Benutzer/<Benutzername>/Library/Preferences/InterCon-NetTool` abgelegt.

Aufbau des InterCon-NetTools

Nach dem Programmstart wird der Hauptdialog mit den folgenden Dialogelementen angezeigt. Die Darstellung kann variieren, da Elemente individuell ein- bzw. ausgeblendet werden können.

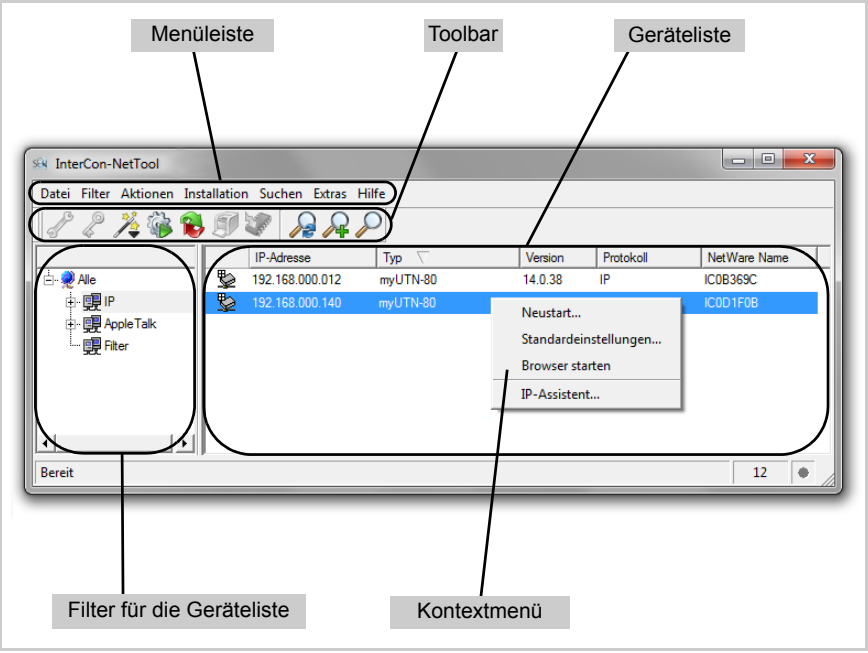


Abb. 4: InterCon-NetTool - Hauptdialog

Welche Funktionen werden unterstützt?

Über das InterCon-NetTool können Sie

- dem 'UTN-Server eine IPv4-Adresse zuweisen' ⇨🗎38
- den 'UTN-Server neu starten' ⇨🗎114
- die 'Parameterwerte des UTN-Servers auf die Standardeinstellung zurücksetzen' ⇨🗎111
- das 'myUTN Control Center starten' ⇨🗎19
- vom 'BIOS-Modus in den Standardmodus wechseln' ⇨🗎141

Detaillierte Informationen zur Bedienung des InterCon-NetTools entnehmen Sie der Online Hilfe. Um die Online Hilfe zu starten, wählen Sie im Menü **Hilfe** den Befehl **Online Hilfe**.

2.4 Administration via E-Mail (nur myUTN-80 und höher)

Sie haben die Möglichkeit, den UTN-Server über E-Mail und somit von jedem internetfähigen Rechner aus zu administrieren.

Funktionalitäten

Mit einer E-Mail können Sie

- UTN-Server-Statusinformationen senden lassen,
- UTN-Server-Parameter definieren oder
- ein Update auf dem UTN-Server durchführen.

Voraussetzung

☑ Auf dem UTN-Server ist ein DNS-Server konfiguriert; siehe: ⇨ 41.

☑ 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; siehe: ⇨ 45.

Anweisung via E-Mail versenden

Um den UTN-Server zu administrieren, geben Sie in die Betreffzeile einer E-Mail entsprechende Anweisungen ein.

Gehen Sie wie folgt vor:

1. *Öffnen Sie ein E-Mail-Programm.*
2. *Erstellen Sie eine neue E-Mail.*
3. *Geben Sie als Adressat die UTN-Server-Adresse ein.*
4. *Geben Sie eine Anweisung in die Betreffzeile ein; siehe: 'Syntax und Format der Anweisung' ⇨ 33.*
5. *Versenden Sie die E-Mail.*

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

Syntax und Format der Anweisung

Beachten Sie für die Anweisungen in der Betreffzeile die folgende Syntax:

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

Folgende Kommandos werden unterstützt:

Kommandos	Option	Beschreibung
<command>	get status	Sendet die Statusseite des UTN-Servers
	get parameters	Sendet die Parameterliste des UTN-Servers
	set parameters	Sendet Parameter zum UTN-Server. Syntax und Wertekonventionen entnehmen Sie der Parameterliste; siehe: ⇨ 119. Parameter und Wert sind in den E-Mail-Textkörper zu schreiben.
	update utn	Führt automatisch ein Update mit der in der Mail angehängten Software durch.
	help	Sendet eine Seite mit Informationen zur Fernwartung.
[<comment>]		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

Sicherheit mit TAN

Bei Updates oder Parameteränderungen im UTN-Server ist eine TAN erforderlich. Eine aktuelle TAN erhalten Sie vom UTN-Server via E-Mail, z.B. beim Empfang einer Statusseite. Geben Sie die TAN in der ersten Zeile des E-Mail-Textkörpers ein. Anschließend muss ein Leerzeichen folgen.

Parameteränderungen

Parameteränderungen werden in den E-Mail-Textkörper mit der folgenden Syntax verfasst:

```
<Parameter> = <Wert>
```

Syntax und Wertekonventionen entnehmen Sie der Parameterliste; siehe: ⇨119.

Beispiel 1

Diese E-Mail veranlasst den UTN-Server, die Parameterliste an den Sender der E-Mail zu senden.

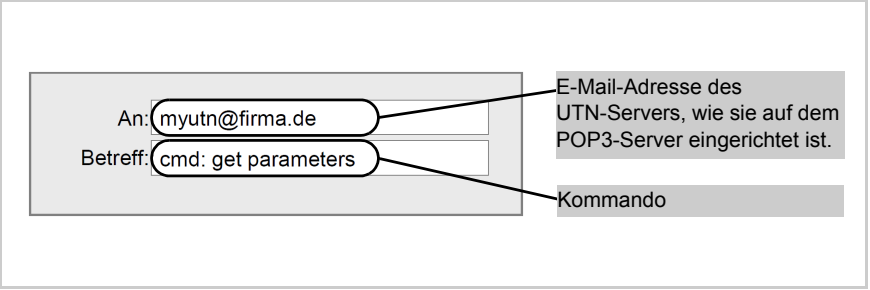


Abb. 5: Administration via E-Mail - Beispiel 1

Beispiel 2

Diese E-Mail konfiguriert am UTN-Server den Parameter 'Beschreibung'.

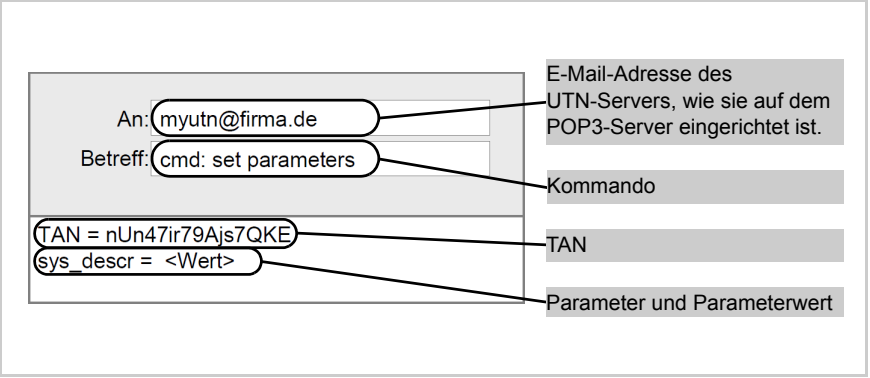


Abb. 6: Administration via E-Mail - Beispiel 2

2.5 Administration via Reset-Taster am Gerät

Am UTN-Server finden Sie LEDs, den Reset-Taster sowie verschiedene Anschlüsse. Eine Beschreibung dieser Komponenten finden Sie im 'Quick Installation Guide'.

Über den Reset-Taster können Sie die Parameterwerte des UTN-Servers auf die Standardeinstellung zurücksetzen; siehe: ⇨111.

3 Netzwerkeinstellungen

Zur optimalen Integration des UTN-Servers in ein TCP/IP-Netzwerk können verschiedene Einstellungen definiert werden. In diesem Kapitel erfahren Sie, welche Netzwerkeinstellungen der UTN-Server unterstützt.

Welche Information benötigen Sie?

- 'Wie konfiguriere ich IPv4-Parameter?' ⇨ 36
- 'Wie konfiguriere ich IPv6-Parameter?' ⇨ 39
- 'Wie konfiguriere ich den DNS?' ⇨ 41
- 'Wie konfiguriere ich SNMP?' ⇨ 42
- 'Wie konfiguriere ich Bonjour?' ⇨ 43
- 'Wie konfiguriere ich POP3 und SMTP? (nur myUTN-80 und höher)' ⇨ 45
- 'Wie konfiguriere ich WLAN? (nur myUTN-54)' ⇨ 48

3.1 Wie konfiguriere ich IPv4-Parameter?

Das TCP/IP (Transmission Control Protocol over Internet Protocol) ist dafür zuständig, Datenpakete über mehrere Verbindungen weiterzuvermitteln und auf dieser Basis Verbindungen zwischen Netzwerkteilnehmern herzustellen.

Zur TCP/IP-Protokollfamilie gehören u.a. die Bootprotokolle DHCP und BOOTP. Zur optimalen Integration des UTN-Servers in ein TCP/IP-Netzwerk können Sie verschiedene IPv4-Parameter definieren. Für weitere Informationen zur IP-Adressenvergabe, siehe: ⇨ 14.

Was möchten Sie tun?

- ☐ 'IPv4-Parameter via myUTN Control Center konfigurieren' ⇨ 37
- ☐ 'IPv4-Parameter via SEH UTN Manager konfigurieren' ⇨ 37
- ☐ 'IPv4-Parameter via InterCon-NetTool konfigurieren' ⇨ 38

IPv4-Parameter via myUTN Control Center konfigurieren

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - IPv4** *an.*
3. *Konfigurieren Sie die IPv4-Parameter; siehe: Tabelle 2* ⇨ 37.
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. *Die Protokolle stellen verschiedene Möglichkeiten dar, die IP-Adresse im UTN-Server zu speichern.* *(Siehe* 'Speichern der IP-Adresse im UTN-Server' ⇨ 14.*)* Es empfiehlt sich, 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
Gateway	Gateway-Adresse des UTN-Servers

IPv4-Parameter via SEH UTN Manager konfigurieren

Voraussetzung

☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.

☑ Der UTN-Server ist der Auswahlliste beigefügt; siehe: ⇨ 64.

Gehen Sie wie folgt vor:

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-Parameter via InterCon-NetTool konfigurieren

Voraussetzung

☑ Das InterCon-NetTool ist auf dem Client installiert; siehe: ⇨ 29.

☑ Im InterCon-NetTool ist die Netzwerksuche via Multicast aktiviert.

☑ Der Router im Netzwerk leitet Multicast-Anfragen weiter.

Gehen Sie wie folgt vor:

1. *Starten Sie das InterCon-NetTool.*
2. *Markieren Sie den UTN-Server in der Geräteliste.*
   Der UTN-Server erscheint in der Geräteliste unter dem Filter 'ZeroConf' mit einer IP-Adresse aus dem für ZeroConf reservierten Adressbereich (169.254.0.0/16).
3. *Wählen Sie im Menü* **Installation** *den Befehl* **IP-Assistent**.
   Der IP-Assistent wird gestartet.
4. *Folgen Sie den Anweisungen des Assistenten.*

↳ Die Einstellungen werden gespeichert.

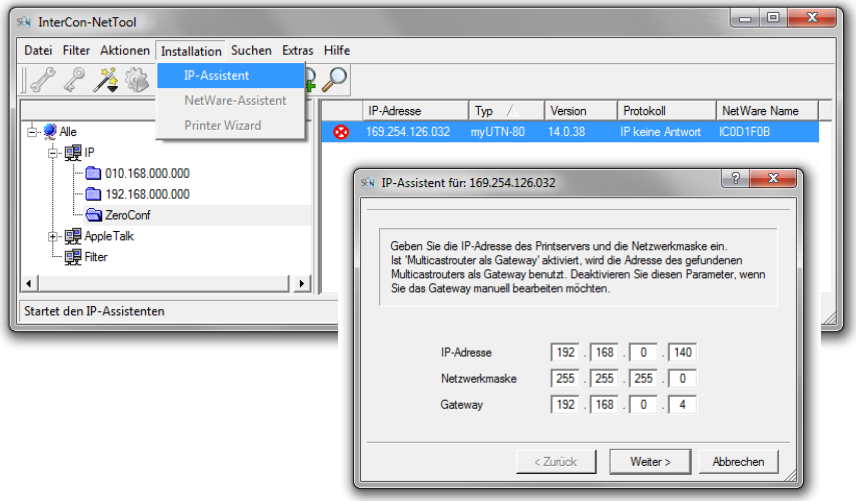


Abb. 7: InterCon-NetTool - IP-Assistent

3.2 Wie konfiguriere ich IPv6-Parameter?

Sie haben die Möglichkeit, den UTN-Server in einem IPv6-Netzwerk einzubinden.

Welche Vorteile bietet IPv6?

IPv6 (Internet Protocol Version 6) ist der Nachfolger des gegenwärtig überwiegend verwendeten Internet-Protokolls in der Version 4. Beide Protokolle sind Standards für die Netzwerkschicht des OSI-Modells und regeln die Adressierung und das Routing von Datenpaketen durch ein Netzwerk. Die Einführung von IPv6 bietet viele Vorteile:

- Vergrößerung des Adressraums von 2^{32} (IPv4) auf 2^{128} (IPv6) IP-Adressen.
- Autokonfiguration und Renumbering
- Effizienzsteigerung beim Routing durch reduzierte Header-Informationen.
- Standardmäßig integrierte Dienste wie IPSec, QoS, Multicast
- Mobile IP

Wie wird eine IPv6-Adresse dargestellt?

IPv6-Adressen sind 128 Bit lang und werden als 8 x 16 Bit hexadezimal dargestellt.

Die acht Blöcke sind durch einen Doppelpunkt zu trennen.
Beispiel: `fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4`

Führende Nullen können zur Vereinfachung vernachlässigt werden.
Beispiel: `fe80 : 0 : 0 : 0 : 0 : 10 : 1000 : 1a4`

Ein Block aus zusammenhängenden Nullen kann mit zwei aufeinander folgenden Doppelpunkten zusammengefasst werden. Damit die Adresse eindeutig bleibt, darf diese Regel nur einmal angewandt werden.
Beispiel: `fe80 : : 10 : 1000 : 1a4`

In einer URL wird eine IPv6-Adresse in eckigen Klammern eingeschlossen. Diese Notation verhindert eine falsche Interpretation von Portnummern als Teil der IPv6-Adresse.
Beispiel: `http://[2001:608:af:1::100]:443`

Die URL wird ausschließlich von IPv6-fähigen Browsern akzeptiert.

Welche IPv6-Adresstypen gibt es?

IPv6-Adressen lassen sich in verschiedene Typen einteilen. Anhand der Präfixe in den IPv6-Adressen lassen sich IPv6-Adressentypen ableiten.

- Unicast-Adressen sind routbare weltweit einzigartige und damit eindeutige Adressen. Ein Paket, das an eine Unicast-Adresse gesendet wird, kommt nur an der Schnittstelle an, die dieser Adresse zugeordnet ist. Unicast-Adressen haben die Präfixe '2' oder '3'.
- Anycast-Adressen können mehrere Teilnehmer gleichzeitig erhalten. Ein Datenpaket das an diese Adresse gesendet wird kommt also an mehreren Geräten an. Anycast-Adressen unterscheiden sich in ihrer Syntax nicht von Unicast-Adressen, sie wählen allerdings aus mehreren Schnittstellen eine Schnittstelle aus.
  Ein für eine Anycast-Adresse bestimmtes Paket kommt an der nächstgelegenen (entsprechend der Router-Metrik) Schnittstelle an. Anycast-Adressen werden nur von Routern verwendet.
- Mit der Multicast-Adresse kann man Datenpakete an mehrere Schnittstellen gleichzeitig versenden, ohne dass die Bandbreite proportional zu den Teilnehmern steigt. Eine Multicast-Adresse erkennt man an dem Präfix 'ff'.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - IPv6** *an.*
3. *Konfigurieren Sie die IPv6-Parameter; siehe: Tabelle 3* ⇨ 41.
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-Unicast-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. Ein Block aus zusammenhängenden Nullen kann mit zwei aufeinander folgenden Doppelpunkten zusammengefasst werden.*
Router	Definiert die IPv6-Unicast-Adresse des Routers, an den der UTN-Server seine 'Router Solicitations' (RS) sendet.
Präfixlänge	Definiert die Länge des Subnetz-Präfixes für die IPv6-Adresse. Der Wert 64 ist voreingestellt. *Adressbereiche werden durch Präfixe angegeben. Dazu wird die Präfixlänge (Anzahl der verwendeten Bits) als Dezimalzahl mit vorangehendem '/' an die IPv6-Adresse angehängt dargestellt.*

3.3 Wie konfiguriere ich den DNS?

DNS (Domain Name Service) erlaubt die gegenseitige Zuordnung von Namen und Adressen. Wird ein DNS-Server in Ihrem Netzwerk betrieben, haben Sie die Möglichkeit, den DNS für Ihren UTN-Server zu nutzen.

Wenn Sie in einer Konfiguration einen Domain-Namen verwenden, muss zuvor der DNS aktiviert und konfiguriert sein. Der DNS wird z.B. bei der Konfiguration des Time-Servers verwendet.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - DNS** *an.*
3. *Konfigurieren Sie die DNS-Parameter; siehe: Tabelle 4* ⇨ 42.
4. *Bestätigen Sie mit* **Speichern & Neustart**.

Die Einstellungen werden gespeichert.

Tabelle 4: DNS-Parameter

Parameter	Beschreibung
DNS	De-/aktiviert den DNS.
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) hat sich zum Standard-Protokoll für die Verwaltung und Überwachung von Netzelementen entwickelt. Das Protokoll regelt die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation.

SNMP erlaubt das Lesen und Verändern von Managementinformationen, die von den Netzelementen (z.B. UTN-Server) bereitgestellt werden. Der UTN-Server unterstützt SNMP in der Version 1 und 3.

SNMPv1

Eine einfache Form des Zugriffsschutzes stellt die SNMP-Community dar. In der Community wird eine Vielzahl von SNMP-Managern zu einer Gruppe zusammengefasst. Der Community werden dann Zugriffsrechte (Lesen/Schreiben) zugewiesen. Der allgemein gültige Community-String ist 'public'.

Der Community-String bei SNMPv1 wird im Klartext übertragen und stellt keinen ausreichenden Schutz dar.

SNMPv3

SNMPv3 ist eine Erweiterung des SNMP-Standards, der verbesserte Anwendungen und ein nutzerbasiertes Sicherheitsmodell mitbringt. SNMPv3 zeichnet sich durch seine Einfachheit und sein Sicherheitskonzept aus.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - SNMP** *an.*
3. *Konfigurieren Sie die SNMP-Parameter; siehe: Tabelle 5* ⇨ 43.
4. *Bestätigen Sie mit* **Speichern & Neustart**.

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. *Die SNMP Community stellt eine einfache Form des Zugriffsschutzes dar, in der mehrere Teilnehmer mit gleichen Zugriffsrechten zusammengefasst werden.*
SNMPv3	De-/aktiviert die SNMPv3-Funktionalität.
Benutzername	Definiert den Namen des SNMP-Benutzers.
Passwort	Definiert das Passwort des SNMP-Benutzers.
Hash	Definiert den Hash-Algorithmus.
Zugriffsrechte	Definiert die Zugriffsrechte des SNMP-Benutzers.
Verschlüsselung	Definiert die Verschlüsselungsmethode.

3.5 Wie konfiguriere ich Bonjour?

Bonjour ermöglicht die automatische Erkennung von Computern, Geräten und Netzwerkdiensten in TCP/IP-basierten Netzwerken.

Der UTN-Server nutzt die folgenden Bonjour-Funktionalitäten:

- Überprüfung der über ZeroConf zugewiesenen IP-Adresse
- Zuordnung von Hostnamen zu IP-Adressen
- Auffinden von Serverdiensten ohne Kenntnis des Hostnamens oder der IP-Adresse des Gerätes

Bei der Überprüfung der über ZeroConf zugewiesenen IP-Adresse (siehe: 'ZeroConf' ⇨15) richtet der UTN-Server eine Anfrage an das Netzwerk. Ist die IP-Adresse im Netzwerk schon belegt, erhält der UTN-Server eine entsprechende Antwort. Der UTN-Server startet dann eine weitere Anfrage mit einer anderen IP-Adresse. Ist die IP-Adresse noch frei, speichert der UTN-Server diese.

Für die weiteren Funktionen von Bonjour wird der Domain Name Service verwendet. Da es keinen zentralen DNS-Server in Bonjour-Netzwerken gibt, verfügt jedes Gerät und jede Anwendung über einen kleinen DNS-Server.

Dieser integrierte DNS-Server (mDNS) sammelt die Informationen aller Teilnehmer im Netz und verwaltet sie. Über die Funktion eines klassischen DNS-Servers hinaus, speichert der mDNS neben der IP-Adresse auch den Dienstnamen und die angebotenen Dienste jedes Teilnehmers.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - Bonjour** *an.*
3. *Konfigurieren Sie die Bonjour-Parameter; siehe: Tabelle 6* ⇨*44.*
4. *Bestätigen Sie mit* **Speichern & Neustart**.

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 Default-Name verwendet (Gerätename@ICxxxxxx).*

3.6 Wie konfiguriere ich POP3 und SMTP? (nur myUTN-80 und höher)

Damit am UTN-Server der Benachrichtigungsservice (⇨📄58) und die Fernwartung via E-Mail (⇨📄32) funktionieren, müssen die Protokolle POP3 und SMTP am UTN-Server konfiguriert werden.

POP3

'POP3' (Post Office Protocol Version 3) ist ein Übertragungsprotokoll, mit dem ein Client E-Mails von einem E-Mail-Server abholen kann. Im UTN-Server wird POP3 benötigt, um den UTN-Server via E-Mail zu administrieren.

SMTP

Das 'SMTP' (Simple Mail Transfer Protocol) ist ein Protokoll, das den Versand von E-Mails in Netzwerken regelt. Im UTN-Server wird SMTP benötigt, um den UTN-Server via E-Mail zu administrieren und um den Benachrichtigungsservice zu betreiben.

Was möchten Sie tun?

- ☐ 'POP3 konfigurieren' ⇨📄45
- ☐ 'SMTP konfigurieren' ⇨📄46

POP3 konfigurieren

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - E-Mail** *an.*
3. *Konfigurieren Sie die POP3-Parameter; siehe: Tabelle 7* ⇨📄*45.*
4. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ 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.*

Parameter	Beschreibung
POP3 - Serverport	Definiert den Port, über den der UTN-Server E-Mails empfängt. Die Portnummer 110 ist voreingestellt. Bei Verwendung von SSL/TLS ist als Portnummer 995 einzutragen.
POP3 - Sicherheit	Definiert das anzuwendende Authentifizierungsverfahren (APOP / SSL/TLS). Bei SSL/TLS wird die Verschlüsselungsstärke über die Verschlüsselungsstufe definiert ⇨ 82.
POP3 - E-Mails abfragen alle	Definiert das Zeitintervall (in Minuten) für die Abfrage der E-Mails auf dem POP3-Server.
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

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - E-Mail** *an.*
3. *Konfigurieren Sie die SMTP-Parameter; siehe: Tabelle 8* ⇨ *46.*
4. *Bestätigen Sie mit* **Speichern & Neustart**.

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.*

Parameter	Beschreibung
SMTP - Serverport	Definiert die Portnummer, über die der SMTP-Server E-Mails von dem UTN-Server empfängt. Die Portnummer 25 ist voreingestellt.
SMTP - TLS	De-/aktiviert die Option TLS. *Über das Sicherheitsprotokoll Transport Layer Security (TLS) wird der Übertragungsweg vom UTN-Server zum SMTP-Server verschlüsselt. Die Verschlüsselungsstärke wird über die Verschlüsselungsstufe definiert* ⇨ 82.
SMTP - Name des Absenders	Definiert die E-Mail-Adresse, die der UTN-Server zum Versenden von E-Mails verwendet. Hinweis: Oft sind der Name des Absenders und der Benutzername identisch.
SMTP - Login	De-/aktiviert die SMTP-Authentifizierung für das Login.
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 das Verschlüsseln und Signieren der E-Mails via S/MIME.
SMTP - E-Mail signieren	Definiert das Signieren von E-Mails. *Eine vom Absender erstellte Signatur ermöglicht es dem Empfänger, die Identität des Absenders zu prüfen und gewährleistet, dass die E-Mail nicht verändert wurde. Für das Signieren wird ein S/MIME-Zertifikat benötigt* ⇨ 91.
SMTP - Vollständig verschlüsseln	Definiert das Verschlüsseln von E-Mails. *Eine verschlüsselte E-Mail kann nur vom Empfänger geöffnet und gelesen werden. Für die Verschlüsselung wird ein S/MIME-Zertifikat benötigt* ⇨ 91.
SMTP - Öffentlichen Schlüssel beifügen	Sendet den öffentlichen Schlüssel zusammen mit der E-Mail. Das Anhängen ist erforderlich zum Anzeigen der E-Mails bei vielen E-Mail-Clients.

3.7 Wie konfiguriere ich WLAN? (nur myUTN-54)

Das UTN-Server-Modell 'myUTN-54' ist WLAN-fähig. Damit haben Sie die Möglichkeit, den UTN-Server drahtlos im Netzwerk zu betreiben.

Was ist WLAN?

WLAN ist eine Funktechnologie, die es ermöglicht, drahtlose Verbindungen zwischen Netzwerkkomponenten bereitzustellen. Die WLAN-Technologie ist als Standard in der IEEE 802.11-Familie definiert. Der myUTN-54 unterstützt die Standards IEEE 802.11b, IEEE 802.11g und IEEE 802.11n.

Zur Umsetzung der Funkttechnologie verfügt der myUTN-54 über zusätzliche Parameter ⇨📄51. Die aktuellen WLAN-Einstellungen können im myUTN Control Center unter dem Menüpunkt **NETZWERK - WLAN** eingesehen werden.

Verbindungsstatus

Der aktuelle Verbindungsstatus wird im myUTN Control Center durch die folgenden Symbole angezeigt:

UTN-Server im WLAN

UTN-Server im drahtgebundenen Netzwerk

WLAN-Sicherheit

Bei einem Wireless LAN ist sicherzustellen, dass sich keine unberechtigten Benutzer anmelden und somit den Internetzugang oder freigegebene Netzwerkressourcen nutzen können. Ihr UTN-Server stellt mehrere Sicherheitsmechanismen zur Verfügung.

Standard	Mechanismus	
	Verschlüsselung	Authentifizierung
WEP	WEP (Open System / Shared Key)	---
WEP+EAP	WEP (Open System)	802.1x/EAP
WPA (Personal Mode)	TKIP/MIC	PSK
WPA2 (Personal Mode)	AES-CCMP	PSK
WPA (Enterprise Mode)	TKIP/MIC	802.1x/EAP
WPA2 (Enterprise Mode)	AES-CCMP	802.1x/EAP

WEP

WEP (Wired Equivalent Privacy) ist ein Verschlüsselungsverfahren nach IEEE 802.11 auf Basis einer RC4-Chiffrierung. WEP stellt Funktionen zur Datenverschlüsselung und Authentifizierung zu Verfügung. WEP verschlüsselt die gesamte Kommunikation mit Hilfe eines Schlüssels. Bei verschlüsselten Basisstationen muss der gleiche WEP-Schlüssel auf der Basisstation und auf dem UTN-Server verwendet werden.

Einige Basisstationen setzen WEP-Schlüssel, die als ASCII-Text eingeben werden, über einen Mechanismus in beliebige Hexadezimalwerte um. In diesem Fall stimmen die Schlüssel auf der Basisstation und auf dem UTN-Server nicht überein. Es wird deshalb empfohlen, hexadezimale WEP-Schlüssel zu verwenden.

WPA/WPA2

WPA (Wi-Fi Protected Access) beinhaltet eine gegenüber WEP verbesserte Aushandlung von Schlüsseln. Der Aushandlungsschlüssel wird nur zu Beginn einer Sitzung verwendet. Im Anschluss kommt ein Sitzungsschlüssel zum Einsatz. Der Schlüssel wird in periodischen Abständen neu generiert. Der WPA-Mechanismus sieht eine Authentifizierung während des Verbindungsaufbaus vor.

Im 'Personal Mode' wird die Authentifizierung über den Pre-Shared-Key (PSK) realisiert. Der PSK ist ein Passwort mit 8–63 alphanummerischen Zeichen. Im 'Enterprise Mode' wird eine EAP-Authentifizierungsmethode angewandt.

Nach der Authentifizierung wird ein individueller 128-bit-Schlüssel für die Datenverschlüsselung verwendet. Zur Datenverschlüsselung stehen die Chiffriermethoden TKIP (Temporal Key Integrity Protocol) und AES (Advanced Encryption Standard) zur Verfügung.

Authentifizierung

Über ein Authentifizierungsverfahren können Sie die Identität eines Gerätes/Benutzers überprüfen, bevor diese(s)/r Zugang zu Ressourcen im Netzwerk hat. Der UTN-Server bietet verschiedene Varianten des EAP (Extensible Authentication Protocol) als Authentifizierungsverfahren an. Für weitere Informationen, siehe: 'Wie verwende ich Authentifizierungsmethoden?' ⇨ 99.

Was möchten Sie tun?

- ☐ 'UTN-Server (myUTN-54) im WLAN betreiben' ⇨ 50
- ☐ 'UTN-Server mit drahtgebundenem Netzwerk verbinden' ⇨ 52

UTN-Server (myUTN-54) im WLAN betreiben

Um den UTN-Server im WLAN betreiben zu können, müssen die WLAN- und Sicherheitseinstellungen des UTN-Servers mit denen des drahtlosen Netzwerkes übereinstimmen.

Damit der UTN-Server konfigurierbar ist, muss zunächst über den Netzwerkanschluss RJ-45 eine Verbindung zu einem drahtgebundenen Netzwerk hergestellt werden; siehe: 'Quick Installation Guide'.

Voraussetzung

☑ Der UTN-Server ist an Netzwerk und Netzspannung angeschlossen.

☑ Der UTN-Server ist mit einer IP-Adresse im drahtgebundenen Netzwerk bekannt; siehe: ⇨ 14.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - WLAN** *an.*
   In der Netzwerkübersicht werden die verfügbaren WLANs angezeigt. Entscheiden Sie, in welchem WLAN der UTN-Server betrieben werden soll.
3. *Konfigurieren Sie die WLAN-Parameter so, dass diese mit den Parametern des zu verwendenden WLANs übereinstimmen; siehe: Tabelle 9* ⇨ *51.*
4. *Aktivieren Sie die Option* **WLAN**, *um das WLAN-Modul im UTN-Server zu aktivieren.*
5. *Bestätigen Sie mit* **Speichern & Neustart**.
   Die Einstellungen werden gespeichert.
6. *Entfernen Sie das Netzwerkkabel (RJ-45) vom UTN-Server.*
   Die Verbindung zum drahtgebundenen Netzwerk wird getrennt.

↳ Der UTN-Server wechselt automatisch in den WLAN-Betrieb.
Die Verbindung zum WLAN wird hergestellt.

Falls der UTN-Server beim Netzwerkwechsel eine neue IP-Adresse erhält, wird die Verbindung zum myUTN Control Center unterbrochen.

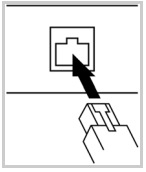
Tabelle 9: WLAN-Parameter

Parameter	Beschreibung
Modus (Kommunikationsmodus)	Definiert den Kommunikationsmodus. Über den Kommunikationsmodus legen Sie fest, in welcher Netzwerkstruktur der UTN-Server installiert werden soll. Zwei Modi stehen zur Verfügung: - Im 'Ad-Hoc'-Modus kommuniziert der UTN-Server direkt mit einem anderen WLAN-Client (Peer-to-Peer). - Der 'Infrastructure'-Modus eignet sich für den Aufbau eines größeren Funknetzes mit mehreren Geräten über mehrere Räume. Hier vermittelt eine an das Netzwerk angeschlossene Basisstation (Access Point) zwischen den Geräten. Die Basisstation kann über eine Verschlüsselung oder eine Authentifizierung geschützt sein.
Netzwerkname (SSID)	Definiert den SSID. Als SSID (Service Set Identifier) oder auch Netzwerkname wird eine Funk-Netzwerk-Kennung bezeichnet. Jedes Wireless LAN besitzt einen konfigurierbaren SSID, um das Funknetz eindeutig identifizieren zu können. Der SSID wird in der Basisstation eines Wireless LAN konfiguriert. Jedes Gerät (PC, UTN-Server usw.), das Zugriff zum Funknetz haben soll, muss mit demselben SSID konfiguriert werden.
Roaming	De-/aktiviert die Verwendung von Roaming. Roaming bezeichnet das 'Wandern' von einer Funkzelle zur nächsten. Der UTN-Server verwendet dann den Access Point, der das bessere Signal liefert. Wird der UTN-Server in den Einflussbereich eines anderen Access Points bewegt, wechselt er automatisch und ohne Verbindungsabbruch in die nächste Funkzelle. Der Parameter 'Roaming' ist nur im 'Infrastructure'-Modus konfigurierbar.
Roaming-Level	Die Sendeleistung des UTN-Servers kann über den Parameter 'Roaming Level' definiert werden. Der Wert 65 -dbm ist voreingestellt. Der Parameter 'Roaming Level' ist nur im 'Infrastructure'-Modus konfigurierbar.

Parameter	Beschreibung
Kanal (Frequenzbereich)	Definiert den Kanal (Frequenzbereich), auf dem gesendet wird. Das Produkt verwendet den Frequenzbereich bei 2,4 GHz im ISM-Band. Ein Kanal hat eine Bandbreite von 22 MHz. Der Abstand zwischen zwei benachbarten Kanälen beträgt 5 MHz. Der Kanal 3 ist voreingestellt. Der Parameter 'Kanal' ist nur im 'Ad-Hoc'-Modus konfigurierbar. Nebeneinander liegende Kanäle überschneiden sich und es kann zu Interferenzen kommen. Wenn in einem kleinen Umkreis mehrere WLANs betrieben werden, dann sollten zwischen jeweils zwei benutzen Kanälen ein Abstand von mindestens 5 Kanälen liegen. ***Informieren Sie sich über die nationalen Bestimmungen für den Einsatz von WLAN-Produkten und verwenden Sie nur zugelassene Kanäle.***
Verschlüsselungsmethode	siehe: 'WLAN-Sicherheit' ⇨ 48
Authentifizierungsmethode	siehe: 'Authentifizierung' ⇨ 49

UTN-Server mit drahtgebundenem Netzwerk verbinden

Um eine Verbindung zum drahtgebundenen Netzwerk herzustellen, verbinden Sie das Netzwerkkabel (RJ-45) mit dem UTN-Server. Der UTN-Server wechselt automatisch in das drahtgebundene Netzwerk.



4 Geräteeinstellungen

Am UTN-Server können Gerätezeit, UTN-Port, Benachrichtigungsservice usw. konfiguriert werden. Dieses Kapitel informiert Sie über diese Geräteeinstellungen.

Welche Information benötigen Sie?

4.1 Wie lege ich eine Beschreibung fest?

Sie haben die Möglichkeit, dem UTN-Server freidefinierbare Beschreibungen zuzuweisen. Auf diese Weise erhalten Sie einen besseren Überblick über die im Netzwerk vorhandenen Geräte.

Gehen Sie wie folgt vor:

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 & Neustart**.

Die Daten werden gespeichert.

Um angeschlossenen USB-Geräten einen Namen zuzuweisen, siehe: ⇨ 56.

4.2 Wie konfiguriere ich die Gerätezeit?

Sie haben die Möglichkeit, die Gerätezeit des UTN-Servers über einen Time-Server (SNTP-Server) im Netzwerk zu steuern. Ein Time-Server synchronisiert die Zeit mehrerer Geräte innerhalb eines Netzwerkes. Der Time-Server wird im UTN-Server über die IP-Adresse oder den Hostnamen definiert.

UTC

Als Basis verwendet der UTN-Server 'UTC' (Universal Time Coordinated). UTC ist eine Referenzzeit, die als globaler Standard benutzt wird.

Zeitzone

Die über den Time-Server empfangene Zeit entspricht also nicht automatisch Ihrer lokalen Zeitzone. Abweichungen zu Ihrem Standort und der damit verbundenen Zeitverschiebung, inklusive länderspezifischer Eigenheiten wie z.B. Sommerzeit, können über den Parameter 'Zeitzone' ausgeglichen werden.

Voraussetzung

☑ Im Netzwerk ist ein Time-Server integriert.

Gehen Sie wie folgt vor:

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 Time-Servers ein.*
   (Der Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.)
5. *Wählen Sie aus der Liste* **Zeitzone** *das Kürzel für Ihre lokale Zeitzone.*
6. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

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

Für den Datentransfer zwischen UTN-Server und Client wird ein gemeinsamer Port verwendet. Je nach Verbindungstyp stehen zwei Portvarianten zur Verfügung.

UTN-Port

Bei einer unverschlüsselten Verbindung kommunizieren der Client und der UTN-Server über den UTN-Port. Die Portnummer 9200 ist voreingestellt.

UTN-SSL-Port

Bei einer verschlüsselten Verbindung kommunizieren der Client und der UTN-Server über den UTN-SSL-Port. Die Portnummer 9443 ist voreingestellt. Um eine verschlüsselte Verbindung zu verwenden, muss die Portverschlüsselung aktiviert werden; siehe: ⇨ 106.

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

Bei Bedarf kann die Portnummer am UTN-Server geändert werden.

Voraussetzung

☑ Damit die auf den Clients installierten SEH UTN Manager die aktuelle Portnummer erhalten, muss der Parameter 'SNMPv1' aktiviert sein; siehe ⇨ 42.

Gehen Sie wie folgt vor:

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 & Neustart**.

↳ Die Einstellungen werden gespeichert.

4.4 Wie weise ich einem USB-Gerät einen Namen zu?

Sie haben die Möglichkeit, einem USB-Gerät eine beliebige Bezeichnung zuzuweisen. Auf diese Weise erhalten Sie einen besseren Überblick über die im Netzwerk vorhandenen Geräte.

Gehen Sie wie folgt vor:

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

Die Einstellungen werden gespeichert.

4.5 Wie kontrolliere ich die Stromzufuhr für einen USB-Port? (nur myUTN-80 und höher)

Sie haben die Möglichkeit, die Stromversorgung eines USB-Ports ein- bzw. auszuschalten. Auf diese Weise können Sie die Stromzufuhr für ein USB-Gerät herstellen bzw. unterbrechen.

Die Stromzufuhr für die USB-Ports ist standardmäßig eingeschaltet.

Nutzen und Zweck

Mit dieser Funktion kann ein USB-Gerät aus- und wieder eingeschaltet werden, ohne es manuell zu entfernen bzw. erneut anzuschließen. USB-Geräte, die sich in einem undefinierten Zustand befinden, können durch die Unterbrechung und Wiederherstellung der Stromzufuhr des USB-Ports neu gestartet werden.

Gehen Sie wie folgt vor:

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

Die Versorgung des USB-Ports mit Strom wird hergestellt bzw. unterbrochen.

4.6 Wie komprimiere ich den Datenstrom des USB-Scanners? (nur myUTN-130)

Der myUTN-130 verfügt über eine hardwarebasierte Datenkomprimierung. Damit haben Sie die Möglichkeit, den Datenstrom des USB-Scanners zu komprimieren. Durch Komprimierung wird der Datenstrom in seinem Umfang reduziert, um das Übertragungsvolumen zu verkleinern und die Übertragungszeit zu verkürzen.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - USB-Port** *an.*
3. *Aktivieren Sie die Option* **Komprimierung**.
4. *Bestätigen Sie mit* **Speichern**.

Der Datenstrom des USB-Scanners wird komprimiert.

Die Komprimierung wird clientseitig im SEH UTN Manager unter Geräteeigenschaften angezeigt.

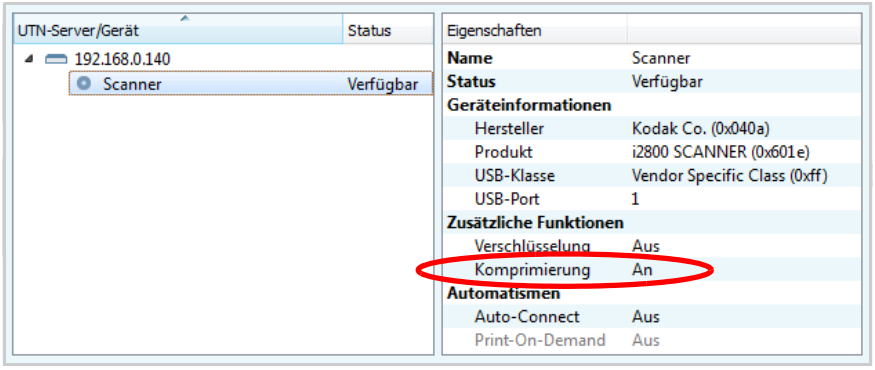


Abb. 8: SEH UTN Manager - Komprimierung

4.7 Wie verwende ich den Benachrichtigungsservice? (nur myUTN-80 und höher)

Sie haben die Möglichkeit, Benachrichtigungen in Form von E-Mails oder SNMP-Traps vom UTN-Server zu erhalten. Mit Hilfe der Benachrichtigungen können bis zu vier Adressaten über verschiedene Meldungen zeitnah und lokalunabhängig informiert werden.

Die folgenden Meldungstypen sind möglich:

- Die Status-E-Mail informiert periodisch über den Status des UTN-Servers inklusive der angeschlossenen USB-Geräte.
- Die Event-Benachrichtigung informiert über ein bestimmtes Ereignis am UTN-Server via E-Mail oder SNMP-Trap. Das Ereignis kann sein:
  - Der Neustart des UTN-Servers.
  - Das Verbinden oder Trennen eines USB-Gerätes am UTN-Server.
  - Das Aktivieren/Deaktivieren eines USB-Gerätes.

Was möchten Sie tun?

☐ 'Versand von Status-E-Mails konfigurieren' ⇨📄58

☐ 'Event-Benachrichtigung via E-Mail konfigurieren' ⇨📄59

☐ 'Event-Benachrichtigung via SNMP-Trap konfigurieren' ⇨📄59

Versand von Status-E-Mails konfigurieren

Voraussetzung

☑ Am UTN-Server sind SMTP-Parameter konfiguriert; siehe: ⇨📄45.

☑ Auf dem UTN-Server ist ein DNS-Server konfiguriert; siehe: ⇨📄41.

Für den Benachrichtigungsservice können bis zu zwei E-Mail-Empfänger definiert werden.

Gehen Sie wie folgt vor:

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 jeweiligen Empfänger.*

5. *Definieren Sie das Sendeintervall.*
6. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

Event-Benachrichtigung via E-Mail konfigurieren

Voraussetzung

☑ Am UTN-Server sind SMTP-Parameter konfiguriert; siehe: ⇨ 45.

☑ Auf dem UTN-Server ist ein DNS-Server konfiguriert; siehe: ⇨ 41.

Für den Benachrichtigungsservice können bis zu zwei E-Mail-Adressaten sowie die Meldungstypen definiert werden.

Gehen Sie wie folgt vor:

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 & Neustart**.

↳ Die Einstellungen werden gespeichert.

Event-Benachrichtigung via SNMP-Trap konfigurieren

Für den Benachrichtigungsservice können bis zu zwei SNMP-Trap-Adressaten sowie die Meldungstypen definiert werden.

Gehen Sie wie folgt vor:

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 & Neustart**.

↳ Die Einstellungen werden gespeichert.

4.8 Wie verteile ich den Zugriff auf donglegeschützte Software (nur myUTN-80) oder USB-Geräte (nur myUTN-150) via VLAN?

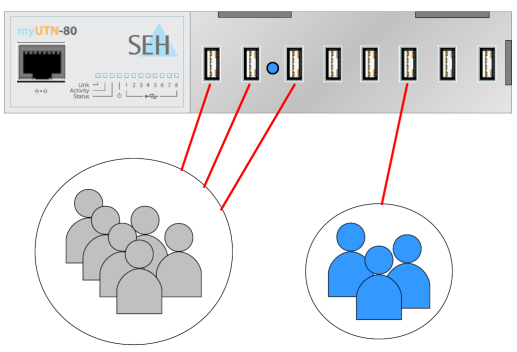
Der UTN-Server unterstützt die Verwendung von virtuellen lokalen Netzwerken (VLAN - Virtual Local Area Network). Das Unterteilen eines physischen Netzwerks in VLANs kann aus Performance- und Sicherheitsgründen sinnvoll sein.

Erstreckt sich ein VLAN über mehrere Switches, so können für deren Verbindung sogenannte VLAN-Trunks (VLT) verwendet werden. Ein VLT dient dazu, Daten der unterschiedlichen VLANs über eine einzige Verbindung weiterzuleiten. Hierzu können sowohl einzelne Ports als auch gebündelte Ports zum Einsatz kommen.

Der UTN-Server unterstützt die Weiterleitung der VLAN-Daten über seine USB-Ports. Hierzu müssen am UTN-Server die VLANs bekannt gemacht werden. Anschließend müssen die USB-Ports, über die die Daten weitergeleitet werden, mit den eingetragenen VLANs verknüpft werden.

Nutzen und Zweck

Die VLANs können verwendet werden, um den Zugriff auf donglegeschütze Software (myUTN-80) bzw. USB-Geräte (myUTN-150) zu kontrollieren. Auf dieser Weise kann einer definierten Gruppe von Netzteilnehmern eine bestimmte Anzahl von donglegeschützer Softwarelizenzen bzw. USB-Geräten zur Verfügung gestellt werden.



Beispiel

6 Konstruktionsmitarbeiter haben Zugriff auf 3 donglegeschütze CAD-Softwarelizenzen.

3 Buchhalter haben Zugriff auf eine donglegeschütze Abrechnungssoftware.

Der Zugriff von Teilnehmern auf eine Software, die nicht für diesen bestimmt ist, wird ausgeschlossen.

Hinweis: Grundsätzlich kann zu einem Zeitpunkt ein USB-Port mit jeweils nur einem Teilnehmer verbunden sein.

Abb. 9: USB-Portbasierte Zuweisung von VLANs

Was möchten Sie tun?

- ☐ 'VLAN eintragen' ⇨ 61
- ☐ 'VLAN einem USB-Port zuordnen' ⇨ 61

VLAN eintragen

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - IPv4-VLAN** *an.*
3. *Konfigurieren Sie die VLAN-Parameter; siehe: Tabelle 10* ⇨ *61.*
4. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 10: IPv4-VLAN-Parameter

Parameter	Beschreibung
VLAN	De-/aktiviert die Weiterleitung der VLAN-Daten.
IP-Adresse	IP-Adresse des UTN-Servers innerhalb des VLAN.
Netzwerkmaske	Netzwerkmaske des UTN-Servers innerhalb des VLAN.
VLAN-ID	ID zur Identifizierung des VLAN (0–4096). *0 = unmarkierte multihomed IP-Adressen*

VLAN einem USB-Port zuordnen

Gehen Sie wie folgt vor:

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.

5 Arbeiten mit dem SEH UTN Manager

Die Zugriffsverteilung der USB-Geräte erfolgt über das Software-Tool SEH UTN Manager. In diesem Kapitel erfahren Sie, wie USB-Geräte im SEH UTN Manager eingebunden und Verbindungen zwischen Client und USB-Gerät hergestellt werden.

Welche Information benötigen Sie?

- 'Wie finde ich UTN-Server/USB-Geräte im Netzwerk?' ⇨ 62
- 'Wie füge ich USB-Geräte der Auswahlliste hinzu?' ⇨ 64
- 'Wie verbinde ich ein USB-Gerät mit dem Client?' ⇨ 65
- 'Wie trenne ich die Verbindung zwischen USB-Gerät und Client?' ⇨ 66
- 'Wie fordere ich ein belegtes USB-Gerät an?' ⇨ 67
- 'Wie automatisiere ich Geräteverbindungen und Programmstarts?' ⇨ 68
- 'Wie erhalte ich Informationen zum USB-Gerät?' ⇨ 74
- 'Wie verwalte ich Auswahllisten für mehrere Teilnehmer?' ⇨ 75

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

Um die im Netzwerk vorhandenen UTN-Server und deren angeschlossene USB-Geräte in der Netzwerkliste darzustellen, muss das Netzwerk gescannt werden. Das Netzwerk kann über Multicast und/oder nach freidefinierbaren Bereichen durchsucht werden. Voreingestellt ist die Multicastsuche in dem lokalen Netzwerksegment.

Was möchten Sie tun?

- ☐ 'Suchparameter definieren' ⇨ 63
- ☐ 'Netzwerk scannen' ⇨ 63

Suchparameter definieren

Voraussetzung

☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager.*
2. *Windows: Wählen Sie im Menü* **Programm** *den Befehl* **Optionen**.
   Mac: Wählen Sie im Menü **SEH UTN Manager** *den Befehl* **Einstellungen**.
   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. *Bestätigen Sie mit* **OK**.

↳ Die Einstellungen werden gespeichert.

Netzwerk scannen

Voraussetzung

☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager.*
2. *Wählen Sie im Menü* **Auswahlliste** *den Befehl* **Bearbeiten**.
3. *Wählen Sie die Schaltfläche* **Suche** *an.*

↳ Das Netzwerk wird durchsucht. Die gefundenen UTN-Server und USB-Geräte werden in der Netzwerkliste angezeigt.

5.2 Wie füge ich USB-Geräte der Auswahlliste hinzu?

Die beim Netzwerkscan gefundenen UTN-Server werden in der 'Netzwerkliste' angezeigt. Um die angeschlossenen USB-Geräte zu verwenden, müssen diese im SEH UTN Manager zusammen mit dem UTN-Server der 'Auswahlliste' zugeordnet werden.

Voraussetzung

☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.

☑ Der UTN-Server wurde beim Netzwerkscan erkannt und wird in der Netzwerkliste angezeigt.

Gehen Sie wie folgt vor:

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 Geräten werden in der Auswahlliste angezeigt.

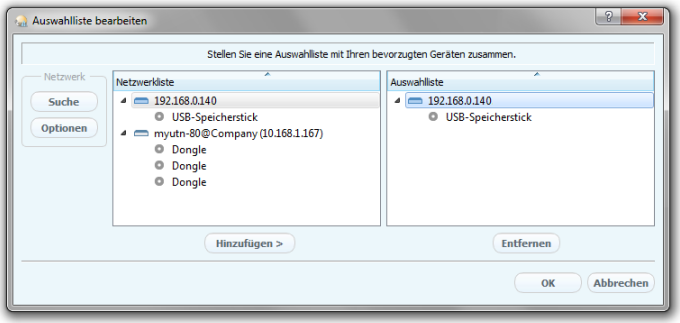


Abb. 10: SEH UTN Manager - Auswahlliste bearbeiten

Um der Auswahlliste einen UTN-Server mit bekannter IP-Adresse direkt hinzuzufügen, wählen Sie im Menü **UTN-Server** den Befehl **Hinzufügen**.

5.3 Wie verbinde ich ein USB-Gerät mit dem Client?

Ein am UTN-Server angeschlossenes USB-Gerät kann mit dem Client verbunden werden. Das USB-Gerät kann dann vom Client genutzt werden, gleich so, als ob das USB-Gerät direkt am Client angeschlossen wäre.

Voraussetzung

- ☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.
- ☑ Das USB-Gerät wird in der Auswahlliste angezeigt; siehe: ⇨ 64.
- ☑ 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.
- ☑ Das USB-Gerät ist nicht mit einem anderen Client verbunden.

Gehen Sie wie folgt vor:

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

↳ Die Verbindung wird hergestellt.

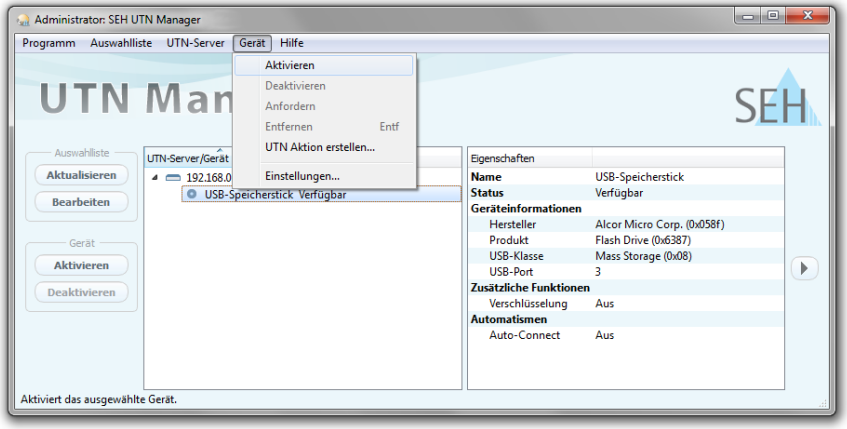


Abb. 11: SEH UTN Manager - Gerät aktivieren

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

Deaktivieren Sie die Verbindung zum USB-Gerät, sobald Sie es nicht mehr benötigen. Auf diese Weise ermöglichen Sie anderen Netzwerkteilnehmern den Zugriff auf das USB-Gerät.

Üblicherweise trennt der Anwender die Verbindung via SEH UTN Manager. Zudem hat der Administrator die Möglichkeit über das myUTN Control Center die Verbindung zu trennen. Weiterhin kann bei einigen Automatismen die Verbindung automatisch getrennt werden (⇨ 68).

Was möchten Sie tun?

- ☐ 'Geräteverbindung via SEH UTN Manager trennen' ⇨ 66
- ☐ 'Geräteverbindung via myUTN Control Center trennen' ⇨ 66

Geräteverbindung via SEH UTN Manager trennen

Voraussetzung

☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.

Gehen Sie wie folgt vor:

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

↳ Die Verbindung wird getrennt.

Geräteverbindung via myUTN Control Center trennen

Gehen Sie wie folgt vor:

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

↳ Die Verbindung wird getrennt.

5.5 Wie fordere ich ein belegtes USB-Gerät an?

Sie haben die Möglichkeit, ein USB-Gerät anzufordern, das von einem anderen Benutzer aktiv verwendet wird.

Der andere Benutzer wird via Popup-Fenster über Ihre Anforderung informiert und kann die Verbindung zum USB-Gerät deaktivieren. Wird das Gerät freigegeben, wird die Verbindung zwischen dem USB-Gerät und Ihrem Client automatisch hergestellt.

Voraussetzung

- ☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.
- ☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client des Benutzers, der das USB-Gerät verwendet, installiert; siehe: ⇨ 21.
- ☑ Der SEH UTN Manager wird auf beiden Clients ausgeführt.
- ☑ Das USB-Gerät wird in der Auswahlliste angezeigt; siehe: ⇨ 64.

Gehen Sie wie folgt vor:

1. *Markieren Sie das USB-Gerät in der Auswahlliste.*
2. *Wählen Sie im Menü* **Gerät** *den Befehl* **Anfordern**.

↳ Die Geräteanforderung wird an den Benutzer gesendet, der das Gerät verwendet.

5.6 Wie automatisiere ich Geräteverbindungen und Programmstarts?

Sie haben die Möglichkeit, Geräteverbindungen und Programmstarts auf verschiedene Arten zu automatisieren. Hierzu stehen unterschiedliche Automatismen zur Verfügung.

Was möchten Sie tun?

- ☐ 'Gerät nach dem Programmstart des SEH UTN Managers automatisch aktivieren (Auto-Connect)' ⇨ 69
- ☐ 'Verbindung zu einem Gerät nach einem definierten Zeitraum automatisch trennen (Auto-Disconnect)' ⇨ 69
- ☐ 'Automatisch eine Verbindung zwischen USB-Gerät und Client herstellen, sobald ein Druckauftrag anliegt (Print-On-Demand)' ⇨ 71
- ☐ 'UTN Aktion erstellen: Automatisierte Geräteverbindungen und Programmstarts ohne SEH UTN Manager-Oberfläche' ⇨ 72
- ☐ 'Zusatztool 'utnm' verwenden' ⇨ 145

Gerät nach dem Programmstart des SEH UTN Managers automatisch aktivieren (Auto-Connect)

Die Funktion ermöglicht das automatische Aktivieren einer Geräteverbindung nach Programmstart des SEH UTN Managers.

Ausschließlich durch einen Administrator konfigurierbar.

Voraussetzung

☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.

☑ Das USB-Gerät wird in der Auswahlliste angezeigt; siehe: ⇨ 64.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager.*
2. *Markieren Sie das USB-Gerät in der Auswahlliste.*
3. *Wählen Sie im Menü* **Gerät** *den Befehl* **Einstellungen**.
4. *Aktivieren Sie die Option* **Aktiviert das Gerät nach dem Programmstart des SEH UTN Manager automatisch. (Auto-Connect)**.
5. *Wählen Sie die Schaltfläche* **OK** *an.*

Die Einstellung wird gespeichert.

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

Die Funktion ermöglicht das automatische Trennen einer Verbindung zu einem USB-Gerät nach einem definierten Zeitraum. Eine einmalige Verlängerung der Verbindung um die Dauer des definierten Zeitraums kann optional aktiviert werden. Die Einstellungen gelten für alle USB-Geräte an einem UTN-Server.

2 Minuten vor Ablauf des definierten Zeitraums erhält der Gerätebenutzer einen Infohinweis, um Datenverlust und Fehlerzuständen vorzubeugen. Wurde die Verlängerung aktiviert, erscheint der Infohinweis inkl. der Möglichkeit, die Verlängerung zu akzeptieren oder abzulehnen.

Sie haben die Möglichkeit, sich nach dem automatischen Trennen einer Verbindung über die Geräteverfügbarkeit informieren zu lassen. Richten Sie hierzu eine Benachrichtigung über die Freigabe eines Gerätes ein; siehe: ⇨ 74.

Der Auto-Disconnect ermöglicht einer großen Anzahl von Netzwerkteilnehmern den Zugriff auf eine geringe Anzahl an Geräten und verhindert Geräteleerläufe.

Ausschließlich durch einen Administrator konfigurierbar.

Voraussetzung

- ☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.
- ☑ Der UTN-Server wird im Bereich 'Automatische Gerätetrennung' angezeigt; siehe: ⇨ 64.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager.*
2. *Windows: Wählen Sie im Menü* **Programm** *den Befehl* **Optionen**.
   Mac: Wählen Sie im Menü **SEH UTN Manager** *den Befehl* **Einstellungen**.
   Der Dialog **Optionen** *erscheint.*
3. *Wählen Sie die Registerkarte* **Automatismen** *an.*
4. *Aktivieren Sie im Bereich* **Automatische Gerätetrennung** *die Option* **Status** *für den entsprechenden UTN-Server.*
5. *Definieren Sie den gewünschten Zeitraum (10–525 Minuten).*
6. *Aktivieren Sie optional die Option* **Verlängerung**.
7. *Wählen Sie die Schaltfläche* **OK** *an.*

↳ Die Einstellung wird gespeichert.

Automatisch eine Verbindung zwischen USB-Gerät und Client herstellen, sobald ein Druckauftrag anliegt (Print-On-Demand)

Zwischen USB-Gerät (Drucker oder MFG) und Client wird, sobald ein Druckauftrag anliegt, automatisch eine Verbindung hergestellt. Nach Beendigung des Druckauftrages wird die Verbindung automatisch deaktiviert.

Ausschließlich durch einen Administrator konfigurierbar.

Voraussetzung

☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.

☑ Das USB-Gerät wird in der Auswahlliste angezeigt; siehe: ⇨ 64.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager.*
2. *Markieren Sie das USB-Gerät in der Auswahlliste.*
3. *Wählen Sie im Menü* **Gerät** *den Befehl* **Einstellungen**.
4. *Aktivieren Sie die Option* **Print-On-Demand**.
5. *Wählen Sie die Schaltfläche* **OK** *an.*

↳ Die Einstellung wird gespeichert.

Um diese Option verwenden zu können, muss der Drucker auf dem Client eingerichtet sein (Treiberinstallation).

UTN Aktion erstellen: Automatisierte Geräteverbindungen und Programmstarts ohne SEH UTN Manager-Oberfläche

Sie haben die Möglichkeit, UTN Aktionen zu erstellen. UTN Aktionen sind kleine Programme, die zum automatischen Aktivieren und Deaktivieren von Geräteverbindungen verwendet werden. Auch das Starten und Beenden einer Applikation in Kombination mit einer Geräteverbindung kann durch eine UTN Aktion automatisiert werden.

Der in der UTN Aktion definierte Vorgang läuft nach der Dateiausführung automatisch ab. Durch den im Hintergrund aktiven 'SEH UTN Service' ist es für den Benutzer nicht erforderlich, die SEH UTN Manager-Oberfläche zu starten. Das heißt, UTN Aktionen können in der vollständigen Variante und in der Minimal-Variante verwendet werden.

Der SEH UTN Manager unterstützt bei der Erstellung einer UTN Aktion durch einen Assistenten (Wizard). Folgende UTN Aktionen können erstellt werden:

- **UTN Aktionen zum Aktivieren und Deaktivieren des Gerätes**
  Der Assistent erstellt automatisch je eine UTN Aktion zum Aktivieren und Deaktivieren des Gerätes. Beide UTN Aktionen werden auf dem Desktop gespeichert.
- **UTN Aktion zum Starten einer Applikation und Aktivieren des Gerätes**
  Nach Auswahl der Applikation durch den Benutzer erstellt der Assistent automatisch eine Aktion zum Starten der Applikation und Aktivieren des Gerätes. Optional kann eine Gerätedeaktivierung nach Applikationsbeendung definiert werden.
- **Benutzerdefinierte UTN Aktion (Expertenmodus)**
  Mit Unterstützung des Assistenten kann eine benutzerdefinierte UTN Aktion geschrieben werden. Wahlweise können erstellt werden:
  - UTN Aktionen zur Aktivierung und Deaktivierung des Gerätes. Zusätzliche Optionen können definiert werden.
  - Ein Skript zum Starten der Applikation und Aktivieren des Gerätes. Optional können eine Verzögerung für den Applikationsstart, das Deaktivieren des Gerätes nach Applikationsbeendung und weitere Optionen definiert werden. Das Skript wird automatisch erzeugt und kann nachfolgend bearbeitet werden. Abschließend wird die vollständige UTN Aktion vom SEH UTN Manager automatisch erstellt und vom Benutzer gespeichert.

Voraussetzung

☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.

☑ Das USB-Gerät wird in der Auswahlliste angezeigt; siehe: ⇨ 64.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager.*
2. *Markieren Sie ein USB-Gerät in der Auswahlliste.*
3. *Wählen Sie im Menü* **Gerät** *den Befehl* **UTN Aktion erstellen**. *Der Dialog* **UTN Aktion erstellen** *wird gestartet.*
4. *Folgen Sie den Anweisungen des Assistenten.*

Es wird eine UTN Aktion erstellt. Mit einem Doppelklick auf die Datei wird die UTN Aktion ausgeführt.

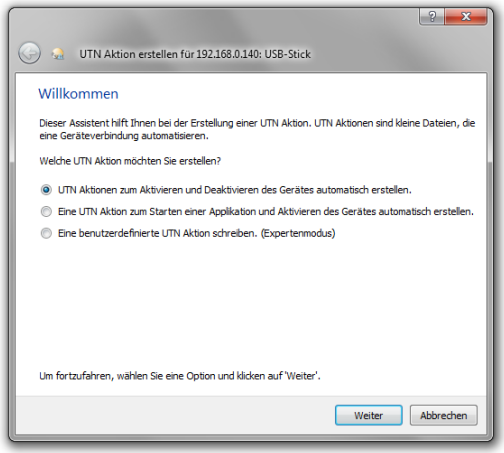


Abb. 12: Dialog **UTN Aktion erstellen**

Tipp 1 Verknüpfungen (Windows) bzw. Apps (Mac) können nach dem Speichern an einen beliebigen Ort verschoben und umbenannt werden.

Tipp 2 Expertenmodus (UTN Aktionen zum Aktivieren und Deaktivieren des Gerätes): Unter Windows enthält das Ziel der Verknüpfung die Kommandozeile. Bei Bedarf kann diese bearbeitet werden. Unter Mac kann in der App das Skript bei Bedarf bearbeitet werden (Pfad: `Contents/Resources/script`).

Tipp 3 Expertenmodus (Skript): Sie können das Skript auch nach der Erstellung mit einem einfachen Texteditor bearbeiten.

5.7 Wie erhalte ich Informationen zum USB-Gerät?

Sie haben die Möglichkeit, die Statusinformation des USB-Gerätes einzusehen. Zudem können Sie automatische Meldungen konfigurieren. Sie werden dann informiert, wenn ein USB-Gerät verfügbar ist, nachdem es belegt war.

Was möchten Sie tun?

- ☐ 'Statusinformationen anzeigen' ⇨📄74
- ☐ 'Meldungen konfigurieren (zurzeit nur Windows)' ⇨📄74

Statusinformationen anzeigen

Voraussetzung

- ☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨📄21.
- ☑ Das USB-Gerät wird in der Auswahlliste angezeigt; siehe: ⇨📄64.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager.*
2. *Markieren Sie das USB-Gerät in der Auswahlliste.*

↳ Die Statusinformationen werden in dem Bereich 'Geräteeigenschaften' angezeigt.

Meldungen konfigurieren (zurzeit nur Windows)

Voraussetzung

- ☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨📄21.
- ☑ Das USB-Gerät wird in der Auswahlliste angezeigt; siehe: ⇨📄64.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager.*
2. *Markieren Sie das USB-Gerät in der Auswahlliste.*
3. *Wählen Sie im Menü* **Gerät** *den Befehl* **Einstellungen**. *Der Dialog* **Geräteeinstellungen** *erscheint.*
4. *Aktivieren Sie im Feld* **Meldungen** *die Option.*
5. *Wählen Sie die Schaltfläche* **OK** *an.*

↳ Die Einstellung wird gespeichert.
Sobald ein Netzteilnehmer die Verbindung zu dem USB-Gerät deaktiviert, wird eine 'Desktop-Benachrichtigung' generiert.

5.8 Wie verwalte ich Auswahllisten für mehrere Teilnehmer?

Was sind Auswahllisten?

Die Auswahlliste ist ein zentrales Element im SEH UTN Manager. Sie zeigt alle eingebundenen UTN-Server sowie die angeschlossenen USB-Geräte an und stellt deren Status dar. Aufgeführte USB-Geräte können mit dem Client verbunden und verwendet werden. Die Auswahlliste ist bearbeitbar und kann bedarfsgerecht durch Hinzufügen und Entfernen der benötigten Geräte eingerichtet werden.

Auswahllisten werden als 'SEH UTN Manager.ini'-Datei gespeichert.

Es stehen zwei Auswahllistentypen zur Verfügung:

- globale Auswahlliste
- benutzerindividuelle Auswahlliste

Nutzen und Zweck

Über den Auswahllistentyp in Kombination mit der Benutzerverwaltung kann ein Administrator den Zugriff auf die im Netzwerk verfügbaren UTN-Server kontrollieren:

Alle Anwender benutzen zunächst immer dieselbe globale Auswahlliste.

Alternativ kann jeder Anwender eine benutzerindividuelle Auswahlliste verwenden. Die Zugriffskontrolle erfolgt durch das Ablegen von vordefinierten Auswahllisten in benutzerindividuelle Verzeichnisse. Weiterhin kann durch den Entzug von Schreibrechten auf die ini-Datei der Zugriff auf Funktionen des SEH UTN Managers für den individuellen Benutzer eingeschränkt und kontrolliert werden.

Nachfolgend werden die Auswahllistentypen im Detail beschrieben.

Globale Auswahlliste

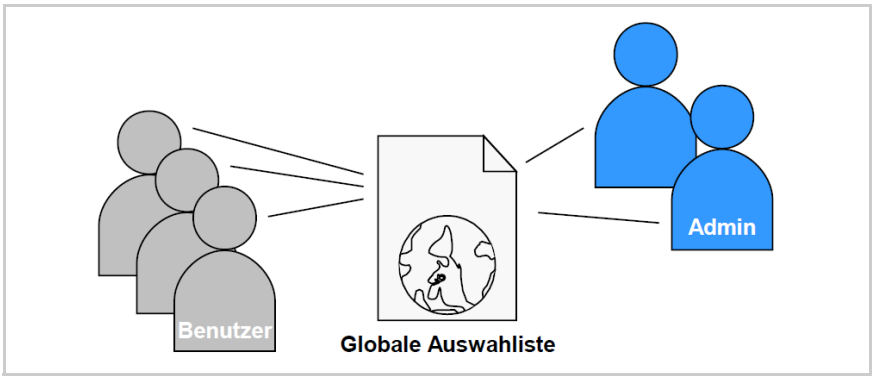


Abb. 13: Globale Auswahlliste

Eigenschaften der globalen Auswahlliste:

- Alle Benutzer eines Clients verwenden dieselbe Auswahlliste.
- Die Benutzer können ausschließlich auf die in der Auswahlliste aufgeführten Geräte zugreifen.
- Unbefugte haben keine Möglichkeit auf Geräte zuzugreifen, die nicht in der Auswahlliste aufgeführt sind.
- Die Auswahlliste kann ausschließlich durch Administratoren bearbeitet werden.

Benutzerindividuelle Auswahlliste

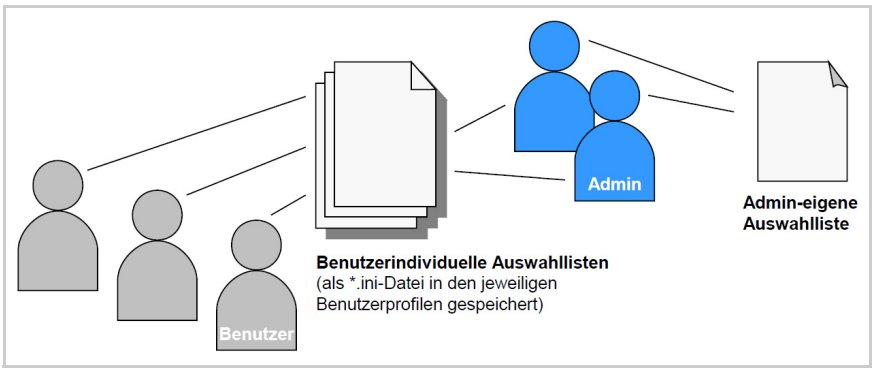


Abb. 14: Benutzerindividuelle Auswahlliste

Eigenschaften der benutzerindividuellen Auswahlliste:

- Jeder Benutzer hat seine individuelle Auswahlliste.
  Alle Administratoren haben dieselbe Auswahlliste.
- Die Auswahlliste kann durch einen Administrator oder durch Benutzer mit Schreibrechten bearbeitet werden.
- Der Benutzer kann auf alle in der Auswahlliste aufgeführten Geräte zugreifen. (Vorausgesetzt es sind keine Schutzmechanismen über das myUTN Control Center definiert.)
- Die Auswahllisten der Benutzer werden als ini-Dateien unter dem folgenden Pfad abgespeichert:
  Windows: `%APPDATA%\SEH Computertechnik GmbH\SEH UTN Manager.ini`
  Mac: `$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`

  Wobei `%APPDATA%` eine Umgebungsvariable von Windows für den Benutzer ist. Mit Hilfe der Kommandozeile kann der Pfad für den aktuellen Benutzer folgendermaßen ermittelt werden: `echo %APPDATA%`

  Beispiel:

  Windows XP:

  `echo %APPDATA%` ergibt `C:\Users\Benutzername\AppData\Roaming`

  +

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

  Vollständiger Pfad zur ini-Datei:

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

  `$HOME` ist eine Umgebungsvariable von Mac für den Benutzerordner. Mit Hilfe der Kommandozeile kann der Pfad für den aktuellen Benutzer folgendermaßen ermittelt werden: `echo $HOME`

  Beispiel:

  Mac OS X 10.7.5 (Lion):

  `echo $HOME` ergibt `/Users/Benutzer-Name`

  +

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

  Vollständiger Pfad zur ini-Datei:

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

Was möchten Sie tun?

- ☐ 'Globale Auswahlliste für alle Benutzer bereitstellen' ⇨ 78
- ☐ 'Benutzerindividuelle Auswahllisten bereitstellen' ⇨ 78
- ☐ 'Benutzern eine vordefinierte Auswahlliste bereitstellen' ⇨ 79
- ☐ 'Benutzerindividuelle Auswahlliste schützen' ⇨ 80

Globale Auswahlliste für alle Benutzer bereitstellen

Voraussetzung

☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager (als Administrator).*
2. *Stellen Sie die Auswahlliste zusammen; siehe: 'Wie füge ich USB-Geräte der Auswahlliste hinzu?'* ⇨ 64.
3. *Windows: Wählen Sie im Menü* **Programm** *den Befehl* **Optionen**.
   Mac: Wählen Sie im Menü **SEH UTN Manager** *den Befehl* **Einstellungen**.
   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 bereitstellen

Voraussetzung

☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager (als Administrator).*

2. *Windows: Wählen Sie im Menü* **Programm** *den Befehl* **Optionen**.
   Mac: Wählen Sie im Menü **SEH UTN Manager** *den Befehl* **Einstellungen**.
   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.*

Die Einstellung wird gespeichert. Jeder Benutzer verwendet eine individuelle Auswahlliste. Die Auswahllisten der Benutzer werden als ini-Dateien in benutzerindividuellen Verzeichnissen abgespeichert (siehe: 'Benutzerindividuelle Auswahlliste' ⇨ 76).

Die Administratoren teilen sich eine Auswahlliste.

Benutzern eine vordefinierte Auswahlliste bereitstellen

Voraussetzung

☑ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 21.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager (als Administrator).*
2. *Stellen Sie die Auswahlliste für den Benutzer zusammen; siehe: 'Wie füge ich USB-Geräte der Auswahlliste hinzu?'* ⇨ 64.
3. *Windows: Wählen Sie im Menü* **Programm** *den Befehl* **Optionen**.
   Mac: Wählen Sie im Menü **SEH UTN Manager** *den Befehl* **Einstellungen**.
   Der Dialog **Optionen** *erscheint.*
4. *Wählen Sie die Registerkarte* **Auswahlliste** *an.*
5. *Aktivieren Sie die Option* **Benutzerindividuelle Auswahlliste**.
6. *Wählen Sie die Schaltfläche* **OK** *an.*
   Die Einstellung wird gespeichert.
7. *Wählen Sie im Menü* **Auswahlliste** *den Befehl* **Exportieren**.
   Der Dialog **Exportieren nach** *erscheint.*

8. *Speichern Sie die Datei 'SEH UTN Manager.ini' unter dem folgenden Pfad:*
   Windows: `%APPDATA%\SEH Computertechnik GmbH\SEH UTN Manager.ini`
   Mac: `$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
   (Siehe: 'Benutzerindividuelle Auswahlliste' ⇨ 76.**)**

↳ Jeder Benutzer greift auf seine vordefinierte Auswahlliste zu.

Benutzerindividuelle Auswahlliste schützen

Beim Einsatz von vordefinierten benutzerindividuellen Auswahllisten ist es sinnvoll, die Auswahlliste vor Änderungen durch den Benutzer zu schützen.

Die Auswahlliste eines Benutzers ist als 'SEH UTN Manager.ini'-Datei unter dem folgenden Pfad abgelegt:

Windows: `%APPDATA%\SEH Computertechnik GmbH\SEH UTN Manager.ini`
Mac: `$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
(Siehe: 'Benutzerindividuelle Auswahlliste' ⇨ 76)

Verwenden Sie die Betriebssytemsteuerung, um ini-Dateien mit einem Schreibschutz zu belegen. Hierzu benötigen Sie administrative Rechte auf dem Client.

Wird einer 'SEH UTN Manager.ini'-Datei das Schreibrecht entzogen, dann sind für den Benutzer alle Funktionen im SEH UTN Manager, die die Auswahlliste betreffen, deaktiviert.

6 Sicherheit

Um beim Einsatz des UTN-Servers eine hohe Sicherheit gewährleisten zu können, stehen dem UTN-Server verschiedene Schutzmechanismen zur Verfügung. In diesem Kapitel erfahren Sie, wie die Schutzmechanismen sinnvoll eingesetzt und realisiert werden.

Die folgenden Schutzmechanismen können je nach Anforderung konfiguriert und aktiviert werden:

Welche Information benötigen Sie?

- 'Wie definiere ich die Verschlüsselungsstufe für SSL-/TLS-Verbindungen?' ⇨ 82
- 'Wie kontrolliere ich den Zugang zum myUTN Control Center?' ⇨ 84
- 'Wie kontrolliere ich den Zugriff zum UTN-Server? (TCP-Portzugriffskontrolle)' ⇨ 86
- 'Wie kontrolliere ich den Zugriff auf USB-Geräte? (nur myUTN-80 und höher)' ⇨ 88
- 'Wie setze ich Zertifikate korrekt ein?' ⇨ 91
- 'Wie verwende ich Authentifizierungsmethoden?' ⇨ 99
- 'Wie verschlüssele ich die Datenübertragung?' ⇨ 106

6.1 Wie definiere ich die Verschlüsselungsstufe für SSL-/TLS-Verbindungen?

Sie haben die Möglichkeit, folgende Verbindungen am UTN-Server via SSL/TLS zu verschlüsseln:

- E-Mail: POP3 (⇨ 45)
- E-Mail: SMTP (⇨ 45)
- Webzugang zum myUTN Control Center: HTTPS (⇨ 84)
- Datenübertragung zwischen den Clients und dem UTN-Server (bzw. den angeschlossenen USB-Geräten): USB-Port (⇨ 106)

Verschlüsselungsstufe

Die Stärke der Verschlüsselung und damit die Sicherheit der Verbindung wird über die Verschlüsselungsstufe definiert.

Cipher Suite

Jede Verschlüsselungsstufe stellt eine Sammlung sog. Cipher Suites dar. Eine Cipher Suite ist eine standardisierte Folge aus vier kryptografischen Algorithmen, die zum Aufbau einer sicheren Verbindung verwendet werden. Cipher Suites werden gemäß ihrer Verschlüsselungsstärke (in Bit) zu einer Verschlüsselungsstufe zusammengefasst. Welche Cipher Suites vom UTN-Server unterstützt werden, also Teil einer Verschlüsselungsstufe sind, hängt vom verwendeten Protokoll (SSLv2, SSLv3, TLSv1) ab.

Verbindungsaufbau

Beim Aufbau einer sicheren Verbindung wird 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. Gibt es keine von beiden unterstützte Cipher Suite, wird keine SSL-/TLS-Verbindung aufgebaut.

Die Kommunikationspartner des UTN-Servers (z.B. Browser) müssen die Cipher Suites der gewählten Verschlüsselungsstufe für einen erfolgreichen Verbindungsaufbau unterstützen. Bei Problemen wählen Sie eine andere Stufe oder setzen die UTN-Server-Parameter zurück; siehe: ⇨ 110.

Folgende Verschlüsselungsstufen sind wählbar:

- **Kompatibel:** Es werden Cipher Suites mit einer Verschlüsselung von 40 bis 256 Bit verwendet.
- **Niedrig:** Es werden nur Cipher Suites mit einer schwachen Verschlüsselung von 56 Bit verwendet. (Schnelle Verbindung)
- **Mittel:** Es werden nur Cipher Suites mit einer Verschlüsselung von 128 Bit verwendet.
- **Hoch:** Es werden nur Cipher Suites mit einer starken Verschlüsselung von 128 bis 256 Bit verwendet. (Langsame Verbindung)

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - SSL-Verbindungen** *an.*
3. *Wählen Sie im Bereich* **Verschlüsselung** *die gewünschte Verschlüsselungsstufe.*
4. *Bestätigen Sie mit* **Speichern & Neustart**.
5. Die Einstellung wird gespeichert.

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

6.2 Wie kontrolliere ich den Zugang zum myUTN Control Center?

Sie haben die Möglichkeit, den administrativen Web- und SNMP-Zugang zum myUTN Control Center zu schützen.

Was möchten Sie tun?

- ☐ 'Erlaubten Webverbindungstypen definieren' ⇨ 84
- ☐ 'Webzugriff via Passwort schützen' ⇨ 85
- ☐ 'Webzugriff via VLAN-Adresse erlauben/sperren (nur myUTN-80 und myUTN-150)' ⇨ 85
- ☐ 'SNMP-Zugriff via VLAN-Adresse erlauben/sperren (nur myUTN-80 und myUTN-150)' ⇨ 86

Zusätzlich kann das myUTN Control Center über das SNMP-Sicherheitskonzept geschützt werden. Das Konzept beinhaltet das Verwalten von Benutzergruppen und Zugriffsrechten. Für weitere Informationen, siehe: 'Wie konfiguriere ich SNMP?' ⇨ 42.

Erlaubten Webverbindungstypen definieren

Verbindungstyp (HTTP/HTTPS)

Der Webzugang zum myUTN Control Center kann durch die Wahl der erlaubten Verbindungstypen (HTTP/HTTPS) gesichert werden.

Wird ausschließlich HTTPS als Verbindungstyp gewählt, ist der administrative Webzugang zum myUTN Control Center via SSL/TLS geschützt. Die Verschlüsselungsstärke wird über die Verschlüsselungsstufe definiert ⇨ 82.

Bei SSL/TLS wird ein Zertifikat benötigt, um die Identität des UTN-Servers zu überprüfen. Bei einem so genannten 'Handshake' fragt der Client via Browser nach einem Zertifikat. Dieses Zertifikat muss vom Browser akzeptiert werden; lesen Sie hierzu die Dokumentation Ihrer Browsersoftware. URLs, die eine SSL-/TLS-Verbindung erfordern, beginnen mit 'https'.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*

2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Gerätezugriff** *an.*
3. *Aktivieren Sie im Bereich* **Web** *die Option* **HTTP/HTTPS** *bzw.* **Nur HTTPS**.
4. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellung wird gespeichert.

Webzugriff via Passwort schützen

Sie haben die Möglichkeit, das myUTN Control Center über ein Passwort vor unberechtigtem Webzugriff zu schützen. Ist ein Passwort gesetzt, kann nur die Startseite des myUTN Control Centers aufgerufen und eingesehen werden. Wird ein Menüpunkt angewählt, findet eine Passwortabfrage statt.

Es wird ebenfalls ein (nicht zu definierender) Benutzername abgefragt. Lassen Sie dieses Feld bei der Passwortabfrage leer.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Gerätezugriff** *an.*
3. *Geben Sie im Bereich* **Web** *im Feld* **Passwort** *ein Passwort ein.*
4. *Wiederholen Sie die Passworteingabe.*
5. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellung wird gespeichert.

Webzugriff via VLAN-Adresse erlauben/sperren (nur myUTN-80 und myUTN-150)

Sie haben die Möglichkeit, den administrativen Webzugang zum myUTN Control Center über eine VLAN-Adresse zu blockieren.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Gerätezugriff** *an.*
3. *De-/Aktivieren Sie im Bereich* **Web** *die Option* **VLAN-Zugriff**.
4. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellung wird gespeichert.

SNMP-Zugriff via VLAN-Adresse erlauben/sperren (nur myUTN-80 und myUTN-150)

Sie haben die Möglichkeit, den administrativen SNMP-Zugang zum myUTN Control Center über eine VLAN-Adresse zu blockieren.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Gerätezugriff** *an.*
3. *De-/Aktivieren im Bereich* **SNMP** *Sie die Option* **VLAN-Zugriff**.
4. *Bestätigen Sie mit* **Speichern & Neustart**.

Die Einstellung wird gespeichert.

6.3 Wie kontrolliere ich den Zugriff zum UTN-Server? (TCP-Portzugriffskontrolle)

TCP-Portzugriffskontrolle

Sie haben die Möglichkeit, den Zugriff auf den UTN-Server zu kontrollieren. Hierzu können verschiedene TCP-Porttypen am UTN-Server gesperrt werden. Zugriffsberechtigte Netzwerkelemente können als Ausnahme definiert und von der Sperrung ausgenommen werden. Der UTN-Server akzeptiert dann nur Datenpakete von den als Ausnahme definierten Netzwerkelementen.

Sicherheitsstufen

Die zu sperrenden Porttypen sind im Bereich 'Sicherheitsstufe' zu definieren. Die folgende Kategorisierung ist wählbar:

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

Ausnahmen

Um Netzwerkelemente (z.B. Clients, DNS-Server, SNTP-Server) von einer Portsperrung auszuschließen, müssen diese als Ausnahme definiert werden. Hierzu werden im Bereich 'Ausnahmen' die IP-Adressen oder MAC-Adressen (Hardwareadressen) der zugriffsberechtigten Netzwerkelemente eingegeben. Beachten Sie:

- MAC-Adressen werden nicht über Router weitergeleitet!

- Mit dem Einsatz von Wildcards (*) können Subnetzwerke definiert werden.

Testmodus

Der 'Testmodus' bietet die Möglichkeit, den eingestellten Zugriffsschutz zu überprüfen. Bei aktiviertem Testmodus bleibt der Zugriffsschutz bis zum Neustart des UTN-Servers aktiv. Nach dem Neustart ist der Schutz nicht mehr wirksam.

Die Option 'Testmodus' ist voreingestellt aktiv. Nach einem erfolgreichen Test müssen Sie den Testmodus deaktivieren, damit der Zugriffsschutz dauerhaft aktiv bleibt.

Gehen Sie wie folgt vor:

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 von der Portsperrung ausgeschlossen sind. Geben Sie hierzu die IP- oder MAC-Adressen ein und aktivieren Sie die Optionen.*
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 die Konfigurationsfähigkeit des UTN-Servers.*

Kann der UTN-Server über das myUTN Control Center nicht mehr erreicht werden, initiieren Sie einen Geräte-Neustart; siehe: ⇨ 114.

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

↳ Die Einstellungen werden gespeichert. Die Portzugriffskontrolle ist aktiv. Der Zugriff auf die Ports ist geschützt.

6.4 Wie kontrolliere ich den Zugriff auf USB-Geräte? (nur myUTN-80 und höher)

Sie haben die Möglichkeit, den Zugriff auf die am UTN-Server angeschlossenen USB-Geräte über die USB-Ports zu kontrollieren. Für jeden USB-Port stehen zwei Sicherheitsmethoden zur Verfügung. Beide Sicherheitsmethoden können auch in Kombination verwendet werden.

USB-Port-schlüsselkontrolle

Bei der Schlüsselkontrolle wird über das myUTN Control Center für den USB-Port ein Schlüssel definiert. Durch die Schlüsseleingabe ist das am USB-Port angeschlossene USB-Gerät vor Zugriff geschützt.

Das USB-Gerät wird im SEH UTN Manager nicht mehr angezeigt. Ein Anwender hat dann keine Möglichkeit Einstellungen am USB-Gerät vorzunehmen oder eine Verbindung zwischen Client und USB-Gerät herzustellen.

Um das USB-Gerät verfügbar zu machen, muss ein Anwender am Client über den SEH UTN Manager den Schlüssel für den USB-Port eingeben. Durch die Änderung des Schlüssels im myUTN Control Center kann dem Anwender der Zugriff auf das USB-Gerät erneut entzogen werden.

USB-Port-Gerätezuordnung

Bei der Gerätezuordnung wird über das myUTN Control Center jedem USB-Port ein USB-Gerät fest zugewiesen. Durch die Zuordnung ist ein USB-Gerät ausschließlich in Kombination mit dem zugewiesenen USB-Port zu betreiben.

Durch eine Gerätezuordnung ist sichergestellt, dass die (sicherheitsrelevanten) Einstellungen von USB-Port und USB-Gerät nicht umgangen werden. Wird an dem USB-Port ein anderes als das zugewiesene USB-Gerät eingesteckt, kann es nicht betrieben werden.

Was möchten Sie tun?

- ☐ 'Zugriff auf USB-Gerät sperren' ⇨ 89
- ☐ 'Zugriff auf USB-Gerät freischalten' ⇨ 89
- ☐ 'Gerätezuordnung am USB-Port definieren' ⇨ 90
- ☐ 'USB-Port-Zugriffskontrolle deaktivieren' ⇨ 90

Zugriff auf USB-Gerät sperren

Um den Zugriff auf ein USB-Gerät zu kontrollieren, muss via myUTN Control Center für den USB-Port ein Schlüssel definiert werden.

Gehen Sie wie folgt vor:

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** *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.

Zugriff auf USB-Gerät freischalten

Damit ein Anwender Zugriff auf ein durch die USB-Portschlüsselkontrolle geschütztes USB-Gerät erhält, muss auf dem Client via SEH UTN Manager ein entsprechender Schlüssel eingegeben werden.

Gehen Sie wie folgt vor:

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 auf das USB-Geräte wird freigegeben. Das USB-Gerät wird in der Auswahlliste angezeigt und kann betrieben werden.

Gerätezuordnung am USB-Port definieren

Um Manipulationen durch Umstecken der USB-Geräte am UTN-Server auszuschließen, können den USB-Ports feste USB-Geräte zugewiesen werden.

Gehen Sie wie folgt vor:

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. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert. Am USB-Port kann ausschließlich das unter 'USB-Port' angezeigte USB-Gerät betrieben werden.

Soll der USB-Port eine Zuweisung mit einem neu angeschlossenen USB-Gerät erzeugen, wählen Sie die Schaltfläche 'Gerät neu zuordnen'.

USB-Port-Zugriffskontrolle deaktivieren

Sie haben die Möglichkeit, die Zugriffskontrolle auf die USB-Ports sowie die angeschlossenen USB-Geräte zu deaktivieren.

Gehen Sie wie folgt vor:

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* **---**.
4. *Bestätigen Sie mit* **Speichern**.

Die USB-Port-Zugriffskontrolle wird deaktiviert. Angeschlossene USB-Geräte können betrieben werden.

6.5 Wie setze ich Zertifikate korrekt ein?

Der UTN-Server verfügt über eine eigene Zertifikatsverwaltung. Dieser Abschnitt informiert Sie über die Anwendung von Zertifikaten und Sie erfahren, in welchen Situationen ein Einsatz sinnvoll ist.

Was sind Zertifikate?

Zertifikate können in TCP/IP-basierten Netzwerken verwendet werden, um Daten zu verschlüsseln und Kommunikationspartner zu authentifizieren. Zertifikate sind elektronische Nachrichten, die einen Schlüssel (Public Key) sowie eine Signatur enthalten.

Nutzen und Zweck

Mit dem Einsatz von Zertifikaten werden mehrere Sicherheitsmechanismen realisiert. Verwenden Sie Zertifikate im UTN-Server,

- um die Identität des UTN-Servers im Netzwerk überprüfen zu lassen; siehe: 'EAP-TLS konfigurieren' ⇨ 100.
- um den UTN-Server/Client zu authentifizieren, wenn der administrative Zugang des myUTN Control Centers via HTTPS (SSL/TLS) geschützt ist.

Wenn Sie Zertifikate verwenden, sollten Sie den administrativen Zugriff zum myUTN Control Center zusätzlich mit einem Passwort schützen, so dass kein Unbefugter Zertifikate auf dem UTN-Server löschen kann; siehe: ⇨ 85.

Welche Zertifikate gibt es?

Im UTN-Server können sowohl selbstsignierte Zertifikate als auch CA-Zertifikate verwendet werden. Es werden die folgenden Zertifikate unterschieden:

- Bei Auslieferung ist im UTN-Server ein Zertifikat gespeichert, das sog. **Defaultzertifikat**. Sie sollten das Defaultzertifikat zeitnah durch ein selbstsigniertes oder ein CA-Zertifikat ersetzen.
- **Selbstsignierte Zertifikate** tragen eine digitale Unterschrift, die vom UTN-Server erstellt wurde.
- **CA-Zertifikate** sind Zertifikate, die von einer Zertifizierungsstelle (Certification Authority - CA) signiert wurden.
- Die Echtheit eines CA-Zertifikats kann mit Hilfe eines **Wurzelzertifikats**, das von der Zertifizierungsstelle ausgegeben

wird, überprüft werden. Dieses Wurzelzertifikat wird auf einem Authentifizierungsserver im Netzwerk hinterlegt.

- **S/MIME-Zertifikate** (*.pem-Datei) werden verwendet zum Signieren und Verschlüsseln der E-Mails, die vom UTN-Server versendet werden. Der zugehörige private Schlüssel ist im PKCS#12-Format (als *.p12-Datei) im vorgesehenen E-Mail-Programm (Mozilla Thunderbird, Microsoft Outlook usw.) als eigenes Zertifikat zu installieren. Nur damit können die E-Mails verifiziert (bzw. im Falle der Verschlüsselung) angesehen werden.
  (nur myUTN-80 und höher)

Im UTN-Server können folgende Zertifikate zeitgleich installiert sein:

- 1 Selbstsigniertes Zertifikat

- 1 CA-Zertifikat oder PKCS#12-Zertifikat

- 1 Wurzelzertifikat

- 1 S/MIME-Zertifikat (nur myUTN-80 und höher)

Zudem kann eine Zertifikatsanforderung für ein CA-Zertifikat generiert sein. Alle Zertifikate können separat gelöscht werden. Durch das Installieren bzw. Generieren neuer Zertifikate werden vorhandene Zertifikate überschrieben.

Ein PKCS#12-Zertifikat kann nur installiert werden, wenn aktuell keine Zertifikatsanforderung generiert bzw. kein CA-Zertifikat installiert ist.

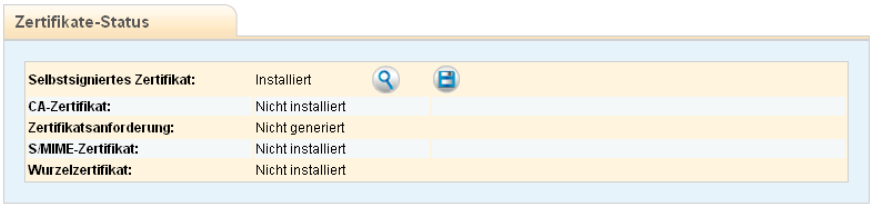


Abb. 15: myUTN Control Center - Zertifikate

Was möchten Sie tun?

- ☐ 'Zertifikat anzeigen' ⇨ 93
- ☐ 'Selbstsigniertes Zertifikat erstellen' ⇨ 93
- ☐ 'Zertifikatsanforderung für ein CA-Zertifikat erstellen' ⇨ 95
- ☐ 'CA-Zertifikat auf dem UTN-Server speichern' ⇨ 95
- ☐ 'Wurzelzertifikat auf dem UTN-Server speichern' ⇨ 96
- ☐ 'PKCS#12-Zertifikat auf dem UTN-Server speichern' ⇨ 97
- ☐ 'S/MIME-Zertifikat auf dem UTN-Server speichern (nur myUTN-80 und höher)' ⇨ 97
- ☐ 'Zertifikat löschen' ⇨ 98

Zertifikat anzeigen

Auf dem UTN-Server installierte Zertifikate oder Zertifikatsanforderungen können dargestellt und eingesehen werden.

Gehen Sie wie folgt vor:

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

Ist bereits ein selbstsigniertes Zertifikat auf dem UTN-Server erstellt worden, muss dieses zunächst gelöscht werden; siehe: ⇨ 98.

Gehen Sie wie folgt vor:

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; siehe: Tabelle 11* ⇨ *94.*

5. *Wählen Sie die Schaltfläche* **Erstellen/Installieren** *an.*

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

Tabelle 11: Parameter für die Erstellung von Zertifikaten

Parameter	Beschreibung
Allgemeiner Name	Dient der eindeutigen Identifizierung des Zertifikats. Es empfiehlt sich, hier z.B. die IP-Adresse oder den Hostnamen des UTN-Servers zu verwenden, um eine eindeutige Zuordnung des Zertifikats zum UTN-Server zu ermöglichen. Maximal 64 Zeichen können eingegeben werden.
E-Mail-Adresse	Gibt eine E-Mail-Adresse an. Maximal 40 Zeichen können eingegeben werden. (Optionale Eingabe)
Organisation	Gibt den Namen der Firma an, die den UTN-Server einsetzt. Maximal 64 Zeichen können eingegeben werden.
Unternehmens-bereich	Gibt die Abteilung oder eine Untergruppe der Firma an. Maximal 64 Zeichen können eingegeben werden. (Optionale Eingabe)
Ort	Gibt den Ort an, an dem die Firma ansässig ist. Maximal 64 Zeichen können eingegeben werden.
Bundesland	Gibt den Namen des Bundeslandes an, in dem die Firma ansässig ist. Maximal 64 Zeichen können eingegeben werden. (Optionale Eingabe)
Domain-Komponente	Ermöglicht das Eintragen weiterer Attribute. (Optionale Eingabe)
Land	Gibt das Land an, in dem die Firma ansässig ist. Geben Sie das zweistellige Länderkürzel gemäß ISO 3166 ein. Beispiele: DE = Deutschland, GB = Großbritannien, US = USA
Ausgestellt am	Gibt das Datum an, ab dem das Zertifikat gültig ist.
Endet am	Gibt das Datum an, 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 (langsame Ver- und Entschlüsselung)

Zertifikatsanforderung für ein CA-Zertifikat erstellen

Als Vorbereitung auf das Verwenden eines CA-Zertifikats kann im UTN-Server eine Zertifikatsanforderung erstellt werden, die an die Zertifizierungsstelle gesendet werden muss. Die Zertifizierungsstelle erstellt anhand der Zertifikatsanforderung ein CA-Zertifikat. Das Zertifikat muss im 'Base64'-Format vorliegen.

Ist bereits eine Zertifikatsanforderung auf dem UTN-Server erstellt worden, muss diese zunächst gelöscht werden; siehe: ⇨ 98.

Gehen Sie wie folgt vor:

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; siehe: Tabelle 11 ⇨ 94.*
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.*

Nach Erhalt muss das CA-Zertifikat auf dem UTN-Server gespeichert werden; siehe: ⇨ 95.

CA-Zertifikat auf dem UTN-Server speichern

Ist bereits ein CA-Zertifikat auf dem UTN-Server installiert, wird es überschrieben.

Voraussetzung

☑ Es wurde zuvor eine entsprechende Zertifikatsanforderung erstellt; siehe: ⇨ 95.

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

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Zertifikate** *an.*
3. *Wählen Sie die Schaltfläche* **Angefordertes Zertifikat** *an.*
4. *Wählen Sie die Schaltfläche* **Durchsuchen** *an.*
5. *Geben Sie das CA-Zertifikat an.*
6. *Wählen Sie die Schaltfläche* **Installieren** *an.*

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

Wurzelzertifikat auf dem UTN-Server speichern

Um in einem Netzwerk die Identität des UTN-Servers zu überprüfen, bietet der UTN-Server mehrere Authentifizierungsverfahren an. Wenn Sie das Authentifizierungsverfahren 'EAP-TLS' verwenden, ist es erforderlich, das Wurzelzertifikat des Authentifizierungsservers (RADIUS) auf den UTN-Server zu installieren; siehe: ⇨ 100.

Ist bereits ein Wurzelzertifikat auf dem UTN-Server installiert, wird es überschrieben.

Voraussetzung

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

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Zertifikate** *an.*
3. *Wählen Sie die Schaltfläche* **Wurzelzertifikat** *an.*
4. *Wählen Sie die Schaltfläche* **Durchsuchen** *an.*
5. *Geben Sie das Wurzelzertifikat an.*
6. *Wählen Sie die Schaltfläche* **Installieren** *an.*

↳ Das Wurzelzertifikat wird auf dem UTN-Server gespeichert.

PKCS#12-Zertifikat auf dem UTN-Server speichern

Zertifikate im PKCS#12-Format werden verwendet, um private Schlüssel mit dem zugehörigen Zertifikat passwortgeschützt zu speichern.

Ist bereits ein PKCS#12-Zertifikat auf dem UTN-Server installiert, wird es überschrieben.

Voraussetzung

- ☑ Das Zertifikat muss im 'Base64'-Format vorliegen.
- ☑ Es darf keine Zertifikatsanforderung vorliegen. Um die Zertifikatsanforderung zu löschen, siehe: ⇨ 98.
- ☑ Es darf kein CA-Zertifikat installiert sein. Um ein CA-Zertifikat zu löschen, siehe: ⇨ 98.

Gehen Sie wie folgt 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. *Wählen Sie die Schaltfläche* **Durchsuchen** *an.*
5. *Geben Sie das PKCS#12-Zertifikat an.*
6. *Geben Sie das Passwort ein.*
7. *Wählen Sie die Schaltfläche* **Installieren** *an.*

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

S/MIME-Zertifikat auf dem UTN-Server speichern (nur myUTN-80 und höher)

S/MIME-Zertifikate (*.pem-Datei) werden verwendet zum Signieren und Verschlüsseln der E-Mails, die vom UTN-Server versendet werden.

Ist bereits ein S/MIME-Zertifikat auf dem UTN-Server installiert, wird es überschrieben.

Gehen Sie wie folgt 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. *Wählen Sie die Schaltfläche* **Durchsuchen** *an.*
5. *Geben Sie das S/MIME-Zertifikat an.*
6. *Wählen Sie die Schaltfläche* **Installieren** *an.*

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

Zertifikat löschen

Gehen Sie wie folgt vor:

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.

6.6 Wie verwende ich Authentifizierungsmethoden?

Durch Authentifizierung kann ein Netzwerk vor unautorisiertem Zugriff geschützt werden. Der UTN-Server ist in der Lage, an verschiedenen Authentifizierungsverfahren teilzunehmen. In diesem Abschnitt erfahren Sie, welche Verfahren unterstützt und wie diese am UTN-Server konfiguriert werden.

Was ist IEEE 802.1x?

Der Standard IEEE 802.1x stellt eine Grundstruktur für verschiedene Authentifizierungs- und Schlüsselverwaltungsprotokolle dar. IEEE 802.1x bietet die Möglichkeit, den Zugang zu Netzwerken zu kontrollieren. Bevor ein Benutzer über ein Netzwerkgerät Zugang zum Netzwerk erhält, muss dieser sich am Netzwerk authentisieren. Nach erfolgreicher Authentisierung wird der Zugang zum Netzwerk freigegeben.

Was ist EAP?

Dem Standard IEEE 802.1x liegt das EAP (Extensible Authentication Protocol) zugrunde. EAP ist ein universelles Protokoll für viele verschiedene Authentifizierungsverfahren. Das EAP ermöglicht einen standardisierten Authentifizierungsvorgang zwischen dem Netzwerkgerät und einem Authentifizierungsserver (RADIUS). Das zu verwendende Authentifizierungsverfahren TLS, PEAP, TTLS usw. muss zuvor definiert und bei allen beteiligten Netzwerkgeräten konfiguriert werden.

Was ist RADIUS?

RADIUS (Remote Authentication Dial-In User Service) ist ein Authentifizierungs- und Kontoverwaltungssystem, das Benutzeranmeldeinformation überprüft und Zugriff auf die gewünschten Ressourcen gewährt.

Damit der UTN-Server sich an einem geschützten Netzwerk authentisieren kann, unterstützt der UTN-Server mehrere EAP-Authentifizierungsverfahren.

Was möchten Sie tun?

- ☐ 'EAP-MD5 konfigurieren' ⇨🗎100
- ☐ 'EAP-TLS konfigurieren' ⇨🗎100
- ☐ 'EAP-TTLS konfigurieren' ⇨🗎102
- ☐ 'PEAP konfigurieren' ⇨🗎103
- ☐ 'EAP-FAST konfigurieren' ⇨🗎104

EAP-MD5 konfigurieren

Nutzen und Zweck

Das EAP-MD5 überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit der UTN-Server in geschützten Netzwerken einen Zugriff erhält, haben Sie die Möglichkeit, den UTN-Server für die EAP-MD5-Netzwerkauthentifizierung zu konfigurieren.

Funktionsweise

EAP-MD5 beschreibt eine benutzerbasierte Authentifizierung über einen RADIUS-Server. Hierzu wird auf dem RADIUS-Server der UTN-Server als Benutzer (mit einem Benutzernamen und einem Passwort) angelegt. Anschließend wird das EAP-MD5-Authentifizierungsverfahren auf dem UTN-Server aktiviert und die beiden Benutzerangaben (Benutzername und Passwort) werden eingegeben.

Voraussetzung

☑ Auf dem RADIUS-Server ist der UTN-Server als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

Gehen Sie wie folgt vor:

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

Nutzen und Zweck

Das EAP-TLS (Transport Layer Security) überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit der UTN-Server in geschützten Netzwerken einen Zugriff erhält, haben Sie die Möglichkeit, den UTN-Server für die EAP-TLS-Netzwerkauthentifizierung zu konfigurieren.

Funktionsweise

EAP-TLS beschreibt eine zertifikatbasierte Authentifizierung über einen RADIUS-Server. Hierzu werden zwischen dem UTN-Server und dem RADIUS-Server Zertifikate ausgetauscht. Dabei wird eine verschlüsselte TLS-Verbindung zwischen UTN-Server und RADIUS-Server aufgebaut. Sowohl RADIUS-Server als auch UTN-Server benötigen ein gültiges digitales von einer CA unterschriebenes Zertifikat, das diese gegenseitig überprüfen müssen. Ist die beidseitige Authentisierung erfolgreich, wird der Zugang freigegeben.

Da jedes Gerät ein Zertifikat benötigt, muss eine PKI (Public Key Infrastructure) vorhanden sein. Benutzerpasswörter sind nicht erforderlich.

Um eine EAP-TLS-Authentifizierung anzuwenden, stellen Sie sicher, dass die unten aufgeführten Punkte in der angegebenen Reihenfolge erfüllt werden. Wird die Vorgehensweise nicht eingehalten, kann der UTN-Server im Netzwerk möglicherweise nicht angesprochen werden. Setzen Sie in diesem Fall die UTN-Server-Parameter zurück; siehe: ⇨ 110.

Vorgehensweise

- Erstellen Sie auf dem UTN-Server eine Zertifikatsanforderung; siehe: ⇨ 95.
- Erstellen Sie mit der Zertifikatsanforderung und mit Hilfe des Authentifizierungsservers ein CA-Zertifikat.
- Installieren Sie das CA-Zertifikat auf dem UTN-Server; siehe: 'CA-Zertifikat auf dem UTN-Server speichern' ⇨ 95.
- Installieren Sie das Wurzelzertifikat des Authentifizierungsservers auf dem UTN-Server; siehe: 'Wurzelzertifikat auf dem UTN-Server speichern' ⇨ 96.
- Aktivieren Sie das Authentifizierungsverfahren 'EAP-TLS' auf dem UTN-Server.

Gehen Sie wie folgt vor:

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

3. *Wählen Sie aus der Liste* **Authentifizierungsmethode** *den Eintrag* **TLS**.
4. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

EAP-TTLS konfigurieren

Nutzen und Zweck

Das EAP-TTLS (Tunneled Transport Layer Security) überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit der UTN-Server in geschützten Netzwerken einen Zugriff erhält, haben Sie die Möglichkeit, den UTN-Server für die EAP-TTLS-Netzwerkauthentifizierung zu konfigurieren.

Funktionsweise

EAP-TTLS besteht aus zwei Phasen:

- In der Phase 1 wird zunächst ein verschlüsselter TLS-Tunnel zwischen UTN-Server und RADIUS-Server aufgebaut. Dazu identifiziert sich nur der RADIUS-Server mit einem von einer CA unterschriebenen Zertifikat beim UTN-Server. Dieser Vorgang wird auch als 'Äußere Authentifizierung' bezeichnet.
- In der Phase 2 wird für die Kommunikation innerhalb des TLS-Tunnels eine weitere Authentifizierungsmethode angewandt. Dabei werden die von EAP definierten sowie ältere Methoden (CHAP, PAP, MS-CHAP und MS-CHAPv2) unterstützt. Dieser Vorgang wird auch als 'Innere Authentifizierung' bezeichnet.

Vorteil dieses Verfahrens ist, dass nur der RADIUS-Server ein Zertifikat benötigt. Es muss somit keine PKI-Struktur vorhanden sein. Zudem unterstützt TTLS die meisten Authentisierungsprotokolle.

Voraussetzung

☑ Auf dem RADIUS-Server ist der UTN-Server als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

Gehen Sie wie folgt vor:

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. *Installieren Sie optional ein Wurzelzertifikat des RADIUS-Servers auf dem UTN-Server (⇨ 96), um die Sicherheit beim Verbindungsaufbau zu erhöhen.*
7. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

PEAP konfigurieren

Nutzen und Zweck

Das PEAP (Protected Extensible Authentication Protocol) überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit der UTN-Server in geschützten Netzwerken einen Zugriff erhält, haben Sie die Möglichkeit, den UTN-Server für die PEAP-Netzwerkauthentifizierung zu konfigurieren.

Funktionsweise

Beim PEAP wird (wie bei EAP-TTLS, vgl. ⇨ 102) 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.

Vorteil dieses Verfahrens ist, dass nur der RADIUS-Server ein Zertifikat benötigt. Es muss somit keine PKI-Struktur vorhanden sein. PEAP nutzt die Vorteile von TLS auf Serverebene und unterstützt verschiedene Authentifizierungsmethoden, einschließlich Benutzerkennwörtern und Einmalkennwörtern.

Voraussetzung

☑ Auf dem RADIUS-Server ist der UTN-Server als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

Gehen Sie wie folgt vor:

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. *Installieren Sie optional ein Wurzelzertifikat (⇨ 96) des RADIUS-Servers auf dem UTN-Server, um die Sicherheit beim Verbindungsaufbau zu erhöhen.*
7. *Bestätigen Sie mit* **Speichern & Neustart**.

Die Einstellungen werden gespeichert.

EAP-FAST konfigurieren

Nutzen und Zweck

Das EAP-FAST (Flexible Authentication via Secure Tunneling) überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit der UTN-Server in geschützten Netzwerken einen Zugriff erhält, haben Sie die Möglichkeit, den UTN-Server für die EAP-FAST-Netzwerkauthentifizierung zu konfigurieren.

Funktionsweise

EAP-FAST nutzt (wie bei EAP-TTLS, vgl. ⇨ 102) einen Tunnel zum Schutz der Datenübertragung. Der Hauptunterschied besteht darin, dass EAP-FAST keine Zertifikate zum Authentifizieren benötigt. (Die Verwendung von Zertifikaten ist optional).

Um den Tunnel aufzubauen werden PACs (Protected Access Credentials) verwendet. PACs sind Anmeldeinformationen, die bis zu drei Komponenten umfassen können:

- Einen gemeinsamen geheimen Schlüssel, der den zwischen dem UTN-Server und dem RADIUS-Server geteilten Schlüssel enthält.
- Ein undurchsichtiges Element, das dem UTN-Server zur Verfügung steht und dem RADIUS-Server vorgelegt wird, wenn der UTN-Server auf die Netzwerkressourcen zugreifen möchte.
- Zusätzliche Informationen, die für den Client nützlich sein können. (Optional)

EAP-FAST verwendet zwei Methoden, um die PACs auszugeben:

- Der manuelle Liefermechanismus kann jeder Mechanismus sein, den der Administrator für das Netzwerk als sicher erachtet und konfiguriert.
- Die automatische Bereitstellung richtet einen verschlüsselten Tunnel ein, um die Authentifizierung des UTN-Servers sowie die Lieferung der PACs zu schützen.

Voraussetzung

☑ Auf dem RADIUS-Server ist der UTN-Server als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN 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.

6.7 Wie verschlüssele ich die Datenübertragung?

Sie haben die Möglichkeit, die Datenübertragung zwischen den Clients und dem UTN-Server (bzw. den angeschlossenen USB-Geräten) zu verschlüsseln.

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

Bei einer verschlüsselten Verbindung kommunizieren der Client und der UTN-Server über den UTN-SSL-Port. Die Portnummer 9443 ist voreingestellt. Um die Portnummer zu ändern, siehe: ⇨ 55.

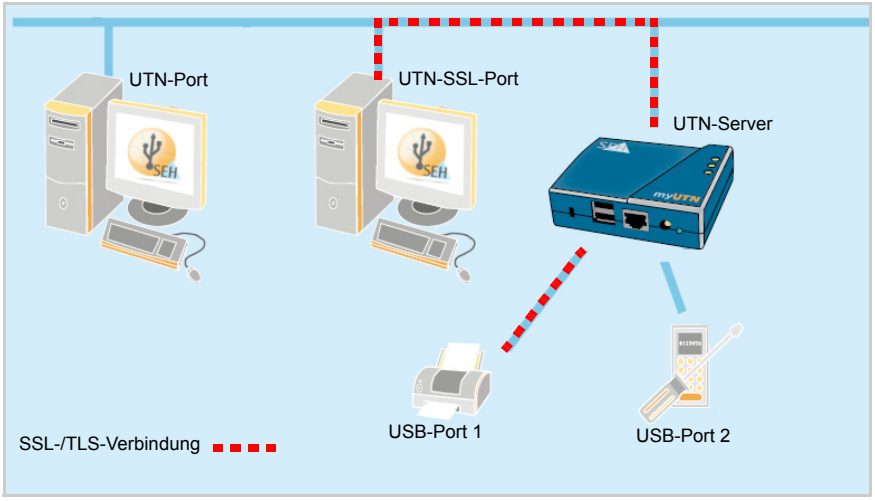


Abb. 16: UTN-Server - SSL-/TLS-Verbindung im Netzwerk

Um eine SSL-/TLS-Verbindung zu verwenden, muss die Verschlüsselung am gewünschten USB-Port aktiviert werden. Die Verschlüsselungsstärke wird über die Verschlüsselungsstufe definiert ⇨ 82.

Gehen Sie wie folgt vor:

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 Geräteeigenschaften angezeigt.

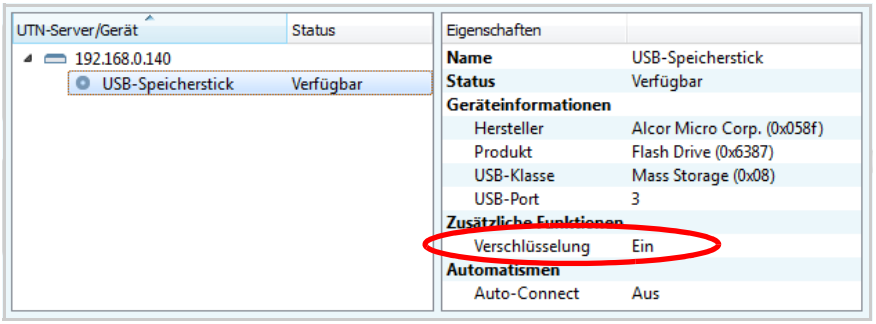


Abb. 17: SEH UTN Manager - Verschlüsselung

7 Wartung

Am UTN-Server können verschiedene Wartungsmaßnahmen durchgeführt werden. Dieses Kapitel informiert Sie über das Sichern und Zurücksetzen der Parameterwerte. Zudem erfahren Sie, wie ein Neustart und ein Update am Gerät durchgeführt werden.

Welche Information benötigen Sie?

- 'Wie sichere ich die UTN-Parameter? (Backup)' ⇨ 108
- 'Wie setze ich die UTN-Parameter auf die Standardwerte zurück?' ⇨ 110
- 'Wie führe ich ein Update aus?' ⇨ 113
- 'Wie starte ich den UTN-Server neu?' ⇨ 114

7.1 Wie sichere ich die UTN-Parameter? (Backup)

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

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

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

Was möchten Sie tun?

- ☐ 'Parameterwerte anzeigen' ⇨ 109
- ☐ 'Parameterdatei sichern' ⇨ 109
- ☐ 'Parameterdatei auf den UTN-Server laden' ⇨ 109

Parameterwerte anzeigen

Gehen Sie wie folgt vor:

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.

Detaillierte Beschreibungen zu den Parametern entnehmen Sie der 'Parameterliste' ⇨119.

Parameterdatei sichern

Gehen Sie wie folgt vor:

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.
4. *Speichern Sie die Datei '<Default-Name>_parameter.txt' mit Hilfe Ihres Browsers auf ein lokales System.*

Die Parameterdatei wird kopiert und ist gesichert.

Parameterdatei auf den UTN-Server laden

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - Parameter-Backup** *an.*
3. *Wählen Sie die Schaltfläche* **Durchsuchen** *an.*
4. *Geben Sie die Datei '<Default-Name>_parameter.txt' an.*
5. *Wählen Sie die Schaltfläche* **Importieren** *an.*

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

7.2 Wie setze ich die UTN-Parameter auf die Standardwerte zurück?

Sie haben die Möglichkeit, die Parameter des UTN-Servers auf die Standardwerte (Werkseinstellung) zurückzusetzen. Dabei werden alle zuvor definierten Parameterwerte gelöscht. Installierte Zertifikate bleiben erhalten.

Durch das Zurücksetzen kann sich die IP-Adresse des UTN-Servers ändern und die Verbindung zum myUTN Control Center abbrechen.

Wann ist das Zurücksetzen sinnvoll?

Das Zurücksetzen der Parameter ist z.B. erforderlich, wenn der UTN-Server durch einen Standortwechsel in einem anderen Netzwerk eingesetzt werden soll. Vor dem Wechsel sollten die Parameter auf die Standardeinstellung zurückgesetzt werden, um den UTN-Server im anderen Netzwerk neu zu installieren.

Was möchten Sie tun?

- ☐ 'Parameter via myUTN Control Center zurücksetzen' ⇨ 110
- ☐ 'Parameter via InterCon-NetTool zurücksetzen' ⇨ 111
- ☐ 'Parameter via Reset-Taster zurücksetzen' ⇨ 111

Über den Reset-Taster am Gerät können die Parameter ohne eine Passworteingabe zurückgesetzt werden.

Parameter via myUTN Control Center zurücksetzen

Gehen Sie wie folgt vor:

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

Die Parameter werden zurückgesetzt.

Parameter via InterCon-NetTool zurücksetzen

Gehen Sie wie folgt vor:

1. *Starten Sie das InterCon-NetTool.*
2. *Markieren Sie den UTN-Server in der Geräteliste.*
3. *Wählen Sie im Menü* **Aktionen** *den Befehl* **Standardeinstellung**.
4. *Wählen Sie die Schaltfläche* **Fertigstellen** *an.*

Die Parameter werden zurückgesetzt.

Parameter via Reset-Taster zurücksetzen

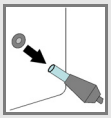
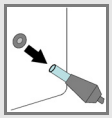
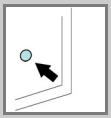
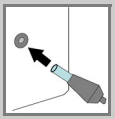
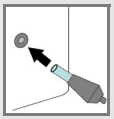
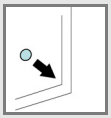
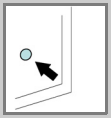
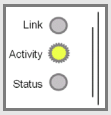
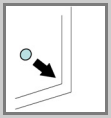
Am UTN-Server finden Sie LEDs, den Reset-Taster sowie verschiedene Anschlüsse. Eine Beschreibung dieser Komponenten finden Sie im 'Quick Installation Guide'.

Über den Reset-Taster können Sie die Parameterwerte des UTN-Servers auf die Standardeinstellung zurücksetzen. Der Reset-Vorgang lässt sich in zwei Phasen gliedern.

- In der 1. Phase wird das Gerät in den Reset-Modus gezwungen. Im Reset-Modus werden die Parameter zurückgesetzt.
- Die 2. Phase beschreibt den Neustart des Gerätes.

WICHTIG: Der Reset-Modus wird durch das synchrone Blinken der Activity-LED (gelb) und der Status-LED (grün) signalisiert und hält für ca. fünf Leuchtintervalle an.
Innerhalb dieses Zeitfensters muss der Reset-Taster losgelassen werden, ansonsten fällt das Gerät in den BIOS-Modus. Beginnen Sie dann den Reset-Vorgang erneut.

Nachfolgend ist der Ablauf aller Phasen visualisiert.

[Phase 1] Reset	[Phase 2] Neustart
 UTN-Server ausschalten (Stromzufuhr unterbrechen).	 UTN-Server ausschalten (Stromzufuhr unterbrechen).
 Reset-Taster drücken und halten.	 UTN-Server einschalten (Stromzufuhr herstellen).
 UTN-Server einschalten (Stromzufuhr herstellen).	
 Warten bis Activity- und Status-LED synchron blinken. *Der Reset-Modus ist aktiviert.*	
 Reset-Taster (für max. 2 Sek) loslassen. *Die LEDs blinken abwechselnd.*	
 Reset-Taster erneut drücken und halten. *Die LEDs blinken synchron.*	
 *Nach einigen Sekunden blinkt ausschließlich die Activity-LED.*	
 Reset-Taster loslassen.	

7.3 Wie führe ich ein Update aus?

Sie haben die Möglichkeit, Soft- und Firmware-Updates auf dem UTN-Server auszuführen. Durch Updates können Sie von aktuell entwickelten Features profitieren.

Was passiert beim Update?

Beim Update wird die vorhandene Firmware/Software von einer neuen Version überschrieben und ersetzt. Die ursprünglichen Parameterwerte des Gerätes bleiben erhalten.

Wann ist ein Update sinnvoll?

Ein Update sollte durchgeführt werden, wenn Funktionen nur eingeschränkt laufen und von der SEH Computertechnik GmbH eine neue Soft- oder Firmware-Version mit neuen Funktionen oder Fehlerbereinigungen bereitgestellt wird.

Überprüfen Sie die installierte Soft- und Firmware-Version auf dem UTN-Server. Die Versionsnummer entnehmen Sie der Startseite des myUTN Control Centers oder der Geräteliste im InterCon-NetTool.

Wo finde ich Update Dateien?

Aktuelle Firmware- und Software-Dateien können von der SEH Computertechnik GmbH-Homepage geladen werden:

http://www.seh.de/services/downloads/myutn.html

Jeder Update-Datei ist eine 'Readme'-Datei zugeordnet. Nehmen Sie die in der 'Readme'-Datei enthaltenen Informationen zur Kenntnis.

Gehen Sie wie folgt vor:

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

Das Update wird ausgeführt. Der UTN-Server wird neu gestartet.

7.4 Wie starte ich den UTN-Server neu?

Nach Parameteränderungen oder nach einem Update wird der UTN-Server automatisch neu gestartet. Befindet sich der UTN-Server in einem undefinierten Zustand, kann der UTN-Server auch manuell neu gestartet werden.

Was möchten Sie tun?

- ☐ 'UTN-Server via myUTN Control Center neu starten' ⇨ 114
- ☐ 'UTN-Server via InterCon-NetTool neu starten' ⇨ 114

UTN-Server via myUTN Control Center neu starten

Gehen Sie wie folgt vor:

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 via InterCon-NetTool neu starten

Gehen Sie wie folgt vor:

1. *Starten Sie das InterCon-NetTool.*
2. *Markieren Sie den UTN-Server in der Geräteliste.*
3. *Wählen Sie im Menü* **Aktionen** *den Befehl* **Neustart**.
4. *Wählen Sie die Schaltfläche* **Fertigstellen** *an.*

↳ Der UTN-Server wird neu gestartet.

8 Anhang

Der Anhang enthält ein Glossar, die Parameterliste des UTN-Servers sowie die Verzeichnislisten dieses Dokumentes.

Welche Information benötigen Sie?

8.1 Glossar

Dieses Glossar informiert Sie über herstellerspezifische Softwarelösungen sowie Begriffe aus der Netzwerktechnologie.

Welche Information benötigen Sie?

Herstellerspezifische Softwarelösungen

- 'myUTN Control Center' ⇨🗎116
- 'InterCon-NetTool' ⇨🗎116
- 'SEH UTN Manager' ⇨🗎116

Netzwerktechnologie

- 'Hardware-Adresse' ⇨🗎117
- 'IP-Adresse' ⇨🗎117
- 'Hostname' ⇨🗎118
- 'Gateway' ⇨🗎118
- 'Netzwerkmaske' ⇨🗎118
- 'Default-Name' ⇨🗎118

myUTN Control Center

Über das myUTN Control Center kann der UTN-Server konfiguriert und überwacht werden. Das myUTN Control Center ist in dem UTN-Server gespeichert und kann mit einer Browsersoftware (Internet Explorer, Mozilla Firefox, Safari) dargestellt werden.

InterCon-NetTool

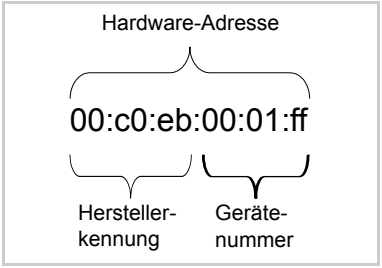
Das InterCon-NetTool ist eine von der SEH Computertechnik GmbH entwickelte Software zur Administration von SEH Netzwerkgeräten innerhalb eines zuvor definierten Netzwerkes.

SEH UTN Manager

Die Zugriffsverteilung der USB-Geräte erfolgt über das Software-Tool SEH UTN Manager. Die Software wird auf alle Clients installiert, die auf ein im Netzwerk bereitgestelltes USB-Gerät zugreifen sollen. Der SEH UTN Manager zeigt die Verfügbarkeit aller in das Netzwerk eingebundenen USB-Geräte an und stellt die Verbindung zwischen Client und USB-Gerät her.

Hardware-Adresse

Der UTN-Server ist über seine weltweit eindeutige Hardware-Adresse adressierbar. Sie wird häufig auch als MAC- oder Ethernet-Adresse bezeichnet. Diese 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 Hardware-Adresse kann am Gehäuse, im SEH UTN Manager oder im InterCon-NetTool abgelesen werden.

Die Verwendung von Trennzeichen in der Hardware-Adresse ist plattformabhängig. Beachten Sie bei Eingabe der Hardware-Adresse die folgende Konvention:

Betriebssystem	Darstellung	Beispiel
Windows	Bindestrich	00-c0-eb-00-01-ff
UNIX	Doppelpunkt oder Punkt	00:c0:eb:00:01:ff bzw. 00.c0.eb.00.01.ff

IP-Adresse

Die IP-Adresse ist eine eindeutige Adresse jedes Knotens in Ihrem Netzwerk, d.h. eine IP-Adresse darf nur einmal in Ihrem lokalen Netzwerk auftreten. Die IP-Adresse wird im Regelfall vom Systemadministrator vergeben. Sie muss im UTN-Server gespeichert werden, damit er im Netzwerk angesprochen werden kann.

Hostname

Der Hostname ist ein Alias für eine IP-Adresse. Mit dem Hostnamen wird der UTN-Server in seinem Netzwerk eindeutig bezeichnet und in einem von Menschen merkbaren Format angegeben.

Gateway

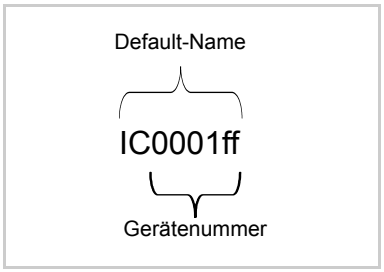
Über ein Gateway können IP-Adressen in einem anderen Netzwerk angesprochen werden. Möchten Sie ein Gateway verwenden, können Sie über das myUTN Control Center den entsprechenden Parameter im UTN-Server konfigurieren.

Netzwerkmaske

Mit Hilfe der Netzwerkmaske können große Netzwerke in Subnetzwerke unterteilt werden. Dabei werden die Teilnehmerkennungen der IP-Adresse verschiedenen Subnetzwerken zugeordnet. Der UTN-Server ist standardmäßig für den Einsatz ohne Subnetzwerke konfiguriert. Möchten Sie ein Subnetzwerk verwenden, können Sie über das myUTN Control Center den entsprechenden Parameter im UTN-Server konfigurieren.

Default-Name

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



Der Default-Name kann im myUTN Control Center oder im Inter-Con-NetTool abgelesen werden.

8.2 Parameterliste

Dieser Abschnitt enthält eine Übersicht mit allen Parametern des UTN-Servers. Die Parameterliste informiert Sie über die Funktion und Wertekonventionen der einzelnen Parameter.

Welche Information benötigen Sie?

Um die aktuellen Parameterwerte Ihres UTN-Servers einzusehen, siehe: 'Parameterwerte anzeigen' ⇨109.

Tabelle 12: Parameterliste - IPv4

Parameter	Wertekonvention	Default	Beschreibung
ip_addr [IP-Adresse]	gültige IP-Adresse	169.254.0.0/16	Definiert die IP-Adresse des UTN-Servers.
ip_mask [Netzwerkmaske]	gültige IP-Adresse	255.255.0.0	Definiert die Netzwerkmaske des UTN-Servers.
ip_gate [Gateway]	gültige IP-Adresse	0.0.0.0	Definiert die Gateway-Adresse des UTN-Servers.
ip_dhcp [DHCP]	on/off	on	De-/aktiviert das DHCP-Protokoll.
ip_bootp [BOOTP]	on/off	on	De-/aktiviert das BOOTP-Protokoll.
ip_auto [ARP/PING]	on/off	on	De-/aktiviert die IP-Adressvergabe via ARP/PING.

Tabelle 13: Parameterliste - IPv4-VLAN (nur myUTN-80 und myUTN-150)

Parameter	Wertekonvention	Default	Beschreibung
ipv4vlan_on_1 ~ ipv4vlan_on_8 [VLan]	on/off	off	De-/aktiviert die Weiterleitung der VLAN-Daten.
ipv4vlan_addr_1 ~ ipv4vlan_addr_8 [IP-Adresse]	gültige IP-Adresse	192.168.0.0	Definiert die IP-Adresse des UTN-Servers innerhalb des VLAN.
ipv4vlan_mask_1 ~ ipv4vlan_mask_8 [Netzwerkmaske]	gültige IP-Adresse	255.255.255.0	Definiert die Netzwerkmaske des UTN-Servers innerhalb des VLAN.

Parameter	Wertekonvention	Default	Beschreibung
ipv4vlan_id_1 ~ ipv4vlan_id_8 [VLAN-ID]	0–4096 [1–4 Zeichen; 0–9]	0	Definiert eine ID zur Identifizierung des VLAN. 0 = unmarkierte multihomed IP-Adressen
ipv4vlan_web [VLAN-Zugriff]	on/off	on	Erlaubt/Sperrt den administrativen Webzugang zum myUTN Control Center über eine VLAN-Adresse.
ipv4vlan_snmp [VLAN-Zugriff]	on/off	on	Erlaubt/Sperrt den administrativen SNMP-Zugang zum myUTN Control Center über eine VLAN-Adresse.

Tabelle 14: Parameterliste - IPv6

Parameter	Wertekonvention	Default	Beschreibung
ipv6 [IPv6]	on/off	on	De-/aktiviert die IPv6-Funktionalität des UTN-Servers.
ipv6_addr [IPv6-Adresse]	n:n:n:n:n:n:n:n	: :	Definiert eine manuell vergebene IPv6-Unicast-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. 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 die IPv6-Unicast-Adresse des Routers, an den der UTN-Server seine 'Router Solicitations' (RS) sendet.

Parameter	Wertekonvention	Default	Beschreibung
ipv6_plen [Präfixlänge]	0–64 [1–2 Zeichen; 0–9]	64	Definiert die Länge des Subnetz-Präfixes für die IPv6-Adresse. *Adressbereiche werden durch Präfixe angegeben. Dazu wird die Präfixlänge (Anzahl der verwendeten Bits) als Dezimalzahl mit vorangehendem '/' an die IPv6-Adresse angehängt dargestellt.*
ipv6_auto [Automatische Konfiguration]	on/off	on	De-/aktiviert die automatische Vergabe der IPv6-Adressen für den UTN-Server.

Tabelle 15: Parameterliste - Bonjour

Parameter	Wertekonvention	Default	Beschreibung
bonjour [Bonjour]	on/off	on	De-/aktiviert den Dienst Bonjour.
bonjour_name [Bonjour-Name]	max. 64 Zeichen [a–z, A–Z, 0–9]	[Default-Name]	Definiert den Bonjour-Namen des UTN-Servers.

Tabelle 16: Parameterliste - SSL-Verbindungen

Parameter	Wertekonvention	Default	Beschreibung
security [Verschlüsselung]	1–4 [1 Zeichen]	2	Definiert die Verschlüsselungsstufe für SSL-/TLS-Verbindungen. *1 = Niedrig (56 Bit)* *2 = Mittel (128 Bit)* *3 = Hoch (128 - 256 Bit)* *4 = Kompatibel (40 - 256 Bit)*

Tabelle 17: Parameterliste - Webzugriff

Parameter	Wertekonvention	Default	Beschreibung
http_pwd [Passwort]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert das Passwort für den administrativen Zugang zum myUTN Control Center.
http_allowed [Zulässige Verbindung]	on/off	on	Definiert den erlaubten Verbindungstyp (HTTP/HTTPS) zum myUTN Control Center. *Wird ausschließlich HTTPS als Verbindungstyp gewählt [http_allowed = off], ist der administrative Zugang zum myUTN Control Center via SSL/TLS geschützt.*

Tabelle 18: Parameterliste - TCP-Portzugriff

Parameter	Wertekonvention	Default	Beschreibung
protection [Portzugriff kontrollieren]	on/off	off	De-/aktiviert die Sperrung von ausgewählten Ports.
protection_test [Testmodus]	on/off	on	De-/aktiviert den Testmodus. *Der Testmodus bietet die Möglichkeit, die über die Zugriffskontrolle eingestellten Parameter zu testen. Bei aktiviertem Testmodus ist der Zugriffsschutz bis zum nächsten Neustart des UTN-Servers aktiv.*
protection_level [Sicherheitsstufe]	protec_utn protec_tcp protec_all	protec_utn	Definiert die zu sperrenden Porttypen: - UTN-Ports - TCP-Ports - alle Ports (IP-Ports)
ip_filter_on_1 ~ ip_filter_on_8 [IP-Adresse]	on/off	off	De-/aktiviert eine Ausnahme von der Portsperrung.

Parameter	Wertekonvention	Default	Beschreibung
ip_filter_1 ~ ip_filter_8 [IP-Adresse]	gültige IP-Adresse	[blank]	Definiert Elemente, die von einer Portsperrung ausgenommen sind über die IP-Adresse.
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 Hardware-Adresse.

Tabelle 19: 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.
utn_sslport [UTN-SSL-Port]	1–9443 [1–4 Zeichen; 0–9]	9443	Definiert die Nummer des UTN-SSL-Ports.

Tabelle 20: Parameterliste - Verschlüsselung

Parameter	Wertekonvention	Default	Beschreibung
utn_sec_1 ~ utn_sec_8 [USB-Port]	on/off	off	De-/aktiviert die SSL-/TLS-Verschlüsselung am USB-Port. *Bei aktivierter Verschlüsselung werden die Nutzdaten zwischen den Clients und den (an den USB-Ports angeschlossenen) USB-Geräten verschlüsselt übermittelt.*

Tabelle 21: Parameterliste - USB-Portzugriff (nur myUTN-80 und höher)

Parameter	Wertekonvention	Default	Beschreibung
utn_heartbeat	1–1800 [1–4 Zeichen; 0–9]	180	**Der Parameter ist ausschließlich in Absprache mit dem SEH Support zu verwenden.**
utn_accctrt_1 ~ utn_accctrt_8 [Methode]	--- ids key keyids	[---]	Definiert Methoden zur Zugriffs- und Nutzungseinschränkung für den USB-Port sowie dem angeschlossenen USB-Gerät. *---* = *kein Schutz* *ids* = *Gerätezuordnung* *key* = *Portschlüsselkontrolle* *keyids* = *Gerätezuordnung und Portschlüsselkontrolle*
utn_keyval_1 ~ utn_keyval_8 [Schlüssel]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert den Schlüssel, mit dem das angeschlossene USB-Gerät vor Zugriff geschützt ist.
utn_prodid_1 ~ utn_prodid_8 [USB-Gerät]			Zeigt die Produkt-ID des USB-Gerätes, welches dem jeweiligen USB-Port zugeordnet ist.
utn_vendid_1 ~ utn_vendid_8 [USB-Gerät]			Zeigt die Vendor-ID des USB-Gerätes, welches dem jeweiligen USB-Port zugeordnet ist.
utn_2vlan_1 ~ utn_2vlan_8 [VLAN zuordnen]	0–9 [1 Zeichen] (vgl. ⇨ 120)	0	Ordnet dem USB-Port ein VLAN zu. *0 = jedes* *1 = VLAN 1* *2 = VLAN 2 usw.* *9 = keines*

Tabelle 22: Parameterliste - USB-Port

Parameter	Wertekonvention	Default	Beschreibung
utn_tag_1 ~ utn_tag_8 [Name]	max. 32 Zeichen [a–z, A–Z, 0–9]	[blank]	Freidefinierbare Beschreibung des USB-Gerätes.
utn_comp_1 [Komprimierung]	on/off	off	De-/aktiviert die Datenkomprimierung für das am USB-Port angeschlossene USB-Gerät (nur myUTN-130).
utn_poff_1 ~ utn_poff_8 [Aktiv]	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*
utn_postreset_1 ~ utn_postreset_8	on/off	off	**Der Parameter ist ausschließlich in Absprache mit dem SEH Support zu verwenden.**

Tabelle 23: 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 den Domain-Namen eines vorhandenen DNS-Servers.
dns_primary [Erster DNS-Server]	gültige IP-Adresse	0.0.0.0	Definiert die IP-Adresse des ersten DNS-Servers.
dns_secondary [Zweiter DNS-Server]	gültige IP-Adresse	0.0.0.0	Definiert die IP-Adresse des zweiten DNS-Servers. *Der zweite DNS-Server wird verwendet, wenn der erste DNS-Server nicht verfügbar ist.*

Tabelle 24: 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	Definiert den Namen der SNMP-Community. *Die SNMP Community stellt eine einfache Form des Zugriffsschutzes dar, in der mehrere Teilnehmer mit gleichen Zugriffsrechten zusammengefasst werden.*
snmpv3 [SNMPv3]	on/off	on	De-/aktiviert die SNMPv3-Funktionalität.
any_name [Benutzername]	max. 64 Zeichen [a–z, A–Z, 0–9]	anonymous	Definiert den Namen der SNMP-Benutzergruppe 1.
any_pwd [Passwort]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert das Passwort der SNMP-Benutzergruppe 1.
any_rights [Zugriffsrechte]	--- [keine] readonly readwrite	readonly	Definiert die Zugriffsrechte der SNMP-Benutzergruppe 1.
any_hash [Hash]	md5 sha	md5	Definiert den Hash-Algorithmus für die SNMP-Benutzergruppe 1.
any_cipher [Verschlüsselung]	--- [keine] aes des	---	Definiert die Verschlüsselungsmethode der SNMP-Benutzergruppe 1.
admin_name [Benutzername]	max. 64 Zeichen [a–z, A–Z, 0–9]	admin	Definiert den Namen der SNMP-Benutzergruppe 2.
admin_pwd [Passwort]	8–64 Zeichen [a–z, A–Z, 0–9]	administrator	Definiert das Passwort der SNMP-Benutzergruppe 2.
admin_rights [Zugriffsrechte]	--- [keine] readonly readwrite	readwrite	Definiert die Zugriffsrechte der SNMP-Benutzergruppe 2.
admin_hash [Hash]	md5 sha	md5	Definiert den Hash-Algorithmus für die SNMP-Benutzergruppe 2.

Parameter	Wertekonvention	Default	Beschreibung
admin_cipher [Verschlüsselung]	--- [keine] aes des	---	Definiert die Verschlüsselungsmethode der SNMP-Benutzergruppe 2.

Tabelle 25: Parameterliste - Datum/Zeit

Parameter	Wertekonvention	Default	Beschreibung
ntp [Datum/Zeit]	on/off	on	De-/aktiviert die Verwendung eines Time-Servers (SNTP).
ntp_server [Time-Server]	max. 64 Zeichen [a–z, A–Z, 0–9]	pool.ntp.org	Definiert einen Time-Server über die IP-Adresse oder den Hostnamen. *Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.*
ntp_tzone [Zeitzone]	UTC, GMT, EST, EDT, CST, CDT, MST, MDT, PST, PDT usw.	CET/CEST (EU)	Gleicht die Differenz zwischen der über einen Time-Server empfangenen Zeit und Ihrer lokalen Zeitzone aus.

Tabelle 26: Parameterliste - Beschreibung

Parameter	Wertekonvention	Default	Beschreibung
sys_name [Hostname]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert den Hostnamen des UTN-Servers.
sys_descr [Beschreibung]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Freidefinierbare Beschreibung
sys_contact [Ansprechpartner]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Freidefinierbare Beschreibung (des Ansprechpartners)

Tabelle 27: Parameterliste - Authentifizierung

Parameter	Wertekonvention	Default	Beschreibung
auth_typ [Authentifizierungsmethode]	--- [keine] MD5 TLS TTLS PEAP FAST	----	Definiert die EAP-Authentifizierungsmethode, mit der sich der UTN-Server im Netzwerk identifiziert.
auth_name [Benutzername]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert den Namen des UTN-Servers, wie er auf dem Authentifizierungsserver (RADIUS) gespeichert ist.
auth_pwd [Passwort]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert das Passwort des UTN-Servers, wie es auf dem Authentifizierungsserver (RADIUS) gespeichert ist.
auth_intern [Innere Authentifizierung]	--- = keine PAP = PAP CHAP = CHAP MSCHAP2 = MS-CHAPv2 EMD5 = EAP-MD5 ETLS = EAP-TLS	---	Definiert die Art der inneren Authentifizierung bei den EAP-Authentifizierungsmethoden TTLS, PEAP und FAST.
auth_extern [PEAP/EAP-FAST-Optionen]	--- = keine PLABEL0 = PEAPLABEL0 PLABEL1 = PEAPLABEL1 PVER0 = PEAPVER0 PVER1 = PEAPVER1 FPROV1 = FASTPROV1	---	Definiert die Art der äußeren Authentifizierung bei den EAP-Authentifizierungsmethoden TTLS, PEAP und FAST.
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.

Tabelle 28: Parameterliste - POP3 (nur myUTN-80 und höher)

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_poll [E-Mails abfragen alle]	1–10080 [1–5 Zeichen; 0–9]	2	Definiert das Zeitintervall (in Minuten) für die Abfrage der E-Mails auf dem POP3-Server.
pop3_port [Serverport]	1–65535 [1–5 Zeichen; 0–9]	110	Definiert den Port des POP3-Servers, über den der UTN-Server E-Mails empfängt. *Bei Verwendung von SSL/TLS ist als Portnummer 995 einzutragen.*
pop3_usr [Benutzername]	max. 128 Zeichen	[blank]	Definiert den Namen, den der UTN-Server benutzt, um sich am POP3-Server anzumelden.
pop3_pwd [Passwort]	max. 128 Zeichen	[blank]	Definiert das Passwort, das der UTN-Server benutzt, um sich am POP3-Server anzumelden.
pop3_sec [Sicherheit]	0 = --- (keine Sicherheit) 1 = APOP 2 = SSL/TLS	0	Definiert ein Authentifizierungsverfahren.
pop3_limit [E-Mails ignorieren mit mehr als]	0–4096 [1–5 Zeichen; 0–9; 0 = unbegrenzt]	4096	Definiert die maximale Größe (in Kbyte) der vom UTN-Server akzeptierten E-Mails.

Tabelle 29: Parameterliste - SMTP (nur myUTN-80 und höher)

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 die Portnummer, über die der SMTP-Server E-Mails von dem UTN-Server empfängt.
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.
smtp_sender [Name des Absenders]	max. 128 Zeichen	[blank]	Definiert die E-Mail-Adresse, die der UTN-Server zum Versenden von E-Mails verwendet. Hinweis: Oft sind der Name des Absenders und der Benutzername identisch.
smtp_ssl [TLS]	on/off	off	De-/aktiviert die Option TLS. *Über das Sicherheitsprotokoll Transport Layer Security (TLS) wird der Übertragungsweg vom UTN-Server zum SMTP-Server verschlüsselt.*
smtp_auth [Anmelden]	on/off	off	De-/aktiviert die SMTP-Authentifizierung für das Login.
smtp_sign [Sicherheit (S/MIME)]	on/off	off	De-/aktiviert das Verschlüsseln und Signieren der E-Mails via S/MIME.

Parameter	Wertekonvention	Default	Beschreibung
smtp_attpkey [Öffentlichen Schlüssel beifügen]	on/off	on	De-/aktiviert das Hinzufügen eines öffentlichen Schlüssels zu einer E-Mail.
smtp_encrypt [Vollständig verschlüsseln] [E-Mail signieren]	on/off	off	Definiert das Signieren und Verschlüsseln von E-Mails. *off = signieren* *on = verschlüsseln*

Tabelle 30: Parameterliste - Benachrichtigung (nur myUTN-80 und höher)

Parameter	Wertekonvention	Default	Beschreibung
trapto_1 trapto_2 [Adresse]	gültige IP-Adresse	0.0.0.0	Definiert die SNMP-Trap-Adresse des Empfängers.
trapcommu_1 trapcommu_2 [Community]	max. 64 Zeichen [a–z, A–Z, 0–9]	public	Definiert die SNMP-Trap-Community des Empfängers.
trapdev [Sende Trap nach dem Verbinden oder Trennen 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.
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.
trapact [Sende Trap nach der Aktivierung oder Deaktivierung eines USB-Gerätes]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch das Aktivieren oder Deaktivieren eines USB-Gerätes ausgelöst wird.
mailto_1 mailto_2 [E-Mail Adresse]	gültige E-Mail Adresse [max. 64 Zeichen]	[blank]	Definiert die E-Mail-Adresse des Empfängers für Benachrichtigungen.

Parameter	Wertekonvention	Default	Beschreibung
noti_dev_1 noti_dev_2 [Sende E-Mail nach dem Verbinden oder Trennen 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.
noti_act_1 noti_act_2 [Sende E-Mail nach der Aktivierung oder Deaktivierung eines USB-Gerätes]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch das Aktivieren oder Deaktivieren eines USB-Gerätes ausgelöst wird.
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.
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.
notistat_d [Intervall]	al = täglich su = Sonntag mo = Montag tu = Dienstag we = Mittwoch th = Donnerstag fr = Freitag sa = Samstag	al	Definiert das Intervall, mit dem eine Status-E-Mail versendet wird.
notistat_h [hh]	1 = 1. Stunde 2 = 2. Stunde 3 = 3. Stunde usw.	0	Definiert die Uhrzeit, zu der eine Status-E-Mail versendet wird.
notistat_tm [mm]	0 = 00 min 1 = 10 min 2 = 20 min 3 = 30 min 4 = 40 min 5 = 50 min 6 = 00 min	0	Definiert die Uhrzeit, zu der eine Status-E-Mail versendet wird.

Tabelle 31: Parameterliste - WLAN (nur myUTN-54)

Parameter	Wertekonvention	Default	Beschreibung
wifi [WLAN]	on/off	on	De-/aktiviert das WLAN-Modul im UTN-Server.
wifi_mode [Modus]	adhoc infra	adhoc	Definiert den Kommunikationsmodus. *Über den Kommunikationsmodus legen Sie fest, in welcher Netzwerkstruktur der UTN-Server installiert werden soll. Zwei Modi stehen zur Verfügung:* *- Ad-Hoc* *- Infrastructure*
wifi_channel [Kanal]	1–14 (länderspezifisch)	3	Definiert den Kanal, auf dem gesendet wird. *Treten Interferenzen auf, sollte der Kanal (Frequenzbereich) gewechselt werden.* **Informieren Sie sich über die nationalen Bestimmungen für den Einsatz von WLAN-Produkten und verwenden Sie nur zugelassene Kanäle.**
wifi_name [Netzwerkname (SSID)]	max. 64 Zeichen [a–z, A–Z, 0–9, _, -]	SEH	Definiert den SSID. *Als SSID (Service Set Identifier) oder auch Netzwerkname wird eine Funk-Netzwerk-Kennung bezeichnet. Jedes Wireless LAN besitzt einen konfigurierbaren SSID, um das Funknetz eindeutig identifizieren zu können.*

Parameter	Wertekonvention	Default	Beschreibung
wifi_encrypt [Verschlüsselungs-methode]	--- [keine] WepOpen = WEP (Open System) WepShared = WEP (Shared Key) TKIP = WPA (TKIP) AES = WPA (AES) TKIP2 = WPA2 (TKIP) AES2 = WPA2 (AES) AESTKIP = WPA (AES/TKIP) AESTKIP2 = WPA2 (AES/TKIP) Auto = WPA (Auto)	---	Definiert das anzuwendende Verschlüsselungsverfahren, über das der Zugang zum WLAN geschützt wird.
wifi_keyid [WEP Schlüssel verwenden]	1 = Schlüssel 1 2 = Schlüssel 2 3 = Schlüssel 3 4 = Schlüssel 4	0	Definiert den anzuwendenden WEP-Schlüssel.
wifi_wepkey1 wifi_wepkey2 wifi_wepkey3 wifi_wepkey4 [Schlüssel 1-4]	Die max. Zeichen-anzahl ist abhängig vom gewählen Schlüsseltyp: 64 ASCII = 5 64 HEX = 10 128 ASCII = 13 128 HEX = 26	[blank]	Definiert die WEP-Schlüssel. Vier WEP-Schlüssel sind möglich. *Folgende Zeichen können eingegeben werden:* *- bei HEX = 0–9, a–f, A–F* *- bei ASCII = 0–9, a–z, A–Z*
wifi_psk [PSK]	8–63 Zeichen	[blank]	Definiert den Pre Shared Key (PSK) für Wi-Fi Protected Access (WPA).

Parameter	Wertekonvention	Default	Beschreibung
wifi_roaming [Roaming]	on/off	off	De-/aktiviert die Verwendung von Roaming. *Roaming bezeichnet das 'Wandern' von einer Funkzelle zur nächsten. Der UTN-Server verwendet dann den Access Point, der das bessere Signal liefert. Wird der UTN-Server in den Einflussbereich eines anderen Access Points bewegt, wechselt er automatisch und ohne Verbindungsabbruch in die nächste Funkzelle.*
wifi_dbmroam [Roaming-Level]	0–100 [1–3 Zeichen; 0–9]	0	Definiert die Sendeleistung des UTN-Servers in -dBm.

8.3 LED-Anzeige

Ein UTN-Server verfügt über LEDs. Durch die Interpretation des LED-Leuchtverhaltens kann der Zustand des UTN-Servers ermittelt werden.

Während des Einschaltvorgangs weicht das LED-Leuchtverhalten von der Beschreibung ab.

LED	Aktion	Farbe	Beschreibung
Link	Dauer-An	grün	Eine Verbindung zum Netzwerk ist vorhanden.
	Dauer-Aus	-	Es besteht keine Verbindung zum Netzwerk.
Activity	unregelmäßiges Blinken	gelb	Signalisiert den Austausch von Netzwerk-Datenpaketen.
Status	Dauer-Aus	-	Es besteht keine Verbindung zu einem USB-Gerät. ACHTUNG: Bei gleichzeitigem zyklischen Blinken der Activity-LED wird der BIOS-Modus signalisiert. Der UTN-Server ist im BIOS-Modus nicht funktionsfähig; siehe: ⇨ 141.
	Dauer-An	grün	Signalisiert die Verbindung von mindestens einem USB-Gerät.
	3 x Blinken	grün	Signalisiert die Vergabe einer ZeroConfig-IP-Adresse. HINWEIS: Dauerhaft ist eine IP-Adresse zu bevorzugen, die nicht aus dem Bereich ZeroConf kommt.
	2 x Blinken	grün	Signalisiert die Vergabe einer IP-Adresse, die nicht 0.0.0.0 entspricht oder aus dem Bereich ZeroConfig kommt.

Die UTN-Server 'myUTN-80', 'myUTN-120', 'myUTN-130' und 'myUTN-150' verfügen abweichende LEDs. Deren Beschreibung entnehmen Sie dem entsprechenden 'Quick Installation Guide'.

8.4 SEH UTN Manager - Funktionsübersicht

Im SEH UTN Manager können Funktionen gar nicht oder als inaktiv (ausgegraut) dargestellt werden. Dies steht in Abhängigkeit zu den folgenden Faktoren:

- Auswahllisten-Modus-Einstellung (global / benutzerindividuell)
- Benutzergruppen
  - Benutzer, die der Gruppe 'Administrator' zugehörig sind
  - Benutzer, die nicht der Gruppe 'Administrator' zugehörig sind
    + Benutzer mit Schreibrecht auf die *.ini-Datei (Auswahlliste)
    + Benutzer ohne Schreibrecht auf die *.ini-Datei (Auswahlliste)

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

Die Tabellen geben einen Überblick:

- für Windows siehe: Tabelle 32 ⇨139
- für Mac siehe: Tabelle 33 ⇨140

Die Tabellen zeigen die grundsätzlich vorhandenen Funktionen. Zusätzlich werden einzelne Funktionen gar nicht oder als inaktiv dargestellt in Abhängigkeit zu
– dem eingebundenen UTN-Server-Modell
– den Einstellungen der produkteigenen Sicherheitsmechanismen

Tabelle 32: SEH UTN Manager - Funktionsübersicht Windows

	Globale Auswahlliste		Benutzerindividuelle Auswahlliste		
	Admin	User	Admin	User (rw) (INI)	User (r) (INI)
Menü					
Auswahlliste – Bearbeiten	✓	×	✓	✓	×
Auswahlliste – Exportieren	✓	×	✓	×	×
Auswahlliste – Aktualisieren	✓	✓	✓	✓	✓
UTN-Server – Konfigurieren	✓	✓	✓	✓	✓
UTN-Server – IP-Adresse definieren	✓	✓	✓	✓	✓
UTN-Server – USB-Portschlüssel eingeben	✓	×	✓	✓	×
UTN-Server – Hinzufügen	✓	×	✓	✓	×
UTN-Server – Entfernen	✓	×	✓	✓	×
UTN-Server – Aktualisieren	✓	✓	✓	✓	✓
Gerät – Aktivieren	✓	✓	✓	✓	✓
Gerät – Deaktivieren	✓	✓	✓	✓	✓
Gerät – Anfordern	✓	✓	✓	✓	✓
Gerät – Entfernen	✓	×	✓	×	×
Gerät – UTN Aktion erstellen	✓	✓	✓	✓	✓
Gerät – Einstellungen	✓	✓	✓	✓	✓
Schaltflächen					
Auswahlliste – Aktualisieren	✓	✓	✓	✓	✓
Auswahlliste – Bearbeiten	✓	×	✓	✓	×
Gerät – Aktivieren	✓	✓	✓	✓	✓
Gerät – Deaktivieren	✓	✓	✓	✓	✓
Dialog 'Programm – Optionen'					
Netzwerksuche – Multicastsuche	✓	×	✓	×	×
Netzwerksuche – Netzwerkbereichsuche	✓	×	✓	×	×
Programm – Programmsprache	✓	✓	✓	✓	✓
Programm – Programmmeldungen	✓	×	✓	×	×
Programm – Programm-Update	✓	×	✓	×	×
Automatismen – Programmstart (Autostart)	✓	✓	✓	✓	✓
Automatismen – Automatische Gerätetrennung (Auto-Disconnect)	✓	×	✓	×	×
Auswahlliste – Auswahllisten-Modus	✓	×	✓	×	×
Auswahlliste – Automatische Aktualisierung	✓	×	✓	×	×
Dialog 'Geräteeinstellungen'					
Automatische Geräteverbindung – Auto-Connect	✓	×	✓	×	×
Automatische Geräteverbindung – Print-On-Demand	✓	×	✓	×	×
Meldungen	✓	✓	✓	✓	✓

✓ = aktiv
× = inaktiv (ausgegraut)

r = read only (schreibgeschützt)
rw = read and write (Lesen und Schreiben)
INI = *.ini-Datei (⇨ 75)

Tabelle 33: SEH UTN Manager - Funktionsübersicht Mac

	Globale Auswahlliste		Benutzerindividuelle Auswahlliste		
	Admin	User	Admin	User (rw) (INI)	User (r) (INI)
Menü					
Auswahlliste – Bearbeiten	✓	×	✓	✓	×
Auswahlliste – Exportieren	✓	×	✓	×	×
Auswahlliste – Aktualisieren	✓	✓	✓	✓	✓
UTN-Server – Konfigurieren	✓	✓	✓	✓	✓
UTN-Server – IP-Adresse definieren	✓	✓	✓	✓	✓
UTN-Server – USB-Portschlüssel eingeben	✓	×	✓	✓	×
UTN-Server – Hinzufügen	✓	×	✓	✓	×
UTN-Server – Entfernen	✓	×	✓	✓	×
UTN-Server – Aktualisieren	✓	✓	✓	✓	✓
Gerät – Aktivieren	✓	✓	✓	✓	✓
Gerät – Deaktivieren	✓	✓	✓	✓	✓
Gerät – Anfordern	✓	✓	✓	✓	✓
Gerät – Entfernen	✓	×	✓	×	×
Gerät – UTN Aktion erstellen	✓	✓	✓	✓	✓
Gerät – Einstellungen	✓	✓	✓	✓	✓
Schaltflächen					
Auswahlliste – Aktualisieren	✓	✓	✓	✓	✓
Auswahlliste – Bearbeiten	✓	×	✓	✓	×
Gerät – Aktivieren	✓	✓	✓	✓	✓
Gerät – Deaktivieren	✓	✓	✓	✓	✓
Dialog 'SEH UTN Manager – Einstellungen'					
Netzwerksuche – Multicastsuche	✓	×	✓	×	×
Netzwerksuche – Netzwerkbereichsuche	✓	×	✓	×	×
Programm – Programmmeldungen	nur in Windows funktional				
Programm – Programm-Update	✓	×	✓	×	×
Automatismen – Programmstart (Autostart)	✓	✓	✓	✓	✓
Automatismen – Automatische Gerätetrennung (Auto-Disconnect)	✓	×	✓	×	×
Auswahlliste – Auswahllisten-Modus	✓	×	✓	×	×
Auswahlliste – Automatische Aktualisierung	✓	×	✓	×	×
Dialog 'Geräteeinstellungen'					
Automatische Geräteverbindung – Auto-Connect	✓	×	✓	×	×
Automatische Geräteverbindung – Print-On-Demand	✓	×	✓	×	×
Meldungen	nur in Windows funktional				

✓ = aktiv
× = inaktiv (ausgegraut)

r = read only (schreibgeschützt)
rw = read and write (Lesen und Schreiben)
INI = *.ini-Datei (⇨ 📄75)

8.5 Problembehandlung

Dieses Kapitel stellt einige Problemursachen und erste Lösungshilfen dar.

Problemdarstellung

- 'Der UTN-Server signalisiert den BIOS-Modus' ⇨ 141
- 'Im SEH UTN Manager sind Funktionen ausgeblendet bzw. deaktiviert' ⇨ 143
- 'Die Verbindung zum UTN-Server kann nicht hergestellt werden' ⇨ 143
- 'Die Verbindung zum USB-Gerät kann nicht hergestellt werden' ⇨ 143
- 'Die Verbindung zum myUTN Control Center kann nicht hergestellt werden' ⇨ 144
- 'Das Passwort ist nicht mehr verfügbar' ⇨ 144

Der UTN-Server signalisiert den BIOS-Modus

Mögliche Ursache

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. Der UTN-Server signalisiert den BIOS-Modus, indem

- die Netzaktivität-LED (gelb) zyklisch blinkt und
- die Status-LED (grün) nicht aktiv ist.

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

Ist ein UTN-Server im BIOS-Modus, wird in der Geräteliste des InterCon-NetTools automatisch der Filter 'BIOS-Modus' angelegt. Innerhalb dieses Filters wird der UTN-Server angezeigt.

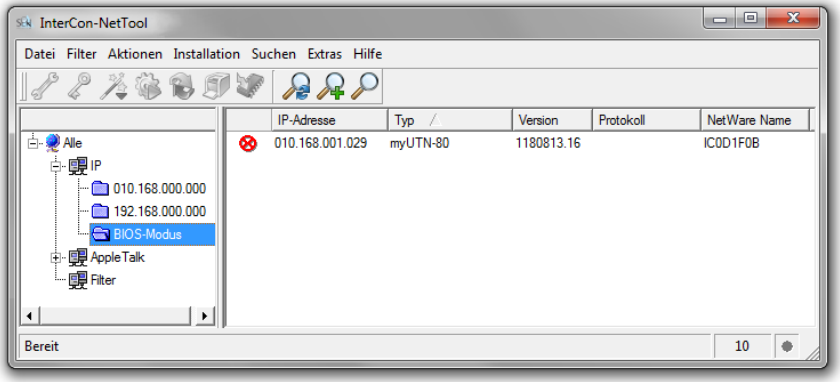


Abb. 18: InterCon-NetTool - UTN-Server im BIOS-Modus

Damit der UTN-Server vom BIOS-Modus in den Standardmodus wechselt, muss auf dem UTN-Server die Software neu aufgespielt werden.

Gehen Sie wie folgt vor:

1. *Starten Sie das InterCon-NetTool.*
2. *Markieren Sie den UTN-Server in der Geräteliste.*
   (Sie finden den UTN-Server unter dem Filter 'BIOS-Modus'.)
3. *Wählen Sie im Menü* **Installation** *den Befehl* **IP-Assistent**.
   Der IP-Assistent wird gestartet.
4. *Weisen Sie dem UTN-Server eine IP-Adresse zu, indem Sie den Anweisungen des Assistenten folgen.*
   Die IP-Adresse wird gespeichert.
5. *Führen Sie auf dem UTN-Server ein Softwareupdate durch;*
   siehe: ⇨ 113.

Die Software wird auf dem UTN-Server gespeichert. Der UTN-Server wechselt in den Standardbetrieb.

Im SEH UTN Manager sind Funktionen ausgeblendet bzw. deaktiviert

Mögliche Ursache

- ☐ Ihr Benutzerkonto verfügt nicht über die erforderlichen administrativen Rechte. Hierdurch haben Sie auch im SEH UTN Manager eingeschränkte Benutzerrechte; siehe: 'SEH UTN Manager - Funktionsübersicht' ⇨📄138.
- ☐ Eine Funktion wird nicht vom angeschlossenen USB-Gerät unterstützt (z.B. kann die Funktion 'Print-On-Demand' nicht durch eine Festplatte unterstützt werden).

Starten Sie den SEH UTN Manager als Administrator. Lesen Sie hierzu die Dokumentation Ihres Betriebssystems.

Die Verbindung zum UTN-Server kann nicht hergestellt werden

Für den Datentransfer zwischen UTN-Server und dem auf den Client installierten SEH UTN Manager wird ein gemeinsamer Port verwendet; siehe: ⇨📄55.

Mögliche Ursache

- ☐ Die Portnummern sind nicht identisch.
  Die aktuelle Portnummer kann nicht an die auf den Clients installierten SEH UTN Manager weitergeleitet werden.
  Der Parameter 'SNMPv1' ist deaktiviert; siehe ⇨📄42.
- ☐ Die Kommunikation wird durch eine Sicherheitssoftware (Firewall) blockiert.

Die Verbindung zum USB-Gerät kann nicht hergestellt werden

Mögliche Ursache

- ☐ Die Zugriffskontrolle für USB-Geräte ist aktiviert ⇨📄88.
- ☐ Auf dem Client ist keine Treibersoftware für das USB-Gerät installiert.
- ☐ Das USB-Gerät ist bereits mit einem anderen Client verbunden.

Die Verbindung zum myUTN Control Center kann nicht hergestellt werden

Schließen Sie Fehlerquellen aus. Überprüfen Sie zunächst:

- die Kabelverbindungen
- die IP-Adresse des UTN-Servers ⇨ 14 sowie
- die Proxy-Einstellungen Ihres Browsers

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

- ☐ Der Zugang ist via SSL/TLS (HTTPS) geschützt ⇨ 84.
- ☐ Die TCP-Portzugriffskontrolle ist aktiviert ⇨ 86.
- ☐ Der Passwortschutz ist aktiviert ⇨ 85.
- ☐ Die Cipher Suites der Verschlüsselungsstufe werden vom Browser nicht unterstützt ⇨ 82.

Das Passwort ist nicht mehr verfügbar

Der Zugriff auf das myUTN Control Center kann durch ein Passwort geschützt werden. Ist das Passwort nicht mehr verfügbar, können die Parameterwerte des UTN-Servers auf die Standardwerte zurückgesetzt werden, um Zugriff zu erhalten ⇨ 110. Dabei gehen sämtliche Einstellungen verloren.

8.6 Zusatztool 'utnm'

utnm

Das Zusatztool 'utnm' wurde speziell entwickelt für die myUTN-Produkte von SEH Computertechnik GmbH. Es wird verwendet zum Aktivieren und Deaktivieren von USB-Geräten.

Verwendung

Für das Aktivieren oder Deaktivieren eines USB-Gerätes mit utnm werden Befehle in einer speziellen Syntax in die Kommandozeile des Betriebssystems eingegeben und ausgeführt.

Alternativ wird ein Skript für das USB-Gerät geschrieben. Das Skript enthält Kommandozeilenbefehle in einer speziellen Syntax. Wird es ausgeführt, werden die Befehle vom Kommandozeileninterpreter Schritt für Schritt automatisch abgearbeitet.

Nutzen und Zweck

Durch die Verwendung von utnm ist es nicht erforderlich, die SEH UTN Manager-Oberfläche zu öffnen bzw. zu installieren (Minimal-Variante des SEH UTN Managers ⇨ 22).

Häufig wiederkehrende Kommandofolgen, z.B. eine Geräteaktivierung, lassen sich mit Skripten automatisieren. Das Ausführen von Skripten kann automatisiert werden, z.B. via Loginskript.

Was möchten Sie tun?

- ☐ 'Kommandozeile verwenden' ⇨ 145
- ☐ 'Skript erstellen' ⇨ 146

Kommandozeile verwenden

Voraussetzung

- ☑ Der SEH UTN Manager ist auf dem Client installiert; siehe: ⇨ 21.
- ☑ IP-Adresse oder Hostname eines UTN-Servers sind bekannt.

Gehen Sie wie folgt vor:

1. *Öffnen Sie die Kommandozeile.*
2. *Geben Sie die Befehlsfolge ein; siehe 'Syntax und Befehle'* ⇨ *146*.
3. *Bestätigen Sie die Eingabe.*

↳ Die Befehlsfolge wird ausgeführt.

Skript erstellen

Voraussetzung

☑ Der SEH UTN Manager ist auf dem Client installiert; siehe: ⇨ 21.

☑ IP-Adresse oder Hostname eines UTN-Servers sind bekannt.

Gehen Sie wie folgt vor:

1. *Öffnen Sie einen Texteditor.*
2. *Geben Sie die Befehlsfolge ein; siehe 'Syntax und Befehle' ⇨ 146.*
3. *Speichern Sie die Datei als ausführbares Skript; lesen Sie hierzu die Dokumentation Ihres Betriebssystems.*

↳ Das Skript ist gespeichert. Informationen zur Verwendung entnehmen Sie der Dokumentation Ihres Betriebssystems.

Syntax und Befehle

Beachten Sie die folgende Syntax.

Windows

```
"<Pfad utnm.exe>" /c "Befehlsstring" [/<Befehl>]
```

Die Datei 'utnm.exe' finden Sie im SEH UTN Manager-Programmordner.

Mac

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

Die ausführbare Datei 'utnm' finden Sie in der 'SEH UTN Manager.app'. Unter `/usr/local/bin/` befindet sich eine symbolische Verknüpfung darauf.

Folgende Befehle werden unterstützt:

Befehl	Beschreibung

`c "Befehlsstring"`
 	
oder
 	
`command "Befehlsstring"`
	Führt einen Befehl aus. Der Befehl wird durch den Befehlsstring näher spezifiziert. Folgende Befehlsstrings können verwendet werden:
	• `activate UTN-Server Vendor-ID Produkt-ID [Portnummer]`
	Aktiviert die Verbindung zu einem USB-Gerät. Sind mehrere USB-Geräte mit identischer Produkt-ID und Vendor-ID an den UTN-Server angeschlossen, wird das erste verfügbare Gerät aktiviert, wenn der Port nicht definiert ist.
	• `deactivate UTN-Server Vendor-ID Produkt-ID [Portnummer]`
	Deaktiviert die Verbindung zu einem USB-Gerät. Wird ein USB-Massenspeichergerät entfernt, wird der Befehl 'eject' verwendet. Bei allen anderen Geräten wird der Befehl 'plugout' verwendet.
	• `plugin UTN-Server Vendor-ID Produkt-ID [Portnummer]`
	Aktiviert die Verbindung zu einem USB-Gerät. Sind mehrere USB-Geräte mit identischer Produkt-ID und Vendor-ID an den UTN-Server angeschlossen, wird das erste verfügbare Gerät aktiviert, wenn der Port nicht definiert ist.
	• `plugout UTN-Server Vendor-ID Produkt-ID [Portnummer]`
	Deaktiviert die Verbindung zu einem USB-Gerät. (Entspricht dem 'Abziehen' des Gerätes.)
	Hinweis: *Der Befehl 'deactivate' ist zu bevorzugen.*
	• `eject UTN-Server Vendor-ID Produkt-ID [Portnummer]`
	(Für USB-Massenspeichergeräte) Wirft das USB-Gerät aus. Die Geräteverbindung wird erst deaktiviert, wenn die Kommunikation ordentlich beendet ist.
	Hinweis: *Der Befehl 'deactivate' ist zu bevorzugen.*
	• `state UTN-Server Vendor-ID Produkt-ID Portnummer`
	Zeigt den Status eines USB-Gerätes.
	• `getlist UTN-Server`
	Zeigt eine Übersicht der an den UTN-Server angeschlossenen USB-Geräte (inkl. Port, Vendor-ID, Produkt-ID, Herstellername, Produktname, Geräteklasse und Status).
	• `set autoconnect = true|false UTN-Server Vendor-ID Produkt-ID Portnummer`
	Aktiviert die Geräteverbindung automatisch, sofern das USB-Gerät angeschlossen und nicht belegt ist.

Befehl	Beschreibung
`p Portnummer` *oder* `port Portnummer`	Verwendet einen alternativen USB-Port am UTN-Server.
`sp` *oder* `ssl-port`	Verwendet einen alternativen USB-Port mit SSL-Verschlüsselung am UTN-Server.
`k USB-Portschlüssel` *oder* `key USB-Portschlüssel`	Spezifiziert einen USB-Portschlüssel. *Bei der Portschlüsselkontrolle wird über das myUTN Control Center für den USB-Port ein Schlüssel definiert, so dass das am USB-Port angeschlossene USB-Gerät vor Zugriff geschützt ist (⇨ 88). Um das USB-Gerät verfügbar zu machen, muss der korrekte Schlüssel eingegeben werden.*
`t Sekunden` *oder* `timeout Sekunden`	Spezifiziert ein Timeout für die Befehle 'activate', 'deactivate', 'plugin', 'plugout' und 'eject'.
`nw` *oder* `no-warnings`	Unterdrückt Warnmeldungen.
`q` *oder* `quiet`	Unterdrückt die Ausgabe.
`o` *oder* `output`	Zeigt die Ausgabe in der Kommandozeile an.
`v` *oder* `version`	Zeigt die Versionsnummer von utnm an.
`?` *oder* `help`	Zeigt die Hilfeseite an.

Für die Befehle gilt:

- UTN-Server = IP-Adresse oder Hostname eines UTN-Servers
- Vendor-ID = Vendor-ID des USB-Geräts
- Produkt-ID = Produkt-ID des USB-Geräts
- Elemente in eckigen Klammern sind optional
- keine Unterscheidung von großer bzw. kleiner Schreibweise (nicht case-sensitive)
- nur das ASCII-Format kann interpretiert werden

Rückgabewerte

Rückgabewert	Beschreibung
0	Das USB-Gerät kann verwendet werden.
20	Die Verbindung zum USB-Gerät konnte nicht hergestellt werden.
21	Die Verbindung zum USB-Gerät konnte nicht beendet werden.
22	Das USB-Gerät konnte nicht ausgeworfen werden.
23	Die Verbindung zum USB-Gerät ist bereits aktiviert.
24	Die Verbindung zum USB-Gerät wurde bereits beendet.
25	Das USB-Gerät wird von einem anderen Benutzer verwendet.
26	Das USB-Gerät ist nicht erreichbar.
27	Unbekannter USB-Gerätestatus.
100	Unbekannter Befehl.
101	Der UTN-Server wurde nicht gefunden. Entweder exisitert der UTN-Server nicht oder die DNS-Auflösung ist fehlgeschlagen.
103	Der USB-Portschlüssel ist zu lang.

Beispiel

Ein USB-Gerät soll aktiviert werden. Befehle und Syntax:

Windows

```
"<Pfad utnm.exe>" /c "activate UTN-Server Vendor-ID Produkt-ID [Portnummer]"
```

Ergibt:

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

Mac

```
utnm -c "activate UTN-Server Vendor-ID Produkt-ID [Portnummer]"
```

Ergibt:

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

8.7 Abbildungsverzeichnis

8.8 Index