USB Device Server

myUTN-50a
myUTN-55
myUTN-2500
Dongleserver myUTN-80
Dongleserver myUTN-800

Benutzerdokumentation Linux

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

Dokument:
Typ: Benutzerdokumentation Linux
Titel: USB Device Server
Version: 3.8

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.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 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.

Hinweis

Die 'Dongleserver' (myUTN-80 und myUTN-800) sind ausschließlich für die Bereitstellung von USB-Dongles konzipiert.

Die Zugriffsverteilung der USB-Geräte erfolgt über das Software-Tool 'SEH UTN Manager'. Die Software wird auf allen Clients installiert, die auf ein im Netzwerk bereitgestelltes USB-Gerät zugreifen sollen. Der SEH UTN Manager zeigt die Verfügbarkeit aller im Netzwerk eingebundenen UTN-Server an und stellt die Verbindung zwischen Client und USB-Port inklusive dem daran angeschlossenen 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 oder höher
- OS X 10.8.x, OS X 10.9.x, OS X 10.10.x, OS X 10.11.2 und höher[1], macOS 10.12.x und höher[2]

1. OS X 10.11.2 und höher: eingeschränkte USB-Geräte-Unterstützung
2. macOS 10.12.x und höher: eingeschränkte USB-Geräte-Unterstützung

- Ubuntu 12.04.x LTS (64-Bit), Ubuntu 14.04.x LTS (64-Bit) oder Oracle Linux 6.5 (64-Bit) mit Linux-Kernel 2.6.32 oder höher, glibc 2.11.1 oder höher und OpenSSL 1.0.1 oder höher[1]

Hinweis

Dieses Dokument beschreibt den Einsatz in Linux-Umgebungen. Für den Einsatz in anderen Umgebungen lesen Sie bitte die jeweilige systemspezifische Benutzerdokumentation. Für mehr Informationen, siehe: 'Dokumentation' ⇨🗎3.

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 USB-Geräte in der 'Netzwerkliste' angezeigt. Die benötigten UTN-Server werden ausgewählt und der 'Auswahlliste' hinzugefügt. Die in der Auswahlliste aufgeführten UTN-Server können dann vom Benutzer verwendet werden. Um ein USB-Gerät zu nutzen, stellt der Benutzer eine Verbindung zwischen seinem Client und dem USB-Port des UTN-Servers her, an den das USB-Gerät angeschlossen ist.

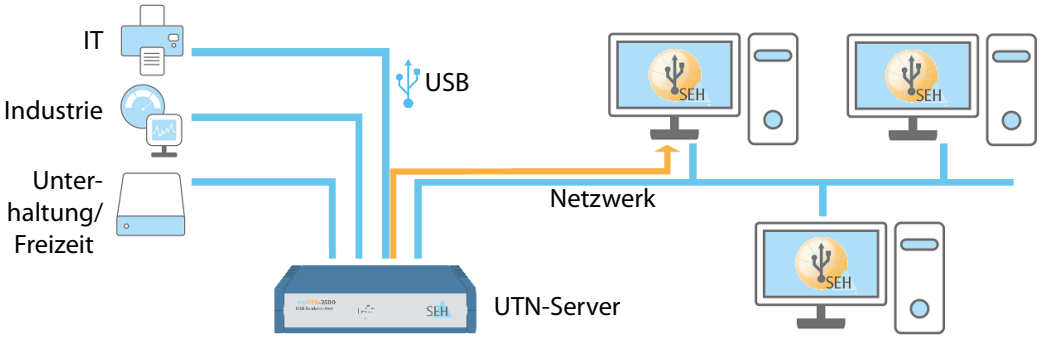


Abbildung 1: UTN-Server im Netzwerk

Hinweis

Art und Anzahl der anschließbaren USB-Geräte entnehmen Sie dem jeweiligen 'Quick Installation Guide'.

1. UTN-Server unterstützen derzeit keine USB 3.0 Geräte unter Linux. Um ein USB 3.0 Gerät zu nutzen, schließen Sie einen USB 2.0 Hub an den UTN-Server an und das USB 3.0 Gerät an den Hub.

1.2 Dokumentation

Beschreibungsumfang und Inhalte

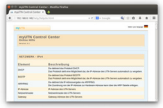
Diese Dokumentation beschreibt mehrere Varianten des USB Deviceservers und die Dongleserver. Das hat zur Folge, dass zum Teil Funktionen beschrieben werden, die nicht dem Leistungsumfang Ihres Produktes entsprechen. Abbildungen können von Ihrem Gerät abweichen.

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
- Dongle → USB-Gerät

Aufbau der Dokumentation

Die myUTN-Dokumentation besteht aus den folgenden Dokumenten:

 PDF	**Benutzerdokumentation** Detaillierte Beschreibung der myUTN-Konfiguration und -Administration. Systemspezifische Anleitungen für folgende Systeme: - Windows - Mac - Linux
 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: ⇨ 89.

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 **Warnung**	Ein Warnhinweis enthält wichtige Informationen, die Sie unbedingt beachten müssen. Nichtbeachtung kann zu Fehlfunktionen führen.
Hinweis Hinweis	Ein Hinweis enthält Informationen, die Sie beachten sollten.
1. Markieren Sie...	Nummerierte Aufzählungen beschreiben Handlungsanweisungen Schritt für Schritt.
↳ 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	8:00–16:45 Uhr und
Freitag	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:

Warnung

Dies ist ein Warnhinweis!

1.5 Erste Schritte

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

1. Lesen und beachten Sie die Sicherheitsinformationen, um Schaden an Personen und Gerät zu vermeiden; siehe: ⇨🗎6.
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: ⇨🗎7.
4. Installieren und starten Sie das Software-Tool 'SEH UTN Manager' auf Ihrem Client; siehe: ⇨🗎13.
5. Fügen Sie der Auswahlliste die UTN-Server hinzu, die Sie nutzen möchten; siehe: ⇨🗎46.
6. Aktivieren Sie die Verbindung zwischen Ihrem Client und dem USB-Port, an den das USB-Gerät angeschlossen ist; siehe: ⇨🗎47.

↳ 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 das Software-Tool 'SEH UTN Manager' ermittelt und verändert werden; siehe: ⇨🗎11.

Nachfolgend sind die verschiedenen Methoden zur IP-Adressenvergabe beschrieben.

Automatische Methoden zur IP-Adressenvergabe

- 'ZeroConf' ⇨🗎8
- 'BOOTP' ⇨🗎8
- 'DHCP' ⇨🗎8
- 'Autokonfiguration (IPv6-Standard)' ⇨🗎9

Manuelle Methoden zur IP-Adressenvergabe

- 'SEH UTN Manager' ⇨🗎9
- 'myUTN Control Center' ⇨🗎9
- 'ARP/PING' ⇨🗎10

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).

Hinweis

Zur Namensauflösung der IP-Adresse kann der Domain Name Service von Bonjour verwendet werden; siehe: ⇨🗎28.

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: ⇨🗎23.
- ✓ 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: ⇨🗎23.
- ✓ 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.

Hinweis

Um die Vergabe von IPv6-Adressen zu konfigurieren, siehe: ⇨ 24.

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: ⇨ 24.

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: ⇨ 23.
- Um eine **IPv6**-Adresse via myUTN Control Center zu konfigurieren, siehe: ⇨ 24.

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: ⇨🗎24.

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' ⇨ 11
- 'Administration via SEH UTN Manager' ⇨ 13
- 'Administration via E-Mail (nur myUTN-80 und höher)' ⇨ 21

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 (z.B. Mozilla Firefox) dargestellt werden.

Voraussetzung

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

myUTN Control Center starten

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

↳ Das **myUTN Control Center** erscheint.

Hinweis

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

Zusätzlich kann das myUTN Control Center über das Software-Tool 'SEH UTN Manager' gestartet werden: Markieren Sie den UTN-Server in der Auswahlliste und wählen Sie im Menü **UTN-Server** den Befehl **Konfigurieren.**

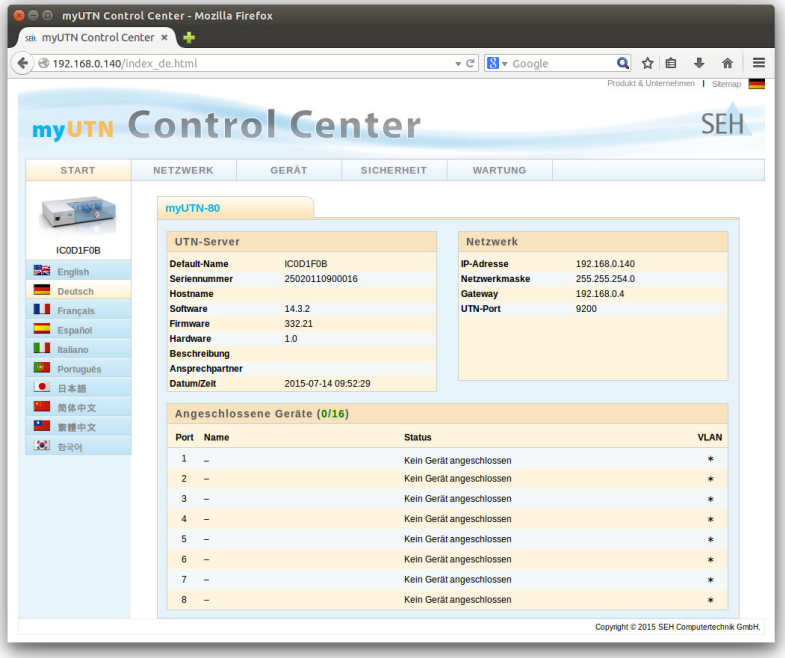


Abbildung 2: myUTN Control Center - START

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-Port inklusive dem daran angeschlossenen USB-Gerät her. Die Software wird auf allen 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 USB-Geräte in der 'Netzwerkliste' angezeigt. Die benötigten UTN-Server werden ausgewählt und der 'Auswahlliste' hinzugefügt. Die in der Auswahlliste aufgeführten Geräte können konfiguriert oder mit dem Client verbunden werden.

Welche Informationen benötigen Sie?

Automatismen

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

- **Auto-Connect**: Die Funktion ermöglicht das automatische Aktivieren einer permanenten Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät beim Starten des Betriebssystems.
- Auto-Disconnect: Die Funktion ermöglicht das automatische Trennen einer Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät nach einem definierten Zeitraum.
- Zusatztool 'utnm': Das Tool wird verwendet zum Aktivieren und Deaktivieren von Portverbindungen. Dies erfolgt über Befehle, die in die Kommandozeile des Betriebssystems eingegeben und ausgeführt werden. Alternativ wird ein Skript geschrieben.

Wodurch unterscheiden sich die Varianten?

SEH UTN Manager-Varianten

Der SEH UTN Manager ist in zwei Varianten verfügbar:

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

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 verwendet werden. Die Minimal-Variante eignet sich z.B. um das De-/aktivieren von Portverbindungen zu automatisieren (mit Skripten); siehe: 'Zusatztool 'utnm'' ⇨🗎118.

Hinweis

Für den Standard-Gebrauch wird die vollständige Variante empfohlen. Die Minimal-Variante ist nur von Experten zu verwenden.

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

Es wird zudem zwischen den folgenden Benutzergruppen unterschieden:

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

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

Installation

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

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

Für Linux-Systeme (64-Bit) sind Installationspakete in den Formaten '*.deb' und '*.rpm' verfügbar. Es gibt jeweils vier Pakete:

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

Hinweis

Installationspakete im Format '.tgz' für andere Linux-Systeme (32- und 64-Bit) sind ebenfalls verfügbar. Mindestanforderungen: Linux-Kernel 2.6.32 und glibc 2.11.1.
Aufgrund der Vielfalt an Linux-System kann eine erfolgreiche Installation jedoch nicht garantiert werden!

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

- Paket 1)–3): Minimalvariante
- Paket 1)–4): vollständige Variante

Hinweis

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

Je nach Distribution sind für die Installation der Dateien unterschiedliche Maßnahmen erforderlich. Lesen Sie hierzu die Dokumentation Ihres Betriebssystems. Beispielhaft werden nachfolgend einige Installationsverfahren beschrieben.

Was möchten Sie tun?

- 'SEH UTN Manager via Ubuntu Software-Center installieren' ⇨🗎15
- 'SEH UTN Manager via Ubuntu-Terminal installieren' ⇨🗎16
- 'SEH UTN Manager via Oracle-Terminal installieren' ⇨🗎16
- 'Dynamic Kernel Module Support (DKMS) installieren' ⇨🗎17

SEH UTN Manager via Ubuntu Software-Center installieren

Systemvoraussetzung

✓ Ubuntu 12.4.x LTS (64-Bit), Ubuntu 14.04.x LTS (64-Bit) mit Linux-Kernel 2.6.32 oder höher, glibc 2.11.1 oder höher und OpenSSL 1.0.1 oder höher.
✓ Der verwendete Benutzer kann über den Befehl 'sudo' Rootrechte erlangen.

1. Starten Sie das Installationspaket Nr. 1.
   Das Ubuntu Software-Center erscheint.

2. Wählen Sie die Schaltfläche **Installieren** an.
   Eine Passwort-Abfrage erscheint.
3. Legitimieren Sie sich mit Ihrem Passwort.
   Das Paket wird auf Ihrem Client installiert.
4. Wiederholen Sie Schritte 1. bis 3. mit den restlichen Paketen.
5. Fügen Sie alle Benutzer, die den SEH UTN Manager auf dem Client nutzen sollen, der Benutzergruppe 'utnusers' hinzu. Öffnen Sie hierzu die Konsole Terminal und geben den Befehl ein:
   `sudo usermod -aG utnusers <Benutzername>`
6. Melden Sie sich ab und wieder an, damit die Zugehörigkeit zur Gruppe wirksam wird.

↳ Der SEH UTN Manager ist auf Ihrem Client installiert.

SEH UTN Manager via Ubuntu-Terminal installieren

System-voraussetzung

- ✓ Ubuntu 12.04.x LTS (64-Bit), Ubuntu 14.04.x LTS(64-Bit)mit Linux-Kernel 2.6.32 oder höher, glibc 2.11.1 oder höher und OpenSSL 1.0.1 oder höher.
- ✓ Der verwendete Benutzer kann über den Befehl 'sudo' Rootrechte erlangen.
- ✓ DKMS (Dynamic Kernel Module Support) ist auf dem Client installiert; siehe: ⇨🗎17.

1. Öffnen Sie die Konsole **Terminal**.
2. Installieren Sie die gewünschten SEH UTN Manager-Pakete:
   `sudo dpkg -i <vollständiger Paketname>`
3. Fügen Sie alle Benutzer, die den SEH UTN Manager auf dem Client nutzen sollen, der Benutzergruppe 'utnusers' hinzu:
   `sudo usermod -aG utnusers <Benutzername>`
4. Melden Sie sich ab und wieder an, damit die Zugehörigkeit zur Gruppe wirksam wird.

↳ Der SEH UTN Manager ist auf Ihrem Client installiert.

SEH UTN Manager via Oracle-Terminal installieren

System-voraussetzung

- ✓ Oracle Linux 6.5 (64-Bit) mit Linux-Kernel 2.6.32 oder höher, glibc 2.11.1 oder höher und OpenSSL 1.0.1 oder höher.
- ✓ DKMS (Dynamic Kernel Module Support) ist auf dem Client installiert; siehe: ⇨🗎17.
- ✓ Der verwendete Benutzer kann über den Befehl 'sudo' Rootrechte erlangen.

1. Öffnen Sie die Konsole **Terminal**.
2. Installieren Sie die gewünschten SEH UTN Manager-Pakete:
   `sudo rpm -i <vollständiger Paketname>.`

3. Fügen Sie alle Benutzer, die den SEH UTN Manager auf dem Client nutzen sollen, der Benutzergruppe 'utnusers' hinzu:
   `sudo usermod -aG utnusers <Benutzername>`
4. Melden Sie sich ab und wieder an, damit die Zugehörigkeit zur Gruppe wirksam wird.

↳ Der SEH UTN Manager ist auf Ihrem Client installiert.

Dynamic Kernel Module Support (DKMS) installieren

Zur Installation des SEH UTN Managers, wird auf dem System Dynamic Kernel Module Support (DKMS) benötigt. DKMS ist in einigen Distributionen standardmäßig nicht enthalten (z.B. in Oracle Linux 6.5).

Beispielhaft wird das Installationsverfahren für Oracle Linux 6.5 beschrieben

Systemvoraussetzung

✓ Der verwendete Benutzer kann über den Befehl 'sudo' Rootrechte erlangen.

1. Öffnen Sie die Konsole **Terminal**.
2. Führen Sie den Befehl aus:
   ```
   sudo wget http://pkgs.repoforge.org/rpmforge-release/
   rpmforge-release-0.5.3-1.el5.rf.x86_64.rpm
   ```
3. Führen Sie den Befehl aus:
   ```
   sudo rpm --import http://apt.sw.be/RPM-GPG-KEY.dag.txt
   ```
4. Führen Sie den Befehl aus:
   ```
   sudo rpm -K rpmforge-release-0.5.3-1.el5.rf.*.rpm
   ```
5. Führen Sie den Befehl aus:
   ```
   sudo rpm -i rpmforge-release-0.5.3-1.el5.rf.*.rpm
   ```
6. Installieren Sie DKMS:
   ```
   sudo yum install dkms
   ```
7. Führen Sie den Befehl aus:
   ```
   sudo yum install chrpath tkcvs rpm-build rpmlint php php-mysql
   ```
   Eine Sicherheitsabfrage erscheint.
8. Bestätigen Sie die Sicherheitsabfrage:
   ```
   y
   ```
9. Ermitteln Sie den aktuellen Kernel und notieren Sie das Ergebnis:
   ```
   uname -r
   ```
10. Führen Sie den Befehl aus:
    ```
    gpk-application
    ```
    Eine Sicherheitsabfrage erscheint.
11. Bestätigen Sie die Sicherheitsabfrage mit **Trotzdem fortsetzen**.
    Der Dialog Software **hinzufügen/entfernen** erscheint.
12. Geben Sie im Suchfeld **building kernel** ein.

13. Wählen Sie die Schaltfläche Suchen an.
    Die Suchergebnisse werden angezeigt.
14. Suchen Sie in der Liste das **Development package for building kernel modules to match the kernel** für Ihren zuvor ermittelten Kernel.
15. Überprüfen Sie, ob das gesuchte Paket **Development package for building kernel modules to match the kernel** für Ihren Kernel installiert ist. Falls nicht, installieren Sie das Paket.

↳ DKMS ist auf Ihrem Client installiert.

Programmstart

Ubuntu

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

Oracle

Der SEH UTN Managers kann auf verschiedene Weisen gestartet werden:

- Rufen Sie im Menü Anwendungen – Systemwerkzeug den UTN Manager  auf.
- Führen Sie in der Konsole 'Terminal' den Befehl `utnmanager` aus.
- Rufen Sie mit Alt+F2 den Dialog Anwendung ausführen auf. Geben Sie im Feld 'utnmanager' ein und wählen Sie die Schaltfläche Ausführen an.

Variantenwechsel

Ist auf Ihrem System bereits die vollständige Variante oder Minimalvariante des SEH UTN Managers installiert und Sie möchten auf die 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.

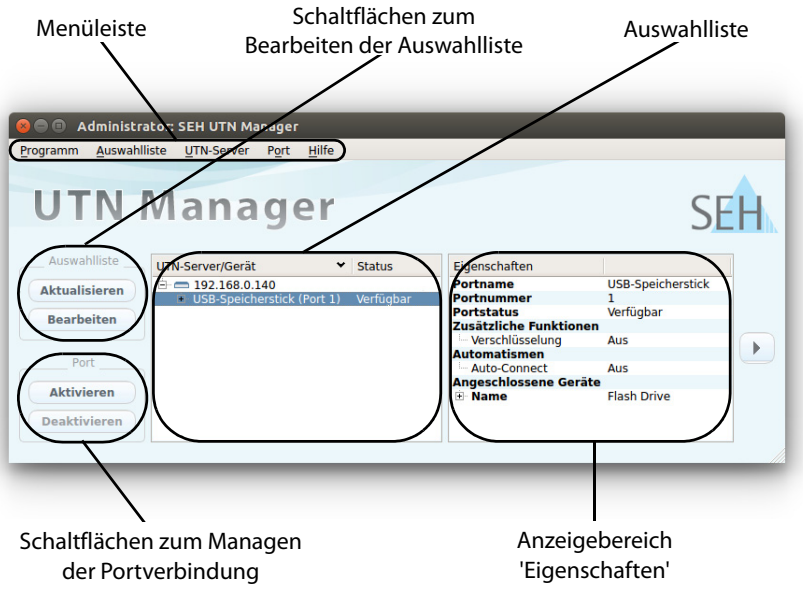


Abbildung 5: SEH UTN Manager - Hauptdialog

Funktionen

Über den SEH UTN Manager können Sie u.a.

- 'UTN-Server der Auswahlliste hinzufügen' ⇨🗎46
- 'USB-Port mit Client verbinden' ⇨🗎47
- 'USB-Port und Client trennen' ⇨🗎48
- 'belegte USB-Ports anfordern' ⇨🗎49
- 'Portverbindungen und Programmstarts automatisieren' ⇨🗎50
- 'UTN-Servern eine IPv4-Adresse zuweisen' ⇨🗎24
- 'myUTN Control Center starten' ⇨🗎11
- 'Zugriff auf gesperrte USB-Ports freischalten' ⇨🗎64
- 'Auswahllisten für mehrere Teilnehmer verwalten' ⇨🗎52

Hinweis

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 und der Gruppenzugehörigkeit auf dem Client
- den Einstellungen der produkteigenen Sicherheitsmechanismen
- dem Client-Betriebssystem

Hinweis

Für weitere Informationen, siehe: 'SEH UTN Manager - Funktionsübersicht' ⇨ 113.

2.3 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: ⇨🗎26.
- ✓ 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: ⇨🗎29.

Anweisung via E-Mail versenden

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

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' ⇨🗎21.
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: <Befehl> [<Kommentar>]
```

Folgende Kommandos werden unterstützt:

Kommandos	Option	Beschreibung
<Befehl>	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: ⇨🗎92. 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.
[<Kommentar>]		Frei definierbarer Text für Beschreibungszwecke.

Für die Anweisungen gilt:

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

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.

Parameter-änderungen

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

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

Syntax und Wertekonventionen entnehmen Sie der Parameterliste; siehe: ⇨🗎92.

Beispiel 1

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

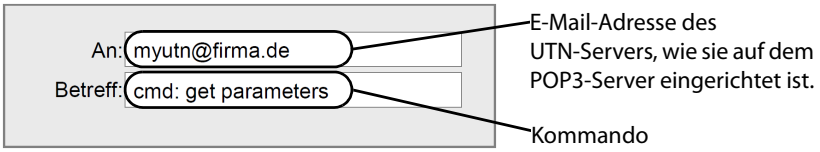


Abbildung 6: Administration via E-Mail - Beispiel 1

Beispiel 2

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

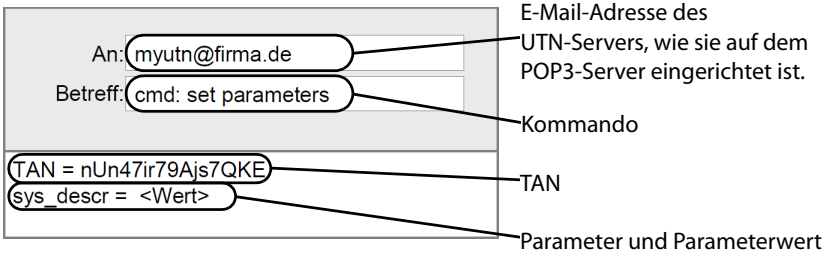


Abbildung 7: Administration via E-Mail - Beispiel 2

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?

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: ⇨🗎7.

Was möchten Sie tun?

☐ 'IPv4-Parameter via myUTN Control Center konfigurieren' ⇨🗎23

☐ 'IPv4-Parameter via SEH UTN Manager konfigurieren' ⇨🗎24

IPv4-Parameter via myUTN Control Center konfigurieren

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - IPv4** an.
3. Konfigurieren Sie die IPv4-Parameter; Tabelle 2 ⇨🗎24.
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' ⇨🗎7.)* 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: ⇨🗎13.
✓ Der UTN-Server wird in der Auswahlliste angezeigt; siehe: ⇨🗎46.

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.

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`

Hinweis

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'.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - IPv6** an.
3. Konfigurieren Sie die IPv6-Parameter; Tabelle 3 ⇨🗎26.
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.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - DNS** an.
3. Konfigurieren Sie die DNS-Parameter; Tabelle 4 ⇨🗎26.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 4: DNS-Parameter

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

3.4 Wie konfiguriere ich SNMP?

SNMP (Simple Network Management Protocol) 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'.

Hinweis

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.

Hinweis

Für SNMPv3 müssen Name und Passwort des SNMP-Benutzers definiert sein. Die hierfür verwendeten Benutzerkonten sind identisch zu den Benutzerkonten für den Zugang zum myUTN Control Center; siehe: ⇨🗎60.

Voraussetzung

✓ Nur bei SNMPv3: Die Benutzerkonten sind definiert; siehe: ⇨🗎60.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - SNMP** an.
3. Konfigurieren Sie die SNMP-Parameter; Tabelle 5 ⇨🗎27.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 5: SNMP-Parameter

Parameter	Beschreibung
SNMPv1	De-/aktiviert die SNMPv1-Funktionalität.
Nur Lesen	De-/aktiviert den Schreibschutz für die Community.

Parameter	Beschreibung
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.
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' ⇨🗎8) 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.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - Bonjour** an.
3. Konfigurieren Sie die Bonjour-Parameter; Tabelle 6 ⇨🗎29.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 6: Bonjour-Parameter

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

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

Damit am UTN-Server der Benachrichtigungsservice (⇨🗎39) und die Fernwartung via E-Mail (⇨🗎21) 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' ⇨🗎29
- ☐ 'SMTP konfigurieren' ⇨🗎30

POP3 konfigurieren

Voraussetzung

✓ Der UTN-Server ist als Benutzer mit eigener E-Mail-Adresse auf einem POP3-Server eingerichtet.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - E-Mail** an.
3. Konfigurieren Sie die POP3-Parameter; Tabelle 7 ⇨🗎30.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 7: POP3-Parameter

Parameter	Beschreibung
POP3	De-/aktiviert die POP3-Funktionalität.
POP3 - Servername	Definiert den POP3-Server über die IP-Adresse oder den Hostnamen. *Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.*
POP3 - Serverport	Definiert den Port, über den der UTN-Server E-Mails empfängt. Die 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 Protokoll und Verschlüsselungsstufe definiert* ⇨🗎58.
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

Voraussetzung

✓ Der UTN-Server ist als Benutzer mit eigener E-Mail-Adresse auf einem SMTP-Server eingerichtet.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - E-Mail** an.
3. Konfigurieren Sie die SMTP-Parameter; Tabelle 8 ⇨🗎31.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 8: SMTP-Parameter

Parameter	Beschreibung
SMTP - Servername	Definiert den SMTP-Server über die IP-Adresse oder den Hostnamen. *Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.*
SMTP - Serverport	Definiert die Portnummer, über die der SMTP-Server E-Mails von dem UTN-Server empfängt. Die Portnummer 25 ist voreingestellt.
SMTP - SSL/TLS	De-/aktiviert die Option SSL/TLS. *Mit SSL/TLS wird der Übertragungsweg vom UTN-Server zum SMTP-Server verschlüsselt. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert* ⇨🗎58.
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* ⇨🗎67.
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* ⇨🗎67.
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-55)

Der UTN-Server 'myUTN-55' ist ein WLAN-Gerät und wird drahtlos im Netzwerk zu betrieben.

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-55 unterstützt die Standards IEEE 802.11b, IEEE 802.11g und IEEE 802.11n.

Der myUTN-55 verfügt über zusätzliche WLAN-Parameter; Tabelle 9 ⇨33. Die aktuellen WLAN-Einstellungen können im myUTN Control Center unter dem Menüpunkt **NETZWERK - WLAN** eingesehen werden.

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.

Hinweis

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 alphanumerischen 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.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - WLAN** an.
3. Konfigurieren Sie die WLAN-Parameter; Tabelle 9 ⇨🗎33.
4. Bestätigen Sie mit **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

Hinweis

Falls der UTN-Server das Netzwerk wechselt, erhält er unter Umständen eine neue IP-Adresse. Dann 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.

Parameter	Beschreibung
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	Definiert den Schwellenwert für Roaming in -dBm. Wird der Schwellenwert überschritten, sucht der UTN-Server nach einem stärkeren WLAN-Signal und wechselt gegebenenfalls in ein anderes WLAN-Netzwerk mit besserer Signalstärke. Der Wert 65 -dbm ist voreingestellt. Der Parameter 'Roaming Level' ist nur im 'Infrastructure'-Modus konfigurierbar.
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. **Warnung** **Informieren Sie sich über die nationalen Bestimmungen für den Einsatz von WLAN-Produkten und verwenden Sie nur zugelassene Kanäle.**
Verschlüsselungsmethode	siehe: 'WLAN-Sicherheit' ⇨🗎32
Authentifizierungsmethode	siehe: 'Wie verwende ich Authentifizierungsmethoden?' ⇨🗎74

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.

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

↳ Die Daten werden gespeichert.

Hinweis

Um USB-Ports einen Namen zuzuweisen, siehe: ⇨🗎38.

4.2 Wie lege ich eine Kennung im Anzeigefeld fest? (nur myUTN-800)

Der Dongleserver myUTN-800 eignet sich für den Einbau in 19-Zoll-Serverschränke. Um einen bestimmten myUTN-800 zu identifizieren wenn mehrere in einen Serverschrank eingebaut sind, wird eine Kennung im Anzeigefeld an der Vorderseite des Dongleservers angezeigt.

Standardmäßig wird die Kennung 'DS' angezeigt. Sie haben die Möglichkeit, eine freidefinierbare zuzuweisen.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **GERÄT - Beschreibung** an.
3. Geben Sie in das Feld **Kennung (Anzeigefeld)** eine freidefinierbare ID ein.
   (Max. 2 Zeichen; A–Z, 0–9. E+Zahl nicht möglich, weil diese Kombination für Fehlercodes ⇨112 verwendet wird.)
4. Bestätigen Sie mit **Speichern**.

↳ Die Daten werden gespeichert.

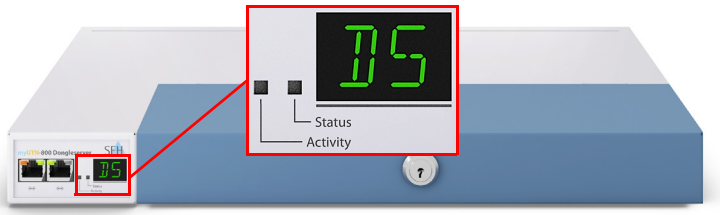


Abbildung 8: Anzeigefeld myUTN-800

4.3 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.

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**.

↳ Die Einstellungen werden gespeichert.

4.4 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: ⇨ 80.

Hinweis

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 ⇨ 27.

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

↳ Die Einstellungen werden gespeichert.

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

Sie haben die Möglichkeit, einem USB-Port eine beliebige Bezeichnung zuzuweisen. Dieser Portname wird im myUTN Control Center und SEH UTN Manager angezeigt. Ist kein Portname definiert, wird der Name des angeschlossenen USB-Gerätes angezeigt.

Tipp

Einige USB-Geräte haben kryptische oder uneindeutige Namen. Weisen Sie dem USB-Port und damit dem USB-Gerät eine klare Bezeichnung zu, z.B. den Namen einer zugehörigen Software. Auf diese Weise erhalten Sie einen besseren Überblick über die im Netzwerk vorhandenen USB-Geräte.

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

↳ Die Einstellungen werden gespeichert.

4.6 Wie schalte ich einen USB-Port ab? (nur myUTN-80 und höher)

Sie haben die Möglichkeit, einen USB-Port ein- bzw. auszuschalten. Dazu unterbrechen Sie die Stromzufuhr bzw. stellen sie wieder her.

Hinweis

Die Stromzufuhr für die USB-Ports ist standardmäßig eingeschaltet.

Nutzen und Zweck

Schalten Sie unbenutzte USB-Ports ab um sicherzustellen, dass keine ungewünschten USB-Geräte in das Netzwerk eingebunden werden. Abgeschaltete USB-Ports sind im SEH UTN Manager nicht sichtbar.

Mit dieser Funktion können Sie zudem ein USB-Gerät aus- und wieder einschalten, 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.

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

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

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-Ports.
  - Die Unterbrechung oder Herstellung der Stromversorgung. (nur myUTN-800)
  - Das Verbinden oder Trennen einer SD-Karte am UTN-Server. (nur myUTN-800)
  - Die Unbenutzbarkeit einer SD-Karte. (nur myUTN-800)
  - Die Unterbrechung oder Herstellung der Netzwerkverbindung. (nur myUTN-800)

Was möchten Sie tun?

☐ 'Versand von Status-E-Mails konfigurieren' ⇨🗎39
☐ 'Event-Benachrichtigung via E-Mail konfigurieren' ⇨🗎40
☐ 'Event-Benachrichtigung via SNMP-Trap konfigurieren' ⇨🗎40

Versand von Status-E-Mails konfigurieren

Voraussetzung

✓ Am UTN-Server sind SMTP-Parameter konfiguriert; siehe: ⇨🗎29.
✓ Auf dem UTN-Server ist ein DNS-Server konfiguriert; siehe: ⇨🗎26.

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

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.**

↳ Die Einstellungen werden gespeichert.

Event-Benachrichtigung via E-Mail konfigurieren

Voraussetzung

✓ Am UTN-Server sind SMTP-Parameter konfiguriert; siehe: ⇨🗎29.
✓ Auf dem UTN-Server ist ein DNS-Server konfiguriert; siehe: ⇨🗎26.

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

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

↳ Die Einstellungen werden gespeichert.

Event-Benachrichtigung via SNMP-Trap konfigurieren

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

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

↳ Die Einstellungen werden gespeichert.

4.8 Wie erhalte ich Fehlermeldungen über das Anzeigefeld? (nur myUTN-800)

Sie haben die Möglichkeit, Fehlerzustände im Anzeigefeld an der Vorderseite des Dongleservers myUTN-800 darstellen zu lassen.

Die folgenden Meldungstypen sind möglich:

- nur eine Stromversorgung liefert Strom
- SD-Karten-Fehler (Lese- und Schreibfehler, fehlende SD Karte)
- nur eine Netzwerkverbindung ist aktiv

Die Fehler werden codiert dargestellt. Die Bedeutung der Codes entnehmen Sie dem Kapitel 'Informationen im Anzeigefeld (nur myUTN-800)' ⇨🗎112.

1. Starten Sie das myUTN Control Center.

2. Wählen Sie den Menüpunkt **GERÄT - Benachrichtigung** an.
3. Aktivieren Sie im Bereich **Anzeigefeld** die Optionen mit den gewünschten Meldungstypen.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Hinweis

Wenn kein Fehlerzustand vorliegt, der UTN-Server also betriebsbereit ist, wird die Kennung angezeigt ⇨🗎36.

Hinweis

Eine ideale Ergänzung zu den Fehlermeldungen im Anzeigefeld sind die optionalen Signaltöne. Für mehr Informationen, siehe: ⇨🗎42.

4.9 Wie konfiguriere ich Signaltöne? (nur myUTN-800)

Der myUTN-800 Dongleserver gibt eine akustische Rückmeldung beim:

- Anschließen eines USB-Dongles
- Neustart des UTN-Servers
- Zurücksetzen der Parameter

Diese akustischen Rückmeldungen können nicht abgeschaltet werden.

Optional kann eine zusätzliche akustische Rückmeldung konfiguriert werden, für den Fall, dass

- nur eine Stromversorgung Strom liefert
- ein SD-Karten-Fehler anliegt (Lese- und Schreibfehler, fehlende SD Karte)
- nur eine Netzwerkverbindung aktiv ist

Hinweis

Diese optionalen akustischen Rückmeldungen sind eine ideale Ergänzung zu den Fehlermeldungen im Anzeigefeld ⇨🗎40.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **GERÄT - Benachrichtigung** an.
3. Aktivieren Sie im Bereich **Signalton** die Optionen mit den gewünschten Signaltypen.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

4.10 Wie setze ich den UTN-Server in VLAN-Umgebungen ein? (nur myUTN-80 und höher)

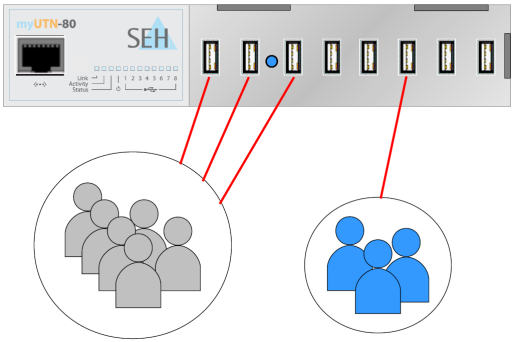
Der UTN-Server unterstützt die Verwendung von virtuellen lokalen Netzwerken (VLAN - Virtual Local Area Network). Das Unterteilen eines physischen Netzwerks in VLANs kann aus Performance- und Sicherheitsgründen sinnvoll sein.

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 Benachrichtigungs-service Daten weitergeleitet werden, mit den eingetragenen VLANs verknüpft werden.

Nutzen und Zweck

Die VLANs können verwendet werden, um den Zugriff auf donglegeschützte Software (myUTN-80, myUTN-800) bzw. USB-Geräte (myUTN-2500) zu kontrollieren. Auf diese Weise kann einer definierten Gruppe von Netzteilnehmern eine bestimmte Anzahl von donglegeschützter Softwarelizenzen bzw. USB-Geräten zur Verfügung gestellt werden.



Beispiel

6 Konstruktionsmitarbeiter haben Zugriff auf 3 donglegeschützte CAD-Softwarelizenzen.

3 Buchhalter haben Zugriff auf eine donglegeschützte 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.

Abbildung 9: USB-Portbasierte Zuweisung von VLANs

Was möchten Sie tun?

- ☐ 'IPv4-Management-VLAN eintragen' ⇨🗎43
- ☐ 'IPv4-Client-VLAN eintragen' ⇨🗎43
- ☐ 'IPv4-Client-VLAN einem USB-Port zuordnen' ⇨🗎44

IPv4-Management-VLAN eintragen

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - IPv4-VLAN** an.
3. Konfigurieren Sie die IPv4-Management-VLAN-Parameter; Tabelle 11 ⇨🗎44.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 10: IPv4-Management-VLAN-Parameter

Parameter	Beschreibung
IPv4-Management-VLAN	De-/aktiviert die Weiterleitung der IPv4-Management-VLAN-Daten. *Ist die Option aktiviert, ist SNMP ist ausschließlich im IPv4-Management-VLAN verfügbar.*
VLAN-ID	ID zur Identifizierung des IPv4-Management-VLAN (0–4096).
IP-Adresse	IP-Adresse des UTN-Servers ⇨🗎24.
Netzwerkmaske	Netzwerkmaske des UTN-Servers ⇨🗎24.
Gateway	Gateway-Adresse des IPv4-Management-VLANs
Zugriff über alle VLANs	De-/aktiviert den administrativen Zugang (Web) zum UTN-Server über IPv4-Client-VLANs. *Ist die Option aktiviert, kann der UTN-Server aus allen VLANs heraus administriert werden.*
Zugriff vom LAN (untagged)	De-/aktiviert den administrativen Zugang zum UTN-Server über IPv4-Pakete ohne Tag. *Ist die Option deaktiviert, kann der UTN-Server ausschließlich über VLANs administriert werden.*

IPv4-Client-VLAN eintragen

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - IPv4-VLAN** an.
3. Konfigurieren Sie die IPv4-VLAN-Parameter; Tabelle 11 ⇨🗎44.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 11: IPv4-Client-VLAN-Parameter

Parameter	Beschreibung
VLAN	De-/aktiviert die Weiterleitung der IPv4-Client-VLAN-Daten.
IP-Adresse	IP-Adresse des UTN-Servers innerhalb des IPv4-Client-VLAN.
Netzwerkmaske	Netzwerkmaske des UTN-Servers innerhalb des IPv4-Client-VLAN.
VLAN-ID	ID zur Identifizierung des IPv4-Client-VLAN (0–4096).
Gateway	Gateway-Adresse des IPv4-Client-VLANs
Automatisch ausfüllen	Füllt alle Felder 'VLAN', 'IP-Adresse' und 'Netzwerkmaske' automatisch mit den Werten aus Zeile 1. Die 'VLAN ID' wird um '1' hochgezählt.

IPv4-Client-VLAN einem USB-Port zuordnen

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

↳ Die Einstellungen werden gespeichert.

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-Port inkl. dem daran angeschlossenen USB-Gerät hergestellt werden.

Welche Information benötigen Sie?

- 'Wie finde ich UTN-Server/USB-Geräte im Netzwerk?' ⇨🗎45
- 'Wie füge ich UTN-Server/USB-Geräte der Auswahlliste hinzu?' ⇨🗎46
- 'Wie verbinde ich einen USB-Port inkl. USB-Gerät mit dem Client?' ⇨🗎47
- 'Wie trenne ich die Verbindung zwischen USB-Port inkl. USB-Gerät und Client?' ⇨🗎48
- 'Wie fordere ich ein belegtes USB-Gerät an?' ⇨🗎49
- 'Wie automatisiere ich Portverbindungen und Programmstarts?' ⇨🗎50
- 'Wie erhalte ich Informationen zum USB-Port und USB-Gerät?' ⇨🗎52
- 'Wie verwalte ich Auswahllisten für mehrere Teilnehmer?' ⇨🗎52

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' ⇨🗎45
- ☐ 'Netzwerk scannen' ⇨🗎46

Suchparameter definieren

Voraussetzung

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨🗎13.

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

↳ Die Einstellungen werden gespeichert.

Netzwerk scannen

Voraussetzung

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 13.

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

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

5.2 Wie füge ich UTN-Server/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: ⇨ 13.

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

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

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

Abbildung 10: SEH UTN Manager - Auswahlliste bearbeiten

Hinweis

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 einen USB-Port inkl. USB-Gerät mit dem Client?

Ein am UTN-Server angeschlossenes USB-Gerät kann mit dem Client verbunden werden. Dazu stellt der Benutzer eine Verbindung zwischen seinem Client und dem USB-Port des UTN-Servers her, an den das USB-Gerät angeschlossen ist. Das USB-Gerät kann dann vom Client genutzt werden, gleich so, als ob das USB-Gerät direkt am Client angeschlossen wäre.

Sonderfall Compound-USB-Gerät

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

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

Tabelle 12: Virtuelle USB-Ports

UTN-Server	Anzahl virtueller USB-Ports	UTN-Server	Anzahl virtueller USB-Ports
myUTN-50a	6	myUTN-800	40
myUTN-55	6	myUTN-2500	12
myUTN-80	16		

Voraussetzung

- ✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨🗎13.
- ✓ Der USB-Port wird in der Auswahlliste angezeigt; siehe: ⇨🗎46.
- ✓ Auf dem Client sind alle Vorbereitungen (Treiberinstallation usw.) getroffen worden, die notwendig wären, um das USB-Gerät lokal (also direkt an dem Client angeschlossen) zu betreiben. Idealerweise ist das USB-Gerät zuvor lokal am Client nach der Anleitung des Herstellers angeschlossen und betrieben worden.
- ✓ Der USB-Port ist nicht mit einem anderen Client verbunden.

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

↳ Die Verbindung wird hergestellt.

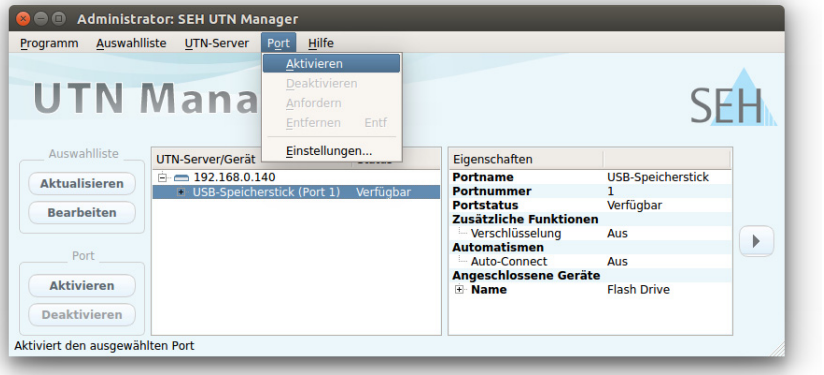


Abbildung 11: SEH UTN Manager - USB-Port aktivieren

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

Deaktivieren Sie die Verbindung zum USB-Port und dem daran angeschlossenen USB-Gerät, sobald Sie das USB-Gerät nicht mehr benötigen. Auf diese Weise ermöglichen Sie anderen Netzwerkteilnehmern den Zugriff auf den USB-Port und das daran angeschlossene 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 (⇨ 50).

Was möchten Sie tun?

- ☐ 'Geräteverbindung via SEH UTN Manager trennen' ⇨ 49
- ☐ 'Geräteverbindung via myUTN Control Center trennen' ⇨ 49

Geräteverbindung via SEH UTN Manager trennen

Voraussetzung

- ✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨🗎13.
- ✓ Der USB-Port wird in der Auswahlliste angezeigt; siehe: ⇨🗎46.
- ✓ Der USB-Port ist mit Ihrem Client verbunden.

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

↳ Die Verbindung wird getrennt.

Geräteverbindung via myUTN Control Center trennen

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

↳ Die Verbindung wird getrennt.

5.5 Wie fordere ich ein belegtes USB-Gerät an?

Sie haben die Möglichkeit, ein USB-Gerät anzufordern, das von einem anderen Benutzer aktiv verwendet wird. Dafür versenden Sie eine Freigabe-Anforderung für den USB-Port, an den das USB-Gerät angeschlossen ist.

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

Voraussetzung

- ✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨🗎13.
- ✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client des Benutzers, der das USB-Gerät verwendet, installiert; siehe: ⇨🗎13.
- ✓ Der SEH UTN Manager (vollständige Variante) wird auf beiden Clients ausgeführt.
- ✓ Der USB-Port wird in der Auswahlliste angezeigt; siehe: ⇨🗎46.
- ✓ Der USB-Port ist mit einem anderen Client verbunden.

1. Markieren Sie den Port in der Auswahlliste.
2. Wählen Sie im Menü **Port** den Befehl **Anfordern**.

↳ Die Freigabe-Anforderung wird gesendet.

5.6 Wie automatisiere ich Portverbindungen und Programmstarts?

Sie haben die Möglichkeit, Verbindungen zu USB-Ports (inklusive angeschlossenen USB-Geräten) und Programmstarts auf verschiedene Arten zu automatisieren. Hierzu stehen unterschiedliche Automatismen zur Verfügung.

Was möchten Sie tun?

- ☐ 'Permanente Portverbindung nach Betriebssystemstart (Auto-Connect)' ⇨🗎50
- ☐ 'Portverbindung nach einem definierten Zeitraum automatisch trennen (Auto-Disconnect)' ⇨🗎51
- ☐ 'Zusatztool 'utnm' verwenden' ⇨🗎118

Permanente Portverbindung nach Betriebssystemstart (Auto-Connect)

Die Funktion stellt automatisch eine permanente Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät her, ohne dass sich ein Benutzer am Client anmelden muss. Die Verbindung wird

- beim Betriebssystemstart aktiviert und beim Herunterfahren des Systems beendet,
- bei einem System-Neustart automatisch wieder hergestellt.

Voraussetzung

- ✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨🗎13.
- ✓ Der USB-Port wird in der Auswahlliste angezeigt; siehe: ⇨🗎46.
- ✓ Sie sind als Administrator am System angemeldet.

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

↳ Die Einstellung wird gespeichert.

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

Die Funktion ermöglicht das automatische Trennen einer Verbindung zu einem USB-Port 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-Ports an einem UTN-Server.

2 Minuten vor Ablauf des definierten Zeitraums erhält der Benutzer eine Meldung die Verbindung zum USB-Port und dem daran angeschlossenen USB-Gerät zu beenden, um Datenverlust und Fehlerzuständen vorzubeugen. Wurde die Verlängerung aktiviert, erscheint der Infohinweis inkl. der Möglichkeit, die Verlängerung zu akzeptieren oder abzulehnen.

Hinweis

Sie haben die Möglichkeit, sich nach dem automatischen Trennen einer Verbindung über die Portverfügbarkeit informieren zu lassen. Richten Sie hierzu eine Benachrichtigung über die Freigabe eines USB-Ports ein; siehe: ⇨🗎52.

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

Voraussetzung

- ✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨🗎13.
- ✓ Der UTN-Server wird im Bereich 'Automatische Gerätetrennung' angezeigt; siehe: ⇨🗎46.
- ✓ Sie sind als Administrator am System angemeldet.

1. Starten Sie den SEH UTN Manager.
2. Wählen Sie im Menü **Programm** den Befehl **Optionen**.
   Der Dialog **Optionen** erscheint.
3. Wählen Sie die Registerkarte **Automatismen** an.
4. Aktivieren Sie im Bereich **Auto-Disconnect** 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.

5.7 Wie erhalte ich Informationen zum USB-Port und USB-Gerät?

Sie haben die Möglichkeit, die Statusinformation des USB-Ports und USB-Gerätes einzusehen. Zudem können Sie automatische Meldungen konfigurieren. Sie werden dann informiert, wenn ein USB-Port und das daran angeschlossene USB-Gerät verfügbar sind, nachdem sie belegt waren.

Was möchten Sie tun?

- ☐ 'Statusinformationen anzeigen' ⇨🗎52
- ☐ 'Meldungen konfigurieren' ⇨🗎52

Statusinformationen anzeigen

Voraussetzung

- ✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨🗎13.
- ✓ Der USB-Port wird in der Auswahlliste angezeigt; siehe: ⇨🗎46.

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

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

Meldungen konfigurieren

Voraussetzung

- ✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨🗎13.
- ✓ Der USB-Port wird in der Auswahlliste angezeigt; siehe: ⇨🗎46.

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

↳ Die Einstellung wird gespeichert.
Sobald ein Netzteilnehmer die Verbindung zu dem USB-Port und dem daran angeschlossenen 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. Diese USB-Geräte können via Portverbindung mit dem Client verbunden und dann verwendet werden. Die Auswahlliste ist bearbeitbar und kann bedarfsgerecht durch Hinzufügen und Entfernen der benötigten UTN-Server eingerichtet werden.

Nutzen und Zweck

Ein Administrator kann über Typ und Verteilung der Auswahlliste in Kombination mit der Benutzerverwaltung den Zugriff auf die im Netzwerk verfügbaren UTN-Server kontrollieren.

Alle Anwender benutzen zunächst immer dieselbe globale Auswahlliste. Alternativ hat ein Administrator die Möglichkeit, den Anwendern benutzerindividuelle Auswahllisten mit Hilfe einer ini-Datei zur Verfügung zu stellen.

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

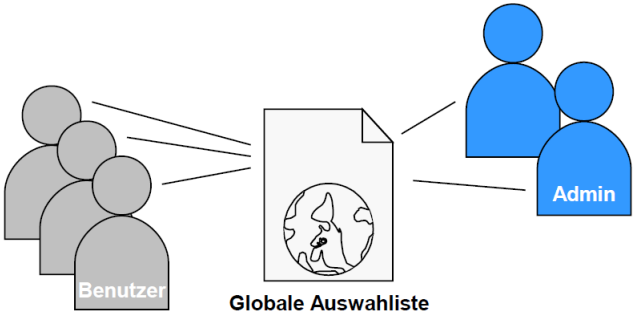


Abbildung 12: Globale Auswahlliste

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.

Benutzer-individuelle Auswahlliste

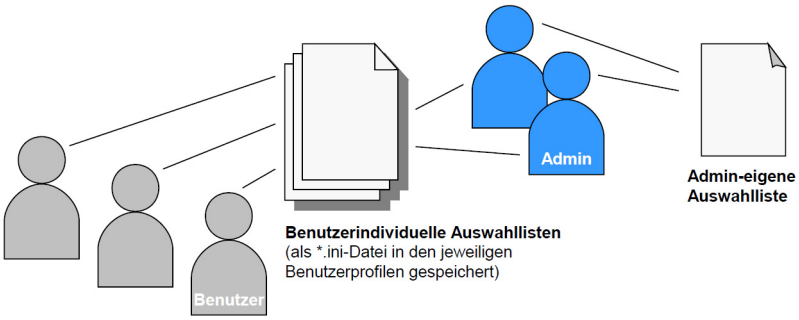


Abbildung 13: Benutzerindividuelle Auswahlliste

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:
  `$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`

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

  Beispiel:

  Ubuntu 14.04.01 LTS:

  `echo $HOME` ergibt `/home/Benutzername`

  \+

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

  Vollständiger Pfad zur ini-Datei:

  `/home/Benutzername/.config/SEH Computertechnik GmbH/SEH`

Was möchten Sie tun?

- ☐ 'Globale Auswahlliste für alle Benutzer bereitstellen' ⇨🗎55
- ☐ 'Benutzerindividuelle Auswahllisten bereitstellen' ⇨🗎55
- ☐ 'Benutzern eine vordefinierte Auswahlliste bereitstellen' ⇨🗎55
- ☐ 'Benutzerindividuelle Auswahlliste schützen' ⇨🗎56

Globale Auswahlliste für alle Benutzer bereitstellen

Voraussetzung

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 13.
✓ Sie sind als Administrator am System angemeldet.

1. Starten Sie den SEH UTN Manager.
2. Stellen Sie die Auswahlliste zusammen; siehe: 'Wie füge ich UTN-Server/USB-Geräte der Auswahlliste hinzu?' ⇨ 46.
3. Wählen Sie im Menü **Programm** den Befehl **Optionen**.
   Der Dialog **Optionen** erscheint.
4. Wählen Sie die Registerkarte **Auswahlliste** an.
5. Aktivieren Sie die Option **Globale Auswahlliste**.
6. Wählen Sie die Schaltfläche **OK** an.

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

Benutzerindividuelle Auswahllisten bereitstellen

Voraussetzung

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 13.
✓ Sie sind als Administrator am System angemeldet.

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

↳ Die Einstellung wird gespeichert. Jeder Benutzer verwendet eine individuelle Auswahlliste. Die Auswahllisten der Benutzer werden als ini-Dateien in benutzerindividuellen Verzeichnissen abgespeichert (siehe: 'Benutzer- individuelle Auswahlliste' ⇨ 54).

Hinweis

Die Administratoren teilen sich eine Auswahlliste.

Benutzern eine vordefinierte Auswahlliste bereitstellen

Voraussetzung

✓ Der SEH UTN Manager (vollständige Variante) ist auf dem Client installiert; siehe: ⇨ 13.

✓ Sie sind als Administrator am System angemeldet.

1. Starten Sie den SEH UTN Manager.
2. Stellen Sie die Auswahlliste für den Benutzer zusammen; siehe: 'Wie füge ich UTN-Server/USB-Geräte der Auswahlliste hinzu?' ⇨🗎46.
3. Wählen Sie im Menü **Programm** den Befehl **Optionen**.
   Der Dialog **Optionen** erscheint.
4. Wählen Sie die Registerkarte **Auswahlliste** an.
5. Aktivieren Sie die Option **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:
   `$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
   (Siehe: 'Benutzerindividuelle Auswahlliste' ⇨🗎54.)

↳ 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:

`$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
(Siehe: 'Benutzer- individuelle Auswahlliste' ⇨🗎54)

Verwenden Sie die Betriebssystemsteuerung, 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.

Welche Information benötigen Sie?

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

- 'Wie definiere ich die Verschlüsselungsstärke für SSL-/TLS-Verbindungen?' ⇨🗎58
- 'Wie verschlüssele ich die Verbindung zum myUTN Control Center?' ⇨🗎60
- 'Wie kontrolliere ich den Zugang zum myUTN Control Center? (Benutzerkonten)' ⇨🗎60
- 'Wie kontrolliere ich den Zugriff zum UTN-Server? (TCP-Portzugriffskontrolle)' ⇨🗎62
- 'Wie kontrolliere ich den Zugriff auf USB-Geräte? (nur myUTN-80 und höher)' ⇨🗎63
- 'Wie blockiere ich USB-Gerätetypen?' ⇨🗎66
- 'Wie setze ich Zertifikate korrekt ein?' ⇨🗎67
- 'Wie verwende ich Authentifizierungsmethoden?' ⇨🗎74
- 'Wie verschlüssele ich die Datenübertragung?' ⇨🗎80

Hinweis

Zusätzlich kann das myUTN Control Center über das SNMP-Sicherheitskonzept und/oder VLAN-Zugriffeinstellungen geschützt werden. Für weitere Informationen, siehe:

- 'Wie konfiguriere ich SNMP?' ⇨🗎27.
- 'Wie setze ich den UTN-Server in VLAN-Umgebungen ein? (nur myUTN-80 und höher)' ⇨🗎42

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

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

- E-Mail: POP3 (⇨ 29)
- E-Mail: SMTP (⇨ 29)
- Webzugang zum myUTN Control Center: HTTPS (⇨ 60)
- Datenübertragung zwischen den Clients und dem UTN-Server (bzw. den angeschlossenen USB-Geräten): USB-Port (⇨ 80)

Verschlüsselungsstärke

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

Protokoll

Zur Verschlüsselung der Verbindung werden die Verschlüsselungsprotokolle SSL (Secure Sockets Layer) und dessen Nachfolger TLS (Transport Layer Security) verwendet. Welche Protokolle vom UTN-Server unterstützt werden, hängt von der Produkt-Hardware und der installierten Firmware/Software ab.

Verschlüsselungsstufe

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 zu einer Verschlüsselungsstufe zusammengefasst. Welche Cipher Suites vom UTN-Server unterstützt werden, also Teil einer Verschlüsselungsstufe sind, hängt vom verwendeten SSL-/TLS-Protokoll ab.

Folgende Verschlüsselungsstufen sind wählbar:

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

Verbindungsaufbau

Beim Aufbau einer sicheren Verbindung wird das zu verwendende Protokoll sowie eine Liste von unterstützten Cipher Suites an den Kommunikationspartner gesendet. Es wird eine Cipher Suite ausgehandelt, die im Weiteren verwendet wird. Standardmäßig handelt es sich um die stärkste von beiden Parteien unterstützte Cipher Suite.

Unterstützt der Kommunikationspartner das gewählte Protokoll nicht und/oder gibt es keine von beiden Seiten unterstützte Cipher Suite, wird keine SSL-/TLS-Verbindung aufgebaut.

Warnung

Die Kommunikationspartner des UTN-Servers (z.B. Browser) müssen das Verschlüsselungsprotokoll und die Cipher Suites der gewählten Verschlüsselungsstufe für einen erfolgreichen Verbindungsaufbau unterstützen. Bei Problemen wählen Sie andere Einstellungen oder setzen die UTN-Server-Parameter zurück; siehe: ⇨🗎84.

Hinweis

Wählen Sie für das Verschlüsselungsprotokoll und die Verschlüsselungsstufe die Option 'Beliebig', werden beide Einstellungen zwischen dem UTN-Server und dem Kommunikationspartner automatisch ausgehandelt. Mit diesen Einstellungen sind die Chancen für einen erfolgreichen Verbindungsaufbau am größten.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - SSL-Verbindungen** an.
3. Wählen Sie im Bereich **Verschlüsselungsprotokoll** das gewünschte Protokoll.

Warnung

Verwenden Sie <u>nicht</u> das Verschlüsselungsprotokoll 'SSL', wenn Sie aktuelle Browser-Software nutzen und für den Webzugang zum myUTN Control Center ausschließlich HTTPS als erlaubter Verbindungstyp definiert ist. Aktuelle Browser unterstützen SSL nicht, somit kann keine Verbindung aufgebaut werden.

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

Warnung

Verwenden Sie <u>nicht</u> die Verschlüsselungsstufe 'Niedrig', wenn Sie aktuelle Browser-Software nutzen und für den Webzugang zum myUTN Control Center ausschließlich HTTPS als erlaubter Verbindungstyp definiert ist. Aktuelle Browser unterstützen Cipher Suites der Stufe 'Niedrig' nicht, somit kann keine Verbindung aufgebaut werden.

5. Bestätigen Sie mit **Speichern**.

↳ Die Einstellung wird gespeichert.

Hinweis

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

6.2 Wie verschlüssele ich die Verbindung zum myUTN Control Center?

Verbindungstyp (HTTP/HTTPS)

Die Verbindung zum myUTN Control Center kann durch die Wahl des erlaubten Verbindungstypen (HTTP/HTTPS) geschützt werden.

Wird ausschließlich HTTPS als Verbindungstyp gewählt, ist die Verbindung zum myUTN Control Center via SSL/TLS verschlüsselt. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert (⇨🗎58).

Warnung

Das Verschlüsselungsprotokoll darf nicht 'SSL' und die Verschlüsselungsstufe darf nicht 'Niedrig' sein. Aktuelle Browser unterstützen diese Einstellungen nicht, wodurch keine Verbindung aufgebaut werden kann.

Bei SSL/TLS wird zudem ein Zertifikat (⇨🗎67) benötigt, um die Identität des UTN-Servers zu überprüfen. Bei einem so genannten 'Handshake' fragt der Client via Browser nach dem 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'.

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

↳ Die Einstellung wird gespeichert.

6.3 Wie kontrolliere ich den Zugang zum myUTN Control Center? (Benutzerkonten)

Sie können den Zugang zum myUTN Control Center limitieren. Dabei wird der Zugriff mithilfe von Benutzerkonten eingeschränkt.

Benutzerkonten

Es gibt zwei Benutzerkonten, für die Name und Passwort zu definieren sind. Sie sind mit unterschiedlichen Rechten ausgestattet.

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

Hinweis

Die Benutzerkonten werden auch für SNMP verwendet; siehe: ⇨🗎27.

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

Login

Ist die Zugriffskontrolle aktiv, erscheint beim Aufrufen des myUTN Control Centers ein Anmeldefenster. Sie können zwischen zwei Login-Masken wählen:

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

Sitzungs-Timeout

Als zusätzliche Sicherheitsmaßnahme können Sie ein Sitzungs-Timeout nutzen. Wenn innerhalb des definierten Timeouts keine Aktivität stattfindet, wird die Verbindung zum myUTN Control Center aus automatisch beendet.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Gerätezugriff** an.
3. Definieren Sie die zwei Benutzerkonten. Geben Sie hierzu im Bereich **Benutzerkonten** jeweils Benutzername und Passwort ein.
   (Um sicherzustellen, dass Sie sich beim Passwort nicht vertippen, können Sie den Klartext einblenden.)
4. Aktivieren Sie die Option **Control Center-Zugriff einschränken**.
5. Wählen Sie für das Anmeldefenster die Art der Login-Maske: **Liste der Benutzer** oder **Name und Passwort**.
6. Aktivieren Sie die Option **Sitzungs-Timeout** und geben Sie im Feld **Sitzungsdauer** den Zeitraum in Minuten ein, nach dem das Timeout wirksam werden soll. (Optional)
7. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

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

TCP-Portzugriffs-kontrolle

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.

Sicherheits-stufen

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.

Warnung

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

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - TCP-Portzugriff** an.
3. Aktivieren Sie die Option **Portzugriff kontrollieren**.
4. Wählen Sie im Bereich **Sicherheitsstufe** den gewünschten Schutz.
5. Definieren Sie im Bereich **Ausnahmen** die Netzwerkelemente, die 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.

Hinweis

Kann der UTN-Server über das myUTN Control Center nicht mehr erreicht werden, initiieren Sie einen Geräte-Neustart; siehe: ⇨🗎87.

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.

6.5 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-Portschlüssel-kontrolle

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.

Weder USB-Port noch das daran angeschlossene USB-Gerät werden im SEH UTN Manager angezeigt. Ein Anwender hat dann keine Möglichkeit, Einstellungen am USB-Port vorzunehmen oder eine Verbindung zwischen Client und USB-Port herzustellen.

Um den USB-Port und das daran angeschlossene 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-Geräte-zuordnung

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.

Hinweis

Wenn Sie den Zugriff auf die USB-Gräte kontrollieren, sollten Sie den administrativen Zugriff zum myUTN Control Center zusätzlich einschränken, so dass kein Unbefugter die Einstellungen ändern kann; siehe: ⇨🗎60.

Was möchten Sie tun?

- ☐ 'Zugriff auf USB-Gerät sperren' ⇨🗎64
- ☐ 'Zugriff auf USB-Gerät freischalten' ⇨🗎64
- ☐ 'Gerätezuordnung am USB-Port definieren' ⇨🗎65
- ☐ 'USB-Port-Zugriffskontrolle deaktivieren' ⇨🗎65

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.

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

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

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.

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

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

↳ Die Einstellungen werden gespeichert. Am USB-Port kann ausschließlich das zugewiesene USB-Gerät betrieben werden.

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

USB-Port-Zugriffskontrolle deaktivieren

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

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.

6.6 Wie blockiere ich USB-Gerätetypen?

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

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

Um den UTN-Server davor zu schützen, haben Sie die Möglichkeit, Eingabegeräte der HID-Klasse zu blockieren.

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

6.7 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' ⇨🗎75.
- um den UTN-Server bei der geschützten E-Mail-Kommunikation (POP3/SMTP via SSL/TLS) zu authentifizieren ⇨🗎29.
- um den UTN-Server/Client zu authentifizieren, wenn die Datenübertragung zwischen den Clients und dem UTN-Server (bzw. den angeschlossenen USB-Geräten) via SSL/TLS verschlüsselt ist ⇨🗎80.
- um den UTN-Server/Client zu authentifizieren, wenn der administrative Zugang des myUTN Control Centers via HTTPS (SSL/TLS) geschützt ist.

Hinweis

Wenn Sie Zertifikate verwenden, sollten Sie den administrativen Zugriff zum myUTN Control Center zusätzlich einschränken, so dass kein Unbefugter Zertifikate auf dem UTN-Server löschen kann; siehe: ⇨🗎60.

Welche Zertifikate gibt es?

Im UTN-Server können sowohl selbstsignierte als auch fremdsignierte 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 angefordertes Zertifikat ersetzen.
- **Selbstsignierte Zertifikate** tragen eine digitale Unterschrift, die vom UTN-Server erstellt wurde.
- Ein **angefordertes Zertifikat** wird auf Basis einer Zertifikatsanforderung von einer Zertifizierungsstelle (Certification Authority - CA) für den UTN-Server erstellt.

- **CA-Zertifikate** sind Zertifikate, die für eine Zertifizierungsstelle (Certification Authority - CA) ausgestellt wurden. Mit ihnen werden Zertifikate überprüft, die von der jeweiligen Zertifizierungsstelle ausgegeben wurden.
- **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 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 Client-Zertifikat, d.h. 1 angefordertes Zertifikat oder 1 PKCS#12-Zertifikat
- 1 S/MIME-Zertifikat (nur myUTN-80 und höher)
- 1–32 CA-Zertifikate

Alle Zertifikate können separat gelöscht werden.

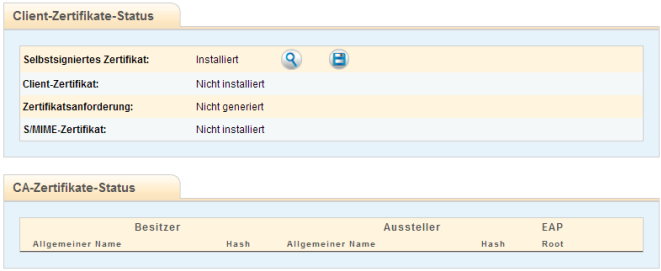


Abbildung 14: myUTN Control Center - Zertifikate

Was möchten Sie tun?

- ☐ 'Zertifikat anzeigen' ⇨🗎69
- ☐ 'Selbstsigniertes Zertifikat erstellen' ⇨🗎69
- ☐ 'Zertifikatsanforderung für ein angefordertes Zertifikat erstellen' ⇨🗎70
- ☐ 'Angefordertes Zertifikat auf dem UTN-Server speichern' ⇨🗎71
- ☐ 'PKCS#12-Zertifikat auf dem UTN-Server speichern' ⇨🗎71
- ☐ 'S/MIME-Zertifikat auf dem UTN-Server speichern (nur myUTN-80 und höher)' ⇨🗎72
- ☐ 'CA-Zertifikat auf dem UTN-Server speichern' ⇨🗎72
- ☐ 'Zertifikat löschen' ⇨🗎73

Zertifikat anzeigen

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

Voraussetzung

✓ Auf dem UTN-Server ist ein Zertifikat installiert.

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

↳ Das Zertifikat wird angezeigt.

Selbstsigniertes Zertifikat erstellen

Hinweis

Ist bereits ein selbstsigniertes Zertifikat auf dem UTN-Server erstellt worden, muss dieses zunächst gelöscht werden; siehe: ⇨🗎73.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate** an.
3. Wählen Sie die Schaltfläche **Selbstsigniertes Zertifikat** an.
4. Geben Sie die entsprechenden Parameter ein; Tabelle 13 ⇨🗎69.
5. Wählen Sie die Schaltfläche **Erstellen/Installieren** an.

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

Tabelle 13: Parameter für die Erstellung von Zertifikaten

Parameter	Beschreibung
Allgemeiner Name	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.*
Unternehmensbereich	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.*

Parameter	Beschreibung
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 angefordertes Zertifikat erstellen

Als Vorbereitung auf das Verwenden eines Zertifikats, das von einer Zertifizierungsstelle für den UTN-Server ausgestellt wird, kann im UTN-Server eine Zertifikatsanforderung erstellt werden. Die Anforderung muss an die Zertifizierungsstelle gesendet werden, welche anhand der Zertifikatsanforderung ein Zertifikat erstellt. Das Zertifikat muss im 'Base64'-Format vorliegen.

Hinweis

Ist bereits eine Zertifikatsanforderung erstellt, muss diese zunächst gelöscht werden; siehe: ⇨🗎73.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate** an.
3. Wählen Sie die Schaltfläche **Zertifikatsanforderung** an.
4. Geben Sie die benötigten Parameter ein; Tabelle 13 ⇨🗎69.
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 angeforderte Zertifikat auf dem UTN-Server gespeichert werden; siehe: ⇨🗎71.

Angefordertes Zertifikat auf dem UTN-Server speichern

Voraussetzung

✓ Es wurde zuvor eine entsprechende Zertifikatsanforderung erstellt; siehe: ⇨🗎70.
✓ Das Zertifikat muss im 'Base64'-Format vorliegen.

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 angeforderte Zertifikat an.
6. Wählen Sie die Schaltfläche **Installieren** an.

↳ Das angeforderte Zertifikat 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.

Hinweis

Ist bereits ein PKCS#12-Zertifikat auf dem UTN-Server installiert, muss dieses zunächst gelöscht werden; siehe: ⇨🗎73.

Voraussetzung

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

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.

Hinweis

Ist bereits ein S/MIME-Zertifikat auf dem UTN-Server installiert, muss dieses zunächst gelöscht werden; siehe: ⇨🗎73.

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.

CA-Zertifikat auf dem UTN-Server speichern

Um in einem Netzwerk die Identität von Kommunikationspartnern des UTN-Servers überprüfen zu können, ist es erforderlich, deren Zertifikate zu validieren. Hierzu werden die Wurzel-CA-Zertifikate von denjenigen Zertifizierungsstellen, die die Zertifikate der Kommunikationspartner ausgestellt haben auf dem UTN-Server installiert.

Bis zu 32 CA-Zertifikate können installiert werden. Dadurch werden mehrstufige Public Key Infrastrukturen (PKI) unterstützt.

Beispiel: Um in einem Netzwerk die Identität des UTN-Servers zu überprüfen, bietet der UTN-Server mehrere Authentifizierungsverfahren an. Wenn Sie das Authentifizierungsverfahren 'EAP-TLS' (⇨🗎75) verwenden, ist es erforderlich, das Wurzel-CA-Zertifikat der Zertifizierungsstelle auf den UTN-Server zu installieren, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat.

Voraussetzung

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

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate** an.
3. Wählen Sie die Schaltfläche **CA-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.

Zertifikat löschen

Warnung

Löschen Sie nicht das Zertifikat (CA/selbstsigniert/PKCS#12), wenn für den Webzugang zum myUTN Control Center ausschließlich HTTPS als erlaubter Verbindungstyp definiert ist. Wird das zugehörige Zertifikat gelöscht, kann das myUTN Control Center nicht mehr erreicht werden. Starten Sie in diesem Fall den UTN-Server neu ⇨🗎87. Dabei generiert der UTN-Server ein neues selbstsigniertes Zertifikat, wodurch eine gesicherte Verbindung aufgebaut werden kann.

Voraussetzung

✓ Auf dem UTN-Server ist ein Zertifikat installiert.

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

↳ Das Zertifikat wird gelöscht.

6.8 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' ⇨🗎74
- ☐ 'EAP-TLS konfigurieren' ⇨🗎75
- ☐ 'EAP-TTLS konfigurieren' ⇨🗎76
- ☐ 'PEAP konfigurieren' ⇨🗎77
- ☐ 'EAP-FAST konfigurieren' ⇨🗎78

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.

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.

Hinweis

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: ⇨84.

Vorgehensweise

- Erstellen Sie auf dem UTN-Server eine Zertifikatsanforderung; siehe: ⇨🗎70.
- Erstellen Sie mit der Zertifikatsanforderung und mit Hilfe des Authentifizierungsservers ein Zertifikat.
- Installieren Sie das angeforderte Zertifikat auf dem UTN-Server; siehe: ⇨🗎71.
- Installieren Sie das Wurzel-CA-Zertifikat der Zertifizierungsstelle auf den UTN-Server, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat; siehe: 'CA-Zertifikat auf dem UTN-Server speichern' ⇨🗎72.
- Aktivieren Sie das Authentifizierungsverfahren 'EAP-TLS' auf dem UTN-Server.

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. Wählen Sie in der Liste **EAP-Wurzelzertifikat** das Wurzel-CA-Zertifikat aus.
5. 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.

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. Um die Sicherheit beim Verbindungsaufbau zu erhöhen, installieren Sie optional ein Wurzel-CA-Zertifikat der Zertifizierungsstelle auf den UTN-Server, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat; siehe: 'CA-Zertifikat auf dem UTN-Server speichern' ⇨🗎72.
   Wählen Sie anschließend in der Liste **EAP-Wurzelzertifikat** das Wurzel-CA-Zertifikat aus.
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. ⇨🗎76) 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.

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. Um die Sicherheit beim Verbindungsaufbau zu erhöhen, installieren Sie optional ein Wurzel-CA-Zertifikat der Zertifizierungsstelle auf den UTN-Server, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat; siehe: 'CA-Zertifikat auf dem UTN-Server speichern' ⇨🗎72.
   Wählen Sie anschließend in der Liste **EAP-Wurzelzertifikat** das Wurzel-CA-Zertifikat aus.
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. ⇨🗎76) 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.

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.

6.9 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.

Hinweis

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: ⇨🗎37.

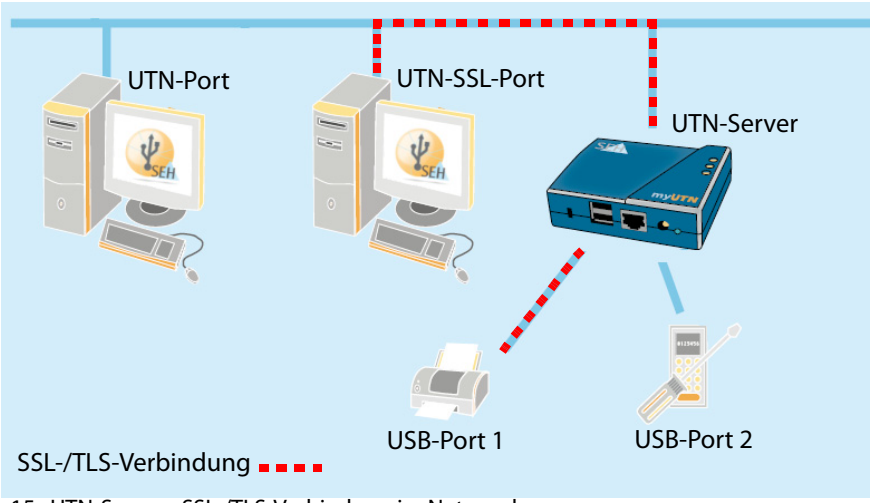


Abbildung 15: UTN-Server - SSL-/TLS-Verbindung im Netzwerk

Um eine SSL-/TLS-Verbindung zu verwenden, muss die Verschlüsselung am gewünschten USB-Port aktiviert werden. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨🗎58.

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

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

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

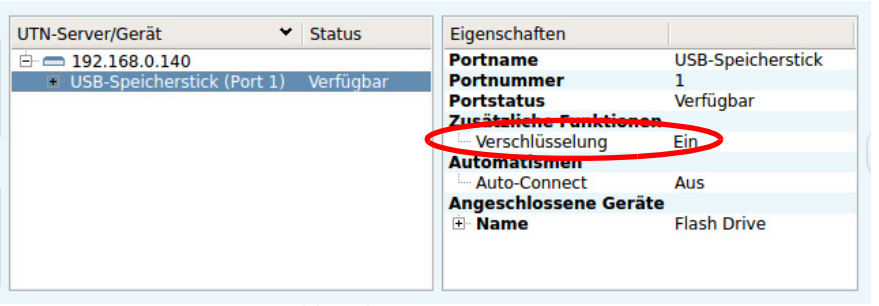


Abbildung 16: SEH UTN Manager - Verschlüsselung

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)' ⇨ 82
- 'Wie setze ich die UTN-Parameter auf die Standardwerte zurück?' ⇨ 84
- 'Wie führe ich ein Update aus?' ⇨ 86
- 'Wie starte ich den UTN-Server neu?' ⇨ 87

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.

Automatisches Backup (nur myUTN-800)

Beim Dongleserver myUTN-800 steht zusätzlich ein automatisches Backup zur Verfügung. Dabei werden die Parameterwerte, Passwörter und auf den UTN-Server geladene Zertifikate automatisch auf einer angeschlossenen SD-Karte gespeichert. Nach einer Parameter- oder Zertifikatänderung wird die Sicherung automatisch aktualisiert.

Warnung

Bei Verlust oder Diebstahl der SD-Karte entsteht eine Sicherheitslücke (Zertifikate, Passwörter) in Ihrer Umgebung. Ergreifen Sie für den myUTN-800 bei Verwendung des automatischen Backups daher geeignete Maßnahmen zum Schutz des UTN-Servers.

Hinweis

Bei Auslieferung befindet sich die SD-Karte bereits im SD-Card-Reader und ist betriebsbereit (kein Anschließen oder Formatieren erforderlich).

Mithilfe der Sicherung kann die vollständige Konfiguration schnell und einfach auf andere UTN-Server übertragen werden (z.B. beim Austausch von UTN-Servern). Parameterwerte, Passwörter und Zertifikate werden automatisch von der SD-Karte auf einen Dongleserver myUTN-800 geladen, wenn ein Kaltstart am UTN-Server durchgeführt wird.

Was möchten Sie tun?

- ☐ 'Parameterwerte anzeigen' ⇨🗎83
- ☐ 'Parameterdatei sichern' ⇨🗎83
- ☐ 'Parameterdatei auf den UTN-Server laden' ⇨🗎83
- ☐ 'Automatisches Backup (nur myUTN-800)' ⇨🗎84

Parameterwerte anzeigen

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.

Hinweis

Detaillierte Beschreibungen zu den Parametern entnehmen Sie der 'Parameterliste' ⇨🗎92.

Parameterdatei sichern

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

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.

Hinweis

myUTN-800: Möchten Sie Parameterwerte und Zertifikate aus einem automatischen Backup von einer SD-Karte laden, führen Sie einen Kaltstart des UTN-Servers durch (Stromversorgung unterbrechen und wiederherstellen).

Automatisches Backup (nur myUTN-800)

Voraussetzung

- ✓ Es ist eine SD-Karte am UTN-Server angeschlossen.
- ✓ Die SD-Karte verfügt über das Dateisystem FAT12, FAT16 oder FAT32.
- ✓ Auf der SD-Karte ist 1 MB Speicherplatz verfügbar.

1. Starten Sie das myUTN Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG - SD-Karte** an.
3. Aktivieren Sie die Option **Parameter-Backup**.
4. Wählen Sie die Schaltfläche **Speichern** an.
↳ Die Einstellungen werden gespeichert.

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.

Hinweis

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' ⇨🗎85
- ☐ 'Parameter via Reset-Taster zurücksetzen' ⇨🗎85

Warnung

myUTN-800: Entnehmen Sie die SD-Karte aus dem UTN-Server bevor Sie die Parameter zurücksetzen. Andernfalls übernimmt der UTN-Server die darauf gesicherten Parameterwerte (automatisches Backup ⇨🗎84).

Hinweis

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

Parameter via myUTN Control Center zurücksetzen

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

↳ Die Parameter werden zurückgesetzt.

Parameter via Reset-Taster zurücksetzen

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.

1. Drücken Sie den Reset-Taster für 5 Sekunden.
   Der UTN-Server startet neu.
   (Beim Dongleserver myUTN-800 ertönt beim Neustart ein Signalton.)

↳ Die Parameter sind zurückgesetzt.

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.

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.html

Hinweis

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

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' ⇨🗎87
- ☐ 'UTN-Server über Restart-Taster neu starten (nur myUTN-800)' ⇨🗎87

UTN-Server via myUTN Control Center neu starten

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

↳ Der UTN-Server wird neu gestartet.

UTN-Server über Restart-Taster neu starten (nur myUTN-800)

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

↳ 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' ⇨🗎89
- 'SEH UTN Manager' ⇨🗎89

Netzwerktechnologie

- 'Hardware- Adresse' ⇨🗎89
- 'IP-Adresse' ⇨🗎90
- 'Hostname' ⇨🗎90
- 'Gateway' ⇨🗎90
- 'Netzwerkmaske' ⇨🗎90
- 'Default-Name' ⇨🗎90

Sonstiges

- 'Compound- USB-Gerät' ⇨🗎91

myUTN Control Center

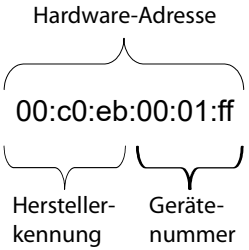
Über das myUTN Control Center kann der UTN-Server konfiguriert und überwacht werden. Das myUTN Control Center ist in dem UTN-Server gespeichert und kann mit einer Browsersoftware (z.B. Mozilla Firefox) dargestellt werden.

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 im Netzwerk eingebundenen UTN-Server an und stellt die Verbindung zwischen Client und USB-Port inklusive dem daran angeschlossenen 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 oder im SEH UTN Manager abgelesen werden.

Die Verwendung von Trennzeichen in der Hardware-Adresse ist plattformabhängig. Unter Linux werden ':' verwendet.

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

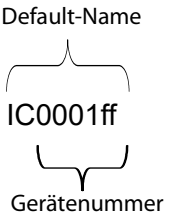
Über ein Gateway können IP-Adressen in einem anderen Netzwerk angesprochen werden. Möchten Sie ein Gateway verwenden, können Sie über das myUTN Control Center den entsprechenden Parameter im UTN-Server konfigurieren.

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 abgelesen werden.

Compound-USB-Gerät

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

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

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?

Hinweis

Um die aktuellen Parameterwerte Ihres UTN-Servers einzusehen, siehe: 'Parameterwerte anzeigen' ⇨🗎83.

Tabelle 14: 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 15: Parameterliste - IPv4-VLAN (nur myUTN-80 und höher)

Parameter	Wertekonvention	Default	Beschreibung
ip4vlan_mgmt [IPv4-Management-VLAN]	on/off	off	De-/aktiviert die Weiterleitung der IPv4-Management-VLAN-Daten.
ip4vlan_mgmt_id [VLAN-ID]	0–4096 [1–4 Zeichen; 0–9]	0	ID zur Identifizierung des IPv4-Management-VLAN (0–4096).
ip4vlan_mgmt_any [Zugriff über alle VLANs]	on/off	off	De-/aktiviert den administrativen Zugang (Web) zum UTN-Server über IPv4-Client-VLANs. *Ist die Option aktiviert, kann der UTN-Server aus allen VLANs heraus administriert werden.*
ip4vlan_mgmt_untag [Zugriff vom LAN (untagged)]	on/off	on	De-/aktiviert den administrativen Zugang zum UTN-Server über IPv4-Pakete ohne Tag. *Ist die Option deaktiviert, kann der UTN-Server ausschließlich über VLANs administriert werden.*
ipv4vlan_on_1 ~ ipv4vlan_on_20 [VLAN]	on/off	off	De-/aktiviert die Weiterleitung der IPv4-Client-VLAN-Daten.
ipv4vlan_addr_1 ~ ipv4vlan_addr_20 [IP-Adresse]	gültige IP-Adresse	192.168.0.0	Definiert die IP-Adresse des UTN-Servers innerhalb des IPv4-Client-VLAN.

Parameter	Wertekonvention	Default	Beschreibung
ipv4vlan_mask_1 ~ ipv4vlan_mask_20 [Netzwerkmaske]	gültige IP-Adresse	255.255.255.0	Definiert die Netzwerkmaske des UTN-Servers innerhalb des IPv4-Client-VLAN.
ip4vlan_gate_1 ~ ip4vlan_gate_20 [Gateway]	gültige IP-Adresse	0.0.0.0	Gateway-Adresse des IPv4-Client-VLANs.
ipv4vlan_id_1 ~ ipv4vlan_id_20 [VLAN-ID]	0–4096 [1–4 Zeichen; 0–9]	0	Definiert eine ID zur Identifizierung des IPv4-Client-VLAN.

Tabelle 16: 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.
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 17: 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 18: Parameterliste - SSL-/TLS-Verbindungen

Parameter	Wertekonvention	Default	Beschreibung
sslmethod [Verschlüsselungs-protokoll]	any sslv3 tls10 tls11 tls12	any	Definiert das Verschlüsselungsprotokoll für SSL-/TLS-Verbindungen. *any = Beliebig* *sslv3 = SSL 3.0* *tls10 = TLS 1.0* *tls11 = TLS 1.1* *tls12 = TLS 1.2* **Verwenden Sie nicht das Verschlüsselungsprotokoll 'SSL', wenn Sie aktuelle Browser-Software nutzen und für den Webzugang zum myUTN Control Center ausschließlich HTTPS als erlaubter Verbindungstyp definiert ist.**
security [Verschlüsselungs-stufe]	1–4 [1 Zeichen]	4	Definiert die Verschlüsselungsstufe für SSL-/TLS-Verbindungen. *1 = Niedrig* *2 = Mittel* *3 = Hoch* *4 = Beliebig* **Verwenden Sie nicht die Verschlüsselungsstufe 'Niedrig', wenn für den Webzugang zum myUTN Control Center ausschließlich HTTPS als erlaubter Verbindungstyp definiert ist.**

Tabelle 19: Parameterliste - myUTN Control Center Sicherheit

Parameter	Wertekonvention	Default	Beschreibung
http_allowed [Verbindung]	on/off	on	Definiert den erlaubten Verbindungstyp (HTTP/HTTPS) zum myUTN Control Center. *Wird ausschließlich HTTPS als Verbindungstyp gewählt [http_allowed = off], ist der administrative Zugang zum myUTN Control Center via SSL/TLS geschützt.*
sessKeys [Control Center-Zugriff einschränken]	on/off	off	De-/aktiviert den eingeschränkten Zugang zum myUTN Control Center. Ist der Zugang eingeschränkt, erscheint beim Anrufen des myUTN Control Centers eine Login-Maske. Hinweis: Aktivieren Sie die Option, sind Benutzerkonten zu definieren.
sessKeyUList [Anmeldefenster zeigt]	on/off	on	Definiert das Aussehen der Login-Maske. on = Liste der Benutzer off = Dialog Name und Passwort
sessKeyTimer [Sitzungs-Timeout]	on/off	on	De-/aktiviert das Sitzungs-Timeout.
sessKeyTimeout [Sitzungs-Timeout]	120–3600 [3–4 Zeichen; 0–9]	600	Zeitraum in Sekunden nach dem das Timeout wirksam wird.
admin_name [Administrator - Benutzername]	max. 64 Zeichen [a–z, A–Z, 0–9]	admin	Definiert den Benutzernamen für das Administrator-Benutzerkonto. Hinweis: Ist gleichzeitig der Benutzername für das SNMP-Admin-Konto.
admin_pwd [Administrator - Passwort]	8–64 Zeichen [a–z, A–Z, 0–9]	administrator	Definiert das Passwort für das Administrator-Benutzerkonto. Hinweis: Ist gleichzeitig das Passwort für das SNMP-Admin-Konto.
any_name [Lesezugriff-Benutzer - Benutzername]	max. 64 Zeichen [a–z, A–Z, 0–9]	anonymous	Definiert den Benutzernamen für das Lesezugriff-Benutze-Benutzerkonto. Hinweis: Ist gleichzeitig der Benutzername für das SNMP-User-Konto.
any_pwd [Lesezugriff-Benutzer - Passwort]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert das Passwort für das Lesezugriff-Benutze-Benutzerkonto. Hinweis: Ist gleichzeitig das Passwort für das SNMP-User-Konto.

Tabelle 20: Parameterliste - USB-Gerätetypen-Blockierung

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

Tabelle 21: 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.
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 22: 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 23: Parameterliste - Verschlüsselung

Parameter	Wertekonvention	Default	Beschreibung
utn_sec_1 ~ utn_sec_20 [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 24: 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_20 [Methode]	--- ids key keyids	[---]	Definiert Methoden zur Zugriffs- und Nutzungseinschränkung für den USB-Port sowie das daran angeschlossene USB-Gerät. --- = *kein Schutz* *ids* = *Gerätezuordnung* *key* = *Portschlüsselkontrolle* *keyids* = *Gerätezuordnung und Portschlüsselkontrolle*
utn_keyval_1 ~ utn_keyval_20 [Schlüssel]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert den Schlüssel, mit dem das angeschlossene USB-Gerät vor Zugriff geschützt ist.
utn_vendprodIDs_1 ~ utn_vendprodIDs_20 [USB-Gerät]			Zeigt die VID (Vendor-ID) und PID (Product-ID) des USB-Gerätes an, das über die 'Gerätezuordnung' dem USB-Port zugewiesen ist.

Parameter	Wertekonvention	Default	Beschreibung
utn_2vlan_1 ~ utn_2vlan_20 [VLAN zuordnen]	0–9 [1 Zeichen] (vgl. ⇨🗎93)	0	Ordnet dem USB-Port ein VLAN zu. *0 = jedes* *1 = VLAN 1* *2 = VLAN 2 usw.* *9 = keines*

Tabelle 25: Parameterliste - USB-Port

Parameter	Wertekonvention	Default	Beschreibung
utn_tag_1 ~ utn_tag_20 [Portname]	max. 32 Zeichen [a–z, A–Z, 0–9]	[blank]	Freidefinierbare Beschreibung des USB-Ports.
utn_poff_1 ~ utn_poff_20 [Port]	on/off	off	De-/aktiviert die Stromzufuhr für den USB-Port (bzw. das an den Port angeschlossene USB-Gerät). *off = Stromzufuhr an* *on = Stromzufuhr aus*
utn_poffdura_1 ~ utn_poffdura_20	0–100 [1–3 Zeichen; 0–9]	0	**Der Parameter ist ausschließlich in Absprache mit dem SEH Support zu verwenden.**
utn_prereset_1 ~ utn_prereset_20	on/off	off	**Der Parameter ist ausschließlich in Absprache mit dem SEH Support zu verwenden.**

Tabelle 26: 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 27: 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_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_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.
admin_cipher [Verschlüsselung]	--- [keine] aes des	---	Definiert die Verschlüsselungsmethode der SNMP-Benutzergruppe 2.

Hinweis

Für SNMP-Benutzerkonten siehe: 'Parameterliste - myUTN Control Center Sicherheit' ⇨🗎96.

Tabelle 28: 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 29: 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 30: Parameterliste - Authentifizierung

Parameter	Wertekonvention	Default	Beschreibung
auth_typ [Authentifizierungs-methode]	--- [keine] MD5 TLS TTLS PEAP FAST	----	Definiert die Authentifizierungsmethode, mit der Geräte oder Benutzer im Netzwerk identifiziert werden.
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 = FAST-PROV1	---	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 31: 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 [1–4 Zeichen; 0–9; 0 = unbegrenzt]	4096	Definiert die maximale Größe (in Kbyte) der vom UTN-Server akzeptierten E-Mails.

Tabelle 32: 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.
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 33: 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-Ports]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch das Aktivieren oder Deaktivieren eines USB-Ports ausgelöst wird.
trap_pwr [Sende Trap nach Unterbrechung oder Herstellung der Stromversorgung]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch die Unterbrechung oder Herstellung einer der beiden Stromversorgungen des UTN-Servers ausgelöst wird (nur myUTN-800).
trap_sdinout [Sende Trap nach dem Verbinden oder Trennen einer SD-Karte]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch das Anschließen oder Entfernen einer SD-Karte am UTN-Server ausgelöst wird (nur myUTN-800).
trap_sdunusable [Sende Trap, falls die SD-Karte nicht nutzbar ist]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch eine unnutzbare SD-Karte ausgelöst wird (nur myUTN-800).
trap_lnk [Sende Trap nach Unterbrechung oder Herstellung der Netzwerk-verbindung]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch die Unterbrechung oder Herstellung einer der beiden Netzwerkverbindungen des UTN-Servers ausgelöst wird (nur myUTN-800).

Parameter	Wertekonvention	Default	Beschreibung
mailto_1 mailto_2 [E-Mail Adresse]	gültige E-Mail Adresse [max. 64 Zeichen]	[blank]	Definiert die E-Mail-Adresse des Empfängers für Benachrichtigungen.
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-Ports]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch das Aktivieren oder Deaktivieren eines USB-Ports ausgelöst wird.
noti_pwr_1 noti_pwr_2 [Sende E-Mail nach Unterbrechung oder Herstellung der Stromversorgung]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch die Unterbrechung oder Herstellung einer der beiden Stromversorgungen des UTN-Servers ausgelöst wird (nur myUTN-800).
noti_sdinout_1 noti_sdinout_2 [Sende E-Mail nach dem Verbinden oder Trennen einer SD-Karte]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch das Anschließen oder Entfernen einer SD-Karte am UTN-Server ausgelöst wird (nur myUTN-800).
noti_sdunusable_1 noti_sdunusable_2 [Sende E-Mail, falls die SD-Karte nicht nutzbar ist]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch eine unnutzbare SD-Karte ausgelöst wird (nur myUTN-800).
noti_lnk_1 noti_lnk_2 [Sende E-Mail nach Unterbrechung oder Herstellung der Netzwerk-verbindung]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch die Unterbrechung oder Herstellung einer der beiden Netzwerkverbindungen des UTN-Servers ausgelöst wird (nur myUTN-800).

Parameter	Wertekonvention	Default	Beschreibung
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 34: Parameterliste - Anzeigefeld (nur myUTN-800)

Parameter	Wertekonvention	Default	Beschreibung
dis_def [Kennung (Anzeigefeld)]	1–2 Zeichen [A–Z, 0–9; E+Zahl nicht möglich, weil diese Kombination für Fehlercodes ⇨🗎112 verwendet wird.]	SD	Definiert die Kennung, welche im Anzeigefeld an der Vorderseite des UTN-Servers dargestellt wird.
dis_pwr [Fehler anzeigen, wenn nur eine Stromversorgung Strom liefert]	on/off	on	De-/aktiviert das Anzeigen einer Fehlermeldung im Anzeigefeld, falls der UTN-Server nur über einen der beiden Anschlüsse mit Strom versorgt wird. *Die Fehler werden codiert dargestellt; siehe:* ⇨🗎112.
disp_sdc [SD-Kartenfehler anzeigen]	on/off	on	De-/aktiviert das Anzeigen einer Fehlermeldung im Anzeigefeld, falls die SD-Karte im UTN-Server fehlt oder nicht verwendbar ist. *Die Fehler werden codiert dargestellt; siehe:* ⇨🗎112.
disp_lnk [Fehler anzeigen, wenn nur eine Netzwerk-verbindung aktiv ist]	on/off	on	De-/aktiviert das Anzeigen einer Fehlermeldung im Anzeigefeld, falls der UTN-Server nur über einen der beiden Anschlüsse mit dem Netzwerk verbunden ist. *Die Fehler werden codiert dargestellt; siehe:* ⇨🗎112.

Tabelle 35: Parameterliste -Signalton (nur myUTN-800)

Parameter	Wertekonvention	Default	Beschreibung
beepPwr [Nur eine Stromversorgung liefert Strom]	on/off	off	De-/aktiviert den akustischen Signalton für den Fall, dass der UTN-Server nur über einen der beiden Anschlüsse mit Strom versorgt wird.
beepSDc [SD-Karten-Fehler]	on/off	off	De-/aktiviert den akustischen Signalton für den Fall, dass die SD-Karte im UTN-Server fehlt oder nicht verwendbar ist.
beepLnk [Nur eine Netzwerkverbindung ist aktiv]	on/off	off	De-/aktiviert den akustischen Signalton für den Fall, dass der UTN-Server nur über einen der beiden Anschlüsse mit dem Netzwerk verbunden ist.

Tabelle 36: Parameterliste - SD-Karte (nur myUTN-800)

Parameter	Wertekonvention	Default	Beschreibung
autoSync [Parameter-Backup]	on/off	on	De-/aktiviert das automatische Sichern der Parameter auf eine angeschlossene SD-Karte.

Tabelle 37: Parameterliste -WLAN (nur myUTN-55)

Parameter	Wertekonvention	Default	Beschreibung
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_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.*
wifi_channel [Kanal]	1–14 [1–2 Zeichen; 0–9; länderspezifisch]	3	Definiert den Kanal (Frequenzbereich), auf dem gesendet wird. *Treten Interferenzen auf, sollte der Kanal gewechselt werden.* **Warnung** **Informieren Sie sich über die nationalen Bestimmungen für den Einsatz von WLAN-Produkten und verwenden Sie nur zugelassene Kanäle.**
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.

Parameter	Wertekonvention	Default	Beschreibung
wifi_keyid [WEP-Schlüssel verwenden]	0–4 [1 Zeichen; 0–4]	0	Definiert den anzuwendenden WEP-Schlüssel. 0 = kein Schlüssel 1 = Schlüssel 1 2 = Schlüssel 2 3 = Schlüssel 3 4 = Schlüssel 4
wifi_wkey1 ~ wifi_wkey4 [Schlüssel 1-4]	Abhängig vom gewählten Schlüsseltyp. Zeichenanzahl: 64 ASCII = 5 64 HEX = 10 128 ASCII = 13 128 HEX = 26 Zeichenvorrat: *bei HEX = 0–9, a–f, A–F* *bei ASCII = 0–9, a–z, A–Z*	[blank]	Definiert die WEP-Schlüssel. Vier WEP-Schlüssel sind möglich.
wifi_psk [PSK]	8–63 Zeichen	[blank]	Definiert den Pre Shared Key (PSK) für Wi-Fi Protected Access (WPA).
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.*
wifi_dbmroam [Roaming-Level]	0–100 [1–3 Zeichen; 0–9]	0	Definiert den Schwellenwert für Roaming in -dBm. Wird der Schwellenwert überschritten, sucht der UTN-Server nach einem stärkeren WLAN-Signal und wechselt gegebenenfalls in ein anderes WLAN-Netzwerk mit besserer Signalstärke.

8.3 Informationen im Anzeigefeld (nur myUTN-800)

Der Dongleserver myUTN-800 verfügt über ein Anzeigefeld an der Vorderseite. Es werden Statusinformationen (Fehlerzustände) zur Verfügung gestellt.

Text	Beschreibung	Problembehandlung
DS (Kennung ⇨🗎36)	Der Dongleserver ist betriebsbereit.	-
RS	Der Dongleserver startet neu.	-
DL	Firmware/Software wird auf den Dongleserver geladen. Anschließend wird ein Update durchgeführt.	-
E1	Eine der beiden Stromversorgungen ist ausgefallen. Welcher Anschluss betroffen ist, zeigt der leuchtende Punkt (linker Punkt, linke Stromversorgung; rechter Punkt, rechte Stromversorgung).	Überprüfen Sie die Kabelverbindungen und Spannungsquelle.
E2	Die SD-Karte ist in einem nicht unterstützten Dateisystem formatiert bzw. ist nicht lesbar und nicht beschreibbar.	Formatieren Sie die SD-Karte im Dateiformat FAT32, FAT16 oder FAT12. Überprüfen Sie, ob die SD-Karte fehlerfrei arbeitet.
E3	Die SD-Karte ist lesbar aber nicht beschreibbar.	Entfernen Sie den Schreibschutz der SD-Karte.
E4	Es ist keine SD-Karte im SD-Card-Reader vorhanden.	Führen Sie eine SD-Karte in den SD-Card-Reader ein: - Typ: SD oder SDHC - Dateiformat: FAT32, FAT16 oder FAT12
E5	Eine oder beide Netzwerkverbindungen sind getrennt.	Überprüfen Sie die Kabelverbindungen und Ihr Netzwerk.

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 mit administrativen Rechten oder Mitglieder der Gruppe 'utnusers'
  - –Benutzer ohne administrative Rechte oder ohne Zugehörigkeit zur Gruppe 'utnusers'
    - +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 Tabelle gibt einen Überblick, Tabelle 38 ⇨🗎114.

Hinweis

Die Tabelle zeigt 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 38: SEH UTN Manager - Funktionsübersicht Linux

	Globale Auswahlliste		Benutzerindividuelle Auswahlliste		
	Adminrechte/ 'utn users'	User	Adminrechte/ 'utn users'	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	✓	✓	✓	✓	✓
Port – Aktivieren	✓	✓	✓	✓	✓
Port – Deaktivieren	✓	✓	✓	✓	✓
Port – Anfordern	✓	✓	✓	✓	✓
Port – Entfernen	✓	×	✓	×	×
Port – Einstellungen	✓	✓	✓	✓	✓
Schaltflächen					
Auswahlliste – Aktualisieren	✓	✓	✓	✓	✓
Auswahlliste – Bearbeiten	✓	×	✓	✓	×
Port – Aktivieren	✓	✓	✓	✓	×
Port – Deaktivieren	✓	✓	✓	✓	✓
Dialog 'Programm – Optionen'					
Netzwerksuche – Multicastsuche	✓	×	✓	×	×
Netzwerksuche – Netzwerkbereichsuche	✓	×	✓	×	×
Programm – Programmmeldungen	✓	×	✓	×	×
Programm – Programm-Update	✓	×	✓	×	×
Automatismen – Auto-Disconnect	✓	×	✓	×	×
Auswahlliste – Auswahllisten-Modus	✓	×	✓	×	×
Auswahlliste – Automatische Aktualisierung	✓	×	✓	×	×
Dialog 'Porteinstellungen'					
Automatische Geräteverbindung – Auto-Connect	✓	×	✓	×	×
Meldungen	✓	✓	✓	✓	✓

✓ = aktiv
× = inaktiv (ausgegraut)

r = read only (schreibgeschützt)
rw = read and write (Lesen und Schreiben)
INI = *.ini-Datei (⇨ 52)

8.5 Problembehandlung

Dieses Kapitel stellt einige Problemursachen und erste Lösungshilfen dar.

Problem-darstellung

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

Warnung

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

Wenden Sie sich in diesem Fall an den Support der SEH Computertechnik GmbH; siehe: 'Support und Service' ⇨🗎5.

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' ⇨🗎113.

☐ Eine Funktion wird nicht vom angeschlossenen USB-Gerät unterstützt.

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

Im SEH UTN Manager werden USB-Geräte nicht angezeigt

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

Mögliche Ursache

- ☐ Der SEH UTN Manager und die Firmware/Software auf dem UTN-Server sind inkompatibel. Aktualisieren Sie den SEH UTN Manager (⇨ 🗎18) und die Firmware/Software (⇨ 🗎86).
- ☐ Am UTN-Server sind mehrere Compound-USB-Geräte (⇨ 🗎91) angeschlossen. Jedes darin eingebaute USB-Gerät belegt einen virtuellen USB-Port des UTN-Servers. Die Anzahl dieser virtuellen USB-Ports ist abhängig vom UTN-Server-Modell begrenzt. Wird sie überschritten, können keine weiteren USB-Geräte am UTN-Server verwendet werden (⇨ 🗎47).
- ☐ Der USB-Port ist abgeschaltet (⇨ 🗎38).

Im SEH UTN Manager werden mehrere USB-Geräte an einem USB-Port angezeigt

Mögliche Ursache

- ☐ Bei dem angeschlossenen USB-Gerät handelt es sich um ein sogenanntes Compound-USB-Gerät. Es besteht aus einem Hub und einem oder mehreren USB-Geräten, die alle in einem einzigen Gehäuse eingebaut sind. Wenn die Verbindung zum Port hergestellt wird, werden alle dargestellten USB-Geräte mit dem Client des Benutzers verbunden und können genutzt werden.

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: ⇨ 🗎37.

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 ⇨ 🗎27.
- ☐ Die Kommunikation wird durch eine Sicherheitssoftware (Firewall) blockiert.

Die Verbindung zum USB-Port kann nicht hergestellt werden

Mögliche Ursache

- ☐ Die Zugriffskontrolle für USB-Geräte ist aktiviert ⇨ 🗎63.
- ☐ Auf dem Client ist keine Treibersoftware für das USB-Gerät installiert.
- ☐ Der USB-Port 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 ⇨🗎7 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 ⇨🗎60.
- ☐ Der Zugang ist via SSL/TLS (HTTPS) geschützt und Sie haben das Zertifikat (CA/selbstsigniert/PKCS#12) gelöscht. Setzen Sie die Parameterwerte des UTN-Servers auf die Standardwerte zurück, um Zugriff zu erhalten ⇨🗎84. Dabei gehen sämtliche Einstellungen verloren.
- ☐ Die TCP-Portzugriffskontrolle ist aktiviert ⇨🗎62.
- ☐ Die Cipher Suites der Verschlüsselungsstufe werden vom Browser nicht unterstützt ⇨🗎58.

Passwort und/oder Benutzername ist nicht mehr verfügbar

Der Zugriff auf das myUTN Control Center kann geschützt werden. Ist das Passwort und/oder der Benutzername nicht mehr verfügbar, können die Parameterwerte des UTN-Servers auf die Standardwerte zurückgesetzt werden, um Zugriff zu erhalten ⇨🗎84. 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-Ports und den daran angeschlossenen USB-Geräten.

Verwendung

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

Alternativ wird ein Skript für den USB-Port 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 ⇨🗎14).

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

Was möchten Sie tun?

- ☐ 'Konsole verwenden' ⇨🗎118
- ☐ 'Skript erstellen' ⇨🗎119

Konsole verwenden

Voraussetzung

- ✓ Der SEH UTN Manager ist auf dem Client installiert; siehe: ⇨🗎13.
- ✓ IP-Adresse oder Hostname eines UTN-Servers ist bekannt.

1. Öffnen Sie die Konsole **Terminal**.
2. Geben Sie die Befehlsfolge ein; siehe 'Syntax und Befehle' ⇨🗎119.
3. Bestätigen Sie die Eingabe.

↳ Die Befehlsfolge wird ausgeführt.

Skript erstellen

Voraussetzung

- ✓ Der SEH UTN Manager ist auf dem Client installiert; siehe: ⇨🗎13.
- ✓ IP-Adresse oder Hostname eines UTN-Servers ist bekannt.

1. Öffnen Sie einen Texteditor.
2. Geben Sie die Befehlsfolge ein; siehe 'Syntax und Befehle' ⇨🗎119.
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.

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

Hinweis

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

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 Portnummer`
	Aktiviert die Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät.
	• `deactivate UTN-Server Portnummer`
	Deaktiviert die Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät. Ist ein USB-Massenspeichergerät an den USB-Port angeschlossen, wird der Befehlsstring 'eject' verwendet. Bei allen anderen USB-Geräten wird der Befehlsstring 'plugout' verwendet.
	• `plugin UTN-Server Portnummer`
	Aktiviert die Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät.
	• `plugout UTN-Server Portnummer`
	Deaktiviert die Verbindung zu einem USB-Port und dem daran angeschlossenen USB-Gerät. (Entspricht dem 'Abziehen' des Gerätes.)
	***Hinweis:** Der Befehlsstring 'deactivate' ist zu bevorzugen.*
	• `eject UTN-Server Portnummer`
	(Für USB-Massenspeichergeräte) Wirft das am USB-Port angeschlossene USB-Gerät aus. Die Geräteverbindung wird erst deaktiviert, wenn die Kommunikation ordnungsgemäß beendet ist.
	***Hinweis:** Der Befehlsstring 'deactivate' ist zu bevorzugen.*
	• `set autoconnect = true|false UTN-Server Portnummer`
	Aktiviert die Portverbindung automatisch, sofern das USB-Gerät an den USB-Port angeschlossen aber nicht belegt ist.
	• `find`
	Sucht alle UTN-Server im Netzwerksegment und zeigt die gefundenen UTN-Server mit IP-Adresse, MAC Adresse, Modell und Softwareversion an.
	• `getlist UTN-Server`
	Zeigt eine Übersicht der an den UTN-Server angeschlossenen USB-Geräte (inkl. Portnummer, Vendor-ID, Produkt-ID, Herstellername, Produktname, Geräteklasse und Status).
	• `state UTN-Server Portnummer`
	Zeigt den Status des am USB-Port angeschlossenen USB-Gerätes.

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

Befehl	Beschreibung
`-k` USB-Portschlüssel *oder* `--key` USB-Portschlüssel	Spezifiziert einen USB-Portschlüssel. *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 (⇨🗎63). Um das USB-Gerät verfügbar zu machen, muss der korrekte Schlüssel eingegeben werden.* **Hinweis:** Über den Befehl wird der Schlüssels nicht konfiguriert. Die Eingabe des Schlüssels ermöglicht den Zugriff auf das USB-Gerät und muss bei jeder Aktivierung der Verbindung erfolgen.
`-mr` *oder* `--machine readable`	Trennt die Ausgabe des Befehlsstrings 'getlist' durch Tabulatoren und die von 'find' durch Kommas.
`-nw` *oder* `--no-warnings`	Unterdrückt Warnmeldungen.
`-o` *oder* `--output`	Zeigt die Ausgabe in der Kommandozeile an.
`-p` Portnummer *oder* `--port` Portnummer	Verwendet einen alternativen UTN-Port. *Der Client und UTN-Server kommunizieren über den UTN-Port. Wurde die UTN-Portnummer geändert (⇨🗎37), verwenden Sie diesen Befehl.*
`-q` *oder* `--quiet`	Unterdrückt die Ausgabe.
`-sp` Portnummer *oder* `--ssl-port` Portnummer	Verwendet einen alternativen UTN-Port mit SSL-Verschlüsselung. *Bei einer verschlüsselten Verbindung kommunizieren der Client und der UTN-Server über den UTN-SSL-Port. Wurde die UTN-SSL-Portnummer geändert (⇨🗎37), verwenden Sie diesen Befehl.*
`-t` Sekunden *oder* `timeout` Sekunden	Spezifiziert ein Timeout für die Befehlsstrings 'activate', 'deactivate', 'plugin', 'plugout' und 'eject'.
`-v` *oder* `--version`	Zeigt die Versionsnummer von utnm an.

Für die Befehle gilt:

- UTN-Server = IP-Adresse oder Hostname eines UTN-Servers
- 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	Der USB-Port und das daran angeschlossene USB-Gerät können verwendet werden.
20	Die Verbindung zum USB-Port und dem daran angeschlossenen USB-Gerät konnte nicht aktiviert werden.
21	Die Verbindung zum USB-Port und dem daran angeschlossenen USB-Gerät konnte nicht deaktiviert werden.
22	Das am USB-Port angeschlossene USB-Gerät konnte nicht ausgeworfen werden.
23	Die Verbindung zum USB-Port und dem daran angeschlossenen USB-Gerät ist bereits aktiviert.
24	Die Verbindung zum USB-Port und dem daran angeschlossenen USB-Gerät wurde bereits deaktiviert.
25	Der USB-Port und das daran angeschlossene USB-Gerät sind mit einem anderen Benutzer verbunden.
26	Das am USB-Port angeschlossene USB-Gerät ist nicht erreichbar.
27	Unbekannter USB-Gerätestatus.
100	Unbekannter Befehl.
101	Der UTN-Server wurde nicht gefunden. Entweder existiert 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:

```
utnm -c "activate UTN-Server Portnummer"
```

Ergibt:

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

8.7 Abbildungsverzeichnis

8.8 Index