SEH

USB Device Server

myUTN-50 / myUTN-52 / myUTN-54

Benutzerdokumentation

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

Dokument:
Typ: Benutzerdokumentation
Titel: USB Device Server
Version: 1.2

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

Inhaltsverzeichnis

1 Allgemeine Information

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

Welche Information benötigen Sie?

1.1 myUTN

Verwendungszweck

myUTN (myUSB to Network) erlaubt das Bereitstellen von nicht-netzwerkfähigen USB-Geräten (z.B. Festplatten, Drucker, usw.) für mehrere Netzwerkteilnehmer. Dazu werden die USB-Geräte an den USB-Port des UTN Server angeschlossen. 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 am Netzwerk eingebundenen USB-Geräte an und stellt die Verbindung zwischen Client und USB-Gerät her.

Systemvoraussetzungen

myUTN ist konzipiert für den Einsatz in TCP/IP basierenden Netzwerken. Der SEH UTN Manager ist für den Einsatz in Windows Systeme (XP und höher) konzipiert.

Ablauf und Funktionsweise

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

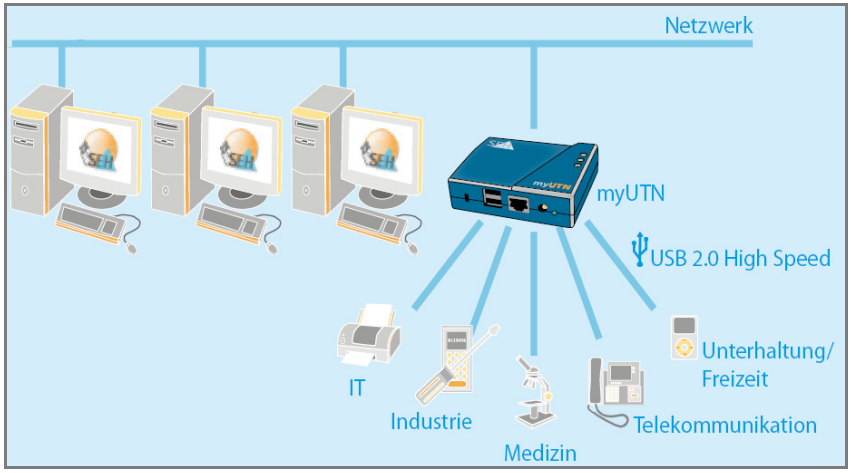


Abb. 1: UTN Server im Netzwerk

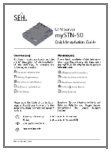
1.2 Dokumentation

Aufbau der Dokumentation

Die myUTN Dokumentation besteht aus den folgenden Dokumenten:

PDF

Benutzerdokumentation
Detaillierte Beschreibung der myUTN Konfiguration und Administration.



Print PDF

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

HTML

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

HTML

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

Merkmale dieses Dokumentes

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

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

Fachbegriffe in diesem Dokument

In diesem Dokument sind Erläuterungen von Fachbegriffen in einem Glossar zusammengefasst. Das Glossar bietet einen schnellen Überblick über technische Zusammenhänge und Hintergrundinformationen; siehe: ⇨ 82.

Symbole und Auszeichnungen

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

Tabelle 1: Konventionen in der Dokumentation

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

1.3 Support und Service

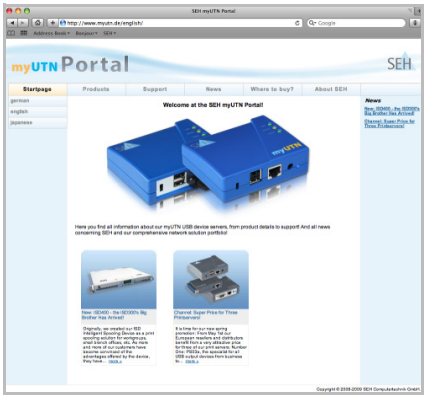
Support

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

	Montag - Donnerstag Freitag	8:00 - 17:45 Uhr und 8:00 - 16:15 Uhr (CET)
	+49 (0)521 94226-44	
	support@seh.de	

Aktuelle Services

Folgende Services finden Sie auf der Internetseite www.myutn.net.



- aktuelle Firmware
- aktuelle Tools
- aktuelle Dokumentationen
- aktuelle Produktinfomationen
- Produktdatenblätter
- FAQ Informationen
- u.v.m.

1.4 Ihre Sicherheit

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

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

Bestimmungsgemäße Verwendung

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

Bestimmungswidrige Verwendung

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

Sicherheitshinweise

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

Warnhinweise

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

Dies ist ein Warnhinweis!

1.5 Erste Schritte

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

Gehen Sie wie folgt vor:

1. *Lesen und beachten Sie die Sicherheitsinformationen um Schaden an Personen und Gerät zu vermeiden; siehe:* ⇨ 10.
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:* ⇨ 12.
4. *Installieren und starten Sie das Software Tool 'SEH UTN Manager' auf Ihren Windows Client; siehe:* ⇨ 19.
5. *Fügen Sie der Auswahlliste die Geräte hinzu, die Sie nutzen möchten; siehe:* ⇨ 46.
6. *Aktivieren Sie die Verbindung zwischen Client und USB-Gerät; siehe:* ⇨ 49.

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?

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

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

Nachdem der UTN Server eine IP-Adresse automatisch über ein Bootprotokoll erhalten hat, können Sie nachträglich manuell eine freidefinierbare IP-Adresse im UTN Server speichern. Die zugewiesene IP-Adresse des UTN Servers kann über die Software Tools 'SEH UTN Manager' und 'InterCon-NetTool' ermittelt und verändert werden; siehe: ⇨🗎16.

Nachfolgend sind die verschiedenen Methoden zur IP-Adressenvergabe beschrieben.

Automatische Methoden zur IP-Adressenvergabe

- 'ZeroConf' ⇨🗎13
- 'BOOTP' ⇨🗎13
- 'DHCP' ⇨🗎13
- 'Autokonfiguration (IPv6 Standard)' ⇨🗎14

Manuelle Methoden zur IP-Adressenvergabe

- 'InterCon-NetTool' ⇨🗎14
- 'SEH UTN Manager' ⇨🗎14
- 'myUTN Control Center' ⇨🗎15
- 'ARP/PING' ⇨🗎15

ZeroConf

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

Zur Namensauflösung der IP-Adresse kann der Domain Name Service von Bonjour verwendet werden; siehe: ⇨📄36.

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: ⇨📄29.

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 Server dynamisch vergeben werden kann.

Voraussetzung

☑ Der Parameter 'DHCP' ist aktiviert; siehe: ⇨📄29.

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 in der RA verschickten Präfix.

Voraussetzung

☑ Der Parameter 'IPv6' ist aktiviert.

☑ Der Parameter 'Automatische Konfiguration' ist aktiviert.

Um die Vergabe von IPv6-Adressen zu konfigurieren; siehe: ⇨ 32.

InterCon-NetTool

Der IP-Assistent des InterCon-NetTools hilft bei der Konfiguration von TCP/IP Parametern, wie z.B. der IP-Adresse. Über den IP-Assistent kann die gewünschte IPv4-Adresse manuell eingeben und im UTN Server gespeichert werden. Um eine IPv4-Adresse via InterCon-NetTool zu konfigurieren; siehe: ⇨ 31.

SEH UTN Manager

Über den SEH UTN Manager kann die gewünschte IPv4-Adresse manuell eingeben und im UTN Server gespeichert werden. Um eine IPv4-Adresse via SEH UTN Manager zu konfigurieren; siehe: ⇨ 30.

myUTN Control Center

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

- Um eine **IPv4**-Adresse via myUTN Control Center zu konfigurieren; siehe: ⇨🗎30.
- Um eine **IPv6**-Adresse via myUTN Control Center zu konfigurieren; siehe: ⇨🗎32.

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 Server. 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: ⇨🗎29.

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 mit den 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' ⇨ 17
- 'Administration via SEH UTN Manager' ⇨ 19
- 'Administration via InterCon-NetTool' ⇨ 26
- 'Administration via Statustaster am Gerät' ⇨ 28

2.1 Administration via myUTN Control Center

Welche Funktionen werden unterstützt?

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

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

Voraussetzung

☑ Der UTN Server ist am Netzwerk und Netzspannung angeschlossen.

☑ Der UTN Server hat eine gültige IP-Adresse.

myUTN Control Center starten

Gehen Sie wie folgt vor:

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

Die **myUTN Control Center - Startseite** erscheint.

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

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

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

Abb. 2: myUTN Control Center - START

Aufbau des myUTN Control Centers

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

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

Über den Punkt **Produkt & Unternehmen** werden die Kontaktdaten des Herstellers sowie weiterführende Informationen zum Produkt angezeigt. Über den Punkt **Sitemap** erhalten Sie eine Übersicht und direkten Zugriff über 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 Center 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 am Netzwerk eingebundenen UTN Server mitsamt USB-Geräten an und stellt die Verbindung zwischen Client und USB-Gerät her. Die Software wird auf alle Clients installiert, die auf ein im Netzwerk bereitgestelltes USB-Gerät zugreifen sollen.

Funktionsweise

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

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

Automatismen

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

- **Autostart**: Der SEH UTN Manager startet sofort, wenn der Rechner des Anwenders gestartet wird.
- **Auto-Connect**: Zwischen USB-Gerät und Client wird, nach Programmstart des SEH UTN Manager, automatisch eine Verbindung hergestellt.
- **Application**: Zwischen USB-Gerät und Client wird, nach Programmstart einer freidefinierbaren Applikation, automatisch eine Verbindung hergestellt.
- **Print-on-Demand**: Zwischen USB-Gerät (Drucker oder MFG) und Client wird, sobald ein Druckauftrag anliegt, automatisch eine Verbindung hergestellt. Nach Beendigung des Druckauftrages wird die Verbindung automatisch deaktiviert.

Programmaufbau

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

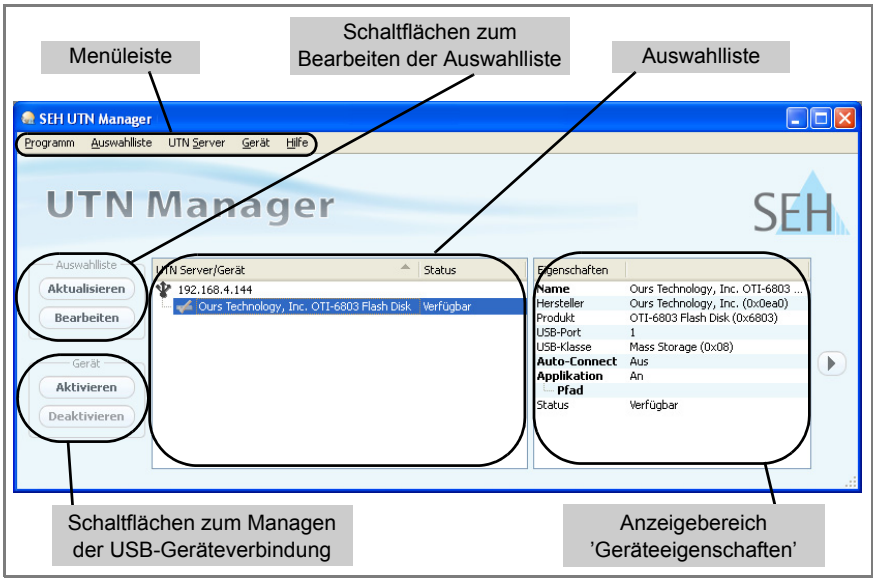


Abb. 3: SEH UTN Manager - Hauptdialog

Welche Funktionen werden unterstützt?

Über den SEH UTN Manager können Sie u.a.

- 'USB-Geräte der Auswahlliste hinzufügen' ⇨ 46
- 'USB-Gerät mit Client verbinden' ⇨ 49
- 'USB-Gerät und Client trennen' ⇨ 50
- 'Automatische Geräteverbindungen konfigurieren' ⇨ 51
- 'UTN Servern eine IPv4-Adresse zuweisen' ⇨ 30
- 'myUTN Control Center starten' ⇨ 17
- 'Zugriff auf USB-Geräte kontrollieren' ⇨ 56

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

SEH UTN Manager Varianten

Der SEH UTN Manager ist in zwei Varianten verfügbar:

- **Single-User Variante** (SEH UTN Manager)
- **Multi-User Variante** (SEH UTN Manager + SEH UTN Service)

Wesentlicher Unterschied zwischen der Single-User und der Multi-User Variante ist der Windows-Dienst 'utnservice'. Der Dienst 'utnservice' agiert im Hintergrund und ist nach Systemstart automatisch aktiv. Der Dienst kann über die üblichen Windows-Administrationsmethoden gesteuert werden.

Der UTN Service erlaubt bis zu vier Teilnehmern (Clients) den zeitgleichen Zugriff auf die am UTN Server angeschlossenen USB-Geräte.

Wodurch unterscheiden sich die Varianten?

Die Vorteile der Multi-User Variante liegen im Mehrbenutzerbetrieb sowie der Differenzierung von Benutzergruppen.

Im Mehrbenutzerbetrieb

- kann auf einem Windows Client jedes Benutzerkonto Zugriff auf den SEH UTN Manager erhalten. Dabei bleiben für jeden Benutzer die individuellen Einstellungen im SEH UTN Manager erhalten.
- können Windows Clients via Remote individuellen Zugriff auf den auf einem Server installierten SEH UTN Manager erhalten.

Die Multi-User Variante unterscheidet zwischen den folgenden Benutzergruppen:

- Benutzer *mit* administrativen Rechten (Windows Admin)
- Benutzer *ohne* administrativen Rechten (Windows User)

Die Differenzierung von Benutzergruppen ermöglicht die Funktion **Gerätezugriffskontrolle**, mit der der Zugriff der Benutzergruppe 'Windows User' auf die angeschlossenen USB-Geräte kontrolliert werden kann.

Nachteil der Multi-User Variante ist die fehlende Unterstützung der Funktion **Application** sowie die Einschränkung der Funktion **Print-On-Demand**, auf die Benutzergruppe 'Windows Admin'.

Tabelle 2: SEH UTN Manager: Funktionsunterschiede im Überblick

Funktion	Variante Single-User	Variante Multi-User
Mehrbenutzerbetrieb		x
Unterscheidung von Benutzergruppen		x
Gerätezugriffskontrolle		x
Application	x	
Print-On-Demand	x	x*

**Ausschließlich für die Windows Benutzergruppe 'Admin' funktional*

Rechteverteilung bei der Multi-User Variante

Die Multi-User Variante differenziert die beiden Windows Benutzergruppen 'Admin' und 'User'. Den Gruppen werden verschiedene Rechte bei der Verwendung des SEH UTN Managers eingeräumt. Die Tabelle gibt einen Überblick.

Tabelle 3: SEH UTN Manager - Multi-User Variante: Rechteverteilung

Funktion	Admin	User
Programm: Sprache ändern	x	x
Programm: Update	x	
Programm: Autostart	x	
Benachrichtigung: Gerät	x	abh. von der Einstellung durch den Admin
Benachrichtigung: Programm	x	
Netzwerkscan: Parameter defnieren	x	
Auswahlliste: Bearbeiten	x	
Auswahlliste: Automatisches Aktualisieren	x	
Auswahlliste: Ansicht ändern	x	x
Gerätezugriffskontrolle	x	
Geräteverbindung: Aktivieren / Deaktivieren	x	abh. von der Einstellung durch den Admin
Geräteverbindung: Automatismus: Auto-Connect	x	abh. von der Einstellung durch den Admin
Geräteverbindung: Automatismus: Application	variantenbedingt nicht verfügbar	variantenbedingt nicht verfügbar
Geräteverbindung: Automatismus: Print-On-Demand	x	variantenbedingt nicht verfügbar

SEH UTN Manager installieren

Um mit dem SEH UTN Manager zu arbeiten, muss das Programm auf einem Rechner mit einem Windows Betriebssystem installiert werden. Sie finden die SEH UTN Manager Installationsdatei auf der myUTN Product CD oder im Internet unter www.myutn.net.

Die selbstausführende Datei 'sehutnmanager.exe' enthält beide Varianten des SEH UTN Managers. Die bevorzugte Variante kann über die Installationsroutine ausgewählt werden.

Systemvoraussetzung

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

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

Gehen Sie wie folgt vor:

1. *Starten Sie die SEH UTN Manager Installationsdatei.*
2. *Wählen Sie die gewünschte Sprache.*
3. *Folgen Sie der Installationsroutine.*

Der SEH UTN Manager wird auf dem System installiert.

Beim Einsatz in virtuellen Umgebungen (z.B. mit VM Ware) können dem Windows System benötigte Treiber fehlen. Die Installationsroutine überprüft während des Installationsvorgang die vorhandenen Treiber. Bei fehlenden Treibern, startet ein weiterer Installer (USB driver for SEH UTN Manager). Dieser leitet die Installation der benötigten Treiber ein.

Variantenwechsel

Ist auf Ihrem System eine Variante des SEH UTN Manager installiert und Sie möchten auf eine andere Variante umsteigen, wird empfohlen, 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.

SEH UTN Manager starten

Single-User Variante

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

Multi-User Variante

Die Multi-User Variante (SEH UTN Manager + Service) läuft automatisch nach Systemstart als Windows-Dienst im Hintergrund. Um die SEH UTN Manager Programmoberfläche anzuzeigen, doppelklicken Sie auf das Symbol  .

In einigen Fällen verlangt die Windows 'Benutzerkontensteuerung' eine Bestätigung, wenn die Multi-User Variante als Administrator ausgeführt werden soll; siehe: ⇨ 98.

UTN Server/USB-Geräte der Auswahlliste hinzufügen

Die beim Netzwerkscan gefundenen UTN Server werden in der 'Netzwerkliste' angezeigt. Um einen UTN Server zu konfigurieren oder um USB-Geräte mit dem Client zu verbinden, muss der UTN Server der 'Auswahlliste' zugeordnet werden; siehe: ⇨ 46.

Bei der Multi-User Variante (SEH UTN Manager + Service) dürfen Benutzer ohne administrative Rechte die Auswahlliste nicht bearbeiten. Ein Windows Admin muss die Auswahlliste zusammenstellen, damit Benutzer Zugriff auf USB-Geräte erhalten.

2.3 Administration via InterCon-NetTool

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

Funktionsweise

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

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

Installation

Um mit dem InterCon-NetTool zu arbeiten, muss das Programm auf einem Rechner mit einem Windows Betriebssystem installiert werden. Sie finden die InterCon-NetTool Installationsdatei auf der myUTN Product CD oder im Internet unter www.myutn.net.

Gehen Sie wie folgt vor:

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

Das InterCon-NetTool wird auf dem System installiert.

Programmstart

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

Die InterCon-NetTool Einstellungen werden in der Datei 'NetTool.ini' gespeichert. Diese ist im Verzeichnis 'Dokumente und Einstellungen' unter dem jeweiligen Benutzernamen abgelegt.

Aufbau des InterCon-NetTools

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

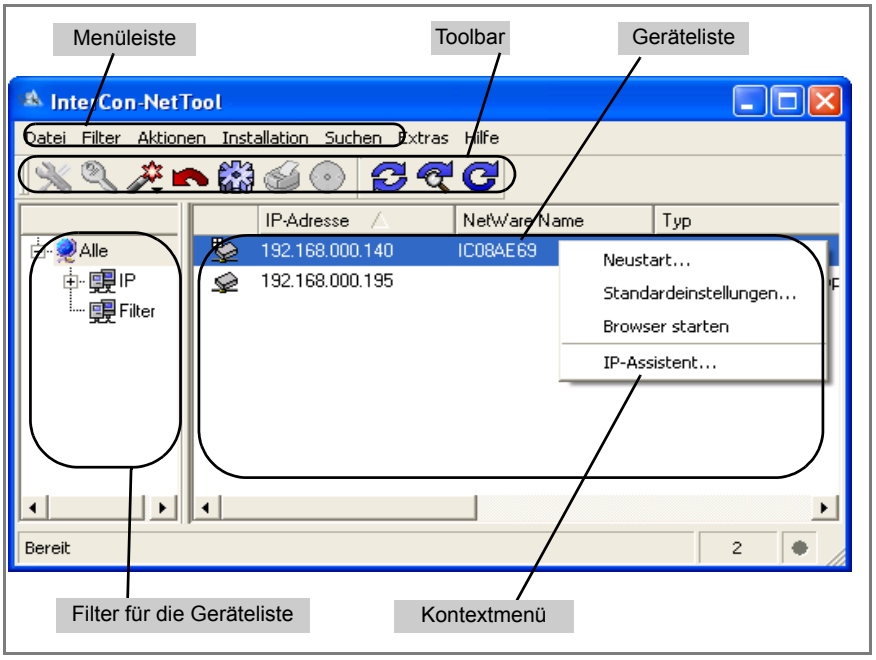


Abb. 4: InterCon-NetTool - Hauptdialog

Welche Funktionen werden unterstützt?

Über das InterCon-NetTool können Sie

- dem UTN Server eine IPv4-Adresse zuweisen ⇨🗎29
- den UTN Server neu starten ⇨🗎80
- die Parameterwerte des UTN Servers auf die Standardeinstellung zurücksetzen ⇨🗎77
- das myUTN Control Center starten ⇨🗎17
- vom BIOS Modus in den Standardmodus wechseln ⇨🗎96

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

2.4 Administration via Statustaster am Gerät

An dem UTN Server finden Sie Netzwerkanschlüsse, LEDs, den Statustaster und einen Stromanschluss. Eine Beschreibung dieser Komponenten finden Sie im 'Quick Installation Guide'.

Über den Statustaster können Sie die Parameterwerte des UTN Servers auf die Standardeinstellung zurücksetzen; siehe: ⇨77.

3 Netzwerk- und Geräteeinstellungen

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: ⇨ 12.

Was möchten Sie tun?

IPv4 Parameter via myUTN Control Center konfigurieren

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - IPv4**.
3. *Konfigurieren Sie die IPv4 Parameter; siehe: Tabelle 4* ⇨ 30.
4. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert.

Tabelle 4: IPv4 Parameter

Parameter	Beschreibung
DHCP BOOTP ARP/PING	Aktiviert bzw. deaktiviert 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' ⇨ 12.) 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	IP-Adresse des Gateway

IPv4 Parameter via SEH UTN Manager konfigurieren

Voraussetzung

☑ Der SEH UTN Manager ist auf dem Client installiert; siehe: ⇨ 19.

☑ Der UTN Server ist der Auswahlliste beigefügt; siehe: ⇨ 46.

Gehen Sie wie folgt vor:

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

Die Einstellungen werden gespeichert.

IPv4 Parameter via InterCon-NetTool konfigurieren

Voraussetzung

☑ Das InterCon-NetTool ist auf dem Client installiert; siehe: ⇨ 26.

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

☑ Der Router im Netzwerk leitet Multicast-Anfragen weiter.

Gehen Sie wie folgt vor:

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

Die Einstellungen werden gespeichert.

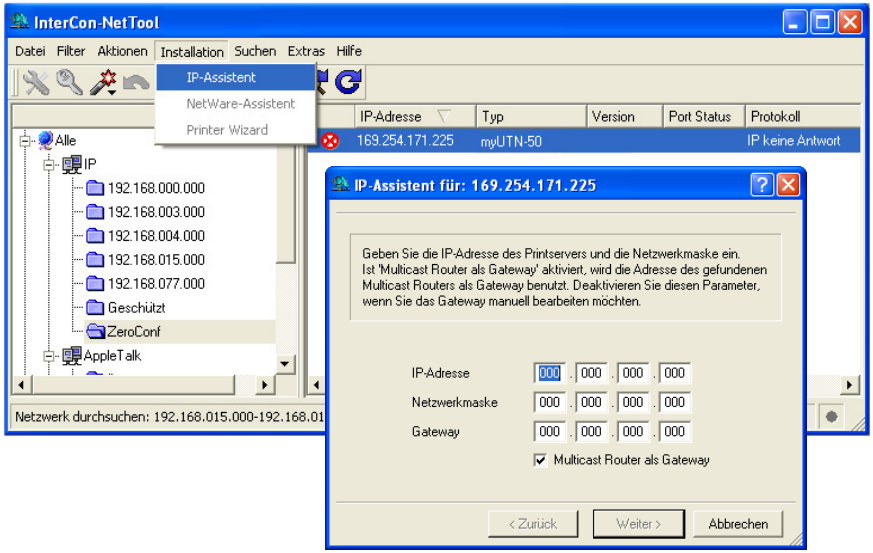


Abb. 5: InterCon-NetTool - IP Assistent

3.2 Wie konfiguriere ich IPv6 Parameter?

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

Welche Vorteile bietet IPv6?

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

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

Wie wird eine IPv6-Adresse dargestellt?

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

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

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

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

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

Die URL wird ausschließlich von IPv6-fähigen Browsern akzeptiert.

Welche IPv6-Adress Typen gibt es?

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

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

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - IPv6**.
3. *Konfigurieren Sie die IPv6 Parameter; siehe: Tabelle 5* ⇨ 34.
4. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert.

Tabelle 5: 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.
Präfix Länge	Definiert die Länge des Subnetz-Präfix für die IPv6-Adresse. (Der Wert 64 ist voreingestellt.) *Adressbereiche werden durch Präfixe angegeben. Dazu wird die Präfixlänge (Anzahl der verwendeten Bits) als Dezimalzahl mit vorangehendem '/' an die IPv6-Adresse angehängt dargestellt.*

3.3 Wie konfiguriere ich den DNS?

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

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

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - DNS**.
3. *Konfigurieren Sie die DNS Parameter; siehe: Tabelle 6* ⇨ 35.
4. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert.

Tabelle 6: DNS Parameter

Parameter	Beschreibung
DNS	De-/aktiviert den DNS.
Erster DNS-Server	IP-Adresse des ersten DNS-Servers (z.B. 192.168.0.21)
Zweiter DNS-Server	IP-Adresse des zweiten DNS-Servers. (Der zweite DNS-Server wird benutzt, wenn der erste nicht verfügbar ist.)
Domain-Name (Suffix)	Domain-Name eines vorhandenen DNS-Servers (z.B. company.de)

3.4 Wie konfiguriere ich SNMP?

SNMP (Simple Network Management Protocol) hat sich zum Standard-Protokoll für die Verwaltung und Überwachung von Netzelementen entwickelt. Das Protokoll regelt die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation.

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

SNMPv1

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

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

SNMPv3

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

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - SNMP**.
3. *Konfigurieren Sie die SNMP Parameter; siehe: Tabelle 7* ⇨ 36.
4. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert.

Tabelle 7: SNMP Parameter

Parameter	Beschreibung
SNMPv1	De-/aktiviert die SNMPv1 Funktionalität.
Nur Lesen	De-/aktiviert den Schreibschutz für die Community.
Community	Name der SNMP-Community. Die SNMP Community stellt eine einfache Form des Zugriffsschutzes dar, in der mehrere Teilnehmer mit gleichen Zugriffsrechten zusammengefasst werden.
SNMPv3	De-/aktiviert die SNMPv3 Funktionalität.
Benutzername	Definiert den Namen des SNMP-Benutzers.
Passwort	Definiert das Passwort des SNMP-Benutzers.
Hash	Definiert den Hash Algorithmus.
Zugriffsrechte	Definiert die Zugriffsrechte des SNMP-Benutzers.
Verschlüsselung	Definiert die Verschlüsselungsmethode.

3.5 Wie konfiguriere ich Bonjour?

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

Der UTN Server nutzt die folgenden Bonjour Funktionalitäten:

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

Bei der Überprüfung der über ZeroConf zugewiesenen IP-Adresse (siehe: 'ZeroConf' ⇨13) richtet der UTN Server eine Anfrage an das Netzwerk. Ist die IP-Adresse im Netzwerk schon belegt, erhält der UTN Server eine entsprechende Antwort. Der UTN Server startet dann eine weitere Anfrage mit einer anderen IP-Adresse. Ist die IP-Adresse noch frei, speichert der UTN Server diese.

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

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

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - Bonjour**.
3. *Konfigurieren Sie die Bonjour Parameter; siehe: Tabelle 8* ⇨*37*.
4. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert.

Tabelle 8: 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 Defaultname verwendet (Gerätename@ICxxxxxx).

3.6 Wie konfiguriere ich WLAN? (Nur myUTN-54)

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

Was ist WLAN?

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

Zur Umsetzung der Funkttechnologie verfügt die myUTN-54 über zusätzliche Parameter ⇨📄41. Die aktuellen WLAN-Einstellungen können im myUTN Control Center unter dem Menüpunkt **NETZWERK - WLAN** eingesehen werden.

Verbindungsstatus

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

UTN Server im WLAN

UTN Server im drahtgebundenen Netzwerk

WLAN Sicherheit

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

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

WEP

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

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

WPA/WPA2

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

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

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

Authentifizierung

Über ein Authentifizierungsverfahren können Sie die Identität eines Gerätes/Benutzers überprüfen, bevor diese(s)/r Zugang zu Ressourcen im Netzwerk hat. Der UTN Server bietet verschiedene Varianten des EAP (Extensible Authentication Protocol) als Authentifizierungsverfahren an. Für weitere Informationen; siehe: 'Wie verwende ich Authentifizierungsmethoden?' ⇨ 65.

Was möchten Sie tun?

- ☐ 'UTN Server (myUTN-54) im WLAN betreiben' ⇨ 40
- ☐ 'UTN Server mit drahtgebundenen Netzwerk verbinden' ⇨ 42

UTN Server (myUTN-54) im WLAN betreiben

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

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

Voraussetzung

☑ Der UTN Server ist am Netzwerk und Netzspannung angeschlossen.

☑ Der UTN Server ist mit einer IP-Adresse im drahtgebundenen Netzwerk bekannt; siehe: ⇨ 12.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - WLAN**.
   In der Netzwerkübersicht werden die verfügbaren WLANs angezeigt. Entscheiden Sie, in welchem WLAN der UTN Server betrieben werden soll.
3. *Konfigurieren Sie die WLAN Parameter so, dass diese mit den Parametern des zu verwendenden WLANs übereinstimmen; siehe: Tabelle 9* ⇨ 41.
4. *Aktivieren Sie die Option* **WLAN**, *um das WLAN Modul im UTN Server zu aktivieren.*
5. *Bestätigen Sie mit* **Speichern**.
   Die Einstellungen werden gespeichert.
6. *Entfernen Sie das Netzwerkkabel (RJ-45) vom UTN Server.*
   Die Verbindung zum drahtgebundenen Netzwerk wird getrennt.

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

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

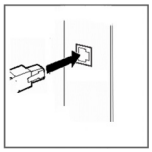
Tabelle 9: WLAN Parameter

Parameter	Beschreibung
Modus (Kommunikationsmodus)	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)	Als SSID (Service Set Identifier) oder auch Netzwerkname wird eine Funk-Netzwerk-Kennung bezeichnet. Jedes Wireless LAN besitzt eine konfigurierbare SSID, um das Funknetz eindeutig identifizieren zu können. Die SSID wird in der Basisstation eines Wireless LAN konfiguriert. Jedes Gerät (PC, UTN Server, usw.), das Zugriff zum Funknetz haben soll, muss mit der selben SSID konfiguriert werden.
Kanal (Frequenzbereich)	WLAN nutzt 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. Im UTN Server stehen die Kanäle1 bis 14 zur Verfügung. Der Kanal 3 ist voreingestellt. Der Parameter 'Kanal' ist nur im 'Ad-Hoc' Modus konfigurierbar. Nebeneinander liegende Kanäle überschneiden sich und es kann zu Interferenzen kommen. Wenn in einem kleinen Umkreis mehrere WLANs betrieben werden, dann sollten zwischen jeweils zwei benutzen Kanälen ein Abstand von mindestens 5 Kanälen liegen. ***Informieren Sie sich über die nationalen Bestimmungen für den Einsatz von WLAN-Produkten und verwenden Sie nur zugelassene Kanäle.***
Roaming	Roaming bezeichnet das 'Wandern' von einer Funkzelle zur nächsten. Der UTN Server verwendet dann den Access Point, der das bessere Signal liefert. Wird der UTN Server in den Einflussbereich eines anderen Access Points bewegt, wechselt er automatisch und ohne Verbindungsabbruch in die nächste Funkzelle. Der Parameter 'Roaming' ist nur im 'Infrastructure' Modus konfigurierbar.
Roaming Level	Die Sendeleistung des UTN Servers kann über den Parameter 'Roaming Level' definiert werden. Der Wert 65 -dbm ist voreingestellt. Der Parameter 'Roaming Level' ist nur im 'Infrastructure' Modus konfigurierbar.

Parameter	Beschreibung
Verschlüsselungsmethode	siehe: 'WLAN Sicherheit' ⇨ 38
Authentifizierungsmethode	siehe: 'Authentifizierung' ⇨ 39

UTN Server mit drahtgebundenen Netzwerk verbinden

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



3.7 Wie lege ich eine Beschreibung fest?

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

Gehen Sie wie folgt vor:

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

Die Daten werden gespeichert.

Um angeschlossenen USB-Geräten einen Namen zuzuweisen; siehe: ⇨ 48.

3.8 Wie konfiguriere ich die Gerätezeit?

Sie haben die Möglichkeit, die Gerätezeit des UTN Server 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 länderspezifische Eigenheiten, wie z.B Sommerzeit, können über den Parameter 'Zeitzone' ausgeglichen werden.

Voraussetzung

☑ Im Netzwerk ist ein Time-Server integriert.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - Datum/Zeit**.
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 auf dem Gerät DNS aktiviert ist und ein DNS-Server eingetragen wurde.)
5. *Wählen Sie aus der Liste* **Zeitzone** *das Kürzel für Ihre lokale Zeitzone.*
6. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert.

3.9 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: ⇨ 72.

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 ⇨ 35.

Gehen Sie wie folgt vor:

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

↳ Die Einstellungen werden gespeichert.

4 Angeschlossene USB-Geräte

Ziel des UTN Servers ist die Bereitstellung von Verbindung zwischen angeschlossenen USB-Geräten und autorisierten Clients. In diesem Kapitel erfahren Sie, wie Verbindungen aktiviert bzw. deaktiviert werden.

Welche Information benötigen Sie?

- 'Wie füge ich USB-Geräte der Auswahlliste hinzu?' ⇨ 46
- 'Wie erhalte ich Informationen zum USB-Gerät?' ⇨ 47
- 'Wie weise ich einem USB-Gerät einen Namen zu?' ⇨ 48
- 'Wie verbinde ich ein USB-Gerät mit dem Client?' ⇨ 49
- 'Wie trenne ich die Verbindung zwischen USB-Gerät und Client?' ⇨ 50
- 'Wie konfiguriere ich automatische Verbindungen?' ⇨ 51

Weitere relevante Themen aus anderen Kapiteln:

- 'Wie kontrolliere ich den Zugriff auf USB-Geräte?' ⇨ 56

4.1 Wie füge ich USB-Geräte der Auswahlliste hinzu?

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 ist auf dem Client installiert; siehe: ⇨ 19.

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

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager.*
2. *Wählen Sie im Menü* **Auswahlliste** *den Befehl* **Bearbeiten**. *Der Dialog* **Auswahlliste bearbeiten** *erscheint.*
3. *Markieren Sie den UTN Server in der Netzwerkliste.*
4. *Wählen Sie die Schaltfläche* **Hinzufügen** *an.*
5. *Wählen Sie die Schaltfläche* **OK** *an.*

Der UTN Server wird in der Auswahlliste angezeigt.

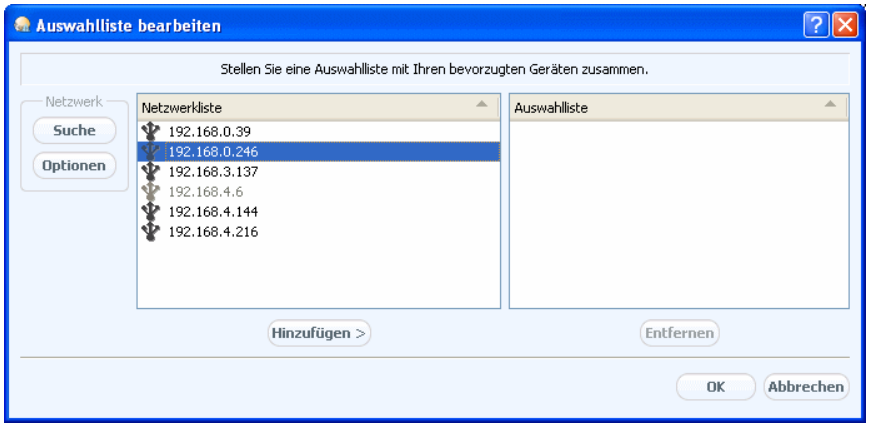


Abb. 6: SEH UTN Manager - Auswahlliste bearbeiten

4.2 Wie erhalte ich Informationen zum USB-Gerät?

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

Was möchten Sie tun?

- ☐ 'Statusinformationen via SEH UTN Manager anzeigen' ⇨📄47
- ☐ 'Statusinformationen via myUTN Control Center anzeigen' ⇨📄47
- ☐ 'Benachrichtigung konfigurieren' ⇨📄48

Statusinformationen via SEH UTN Manager anzeigen

Voraussetzung

- ☑ Der SEH UTN Manager ist auf dem Client installiert; siehe: ⇨📄19.
- ☑ Das USB-Gerät wird in der Auswahlliste angezeigt; siehe: ⇨📄46.

Gehen Sie wie folgt vor:

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

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

Statusinformationen via myUTN Control Center anzeigen

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **START**.

↳ Die Statusinformationen werden in der Liste **Angeschlossene Geräte** angezeigt.

Benachrichtigung konfigurieren

Voraussetzung

☑ Der SEH UTN Manager ist auf dem Client installiert; siehe: ⇨ 19.

☑ Das USB-Gerät wird in der Auswahlliste angezeigt; siehe: ⇨ 46.

Gehen Sie wie folgt vor:

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

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

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

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

Voraussetzung

☑ Der SEH UTN Manager ist auf dem Client installiert; siehe: ⇨ 19.

☑ Das USB-Gerät wird in der Auswahlliste angezeigt; siehe: ⇨ 46.

Gehen Sie wie folgt vor:

1. *Starten Sie den SEH UTN Manager.*
2. *Markieren Sie das USB-Gerät in der Auswahlliste.*
3. *Wählen Sie im Menü* **Gerät** *den Befehl* **Einstellungen**.
4. *Geben Sie im Feld* **Name** *die bevorzugte Bezeichnung ein.*
5. *Wählen Sie die Schaltfläche* **OK** *an.*

↳ Die Einstellung wird gespeichert.

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

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

Voraussetzung

- ☑ Der SEH UTN Manager ist auf dem Client installiert; siehe: ⇨ 19.
- ☑ Das USB-Gerät 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.
- ☑ Das USB-Gerät ist nicht mit einem anderen Client verbunden.

Gehen Sie wie folgt vor:

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

↳ Die Verbindung wird hergestellt.

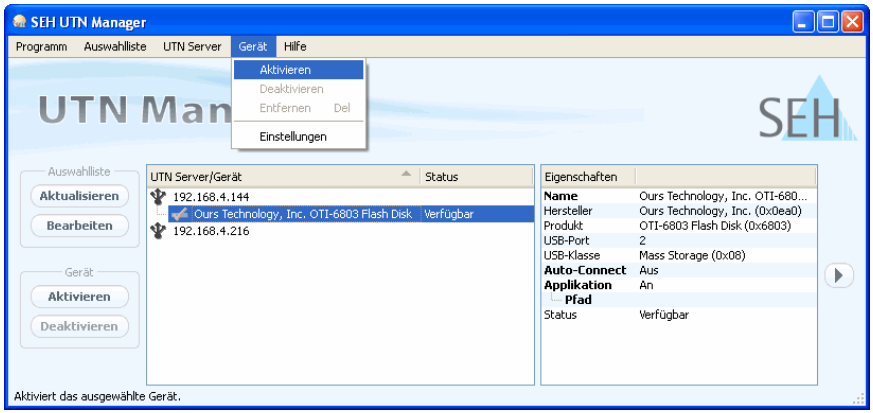


Abb. 7: SEH UTN Manager - Gerät aktivieren

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

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

Üblicherweise trennt der Anwender die Verbindung via SEH UTN Manager. Zudem hat der Administrator die Möglichkeit über das myUTN Control Center die Verbindung zu trennen.

Was möchten Sie tun?

☐ 'Geräteverbindung via SEH UTN Manager trennen' ⇨ 50

☐ 'Geräteverbindung via UTN Control Center trennen' ⇨ 50

Geräteverbindung via SEH UTN Manager trennen

Gehen Sie wie folgt vor:

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

Die Verbindung wird getrennt.

Geräteverbindung via UTN Control Center trennen

Gehen Sie wie folgt vor:

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

Die Verbindung wird getrennt.

4.6 Wie konfiguriere ich automatische Verbindungen?

Beim Auftreten bestimmter Ereignisse kann eine Verbindung zwischen Client und USB-Gerät automatisch initiiert werden. Hierzu stehen die folgenden Automatismen zur Verfügung.

- **Auto-Connect**: Zwischen USB-Gerät und Client wird, nach Programmstart des SEH UTN Manager, automatisch eine Verbindung hergestellt.
- **Application**: Zwischen USB-Gerät und Client wird, nach Programmstart einer freidefinierbaren Applikation, automatisch eine Verbindung hergestellt.
- **Print-on-Demand**: Zwischen USB-Gerät (Drucker oder MFG) und Client wird, sobald ein Druckauftrag anliegt, automatisch eine Verbindung hergestellt. Nach Beendigung des Druckauftrages wird die Verbindung automatisch deaktiviert.

Die Funktion 'Print-on-Demand' ist bei der Multi-User Variante des SEH UTN Manager ausschließlich für die Windows Benutzergruppe 'Admin' verfügbar. Die Funktion 'Application' ist ausschließlich über die Single-User Variante des SEH UTN Manager verfügbar.
Für weitere Information; siehe: 'SEH UTN Manager Varianten' ⇨🗎21.

Voraussetzung

☑ Der SEH UTN Manager ist auf dem Client installiert; siehe: ⇨🗎19.

☑ Das USB-Gerät wird in der Auswahlliste angezeigt; siehe: ⇨🗎46.

Gehen Sie wie folgt vor:

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

↳ Die Einstellung wird gespeichert.

5 Sicherheit

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

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

Welche Information benötigen Sie?

- 'Wie kontrolliere ich den Zugang zum myUTN Control Center?' ⇨ 52
- 'Wie kontrolliere ich den Zugriff zum UTN Server?' ⇨ 54
- 'Wie kontrolliere ich den Zugriff auf USB-Geräte?' ⇨ 56
- 'Wie setze ich Zertifikate korrekt ein?' ⇨ 58
- 'Wie verwende ich Authentifizierungsmethoden?' ⇨ 65
- 'Wie verschlüssele ich die Datenübertragung?' ⇨ 72

5.1 Wie kontrolliere ich den Zugang zum myUTN Control Center?

Sie haben die Möglichkeit, den administrativen Zugang zum myUTN Control Center über ein Passwort oder durch die Wahl des erlaubten Verbindungstypen zu schützen.

Verbindungstyp (HTTP/HTTPs)

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

Wird ausschließlich HTTPs als Verbindungstyp gewählt, ist der administrative Zugang zum myUTN Control Center via SSL geschützt.

Bei SSL wird ein Zertifikat benötigt, um die Identität des UTN Servers zu überprüfen. Bei einem so genannten 'Handshake' fragt der Client via Browser nach einem Zertifikat. URLs, die eine SSL-Verbindung erfordern, beginnen mit 'https'.

Passwort

Sie haben die Möglichkeit, das myUTN Control Center über ein Passwort vor unberechtigten Zugriff zu schützen. Ist ein Passwort gesetzt, findet vor dem Öffnen des myUTN Control Centers eine Passwortabfrage statt.

Zusätzlich kann das myUTN Control Center über das SNMP Sicherheitskonzept geschützt werden. Das Konzept beinhaltet das Verwalten von Benutzergruppen und Zugriffsrechten. Für weitere Informationen, siehe: 'Wie konfiguriere ich SNMP?' ⇨ 35.

Was möchten Sie tun?

- ☐ 'Verbindungstypen definieren' ⇨ 53
- ☐ 'Passwort definieren' ⇨ 53

Verbindungstypen definieren

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Webzugriff**.
3. *Aktivieren Sie die Option* **HTTP/HTTPs** *bzw.* **Nur HTTPs**.
4. *Bestätigen Sie mit* **Speichern**.

Die Einstellung wird gespeichert.

Passwort definieren

Gehen Sie wie folgt vor:

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

Die Einstellung wird gespeichert.

5.2 Wie kontrolliere ich den Zugriff zum UTN Server?

Portzugriffskontrolle

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

Sicherheitsstufen

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

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

Ausnahmen

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

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

Testmodus

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

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

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Portzugriff**.
3. *Aktivieren Sie die Option* **Portzugriff kontollieren**.
4. *Wählen Sie im Bereich* **Sicherheitstufe** *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**.
   Die Einstellungen werden gespeichert.
   Die Portzugriffskontrolle ist bis zum Geräte-Neustart aktiv.
8. *Überprüfen Sie den Portzugriff und die Konfigurationsfähigkeit des UTN Servers.*

Kann der UTN Server über das myUTN Control Center nicht mehr erreicht werden, initiieren Sie einen Geräte-Neustart; siehe: ⇨ 80.

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

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

5.3 Wie kontrolliere ich den Zugriff auf USB-Geräte?

Sie haben die Möglichkeit, den Zugriff auf die am UTN Server angeschlossene USB-Geräte zu kontrollieren. Wird der Zugriff gesperrt, kann eine definierte Benutzergruppe keine Geräteverbindung zwischen Client und USB-Gerät aktivieren.

Die Funktion 'Gerätezugriffskontrolle' ist ausschließlich über die Multi-User Variante des SEH UTN Manager verfügbar. Für weitere Information; siehe: 'SEH UTN Manager Varianten' ⇨ 21.

Die Multi-User Variante übernimmt Einstellungen aus den Windows Benutzerkonten und ermöglicht so die Unterscheidung nach den folgenden Benutzergruppen.

- Benutzer *mit* administrativen Rechten (Windows Admin)
  Die Benutzergruppe 'Windows Admin' hat ein uneingeschränktes Zugriffsrecht auf die USB-Geräte.
- Benutzer *ohne* administrativen Rechten (Windows User)
  Der Benutzergruppe 'Windows User' kann der generelle Zugriff für die angeschlossenen USB-Geräte entzogen werden.

Neu angeschlossene (bzw. in der Auswahlliste neu angezeigte) USB-Geräte sind zunächst für alle Benutzer zugänglich.

Ein 'Windows Admin' kann den generellen Zugriff auf die angeschlossenes USB-Geräte für die Benutzergruppe 'Windows User' sperren. Anschließend können Ausnahmen generiert werden, bei denen der Benutzergruppe 'Windows User' das Zugriffsrecht für einzelne USB-Geräte wieder zugewiesen werden.

Voraussetzung

☑ Die Multi-User Variante des SEH UTN Manager ist auf dem Client installiert; siehe: ⇨ 29.

☑ Sie verfügen auf dem Windows Client über administrative Rechte.

Was möchten Sie tun?

☐ 'Zugriff auf alle USB-Geräte sperren/freigeben' ⇨ 57

☐ 'Zugriff auf einzelne USB-Geräte freigeben' ⇨ 57

Zugriff auf alle USB-Geräte sperren/freigeben

Der Benutzergruppe 'Windows User' kann der generelle Zugriff für die angeschlossenen USB-Geräte entzogen werden.

Gehen Sie wie folgt vor:

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* **Administration**.
4. *De-/aktivieren Sie die Option* **Zugriff auf alle USB-Geräte sperren**.
5. *Wählen Sie die Schaltfläche* **OK** *an.*

Der Zugriff auf alle angeschlossenen USB-Geräte wird für die Benutzergruppe 'Windows User' gesperrt/freigegeben.

Zugriff auf einzelne USB-Geräte freigeben

Einzelne USB-Geräte können von der generellen Sperrung ausgenommen werden. Die Benutzergruppe 'Windows User' hat dann Zugriff auf das freigegebene USB-Gerät.

Gehen Sie wie folgt vor:

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

Der Zugriff auf das USB-Geräte wird für die Benutzergruppe 'Windows User' freigegeben.

Die Freigaben und Sperrungen gelten ausschließlich für Benutzer, die den selben Client für den Zugang zum USB-Gerät verwenden.

5.4 Wie setze ich Zertifikate korrekt ein?

Der UTN Server verfügt über eine eigene Zertifikatsverwaltung. Diese 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' ⇨ 66.
- um den UTN Server/Client zu authentifizieren, wenn der administrative Zugang des myUTN Control Center via HTTPs (SSL) geschützt ist.

Wenn Sie Zertifikate verwenden, sollten Sie den administrativen Zugriff zum myUTN Control Center zusätzlich mit einem Passwort schützen, so dass kein Unbefugter das Zertifikat auf dem UTN Server löschen kann; siehe: ⇨ 52.

Welche Zertifikate gibt es?

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

- **Selbstsignierte Zertifikate** tragen eine digitale Unterschrift, die vom UTN Server erstellt wurde.
- **CA-Zertifikate** sind Zertifikate, die von einer Zertifizierungsstelle (Certification Authority - CA) signiert wurden.
- Die Echtheit eines CA-Zertifikates kann mit Hilfe eines **Wurzelzertifikates**, das von der Zertifizierungsstelle ausgegeben wird, überprüft werden. Dieses Wurzelzertifikat wird auf einem Authentifizierungsserver im Netzwerk hinterlegt.

- Bei Auslieferung ist im UTN Server ein Zertifikat gespeichert, das sog. **Defaultzertifikat**. Sie sollten das Defaultzertifikat zeitnah durch ein selbstsigniertes oder ein CA-Zertifikat ersetzen.

Im UTN Server können bis zu drei Zertifikate zeitgleich installiert sein.

- 1 Selbstsigniertes Zertifikat

- 1 CA-Zertifikat oder pkcs12 Zertifikat

- 1 Wurzelzertifikat

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

Ein pkcs12 Zertifikat kann nur installiert werden, wenn aktuell keine Zertifikatsanforderung generiert bzw. kein CA-Zertifikat installiert ist.

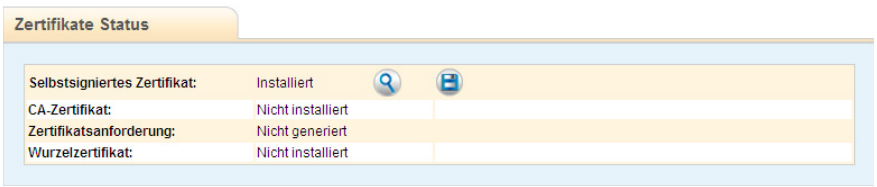


Abb. 8: myUTN Control Center - Zertifikate

Was möchten Sie tun?

- ☐ 'Zertifikat anzeigen' ⇨🗎60
- ☐ 'Selbstsigniertes Zertifikat erstellen' ⇨🗎60
- ☐ 'Zertifikatsanforderung für ein CA-Zertifikat erstellen' ⇨🗎61
- ☐ 'CA-Zertifikat auf dem UTN Server speichern' ⇨🗎62
- ☐ 'Wurzelzertifikat auf dem UTN Server speichern' ⇨🗎62
- ☐ 'pkcs12 Zertifikat auf dem UTN Server speichern' ⇨🗎63
- ☐ 'Zertifikat löschen' ⇨🗎64

Zertifikat anzeigen

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

Gehen Sie wie folgt vor:

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

Das Zertifikat wird angezeigt.

Selbstsigniertes Zertifikat erstellen

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

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Zertifikate**.
3. *Wählen Sie die Schaltfläche* **Selbstsigniertes Zertifikat** *an.*
4. *Geben Sie die entsprechenden Parameter ein; siehe: Tabelle 10* ⇨ *60.*
5. *Wählen Sie die Schaltfläche* **Erstellen/Installieren** *an.*

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

Tabelle 10: 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)

Parameter	Beschreibung
Organisation	gibt den Namen der Firma an, die den UTN Server einsetzt. Maximal 64 Zeichen können eingegeben werden.
Unternehmens-bereich	gibt die Abteilung oder eine Untergruppe der Firma an. Maximal 64 Zeichen können eingegeben werden. (Optionale Eingabe)
Ort	gibt den Ort an, an dem die Firma ansässig ist. Maximal 64 Zeichen können eingegeben werden.
Bundesland	gibt den Namen des Bundeslandes an, in dem die Firma ansässig ist. Maximal 64 Zeichen können eingegeben werden. (Optionale Eingabe)
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.

Zertifikatsanforderung für ein CA-Zertifikat erstellen

Für ein CA-Zertifikat wird im UTN Server eine Zertifikatsanforderung erstellt, die an die Zertifizierungsstelle gesendet werden muss. Die Zertifizierungsstelle erstellt anhand der Zertifikatsanforderung ein CA-Zertifikat. Das Zertifikat muss im 'Base 64' Format vorliegen.

Ist bereits eine Zertifikatsanforderung auf dem UTN Server erstellt worden, muss diese zunächst gelöscht werden; siehe: ⇨ 64.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Zertifikate**.
3. *Wählen Sie die Schaltfläche* **Zertifikatsanforderung** *an.*
4. *Geben Sie die benötigten Parameter ein; siehe: Tabelle 10 ⇨ 60.*

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. *Senden Sie die Textdatei als Zertifikatsanforderung an eine Zertifizierungsstelle.*

Nach Erhalt muss das CA-Zertifikat auf dem UTN Server gespeichert werden; siehe: ⇨62.

CA-Zertifikat auf dem UTN Server speichern

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

Voraussetzung

☑ Es wurde zuvor eine entsprechende Zertifikatsanforderung erstellt; siehe: ⇨61.

☑ Das Zertifikat muss im 'Base 64' Format vorliegen.

Gehen Sie wie folgt vor:

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

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

Wurzelzertifikat auf dem UTN Server speichern

Um in einem Netzwerk die Identität des UTN Servers zu überprüfen, bietet der UTN Server mehrere Authentifizierungsverfahren an. Wenn Sie das Authentifizierungsverfahren 'EAP-TLS' verwenden, ist es erforderlich, das Wurzelzertifikat des Authentifizierungsservers (RADIUS) auf den UTN Server zu installieren; siehe: ⇨66.

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

Voraussetzung

☑ Das Zertifikat muss im 'Base 64' Format vorliegen.

Gehen Sie wie folgt vor:

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

Das Wurzelzertifikat wird auf dem UTN Server gespeichert.

pkcs12 Zertifikat auf dem UTN Server speichern

Zertifikate im pkcs12 Format werden verwendet, um private Schlüssel mit dem zugehörigen Zertifikat passwortgeschützt zu speichern.

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

Voraussetzung

☑ Das Zertifikat muss im 'Base 64' Format vorliegen.

☑ Es darf keine Zertifikatsanforderung vorliegen. Um die Zertifikatsanforderung zu löschen; siehe: ⇨ 64.

☑ Es darf kein CA-Zertifikat installiert sein. Um ein CA-Zertifikat zu löschen; siehe: ⇨ 64.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Zertifikate**.
3. *Wählen Sie die Schaltfläche* **pkcs12 Zertifikat** *an.*
4. *Wählen Sie die Schaltfläche* **Durchsuchen** *an.*

5. *Geben Sie das pkcs12 Zertifikat an.*
6. *Geben Sie das Passwort ein.*
7. *Wählen Sie die Schaltfläche* **Installieren** *an.*

↳ Das pkcs12 Zertifikat wird auf dem UTN Server gespeichert.

Zertifikat löschen

Gehen Sie wie folgt vor:

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

5.5 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, etc. 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' ⇨🗎66
- ☐ 'EAP-TLS konfigurieren' ⇨🗎66
- ☐ 'EAP-TTLS konfigurieren' ⇨🗎68
- ☐ 'PEAP konfigurieren' ⇨🗎69
- ☐ 'EAP-FAST konfigurieren' ⇨🗎70

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 (Benutzernamen und Passwort) eingegeben.

Voraussetzung

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

Gehen Sie wie folgt vor:

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

↳ 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. Benutzerpasswörte sind nicht erforderlich.

Um eine EAP-TLS Authentifizierung anzuwenden, stellen Sie sicher, dass die aufgeführten Punkte in der angegebenen Reihenfolge erfüllt werden. Wird die Vorgehensweise nicht eingehalten, kann es vorkommen, dass der UTN Server im Netzwerk nicht angesprochen werden kann. Setzen Sie in diesem Fall die UTN Server Parameter zurück; siehe: ⇨ 76.

Vorgehensweise

- ☐ Erstellen Sie auf dem UTN Server eine Zertifikatsanforderung; siehe: ⇨ 61.
- ☐ Erstellen Sie mit der Zertifikatsanforderung und mit Hilfe des Authentifizierungsservers ein CA Zertifikat.
- ☐ Installieren Sie das CA-Zertifikat auf dem UTN Server; siehe: 'CA-Zertifikat auf dem UTN Server speichern' ⇨ 62.
- ☐ Installieren Sie das Wurzelzertifikat des Authentifizierungsservers auf dem UTN Server; siehe: 'Wurzelzertifikat auf dem UTN Server speichern' ⇨ 62.
- ☐ Aktivieren Sie das Authentifizierungsverfahren 'EAP-TLS' auf dem UTN Server.

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Authentifizierung**.
3. *Wählen Sie aus der Liste* **Authentifizierungsmethode** *den Eintrag* **TLS**.

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

↳ Die Einstellungen werden gespeichert.

EAP-TTLS konfigurieren

Nutzen und Zweck

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

Funktionsweise

EAP-TTLS besteht aus zwei Phasen:

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

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

Voraussetzung

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

Gehen Sie wie folgt vor:

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

5. *Wählen Sie die Einstellungen, mit denen die Kommunikation im TLS Tunnel gesichert werden soll.*
6. *Installieren Sie optional ein Wurzelzertifikat des RADIUS-Servers auf dem UTN Server, um die Sicherheit beim Verbindungsaufbau zu erhöhen.*
7. *Bestätigen Sie mit* **Speichern**.

↳ 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. ⇨🗎68) zunächst ein verschlüsselter TLS Tunnel (Transport Layer Security) zwischen UTN Server und RADIUS-Server aufgebaut. Dazu identifiziert sich nur der RADIUS-Server mit einem von einer CA unterschriebenen Zertifikat beim UTN Server.

Der TLS Tunnel wird anschließend benutzt, um eine weitere Verbindung aufzubauen, wobei diese mit zusätzlichen EAP-Authentifizierungsmethoden (z.B. MSCHAPv2) geschützt werden kann.

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

Voraussetzung

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

Gehen Sie wie folgt vor:

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

3. *Wählen Sie aus der Liste* **Authentifizierungsmethode** *den Eintrag* **PEAP**.
4. *Geben Sie Benutzername und Passwort ein, mit denen der UTN Server auf dem RADIUS-Server eingerichtet ist.*
5. *Wählen Sie die Einstellungen, mit denen die Kommunikation im TLS Tunnel gesichert werden soll.*
6. *Installieren Sie optional ein Wurzelzertifikat des RADIUS-Servers auf dem UTN Server, um die Sicherheit beim Verbindungsaufbau zu erhöhen.*
7. *Bestätigen Sie mit* **Speichern**.

↳ 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. ⇨🗎68) 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 Credential) verwendet. PACs sind Anmeldeinformationen, die bis zu drei Komponenten umfassen können:

- Ein gemeinsamer geheimer 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 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 PAC zu schützen.

Voraussetzung

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

Gehen Sie wie folgt vor:

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

Die Einstellungen werden gespeichert.

5.6 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.

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: ⇨ 44.

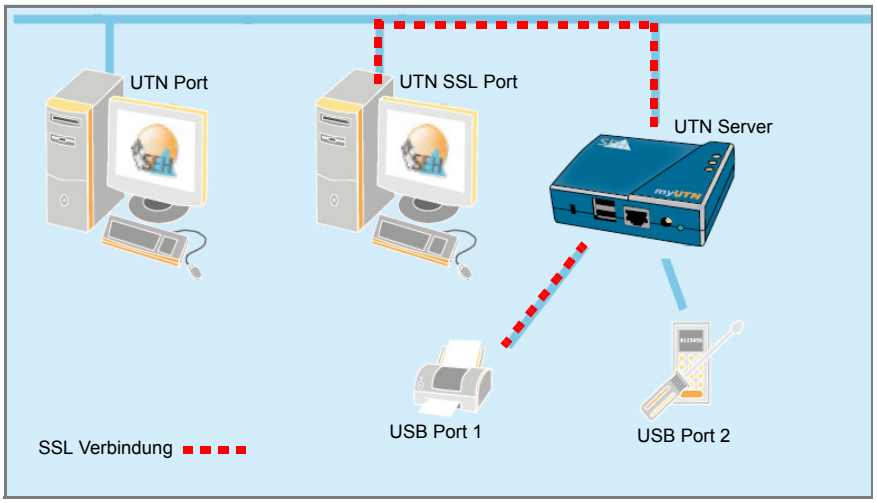


Abb. 9: UTN Server - SSL Verbindung im Netzwerk

Um eine SSL Verbindung zu verwenden, muss der Verschlüsselungsalgorithmus (RC4 oder AES256) ausgewählt und die Verschlüsselung am gewünschten USB Port aktiviert werden.

Gehen Sie wie folgt vor:

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

Die Daten zwischen den Clients und dem USB-Gerät werden, gemäß der ausgewählten Methode, verschlüsselt übermittelt.

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

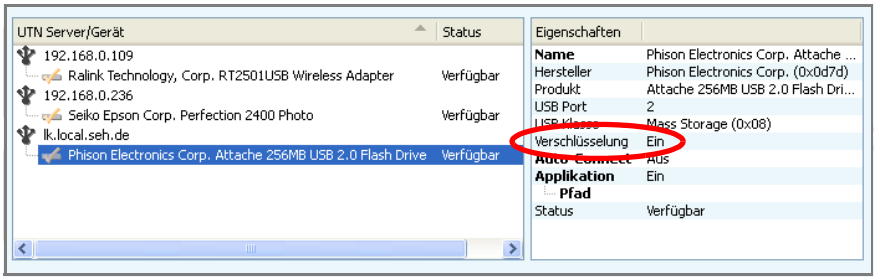


Abb. 10: SEH UTN Manager - Verschlüsselung

6 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)' ⇨ 74
- 'Wie setze ich die UTN Parameter auf die Standardwerte zurück?' ⇨ 76
- 'Wie führe ich ein Update aus?' ⇨ 79
- 'Wie starte ich den UTN Server neu?' ⇨ 80

6.1 Wie sichere ich die UTN Parameter? (Backup)

Alle Parameterwerte des UTN Servers (Ausnahme: Passwörter) sind in der Datei 'parameters' gespeichert.

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

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

Was möchten Sie tun?

- ☐ 'Parameterwerte anzeigen' ⇨ 75
- ☐ 'Parameterdatei sichern' ⇨ 75
- ☐ 'Parameterdatei auf den UTN Server laden' ⇨ 75

Parameterwerte anzeigen

Gehen Sie wie folgt vor:

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

Die aktuellen Parameterwerte werden angezeigt.

Detaillierte Beschreibungen zu den Parametern entnehmen Sie der 'Parameterliste' ⇨ 85.

Parameterdatei sichern

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - Parameter Backup**.
3. *Wählen Sie das Symbol* *an.*
   Die aktuellen Parameterwerte werden angezeigt.
4. *Speichern Sie die Datei 'parameters' mit Hilfe Ihres Browsers auf ein lokales System.*

Die Parameterdatei wird kopiert und ist gesichert.

Parameterdatei auf den UTN Server laden

Gehen Sie wie folgt vor:

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

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

6.2 Wie setze ich die UTN Parameter auf die Standardwerte zurück?

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

Durch das Zurücksetzen kann sich die IP-Adresse im UTN Server 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' ⇨ 76
- ☐ 'Parameter via InterCon-NetTool zurücksetzen' ⇨ 77
- ☐ 'Parameter via Statustaster zurücksetzen' ⇨ 77

Über den Statustaster am Gerät können die Parameter ohne eine Passworteingabe zurückgesetzt werden.

Parameter via myUTN Control Center zurücksetzen

Gehen Sie wie folgt vor:

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

Die Parameter werden zurückgesetzt.

Parameter via InterCon-NetTool zurücksetzen

Gehen Sie wie folgt vor:

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

Die Parameter werden zurückgesetzt.

Parameter via Statustaster zurücksetzen

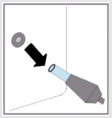
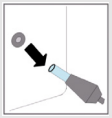
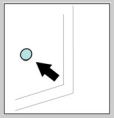
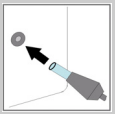
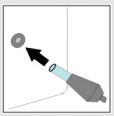
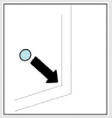
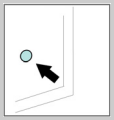
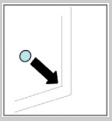
Am UTN Server finden Sie LEDs, den Statustaster sowie verschiedene Anschlüsse. Eine Beschreibung dieser Komponenten finden Sie im 'Quick Installation Guide'.

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

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

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

Nachfolgend ist der Ablauf aller Phasen visualisiert.

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

6.3 Wie führe ich ein Update aus?

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

Was passiert beim Update?

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

Wann ist ein Update sinnvoll?

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

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

Wo finde ich Update Dateien?

Aktuelle Firmware und Software Dateien können von der Internetseite www.myutn.net heruntergeladen werden.

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

Gehen Sie wie folgt vor:

1. *Starten Sie das myUTN Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - Update**.
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.

6.4 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' ⇨ 80
- ☐ 'UTN Server via InterCon-NetTool neu starten' ⇨ 80

UTN Server via myUTN Control Center neu starten

Gehen Sie wie folgt vor:

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

↳ Der UTN Server wird neu gestartet.

UTN Server via InterCon-NetTool neu starten

Gehen Sie wie folgt vor:

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

↳ Der UTN Server wird neu gestartet.

7 Anhang

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

Welche Information benötigen Sie?

7.1 Glossar

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

Welche Information benötigen Sie?

Herstellerspezifische Softwarelösungen

- 'myUTN Control Center' ⇨🗎82
- 'InterCon-NetTool' ⇨🗎82
- 'SEH UTN Manager' ⇨🗎82

Netzwerktechnologie

- 'Hardware-Adresse' ⇨🗎83
- 'IP-Adresse' ⇨🗎83
- 'Hostname' ⇨🗎84
- 'Gateway' ⇨🗎84
- 'Netzwerkmaske' ⇨🗎84
- 'Default Name' ⇨🗎84

myUTN Control Center

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

InterCon-NetTool

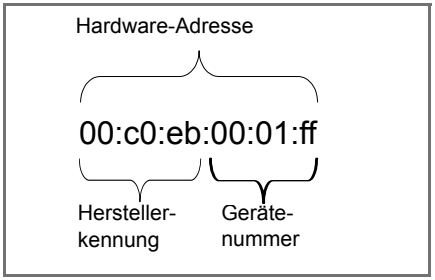
Das InterCon-NetTool ist eine von der SEH Computertechnik GmbH entwickelte Software zur Administration von SEH Netzwerkgeräten innerhalb eines zuvor definierten Netzwerkes.

SEH UTN Manager

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

Hardware-Adresse

Der UTN Server ist über seine weltweit eindeutige Hardware-Adresse adressierbar. Sie wird häufig auch als MAC- oder Ethernet-Adresse bezeichnet. Diese Adresse wird vom Hersteller in der Hardware des Gerätes festgelegt. Sie besteht aus zwölf hexadezimalen Ziffern. Die ersten sechs Ziffern kennzeichnen den Hersteller, die letzten sechs Ziffern identifiziert das individuelle Gerät.



Die Hardware-Adresse kann am Gehäuse, im SEH UTN Manager oder im InterCon-NetTool abgelesen werden.

Die Verwendung von Trennzeichen in der Hardwareadresse ist plattformabhängig. Beachten Sie bei Eingabe der Hardwareadresse die folgende Konvention.

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

IP-Adresse

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

Hostname

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

Gateway

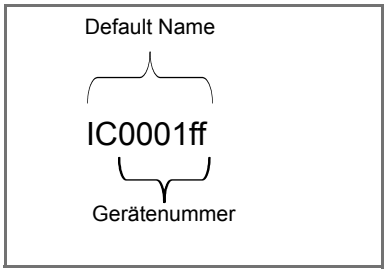
Über ein Gateway können IP-Adressen in einem anderen Netzwerk angesprochen werden. Möchten Sie ein Gateway verwenden, können Sie über das myUTN Control Center den entsprechenden Parameter im UTN Server konfigurieren.

Netzwerkmaske

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

Default Name

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



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

7.2 Parameterliste

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

Welche Information benötigen Sie?

Um die aktuellen Parameterwerte Ihres UTN Servers einzusehen; siehe: 'Parameterwerte anzeigen' ⇨ 75.

Tabelle 11: Parameterliste - IPv4

Parameter	Wertekonvention	Default	Beschreibung
ip_addr [IP-Adresse]	gültige IP-Adresse	169.254. 0.0/16	Definiert die IP-Adresse des UTN Server.
ip_mask [Netzwerkmaske]	gültige IP-Adresse	255.255. 0.0	Definiert die Netzwerkmaske des UTN Server.
ip_gate [Gateway]	gültige IP-Adresse	0.0.0.0	Definiert die Gateway-Adresse des UTN Server.
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 12: Parameterliste - IPv6

Parameter	Wertekonvention	Default	Beschreibung
ipv6 [IPv6]	on/off	on	De-/aktiviert die IPv6-Funktionalität des UTN Servers.
ipv6_addr [IPv6-Adresse]	n:n:n:n:n:n:n:n	: :	Definiert eine manuell vergebene IPv6 Unicast-Adresse im Format n:n:n:n:n:n:n:n für den UTN Server. *Jedes 'n' stellt den hexadezimalen Wert von einem der acht 16-Bit-Elemente der Adresse dar. Ein Block aus zusammenhängenden Nullen kann mit zwei aufeinander folgenden Doppelpunkten zusammengefasst werden.*
ipv6_gate [Router]	n:n:n:n:n:n:n:n	: :	Definiert die IPv6 Unicast-Adresse des Routers, an den der UTN Server seine 'Router Solicitations' (RS) sendet.

Parameter	Wertekonvention	Default	Beschreibung
ipv6_plen [Präfix Länge]	0 - 64 [2 Zeichen, 0-9]	64	Definiert die Länge des Subnetz-Präfix 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 13: 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 Hostnamen des UTN Servers.

Tabelle 14: Parameterliste - Webzugriff

Parameter	Wertekonvention	Default	Beschreibung
http_pwd [Passwort]	max. 64 Zeichen [a-z, A-Z, 0-9]	[blank]	Definiert das Passwort für den administrativen Zugang zum myUTN Control Center.
http_allowed [Zulässige Verbindung]	on/off	on	Definiert den zulässigen 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 geschützt.*

Tabelle 15: Parameterliste - Portzugriff

Parameter	Wertekonvention	Default	Beschreibung
protection [Portzugriff kontrollieren]	on/off	off	De-/aktiviert die Sperrung von ausgewählten Port.
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 Reboot des UTN Servers aktiv.*
protection_level [Sicherheitsstufe]	protec_utn protec_tcp protec_all	protec_ utn	Definiert die zu sperrenden Porttypen: - UTN Ports - TCP Ports - IP Ports (all)
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 16: Parameterliste - UTN Port

Parameter	Wertekonvention	Default	Beschreibung
utn_port [UTN Port]	max. 4 Zeichen [0-9]	9200	Definiert die Nummer des UTN Ports.
utn_sslport [UTN SSL Port]	max. 4 Zeichen [0-9]	9443	Definiert die Nummer des UTN SSL Ports.
utn_cipher [Verschlüsselungs-algorithmus]	RC4-MD5 AES 256	RC4-MD5	Definiert das SSL-Verschlüs-selungsverfahren bei der Datenübertragung zwischen den Clients und UTN Server.
utn_sec_1 ~ utn_sec_5 [USB Port]	on/off	off	De-/aktiviert die SSL-Ver-schlüsselung am USB Port. *Bei aktivierter Verschlüsselung werden die Daten zwischen den Clients und den (an den USB Ports angeschlossenen) USB-Geräten, gemäß der aus-gewählten Methode, ver-schlüsselt übermittelt.*

Tabelle 17: 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 18: Parameterliste - SNMP

Parameter	Wertekonvention	Default	Beschreibung
snmpv1 [SNMPv1]	on/off	on	De-/aktiviert die SNMPv1 Funktionalität.
snmpv1_ronly [Nur Lesen]	on/off	off	De-/aktiviert den Schreibschutz für die Community.
snmpv1_community [Community]	max. 64 Zeichen [a-z, A-Z, 0-9]	public	Definiert den Namen der SNMP-Community. *Die SNMP Community stellt eine einfache Form des Zugriffsschutzes dar, in der mehrere Teilnehmer mit gleichen Zugriffsrechten zusammengefasst werden.*
snmpv3 [SNMPv3]	on/off	on	De-/aktiviert die SNMPv3 Funktionalität.
any_name [Benutzername]	max. 64 Zeichen [a-z, A-Z, 0-9]	anonymous	Definiert den Namen der SNMP-Benutzergruppe 1.
any_pwd [Passwort]	max. 64 Zeichen [a-z, A-Z, 0-9]	[blank]	Definiert das Passwort der SNMP-Benutzergruppe 1.
any_rights [Zugriffsrechte]	--- [keine] readonly readwrite	readonly	Definiert die Zugriffsrechte der SNMP-Benutzergruppe 1.
any_hash [Hash]	md5 sha	md5	Definiert den HASH Algorithmus für die SNMP-Benutzergruppe 1.
any_cipher [Verschlüsselung]	--- [keine] aes des	---	Definiert die Verschlüsselungsmethode der SNMP-Benutzergruppe 1.
admin_name [Benutzername]	max. 64 Zeichen [a-z, A-Z, 0-9]	admin	Definiert den Namen der SNMP-Benutzergruppe 2.
admin_pwd [Passwort]	8 - 64 Zeichen [a-z, A-Z, 0-9]	administrator	Definiert das Passwort der SNMP-Benutzergruppe 2.
admin_rights [Zugriffsrechte]	--- [keine] readonly readwrite	readwrite	Definiert die Zugriffsrechte der SNMP-Benutzergruppe 2.
admin_hash [Hash]	md5 sha	md5	Definiert den HASH Algorithmus für die SNMP-Benutzergruppe 2.

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

Tabelle 19: Parameterliste - Datum/Zeit

Parameter	Wertekonvention	Default	Beschreibung
ntp [Datum/Zeit]	on/off	on	De-/aktiviert die Verwendung eines Time-Servers.
ntp_server [Time-Server]	max. 64 Zeichen [a-z, A-Z, 0-9]	0.0.0.0	Definiert einen Time-Server über die IP-Adresse oder den Domain-Namen. *Ein Domain-Name 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.	GMT	Gleicht die Differenz zwischen der über einen Time-Server empfangenen Zeit und Ihrer lokalen Zeitzone aus.

Tabelle 20: Parameterliste - Beschreibung

Parameter	Wertekonvention	Default	Beschreibung
sys_name [Hostname]	max. 64 Zeichen [a-z, A-Z, 0-9]	[Default-name]	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 21: Parameterliste - Authentifizierung

Parameter	Wertekonvention	Default	Beschreibung
auth_typ [Authentifizierungs-methode]	--- [keine] MD5 TLS TTLS PEAP FAST	----	Definiert die EAP Authentifi-zierungsmethode mit der sich der UTN Server im Netzwerk identifiziert.
auth_name [Benutzername]	max. 64 Zeichen [a-z, A-Z, 0-9]	[blank]	Definiert den Name 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 er auf dem Authentifizierungsserver (RADIUS) gespeichert ist.
auth_intern [Innere Authentifizierung]	--- [keine] MSCHAP MSCHAPV2 PAP CHAP EAP-MD5 EAP-MSCHAP EAP-MSCHAPV2 EAP-TLS	---	Definiert die Art der inneren Authentifizierung bei den EAP Authentifizierungsmethoden PEAP und TTLS.
auth_extern [PEAP/EAP-FAST Optionen]	--- [keine] PEAPLABEL0 PEAPLABEL1 PEAPV0 PEAPV1	---	Definiert die Art der äußeren Authentifizierung bei den EAP Authentifizierungsmethoden PEAP und FAST.
auth_ano_name [Anonymer Name]	max. 64 Zeichen [a-z, A-Z, 0-9]	[blank]	Definiert den anonymen Namen für den unverschlüs-selten Teil der EAP Authentifi-zierungsmethoden 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 22: Parameterliste - WLAN (nur myUTN-54)

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

Parameter	Wertekonvention	Default	Beschreibung
wifi_keyid [WEP Schlüssel verwenden]	1 = Schlüssel 1 2 = Schlüssel 2 3 = Schlüssel 3 4 = Schlüssel 4	1	Definiert den anzuwendenden WEP Schlüssel.
wifi_wepkey1 wifi_wepkey2 wifi_wepkey3 wifi_wepkey4 [Schlüssel 1-4]	Die max. Zeichenanzahl ist abhängig vom gewählen Schlüsseltyp: 64 ASCII = 5 64 HEX = 10 128 ASCII = 13 128 HEX = 26	[blank]	Definiert die WEP Schlüssel. Vier WEP Schlüssel sind möglich. *Folgende Zeichen können eingegeben werden:* *- bei HEX = 0-9, a-f, A-F* *- bei ASCII = 0-9, a-z, A-Z*
wifi_psk [PSK]	8 - 63 Zeichen	[blank]	Definiert den Pre Shared Key (PSK) für Wi-Fi Protected Access (WPA).
wifi_roaming [Roaming]	on/off	off	De-/aktiviert die Verwendung von Roaming. *Roaming bezeichnet das 'Wandern' von einer Funkzelle zur nächsten. Der UTN Server verwendet dann den Access Point, der das bessere Signal liefert. Wird der UTN Server in den Einflussbereich eines anderen Access Points bewegt, wechselt er automatisch und ohne Verbindungsabbruch in die nächste Funkzelle.*
wifi_dbmroam [Roaming Level]	0-100	65	Definiert die Sendeleistung des UTN Servers in -dBm.

7.3 LED Anzeige

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

LED	Aktion	Beschreibung
Link-LED (grün)	Dauer-An	Signalisiert eine vorhandene Verbindung zum Netzwerk
Netzwerkaktivität-LED (gelb)	unregelmäßiges Blinken	Signalisiert den Empfang von Datenpaketen
Status-LED (grün)	Dauer-Aus	Signalisiert, dass keine Verbindung zu einem USB-Gerät besteht. ACHTUNG: Bei gleichzeitigen zyklischem Blinken der Netzwerkaktivität-LED wird der BIOS-Modus signalisiert. Der UTN Server ist im BIOS-Modus nicht funktionsfähig; siehe: ⇨ 96.
	Dauer-An	Signalisiert die Verbindung von mindestens einem USB-Gerät
	3 x Blinken	Signalisiert die Vergabe einer ZeroConfig IP-Adresse. HINWEIS: Dauerhaft ist eine IP-Adresse zu bevorzugen, die nicht aus dem Bereich ZeroConf kommt.
	2 x Blinken	Signalisiert die Vergabe einer IP-Adresse, die nicht 0.0.0.0 entspricht oder aus dem Bereich ZeroConfig kommt.

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

7.4 Problembehandlung

Dieses Kapitel stellt einige Problemursachen und erste Lösungshilfen dar.

Problemdarstellung

- 'Der UTN Server signalisiert den BIOS-Modus' ⇨ 96
- 'Im SEH UTN Manager sind Funktionen ausgeblendet bzw. deaktiviert' ⇨ 98
- 'Die Verbindung zum UTN Server kann nicht hergestellt werden' ⇨ 98
- 'Die Verbindung zum USB-Gerät kann nicht hergestellt werden' ⇨ 99
- 'Die Verbindung zum myUTN Control Center kann nicht hergestellt werden' ⇨ 99
- 'Das Passwort ist nicht mehr verfügbar' ⇨ 99

Der UTN Server signalisiert den BIOS-Modus

Mögliche Ursache

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

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

Der UTN Server ist im BIOS-Modus nicht funktionsfähig.

Ist ein UTN Server im BIOS-Modus, wird in der Geräteliste des Inter-Con-NetTool automatisch der Filter 'BIOS Mode' angelegt. Innerhalb dieses Filters wird der UTN Server angezeigt.

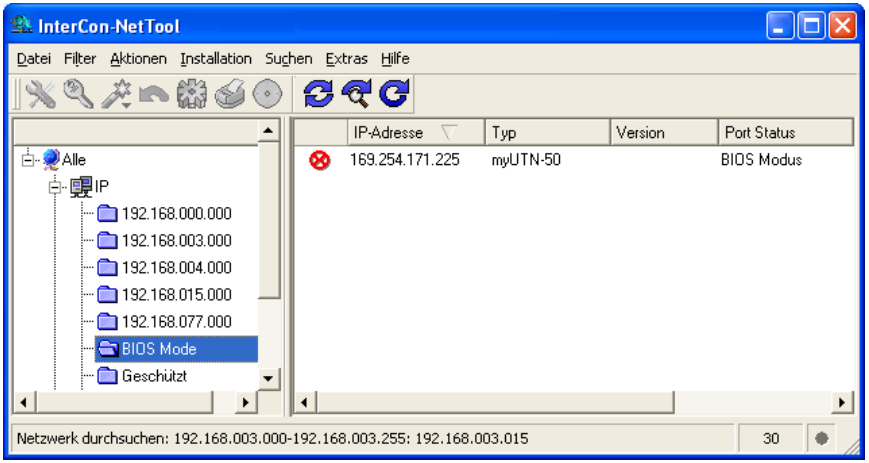


Abb. 11: InterCon-NetTool - UTN Server im BIOS-Modus

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

Gehen Sie wie folgt vor:

1. *Starten Sie das InterCon-NetTool.*
2. *Markieren Sie den UTN Server in der Geräteliste.*
   (Sie finden den UTN Server unter dem Filter 'BIOS Mode'.)
3. *Wählen Sie im Menü* **Installation** *den Befehl* **IP-Assistent**.
   Der IP-Assistent wird gestartet.
4. *Weisen Sie dem UTN Server eine IP-Adresse zu, indem Sie den Anweisungen des Assistenten folgen.*
   Die IP-Adresse wird gespeichert.
5. *Führen Sie auf dem UTN Server ein Softwareupdate durch; siehe:* ⇨ 79.

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

Im SEH UTN Manager sind Funktionen ausgeblendet bzw. deaktiviert

Mögliche Ursache

- ☐ Auf dem Windows Client ist die Multi-User Variante des SEH UTN Managers (SEH UTN Manager + Service) installiert und Ihr Windows Benutzerkonto verfügt nicht über die erforderlichen administrativen Rechte. Hierdurch haben Sie auch im SEH UTN Manager eingeschränkte Benutzerechte; siehe: 'Rechteverteilung bei der Multi-User Variante' ⇨📄23.
- ☐ Eine Funktion wird nicht vom angeschlossenen USB-Gerät unterstützt (z.B. kann die Funktion 'Print-on-demand' nicht durch eine Festplatte unterstützt werden)
- ☐ Eine Multi-User Variante ist auf einem Windows Client mit 'Benutzerkontensteuerung' installiert. Die 'Benutzerkontensteuerung' verlangt eine Bestätigung, wenn die Multi-User Variante als Administrator ausgeführt werden soll.

Gehen Sie wie folgt vor:

1. *Markieren Sie das SEH UTN Manager Symbol*  *auf dem Desktop.*
2. *Wählen Sie im Kontextmenü (rechte Maustaste) den Befehl* **Als Administrator ausführen**.

Der SEH UTN Manager startet mit administrativen Rechten.

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: ⇨📄44.

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 ⇨📄35.
- ☐ Die Kommunikation wird durch eine Sicherheitssoftware (Firewall) blockiert.

Die Verbindung zum USB-Gerät kann nicht hergestellt werden

Mögliche Ursache

- ☐ Die Gerätezugriffskontrolle ist aktiviert ⇨🗎56.
- ☐ Auf dem Client ist keine Treibersoftware für das USB-Gerät installiert.
- ☐ Das USB-Gerät ist bereits mit einem anderen Client verbunden.
- ☐ Die maximale Teilnehmerzahl ist überschritten.
  Der UTN Service erlaubt bis zu vier Teilnehmern (Clients) den zeitgleichen Zugriff auf die am UTN Server angeschlossenen USB-Geräte ⇨🗎21. Warten Sie bis ein Teilnehmer die Verbindung zu einem USB-Gerät deaktiviert hat.

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 ⇨🗎12 sowie
- die Proxy-Einstellungen Ihres Browsers

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

- ☐ Der Zugang ist via SSL (HTTPs) geschützt ⇨🗎52.
- ☐ Die Portzugriffskontolle ist aktiviert ⇨🗎54.
- ☐ Der Passwortschutz ist aktiviert ⇨🗎53.

Das Passwort ist nicht mehr verfügbar

Der Zugriff auf das myUTN Control Center kann durch ein Passwort geschützt werden. Ist das Passwort nicht mehr verfügbar, können die Parameterwerte des UTN Servers auf die Standardwerte zurückgesetzt werden um Zugriff zu erhalten ⇨🗎76. Dabei gehen sämtliche Einstellungen verloren.

7.5 Abbildungsverzeichnis

7.6 Index

V

W

Z