ThinPrint®Reader

TPR-10
TPR-11

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: ThinPrint®Reader
Version: 1.3

Online Links zu den wichtigsten Internet-Seiten:

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

Inhaltsverzeichnis

1 Allgemeine Information

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

Welche Information benötigen Sie?

1.1 ThinPrint®Reader

Was ist ThinPrint Personal Printing Essentials®?

ThinPrint Personal Printing Essentials® ist eine softwarebasierte Technologie zur sicheren Kontrolle der Druckausgabe in Netzwerken. ThinPrint Personal Printing Essentials ist druckerunabhängig.

Von einem Client wird auf das Druckerobjekt '**Personal-Printer**' gedruckt. Der Druckauftrag wird auf dem Personal-Printing-Server gespeichert. Nachdem sich der Benutzer an einem beliebigen, für Personal Printing eingerichteten Netzwerkdrucker erfolgreich authentifiziert hat, wird der Druckauftrag ausgegeben.

Was ist ThinPrint®?

ThinPrint® ist eine softwarebasierte Technologie, die unter anderem für den Netzwerkdruck die Möglichkeit zur Komprimierung von Druckaufträgen und zur Bandbreitenkontrolle bietet. Der Datenverkehr zwischen Application-Server oder Printserver und lokalem Drucker reduziert sich erheblich und entlastet das Netz.

Die ThinPrint-Technologie ermöglicht die Übertragung komprimierter und bandbreitenoptimierter Druckdaten innerhalb von Netzwerken. Die Komprimierung wird über die Server-Komponente **ThinPrint Engine** vorgenommen. Der Server schickt die komprimierten Druck-

daten zu einem Gerät, auf dem ein **ThinPrint Client** implementiert ist. Dieser dekomprimiert die Druckdaten und leitet sie an beliebige Drucker weiter.

Verwendungszweck

TPR (ThinPrint®Reader) sind speziell für Umgebungen entwickelt worden, in denen ThinPrint Personal-Printing-Technologie im Einsatz ist. Der TPR enthält einen vollständig integrierten **Personal-Printing-Client**. Gemeinsam mit dem Personal-Printing-Server ermöglicht er den Authentifizierungsprozess.

TPR sind eine Authentifizierungshardware, mit der Netzwerkdrucker unabhängig von Druckerhersteller und -model als Personal-Printing-Drucker eingesetzt werden können. Dafür wird pro Netzwerkdrucker ein TPR zwischen Netzwerk und Drucker geschaltet.

Anwender drucken auf das Personal-Printer-Druckerobjekt. Anschließend authentifizieren sie sich am TPR mittels einer kontaktlosen RFID-basierten Smartcard. Der Personal-Printing-Server sendet daraufhin den Druckauftrag zum TPR, welcher ihn an den Drucker weiterleitet.

Optional kann mit dem TPR die ThinPrint-Technologie genutzt werden. Dafür enthält der TPR einen vollständig integrierten **ThinPrint Client**. Dieser ermöglicht das Empfangen und Dekomprimieren der Druckdaten in ThinPrint-Umgebungen. Ein Netzwerkdrucker lässt sich schnell und einfach mit dem integriertem ThinPrint Client ins Netz einbinden.

Leistungsmerkmale

Der TPR unterstützt u.a. die folgenden Features:

- Mit der **Personal-Printing-SSL-/TLS-Verschlüsselung** wird die Verbindung zwischen TPR und Personal-Printing-Server sicher geschützt.
- Das Feature **AutoConnect** ermöglicht es, die für den jeweiligen Client benötigten Druckerobjekte automatisch auf dem Server anzulegen. Alle auf diese Weise ausgewählten Drucker werden auf dem Server durch den Aufruf von **AutoConnect** automatisch mit einem ThinPrint-Port verbunden (sofern entsprechende Templates existieren).
- Der **ThinPrint Connection Service** ermöglicht das Drucken zu ThinPrint Clients, die z.B. hinter einer Firewall versteckt sind.

Dabei wird sowohl die Verbindung über maskierte Netzwerke ermöglicht als auch die Zuordnung des jeweiligen Druckauftrages zum entsprechenden Zielgerät gemanagt.

- Mit der **ThinPrint SSL-/TLS-Verschlüsselung** sind die Druckdaten während der Übertragung sicher geschützt und werden von den ThinPrint Clients oder Gateways vor dem Druckvorgang entschlüsselt.

Systemvoraussetzungen

Der TPR ist konzipiert für den Einsatz in TCP/IP-basierten Netzwerken. Innerhalb des Netzwerkes muss ein Personal-Printing-Server integriert sein. Die beteiligten Netzwerkdrucker müssen RAW- bzw. Socket-Printing (Drucken via TCP/IP-Ports), IPP-Printing oder LPD-Printing unterstützen. Bei Verwendung der ThinPrint-Funktion muss innerhalb des Netzwerkes ein ThinPrint Server integriert sein. Werden **ThinPrint** bzw. der **ThinPrint Connection Service** verwendet, müssen entsprechende Lizenzen vorhanden sein.

1.2 Dokumentation

Beschreibungsumfang und Inhalte

Diese Dokumentation beschreibt mehrere Varianten des ThinPrint®Readers (TPR). Informationen zum Leistungsumfang Ihres Produktes entnehmen Sie dem Datenblatt Ihres TPR-Modells.

Aufbau der Dokumentation

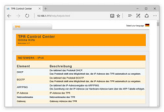
Die TPR-Dokumentation besteht aus den folgenden Dokumenten:

PDF

Benutzerdokumentation
Detaillierte Beschreibung der TPR-Konfiguration und -Administration.

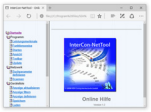
Print PDF

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



HTML

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



HTML

Online Hilfe (InterCon-NetTool)
Die Online Hilfe enthält detaillierte Informationen zur Bedienung des Software-Tools 'InterCon-NetTool'.

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: ⇨100.

Symbole und Auszeichnungen

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

Tabelle 1: Konventionen in der Dokumentation

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

1.3 Support und Service

Support

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

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

Aktuelle Services

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

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

1.4 Ihre Sicherheit

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

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

Bestimmungsgemäße Verwendung

Der TPR wird in TCP/IP-Netzwerken eingesetzt. Der TPR ist eine Authentifizierungshardware, mit der Netzwerkdrucker unabhängig von Druckerhersteller und -model als Personal-Printing-Drucker eingesetzt werden können. Der TPR ist konzipiert für den Einsatz in Büroumgebungen.

Bestimmungswidrige Verwendung

Alle Verwendungen des Gerätes, die den in der TPR-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 TPR 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: ⇨🗎**11**.*
2. *Führen Sie die Hardware-Installation aus. Die Hardware-Installation beinhaltet das Anschließen des TPR an Drucker, Netzwerk und Stromnetz; siehe: 'Quick Installation Guide'.*
3. *Stellen Sie sicher, dass die vormalige IP-Adresse des Druckers im TPR gespeichert und der Drucker auf DHCP konfiguriert ist; siehe: 'Speichern der IP-Adresse im TPR' ⇨🗎**13**.*
4. *Definieren Sie den Personal-Printing-Server und andere Personal-Printing-Einstellungen; siehe: ⇨🗎**43**.*

Der TPR ist funktionsbereit.

1.6 Speichern der IP-Adresse im TPR

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 TPR zu speichern, damit das Gerät im Netzwerk angesprochen werden kann.

Wie erhält der TPR eine IP-Adresse?

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

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

Nachdem der TPR eine IP-Adresse automatisch über ein Bootprotokoll erhalten hat, können Sie nachträglich manuell eine freidefinierbare IP-Adresse im TPR speichern. Die zugewiesene IP-Adresse des TPR kann über das Software-Tool 'InterCon-NetTool' ermittelt und verändert werden.

Weisen Sie dem TPR die vormalige IP-Adresse des Druckers zu. Konfigurieren Sie den Drucker auf DHCP (andernfalls besteht keine Funktionalität).

Nachfolgend sind die verschiedenen Methoden zur IP-Adressenvergabe beschrieben.

Automatische Methoden zur IP-Adressenvergabe

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

Manuelle Methoden zur IP-Adressenvergabe

- 'InterCon-NetTool' ⇨🗎15
- 'TPR Control Center' ⇨🗎16
- 'ARP/PING' ⇨🗎16

ZeroConf

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

Zur Namensauflösung der IP-Adresse kann der Domain Name Service von Bonjour verwendet werden; siehe: ⇨🗎34.

BOOTP

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

Voraussetzung

☑ Der Parameter 'BOOTP' ist aktiviert; siehe: ⇨🗎25.

☑ Im Netzwerk ist ein BOOTP-Server vorhanden.

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

DHCP

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

Voraussetzung

☑ Der Parameter 'DHCP' ist aktiviert; siehe: ⇨🗎25.

☑ Im Netzwerk ist ein DHCP-Server vorhanden.

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

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

Autokonfiguration (IPv6-Standard)

Der TPR 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 TPR in einem IPv6-fähigen Netzwerk angeschlossen, erhält der TPR automatisch eine zusätzliche 'link-local'-IP-Adresse aus dem IPv6-Adressbereich.

Mit Hilfe der 'link-local'-IP-Adresse hält der TPR Ausschau nach einem Router. Der TPR 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 TPR seine Adresse selbst zusammensetzen. Er ersetzt einfach die ersten 64 Bit (Präfix FE80::) mit dem im RA verschickten Präfix.

Voraussetzung

☑ Der Parameter 'IPv6' ist aktiviert.

☑ Der Parameter 'Automatische Konfiguration' ist aktiviert; siehe: ⇨📄27.

Um die Vergabe von IPv6-Adressen zu konfigurieren, siehe: ⇨📄27.

InterCon-NetTool

Das InterCon-NetTool ist eine von der SEH Computertechnik GmbH entwickelte Software zur Administration von SEH Netzwerkgeräten. Der IP-Assistent des InterCon-NetTools hilft bei der Konfiguration von TCP/IP-Parametern, wie z.B. der IP-Adresse. Über den IP-Assistenten kann die gewünschte IPv4-Adresse manuell eingegeben und im TPR gespeichert werden. Um eine IPv4-Adresse via InterCon-NetTool zu konfigurieren, siehe: ⇨📄25.

TPR Control Center

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

- Um eine **IPv4**-Adresse via TPR Control Center zu konfigurieren, siehe: ⇨🗎25.
- Um eine **IPv6**-Adresse via TPR Control Center zu konfigurieren, siehe: ⇨🗎27.

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 Minuten) gespeichert wird. Diese Tabelle wird vom ARP-Protokoll verwaltet.

Mit Hilfe der Befehle 'arp' und 'ping' kann die IP-Adresse im TPR gespeichert werden. Verfügt der TPR 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 TPR. Bei Empfang des Datenpaketes speichert das TPR 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: ⇨🗎25.

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 TPR eine neue IP-Adresse zu:
Syntax: `ping <IP-Adresse>`
Beispiel: `ping 192.168.0.123`

Die in dem Beispiel verwendeten Trennzeichen in der Hardware-Adresse entsprechen der Windows®-Plattform.

2 Administrationsmethoden

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

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

Welche Information benötigen Sie?

- 'Administration via TPR Control Center' ⇨🗎17
- 'Administration via InterCon-NetTool' ⇨🗎19
- 'Administration via E-Mail' ⇨🗎21

2.1 Administration via TPR Control Center

Welche Funktionen werden unterstützt?

Das TPR Control Center umfasst alle Funktionalitäten zur Administration Ihres TPR.

Das TPR Control Center ist in Ihrem TPR gespeichert und kann mit einer Browsersoftware (Internet Explorer, Mozilla Firefox, Safari) dargestellt werden.

Voraussetzung

☑ Der TPR ist an Netzwerk und Netzspannung angeschlossen.

☑ Der TPR hat eine gültige IP-Adresse.

TPR Control Center starten

Gehen Sie wie folgt vor:

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

↳ Das TPR Control Center wird im Browser dargestellt.

Falls das TPR Control Center nicht erscheint, überprüfen Sie die Proxy-Einstellungen des Browsers.

Zusätzlich kann das TPR Control Center über das Software-Tool 'InterCon-NetTool' gestartet werden.

Gehen Sie wie folgt vor:

1. *Markieren Sie den TPR in der Geräteliste.*
2. *Wählen Sie im Menü* **Aktionen** *den Befehl* **Browser starten**.

Das TPR Control Center wird im Browser dargestellt.

Abb. 1: TPR Control Center - START

Aufbau des TPR Control Centers

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

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

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

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

2.2 Administration via InterCon-NetTool

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

Funktionsweise

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

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

Installation

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 SEH Computertechnik GmbH-Homepage:

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

Gehen Sie wie folgt vor:

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

↳ Das InterCon-NetTool wird auf Ihrem Client installiert.

Programmstart

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

Die InterCon-NetTool-Einstellungen werden in der Datei 'NetTool.ini' gespeichert. Diese ist im 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.

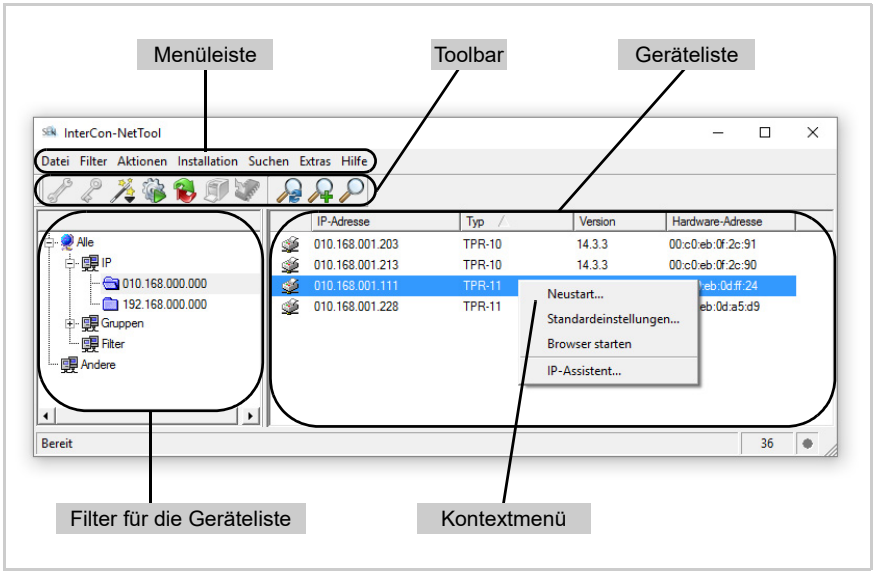


Abb. 2: InterCon-NetTool - Hauptdialog

Welche Funktionen werden unterstützt?

Über das InterCon-NetTool können Sie

- dem 'TPR eine IPv4-Adresse zuweisen' ⇨🗎25
- den 'TPR neu starten' ⇨🗎94
- die 'Parameterwerte des TPR auf die Standardeinstellung zurücksetzen' ⇨🗎91
- das 'TPR Control Center starten' ⇨🗎17
- vom 'BIOS-Modus in den Standardmodus wechseln' ⇨🗎125

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

2.3 Administration via E-Mail

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

Funktionalitäten

Mit einer E-Mail können Sie

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

Voraussetzung

☑ Auf dem TPR ist ein DNS-Server konfiguriert; siehe: ⇨📄29.

☑ Damit der TPR E-Mails empfangen kann, muss der TPR als Benutzer mit eigener E-Mail-Adresse auf einem POP3-Server eingerichtet sein.

☑ Am TPR sind POP3- und SMTP-Parameter konfiguriert; siehe: ⇨📄32.

Anweisung via E-Mail versenden

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

Gehen Sie wie folgt vor:

1. *Öffnen Sie ein E-Mail-Programm.*
2. *Erstellen Sie eine neue E-Mail.*
3. *Geben Sie als Adressat die TPR-Adresse ein.*
4. *Geben Sie eine Anweisung in die Betreffzeile ein; siehe: 'Syntax und Format der Anweisung' ⇨📄22.*
5. *Versenden Sie die E-Mail.*

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

Syntax und Format der Anweisung

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

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

Folgende Kommandos werden unterstützt:

Kommandos	Option	Beschreibung
<command>	get status	Sendet die Statusseite des TPR.
	get parameters	Sendet die Parameterliste des TPR.
	set parameters	Sendet Parameter zum TPR. Syntax und Wertekonventionen entnehmen Sie der Parameterliste; siehe: ⇨103. Parameter und Wert sind in den E-Mail-Textkörper zu schreiben.
	update TPR	Führt automatisch ein Update mit der in der E-Mail angehängten Software durch.
	help	Sendet eine Seite mit Informationen zur Fernwartung.
[<comment>]		Frei definierbarer Text für Beschreibungszwecke.

Für die Anweisungen gilt:

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

Sicherheit mit TAN

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

Parameteränderungen

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

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

Syntax und Wertekonventionen entnehmen Sie der Parameterliste; siehe: ⇨103.

Beispiel 1

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

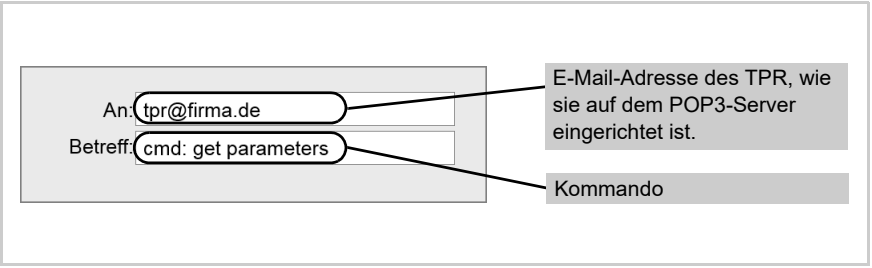


Abb. 3: Administration via E-Mail - Beispiel 1

Beispiel 2

Diese E-Mail konfiguriert am TPR den Parameter 'Beschreibung'.

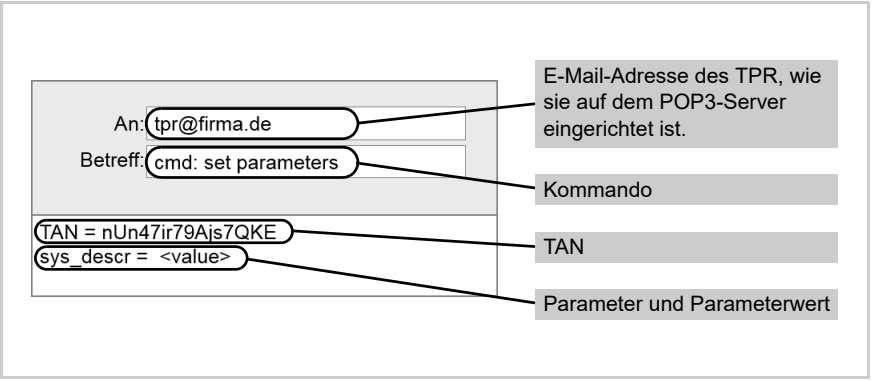


Abb. 4: Administration via E-Mail - Beispiel 2

3 Netzwerkeinstellungen

Zur optimalen Integration des TPR in ein Netzwerk können verschiedene Einstellungen definiert werden. In diesem Kapitel erfahren Sie, welche Netzwerkeinstellungen unterstützt werden.

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 TPR in ein TCP/IP-Netzwerk können Sie verschiedene IPv4-Parameter definieren. Für weitere Informationen zur IP-Adressenvergabe, siehe: ⇨🗎13.

Was möchten Sie tun?

- ☐ 'IPv4-Parameter via TPR Control Center konfigurieren' ⇨🗎25
- ☐ 'IPv4-Parameter via InterCon-NetTool konfigurieren' ⇨🗎26

IPv4-Parameter via TPR Control Center konfigurieren

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - IPv4 an**.
3. *Konfigurieren Sie die IPv4-Parameter; siehe: Tabelle 2* ⇨🗎***25.***
4. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

Tabelle 2: IPv4-Parameter

Parameter	Beschreibung
DHCP BOOTP ARP/PING	De-/aktiviert die Protokolle DHCP, BOOTP und ARP/PING. *Die Protokolle stellen verschiedene Möglichkeiten dar, die IP-Adresse im TPR zu speichern.* *(Siehe 'Speichern der IP-Adresse im TPR' ⇨🗎13.)* Es empfiehlt sich, diese Optionen zu deaktivieren, sobald der TPR eine IP-Adresse zugewiesen bekommen hat.
IP-Adresse	IP-Adresse des TPR
Netzwerkmaske	Netzwerkmaske des TPR
Gateway	Gateway-Adresse des TPR

IPv4-Parameter via InterCon-NetTool konfigurieren

Voraussetzung

☑ Das InterCon-NetTool ist auf dem Client installiert; siehe: ⇨19.

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

Gehen Sie wie folgt vor:

1. *Starten Sie das InterCon-NetTool.*
2. *Markieren Sie den TPR in der Geräteliste.*
   Der TPR 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 IP-Assistenten.*

↳ Die Einstellungen werden gespeichert.

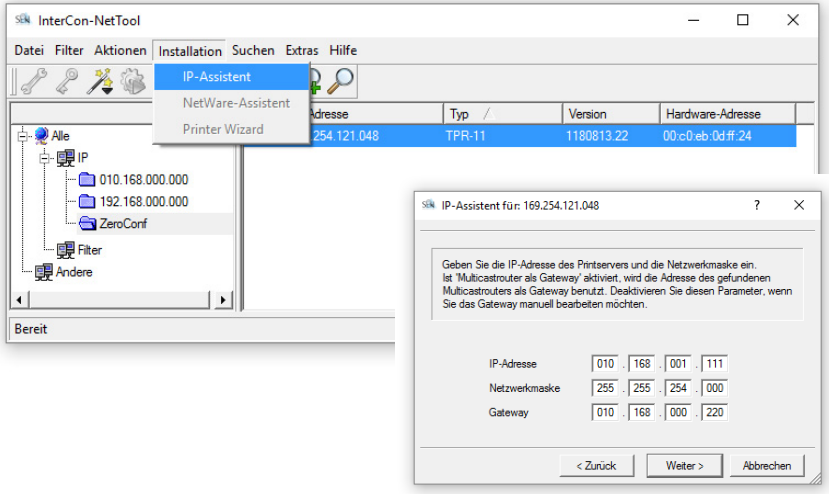


Abb. 5: InterCon-NetTool - IP-Assistent

3.2 Wie konfiguriere ich IPv6-Parameter?

Sie haben die Möglichkeit, den TPR in ein IPv6-Netzwerk einzubinden.

Welche Vorteile bietet IPv6?

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

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

Wie wird eine IPv6-Adresse dargestellt?

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

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

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

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

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

Die URL wird ausschließlich von IPv6-fähigen Browsern akzeptiert.

Welche IPv6-Adresstypen gibt es?

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

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

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - IPv6** *an.*
3. *Konfigurieren Sie die IPv6-Parameter; siehe: Tabelle 3* ⇨📄*29.*
4. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

Tabelle 3: IPv6-Parameter

Parameter	Beschreibung
IPv6	De-/aktiviert die IPv6-Funktionalität des TPR.
Automatische Konfiguration	De-/aktiviert die automatische Vergabe der IPv6-Adressen für den TPR.
IPv6-Adresse	Definiert eine manuell vergebene IPv6-Unicast-Adresse im Format n:n:n:n:n:n:n:n für den TPR. 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 TPR seine 'Router Solicitations' (RS) sendet.
Präfixlänge	Definiert die Länge des Subnetz-Präfixes für die IPv6-Adresse. Der Wert 64 ist voreingestellt. Adressbereiche werden durch Präfixe angegeben. Dazu wird die Präfixlänge (Anzahl der verwendeten Bits) als Dezimalzahl mit vorangehendem '/' an die IPv6-Adresse angehängt dargestellt.

3.3 Wie konfiguriere ich den DNS?

Der DNS (Domain Name Service) erlaubt die gegenseitige Zuordnung von Namen und IP-Adressen. Wird ein DNS-Server in Ihrem Netzwerk betrieben, haben Sie die Möglichkeit, den DNS für Ihren TPR 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 TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - DNS**.
3. *Konfigurieren Sie die DNS-Parameter; siehe: Tabelle 4* ⇨🗎*30*.
4. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert.

Tabelle 4: DNS-Parameter

Parameter	Beschreibung
DNS	De-/aktiviert die Namensauflösung über einen DNS-Server.
Erster DNS-Server	Definiert die IP-Adresse des ersten DNS-Servers (z.B. 192.168.0.21).
Zweiter DNS-Server	Definiert die IP-Adresse des zweiten DNS-Servers. *Der zweite DNS-Server wird benutzt, wenn der erste nicht verfügbar ist.*
Domain-Name (Suffix)	Definiert den Domain-Namen eines vorhandenen DNS-Servers (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. dem TPR oder Drucker) bereitgestellt werden. Der TPR 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.

Für SNMPv3 müssen Name und Passwort des SNMP-Benutzers definiert sein. Die hierfür verwendeten Benutzerkonten sind identisch zu den Benutzerkonten für den Zugang zum TPR Control Center; siehe: ⇨🗎65.

Voraussetzung

☑ Nur bei SNMPv3: Die Benutzerkonten sind definiert; siehe: ⇨🗎65.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - SNMP** *an.*
3. *Konfigurieren Sie die SNMP-Parameter; siehe: Tabelle 5* ⇨🗎***31.***
4. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 5: SNMP-Parameter

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

3.5 Wie konfiguriere ich POP3 und SMTP?

Damit am TPR die Administration via E-Mail (⇨🗎21) und der Benachrichtigungsservice (⇨🗎40) funktionieren, müssen die Protokolle POP3 und SMTP am TPR konfiguriert werden.

POP3

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

SMTP

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

Was möchten Sie tun?

- ☐ 'POP3 konfigurieren' ⇨🗎32
- ☐ 'SMTP konfigurieren' ⇨🗎33

POP3 konfigurieren

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - E-Mail an**.
3. *Konfigurieren Sie die POP3-Parameter; siehe: Tabelle 6 ⇨🗎32.*
4. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 6: POP3-Parameter

Parameter	Beschreibung
POP3	De-/aktiviert die POP3-Funktionalität.
POP3 - Servername	Definiert einen POP3-Server über die IP-Adresse oder den Hostnamen. *Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.*
POP3 - Serverport	Definiert den Port, über den der TPR E-Mails empfängt. Die Portnummer 110 ist voreingestellt. Bei Verwendung von SSL/TLS ist als Portnummer 995 einzutragen.

Parameter	Beschreibung
POP3 - Sicherheit	Definiert das anzuwendende Authentifizierungsverfahren (APOP / SSL/TLS). *Bei SSL/TLS wird die Verschlüsselungsstärke über Protokoll und Verschlüsselungsstufe definiert ⇨61.*
POP3 - E-Mails abfragen alle	Definiert das Zeitintervall (in Minuten) für die Abfrage der E-Mails auf dem POP3-Server.
POP3 - E-Mails ignorieren mit mehr als	Definiert die maximale Größe (in Kbyte) der vom TPR akzeptierten E-Mails. *(0 = unbegrenzt)*
POP3 - Benutzername	Definiert den Benutzernamen, den der TPR benutzt, um sich am POP3-Server anzumelden.
POP3 - Passwort	Definiert das Benutzerpasswort, das der TPR benutzt, um sich am POP3-Server anzumelden.

SMTP konfigurieren

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - E-Mail an**.
3. *Konfigurieren Sie die SMTP-Parameter; siehe: Tabelle 7 ⇨33.*
4. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 7: SMTP-Parameter

Parameter	Beschreibung
SMTP - Servername	Definiert einen SMTP-Server über die IP-Adresse oder den Hostnamen. *Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.*
SMTP - Serverport	Definiert die Portnummer, über die der SMTP-Server E-Mails von dem TPR empfängt. Die Portnummer 25 ist voreingestellt.

Parameter	Beschreibung
SMTP - TLS	De-/aktiviert die Option TLS. *Über das Sicherheitsprotokoll Transport Layer Security (TLS) wird der Übertragungsweg vom TPR zum SMTP-Server verschlüsselt. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨🗎61.*
SMTP - Name des Absenders	Definiert die E-Mail-Adresse, die der TPR zum Versenden von E-Mails verwendet. Hinweis: Oft sind der Name des Absenders und der Benutzername identisch.
SMTP - Login	De-/aktiviert die SMTP-Authentifizierung für das Login.
SMTP - Benutzername	Definiert den Benutzernamen, den der TPR benutzt, um sich am SMTP-Server anzumelden.
SMTP - Passwort	Definiert das Passwort, das der TPRr benutzt, um sich am SMTP-Server anzumelden.
SMTP - Sicherheit (S/MIME)	De-/aktiviert das Verschlüsseln und Signieren der E-Mails via S/MIME.
SMTP - E-Mail signieren	Definiert das Signieren von E-Mails. *Eine vom Absender erstellte Signatur ermöglicht es dem Empfänger, die Identität des Absenders zu prüfen und gewährleistet, dass die E-Mail nicht verändert wurde. Für das Signieren wird ein S/MIME-Zertifikat (⇨🗎70) benötigt.*
SMTP - Vollständig verschlüsseln	Definiert das Verschlüsseln von E-Mails. *Eine verschlüsselte E-Mail kann nur vom Empfänger geöffnet und gelesen werden. Für die Verschlüsselung wird ein S/MIME-Zertifikat (⇨🗎70) benötigt.*
SMTP - Öffentlichen Schlüssel beifügen	Sendet den öffentlichen Schlüssel zusammen mit der E-Mail. Das Anhängen ist erforderlich zum Anzeigen der E-Mails bei vielen E-Mail-Clients.

3.6 Wie konfiguriere ich Bonjour?

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

Der TPR 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' ⇨🗎14) richtet der TPR eine Anfrage an das Netzwerk. Ist die IP-Adresse im Netzwerk schon belegt, erhält der TPR eine entsprechende Antwort. Der TPR startet dann eine weitere Anfrage mit einer anderen IP-Adresse. Ist die IP-Adresse noch frei, speichert der TPR 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 TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **NETZWERK - Bonjour** *an.*
3. *Konfigurieren Sie die Bonjour-Parameter; siehe: Tabelle 8* ⇨🗎***35.***
4. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellung wird gespeichert.

Tabelle 8: Bonjour-Parameter

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

3.7 Wie konfiguriere ich die Gerätezeit?

Sie haben die Möglichkeit, die TPR-Gerätezeit 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 TPR über die IP-Adresse oder den Hostnamen definiert.

Nutzen und Zweck

Ist der Time-Server aktiviert, erhalten ThinPrint-Druckaufträge, die über den TPR abgewickelt werden, einen Zeitstempel. In der 'Job History' (⇨96) werden dann Datum und Uhrzeit angezeigt.

UTC

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

Zeitzone

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

Voraussetzung

☑ Im Netzwerk ist ein Time-Server integriert.

Gehen Sie wie folgt vor:

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

↳ Die Einstellungen werden gespeichert.

4 Geräteeinstellungen

Am TPR können Beschreibungen, die Kommunikation mit dem Drucker, lokale Service-Ports und der Benachrichtigungsservice konfiguriert werden. Dieses Kapitel informiert Sie über diese Geräteeinstellungen.

Welche Information benötigen Sie?

- 'Wie lege ich eine Beschreibung fest?' ⇨🗎38
- 'Wie konfiguriere ich die Kommunikation zwischen TPR und Drucker?' ⇨🗎38
- 'Wie definiere ich lokale Service-Ports?' ⇨🗎39
- 'Wie verwende ich den Benachrichtigungsservice?' ⇨🗎40

4.1 Wie lege ich eine Beschreibung fest?

Sie haben die Möglichkeit, dem TPR 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 TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - Beschreibung** *an.*
3. *Geben Sie in die Felder* **Hostname, Beschreibung** *und* **Ansprechpartner** *freidefinierbare Bezeichnungen ein.*
4. *Bestätigen Sie mit* **Speichern**.

Die Daten werden gespeichert.

4.2 Wie konfiguriere ich die Kommunikation zwischen TPR und Drucker?

Internes IP-Netzwerk

Der TPR ist physikalisch zwischen Drucker und Netzwerk zu schalten. Beide Geräte bilden ein internes lokales Netzwerk, in dem der TPR über eine zweite, lokale IP-Adresse für die interne Kommunikation mit dem Drucker verfügt. Der interne DHCP-Server des TPR konfiguriert automatisch die IP-Adresse des Druckers und zugehörige Parameter.

Masquerading (NAT)

Um das interne Netzwerk mit dem externen Netzwerk zu verbinden, werden die Adressinformationen via Masquerading umgeschrieben. Masquerading ist eine Form von NAT (Network Address Translation). Datenpakete werden auf diese Weise durch den TPR an den Drucker weitergeleitet. Dadurch ist der TPR transparent eingebunden und die Infrastruktur sowie eventuell bestehende Output-Monitoring-Systeme bleiben unbeeinflusst.

Sie haben die Möglichkeit, die Einstellungen des internen Netzwerks anzupassen.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - TPR-10** *an.*

3. *Konfigurieren Sie die Drucker-Parameter; siehe: Tabelle 9* ⇨🗎*39*.
4. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 9: Drucker-Konfiguration

Parameter	Beschreibung
Lokale IP-Adresse	Definiert die IP-Adresse des TPR für die interne Kommunikation. *TPR und Drucker bilden ein internes IP-Netzwerk. Die lokale IP-Adresse ist das Gateway zur Drucker-IP-Adresse. Die Netzwerkmaske lautet 255.255.255.240.*
Drucker-IP-Adresse	Definiert die IP-Adresse des Druckers für die interne Kommunikation. *TPR und Drucker bilden ein internes IP-Netzwerk. Die Drucker-IP-Adresse und zugehörige Parameter werden vom internen DHCP-Server des TPR konfiguriert.*
Masquerading	De-/aktiviert das Masquerading. *Masquerading ist eine Form von NAT (Network Address Translation). Bei NAT werden alle externen IP-Adressen durch lokale IP-Adressen ersetzt.*
ICMP	De-/aktiviert das Weiterleiten von ICMP-Paketen an die Drucker-IP-Adresse. *In IP-Netzwerken wird ICMP zum Übertragen von Fehlermeldungen und Abfragen, z.B. 'ping', verwendet. Wenn die Option aktiviert ist, werden Abfragen vom Drucker und nicht vom TPR beantwortet.*

4.3 Wie definiere ich lokale Service-Ports?

Der TPR nutzt TCP-Ports für den Datentransfer im Netzwerk. TCP-Ports sind Adresskomponenten, die durch ihre Portnummer gekennzeichnet sind. Über die Ports werden Verbindungen aufgebaut und Datenpakete den richtigen Diensten (Services) zugeordnet.

Bestimmte Dienste (u.a. HTTP, HTTPS und SNMP) verfügen über fest zugeordnete Ports.

Sie haben die Möglichkeit, Portnummern für die folgenden lokalen Dienste zu definieren:

- HTTP (Standard = 80)
- HTTPS (Standard = 443)
- SNMP (Standard = 161)
- ThinPrint (Standard = 4000)

TCP-Ports, die als lokale Service-Ports konfiguriert sind, können nicht zur Kommunikation mit dem Drucker verwendet werden. Weisen Sie den lokalen Service-Ports freie Portnummern zu, um die Standard-TCP-Ports zur Kommunikation mit dem Drucker zu verwenden.

Beispiel

Weisen Sie HTTP die Portnummer 8080 zu, wird bei Aufruf der IP-Adresse des TPR im Browser die Druckerhomepage dargestellt. Um das TPR Control Center aufzurufen, fügen Sie der IP-Adresse die Portnummer hinzu (<IP-Adresse>:8080). Im InterCon-NetTool erscheint der TPR als Drucker (Spalte 'Typ').

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - TPR-10** *an.*
3. *Geben Sie im Bereich* **Lokale Service-Ports** *in den entsprechenden Feldern die Portnummern ein.*
4. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert.

4.4 Wie verwende ich den Benachrichtigungsservice?

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

Die folgenden Meldungstypen sind möglich:

- Die Status-E-Mail informiert periodisch über den Status des TPR.

- Die Event-Benachrichtigung informiert über ein bestimmtes Ereignis am TPR via E-Mail oder SNMP-Trap. Das Ereignis kann sein:
  - Der Neustart des TPR.
  - Ein Kartenereignis am TPR.
  - Das Anschließen oder Entfernen eines USB-Sticks am TPR.
  - Ein Problem am TPR.

Was möchten Sie tun?

☐ 'Versand von Status-E-Mails konfigurieren' ⇨📄41
☐ 'Event-Benachrichtigung via E-Mail konfigurieren' ⇨📄41
☐ 'Event-Benachrichtigung via SNMP-Trap konfigurieren' ⇨📄42

Versand von Status-E-Mails konfigurieren

Voraussetzung

☑ Am TPR sind SMTP-Parameter konfiguriert; siehe: ⇨📄32.
☑ Auf dem TPR ist ein DNS-Server konfiguriert; siehe: ⇨📄29.

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

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - Benachrichtigung an**.
3. *Geben Sie im Feld* **E-Mail-Empfänger** *die E-Mail-Adresse des Empfängers ein.*
4. *Aktivieren Sie die Option* **Status** *für den jeweiligen Empfänger.*
5. *Definieren Sie im Bereich* **Status - Benachrichtungszeit** *das Sendeintervall.*
6. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

Event-Benachrichtigung via E-Mail konfigurieren

Voraussetzung

☑ Am TPR sind SMTP-Parameter konfiguriert; siehe: ⇨📄32.
☑ Auf dem TPR ist ein DNS-Server konfiguriert; siehe: ⇨📄29.

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

Gehen Sie wie folgt vor:

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

↳ Die Einstellungen werden gespeichert.

Event-Benachrichtigung via SNMP-Trap konfigurieren

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

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - Benachrichtigung an**.
3. *Geben Sie im Feld* **Trap-Empfänger** *die Trap-Adresse des Empfängers ein.*
4. *Geben Sie im Feld* **Trap-Community** *die Community des Empfängers ein.*
5. *Aktivieren Sie die Optionen mit den gewünschten Meldungstypen.*
6. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

5 Personal-Printing-Einstellungen

Damit der TPR mit dem Personal-Printing-Server kommunizieren und den Authentifizierungsprozess durchführen sowie Druckaufträge empfangen und weiterleiten kann, sind Server- und Druckereinstellungen zu definieren. In diesem Kapitel erfahren Sie, wie Sie die Parameterwerte optimal aufeinander abstimmen.

Welche Information benötigen Sie?

- 'Wie definiere ich den Personal-Printing-Server?' ⇨ 43
- 'Wie verschlüssele ich die Verbindung zum Personal-Printing-Server?' ⇨ 45
- 'Wie überprüfe ich die Identität des Personal-Printing-Servers?' ⇨ 46
- 'Wie konfiguriere ich den Personal-Printing-Drucker?' ⇨ 47

Hier beschriebene Einstellungen beziehen sich auf die Clientseite (TPR). Informationen zur Installation, Konfiguration und Administration der Personal-Printing-Umgebung entnehmen Sie der Personal-Printing-Dokumentation unter http://www.personal-printing.com.

5.1 Wie definiere ich den Personal-Printing-Server?

In der Personal-Printing-Umgebung werden Druckaufträge zunächst auf dem Personal-Printing-Server zwischengespeichert. Erst nachdem sich der Benutzer am TPR authentifiziert hat, werden die Druckaufträge an den Drucker weitergeleitet und ausgegeben.

Es können zwei Personal-Printing-Server auf dem TPR definiert werden.

Verbindung

Damit eine Verbindung zum Personal-Printing-Server hergestellt werden kann, sind Servername und -port zu definieren.

Authentifizierungsprozess

Für den Authentifizierungsprozess am Personal-Printing-Server ist eine Nutzer-PIN erforderlich. Weil die Authentifizierung am TPR

über eine Chipkarte erfolgt, wird keine individuelle PIN-Eingabe verlangt. Stattdessen erhalten alle Benutzer des TPR dieselbe Nutzer-PIN. Diese PIN wird auf dem Personal-Printing-Server definiert und muss auf dem TPR identisch gespeichert werden.

Konfigurieren Sie auf dem Personal-Printing-Server eine Standard-Nutzer-PIN (z.B. 'SEH') für alle Benutzer des TPR. Auf dem TPR ist die Nutzer-PIN 'SEH' voreingestellt.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - Personal Printing**.
3. *Aktivieren Sie die Option* **Personal Printing**.
4. *Definieren Sie die Personal-Printing-Parameter; siehe: Tabelle 10 ⇨🗎44.*
5. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellung wird gespeichert.

Tabelle 10: Personal-Printing-Parameter

Parameter	Beschreibung
Server	De-/aktiviert den Personal Printing Server.
Servername	Definiert einen Personal-Printing-Server über die IP-Adresse oder den Hostnamen. *Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.*
Serverport	Definiert den TCP-Port, über den der TPR mit dem Personal-Printing-Server kommuniziert. *Die Portnummer 80 ist voreingestellt. Bei Verwendung von SSL ist als Portnummer 443 einzutragen (⇨🗎45).*
Nutzer-PIN	Definiert die Nutzer-PIN. *Die definierte Nutzer-PIN und die Nutzer-PIN in den Nutzerkonten des Active Directory müssen identisch sein. Die voreingestellte Nutzer-PIN ist 'SEH'.*

5.2 Wie verschlüssele ich die Verbindung zum Personal-Printing-Server?

Eine sichere Verbindung zwischen Personal-Printing-Server und TPR wird durch den Einsatz einer SSL-/TLS-Verschlüsselung ermöglicht. Bei der Abfrage von Druckaufträgen werden Nutzdaten (Nutzer-ID, Nutzer-PIN usw.) verschlüsselt übertragen. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert. ⇨🗎61.

Dafür wird das Personal-Printing-Protokoll, das die Verbindung zwischen Personal-Printing-Server und TPR herstellt und die Datenpakete übermittelt, via SSL/TLS verschlüsselt. D.h. es werden Zertifikate zur Authentifizierung benötigt.

Sowohl auf dem Personal-Printing-Server als auch auf dem TPR muss ein Zertifikat von einer übereinstimmenden CA (Certification Authority) installiert sein.

Der Personal-Printing-Server fordert vom TPR ein Zertifikat an. Mit Hilfe des zugehörigen CA-Zertifikats wird das Zertifikat vom Personal-Printing-Server überprüft. Dazu muss das CA-Zertifikat auf dem Personal-Printing-Server hinterlegt sein.

Vorgehensweise

- Erstellen Sie auf dem TPR eine Zertifikatsanforderung; siehe: ⇨🗎74.
- Erstellen Sie mit der Zertifikatsanforderung und mit Hilfe einer Zertifizierungsstelle ein Zertifikat.
- Installieren Sie das angeforderte Zertifikat auf dem TPR; siehe: ⇨🗎75.
- Installieren Sie das CA Zertifikat der Zertifizierungsstelle auf dem Personal-Printing-Server ⇨🗎77.
- Aktivieren Sie die SSL-/TLS-Verschlüsselung auf dem TPR.

Voraussetzung

☑ Die Portnummer des Personal-Printing-Servers ist auf 443 konfiguriert; siehe: ⇨🗎43.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - Personal Printing** *an.*

3. *Aktivieren Sie die Option* **SSL-Verbindung**.
4. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

5.3 Wie überprüfe ich die Identität des Personal-Printing-Servers?

Die Identität des Personal-Printing-Servers kann mit Hilfe von Zertifikaten überprüft werden. Schlägt die Überprüfung fehl, wird keine Verbindung zum Personal-Printing-Server aufgebaut.

Wenn beim Personal Printing eine Identitätsprüfung aktiviert ist, muss sowohl auf dem Personal-Printing-Server als auch auf dem TPR ein Zertifikat von einer übereinstimmenden CA (Certification Authority) installiert sein.

Der TPR fordert vom Personal-Printing-Server ein Personal-Printing-Zertifikat (Serverzertifikat) an. Mit Hilfe des zugehörigen CA-Zertifikats und/oder des Personal-Printing-Zertifikats selbst verifiziert der TPR das Zertifikat vom Personal-Printing-Server und damit dessen Identität.

Voraussetzung

☑ Auf dem Personal-Printing-Server ist ein Personal-Printing-Zertifikat gespeichert.

☑ Auf dem TPR ist ein CA-Zertifikat und/oder Personal-Printing-Zertifikat gespeichert (⇨ 70).

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - Personal Printing** *an.*
3. *Aktivieren Sie die Option* **Zertifikat verifizieren**.
4. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellung wird gespeichert.

5.4 Wie konfiguriere ich den Personal-Printing-Drucker?

Die Authentifizierung für das Abholen von Druckaufträgen erfolgt am TPR, d.h. direkt am Drucker.

Damit ein Drucker für Personal Printing genutzt werden kann, muss der Drucker zuerst auf dem Personal-Printing-Server eingerichtet werden. Dabei erhält er automatisch eine Drucker-ID. Die Zuteilung der Druckaufträge erfolgt über die Drucker-ID.

Anschließend muss der an den TPR angeschlossene Drucker am TPR eingebunden werden. Dafür ist am TPR die Drucker-ID zu definieren. Die Drucker-ID muss mit der ID auf dem Personal-Printing-Server identisch sein.

Zur Anpassung der Druckausgabe können Sie verschiedene Parameter konfigurieren.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - Personal Printing**.
3. *Geben Sie im Feld* **Drucker-ID** *die ID des angeschlossenen Druckers an.*
4. *Definieren Sie die Druckausgabe-Parameter; siehe: Tabelle 11* ⇨🗎*47*
5. *Bestätigen Sie mit* **Speichern**.

Die Einstellung wird gespeichert.

Tabelle 11: Druckausgabe-Parameter

Parameter	Beschreibung
Druckaufträge einzeln auslösen	De-/aktiviert das Auslösen eines einzelnen Druckauftrags pro Kartenstreich. Wenn mehrere Druckaufträge anliegen, müssen diese einzeln nacheinander ausgelöst werden.

Parameter	Beschreibung
User-ID formatieren	De-/aktiviert das Formatieren der Nutzer-IDs. Ist die Option aktiviert, werden die ID-Elemente mit Bindestrichen getrennt und Buchstaben groß geschrieben. *Das Format der Nutzer-ID muss mit dem auf dem Personal-Printing-Server verwendeten Format übereinstimmen. Aktivieren Sie die Option, wenn Sie Ihre Personal-Printing-Umgebung für TPR-Soft- und Firmware-Versionen 14.0.16 und kleiner konfiguriert haben.*
Signaltongeber	De-/aktiviert die akustische Rückmeldung. Akustische Signale stellen beim Auslösen von Druckaufträgen Informationen zur Verfügung; siehe 'Quick Installation Guide'.
Löschen der Druckaufträge	- durch den Personal-Printing-Server: Gedruckte Aufträge werden sofort gelöscht durch den Personal-Printing-Server. - durch den TPR: Gedruckte Aufträge werden durch den TPR gelöscht. Der Löschzeitpunkt kann über die Verzögerung bestimmt werden. - ohne: Gedruckte Aufträge werden gemäß den Einstellungen auf dem Personal-Printing-Server gelöscht.
Verzögerung	Definiert eine Verzögerung (in Sekunden) für das Löschen von gedruckten Aufträgen durch den TPR. (0 = sofortiges Löschen) *Eine Verzögerung stellt eine vollständige Übertragung an den Drucker und das vollständige Ausdrucken des Druckauftrages sicher.*

6 ThinPrint-Einstellungen

Der TPR kann zusätzlich als ThinPrint Gateway eingesetzt werden. Damit der TPR mit dem ThinPrint Server über einen Port kommunizieren bzw. Druckaufträge empfangen und weiterleiten kann, sind Port, Bandbreite sowie Drucker und Druckereigenschaften zu definieren. In diesem Kapitel erfahren Sie, wie Sie die Parameterwerte optimal aufeinander abstimmen.

Welche Information benötigen Sie?

Hier beschriebene Einstellungen beziehen sich auf die Clientseite (TPR). Informationen zur Installation, Konfiguration und Administration der ThinPrint-Umgebung entnehmen Sie der ThinPrint-Dokumentation unter http://www.thinprint.de.

6.1 Wie definiere ich den ThinPrint-Port?

In der ThinPrint-Umgebung wird über eine Socketverbindung auf einen TCP/IP-Port gedruckt. Die Portnummer am TPR muss mit der am ThinPrint Server definierten Portnummer identisch sein.

Am TPR ist der Port 4000 voreingestellt. Sie haben die Möglichkeit, bei Bedarf eine andere Portnummer zu konfigurieren.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - ThinPrint®** *an.*
3. *Geben Sie im Feld* **ThinPrint®-Port** *die Portnummer ein.*
4. *Bestätigen Sie mit* **Speichern**.

Die Einstellung wird gespeichert.

6.2 Wie definiere ich die Bandbreite?

Die Bandbreite beschreibt die Kapazität einer Datenverbindung. Beim TPR wird die Bandbreite in Bit/Sekunde (bit/s) angegeben.

Serverseitig kann die für Druckaufträge benötigte Bandbreite individuell für jeden ThinPrint-Port auf einen frei definierbaren Wert begrenzt sein. Sie haben die Möglichkeit, auf der Clientseite (also am TPR) das Bandbreitenlimit am Port weiter herabzusetzen.

Das Setzen eines Bandbreitenwerts am TPR, der höher ist als der serverseitig definierte Wert, hat keine Auswirkung. In diesem Fall gilt der serverseitig definierte Wert.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - ThinPrint®** *an.*
3. *Aktivieren Sie die Option* **Bandbreite.**
4. *Geben Sie in dem Feld die gewünschte Bandbreite ein.*
5. *Bestätigen Sie mit* **Speichern**.

Die Einstellung wird gespeichert.

6.3 Wie binde ich den Drucker ein?

Vom ThinPrint Server werden die Druckaufträge zum TPR geschickt. Nach der Dekomprimierung leitet der TPR die Druckaufträge an den Drucker weiter.

Die Zuteilung der Druckaufträge erfolgt über die Drucker-ID. Es kann ein Netzwerkdrucker über den TPR eingebunden werden.

Beim Einbinden des angeschlossenen Netzwerkdruckers sind die Druckerparameter (Name, Klasse, Treiber) und eine Übertragungsmethode zu definieren.

Übertragungsmethoden

Die Übertragung der Daten zwischen dem TPR und dem Netzwerkdrucker kann durch drei Methoden erfolgen:

- Standardmäßig werden die Daten über eine **RAW-/Socketverbindung** auf einen TCP/IP-Port übertragen. Am TPR ist der Port 9100 voreingestellt. Bei Bedarf kann eine andere Portnummer konfiguriert werden.
- Bei **IPP-Verbindungen** (Internet Printing Protocol) werden die Druckdaten via HTTP 1.1 über lokale Netzwerke oder das Internet an den Drucker gesendet. Dafür ist eine Drucker-URL zu konfigurieren, deren Implementierung herstellerabhängig ist. Lesen Sie hierzu die Dokumentation Ihres Druckers. Die Drucker-URL 'ipp/lp1' ist voreingestellt und kann bei Bedarf geändert werden.
  Vorteil: Via SSL/TLS kann die Verbindung zwischen TPR und Drucker verschlüsselt werden.
- Alternativ kann die Übertragung über das **LPD-Protokoll** (Line Printer Daemon) erfolgen. Dabei werden die Druckdaten über eine LPD-Queue an die IP-Adresse des Druckers gesendet.
  Der LPD-Queue-Name 'lp1' ist voreingestellt. Bei Bedarf kann ein anderer LPD-Queue-Name konfiguriert werden. Je nach Konfiguration ist das Druckverhalten entweder konform zu RFC1179 oder ähnelt dem Microsoft-LPD-Printing.
  Vorteil: Bei der Übertragung über das LPD-Protokoll werden zusätzliche Druckauftrag-Attribute übermittelt, die in der 'Job History' (⇨96) dargestellt werden.

Die Unterstützung der Übertragungsmethoden ist druckerabhängig. Nähere Informationen finden Sie im Druckerhandbuch.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - ThinPrint®-Drucker** *an.*
3. *Geben Sie in den Feldern die Drucker-Parameter ein; siehe: Tabelle 12* ⇨🗎*52.*
4. *Wählen Sie für den Drucker eine Übertragungsmethode.*
5. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 12: Drucker-Parameter

Parameter	Beschreibung
ID	Über die ID wird der Drucker beim ThinPrint Server identifiziert.
Drucker	Definiert den Druckernamen. Dieser ist eine reine Beschreibung und dient zur Unterscheidung der Drucker. *Das Hinterlegen eines Druckernamens ist eine Voraussetzung des Druckers für die Teilnahme am ThinPrint AutoConnect-Verfahren. Sofern der Drucker SNMP unterstützt, wird der Name automatisch über SNMP bezogen. Es kann jederzeit eine freidefinierbare Beschreibung eingegeben werden, die jeden automatisch bezogenen Druckernamen überschreibt.*
Klasse	Drucker, deren Treiber untereinander kompatibel sind, können zu einer Klasse zusammengefasst werden. *Das Hinterlegen einer Druckerklasse ist (neben dem Hinterlegen des Druckernamen) für die Teilnahme am ThinPrint AutoConnect-Verfahren optional anwendbar. Sofern der Drucker SNMP unterstützt, wird der Klassenname automatisch über SNMP bezogen. Es kann jederzeit eine freidefinierbare Beschreibung eingegeben werden, die jede automatisch bezogene Druckerklasse überschreibt.*
Treiber	Definiert den Druckertreiber für das ThinPrint® AutoConnect-Verfahren.

Parameter	Beschreibung
Port	Definiert die Portnummer für das RAW-/Socket-Printing. (Default = 9100) *Wird verwendet, wenn als Übertragungsmethode 'RAW' gewählt wurde.*
URL	Definiert den zweiten Teil der Drucker-URL für das IPP-Printing. (Default = ipp/lp1) *Wird verwendet, wenn als Übertragungsmethode 'IPP' gewählt wurde.*
SSL	De-/aktiviert die SSL-/TLS-Verschlüsselung für das IPP-Printing. Die Verschlüsselungsstärke wird über die Verschlüsselungsstufe definiert ⇨61. *Wird verwendet, wenn als Übertragungsmethode 'IPP' gewählt wurde.*
LPD-Queue	Definiert den Queue-Namen für das LPD-Printing. (Default = lp1) *Wird verwendet, wenn als Übertragungsmethode 'LPD' gewählt wurde.*
RFC	De-/aktiviert das RFC1179-konforme LPD-Printing. *Wird verwendet, wenn als Übertragungsmethode 'LPD' gewählt wurde. Ist diese Option deaktiviert, ähnelt das Verhalten dem Microsoft-LPD-Printing.*

6.4 Wie definiere ich Timeouts? (nur für Experten)

Sie haben die Möglichkeit, die Behandlung von Fehlerzuständen vor und während eines Druckauftrags durch Timeouts zu kontrollieren.

Druckerverbindungsabbruch

Der Parameter 'Druckerverbindungsabbruch' definiert den Zeitraum (in Sekunden), nach dem ein Verbindungsversuch zum Drucker abgebrochen werden soll. Der Abbruch eines Verbindungsversuchs ist zweckmäßig, wenn z.B. der Drucker für den TPR physikalisch nicht erreichbar ist und der ThinPrint-Port für nachfolgende Druckaufträge freigemacht werden soll.

Timeout für das Senden von Druckaufträgen

Der Parameter 'Timeout für das Senden von Druckaufträgen' definiert den Zeitraum (in Sekunden), nach dem ein laufender Druckauftrag abgebrochen werden soll. Der Abbruch eines Druckauftrags ist zweckmäßig, wenn aufgrund eines Druckerfehlers (z.B. kein Papier) der Druckauftrag nicht abgearbeitet werden kann.

Beide Timeouts bewirken, dass die Druckaufträge gelöscht werden. Beim 'reinen' ThinPrint-Drucken wird zusätzlich eine Fehlermeldung an den ThinPrint Server gesendet. Beim Drucken über den Connection Service erhält der ThinPrint Server keine Fehlermeldung.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - ThinPrint®** *an.*
3. *Geben Sie in den Feldern* **Druckerverbindungsabbruch** *und* **Timeout für das Senden von Druckaufträgen** *den Zeitraum in Sekunden ein, nach dem die Timeouts wirksam werden sollen (0 s = aus).*
4. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert.

6.5 Wie erhalte ich Statusinformationen zur Druckerverbindung?

Sie können den Verbindungsstatus des eingebundenen Druckers abfragen lassen. Dafür müssen Sie eine 'ping'-Abfrage konfigurieren.

Nutzen und Zweck

Der Verbindungsstatus des eingebundenen Druckers wird im TPR Control Center angezeigt:

Verbindungsstatus	Beschreibung
Timeout	Die Verbindung zum Drucker ist zurzeit nicht vorhanden. Zuvor war eine Verbindung vorhanden.
erreichbar	Die Verbindung zum Drucker ist zurzeit vorhanden.
nicht erreichbar	Es konnte bislang keine Verbindung zum Drucker hergestellt werden.
Unbekannt	Der Verbindungsstatus zum Drucker kann nicht festgestellt werden.

Die Druckstatus-LED am TPR signalisiert ebenfalls den Verbindungsstatus; siehe: 'Quick Installation Guide'.

Sind die Abfragen über ping und SNMP (⇨55) deaktiviert, leuchtet die LED nicht.

Was möchten Sie tun?

- ☐ ''ping'-Abfrage via TPR Control Center konfigurieren' ⇨55
- ☐ 'Druckerverbindungsstatus via TPR Control Center anzeigen' ⇨55

'ping'-Abfrage via TPR Control Center konfigurieren

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - ThinPrint®-Drucker** *an.*
3. *Aktivieren Sie die Option* **Überwachung über Ping**.
4. *Geben Sie im Feld* **Überwachungsintervall** *das Abfrage-Intervall in Sekunden ein.*
5. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

Druckerverbindungsstatus via TPR Control Center anzeigen

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - ThinPrint®-Drucker** *an.*

↳ Der Druckerverbindungsstatus wird unter 'ThinPrint®-Druckerstatus' in der Zeile **'Status'** angezeigt.

6.6 Wie erhalte ich Druckermeldungen?

Sie können Druckerfehlermeldungen (Kein Papier, Offline, Papierstau usw.) und Druckerstatusmeldungen (Ruhezustand, Aufwärmphase usw.) abfragen lassen. Dafür müssen Sie eine SNMP-Abfrage konfigurieren.

Nicht alle Drucker unterstützen SNMP. Nähere Informationen finden Sie im Druckerhandbuch.

Nutzen und Zweck

Die Druckermelden des eingebundenen Druckers werden im TPR Control Center angezeigt. Die Druckstatus-LED am TPR signalisiert ebenfalls Druckermeldungen; siehe: 'Quick Installation Guide'.

Sind die Abfragen über SNMP und ping (⇨🗎54) deaktiviert, leuchtet die LED nicht.

Was möchten Sie tun?

- ☐ 'SNMP-Abfrage via TPR Control Center konfigurieren' ⇨🗎56
- ☐ 'Druckermeldungen via TPR Control Center anzeigen' ⇨🗎56

SNMP-Abfrage via TPR Control Center konfigurieren

Voraussetzung

☑ Der Drucker unterstützt SNMP.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - ThinPrint®-Drucker** *an.*
3. *Aktivieren Sie die Option* **SNMP**.
4. *Geben Sie im Feld* **Überwachungsintervall** *das Abfrage-Intervall in Sekunden ein.*
5. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

Druckermeldungen via TPR Control Center anzeigen

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - ThinPrint®-Drucker** *an.*

↳ Die Druckermeldungen werden unter 'ThinPrint®-Druckerstatus' in der Zeile **'Status'** angezeigt.

6.7 Wie verwende ich den ThinPrint Connection Service?

Der ThinPrint Connection Service ermöglicht u.a. das Zustellen von Druckaufträgen über TCP/IP an ThinPrint Clients (also den TPR) in maskierten Netzwerken (NAT).

Der Connection Service übernimmt die gesamte Kommunikation von Anwendungen des ThinPrint Servers zum jeweiligen Client. Dabei wird sowohl die Verbindung über maskierte Netzwerke ermöglicht wie auch die Zuordnung des jeweiligen Druckauftrages zum entsprechenden Zielgerät gemanagt.

Um diesen Dienst zu nutzen, muss der TPR vorbereitet werden. Für jedes Endgerät, das den Connection Service nutzt, müssen Sie eine Client-ID inkl. eines Authentifizierungsschlüssels in der Datenbank des Connection Services hinterlegen. Diese beiden Werte müssen auch im TPR eingerichtet werden.

Beachten Sie, dass Sie für jede Client-ID eine ThinPrint-Lizenz benötigen.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - ThinPrint®** *an.*
3. *Aktivieren Sie die Option* **Connection Service**.
4. *Geben Sie in den Feldern die entsprechenden Parameter ein; siehe: Tabelle 13* ⇨🗎***58***.
5. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert.

Tabelle 13: Connection Service-Parameter

Parameter	Beschreibung
Connection Service	De-/aktiviert den ThinPrint Connection Service
Servername	IP-Adresse oder Hostname des Servers, auf dem der Connection Service installiert ist. *Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.*
Port	Definiert den TCP-Port, über den der TPR mit dem Connection Service kommuniziert. *Die Portnummer 4001 ist voreingestellt.*
Client-ID	Client-ID, mit der der TPR in der Datenbank des Connection Services hinterlegt ist. Der Connection Service benötigt die Client-ID, um Druckaufträge an den TPR zu senden.
Authentifizierungsschlüssel	Authentifizierungsschlüssel, mit dem der TPR in der Datenbank des Connection Services hinterlegt ist.
Keep alive	Intervall (in Sekunden) mit dem die Verbindung zum Connection Service aktualisiert wird. Der Wert muss genauso groß wie oder kleiner als der auf dem Connection Service-Server eingestellte Wert 'KeepAliveTO' sein. *(Erlaubte Eingabe 1–60000 | Default = 60)*
Erneuter Verbindungsversuch	Definiert das Zeitintervall (in Sekunden), nach dem ein erneuter Verbindungsversuch stattfindet, wenn der Connection Service nicht erreichbar ist. *(Erlaubte Eingabe 1–60000 | Default = 120)*

Der Verbindungsstatus wird in der Tabelle 'ThinPrint®-Status' angezeigt. Wird die Verbindung zum Connection Service abgelehnt, ist ein Wert (Client-ID, Authentifizierungsschlüssel, Port oder Servername) falsch gesetzt. Überprüfen und ändern Sie in diesem Fall Ihre Einstellungen und wählen Sie die Schaltfläche **Speichern** an.

6.8 Wie empfängt der TPR verschlüsselte Daten?

Eine sichere Verbindung beim Versenden von Druckaufträgen zwischen ThinPrint (Server oder Connection Service) und dem TPR wird durch den Einsatz einer SSL-/TLS-Verschlüsselung ermöglicht. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨61.

Der ThinPrint Server fordert vom TPR ein Zertifikat an. Anhand des Zertifikats überprüft der ThinPrint Server, ob der TPR berechtigt ist, die Druckdaten zu empfangen.

Wenn beim ThinPrint Server eine Verschlüsselung aktiviert ist, muss sowohl auf dem ThinPrint Server als auch auf dem TPR ein Zertifikat von einer übereinstimmenden CA (Certification Authority) installiert sein. Um das Empfangen von verschlüsselten Druckdaten auf dem TPR zu ermöglichen, gehen Sie wie folgt vor:

- Erstellen Sie eine Zertifikatsanforderung; siehe: ⇨74.
- Speichern Sie das angeforderte Zertifikat auf dem TPR; siehe: ⇨75.

7 Sicherheit

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

Welche Information benötigen Sie?

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

- 'Wie definiere ich die Verschlüsselungsstärke für SSL-/TLS-Verbindungen?' ⇨ 61
- 'Wie verschlüssele ich die Verbindung zum TPR Control Center?' ⇨ 64
- 'Wie kontrolliere ich den Zugang zum TPR Control Center? (Benutzerkonten)' ⇨ 65
- 'Wie sperre ich einzelne Ports?' ⇨ 67
- 'Wie kontrolliere ich den Zugriff auf den TPR? (TCP-Portzugriffskontrolle)' ⇨ 68
- 'Wie setze ich Zertifikate korrekt ein?' ⇨ 70
- 'Wie verwende ich Authentifizierungsmethoden?' ⇨ 79
- 'Wie richte ich eine Gerätezuordnung ein?' ⇨ 86

Zusätzlich kann das TPR 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?' ⇨ 30.

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

Sie haben die Möglichkeit, folgende Verbindungen am TPR via SSL/TLS zu verschlüsseln:

- E-Mail: POP3 (⇨🗎32)
- E-Mail: SMTP (⇨🗎32)
- Personal Printing: Verbindung zum Server (⇨🗎45)
- ThinPrint-Drucker: IPP-Verbindung (⇨🗎51)
- ThinPrint: Verschlüsselung von Daten (⇨🗎59)
- Webzugang zum TPR Control Center: HTTPS (⇨🗎65)

Verschlüsselungsstärke

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

Protokoll

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

Verschlüsselungsstufe

Jede Verschlüsselungsstufe stellt eine Sammlung sog. Cipher Suites dar. Eine Cipher Suite ist eine standardisierte Folge aus vier kryptografischen Algorithmen, die zum Aufbau einer sicheren Verbindung verwendet werden. Cipher Suites werden gemäß ihrer Verschlüsselungsstärke zu einer Verschlüsselungsstufe zusammengefasst. Welche Cipher Suites vom TPR unterstützt werden, also Teil einer Verschlüsselungsstufe sind, hängt vom verwendeten SSL-/TLS-Protokoll ab.

Folgende Verschlüsselungsstufen sind wählbar:

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

- **Hoch: Es werden nur Cipher Suites mit einer starken Verschlüsselung verwendet. (Langsame Übertragung)**

Verbindungsaufbau

Beim Aufbau einer sicheren Verbindung wird das zu verwendende Protokoll sowie eine Liste von unterstützten Cipher Suites an den Kommunikationspartner gesendet. Es wird eine Cipher Suite ausgehandelt, die im Weiteren verwendet wird. Standardmäßig handelt es sich um die stärkste von beiden Parteien unterstützte Cipher Suite. Unterstützt der Kommunikationspartner das gewählte Protokoll nicht und/oder gibt es keine von beiden Seiten unterstützte Cipher Suite, wird keine SSL-/TLS-Verbindung aufgebaut.

Die Kommunikationspartner des TPR (z.B. Browser, ThinPrintServer) müssen das Verschlüsselungsprotokoll und die Cipher Suites der gewählten Verschlüsselungsstufe für einen erfolgreichen Verbindungsaufbau unterstützen. Bei Problemen wählen Sie andere Einstellungen oder setzen die TPR-Parameter zurück; siehe: ⇨🗎91.

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

Gehen Sie wie folgt vor:

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

Verwenden Sie nicht das Verschlüsselungsprotokoll 'SSL', wenn Sie aktuelle Browser-Software nutzen und für den Webzugang zum TPR Control Center ausschließlich HTTPS als erlaubter Ver-

bindungstyp definiert ist. Aktuelle Browser unterstützen SSL nicht, somit kann keine Verbindung aufgebaut werden.

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

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

5. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellung wird gespeichert.

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

7.2 Wie verschlüssele ich die Verbindung zum TPR Control Center?

Verbindungstyp (HTTP/HTTPS)

Die Verbindung zum TPR Control Center kann durch die Wahl der erlaubten Verbindungstypen (HTTP/HTTPS) gesichert werden.

Wird ausschließlich HTTPS als Verbindungstyp gewählt, ist die Verbindung zum TPR Control Center via SSL/TLS verschlüsselt. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert (⇨61).

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

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

Gehen Sie wie folgt vor:

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

Die Einstellung wird gespeichert.

7.3 Wie kontrolliere ich den Zugang zum TPR Control Center? (Benutzerkonten)

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

Benutzerkonten

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

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

Die Benutzerkonten werden auch für SNMP verwendet; siehe: ⇨30.

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

Login

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

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

Sitzungs-Timeout

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

Gehen Sie wie folgt vor:

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

Die Einstellungen werden gespeichert.

7.4 Wie sperre ich einzelne Ports?

Der TPR kann nicht direkt von Viren befallen werden. Lediglich durch Angriffe auf offene Ports kann der TPR beeinflusst und in seiner Funktion beeinträchtigt werden.

Um Angriffe auf offene Ports zu verhindern, ist es möglich, einzelne Ports am TPR zu sperren. Eingerichtet werden können z.B. kurzfristige Sperrungen für aktuelle Sicherheitsprobleme (Würmer usw.) oder langfristige Sperrungen gängiger Ports für Malware-Angriffe.

Dienste (z.B. Drucken via IPP/Port 632) lassen sich ebenfalls über die Sperrung ihres Ports blockieren.

Lokale Service-Ports (⇨🗎39) können nicht gesperrt werden.

Gehen Sie wie folgt vor:

1. *Wählen Sie den Menüpunkt* **SICHERHEIT - Portsperrung an**.
2. *Geben Sie im Feld* **Port** *die Portnummer des zu sperrenden Ports ein.*
3. *Aktivieren Sie die Optionen für die Sperrung der gewünschten Protokolltypen und Schnittstellen.*
   (Beide Protokolltypen und Schnittstellen können gleichzeitig gesperrt werden.)
4. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellung wird gespeichert.

Um alle TCP- oder IP-Ports zu sperren, siehe: 'Wie kontrolliere ich den Zugriff auf den TPR? (TCP-Portzugriffskontrolle)' ⇨🗎68.

7.5 Wie kontrolliere ich den Zugriff auf den TPR? (TCP-Portzugriffskontrolle)

TCP-Portzugriffskontrolle

Sie haben die Möglichkeit, den Zugriff auf den TPR zu kontrollieren. Hierzu können verschiedene TCP-Porttypen am TPR gesperrt werden. Zugriffsberechtigte Netzwerkelemente können als Ausnahme definiert und von der Sperrung ausgenommen werden. Der TPR 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:

- TCP-Zugriff sperren (Sperrt TCP-Ports: HTTP/HTTPS/...)
- 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 (Hardware-Adressen) 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 TPR 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 TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - TCP-Portzugriff an**.
3. *Aktivieren Sie die Option* **Portzugriff kontrollieren**.
4. *Wählen Sie im Bereich* **Sicherheitsstufe** *den gewünschten Schutz.*
5. *Definieren Sie im Bereich* **Ausnahmen** *die Netzwerkelemente, die von der Portsperrung ausgeschlossen sind. Geben Sie hierzu die IP- oder MAC-Adressen ein und aktivieren Sie die Optionen.*
6. *Stellen Sie sicher, dass der* **Testmodus** *aktiviert ist.*
7. *Bestätigen Sie mit* **Speichern & Neustart**.
   Die Einstellungen werden gespeichert.
   Die Portzugriffskontrolle ist bis zum Geräte-Neustart aktiv.
8. *Überprüfen Sie den Portzugriff und die Konfigurationsfähigkeit des TPR.*

Kann der TPR über das TPR Control Center nicht mehr erreicht werden, initiieren Sie einen Geräte-Neustart; siehe: ⇨ 94.

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

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

7.6 Wie setze ich Zertifikate korrekt ein?

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

Was sind Zertifikate?

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

Nutzen und Zweck

Mit dem Einsatz von Zertifikaten werden mehrere Sicherheitsmechanismen realisiert. Verwenden Sie Zertifikate im TPR,

- um die Verbindung zum Personal-Printing-Server zu verschlüsseln; siehe: ⇨🗎45.
- um die Identität des Personal-Printing-Servers überprüfen zu lassen; siehe: ⇨🗎46.
- um verschlüsselte Druckdaten zu empfangen; siehe: ⇨🗎59.
- um die Identität des TPR im Netzwerk überprüfen zu lassen; siehe: 'EAP-TLS konfigurieren' ⇨🗎80.
- um den TPR/den Client zu authentifizieren, wenn der administrative Webzugang zum TPR Control Center via HTTPS (SSL/TLS) geschützt ist; siehe: ⇨🗎65.

Wenn Sie Zertifikate verwenden, sollten Sie den administrativen Webzugriff zum TPR Control Center zusätzlich einschränken, so dass kein Unbefugter Zertifikate auf dem TPR löschen kann; siehe: ⇨🗎65.

Welche Zertifikate gibt es?

Im TPR können sowohl selbstsignierte Zertifikate als auch fremdsignierte Zertifikate verwendet werden. Es werden die folgenden Zertifikate unterschieden:

- Bei Auslieferung ist im TPR ein Zertifikat gespeichert, das sog. **Default-Zertifikat**. Sie sollten das Default-Zertifikat zeitnah durch ein selbstsigniertes oder ein angefordertes Zertifikat ersetzen.

- **Selbstsignierte Zertifikate** tragen eine digitale Unterschrift, die vom TPR erstellt wurde. Wird ein selbstsigniertes Zertifikat verwendet, kann von einem ThinPrint Server nicht via SSL/TLS gedruckt werden. Die Verbindung zum Personal-Printing-Server und die Prüfung seiner Identität sind ebenfalls nicht möglich. Hierzu ist zwingend ein CA-Zertifikat erforderlich.
- Ein **angefordertes Zertifikat** wird auf Basis einer Zertifikatsanforderung von einer Zertifizierungsstelle (Certification Authority - CA) für den TPR erstellt.
- **CA-Zertifikate** sind Zertifikate, die für eine Zertifizierungsstelle (Certification Authority - CA) ausgestellt wurden. Mit ihnen werden Zertifikate überprüft, die von der jeweiligen Zertifizierungsstelle ausgegeben wurden.
- S/MIME-Zertifikate (*.pem-Datei) werden verwendet zum Signieren und Verschlüsseln der E-Mails, die vom TPR versendet werden. Der zugehörige private Schlüssel ist im PKCS#12-Format (als *.p12-Datei) im vorgesehenen E-Mail-Programm (Thunderbird, Outlook usw.) als eigenes Zertifikat zu installieren. Nur damit können die E-Mails verifiziert (bzw. im Falle der Verschlüsselung) angesehen werden.
- **Personal-Printing-Zertifikate** werden verwendet zur Überprüfung der Identität des Personal-Printing-Servers.

Im TPR können folgende Zertifikate zeitgleich installiert sein:

- 1 Selbstsigniertes Zertifikat
- 1 Client-Zertifikat, d.h. 1 angefordertes Zertifikat ODER 1 PKCS#12-Zertifikat
- 1 S/MIME-Zertifikat
- 1–32 CA-Zertifikate
- 1 Personal-Printing-Zertifikat

Alle Zertifikate können separat gelöscht werden.

Abb. 6: TPR Control Center - Zertifikate

Was möchten Sie tun?

- ☐ 'Zertifikat anzeigen' ⇨🗎72
- ☐ 'Selbstsigniertes Zertifikat erstellen' ⇨🗎73
- ☐ 'Zertifikatsanforderung für ein angefordertes Zertifikat erstellen' ⇨🗎74
- ☐ 'Angefordertes Zertifikat auf dem TPR speichern' ⇨🗎75
- ☐ 'PKCS#12-Zertifikat auf dem TPR speichern' ⇨🗎75
- ☐ 'S/MIME-Zertifikat auf dem TPR speichern' ⇨🗎76
- ☐ 'CA-Zertifikat auf dem TPR speichern' ⇨🗎77
- ☐ 'Personal-Printing-Zertifikat auf dem TPR speichern' ⇨🗎77
- ☐ 'Zertifikat löschen' ⇨🗎78

Zertifikat anzeigen

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

Voraussetzung

☑ Auf dem TPR ist ein Zertifikat installiert.

Gehen Sie wie folgt vor:

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

↳ Das Zertifikat wird angezeigt.

Selbstsigniertes Zertifikat erstellen

Ist bereits ein selbstsigniertes Zertifikat auf dem TPR erstellt worden, muss dieses zunächst gelöscht werden; siehe: ⇨78.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Zertifikate an**.
3. *Wählen Sie die Schaltfläche* **Selbstsigniertes Zertifikat** *an.*
4. *Geben Sie die entsprechenden Parameter ein; siehe: Tabelle 14 ⇨73.*
5. *Wählen Sie die Schaltfläche* **Erstellen/Installieren** *an.*

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

Tabelle 14: 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 TPR zu verwenden, um eine eindeutige Zuordnung des Zertifikats zum TPR zu ermöglichen. *Maximal 64 Zeichen können eingegeben werden.*
E-Mail-Adresse	Gibt eine E-Mail-Adresse an. Maximal 40 Zeichen können eingegeben werden. *(Optionale Eingabe)*
Organisation	Gibt den Namen der Firma an, die den TPR einsetzt. *Maximal 64 Zeichen können eingegeben werden.*
Unternehmensbereich	Gibt die Abteilung oder eine Untergruppe der Firma an. *Maximal 64 Zeichen können eingegeben werden. (Optionale Eingabe)*
Ort	Gibt den Ort an, an dem die Firma ansässig ist. *Maximal 64 Zeichen können eingegeben werden.*
Bundesland	Gibt den Namen des Bundeslandes an, in dem die Firma ansässig ist. *Maximal 64 Zeichen können eingegeben werden. (Optionale Eingabe)*
Domain-Komponente	Ermöglicht das Eintragen weiterer Attribute. *(Optionale Eingabe)*

Parameter	Beschreibung
Land	Gibt das Land an, in dem die Firma ansässig ist. Geben Sie das zweistellige Länderkürzel gemäß ISO 3166 ein. Beispiele: DE = Deutschland, GB = Großbritannien, US = USA
Ausgestellt am	Gibt das Datum an, ab dem das Zertifikat gültig ist.
Endet am	Gibt das Datum an, an dem das Zertifikat ungültig wird.
RSA-Schlüssellänge	Definiert die Länge des verwendeten RSA-Schlüssels: - 512 Bit (schnelle Ver- und Entschlüsselung) - 768 Bit - 1024 Bit (standardmäßige Ver- und Entschlüsselung) - 2048 Bit (langsame Ver- und Entschlüsselung)

Zertifikatsanforderung für ein angefordertes Zertifikat erstellen

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

Ist bereits eine Zertifikatsanforderung erstellt, muss diese zunächst gelöscht werden; siehe: ⇨78.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Zertifikate** *an.*
3. *Wählen Sie die Schaltfläche* **Zertifikatsanforderung** *an.*
4. *Geben Sie die benötigten Parameter ein; siehe: Tabelle 14 ⇨73.*
5. *Wählen Sie die Schaltfläche* **Anforderung erstellen** *an.*
   Die Zertifikatsanforderung wird erstellt. Dieser Vorgang kann einige Minuten dauern.
6. *Wählen Sie die Schaltfläche* **Upload** *an und speichern Sie die Anforderung in einer Textdatei.*

7. *Wählen Sie die Schaltfläche* **OK** *an.*
8. *Senden Sie die Textdatei als Zertifikatsanforderung an eine Zertifizierungsstelle.*

Nach Erhalt muss das angeforderte Zertifikat auf dem TPR gespeichert werden; siehe: ⇨ 75.

Angefordertes Zertifikat auf dem TPR speichern

Voraussetzung

☑ Es wurde zuvor eine entsprechende Zertifikatsanforderung erstellt; siehe: ⇨ 74.

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

Ist bereits ein angefordertes Zertifikat installiert, muss dieses zunächst gelöscht werden; siehe: ⇨ 78.

Gehen Sie wie folgt vor:

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

↳ Das angeforderte Zertifikat wird auf dem TPR gespeichert.

PKCS#12-Zertifikat auf dem TPR speichern

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

Ist bereits ein PKCS#12-Zertifikat auf dem TPR installiert, muss dieses zunächst gelöscht werden; siehe: ⇨ 78

Voraussetzung

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

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Zertifikate** *an.*
3. *Wählen Sie die Schaltfläche* **PKCS#12-Zertifikat** *an.*
4. *Wählen Sie die Schaltfläche* **Durchsuchen** *an.*
5. *Geben Sie das PKCS#12-Zertifikat an.*
6. *Geben Sie das Passwort ein.*
7. *Wählen Sie die Schaltfläche* **Installieren** *an.*

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

S/MIME-Zertifikat auf dem TPR speichern

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

Ist bereits ein S/MIME-Zertifikat auf dem TPR installiert, muss dieses zunächst gelöscht werden; siehe: ⇨📄78.

Voraussetzung

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

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Zertifikate** *an.*
3. *Wählen Sie die Schaltfläche* **S/MIME-Zertifikat** *an.*
4. *Wählen Sie die Schaltfläche* **Durchsuchen** *an.*
5. *Geben Sie das S/MIME-Zertifikat an.*
6. *Wählen Sie die Schaltfläche* **Installieren** *an.*

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

Personal-Printing-Zertifikat auf dem TPR speichern

Personal-Printing-Zertifikate werden zur Überprüfung der Identität des Personal-Printing-Servers verwendet (⇨ 46).

Ist bereits ein Personal-Printing-Zertifikat auf dem TPR installiert, uss dieses zunächst gelöscht werden; siehe: ⇨ 78.

Voraussetzung

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

Gehen Sie wie folgt vor:

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

↳ Das Personal-Printing-Zertifikat wird auf dem TPR gespeichert.

CA-Zertifikat auf dem TPR speichern

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

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

Beispiel: Um in einem Netzwerk die Identität des TPRs zu überprüfen, bietet der TPR mehrere Authentifizierungsverfahren an. Wenn Sie das Authentifizierungsverfahren 'EAP-TLS' (⇨ 80) verwenden, ist es erforderlich, das Wurzel-CA-Zertifikat der Zertifizierungsstelle auf dem TPR zu installieren, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat.

Voraussetzung

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

Gehen Sie wie folgt vor:

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

↳ Das CA-Zertifikat wird auf dem TPR gespeichert.

Zertifikat löschen

Löschen Sie nicht das Zertifikat (CA/selbstsigniert/PKCS#12), wenn für den Webzugang zum TPR Control Center ausschließlich HTTPS als erlaubter Verbindungstyp definiert ist. Wird das zugehörige Zertifikat gelöscht, kann das TPR Control Center nicht mehr erreicht werden. Setzen Sie in diesem Fall die TPR-Parameter zurück; siehe: ⇨91.

Voraussetzung

☑ Auf dem TPR ist ein Zertifikat installiert.

Gehen Sie wie folgt vor:

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

↳ Das Zertifikat wird gelöscht.

7.7 Wie verwende ich Authentifizierungsmethoden?

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

Was ist IEEE 802.1X?

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

Was ist EAP?

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

Was ist RADIUS?

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

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

Was möchten Sie tun?

- ☐ 'EAP-MD5 konfigurieren' ⇨🗎80
- ☐ 'EAP-TLS konfigurieren' ⇨🗎80
- ☐ 'EAP-TTLS konfigurieren' ⇨🗎82
- ☐ 'PEAP konfigurieren' ⇨🗎83
- ☐ 'EAP-FAST konfigurieren' ⇨🗎84

EAP-MD5 konfigurieren

Nutzen und Zweck

Das EAP-MD5 überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit der TPR in geschützten Netzwerken einen Zugriff erhält, haben Sie die Möglichkeit, den TPR 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 TPR als Benutzer (mit einem Benutzernamen und einem Passwort) angelegt. Anschließend wird das EAP-MD5-Authentifizierungsverfahren auf dem TPR aktiviert und die beiden Benutzerangaben (Benutzername und Passwort) werden eingegeben.

Voraussetzung

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

Gehen Sie wie folgt vor:

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

↳ Die Einstellungen werden gespeichert.

EAP-TLS konfigurieren

Nutzen und Zweck

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

Funktionsweise

EAP-TLS beschreibt eine zertifikatbasierte Authentifizierung über einen RADIUS-Server. Hierzu werden zwischen dem TPR und dem

RADIUS-Server Zertifikate ausgetauscht. Dabei wird eine verschlüsselte TLS-Verbindung zwischen TPR und RADIUS-Server aufgebaut. Sowohl RADIUS-Server als auch TPR benötigen ein gültiges digitales von einer CA unterschriebenes Zertifikat, das diese gegenseitig überprüfen müssen. Ist die beidseitige Authentisierung erfolgreich, wird der Zugang freigegeben.

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

Um eine EAP-TLS-Authentifizierung anzuwenden, stellen Sie sicher, dass die unten aufgeführten Punkte in der angegebenen Reihenfolge erfüllt werden. Wird die Vorgehensweise nicht eingehalten, kann der TPR im Netzwerk möglicherweise nicht angesprochen werden. Setzen Sie in diesem Fall die TPR-Parameter zurück; siehe: ⇨📄91.

Vorgehensweise

- Erstellen Sie auf dem TPR eine Zertifikatsanforderung; siehe: ⇨📄74.
- Erstellen Sie mit der Zertifikatsanforderung und mit Hilfe des Authentifizierungsservers ein Zertifikat.
- Installieren Sie das angeforderte Zertifikat auf dem TPR; siehe: ⇨📄75.
- Installieren Sie das Wurzel-CA-Zertifikat der Zertifizierungsstelle auf den TPR, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat; siehe: 'CA-Zertifikat auf dem TPR speichern' ⇨📄77.
- Aktivieren Sie das Authentifizierungsverfahren 'EAP-TLS' auf dem TPR.

Gehen Sie wie folgt vor:

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

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

↳ Die Einstellungen werden gespeichert.

EAP-TTLS konfigurieren

Nutzen und Zweck

Das EAP-TTLS (Tunneled Transport Layer Security) überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit der TPR in geschützten Netzwerken einen Zugriff erhält, haben Sie die Möglichkeit, den TPR 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 TPR und RADIUS-Server aufgebaut. Dazu identifiziert sich nur der RADIUS-Server mit einem von einer CA unterschriebenen Zertifikat beim TPR. 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 TPR als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

Gehen Sie wie folgt vor:

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

4. *Geben Sie Benutzername und Passwort ein, mit denen der TPR auf dem RADIUS-Server eingerichtet ist.*
5. *Wählen Sie die Einstellungen, mit denen die Kommunikation im TLS-Tunnel gesichert werden soll.*
6. *Um die Sicherheit beim Verbindungsaufbau zu erhöhen, installieren Sie optional ein Wurzel-CA-Zertifikat der Zertifizierungsstelle auf den TPR, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat; siehe: 'CA-Zertifikat auf dem TPR speichern' ⇨🗎77.*
   Wählen Sie anschließend in der Liste **EAP-Wurzelzertifikat** *das Wurzel-CA-Zertifikat aus.*
7. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

PEAP konfigurieren

Nutzen und Zweck

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

Funktionsweise

Beim PEAP wird (wie bei EAP-TTLS, vgl. ⇨🗎82) zunächst ein verschlüsselter TLS-Tunnel (Transport Layer Security) zwischen TPR und RADIUS-Server aufgebaut. Dazu identifiziert sich nur der RADIUS-Server mit einem von einer CA unterschriebenen Zertifikat beim TPR.

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 TPR als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **SICHERHEIT - Authentifizierung** *an.*
3. *Wählen Sie aus der Liste* **Authentifizierungsmethode** *den Eintrag* **PEAP**.
4. *Geben Sie Benutzername und Passwort ein, mit denen der TPR auf dem RADIUS-Server eingerichtet ist.*
5. *Wählen Sie die Einstellungen, mit denen die Kommunikation im TLS-Tunnel gesichert werden soll.*
6. *Um die Sicherheit beim Verbindungsaufbau zu erhöhen, installieren Sie optional ein Wurzel-CA-Zertifikat der Zertifizierungsstelle auf den TPR, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat; siehe: 'CA-Zertifikat auf dem TPR speichern' ⇨🗎77.*
   Wählen Sie anschließend in der Liste **EAP-Wurzelzertifikat** *das Wurzel-CA-Zertifikat aus.*
7. *Bestätigen Sie mit* **Speichern & Neustart**.

↳ Die Einstellungen werden gespeichert.

EAP-FAST konfigurieren

Nutzen und Zweck

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

Funktionsweise

EAP-FAST nutzt (wie EAP-TTLS, vgl. ⇨🗎82) einen Tunnel zum Schutz der Datenübertragung. Der Hauptunterschied besteht darin, dass EAP-FAST keine Zertifikate zum Authentifizieren benötigt. (Die Verwendung von Zertifikaten ist optional.)

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

- Einen gemeinsamen geheimen Schlüssel, der den zwischen dem TPR und dem RADIUS-Server geteilten Schlüssel enthält.
- Ein undurchsichtiges Element, das dem TPR zur Verfügung steht und dem RADIUS-Server vorgelegt wird, wenn der TPR 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 TPR sowie die Lieferung der PACs zu schützen.

Voraussetzung

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

Gehen Sie wie folgt vor:

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

Die Einstellungen werden gespeichert.

7.8 Wie richte ich eine Gerätezuordnung ein?

Man-In-The-Middle-Angriff

Bei einem Man-In-The-Middle-Angriff schaltet sich ein unsichtbarer Angreifer in den Kommunikationskanal zwischen zwei Kommunikationspartnern. Der Angreifer kann den Datenverkehr einsehen und manipulieren.

Schutz

Sie haben die Möglichkeit, den Kommunikationskanal zwischen TPR und Drucker durch eine Gerätezuordnung vor einem Man-in-the-Middle-Angriff zu schützen.

Bei der Gerätezuordnung wird dem Netzwerkdrucker ein TPR fest zugewiesen. Der TPR ist dann ausschließlich in Kombination mit dem zugewiesenen Netzwerkdrucker zu betreiben. Der Datenverkehr lässt nicht über einen zwischengeschalteten Angreifer leiten und ist geschützt.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **GERÄT - ThinPrint®-Drucker**.
3. *Aktivieren Sie die Option* **Gerätezuordnung**.
4. *Bestätigen Sie mit* **Speichern**.

Die Einstellungen werden gespeichert.

8 Wartung

Am TPR können verschiedene Wartungsmaßnahmen durchgeführt werden. Dieses Kapitel gibt einen Überblick.

Welche Information benötigen Sie?

8.1 Wie sichere ich die TPR-Parameter? (Backup)

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

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

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

Was möchten Sie tun?

Parameterwerte anzeigen

Gehen Sie wie folgt vor:

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

↳ Die aktuellen Parameterwerte werden angezeigt.

Detaillierte Beschreibungen zu den Parametern entnehmen Sie der 'Parameterliste' ⇨103.

Parameterdatei sichern

Gehen Sie wie folgt vor:

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

↳ Die Parameterdatei wird kopiert und ist gesichert.

Parameterdatei auf einen TPR laden

Gehen Sie wie folgt vor:

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

↳ Die in der Datei enthaltenen Parameterwerte werden von dem TPR übernommen.

Sie haben zudem die Möglichkeit, eine Parameterdatei von einem USB-Stick automatisch auf einen TPR zu laden; siehe: ⇨89.

8.2 Wie verwende ich ein angeschlossenes USB-Gerät?

Sie haben die Möglichkeit, einen USB-Stick an den USB-Port des TPR anzuschließen, um zusätzliche TPR-Funktionen zu nutzen.

Parameter-Backup

Beim 'Parameter-Backup' wird die Datei '<Default-Name>_parameter.txt' automatisch auf dem USB-Stick gespeichert und nach einer Parameteränderung aktualisiert. Die Datei enthält alle Parameterwerte des TPR (Ausnahme: Passwörter). TPR übernehmen die in der Parameterdatei auf dem USB-Stick enthaltenen Werte automatisch sobald das Gerät neu startet. Parameterwerte können so via USB-Stick einfach und schnell auf andere TPR geladen werden (z.B. bei der Konfiguration neuer Geräte).

Formatieren

Um den USB-Stick am TPR zu nutzen, muss der USB-Stick über das korrekte Dateisystem verfügen. Gegebenenfalls ist ein Formatieren des USB-Sticks erforderlich.

Ob ein Formatieren erforderlich ist, wird im TPR Control Center über den Menüpunkt 'WARTUNG' unter 'USB-Gerätestatus' angezeigt.

Was möchten Sie tun?

- ☐ 'USB-Stick formatieren' ⇨🗎89
- ☐ 'Parameterwerte automatisch speichern' ⇨🗎90
- ☐ 'Parameterwerte automatisch auf einen TPR laden' ⇨🗎90

USB-Stick formatieren

Beim Formatieren gehen alle auf dem USB-Stick befindlichen Daten unwiderruflich verloren.

Voraussetzung

☑ Es ist ein USB-Stick an den TPR angeschlossen.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - USB-Gerät** *an.*
3. *Wählen Sie die Schaltfläche* **Formatieren** *an.*

↳ Der USB-Stick wird formatiert.

Parameterwerte automatisch speichern

Voraussetzung

☑ Es ist ein USB-Stick an den TPR angeschlossen.

☑ Der USB-Stick ist korrekt formatiert; siehe: ⇨ 89.

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - USB-Gerät** *an.*
3. *Aktivieren Sie die Option* **Parameter-Backup**.
4. *Wählen Sie die Schaltfläche* **Speichern** *an.*

↳ Die Einstellungen werden gespeichert.

Parameterwerte automatisch auf einen TPR laden

Voraussetzung

☑ Der USB-Stick ist korrekt formatiert; siehe: ⇨ 89.

☑ Auf dem USB-Stick ist eine Parameterdatei vorhanden; siehe 'Parameter-Backup' ⇨ 89.

Gehen Sie wie folgt vor:

1. *Schließen Sie einen USB-Stick an den USB-Port des TPR an.*

↳ Die in der Datei enthaltenen Parameterwerte werden von dem TPR beim nächsten Neustart des Gerätes automatisch übernommen.

8.3 Wie setze ich die Parameter auf die Standardwerte zurück? (Reset)

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

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

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

Entfernen Sie vor dem Reset einen angeschlossenen USB-Stick. Ist auf dem USB-Stick eine Parameterdatei gespeichert, verwendet der TPR nach dem Reset automatisch die auf dem USB-Stick gespeicherten Parameterwerte (siehe: ⇨ 89).

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

Was möchten Sie tun?

- ☐ 'Parameter via TPR Control Center zurücksetzen' ⇨ 91
- ☐ 'Parameter via InterCon-NetTool zurücksetzen' ⇨ 92
- ☐ 'Parameter via Status-/Reset-Taster zurücksetzen' ⇨ 92

Parameter via TPR Control Center zurücksetzen

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - Standardeinstellung** *an.*

3. *Wählen Sie die Schaltfläche* **Standardeinstellung** *an.*

↳ Die Parameter werden zurückgesetzt.

Parameter via InterCon-NetTool zurücksetzen

Gehen Sie wie folgt vor:

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

↳ Die Parameter werden zurückgesetzt.

Parameter via Status-/Reset-Taster zurücksetzen

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

Über den Status-/Reset-Taster können Sie die Parameterwerte des TPR auf die Standardeinstellung zurücksetzen.

Gehen Sie wie folgt vor:

1. *Drücken Sie den Reset-Taster für 5 Sekunden.*
   Der TPR startet neu.

↳ Die Parameter sind zurückgesetzt.

Um das Zurücksetzen zu überprüfen, können Sie eine Serviceseite drucken. Drücken Sie hierzu kurz den Status-/Reset-Taster.

8.4 Wie führe ich ein Update aus?

Sie haben die Möglichkeit, Soft- und Firmware-Updates auf dem TPR 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 TPR. Die Versionsnummer entnehmen Sie der Startseite des TPR Control Centers oder der Geräteliste im InterCon-NetTool.

Wo finde ich Update-Dateien?

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

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

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

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - Update** *an.*
3. *Wählen Sie die Schaltfläche* **Durchsuchen** *an.*

4. *Geben Sie die Update-Datei an.*
5. *Wählen Sie die Schaltfläche* **Installieren** *an.*

↳ Das Update wird ausgeführt. Das TPR wird neu gestartet.

8.5 Wie starte ich den TPR neu?

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

Was möchten Sie tun?

- ☐ 'TPR via TPR Control Center neu starten' ⇨94
- ☐ 'TPR via InterCon-NetTool neu starten' ⇨94

TPR via TPR Control Center neu starten

Gehen Sie wie folgt vor:

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

↳ Der TPR wird neu gestartet.

TPR via InterCon-NetTool neu starten

Gehen Sie wie folgt vor:

1. *Starten Sie das InterCon-NetTool.*
2. *Markieren Sie den TPR in der Geräteliste.*
3. *Wählen Sie im Menü* **Aktionen** *den Befehl* **Neustart**.
   Der Dialog **Printserver-Neustart** *erscheint.*
4. *Wählen Sie die Schaltfläche* **Fertig stellen** *an.*

↳ Der TPR wird neu gestartet.

8.6 Wie drucke ich eine Status- oder Serviceseite?

Sie haben die Möglichkeit, Statusseiten oder Serviceseiten auf dem angeschlossenen Netzwerkdrucker auszudrucken. Beide Seiten sind in der englischen Sprache verfügbar.

Statusseite

Eine Statusseite enthält TPR-Basisinformationen wie Modelltyp, Hardware-Adresse, IP-Adresse, Subnetz-Maske, Gateway usw.

Serviceseite

Eine Serviceseite enthält TPR-Basisinformationen sowie eine Auflistung der aktuellen Parameterwerte des TPR.

Bevor eine Statusseite oder Serviceseite gedruckt wird, müssen die Druckfunktion aktiviert und das Datenformat der Status- bzw. Serviceseite (ASCII, PostScript, DATAMAX oder Citizen-Z) spezifiziert werden. Das Datenformat ASCII ist voreingestellt.

Was möchten Sie tun?

- ☐ 'Druckfunktion und Datenformat via TPR Control Center konfigurieren' ⇨📄95
- ☐ 'Statusseite via TPR Control Center drucken' ⇨📄96
- ☐ 'Serviceseite via TPR Control Center drucken' ⇨📄96
- ☐ 'Serviceseite via Status-/Reset-Taster drucken' ⇨📄96

Druckfunktion und Datenformat via TPR Control Center konfigurieren

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - Statusseite** *an.*
3. *Wählen Sie aus der Liste* **Modus Statusseite** *das gewünschte Datenformat.*
4. *Aktivieren Sie die Option* **Drucken**.
5. *Bestätigen Sie mit* **Speichern**.

↳ Die Einstellungen werden gespeichert.

Statusseite via TPR Control Center drucken

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - Statusseite** *an.*
3. *Wählen sie die Schaltfläche* **Statusseite** *an.*

↳ Die Statusseite wird gedruckt.

Serviceseite via TPR Control Center drucken

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - Statusseite** *an.*
3. *Wählen sie die Schaltfläche* **Serviceseite** *an.*

↳ Die Serviceseite wird gedruckt.

Serviceseite via Status-/Reset-Taster drucken

Über den Status-/Reset-Taster am Gerät können Sie eine Serviceseite ausdrucken.

Gehen Sie wie folgt vor:

1. *Drücken Sie kurz den Status-/Reset-Taster.*

↳ Die Serviceseite wird gedruckt.

8.7 Wie lasse ich die Job History anzeigen?

Sie haben die Möglichkeit, Informationen über die ThinPrint-Druckaufträge, die an den TPR gesendet wurden, anzeigen zu lassen. Nur diese Druckaufträge werden in der Job History aufgezeichnet und dargestellt.

Damit Datum und Uhrzeit korrekt angezeigt werden, muss ein Time-Server (⇨📄36) auf dem TPR konfiguriert sein. Ist kein Time-Server konfiguriert, entspricht der Zeitstempel der Defaultzeit.

Maximal 32 Druckaufträge werden angezeigt. Ab dem 33. Druckauftrag gilt das FIFO-Prinzip (First In - First Out). Durch Ausschalten oder Reset des TPR werden die gespeicherten Aufträge gelöscht. Sie können ebenfalls manuell gelöscht werden. Bei einem Neustart des TPR bleiben die Aufträge erhalten.

Was möchten Sie tun?

- ☐ 'Job History aufrufen' ⇨🗎97
- ☐ 'Aufträge manuell löschen' ⇨🗎98

Job History aufrufen

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - Job History** *an.*

↳ Die Job History wird angezeigt.

Folgende Informationen werden in der Job History angezeigt:

Information	Beschreibung
ID	Identifikationsnummer des Druckers, der den Druckauftrag gespoolt hat.
Status	Status der Druckverbindung. Folgende Status sind möglich: - Initialisiert: Es besteht eine Verbindung zum ThinPrint Server. Als nächster Schritt wird die Druckerverbindung aufgebaut. - Verbindungsversuch: Die Verbindung zum Drucker wird aufgebaut. - Verbindung abgewiesen: Der Drucker hat die Verbindung abgelehnt. - Erzeugt: Der Druckauftrag wurde vom TPR angenommen, aber die Datenübertragung zum Drucker hat noch nicht begonnen. - In Bearbeitung: Der Druckauftrag wird vom TPR an den Drucker übertragen. - Bearbeitung unterbrochen: Die Datenübertragung zum Drucker wurde unterbrochen. Dies kann z.B. entstehen, wenn im Drucker Papier fehlt. - Beendet: Der Druckauftrag wurde vom TPR vollständig an den Drucker weitergeleitet. - Abgebrochen: Der Druckauftrag wurde abgebrochen. Dies kann z.B. auftreten, wenn das TPR neu gestartet wurde, während der Druckauftrag bearbeitet wurde.

Information	Beschreibung
Protokoll	Protokoll, mit dem die Druckdaten übertragen wurden. Die Darstellung erfolgt in Form einer Kombination der folgenden Werte: - ThP: ThinPrint - Stp: Status- bzw. Serviceseite - Sock: RAW-/Socket-Printing - IPP: IPP-Printing - LPD: LPD-Printing
Name	Name des Druckauftrags
Sender	Name des sendenden Hosts: - '<Domain-User-Name>@<Domain>' erscheint bei ThinPrint-Druckaufträgen. - 'TPR-10' erscheint beim Drucken einer Status- oder Serviceseite.
Start	Zeitpunkt, an dem der Druckauftrag an den TPR gesendet wurde.
Größe	Größe des Druckauftrages in Kb.
Dauer	Bearbeitungsdauer, die der TPR zum Abwickeln des Druckauftrags benötigt hat.

Aufträge manuell löschen

Gehen Sie wie folgt vor:

1. *Starten Sie das TPR Control Center.*
2. *Wählen Sie den Menüpunkt* **WARTUNG - Job History** *an.*
3. *Wählen Sie die Schaltfläche* **Löschen** *an.*

Alle in der Job History gespeicherten Aufträge werden gelöscht.

9 Anhang

Der Anhang enthält ein Glossar, die TPR-Parameterliste, eine Problembehandlung sowie die Verzeichnislisten dieses Dokumentes.

Welche Information benötigen Sie?

9.1 Glossar

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

Welche Information benötigen Sie?

Herstellerspezifische Softwarelösungen

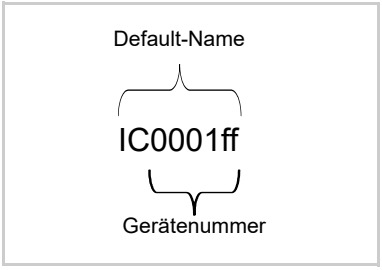
- 'InterCon-NetTool' ⇨🗎102
- 'TPR Control Center' ⇨🗎102

Netzwerktechnologie

- 'Default-Name' ⇨🗎100
- 'Gateway' ⇨🗎101
- 'Hardware-Adresse' ⇨🗎101
- 'Hostname' ⇨🗎101
- 'IP-Adresse' ⇨🗎102
- 'Netzwerkmaske' ⇨🗎102

Default-Name

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



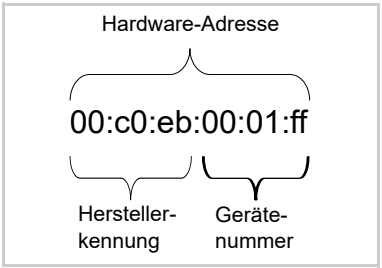
Der Default-Name kann im TPR Control Center, im InterCon-NetTool, auf der Statusseite oder auf der Serviceseite abgelesen werden.

Gateway

Über ein Gateway können IP-Adressen in einem anderen Netzwerk angesprochen werden. Möchten Sie ein Gateway verwenden, können Sie über das TPR Control Center oder InterCon-NetTool den entsprechenden Parameter im TPR konfigurieren.

Hardware-Adresse

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



Die Hardware-Adresse kann am Gehäuse, im InterCon-NetTool, auf der Statusseite oder auf der Serviceseite abgelesen werden.

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

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

Hostname

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

InterCon-NetTool

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

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 TPR gespeichert werden, damit er im Netzwerk angesprochen werden kann.

Netzwerkmaske

Mit Hilfe der Netzwerkmaske können große Netzwerke in Subnetzwerke unterteilt werden. Dabei werden die Teilnehmerkennungen der IP-Adresse verschiedenen Subnetzwerken zugeordnet.

Der TPR ist standardmäßig für den Einsatz ohne Subnetzwerke konfiguriert. Möchten Sie ein Subnetzwerk verwenden, können Sie über das TPR Control Center oder InterCon-NetTool den entsprechenden Parameter im TPR konfigurieren.

TPR Control Center

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

9.2 Parameterliste

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

Welche Information benötigen Sie?

Um die aktuellen Parameterwerte Ihres TPR einzusehen, siehe: 'Parameterwerte anzeigen' ⇨ 88 und 'Wie drucke ich eine Status- oder Serviceseite?' ⇨ 95.

Tabelle 15: Parameterliste - IPv4

Parameter	Wertekonvention	Default	Beschreibung
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-Adressenvergabe via ARP/PING.
ip_addr [IP-Adresse]	gültige IP-Adresse	169.254.0.0/16	Definiert die IP-Adresse des TPR.
ip_mask [Netzwerkmaske]	gültige IP-Adresse	255.255.0.0	Definiert die Netzwerkmaske des TPR.
ip_gate [Gateway]	gültige IP-Adresse	0.0.0.0	Definiert die Gateway-Adresse des TPR.

Tabelle 16: Parameterliste - IPv6

Parameter	Wertekonvention	Default	Beschreibung
ipv6 [IPv6]	on/off	on	De-/aktiviert die IPv6-Funktionalität des TPR.
ipv6_auto [Automatische Konfiguration]	on/off	on	De-/aktiviert die automatische Vergabe der IPv6-Adressen für den TPR.
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 TPR. *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 TPR seine 'Router Solicitations' (RS) sendet.

Parameter	Wertekonvention	Default	Beschreibung
ipv6_plen [Präfixlänge]	0–64 [1–2 Zeichen; 0–9]	64	Definiert die Länge des Subnetz-Präfixes für die IPv6-Adresse. *Adressbereiche werden durch Präfixe angegeben. Dazu wird die Präfixlänge (Anzahl der verwendeten Bits) als Dezimalzahl mit vorangehendem '/' an die IPv6-Adresse angehängt dargestellt.*

Tabelle 17: Parameterliste - DNS

Parameter	Wertekonvention	Default	Beschreibung
dns [DNS]	on/off	on	De-/aktiviert die Namensauflösung über einen DNS-Server.
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.*
dns_domain [Domain-Name (Suffix)]	max. 255 Zeichen [., a–z, A–Z, 0–9]	[blank]	Definiert den Domain-Namen eines vorhandenen DNS-Servers.

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.

Parameter	Wertekonvention	Default	Beschreibung
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_hash [Hash]	md5 sha	md5	Definiert den Hash-Algorithmus für die SNMP-Benutzergruppe 1. --- = *keine* *readonly* = *nur lesen* *readwrite* = *lesen und schreiben*
any_rights [Zugriffsrechte]	--- readonly readwrite	readonly	Definiert die Zugriffsrechte der SNMP-Benutzergruppe 1.
any_cipher [Verschlüsselung]	--- aes des	---	Definiert die Verschlüsselungsmethode der SNMP-Benutzergruppe 1.
admin_hash [Hash]	md5 sha	md5	Definiert den Hash-Algorithmus für die SNMP-Benutzergruppe 2.
admin_rights [Zugriffsrechte]	--- readonly readwrite	readwrite	Definiert die Zugriffsrechte der SNMP-Benutzergruppe 2. --- = *keine* *readonly* = *nur lesen* *readwrite* = *lesen und schreiben*
admin_cipher [Verschlüsselung]	--- aes des	---	Definiert die Verschlüsselungsmethode der SNMP-Benutzergruppe 2.

Für SNMP-Benutzerkonten siehe: 'Parameterliste - TPR Control Center Sicherheit' ⇨ 120.

Tabelle 19: Parameterliste - POP3

Parameter	Wertekonvention	Default	Beschreibung
pop3 [POP3]	on/off	off	De-/aktiviert die POP3-Funktionalität.
pop3_srv [Servername]	max. 128 Zeichen	[blank]	Definiert einen POP3-Server über die IP-Adresse oder den Hostnamen. *Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.*
pop3_port [Serverport]	1–65535 [1–5 Zeichen; 0–9]	110	Definiert den Port des POP3-Servers, über den der TPR E-Mails empfängt. *Bei Verwendung von SSL/TLS ist als Portnummer 995 einzutragen.*
pop3_sec [Sicherheit]	0–2 [1 Zeichen; 0–2]	0	Definiert das anzuwendende Authentifizierungsverfahren. *0 = keine Sicherheit* *1 = APOP* *2 = SSL/TLS*
pop3_poll [E-Mails abfragen alle]	1–10080 [1–5 Zeichen; 0–9]	15	Definiert das Zeitintervall (in Minuten) für die Abfrage der E-Mails auf dem POP3-Server.
pop3_limit [E-Mails ignorieren mit mehr als]	0–4096 [1–4 Zeichen; 0–9; 0 = unbegrenzt]	10	Definiert die maximale Größe (in Kbyte) der vom TPR akzeptierten E-Mails.
pop3_usr [Benutzername]	max. 128 Zeichen	[blank]	Definiert den Namen, den der TPR benutzt, um sich am POP3-Server anzumelden.
pop3_pwd [Passwort]	max. 128 Zeichen	[blank]	Definiert das Passwort, das der TPR benutzt, um sich am POP3-Server anzumelden.

Tabelle 20: Parameterliste - SMTP

Parameter	Wertekonvention	Default	Beschreibung
smtp_srv [Servername]	max. 128 Zeichen	[blank]	Definiert einen SMTP-Server über die IP-Adresse oder den Hostnamen. *Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.*
smtp_port [Serverport]	1–65535 [1–5 Zeichen; 0–9]	25	Definiert die Portnummer, über die der SMTP-Server E-Mails von dem TPR empfängt.
smtp_ssl [TLS]	on/off	off	De-/aktiviert die Option TLS. *Über das Sicherheitsprotokoll Transport Layer Security (TLS) wird der Übertragungsweg vom TPR zum SMTP-Server verschlüsselt.*
smtp_sender [Name des Absenders]	max. 128 Zeichen	[blank]	Definiert die E-Mail-Adresse, die der TPR zum Versenden von E-Mails verwendet. Hinweis: Oft sind der Name des Absenders und der Benutzername identisch.
smtp_auth [Anmelden]	on/off	off	De-/aktiviert die SMTP-Authentifizierung für das Login.
smtp_usr [Benutzername]	max. 128 Zeichen	[blank]	Definiert den Benutzernamen, den der TPR benutzt, um sich am SMTP-Server anzumelden.
smtp_pwd [Passwort]	max. 128 Zeichen	[blank]	Definiert das Passwort, das der TPRr benutzt, um sich am SMTP-Server anzumelden.
smtp_sign [Sicherheit (S/MIME)]	on/off	off	De-/aktiviert das Verschlüsseln und Signieren der E-Mails via S/MIME.
smtp_encrypt [Vollständig verschlüsseln] [E-Mail signieren]	on/off	off	Definiert das Signieren und Verschlüsseln von E-Mails. *off = signieren* *on = verschlüsseln*

Parameter	Wertekonvention	Default	Beschreibung
smtp_attpkey [Öffentlichen Schlüssel beifügen]	on/off	on	De-/aktiviert das Hinzufügen eines öffentlichen Schlüssels zu einer E-Mail.

Tabelle 21: Parameterliste - Bonjour

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

Tabelle 22: Parameterliste - Datum/Zeit

Parameter	Wertekonvention	Default	Beschreibung
ntp [Datum/Zeit]	on/off	on	De-/aktiviert die Verwendung eines Time-Servers (SNTP).
ntp_server [Time-Server]	max. 255 Zeichen [., a–z, A–Z, 0–9]	pool.ntp.org	Definiert einen Time-Server über die IP-Adresse oder den Hostnamen. *Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.*
ntp_tzone [Zeitzone]	UTC, GMT, EST, EDT, CST, CDT, MST, MDT, PST, PDT usw.	CET/CEST (EU)	Gleicht die Differenz zwischen der über einen Time-Server empfangenen Zeit und Ihrer lokalen Zeitzone aus.

Tabelle 23: Parameterliste - Beschreibung

Parameter	Wertekonvention	Default	Beschreibung
sys_name [Hostname]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert den Hostnamen des TPR.

Parameter	Wertekonvention	Default	Beschreibung
sys_descr [Beschreibung]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Freidefinierbare Beschreibung (des TPR).
sys_contact [Ansprechpartner]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Freidefinierbare Beschreibung (des Ansprechpartners).

Tabelle 24: Parameterliste - TPR-10

Parameter	Wertekonvention	Default	Beschreibung
nat_local [Lokale IP-Adresse]	gültige IP-Adresse	192.168. 156.156/ 28	Definiert die IP-Adresse des TPR für die interne Kommunikation. *TPR und Drucker bilden ein internes IP-Netzwerk. Die lokale IP-Adresse ist das Gateway zur Drucker-IP-Adresse. Die Netzwerkmaske lautet 255.255.255.240.*
nat_remote [Drucker-IP-Adresse]	gültige IP-Adresse	192.168. 156.157/ 28	Definiert die IP-Adresse des Druckers für die interne Kommunikation. *TPR und Drucker bilden ein internes IP-Netzwerk. Die Drucker-IP-Adresse und zugehörige Parameter werden vom internen DHCP-Server des TPR konfiguriert.*
nat_src [Masquerading]	on/off	off	De-/aktiviert das Masquerading. *Masquerading ist eine Form von NAT (Network Address Translation). Bei NAT werden alle externen IP-Adressen durch lokale IP-Adressen ersetzt.*
auto_rst_h	0–24 [1–2 Zeichen; 0–9; 0 = aus 1 = 1. Stunde 2 = 2. Stunde 3 = 3. Stunde usw.]	0	**Der Parameter ist ausschließlich in Absprache mit dem SEH Support zu verwenden.**

Parameter	Wertekonvention	Default	Beschreibung
nat_icmp [ICMP]	on/off	on	De-/aktiviert das Weiterleiten von ICMP-Paketen an die Drucker-IP-Adresse. *In IP-Netzwerken wird ICMP zum Übertragen von Fehlermeldungen und Abfragen, z.B. 'ping', verwendet. Wenn die Option aktiviert ist, werden Abfragen vom Drucker und nicht vom TPR beantwortet.*

Tabelle 25: Parameterliste - Lokale Service-Ports

Parameter	Wertekonvention	Default	Beschreibung
httpd_port [HTTP]	1–65535 [1–5 Zeichen; 0–9]	80	Definiert den TCP-Port, der bei der Netzwerkkommunikation von dem TPR für HTTP verwendet wird.
httpsd_port [HTTPS]	1–65535 [1–5 Zeichen; 0–9]	443	Definiert den TCP-Port, der bei der Netzwerkkommunikation von dem TPR für HTTPS verwendet wird.
snmp_port [SNMP]	1–65535 [1–5 Zeichen; 0–9]	161	Definiert den TCP-Port, der bei der Netzwerkkommunikation von dem TPR für SNMP verwendet wird.
tpgPort [ThinPrint®]	1–65535 [1–5 Zeichen; 0–9]	4000	Definiert den TCP-Port, über den der TPR mit dem ThinPrint Server kommuniziert

Tabelle 26: Parameterliste - Personal Printing

Parameter	Wertekonvention	Default	Beschreibung
pps [Personal Printing]	on/off	on	De-/aktiviert die Personal-Printing-Funktionalität des TPR.

Parameter	Wertekonvention	Default	Beschreibung
pps_on_1 pps_on_2 [Server]	on/off	off	De-/aktiviert den Personal Printing Server 1 bzw. 2.
pps_server_1 pps_server_2 [Servername]	max. 255 Zeichen [., a–z, A–Z, 0–9]	[blank]	Definiert einen Personal-Printing-Server über die IP-Adresse oder den Hostnamen. *Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.*
pps_port_1 pps_port_2 [Serverport]	1–65535 [1–5 Zeichen; 0–9]	80	Definiert den TCP-Port, über den der TPR mit dem Personal-Printing-Server kommuniziert. *Ist die SSL-Verbindung aktiviert, ist als Portnummer 443 zu verwenden.*
pps_ssl_1 pps_ssl_2 [SSL-Verbindung]	on/off	off	De-/aktiviert die SSL-/TLS-Verschlüsselung und zertifikatbasierte Authentifizierung für das Personal-Printing-Protokoll.
pps_verify_1 pps_verify_2 [Zertifikat verifizieren]	on/off	off	De-/aktiviert das Überprüfen des Personal-Printing-Server-Zertifkates mit Hilfe des Wurzelzertifikats und/oder Personal-Printing-Zertifikats.
pps_pin_1 pps_pin_2 [Nutzer-PIN]	max. 32 Zeichen	SEH	Definiert die Nutzer-PIN. Die definierte Nutzer-PIN und die Nutzer-PIN in den Nutzerkonten des Active Directory müssen identisch sein.
pps_prtID_1 pps_prtID_2 [Drucker-ID]	0–64 [1–2 Zeichen; 0–9]	1	Definiert die ID des Druckerobjektes, das vom Personal-Printing-Server verwendet wird.

Parameter	Wertekonvention	Default	Beschreibung
pps_delete_1 pps_delete_2 [Löschen der Druckaufträge]	none = ohne tpr = durch den TPR srv = durch den Personal Printing Server	srv	Definiert das Löschen von Druckaufträgen. - durch den Personal-Printing-Server: Gedruckte Aufträge werden sofort gelöscht durch den Personal-Printing-Server. - durch den TPR: Gedruckte Aufträge werden durch den TPR gelöscht. Der Löschzeitpunkt kann über die Verzögerung bestimmt werden. - ohne: Gedruckte Aufträge werden gemäß den Einstellungen auf dem Personal-Printing-Server gelöscht.
pps_delDelay_1 pps_delDelay_2 [Verzögerung]	0 –60 [1–2 Zeichen; 0–9; 0 = sofortiges Löschen]	0	Definiert eine Verzögerung (in Sekunden) für das Löschen von gedruckten Aufträgen durch den TPR. Eine Verzögerung stellt eine vollständige Übertragung an den Drucker und das vollständige Ausdrucken des Druckauftrages sicher.
pps_single [Druckaufträge einzeln auslösen]	on/off	off	De-/aktiviert das Auslösen eines einzelnen Druckauftrags pro Kartenstreich. Wenn mehrere Druckaufträge anliegen, müssen diese einzeln nacheinander ausgelöst werden.
pps_USRformat [User-ID formatieren]	on/off	off	De-/aktiviert das Formatieren der Nutzer-IDs. Ist die Option aktiviert, werden die ID-Elemente mit Bindestrichen getrennt und Buchstaben groß geschrieben. *Das Format der Nutzer-ID muss mit dem auf dem Personal-Printing-Server verwendeten Format übereinstimmen. Aktivieren Sie die Option, wenn Sie Ihre Personal-Printing-Umgebung für TPR-Soft- und Firmware-Versionen 14.0.16 und kleiner konfiguriert haben.*

Parameter	Wertekonvention	Default	Beschreibung
beep [Signaltongeber]	on/off	on	De-/aktiviert die akustische Rückmeldung. Akustische Signale stellen beim Auslösen von Druckaufträgen Informationen zur Verfügung.

Tabelle 27: Parameterliste - ThinPrint®

Parameter	Wertekonvention	Default	Beschreibung
tpgPort [ThinPrint®-Port]	1–65535 [1–5 Zeichen; 0–9]	4000	Definiert den TCP-Port, über den das TPR mit dem ThinPrint Server kommuniziert.
tpgBdwidth [Bandbreite]	on/off	off	De-/aktiviert die clientseitige (TPR) Bandbreitenregulierung des ThinPrint®-Ports.
tpgBdwidthVal [Bandbreitenwert]	1600 –1000000 [4–7 Zeichen; 0–9]	256000	Definiert die Bandbreite (in Bit/Sekunde) mit der clientseitig (TPR) das Bandbreitenlimit am ThinPrint®-Port herabgesetzt wird.
tpgPrtoToVal [Druckerverbindungsabbruch]	0–86400 [1–5 Zeichen; 0–9; 0 = aus]	60	Definiert das Zeitintervall (in Sekunden), nach dem ein Verbindungsversuch zum Drucker abgebrochen wird. *Ein Verbindungsversuch sollte abgebrochen werden, wenn ein Drucker physikalisch nicht verfügbar ist. Das macht den ThinPrint®-Port für nachfolgende Druckaufträge frei.*
tpgJobSndTout [Timeout für das Senden von Druckaufträgen]	0–86400 [1–5 Zeichen; 0–9; 0 = aus]	180	Definiert das Zeitintervall (in Sekunden), nach dem ein anliegender Druckauftrag abgebrochen wird, wenn er aufgrund eines Druckerfehlers, z.B. kein Papier, nicht gedruckt werden kann.
tpgJobRcvTout	0–1440 [1–4 Zeichen; 0–9; 0 = aus]	0	**Der Parameter ist ausschließlich in Absprache mit dem SEH Support zu verwenden.**

Tabelle 28: Parameterliste - ThinPrint Connection Service

Parameter	Wertekonvention	Default	Beschreibung
conService [Connection Service]	on/off	off	De-/aktiviert den ThinPrint Connection Service.
conServer [Servername]	max. 255 Zeichen [., a–z, A–Z, 0–9]	[blank]	Definiert einen Connection Service-Server über die IP-Adresse oder den Hostnamen. *(Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.)*
tpgClientID [Client-ID]	0–99999 [1–5 Zeichen; 0–9]	0	Definiert die Client-ID, mit der der TPR in der Datenbank des Connection Services hinterlegt ist.
tpgAuthKey [Authentifizierungsschlüssel]	0–99999 [1–5 Zeichen; 0–9]	0	Definiert den Authentifizierungsschlüssel, mit dem der TPR in der Datenbank des Connection Services hinterlegt ist.
conPort [Port]	1–65535 [1–5 Zeichen; 0–9]	4001	Definiert den TCP-Port, über den der TPR mit dem Connection Service kommuniziert.
tpgKeepalive [Keep alive]	1–60000 [1–5 Zeichen; 0–9]	60	Definiert das Zeitintervall (in Sekunden), mit dem die Verbindung zum Connection Service aktualisiert wird. *Hinweis: Der Wert muss genauso groß wie oder kleiner als der auf dem Connection Service-Server eingestellte Wert 'KeepAliveTO' sein.*
tpgRetry [Erneuter Verbindungsversuch]	1–60000 [1–5 Zeichen; 0–9]	120	Definiert das Zeitintervall (in Sekunden), nach dem ein erneuter Verbindungsversuch stattfindet, wenn der Connection Service nicht erreichbar ist.

Tabelle 29: Parameterliste - ThinPrint®-Drucker

Parameter	Wertekonvention	Default	Beschreibung
prtName_1 [Drucker]	max. 32 Zeichen [a–z, A–Z, 0–9, _, -]	[blank]	Definiert den Druckernamen für das ThinPrint Auto-Connect-Verfahren.
prtClass_1 [Klasse]	max. 7 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert den Druckerklassen-namen für das ThinPrint Auto-Connect-Verfahren.
prtDriver_1 [Treiber]	max. 64 Zeichen [a–z, A–Z, 0–9, _, -]	[blank]	Definiert den Druckertreiber für das ThinPrint Auto-Connect-Verfahren.
remoteMode_1 [Druckprotokoll]	raw ipp lpd	raw	Definiert die Übertragungsme-thode zwischen TPR und dem Drucker. *raw = RAW-/Socket-Verbindung* *ipp = IPP-Verbindung* *lpd = LPD-Verbindung*
remotePort_1 [Port]	1–65535 [1–5 Zeichen; 0–9]	9100	Definiert die Portnummer für das RAW-/Socket-Printing.
remoteUrl_1 [URL]	max. 64 Zeichen	ipp/lp1	Definiert den zweiten Teil der Drucker-URL für das IPP-Printing. *Die Implementierung der Dru-cker-URL ist herstellerabhän-gig. Nähere Informationen finden Sie im Druckerhand-buch.*
remoteIPPs_1 [SSL]	on/off	off	De-/aktiviert die SSL-/TLS-Verschlüsselung für das IPP-Printing.
remoteQ_1 [Queue]	max. 64 Zeichen [a–z, A–Z, 0–9]	lp1	Definiert den Queue-Namen für das LPD-Printing.
lpdModeRFC_1 [RFC]	on/off	on	De-/aktiviert das RFC1179-konforme LPD-Printing.
monitorPing [Überwachung über Ping]	on/off	on	De-/aktiviert die Überwachung über 'ping', d.h. ICMP. *Die 'ping'-Abfrage ermöglicht die Anzeige der Druckerver-fügbarkeit.*

Parameter	Wertekonvention	Default	Beschreibung
monitorSNMP [SNMP]	on/off	on	De-/aktiviert die Überwachung über SNMP. *Die SNMP-Abfrage ermöglicht die Anzeige von Druckermeldungen.*
monitorPoll [Überwachungsintervall]	10–86400 [2–5 Zeichen; 0–9]	30	Definiert das Intervall einer 'ping'- bzw. 'SNMP'-Abfrage in Sekunden.
prtLock [Gerätezuordung]	on/off	off	De-/aktiviert die Gerätezuordnung. Der TPR kann dem Drucker dauerhaft zugeordnet werden. Der TPR kann dann nur mit dem zugeordneten Drucker betrieben werden.

Tabelle 30: Parameterliste - Benachrichtigung

Parameter	Wertekonvention	Default	Beschreibung
mailto_1 mailto_2 [E-Mail-Empfänger]	gültige E-Mail Adresse [max. 64 Zeichen]	[blank]	Definiert die E-Mail-Adresse des Empfängers für Benachrichtigungen.
noti_pup_1 noti_pup_2 [Neustart]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch einen Neustart des TPR ausgelöst wird.
noti_stat_1 noti_stat_2 [Status]	on/off	off	De-/aktiviert den periodischen Versand einer Status-E-Mail an den Empfänger 1 oder 2.
notistat_d [Intervall]	al = täglich su = Sonntag mo = Montag tu = Dienstag we = Mittwoch th = Donnerstag fr = Freitag sa = Samstag	al	Definiert das Intervall, mit dem eine Status-E-Mail versendet wird.

Parameter	Wertekonvention	Default	Beschreibung
notistat_h [hh]	1 = 1. Stunde 2 = 2. Stunde 3 = 3. Stunde usw.	0	Definiert die Uhrzeit, zu der eine Status-E-Mail versendet wird.
notistat_tm [mm]	0 = 00 min 1 = 10 min 2 = 20 min 3 = 30 min 4 = 40 min 5 = 50 min 6 = 00 min	0	Definiert die Uhrzeit, zu der eine Status-E-Mail versendet wird.
noti_card_1 noti_card_2 [Karten]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch ein Kartenereignis am TPR ausgelöst wird.
noti_usb_1 noti_usb_2 [USB]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch das Anschließen oder Entfernen eines USB-Sticks am TPR ausgelöst wird.
noti_err_1 noti_err_2 [Probleme]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch ein Problem am TPR ausgelöst wird.
trapto_1 trapto_2 [Trap-Empfänger]	gültige IP-Adresse	0.0.0.0	Definiert die SNMP-Trap-Adresse des Empfängers für Benachrichtigungen.
trapcommu_1 trapcommu_2 [Trap-Community]	max. 64 Zeichen [a–z, A–Z, 0–9]	public	Definiert die SNMP-Trap-Community des Empfängers.
trappup [Neustart]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch einen Neustart des TPR ausgelöst wird.
trapcard [Karten]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch ein Kartenereignis am TPR ausgelöst wird.
trapusb [USB]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch das Anschließen oder Entfernen eines USB-Sticks am TPR ausgelöst wird.

Parameter	Wertekonvention	Default	Beschreibung
traperr [Probleme]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch ein Problem am TPR ausgelöst wird.

Tabelle 31: Parameterliste - SSL-/TLS-Verbindungen

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

Tabelle 32: Parameterliste - TPR Control Center Sicherheit

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

Parameter	Wertekonvention	Default	Beschreibung
any_name [Lesezugriff-Benutzer-Benutzername]	max. 64 Zeichen [a–z, A–Z, 0–9]	anony-mous	Definiert den Benutzernamen für das Lesezugriff-Benutze-Benutzerkonto. Hinweis: Ist gleichzeitig der Benutzername für das SNMP-User-Konto.
any_pwd [Lesezugriff-Benutzer-Passwort]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert das Passwort für das Lesezugriff-Benutze-Benut-zerkonto. Hinweis: Ist gleichzeitig das Passwort für das SNMP-User-Konto.

Tabelle 33: Parameterliste - Portsperrung

Parameter	Wertekonvention	Default	Beschreibung
drop_port_1 ~ drop_port_12 [Port]	1–65535 [1–5 Zeichen; 0–9]	0	Definiert die Portnummer des zu sperrenden Ports. Insge-samt können 12 Ports gesperrt werden.
drop_tcp_1 ~ drop_tcp_12 [TCP]	on/off	off	Sperrt den Zugriff auf ausge-wählte TCP-Ports. *TCP- und UDP-Ports können gleichzeitig gesperrt werden.*
drop_udp_1 ~ drop_udp_12 [UDP]	on/off	off	Sperrt den Zugriff auf ausge-wählte UDP-Ports. *TCP- und UDP-Ports können gleichzeitig gesperrt werden.*
drop_lan_1 ~ drop_lan_12 [LAN]	on/off	off	Sperrt den Zugriff auf ausge-wählte LAN-Schnittstellen (Netzwerkanschluss). *Drucker- und LAN-Schnittstel-len können gleichzeitig gesperrt werden.*
drop_nat_1 ~ drop_nat_12 [Drucker]	on/off	off	Sperrt den Zugriff auf ausge-wählte Drucker-Schnittstellen (Druckeranschluss). *Drucker- und LAN-Schnittstel-len können gleichzeitig gesperrt werden.*

Tabelle 34: Parameterliste - TCP-Portzugriff

Parameter	Wertekonvention	Default	Beschreibung
protection [Portzugriff kontrollieren]	on/off	off	De-/aktiviert die Sperrung von ausgewählten Ports.
protection_test [Testmodus]	on/off	on	De-/aktiviert den Testmodus. *Der Testmodus bietet die Möglichkeit, die über die Zugriffskontrolle eingestellten Parameter zu testen. Bei aktiviertem Testmodus ist der Zugriffsschutz bis zum nächsten Neustart des TPR aktiv.*
protection_level [Sicherheitsstufe]	protec_tcp protec_all	protec_tcp	Definiert die zu sperrenden Porttypen. *protec_tcp = TCP-Ports protec_all = alle Ports (IP-Ports)*
ip_filter_on_1 ~ ip_filter_on_8 [IP-Adresse]	on/off	off	De-/aktiviert eine Ausnahme von der Portsperrung.
ip_filter_1 ~ ip_filter_8 [IP-Adresse]	gültige IP-Adresse	[blank]	Definiert 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 35: Parameterliste - Authentifizierung

Parameter	Wertekonvention	Default	Beschreibung
auth_typ [Authentifizierungsmethode]	--- [keine] MD5 TLS TTLS PEAP FAST	----	Definiert die Authentifizierungsmethode, mit der Geräte oder Benutzer im Netzwerk identifiziert werden.
auth_name [Benutzername]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert den Namen des TPR, 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 TPR, wie es auf dem Authentifizierungsserver (RADIUS) gespeichert ist.
auth_extern [PEAP/EAP-FAST-Optionen]	--- = keine PLABEL0 = PEAPLABEL0 PLABEL1 = PEAPLABEL1 PVER0 = PEAPVER0 PVER1 = PEAPVER1 FPROV1 = FASTPROV1	---	Definiert die Art der äußeren Authentifizierung bei den EAP-Authentifizierungsmethoden TTLS, PEAP und FAST.
auth_intern [Innere Authentifizierung]	--- = keine PAP = PAP CHAP = CHAP MSCHAP2 = MS-CHAPv2 EMD5 = EAP-MD5 ETLS = EAP-TLS	---	Definiert die Art der inneren Authentifizierung bei den EAP-Authentifizierungsmethoden TTLS, PEAP und FAST.
auth_ano_name [Anonymer Name]	max. 64 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert den anonymen Namen für den unverschlüsselten Teil der EAP-Authentifizierungsmethoden TTLS, PEAP und FAST.
auth_wpa_addon [WPA-Add-on]	max. 255 Zeichen [a–z, A–Z, 0–9]	[blank]	Definiert eine optionale WPA-Erweiterung.

Tabelle 36: Parameterliste - USB-Gerät

Parameter	Wertekonvention	Default	Beschreibung
autoSync [Parameter-Backup]	on/off	on	De-/aktiviert das automatische Sichern der Parameter auf einen angeschlossenen USB-Stick.

Tabelle 37: Parameterliste - Statusseite

Parameter	Wertekonvention	Default	Beschreibung
spage [Statusseite]	on/off	on	De-/aktiviert das Drucken von Status- und Serviceseiten auf dem Drucker. *Der Druckauftrag kann ausgelöst werden, indem der Status-/Reset-Taster am Gerät betätigt oder die entsprechende Schaltfläche im TPR Control Center angewählt wird.*
spMode [Modus Statusseite]	ASCII PostScript DATAMAX Citizen-Z	ASCII	Definiert das Datenformat, in dem eine Statusseite gedruckt wird.

9.3 Problembehandlung

Dieses Kapitel stellt einige Problemursachen und erste Lösungshilfen dar.

Problemdarstellung

Der TPR signalisiert den BIOS-Modus

Mögliche Ursache

Der TPR 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 TPR signalisiert den BIOS-Modus, indem die Activity-LED grün blinkt.

Der TPR ist im BIOS-Modus nicht funktionsfähig.

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

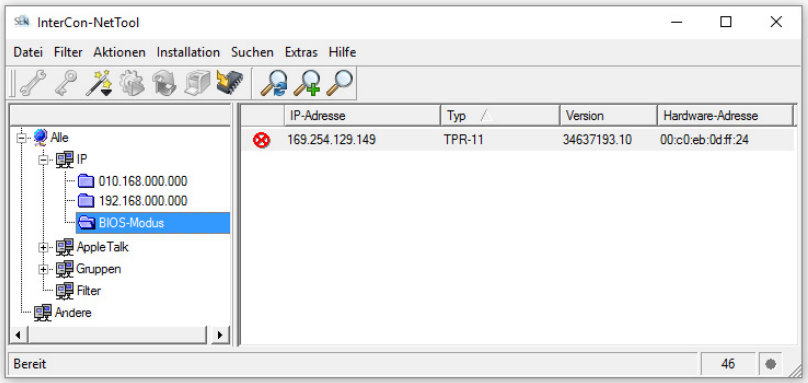


Abb. 7: InterCon-NetTool - TPR im BIOS-Modus

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

Gehen Sie wie folgt vor:

1. *Starten Sie das InterCon-NetTool.*
2. *Markieren Sie den TPR in der Geräteliste.*
   (Sie finden den TPR unter dem Filter 'BIOS-Modus'.)
3. *Wählen Sie im Menü* **Installation** *den Befehl* **IP-Assistent**.
   Der IP-Assistent wird gestartet.
4. *Weisen Sie dem TPR eine IP-Adresse zu, indem Sie den Anweisungen des Assistenten folgen.*
   Die IP-Adresse wird gespeichert.
5. *Führen Sie auf dem TPR ein Softwareupdate durch; siehe:* ⇨ *93.*

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

Die Verbindung zum TPR Control Center kann nicht hergestellt werden

Schließen Sie Fehlerquellen aus. Überprüfen Sie zunächst:

- die Kabelverbindungen,

- die IP-Adresse des TPR (⇨ 13) sowie

- die Proxy-Einstellungen Ihres Browsers.

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

- ☐ Der Zugang ist via SSL/TLS (HTTPS) geschützt ⇨ 64.
- ☐ Die TCP-Portzugriffskontrolle ist aktiviert ⇨ 68.
- ☐ Der HTTP-Port wurde geändert ⇨ 39.
- ☐ Die Cipher Suites der Verschlüsselungsstufe werden vom Browser nicht unterstützt ⇨ 61.

Das Passwort ist nicht mehr verfügbar

Der Zugriff auf das TPR Control Center kann geschützt werden. Ist das Passwort und/oder der Benutzername nicht mehr verfügbar, können die Parameterwerte des TPR auf die Standardwerte zurückgesetzt werden, um Zugriff zu erhalten ⇨ 91. Dabei gehen sämtliche Einstellungen verloren.

Personal Printing: Der Drucker druckt nicht

Mögliche Ursache

Es kann keine Verbindung zum Personal-Printing-Server hergestellt werden. Überprüfen Sie, ob

- ☐ der bzw. die Personal Printing Server korrekt definiert sind ⇨ 43.
  Beachten Sie dabei besonders die Nutzer-PIN, die auf dem Personal-Printing-Server und auf dem TPR identisch sein muss .
- ☐ der Drucker korrekt eingebunden ist ⇨ 47.
  Achten Sie dabei besonders auf die Drucker-ID, die auf dem Personal-Printing-Server und auf dem TPR identisch sein muss.
- ☐ die eingesetzte Verschlüsselung korrekt konfiguriert ist:
  - Auf dem Personal-Printing-Server und auf dem TPR ist die Verschlüsselung aktiviert ⇨ 43.

(Eine aktivierte Verschlüsselung bei nur einem der beiden Kommunikationspartnern führt zum Fehlerfall.)

- Die benötigten Zertifikate sind installiert ⇨ 70.
- Die benötigten Zertifikate sind gültig ⇨ 70.

☐ die Software/Firmware veraltet ist. Führen Sie ggf. ein Update durch ⇨ 93.

☐ der Benutzer zum Drucken über den TPR berechtigt ist. Hierzu können Sie die zuletzt am TPR verwendete Nutzer-ID im Control Center einsehen in der Tabelle **Personal-Printing-Status** unter **Gerät - Personal Printing**.

Bei Fragen zur und Problemen mit der Personal-Printing-Umgebung wenden Sie sich bitte an den Personal-Printing-Support (http://www.personal-printing.com).

ThinPrint: Der Drucker druckt nicht, wenn Druckaufträge an den TPR gesendet werden

Überprüfen Sie zunächst, ob der Drucker auf dem TPR korrekt eingebunden ist; siehe: 'Wie binde ich den Drucker ein?' ⇨ 51.

Kann weiterhin nicht über den TPR gedruckt werden, können folgende Faktoren verantwortlich sein:

☐ Der Drucker unterstützt das gewählte Druckprotokoll nicht. Wählen Sie ein unterstütztes Druckprotokoll ⇨ 42. Lesen Sie hierzu die Dokumentation Ihres Druckers.

☐ Für das Druckerobjekt auf dem ThinPrint Server, welches die Druckaufträge an den TPR sendet, muss ein nativer Treiber konfiguriert sein. Ist als Druckertreiber das 'ThinPrint Output Gateway' definiert, werden die Druckdaten in einem Format ('EMF') gesendet, welches nicht vom TPR unterstützt wird.

☐ Über Timeouts haben Sie die Möglichkeit, die Behandlung von Fehlerzuständen vor und während eines Druckauftrags zu kontrollieren ⇨ 53. Überprüfen Sie, ob die Timeouts zu kurz

sind und die Verbindung zum Drucker oder das Senden des Druckauftrag vorzeitig abgebrochen werden.

- ☐ In der ThinPrint-Umgebung wird über den ThinPrint-Port (Default: 4000) gedruckt ⇨ 50. Dieser Port darf nicht durch eine Sicherheitssoftware (z.B. Firewall) blockiert werden.
- ☐ In der ThinPrint-Umgebung kann der Connection Service genutzt werden ⇨ 57. Der Port für diesen Dienst (Default: 4001) darf nicht durch eine Sicherheitssoftware (z.B. Firewall) blockiert werden.
- ☐ Die Druckdaten werden verschlüsselt an den TPR gesendet ⇨ 59. Überprüfen Sie, ob
  - die benötigten Zertifikate installiert sind.
  - die benötigten Zertifikate gültig sind.

9.4 Abbildungsverzeichnis

9.5 Index