



ThinPrint® Gateway

TPG-25 / TPG-65



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: TPG-25 / TPG-65
Version: 1.0

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/tpg.html>

InterCon ist ein eingetragenes Warenzeichen der SEH Computertechnik GmbH.

SEH Computertechnik GmbH hat diese Dokumentation mit größter Sorgfalt erarbeitet. Da sich Fehler trotz aller Bemühungen nicht vollständig vermeiden lassen, sind wir für Hinweise jederzeit dankbar. SEH Computertechnik GmbH kann jedoch für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen. Änderungen, die dem technischen Fortschritt dienen, sind vorbehalten.

Alle Rechte sind vorbehalten. Reproduktion, Adaption oder Übersetzung sind ohne schriftliche Genehmigung von SEH Computertechnik GmbH verboten.

© 2012 SEH Computertechnik GmbH

All trademarks, registered trademarks, logos and product names are property of their respective owners.

Inhaltsverzeichnis

1 Allgemeine Information	5
1.1 ThinPrint® Gateway	6
1.2 Dokumentation	8
1.3 Support und Service	10
1.4 Ihre Sicherheit	11
1.5 Erste Schritte	12
1.6 Speichern der IP-Adresse im TPG	13
2 Administrationsmethoden	17
2.1 Administration via TPG Control Center	18
2.2 Administration via InterCon-NetTool	20
2.3 Administration via E-Mail	22
2.4 Administration via Status-/Reset-Taster am Gerät	25
3 Netzwerk- und Geräteeinstellungen	26
3.1 Wie konfiguriere ich IPv4-Parameter?	27
3.2 Wie konfiguriere ich IPv6-Parameter?	29
3.3 Wie konfiguriere ich den DNS?	31
3.4 Wie konfiguriere ich SNMP?	32
3.5 Wie konfiguriere ich POP3 und SMTP?	33
3.6 Wie konfiguriere ich Bonjour?	36
3.7 Wie konfiguriere ich die Gerätezeit?	37
3.8 Wie lege ich eine Beschreibung fest?	38
3.9 Wie verwende ich den Benachrichtigungsservice?	39
4 ThinPrint-Einstellungen	41
4.1 Wie definiere ich den ThinPrint-Port?	42
4.2 Wie definiere ich die Bandbreite?	42
4.3 Wie binde ich die Drucker ein?	43
4.4 Wie definiere ich Timeouts?	46
4.5 Wie erhalte ich Statusinformationen zu den Druckerverbindungen?	47
4.6 Wie erhalte ich Drucker Meldungen?	48
4.7 Wie verwende ich den ThinPrint Connection Service?	49
4.8 Wie empfängt das TPG verschlüsselte Daten?	51

5 Sicherheit	52
5.1 Wie kontrolliere ich den Zugang zum TPG Control Center?	53
5.2 Wie kontrolliere ich den Zugriff auf das TPG (TCP-Portzugriffskontrolle)	55
5.3 Wie setze ich Zertifikate korrekt ein?	57
5.4 Wie verwende ich Authentifizierungsmethoden?	65
6 Wartung	72
6.1 Wie sichere ich die TPG-Parameter? (Backup)	73
6.2 Wie verwende ich ein angeschlossenes USB-Gerät?	74
6.3 Wie setze ich die Parameter auf die Standardwerte zurück? (Reset) .	77
6.4 Wie führe ich ein Update aus?	80
6.5 Wie starte ich das TPG neu?	81
6.6 Wie drucke ich eine Status- oder Serviceseite?	82
6.7 Wie lasse ich die Job History anzeigen?	84
7 Anhang	87
7.1 Glossar	88
7.2 Parameterliste	91
7.3 Problembehandlung	107
7.4 Abbildungsverzeichnis	110
7.5 Index	111

1 Allgemeine Information



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

Welche Information benötigen Sie?

- 'ThinPrint® Gateway' ⇨ 6
- 'Dokumentation' ⇨ 8
- 'Support und Service' ⇨ 10
- 'Ihre Sicherheit' ⇨ 11
- 'Erste Schritte' ⇨ 12
- 'Speichern der IP-Adresse im TPG' ⇨ 13

1.1 ThinPrint® Gateway

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

Verwendungszweck

Das TPG (ThinPrint® Gateway) enthält einen vollständig integrierten **ThinPrint Client**. Dieser ermöglicht das Empfangen und Dekomprimieren der Druckdaten.

Die ThinPrint® Gateways TPG-25 und TPG-65 sind speziell für Umgebungen entwickelt worden, in denen ThinPrint-Technologie zur Druckauftrag-Komprimierung und Bandbreitenkontrolle im Einsatz ist.

Bis zu zwei Netzwerkdrucker lassen sich schnell und einfach mit dem TPG-25 ins Netzwerk einbinden. Mit dem TPG-65 sind es bis zu sechs Geräte. Anwender schicken komprimierte Druckaufträge an das ThinPrint® Gateway, welches diese Druckaufträge dekomprimiert und an die entsprechenden Drucker sendet.

Leistungsmerkmale

Das TPG unterstützt u.a. die folgenden Features:

- 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.

**System-
voraussetzungen**

Das TPG ist konzipiert für den Einsatz in TCP/IP-basierten Netzwerken. Innerhalb dieses Netzwerkes muss ein ThinPrint Server integriert sein. Die beteiligten Netzwerkdruker müssen RAW- bzw. Socket-Printing (Drucken via TCP/IP-Ports), IPP-Printing oder LPD-Printing unterstützen. Wird der **ThinPrint Connection Service** verwendet, muss eine entsprechende Lizenz vorhanden sein.

Aufbau der Dokumentation

Merkmale dieses Dokumentes

Fachbegriffe in diesem Dokument

1.2 Dokumentation

Die TPG-Dokumentation besteht aus den folgenden Dokumenten:



PDF

Benutzerdokumentation

Detaillierte Beschreibung der TPG-Konfiguration und Administration.

Print
PDF

Quick Installation Guide

Informationen zur Sicherheit, Hardware-Installation sowie zur Inbetriebnahme.



HTML

Online Hilfe (TPG Control Center)

Die Online Hilfe enthält detaillierte Informationen zur Bedienung des 'TPG Control Center'.



HTML

Online Hilfe (InterCon-NetTool)

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

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'.

In diesem Dokument sind Erläuterungen von Fachbegriffen in einem Glossar zusammengefasst. Das Glossar bietet einen schnellen Überblick über technische Zusammenhänge und Hintergrundinformationen; siehe: ⇨ 88.

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: <i>1. Markieren Sie ...</i>	Das Hand-Symbol leitet eine Handlungsanweisung ein. Einzelne Handlungsschritte sind kursiv dargestellt.
 Bestätigung	Der Pfeil bestätigt die Auswirkung einer ausgeführten Handlung.
<input checked="" type="checkbox"/> Voraussetzung	Ein Haken kennzeichnet Bedingungen, die erfüllt sein müssen, bevor Sie mit einer Handlung beginnen.
<input type="checkbox"/> 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 Kapitels.
	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.
<code>Courier</code>	Kommandozeilen sind im Schrifttyp Courier dargestellt.
'Eigennamen'	Eigennamen sind in Anführungszeichen gesetzt

Support

1.3 Support und Service

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
- aktuelle Tools
- aktuelle Dokumentationen
- aktuelle Produktinformationen
- 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

Das TPG wird in TCP/IP-Netzwerken eingesetzt. Ein TPG ermöglicht bis zu zwei bzw. sechs Netzwerkdruckern die Kommunikation mit einem ThinPrint Server. Das TPG ist konzipiert für den Einsatz in Büroumgebungen.

Bestimmungswidrige Verwendung

Alle Verwendungen des Gerätes, die den in der TPG-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 TPG 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 TPG an Netzwerk und Stromnetz; siehe: 'Quick Installation Guide'.*
 3. *Stellen Sie sicher, dass eine IP-Adresse im TPG gespeichert ist; siehe: 'Speichern der IP-Adresse im TPG' ⇨  13.*
 4. *Definieren Sie den ThinPrint-Port und andere ThinPrint-Einstellungen; siehe: ⇨  41.*
 5. *Definieren Sie die Drucker, an die das TPG die Druckaufträge weiterleiten soll; siehe: 'Wie binde ich die Drucker ein?' ⇨  43.*
-  Das TPG ist funktionsbereit.

1.6 Speichern der IP-Adresse im TPG

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

Wie erhält das TPG eine IP-Adresse?

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

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

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

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
- 'TPG Control Center' ⇨ 15
- 'ARP/PING' ⇨ 16

ZeroConf

Erhält das TPG keine IP-Adresse über Bootprotokolle, gibt sich das TPG über ZeroConf selbst eine IP-Adresse. Hierzu wählt das TPG 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: ⇨ 36.

BOOTP

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

Voraussetzung

- Der Parameter 'BOOTP' ist aktiviert; siehe: ⇨ 27.
- Im Netzwerk ist ein BOOTP-Server vorhanden.

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

DHCP

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

Voraussetzung

- Der Parameter 'DHCP' ist aktiviert; siehe: ⇨ 27.
- Im Netzwerk ist ein DHCP-Server vorhanden.

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

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

Voraussetzung**Autokonfiguration (IPv6-Standard)**

Das TPG 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 das TPG in einem IPv6-fähigen Netzwerk angeschlossen, erhält das TPG automatisch eine zusätzliche 'link-local'-IP-Adresse aus dem IPv6-Adressbereich.

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

- Der Parameter 'IPv6' ist aktiviert.
- Der Parameter 'Automatische Konfiguration' ist aktiviert; siehe: [⇒ 29](#).



Um die Vergabe von IPv6-Adressen zu konfigurieren, siehe: [⇒ 29](#).

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 TPG gespeichert werden. Um eine IPv4-Adresse via InterCon-NetTool zu konfigurieren, siehe: [⇒ 27](#).

TPG Control Center

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

- Um eine IPv4-Adresse via TPG Control Center zu konfigurieren, siehe: ⇒ 27.
- Um eine IPv6-Adresse via TPG Control Center zu konfigurieren, siehe: ⇒ 29.

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 TPG gespeichert werden. Verfügt das TPG 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 TPG. Bei Empfang des Datenpaketes speichert das TPG 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: ⇒ 27.

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 TPG 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 das TPG 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 TPG Control Center' ⇨ 18
- 'Administration via InterCon-NetTool' ⇨ 20
- 'Administration via E-Mail' ⇨ 22
- 'Administration via Status-/Reset-Taster am Gerät' ⇨ 25

Welche Funktionen werden unterstützt?

Voraussetzung

TPG Control Center starten

2.1 Administration via TPG Control Center

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

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

- Das TPG ist an Netzwerk und Netzspannung angeschlossen.
- Das TPG hat eine gültige IP-Adresse.

 Gehen Sie wie folgt vor:

1. *Öffnen Sie Ihren Browser.*
 2. *Geben Sie als URL die IP-Adresse des TPG ein.*
-  Das TPG Control Center wird im Browser dargestellt.



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

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

 Gehen Sie wie folgt vor:

1. *Markieren Sie das TPG in der Geräteliste.*
 2. *Wählen Sie im Menü **Aktionen** den Befehl **Browser starten**.*
-  Das TPR Control Center wird im Browser dargestellt.

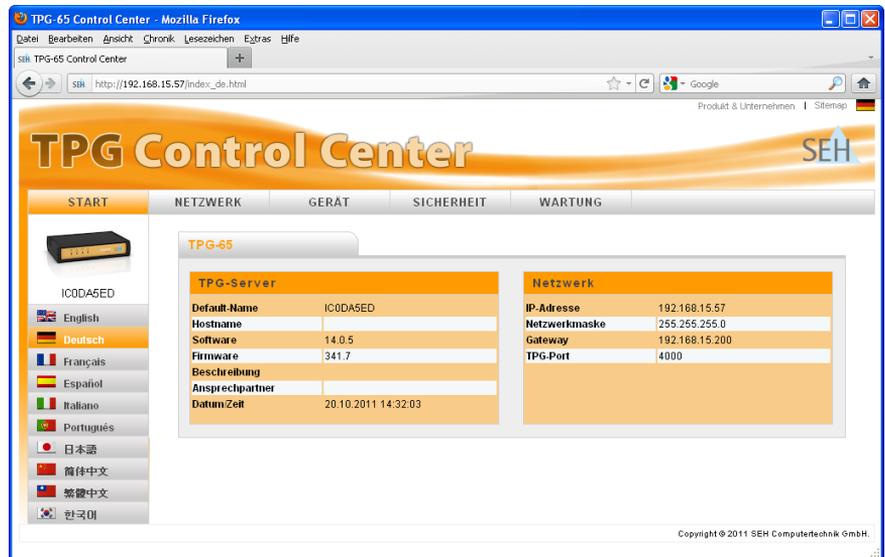


Abb. 1: TPG Control Center – START

Aufbau des TPG 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 TPG Control Centers.

Alle anderen Menüpunkte beziehen sich auf die Konfiguration des TPG. Die Menüpunkte sind in der Online Hilfe des TPG 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 (TPG, TPR, 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/tpg.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 --> 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.

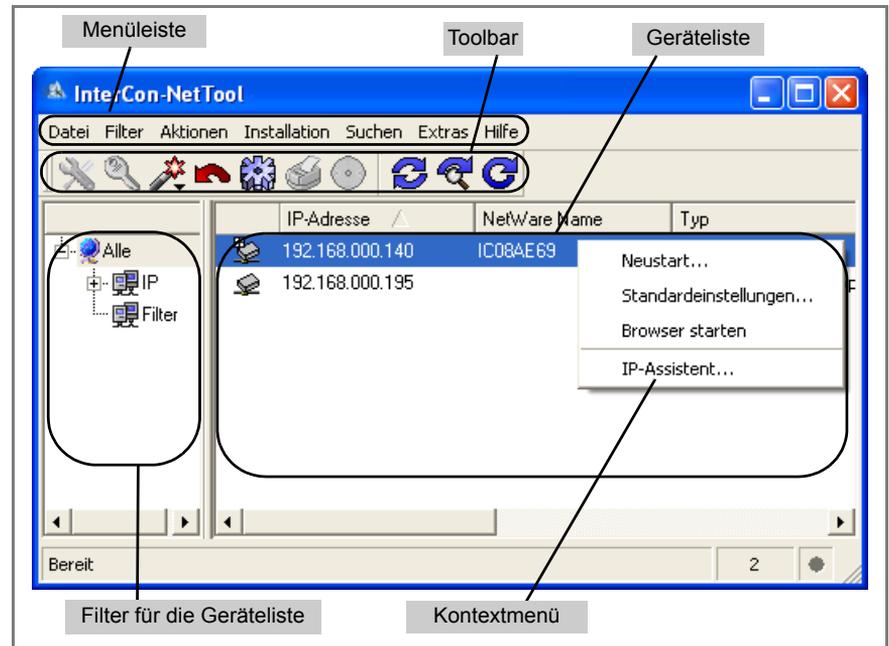


Abb. 2: InterCon-NetTool - Hauptdialog

Welche Funktionen werden unterstützt?

Über das InterCon-NetTool können Sie

- dem 'TPG eine IPv4-Adresse zuweisen' ⇨ 27
- das 'TPG neu starten' ⇨ 81
- die 'Parameterwerte des TPG auf die Standardeinstellung zurücksetzen' ⇨ 77
- das 'TPG Control Center starten' ⇨ 18
- vom 'BIOS-Modus in den Standardmodus wechseln' ⇨ 107



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, das TPG über E-Mail und somit von jedem internetfähigen Rechner aus zu administrieren.

Funktionalitäten

Mit einer E-Mail können Sie

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

Voraussetzung

- Damit das TPG E-Mails empfangen kann, muss das TPG als Benutzer mit eigener E-Mail-Adresse auf einem POP3-Server eingerichtet sein.
- Auf dem TPG ist ein DNS-Server konfiguriert; siehe: ⇨ [31](#).
- Am TPG sind POP3- und SMTP-Parameter konfiguriert; siehe: ⇨ [33](#).

Anweisung via E-Mail versenden

Um das TPG 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 TPG-Adresse ein.
 4. Geben Sie eine Anweisung in die Betreffzeile ein; siehe: 'Syntax und Format der Anweisung' ⇨ [23](#).
 5. Versenden Sie die E-Mail.
-  Das TPG 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 TPG.
	get parameters	Sendet die Parameterliste des TPG.
	set parameters	Sendet Parameter zum TPG. Syntax und Wertekonventionen entnehmen Sie der Parameterliste; siehe:  91. Parameter und Wert sind in den E-Mail-Textkörper zu schreiben.
	update tpg	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 TPG ist eine TAN erforderlich. Eine aktuelle TAN erhalten Sie vom TPG 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> = <value>`

Syntax und Wertekonventionen entnehmen Sie der Parameterliste; siehe: ⇒ 91.

Beispiel 1

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

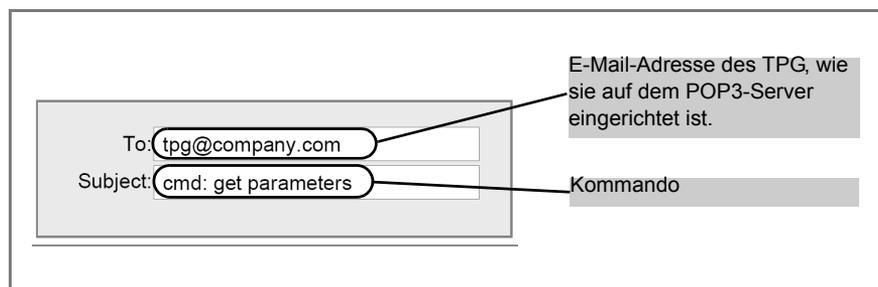


Abb. 3: Administration via E-Mail - Beispiel 1

Beispiel 2

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

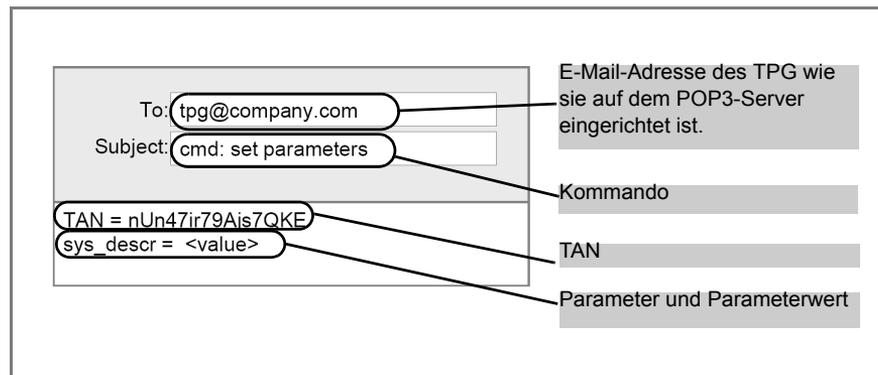


Abb. 4: Administration via E-Mail - Beispiel 2

2.4 Administration via Status-/Reset-Taster am Gerät

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

Über den Status-/Reset-Taster können Sie

- eine Statusseite drucken; siehe: ⇨ 82.
- eine Serviceseite drucken; siehe: ⇨ 82.
- die TPG-Parameter auf die Standardeinstellung zurücksetzen; siehe: ⇨ 77.

3 Netzwerk- und Geräteeinstellungen



Zur optimalen Integration des TPG in ein Netzwerk können verschiedene Einstellungen definiert werden. Zudem können verschiedene Geräteeinstellungen konfiguriert werden. In diesem Kapitel erfahren Sie, welche Netzwerk- und Geräteeinstellungen unterstützt werden.

Welche Information benötigen Sie?

- 'Wie konfiguriere ich IPv4-Parameter?' ⇨ [27](#)
- 'Wie konfiguriere ich IPv6-Parameter?' ⇨ [29](#)
- 'Wie konfiguriere ich den DNS?' ⇨ [31](#)
- 'Wie konfiguriere ich SNMP?' ⇨ [32](#)
- 'Wie konfiguriere ich POP3 und SMTP?' ⇨ [33](#)
- 'Wie konfiguriere ich Bonjour?' ⇨ [36](#)
- 'Wie konfiguriere ich die Gerätezeit?' ⇨ [37](#)
- 'Wie lege ich eine Beschreibung fest?' ⇨ [38](#)
- 'Wie verwende ich den Benachrichtigungsservice?' ⇨ [39](#)

Was möchten
Sie tun?

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 TPG in ein TCP/IP-Netzwerk können Sie verschiedene IPv4-Parameter definieren. Für weitere Informationen zur IP-Adressenvergabe, siehe: ⇨ [13](#).

- 'IPv4-Parameter via TPG Control Center konfigurieren' ⇨ [27](#)
- 'IPv4-Parameter via InterCon-NetTool konfigurieren' ⇨ [28](#)

IPv4-Parameter via TPG Control Center konfigurieren

 Gehen Sie wie folgt vor:

1. Starten Sie das TPG Control Center.
 2. Wählen Sie den Menüpunkt **NETZWERK - IPv4 an**.
 3. Konfigurieren Sie die IPv4-Parameter; siehe: [Tabelle 2](#) ⇨ [27](#).
 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 TPG zu speichern. (Siehe 'Speichern der IP-Adresse im TPG' ⇨ 13 .) Es empfiehlt sich, diese Optionen zu deaktivieren, sobald das TPG eine IP-Adresse zugewiesen bekommen hat.
IP-Adresse	IP-Adresse des TPG
Netzwerkmaske	Netzwerkmaske des TPG
Gateway	Gateway-Adresse des TPG

Voraussetzung

IPv4-Parameter via InterCon-NetTool konfigurieren

- Das InterCon-NetTool ist auf dem Client installiert; siehe: ⇒ 20.
- Im InterCon-NetTool ist die Netzwerksuche via Multicast aktiviert.
- Der Router im Netzwerk leitet Multicast-Anfragen weiter.

 Gehen Sie wie folgt vor:

1. *Starten Sie das InterCon-NetTool.*
 2. *Markieren Sie das TPG in der Geräteliste.*
Das TPG 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.

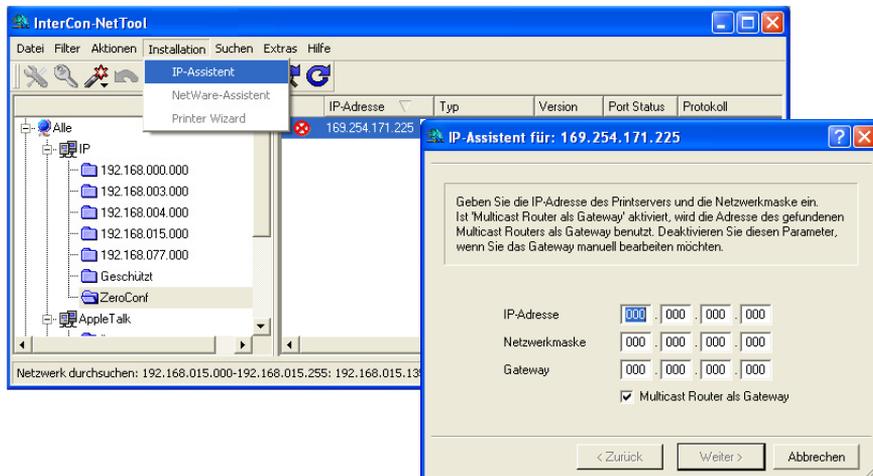


Abb. 5: InterCon-NetTool - IP-Assistent

Welche Vorteile bietet IPv6?

Wie wird eine IPv6-Adresse dargestellt?

3.2 Wie konfiguriere ich IPv6-Parameter?

Sie haben die Möglichkeit, das TPG in ein IPv6-Netzwerk einzubinden.

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

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

Welche IPv6-Adresstypen gibt es?



Die URL wird ausschließlich von IPv6-fähigen Browsern akzeptiert.

IPv6-Adressen lassen sich in verschiedene Typen einteilen. Anhand der Präfixe in den IPv6-Adressen lassen sich IPv6-Adresstypen 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 TPG Control Center.*
 2. *Wählen Sie den Menüpunkt **NETZWERK - IPv6** an.*
 3. *Konfigurieren Sie die IPv6-Parameter; siehe: Tabelle 3 ⇒ 31.*
 4. *Bestätigen Sie mit **Speichern & Neustart**.*
- ↪ Die Einstellungen werden gespeichert.

Tabelle 3: IPv6-Parameter

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

3.3 Wie konfiguriere ich den DNS?

DNS (Domain Name Service) erlaubt die gegenseitige Zuordnung von Namen und Adressen. Wird ein DNS-Server in Ihrem Netzwerk betrieben, haben Sie die Möglichkeit, den DNS für Ihr TPG 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 TPG Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK – DNS** an.
3. Konfigurieren Sie die DNS-Parameter; siehe: Tabelle 4  32.
4. Bestätigen Sie mit **Speichern & Neustart**.

 Die Einstellungen werden gespeichert.

Tabelle 4: DNS-Parameter

Parameter	Beschreibung
DNS	De-/aktiviert den DNS.
Erster DNS-Server	Definiert die IP-Adresse des ersten DNS-Servers (z.B. 192.168.0.21).
Zweiter DNS-Server	Definiert die IP-Adresse des zweiten DNS-Servers. <i>Der zweite DNS-Server wird benutzt, wenn der erste nicht verfügbar ist.</i>
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 TPG oder Druckern) bereitgestellt werden. Das TPG unterstützt SNMP in der Version 1 und 3.

SNMPv1

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



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

SNMPv3

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

 Gehen Sie wie folgt vor:

1. Starten Sie das TPG Control Center.
 2. Wählen Sie den Menüpunkt **NETZWERK – SNMP an**.
 3. Konfigurieren Sie die **SNMP-Parameter**; siehe: Tabelle 5 ⇔  33.
 4. Bestätigen Sie mit **Speichern & Neustart**.
-  Die Einstellungen werden gespeichert.

Tabelle 5: SNMP-Parameter

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

3.5 Wie konfiguriere ich POP3 und SMTP?

Damit am TPG die Administration via E-Mail (⇔  22) und der Benachrichtigungsservice (⇔  39) funktionieren, müssen die Protokolle POP3 und SMTP am TPG 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 TPG wird POP3 benötigt, um das TPG via E-Mail zu administrieren.

SMTP

Was möchten
Sie tun?

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

- 'POP3 konfigurieren' ⇨  34
- 'SMTP konfigurieren' ⇨  35

POP3 konfigurieren

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
 2. *Wählen Sie den Menüpunkt NETZWERK - E-Mail an.*
 3. *Konfigurieren Sie die POP3-Parameter; siehe: Tabelle 6 ⇨  34.*
 4. *Bestätigen Sie mit Speichern & Neustart.*
-  Die Einstellungen werden gespeichert.

Tabelle 6: POP3-Parameter

Parameter	Beschreibung
POP3	De-/aktiviert die POP3-Funktionalität.
POP3 - Servername	Name des POP3-Servers.
POP3 - Serverport	Definiert den Port, über den das TPG E-Mails empfängt. Die Portnummer 110 ist voreingestellt. Bei Verwendung von SSL/TLS ist als Portnummer 995 einzutragen.
POP3 - Sicherheit	Definiert das anzuwendende Authentifizierungsverfahren. (APOP / SSL/TLS)
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 TPG akzeptierten E-Mails. (0 = unbegrenzt)
POP3 - Benutzername	Definiert den Benutzernamen, den das TPG benutzt, um sich mit dem POP3-Server zu verbinden.
POP3 - Passwort	Definiert das Benutzerpasswort, das das TPG benutzt, um sich mit dem POP3-Server zu verbinden.

SMTP konfigurieren

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
 2. *Wählen Sie den Menüpunkt NETZWERK - E-Mail an.*
 3. *Konfigurieren Sie die SMTP-Parameter; siehe: Tabelle 7 ⇨  35.*
 4. *Bestätigen Sie mit Speichern & Neustart.*
-  Die Einstellungen werden gespeichert.

Tabelle 7: SMTP-Parameter

Parameter	Beschreibung
SMTP - Servername	Definiert den Namen des SMTP-Servers.
SMTP - Serverport	Definiert die Portnummer, über die der SMTP-Server E-Mails von dem TPG empfängt. Die Portnummer 25 ist voreingestellt.
SMTP - TLS	De-/aktiviert die Option TLS. <i>Über das Sicherheitsprotokoll Transport Layer Security (TLS) wird der Übertragungsweg vom TPG zum SMTP-Server verschlüsselt.</i>
SMTP - Name des Absenders	Definiert den Absendernamen, den eine vom TPG generierte E-Mail enthalten soll.
SMTP - Login	De-/aktiviert die SMTP-Authentifizierung für das Login.
SMTP - Benutzername	Definiert den Benutzernamen für die SMTP-Authentifizierung.
SMTP - Passwort	Definiert das Passwort für die SMTP-Authentifizierung.
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. <i>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 (⇨  57) benötigt.</i>
SMTP - Vollständig verschlüsseln	Definiert das Verschlüsseln von E-Mails. <i>Eine verschlüsselte E-Mail kann nur vom Empfänger geöffnet und gelesen werden. Für die Verschlüsselung wird ein S/MIME-Zertifikat (⇨  57) benötigt.</i>

Parameter	Beschreibung
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.

Das TPG 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 das TPG eine Anfrage an das Netzwerk. Ist die IP-Adresse im Netzwerk schon belegt, erhält das TPG eine entsprechende Antwort. Das TPG startet dann eine weitere Anfrage mit einer anderen IP-Adresse. Ist die IP-Adresse noch frei, speichert das TPG 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 Dienstenamen und die angebotenen Dienste jedes Teilnehmers.

 Gehen Sie wie folgt vor:

1. Starten Sie das TPG Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - Bonjour an**.

3. Konfigurieren Sie die Bonjour-Parameter; siehe: Tabelle 8
⇒  37.
4. Bestätigen Sie mit Speichern & Neustart.
⇒ Die Einstellung wird gespeichert.

Tabelle 8: Bonjour-Parameter

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

3.7 Wie konfiguriere ich die Gerätezeit?

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

Nutzen und Zweck

Ist der Time-Server aktiviert, erhalten die ThinPrint-Druckaufträge, die über das TPG abgewickelt werden, einen Zeitstempel. In der 'Job History' (⇒  84) werden dann Datum und Uhrzeit angezeigt.

UTC

Als Basis verwendet das TPG '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 länder-spezifischer 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 TPG 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 & Neustart.*
-  Die Einstellungen werden gespeichert.

3.8 Wie lege ich eine Beschreibung fest?

Sie haben die Möglichkeit, dem TPG 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 TPG Control Center.*
 2. *Wählen Sie den Menüpunkt GERÄT – Beschreibung an.*
 3. *Geben Sie in die Felder Hostname, Beschreibung und Ansprechpartner freidefinierbare Bezeichnungen ein.*
 4. *Bestätigen Sie mit Speichern & Neustart.*
-  Die Daten werden gespeichert.

3.9 Wie verwende ich den Benachrichtigungsservice?

Sie haben die Möglichkeit, Benachrichtigungen in Form von E-Mails oder SNMP-Traps vom TPG 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 TPG.
- Die Event-Benachrichtigung informiert über ein bestimmtes Ereignis am TPG via E-Mail oder SNMP-Trap. Das Ereignis kann sein:
 - Der Neustart des TPG.
 - Das Anschließen oder Entfernen eines USB-Sticks am TPG.
 - Ein Problem am TPG.

Was möchten
Sie tun?

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

Voraussetzung

Versand von Status-E-Mails konfigurieren

- Am TPG sind SMTP-Parameter konfiguriert; siehe: ⇨  33.
- Auf dem TPG ist ein DNS-Server konfiguriert; siehe: ⇨  31.

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

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG 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-Benachrichtigungszeit das Sendeintervall.*

Voraussetzung

6. *Bestätigen Sie mit Speichern & Neustart.*

 Die Einstellungen werden gespeichert.

Event-Benachrichtigung via E-Mail konfigurieren

Am TPG sind SMTP-Parameter konfiguriert; siehe:  33.

Auf dem TPG ist ein DNS-Server konfiguriert; siehe:  31.

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

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG 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 & Neustart.*

 Die Einstellungen werden gespeichert.

Event-Benachrichtigung via SNMP-Trap konfigurieren

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

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG 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 & Neustart.*

 Die Einstellungen werden gespeichert.

4 ThinPrint-Einstellungen



Damit das TPG 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?

- 'Wie definiere ich den ThinPrint-Port?' ⇨ 42
- 'Wie definiere ich die Bandbreite?' ⇨ 42
- 'Wie binde ich die Drucker ein?' ⇨ 43
- 'Wie definiere ich Timeouts?' ⇨ 46
- 'Wie erhalte ich Statusinformationen zu den Druckerverbindungen?' ⇨ 47
- 'Wie erhalte ich Drucker Meldungen?' ⇨ 48
- 'Wie verwende ich den ThinPrint Connection Service?' ⇨ 49
- 'Wie empfängt das TPG verschlüsselte Daten?' ⇨ 51



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

4.1 Wie definiere ich den ThinPrint-Port?

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

Am TPG 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 TPG 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 & Neustart.*

 Die Einstellung wird gespeichert.

4.2 Wie definiere ich die Bandbreite?

Die Bandbreite beschreibt die Kapazität einer Datenverbindung. Beim TPG 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 TPG) das Bandbreitenlimit am Port weiter herabzusetzen.



Das Setzen eines Bandbreitenwerts am TPG, 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 TPG 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 & Neustart.*

 Die Einstellung wird gespeichert.

4.3 Wie binde ich die Drucker ein?

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

Die Zuteilung der Druckaufträge erfolgt über die Drucker-ID. Es können bis zu zwei (TPG-25) bzw. sechs (TPG-65) Netzwerkdrucker über das TPG eingebunden werden.

Beim Einbinden der angeschlossenen Netzwerkdrucker sind die Druckerparameter (Name, Klasse, Treiber, Adresse) und eine Übertragungsmethode zu definieren.

Die Übertragung der Daten zwischen dem TPG und den Netzwerkdruckern kann durch drei Methoden erfolgen:

- Standardmäßig werden die Daten über eine **RAW-/Socketverbindung** auf einen TCP/IP-Port übertragen. Am TPG 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 TPG 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' (⇒ 84) dargestellt werden.



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



Gehen Sie wie folgt vor:

1. Starten Sie das TPG Control Center.
 2. Wählen Sie den Menüpunkt **GERÄT - ThinPrint® an**.
 3. Geben Sie in den Feldern die Drucker-Parameter ein; siehe: Tabelle 9 ⇒ 44.
 4. Wählen Sie für jeden Drucker eine Übertragungsmethode.
 5. Bestätigen Sie mit **Speichern & Neustart**.
- Die Einstellungen werden gespeichert.

Tabelle 9: Drucker-Parameter

Parameter	Beschreibung
ID	Über die ID werden die Drucker beim ThinPrint Server identifiziert.
Drucker	Definiert den Druckernamen. Dieser ist eine reine Beschreibung und dient zur Unterscheidung der Drucker. <i>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.</i>
Klasse	Drucker, deren Treiber untereinander kompatibel sind, können zu einer Klasse zusammengefasst werden. <i>Das Hinterlegen einer Druckerklasse ist (neben dem Hinterlegen des Druckernamens) 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.</i>
Treiber	Definiert den Druckertreiber für das ThinPrint® AutoConnect-Verfahren.

Parameter	Beschreibung
Druckeradresse	Definiert die IP-Adresse oder den Hostnamen des Druckers. <i>Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.</i>
Port	Definiert die Portnummer für das RAW/Socket-Printing. (Default = 9100) <i>Wird verwendet, wenn als Übertragungsmethode 'RAW' gewählt wurde.</i>
URL	Definiert den zweiten Teil der Drucker-URL für das IPP-Printing. (Default = ipp/lp1) <i>Wird verwendet, wenn als Übertragungsmethode 'IPP' gewählt wurde.</i>
SSL	De-/aktiviert die SSL-/TLS-Verschlüsselung für das IPP-Printing. <i>Wird verwendet, wenn als Übertragungsmethode 'IPP' gewählt wurde.</i>
LPD-Queue	Definiert den Queue-Namen für das LPD-Printing. (Default = lp1) <i>Wird verwendet, wenn als Übertragungsmethode 'LPD' gewählt wurde.</i>
RFC	De-/aktiviert das RFC1179-konforme LPD-Printing. <i>Wird verwendet, wenn als Übertragungsmethode 'LPD' gewählt wurde. Ist diese Option deaktiviert, ähnelt das Verhalten dem Microsoft-LPD-Printing.</i>

**Druckerverbindungs
abbruch****Timeout für das
Senden von
Druckaufträgen**

4.4 Wie definiere ich Timeouts?

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

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 das TPG physikalisch nicht erreichbar ist und der ThinPrint-Port für nachfolgende Druckaufträge freigemacht werden soll.

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 TPG 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 & Neustart.*
-  Die Einstellungen werden gespeichert.

4.5 Wie erhalte ich Statusinformationen zu den Druckerverbindungen?

Sie haben die Möglichkeit, die Verbindungsstatus der eingebundenen Drucker anzeigen zu lassen. Folgende Verbindungsstatus können angezeigt werden:

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.



Um den Verbindungsstatus erhalten zu können, müssen Sie eine 'ping'-Abfrage konfigurieren.

Was möchten Sie tun?

- 'ping'-Abfrage via TPG Control Center konfigurieren' ⇒ 47
- 'Druckerverbindungsstatus via TPG Control Center anzeigen' ⇒ 48

'ping'-Abfrage via TPG Control Center konfigurieren

Gehen Sie wie folgt vor:

1. Starten Sie das TPG 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 & Neustart.
- Die Einstellungen werden gespeichert.

Druckerverbindungsstatus via TPG Control Center anzeigen

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
 2. *Wählen Sie den Menüpunkt GERÄT - ThinPrint®-Drucker an.*
-  Der Druckerverbindungsstatus wird unter 'ThinPrint®-Druckerstatus' in der Spalte 'Status' angezeigt und ist den Drucker-IDs zugeordnet.

4.6 Wie erhalte ich Druckermeldungen?

Sie haben die Möglichkeit, Druckerfehlermeldungen (Kein Papier, Offline, Papierstau usw.) und Druckerstatusmeldungen (Ruhezustand, Aufwärmphase usw.) anzeigen zu lassen. Um Druckermeldungen erhalten zu können, müssen Sie zuvor eine SNMP-Abfrage konfigurieren.



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

Was möchten
Sie tun?

- 'SNMP-Abfrage via TPG Control Center konfigurieren' ⇨  48
- 'Druckermeldungen via TPG Control Center anzeigen' ⇨  49

Voraussetzung

SNMP-Abfrage via TPG Control Center konfigurieren

- Der Drucker unterstützt SNMP.

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG 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 & Neustart.*
-  Die Einstellungen werden gespeichert.

Druckermeldungen via TPG Control Center anzeigen

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
 2. *Wählen Sie den Menüpunkt GERÄT - ThinPrint®-Drucker an.*
- ↳ Die Druckermeldungen werden unter 'ThinPrint®-Druckerstatus' in der Spalte 'Status' angezeigt und sind den Drucker-IDs zugeordnet.

4.7 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 das TPG) 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 das TPG 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 TPG eingerichtet werden.



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

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG 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 10 ⇨  50.*

5. Bestätigen Sie mit Speichern & Neustart.

↪ Die Einstellungen werden gespeichert.

Tabelle 10: 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. <i>Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.</i>
Port	Definiert den TCP-Port, über den das TPG mit dem Connection Service kommuniziert. <i>Die Portnummer 4001 ist voreingestellt.</i>
Client-ID	Client-ID, mit der das TPG in der Datenbank des Connection Services hinterlegt ist. Der Connection Service benötigt die Client-ID, um Druckaufträge an das TPG zu senden.
Authentifizierungsschlüssel	Authentifizierungsschlüssel, mit dem das TPG 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 gleich oder kleiner als der auf dem Connection Service-Server eingestellte Wert 'KeepAliveTO' sein. <i>(Erlaubte Eingabe 1 - 60000 Default = 60)</i>
Erneuter Verbindungsversuch	Definiert das Zeitintervall (in Sekunden), nach dem ein erneuter Verbindungsversuch stattfindet, wenn der Connection Service nicht erreichbar ist. <i>(Erlaubte Eingabe 1 - 60000 Default = 120)</i>



Der Verbindungsstatus wird hinter der Option 'Connection Service' 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 & Neustart** an.

4.8 Wie empfängt das TPG verschlüsselte Daten?

Eine sichere Verbindung beim Versenden von Druckaufträgen zwischen ThinPrint (Server oder Connection Service) und dem TPG wird durch den Einsatz einer SSL-/TLS-Verschlüsselung ermöglicht.

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

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

- Erstellen Sie eine Zertifikatsanforderung; siehe: ⇒  61.
- Speichern Sie das CA-Zertifikat; siehe: ⇒  62.

5 Sicherheit



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

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

Welche Information benötigen Sie?

- 'Wie kontrolliere ich den Zugang zum TPG Control Center?'
⇒ 53
- 'Wie kontrolliere ich den Zugriff auf das TPG? (TCP-Portzugriffskontrolle)' ⇒ 55
- 'Wie setze ich Zertifikate korrekt ein?' ⇒ 57
- 'Wie verwende ich Authentifizierungsmethoden?' ⇒ 65

5.1 Wie kontrolliere ich den Zugang zum TPG Control Center?

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

Was möchten Sie tun?

- 'Erlaubten Webverbindungstypen definieren' ⇨ 53
- 'Webzugang via Passwort schützen' ⇨ 54



Zusätzlich kann das TPG 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?' ⇨ 32.

Verbindungstyp (HTTP/HTTPS)

Erlaubten Webverbindungstypen definieren

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

Wird ausschließlich HTTPS als Verbindungstyp gewählt, ist der administrative Webzugang zum TPG Control Center via SSL/TLS geschützt.

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



Gehen Sie wie folgt vor:

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

↪ Die Einstellung wird gespeichert.

Webzugang via Passwort schützen

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



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

 Gehen Sie wie folgt vor:

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

5.2 Wie kontrolliere ich den Zugriff auf das TPG? (TCP-Portzugriffskontrolle)

TCP- Portzugriffskontrolle

Sie haben die Möglichkeit, den Zugriff auf das TPG zu kontrollieren. Hierzu können verschiedene TCP-Porttypen am TPG gesperrt werden. Zugriffsberechtigte Netzwerkelemente können als Ausnahme definiert und von der Sperrung ausgenommen werden. Das TPG 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, SMTP-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 TPG 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 TPG 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 TPG.*



Kann das TPG über das TPG Control Center nicht mehr erreicht werden, initiieren Sie einen Geräte-Neustart; siehe: ⇨  81.

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.

5.3 Wie setze ich Zertifikate korrekt ein?

Das TPG 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 TPG,

- um verschlüsselte Druckdaten zu empfangen; siehe: ⇨ [51](#).
- um die Identität des TPG im Netzwerk überprüfen zu lassen; siehe: 'EAP-TLS konfigurieren' ⇨ [66](#).
- um das TPG/den Client zu authentifizieren, wenn der administrative Webzugang des TPG Control Centers via HTTPS (SSL/TLS) geschützt ist; siehe: ⇨ [53](#).



Wenn Sie Zertifikate verwenden, sollten Sie den administrativen Webzugriff zum TPG Control Center zusätzlich mit einem Passwort schützen, so dass kein Unbefugter das Zertifikat auf dem TPG löschen kann; siehe: ⇨ [53](#).

Welche Zertifikate gibt es?

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

- **Selbstsignierte Zertifikate** tragen eine digitale Unterschrift, die vom TPG erstellt wurde. Wird ein selbstsigniertes Zertifikat verwendet, kann von einem ThinPrint Server nicht via SSL/TLS gedruckt werden. Hierzu ist zwingend ein CA-Zertifikat erforderlich.
- **CA-Zertifikate** sind Zertifikate, die von einer Zertifizierungsstelle (Certification Authority - CA) signiert wurden.

- Die Echtheit eines CA-Zertifikates kann mit Hilfe eines **Wurzelzertifikates**, das von der Zertifizierungsstelle ausgegeben wird, überprüft werden. Dieses Wurzelzertifikat wird auf einem Authentifizierungsserver im Netzwerk hinterlegt.
- Bei Auslieferung ist im TPG ein Zertifikat gespeichert, das sog. **Default-Zertifikat**. Sie sollten das Default-Zertifikat zeitnah durch ein selbstsigniertes oder ein CA-Zertifikat ersetzen.
- **S/MIME-Zertifikat**
S/MIME-Zertifikate (*.pem-Datei) werden verwendet zum Signieren und Verschlüsseln der E-Mails, die vom TPG 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.

Im TPG können folgende Zertifikate zeitgleich installiert sein:

- 1 Selbstsigniertes Zertifikat
- 1 CA-Zertifikat oder pkcs(12)-Zertifikat
- 1 Wurzelzertifikat
- 1 S/MIME-Zertifikat

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

Ein pkcs(12)-Zertifikat kann nur installiert werden, wenn aktuell keine Zertifikatsanforderung generiert bzw. kein CA-Zertifikat installiert ist.

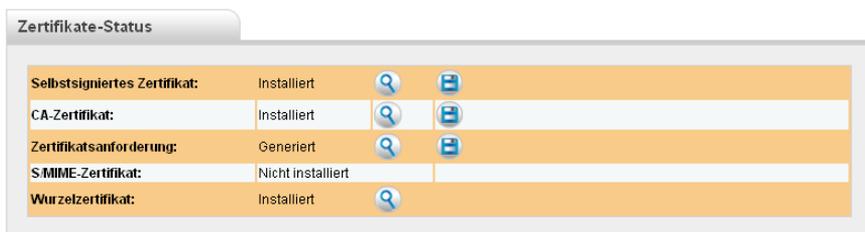


Abb. 6: TPG Control Center - Zertifikate

Was möchten Sie tun?

- 'Zertifikat anzeigen' ⇨ 59
- 'Selbstsigniertes Zertifikat erstellen' ⇨ 60
- 'Zertifikatsanforderung für ein CA-Zertifikat erstellen' ⇨ 61
- 'CA-Zertifikat auf dem TPG speichern' ⇨ 62
- 'Wurzelzertifikat auf dem TPG speichern' ⇨ 62
- 'pkcs(12)-Zertifikat auf dem TPG speichern' ⇨ 63
- 'S/MIME-Zertifikat auf dem TPG speichern' ⇨ 64
- 'Zertifikat löschen' ⇨ 64

Zertifikat anzeigen

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

Gehen Sie wie folgt vor:

1. Starten Sie das TPG 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 TPG erstellt worden, muss dieses zunächst gelöscht werden; siehe: ⇨ 64.



Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
 2. *Wählen Sie den Menüpunkt SICHERHEIT - Zertifikate an.*
 3. *Wählen Sie die Schaltfläche Selbstsigniertes Zertifikat an.*
 4. *Geben Sie die entsprechenden Parameter ein; siehe: Tabelle 11 ⇨ 60.*
 5. *Wählen Sie die Schaltfläche Erstellen/Installieren an.*
- ↳ Das Zertifikat wird erstellt und installiert. Dieser Vorgang kann einige Minuten dauern.

Tabelle 11: Parameter für die Erstellung von Zertifikaten

Parameter	Beschreibung
Allgemeiner Name	Dient der eindeutigen Identifizierung des Zertifikats. Es empfiehlt sich, hier z.B. die IP-Adresse oder den Hostnamen des TPG zu verwenden, um eine eindeutige Zuordnung des Zertifikats zum TPG 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 das TPG 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.

Zertifikatsanforderung für ein CA-Zertifikat erstellen

Als Vorbereitung auf das Verwenden eines CA-Zertifikates kann im TPG eine Zertifikatsanforderung erstellt werden, die an die Zertifizierungsstelle gesendet werden muss. Die Zertifizierungsstelle erstellt anhand der Zertifikatsanforderung ein CA-Zertifikat. Das Zertifikat muss im 'Base 64'-Format vorliegen.



Ist bereits eine Zertifikatsanforderung auf dem TPG erstellt worden, wird sie überschrieben.



Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
2. *Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate an**.*
3. *Wählen Sie die Schaltfläche **Zertifikatsanforderung an**.*
4. *Geben Sie die benötigten Parameter ein; siehe: Tabelle 11 ⇨ 60.*
5. *Wählen Sie die Schaltfläche **Anforderung erstellen an**. Die Zertifikatsanforderung wird erstellt. Dieser Vorgang kann einige Minuten dauern.*
6. *Wählen Sie die Schaltfläche **Upload an** und speichern Sie die Anforderung in einer Textdatei.*
7. *Wählen Sie die Schaltfläche **OK an**.*
8. *Senden Sie die Textdatei als Zertifikatsanforderung an eine Zertifizierungsstelle.*

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

CA-Zertifikat auf dem TPG speichern



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

Voraussetzung

Es wurde zuvor eine entsprechende Zertifikatsanforderung erstellt; siehe: ⇨ [61](#).

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



Gehen Sie wie folgt vor:

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

⇨ Das CA-Zertifikat wird auf dem TPG gespeichert.

Wurzelzertifikat auf dem TPG speichern

Um in einem Netzwerk die Identität des TPG zu überprüfen, bietet das TPG mehrere Authentifizierungsverfahren an. Wenn Sie das Authentifizierungsverfahren 'EAP-TLS' verwenden, ist es erforderlich, das Wurzelzertifikat des Authentifizierungsservers (RADIUS) auf dem TPG zu installieren; siehe: ⇨ [66](#).



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

Voraussetzung

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



Gehen Sie wie folgt vor:

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

3. Wählen Sie die Schaltfläche **Wurzelzertifikat an**.
 4. Wählen Sie die Schaltfläche **Durchsuchen an**.
 5. Geben Sie das **Wurzelzertifikat an**.
 6. Wählen Sie die Schaltfläche **Installieren an**.
- ☞ Das Wurzelzertifikat wird auf dem TPG gespeichert.

pkcs(12)-Zertifikat auf dem TPG 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 TPG installiert, wird es überschrieben.

Voraussetzung

- Das Zertifikat muss im 'Base 64'-Format vorliegen.
- Es darf keine Zertifikatsanforderung vorliegen. Um die Zertifikatsanforderung zu löschen, siehe: ☞ 64.
- Es darf kein CA-Zertifikat installiert sein. Um ein CA-Zertifikat zu löschen, siehe: ☞ 64.



Gehen Sie wie folgt vor:

1. Starten Sie das **TPG Control Center**.
 2. Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate an**.
 3. Wählen Sie die Schaltfläche **pkcs12-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 TPG gespeichert.

Voraussetzung**S/MIME-Zertifikat auf dem TPG speichern**

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



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

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



Gehen Sie wie folgt vor:

1. *Starten Sie das TPG 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 TPG gespeichert.

Zertifikat löschen

Gehen Sie wie folgt vor:

1. *Starten Sie das TPG 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.

5.4 Wie verwende ich Authentifizierungsmethoden?

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

Was ist IEEE 802.1x?

Der Standard IEEE 802.1x stellt eine Grundstruktur für verschiedene Authentifizierungs- und Schlüsselmanagementsprotokolle 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 authentifizieren. Nach erfolgreicher Authentifizierung 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 Benutzeranmeldeinformationen überprüft und Zugriff auf die gewünschten Ressourcen gewährt.

Damit das TPG sich an einem geschützten Netzwerk authentifizieren kann, unterstützt das TPG mehrere EAP-Authentifizierungsverfahren.

Was möchten Sie tun?

- 'EAP-MD5 konfigurieren' ⇨  66
- 'EAP-TLS konfigurieren' ⇨  66
- 'EAP-TTLS konfigurieren' ⇨  68
- 'PEAP konfigurieren' ⇨  69
- 'EAP-FAST konfigurieren' ⇨  70

EAP-MD5 konfigurieren

Nutzen und Zweck

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

Funktionsweise

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

Voraussetzung

Auf dem RADIUS-Server ist das TPG als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG 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 das TPG 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 das TPG in geschützten Netzwerken einen Zugriff erhält, haben Sie die Möglichkeit, das TPG für die EAP-TLS-Netzwerkauthentifizierung zu konfigurieren.

Funktionsweise

EAP-TLS beschreibt eine zertifikatbasierte Authentifizierung über einen RADIUS-Server. Hierzu werden zwischen dem TPG und dem RADIUS-Server Zertifikate ausgetauscht. Dabei wird eine verschlüsselte TLS-Verbindung zwischen TPG und RADIUS-Server aufgebaut. Sowohl RADIUS-Server als auch TPG 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 das TPG im Netzwerk möglicherweise nicht angesprochen werden. Setzen Sie in diesem Fall die TPG-Parameter zurück; siehe: ⇨ [77](#).

Vorgehensweise

- Erstellen Sie auf dem TPG eine Zertifikatsanforderung; siehe: 'Zertifikatsanforderung für ein CA-Zertifikat erstellen' ⇨ [61](#).
- Erstellen Sie mit der Zertifikatsanforderung und mit Hilfe des Authentifizierungsservers ein CA-Zertifikat.
- Installieren Sie das CA-Zertifikat auf dem TPG; siehe: 'CA-Zertifikat auf dem TPG speichern' ⇨ [62](#).
- Installieren Sie das Wurzelzertifikat des Authentifizierungsservers auf dem TPG; siehe: 'Wurzelzertifikat auf dem TPG speichern' ⇨ [62](#).
- Aktivieren Sie das Authentifizierungsverfahren 'EAP-TLS' auf dem TPG.



Gehen Sie wie folgt vor:

1. *Starten Sie das TPG 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 das TPG in geschützten Netzwerken einen Zugriff erhält, haben Sie die Möglichkeit, das TPG 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 TPG und RADIUS-Server aufgebaut. Dazu identifiziert sich nur der RADIUS-Server mit einem von einer CA unterschriebenen Zertifikat beim TPG. 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 das TPG als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

👉 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG 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 das TPG auf dem RADIUS-Server eingerichtet ist.
 5. Wählen Sie die **Einstellungen**, mit denen die Kommunikation im TLS-Tunnel gesichert werden soll.
 6. Installieren Sie optional ein **Wurzelzertifikat** des RADIUS-Servers auf dem TPG (⇒ 62), um die Sicherheit beim Verbindungsaufbau zu erhöhen.
 7. **Bestätigen Sie mit Speichern & Neustart**.
- ↪ Die Einstellungen werden gespeichert.

PEAP konfigurieren

Nutzen und Zweck

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

Funktionsweise

Beim PEAP wird (wie bei EAP-TTLS, vgl. ⇒ 68) zunächst ein verschlüsselter TLS-Tunnel (Transport Layer Security) zwischen TPG und RADIUS-Server aufgebaut. Dazu identifiziert sich nur der RADIUS-Server mit einem von einer CA unterschriebenen Zertifikat beim TPG.

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 das TPG als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
 2. *Wählen Sie den Menüpunkt **SICHERHEIT - Authentifizierung an.***
 3. *Wählen Sie aus der Liste **Authentifizierungsmethode** den Eintrag **PEAP.***
 4. *Geben Sie Benutzernamen und Passwort ein, mit denen das TPG auf dem RADIUS-Server eingerichtet ist.*
 5. *Wählen Sie die Einstellungen, mit denen die Kommunikation im TLS-Tunnel gesichert werden soll.*
 6. *Installieren Sie optional ein Wurzelzertifikat des RADIUS-Servers auf dem TPG (⇒  62), um die Sicherheit beim Verbindungsaufbau zu erhöhen.*
 7. *Bestätigen Sie mit **Speichern & Neustart.***
-  Die Einstellungen werden gespeichert.

EAP-FAST konfigurieren**Nutzen und Zweck**

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

Funktionsweise

EAP-FAST nutzt (wie EAP-TTLS, vgl. ⇒  68) einen Tunnel zum Schutz der Datenübertragung. Der Hauptunterschied besteht darin, dass EAP-FAST keine Zertifikate zum Authentifizieren benötigt. (Die Verwendung von Zertifikaten ist optional.)

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

- Einen gemeinsamen geheimen Schlüssel, der den zwischen dem TPG und dem RADIUS-Server geteilten Schlüssel enthält.

Voraussetzung

- Ein undurchsichtiges Element, das dem TPG zur Verfügung steht und dem RADIUS-Server vorgelegt wird, wenn das TPG 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 TPG sowie die Lieferung der PACs zu schützen.

- Auf dem RADIUS-Server ist das TPG als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG 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 das TPG auf dem RADIUS-Server eingerichtet ist.*
 5. *Wählen Sie die Einstellungen, mit denen die Kommunikation im Tunnel gesichert werden soll.*
 6. *Bestätigen Sie mit **Speichern & Neustart**.*
-  Die Einstellungen werden gespeichert.

6 Wartung



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

Welche Information benötigen Sie?

- 'Wie sichere ich die TPG-Parameter? (Backup)' ⇨ [73](#)
- 'Wie verwende ich ein angeschlossenes USB-Gerät?' ⇨ [74](#)
- 'Wie setze ich die Parameter auf die Standardwerte zurück? (Reset)' ⇨ [77](#)
- 'Wie führe ich ein Update aus?' ⇨ [80](#)
- 'Wie starte ich das TPG neu?' ⇨ [81](#)
- 'Wie drucke ich eine Status- oder Serviceseite?' ⇨ [82](#)
- 'Wie lasse ich die Job History anzeigen?' ⇨ [84](#)

Was möchten
Sie tun?

6.1 Wie sichere ich die TPG-Parameter? (Backup)

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

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

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

- 'Parameterwerte anzeigen' ⇨  73
- 'Parameterdatei sichern' ⇨  73
- 'Parameterdatei auf ein TPG laden' ⇨  74

Parameterwerte anzeigen

 Gehen Sie wie folgt vor:

1. Starten Sie das TPG 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' ⇨  91.

Parameterdatei sichern

 Gehen Sie wie folgt vor:

1. Starten Sie das TPG 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 'parameters' mit Hilfe Ihres Browsers auf ein lokales System.
- ↪ Die Parameterdatei wird kopiert und ist gesichert.

Parameterdatei auf ein TPG laden

 Gehen Sie wie folgt vor:

1. Starten Sie das TPG Control Center.
 2. Wählen Sie den Menüpunkt **WARTUNG – Parameter-Backup** an.
 3. Wählen Sie die Schaltfläche **Durchsuchen** an.
 4. Geben Sie die Datei 'parameters' an.
 5. Wählen Sie die Schaltfläche **Importieren** an.
- ↪ Die in der Datei enthaltenen Parameterwerte werden von dem TPG übernommen.



Sie haben zudem die Möglichkeit, eine Parameterdatei von einem USB-Stick automatisch auf ein TPG zu laden; siehe: ⇨  74.

6.2 Wie verwende ich ein angeschlossenes USB-Gerät?

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

Ist ein Drucker nicht verfügbar, können an diesen Drucker gesendete Druckaufträge auf dem USB-Stick automatisch zwischengespeichert werden. Sobald der Drucker wieder verfügbar ist, werden die Aufträge an den Drucker weitergeleitet und gedruckt. Ist diese Option deaktiviert und ein Drucker nicht verfügbar, werden Druckaufträge nach dem spezifizierten Timeout ('Druckerverbindungsabbruch' ⇨  46) verworfen.

**Zwischenspeichern
von Druckaufträgen**

Parameter-Backup

Beim 'Parameter-Backup' wird die Datei 'parameters' automatisch auf dem USB-Stick gespeichert und nach einer Parameteränderung aktualisiert. Die Datei enthält alle Parameterwerte des TPG (Ausnahme: Passwörter). TPG übernehmen die in der Parameterdatei auf dem USB-Stick enthaltenen Werte automatisch. Parameterwerte können so via USB-Stick einfach und schnell auf andere TPG geladen werden (z.B. bei der Konfiguration neuer Geräte).

Formatieren

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



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



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

Was möchten Sie tun?

- 'USB-Stick formatieren' ⇨ 75
- 'Druckaufträge automatisch zwischenspeichern' ⇨ 76
- 'Parameterwerte automatisch speichern' ⇨ 76
- 'Parameterwerte automatisch auf ein TPG laden' ⇨ 76

USB-Stick formatieren**Voraussetzung**

- Es ist ein USB-Stick an das TPG angeschlossen.



Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
 2. *Wählen Sie den Menüpunkt WARTUNG - USB-Gerät an.*
 3. *Wählen Sie die Schaltfläche Formatieren an.*
- ↪ Der USB-Stick wird formatiert.

Voraussetzung**Druckaufträge automatisch zwischenspeichern**

- Es ist ein USB-Stick an das TPG angeschlossen.
- Der USB-Stick ist korrekt formatiert; siehe: ⇨ 75.

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
 2. *Wählen Sie den Menüpunkt WARTUNG - USB-Gerät an.*
 3. *Aktivieren Sie die Option Zwischenspeichern von Druckaufträgen.*
 4. *Wählen Sie die Schaltfläche Speichern & Neustart an.*
-  Die Einstellungen werden gespeichert.

Voraussetzung**Parameterwerte automatisch speichern**

- Es ist ein USB-Stick an das TPG angeschlossen.
- Der USB-Stick ist korrekt formatiert; siehe: ⇨ 75.

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
 2. *Wählen Sie den Menüpunkt WARTUNG - USB-Gerät an.*
 3. *Aktivieren Sie die Option Parameter-Backup.*
 4. *Wählen Sie die Schaltfläche Speichern & Neustart an.*
-  Die Einstellungen werden gespeichert.

Voraussetzung**Parameterwerte automatisch auf ein TPG laden**

- Der USB-Stick ist korrekt formatiert; siehe: ⇨ 75.
- Auf dem USB-Stick ist eine Parameterdatei vorhanden; siehe: ⇨ 74.

 Gehen Sie wie folgt vor:

1. *Schließen Sie einen USB-Stick an den USB-Port des TPG an.*
-  Die in der Datei enthaltenen Parameterwerte werden von dem TPG automatisch übernommen.

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

Sie haben die Möglichkeit, die Parameter des TPG 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 TPG ändern und die Verbindung zum TPG Control Center abbrechen.

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



Entfernen Sie vor dem Reset einen angeschlossenen USB-Stick. Ist auf dem USB-Stick eine Parameterdatei gespeichert, verwendet das TPG nach dem Reset automatisch die auf dem USB-Stick gespeicherten Parameterwerte (siehe: ⇒ 75).



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

Was möchten Sie tun?

- 'Parameter via TPG Control Center zurücksetzen' ⇒ 77
- 'Parameter via InterCon-NetTool zurücksetzen' ⇒ 78
- 'Parameter via Status-/Reset-Taster zurücksetzen' ⇒ 78

Parameter via TPG Control Center zurücksetzen

Gehen Sie wie folgt vor:

1. Starten Sie das TPG 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 das TPG in der Geräteleiste.
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 TPG 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 TPG auf die Standardeinstellung zurücksetzen. Der Reset-Vorgang lässt sich in drei Phasen gliedern.

- In der 1. Phase wird das TPG in den Reset-Modus gezwungen. Im Reset-Modus werden die Parameter zurückgesetzt.
- Die 2. Phase beschreibt den Neustart des Gerätes.
- Die 3. Phase beschreibt das Drucken einer Statusseite. Anhand der Statusseite kann der Erfolg des Reset-Vorganges überprüft werden.

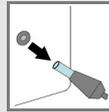


WICHTIG: Der Reset-Modus wird durch das abwechselnd grün-rote Blinken der Activity-LED signalisiert. Anschließend blinkt die Activity-LED orange.

Zu diesem Zeitpunkt muss der Status-/Reset-Taster losgelassen werden, ansonsten fällt das TPG in den BIOS-Modus. Beginnen Sie dann den Reset-Vorgang erneut.

Nachfolgend ist der Ablauf aller Phasen visualisiert.

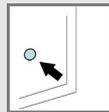
[Phase 1] Reset



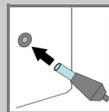
TPG ausschalten
(Stromzufuhr unterbrechen).



Netzwerkabel (RJ-45) vom
TPG entfernen.

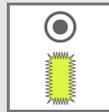


Status-/Reset-Taster drücken
und halten.

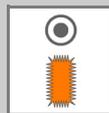


TPG einschalten
(Stromzufuhr herstellen).

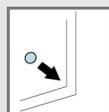
*Die Activity-LED leuchtet
dauerhaft orange.*



Nach einigen Sekunden blinkt
die Activity-LED abwechselnd
grün und rot.

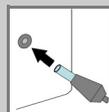


Warten bis die Activity-LED
orange blinkt.

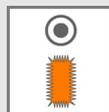


Status-/Reset-Taster (für max. 1
Sek) loslassen.

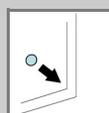
*Die Activity-LED blinkt
abwechselnd grün und rot.*



Status-/Reset-Taster erneut
drücken und halten.



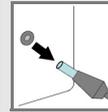
*Die Activity-LED blinkt zweimal
orange.*



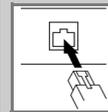
Status-/Reset-Taster loslassen.

Die Activity-LED blinkt grün.

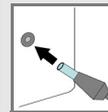
[Phase 2] Gerät neu starten



TPG ausschalten
(Stromzufuhr unterbrechen).

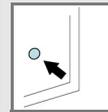


Netzwerkabel (RJ-45) mit dem
TPG verbinden.



TPG einschalten
(Stromzufuhr herstellen).

[Phase 3] Status überprüfen



Status-/Reset-Taster kurz
drücken.

Statusseite wird gedruckt.

6.4 Wie führe ich ein Update aus?

Sie haben die Möglichkeit, Soft- und Firmware-Updates auf dem TPG 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 TPG. Die Versionsnummer entnehmen Sie der Startseite des TPG 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/tpg.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 TPG 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 TPG wird neu gestartet.

Was möchten
Sie tun?

6.5 Wie starte ich das TPG neu?

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

- 'TPG via TPG Control Center neu starten' ⇨ 81
- 'TPG via InterCon-NetTool neu starten' ⇨ 81

TPG via TPG Control Center neu starten

 Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
 2. *Wählen Sie den Menüpunkt WARTUNG – Neustart an.*
 3. *Wählen Sie die Schaltfläche Neustart an.*
-  Das TPG wird neu gestartet.

TPG via InterCon-NetTool neu starten

 Gehen Sie wie folgt vor:

1. *Starten Sie das InterCon-NetTool.*
 2. *Markieren Sie das TPG 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.*
-  Das TPG wird neu gestartet.

6.6 Wie drucke ich eine Status- oder Serviceseite?

Sie haben die Möglichkeit, Statusseiten oder Serviceseiten auszu-
drucken. Beide Seiten sind in der englischen Sprache verfügbar.

Statusseite

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

Serviceseite

Eine Serviceseite enthält TPG-Basisinformationen sowie eine Auflis-
tung der aktuellen Parameterwerte des TPG.



Bevor eine Statusseite oder Serviceseite gedruckt wird, müssen die
Druckfunktion aktiviert sowie der ausführende Drucker und das
Datenformat der Status- bzw. Serviceseite (ASCII, PostScript, DATA-
MAX oder Citizen-Z) spezifiziert werden. Der Drucker mit der ID 1
und das Datenformat ASCII sind voreingestellt.



Der ausführende Drucker wird im Menü **Gerät - ThinPrint®-Drucker**
blau hinterlegt dargestellt.

Was möchten Sie tun?

- 'Druckfunktion, Drucker und Datenformat via TPG Control
Center konfigurieren' ⇨ 82
- 'Statusseite via TPG Control Center drucken' ⇨ 83
- 'Statusseite via Status-/Reset-Taster drucken' ⇨ 83
- 'Serviceseite via TPG Control Center drucken' ⇨ 83
- 'Serviceseite via Status-/Reset-Taster drucken' ⇨ 84

Druckfunktion, Drucker und Datenformat via TPG Control Center konfigurieren

Gehen Sie wie folgt vor:

1. *Starten Sie das TPG Control Center.*
2. *Wählen Sie den Menüpunkt **WARTUNG - Statusseite an.***

3. Wählen Sie aus der Liste **Statusseiten-Drucker** die gewünschte Drucker-ID.
 4. Wählen Sie aus der Liste **Modus Statusseite** das gewünschte Datenformat.
 5. Aktivieren Sie die Option **Drucken**.
 6. Bestätigen Sie mit **Speichern & Neustart**.
- ↪ Die Einstellungen werden gespeichert.

Statusseite via TPG Control Center drucken

 Gehen Sie wie folgt vor:

1. Starten Sie das **TPG Control Center**.
 2. Wählen Sie den Menüpunkt **WARTUNG - Statusseite an**.
 3. Wählen sie die Schaltfläche **Statusseite an**.
- ↪ Die Statusseite wird gedruckt.

Statusseite via Status-/Reset-Taster drucken

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

 Gehen Sie wie folgt vor:

1. Drücken Sie kurz den **Status-/Reset-Taster**.
- ↪ Die Statusseite wird gedruckt.

Serviceseite via TPG Control Center drucken

 Gehen Sie wie folgt vor:

1. Starten Sie das **TPG 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. *Halten Sie den Status-/Reset-Taster fünf Sekunden lang gedrückt.*

 Die Serviceseite wird gedruckt.

6.7 Wie lasse ich die Job History anzeigen?

Sie haben die Möglichkeit, Informationen über die ThinPrint-Druckaufträge, die an das TPG 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 (⇒ [837](#)) auf dem TPG 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 TPG werden die gespeicherten Aufträge gelöscht. Sie können ebenfalls manuell gelöscht werden. Bei einem Neustart des TPG bleiben die Aufträge erhalten.

- 'Job History aufrufen' ⇒ [84](#)
- 'Aufträge manuell löschen' ⇒ [86](#)

Job History aufrufen

 Gehen Sie wie folgt vor:

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

 Die Job History wird angezeigt.

Was möchten Sie tun?

Folgende Informationen werden in der Job History angezeigt:

Information	Beschreibung
ID	Identifikationsnummer des Druckers, der den Druckauftrag gespooled hat.
Status	Status der Druckverbindung. Folgende Status sind möglich: <ul style="list-style-type: none"> • 'Initialisiert' bedeutet, dass eine Verbindung zum ThinPrint Server besteht. Als nächster Schritt wird die Druckerverbindung aufgebaut. • 'Verbindungsversuch' bedeutet, dass die Verbindung zum Drucker aufgebaut wird. • 'Verbindung abgewiesen' bedeutet, dass der Drucker die Verbindung abgelehnt hat. • 'Erzeugt' bedeutet, dass der Druckauftrag vom TPG angenommen wurde, aber die Datenübertragung zum Drucker noch nicht begonnen hat. • 'In Bearbeitung' bedeutet, dass der Druckauftrag vom TPG an den Drucker übertragen wird. • 'Bearbeitung unterbrochen' bedeutet, dass die Datenübertragung zum Drucker unterbrochen wurde. Dies kann z.B. entstehen, wenn im Drucker Papier fehlt. Wird der Druckerfehler behoben, wird die Datenübertragung fortgesetzt. • 'Beendet' bedeutet, dass der Druckauftrag vom TPG vollständig an den Drucker weitergeleitet wurde. • 'Abgebrochen' bedeutet, dass der Druckauftrag abgebrochen wurde. Dies kann z.B. auftreten, wenn das TPG neu gestartet wurde, während der Druckauftrag bearbeitet wurde.
Protokoll	Protokoll, mit dem die Druckdaten übertragen wurden. Die Darstellung erfolgt in Form einer Kombination der folgenden Werte: <ul style="list-style-type: none"> • '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: <ul style="list-style-type: none"> • '<Domain-User-Name>@<Domain>' erscheint bei ThinPrint-Druckaufträgen. • 'TPG-25' bzw. 'TPG-65' erscheint beim Drucken einer Status- oder Serviceseite.
Start	Zeitpunkt, an dem der Druckauftrag an das TPG gesendet wurde.
Größe	Größe des Druckauftrages in Kb.
Dauer	Bearbeitungsdauer, die das TPG 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.

7 Anhang



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

**Welche Information
benötigen Sie?**

- 'Glossar' ⇨ 88
- 'Parameterliste' ⇨ 91
- 'Problembehandlung' ⇨ 107
- 'Abbildungsverzeichnis' ⇨ 110
- 'Index' ⇨ 111

Welche Information
benötigen Sie?

Default-Name

7.1 Glossar

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

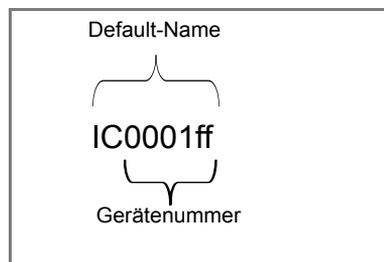
Herstellerspezifische Softwarelösungen

- 'InterCon-NetTool' ⇨ 90
- 'TPG Control Center' ⇨ 90

Netzwerktechnologie

- 'Default-Name' ⇨ 88
- 'Gateway' ⇨ 89
- 'Hardware-Adresse' ⇨ 89
- 'Hostname' ⇨ 89
- 'IP-Adresse' ⇨ 90
- 'Netzwerkmaske' ⇨ 90

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



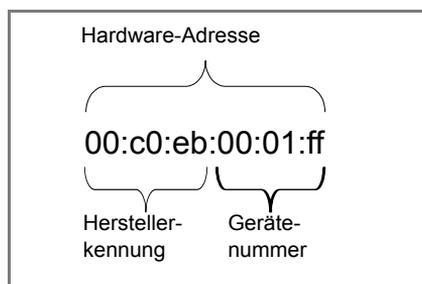
Der Default-Name kann im TPG Control Center, im InterCon-Net-Tool, auf der Statusseite oder auf der Serviceseite abgelesen werden.

Gateway

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

Hardware-Adresse

Das TPG 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 das TPG 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 TPG gespeichert werden, damit es 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.

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

TPG Control Center

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

**Welche Information
benötigen Sie?**

7.2 Parameterliste

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

- 'Parameterliste - IPv4' ⇨ [92](#)
- 'Parameterliste - IPv6' ⇨ [92](#)
- 'Parameterliste - DNS' ⇨ [93](#)
- 'Parameterliste - SNMP' ⇨ [93](#)
- 'Parameterliste - POP3' ⇨ [95](#)
- 'Parameterliste - SMTP' ⇨ [96](#)
- 'Parameterliste - Bonjour' ⇨ [97](#)
- 'Parameterliste - Datum/Zeit' ⇨ [97](#)
- 'Parameterliste - Beschreibung' ⇨ [97](#)
- 'Parameterliste - ThinPrint®' ⇨ [98](#)
- 'Parameterliste - ThinPrint Connection Service' ⇨ [99](#)
- 'Parameterliste - ThinPrint®-Drucker' ⇨ [100](#)
- 'Parameterliste - Benachrichtigung' ⇨ [101](#)
- 'Parameterliste - Webzugriff' ⇨ [103](#)
- 'Parameterliste - TCP-Portzugriff' ⇨ [103](#)
- 'Parameterliste - Authentifizierung' ⇨ [104](#)
- 'Parameterliste - USB-Gerät' ⇨ [105](#)
- 'Parameterliste - Statusseite' ⇨ [105](#)



Um die aktuellen Parameterwerte Ihres TPG einzusehen, siehe: 'Parameterwerte anzeigen' ⇨ [73](#) und 'Wie drucke ich eine Status- oder Serviceseite?' ⇨ [82](#).

Tabelle 12: 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 TPG.
ip_mask [Netzwerkmaske]	gültige IP-Adresse	255.255. 0.0	Definiert die Netzwerkmaske des TPG.
ip_gate [Gateway]	gültige IP-Adresse	0.0.0.0	Definiert die Gateway-Adresse des TPG.

Tabelle 13: Parameterliste - IPv6

Parameter	Wertekonvention	Default	Beschreibung
ipv6 [IPv6]	on/off	on	De-/aktiviert die IPv6-Funktionalität des TPG.
ipv6_auto [Automatische Konfiguration]	on/off	on	De-/aktiviert die automatische Vergabe der IPv6-Adressen für das TPG.
ipv6_addr [IPv6-Adresse]	n:n:n:n:n:n	::	Definiert eine manuell vergabene IPv6-Unicast-Adresse im Format n:n:n:n:n:n für das TPG. <i>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.</i>

Parameter	Wertekonvention	Default	Beschreibung
ipv6_gate [Router]	n:n:n:n:n:n	::	Definiert die IPv6-Unicast-Adresse des Routers, an den das TPG seine 'Router Solicitations' (RS) sendet.
ipv6_plen [Präfixlänge]	0 - 64 [2 Zeichen; 0-9]	64	Definiert die Länge des Subnetz-Präfixes für die IPv6-Adresse. <i>Adressbereiche werden durch Präfixe angegeben. Dazu wird die Präfixlänge (Anzahl der verwendeten Bits) als Dezimalzahl mit vorangehendem '/' an die IPv6-Adresse angehängt dargestellt.</i>

Tabelle 14: 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. <i>Der zweite DNS-Server wird verwendet, wenn der erste DNS-Server nicht verfügbar ist.</i>
dns_domain [Domain-Name (Suffix)]	max. 255 Zeichen [, a-z, A-Z, 0-9]	[blank]	Definiert den Domain-Namen eines vorhandenen DNS-Servers.

Tabelle 15: Parameterliste - SNMP

Parameter	Wertekonvention	Default	Beschreibung
snmpv1 [SNMPv1]	on/off	on	De-/aktiviert die SNMPv1-Funktionalität.

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

Tabelle 16: Parameterliste - POP3

Parameter	Wertekonvention	Default	Beschreibung
pop3 [POP3]	on/off	off	De-/aktiviert die POP3-Funktionalität.
pop3_srv [Servername]	max. 128 Zeichen	[blank]	Definiert den Namen des POP3-Servers.
pop3_port [Serverport]	1-65535 [max. 5 Zeichen; 0-9]	110	Definiert den Port des POP3-Servers, über den das TPG E-Mails empfängt. <i>Bei Verwendung von SSL/TLS ist als Portnummer 995 einzutragen.</i>
pop3_sec [Sicherheit]	0 = --- [keine Sicherheit] 1 = APOP 2 = SSL/TLS	0	Definiert das anzuwendende Authentifizierungsverfahren.
pop3_poll [E-Mails abfragen alle]	1-10080 [max. 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 [max. 4 Zeichen; 0-9; 0 = unbegrenzt]	10	Definiert die maximale Größe (in Kbyte) der vom TPG akzeptierten E-Mails.
pop3_usr [Benutzername]	max. 128 Zeichen	[blank]	Definiert den Namen, den das TPG benutzt, um sich am POP3-Server anzumelden.
pop3_pwd [Passwort]	max. 128 Zeichen	[blank]	Definiert das Passwort, das das TPG benutzt, um sich am POP3-Server anzumelden.

Tabelle 17: Parameterliste - SMTP

Parameter	Wertekonvention	Default	Beschreibung
smtp_srv [Servername]	max. 128 Zeichen	[blank]	Definiert den Namen des SMTP-Servers.
smtp_port [Serverport]	1-65535 [max. 5 Zeichen; 0-9]	25	Definiert die Portnummer, über die der SMTP-Server E-Mails von dem TPG empfängt.
smtp_ssl [TLS]	on/off	off	De-/aktiviert die Option TLS. Über das Sicherheitsprotokoll Transport Layer Security (TLS) wird der Übertragungsweg vom TPG zum SMTP-Server verschlüsselt.
smtp_sender [Name des Absenders]	max. 128 Zeichen	[blank]	Definiert den Absendernamen, den eine vom TPG generierte E-Mail enthalten soll.
smtp_auth [Anmelden]	on/off	off	De-/aktiviert die SMTP-Authentifizierung für das Login.
smtp_usr [Benutzername]	max. 128 Zeichen	[blank]	Definiert den Namen, den das TPG benutzt, um sich mit dem SMTP-Server zu verbinden.
smtp_pwd [Passwort]	max. 128 Zeichen	[blank]	Definiert das Passwort, das das TPG benutzt, um sich mit dem SMTP-Server zu verbinden.
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 = signieren, on = verschlüsseln]	off	Definiert das Signieren und Verschlüsseln von E-Mails.
smtp_attpkey [Öffentlichen Schlüssel beifügen]	on/off	on	De-/aktiviert das Hinzufügen eines öffentlichen Schlüssels zu einer E-Mail.

Tabelle 18: 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 TPG.

Tabelle 19: 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. <i>(Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.)</i>
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 20: Parameterliste – Beschreibung

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

Tabelle 21: Parameterliste - ThinPrint®

Parameter	Wertekonvention	Default	Beschreibung
tpgPort [ThinPrint®-Port]	1 - 65535 [max. 5 Zeichen; 0-9]	4000	Definiert den TCP-Port, über den das TPG mit dem ThinPrint Server kommuniziert.
tpgBdwidth [Bandbreite]	on/off	off	De-/aktiviert die clientseitige (TPG) Bandbreitenregulierung des ThinPrint®-Ports.
tpgBdwidthVal [Bandbreitenwert]	1600 - 1000000 [mind. 4 Zeichen, max. 7 Zeichen; 0-9]	256000	Definiert die Bandbreite (in Bit/Sekunde) mit der clientseitig (TPG) das Bandbreitenlimit am ThinPrint®-Port herabgesetzt wird.
tpgPrtoToVal [Druckerverbindungsabbruch]	0 - 86400 [max. 5 Zeichen; 0-9; 0 = aus]	60	Definiert das Zeitintervall (in Sekunden), nach dem ein Verbindungsversuch zum Drucker abgebrochen wird. <i>Ein Verbindungsversuch sollte abgebrochen werden, wenn ein Drucker physikalisch nicht verfügbar ist. Das macht den ThinPrint®-Port für nachfolgende Druckaufträge frei.</i>
tpgJobSndTout [Timeout für das Senden von Druckaufträgen]	0 - 86400 [max. 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.

Tabelle 22: 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. <i>(Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.)</i>
tpgClientID [Client-ID]	0 - 99999 [max. 5 Zeichen; 0-9]	0	Definiert die Client-ID, mit der das TPG in der Datenbank des Connection Services hinterlegt ist.
tpgAuthKey [Authentifizierungsschlüssel]	0 - 99999 [max. 5 Zeichen; 0-9]	0	Definiert den Authentifizierungsschlüssel, mit dem das TPG in der Datenbank des Connection Services hinterlegt ist.
conPort [Port]	1 - 65535 [max. 5 Zeichen; 0-9]	4001	Definiert den TCP-Port, über den das TPG mit dem Connection Service kommuniziert.
tpgKeepalive [Keep alive]	1 - 60000 [max. 5 Zeichen; 0-9]	60	Definiert das Zeitintervall (in Sekunden), mit dem die Verbindung zum Connection Service aktualisiert wird. <i>Hinweis: Der Wert muss gleich oder kleiner als der auf dem Connection Service-Server eingestellte Wert 'KeepAliveTO' sein.</i>
tpgRetry [Erneuter Verbindungsversuch]	1 - 60000 [max. 5 Zeichen; 0-9]	120	Definiert das Zeitintervall (in Sekunden), nach dem ein erneuter Verbindungsversuch stattfindet, wenn der Connection Service nicht erreicht werden kann.

Tabelle 23: Parameterliste - ThinPrint®-Drucker

Parameter	Wertekonvention	Default	Beschreibung
prtName_1 ~ prtName_6 [Drucker]	max. 32 Zeichen [a-z, A-Z, 0-9, _, -]	[blank]	Definiert den Druckernamen für das ThinPrint AutoConnect-Verfahren.
prtClass_1 ~ prtClass_6 [Klasse]	max. 7 Zeichen [a-z, A-Z, 0-9]	[blank]	Definiert den Druckerklassennamen für das ThinPrint AutoConnect-Verfahren.
prtDriver_1 ~ prtDriver_6 [Treiber]	max. 64 Zeichen [a-z, A-Z, 0-9, _, -]	[blank]	Definiert den Druckertreiber für das ThinPrint AutoConnect-Verfahren.
remotep_1 ~ remotep_6 [Druckeradresse]	max. 64 Zeichen [., a-z, A-Z, 0-9]	[blank]	Definiert die IP-Adresse oder den Hostnamen des Druckers. <i>(Ein Hostname kann nur verwendet werden, wenn zuvor DNS eingerichtet wurde.)</i>
remoteMode_1 ~ remoteMode_6 [Druckprotokoll]	raw = RAW-/Socket- Verbindung ipp = IPP-Verbindung lpd = LPD-Verbindung	raw	Definiert die Übertragungsmethode zwischen TPG und dem Drucker.
remotePort_1 ~ remotePort_6 [Port]	1 - 65535 [max. 5 Zeichen; 0-9]	9100	Definiert die Portnummer für das RAW-/Socket-Printing.
remoteUrl_1 ~ remoteUrl_6 [URL]	max. 64 Zeichen	ipp/lp1	Definiert den zweiten Teil der Drucker-URL für das IPP-Printing. <i>Die Implementierung der Drucker-URL ist herstellerabhängig. Nähere Informationen finden Sie im Druckerhandbuch.</i>
remoteIPPs_1 ~ remoteIPPs_6 [SSL]	on/off	off	De-/aktiviert die SSL-/TLS-Verschlüsselung für das IPP-Printing.
remoteQ_1 ~ remoteQ_6 [Queue]	max. 64 Zeichen [a-z, A-Z, 0-9]	lp1	Definiert den Queue-Namen für das LPD-Printing.

Parameter	Wertekonvention	Default	Beschreibung
lpdModeRFC_1 ~ lpdModeRFC_6 [RFC]	on/off	on	De-/aktiviert das RFC1179-konforme IPP-Printing.
monitorPing [Überwachung über Ping]	on/off	on	De-/aktiviert die Überwachung über Ping. <i>Die Ping-Abfrage ermöglicht die Anzeige der Druckerverfügbarkeit.</i>
monitorSNMP [SNMP]	on/off	on	De-/aktiviert die Überwachung über SNMP. <i>Die SNMP-Abfrage ermöglicht die Anzeige von Druckermeldungen.</i>
monitorPoll [Überwachungs- intervall]	10 - 86400 [max. 5 Zeichen; 0-9]	30	Definiert das Intervall einer 'Ping'- bzw. 'SNMP'-Abfrage in Sekunden.

Tabelle 24: 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 TPG 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_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 TPG ausgelöst wird.
noti_err_1 noti_err_2 [Probleme]	on/off	off	De-/aktiviert den E-Mail-Versand, welcher durch ein Problem am TPG 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 TPG ausgelöst wird.
trapusb [USB]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch das Anschließen oder Entfernen eines USB-Gerätes am TPG ausgelöst wird.
traperr [Probleme]	on/off	off	De-/aktiviert den SNMP-Trap-Versand, welcher durch ein Problem am TPG ausgelöst wird.

Tabelle 25: Parameterliste – Webzugriff

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

Tabelle 26: 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. <i>Der Testmodus bietet die Möglichkeit, die über die Zugriffskontrolle eingestellten Parameter zu testen. Bei aktiviertem Testmodus ist der Zugriffsschutz bis zum nächsten Neustart des TPG aktiv.</i>
protection_level [Sicherheitsstufe]	protec_tcp protec_all	protec_tcp	Definiert die zu sperrenden Porttypen: - TCP-Ports - alle Ports (IP-Ports)
ip_filter_on_1 ~ ip_filter_on_8 [IP-Adresse]	on/off	off	De-/aktiviert eine Ausnahme von der Portsperrung.
ip_filter_1 ~ ip_filter_8 [IP-Adresse]	gültige IP-Adresse	[blank]	Definiert Elemente, die von einer Portsperrung ausgenommen sind über die IP-Adresse.

Parameter	Wertekonvention	Default	Beschreibung
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 :00:00:0 0	Definiert Elemente, die von einer Portsperrung ausgenommen sind über die Hardware-Adresse.

Tabelle 27: 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 TPG, 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 TPG, wie es auf dem Authentifizierungsserver (RADIUS) gespeichert ist.
auth_extern [PEAP/EAP-FAST-Optionen]	--- [keine] PEAPLABEL0 PEAPLABEL1 PEAPVER0 PEAPVER1 FASTPROV1	---	Definiert die Art der äußeren Authentifizierung bei den EAP-Authentifizierungsmethoden TTLS, PEAP und FAST.
auth_intern [Innere Authentifizierung]	--- [keine] PAP CHAP MSCHAPV2 EAP-MD5 EAP-TLS	---	Definiert die Art der inneren Authentifizierung bei den EAP-Authentifizierungsmethoden TTLS, PEAP und FAST.

Parameter	Wertekonvention	Default	Beschreibung
auth_ano_name [Anonymer Name]	max. 64 Zeichen [a-z, A-Z, 0-9]	[blank]	Definiert den anonymen Namen für den unverschlüsselten Teil der EAP-Authentifizierungsmethoden TTLS, PEAP und FAST.
auth_wpa_addon [WPA-Add-on]	max. 255 Zeichen [a-z, A-Z, 0-9]	[blank]	Definiert eine optionale WPA-Erweiterung.

Tabelle 28: Parameterliste - USB-Gerät

Parameter	Wertekonvention	Default	Beschreibung
tpgBuffer [Zwischenspeichern von Druckaufträgen]	on/off	off	De-/aktiviert das automatische Speichern von Druckaufträgen, wenn der Drucker nicht erreicht werden kann.
autoSync [Parameter-Backup]	on/off	on	De-/aktiviert das automatische Sichern der Parameter auf einen angeschlossenen USB-Stick.

Tabelle 29: Parameterliste - Statusseite

Parameter	Wertekonvention	Default	Beschreibung
spage [Statusseite]	on/off	on	De-/aktiviert das Drucken von Status- und Serviceseiten auf dem dafür definierten Drucker. <i>Der Druckauftrag kann ausgelöst werden, indem der Status-/Reset-Taster am Gerät betätigt oder die entsprechende Schaltfläche im TPG Control Center angewählt wird.</i>
spPrinter [Statusseiten-Drucker]	TPG-25 = 1-2 TPG-65 = 1-6	1	Definiert den Drucker, auf dem Status- und Serviceseiten gedruckt werden, über die Drucker-ID.

Parameter	Wertekonvention	Default	Beschreibung
spMode [Modus Status- seite]	ASCII PostScript DATAMAX Citizen-Z	ASCII	Definiert das Datenformat, in dem eine Statusseite gedruckt wird.

7.3 Problembehandlung

Dieses Kapitel stellt einige Problemursachen und erste Lösungshilfen dar.

Problemdarstellung

- 'Das TPG signalisiert den BIOS-Modus' ⇨ 107
- 'Die Verbindung zum TPG Control Center kann nicht hergestellt werden' ⇨ 108
- 'Das Passwort ist nicht mehr verfügbar' ⇨ 109

Mögliche Ursache

Das TPG signalisiert den BIOS-Modus

Das TPG 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. Das TPG signalisiert den BIOS-Modus, indem die Activity-LED grün blinkt.



Das TPG ist im BIOS-Modus nicht funktionsfähig.

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

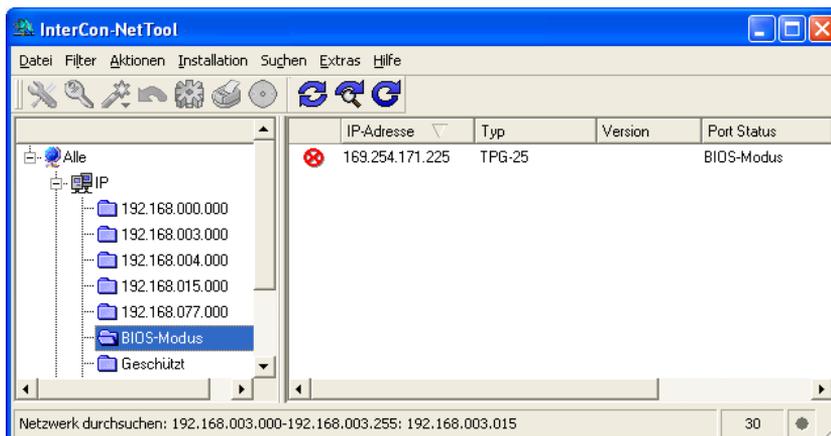


Abb. 7: InterCon-NetTool – TPG im BIOS-Modus

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

 Gehen Sie wie folgt vor:

1. *Starten Sie das InterCon-NetTool.*
2. *Markieren Sie das TPG in der Geräteliste.
(Sie finden das TPG unter dem Filter 'BIOS-Modus').*
3. *Wählen Sie im Menü **Installation** den Befehl **IP-Assistent**.
Der IP-Assistent wird gestartet.*
4. *Weisen Sie dem TPG eine IP-Adresse zu, indem Sie den Anweisungen des Assistenten folgen.
Die IP-Adresse wird gespeichert.*
5. *Führen Sie auf dem TPG ein Softwareupdate durch; siehe:
⇨  80.*

 Die Software wird auf dem TPG gespeichert. Das TPG wechselt in den Standardbetrieb.

Die Verbindung zum TPG Control Center kann nicht hergestellt werden
Schließen Sie Fehlerquellen aus. Überprüfen Sie zunächst:

- die Kabelverbindungen,
- die IP-Adresse des TPG (⇨  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 ⇨  53.
- Die TCP-Portzugriffskontrolle ist aktiviert ⇨  55.
- Der Passwortschutz ist aktiviert ⇨  53.

Das Passwort ist nicht mehr verfügbar

Der Zugriff auf das TPG Control Center kann durch ein Passwort geschützt werden. Ist das Passwort nicht mehr verfügbar, können die Parameterwerte des TPG auf die Standardwerte zurückgesetzt werden, um Zugriff zu erhalten ⇒ 80. Dabei gehen sämtliche Einstellungen verloren.

7.4 Abbildungsverzeichnis

TPG Control Center – START	19
InterCon-NetTool – Hauptdialog	21
Administration via E-Mail – Beispiel 1	24
Administration via E-Mail – Beispiel 2	24
InterCon-NetTool – IP-Assistent	28
TPG Control Center – Zertifikate	59
InterCon-NetTool – TPG im BIOS-Modus	107

7.5 Index

Ā

Administration 17
 E-Mail 22
 Status-/Reset-Taster 25
 TPG Control Center 18
 Adresse
 Ethernet-Adresse 89
 Hardware-Adresse 89
 IP-Adresse 90
 MAC-Adresse 89
 ARP/PING 16
 Authentifizierung 65
 AutoConnect 7

B̄

Bandbreite 42
 Bandbreitenlimit 42
 Benachrichtigungen 39
 Benachrichtigungsservice 39
 E-Mail 40
 SNMP-Trap 40
 Beschreibungen 38
 Bestimmungsgemäße
 Verwendung 11
 Bestimmungswidrige
 Verwendung 11
 BIOS-Modus 107
 Bonjour 36
 BOOTP 14

C̄

CA-Zertifikat 57
 Connection Service 7
 konfigurieren 49

D̄

Datei 'parameters' 73, 75
 Default-Name 88
 Default-Zertifikat 58
 DHCP 14
 DNS (Domain Name Service) 31
 Dokumentation 8
 Domain-Namen 31
 Drucken
 Serviceseite 84
 Statusseite 83
 Drucker
 einbinden 43
 ID 43
 Meldungen 48
 Übertragungsmethode 43
 Verbindungsstatus 47
 Drucker Meldungen 48

Ē

EAP 65
 EAP-FAST 70
 EAP-MD5 66
 EAP-TLS 66
 EAP-TTLS 68
 E-Mail 22
 Ethernet-Adresse 89

F̄

Firmware 80

Ḡ

Gateway 89
 Gerätenummer 88
 Gerätezeit 37

H̄

Hardware-Adresse 89
 Hostname 89
 Hotline 10

HTTP/HTTPS 53

I

IEEE 802.1x 65
 InterCon-NetTool 20, 90
 Aufbau 21
 installieren 20
 IP-Assistent 15
 starten 20
 IP-Adresse 90
 speichern 13
 IPP-Verbindung 43
 IPv4 27
 IPv6 29

J

Job History 84
 anzeigen 84
 löschen 86

L

LPD-Protokoll 43

M

MAC-Adresse 89

N

NAT 49
 Netzwerkmaske 90
 Neustart 81

P

Parameter
 anzeigen 73
 automatisch laden 76
 automatisch speichern 76
 laden 74
 Parameterliste 91
 sichern 73

 Standardeinstellung 77
 Parameter-Backup 75
 Parameterliste 91
 Passwort 54
 PEAP 69
 ping 47
 pkcs(12) 63
 POP3 33
 Protokoll
 BOOTP 14
 DHCP 14
 IPP 43
 IPv4 27
 IPv6 29
 LPD 43
 POP3 33
 SMTP 34
 SNMP 32
 ZeroConf 14

R

RADIUS 65
 RAW-/Socketverbindung 43
 Reset 77

S

S/MIME-Zertifikat 58
 SEH Homepage 10
 Selbstsigniertes Zertifikat 57
 Serviceseite 82
 Datenformat 82
 drucken 83
 Drucker 82
 Sicherheit 52
 Sicherheitsstufe 55
 Sicherungskopie 73
 SMTP 34
 SNMP 48
 SNMPv1 32
 SNMPv3 32
 SNMP-Trap 39
 Sntp-Server 37

Software 80
 SSL-/TLS-Verschlüsselung 51
 Standardeinstellung 77
 Status-/Reset-Taster 25, 78
 Parameter zurücksetzen 78
 Serviceseite drucken 84
 Statusseite drucken 83
 Status-E-Mail 39
 Statusseite 82
 Datenformat 82
 drucken 82
 Drucker 82
 Support 10
 Systemvoraussetzungen 7

T

TCP/IP 27
 TCP-Portzugriffskontrolle 55
 Testmodus 55
 ThinPrint 6
 ThinPrint Client 6
 ThinPrint Connection Service 7
 konfigurieren 49
 ThinPrint Engine 6
 ThinPrint-Port 42
 ThinPrint-Verschlüsselung 7, 51
 Time-Server 37
 TPG Control Center 18, 90
 Aufbau 19
 Sprache 19
 starten 18

U

Übertragungsmethoden 43
 Update 80
 USB-Gerät
 formatieren 75
 Parameter-Backup 75
 Zwischenspeichern von
 Druckaufträgen 74
 UTC 37

V

Verbindungstypen 53
 Verschlüsselte Druckdaten 51
 Verschlüsselung 51
 Versionsnummer 80
 Verwendungszweck 6

W

Webverbindungstypen
 definieren 53
 Webzugang 53
 Wurzelzertifikat 58

Z

Zeitzone 37
 ZeroConf 14
 Zertifikat 57
 anzeigen 59
 erstellen 60
 löschen 64
 speichern 62
 Zertifikatsanforderung 61
 Zurücksetzen 77
 Zwischenspeichern von
 Druckaufträgen 74