



ThinPrint® Gateway

TPG-25
TPG-65
TPG-125



User Manual

Manufacturer:
SEH Computertechnik GmbH
Suedring 11
33647 Bielefeld
Germany

Phone: +49 (0)521 94226-29

Fax: +49 (0)521 94226-99

Support: +49 (0)521 94226-44

Email: info@seh.de

Web: <http://www.seh.de>



Document:

Type: User Manual

Title: TPG-25 / TPG-65 / TPG-125

Version: 1.5

Online Links to Important Websites:

Support Contacts & Information: <http://www.seh-technology.com/support>

Sales Contacts & Information: <http://www.seh-technology.com/sales>

Downloads: <http://www.seh-technology.com/services/downloads.html>

InterCon is a registered trademark of SEH Computertechnik GmbH.

SEH Computertechnik GmbH has endeavored to ensure that the information in this documentation is correct. If you detect any inaccuracies please inform us at the address indicated above. SEH Computertechnik GmbH will not accept any liability for any error or omission. The information in this manual is subject to change without notification.

All rights are reserved. Copying, other reproduction, or translation without the prior written consent from SEH Computertechnik GmbH is prohibited.

© 2016 SEH Computertechnik GmbH

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

Table of Contents

1 General Information	5
1.1 ThinPrint® Gateway	5
1.2 Documentation	7
1.3 Support and Service	9
1.4 Your Safety	10
1.5 First Steps	11
1.6 Saving the IP Address in the TPG	12
2 Administration Methods	16
2.1 Administration via the TPG Control Center	16
2.2 Administration via the InterCon-NetTool	18
2.3 Administration via Email	20
3 Network and Device Settings	23
3.1 How to Configure IPv4 Parameters	23
3.2 How to Configure IPv6 Parameters	25
3.3 How to Configure the DNS	27
3.4 How to Configure SNMP	28
3.5 How to Configure POP3 and SMTP	30
3.6 How to Configure Bonjour	33
3.7 How to Configure the Device Time	34
3.8 How to Determine a Description	35
3.9 How to Use the Notification Service	35
4 ThinPrint Settings	38
4.1 How to Define the ThinPrint Port	39
4.2 How to Define the Bandwidth	39
4.3 How to Embed Printers	40
4.4 How to Define Timeouts (Experts Only)	42
4.5 How to Get Status Information on the Printer Connections	43
4.6 How to get Printer Messages	45
4.7 How to Use the ThinPrint Connection Service	46
4.8 How Does the TPG Receive Encrypted Data?	47

5 Security	48
5.1 How to Define the Encryption Level for SSL/TLS Connections	49
5.2 How to Encrypt the Connection to the TPG Control Center	51
5.3 How to Control the Access to the TPG Control Center (User Accounts)	52
5.4 How to Control the Access to the TPG (TCP Port Access Control) ...	53
5.5 How to Use Certificates Correctly	55
5.6 How to Use Authentication Methods	63
6 Maintenance	70
6.1 How to Secure the TPG Parameters (Backup)	71
6.2 How to Use a Connected USB Device	72
6.3 How to Reset Parameters to their Default Values (Reset)	75
6.4 How to Perform an Update	77
6.5 How to Restart the TPG?	78
6.6 How to Print a Status or Service Page	79
6.7 How to Display the Job History	81
7 Appendix	84
7.1 Glossary	85
7.2 Parameter List	88
7.3 Troubleshooting	105
7.4 List of Figures	109
7.5 Index	110

1 General Information



This chapter contains information concerning the device and the documentation as well as notes about your safety.

You will learn how to benefit from your ThinPrint® Gateway and how to operate the device properly.

What information do you need?

- 'ThinPrint® Gateway' ⇨ 5
- 'Documentation' ⇨ 7
- 'Support and Service' ⇨ 9
- 'Your Safety' ⇨ 10
- 'First Steps' ⇨ 11
- 'Saving the IP Address in the TPG' ⇨ 12

What is ThinPrint®?

ThinPrint® is a software-based technology providing print job compression and bandwidth control for network printing. The data traffic between the application server or the print server and the local printer is reduced considerably and networks are relieved.

The ThinPrint technology enables the transmission of compressed and bandwidth-optimized print jobs within a network. Print jobs are compressed using the server component **ThinPrint Engine**. The server sends the compressed print data to a device with the implemented **ThinPrint Client**. This client then decompresses the print data, transferring it to any printer.

Purpose

The TPG (ThinPrint® Gateway) contains a fully embedded **ThinPrint client**. This client allows you to receive and decompress print data.

The ThinPrint® gateways TPG-25, TPG-65 and TPG-125 have been specifically designed for environments in which the ThinPrint technology for print job compression and bandwidth control are used.

Up to two network printers can be quickly and easily embedded into the network using the TPG-25. Up to six devices can be embedded

using the TPG-65, up to twelve network printers with the TPG-125. Users send compressed print jobs to the ThinPrint® Gateway, which decompresses these print jobs and sends them to the appropriate printers.

Features

The TPG supports the following features (amongst others):

- The feature **AutoConnect** allows you to automatically create the required printer objects for the relevant client on the server. **AutoConnect** will automatically connect all selected printers on the server with a ThinPrint port; provided that templates exist.
- The **ThinPrint Connection Service** allows you to print to ThinPrint clients, that are found behind a firewall, for example. This allows the connection via masked networks as well as the assignment of the relevant print job to the respective end device.
- By means of the **ThinPrint SSL/TLS encryption**, the print data is protected during the transmission and will be decrypted by the ThinPrint clients or gateways before printing.

System Requirements

The TPG has been designed for the use in TCP/IP-based networks. A ThinPrint server must be integrated within this network. The network printers involved must support RAW or socket printing (printing via TCP/IP ports), IPP printing or LPD printing. If you want to use the **ThinPrint Connection Service**, you need a license.

1.2 Documentation

Scope and Content

This documentation describes several versions of the TPG. This means that functions will be described that may not be applicable to your product. Some illustrations may differ from your device.

Refer to the data sheet of your TPG model for information about the functional range of your product.

Structure of the Documentation

The TPG documentation consists of the following documents:



PDF

User Documentation

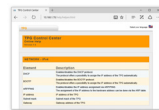
Detailed description of the TPG configuration and administration.



Printed
PDF

Quick Installation Guide

Information about security, hardware installation, and the initial operation procedure.



HTML

Online Help (TPG Control Center)

The Online Help contains detailed information about how to use the 'TPG Control Center'.



HTML

Online Help (InterCon-NetTool)

The Online Help contains detailed information about how to use the software tool 'InterCon-NetTool'.


Document Features

This documentation has been designed as an electronic document for screen use. Many programs (e.g. Adobe® Reader®) offer a bookmark navigation feature that allows you to view the entire document structure.

This document contains hyperlinks to the associated information units. If you want to print this documentation, we recommend using the printer setting 'Duplex' or 'Booklet'.







Terminology Used in this Document

Symbols and Conventions

The explanation of technical terms used in this document is summarized in a glossary. The glossary provides a quick overview of technical matters and background information; see: 85.

A variety of symbols are used within this document. Their meaning is listed in the following table:

Tabelle 1: Conventions within the documentation

Symbol / Convention	Description
 Warning	A warning contains important information that must be heeded. Non-observance may lead to malfunctions.
 Note	A notice contains information that should be heeded.
 Proceed as follows: 1. <i>Mark...</i>	The 'hand' symbol marks the beginning of instructions. Individual instructions are set in italics.
 Confirmation	The arrow confirms the consequence of an action.
<input checked="" type="checkbox"/> Requirements	Hooks mark requirements that must be met before you can begin the action.
<input type="checkbox"/> Option	A square marks procedures and options that you can choose.
•	Eye-catchers mark lists.
	This sign indicates the summary of a chapter.
	The arrow marks a reference to a page within this document. In the PDF file, you can jump to this page by clicking the symbol.
Bold	Established terms (of buttons or menu items, for example) are set in bold.
Courier	Command lines are set in Courier font.
'Proper names'	Proper names are put in inverted commas

Support

1.3 Support and Service

If questions remain, please contact our hotline. SEH Computertechnik GmbH offers extensive support.



Monday through Thursday
Friday

from 8:00 a.m. to 4:45 p.m. and
from 8:00 a.m. to 3:15 p.m. (CET)



+49 (0)521 94226-44



support@seh.de

Current Services

The following services can be found on the SEH Computertechnik GmbH homepage <http://www.seh-technology.com>:



- current firmware/software
- current tools
- current documentation
- current product information
- product data sheet
- and much more

1.4 Your Safety

Read and observe all safety regulations and warnings found in the documentation, on the device and on the packaging. This will avoid potential misuse and prevent damages to people and devices.

SEH Computertechnik GmbH will not accept any liability for personal injuries, property damages and consequential damages resulting from the non-observance of the mentioned safety regulations and warnings. Non-observance will result in the warranty claims becoming void.

Intended Use

The TPG is used in TCP/IP networks. The TPG allows communication between up to two/six/twelve network printers and one ThinPrint server. The TPG has been designed for use in office environments.

Improper Use

All uses of the device that do not comply with the TPG functionalities described in the documentation are regarded as improper uses. It is not allowed to make modifications to the hardware and software or to try to repair the device.

Safety Regulations

Before starting the initial operation procedure of the TPG, please note the safety regulations in the 'Quick Installation Guide'. The Quick Installation Guide is enclosed in the packaging.

Warnings

Read and observe all warnings mentioned in this document. Warnings are found before any instructions known to be dangerous. They are presented as follows:



Warning!

1.5 First Steps

This section provides all the information that you need for a fast operational readiness.



Proceed as follows:

1. *Read and observe the security regulations in order to avoid damages to people and devices, see: ↔ 10.*
 2. *Carry out the hardware installation. The hardware installation comprises the connection of the ISD to the network and the mains supply; see: 'Quick Installation Guide'.*
 3. *Make sure that an IP address is stored in the TPG; see: 'Saving the IP Address in the TPG' ↔ 12.*
 4. *Specify the ThinPrint port and other ThinPrint settings; see: ↔ 38.*
 5. *Specify the printers to which the TPG6 will send the print jobs; see: 'How to Embed Printers' ↔ 40.*
- ↪ The TPG is operational.

1.6 Saving the IP Address in the TPG

Why IP Addresses?

An IP address is used to address network devices in an IP network. TCP/IP network protocols require the storing of the IP address in the TPG so that the device can be addressed within the network.

How Does the TPG Obtain IP Addresses?

TPG are shipped without an IP address. The TPG is able to assign itself an IP address during the initial installation. Boot protocols are used to assign an IP address automatically to the TPG. Upon delivery, the boot protocols 'BOOTP' and 'DHCP' are enabled.

Once the TPG is connected to the network, it checks whether an IP address can be obtained via the boot protocols BOOTP or DHCP. If this is not the case, the TPG assigns itself an IP address via ZeroConf from the address range (169.254.0.0/16) which is reserved for Zero-Conf.

Once the TPG has automatically received an IP address via a boot protocol, you can save a freely definable IP address in the TPG. The assigned IP address of the TPG can be determined and modified via the software tool 'InterCon-NetTool'.

Different methods for the assignment of the IP address are described in the following.

Automatic Methods of IP Address Assignments

- 'ZeroConf' ⇨ 13
- 'BOOTP' ⇨ 13
- 'DHCP' ⇨ 13
- 'Auto Configuration (IPv6 Standard)' ⇨ 14

Manual Methods of IP Address Assignments

- 'InterCon-NetTool' ⇨ 14
- 'TPG Control Center' ⇨ 14
- 'ARP/PING' ⇨ 15

ZeroConf

If no IP address can be assigned via boot protocols, the TPG assigns itself an IP address via ZeroConf. For this purpose, the TPG picks an IP address at random from the address range (169.254.0.0/16) which is reserved for ZeroConf.



You can use the domain name service of Bonjour for the name resolution of the IP address; see: ⇒ 33.

Requirements

BOOTP

The TPG supports BOOTP, which means that the IP address of the TPG can be assigned via a BOOTP server.

- ☑ The 'BOOTP' parameter has been enabled, see: ⇒ 23.
- ☑ A BOOTP server is available in the network.

If the TPG is connected, it asks the BOOTP host for the IP address and the host name. The BOOTP host answers and sends a data packet containing the IP address. The IP address is saved in the TPG.

DHCP

The TPG supports DHCP, which means that the IP address of the TPG can be assigned dynamically via a DHCP server.

Requirements

- ☑ The 'DHCP' parameter has been enabled, see: ⇒ 23.
- ☑ A DHCP server is available in the network.

After the hardware installation, the TPG asks a DHCP server for an IP address by means of a broadcast query. The DHCP server identifies the TPG on the basis of its hardware address and sends a data packet to the TPG.

This data packet contains, among others, the IP address of the TPG, the default gateway, and the IP address of the DNS server. The data is saved in the TPG.

Requirements

Auto Configuration (IPv6 Standard)

The TPG can have an IPv4 address and several IPv6 addresses at the same time. The IPv6 standard is used to automatically assign IP addresses in IPv6 networks. When connected to an IPv6 network, the TPG will automatically obtain an additional 'link-local' IPv6 address from the IPv6 address range.

The TPG uses the 'link-local' IP address to search for a router. The TPG sends so-called 'Router Solicitations' (RS) to the special multi-cast address FF02::2. The available router will then return a 'Router Advertisement' (RA) containing the required information.

With a prefix from the range of the global unicast addresses, the TPG can compose its own address. It simply replaces the first 64 bits (prefix FE80::) with the prefix that was sent in the RA.

- ☑ The 'IPv6' parameter has been activated.
- ☑ The 'Automatic configuration' parameter has been activated; see: ⇒ [25](#).



To configure the assignment of IPv6 addresses, see: ⇒ [25](#).

InterCon-NetTool

The InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices. The IP Wizard of the InterCon-NetTool helps you to configure the TCP/IP parameters, e.g. the IP address. You can manually enter the desired IPv4 address and save it in the TPG using the IP Wizard. To configure an IPv4 address via the InterCon-NetTool, see: ⇒ [23](#).

TPG Control Center

You can manually enter the desired IP address and save it in the TPG using the TPG Control Center.

- To configure an **IPv4** address via the TPG Control Center, see: ⇒ [23](#).
- To configure an **IPv6** address via the TPG Control Center, see: ⇒ [25](#).

ARP/PING

The assignment of the IP address to the hardware address can be done via the ARP table. The ARP table is an internal system file in which the assignment is temporarily saved (about 15 min). This table is administered by the ARP protocol.

By means of the 'arp' and 'ping' commands, you can save the IP address in the TPG. If the TPG already has an IP address, the 'arp' and 'ping' commands cannot be used to save a new IP address.

However, an IP address from the address range (169.254.0.0/16) which is reserved for ZeroConf can be overwritten by means of the 'arp' and 'ping' commands.

The 'arp' command is used for editing the ARP table. The 'ping' command transfers a data packet containing the IP address to the hardware address of the TPG. If the data packet has been successfully sent and received, the TPG permanently saves the IP address.

The implementation of the 'arp' and 'ping' command depends on the system used. Read the documentation for your operating system.

Requirements

- The 'ARP/PING' parameter has been enabled, see: ⇒ 23.

Edit the ARP table:

Syntax: arp -s <IP address> <hardware address>

Example: arp -s 192.168.0.123 00-c0-eb-00-01-ff

Assign a new IP address to the TPG:

Syntax: ping <IP address>

Example: ping 192.168.0.123

The separators within the hardware address that are used in this example correspond to the Windows® platform.

2 Administration Methods



You can administer and configure the TPG in a number of ways. The following chapter gives you an overview of the various administration options.

You will get information on when to use these methods and which functions these methods support.

What information do you need?

- 'Administration via the TPG Control Center' ⇨ 16
- 'Administration via the InterCon-NetTool' ⇨ 18
- 'Administration via Email' ⇨ 205

Which Functions Are Supported?

The TPG Control Center comprises all features for the administration of the TPG.

The TPG Control Center is stored in the TPG and can be displayed by means of a browser software (Internet Explorer, Firefox, Safari).

Requirements

- The TPG is connected to the network and the mains voltage.
- The TPG has a valid IP address.

Starting the TPG Control Center




Proceed as follows:

1. *Open your browser.*
 2. *Enter the IP address of the TPG as the URL.*
- ↳ The TPG Control Center appears in the browser.



If the TPG Control Center is not displayed, check the proxy settings of your browser.

You can also start the TPG Control Center via the software tool 'InterCon-NetTool'.

 Proceed as follows:

1. *Highlight the TPG in the device list.*
 2. *Select Actions – Launch Browser from the menu bar.*
- ↪ The TPG Control Center appears in the browser.




Abb. 1: TPG Control Center - START

Structure of the TPG Control Center

The available menu items are located in the navigation bar (top). After selecting a menu item (simple mouse click), the available sub-menu items are displayed at the left. After selecting a submenu item, the corresponding page with its content is displayed (at the right).

You can set the language via the menu item **START**. Simply select the relevant flag.

The manufacturer's contact details and additional information regarding the product are displayed under **Product & Company**. The **Sitemap** provides an overview of and direct access to all pages of the TPG Control Center.

All other menu items refer to the configuration of the TPG. They are described in the Online Help of the TPG Control Center. To start the Online Help, click the  icon.

2.2 Administration via the InterCon-NetTool

The software InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices (TPG, TPR, print server, etc.). Depending on the network device you can configure various features via the InterCon-NetTool.

Mode of Operation

After the InterCon-NetTool is started, the network will be scanned for connected network devices. The network range to be scanned is freely definable. All network devices found will be displayed in the 'device list'.


You can modify the device list and adopt it to your individual needs. You can mark and configure the devices in the device list.

Installation

In order to use the InterCon-NetTool, the program must be installed on a computer with a Windows operating system. The installation file of the InterCon-NetTool can be found on the SEH Computertechnik GmbH homepage:

<http://www.seh-technology.com/services/downloads.html>




 Proceed as follows:

1. *Start the InterCon-NetTool installation file.*
2. *Select the desired language.*
3. *Follow the installation routine.*

↳ The InterCon-NetTool will be installed on your client.

Program Start

To start the program, double-click the InterCon-NetTool icon . The icon is found on the desktop or the Windows start menu. (Start → All Programs → SEH Computertechnik GmbH → InterCon-NetTool)

The settings of the InterCon-NetTool are saved in the 'NetTool.ini' file. The file is stored in the directory 'Documents and Settings' with the relevant user name.

Structure of the InterCon-NetTool

After the program start you will see the main dialog with the following elements. The dialog may vary, depending on which elements you have chosen to be shown or hidden.

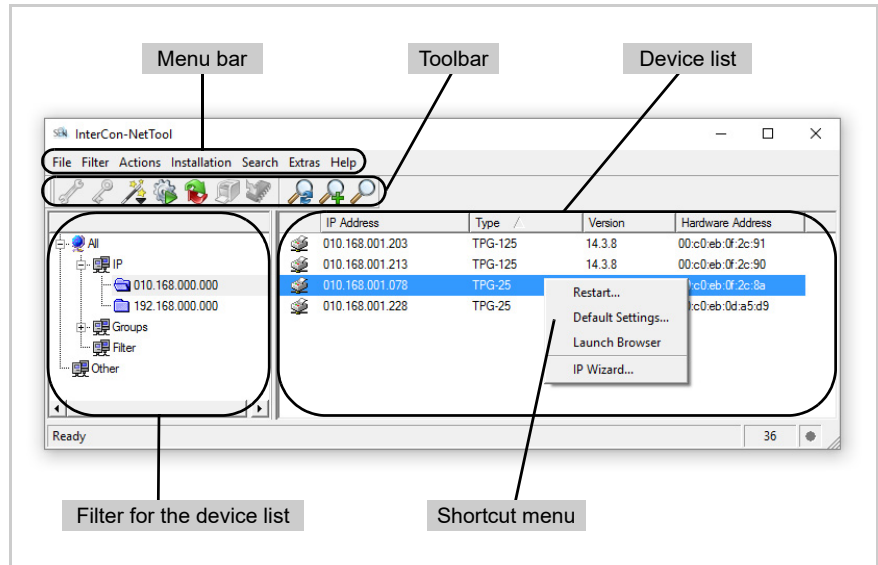


Abb. 2: InterCon-NetTool - Main Dialog

Which Functions Are Supported?

The InterCon-NetTool allows you to

- 'assign an IPv4 address to the TPG' ⇒ 23
- 'restart the TPG' ⇒ 78
- 'reset the parameter values of the TPG to their default settings' ⇒ 75
- 'start the TPG Control Center' ⇒ 16
- 'switch from the BIOS mode to the default mode' ⇒ 105



Detailed information on how to use the InterCon-NetTool can be found in the Online Help. To start the Online Help, select **Help – Online Help** from the menu bar.

2.3 Administration via Email

You can administer the TPG via email and thus via any computer with Internet access.

Functionalities

An email allows you to

- send TPG status information
- specify TPG parameters or
- perform an update on the TPG.

Requirements

- ☑ A DNS server has been configured on the TPG; see: ⇒ 27.
- ☑ In order to receive emails, the TPG must be set up as user with its own email address on a POP3 server.
- ☑ POP3 and SMTP parameters have been configured on the TPG; see: ⇒ 30.

Sending Instructions via Email

If you want to administer the TPG, you must enter the relevant instructions into the subject line of your email.



Proceed as follows:

1. *Open an email program.*
 2. *Write a new email.*
 3. *Enter the TPG address as recipient.*
 4. *Enter an instruction into the subject line; see: 'Syntax and Format of an Instruction' ⇒ 20.*
 5. *Send the email.*
- ↳ The TPG receives the email and carries out the instruction.

Syntax and Format of an Instruction

Note the following syntax for instructions in the subject line:

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

The following commands are supported:

Commands	Option	Description
<command>	get status	Sends the status page of the TPG.
	get parameters	Sends the parameter list of the TPG.
	set parameters	Sends parameters to the TPG. The syntax and values can be obtained from the parameter list, see: ⇒ 88. Parameter and value must be entered into the email body.
	update tpg	Carries out an automatic update using the software that is attached to the email.
	help	Sends a page containing information about the remote maintenance.
<comment>		Freely definable text for descriptions.

The following applies for the instructions:

- not case-sensitive
- one or more space characters are allowed
- max. length is 128 byte
- only the ASCII format can be read

Security with TAN

You will need a TAN for updates or parameter changes on the TPG. You will get a current TAN from the TPG via email, e.g. when receiving a status page. Enter the TAN into the first line of the email body. A space character must follow.

Parameter Changes

Parameter changes are integrated into the email body with the following syntax:

```
<parameter> = <value>
```

The syntax and values can be obtained from the parameter list, see: ⇒ 88.

Example 1

This email causes the TPG to send the parameter list to the sender of the email.

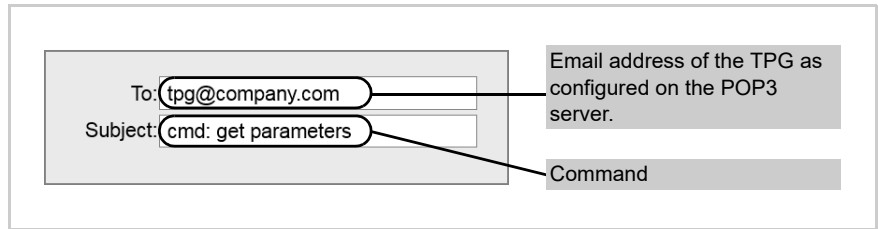


Abb. 3: Administration via Email - Example 1

Example 2

This email configures the parameter 'Description' on the TPG.

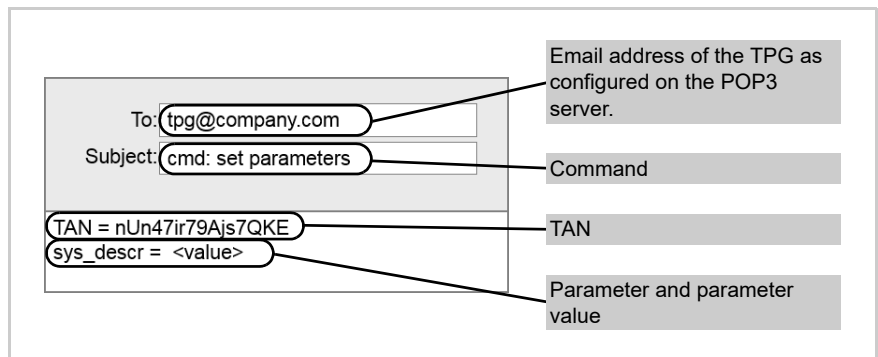


Abb. 4: Administration via Email - Example 2

3 Network and Device Settings



You can define various settings for an ideal integration of the TPG into a network. You can also configure various device settings. This chapter describes which network and device settings are supported.

What information do you need?

- 'How to Configure IPv4 Parameters' ⇨ 23
- 'How to Configure IPv6 Parameters' ⇨ 25
- 'How to Configure the DNS' ⇨ 27
- 'How to Configure SNMP' ⇨ 28
- 'How to Configure POP3 and SMTP' ⇨ 30
- 'How to Configure Bonjour' ⇨ 33
- 'How to Configure the Device Time' ⇨ 34
- 'How to Determine a Description' ⇨ 35
- 'How to Use the Notification Service' ⇨ 35

3.1 How to Configure IPv4 Parameters

TCP/IP (Transmission Control Protocol over Internet Protocol) forwards data packets across several connections and establishes a connection between the network participants.

The boot protocols DHCP and BOOTP belong to the TCP/IP protocol family. You can define various IPv4 parameters for an ideal integration of your TPG into a TCP/IP network. For further information about the assignment of IP addresses, see: ⇨ 12.

What do you want to do?

- 'Configuring IPv4 Parameters via the TPG Control Center' ⇨ 23
- 'Configuring IPv4 Parameters via the InterCon-NetTool' ⇨ 24

Configuring IPv4 Parameters via the TPG Control Center



Proceed as follows:

1. *Start the TPG Control Center.*

Requirements


2. *Select NETWORK – IPv4.*
 3. *Configure the IPv4 parameters; siehe: Tabelle 2 ⇒ 124.*
 4. *Click Save & Restart to confirm.*
- ↪ The settings are saved.

Tabelle 2: IPv4 Parameters

Parameters	Description
DHCP BOOTP ARP/PING	Enables or disables the protocols DHCP, BOOTP, and ARP/PING. <i>Protocols offer various possibilities to save the IP address in the TPG.(See 'Saving the IP Address in the TPG' ⇒ 12.)</i> We recommend disabling these options once an IP address has been assigned to the TPG.
IP address	IP address of the TPG
Subnet mask	Subnet mask of the TPG
Gateway	Gateway address of the TPG

Configuring IPv4 Parameters via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇒ 18.
- The network scan via Multicast has been enabled in the InterCon-NetTool.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Highlight the TPG in the device list.*
The TPG is displayed in the device list under 'ZeroConf' with an IP address from the address range (169.254.0.0/16) which is reserved for ZeroConf.
 3. *Select Installation – IP Wizard from the menu bar.*
The IP Wizard is started.
 4. *Follow the instructions of the IP Wizard.*
- ↪ The settings are saved.

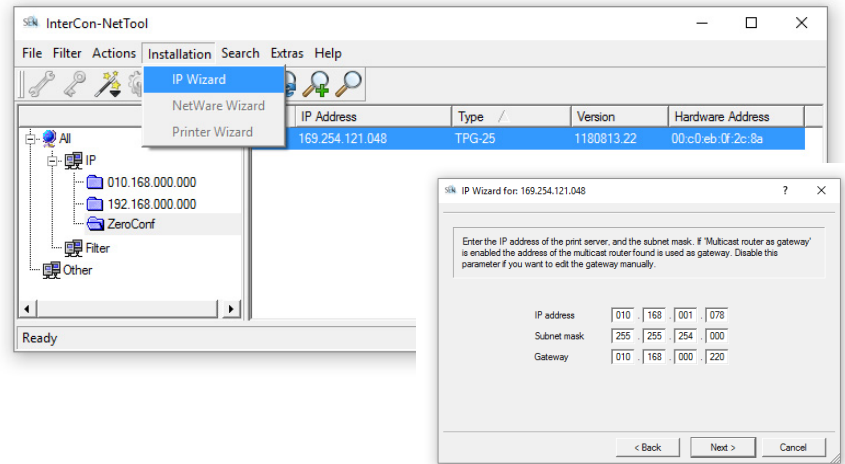


Abb. 5: InterCon-NetTool - IP Wizard

3.2 How to Configure IPv6 Parameters

You can integrate the TPG into an IPv6 network.

IPv6 (Internet Protocol version 6) is the successor of the more common IPv4. Both protocols are standards for the network layer of the OSI model and regulate the addressing and routing of data packets via a network. The introduction of IPv6 has many benefits:

- IPv6 increases the IP address space from 2^{32} (IPv4) to 2^{128} (IPv6) IP addresses
- Auto Configuration and Renumbering
- Efficiency increase during routing due to reduced header information
- Integrated services such as IPSec, QoS, Multicast
- Mobile IP

An IPv6 address consists of 128 bits. The normal format of an IPv6 address is eight fields. Each field contains four hexadecimal digits representing 16 bits.

What are the Advantages of IPv6?

What is the Structure of an IPv6 Address?

Each field is separated by a colon (:).

Example: fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4

Leading zeros in a field can be omitted.

Example: fe80 : 0 : 0 : 0 : 0 : 10 : 1000 : 1a4

An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used. However, the use of two colons can be used only once in an address.

Example: fe80 : : : : : 10 : 1000 : 1a4

As a URL in a Web browser, an IPv6 address must be enclosed in brackets. This prevents port numbers from being mistakenly regarded as part of an IPv6 address.

Example: http://[2001:608:af:1::100]:443



The URL will only be accepted by browsers that support IPv6.

Which Types of IPv6 Addresses are available?

There are different types of IPv6 addresses. The prefixes of the IPv6 addresses provide information about the IPv6 address types.

- Unicast addresses can be routed globally. These addresses are unique and therefore unambiguous. A packet that is sent to a unicast address will only arrive to the interface that is assigned to this address. Unicast addresses have the prefixes '2' or '3'.
- Anycast addresses are assigned to more than one interface. This means that a data packet that is sent to this address will arrive at various devices. The syntax of anycast addresses is the same as the one of unicast addresses. The difference is that anycast addresses choose one interface out of many. A packet that is dedicated to an anycast address arrives at the nearest interface (in line with the router metrics). Anycast addresses are only used by routers.
- Multicast addresses allow you to send data packets to different interfaces at the same time without a proportional increase of the bandwidth. A multicast address can be recognized by the prefix 'ff'.



Proceed as follows:

1. Start the TPG Control Center.
 2. Select **NETWORK – IPv6**.
 3. Configure the IPv6 parameters; siehe: Tabelle 3 ⇒ 27.
 4. Click **Save & Restart** to confirm.
- ↪ The settings are saved.

Tabelle 3: IPv6 Parameters

Parameters	Description
IPv6	Enables/disables the IPv6 functionality of the TPG.
Automatic configuration	Enables/disables the automatic assignment of the IPv6 address for the TPG.
IPv6 address	Defines a manually assigned IPv6 Unicast address in the n:n:n:n:n:n:n:n format for the TPG. <i>Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.</i>
Router	Defines the IPv6 unicast address of the router. The TPG sends its 'Router Solicitations' (RS) to this router.
Prefix length	Defines the length of the subnet prefix for the IPv6 address. The value 64 is preset. <i>Address ranges are indicated by prefixes. The prefix length (number of bits used) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/'.</i>

3.3 How to Configure the DNS

DNS is a service that translates domain names into IP addresses. Using DNS, names can be assigned to IP addresses and vice versa. If a DNS server is available in your network, you can use DNS for your TPG.

If you use a domain name during the configuration process, you must first enable and configure DNS. DNS is used for the configuration of the time server, for example.



Proceed as follows:

1. Start the TPG Control Center.
 2. Select **NETWORK – DNS**.
 3. Configure the DNS parameters; siehe: Tabelle 4 → 28.
 4. Click **Save** to confirm.
- ↪ The settings are saved.

Tabelle 4: DNS Parameters

Parameters	Description
DNS	Enables/disables DNS.
Primary DNS server	Defines the IP address of the primary DNS server.
Secondary DNS server	Defines the IP address of the secondary DNS server. <i>The secondary DNS server is used if the first one is not available.</i>
Domain name (suffix)	Defines the domain name of an existing DNS server.

3.4 How to Configure SNMP

SNMP (Simple Network Management Protocol) has become the standard protocol for the administration and monitoring of network elements. The protocol controls communication between the monitored devices and the monitoring station.

SNMP allows you to read and edit management information provided by the network elements (e.g. the TPG or printers). The TPG supports versions 1 and 3 of SNMP.

SNMPv1

The SNMP Community is a basic form of access protection. A large number of SNMP managers are grouped together in the community. The community is then assigned (read/write) access rights. The general community string is 'public'.



The community string for SNMPv1 is transferred in plain text and does not provide sufficient protection.

SNMPv3

SNMPv3 is a continuation of the SNMP standard, which provides improved applications and a user-based security model. Distinguishing features of SNMPv3 include its simplicity and security concept.



For SNMPv3 a name and password for the SNMP user have to be defined. The user accounts used for this are those that are used for the TPG Control Center access; see: ⇨ 52.

Requirements

Only for SNMPv3: The user accounts have been defined; see: ⇨ 52.



Proceed as follows:

1. Start the TPG Control Center.
2. Select **NETWORK – SNMP**.
3. Configure the SNMP parameters; siehe: Tabelle 5 ⇨ 29.
4. Click **Save** to confirm.

↵ The settings are saved.

Tabelle 5: SNMP Parameters

Parameters	Description
SNMPv1	Enables/disables SNMPv1.
Read-only	Enables/disables the write protection for the community.
Community	SNMP community name <i>The SNMP Community is a basic form of access protection in which several participants with the same access rights are grouped together.</i>
SNMPv3	Enables/disables SNMPv3.
Hash	Defines the Hash algorithm.
Access rights	Defines the access rights of the SNMP user.
Encryption	Defines the encryption method.

3.5 How to Configure POP3 and SMTP

You must configure the protocols POP3 and SMTP on the TPG so that the notification service (⇒ 35) and the administration via email (⇒ 20) will work properly.

POP3

'POP3' (Post Office Protocol Version 3) is a transfer protocol that a client can use to fetch emails from a mail server. POP3 is required in the TPG to administer the TPG via email.

SMTP

'SMTP' (Simple Mail Transfer Protocol) is a protocol that controls the sending of emails in networks. SMTP is required in the TPG to administer the TPG via email and to run the notification service.

What do you want to do?

- 'Configuring POP3' ⇒ 30
- 'Configuring SMTP' ⇒ 31

Requirements

Configuring POP3

- The TPG is set up as user with its own email address on a POP3 server.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **NETWORK – Email**.*
 3. *Configure the POP3 parameters; siehe: Tabelle 6 ⇒ 30.*
 4. *Click **Save** to confirm.*
- ↪ The settings are saved.

Tabelle 6: POP3 Parameters

Parameters	Description
POP3	Enables/disables the POP3 functionality.
POP3 - Server name	Defines a POP3 server via the IP address or the host name. <i>A host name can only be used if a DNS server was configured beforehand.</i>

Requirements

Parameters

Description

POP3 - Server port	Defines the port used by the TPG for receiving emails. The port number 110 is preset. When using SSL/TLS, enter 995 as port number.
POP3 - Security	Defines the authentication method to be used (APOP / SSL/TLS). <i>When using SSL/TLS, the encryption strength is defined via the encryption protocol and level ↗ 49.</i>
POP3 - Check mail every	Defines the time interval (in minutes) for retrieving emails from the POP3 server.
POP3 - Ignore mail exceeding	Defines the maximum email size (in Kbyte) to be accepted by the TPG. <i>(0 = unlimited)</i>
POP3 - User name	Defines the user name used by the TPG to connect to the POP3 server.
POP3 - Password	Defines the user password used by the TPG to connect to the POP3 server.

Configuring SMTP

- The TPG is set up as user with its own email address on an SMTP server.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **NETWORK – Email**.*
 3. *Configure the SMTP parameters; siehe: Tabelle 7 ↗ 31.*
 4. *Click **Save** to confirm.*
- ↗ The settings are saved.

Tabelle 7: SMTP Parameters

Parameters

Description

SMTP - Server name	Defines an SMTP server via the IP address or the host name. <i>A host name can only be used if a DNS server was configured beforehand.</i>
--------------------	-----------------------------------------------------------------------------------------------------------------------------------------------

Parameters	Description
SMTP - Server port	Defines the port number used by the TPG to send emails to the SMTP server. The port number 25 is preset.
SMTP - TLS	Enables/disables TLS. <i>The security protocol TLS (Transport Layer Security) is used to encrypt the transmission between the TPG and the SMTP server. The encryption strength is defined via the encryption protocol and level ⇒ 49.</i>
SMTP - Sender name	Defines the email address used by the TPG to send emails. Note: Very often the name of the sender and the user name are identical.
SMTP - Login	Enables/disables the SMTP authentication for the login.
SMTP - User name	Defines the user name for the SMTP authentication.
SMTP - Password	Defines the password for the SMTP authentication.
SMTP - Security (S/MIME)	Enables/disables the encryption and signing of emails via S/MIME.
SMTP - Signing emails	Defines the signing of emails. <i>A signature created by the sender allows the recipient to verify the identity of the sender and to make sure that the email was not modified. An S/MIME certificate (⇒ 55) is required for the signing of emails.</i>
SMTP - Full encryption	Defines the encryption of emails. <i>Only the recipient can open and read the encrypted email. An S/MIME certificate (⇒ 55) is required for the encryption.</i>
SMTP- Attach public key	Sends the public key together with the email. Many email clients require the public key to be attached in order to view the emails.

3.6 How to Configure Bonjour

Bonjour allows the automatic recognition of computers, devices, and network services in TCP/IP-based networks.

The TPG uses the following Bonjour functions:

- Checking the IP address assigned via ZeroConf
- Assignment of host names to IP addresses
- Location of server services without knowledge of the device's host name or IP address.

When checking the IP address assigned via ZeroConf (see: 'ZeroConf' ⇨ 13) the TPG sends a query to the network. If the IP address has already been assigned elsewhere in the network, the TPG will receive a message. The TPG then sends another query with a different IP address. If the IP address is available, it is saved in the TPG.

The domain name service is used for additional Bonjour features. Since there is no central DNS server in Bonjour networks, each device and application has its own small DNS server.

This integrated DNS server (mDNS) collects and administers the information of all participants in the net. In addition to the features of a classical DNS server, the mDNS server also saves the IP address, the service name and the offered services of each participant.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. **Select NETWORK – Bonjour.**
 3. *Configure the Bonjour parameters; siehe: Tabelle 8 ⇨ 33.*
 4. **Click Save to confirm.**
- ✎ The setting will be saved.

Tabelle 8: Bonjour Parameters

Parameters	Description
Bonjour	Enables/disables Bonjour.
Bonjour name	Defines the Bonjour name of the TPG. The TPG uses this name for its Bonjour services. If no Bonjour name is entered, the default name will be used (device name@ICxxxxxx).

3.7 How to Configure the Device Time

You can set the time of the TPG via a time server (SNTP server) in the network. A timeserver is a computer networking device that reads the actual time from a reference clock and distributes this information to its clients. In the TPG, the time server is defined via the IP address or the host name.

Benefits and Purpose

If the time server is activated, all ThinPrint print jobs that are handled by the TPG will get a time stamp. Date and time are then displayed under (⇒ 81) 'Job History'.

UTC

The TPG uses 'UTC' (Universal Time Coordinated) as a basis. UTC is a reference time and used as a time standard.

Time zone

The time received by the time server does not necessarily correspond to your local time zone. Deviations from your location and the resulting time difference (including country-specific particularities such as Daylight Saving Time) can be handled by means of the 'Time zone' parameter.

Requirements

A time server is integrated into the network.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select NETWORK – Date/Time.*
 3. *Tick Date/Time.*
 4. *Enter the IP address or the host name of the time server into the Time server box.*
(A host name can only be used if a DNS server was configured beforehand.)
 5. *Select the code for your local time zone from the Time zone list.*
 6. *Click Save to confirm.*
- ↩ The settings are saved.

3.8 How to Determine a Description

You can assign freely definable descriptions to the TPG. This gives you a better overview of the devices available in the network.



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select **DEVICE – Description**.*
3. *Enter freely definable names for **Host name, Description and Contact person**.*
4. *Click **Save** to confirm.*

↪ The data is saved.

3.9 How to Use the Notification Service

You can get notifications in the form of emails or SNMP traps from the TPG. By means of these notifications up to four email recipients can be informed about various events irrespective of time and location.

The following message types are possible:

- The status email periodically informs the recipient about the status of the TPG.
- The event notification informs you about a specific event on the TPG via email or SNMP trap. The event can be:
 - The restart of the TPG.
 - The connection or disconnection of a USB flash drive to/from the TPG.
 - A problem with the TPG.

- 'Configuring the sending of status emails' ⇨ 35
- 'Configuring event notifications via email' ⇨ 36
- 'Configuring event notifications via SNMP traps' ⇨ 37

Configuring the sending of status emails

- SMTP parameters can be configured on the TPG, see: ⇨ 30.


What do you want to do?

Requirements

Requirements

- ☑ A DNS server has been configured on the TPG; see: ⇨ 27.

For the notification service you can specify up to two email recipients.

 Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select **DEVICE – Notification**.*
3. *Enter the email address of the recipient into the **Email recipient** box.*
4. *Tick **Status** for the relevant recipient.*
5. *Specify the sending interval in the **Status notification time** area.*
6. *Click **Save** to confirm.*


↪ The settings are saved.

Configuring event notifications via email

- ☑ SMTP parameters can be configured on the TPG, see: ⇨ 30.

- ☑ A DNS server has been configured on the TPG; see: ⇨ 27.

For the notification service you can specify up to two email recipients and the message types.

 Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select **DEVICE – Notification**.*
3. *Enter the email address of the recipient into the **Email recipient** box.*
4. *Tick the options with the desired message types.*
5. *Click **Save** to confirm.*

↪ The settings are saved.

Configuring event notifications via SNMP traps

For the notification service you can specify up to two SNMP trap recipients and the message types.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **DEVICE – Notification**.*
 3. *Enter the trap address of the recipient into the **Trap target** box.*
 4. *Enter the trap community of the recipient into the **Trap community** box.*
 5. *Tick the options with the desired message types.*
 6. *Click **Save** to confirm.*
- ↪ The settings are saved.

4 ThinPrint Settings



You must define the port, the bandwidth as well as the printer and the printer properties if you want the TPG to communicate with a ThinPrint server via a port or if you want the TPG to receive and forward print jobs. This chapter describes how to match the parameter values in an ideal way.

What information do you need?

- 'How to Define the ThinPrint Port' ⇒ 39
- 'How to Define the Bandwidth' ⇒ 39
- 'How to Embed Printers' ⇒ 40
- 'How to Define Timeouts (Experts Only)' ⇒ 42
- 'How to Get Status Information on the Printer Connections' ⇒ 43
- 'How to get Printer Messages' ⇒ 45
- 'How to Use the ThinPrint Connection Service' ⇒ 46
- 'How Does the TPG Receive Encrypted Data?' ⇒ 47



The settings described here refer to the client-side (TPG). Information about the installation, configuration and administration of the ThinPrint environment can be found in the ThinPrint documentation at <http://www.thinprint.com>.

4.1 How to Define the ThinPrint Port

In ThinPrint environments, printing is done to a TCP/IP port via a socket connection. The port number of the TPG must be identical to the port number that was defined for the ThinPrint server.

Port 4000 is preset. You can change the port number, if necessary.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **DEVICE – ThinPrint®**.*
 3. *Enter the port number into the **ThinPrint® port box**.*
 4. *Click **Save** to confirm.*
- ↪ The setting will be saved.

4.2 How to Define the Bandwidth

Bandwidth describes the capacity of a data connection. The bandwidth of the TPG is indicated in bit/second (bit/s).

The bandwidth that is needed for print jobs can be limited to a freely definable value for each ThinPrint port (server side). You can further decrease the bandwidth limit on the port of the TPG (client side).



Defining a bandwidth value on the TPG which is higher than the defined value (server side) will have no effect. In this case, the pre-defined value will be applied.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **DEVICE – ThinPrint®**.*
 3. *Tick **Bandwidth**.*
 4. *Enter the desired bandwidth.*
 5. *Click **Save** to confirm.*
- ↪ The setting will be saved.

**Transfer
Methods**

4.3 How to Embed Printers

Print jobs are sent from the ThinPrint server to the TPG. After the decompression of the print jobs, the TPG forwards the print jobs to the printers.

The print jobs are assigned via the printer ID. Up to two (TPG-25) or six (TPG-65) or twelve (TPG-125) network printers can be embedded via the TPG.

When embedding the connected network printers you must define the printer address and a transfer method. If you use the ThinPrint AutoConnect feature, additional parameters (name, class, driver) must be defined.

The data transfer between the TPG and the network printers can be done in three ways:

- Usually the data is transferred to the TCP/IP port via a **raw/socket connection**. Port 9100 is preset. If required, you can configure a different port number.
- By means of **IPP connections** (Internet Printing Protocol) the print data is transmitted via HTTP via local networks or the Internet to the printer. To this purpose, you must configure a printer URL that needs to be implemented according to the information of the manufacturer. Please refer to the documentation of your printer. The printer URL 'ipp/lp1' is preset and can be changed, if needed.

Your advantage: The connection between the TPG and the printer can be encrypted via SSL/TLS.

- Data transfer can also be done via the **LPD protocol** (Line Printer Daemon). During LPD printing the print data is sent to the IP address of the printer by means of an LPD queue.

The LPD queue name 'lp1' is preset. If required, you can configure a different LPD queue name. Depending on the configuration, the printing behavior is either compliant to RFC1179 or resembles Microsoft LPD printing.

Your advantage: When using the LPD protocol for data transfer, additional print job attributes will be transferred and displayed in the 'job history' (⇒ 81).



The support of the transfer methods depends on the printer. Consult your printer manual for more information.



Proceed as follows:

1. Start the TPG Control Center.
 2. Select **DEVICE – ThinPrint®**.
 3. Enter the printer parameters into the boxes; siehe: Tabelle 9
⇒ 41.
 4. Select a transfer method for every printer.
 5. Click **Save** to confirm.
- ↩ The settings are saved.

Tabelle 9: Printer Parameters

Parameters	Description
ID	The ID clearly identifies the printers for the ThinPrint server.
Printer	Defines the printer name for the ThinPrint AutoConnect feature. The printer name is purely a description and is used to distinguish the printers. <i>The printer can only use the ThinPrint AutoConnect feature if a printer name was defined. If the printer supports SNMP, the printer class is derived automatically via SNMP. A freely definable description can be entered at any time and will override any automatically derived printer name.</i>
Class	Defines the printer class for the ThinPrint AutoConnect feature. Printers with compatible drivers can be arranged in one class. <i>In addition to the defining of the printer name, you can also define a printer class if you want to use the ThinPrint AutoConnect feature (optional). If the printer supports SNMP, the class name is obtained automatically via SNMP. A freely definable description can be entered at any time and will override any automatically derived class name.</i>

Parameters	Description
Driver	Defines the printer driver for the ThinPrint® AutoConnect feature. <i>In addition to the defining of the printer name, you can also define a printer driver if you want to use the ThinPrint AutoConnect feature (optional).</i>
Printer address	Defines the IP address or host name of the printer. The host name can only be used if a DNS server was configured beforehand.
Port	Defines the port number for RAW/socket printing. <i>(Default = 9100)</i> <i>Is used when selecting 'RAW' as the transfer method.</i>
URL	Specifies the second part of the printer URL for IPP printing. <i>(Default = ipp/lp1)</i> <i>Is used when selecting 'IPP' as the transfer method.</i>
SSL	Enables/disables the SSL/TLS encryption for IPP printing. The encryption strength is defined via the encryption protocol and level ⇒ 49. <i>Is used when selecting 'IPP' as the transfer method.</i>
LPD Queue	Defines the queue name for LPD printing. <i>(Default = lp1)</i> <i>Is used when selecting 'LPD' as the transfer method.</i>
RFC	Enables/disables the RFC1179 conformity for LPD printing. <i>Is used when selecting 'LPD' as the transfer method. If this option is disabled, the printing behavior resembles that of Microsoft® LPD printing.</i>

4.4 How to Define Timeouts (Experts Only)

You can use timeouts to control how errors are handled before and during a print job.

The 'Printer connection timeout' parameter specifies the period of time (in seconds) after which a connection attempt to the printer should be aborted. It is advisable to abort a connection attempt if the printer is not physically available for the TPG and the ThinPrint port is to be freed for subsequent print jobs, for example.

Printer connection timeout


Job sending timeout

The 'Job sending timeout' parameter specifies the period of time (in seconds) after which a current print job should be aborted. It is advisable to abort a print job if the print job cannot be executed due to a printer error (for example, no paper).

Both timeouts cause the print jobs to be deleted. In 'pure' ThinPrint printing, the ThinPrint server additionally generates an error message. No error message is generated by the ThinPrint server when printing takes place via the Connection Service.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **DEVICE – ThinPrint®**.*
 3. *In the **Printer connection timeout and Job sending timeout** fields, enter the periods of time in seconds after which the timeouts should take effect (0 s = off).*
 4. *Click **Save** to confirm.*
-  The settings are saved.

4.5 How to Get Status Information on the Printer Connections

You can view the connection status of the embedded printers. The following connection statuses can be displayed:

Connection Status	Description
Time out	No connection to the printer at present. A connection was available at an earlier stage.
reachable	A connection to the printer is available at present.
unreachable	No connection to the printer so far.
Unknown	The connection status to the printer cannot be determined.


In order to get the connection status, you must configure a 'ping' query. The query result is displayed in the TPG Control Center. In addition, the print status LED shows whether the query was success-

What do you want to do?

ful. For more information on the LEDs, see: 'Quick Installation Guide'.


- 'Configuring a 'ping' Query via the TPG Control Center' ⇒ 44
- 'Displaying the Printer Connection Status via the TPG Control Center' ⇒ 44

Configuring a 'ping' Query via the TPG Control Center

 Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **DEVICE – ThinPrint® printer.***
 3. *Tick **Monitoring via ping.***
 4. *Enter the interval (in seconds) into the **Monitoring interval box.***
 5. *Click **Save to confirm.***
- ↪ The settings are saved.

Displaying the Printer Connection Status via the TPG Control Center

 Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **DEVICE – ThinPrint® printer.***
- ↪ The printer connection status is displayed under 'ThinPrint® printer status' in the '**Status**' column and is assigned to the printer IDs.

4.6 How to get Printer Messages

You can view printer error messages (paper empty, offline, paper jam, etc.) and printer status messages (idle, printing, warming up, etc.). In order to get printer messages, you must configure an SNMP query beforehand.



Not all printers support SNMP. Consult your printer manual for more information.

The query result is displayed in the TPG Control Center. In addition, the print status LED shows whether the query was successful. For more information on the LEDs, see: 'Quick Installation Guide'.

What do you want to do?

- 'Configuring an SNMP Query via the TPG Control Center' ⇨ 45
- 'Displaying Printer Status Messages via the TPG Control Center' ⇨ 45

Requirements

Configuring an SNMP Query via the TPG Control Center

- The printer supports SNMP.



Proceed as follows:

1. Start the TPG Control Center.
 2. Select **DEVICE – ThinPrint® printer**.
 3. Tick **SNMP**.
 4. Enter the interval (in seconds) into the **Monitoring interval box**.
 5. Click **Save to confirm**.
- ↳ The settings are saved.

Displaying Printer Status Messages via the TPG Control Center



Proceed as follows:

1. Start the TPG Control Center.
 2. Select **DEVICE – ThinPrint® printer**.
- ↳ The printer messages are shown under 'ThinPrint® printer status' in the 'Status' column and are assigned to the printer IDs.

4.7 How to Use the ThinPrint Connection Service

The ThinPrint Connection Service sends print jobs via TCP/IP to ThinPrint clients (i.e. the TPG) in masked networks (NAT).

The Connection Service manages the entire communication between the ThinPrint server and the corresponding client. This allows the connection via masked networks as well as the assignment of the relevant print job to the respective end device.

To use this service, you must prepare the TPG. For each end device that uses the Connection Service, you must store the client ID and an authentication key in the database of the Connection Service. You must also set these two values on the TPG.



Please note that you need a ThinPrint license for each client ID.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **DEVICE – ThinPrint®**.*
 3. *Tick **Connection Service**.*
 4. *Enter the relevant parameters; siehe: Tabelle 10 ⇨ 46.*
 5. *Click **Save** to confirm.*
- ↳ The settings are saved.

Tabelle 10: Connection Service Parameters

Parameters	Description
Connection Service	Enables/disables the ThinPrint Connection Service.
Server name	IP address or host name of the server on which the Connection Service is installed. <i>The host name can only be used if a DNS server was configured beforehand.</i>
Port	Defines the TCP port used by the TPG for communicating with the Connection Service. <i>The port number 4001 is preset.</i>
Client ID	Client ID as stored in the database of the Connection Service. The Connection Service needs the Client ID to send print jobs to the TPG.

Parameters	Description
Authentication key	Authentication key as stored in the database of the Connection Service.
Keep alive	Interval (in seconds) after which the connection to the Connection Service is refreshed. The value has to be equal to or lower than the 'KeepAliveTO' value set on the Connection Service server. <i>(allowed entry: 1–60000 default = 60)</i>
Connection retry	Defines the time interval (in seconds) after which a connection retry is executed if the Connection Service cannot be reached. <i>(allowed entry: 1–60000 default = 120)</i>



The connection status is displayed in the table 'ThinPrint® status'. If the connection to the Connection Service was refused, it is because a value (client ID, authentication key, port or server name) was entered incorrectly. In this case, verify and correct your settings and click **Save**.

4.8 How Does the TPG Receive Encrypted Data?

A secure connection during the transfer of print jobs between ThinPrint (server or Connection Service) and the TPG is guaranteed by means of an SSL/TLS encryption. The encryption strength is defined via the encryption protocol and level ⇨ 49.

The ThinPrint server requests a certificate from the TPG. By means of this certificate, the ThinPrint server checks whether the TPG is authorized to receive the print data.

If an encryption was enabled on the ThinPrint server, you must install a certificate from a corresponding Certification Authority both on the ThinPrint server and the TPG. To authorize the TPG to receive encrypted print data, proceed as follows:

- Create a certificate request; see: ⇨ 59.
- Save the CA certificate; see: ⇨ 61.

5 Security



A number of security mechanisms are available to ensure optimum security for the TPG. This chapter describes how to make use of these security mechanisms.

What information do you need?

The following security mechanisms can be configured and activated according to your demands:

- 'How to Define the Encryption Level for SSL/TLS Connections' ⇒ 49
- 'How to Encrypt the Connection to the TPG Control Center' ⇒ 51
- 'How to Control the Access to the TPG Control Center (User Accounts)' ⇒ 52
- 'How to Control the Access to the TPG (TCP Port Access Control)' ⇒ 53
- 'How to Use Certificates Correctly' ⇒ 55
- 'How to Use Authentication Methods' ⇒ 63



The TPG Control Center can also be protected by the SNMP security concept. The concept includes administration of user groups and access rights. For further information; see: 'How to Configure SNMP' ⇒ 28.

5.1 How to Define the Encryption Level for SSL/TLS Connections

The following connections on the TPG can be encrypted via SSL/TLS:

- Email: POP3 (⇒ 30)
- Email: SMTP (⇒ 30)
- ThinPrint printer: IPP connection (⇒ 40)
- ThinPrint: data encryption (⇒ 47)
- Web access to the TPG Control Center: HTTPS (⇒ 51)

Encryption strength

The encryption strength and thus the safety of the connection is defined via the encryption protocol and level.

Protocol

The encryption protocols SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) are used to encrypt the connections. Which protocols are supported by the TPG depends on the product hardware and the installed firmware/software.

Encryption Level

Each encryption level is a collection of so-called cipher suites. A cipher suite is a standardized sequence of four cryptographic algorithms that are used to establish a secure connection. Depending on their cipher strength, cipher suites are grouped to form an encryption level. Which cipher suites are supported by the TPG, i.e. are part of an encryption level, depends on the SSL/TLS protocol used.

The following encryption levels can be selected:

- **Any:** The encryption is automatically negotiated by both communicating parties. The strongest encryption supported by both parties will always be chosen.
- **Low:** Only cipher suites with a low encryption are used. (Fast data transfer)
- **Medium**
- **High:** Only cipher suites with a strong encryption are used. (Slow data transfer)

Establishing Connections

When establishing a secure connection, the protocol to be used and a list of supported cipher suites is sent to the communicating party. A cipher suite is agreed upon that will be used later on. The strongest cipher suite that is supported by both parties will be used by default. If the communication partner does not support the protocol selected and/or if there is no cipher suite that is supported by both parties, no SSL/TLS connection will be established.



The communicating partners of the TPG (e.g. browser, ThinPrint server) must support the protocol selected and the cipher suites of the selected encryption level in order to successfully establish a connection. If problems occur, select different settings or reset the parameters of the TPG; see: ⇨ 75.



If you set 'Any' for encryption protocol and level, they will be negotiated automatically by both communicating parties. With these settings, the chances that a secure connection can be established are the highest.



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select SECURITY – SSL connections.*
3. *From the Encryption protocol area, select the desired protocol.*



Do not use the encryption protocol 'SSL' if you use up-to-date browser software and if only HTTPS is defined as the permitted connection type for the web access to the TPG Control Center. As current browsers do not support SSL, a connection can then not be established.

4. *From the Encryption level area, select the desired level.*



Do not use the encryption level 'Low' if you use up-to-date browser software and if only HTTPS is defined as the permitted connection type for the web access to the TPG Control Center. As

current browsers do not support cipher suites of 'Low', a connection can then not be established.

5. Click **Save to confirm**.

↪ The setting will be saved.



Detailed information about the individual SSL/TLS connection status (e.g. supported cipher suites) can be found on the Details page at **SSL connection status – Details**.

Types of Connection (HTTP/HTTPS)

5.2 How to Encrypt the Connection to the TPG Control Center

The web access to the TPG Control Center can be secured by selecting the permitted types of connection (HTTP/HTTPS).

If HTTPS is exclusively chosen as the connection type, the administrative web access to the TPG Control Center is protected by SSL/TLS. The encryption strength is defined via the encryption protocol and level ⇨ 49.

SSL/TLS requires a certificate to check the identity of the TPG. During a so-called 'handshake', the client asks for a certificate via a browser. This certificate must be accepted by the browser. Please refer to the documentation of your browser software. URLs that require an SSL/TLS connection start with 'https'.



Proceed as follows:

1. Start the TPG Control Center.
2. Select **SECURITY – Device access**.
3. In the **Connection area**, Tick **HTTP/HTTPS** or **HTTPS** only.
4. Click **Save to confirm**.

↪ The setting will be saved.

5.3 How to Control the Access to the TPG Control Center (User Accounts)

You can limit the access to the TPG Control Center. This is done with the help of user accounts.

User Accounts

There are two types of user accounts for which a name and password have to be defined. The accounts have different rights.

- Administrator: Complete access to the TPG Control Center. The user can see all pages and administrate.
- Read-only user: Very restricted access to the TPG Control Center. The user can only see the 'START' page.



The user accounts are also used for SNMP; see: ⇒ 28.

A user account allows for multiple logins, i.e. the account can be used by a single user or by a group of users. Up to 16 users can be logged in at the same time.

Login

If the access control is active, a login screen is displayed when the TPG Control Center is started. You can choose between two login screens:

- list of users
(User names are displayed. Only the password must be entered.)
- name and password request
(Neutral login screen in which user name and password are to be entered.)

Session Timeout

For stronger security, you can use a session timeout. If there is no activity during the timeout defined, the connection to the TPG Control Center is terminated automatically.



Proceed as follows:

1. Start the TPG Control Center.
2. Select SECURITY – Device access.

3. *Define the two user accounts. To do this, in the area **User accounts** enter a **User name** and **Password** respectively. (You can show the typing if you want to make sure that there are no typing errors in the password.)*
 4. *Tick **Restrict Control Center** access.*
 5. *Choose the **login screen type**: list of users or name and password.*
 6. *Tick **Session timeout** and into the **Session duration** box, enter the time in **Minutes** after which the timeout is to be effective. (Optional)*
 7. *Click **Save** to confirm.*
- ↳ The settings are saved.

5.4 How to Control the Access to the TPG (TCP Port Access Control)

TCP Port Access Control

You can control the access to the TPG. To do so, various TCP port types on the TPG can be locked. Network elements with access rights can be defined as exceptions and excluded from blocking. The TPG only accepts data packets from network elements defined as exceptions.

Security Levels

The port types to be blocked must be defined in the 'Security level' area. The following categorization can be selected:

- Lock TCP access (locks TCP ports: HTTP/HTTPS/...)
- Lock all (locks IP ports)

Exceptions

In order to exclude network elements (e.g. clients, DNS server, SMTP server) from port locking, they must be defined as exceptions. To do so, the IP addresses or MAC addresses (hardware addresses) of the network elements with access rights must be entered in the 'Exceptions' area. Please note:

- MAC addresses are not delivered through routers!
- The use of wildcards (*) allows you to define subnetworks.

Test Mode

The 'test mode' allows you to check the configured access protection. If the test mode is activated, access protection remains active

until the TPG is rebooted. After restarting, the protection is no longer effective.



The 'test mode' option is activated by default. After a successful test, you must deactivate the test mode so that access protection remains permanently active.



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select SECURITY – TCP port access.*
3. *Tick Port access control.*
4. *Select the desired protection in the Security level area.*
5. *In the Exceptions area, define the network elements which are excluded from port blocking. Enter the IP or MAC addresses and tick the options.*
6. *Make sure that the test mode is enabled.*
7. *Click Save & Restart to confirm.*
The settings are saved.
The port access control is activated until the device is restarted.
8. *Check the port access and configurability of the TPG.*



If the TPG can no longer be reached using the TPG Control Center, restart the device; see: ⇒ 78.

9. *Clear Test mode.*
 10. *Click Save & Restart to confirm.*
- ↪ The settings are saved. The port access control is active. Access to the ports is restricted.

5.5 How to Use Certificates Correctly

The TPG has its own certificate management. This section explains how certificates are used and when the use of certificates is recommended.

What are Certificates?

Certificates can be used in TCP/IP-based networks to encrypt data and to authenticate communication partners. Certificates are electronic messages containing a key (public key) and a signature.

Benefits and Purpose

The use of certificates allows for various security mechanisms. Use certificates on your TPG

- to receive encrypted print data; see: ⇒ 47.
- to check the identity of the TPG in the network; see: 'Configuring EAP-TLS' ⇒ 64.
- to authenticate the TPG/client if the administrative access to the TPG Control Center is protected via HTTPS (SSL/TLS); see: ⇒ 51.



If you want to use certificates, it is advisable to restrict the administrative web access to the TPG Control Center so that certificates on the TPG cannot be deleted by unauthorized persons; see: ⇒ 51.

Which Certificates are available?

Both self-signed and externally signed certificates can be used with the TPG. The following certificates can be distinguished:

- Upon delivery, a certificate (the so-called **default certificate**) is stored in the TPG. It is recommended that you replace the default certificate by a self-signed certificate or requested certificate as soon as possible.
- **Self-signed certificates** have a digital signature that has been created by the TPG. If a self-signed certificate is used, the ThinPrint server cannot print via SSL/TLS. A CA certificate is mandatory to print via SSL.
- A **requested certificate** is created by a certification authority (CA) for the TPG on the basis of a certificate request.
- **CA certificates** are certificates that have been issued for a certification authority (CA). They are used for verifying

certificates that have been issued by the respective certification authority.

- **S/MIME certificates** (*.pem file) are used to sign and encrypt the emails that are sent by the TPG. The corresponding private key must be installed as an own certificate in the PKCS#12 format (as *.p12 file) in the intended email program (Thunderbird, Outlook, etc.). Only then can the emails be verified and displayed (in the case of encryption).

The following certificates can be installed at the same time in the TPG:

- 1 Self-signed certificate
- 1 client certificate, i.e. 1 requested certificate OR 1 PKCS#12 certificate
- 1–32 CA certificates
- 1 S/MIME certificate

All certificates can be deleted separately.

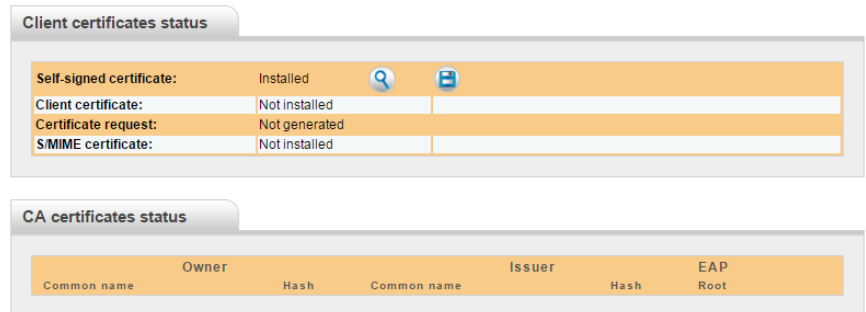










Abb. 6: TPG Control Center - Certificates

What do you want to do?

- 'Displaying Certificates' ⇒  57
- 'Creating a Self-Signed Certificate' ⇒  57
- 'Creating a Certificate Request for a Requested Certificate' ⇒  59
- 'Installing the Requested Certificate in the TPG' ⇒  59
- 'Installing the PKCS#12 certificate in the TPG' ⇒  60
- 'Saving S/MIME certificates in the TPG' ⇒  60
- 'Installing the CA Certificate in the TPG' ⇒  61
- 'Deleting Certificates' ⇒  62

Displaying Certificates


Certificates installed on the TPG and certificate requests can be displayed and viewed.

Requirements

- A certificate is installed on the TPG.




Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select SECURITY – Certificates.*
 3. *Select the certificate via the icon .*
- ↳ The certificate is displayed.


Creating a Self-Signed Certificate



If a self-signed certificate has already been created on the TPG, you must first delete it; see: ⇒  62.



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select SECURITY – Certificates.*
3. *Click Self-signed certificate.*
4. *Enter the relevant parameters, siehe: Tabelle 11 ⇒  58.*

5. Click Install.

↳ The certificate will be created and installed. This may take a few minutes.

Tabelle 11: Parameters for the Creation of Certificates

Parameters	Description
Common name	Is used to clearly identify the certificate. It is advisable to use the IP address or the host name of the TPG to allow a clear assignment of the certificate to the TPG. <i>You can enter a maximum of 64 characters.</i>
Email address	Specifies an email address. <i>You can enter a maximum of 40 characters. (Optional Entry)</i>
Organization name	Specifies the company that uses the TPG. <i>You can enter a maximum of 64 characters.</i>
Organizational unit	Specifies the department or subsection of a company. <i>You can enter a maximum of 64 characters. (Optional Entry)</i>
Location	Specifies the locality where the company is based. <i>You can enter a maximum of 64 characters.</i>
State name	Specifies the state in which the company is based. <i>You can enter a maximum of 64 characters. (Optional Entry)</i>
Domain component	Allows you to enter additional attributes. <i>(Optional Entry)</i>
Country	Specifies the country in which the company is based. Enter the two-digit country code according to ISO 3166. Examples: DE = Germany, GB = Great Britain, US = USA
Issued on	Specifies the date from which on the certificate is valid.
Expires on	Specifies the date from which on the certificate becomes invalid.
RSA key length	Defines the length of the RSA key used: - 512 bit (fast encryption and decryption) - 768 bit - 1024 bit (standard encryption and decryption) - 2048 bit (slow encryption and decryption)

Requirements

Creating a Certificate Request for a Requested Certificate

As preparation for using a certificate which is issued by a certification authority for the TPG, a certificate request can be created in the TPG. The request must be sent to the certification authority which creates an certificate on the basis of this request. The certificate must be in 'base64' format.



If a certificate request has already been created, you must first delete it; see: ⇒ 62.



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select SECURITY – Certificates.*
3. *Click Certificate request.*
4. *Enter the required parameters, siehe: Tabelle 11 ⇒ 58.*
5. *Click Create a request.*
The creation of the certificate request is in progress. This may take a few minutes.
6. *Select Upload and save the requests in a text file.*
7. *Click OK.*
8. *Send the text file as certificate request to a certification authority.*

When the requested certificate has been received, it must be saved in the TPG; see: ⇒ 59.

Installing the Requested Certificate in the TPG

- A certificate request has been created at an earlier date; see: ⇒ 59.
- The certificate must be in 'base64' format.



If a PKCS#12 certificate has already been installed on the TPG, you must first delete it; see: ⇒ 62.

Requirements



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select SECURITY – Certificates.*
3. *Click Requested certificate.*
4. *Click Browse.*
5. *Specify the requested certificate.*
6. *Click Install.*

↳ The requested certificate will be installed in the TPG.

Installing the PKCS#12 certificate in the TPG

Certificates with the PKCS#12 format are used to save private keys and their respective certificates and to protect them by means of a password.



If a PKCS#12 or a requested certificate has already been installed on the TPG, you must first delete it; see: ⇒ 62.

- The certificate must be in 'base64' format.



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select SECURITY – Certificates.*
3. *Click PKCS#12 certificate.*
4. *Click Browse.*
5. *Specify the PKCS#12 certificate.*
6. *Enter the password.*
7. *Click Install.*

↳ The PKCS#12 certificate is saved in the TPG.

Saving S/MIME certificates in the TPG

S/MIME certificates (*.pem file) are used to sign and encrypt the emails that are sent by the TPG.



If an S/MIME certificate has already been installed on the TPG, you must first delete it; see: ⇒ 62.

Requirements

- ☑ The certificate must be in base64 format.



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select **SECURITY – Certificates.***
3. *Click S/MIME certificate.*
4. *Click **Browse.***
5. *Specify the S/MIME certificate.*
6. *Click **Install.***

↪ The S/MIME certificate is be saved on the TPG.

Installing the CA Certificate in the TPG

In order to check the identity of the communicating parties of the TPG, it is necessary to validate their certificates. For this, the root CA certificates of the certification authorities that have issued the certificates of said communicating parties are installed on the TPG.

Up to 32 CA certificates can be installed. Thus multi-level public key infrastructures (PKIs) are supported.

Example: The TPG offers a number of authentication methods to verify its identity in a network. If you use the authentication method 'EAP-TLS' (⇒ 64), you must install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the TPG.

Requirements

- ☑ The certificate must be in base64 format.



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select **SECURITY – Certificates.***
3. *Click **CA certificate.***
4. *Click **Browse.***

5. *Specify the root certificate.*
6. *Click Install.*

The CA certificate will be saved in the TPG.

Deleting Certificates





Do not delete the certificate (CA/self-signed/PKCS#12) if only HTTPS is defined as the permitted connection type for the web access to the TPG Control Center. If the corresponding certificate is deleted, the TPG Control Center can no longer be reached. In this case you have to reset the parameters of the TPG; see: ⇒ 75.

Requirements

- A certificate is installed on the TPG.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select SECURITY – Certificates.*
 3. *Select the certificate to be deleted via the icon . The certificate is displayed.*
 4. *Click Delete.*
-  The certificate is deleted.

5.6 How to Use Authentication Methods

By means of an authentication, a network can be protected against unauthorized access. The TPG can participate in various authentication procedures. This section describes which procedures are supported and how these procedures are configured on the TPG.

What is IEEE 802.1X?

The IEEE 802.1X standard provides a basic structure for various authentication and key management protocols. IEEE 802.1X allows you to control the access to networks. Before users gain access to a network via a network device, they must authenticate themselves in the network. After the authentication was successful, the access to the network will be freed.

What is EAP?

The standard IEEE 802.1X is based upon the EAP (Extensible Authentication Protocol). EAP is a universal protocol for many authentication procedures. EAP allows for a standardized authentication procedure between the network device and an authentication server (RADIUS). First you must define the authentication procedure (TLS, PEAP, TTLS, etc.) to be used and configure it on all network devices involved.

What is RADIUS?

RADIUS (Remote Authentication Dial-In User Service) is an authentication and account management system that validates user login information and grants access to the desired resources.

The TPG supports various EAP authentication methods in order to authenticate itself in a protected network.

What do you want to do?

- 'Configuring EAP-MD5' ⇒ 64
- 'Configuring EAP-TLS' ⇒ 64
- 'Configuring EAP-TTLS' ⇒ 65
- 'Configuring PEAP' ⇒ 67
- 'Configuring EAP-FAST' ⇒ 68

Configuring EAP-MD5

Benefits and Purpose

EAP-MD5 validates the identity of devices or users before they gain access to network resources. You can configure the TPG for the EAP-MD5 network authentication. This makes sure that the TPG gets access to protected networks.

Mode of Operation


EAP-MD5 describes a user-based authentication method via a RADIUS server. The TPG must be defined as user (with user name and password) on a RADIUS server. The authentication method EAP-MD5 must then be enabled on the TPG and the user name and password need to be entered.

Requirements

- The TPG is defined as user (with user name and password) on a RADIUS server.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **SECURITY – Authentication**.*
 3. *Select **MD5** from the **Authentication method list**.*
 4. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*
 5. *Click **Save & Restart** to confirm.*
-  The settings are saved.

Configuring EAP-TLS

Benefits and Purpose

EAP-TLS (Transport Layer Security) validates the identity of devices or users before they gain access to network resources. You can configure the TPG for the EAP-TLS network authentication. This makes sure that the TPG gets access to protected networks.

Mode of Operation

EAP-TLS describes a certificate-based authentication method via a RADIUS server. For this purpose, certificates are exchanged between the TPG and the RADIUS server. An encrypted TLS connection between the TPG and the RADIUS server is established in this process. Both RADIUS server and TPG need a valid, digital certificate signed by a CA. The RADIUS server and the print server must validate

the certificate. After the mutual authentication was successful, the access to the network will be freed.

Since each device needs a certificate, a PKI (Public Key Infrastructure) must be available. User passwords are not necessary.



If you want to use the EAP-TLS authentication, you must observe the instructions below in the indicated order. If this procedure is not adhered to, the TPG in the network may not be addressable. In this case you have to reset the TPG parameters; see: ⇒ 75.

Procedure

- Create a certificate request on the TPG; see: ⇒ 59.
- Create a certificate using the certificate request and the authentication server.
- Install the requested certificate on the TPG; see: ⇒ 59.
- Install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the TPG; see: 'Installing the CA Certificate in the TPG' ⇒ 61.
- Enable the authentication method 'EAP-TLS' on the TPG.



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select **SECURITY – Authentication**.*
3. *Select **TLS** from the Authentication method list.*
4. *Select the root CA certificate from the list EAP root certificate.*
5. *Click **Save & Restart** to confirm.*

↪ The settings are saved.

Configuring EAP-TTLS

EAP-TTLS (Tunneled Transport Layer Security) validates the identity of devices or users before they gain access to network resources. You can configure the TPG for the EAP-TTLS network authentication. This makes sure that the TPG gets access to protected networks.

Benefits and Purpose

Mode of Operation

EAP-TTLS consists of two phases:

- In phase 1, a TLS-encrypted channel between the TPG and the RADIUS server will be established. Only the RADIUS server authenticates itself using a certificate that was signed by a CA. This process is also referred to as 'outer authentication'.
- In phase 2, an additional authentication method is used for the communication within the TLS channel. EAP-defined methods and older methods (CHAP, PAP, MS-CHAP and MS-CHAPv2) are supported. This process is also referred to as 'inner authentication'.

The advantage of this procedure is that only the RADIUS server needs a certificate. Therefore no PKI is needed. Moreover, TTLS supports most authentication protocols.

Requirements

- ☑ The TPG is defined as user (with user name and password) on a RADIUS server.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **SECURITY – Authentication**.*
 3. *Select **TTLS** from the **Authentication method list**.*
 4. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*
 5. *Select the settings intended to secure the communication in the TLS channel.*
 6. *To make the connection more secure, you can also install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the TPG; see: 'Installing the CA Certificate in the TPG' ⇨ 61. Afterwards, select the root CA certificate from the list **EAP root certificate**.*
 7. *Click **Save & Restart** to confirm.*
- ↪ The settings are saved.

Configuring PEAP

Benefits and Purpose

PEAP (Protected Extensible Authentication Protocol) validates the identity of devices or users before they gain access to network resources. You can configure the TPG for the PEAP network authentication. This makes sure that the TPG gets access to protected networks.

Mode of Operation

In the case of PEAP (compare EAP-TTLS, see ⇨ 65), an encrypted TLS (Transport Layer Security) channel is established between the TPG and the RADIUS server. Only the RADIUS server authenticates itself using a certificate that was signed by a CA.

The TLS channel is then used to establish another connection that can be protected by means of additional EAP authentication methods (e.g. MSCHAPv2).

The advantage of this procedure is that only the RADIUS server needs a certificate. Therefore no PKI is needed. PEAP uses the advantages of TLS and supports various authentication methods, including user passwords and one-time passwords.

Requirements

- ☑ The TPG is defined as user (with user name and password) on a RADIUS server.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select **SECURITY – Authentication**.*
 3. *Select **PEAP** from the **Authentication method** list.*
 4. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*
 5. *Select the settings intended to secure the communication in the TLS channel.*
 6. *To make the connection more secure, you can also install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the TPG; see: 'Installing the CA Certificate in the TPG' ⇨ 61. Afterwards, select the root CA certificate from the list **EAP root certificate**.*
 7. *Click **Save & Restart** to confirm.*
- ↳ The settings are saved.

Configuring EAP-FAST

Benefits and Purpose

EAP-FAST (Flexible Authentication via Secure Tunneling) validates the identity of devices or users before they gain access to network resources. You can configure the TPG for the EAP-FAST network authentication. This makes sure that the TPG gets access to protected networks.

Mode of Operation

EAP-FAST uses (as in the case of EAP-TTLS, see ⇒ 65) a channel in order to protect the data transfer. The main difference is that EAP-FAST does not require certificates for authentication purposes. (The use of certificates is optional.)

PACs (Protected Access Credentials) are used to build the channel. PACs are credentials that comprise up to three components.

- A shared secret key that contains the preshared key between the TPG and the RADIUS server.
- An opaque part that is provided to the TPG and presented to the RADIUS server when the TPG wishes to obtain access to network resources.
- Other information that may be useful to the client. (Optional)

EAP-FAST uses two methods to generate PACs:

- The manual delivery mechanism can be every mechanism that the administrator configures and considers to be safe for the network.
- In the case of the automatic delivery, an encrypted channel is established in order to protect the authentication of the TPG as well as the delivery of the PACs.

Requirements

- The TPG is defined as user (with user name and password) on a RADIUS server.



Proceed as follows:

1. *Start the TPG Control Center.*
2. **Select SECURITY – Authentication.**
3. **Select FAST from the Authentication method list.**

4. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*
 5. *Select the settings intended to secure the communication in the channel.*
 6. *Click **Save & Restart** to confirm.*
- ↪ The settings are saved.

6 Maintenance



A number of maintenance activities can be carried out on the TPG. This chapter gives a short overview.

What information do you need?

- 'How to Secure the TPG Parameters (Backup)' ⇨ 71
- 'How to Use a Connected USB Device' ⇨ 72
- 'How to Reset Parameters to their Default Values (Reset)' ⇨ 75
- 'How to Perform an Update' ⇨ 77
- 'How to Restart the TPG?' ⇨ 78
- 'How to Print a Status or Service Page' ⇨ 79
- 'How to Display the Job History' ⇨ 81

6.1 How to Secure the TPG Parameters (Backup)

All parameter values of the TPG (exception: passwords) are saved in the '<Default name>_parameter.txt' file.


You can save the parameters file as backup copy on your local client. This allows you to get back to a stable configuration status at any time.


You can edit the parameter values of the copied file using a text editor. Afterwards, the configured file can be downloaded to a TPG. The parameter values included in the file will be taken over by the device.

What do you want
to do?

- 'Displaying Parameter Values' ⇨ 71
- 'Saving the Parameter File' ⇨ 71
- 'Loading the parameters file to a TPG' ⇨ 72

Displaying Parameter Values


 Proceed as follows:


1. Start the TPG Control Center.
 2. Select **MAINTENANCE – Parameter backup**.
 3. Click the icon .
- ↪ The current parameter values are displayed.



A detailed description of the parameters can be found in the 'Parameter List' ⇨ 88.

Saving the Parameter File


 Proceed as follows:

1. Start the TPG Control Center.
 2. Select **MAINTENANCE – Parameter backup**.
 3. Click the icon .
- The current parameter values are displayed.*

4. Save the '<Default name>_parameter.txt' file on a local system with the help of your browser.

↪ The parameter file is copied and secured.

Loading the parameters file to a TPG

 Proceed as follows:

1. Start the TPG Control Center.
2. Select **MAINTENANCE – Parameter backup**.
3. Click **Browse**.
4. Specify the '<Default name>_parameter.txt' file.
5. Click **Import**.

↪ The parameter values in the file are applied to the TPG.



You can also automatically load a parameters file from a USB flash drive to a TPG; see: ⇒ 72.

6.2 How to Use a Connected USB Device

You can connect a USB flash drive to the USB port of the TPG to make use of additional features of the TPG.

Print job buffering

If a printer is not available, the print jobs that are sent to that printer can be automatically buffered in the USB flash drive. As soon as the printer becomes available, the print jobs will be transferred to the printer and printed. If this option has been disabled and the printer is not available, the print jobs will be canceled after a specified timeout ('printer connection timeout' ⇒ 42).

Parameter Backup

During the 'parameter backup', the '<Default name>_parameter.txt' file will be saved automatically on the USB flash drive and updated after a parameter change. The file contains all parameter values of the TPG (exception: passwords). As soon as the TPG restarts, it will automatically take over the values contained in the parameters file on the USB flash drive. This way, the parameter values can be quickly and easily loaded to other TPG via a USB flash drive (e.g. when configuring new devices).

Formatting

To use the USB flash drive on the TPG, the USB flash drive must have the correct file system. You may have to format the USB flash drive, if necessary.



Whether formatting is required, will be displayed under 'MAINTENANCE – USB device status' in the TPG Control Center.

What do you want to do?

- 'Formatting the USB Flash Drive' ⇨ [73](#)
- 'Automatic print job buffering' ⇨ [73](#)
- 'Saving the Parameter Values Automatically' ⇨ [74](#)
- 'Loading the Parameter Values Automatically to a TPG' ⇨ [74](#)

Formatting the USB Flash Drive

During the formatting process, all data on the USB flash drive will be permanently lost.

Requirements

- A USB flash drive has been connected to the TPG.



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select MAINTENANCE – USB device.*
3. *Click Formatting.*

↳ The USB flash drive will be formatted.

Automatic print job buffering**Requirements**

- A USB flash drive has been connected to the TPG.
- The USB flash drive has been formatted correctly; see: ⇨ [73](#).



Proceed as follows:


1. *Start the TPG Control Center.*

Requirements

2. *Select MAINTENANCE – USB device.*
 3. *Tick Print job buffering.*
 4. *Click Save.*
- ↪ The settings are saved.

Saving the Parameter Values Automatically


- A USB flash drive has been connected to the TPG.
- The USB flash drive has been formatted correctly; see: ⇨ [73](#).

 Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select MAINTENANCE – USB device.*
 3. *Tick Parameter backup.*
 4. *Click Save.*
- ↪ The settings are saved.

Requirements**Loading the Parameter Values Automatically to a TPG**

- The USB flash drive has been formatted correctly; see: ⇨ [73](#).
- A parameter file exists on the USB flash drive; see: ⇨ [72](#).

 Proceed as follows:

1. *Connect a USB flash drive to the USB port of the TPG.*
 2. *Restart the TPG; see: ⇨ [78](#).*
- ↪ Upon the next device restart, the parameter values in the file are automatically applied to the TPG.

6.3 How to Reset Parameters to their Default Values (Reset)

It is possible to reset the parameters of the TPG to their default values (factory settings). All previously configured parameter values will be deleted in this process. Installed certificates will not be deleted.



If you reset the parameters, the IP address of the TPG may change and the connection to the TPG Control Center may be terminated.

You must reset the parameters, for example, if you have changed the location of the TPG and if you want to use the TPG in a different network. Before this change of location, you should reset the parameters to their default settings to install the TPG in a different network.



Remove an attached USB flash drive before resetting the parameters. If a parameters file is saved on the USB flash drive, the TPG will – after the reset – automatically use the parameter values saved on the USB flash drive (see: ⇒ 72).



By means of the status/reset button of the device you can reset the parameters without entering the password.

What do you want to do?

- 'Resetting the parameters via the TPG Control Center' ⇒ 75
- 'Resetting Parameters via the InterCon-NetTool' ⇒ 76
- 'Resetting the parameters via the status/reset button' ⇒ 76

Resetting the parameters via the TPG Control Center



Proceed as follows:

1. *Start the TPG Control Center.*
 2. **Select MAINTENANCE – Default settings.**
 3. **Click Default settings.**
- ↪ The parameters are reset.

Resetting Parameters via the InterCon-NetTool



Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Highlight the TPG in the device list.*
3. *Select Actions – Default Settings from the menu bar.*
4. *Click Finish.*



The parameters are reset.

Resetting the parameters via the status/reset button



Proceed as follows:

1. *Press the reset button for 5 seconds.*
The TPG restarts.



The parameters are reset.



If you want verify the reset, you can print a service page. To do this, press the status/reset button for a short time.

6.4 How to Perform an Update

You can carry out software and firmware updates on the TPG. Updates allow you to benefit from currently developed features.

What Happens during an Update?

In the course of an update, the old firmware/software will be overwritten and replaced by the new firmware/software. The parameter default settings of the device remain unchanged.

When is an Update recommended?

An update should be undertaken if function do not work properly and if SEH Computertechnik GmbH has released a new software or firmware version with new functions or bug fixes.

Where do I Find the Update Files?

Check the installed software and firmware version on the TPG. You will find the version number on the TPG Control Center homepage or in the product list in the InterCon-NetTool.

Current firmware and software files can be downloaded from the homepage of SEH Computertechnik GmbH:

<http://www.seh-technology.com/services/downloads.html>



Every update file has its own 'readme' file. Take note of the information contained in the 'readme' file.



Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select MAINTENANCE – Update.*
 3. *Click Browse.*
 4. *Select the update file.*
 5. *Click Install.*
- The update is executed. The TPG is restarted.


What do you want to do?

6.5 How to Restart the TPG?

The TPG is rebooted automatically after parameter changes or updates. If the TPG is in an undefined state it can also be rebooted manually.

- 'Rebooting the TPG via the TPG Control Center' ⇒ 78
- 'Restarting the TPG via the InterCon-NetTool' ⇒ 78


Rebooting the TPG via the TPG Control Center

 Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select MAINTENANCE – Restart.*
3. *Click Restart.*

↪ The TPG is restarted.

Restarting the TPG via the InterCon-NetTool

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Highlight the TPG in the device list.*
3. *Select Actions – Restart from the menu bar.*
The Restart print server dialog appears.

4. *Click Finish.*

↪ The TPG is restarted.

6.6 How to Print a Status or Service Page

You can print status or service pages. Both pages are available in English.

Status Page

A status page contains basic information of the TPG such as the model type, hardware address, IP address, subnet mask, gateway, etc.

Service page

A service page contains basic information of the TPG as well as a list of the current parameter values of the TPG.



Before a status or service page is printed, the printing function must be enabled and the relevant printer as well as the data format of the status or service page (ASCII, PostScript, DATAMAX or Citizen-Z) must be specified. The printer ID 1 and the data format ASCII are preset.



The relevant printer is highlighted in blue in the **Device – ThinPrint® printer** menu bar.

What do you want to do?

- 'Specifying the Printing Function, Printer and the Data Format via the TPG Control Center' ⇒ 79
- 'Printing a status page via the TPG Control Center' ⇒ 80
- 'Printing a service page via the TPG Control Center' ⇒ 80
- 'Printing a service page via the TPG Control Center' ⇒ 80
- 'Printing a Service Page via the Status/Reset Button' ⇒ 80

Specifying the Printing Function, Printer and the Data Format via the TPG Control Center




Proceed as follows:

1. Start the TPG Control Center.
2. Select **MAINTENANCE – Status page**.
3. Select the desired printer ID from the **Status Page Printer list**.
4. Select the desired data format from the **Status page mode list**.


5. *Tick Printing.*
 6. *Click Save to confirm.*
- ↪ The settings are saved.

Printing a status page via the TPG Control Center

 Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select MAINTENANCE – Status page.*
 3. *Click Status page.*
- ↪ The status page is printed.


Printing a service page via the TPG Control Center

 Proceed as follows:

1. *Start the TPG Control Center.*
 2. *Select MAINTENANCE – Status page.*
 3. *Click Service page.*
- ↪ The service page will be printed.

Printing a Service Page via the Status/Reset Button

You can print a service page via the status/reset button of the device.

 Proceed as follows:

1. *Press the status/reset button for a short time.*
- ↪ The service page is printed.

6.7 How to Display the Job History

You can get information about the ThinPrint print jobs that have been sent to the TPG. Only these print jobs are registered and shown in the job history.



A time server (⇒ 34) must be configured on the TPG so that the date and time can be displayed correctly. If no time server is configured, the time stamp corresponds to the default time.

A maximum of 32 print jobs are displayed. The first-in, first-out method is applied from the 33rd print job onwards. The saved print jobs will be deleted when the TPG is turned off or reset. The print jobs can also be deleted manually. The print jobs will not be deleted when the TPG is restarted.

What do you want to do?

- 'Displaying the job history' ⇒ 81
- 'Deleting Print Jobs Manually' ⇒ 83

Displaying the job history



Proceed as follows:

1. Start the TPG Control Center.
 2. Select **MAINTENANCE – Job history**.
- ↪ The Job History is displayed.

The following information is shown in the Job History:

Information	Description
ID	Identification number of the printer that has spooled the print job.

Information	Description
Status	<p>Status of the print connection. The following statuses are possible:</p> <ul style="list-style-type: none"> - Initialized: The connection to the ThinPrint Server is established. In a next step, the connection to the printer will be established. - Try to connect: The connection to the printer is being established. - Connection rejected: The printer has refused the connection. - Pending: The print job has been accepted by the TPG but the data transfer to the printer has not yet started. - Processing: The print job is being transferred from the TPG to the printer. - Processing stopped: The data transfer to the printer has been interrupted. This can occur if, for example, the printer ran out of paper. - Completed: The TPG has completely transferred the print job to the printer. - Aborted: The print job has been aborted. This can occur if, for example, the TPG has been restarted while the print job was processed. - Buffering: The print job is being saved to the USB flash drive; see: ⇒ 72. - Buffered: The print job has been saved in the USB flash drive; see: ⇒ 72. - Buffering failed: The print job could not be saved in the USB flash drive. See: 'Troubleshooting' ⇒ 105.
Protocol	<p>Protocol used to transfer the print data. The presentation consists in a combination of the following values:</p> <ul style="list-style-type: none"> - ThP: ThinPrint - Stp: status or service page - USB: buffered on USB flash drive - Sock: RAW/socket printing - IPP: IPP printing - LPD: LPD printing
Name	Name of the print job
Sender	<p>Name of the sending host:</p> <ul style="list-style-type: none"> - '<domain user name>@<domain>' appears with ThinPrint print jobs. - 'TPG-25' or 'TPG-65' or 'TPG-125' appears when printing a status or service page.
Start	Time at which the print job has been sent to the TPG.
Size	Size (in Kb) of the print job.
Duration	The time needed by the TPG for processing the print job.

Deleting Print Jobs Manually



Proceed as follows:

1. *Start the TPG Control Center.*
2. *Select **MAINTENANCE – Job history.***
3. *Click **Delete.***

↪ All print jobs listed in the job history will be deleted.

7 Appendix



The appendix contains a glossary, the TPG parameter list, a trouble shooting and the index lists of this document.

What information do you need?

- 'Glossary' ⇨ 85
- 'Parameter List' ⇨ 88
- 'Troubleshooting' ⇨ 105
- 'List of Figures' ⇨ 109
- 'Index' ⇨ 110

What information do you need?

Default Name

Gateway

7.1 Glossary

The glossary contains information about manufacturer-specific software solutions and terms from the world of network technology.

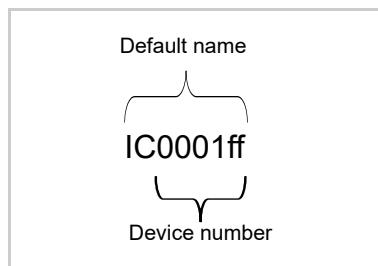
Manufacturer-Specific Software Solutions

- 'InterCon-NetTool' ⇒ 86
- 'TPG Control Center' ⇒ 87

Network Technology

- 'Default Name' ⇒ 85
- 'Gateway' ⇒ 85
- 'Hardware Address' ⇒ 86
- 'Host Name' ⇒ 86
- 'IP Address' ⇒ 86
- 'Subnet Mask' ⇒ 87

The default name of the TPG is made up of the two letters 'IC' and the device number. The device number consists of the last six numbers of its hardware address.

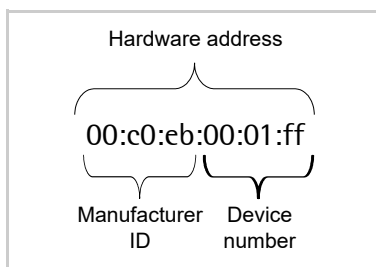


The default name can be found in the TPG Control Center, the InterCon-NetTool, on the status or service page.

Using a gateway, you can address IP addresses from external networks. If you wish to use a gateway, you can configure the relevant parameter via the TPG Control Center or the InterCon-NetTool.

Hardware Address

The TPG is addressable by means of its world-wide unique hardware address. This address is commonly referred to as the MAC or Ethernet address. The manufacturer has defined this address in the hardware of the device. The address consists of 12 hexadecimal numbers. The first six numbers represent the manufacturer, while the last six numbers identify the individual device.



The hardware address can be found on the housing, the InterCon-NetTool, the status or service page.

The use of separators within the hardware address depends on the platform. Note the following conventions when entering the hardware address:

Operating system	Representation	Example
Windows	Hyphen	00-c0-eb-00-01-ff
UNIX	Colon or period	00:c0:eb:00:01:ff or 00.c0.eb.00.01.ff

Host Name

The host name is an alias for an IP address. The host name uniquely identifies the TPG in the network and makes it easier to remember.

InterCon-NetTool

The software InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices within a predefined network.

IP Address

The IP address is the unique address of each node in a network, i.e. an IP address may occur only once on a local network. The system administrator usually assigns the IP address. The address must be

saved in the TPG to make sure that it can be addressed within the network.

Subnet Mask

With the help of the subnet mask, large networks can be split up into subnetworks. In this case, the user IDs of the IP addresses are assigned to the various subnetworks.

The TPG is configured not to use subnetworks by default. If you wish to use a subnet, you can configure the relevant parameter via the TPG Control Center or the InterCon-NetTool.

TPG Control Center

The TPG can be configured and monitored via the TPG Control Center. The TPG Control Center is stored in the TPG and can be displayed by means of a browser software (Internet Explorer, Firefox, Safari).

**What information do
you need?**

7.2 Parameter List

This chapter gives an overview of all parameters of the TPG. The parameter list gives details about the functions and values of the individual parameters.

- 'Parameter List - IPv4' ⇨ 89
- 'Parameter List - IPv6' ⇨ 89
- 'Parameter List - DNS' ⇨ 90
- 'Parameter List - SNMP' ⇨ 91
- 'Parameter List - POP3' ⇨ 92
- 'Parameter List - SMTP' ⇨ 93
- 'Parameter List - Bonjour' ⇨ 94
- 'Parameter List - Date/Time' ⇨ 94
- 'Parameter List - Description' ⇨ 94
- 'Parameter List - ThinPrint®' ⇨ 95
- 'Parameter List - ThinPrint Connection Service' ⇨ 95
- 'Parameter List - ThinPrint® printer' ⇨ 97
- 'Parameter List - Notification' ⇨ 98
- 'Parameter List - SSL/TLS connections' ⇨ 100
- 'Parameter List - TPG Control Center security' ⇨ 101
- 'Parameter List - TCP port access' ⇨ 102
- 'Parameter List - Authentication' ⇨ 103
- 'Parameter List - USB device' ⇨ 104
- 'Parameter List - Status page' ⇨ 104



To view the current parameter values of your TPG, see: 'Displaying Parameter Values' ⇨ 71 and 'How to Print a Status or Service Page' ⇨ 79.

Tabelle 12: Parameter List - IPv4

Parameters	Value	Default	Description
ip_dhcp [DHCP]	on/off	on	Enables/disables the DHCP protocol.
ip_bootp [BOOTP]	on/off	on	Enables/disables the BOOTP protocol.
ip_auto [ARP/PING]	on/off	on	Enables/disables the IP address assignment via ARP/PING.
ip_addr [IP address]	valid IP address	169.254. 0.0/16	Defines the IP address of the TPG.
ip_mask [Subnet mask]	valid IP address	255.255. 0.0	Defines the subnet mask of the TPG.
ip_gate [Gateway]	valid IP address	0.0.0.0	Defines the gateway address of the TPG.

Tabelle 13: Parameter List – IPv6

Parameters	Value	Default	Description
ipv6 [IPv6]	on/off	on	Enables/disables the IPv6 functionality of the TPG.
ipv6_auto [Automatic configuration]	on/off	on	Enables/disables the automatic assignment of the IPv6 address for the TPG.
ipv6_addr [IPv6 address]	n:n:n:n:n:n	::	Defines a manually assigned IPv6 Unicast address in the n:n:n:n:n:n format for the TPG. <i>Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.</i>

Parameters	Value	Default	Description
ipv6_gate [Router]	n:n:n:n:n:n	::	Defines the IPv6 unicast address of the router. The TPG sends its 'Router Solicitations' (RS) to this router.
ipv6_plen [Prefix length]	0–64 [1–2 characters; 0-9]	64	Defines the length of the subnet prefix for the IPv6 address. <i>Address ranges are indicated by prefixes. The prefix length (number of bits used) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/'.</i>

Tabelle 14: Parameter List - DNS

Parameters	Value	Default	Description
dns [DNS]	on/off	on	Enables/disables the name resolution via a DNS server.
dns_primary [Primary DNS server]	valid IP address	0.0.0.0	Defines the IP address of the primary DNS server.
dns_secondary [Secondary DNS server]	valid IP address	0.0.0.0	Defines the IP address of the secondary DNS server. <i>The secondary DNS server is used if the primary DNS server is not available.</i>
dns_domain [Domain name (suffix)]	max. 255 characters [., a–z, A–Z, 0–9]	[blank]	Defines the domain name of an existing DNS server.

Tabelle 15: Parameter List - SNMP

Parameters	Value	Default	Description
snmpv1 [SNMPv1]	on/off	on	Enables/disables SNMPv1.
snmpv1_ronly [Read-only]	on/off	off	Enables/disables the write protection for the community.
snmpv1_community [Community]	max. 64 characters [a-z, A-Z, 0-9]	public	Defines the name of the SNMP community. <i>The SNMP Community is a basic form of access protection in which several participants with the same access rights are grouped together.</i>
snmpv3 [SNMPv3]	on/off	on	Enables/disables SNMPv3.
any_hash [Hash]	md5 sha	md5	Specifies the HASH algorithm of the SNMP user group 1.
any_rights [Access rights]	--- readonly readwrite	readonly	Defines the access rights of the SNMP user group 1. --- = none readonly = read only readwrite = read and write
any_cipher [Encryption]	--- [None] aes des	---	Defines the encryption method of the SNMP user group 1.
admin_hash [Hash]	md5 sha	md5	Specifies the HASH algorithm of the SNMP user group 2.
admin_rights [Access rights]	--- readonly readwrite	readwrite	Defines the access rights of the SNMP user group 2. --- = none readonly = read only readwrite = read and write
admin_cipher [Encryption]	--- [None] aes des	---	Defines the encryption method of the SNMP user group 2.



For SNMP user accounts see: 'Parameter List - TPG Control Center security' ⇨ 101.

Tabelle 16: Parameter List - POP3

Parameters	Value	Default	Description
pop3 [POP3]	on/off	off	Enables/disables the POP3 functionality.
pop3_srv [Server name]	max. 128 characters	[blank]	Defines a POP3 server via the IP address or the host name. <i>A host name can only be used if a DNS server was configured beforehand.</i>
pop3_port [Server port]	1–65535 [1–5 characters; 0–9]	110	Defines the port of the POP3 server used by the TPG for receiving emails. When using SSL/TLS, enter 995 as port number.
pop3_sec [Security]	0–2 [1 character; 0–2]	0	Defines the authentication method to be used. <i>0 = no security 1 = APOP 2 = SSL/TLS</i>
pop3_poll [Check mail every]	1–10080 [1–5 characters; 0–9]	15	Defines the time interval (in minutes) for retrieving emails from the POP3 server.
pop3_limit [Ignore mail exceeding]	0–4096 [1–4 characters; 0–9; 0 = unlimited]	10	Defines the maximum email size (in Kbyte) to be accepted by the TPG.
pop3_usr [User name]	max. 128 characters	[blank]	Defines the name used by the TPG to log on to the POP3 server.
pop3_pwd [Password]	max. 128 characters	[blank]	Defines the password used by the TPG to log on to the POP3 server.

Tabelle 17: Parameter List - SMTP

Parameters	Value	Default	Description
smtp_srv [Server name]	max. 128 characters	[blank]	Defines an SMTP server via the IP address or the host name. <i>A host name can only be used if a DNS server was configured beforehand.</i>
smtp_port [Server port]	1–65535 [1–5 characters; 0–9]	25	Defines the port number used by the TPG to send emails to the SMTP server.
smtp_ssl [TLS]	on/off	off	Enables/disables TLS. <i>The security protocol TLS (Transport Layer Security) is used to encrypt the transmission between the TPG and the SMTP server.</i>
smtp_sender [Sender name]	max. 128 characters	[blank]	Defines the email address used by the TPG to send emails. Note: Very often the name of the sender and the user name are identical.
smtp_auth [Login]	on/off	off	Enables/disables the SMTP authentication for the login.
smtp_usr [User name]	max. 128 characters	[blank]	Defines the name used by the TPG to log on to the SMTP server.
smtp_pwd [Password]	max. 128 characters	[blank]	Defines the password used by the TPG to log on to the SMTP server.
smtp_sign [Security (S/MIME)]	on/off	off	Enables/disables the encryption and signing of emails via S/MIME.
smtp_encrypt [Full encryption] [Signing of emails]	on/off	off	Defines the signing and encryption of emails. <i>off = sign</i> <i>on = encrypt</i>
smtp_attpkey [Attach public key]	on/off	on	Enables/disables the attachment of a public key to an email.

Tabelle 18: Parameter List - Bonjour

Parameters	Value	Default	Description
bonjour [Bonjour]	on/off	on	Enables/disables the Bonjour service.
bonjour_name [Bonjour name]	max. 64 characters [a–z, A–Z, 0–9]	[Default Name]	Defines the Bonjour name of the TPG.

Tabelle 19: Parameter List - Date/Time

Parameters	Value	Default	Description
ntp [Date/Time]	on/off	on	Enables/disables the use of a time server (SNTP).
ntp_server [Time server]	max. 255 characters [, a–z, A–Z, 0–9]	pool.ntp.org	Defines a time server via the IP address or the host name. <i>A host name can only be used if a DNS server was configured beforehand.</i>
ntp_tzone [Time zone]	UTC, GMT, EST, EDT, CST, CDT, MST, MDT, PST, PDT, etc.	CET/CEST (EU)	The time zone is used to equalize the difference between the time received over the time server and the local time.

Tabelle 20: Parameter List - Description

Parameters	Value	Default	Description
sys_name [Host name]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the host name of the TPG.
sys_descr [Description]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Freely definable description
sys_contact [Contact person]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Freely definable description (of the contact person)

Tabelle 21: Parameter List - ThinPrint®

Parameters	Value	Default	Description
tpgPort [ThinPrint® port]	1–65535 [1–5 characters; 0–9]	4000	Defines the TCP port used by the TPG for communicating with the ThinPrint server.
tpgBdwidth [Bandwidth]	on/off	off	Enables/disables the bandwidth functionality of the ThinPrint® port (TPG side).
tpgBdwidthVal [Bandwidth value]	1600–1000000 [4–7 characters; 0–9]	256000	Defines the bandwidth (in bit/second) used to decrease the bandwidth of the ThinPrint® port (TPG side).
tpgPrtoToVal [Printer connection timeout]	0–86400 [1–5 characters; 0–9; 0 = off]	60	(experts only) Defines the period of time (in seconds) after which a connection attempt to a printer is aborted. <i>A connection attempt should be aborted if a printer is physically not available. This frees the ThinPrint® port for subsequent print jobs.</i>
tpgJobSndTout [Job sending timeout]	0–86400 [1–5 characters; 0–9; 0 = off]	180	(experts only) Defines the period of time (in seconds) after which a current print job is aborted if it cannot be printed due to a printer error, e.g. no paper.

Tabelle 22: Parameter List - ThinPrint Connection Service

Parameters	Value	Default	Description
conService [Connection Service]	on/off	off	Enables/disables the ThinPrint Connection Service.
conServer [Server name]	max. 255 characters [., a–z, A–Z, 0–9]	[blank]	Defines the Connection Service server via the IP address or the host name. <i>A host name can only be used if a DNS server was configured beforehand.</i>

Parameters	Value	Default	Description
tpgClientID [Client ID]	0–99999 [1–5 characters; 0–9]	0	Defines the client ID as stored in the database of the Connection Service.
tpgAuthKey [Authentication key]	0–99999 [1–5 characters; 0–9]	0	Defines the authentication key as stored in the database of the Connection Service.
conPort [Port]	1–65535 [1–5 characters; 0–9]	4001	Defines the TCP port used by the TPG for communicating with the Connection Service.
tpgKeepalive [Keep alive]	1–60000 [1–5 characters; 0–9]	60	Defines the time interval (in seconds) after which the connection to the Connection Service is refreshed. Note: The value has to be equal to or lower than the 'KeepAliveTO' value set on the Connection Service server.
tpgRetry [Connection retry]	1–60000 [1–5 characters; 0–9]	120	Defines the time interval (in seconds) after which a connection retry is executed if the Connection Service cannot be reached.

Tabelle 23: Parameter List - ThinPrint® printer

Parameters	Value	Default	Description
prtName_1 ~ prtName_6 [Printer]	max. 32 characters [a-z, A-Z, 0-9, _, -]	[blank]	Defines the printer name for the ThinPrint AutoConnect feature.
prtClass_1 ~ prtClass_6 [Class]	max. 7 characters [a-z, A-Z, 0-9]	[blank]	Defines the printer class name for the ThinPrint AutoConnect feature.
prtDriver_1 ~ prtDriver_6 [Driver]	max. 64 characters [a-z, A-Z, 0-9, _, -]	[blank]	Defines the printer driver for the ThinPrint AutoConnect feature.
remotelp_1 ~ remotelp_6 [Printer address]	max. 64 characters [., a-z, A-Z, 0-9]	[blank]	Defines the IP address or host name of the printer. <i>A host name can only be used if DNS was configured beforehand.</i>
remoteMode_1 ~ remoteMode_6 [Printing protocol]	raw ipp lpd	raw	Specifies the transfer method between the TPG and the printer. <i>raw = RAW/Socket connection</i> <i>ipp = IPP connection</i> <i>lpd = LPD connection</i>
remotePort_1 ~ remotePort_6 [Port]	1-65535 [1-5 characters; 0-9]	9100	Defines the port number for RAW/socket printing.
remoteUrl_1 ~ remoteUrl_6 [URL]	max. 64 characters	ipp/lp1	Specifies the second part of the printer URL for IPP printing. <i>The implementation of the printer URL is depends on the manufacturer. Consult your printer manual for more information.</i>
remoteIPPs_1 ~ remoteIPPs_6 [SSL]	on/off	off	Enables/disables the SSL/TLS encryption for IPP printing.

Parameters	Value	Default	Description
remoteQ_1 ~ remoteQ_6 [Queue]	max. 64 characters [a–z, A–Z, 0–9]	lp1	Defines the queue name for LPD printing.
lpdModeRFC_1 ~ lpdModeRFC_6 [RFC]	on/off	on	Enables/disables the RFC1179 conformity for LPD printing.
monitorPing [Monitoring via ping]	on/off	on	Enables/disables monitoring via 'ping', i.e. ICMP. <i>The 'ping' query allows you to view the printer availability.</i>
monitorSNMP [SNMP]	on/off	on	Enables/disables monitoring via SNMP. <i>The SNMP query shows printer messages.</i>
monitorPoll [Monitoring interval]	10–86400 [2–5 characters; 0–9]	30	Defines the interval of a 'ping' or 'SNMP' query in seconds.

Tabelle 24: Parameter List - Notification

Parameters	Value	Default	Description
mailto_1 mailto_2 [Mail recipient]	valid email address [max. 64 characters]	[blank]	Defines the email address of the recipient for notifications.
noti_pup_1 noti_pup_2 [Restart]	on/off	off	Enables/disables the sending of emails when the TPG is restarted.
noti_stat_1 noti_stat_2 [Status]	on/off	off	Enables/disables the periodical sending of a status email to recipient 1 or 2.
notistat_d [Interval]	al = daily su = Sunday mo = Monday tu = Tuesday we = Wednesday th = Thursday fr = Friday sa = Saturday	al	Specifies the interval at which a status email is sent.

Parameters	Value	Default	Description
notistat_h [hh]	1 = 1. Hour 2 = 2. Hour 3 = 3. Hour etc.	0	Specifies the time at which a status email is sent.
notistat_tm [mm]	0 = 00 min 1 = 10 min 2 = 20 min 3 = 30 min 4 = 40 min 5 = 50 min	0	Specifies the time at which a status email is sent.
noti_usb_1 noti_usb_2 [USB]	on/off	off	Enables/disables the sending of emails after a USB flash drive was connected to or removed from the TPG.
noti_err_1 noti_err_2 [Problems]	on/off	off	Enables/disables the sending of emails if a problem occurs at the TPG.
trapto_1 trapto_2 [Trap target]	valid IP address	0.0.0.0	Defines the SNMP trap address of the recipient for notifications.
trapcommu_1 trapcommu_2 [Trap community]	max. 64 characters [a-z, A-Z, 0-9]	public	Defines the SNMP trap community of the recipient.
trappup [Restart]	on/off	off	Enables/disables the sending of SNMP traps when the TPG is restarted.
trapusb [USB]	on/off	off	Enables/disables the sending of SNMP traps after a USB device was connected to or removed from the TPG.
traperr [Problems]	on/off	off	Enables/disables the sending of SNMP traps if a problem occurs at the TPG.

Tabelle 25: Parameter List - SSL/TLS connections

Parameter	Value	Default	Description
sslmethod [Encryption protocol]	any sslv3 tls10 tls11 tls12	tls10	<p>Defines the encryption protocol to be used for SSL/TLS connections.</p> <p><i>sslv3 = SSL 3.0</i> <i>tls10 = TLS 1.0</i> <i>tls11 = TLS 1.1</i> <i>tls12 = TLS 1.2</i></p> <p>Do <u>not</u> use the encryption protocol 'SSL' if only HTTPS is defined as the permitted connection type for the web access to the TPG Control Center.</p>
security [Encryption level]	1-4 [1 character]	2	<p>Defines the encryption level to be used for SSL/TLS connections.</p> <p><i>1 = Low</i> <i>2 = Medium</i> <i>3 = High</i> <i>4 = Compatible</i></p> <p>Do <u>not</u> use the encryption level 'Low' if only HTTPS is defined as the permitted connection type for the web access to the TPG Control Center.</p>

Tabelle 26: Parameter List – TPG Control Center security

Parameters	Value	Default	Description
http_allowed [Connection]	on/off	on	Defines the permitted type of connection (HTTP/HTTPS) to the TPG Control Center. <i>If HTTPS is exclusively chosen as the connection type [http_allowed = off], the administrative access to the TPG Control Center is protected via SSL/TLS.</i>
sessKeys [Restrict Control Center access]	on/off	off	Enables/disables the TPG Control Center access restriction. If access is restricted, a login screen is displayed when opening the TPG Control Center. <u>Note:</u> If access is restricted, user accounts must be defined.
sessKeyUList [Login screen displays]	on/off	on	Defines the type of login screen. on = list of users off = name and password request
sessKeyTimer [Session timeout]	on/off	on	Enables/disables the session timeout.
sessKeyTimeout [Session timeout]	120–3600 [3–4 characters; 0–9]	600	Time in seconds after which the timeout is to be effective.
admin_name [Administrator - User name]	max. 64 characters [a–z, A–Z, 0–9]	admin	Defines the user name for the administrator user account. <u>Note:</u> Also is the user name of the SNMP admin account.
admin_pwd [Administrator - Password]	8-64 characters [a–z, A–Z, 0–9]	adminis- trator	Defines the password for the administrator user account. <u>Note:</u> Also is the password of the SNMP admin account.
any_name [Read-only user - User name]	max. 64 characters [a–z, A–Z, 0–9]	anony- mous	Defines the user name for the read-only user account. <u>Note:</u> Also is the user name of the SNMP user account.

Parameters	Value	Default	Description
any_pwd [Read-only user - Password]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the password for the read-only user account. Note: Also is the password of the SNMP user account.

Tabelle 27: Parameter List – TCP port access

Parameters	Value	Default	Description
protection [Port access control]	on/off	off	Enables/disables the locking of the selected ports.
protection_test [Test mode]	on/off	on	Enables/disables the test mode. <i>The test mode allows you to test the parameters set using the access control. If the test mode is activated, the access protection remains active until the TPG is rebooted.</i>
protection_level [Security level]	protec_tcp protec_all	protec_tcp	Specifies the port types to be locked. <i>protec_tcp = TCP ports protec_all = all ports (IP ports)</i>
ip_filter_on_1 ~ ip_filter_on_8 [IP address]	on/off	off	Enables/disables an exception from the port locking.
ip_filter_1 ~ ip_filter_8 [IP address]	valid IP address	[blank]	Defines elements that are excluded from port locking, using the IP address.
hw_filter_on_1 ~ hw_filter_on_8 [MAC address]	on/off	off	Enables/disables an exception from the port locking.
hw_filter_1 ~ hw_filter_8 [MAC address]	valid hardware address	00:00:00: 00:00:00	Defines elements that are excluded from port locking, using the hardware address.

Tabelle 28: Parameter List - Authentication

Parameters	Value	Default	Description
auth_typ [Authentication method]	--- [None] MD5 TLS TTLS PEAP FAST	---	Defines the authentication method that is used to identify devices or users in the network.
auth_name [User name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the name of the TPG as saved in the authentication server (RADIUS).
auth_pwd [Password]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the password of the TPG as saved in the authentication server (RADIUS).
auth_extern [PEAP/EAP-FAST Options]	--- = none PLABEL0 = PEAPLABEL0 PLABEL1 = PEAPLABEL1 PVER0 = PEAPVER0 PVER1 = PEAPVER1 FPROV1 = FASTPROV1	---	Defines the kind of external authentication for the EAP authentication methods TTLS, PEAP, and FAST.
auth_intern [Inner Authentication]	--- = none PAP = PAP CHAP = CHAP MSCHAP2 = MS-CHAPv2 EMD5 = EAP-MD5 ETLS = EAP-TLS	---	Defines the kind of inner authentication for the EAP authentication methods TTLS, PEAP, and FAST.
auth_ano_name [Anonymous name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the anonymous name for the unencrypted part of the EAP authentication methods TTLS, PEAP, and FAST.
auth_wpa_addon [WPA add-on]	max. 255 characters [a-z, A-Z, 0-9]	[blank]	Specifies an optional WPA expansion.

Tabelle 29: Parameter List - USB device

Parameters	Value	Default	Description
tpgBuffer [Print job buffering]	on/off	off	Enables/disables the automatic buffering of print jobs if a printer cannot be reached.
autoSync [Parameter backup]	on/off	on	Enables/disables the automatic parameter backup to a connected USB flash drive.

Tabelle 30: Parameter List – Status page

Parameters	Value	Default	Description
spage [Status page]	on/off	on	Enables/disables the printing of status and service pages on the relevant printer. The print job can be triggered by pressing the status/reset button on the device or by clicking the corresponding button in the TPG Control Center.
spPrinter [Status page printer]	TPG-25 = 1–2 TPG-65 = 1–6 TPG-125 = 1–12	1	Defines the printer on which status pages and services pages are printed, via the printer ID.
spMode [Status page mode]	ASCII PostScript DATAMAX Citizen-Z	ASCII	Defines the data format in which the status page is printed.

7.3 Troubleshooting

This chapter describes some problems and their solutions.

Problem

- 'The TPG indicates the BIOS mode' ⇨ 105
- 'A connection to the TPG Control Center cannot be established' ⇨ 106
- 'The password is no longer available' ⇨ 107
- 'The print job buffering does not work' ⇨ 108
- 'The automatic parameter backup does not work' ⇨ 108

Possible Cause

The TPG indicates the BIOS mode

The TPG switches to the BIOS mode if the firmware functions well but the software is faulty. This may happen in the case of an incorrect software update, for example. The TPG indicates the BIOS mode when the activity LED is blinking green.



The TPG is not operational in the BIOS mode.

If the TPG is in the BIOS mode, the filter 'BIOS mode' will be created automatically in the device list of the InterCon-NetTool. The TPG is displayed within this filter.

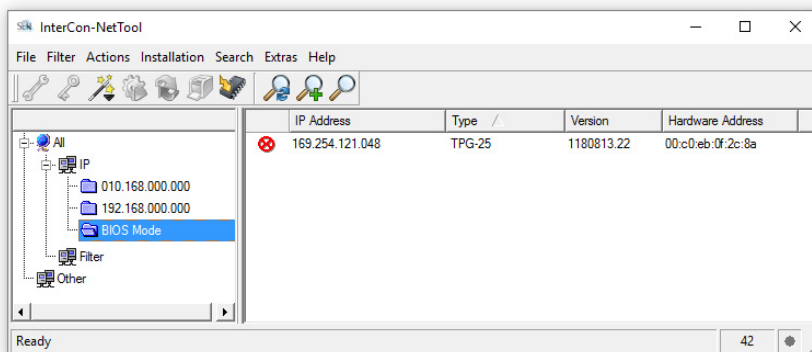


Abb. 7: InterCon-NetTool - TPG in the BIOS Mode

The software must be reloaded to the TPG so that the TPG can switch from the BIOS mode to the normal mode.



Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Highlight the TPG in the device list.
(You will find the TPG under the filter 'BIOS mode'.)*
 3. *Select **Installation – IP Wizard** from the menu bar.
The IP Wizard is started.*
 4. *Follow the instructions of the wizard in order to assign an IP address to the TPG.
The IP address is saved.*
 5. *Carry out a software update on the TPG; see: ⇒ 77.*
- ✎ The software will be saved in the TPG. The TPG switches to the normal mode.

A connection to the TPG Control Center cannot be established

Eliminate possible error sources. First of all, check:

- the cabling connections,
- the IP address of the TPG (⇒ 12) as well as
- the proxy settings of your browser.

If you still cannot establish any connection, the following safety mechanisms might be the cause:

- The access is protected via SSL/TLS (HTTPS) ⇒ 51.
- The TCP port access control is enabled ⇒ 53.
- The cipher suites of the encryption level are not supported by the browser ⇒ 49.

The password is no longer available

Access to the TPG Control Center can be restricted. If the password and/or user name is no longer available, you can reset the parameter values of the TPG to their default settings to get access to the TPG Control Center ⇒ 77. Previous settings will be deleted.

The printer does not print when print jobs are sent to the TPG

Check first if the printer is correctly embedded on the TPG; see: ⇒ 40.

If printing via the TPG is still not possible, the following issues may be the cause:

- ❑ The printer does not support the selected printing protocol. Choose a supported printing protocol ⇒ 40. Please refer to the documentation of your printer.
- ❑ The printer object on the ThinPrint server, which sends the print jobs to the TPG, must be configured to use a native printer driver. If the 'ThinPrint Output Gateway' is configured as printer driver, the print jobs are sent to the TPG in a format ('EMF') not supported by the TPG.
- ❑ You can use timeouts to control how errors are handled before and during a print job ⇒ 42. Check if the timeouts are too short and thus prematurely terminate the connection to the printer or the sending of the print job.
- ❑ In ThinPrint environments, the ThinPrint port (default: 4000) is used for printing ⇒ 39. This port must not be blocked by a security software (e.g. firewall).
- ❑ In ThinPrint environments, the Connection Service can be used ⇒ 46. The port used by this service (default: 4001) must not be blocked by a security software (e.g. firewall).
- ❑ The print data is sent to the TPG in encrypted form ⇒ 47. Check if
 - the required certificates are installed.
 - the required certificates are valid.

The print job buffering does not work

Print jobs are not automatically buffered in the USB flash drive.

Check if

- a USB flash drive is connected to the USB port of the USB and if it is mounted. This information is displayed in the TPG Control Center under 'MAINTENANCE' in the table 'USB device status'.
- if the print job buffering is configured ⇒ 72.
- if the connected USB flash drive has the wrong file system and must be formatted. Whether formatting is required, is displayed in the TPG Control Center under 'MAINTENANCE' in the table 'USB device status'. If necessary, format the USB flash drive ⇒ 72.
- if there is sufficient free space available on the USB flash drive. The free space available on the USB flash drive, is displayed in the TPG Control Center under 'MAINTENANCE' in the table 'USB device status'.

The automatic parameter backup does not work

The parameters file is not saved automatically on the USB flash drive or is not updated after a parameter change.

Check if

- a USB flash drive is connected to the USB port of the USB and if it is mounted. This information is displayed in the TPG Control Center under 'MAINTENANCE' in the table 'USB device status'.
- the automatic parameter backup is configured ⇒ 72.
- if the connected USB flash drive has the wrong file system and must be formatted. Whether formatting is required, is displayed in the TPG Control Center under 'MAINTENANCE' in the table 'USB device status'. If necessary, format the USB flash drive ⇒ 72.
- if there is sufficient free space available on the USB flash drive. The free space available on the USB flash drive, is displayed in the TPG Control Center under 'MAINTENANCE' in the table 'USB device status'.

7.4 List of Figures

TPG Control Center - START	17
InterCon-NetTool - Main Dialog	19
Administration via Email - Example 1	22
Administration via Email - Example 2	22
InterCon-NetTool - IP Wizard	25
TPG Control Center - Certificates	56
InterCon-NetTool - TPG in the BIOS Mode	105

7.5 Index

A

Address
 Ethernet address 86
 Hardware address 86
 IP address 86
 MAC address 86
 Administration 16
 Email 20
 Status/reset button 23
 TPG Control Center 16
 Administrator 52
 ARP/PING 15
 Authentication 63
 AutoConnect 6

B

Backup copy 71
 Bandwidth 39
 Bandwidth limit 39
 BIOS mode 105
 Bonjour 33
 BOOTP 13

C

CA certificate 55
 Certificate 55
 Create 57
 Delete 62
 Display 57
 Save 59
 Certificate request 59
 Cipher Suite 49
 Connection Service 6
 Configuring 46

D

Default certificate 55

Default name 85
 Default setting 75
 Descriptions 35
 Device number 85
 DHCP 13
 DNS (Domain Name Service) 27
 Documentation 7
 Domain name 27

E

EAP 63
 EAP-FAST 68
 EAP-MD5 64
 EAP-TLS 64
 EAP-TTLS 65
 Email 20
 Encrypted print data 47
 Encryption 47
 Cipher suite 49
 Level 49
 Protocol 49
 strength 49
 Encryption level 49
 Encryption protocol 49
 Encryption strength 49
 Ethernet address 86

F

Firmware 77

G

Gateway 85

H

Hardware address 86
 Host name 86
 Hotline 9
 HTTP/HTTPS 51

I

IEEE 802.1x 63
 Improper use 10
 Intended use 10
 InterCon-NetTool 18, 86
 Install 18
 IP Wizard 14
 Start 18
 Structure 19
 IP address 86
 Save 12
 IPP connection 40
 IPv4 23
 IPv6 25

J

Job history 81
 Delete 83
 Display 81
 Job sending timeout 43

L

Login 52
 Screen 52
 LPD protocol 40

M

MAC address 86

N

NAT 46
 Notification service 35, 36
 Email 36
 SNMP trap 37
 Notifications 35

P

Parameter backup 72
 Parameter list 88
 Parameters

 Default settings 75
 Display 71
 Load 72
 Load automatically 74
 Parameter list 88
 Save 71
 Save automatically 74
 Parameters file 71, 72
 password 52
 PEAP 67
 Ping 43
 PKCS#12 60
 POP3 30
 Print
 Service page 80
 Print job buffering 72
 Printer
 Connection status 43
 ID 40
 Integrate 40
 Messages 45
 Transfer method 40
 Printer connection timeout 42
 Printer messages 45
 Protocol
 BOOTP 13
 DHCP 13
 IPP 40
 IPv4 23
 IPv6 25
 LPD 40
 POP3 30
 SMTP 30
 SNMP 28
 SSL/TLS 49
 ZeroConf 13
 Purpose 5

R

RADIUS 63
 RAW/socket connection 40
 Read-only user 52
 Reset 75
 Restart 78

S

- S/MIME certificate 56
- Security 48
- Security level 53
- SEH Homepage 9
- Self-signed certificate 55
- Service page 79
 - Data format 79
 - Print 80
 - Printer 79
- Session timeout 52
- SMTP 30
- SNMP 45
 - SNMPv1 28
 - SNMPv3 29
 - User accounts 52
- SNMP trap 35
- SNTP server 34
- Software 77
- SSL/TLS connection 50
- SSL/TLS encryption 47
- Status email 35
- Status page 79
 - Data format 79
 - Print 79
 - Printer 79
- Status/reset button
 - Print service page 80
 - Reset parameters 76
- Subnet mask 87
- Support 9
- System requirements 6

T

- TCP port access control 53
- TCP/IP 23
- Test mode 53
- ThinPrint 5
- ThinPrint Client 5
- ThinPrint Connection Service 6
 - Configuring 46
- ThinPrint encryption 6, 47
- ThinPrint Engine 5

- ThinPrint port 39
- Time of the device 34
- Time server 34
- Time zone 34
- Timeout 42
 - Job sending 43
 - Printer connection 42
 - Session 52
- TPG Control Center 16, 87
 - Language 17
 - Start 16
 - Structure 17
- Transfer methods 40
- Types of connection 51, 62

U

- Update 77
- USB device
 - Format 73
 - Parameter backup 72
 - Print job buffering 72
- User accounts 52
- UTC 34

V

- Version number 77

Z

- ZeroConf 13