ThinPrint® Gateway

TPG60 / TPG120

User Manual

Manufactured by:
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: TPG60 / TPG120
Version: 1.4

Online Links to important Internet Resources:

Free Guarantee Extension:	http://www.seh-technology.com/guarantee
Support Contacts and Information:	http://www.seh-technology.com/support
Sales Contacts and Information:	http://www.seh-technology.com/sales

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

Table of Contents

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 TPG and how to operate the device properly.

What information do you need?

1.1 ThinPrint® Gateway

What is ThinPrint .print?

ThinPrint .print is a software-based technology with many print management functions for network printing, among them the possibility to compress print jobs and to control bandwidth usage. It significantly reduces print data traffic between the application server or print server and the local printer, relieving the network.

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

Purpose

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

The ThinPrint .print gateways TPG60 an TPG120 were especially developed for environments using ThinPrint .print technology for print job compression and bandwidth control.

Up to six network printers can be quickly and easily connected to the network via the TPG60 with integrated ThinPrint .print Client v7.x. The TPG120 connects up to twelve printers. Users send compressed print jobs to the ThinPrint .print gateways which in turn decompress these print jobs and send them to the respective printers.

Features

The TPG supports the following features:

- The feature **.print AutoConnect** allows you to automatically create the required printer objects for the relevant client on the server. **.print AutoConnect** will automatically connect all selected printers on the server with a ThinPrint® port; provided that templates exist.
- The **.print Connection Service** allows you to print to .print 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.
- **ThinPrint SSL encryption** safely protects print data during their transmission in the network. ThinPrint .print Clients or Gateways decrypt the data before printing.

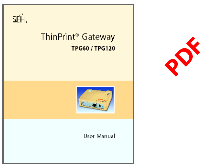
System Requirements

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 socket printing (printing via TCP/IP ports) or LPD-Printing. If you want to use the **.print Connection Service**, you need a license.

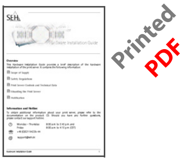
1.2 Documentation

Structure of the Documentation

The TPG documentation consists of the following documents:



User Manual
Detailed description of the TPG configuration and administration.



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

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

The explanation of technical terms used in this document is summarized in a glossary; see: ⇨🗎104. The glossary provides an overview of technical matters and background information that are necessary for a proper installation and configuration.

Symbols and Conventions

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

Table 1: Conventions within the documentation

Symbol / Convention	Description
⚠ Warning	A warning contains important information that must be heeded. Non-observance may lead to malfunctions.
ℹ Note	A notice contains information that should be heeded.
☞ Proceed as follows: *1. Mark ...*	The 'hand' symbol marks the beginning of instructions. Individual instructions are set in italics.
↳ Confirmation	The arrow confirms the consequence of an action.
☑ Requirements	Hooks mark requirements that must be met before you can begin the action.
□ 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

1.3 Support and Service

Support

If questions remain, please contact our hotline. SEH Computertechnik offers extensive support and user training sessions.

🕓	Monday through Thursday
	Friday
		from 8:00 a.m. to 5:45 p.m. and
		from 8:00 a.m. to 4:15 p.m. (CET)

☎	+49 (0)521 94226-44	
@	support@seh.de	

Current Services

The following services can be found on the SEH website at www.seh.de.

· Professional Print Servers for all Networks
· Free Tech Support
· 3 to 5 years Guarante

Newsticker

New! ** New! ** New!
PS105 Print Server of "PS" Series Now Available ... [more]
Channel News:
MIEL is the New SEH Distributor in France ... [more]
Trade Shows and Events:
Second SEH Trade Show Appearance in Japan ... [more]
English Spoken Here:
Support Forum at the SEH Website Really is Bilingual... [more]
Tech?Update!
Centronics / Parallel Interfaces, IEEE 1284

Information Links

Subscribe to the SEH Newsletter
Update information, tips, hints & more...
free of charge via Email

Any more Questions?
Simply send us an Email -
we will get back to you as soon as we can

Product of the Month: PS105

PS105
PS105 Print Server of Latest "PS" Series Now Available

- current update files
- current tools
- current documentation
- current product information
- product data sheet
- FAQ
- 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 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 Hardware 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 to operate the TPG.

☞ Proceed as follows:

1. *Connect the TPG to the network and the mains supply. 'Quick Installation Guide'.*
2. *Make sure that an IP address is stored in the TPG; see: 'Saving the IP Address in the TPG' ⇨🗎13.*
3. *Define the ThinPrint® port and other ThinPrint® settings; see: ⇨🗎52.*
4. *Define the printers to which the TPG will send print jobs; see: 'How to Integrate Printers' ⇨🗎54.*

↳ 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?

TPGs are shipped without an IP address. 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 from 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 ZeroConf.

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 TPG's assigned IP address can be determined and changed using the software tool 'InterCon-NetTool'.

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

- 'ZeroConf' ⇨🗎14
- 'BOOTP' ⇨🗎14
- 'DHCP' ⇨🗎14
- 'ARP/PING' ⇨🗎15
- 'InterCon-NetTool (IP Wizard)' ⇨🗎16

ZeroConf

If no IP address can be assigned via boot protocols, the TPG assigns itself an IP address via ZeroConf.

Requirements

☑ The 'ZeroConf' parameter has been activated; see: ⇨🗎42.

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 and sends a query to the network. If this 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.

If you wish to use an IP address different from the one assigned via ZeroConf, you can save a freely definable IP address in the TPG later on.

BOOTP

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

Requirements

☑ The 'BOOTP' parameter has been activated; see: ⇨🗎42.

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 activated; see: ⇨🗎42.

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.

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 activated; see: ⇨🗎42.

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.

InterCon-NetTool (IP Wizard)

The IP Wizard of the InterCon-NetTool helps you to configure the TCP/IP parameters, e.g. the IP address. You can easily enter the desired IP address and save it in the TPG using the IP Wizard.

Requirements

☑ The TPG is connected to the network and the mains voltage.

☑ The InterCon-NetTool is installed on the client; see: ⇨🗎19.

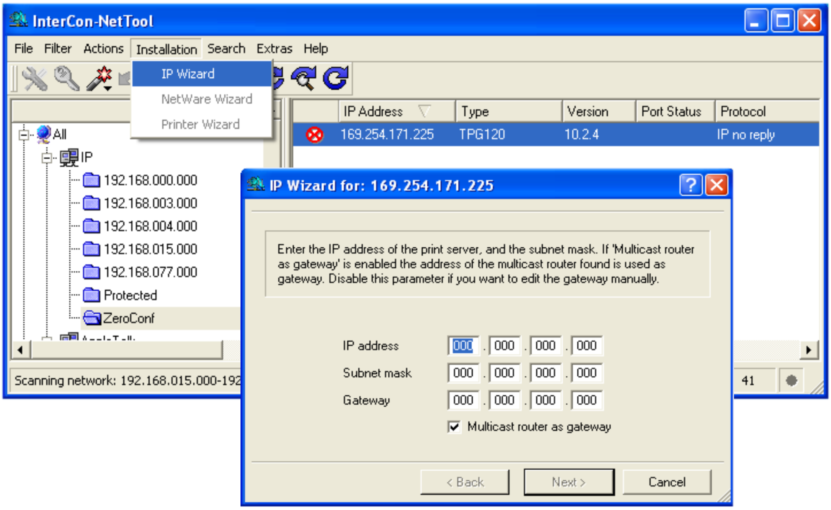
☑ By means of the InterCon-NetTool you can scan the network via Multicast.

☑ The router in the network forwards multicast requests.

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark 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 Wizard.*

↳ The settings are saved.



IP Address	Type	Version	Port Status	Protocol
169.254.171.225	TPG120	10.2.4		IP no reply

Scanning network: 192.168.015.000-192

Enter the IP address of the print server, and the subnet mask. If 'Multicast router as gateway' is enabled the address of the multicast router found is used as gateway. Disable this parameter if you want to edit the gateway manually.

IP address 000 . 000 . 000 . 000
Subnet mask 000 . 000 . 000 . 000
Gateway 000 . 000 . 000 . 000
☑ Multicast router as gateway

Fig. 1: InterCon-NetTool - IP Wizard

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 Homepage' ⇨🗎17
- 'Administration via the InterCon-NetTool' ⇨🗎19
- 'Administration via an FTP/FTPS Connection' ⇨🗎28
- 'Administration via the TPG Status Button' ⇨🗎29

2.1 Administration via the TPG Homepage

The TPG Homepage comprises all features for the administration of the TPG.

The TPG Homepage is stored in your TPG and can be started by means of an internet browser (Internet Explorer, Netscape, Firefox, Safari).

Requirements

☑ The TPG is connected to the network and the mains voltage.

☑ The TPG has a valid IP address.

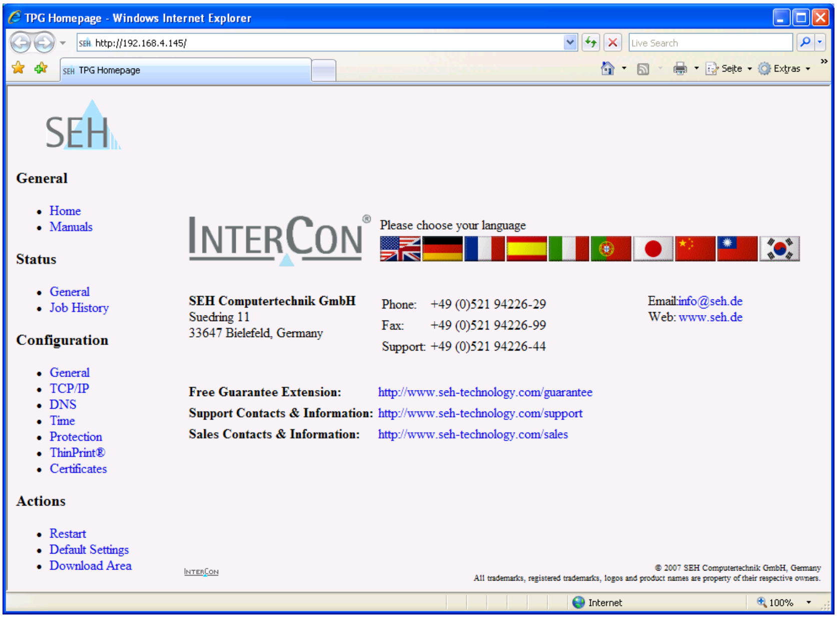
Proceed as follows:

Starting the TPG Homepage

1. *Open your browser.*
2. *Enter the IP address of the TPG as the URL.*

↳ The **TPG Homepage** appears.

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



General

- Home
- Manuals

Status

- General
- Job History

Configuration

- General
- TCP/IP
- DNS
- Time
- Protection
- ThinPrint®
- Certificates

Actions

- Restart
- Default Settings
- Download Area

Please choose your language

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: www.seh.de

Free Guarantee Extension:	http://www.seh-technology.com/guarantee
Support Contacts & Information:	http://www.seh-technology.com/support
Sales Contacts & Information:	http://www.seh-technology.com/sales

© 2007 SEH Computertechnik GmbH, Germany
All trademarks, registered trademarks, logos and product names are property of their respective owners.

Fig. 2: TPG Homepage - Home

Structure of the TPG Homepage

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

You can set the language of the TPG Homepage via **General – Home.** Simply select the relevant flag. You will also see contact information of the manufacturer.

Clicking the **General - Manuals** link brings you to the SEH web site. Here, you can download the latest manuals as *.pdf files.

All other menu items are intended for the configuration of the TPG and are described in this manual.

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 (print server, TPG, ISD, etc.). Depending on the network device you can configure various features via the InterCon-NetTool.

The InterCon-NetTool has been designed for use in Windows, Mac OS X, and Linux networks. The software is installed on all clients that are meant to access a network device in the network.

Basic Functions

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 and Program Start

In order to use the InterCon-NetTool, the program must be installed on a computer with Windows, Linux, or Mac OS X operating system. Different installation files are available, depending on the operating system. You will find the InterCon-NetTool installation files on the Product CD or on the Internet at www.seh.de.

If you use the InterCon-NetTool in Mac OS X or Linux networks, some functions will notbe available.

Windows

The installation file is available as '*.exe' for Windows systems.

Proceed as follows:

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

↳ The InterCon-NetTool is installed on the system.

To start the program, double-click the InterCon-NetTool icon . The icon is found on the desktop or the Windows start menu.

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. (Only for multi-user operating systems)

MAC OS X

The installation file is available as '*.dmg' for MAC systems.

Proceed as follows:

1. *Open the InterCon-NetTool installation file.*
   The content of the file will appear on the screen.
2. *Start the .'*.pkg' file.*
3. *Follow the installation routine.*

↳ The InterCon-NetTool is installed on the system.

To start the program, double-click the 'intercon-nettool.app' file.

The program settings are saved in the 'InterCon-NetTool.ini' file. This file can be found in the directory '/Users/<NAME>/Library/Preferences/InterCon-NetTool'.

Linux

Linux commonly offers software programs as packages. The InterCon-NetTool software packet for Linux is made available as '*.rpm' file. The '*.rpm' file can be unpacked and installed using the RPM Package Manager. The RPM Package Manager is a system that is used for package management. It can be used in many Linux and UNIX distributions.

If no suitable Package Manager is available, you can obtain '*.tgz' or '*.deb' installation files upon request from SEH Computertechnik GmbH.

The installation of the files depends on the distribution. '*.tgz' files can be extracted directly without the Package Manager in the root directory. '*.deb' files can be extracted using the Debian Package Manager.

Installation of the '*.rpm' Software Packet

Proceed as follows:

1. *Log on to your system as 'root'.*
2. *Enter the following command via the console:*
   Syntax:
   ```
   root# rpm -i <complete packet name>
   ```
   Example:
   ```
   root# rpm -i InterCon-NetTool-1_8-28.i386.rpm
   ```

↳ The InterCon-NetTool is installed on the system.

All packages contain the following directory structure. The files will be installed in the specified directories on the system.

```
./
./usr/
./usr/local/
./usr/local/bin/
./usr/local/bin/nettool
./usr/local/lib/
./usr/local/lib/nettool/
./usr/local/lib/nettool/tcpmon.ini
./usr/local/lib/nettool/lang_cn.qm
```

```
./usr/local/lib/nettool/lang_de.qm
./usr/local/lib/nettool/lang_es.qm
./usr/local/lib/nettool/lang_fr.qm
./usr/local/lib/nettool/lang_it.qm
./usr/local/lib/nettool/lang_jp.qm
./usr/local/lib/nettool/lang_kr.qm
./usr/local/lib/nettool/lang_pt.qm
./usr/local/lib/nettool/lang_zh.qm
./usr/local/lib/nettool/InterCon-NetTool.png
./usr/local/lib/nettool/license.txt
./usr/local/lib/nettool/lang_wt_de.qm
./usr/local/lib/nettool/lang_wt_es.qm
./usr/local/lib/nettool/lang_wt_fr.qm
./usr/local/lib/nettool/lang_wt_it.qm
./usr/local/lib/nettool/lang_wt_pt.qm
```

Before you start the InterCon-NetTool make sure that the '*.qm' language files, the license file 'license.txt' and the 'tcpmon.ini' file are in the '/usr/local/lib/nettool' directory.

☞ Proceed as follows:

1. *Enter the following command via the console:*
   Syntax:
   `user$ /<complete path name and program name>`
   Example:
   `user$ /usr/local/bin/nettool`

↳ The InterCon-NetTool is started.

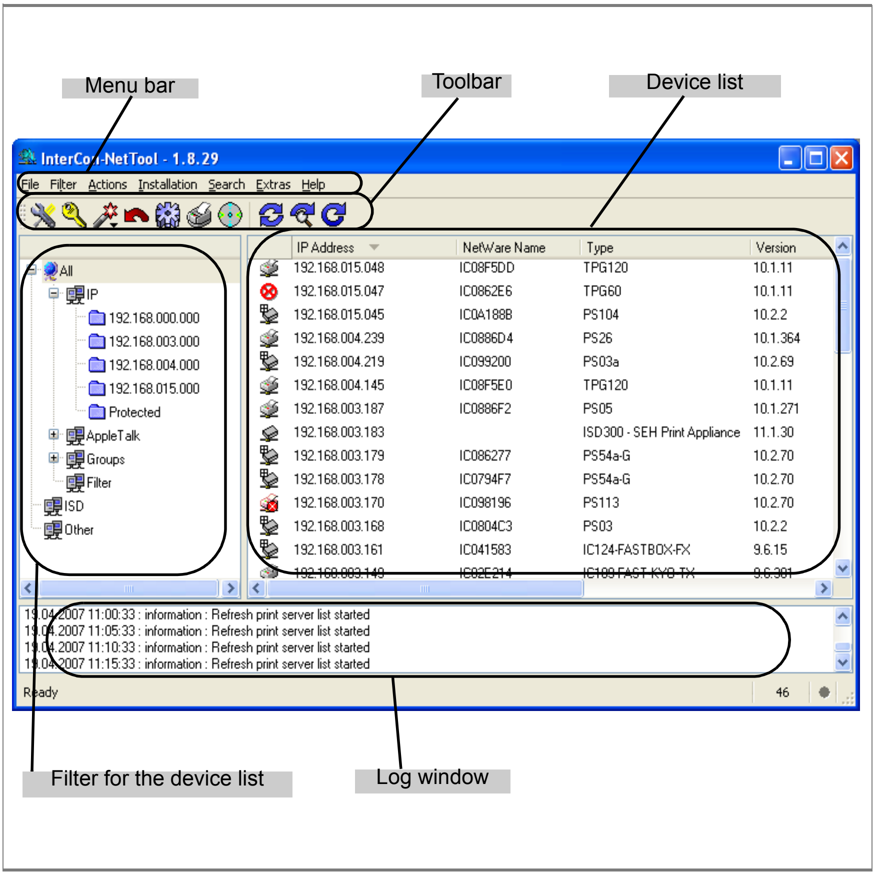
If the path '/usr/local/bin' is part of the environmental variable PATH, the InterCon-NetTool can be started by entering the program name 'nettool'.

When the InterCon-NetTool is started for the first time, a licensing agreement will appear. Accept the licensing agreement if you wish to use the program.

The settings of the InterCon-NetTool are saved in the user's home directory in the 'nettool' file.

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.



IP Address	NetWare Name	Type	Version
192.168.015.048	IC08F5DD	TPG120	10.1.11
192.168.015.047	IC0862E6	TPG60	10.1.11
192.168.015.045	IC0A188B	PS104	10.2.2
192.168.004.239	IC0886D4	PS26	10.1.364
192.168.004.219	IC099200	PS03a	10.2.69
192.168.004.145	IC08F5E0	TPG120	10.1.11
192.168.003.187	IC0886F2	PS05	10.1.271
192.168.003.183		ISD300 - SEH Print Appliance	11.1.30
192.168.003.179	IC086277	PS54a-G	10.2.70
192.168.003.178	IC0794F7	PS54a-G	10.2.70
192.168.003.170	IC098196	PS113	10.2.70
192.168.003.168	IC0804C3	PS03	10.2.2
192.168.003.161	IC041583	IC124-FASTBOX-FX	9.6.15
192.168.003.149	IC02E214	IC109-FAST-KYO-TX	9.6.301

```
19.04.2007 11:00:33 : information : Refresh print server list started
19.04.2007 11:05:33 : information : Refresh print server list started
19.04.2007 11:10:33 : information : Refresh print server list started
19.04.2007 11:15:33 : information : Refresh print server list started
```

Fig. 3: InterCon-NetTool - Main Dialog

The functions of the program elements will be described in the following. 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.

Toolbar

A toolbar with various commands is available in the InterCon-NetTool. The toolbar can either be shown or hidden. Select **Extras – Show Toolbar** from the menu bar.

Table 2: Description of the Toolbar Icons

Icon	Name	Description
	Properties	This opens the 'Properties' dialog.*
	Change password	This opens the 'Change password' dialog.*
	Installation	This starts a Wizard. A wizard helps you to configure certain parameters.
	Restart	This opens the 'Restart' dialog.*
	Default settings	This opens the 'Load default settings' dialog.*
	Print status page	This opens the 'Print status page' dialog.*
	Firmware Update	This opens the 'Firmware Update' dialog.*
	Refresh	Refreshes the device list.
	Find New	Adds newly connected network devices to the device list.
	Rebuild	Creates a new device list.

***The button is active if a device was marked in the list.**

Device List

All connected devices are shown in a list in the right-hand section of the main dialog of the InterCon-NetTool. This section is referred to as the device list.

Icons indicate the status or the kind of network device. Devices that are not available in the network, appear dimmed.

The device list is divided into columns that contain information about the device, the version, etc. You can adapt the information according to your needs. Select **Extras – Columns** from the menu bar.

You can select various filters in the left-hand section of the main dialog. Filters determine which network devices are shown in the device list. The filters can be created and configured via the **Filter** menu.

You can modify the status of the device list by

- adding network devices
- creating a new list or
- refreshing the list

Select the relevant command in the **Search** menu.

By activating an automatic refresh, the device list will be refreshed automatically in a fixed time interval. Select **Extras – Settings** from the menu bar (category: Auto Refresh).

You can save the device list as a file. The file ending is '*.lst'. This allows you to preserve a certain status and to restore it promptly. Select **File – Save as** or **Open** from the menu bar.

Search Parameters for the Network Scan

The InterCon-NetTool searches the network for existing devices and displays them in the device list. The following search options can be selected for the network scan:

- Searching via the IPX protocol (Novell NetWare)
- Searching via multicast requests (TCP/IP)
- Searching within defined IP ranges (TCP/IP)

In IPX based networks, the devices should be searched for via IPX. SAP search has to be enabled for Novell NetWare 4.x and later (NDS). Bindery search has to be enabled for Novell NetWare 3.x networks.

The default setting is multicast search in local networks. Searching via multicast requests beyond subnetworks is only possible if the routers in the network can handle multicast requests. In networks without multicast support you can search for network devices within defined IP ranges.

To define the search parameters, select **Extras – Settings** from the menu bar (category: Search Options).

Logging Functions

Logging means that actions carried out by the user or the InterCon-NetTool will be registered automatically and saved in a log file.

The logging functions can either be shown or hidden. Select **Extras – Settings** from the menu bar (category: Logging Options).

The contents of the log file can be displayed in a log window. To hide or show the log window, select **Extras – Show Log File** from the menu bar. If logging is disabled, the log window will not be displayed.

You can define the log file name, the log directory, and the maximum size of the log file. Select **Extras – Settings** from the menu bar (category: Logging Options).

Configuring TPG Parameters

The InterCon-NetTool offers three methods to configure the parameters of SEH network devices.

Configuration via the 'Properties' Dialog

Many SEH network devices offer the 'Properties' dialog where you can display and edit the individual configuration parameters of the device. Double-click the TPG in the device list to start the dialog.

Configuration via Wizards

Wizards facilitate the installation and configuration of network devices. Wizards are subprograms aimed at querying required parameter values.

The IP wizard is available for the TPG. The IP Wizard helps you to configure the TCP/IP parameters, e.g. the IP address. To start the Wizard, select **Installation – IP Wizard** from the menu bar.

Configuration via the ‘Actions’ Menu

Depending on the network device, you can use the Actions menu for individual operations (such as an Update). Select the relevant command from the **Actions** menu.

2.3 Administration via an FTP/FTPS Connection

FTP

The File Transfer Protocol (FTP) allows the exchange of data between a server and an FTP client in TCP/IP networks.

FTP over SSL

The TPG also supports FTPS (FTP over SSL) for a safe data interchange between the server and the client. FTPS is an encrypted procedure for file transfers. The encryption of the control channel and the data channel is done via the SSL or TLS authentication.

We recommend using SSL. This way, no unencrypted user names, passwords, and data can be read by unauthorized persons. In order to use FTPS, you must install an FTP client on your computer that supports FTPS.

The following functionalities are supported:

- 'Configuring Parameters via an FTP Connection' ⇨🗎29
- 'Printing the Status Page via an FTP Connection' ⇨🗎39
- 'Printing the Service Page via an FTP Connection' ⇨🗎40
- 'Resetting Parameters via an FTP Connection' ⇨🗎94
- 'Perform updates' ⇨🗎96

Requirements

The 'FTP' parameter has been activated.

You can disable the protocols to protect the ports against attacks; see: ⇨🗎63.

Configuring Parameters via an FTP Connection

You can configure all TPG parameters via FTP. To this purpose, you must download the 'parameters' file to your local computer via FTP and then edit it. A detailed description of the TPG parameters can be found in the 'Parameter List' ⇨🗎107.

Proceed as follows:

1. *Switch to the directory in which you wish to save the file.*
2. *Open an FTP connection to the TPG:*
   Syntax: `ftp <IP Address>`
   Example: `ftp 192.168.0.123`
3. *Enter an arbitrary user name.*
4. *Enter either the TPG password or press ENTER if no password has been assigned.*
5. *Transfer the 'parameters' file from the TPG to your local computer:*
   ```
   get parameters
   ```
6. *Edit the file using any text editor; see: 'Parameter List'* ⇨🗎*107.*
7. *Send the file back to the TPG:*
   ```
   put parameters
   ```
8. *Close the FTP connection:*
   ```
   quit
   ```

↳ The TPG will be configured using the new values.

2.4 Administration via the TPG Status Button

At the front panel of the TPG you will find the network connector, LEDs, the status button, and the power supply connector. These components are described in the 'Quick Installation Guide'.

The status button allows you to

- print a status page; see: ⇨🗎40
- print a service page; see: ⇨🗎40
- reset the TPG parameters to their default settings; see: ⇨🗎94

3 Status Information

The TPG offers you a multitude of information. This chapter describes how to receive, display, and interpret the information.

You can get information on the TPG, the embedded printers, the printer connections, and the print jobs (Job History).

What information do you need?

- 'How to Display TPG Status Information' ⇨🗎30
- 'How to get Printer Status Messages' ⇨🗎31
- 'How to Get Status Information on the Printer Connections' ⇨🗎33
- 'How to Display the Job History' ⇨🗎35
- 'How to Print a Status or Service Page' ⇨🗎37

3.1 How to Display TPG Status Information

You can display status information such as the name of the TPG, the hardware address, serial and version numbers etc.

What do you want to do?

□ 'Displaying Status Information via the TPG Homepage' ⇨🗎30

□ 'Displaying Status Information via the InterCon-NetTool' ⇨🗎31

Displaying Status Information via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Status – General***.*

↳ The status information is shown.

Displaying Status Information via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Status – General** *from the navigation bar.*

↳ The status information is shown.

3.2 How to get Printer Status 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.

What do you want to do?

- □ 'Configuring an SNMP Query via the TPG Homepage' ⇨🗎31
- □ 'Configuring an SNMP Query via the InterCon-NetTool' ⇨🗎32
- □ 'Displaying Printer Messages via the TPG Homepage' ⇨🗎32
- □ 'Displaying Printer Messages via the InterCon-NetTool' ⇨🗎32

Configuring an SNMP Query via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – ThinPrint®***.*
3. *Tick* **snmp***.*
4. *Enter the interval (in seconds) into the* **Monitoring interval** *box.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

Configuring an SNMP Query via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – ThinPrint®** *from the navigation bar.*
4. *Tick* **snmp**.
5. *Enter the interval (in seconds) into the* **Monitoring interval** *box.*
6. *Click* **OK** *to confirm.*

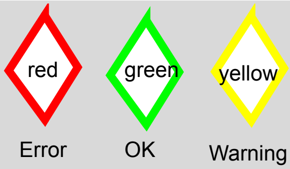
↳ The settings are saved.

Displaying Printer Messages via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – ThinPrint®**.

↳ The printer messages are displayed under **Status** and are assigned to the printer IDs.



Colored symbols indicate the type of message. Do not mistake these symbols for the symbols of the status page printer.

Displaying Printer Messages via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – ThinPrint®** *from the navigation bar.*

↳ The printer messages are displayed under **Status** and are assigned to the printer IDs.

3.3 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.

ℹ In order to get the connection status you must configure a 'ping' query.

What do you want to do?

- □ 'Configuring a 'ping' Query via the TPG Homepage' ⇨🗎33
- □ 'Configuring a 'ping' Query via the InterCon-NetTool' ⇨🗎34
- □ 'Displaying the Printer Connection Status via the TPG Homepage' ⇨🗎34
- □ 'Displaying the Printer Connection Status via the InterCon-NetTool' ⇨🗎34

Configuring a 'ping' Query via the TPG Homepage

☞ Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – ThinPrint®***.*
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.

Configuring a 'ping' Query via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – ThinPrint®** *from the navigation bar.*
4. *Tick* **Monitoring via ping***.*
5. *Enter the interval (in seconds) into the* **Monitoring interval** *box.*
6. *Click* **OK** *to confirm.*

↳ The settings are saved.

Displaying the Printer Connection Status via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – ThinPrint®***.*

↳ The printer connection status is displayed under **Status** and is assigned to the printer IDs.

Displaying the Printer Connection Status via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – ThinPrint®** *from the navigation bar.*

↳ The printer connection status is displayed under **Status** and is assigned to the printer IDs.

3.4 How to Display the Job History

You can get information about the print jobs that have been sent to the TPG. The print jobs are registered and shown in the Job History.

A maximum of 64 print jobs are displayed. The first-in, first-out method is applied from the 65th print job onwards. The saved print jobs will be deleted when the TPG is turned off or reset. The print jobs will not be deleted when the TPG is restarted.

What do you want to do?

- □ 'Displaying the Job History via the TPG Homepage' ⇨🗎35
- □ 'Displaying the Job History via the InterCon-NetTool' ⇨🗎35

Displaying the Job History via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Status – Job History***.*

↳ The Job History is displayed.

Displaying the Job History via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Status – Job History** *from the navigation bar.*

↳ The Job History is displayed.

The following information is shown in the Job History:

Information	Description
Status	Status of the print connection. The following statuses are possible: • 'Completed' means that the TPG has completely forwarded the print job to the printer. • 'Pending' means that the print job has been accepted by the TPG but that the data transfer has not yet started. • 'Processing' means that the print job has been transferred from the TPG to the printer. • 'Processing stopped' means that the data transfer to the printer has been stopped. This can occur if, for example, the printer ran out of paper. If the printer error is fixed, data transfer will be resumed. • 'Aborted' means that the print job has been aborted. This can occur if, for example, the TPG has been restarted while the print job was processed.
Protocol	Protocol used to transfer the print data
Name	Name of the print job
Sender	IP address of the sending host
Size	Size (in KB) of the print job. The minimal size that is displayed is 1 KB.
Printer ID	Identification number of the printer that has spooled the print job
Creation time	Time at which the print job has been sent to the TPG.
Duration	The time needed by the TPG for processing the print job. The minimal duration that is displayed is 1 second.

3.5 How to Print a Status or Service Page

You can print status pages or a service page.

Status page

The status page contains TPG basic information such as TPG model, MAC address, IP address, subnet mask, gateway etc.

Service page

The service page contains a list of the current TPG parameter values. The service page is available in English.

ℹ

Before a status page can be printed, you need to specify the printer and the data format of the status page (ASCII, PostScript, DATAMAX, or Citizen-Z). The default setting is the printer with the ID 1.

What do you want to do?

□ 'Specifying the Data Format and the Printer via the TPG Homepage' ⇨🗎38

□ 'Specifying the Data Format and the Printer via the InterCon-NetTool' ⇨🗎38

□ 'Printing the Status Page via the InterCon-NetTool' ⇨🗎38

□ 'Printing the Status Page via an FTP Connection' ⇨🗎39

□ 'Printing the Status Page via the TPG Status Button' ⇨🗎40

□ 'Printing the Service Page via the TPG Status Button' ⇨🗎40

□ 'Printing the Service Page via an FTP Connection' ⇨🗎40

Specifying the Data Format and the Printer via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – General***.*
3. *Select the desired data format from the* **Status page mode** *list.*
4. *Select the desired printer ID from the* **Status Page Printer** *list.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

Specifying the Data Format and the Printer via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – General** *from the navigation bar.*
4. *Select the desired data format from the* **Status page mode** *list.*
5. *Select* **Configuration – ThinPrint®** *from the navigation bar.*
6. *Tick* **Status Page Printer** *for the desired printer.*
7. *Click* **OK** *to confirm.*

↳ The settings are saved.

Printing the Status Page via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark the TPG in the device list.*
3. *Select* **Actions – Print Status Page** *from the menu bar.*
4. *Click* **Finish***.*

↳ The status page is printed.

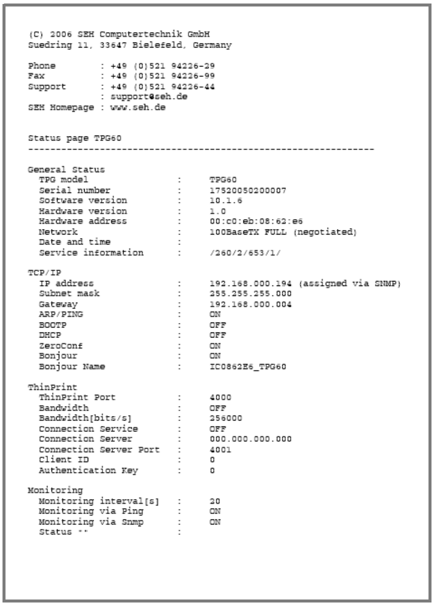
Printing the Status Page via an FTP Connection

Using an FTP connection, you can download a status page to your local computer and print it.

Proceed as follows:

1. *Switch to the directory in which you wish to save the file.*
2. *Open an FTP connection to the TPG:*
   Syntax: `ftp <IP Address>`
   Example: `ftp 192.168.0.123`
3. *Enter an arbitrary user name.*
4. *Enter either the TPG password or press ENTER if no password has been assigned.*
5. *Transfer the status page from the TPG to your local computer:*
   `get statuspage`
6. *Close the FTP connection:*
   `quit`
7. *Open and print the file using a text editor.*

↳ The status page will be printed.



```
(C) 2006 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
             : support@seh.de
SEH Homepage : www.seh.de


Status page TPG60
---------------------------------------------------------------

General Status
  TPG model                 :     TPG60
  Serial number             :     17520050200007
  Software version          :     10.1.6
  Hardware version          :     1.0
  Hardware address          :     00:c0:eb:08:62:e6
  Network                   :     100BaseTX FULL (negotiated)
  Date and time             :
  Service information       :     /260/2/653/1/

TCP/IP
  IP address                :     192.168.000.194 (assigned via SNMP)
  Subnet mask               :     255.255.255.000
  Gateway                   :     192.168.000.004
  ARP/PING                  :     ON
  BOOTP                     :     OFF
  DHCP                      :     OFF
  ZeroConf                  :     ON
  Bonjour                   :     ON
  Bonjour Name              :     IC0862E6_TPG60

ThinPrint
  ThinPrint Port            :     4000
  Bandwidth                 :     OFF
  Bandwidth[bits/s]         :     256000
  Connection Service        :     OFF
  Connection Server         :     000.000.000.000
  Connection Server Port    :     4001
  Client ID                 :     0
  Authentication Key        :     0

Monitoring
  Monitoring interval[s]    :     20
  Monitoring via Ping       :     ON
  Monitoring via Snmp       :     ON
  Status ""                 :
```

Fig. 4: TPG Status Page

Printing the Status Page via the TPG Status Button

Using the status button of the TPG, you can print a status page.

Proceed as follows:

1. *Press the status button for a short time.*

↳ The status page is printed.

Printing the Service Page via the TPG Status Button

Using the status button of the TPG, you can print a service page.

Proceed as follows:

1. *Keep the status button pressed for five seconds.*

↳ The status page is printed.

Printing the Service Page via an FTP Connection

Using an FTP connection, you can download a service page to your local computer and print it.

Proceed as follows:

1. *Switch to the directory in which you wish to save the file.*
2. *Open an FTP connection to the TPG:*
   Syntax: `ftp <IP Address>`
   Example: `ftp 192.168.0.123`
3. *Enter an arbitrary user name.*
4. *Enter either the TPG password or press ENTER if no password has been assigned.*
5. *Transfer the service page from the TPG to your local computer:*
   `get servicepage`
6. *Close the FTP connection:*
   `quit`
7. *Open and print the file using a text editor.*

↳ The service page will be printed.

4 Network and Device Settings

You can configure the device time and the device language on the TPG. You can define various parameters for an ideal integration of your TPG into a network. This chapter explains which network settings are supported by the TPG.

What information do you need?

- 'How to Configure TCP/IP Parameters' ⇨🗎42
- 'How to Configure the DNS' ⇨🗎44
- 'How to Enable/Disable Bonjour' ⇨🗎45
- 'How to Adapt the Network Speed' ⇨🗎47
- 'How to Configure the Device Time' ⇨🗎48
- 'How to Configure the Language of the Device' ⇨🗎49
- 'How to Determine a Description' ⇨🗎51

4.1 How to Configure TCP/IP Parameters

The TCP/IP (Transmission Control Protocol over Internet Protocol) is divided into two areas. The Internet Protocol (IP) is used for the fragmentation and addressing of data and transfers the data from the sender to the recipient.

The Transmission Control Protocol (TCP) guarantees reliable and in-order delivery of sender to receiver data. Upon receipt of one or more packets, the receiver returns an acknowledgement.

The protocol forwards data packets across several connections and establishes a connection between the network participants. The boot protocols BOOTP, DHCP, and ZeroConf belong to the TCP/IP protocol family. You can define various parameters for an ideal integration of your TPG into a TCP/IP network.

What do you want to do?

□ 'Configuring TCP/IP Parameters via the TPG Homepage' ➪🗎42

□ 'Configuring TCP/IP Parameters via the InterCon-NetTool' ➪🗎42

Configuring TCP/IP Parameters via the TPG Homepage

☞ Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – TCP/IP***.*
3. *Configure the TCP/IP parameters; see: Table 3* ➪🗎*43.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Configuring TCP/IP Parameters via the InterCon-NetTool

☞ Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – TCP/IP** *from the navigation bar.*
4. *Configure the TCP/IP parameters; see: Table 3* ➪🗎*43.*

5. *Click* **OK** *to confirm.*

↳ The settings are saved.

Table 3: TCP/IP Parameters

Parameters	Description
IP Address	IP address of the TPG
Subnet Mask	Subnet mask of the TPG
Gateway	IP address of the gateway
Multicast router as gateway	If this parameter has been enabled, the address of the found multicast router will be entered automatically as gateway address. If disabled, the gateway address has to be entered manually.
Host name	Host name of the TPG
Contact person	Freely definable description
Location	Freely definable description
DHCP BOOTP ARP/PING ZeroConf	Enables or disables the protocols DHCP, BOOTP, ARP/PING, and ZeroConf. Protocols offer various possibilities to save the IP address in the TPG. (See ⇨ 🗎13.) *We recommend to disable these options once an IP address has been assigned to the TPG.*
Bonjour	Bonjour allows the automatic recognition of computers, devices, and network services in TCP/IP-based networks. (see ⇨ 🗎45)

4.2 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.

Benefits and Purpose

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.

What do you want to do?

- ☐ 'Configuring DNS via the TPG Homepage' ⇨🗎44
- ☐ 'Configuring DNS via the InterCon-NetTool' ⇨🗎44

Configuring DNS via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – DNS***.*
3. *Configure the DNS parameters; see: Table 4* ⇨🗎*45.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Configuring DNS via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – DNS** *from the navigation bar.*
4. *Configure the DNS parameters; see: Table 4* ⇨🗎*45.*
5. *Click* **OK** *to confirm.*

↳ The settings are saved.

Table 4: DNS Parameters

Parameters	Description
DNS	Enables/disables DNS.
Domain name	Domain name of an existing DNS server (e.g. company.de)
Primary DNS server	IP address of the primary DNS server (e.g. 192.168.0.21)
Secondary DNS server	IP address of the secondary DNS server. *The secondary DNS server is used if the primary DNS server is not available.*

4.3 How to Enable/Disable 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 by ZeroConf
- Assignment of host names to IP addresses
- Location of server services without knowledge of the device's hostname or IP address

The TPG examines the network while checking the IP address selected by ZeroConf (see: 'ZeroConf' ⇨🗎14). If this 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.

What do you want to do?

- □ 'Configuring DNS via the TPG Homepage' ⇨🗎44
- □ 'Configuring DNS via the InterCon-NetTool' ⇨🗎44

Configuring Bonjour via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – TCP/IP***.*
3. *Tick/clear* **Bonjour***.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Configuring Bonjour via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – TCP/IP** *from the navigation bar.*
4. *Tick/clear* **Bonjour***.*
5. *Click* **OK** *to confirm.*

↳ The settings are saved.

4.4 How to Adapt the Network Speed

You can adapt the speed of the TPG to other network components, such as switches or hubs. The 'Auto' mode is preset. The speed is identified automatically and adapted to the other network components.

If you set the speed manually, the speed must correspond to the speed of the other network components. It is not possible to operate the TPG with full duplex if the hub is operated with half duplex.

What do you want to do?

☐ 'Adapting the Speed via the TPG Homepage' ⇨🗎47

☐ 'Adapting the Speed via the InterCon-NetTool' ⇨🗎47

Adapting the Speed via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – General***.*
3. *Select the desired setting from the* **Ethernet settings** *list.*
4. *Click* **Save** *to confirm.*

↳ The setting is saved.

Adapting the Speed via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – General** *from the navigation bar.*
4. *Select the desired setting from the* **Ethernet settings** *list.*
5. *Click* **OK** *to confirm.*

↳ The setting is saved.

4.5 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. The time server is defined via the IP address or the domain name.

Benefits and Purpose

If the time server is activated, all print jobs that are handled by the TPG will get a time stamp. Date and time are then displayed under 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.

What do you want to do?

□ 'Configuring the Device Time via the TPG Homepage' ⇨🗎48

□ 'Configuring the Device Time via the InterCon-NetTool' ⇨🗎49

Configuring the Device Time via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Time***.*
3. *Tick* **SNTP***.*
4. *Enter the IP address or the domain name of the time server into the* **Time server** *box.*
   (The domain name can only be used if DNS is enabled on the device and if a DNS server was specified).
5. *Select the code for your local time zone from the* **Time zone** *list.*
6. *Click* **Save** *to confirm.*

↳ The settings are saved.

Configuring the Device Time via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – Time** *from the navigation bar.*
4. *Tick* **SNTP***.*
5. *Enter the IP address or the domain name of the time server into the* **Time server** *box.*
   (The domain name can only be used if DNS is enabled on the device and if a DNS server was specified).
6. *Select the code for your local time zone from the* **Time zone** *list.*
7. *Click* **OK** *to confirm.*

↳ The settings are saved.

4.6 How to Configure the Language of the Device

You can define the language of the device. The language of the device is displayed on the TPG Homepage and in the status information (e.g. the status page). The TPG supports the following languages:

- English
- German
- French
- Spanish
- Italian
- Portuguese
- Japanese
- Korean
- Chinese (simplified/traditional)

What do you want to do?

□ 'Configuring the Language of the Device via the TPG Homepage' ⇨🗎50

□ 'Configuring the Language of the Device via the InterCon-NetTool' ⇨🗎50

If you only want to change the language of the TPG Homepage, you can define the language separately; see ⇨🗎17.

Configuring the Language of the Device via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – General***.*
3. *Select the desired language from the* **TPG language** *list.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Restart the TPG Homepage for the new settings to take effect.

Configuring the Language of the Device via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – General** *from the navigation bar.*
4. *Select the desired language from the* **TPG language** *list.*
5. *Click* **OK** *to confirm.*

↳ The settings are saved.

4.7 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.

What do you want to do?

- □ 'Determining Descriptions via the TPG Homepage' ⇨🗎51
- □ 'Determining Descriptions via the InterCon-NetTool' ⇨🗎51

Determining Descriptions via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – General***.*
3. *Enter freely definable names for* **Description**, **Dealer**, *and* **Dealer URL***.*
4. *Click* **Save** *to confirm.*

↳ The data is saved.

Determining Descriptions via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – General** *from the navigation bar.*
4. *Enter freely definable names for* **Description**, **Dealer**, *and* **Dealer URL***.*
5. *Click* **OK** *to confirm.*

↳ The data is saved.

5 ThinPrint® Settings

You must define the port, bandwidth, and printer 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' ⇨🗎52
- 'How to Define the Bandwidth' ⇨🗎53
- 'How to Integrate Printers' ⇨🗎54
- 'How to define Timeouts' ⇨🗎56
- 'How to Use the ThinPrint® Connection Service' ⇨🗎58

5.1 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.

What do you want to do?

□ 'Defining the ThinPrint® Port via the TPG Homepage' ⇨🗎52

□ 'Defining the ThinPrint® Port via the InterCon-NetTool' ⇨🗎53

Defining the ThinPrint® Port via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – ThinPrint®***.*
3. *Enter the port number into the* **ThinPrint® port** *box.*
4. *Click* **Save** *to confirm.*

↳ The setting is saved.

Defining the ThinPrint® Port via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – ThinPrint®** *from the navigation bar.*
4. *Enter the port number into the* **ThinPrint® port** *box.*
5. *Click* **OK** *to confirm.*

↳ The setting is saved.

5.2 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 bandwith 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.

What do you want to do?

- □ 'Decrease the Bandwidth via the TPG Homepage' ⇨ 53
- □ 'Decrease the Bandwidth via the InterCon-NetTool' ⇨ 54

Decrease the Bandwidth via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – ThinPrint®***.*
3. *Tick* **Bandwidth***.*
4. *Enter the desired bandwidth.*

5. *Click* **Save** *to confirm.*

↳ The setting is saved.

Decrease the Bandwidth via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – ThinPrint®** *from the navigation bar.*
4. *Tick* **Bandwidth**.
5. *Enter the desired bandwidth.*
6. *Click* **OK** *to confirm.*

↳ The setting is saved.

5.3 How to Integrate Printers

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

The print jobs are assigned via a printer ID. Up to six (TPG60) or twelve (TPG120) network printers can be connected to the TPG.

When integrating the connected printers you must define the printer parameters (name, driver, remote address) and a transfer method.

Transfer method

Data transfer between the TPG and the printers can be done in two ways:

- Usually data is transferred to the TCP/IP port via a **socket connection**. Port 9100 is preset. If required, you can configure a different port number.
- 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.

<u>Your advantage</u>: When using the LPD protocol for data transfer, additional print job attributes will be transferred and displayed in the job history.

What do you want to do?

- □ 'Integrating Printers via the TPG Homepage' ⇨🖹55
- □ 'Integrating Printers via the InterCon-NetTool' ⇨🖹55

Integrating Printers via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – ThinPrint®**.
3. *Enter the printer parameters; see: Table 5* ⇨🖹*56.*
4. *Select a transfer method for every printer.*
   - To choose a socket connection, mark the option in front of the field with the TCP/IP port number.
   - To choose an LPD connection, mark the option in front of the field with the LPD queue name.
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

Integrating Printers via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – ThinPrint®** *from the navigation bar.*
4. *Enter the printer parameters; see: Table 5* ⇨🖹*56.*
5. *Select a transfer method for every printer.*
   - To choose a socket connection, mark the option in front of the field with the TCP/IP port number.
   - To choose an LPD connection, mark the option in front of the field with the LPD queue name.
6. *Click* **OK** *to confirm.*

↳ The settings are saved.

Table 5: Printer Parameters

Parameters	Description
ID	A printer is identified by its printer ID.
Printer	The printer name is a description and is used to distinguish the printers. *The printer can only use the .print AutoConnect feature if a printer name was defined.*
Class	Printers with compatible drivers can be arranged in one class. *You can also define a printer class if you want to use the .print AutoConnect feature.*
Driver	Printer driver for the embedded printers.
Remote address	IP address or host name of the printer. *A host name can only be used if DNS was configured beforehand.*
Port	Port number for the socket connection (default = 9100) *Is used when selecting ’Socket’as transfer method.*
LPD Queue	LPD Queue name (default = lp1) *Is used when selecting the LPD protocol as transfer method.*
Status page printer	The symbol indicates which printer is used to print the status page. (default = printer ID 1) **This parameter can be defined via Configuration – General on the TPG Homepage.*

5.4 How to define Timeouts

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

Printer open timeout

The 'Printer open 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 freed up for subsequent print jobs, for example.

Job send timeout

The 'Job send 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, an error message is also sent to the ThinPrint® server. No error message is sent to the ThinPrint® server when printing takes place via the 'Connection Services'.

What do you want to do?

- □ 'Defining Timeouts via TPG Homepage' ⇨🖹57
- □ 'Defining Timeouts via InterCon-NetTool' ⇨🖹57

Defining Timeouts via TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – ThinPrint®***.*
3. *In the* **Printer open timeout** *and* **Job send timeout** *fields, enter the periods of time in seconds after which the timeouts should take effect. (0 seconds = off)*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Defining Timeouts via InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – ThinPrint®** *from the navigation bar.*
4. *In the* **Printer open timeout** *and* **Job send timeout** *fields, enter the periods of time in seconds after which the timeouts should take effect. (0 seconds = off)*
5. *Click* **OK** *to confirm.*

↳ The settings are saved.

5.5 How to Use the ThinPrint® Connection Service

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

The Connection Service manages the entire communication between the ThinPrint® server and the 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.

What do you want to do?

- ☐ 'Configuring the Connection Service via the TPG Homepage' ⇨🗎58
- ☐ 'Configuring the Connection Service via the InterCon-NetTool' ⇨🗎58

Configuring the Connection Service via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – ThinPrint®**.
3. *Tick* **Connection Service**.
4. *Enter the relevant data; see: Table 6 ⇨🗎59.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

Configuring the Connection Service via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*

2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – ThinPrint®** *from the navigation bar.*
4. *Select the* **Connection Service** *tab.*
5. *Tick* **Connection Service***.*
6. *Enter the relevant data; see: Table 6* ⇨🗎*59.*
7. *Click* **OK** *to confirm.*

↳ The settings are saved.

Table 6: Connection Service Parameter

Parameters	Description
Connection Service	Enables/disables the .print Connection Service
Connection Server	IP address of the server on which the Connection Service is installed.
Port	Port number used by the TPG to communicate with the Connection Service (default = 4001)
Client ID	Client ID as stored in the database of the Connection Service. The client ID is needed by the Connection Service to forward print jobs to the TPG.
Authentication key	Authentication key as stored in the database of the Connection Service.
Keep alive	Interval (in seconds) for refreshing the connection to the Connection Service. The value has to be lower or equal than the 'KeepAliveTO' parameter of the .print Connection Service (server side). (allowed entry: 30 - 180 | default = 60)
Connection retry	Interval (in seconds) for connection retries if the Connection Service is not reachable. (allowed entry: 5 -6000 | default = 120)

If a connection to the Connection Service was refused, it is because a value (client ID, authentication key, or IP address) was entered incorrectly. Check and modify your settings and reestablish the connection to the Connection Service manually. For this purpose, click **Reconnect.**

6 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.

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

What information do you need?

- 'How to Define a Password for the TPG (Read/Write Protection)' ⇨🗎61
- 'How to Protect the TPG against Unauthorized Access (IP Sender Control)' ⇨🗎62
- 'How to Enable/Disable FTP & HTTP (Port Control)' ⇨🗎63
- 'How Does the TPG Receive Encrypted Data' ⇨🗎65

More secure-related topics from other chapters:

- Administer the TPG via FTPS Connections ⇨🗎28
- Authenticate the TPG in the Network ⇨🗎66
- Authenticate the TPG/Client if the administrative access to the TPG Homepage via SSL (HTTPs) is protected ⇨🗎86

6.1 How to Define a Password for the TPG (Read/Write Protection)

Write Protection

A password can protect the TPG against unauthorized access. If a password was set, you must enter the password before you can save the changes to the parameters. This means that changes to the parameters can only be made using a valid password.

Read Protection

If you do not want your parameters to be displayed, you can set a password at this stage as well. For this purpose, the parameter **Access control** must be enabled. If this parameter is enabled, a password must be entered when starting the TPG Homepage or when opening the **Properties** dialog.

What do you want to do?

□ 'Defining the Password via the TPG Homepage' ⇨🗎61

□ 'Defining the Password via the InterCon-NetTool' ⇨🗎61

Defining the Password via the TPG Homepage

👉 Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Protection***.*
3. *Enter a password into the* **Password** *box in order to define the write protection.*
4. *Tick* **Access control** *in order to define the read protection.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

Defining the Password via the InterCon-NetTool

👉 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – Protection** *from the navigation bar.*

4. *Enter a password into the* **Password** *box in order to define the write protection.*
5. *Tick* **Access control** *in order to define the read protection.*
6. *Click* **OK** *to confirm.*

↳ The settings are saved.

You can also define the password using the menu bar of the InterCon-NetTool. Select **Actions – Change password** from the menu bar.

6.2 How to Protect the TPG against Unauthorized Access (IP Sender Control)

You can restrict the access to the TPG to a certain number of clients. For this purpose, you must enter the IP addresses or host names of the clients into the **IP sender** box. The TPG will only accept data packets from the specified clients. Up to eight IP senders can be specified. The use of wildcards (*) allows you to define subnetworks.

Once an IP sender has been defined, all undefined clients lose their access rights.

What do you want to do?

- □ 'Assigning Authorizations via the TPG Homepage' ⇨ 🗎62
- □ 'Assigning Authorizations via the InterCon-NetTool' ⇨ 🗎63

Assigning Authorizations via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Protection***.*
3. *Enter the IP addresses or host names of authorized clients into the* **IP sender** *box. (A host name can only be used if DNS was configured beforehand.)*

4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Assigning Authorizations via the InterCon-NetTool

☞ Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – Protection** *from the navigation bar.*
4. *Enter the IP addresses or host names of authorized clients into the* **IP sender** *box. (A host name can only be used if DNS was configured beforehand.)*
5. *Click* **OK** *to confirm.*

↳ The settings are saved.

6.3 How to Enable/Disable FTP & HTTP (Port Control)

The TPG cannot be attacked directly by viruses. Attacks to open ports can have a certain influence on the TPG and affect its functions.

Protecting the TPG against Attacks

To prevent attacks to these ports, you can disable the protocols FTP/FTPS or HTTP on the TPG.

- If you have disabled FTP/FTPS, all functions based on these protocols are no longer available; see: 'Administration via an FTP/FTPS Connection' ⇨🗎28.
- If you have disabled HTTP, all functions based on this protocol are no longer available. This means that, for example, access to the TPG Homepage will no longer be available.

ℹ

If HTTP is disabled, HTTPs will remain active. Access to the TPG Homepage will be protected via SSL. This means that a certificate is required for working via HTTPs; see: ⇨🗎86.

Never disable the protocols HTTP and FTP/FTPS at the same time. Otherwise the TPG can no longer be configured.

What do you want to do?

- □ 'Enabling/Disabling a Protocol via the TPG Homepage' ⇨🗎64
- □ 'EnablingDisabling a Protocol via the InterCon-NetTool' ⇨🗎64

Enabling/Disabling a Protocol via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Protection***.*
3. *Tick/Clear* **HTTP** *or* **FTP***.*
4. *Click* **Save** *to confirm.*

↳ The setting is saved.

EnablingDisabling a Protocol via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – Protection** *from the navigation bar.*
4. *Tick/Clear* **HTTP** *or* **FTP***.*
5. *Click* **OK** *to confirm.*

↳ The setting is saved.

6.4 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 encryption.

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: 'How to Create a Certificate Request for CA Certificates' ⇨🗎79.
- Save the CA certificate; see: 'How to Save CA Certificates in the TPG' ⇨🗎81.

7 Network Authentication

By means of an authentication, a network can be protected against unauthorized access. The TPG can participate in various authentication procedures. This chapter 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.

What information do you need?

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

- 'How to Configure EAP-MD5' ⇨🗎67
- 'How to Configure EAP-TLS' ⇨🗎68
- 'How to Configure EAP-TTLS' ⇨🗎70
- 'How to Configure PEAP' ⇨🗎72
- 'How to Configure EAP-FAST' ⇨🗎74

7.1 How to Configure 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.

Basic Functions

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.

What do you want to do?

□ 'Enabling EAP-MD5 via the TPG Homepage' ⇨🗎67

□ 'Enabling EAP-MD5 via the InterCon-NetTool' ⇨🗎67

Enabling EAP-MD5 via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Protection***.*
3. *Select* **Authentication***.*
4. *Select* **EAP-MD5** *from the* **Authentication** *list.*
5. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*
6. *Click* **Save** *to confirm.*

↳ The settings are saved.

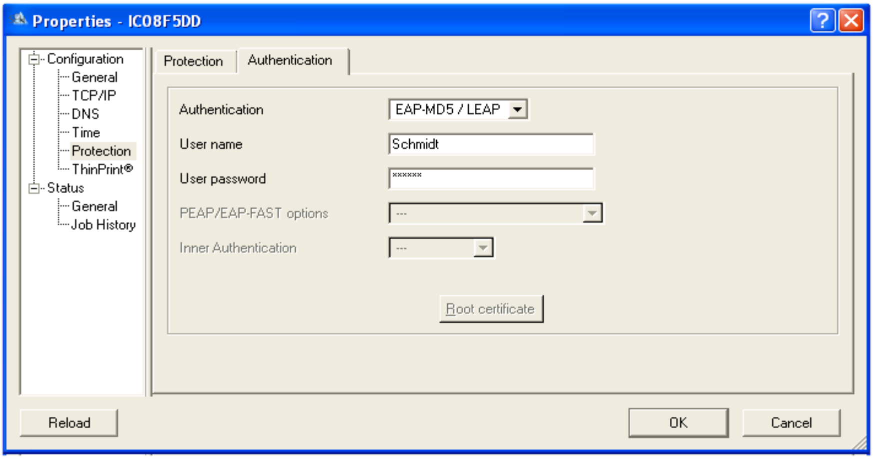
Enabling EAP-MD5 via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*

2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – Protection** *from the navigation bar.*
4. *Select the* **Authentication** *tab.*
5. *Select* **EAP-MD5** *from the* **Authentication** *list.*
6. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*
7. *Click* **OK** *to confirm.*

↳ The settings are saved.



Authentication: EAP-MD5 / LEAP
User name: Schmidt
User password: ******
PEAP/EAP-FAST options: ---
Inner Authentication: ---

Fig. 5: InterCon-NetTool - Authentication

7.2 How to Configure 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.

Basic Functions

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 TPG 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 following instructions in the indicated order. Otherwise the TPG cannot be addressed in the network. In this case you have to reset the TPG parameters; see: ⇨🗎92.

Procedure

- □ Create a certificate request on the TPG; see: ⇨🗎79.
- □ Create a CA certificate using the certificate request and the authentication server.
- □ Install the CA certificate on the TPG; see: 'How to Save CA Certificates in the TPG' ⇨🗎81.
- □ Install the root certificate of the authentication server on the TPG; see 'How to Save Root Certificates in the TPG' ⇨🗎83.
- □ Enable the authentication method 'EAP-TLS' on the TPG.

Proceed as follows:

1. *Start the TPG Homepage or start the InterCon-NetTool and double-click the TPG in the device list.*
2. *Select* **Configuration – Protection***.*
3. *Select* **Authentication***.*
4. *Select* **EAP-TLS** *from the* **Authentication** *list.*
5. *Click* **Save** *or* **OK** *to confirm.*

↳ The settings are saved.

7.3 How to Configure EAP-TTLS

Benefits and Purpose

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.

Basic Functions

EAP-TTLS consists of two phases:

- During 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 und 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.

To make the connection more secure, you can install the root certificate of the RADIUS server on the TPG (Phase 1). The TPG validates the identity of the RADIUS server by means of the certificate.

Requirements

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

What do you want to do?

□ 'Enabling EAP-TTLS via the TPG Homepage' ⇨🗎70

□ 'Enabling EAP-TTLS via the InterCon-NetTool' ⇨🗎71

Enabling EAP-TTLS via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*

2. *Select* **Configuration – Protection***.*
3. *Select* **Authentication***.*
4. *Select* **EAP-TTLS** *from the* **Authentication** *list.*
5. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*
6. *Select the settings intended to secure the communication in the TLS channel.*
7. *To make the connection more secure, you can also install the root certificate of the RADIUS server on the TPG.*
8. *Click* **Save** *to confirm.*

➥ The settings are saved.

Enabling EAP-TTLS via the InterCon-NetTool

☞ Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – Protection** *from the navigation bar.*
4. *Select the* **Authentication** *tab.*
5. *Select* **EAP-TTLS** *from the* **Authentication** *list.*
6. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*
7. *Select the settings intended to secure the communication in the TLS channel.*
8. *To make the connection more secure, you can also install the root certificate of the RADIUS server on the TPG.*
9. *Click* **OK** *to confirm.*

➥ The settings are saved.

7.4 How to Configure 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.

Basic Functions

In the case of PEAP (compare EAP-TTLS; see ⇨🖹70), 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.

What do you want to do?

□ 'Enabling PEAP via the TPG Homepage' ⇨🖹72

□ 'Enabling PEAP via the InterCon-NetTool' ⇨🖹73

Enabling PEAP via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Protection***.*
3. *Select* **Authentication***.*
4. *Select* **EAP-PEAP** *from the* **Authentication** *list.*
5. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*

6. *Select the settings intended to secure the communication in the TLS channel.*
7. *To make the connection more secure, you can also install the root certificate of the RADIUS server on the TPG.*
8. *Click* **Save** *to confirm.*

↳ The settings are saved.

Enabling PEAP via the InterCon-NetTool

☞ Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – Protection** *from the navigation bar.*
4. *Select the* **Authentication** *tab.*
5. *Select* **EAP-PEAP** *from the* **Authentication** *list.*
6. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*
7. *Select the settings intended to secure the communication in the TLS channel.*
8. *To make the connection more secure, you can also install the root certificate of the RADIUS server on the TPG.*
9. *Click* **OK** *to confirm.*

↳ The settings are saved.

7.5 How to Configure 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.

Basic Functions

EAP-FAST uses (as in the case of EAP-TTLS; see ⇨🗎70) 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 Credential) 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 TPG authentication as well as the delivery of PACs.

Requirements

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

What do you want to do?

□ 'Enabling EAP-FAST via the TPG Homepage' ⇨🗎75

□ 'Enabling EAP-FAST via the InterCon-NetTool' ⇨🗎75

Enabling EAP-FAST via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Protection***.*
3. *Select* **Authentication***.*
4. *Select* **EAP-FAST** *from the* **Authentication** *list.*
5. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*
6. *Select the settings intended to secure the communication in the channel.*
7. *Click* **Save** *to confirm.*

↳ The settings are saved.

Enabling EAP-FAST via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the TPG in the device list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – Protection** *from the navigation bar.*
4. *Select the* **Authentication** *tab.*
5. *Select* **EAP-FAST** *from the* **Authentication** *list.*
6. *Enter the user name and the password that are used for the configuration of the TPG on the RADIUS server.*
7. *Select the settings intended to secure the communication in the channel.*
8. *Click* **OK** *to confirm.*

↳ The settings are saved.

8 Certificate Management

The TPG has its own certificate management. This chapter 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 mechanismen. Use certificates on your TPG

- to receive encrypted print data; see: ⇨🗎65.
- to authenticate the TPG in a network that is protected by EAP authentication; see: 'Network Authentication' ⇨🗎66.
- to authenticate the TPG if the administrative access to the TPG Homepage via HTTPs (SSL) is protected; see: ⇨🗎86.
- to administer the TPG via an FTPS connection; see: ⇨🗎28.

If you want to use certificates, it is advisable to protect the TPG by a password so that certificates cannot be deleted by unauthorized persons; see ⇨🗎61.

Which Certificates are available?

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

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. A CA certificate is mandatory to print via SSL.

CA certificates are certificates that have been signed by a certification authority (CA).

The authenticity of the CA certificate can be verified by means of a so-called **root certificate** issued by the certification authority. The root certificate is stored on an authentication server in the network.

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 CA certificate as soon as possible.

What information do you need?

- 'How to Create a Self-Signed Certificate' ⇨🗎77
- 'How to Create a Certificate Request for CA Certificates' ⇨🗎79
- 'How to Save CA Certificates in the TPG' ⇨🗎81
- 'How to Save PKCS12 Certificates in the TPG' ⇨🗎82
- 'How to Save Root Certificates in the TPG' ⇨🗎83
- 'How to Delete Certificates' ⇨🗎84
- 'How to Install Certificates on a Windows Client' ⇨🗎86

8.1 How to Create a Self-Signed Certificate

When a certificate is created on the TPG for the first time, a list of parameters is displayed that are required for the certificate.

If a self-signed certificate or a CA certificate has already been saved in the TPG, the content of this certificate will be displayed. In this case you have to delete the existing certificate first; see: 'How to Delete Certificates' ⇨🗎84.

What do you want to do?

□ 'Creating Self-signed Certificates via the TPG Homepage' ⇨🗎77

□ 'Creating Self-Signed Certificates via the InterCon-NetTool' ⇨🗎78

Creating Self-signed Certificates via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Certificates.**

3. *Select* **TPG certificate***.*
4. *Enter the relevant parameters, see: Table 7* ⇨🗎*78.*
5. *Click* **Create self-signed certificate***.*

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

Creating Self-Signed Certificates via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark the TPG in the device list.*
3. *Select* **Actions – Certificate – Server certificate** *from the menu bar. The* **Certificate** *dialog appears.*
4. *Tick* **Create self-signed certificate***.*
5. *Click* **Next***.*
6. *Enter the relevant parameters, see: Table 7* ⇨🗎*78.*
7. *Click* **Next***. The parameters are listed.*
8. *Confirm by clicking* **Next***.*

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

Table 7: 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. You can enter a maximum of 64 characters.
E-mail address	Specifies an email address. You can enter a maximum of 40 characters. (Optional Entry)
Organization name	Specifies the company that uses the TPG. You can enter a maximum of 64 characters.
Organizational unit	Specifies the department or subsection of a company. You can enter a maximum of 64 characters. (Optional Entry)
Locality name	Specifies the locality where the company is based. You can enter a maximum of 64 characters.

Parameters	Description
State name	Specifies the state in which the company is based. You can enter a maximum of 64 characters. (Optional Entry)
Country name	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 after which the certificate is valid.
Expires on	Specifies the date after which the certificate is invalid.

8.2 How to Create a Certificate Request for CA Certificates

For using a CA certificate, a certificate request must be created in the TPG and sent to the certification authority. The certification authority will then create a CA certificate on the basis of the certificate request. The certificate must be in base 64 format. When the CA certificate has been received, it must be saved in the TPG.

When a certificate request is created on the TPG for the first time, a list of parameters is displayed that are required for the certificate.

If a self-signed certificate or a CA certificate has already been saved in the TPG, the content of this certificate will be displayed. In this case you have to delete the existing certificate first; see: 'How to Delete Certificates' ⇨🗎84.

After the creation of a certificate request, no self-signed certificate can be created until the CA certificate has been saved in the TPG.

What do you want to do?

☐ 'Creating a Certificate Request via the TPG Homepage' ⇨🗎79

☐ 'Creating a Certificate Request via the InterCon-NetTool' ⇨🗎80

Creating a Certificate Request via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*

2. *Select* **Configuration – Certificates**.
3. *Select* **TPG certificate**.
4. *Enter the required parameters, see: Table 7 ⇨🗎78.*
5. *Click* **Create certificate request**.
   The creation of the certificate request is in progress. This may take a few minutes.
6. *Save the request in a text file.*
7. *Send the text file as certificate request to a certification authority.*

When the CA certificate has been received, it must be saved in the TPG; see: 'How to Save CA Certificates in the TPG' ⇨🗎81.

Creating a Certificate Request via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark the TPG in the device list.*
3. *Select* **Actions – Certificate – Server certificate** *from the menu bar. The* **Certificate** *dialog appears.*
4. *Tick* **Create certificate request**.
5. *Click* **Next**.
6. *Enter the relevant parameters, see: Table 7 ⇨🗎78.*
7. *Click* **Next**. *The parameters are listed.*
8. *Confirm by clicking* **Next**. *The creation of the certificate request is in progress. This may take a few minutes.*
9. *Save the request in a text file.*
10. *Send the text file as certificate request to a certification authority.*

When the CA certificate has been received, it must be saved in the TPG; see: 'How to Save CA Certificates in the TPG' ⇨🗎81.

8.3 How to Save CA Certificates in the TPG

ℹ The certificate must be in base 64 format.

What do you want to do?

□ 'Saving CA Certificates via the TPG Homepage' ⇨🗎81

□ 'Saving CA Certificates via the InterCon-NetTool' ⇨🗎81

Saving CA Certificates via the TPG Homepage

☞ Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Certificates***.*
3. *Select* **TPG certificate***.*
4. *Click* **Browse***.*
5. *Specify the CA certificate.*
6. *Click* **Load Certificate***.*

↳ The CA certificate is saved in the TPG. This may take a few minutes.

Saving CA Certificates via the InterCon-NetTool

☞ Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark the TPG in the device list.*
3. *Select* **Actions – Certificate – Server certificate** *from the menu bar. The* **Certificate** *dialog appears.*
4. *Click* **...***.*
5. *Specify the CA certificate.*
6. *Click* **Load***.*

↳ The CA certificate is saved in the TPG. This may take a few minutes.

8.4 How to Save PKCS12 Certificates in the TPG

PKCS12 Certificates can be used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.

If a self-signed certificate or a CA certificate has already been saved in the TPG, the content of this certificate will be displayed. In this case you have to delete the existing certificate first; see: 'How to Delete Certificates' ⇨🗎84.

What do you want to do?

- □ 'Saving PKCS12 Certificates via the TPG Homepage' ⇨🗎82
- □ 'Saving PKCS12 Certificates via the InterCon-NetTool' ⇨🗎82

Saving PKCS12 Certificates via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Certificates***.*
3. *Select* **TPG certificate***.*
4. *Click* **Load certificate (pkcs12 format)***.*
5. *Click* **Browse***.*
6. *Specify the CA certificate.*
7. *Enter the password.*
8. *Click* **Load PKCS12***.*

↳ The PKCS12 certificate is saved in the TPG. This may take a few minutes.

Saving PKCS12 Certificates via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark the TPG in the device list.*
3. *Select* **Actions – Certificate – Server certificate** *from the menu bar. The* **Certificate** *dialog appears.*
4. *Tick* **Load certificate (pkcs12 format)***.*

5. *Click* **Next.**
6. *Specify the certificate.*
7. *Enter the password.*
8. *Click* **Next.**

↳ The PKCS12 certificate is saved in the TPG. This may take a few minutes.

8.5 How to Save Root Certificates in the TPG

The TPG offers a number of authentication methods to verify its identity in a network. If you use the authentication method 'EAP-TLS', you must install the root certificate of the authentication server (RADIUS) on the TPG; see: 'How to Configure EAP-TLS' ⇨🗎68.

The certificate must be in base 64 format.

What do you want to do?

☐ 'Saving Root Certificates via the TPG Homepage' ⇨🗎83

☐ 'Saving Root Certificates via the InterCon-NetTool' ⇨🗎84

Saving Root Certificates via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Certificates.**
3. *Select* **Root certificate.**
4. *Click* **Browse.**
5. *Select the root certificate.*
6. *Click* **Load root certificate.**

↳ The root certificate is saved in the TPG. This may take a few minutes.

Saving Root Certificates via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark the TPG in the device list.*
3. *Select* **Actions – Certificate – Root certificate** *from the menu bar. The* **Certificate** *dialog appears.*
4. *Click* **...**.
5. *Enter the root certificate.*
6. *Click* **Load***.*

↳ The root certificate is saved in the TPG. This may take a few minutes.

8.6 How to Delete Certificates

If a self-signed certificate or a CA certificate is saved in the TPG, the content of this certificate will be displayed under **TPG certificate.** If you want to use a different certificate you must first delete the existing certificate.

What do you want to do?

□ 'Deleting Certificates via the TPG Homepage' ⇨🗎84

□ 'Deleting Certificates via the InterCon-NetTool' ⇨🗎85

Deleting Certificates via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Configuration – Certificates***.*
3. *Select* **TPG certificate***.*
4. *Click* **Delete certificate***.*

↳ The certificate is deleted.

Deleting Certificates via the InterCon-NetTool

☞ Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark the TPG in the device list.*
3. *Select* **Actions – Certificate – Server certificate** *from the menu bar. The* **Certificate** *dialog appears.*
4. *Click* **Delete***.*

↳ The certificate is deleted.

8.7 How to Install Certificates on a Windows Client

Why do I need Certificates on the Client?

The following cases require a certificate on the client:

- If, during the transfer of print data, an encrypted connection between the client and the TPG is additionally secured by means of an authentication.
- If the administrative access to the TPG Homepage is protected via SSL (HTTPs).

URLs that require an SSL connection start with 'https'. During a so-called 'handshake', the client asks the SSL server via browser for a CA certificate.

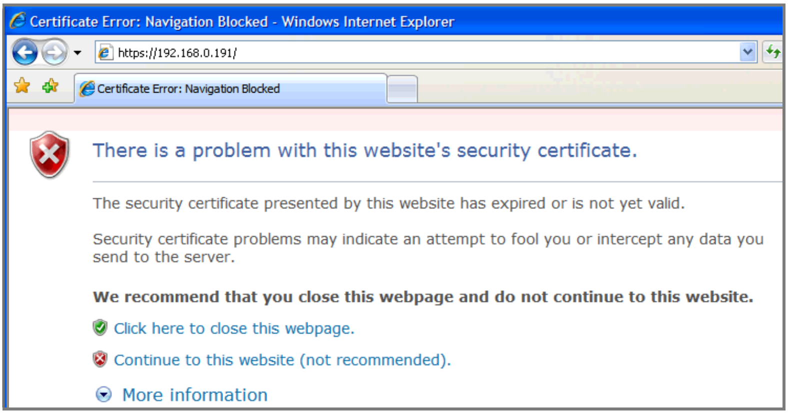
If a certificate is unknown to the Windows client, the certificate is not classed as 'trusted'. In this case, you will get an error message. Install the certificate on the Windows client using a browser in order to make the certificate known to the client.

Example

One method using the 'Internet Explorer 7' is described in the following.

Proceed as follows:

1. *Establish a safe connection to your TPG Homepage. To do this, enter 'https://' and the IP address of the TPG into the address box of your browser.*
   (e.g. https://192.168.0.191). A security alert appears.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.0.191/
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website has expired or is not yet valid.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

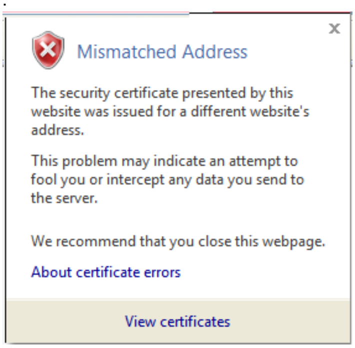
Click here to close this webpage.

Continue to this website (not recommended).

More information

Fig. 6: Internet Explorer – Security Alert

2. *Click* **Continue to this website.**
   A note (Certificate Error) is displayed



Mismatched Address

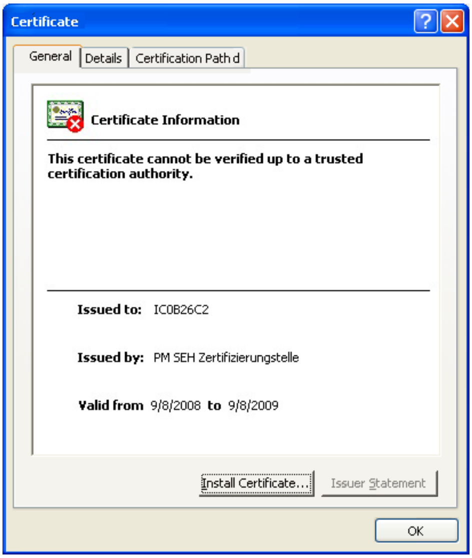
The security certificate presented by this website was issued for a different website's address.

This problem may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

Fig. 7: Internet Explorer - Certificate Error

3. *Click* **View certificates.**
   The **Certificate** *dialog appears.*



This certificate cannot be verified up to a trusted certification authority.

Issued to: IC0B26C2

Issued by: PM SEH Zertifizierungstelle

Valid from 9/8/2008 to 9/8/2009

Fig. 8: Internet Explorer - Certificate

4. *Class the certificate as 'trusted' and click* **Install Certificate.**
   The Certificate Import Wizard is started.
5. *Follow the instructions of the Wizard.*

↳ The certificate is installed on the client and is classed as 'trusted'.

9 Maintenance

Various maintenance procedures can be carried out on the TPG. This chapter contains information on securing and resetting the parameter values. It also explains how to restart and update the device.

What information do you need?

- 'How to Save TPG Parameters (Backup)' ⇨🗎89
- 'How to Reset Parameters to their Default Values' ⇨🗎92
- 'How to Perform an Update' ⇨🗎96
- 'How to Restart the TPG' ⇨🗎102

9.1 How to Save TPG Parameters (Backup)

All TPG settings (with the exception of passwords) are saved in the parameters 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 also edit the TPG parameters using a text editor. Afterwards, the configured file can be downloaded to one or more TPG. The parameters included in the file will be taken over by the device.

What do you want to do?

- □ 'Saving the Parameters File to the Client via the InterCon-NetTool' ⇨🗎89
- □ 'Editing the Parameters File using a Text Editor' ⇨🗎90
- □ 'Downloading the Parameters File to one or more TPG using the InterCon-NetTool' ⇨🗎91
- □ 'Downloading the Parameters File to the TPG using the TPG Homepage' ⇨🗎92

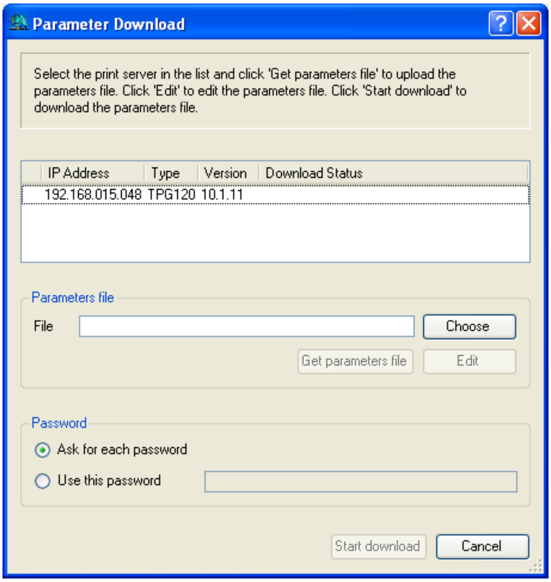
Saving the Parameters File to the Client via the InterCon-NetTool

The parameters file can be copied to any system using the InterCon-NetTool.

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark the TPG in the device list.*
3. *Select* **Actions – Download Parameters File** *from the menu bar.*
   The **Parameter Download** *dialog appears; see: Fig. 9 ⇨🗎90.*
4. *Highlight the TPG.*
5. *Click* **Get parameters file.**
   The **Save As** *dialog appears.*
6. *Enter the file name and path.*
7. *Click* **Save.**

↳ The parameters file is saved in your client.



Select the print server in the list and click 'Get parameters file' to upload the parameters file. Click 'Edit' to edit the parameters file. Click 'Start download' to download the parameters file.

IP Address	Type	Version	Download Status
192.168.015.048	TPG120	10.1.11	

● Ask for each password

○ Use this password

Fig. 9: InterCon-NetTool - Parameter Download

Editing the Parameters File using a Text Editor

You can edit the parameters file using any text editor. Use a text editor that is installed on your computer or the text editor that is provided by the InterCon-NetTool.

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark the TPG in the device list.*
3. *Select* **Actions – Download Parameters File** *from the menu bar.*
   The **Parameter Download** *dialog appears.*
4. *Click* **Choose***.*
   The **Parameter Download** *dialog appears.*
5. *Specify the 'parameters' file.*
6. *Click* **Open***.*
7. *Click* **Edit***.*
   A text editor with the 'parametrers' file will be opened.
8. *Edit the file; see: 'Parameter List' ⇨🗎107.*
9. *Save the file.*

Downloading the Parameters File to one or more TPG using the InterCon-NetTool

You can configure one or more TPG using the parameters file. For this purpose, the file is downloaded to the TPG.

When downloading the parameters file to several TPG, the parameter default settings 'IP address,' and 'Host name,' of the respective TPG will be maintained. All other settings will be overwritten by the ones in the new parameters file.

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select one or more TPG from the device list.*
3. *Select* **Actions – Download Parameters File** *from the menu bar.*
4. *Click* **Choose***. The* **Parameter Download** *dialog appears; see: Fig. 9 ⇨ 🗎 90.*
5. *Specify the 'parameters' file.*
6. *Click* **Open***.*
7. *Decide on the password option:*
   If the TPG displayed in the list are not password-protected or protected by different passwords, activate **Ask for each password***.*
   If the TPG are protected by the same password, activate **Use this password** *and enter the password.*
8. *Click* **Start download***.*

By clicking 'Start download', the selected file will be downloaded to all TPG displayed in the list. If you do not want to download the file to all TPG, you must close the window and only select the desired TPG from the device list (see step 2).

9. *Confirm the security query.*
10. *Enter the password(s), if necessary.*

↳ The parameters file will be downloaded to the TPG. The TPG parameters will be configured in accordance with the file.

Downloading the Parameters File to the TPG using the TPG Homepage

The TPG Homepage can be used to configure the TPG via the parameters file. All previous TPG settings will be overwritten by the parameters file.

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Actions – Download Area***.*
3. *Select* **Parameter Download***.*
4. *Click* **Browse...***.*
5. *Specify the 'parameters' file.*
6. *Click* **Open***.*
7. *Click* **Download***.*
8. *Enter the TPG password, if necessary.*

↳ The parameters file will be downloaded to the TPG. The TPG parameters will be configured in accordance with the file.

9.2 How to Reset Parameters to their Default Values

You can reset all TPG parameters to their default values (factory default settings). All previously configured parameters will be deleted in this process. Installed certificates will not be deleted.

Since the IP address of the TPG will be reset as well, the TPG Homepage cannot be started or displayed.

You must reset the parameters, for example, if you have changed the location of the TPG60 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.

If the TPG is protected by a password, the password has to be entered before resetting the parameters. Only by using the status button of the TPG can the parameters be reset without entering the password.

What do you want to do?

□ 'Resetting Parameters via the TPG Homepage' ⇨🗎93

□ 'Resetting Parameters via the InterCon-NetTool' ⇨🗎93

□ 'Resetting Parameters via an FTP Connection' ⇨🗎94

□ 'Resetting Parameters via the TPG Status Button' ⇨🗎94

Resetting Parameters via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Actions – 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. *Mark the TPG in the device list.*
3. *Select* **Actions – Default Settings** *from the menu bar.*
4. *Click* **Finish***.*

↳ The parameters are reset.

Resetting Parameters via an FTP Connection

Proceed as follows:

1. *Open an FTP connection to the TPG:*
   Syntax: `ftp <IP Address>`
   Example: `ftp 192.168.0.123`
2. *Enter the password of the TPG, if applicable, or press ENTER.*
3. *Reset the parameters:*
   `quote SITE RESET`
4. *Close the FTP connection:*
   `quit`
5. *Disconnect the power socket on the TPG for a moment.*

↳ The parameters are reset.

Resetting Parameters via the TPG Status Button

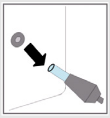
The reset process comprises three different steps.

- In the first step, the TPG is forced into reset mode. The parameters are reset in this mode.
- The second step involves restarting the device.
- In the third step, a status page is printed. The status page can be used to check whether the parameters were successfully reset.

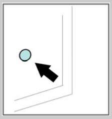
IMPORTANT: The reset mode is signaled by the simultaneous flashing of the Activity LED (yellow) and the Status LED (green) and remains active for the duration of five flashes.
The status button must be released within this time frame, otherwise the TPG will go into BIOS mode. In this case you need to start the reset process again.

These three steps are illustrated in the following. The illustrations may vary slightly from your device model.

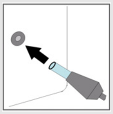
[Phase 1] Reset



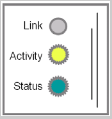
Turn the TPG off
(Disconnect the power socket)



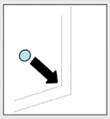
Press the status button and keep it pressed.



Turn the TPG on
(Reconnect the power socket)

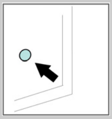


Wait until the Activity- and Status-LED start blinking simultaneously.
The Reset Mode is activate.



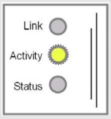
Release the status button for about 2 seconds.

The LEDs blink alternatingly.

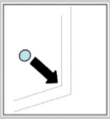


Press the status button once again and keep it pressed.

The LEDs blink simultaneously.

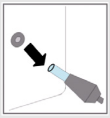


After few seconds only the Activity-LED blinks consistently.

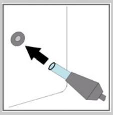


Release the status button.

[Phase 2] Device start

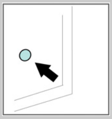


Turn the TPG off
(Disconnect the power socket)



Turn the TPG on
(Reconnect the power socket)

[Phase 3] Status Check



Press the status button for a short time.

9.3 How to Perform an Update

You can perform software updates. Updates allow you to benefit from currently developed features.

What Happens During an Update?

In the course of an update, the old software will be overwritten and replaced by the new software. The configuration parameters retain their original settings.

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 version with new functions or bug fixes.

Check the currently installed software version of your TPG. The version number can be found in the device list of the InterCon-NetTool. You can also start the TPG Homepage and select **Status - General.**

Where Do I Find the Update Files?

You can download the current software files from the website www.seh.de.

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

Update Types

An update can be carried out manually (standard update) or automatically (dynamic update).

- In the case of a standard update, the update file is downloaded manually from a server or a data medium and saved in the TPG.
- In the case of a dynamic update, polling is performed during a TPG restart to determine whether, in the meantime, a later version of the software file has been stored on the specified file server. If this is the case, the software file is automatically saved in the TPG via FTP.

The dynamic update cannot be used to save an earlier version of the software in the TPG. In this case use the standard update.

In order to reduce the amount of administration you can carry out an update for several TPGs at the same time. To this purpose, the update files have to be stored in a directory.

Requirements

☑ The TPG is known to the network via its IP address.

☑ All print jobs are finished.

What do you want to do?

□ 'Standard Update via the TPG Homepage' ⇨🗎97

□ 'Standard Update via the InterCon-NetTool' ⇨🗎97

□ 'Standard Update via FTP' ⇨🗎98

□ 'Dynamic Update via the TPG Homepage' ⇨🗎99

□ 'Dynamic Update via the InterCon-NetTool' ⇨🗎100

□ 'Dynamic Update via FTP' ⇨🗎101

□ 'Perform an Update to more than one TPG' ⇨🗎101

Standard Update via the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Actions – Download Area**.
3. *Select* **Standard Firmware Update**.
4. *Click* **Browse**.
5. *Select the update file.*
6. *Click* **Download**.

↳ The update is executed. The TPG is restarted.

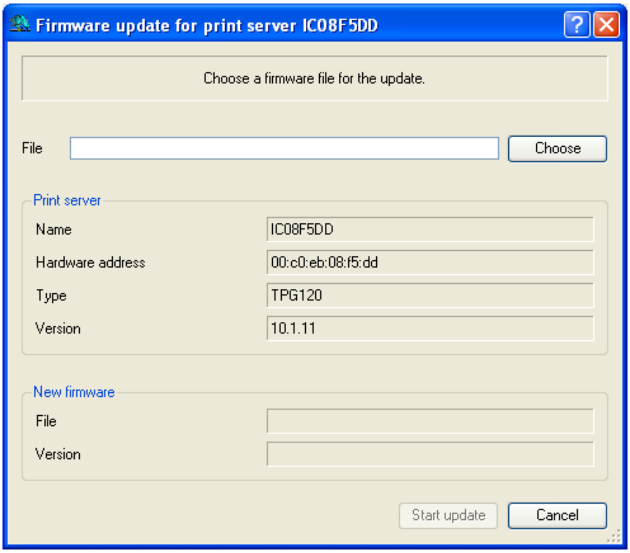
Standard Update via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark the TPG in the device list.*
3. *Select* **Actions – Firmware Update – Standard Update** *from the menu bar. The* **update** *dialog appears; see Fig. 10* ⇨🗎*98.*

4. *Click* **Choose***.*
5. *Select the update file.*
6. *Click* **Start update***.*
7. *Confirm the security query.*

↳ The update is executed. The TPG is restarted.



Firmware update for print server IC08F5DD

Choose a firmware file for the update.

File:

Print server

Name: IC08F5DD

Hardware address: 00:c0:eb:08:f5:dd

Type: TPG120

Version: 10.1.11

New firmware

File:

Version:

Fig. 10: InterCon-NetTool - Update

Standard Update via FTP

You can update the standard of your TPG via an FTP connection.

Proceed as follows:

1. *Change to the directory where the update file is located.*
2. *Open an FTP connection to the TPG:*
   Syntax: `ftp <IP address of the TPG>`
   Example: `ftp 192.168.0.123`
3. *Enter an arbitrary user name.*
4. *Enter either the TPG password or press ENTER if no password has been assigned.*
5. *Switch to binary mode:*
   `bin`

6. *Transfer the update file to the TPG:*
   <u>Syntax:</u> `put <name of update file> binfile`
   <u>Example:</u> `put tpg-10.1.3.bin binfile`
7. *Close the FTP connection:*
   `quit`

Dynamic Update via the TPG Homepage

Specify a directory on the file server for automatic (dynamic) updates. The directory contains the current software files.

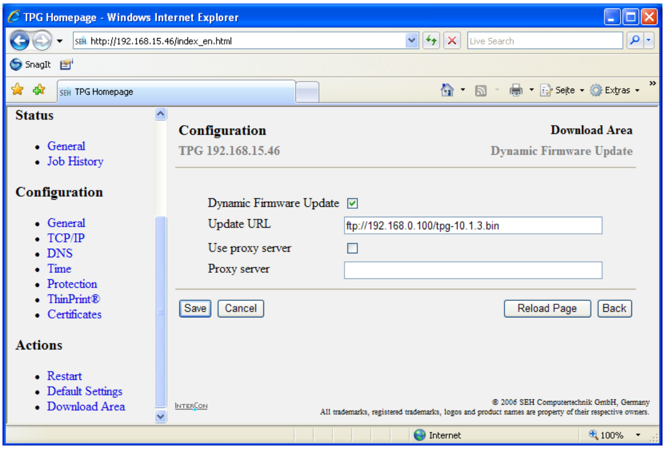
Requirements

☑ The file server on which the software files are stored either uses the anonymous login or the TPG is set up as user on the file server.

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Actions – Download Area**.
3. *Select* **Dynamic Firmware Update**.
4. *Tick* **Dynamic Firmware Update**.
5. *Specify the IP address of the file server on which the new software files are to be stored.*
   <u>Syntax:</u> `ftp://<file server IP address>/<Software file name>`
   <u>Example:</u> `ftp://192.168.0.100/tpg-10.1.3.bin`
   (If your system supports name resolution via WINS, DHCP, or DNS, you can enter the name of the file server instead of the IP address of the file server).
   <u>Example:</u> `ftp://file.server.de/tpg-10.1.3.bin`
6. *If you use a proxy server, tick* **Use proxy server** *and enter the IP address of the proxy server.*
7. *Click* **Save** *to confirm.*

↳ The settings are saved. At each restart, the TPG verifies the version of the software files. If the TPG detects a higher version, this version will be installed automatically on the TPG.



Configuration — **Download Area**

TPG 192.168.15.46 — Dynamic Firmware Update

Dynamic Firmware Update ☑

Update URL: ftp://192.168.0.100/tpg-10.1.3.bin

Use proxy server □

Proxy server:

© 2006 SEH Computertechnik GmbH, Germany
All trademarks, registered trademarks, logos and product names are property of their respective owners.

Fig. 11: TPG Homepage - Dynamic Firmware Update

Dynamic Update via the InterCon-NetTool

Specify a directory on the file server for automatic (dynamic) updates. The directory contains the current software files.

Requirements

☑ The file server on which the software files are stored either uses the anonymous login or the TPG is set up as user on the file server.

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark the TPG in the device list.*
3. *Select* **Actions – Firmware Update – Dynamic Update** *from the menu bar. The* **Dynamic Update***dialog appears.*
4. *Tick* **Dynamic Firmware Update***.*
5. *Specify the IP address of the file server on which the new software files are to be stored.*
   Syntax: `ftp://<file server IP address>/<Software file name>`
   Example: `ftp://192.168.0.100/tpg-10.1.3.bin`
   (If your system supports name resolution via WINS, DHCP, or DNS, you can enter the name of the file server instead of the IP address of the file server).
   Example: `ftp://file.server.de/tpg-10.1.3.bin`

6. *If you use a proxy server, tick* **Use proxy server** *and enter the IP address of the proxy server.*
7. *Click* **OK** *to confirm.*

↳ The settings are saved. At each restart, the TPG verifies the version of the software files. If the TPG detects a higher version, this version will be installed automatically on the TPG.

Dynamic Update via FTP

The parameters for a dynamic update can also be configured via FTP. For further information, read section 'Configuring Parameters via an FTP Connection' ⇨🗎29.

Perform an Update to more than one TPG

The InterCon-NetTool allows you to carry out an update to more than one TPG.

Requirements

☑ All required software files (Updates) are located in one directory.

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the TPGs from the device list.*
3. *Select* **Actions – Firmware Update from the menu bar.** *The* **Dynamic Update***dialog appears.*
4. *Click* **Choose***.*
5. *Select the directory in which the software files are located.*
6. *Click* **OK** *to confirm.*
7. *Check whether the right software files are shown in the list. If necessary, change the assignment of the software files to the TPG by right-clicking the TPG.*
8. *If one single password is used for all TPG, select* **Use this password** *and enter the password.*
9. *Click* **Start update***.*
10. *Confirm the security query.*

↳ The update is executed. The TPGs are restarted.

9.4 How to Restart the TPG

Some situations make it necessary to restart the TPG.

What do you want to do?

□ 'Restarting the TPG using the TPG Homepage' ⇨🗎102

□ 'Restarting the TPG via the InterCon-NetTool' ⇨🗎102

Restarting the TPG using the TPG Homepage

Proceed as follows:

1. *Start the TPG Homepage.*
2. *Select* **Actions – Restart**.
3. *Click* **Restart TPG**.

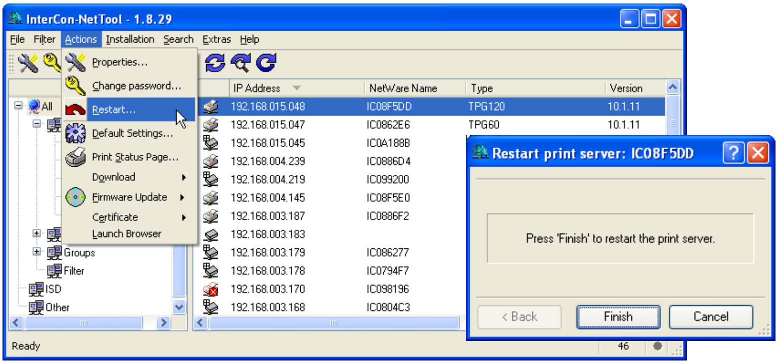
↳ The TPG is restarted.

Restarting the TPG via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Mark 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.



IP Address	NetWare Name	Type	Version
192.168.015.048	IC08F5DD	TPG120	10.1.11
192.168.015.047	IC0862E6	TPG60	10.1.11
192.168.015.045	IC0A188B		
192.168.004.239	IC0886D4		
192.168.004.219	IC099200		
192.168.004.145	IC08F5E0		
192.168.003.187	IC0886F2		
192.168.003.183			
192.168.003.179	IC086277		
192.168.003.178	IC0794F7		
192.168.003.170	IC098196		
192.168.003.168	IC0804C3		

Press 'Finish' to restart the print server.

Fig. 12: InterCon-NetTool - Restart

10 Appendix

The appendix contains a glossary, the TPG parameter list, and the index lists.

What information do you need?

10.1 Glossary

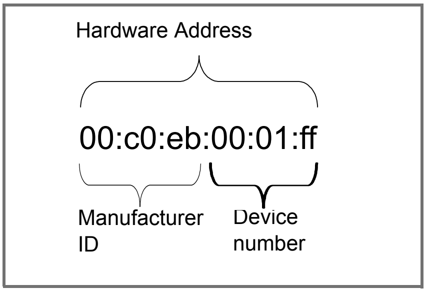
The glossary contains terms from the world of network technology.

What information do you need?

- 'Hardware Address' ⇨🗎104
- 'TPG Default Name' ⇨🗎105
- 'IP Address' ⇨🗎105
- 'Host Name' ⇨🗎106
- 'Gateway' ⇨🗎106
- 'Subnet mask' ⇨🗎106

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.



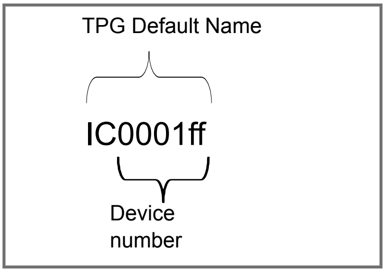
The hardware address is found on the housing, the TPG Homepage, the InterCon-NetTool, or the status page.

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

TPG Default Name

The TPG name 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 TPG default name is found on the TPG Homepage, the InterCon-NetTool, or the status page.

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.

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.

Gateway

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 Homepage or the InterCon-NetTool.

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 subnetwork, you can configure the relevant parameter via the TPG Homepage or the InterCon-NetTool.

10.2 Parameter List

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

What information do you need?

- 'Parameter List - General' ⇨🗎108
- 'Parameter List - ThinPrint®' ⇨🗎108
- 'Parameter List - TCP/IP' ⇨🗎111
- 'Parameter List - DNS' ⇨🗎113
- 'Parameter List - SNTP' ⇨🗎113
- 'Parameter List - Protection' ⇨🗎114
- 'Parameter List - EAP Authentication' ⇨🗎115
- 'Parameter List - Dynamic Update' ⇨🗎116

To view the current parameter values of your TPG, see: 'How to Print a Status or Service Page' ⇨🗎37.

Table 8: Parameter List - General

Parameters	Value	Default	Description
info_txt [Dealer]	64 characters [a-z, A-Z, 0-9, _, -]	[blank]	Freely definable description of the dealer or supplier.
info_url [Dealer URL]	64 characters [a-z, A-Z, 0-9, _, -]	[blank]	Freely definable description of the URL of a dealer or supplier.

language
[TPG language]
	en = English
	de = German
	fr = French
	es = Spanish
	it = Italian
	pt = Portuguese
	jp = Japanese
	cn = Chinese simplified
	zh = Chinese traditional
	kr = Korean
		en	Defines the language of the TPG.

sp_mode [Status page mode]	ASCII PostScript DATAMAX Citizen-Z	ASCII	Defines the data format in which the status page is printed.
eth_conf [Ethernet-Settings]	0 = Auto 1 = 10BaseT/FL HALF 2 = 10BaseT/FL FULL 3 = 100BaseTX/FX HALF 4 = 100BaseTX/FX FULL	0	Defines the network speed of the TPG. *'Auto' means that the network speed is recognized automatically. If the speed is set manually, it must be adapted to the other network devices.*

Table 9: Parameter List - ThinPrint®

Parameters	Value	Default	Description
tp_port [ThinPrint® Port]	1 - 65535 [5 characters, 0-9]	4000	Defines the ThinPrint® port number.
tp_clientid [Client ID]	0 - 2147483647 [10 characters, 0-9]	0	Defines the client ID as stored in the database of the Connection Service.

Parameters	Value	Default	Description
tp_authkey [Authentication key]	0 - 2147483647 [10 characters, 0-9]	0	Defines the authentication key as stored in the database of the Connection Service.
tp_bandwidth [Bandwidth]	on/off	off	Enables/disables the bandwidth value of the ThinPrint® port (client side).
tp_bandwidthval [Bandwidth]	1600 - 1000000 [7 characters, 0-9]	25600	Defines the bandwidth in bit/second (bit/s) used to decrease the bandwidth limit on the ThinPrint® port (client side).
tp_conservice [Connection Service]	on/off	off	Enables/disables the .print Connection Service.
tp_conserver [Connection Server]	valid IP address	000.000.000.000	Defines the IP address of the server on which the Connection Service is installed.
tp_conport [Port]	1 - 65535 [5 characters, 0-9]	4001	Defines the port number used by the TPG60 to communicate with the Connection Service.
tp_retry [Connection retry] versuch]	5 - 6000 [4 characters, 0-9]	120	Defines the interval (in seconds) for connection retries if the Connection Service is not reachable.
tp_keepalive [Keep alive]	30 - 180 [3 characters, 0-9]	60	Defines the interval (in seconds) for refreshing the connection to the Connection Service. *The value has to be lower or equal than the 'KeepAliveTO' parameter of the .print Connection Service (server side).*

Parameters	Value	Default	Description
tp_prtotoval [Printer open timeout]	0 - 86400 [5 characters, 0-9]	0 = off	Defines 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 freed up for subsequent print jobs, for example.*
tp_job_sdtmout [Job send timeout]	0 - 86400 [5 characters, 0-9]	0 = off	Defines 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).*

spage_printer
[Status page printer]
	TPG60 = 1-6
	TPG120 = 1-12
		1	Defines the ID of the status page printer.

tp1_printer_name ~ tp12_printer_name [Printer]	max. 32 characters [a-z, A-Z, 0-9, _, -]	[blank]	Freely definable description (of the printer name)
tp1_printer_class ~ tp12_printer_class [Class]	max. 7 characters [a-z, A-Z, 0-9]	[blank]	Defines the printer class. *Printers with compatible drivers can be arranged in one class.*
tp1_printer_driver ~ tp12_printer_driver [Driver]	max. 64 characters [a-z, A-Z, 0-9, _, -]	[blank]	Defines the printer driver.
tp1_remote_ip ~ tp12_remote_ip [Remote address]	max. 128 characters [.,0-9,A-Z,a-z]	[blank]	Defines the IP address or host name of the printer.
tp1_remote_port ~ tp12_remote_port [Port]	1 - 65535 [5 characters, 0-9]	9100	Defines the printer port. *Is used when socket printing was selected as transfer method between the TPG and the printer.*

Parameters	Value	Default	Description
tp1_remote_queue ~ tp12_remote_queue [Port]	max. 64 characters	lp1	Defines the LPD Queue name. *Is used when the LPD protocol was selected as transfer method between the TPG and the printer.*
tp1_remote_lpd ~ tp12_remote_lpd	on/off	off	Specifies the transfer method between the TPG and the printer: - on = LPD protocol - off = Socket
monitor_ping [Monitoring via ping]	on/off	on	Enables/disables a periodical 'ping' query to the remote addresses of the assigned printers. *The 'ping' query allows you to view status information about the printer connection.*
monitor_snmp [Monitoring via SNMP]	on/off	on	Enables/disables a periodical 'snmp' query to the remote addresses of the assigned printers. *The 'snmp' query allows you to view printer messages.*
monitor_poll [Monitoring interval]	1 - 6000 [4 characters, 0-9]	20	Defines the interval of an 'snmp' or 'ping' query in seconds.

Table 10: Parameter List - TCP/IP

Parameters	Value	Default	Description
ip_addr [IP Address]	valid IP address	000.000.000.000	Defines the IP address of the TPG.
ip_mask [Subnet mask]	valid IP address	depends on the IP address	Defines the subnet mask of the TPG.
ip_gate [Gateway]	valid IP address	000.000.000.000	Defines the gateway address of the TPG.
ip_dhcp [DHCP]	on/off	off	Enables/disables the DHCP protocol.

Parameters	Value	Default	Description
ip_bootp [BOOTP]	on/off	off	Enables/disables the BOOTP protocol.
ip_auto [ARP/PING]	on/off	on	Enables/disables the IP address assignment via ARP/PING.
ip_set_by [IP Address]	0 = Unknown 1 = SNMP 2 = BOOTP 3 = DHCP 4 = PING 5 = not defined 6 = ZeroConf 7 = 'parameters' file 8 = not defined 9 = not defined 10 = not defined 11 = not defined 12 = HTTP	[blank]	Shows the applied method for the IP address assignment.
ip_auto_gate [Multicast router as gateway]	on/off	on	Enables/disables the automatic entry of a found multicast router as gateway address. *If disabled, the gateway address has to be entered manually.*
ip_zconf [ZeroConf]	on/off	on	Enables/disables the automatic verification of an IP address conflict via ZeroConf. *ZeroConf describes a procedure for the automatic assignment of IP addresses.*
bonjour [Bonjour]	on/off	on	Enables/disables the Bonjour service.
sys_name [Host name]	max. 64 characters	[Default name]	Defines the host name of the TPG.
sys_descr [Description]	max. 128 characters	[blank]	Freely definable description (of the TPG)
sys_contact [Contact person]	max. 64 characters	[blank]	Freely definable description (of the contact person)
sys_location [Location]	max. 64 characters	[blank]	Freely definable description (of the device location)

Table 11: Parameter List - DNS

Parameters	Value	Default	Description
dns [DNS]	on/off	on	Enables/disables the name resolution via a DNS server.
dns_domain [Domain name]	max. 255 characters	[blank]	Defines the domain name of an existing DNS server.
dns_primary [Primary DNS server]	valid IP address	000.000.000.000	Defines the IP address of the primary DNS server.
dns_secondary [Secondary DNS server]	valid IP address	000.000.000.000	Defines the IP address of the secondary DNS server. *The secondary DNS server is used if the primary DNS server is not available.*

Table 12: Parameter List - SNTP

Parameters	Value	Default	Description
sntp [SNTP]	on/off	on	Enables/disables the use of a time server.
sntp_server [Time server]	max. 255 characters	[blank]	Defines a time server via the IP address or the domain name. *The domain name can only be used if a DNS server was configured beforehand.*
time_zone [Time zone]	UTC, GMT, EST, EDT, CST, CDT, MST, MDT, PST, PDT, etc.	GMT	Compensates for the difference between the time received via a time server and the local time zone.

Table 13: Parameter List - Protection

Parameters	Value	Default	Description
passwd [Password]	max. 16 characters	[blank]	Defines the password for the authorization to change TPG parameters. *If a password was set, you must enter the password before you can save the changes to the parameters.*
access_control [Access control]	on/off	off	Enables/disables the password demand for TPG parameters. *This parameter only makes sense if a password was set at an earlier stage; see above.*
ip1_sender ~ ip8_sender [IP sender]	max. 255 characters	*	Defines the IP address or host name of the client that is authorized to address the TPG in the network. *Once an IP sender has been defined, all undefined clients lose their authorization. Up to eight IP senders can be specified. The use of wildcards (*) is possible to authorize subnetworks, for example.*
http [HTTP]	on/off	on	Enables/disables the HTTP protocol on the TPG. *If the HTTP protocol is disabled, those functions that are based on the protocol will not be available (e.g. the TPG Homepage cannot be started).*
ftp [FTP]	on/off	on	Enables/disables the FTP/FTPS protocol on the TPG.

Table 14: Parameter List - EAP Authentication

Parameters	Value	Default	Description
eap_auth_type [Authentication]	1 = not defined 2 = not defined 3 = EAP-MD5 4 = EAP-TLS 5 = EAP-TTLS 6 = PEAP 7 = EAP-FAST	1	Defines the authentication method applied by the TPG to identify itself in the network.
eap_auth_name [User name]	max. 64 characters	[blank]	Defines the name of the TPG as saved in the authentication server (RADIUS).
eap_auth_pwd [Password]	max. 64 characters	[blank]	Defines the password of the TPG as saved in the authentication server (RADIUS).
eap_auth_ anonymous_name [Anonymous name]	max. 64 characters	[blank]	Defines the anonymous name for the unencrypted part of the EAP authentication methods TTLS, PEAP, and FAST.
eap_auth_intern [Inner Authentication]	0 = none 1 = MSCHAP 2 = MSCHAPv2 3 = PAP 4 = CHAP 5 = EAP-MD5 6 = EAP-MSCHAP 7 = EAP-MSCHAPv2 8 = EAP-TLS	0	Defines the kind of inner authentication for the EAP authentication methods PEAP and TTLS.
eap_auth_extern [PEAP/EAP-FAST Options]	0 = none 1 = PEAP LABEL0 2 = PEAP LABEL1 3 = PEAP V0 4 = PEAP V1 5 = FAST INLINE PROVISIONING	0	Defines the kind of external authentication for the EAP authentication methods PEAP and FAST.

Table 15: Parameter List - Dynamic Update

Parameters	Value	Default	Description
dyn_update [Dynamic firmware update]	on/off	off	Enable/disables the dynamic update.
dyn_update_url [Update URL]	max. 255 characters	[blank]	Defines the location of the files needed for the dynamic update.
dyn_proxy [Use proxy server]	on/off	off	Enables/disables the use of a proxy server for the dynamic update.
dyn_proxy_ur [Proxy server]	max. 255 characters	[blank]	Defines the URL of the proxy server used for the dynamic update.

10.3 List of Figures

10.4 Index