Tally
DASCOM

7106 7206 7010   Print Server Manual

Printer Server Manual for LAN (043941) and WLAN (043942) interfaces of the 7106, 7206 and 7010 series

Table of Contents

1 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 print server and how to operate the device properly.

What information do you need?

- '... about Your Print Server' ⇨▤7
- '... about the Documentation' ⇨▤10
- '... about Your Safety' ⇨▤13
- '... about a Fast Operational Readiness' ⇨▤14

1.1   ... about Your Print Server

Purpose

Print servers are active network components that receive print jobs from connected users or user groups within a network and forward them to printers or other end devices.

Features

Your print server offers you high performance, high data transfer rates, various management options and comprehensive support of operating systems and protocols.

- Highest data rates (depending on print server and printer model)
- Installation wizards for all major operating systems
- Administration via Browser
- Support of many management tools of well-known manufacturers
- Automatic printer error notification via email (SMTP) or SNMP Traps
- Transparent job history for optimal monitoring
- Status and diagnostics information via push button

- Comprehensive security options:
  - access protection,
  - encryption,
  - authentication via certificates etc.
  - Internet Protocol Security (IPsec)

- Remote administration via email (POP3):
  - sending of emails to printers,
  - request of service and status information,
  - setting of parameters,
  - printing of attachments, etc.

- Printer panel support (depending on printer model)

- Enhanced update functionality:
  simultaneous update of several print servers
  - automated updates when a new update file is available

- Implementation of filters via logical printers

- Assignment of IP addresses without DHCP server via IPv6 and ZeroConf

- Integrated ThinPrint client for bandwidth-friendly compression of print jobs in SBC environments including decryption of encrypted print data via SSL

Supported Administration Methods

- PRINTSERVER-NetTool for Windows

- Installation wizards for IP, and Wireless

- Windows Printer Wizard

- Browser (HTTP, HTTPs, HTML)

- SNMP

- Internet Print, NDPS Gateway, Web Manager, Status Monitor 2 and 3, WinAssist

- FTP/FTPs

Supported Systems	• Windows 95, 98, Me, NT3.x, NT4.x, 2000, XP, Vista, 7
Supported Printing Methods	• LPR/LPD Printing, Socket Printing, IPP v1.1 • HTTP/HTTPS Printing • ThinPrint Printing • NetBIOS/SMB Printing
Supported Network Protocols	• TCP/IP DHCP, BootP, ARP, IPv4, IPv6, IPv6/FTP, IPv6/FTPs, IPv6/TFTP, IPv6/HTTP-HTTPs, IPv6/SSL-TLS, IPv6/Raw TCP, TCP, UDP, ICMP, IGMP, FTP, FTPs, TFTP, LDP, HTTP, HTTPs, ZeroConf, DNS, SLP, SNMPv1, SNTP, SMTP, POP3, SSL/TLS, IPPv1.0, IPPv1.1, Raw TCP compatible • Windows SMB/CIFS (NetBIOS over TCP/IP) WINS

1.2   ... about the Documentation

Structure of the Documentation

The print server documentation consists of the following documents:

User Manual
Detailed description of the print server installation, configuration, and administration

Installation Guide for Wireless LAN
Information about how to install WLAN

If there is no documentation included in the delivery, please consult your retailer or printer manufacturer.

Scope and Content

This documentation describes a variety of print server models. This means that features will be described that may not be applicable to your print server. Information about the features of your print server can be found in the data sheet of your print server model.

Your print server offers a variety of administration methods; see: ⇨ 📄 24. The administration via the PRINTSERVER Homepage and the PRINTSERVER-NetTool is described in a complete and detailed way. The other administration methods describe the concept that you can use to configure your print server.

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. The glossary provides an overview of technical matters and background information; see: ⇨ 📄 202.

Symbols and Conventions

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

Table 1: Symbols and Conventions used in the Documentation

Symbol / Convention	Description
Warning	A warning contains important information that must be heeded. Non-observance may lead to malfunctions.
Note	A notice contains information that should be heeded.
Proceed as follows: *1. 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 ... about 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.

The manufacturer 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

Print servers are network interfaces for printers. They are designed for the direct integration of printers into networks. The print server has been designed for use in office environments.

Improper Use

All uses of the device that do not comply with the print server 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 print server, please note the safety regulations in the 'Hardware Installation Guide'. The Hardware Installation Guide is enclosed in the packaging. If there is no documentation included in the delivery, please consult your retailer or printer manufacturer.

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!

1.4 ... about a Fast Operational Readiness

In order to install your print server, you will need various data and parameters. This section provides the necessary information that you need to operate your print server.

Proceed as follows:

1. *Read and observe the security regulations in order to avoid damages to people and devices; see: ⇨🗎13.*
2. *Carry out the hardware installation. The hardware installation comprises the connection of the print server to the network and the mains supply as well as the installation into an external device (in the case of network interface cards).*
3. *Make sure that an IP address is stored in the print server; see: 'Saving the IP Address in the Print Server' ⇨🗎15.*
4. *Carry out the software installation in accordance with your network environment; see: 'Print Server Installation' ⇨🗎40.*

↳ The print server is operational.

2 Saving the IP Address in the Print Server

TCP/IP network protocols require the storing of the IP address in the print server so that the device can be addressed within the network. This chapter describes the various methods of IP address assignments.

Why IP Addresses?

An IP address is used to address network devices in an IP network. The address is required for sending and receiving data in an network.

Depending on the network type the print server can also be addressed via alternative parameters such as the host name or the print server name.

How Does the Print Server Obtain IP Addresses?

The print server is able to assign itself an IP address during the initial installation. Boot protocols are used to assign an IP address automatically to the print server. Upon delivery, the boot protocols 'BOOTP', 'DHCP', and 'ZeroConf' are enabled.

Once the print server 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 print server assigns itself an IP address via ZeroConf from the address range (169.254.0.0/16) which is reserved for ZeroConf.

Once the print server has automatically received an IP address via a boot protocol, you can save a freely definable IP address in the print server.

If you want to assign an IP address to a print server that supports WLAN; see: ⇨ 📄188. To use IPv6 addresses; see: ⇨ 📄194.

The different methods for the assignment of the IP address (automatically and manually) are described in the following.

Automatic Methods of IP Address Assignments

- '... via ZeroConf' ⇨ 🖹16
- '... via BOOTP' ⇨ 🖹17
- '... via DHCP' ⇨ 🖹18
- '... via Auto Configuration (IPv6 Standard)' ⇨ 🖹20

Manual Methods of IP Address Assignments

- '... via the IP Wizard (PRINTSERVER-NetTool)' ⇨ 🖹21
- '... via ARP/PING' ⇨ 🖹22

2.1　… via ZeroConf

ZeroConf

ZeroConf describes the automatic assignment of IP addresses within a network.

Requirements

☑ The 'ZeroConf' parameter has been activated; see: 'TCP/IP' ⇨ 🖹167.

What Happens When the Print Server is Turned on?

If no IP address can be assigned via boot protocols, the print server assigns itself an IP address via ZeroConf. For this purpose, the print server 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 print server will receive a message. The print server then sends another query with a different IP address. If the IP address is available, it is saved in the print server.

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 print server later on.

What Happens When the Print Server is Turned on?

The print server repeats the same procedure (see ZeroConf) for the service name. The service name consists of the default print server name and the name of the connected printer. The print server will then start the printing process and an HTTP service and advertises both services in the network. The print server is now visible in the network and the printing process can begin.

Integration of the Printer Server in Other Networks

In many cases, the print server is to be integrated into the actual network after the automatic configuration in the 169.254.0.0/16 segment.

2.2 ... via BOOTP

The print server supports BOOTP, which means that the IP address of the print server can be assigned via a BOOTP server. If the BOOTP boot protocol has been installed in your network, you must edit the '/etc/bootptab' file. This file is located on the host running the BOOTP daemon. The '/etc/bootptab' file contains a permanent copy of the assignment of the host name and the IP address to the hardware address.

Requirements

☑ The 'BOOTP' parameter has been activated; see: 'TCP/IP' ⇨ 🖹167.

What Happens When the Print Server is Turned on?

Once the print server has been turned on, it asks the BOOTP 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 print server.

What Happens When Printing?

During the installation of the print server, its host name is displayed on the monitor of the computer intended for printing. The computer finds the IP address of the print server by means of either the local 'etc/hosts' file or the DNS server. The print data can then be sent to this IP address.

2.3 ... via DHCP

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

In networks with DHCP servers, the dynamic name registration is done by DNS servers, which can be dynamically configured by the DHCP server. Most systems additionally use a WINS server, which answers name enquires that the DNS server cannot handle.

The print server does not support DHCPv6.

Requirements

☑ The 'DHCP' parameter has been enabled; see: 'TCP/IP' ⇨ 🖹167.

☑ The parameter 'WINS registration' has been enabled; see ⇨ 🖹170.

☑ The parameter 'WINS via DHCP' has been enabled; see ⇨ 🖹170.

What Happens When the Print Server is Turned on?

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

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

The print server now transmits a name registration request to the WINS server, along with the IP address and host name assignment. The answer from the WINS server contains the period of validity of the name entry in the WINS database. Once this period has expired, the print server renews its registration with the WINS server so that its IP address and host name remain constantly valid.

What Happens When Printing?

During the installation of the print server, its host name is displayed on the monitor of the computer intended for printing. In order for you to be able to assign the host name to the IP address, the computer asks the DNS server for the IP address of the print server. If the DNS server cannot answer this request, it forwards the request to the WINS server. Once the computer receives the answer, it sends the print data to the IP address of the print server.

You can also enter the IP address instead of the host name during the print server installation. In this case, you can send print data directly to the IP address. The configuration of a print server on a DHCP server depends on the operating system.

WINS Without DHCP

You can set up the print server in a network only with WINS and without DHCP. In this case, the print server registers with the WINS server directly. In this process, you must configure the IP address of the WINS server manually in the print server.

Requirements

To use WINS without DHCP, the following requirements are necessary:

☑ The 'DHCP' parameter has been disabled; see: 'TCP/IP' ⇨🖹167.

☑ The parameter 'WINS registration' has been disabled; see ⇨🖹170.

☑ The parameter 'WINS via DHCP' has been disabled; see ⇨🖹170.

2.4　… via Auto Configuration (IPv6 Standard)

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

What Happens When the Print Server is Turned on?

The IPv6 standard uses the following mechanism to assign IP addresses automatically. When the print server is started in an IPv6 network, the print server will be addressed via an automatically generated address from the link-local address range (FE8 ...).

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

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

Requirements

☑ The 'IPv6' parameter has been activated.

☑ The 'Automatic configuration' parameter has been activated.

2.5 ... via the IP Wizard (PRINTSERVER-NetTool)

The IP Wizard of the PRINTSERVER-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 print server using the IP Wizard.

Requirements

☑ The PRINTSERVER-NetTool is installed on the client; see: ⇨🗎27.

☑ The network scan via Multicast has been enabled in the PRINTSERVER-NetTool; see: ⇨🗎32.

☑ The router in the network forwards multicast requests; see: ⇨🗎32.

📂 Proceed as follows:

1. Start the PRINTSERVER-NetTool.

2. Select the print server from the print server list.
The print server is displayed in the print server 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.
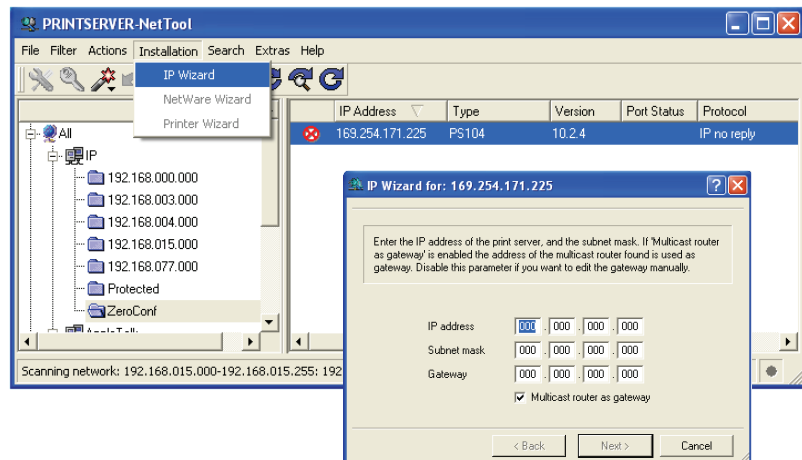
Fig. 1: PRINTSERVER-NetTool - IP Wizard

2.6 ... via ARP/PING

ARP Table

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 print server. If the print server 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.

Use the 'arp' and 'ping' commands to save the IP address if your network has no superordinate management of IP addresses (e.g. DHCP, BOOTP).

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 print server. If the data packet has been successfully sent and received, the print server permanently saves the IP address.

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

Requirements

☑ The 'ARP/PING' parameter has been enabled; see: 'TCP/IP' ⇨ 🖹167.

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 print server:
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.

Troubleshooting   The 'Addition failed' error occurs when you use the 'arp' command. This error informs you that the ARP table is empty and that the new entry cannot be added. This problem occurs with certain operating systems such as all Microsoft Windows versions with the exception of NT 4.0. The solution to the problem is to ping a station in the network before using the 'arp' command for the first time or use the PRINTSERVER-NetTool to enter the IP address.

3 Print Server Administration

> You can administer and configure the print server 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.

3.1 ... via the PRINTSERVER Homepage

Functionalities

The PRINTSERVER Homepage supports all features for the administration of the print server.

The PRINTSERVER Homepage is stored in your print server and can be started by means of an Internet browser (Internet Explorer, Firefox). When using other browsers, the full functionality of the PRINTSERVER Homepage cannot be guaranteed.

Requirements

☑ The print server is connected to the network and the printer.

☑ The print server is known to the network via its IP address; see: ⇨ 🖹15.

What information do you need?

📋 Proceed as follows:

1. Open your browser.
2. Enter the IP address of the print server as the URL.

↳ The **PRINTSERVER Homepage – Home** appears.

Fig. 2: PRINTSERVER Homepage - Home

The appearance of the PRINTSERVER Homepage depends on the print server model and software version. If the PRINTSERVER Homepage is not displayed, check the proxy settings of your browser.

Structure of the PRINTSERVER 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 PRINTSERVER Homepage via **General – Home**. Simply select the relevant flag.

All other menu items refer to the configuration of the print server and are described in this manual.

3.2   … via the PRINTSERVER-NetTool

The software PRINTSERVER-NetTool has been developed for the administration of network devices. Depending on the network device you can configure various features via the PRINTSERVER-NetTool.

—————— ⚙ ——————

Information about the device functions can be found in the relevant chapters in this documentation.

The PRINTSERVER-NetTool has been designed for use in Windows networks. The software is installed on all clients that are meant to access a network device in the network.

Basic Functions

After the PRINTSERVER-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 'print server list'.

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

Installation and Program Start

In order to use the PRINTSERVER-NetTool, the program must be installed on a computer with Windows operating system. Different installation files are available, depending on the operating system. You will find the PRINTSERVER-NetTool installation files on the PRINTSERVER LIBRARY CD.

If there is no PRINTSERVER LIBRARY CD included in the delivery, please consult your retailer or printer manufacturer.

Windows

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

📋 Proceed as follows:

1. *Start the PRINTSERVER-NetTool installation file.*
2. *Select the desired language.*
3. *Follow the installation routine.*
✤ The PRINTSERVER-NetTool is installed on the system.

To start the program, double-click the PRINTSERVER-NetTool icon. The icon is found on the desktop and the Windows start menu.
(Start --> Programs --> Smart Network Utilities--> PRINTSERVER-NetTool)

The program settings are saved in the 'PRINTSERVER-NetTool.ini' file. The file is stored in the directory 'Documents and Settings' with the relevant user name. (Only for multi-user operating systems)

Structure of the PRINTSERVER-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.
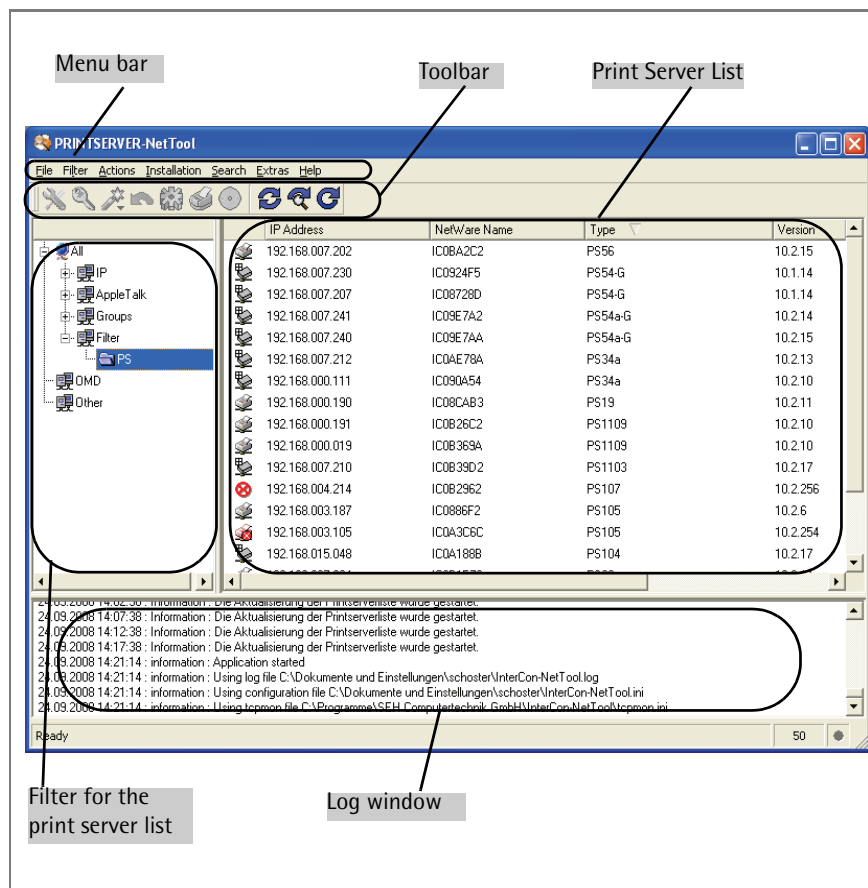
Fig. 3: PRINTSERVER–NetTool - Main Dialog

The functions of the program elements will be described in the following. Detailed information on how to use the program can be found in the PRINTSERVER–NetTool Online Help.

Toolbar   A toolbar with various commands is available in the PRINTSERVER-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	Starts a Wizard. A wizard helps you to configure certain parameters.
	Restart	This opens the 'Restart' dialog.*
	Default settings	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 print server list.
	Find New	Adds newly connected network devices to the print server list.
	Rebuild	Creates a new print server list.

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

Print Server List   All connected devices are shown in a list in the right-hand section of the main dialog of the PRINTSERVER-NetTool. This section is referred to as the print server list.

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

The print server 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 print server list. The filters can be created and configured via the **Filter** menu.

You can modify the status of the print server 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 print server list will be refreshed automatically in a fixed time interval. Select **Extras – Settings** from the menu bar (category: Auto Refresh).

You can save the print server 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 PRINTSERVER-NetTool searches the network for existing print servers and displays them in the print server list. The following search options can be selected for the network scan:

- Searching via multicast requests (TCP/IP)
- Searching within defined IP ranges (TCP/IP)

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 PRINTSERVER-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 Print Server Parameters

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

Configuration via the 'Properties' Dialog

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

Configuration via Wizards

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

Depending on the print server model and network, you can choose from the following wizards:

IP Wizard	The IP Wizard helps you to configure the TCP/IP parameters, e.g. the IP address. You can choose between the manual configuration and the automatic configuration via boot protocols. The IP Wizard is not available for WLAN print servers.
Wireless Wizard	The Wireless Wizard helps you to install WLAN print servers. The Wireless Wizard helps you to configure TCP/IP and WLAN parameters and the details about encryption and authentication. The Wireless Wizard is only available for WLAN print servers.
PRINTSERVER Printer Wizard	The PRINTSERVER Printer Wizard is available for installing the print server in Windows networks. This PRINTSERVER Printer Wizard helps you to install a print server connected to a printer.

Mark the print server in the print server list and start the required wizard via the **Installation** menu.

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.

3.3 ... via the FTP/FTPS Connection

FTP

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

FTP over SSL

The print server also supports FTPS (FTP over SSL) for a safe data interchange between the print 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.

Functionalities

An FTP/FTPS connection allows the following:

- Printing a Status Page; see: ⇨ 🗎61
- Printing a Service Page; see: ⇨ 🗎147
- Configuring Print Server Parameters; see: ⇨ 🗎34
- Resetting Print Server Parameters; see: ⇨ 🗎153
- Querying the Printer Status; see: ⇨ 🗎133
- Performing Updates; see: ⇨ 🗎157

Requirements

☑ The 'TCP/IP' parameter has been activated; see: ⇨ 🗎167.

Configuring Parameters via an FTP Connection

You can configure all print server parameters via FTP. To this purpose, you must download the 'parameters' file to your local computer via FTP and then edit it. For additional information; see: ⇨ 🗎34.

🗂 Proceed as follows:

1. *Change to the directory in which you wish to save the file.*

---

2. *Open an FTP connection to the print server:*
   <u>*Syntax:*</u>   `ftp <IP Address>`
   <u>*Example:*</u> `ftp 192.168.0.123`

3. *Enter an arbitrary user name.*

4. *Enter the print server password or press ENTER if no password has been assigned.*

5. *Transfer the 'parameters' file from the print server to your local computer:*
   `get parameters`

6. *Edit the file using a text editor. The syntax and values can be obtained from the parameter list; see:* ⇨▤*209.*

7. *Send the file back to the print server:*
   `put parameters`

8. *Close the FTP connection:*
   `quit`

↳ The print server will be configured using the new values.

3.4   ... via the Print Server Operating Panel

On every print server you will find the network connectors, several LEDs, the status button and an optional power supply connector. These components are described in the 'Hardware Installation Guide'.

Functionalities   The status button of the print server allows the following

- Printing a Status Page; see: ⇨▤62

- Print a Service Page; see: ⇨▤146

- Resetting the Print Server Parameters to their Default Settings; see: ⇨▤154

3.5 ... via Email (Remote Management)

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

Functionalities

An email allows you to

- send print server information
- print emails and attachments
- perform an update on the print server or
- define print server parameters.

Requirements

☑ In order to receive emails, the print server must be set up as user with its own email address on a POP3 server.

☑ A DNS server has been configured on the print server; see: ⇨📄65.

☑ SMTP parameters can be configured on the print server; see: ⇨📄173.

☑ POP3 parameters are configured on the print server; see: ⇨📄172.

Sending Instructions via Email

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

📫 Proceed as follows:

1. *Open an email program.*
2. *Write a new email.*
3. *Enter the print server address as recipient.*
4. *Enter an instruction into the subject line; see: 'Syntax and Format of an Instruction' ⇨📄37.*
5. *Send the email.*
↳ The print server receives the email and carries out the instruction.

Syntax and Format of an Instruction

Note the following syntax for instructions in the subject line:
```
cmd: <command> [<port>] [ack] [<comment>]
```

The following commands are supported:

Commands	Option	Description
[<command>]	get statuspage get servicepage get parameters get jobhistory get pagecounter	sends the status page of the print server sends the service page of the print server sends the parameter list of the print server sends the Job History sends the number of printed pages
	set parameters	sends parameters to the print server Parameter changes are integrated into the email body with the following syntax: `<parameter> = <value>` The syntax and values can be obtained from the parameter list; see: ⇨ 📄209.
	print printa print attachment	prints the email (text only) prints the email attachment see: 'printa'
	update ps	carries out an automatic update using the update file that is attached to the mail
	clean mailqueue	cleans the email printer queue and deletes all entries from the mailbox
[<port>] *(optional)* *Default: LP1*		Defines the port used by print server models with several physical ports for sending data. If no port was defined, the default value LP1 will be used.
	LP1 LP2 LP3 LP4 LP5	- LPT1 or USB1 - LPT2 or USB2 - LPT3 or USB3 (connected via USB hub) - COM1 or USB4 (connected via USB hub) - USB5 (connected via USB hub)
[ack] *(optional)*	---	sends an acknowledgment back to the sender

The following applies for the commands:

- not case-sensitive
- one or more space characters are allowed
- max. length is 128 byte

Must be in ASCII format. Emails are printed in ASCII format. HTML or Rich Text formats are not supported. For a perfect text output of your emails and attachments, make sure that the text encoding of the printer corresponds to that of the email client.

Security If you want to change parameters or do an update for print servers that have a write protection (see: ⇨📄81), you also need a password. Enter the password into the first line of the email body. Note the following syntax:

```
password: <password>
```

If the print server is protected against unauthorized access by means of the IP sender control, the print server only accepts emails from IP addresses that are listed in the IP sender list. For information on how to define the IP sender list; see: ⇨📄82.

Example 1
This email causes the print server to send the parameter list to the sender of the email.
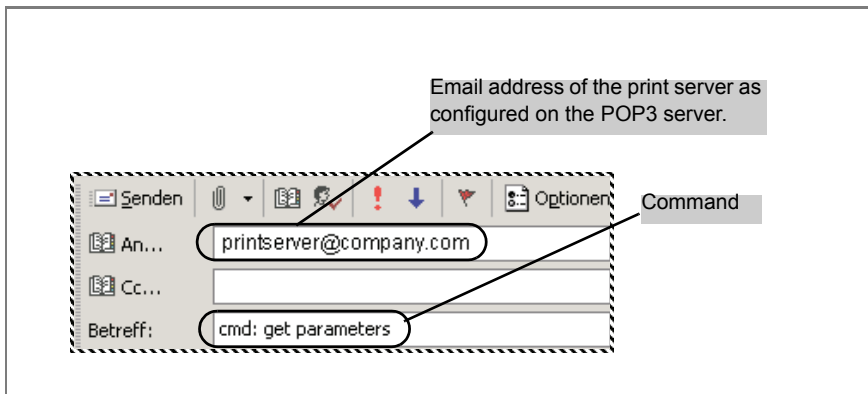
Fig. 4: Administration via Email – Example 1

Example 2
This email causes the printer that is connected to the port LPT2 or USB2 of the print server to print the attachment of the email. The sender also receives an acknowledgment of receipt by the print server.
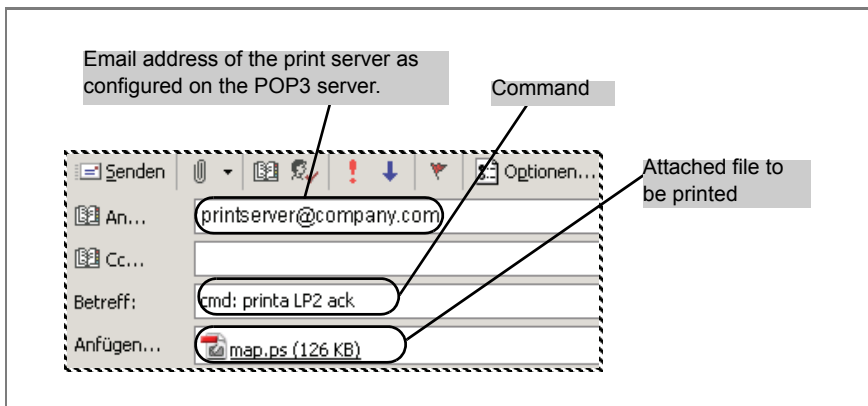
Fig. 5: Administration via Email – Example 2

4 Print Server Installation

Depending on the selected printing method, the print server can be integrated into various systems and networks. This chapter presents various printing methods and describes several installation procedures.

Depending on your printing requirements and your network environment, there are various installation methods.

The table shows the installation procedures that are described in this document. Select the installation procedure that meets your requirements and follow the information reference.

System	Printing Method	Information Reference
Windows (95/98/Me/NT 4.x /2000/XP/Vista/7)	Socket Printing	see: 'Installation in Windows Systems' ⇨ 📄42

Windows
'Print Server Installation in Windows (Socket Printing)' ⇨ 📄44

ThinPrint®
'Using the Print Server to Print compressed ThinPrint Data' ⇨ 📄184

IPv6
'Installing the Print Server in IPv6 Networks (LPD Printing)' ⇨ 📄194

4.1   Installation in Windows Systems

Depending on the selected printing method, the print server can be imbedded into Windows systems. This section presents various printing methods and describes several installation procedures.

Overview of Printing Methods

- The LPD protocol is used for printing in Windows NT 4.0 and NT 3.51 systems. The LPD protocol is a special protocol used for print data. During **LPD printing** the server sends the print data to the IP address of the print server by means of the LPR port. The print server receives the print data and routes it to the printer.

- In **Peer-to-Peer** networks all clients have the same rights and can share their resources with other computers. The print server acts as network connection for a printer which is independent of a client. The print data is transferred from the individual client to the network. The print server receives the print data and routes it to the printer. Peer-to-Peer printing via NetBIOS is supported by all Windows systems.

- The **Internet Printing Protocol** (IPP) provides printing services via a network. In a client/server system, such as Windows 7/Vista/XP/2000, the client sends a query to the print server. After transmission of the print data, the data is printed.

- During **socket printing**, the print server acts as network connection for a printer which is independent of a client. Printing is carried out by means of direct TCP/IP ports. The ports are installed with the aid of the PRINTSERVER Print Monitor (see ⇨ 📄45). The print data is transferred from the individual client to the network using the PRINTSERVER Print Monitor. The print server receives the print data and routes it to the printer.

Requirements ☑ The print server is connected to the network and the printer.

☑ The print server and the printer are turned on.

☑ The print server is known to the network via its IP address; see: ⇨🖹15.

Procedure Follow the instructions if you want to prepare the print server for socket printing in Windows systems.

☐ Installing the Print Server*

☐ Installing and Configuring the Printer*

☐ Installing the Printer Driver*

☐ Adding the Printer Port**

☐ Configuring the Printer Port**

* This step is carried out while the PRINTSERVER Printer Wizard is run.
** This step is carried out while the PRINTSERVER Print Monitor is run.

The tools PRINTSERVER Printer Wizard and PRINTSERVER Print Monitor help you to operate the print server quickly and easily. The supports 32-bit systems. If you want to install the print server on a 64-bit system, use the Windows default printer installation. Contact the manufacturer of your operating system for further information.

What do you want to do? ☐ 'Installing the Print Server using the PRINTSERVER Printer Wizard' ⇨🖹44

☐ 'Configuring the Printer Port using the PRINTSERVER Print Monitor' ⇨🖹45

Installing the Print Server using the PRINTSERVER Printer Wizard

What is the PRINTSERVER Printer Wizard?

The PRINTSERVER Printer Wizard is available for installing the print server in Windows systems. The PRINTSERVER Printer Wizard is a self-extracting program and carries out the following steps:

- Installing the PRINTSERVER Print Monitor on the Client
- Installing the Printer Driver
  If you use Windows Me/98/95 or NT4.0 you must install the required printer driver manually.
- Installing the Print Server
- Installing and Configuring the Printer
- Print a Test Page

How to Start the PRINTSERVER Printer Wizard

When you install the PRINTSERVER-NetTool (see: ⇨🗎27) the PRINTSERVER Printer Wizard will be provided automatically. The PRINTSERVER Printer Wizard can be started in the PRINTSERVER-NetTool via the 'Installation' menu.

If you do not use the PRINTSERVER-NetTool, the installation file can be copied and started the PRINTSERVER LIBRARY CD. If there is no PRINTSERVER LIBRARY CD included in the delivery, please consult your retailer or printer manufacturer. .

Use the installation file that corresponds to your operating system.

Operating Systems	Installation File
Windows 7 Windows Vista Windows XP Windows 2000 Windows NT4.0	printerwizard.exe
Windows ME Windows 98 Windows 95	printerwizard9x.exe

Configuring the Printer Port using the PRINTSERVER Print Monitor

As far as socket printing is concerned, a printer port must be added to every client intended for printing. This section describes the installation and configuration of TCP/IP and HTTP ports on the client. The PRINTSERVER Print Monitor is available for configuration purposes.

What is the PRINTSERVER Print Monitor?

The PRINTSERVER Print Monitor constitutes the connecting piece between the computer and the print server. It ensures the transfer of print data from the client to the print server by means of direct TCP/IP ports. The PRINTSERVER Print Monitor can be installed on every client intended for printing. It is not possible to share the printer.

Which Ports Are Available?

Using the PRINTSERVER Print Monitor you can adapt printing to your individual needs. You can define whether printing is done via a **TCP/IP port** or a **HTTP** port. The following features can be realized when printing via HTTP ports:

- Encryption of print data
- Identity check of the users and devices before they gain access to the print server (authentication)
- Using a proxy server, print jobs can be sent to a print server via the Internet
- Detailed and print server specific error messages

Procedure

In order to configure a printer port at the client, follow the instructions:

- ☐ 'PRINTSERVER Print Monitor' ⇨ 🖹47
- ☐ 'Starting the PRINTSERVER Print Monitor (no Print Object available)' ⇨ 🖹47
- ☐ 'Starting the PRINTSERVER Print Monitor (Print Object available)' ⇨ 🖹49
- ☐ 'Adding or Editing Printer Ports' ⇨ 🖹50

The following descriptions refer to the configuration in Windows XP. Depending on your Windows system, the menu navigation can vary.

PRINTSERVER Print Monitor

Automatic Installation

When the PRINTSERVER Printer Wizard is run (see: ⇨📄44), the PRINTSERVER Print Monitor will be installed automatically to your system.

The automatic installation is only carried out if the PRINTSERVER Printer Wizard was started via the PRINTSERVER LIBRARY CD.

Manual Installation

If the PRINTSERVER Print Monitor is not yet installed to your system or if you want to install a higher version of the PRINTSERVER Print Monitor, you can do this manually.

Proceed as follows:

1. *Double-click the file pmonitor-xxx.exe'.*
   The file can be copied and started from or the PRINTSERVER LIBRARY CD.
2. *Follow the installation routine.*
✎ The PRINTSERVER Print Monitor will be installed to your system.

Starting the PRINTSERVER Print Monitor (no Print Object available)

The PRINTSERVER Print Monitor is started by adding a new print object with a port.

Requirements

☑ The PRINTSERVER Print Monitor is installed on the client.

☑ The required printer drivers are installed on the client.

Proceed as follows:

1. *Click 'Start' > 'Settings' > 'Printers and Faxes'.*
2. *Select* **File – Add Printer** *from the menu bar.*
   The 'Add Printer Wizard' appears.
3. *Click* **Next**.
4. *Tick* **Local printer attached to this computer**.
5. *Click* **Next**.
6. *Tick* **Create a new port**.

Fig. 6: Windows – Add Printer Wizard

7. Select 'PRINTSERVER Print Monitor' from the **Type of port** *list.*
8. Click **Next**.
↳ The PRINTSERVER Print Monitor is started. The dialog **TCP/IP Port Configuration** appears.

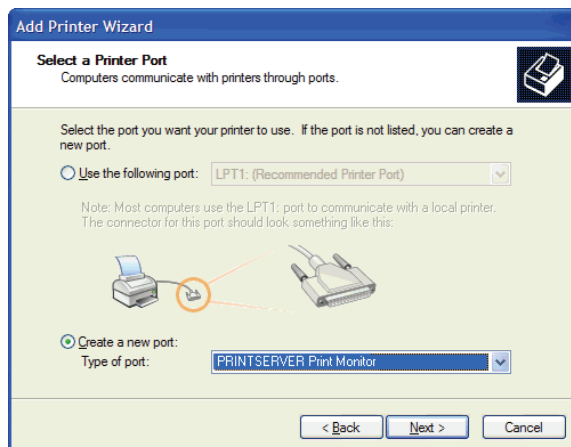If the print server is protected by a password, the password will be demanded; see ⇨📄81.
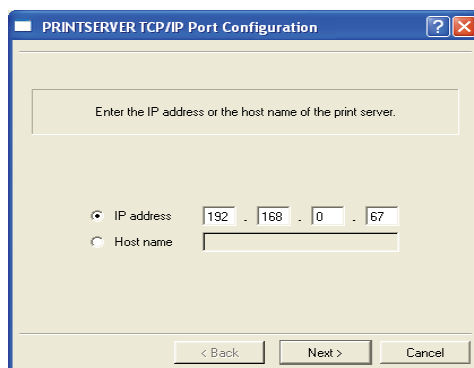
Fig. 7: PRINTSERVER Print Monitor – TCP/IP Port Configuration

Starting the PRINTSERVER Print Monitor (Print Object available)

The PRINTSERVER Print Monitor is started by adding a new port to the print object.

Requirements
☑ The PRINTSERVER Print Monitor is installed on the client.

☑ The print object is already available on the client.

Proceed as follows:

1. *Click 'Start' > 'Settings' > 'Printers and Faxes'.*
2. *Select the printer from the list.*
3. *Select* **File – Settings** *from the menu bar.*
   The **Properties** *dialog appears.*
4. *Select the* **Ports** *tab.*
5. *Click* **Add**.
   The **Printer Ports** *dialog appears.*
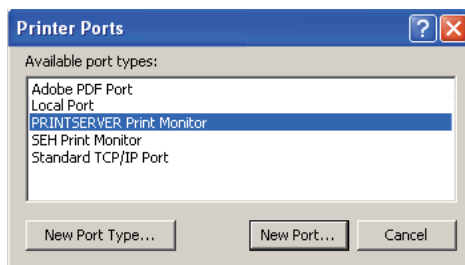
Fig. 8: Windows – Printer Ports

6. *Select PRINTSERVER Print Monitor.*
7. *Click* **New Port**.
↳ The PRINTSERVER Print Monitor is started. The dialog **TCP/IP Port Configuration** appears; see: ⇨▤48.

If the print server is protected by a password, the password will be demanded; see ⇨▤81.

Adding or Editing Printer Ports

Add a printer port to the client by means of the PRINTSERVER Print Monitor.

Adding a TCP/IP Printer Port

📑 Proceed as follows:

1. *Start the PRINTSERVER Print Monitor; see:* ⇨🗎*47.*
2. *Enter the IP address or the host name of the print server and click* **Next***. The following dialog appears:*

Fig. 9: PRINTSERVER Print Monitor – Selecting a Printing Method

3. *Tick* **Standard TCP/IP printing** *and click* **Next***. The following dialog appears:*
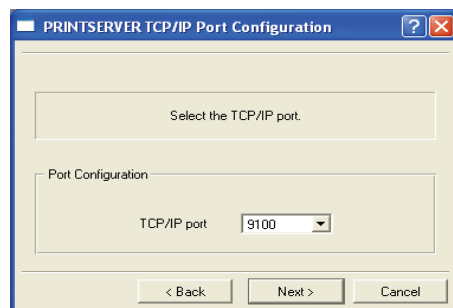
Fig. 10: PRINTSERVER Print Monitor - Port Configuration-TCP/IP

4. *Select a port number from the list and confirm by clicking* **Next**. *The following dialog appears:*

Different logical printers are addressed via the port number (9100 - 9107). The logical printer defines the printer port to which the print data is sent. This is relevant for print server models with several physical printer ports (COM1, USB1, etc.).

Fig. 11: PRINTSERVER Print Monitor – SNMP

5. *Tick* **SNMP monitoring** *in order to enable the reception of printer status messages.*

6. *Enter the following into the 'Community' box:*

If there is a write protection on the print server (see ⇨ 🗏 81), you must enter the password.
If there is no write protection on the print server, you must enter 'public'.

If there is a read protection on the print server (see ⇨ 🗏 81), the 'Community' box does not appear. When starting thePRINTSERVER Print Monitor you will be asked to enter a password. The password will be used as Community name within the SNMP communication.

7. *Click* **Next**. *The dialog that appears contains all entries.*

8. *Check your entries and click* **Finish**.

↳ The configuration is saved and the TCP/IP printer port is added to the client.

Adding an HTTP Printer Port

📑 Proceed as follows:

1. Start the PRINTSERVER Print Monitor; see: ⇨🖹47.

2. Enter the IP address or the host name of the print server and click **Next***. The following dialog appears:*
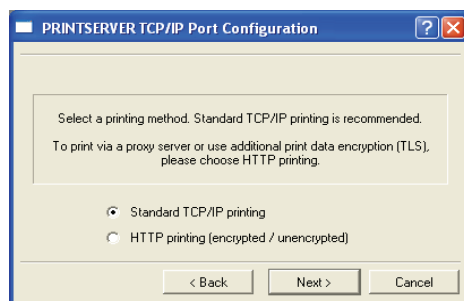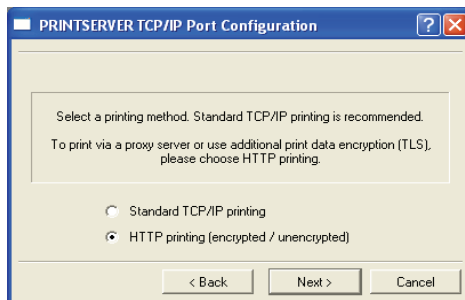

Fig. 12: PRINTSERVER Print Monitor – Selecting a Printing Method

3. Tick **HTTP printing** *and click* **Next***. The following dialog appears:*
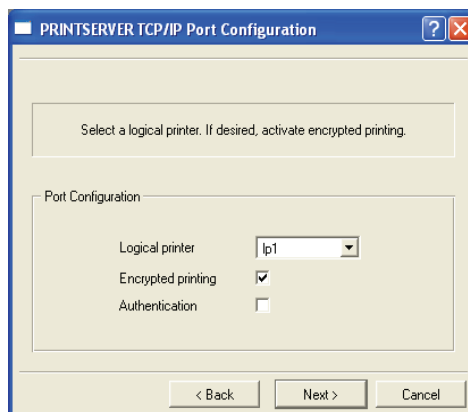
Fig. 13: PRINTSERVER Print Monitor - Port Configuration-HTTP

4. Select a logical printer (lp1 - lp8) from the list.
The logical printer defines the printer port to which the print data is sent. This is relevant for print server models with several physical printer ports (COM1, USB1, etc.).

5. Select **Encrypted printing** *if you wish to encrypt the print data; see: 'Encrypted Socket Printing (Windows)' ⇨🖹84.*

6. *Select* **Authentication**, *if necessary; see: 'Encrypted Socket Printing with Certificate Validation (Windows)'* ⇨📄*85.*

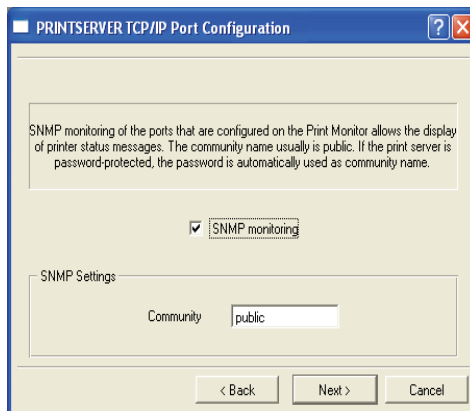7. *Click* **Next***. The following dialog appears:*
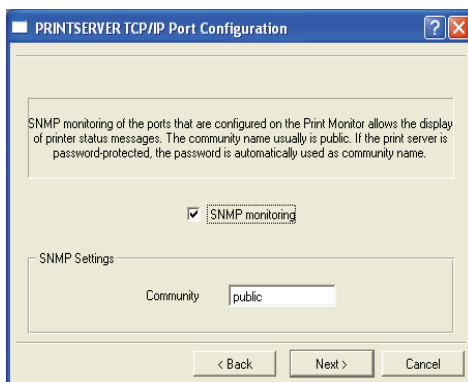
Fig. 14: PRINTSERVER Print Monitor – SNMP

8. *Tick* **SNMP monitoring** *in order to enable the reception of printer status messages.*

9. *Enter the following into the 'Community' box:*

**If there is a write protection on the print server (see ⇨📄81), you must enter the password.
If there is no write protection on the print server, you must enter 'public'.**

If there is a read protection on the print server (see ⇨📄81), the 'Community' box does not appear. When starting thePRINTSERVER Print Monitor you will be asked to enter a password. The password will be used as Community name within the SNMP communication.

10. *Click* **Next***. The following dialog appears:*
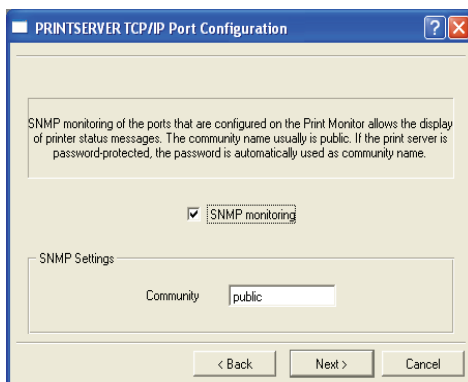
Fig. 15: PRINTSERVER Print Monitor – Proxy Server

11. *You can print via a proxy server. If necessary, tick **Use proxy** and enter the IP address and the port number of the proxy server.*

12. *Click **Next**. The dialog that appears contains all entries.*

13. *Check your entries and click **Finish**.*

↳ The configuration is saved and the HTTP printer port is added to the client.

Modifying an Existing Printer Port

You can modify the settings of a printer port.

📑 Proceed as follows:

1. *Click 'Start' > 'Settings' > 'Printers and Faxes'.*
2. *Select the printer from the list.*
3. *Select* **File – Settings** *from the menu bar.*
   The **Properties** *dialog appears.*
4. *Select the* **Ports** *tab.*
5. *Select the port from the list.*
6. *Click* **Configure**. *The dialog* **TCP/IP Port Configuration** *appears.*
7. *Configure the parameters; see: Table 3 ⇨▤ 55.*
8. *Click* **OK** *to confirm.*
↳ The settings are saved.

Table 3: Changing the Port Configuration

Parameters	Description
Time out	If an error occurs during the sending of the print job, the print job will automatically be sent again. You can limit the duration of this process by defining a time out (1 - 120 min). *This will prevent the process from being repeated endlessly and from blocking other connections.*
SNMP monitoring	Enables/disables the reception of printer status messages. *If parameter changes are controlled by a print server password, you must enter the password for the SNMP monitoring into the 'Community' box. If no password is used, you must enter 'public'.*
Authentication	Enables/disables the option 'Authentication'; see: 'Encrypted Socket Printing with Certificate Validation (Windows)' ⇨▤ 85.
Use proxy server	You can print via a proxy server. Tick 'Use proxy server' and enter the IP address and the port number of the proxy server.

5 Print Server Status Information

The print server can display status information. This chapter describes which status information is available and how to display and read this information.

5.1　How to Display Status Information

Print server status information can be displayed in many ways.

Displaying Status Information via the PRINTSERVER Homepage

📁 Proceed as follows:

1.　Start the PRINTSERVER Homepage.

2.　Select the desired menu item from the navigation bar in the **Status** *category.*

✎ The status information is shown.

Displaying Status Information via the PRINTSERVER–NetTool

📁 Proceed as follows:

1.　Start the PRINTSERVER-NetTool.

2.　Double-click the print server in the print server list. The **Properties** *dialog appears.*

3.　Select the desired menu item from the navigation bar in the **Status** *category.*

✎ The status information is shown.

5.2　Which Status Information Is Available?

This section gives an overview of the print server status information. Depending on the features supported by the print server model, different status information can be available.

General Status

The **General** page shows status information, such as the name of the print server, the hardware address, the serial and version numbers, network type etc. The text which you previously entered under 'Configuration – General' will now appear under 'Description.' A description is freely definable and can be used to gain a better overview of the print servers and printers in the system.

WLAN Status

The **WLAN** page contains information about the current WLAN settings.

- 'Connection Status' indicates the status of the network connection. The following statuses are possible:

    'Ad-Hoc', when the print server is working in the ad-hoc mode.

    'Infrastructure', when the print server is working in the infrastructure mode.

    'Out of range', when the print server is logged onto an access point in the infrastructure mode and this access point cannot be reached because it has been turned off, for example.

    'Searching', when the print server has been turned on and searches for an access point.

- 'Current network name' specifies the SSID.
- 'Speed' indicates the data transfer rate.
- 'Level' indicates the intensity of the signal.
- 'Manufacturer' indicates the manufacturer of the WLAN module.
- 'Serial number WLAN' indicates the serial number of the WLAN module.

Printer Port Status

The **Printer Port** page contains information about the connected printers. The page includes information about the manufacturer, the printer model or the total number of printed pages. The printer operating panel and printer status messages can also be displayed. The information that can be shown depends on the printer and print server model. As for print servers with several physical printer ports, the information is displayed separately for each port.

IPv6 Status   The **IPv6** page shows assigned IPv6 addresses. The print server obtains IPv6 addresses if it is connected to a network that supports IPv6. (Only available via PRINTSERVER Homepage.)

IPsec Status   The **IPsec** page shows the entries of the Internet Protocol Security in the Security Association Database (SAD) and the Security Policy Database (SPD). The 'raccon' logging information is also displayed.

Mail Status   The **Mail** page shows the status of the POP3 and SMTP settings.

- 'Mails fetched' shows the number of received emails.
- 'Last POP3 error' shows the last POP3 error.
- 'Next check for mails in' shows the time left till the next mail scan.
- 'Mails sent' shows the number of sent emails.
- 'Last SMTP error' shows the last SMTP error.

Job History   The **Job History** page displays information about the print jobs that have been sent to the print server. 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 print server or printer is turned off or reset. The print jobs will not be deleted when the print server is restarted.

The information that is shown depends on the connected printer model. For a more detailed description; see: 'Job History - Status Information' ⇨🖹139.

5.3   How to Print a Status Page

You can print status pages. The print server status page contains all important basic information, such as the print server model, IP address, etc.

Before a status page can be printed, you need to define the data format of the status page. The data formats ASCII, DATAMAX (label printer), and Citizen-Z (label printer) are available. The preset 'Auto mode' automatically uses the appropriate data format.

A status page can only be printed if the printer supports one of these data format: ASCII, DATAMAX, or Citizen-Z.

What do you want to do?

☐ 'Defining the Data Format of the Status Page' ⇨🗎60

☐ 'Printing the Status Page via the PRINTSERVER-NetTool' ⇨🗎61

☐ 'Printing the Status Page via an FTP Connection' ⇨🗎61

☐ 'Printing the Status Page via the Status Button' ⇨🗎62

Defining the Data Format of the Status Page

🗂 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*

2. *Select* **Configuration – General***.*

3. *Select the desired data format from the* **Status page mode** *list.*

4. *Click* **Save** *or* **OK** *to confirm.*

↳ The setting is saved.

Printing the Status Page via the PRINTSERVER-NetTool

Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Select a print server from the print server list.*
3. *Select* **Actions – Print Status Page...** *from the menu bar.*
4. *(Depending on the print server model, you may be asked to specify the printer port. Select the printer port and confirm by clicking* **Next***.)*
5. *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. *Change to the directory in which you wish to save the file.*
2. *Open an FTP connection to the print server:*
   Syntax: `ftp <IP Address>`
   Example: `ftp 192.168.0.123`
3. *Enter an arbitrary user name.*
4. *Enter the print server password or press ENTER if no password has been assigned.*
5. *Transfer the status page from the print server to your local computer:*
   `get statuspage`
6. *Close the FTP connection:*
   `quit`
7. *Open and print the file using any text editor.*

↳ The status page will be printed.

Printing the Status Page via the Status Button

Using the status button of the print server operating panel, you can print a status page.

📇 Proceed as follows:

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

↳ The status page is printed.

5.4   How to Determine the Print Server Status using the LEDs

Each print server has three LEDs. The LEDs of the print server give you information about the three different statuses of the print server.

- Print Server when Turned on

- Print Server in Normal Mode

- Print Server in BIOS Mode

Print Server when Turned on

After the print server is turned on, the status and link LEDs (green) light up for a short time and then extinguish again. Internal tests are undertaken and the network connection is detected.

After the internal tests have been carried out successfully, the yellow LED lights up until the printer recognizes the print server. The print server is now looking for the network configuration, the print queues etc. and the print server switches to the normal mode.

Print Server in Normal Mode

When the print server is in normal mode, the LEDs tell you the following:

Status LED <green>	The status LED indicates that the print server is operational. To determine whether the print server is operational, the print server must have received at least one data packet. When the print server is in normal mode, the status LED is permanently lit. If the LED is not lit (after a data packet has been received), you should do a firmware update.
Link LED <green>	The link LED shows a (physical) connection to the network. The LED of external print server models is labelled whereas the LED of internal print server models is located above the status button. When the print server is in normal mode, the link LED is permanently lit.
Activity LED <yellow>	The yellow LED lights up when data packets are received. When there are high volumes of data traffic (e.g. during an update) the LED may be permanently lit.

Print Server in BIOS Mode

The print server switches to the BIOS mode if the firmware functions well but the software is faulty. This may happen in the case of an incorrect software update, for example. The print server is in the BIOS mode, if

- the activity LED (yellow) blinks periodically and
- the status LED (green) is <u>not</u> active.

The print server is not operational in the BIOS mode.

If the print server is in the BIOS mode, the filter 'BIOS Mode' will be created automatically in the print server list of the PRINTSERVER-NetTool. The print server is displayed within this filter.
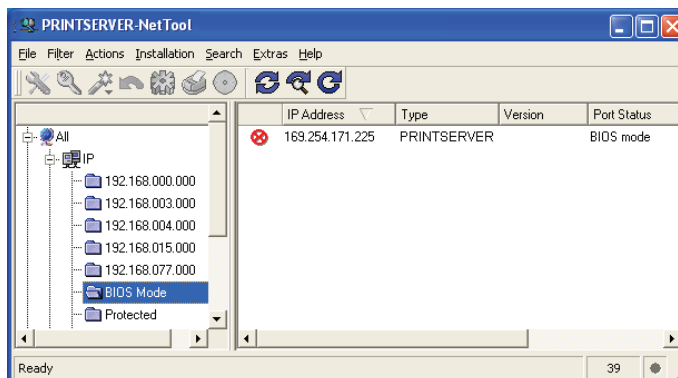
Fig. 16: PRINTSERVER-NetTool – Print Server in BIOS Mode

Troubleshooting

The software must be loaded on the print server so that the print server can switch from the BIOS mode to the normal mode.

Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Select the print server from the print server list. (You will find the print server under 'BIOS Mode'.)*
3. *Select* **Installation – IP Wizard** *from the menu bar. The IP Wizard is started.*
4. *Follow the instructions of the wizard in order to assign an IP address to the print server. The IP address is saved.*
5. *Do a software update on the print server; see: 'How to Perform an Update'* ⇨ 157.

↳ The software is saved in the print server. The print server switches to the normal mode.

6 Device Settings of the Print Server

📄 You can configure the device time, the device language, DNS, etc. on the print server. This chapter describes the device settings. You will learn how to do a restart and define a description.

What information do you need?

- 'How to Configure the DNS' ⇨📄65
- 'How to Configure the Device Time' ⇨📄67
- 'How to Configure the Language of the Device' ⇨📄69
- 'How to Adapt the Network Speed' ⇨📄71
- 'How to Determine a Description' ⇨📄73

6.1 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. DNS also allows the saving of additional attributes of a device. If a DNS server is available in your network, you can use DNS for your print server.

Benefits and Purpose

If DNS is enabled, you can assign network devices via the domain name when configuring the print server. DNS is needed for the SMTP, SNTP, and POP3 functionality, for example.

If DNS is disabled, the SMTP and POP3 protocols are not available.

What do you want to do?

- ☐ 'Configuring DNS via the PRINTSERVER Homepage' ⇨📄66
- ☐ 'Configuring DNS via the PRINTSERVER-NetTool' ⇨📄66

Configuring DNS via the PRINTSERVER Homepage

🖰 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – DNS**.
3. *Configure the DNS parameters; see: Table 4* ⇨🖹*66.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Configuring DNS via the PRINTSERVER-NetTool

🖰 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server in the print server list. The* **Properties** *dialog appears.*
3. *Select* **Configuration – DNS** *from the navigation bar.*
4. *Configure the DNS parameters; see: Table 4* ⇨🖹*66.*
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.

6.2 How to Configure the Device Time

You can set the time of the print server via a time server (SNTP server) in the network. A time server 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 print server will get a time stamp. Date and time are then displayed under Job History.

UTC

The print server uses 'UTC' (Universal Time Coordinated) as a basis. UTC is a reference time and used as a time standard. The reference point for UTC is the prime meridian.

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 PRINTSERVER Homepage'
⇨ 🗎67

☐ 'Configuring the Device Time via the PRINTSERVER-NetTool'
⇨ 🗎68

Configuring the Device Time via the PRINTSERVER Homepage

🖥 Proceed as follows:

1. *Start the PRINTSERVER 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 was configured beforehand).*

5. *Select the code for your local time zone from the* **Time zone** *list.*
6. *Click* **Save** *to confirm.*
✎ The settings are saved.

Configuring the Device Time via the PRINTSERVER-NetTool

📑 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server in the print server 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 was configured beforehand).*
6. *Select the code for your local time zone from the* **Time zone** *list.*
7. *Click* **OK** *to confirm.*
✎ The settings are saved.

6.3 How to Configure the Language of the Device

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

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

Configuring the Device Language via the PRINTSERVER Homepage

Proceed as follows:

1. Start the PRINTSERVER Homepage.
2. Select **Configuration – General***.*
3. Select the desired language from the **Print server language** *list.*
4. Click **Save** *to confirm.*
↳ The settings are saved.

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

Configuring the Device Language via the PRINTSERVER-NetTool

The setting has no effect on the language of the PRINTSERVER-NetTool.

📂 Proceed as follows:

1. Start the PRINTSERVER-NetTool.

2. Double-click the print server in the print server list.
   The **Properties** *dialog appears.*

3. Select **Configuration – General** *from the navigation bar.*

4. Select the desired language from the **Print server language** *list.*

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

↳ The settings are saved.

6.4 How to Adapt the Network Speed

Three modes of transmission between two equal nodes provide for network communication: simplex, half duplex, and duplex.

Duplex Mode

The print server is able to recognize the duplex mode used in a ether network and to adapt to it automatically. This happens via autonegotiation (also: autosensing). The print server recognizes the network speed and the duplex mode of the network port to which it is attached and configures its own parameters accordingly.

This 'Auto' mode is preset. In addition, users can also configure the duplex mode manually.

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 print server with full duplex if the hub functions with half duplex, for example.

What do you want to do?

☐ 'Adapting the Speed via the PRINTSERVER Homepage' ⇨ 🖹71

☐ 'Adapting the Speed via the PRINTSERVER-NetTool' ⇨ 🖹71

Adapting the Speed via the PRINTSERVER Homepage

🖬 Proceed as follows:

1. Start the PRINTSERVER 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 PRINTSERVER-NetTool

🖬 Proceed as follows:

1. Start the PRINTSERVER-NetTool.

2. *Double-click the print server in the print server 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.

6.5 How to Determine a Description

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

☐ 'Determining Descriptions via the PRINTSERVER Homepage' ⇨ 🖹73

☐ 'Determining Descriptions via the PRINTSERVER-NetTool' ⇨ 🖹73

Determining Descriptions via the PRINTSERVER Homepage

📁 Proceed as follows:

1. Start the PRINTSERVER Homepage.

2. Select **Configuration – General**.

3. Enter freely definable names for **Description** *and* **Dealer**.

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

↳ The data is saved.

Determining Descriptions via the PRINTSERVER-NetTool

📁 Proceed as follows:

1. Start the PRINTSERVER-NetTool.

*2. Double-click the print server in the print server list.
The* **Properties** *dialog appears.*

3. Select **Configuration – General** *from the navigation bar.*

4. Enter freely definable names for **Description** *and* **Dealer**.

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

↳ The data is saved.

7 Print Server Port Settings

This chapter explains how you can improve the interaction between printer and print server by choosing the right port settings.

Feasible port settings depend on your print server model. In the case of print servers with several ports, you can configure the parameters for each port individually.

What information do you need?

- 'How to Enable the ECP Mode' ⇨ 🖹75
- 'How to Enable the Fast Mode' ⇨ 🖹76
- 'How to Define the Communication Mode' ⇨ 🖹77
- 'How to Configure COM1 Port Settings' ⇨ 🖹78

In order to determine to which port the print data is to be forwarded in the case of print servers with several physical ports; see: 'Logical Printers (Filters)' ⇨ 🖹178.

7.1   How to Enable the ECP Mode

The ECP (Enhanced Capability Port) mode can be used for quick and compressed data transfer. Data compression using the RLE method (Run Length Encoding) leads to compression rates of up to 64:1.

This ECP mode is only available for external print server models.

What do you want to do?

☐ 'Enabling the ECP Mode via the PRINTSERVER Homepage' ⇨ 🖺75

☐ 'Enabling the ECP Mode via the PRINTSERVER-NetTool' ⇨ 🖺75

Enabling the ECP Mode via the PRINTSERVER Homepage

Proceed as follows:

1.   Start the PRINTSERVER Homepage.

2.   Select **Configuration – Printer Port***.*

3.   Tick **ECP mode***.*

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

↳ The setting is saved.

Enabling the ECP Mode via the PRINTSERVER-NetTool

Proceed as follows:

1.   Start the PRINTSERVER-NetTool.

2.   Double-click the print server in the print server list. The **Properties** *dialog appears.*

3.   Select **Configuration – Printer Port***.*

4.   Tick **ECP mode***.*

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

↳ The setting is saved.

7.2   How to Enable the Fast Mode

The fast mode can be used to increase the speed. With older printer models, it is recommended to disable the fast mode.

This fast mode is only available for external print server models.

☐ 'Enabling the Fast Mode via the PRINTSERVER Homepage' ⇨ 🖹76

☐ 'Enabling the Fast Mode via the PRINTSERVER-NetTool' ⇨ 🖹76

Requirements
☑ The ECP mode must be disabled; see: ⇨ 🖹75.

Enabling the Fast Mode via the PRINTSERVER Homepage

Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – Printer Port***.*
3. *Tick* **Fast mode***.*
4. *Click* **Save** *to confirm.*
↳ The setting is saved.

Enabling the Fast Mode via the PRINTSERVER-NetTool

Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server in the print server list. The* **Properties** *dialog appears.*
3. *Select* **Configuration – Printer Port***.*
4. *Tick* **Fast mode***.*
5. *Click* **OK** *to confirm.*
↳ The setting is saved.

7.3 How to Define the Communication Mode

You can define the communication mode between the print server and the printer via the 'Port Mode'.

The 'Port mode' is only available for external print server models with USB, Centronics, or serial interface.

The following communication modes are available:

- Unidirectional: for unidirectional communication
- Bidirectional: for bidirectional communication with advanced options for acknowledgment and diagnostics.

What do you want to do?

☐ 'Defining the Communication Mode via the PRINTSERVER Homepage' ⇨ 📄77

☐ 'Defining the Communication Mode via the PRINTSERVER-NetTool' ⇨ 📄77

Defining the Communication Mode via the PRINTSERVER Homepage

🗗 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – Printer Port***.*
3. *Select the desired mode from the* **Port mode** *list.*
4. *Click* **Save** *to confirm.*
↳ The setting is saved.

Defining the Communication Mode via the PRINTSERVER-NetTool

🗗 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*

2. *Double-click the print server in the print server list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – Printer Port**.
4. *Select the desired mode from the* **Port mode** *list.*
5. *Click* **OK** *to confirm.*

↳ The setting is saved.

7.4 How to Configure COM1 Port Settings

In the case of print server models with COM1 port, you can adapt the COM1 interface to your individual needs.

Configuring the COM1 Port via the PRINTSERVER Homepage

📝 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – Printer Port**.
3. *Select the desired settings from the COM1 list boxes; see:*
   Table 5 ⇨ 🖹*79.*
4. *Click* **Save** *to confirm.*

↳ The setting is saved.

Configuring the COM1 Port via the PRINTSERVER-NetTool

📝 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server in the print server list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – Printer Port**.

4. *Select the desired settings from the COM1 list boxes; see:*
   Table 5 ⇨ 🖹 *79.*

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

↳ The setting is saved.

Table 5: COM1 Parameters

Parameters	Description
Baud rate	Specifies the baud rate for data transfer.
Parity	Specifies the parity bit for the detection of incorrectly transmitted bit sequences (parity check). The following settings are possible: - none = no parity check - even = even parity check - odd = odd parity check
Data bits	Specifies how many data bits will be transferred in one data packet.
Stop bits	Stop bits mark the end of a data transfer unit and allow the recipient of a data transfer to synchronize the data flow.
Flow control	Defines the handshake procedure to control the data flow between print server and printer. The following settings are possible: - none = handshake is disabled - xon/xoff = software handshake is enabled - dsr/dtr = hardware handshake is enabled - both = software and hardware handshake are enabled

8 Print Server Security

> A number of security mechanisms are available to ensure optimum security for the print server. 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 Print Server (Read/Write Protection)' ⇨🗎81

- 'How to Protect Printers against Unauthorized Access (IP Sender Control)' ⇨🗎82

- 'How to Protect the Print Server against Viruses' ⇨🗎84

- 'How to Organize Encrypted Printing' ⇨🗎84

More security-related topics from other chapters:

- Administer the Print Server via FTPS Connections ⇨🗎34

- Authenticate the Print Server in the Network ⇨🗎87

- Authenticate the print server/client if the administrative access to the Print Server Homepage via SSL (HTTPs) is protected ⇨🗎109.

- Protect the print server via Internet Protocol Security (IPsec) ⇨🗎111.

- Secure mechanisms of WLAN Print Server ⇨🗎189

8.1 How to Define a Password for the Print Server (Read/Write Protection)

Write Protection

A password can protect the print server against unauthorized parameter modifications. 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 opening the PRINTSERVER Homepage or the **Properties** dialog via the PRINTSERVER-NetTool.

Note that the print server password is not identical to the password which the print server needs for logging in Novell networks. The Novell password is generated automatically by the print server and is invisible to the user.

What do you want to do?

Defining the Password via the PRINTSERVER Homepage

Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – Protection***.*
3. *Enter a password into the* **Password** *box in order to enable the write protection.*
4. *Tick* **Access control** *in order to define the read protection, if required.*
5. *Click* **Save** *to confirm.*
⮡ The settings are saved.

Defining the Password via the PRINTSERVER-NetTool

Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server in the print server list.*
   The **Properties** *dialog appears.*
3. *Select* **Configuration – Protection** *from the navigation bar.*
4. *Enter a password into the* **Password** *box in order to enable the write protection.*
5. *Tick* **Access control** *in order to define the read protection, if required.*
6. *Click* **OK** *to confirm.*

↳ The settings are saved.

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

8.2 How to Protect Printers against Unauthorized Access (IP Sender Control)

In TCP/IP networks, you can define which IP addresses and thus which workstations are allowed to access a printer and carry out print jobs.

Benefits and Purpose

The 'IP Sender Control' allows you to protect printers and sensitive data from unauthorized access and to attribute print costs precisely within the company.

To enable the 'IP Sender Control', you must enter the IP addresses or host names of the clients into an **IP sender** list. The print server will only accept print jobs from clients specified in the list.

Up to eight IP senders can be specified. The use of wildcards (*) allows you to define subnetworks (e.g. 192.168.122.*) and to authorize these subnetworks for printing.

In order to disable the IP sender control you must enter '*' into the first IP sender box. Once an IP sender has been defined, all undefined clients lose their authorization to print via the print server.

☐ 'Assigning Authorizations via the PRINTSERVER Homepage'
⇨ 🖹83

☐ 'Assigning Authorizations via the PRINTSERVER-NetTool' ⇨ 🖹83

Assigning Authorizations via the PRINTSERVER Homepage

📁 Proceed as follows:

1. *Start the PRINTSERVER 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 PRINTSERVER-NetTool

📁 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server in the print server 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.

8.3   How to Protect the Print Server against Viruses

The print server cannot be attacked directly by viruses. Attacks to open ports (port 80 / HTTP, for example) can have a certain influence on the print server and affect its functions.

To prevent attacks to open ports, you can disable the HTTP protocol on the print server; see: 'HTTP' ⇨🖹167.

⚠

If you have disabled HTTP, all functions based on this protocol are no longer available. The PRINTSERVER Homepage or printing via HTTP using the PRINTSERVER Print Monitor will no longer be available.

8.4   How to Organize Encrypted Printing

The print server supports the transmission of encrypted print data. Depending on the printing method, different procedures can be used.

What do you want to do?

☐ 'Encrypted Socket Printing (Windows)' ⇨🖹84

☐ 'Encrypted Socket Printing with Certificate Validation (Windows)' ⇨🖹85

☐ 'Receiving Encrypted ThinPrint® Data' ⇨🖹86

Encrypted Socket Printing (Windows)

In Windows systems, the PRINTSERVER Print Monitor ensures the transfer of encrypted print data from the client to the print server by means of direct TCP/IP ports.

Requirements

☑ The PRINTSERVER Print Monitor is installed on the Windows client.

☑ The required printer driver is installed on the client.

If you want to encrypt your print data, create a HTTP port using the PRINTSERVER Print Monitor. During the configuration, tick **Encrypted printing**.

For more detailed information about the configuration using the PRINTSERVER Print Monitor; see: 'Configuring the Printer Port using the PRINTSERVER Print Monitor' ⇨📄45.

Data encryption reduces the data transfer rate of you print server. We therefore recommend configuring an additional port without data encryption.

Encrypted Socket Printing with Certificate Validation (Windows)

The PRINTSERVER Print Monitor allows you to encrypt your print data in Windows systems with certificate validation.

Basic Functions

The following chart shows the function of certificates in networks with encrypted printing.

1. The certificate and the corresponding private key are stored on the print server.	
↳	2. The PRINTSERVER Print Monitor wants to print on the print server.
3. The print server sends the certificate and the public key to the PRINTSERVER Print Monitor.	↲
↳	4. The PRINTSERVER Print Monitor generates another key (symmetric key), encrypts it using a public key and sends it to the print server.
5. The print server decrypts the symmetric key using the private key.	↲
↳	6. The PRINTSERVER Print Monitor encrypts the print data using a symmetric key.
7. The print server encrypts the print data using a symmetric key and prints the data.	↲

Requirements

☑ The PRINTSERVER Print Monitor is installed on the Windows client.

☑ The required printer driver is installed on the client.

☑ The Windows operating system contains the components:
- Internet Explorer (version 5.01 or later)
- Directory Service Client (Dsclient.exe)

Procedure

Follow the instructions if you want to use encrypted printing with additional certificate validation:

☐ Create a HTTP port using the PRINTSERVER Print Monitor. During the configuration, tick **Encrypted printing** and **Authentication**; see: 'Configuring the Printer Port using the PRINTSERVER Print Monitor' ⇨▤45.

☐ Create a self-signed certificate or a CA certificate or use the default certificate that is installed on the print server; see: 'Print Server Certificate Management' ⇨▤98.

☐ Install the certificate on the Windows client in order to make the certificate known to the client; see: 'How to Install Certificates on a Windows Client' ⇨▤109.

Receiving Encrypted ThinPrint® Data

The print server supports the transmission of encrypted ThinPrint® print data. For further information; see: 'ThinPrint® (Print Data Compression)' ⇨▤184.

9 Print Server Network Authentication

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

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 (computer, print server, etc.), 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 print server supports various EAP authentication methods in order to authenticate itself in a protected network.

- 'How to Configure EAP-MD5/LEAP' ⇨🖹88
- 'How to Configure EAP-TLS' ⇨🖹90
- 'How to Configure EAP-TTLS' ⇨🖹91
- 'How to Configure PEAP' ⇨🖹94
- 'How to Configure EAP-FAST' ⇨🖹96

9.1 How to Configure EAP-MD5/LEAP

Benefits and Purpose

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

Basic Functions

EAP-MD5 describes a password-based authentication method that uses MD5 hashing algorithms. This method is used in LANs to control access to hotspots.

In wireless networks, the use of EAP-MD5 is restricted. In wireless networks, the authentication method LEAP (Light Extensible Authentication Protocol) that has been developed by Cisco is preferred. For further information about authentication of WLAN print servers; see: 'WLAN (Wireless Local Area Network)' ⇨🖹188.

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

Requirements

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

What do you want to do?

☐ 'Enabling EAP-MD5/LEAP via the PRINTSERVER Homepage' ⇨🖹89

☐ 'Enabling EAP-MD5/LEAP via the PRINTSERVER-NetTool' ⇨🖹89

The authentication of print server models with WLAN support is configured via the menu item **Configuration – WLAN**.

Enabling EAP-MD5/LEAP via the PRINTSERVER Homepage

📋 Proceed as follows:

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

Enabling EAP-MD5/LEAP via the PRINTSERVER-NetTool

📋 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server in the print server list. The* **Properties** *dialog appears.*
3. *Select* **Configuration – Protection** *from the navigation bar.*
4. *Select the* **Authentication** *tab.*
5. *Select* **EAP-MD5/LEAP** *from the* **Authentication** *list.*
6. *Enter the user name and the password that are used for the configuration of the print server on the RADIUS server.*
7. *Click* **OK** *to confirm.*
↳ The settings are saved.

9.2 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 print server for the EAP-TLS network authentication. This makes sure that the print server 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 print server and the RADIUS server. An encrypted TLS connection between the print server and the RADIUS server is established in this process. Both RADIUS server and print server need a valid, digital certificate signed by a CA. The RADIUS server and the print server must validate the certificate. After the mutual authentication was successful, the access to the network will be freed.

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

If you want to use the EAP-TLS authentication, you must observe the following instructions in the indicated order. Otherwise the print server cannot be addressed in the network. In this case you have to reset the print server parameters; see: ⇨🗎152.

Procedure

☐ Create a certificate request on the print server; see: ⇨🗎102.

☐ Create a CA certificate using the certificate request and the RADIUS server.

☐ Install the CA certificate on the print server; see: 'How to Save CA Certificates in the Print Server' ⇨🗎104.

☐ Install the root certificate of the RADIUS server on the print server; see 'How to Save Root Certificates in the Print Server' ⇨🗎107.

☐ Enable the authentication method 'EAP-TLS' on the print server.

☐ 'Enabling EAP-TLS via the PRINTSERVER Homepage' ⇨ 🗎91

☐ 'Enabling EAP-TLS via the PRINTSERVER-NetTool' ⇨ 🗎91

The authentication of print server models with WLAN support is configured via the menu item **Configuration - WLAN**.

Enabling EAP-TLS via the PRINTSERVER Homepage

Proceed as follows:

1. Start the PRINTSERVER Homepage.

2. Select **Configuration – Protection***.*

3. Select **Authentication***.*

4. Select **EAP-TLS** *from the* **Authentication** *list.*

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

↳ The settings are saved.

Enabling EAP-TLS via the PRINTSERVER-NetTool

Proceed as follows:

1. Start the PRINTSERVER-NetTool.

*2. Double-click the print server in the print server list.
The* **Properties** *dialog appears.*

3. Select **Configuration – Protection** *from the navigation bar.*

4. Select the **Authentication** *tab.*

5. Select **EAP-TLS** *from the* **Authentication** *list.*

6. Click **OK** *to confirm.*

↳ The settings are saved.

9.3   How to Configure EAP-TTLS

EAP-TTLS (Tunneled Transport Layer Security) validates the identity of devices or users before they gain access to network resources. You can configure the print server for the EAP-TTLS network

authentication. This makes sure that the print server gets access to protected networks.

Basic Functions

EAP-TTLS consists of two phases:

- In phase 1, a TLS-encrypted channel between the print server 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 print server. (Phase 1) The print server validates the identity of the RADIUS server by means of the certificate.

Requirements

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

What do you want to do?

☐ 'Enabling EAP-TTLS via the PRINTSERVER Homepage' ⇨🗎93

☐ 'Enabling EAP-TTLS via the PRINTSERVER-NetTool' ⇨🗎93

The authentication of print server models with WLAN support is configured via the menu item **Configuration – WLAN**.

Enabling EAP-TTLS via the PRINTSERVER Homepage

📋 Proceed as follows:

1. *Start the PRINTSERVER 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 print server 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 print server.*
8. *Click* **Save** *to confirm.*

↳ The settings are saved.

Enabling EAP-TTLS via the PRINTSERVER-NetTool

📋 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server in the print server 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 print server 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 print server.*
9. *Click* **OK** *to confirm.*

↳ The settings are saved.

9.4 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 print server for the PEAP network authentication. This makes sure that the print server gets access to protected networks.

Basic Functions

In the case of PEAP (compare EAP-TTLS; see ⇨📄91), an encrypted TLS (Transport Layer Security) channel is established between the print server 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 print server is defined as user (with user name and password) on a RADIUS server.

What do you want to do?

☐ 'Enabling PEAP via the PRINTSERVER Homepage' ⇨📄94

☐ 'Enabling PEAP via the PRINTSERVER-NetTool' ⇨📄95

The authentication of print server models with WLAN support is configured via the menu item **Configuration – WLAN**.

Enabling PEAP via the PRINTSERVER Homepage

📁 Proceed as follows:

1. *Start the PRINTSERVER 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 print server 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 print server.*
8. *Click* **Save** *to confirm.*
- The settings are saved.

Enabling PEAP via the PRINTSERVER-NetTool

Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server in the print server 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 print server 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 print server.*
9. *Click* **OK** *to confirm.*
- The settings are saved.

9.5   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 print server for the EAP-FAST network authentication. This makes sure that the print server gets access to protected networks.

Basic Functions

EAP-FAST uses (as in the case of EAP-TTLS; see ⇨📄91) 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 print server and the RADIUS server.
- An opaque part that is provided to the print server and presented to the RADIUS server when the print server 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 print server authentication as well as the delivery of PACs.

Requirements

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

What do you want to do?

☐ 'Enabling EAP-FAST via the PRINTSERVER Homepage' ⇨📄97

☐ 'Enabling EAP-FAST via the PRINTSERVER-NetTool' ⇨📄97

The authentication of print server models with WLAN support is configured via the menu item **Configuration - WLAN**.

Enabling EAP-FAST via the PRINTSERVER Homepage

Proceed as follows:

1. *Start the PRINTSERVER 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 print server 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 PRINTSERVER-NetTool

Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server in the print server 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 print server 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.

10 Print Server Certificate Management

> The print server 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 mechanisms. Use certificates in your print server

- to encrypt print data; see: ⇨🗎85.

- to authenticate the print server in a network that is protected by EAP authentication; see: 'Print Server Network Authentication' ⇨🗎87.

- to verify the identity of users and devices that have access to the print server via a WLAN; see: 'WLAN (Wireless Local Area Network)' ⇨🗎188.

- to authenticate the print server if the administrative access to the Print Server Homepage via SSL (HTTPs) is protected; see: ⇨🗎109.

- to administer the print server via an FTPS connection; see: ⇨🗎34.

- to allow for a certificate-based authentication of the remote server in the case of IPsec; see: ⇨🗎111.

If you want to use certificates, it is advisable to protect the print server by a password so that the certificate cannot be deleted by unauthorized persons; see ⇨🗎81.

Which Certificates are available?

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

Self-signed certificates have a digital signature that has been created by the print server.

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 self-signed certificate (the so-called **default certificate**) is stored in the print server. If you set up encrypted printing via HTTP (SSL) in the PRINTSERVER Print Monitor, the default certificate is used; see: 'Encrypted Socket Printing with Certificate Validation (Windows)' ⇨🗎85. 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' ⇨🗎100
- 'How to Create a Certificate Request for CA Certificates' ⇨🗎102
- 'How to Save CA Certificates in the Print Server' ⇨🗎104
- 'How to Save PKCS12 Certificates in the Print Server' ⇨🗎105
- 'How to Save Root Certificates in the Print Server' ⇨🗎107
- 'How to Delete Certificates' ⇨🗎108
- 'How to Install Certificates on a Windows Client' ⇨🗎109

10.1 How to Create a Self-Signed Certificate

When a certificate is created on the print server 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 print server, the content of this certificate will be displayed. In this case you have to delete the existing certificate first; see: 'How to Delete Certificates' ⇨▤108.

☐ 'Creating Self-Signed Certificates via the PRINTSERVER Homepage' ⇨▤100

☐ 'Creating Self-Signed Certificates via the PRINTSERVER-NetTool' ⇨▤100

Creating Self-Signed Certificates via the PRINTSERVER Homepage

Proceed as follows:

1. Start the PRINTSERVER Homepage.
2. Select **Configuration – Certificates***.*
3. Select **Print server certificate***.*
4. Enter the relevant parameters, see: Table 6 ⇨▤*101.*
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 PRINTSERVER-NetTool

Proceed as follows:

1. Start the PRINTSERVER-NetTool.
2. Select a print server from the print server 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 6 ⇨▤*101.*

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 6: 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 print server to allow a clear assignment of the certificate to the print server. 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 print server. 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.
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.

10.2 How to Create a Certificate Request for CA Certificates

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

When a certificate is created on the print server 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 print server, the content of this certificate will be displayed. In this case you have to delete the existing certificate first; see: 'How to Delete Certificates' ⇨🖹108.

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

What do you want to do?

☐ 'Creating a Certificate Request via the PRINTSERVER Homepage' ⇨🖹102

☐ 'Creating a Certificate Request via the PRINTSERVER-NetTool' ⇨🖹103

Creating a Certificate Request via the PRINTSERVER Homepage

Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – Certificates**.
3. *Select* **Print server certificate**.
4. *Enter the required parameters, see: Table 6* ⇨🖹*101.*
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 print server; see: 'How to Save CA Certificates in the Print Server' ⇨🖹104.

Creating a Certificate Request via the PRINTSERVER-NetTool

📁 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Select a print server from the print server 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 6* ⇨🖹*101.*
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 print server; see: 'How to Save CA Certificates in the Print Server' ⇨🖹104.

10.3 How to Save CA Certificates in the Print Server

The CA certificate must be in 'base 64' format.

Saving CA Certificates via the PRINTSERVER Homepage

📋 Proceed as follows:

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

✎ The CA certificate is saved in the print server. This may take a few minutes.

Saving CA Certificates via the PRINTSERVER-NetTool

📋 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Select a print server from the print server 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 print server. This may take a few minutes.

10.4 How to Save PKCS12 Certificates in the Print Server

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 print server, the content of this certificate will be displayed. In this case you have to delete the existing certificate first; see: 'How to Delete Certificates' ⇨ 📄108.

Saving PKCS12 Certificates via the PRINTSERVER Homepage

📷 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – Certificates***.*
3. *Select* **Print server certificate***.*
4. *Click* **Load certificate (pkcs12 format)***.*
5. *Click* **Browse***.*
6. *Specify the certificate.*
7. *Enter the password.*
8. *Click* **Load PKCS12***.*
↳ The PKCS12 certificate is saved in the print server. This may take a few minutes.

Saving PKCS12 Certificates via the PRINTSERVER-NetTool

📷 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Select a print server from the print server 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 print server. This may take a few minutes.

10.5 How to Save Root Certificates in the Print Server

The print server has got several EAP authentication procedures. If you use EAP-TLS, for example, you must load the root certificate of the authentication server (RADIUS) to the print server.

The root certificate must be in base 64 format.

Saving Root Certificates via the PRINTSERVER Homepage

📥 Proceed as follows:

1. *Start the PRINTSERVER 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 print server. This may take a few minutes.

Saving Root Certificates via the PRINTSERVER-NetTool

📥 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Select a print server from the print server 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 print server. This may take a few minutes.

10.6 How to Delete Certificates

If a self-signed certificate or a CA certificate has been saved in the print server, the content of this certificate will be displayed. If you want to use a different certificate you must first delete the existing certificate.

☐ 'Deleting Certificates via the PRINTSERVER Homepage' ⇨ 🖹 108

☐ 'Deleting Certificates via the PRINTSERVER-NetTool' ⇨ 🖹 108

Deleting Certificates via the PRINTSERVER Homepage

📋 Proceed as follows:

1. Start the PRINTSERVER Homepage.
2. Select **Configuration – Certificates***.*
3. Select **Print server certificate***.*
4. Click **Delete certificate***.*
↳ The certificate is deleted.

Deleting Certificates via the PRINTSERVER-NetTool

📋 Proceed as follows:

1. Start the PRINTSERVER-NetTool.
2. Select a print server from the print server list.
3. Select **Actions – Certificate – Server certificate** *from the menu bar. The* **Certificate** *dialog appears.*
4. Click **Delete***.*
↳ The certificate is deleted.

10.7 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 print server is additionally secured by means of an authentication.

- If the administrative access to the Print Server 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 PRINTSERVER Homepage. To do this, enter 'https://' and the IP address of the print server into the address box of your browser. (e.g. https://192.168.0.191). A security alert appears.*
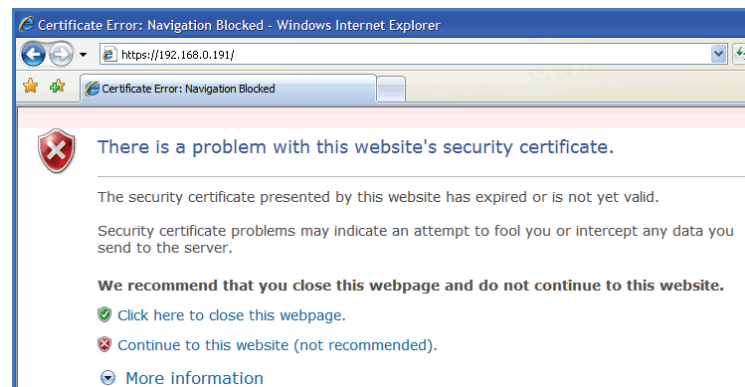
Fig. 17: Internet Explorer – Security Alert

---

2. *Click* **Continue to this website**.
   A note (Certificate Error) is displayed
.
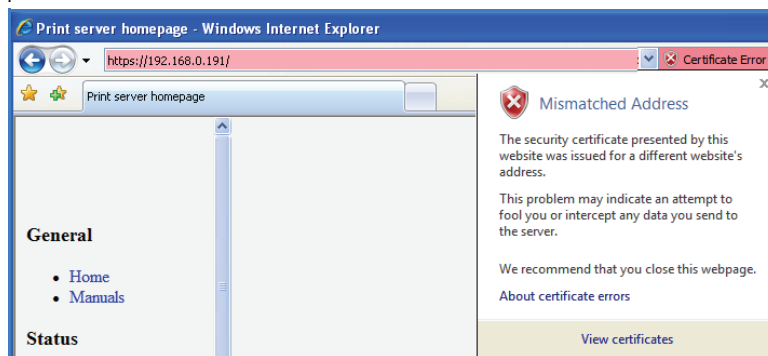
Fig. 18: Internet Explorer

3. *Click* **View certificates**.
   The **Certificate** *dialog appears.*
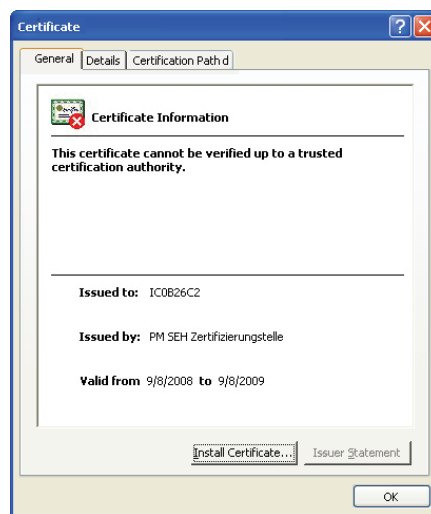
Fig. 19: Internet Explorer - Certificate

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'.

11 Internet Protocol Security (IPsec)

To defend against the internal threads for the network, the IPsec protocol provides confidentiality, authenticity and integrity for the IP-based network traffic. The print server can participate in various IPsec procedures. This chapter describes which procedures are supported and how these procedures are configured on the print server.

What is IPsec?

'Internet Protocol Security' (IPsec) is a protocol that provides security mechanisms such as access control, data integrity, encryption and authentication for the communication via IP networks.

What is special about IPsec is its flexibility. You can enable or disable functions according to your needs. When it comes to encryption and authentication, you can freely define the algorithms to be used.

The IPsec security mechanisms are provided by two protocols – the 'Authentication Header' (AH) or 'Encapsulating Security Payload' (ESP). AH will only provide for authentication while ESP will (in addition to authentication) encrypt the IP data packets.

IPsec Policy

IPsec policies are used to assign and handle IP data packets. You can specify several policies. However, only one policy can be active at a time. An IPsec policy is a collection of one or more rules.

IPsec analyzes all IP data packets for addresses, ports, and transport protocols via packet filtering. Based on the rules it is decided how to proceed with the IP data packet. An IPsec policy consists of the following elements:

Table 7: Components of an IPsec policy

Component	Description
Filter list	A filter list contains one or several filters. A filter is the description of - IP traffic (IP address / IP address range) and - protocols and services that are used.
Filter action	This is the action to be carried out if a data packet matches the description of a filter. The following actions can be defined: - Allow IP data packets - Block IP data packets - Forward IP data packets via a 'security association'.
Rule	A rule is composed of a filter list and a filter action. Thus it is specified that a certain action belongs to a certain filter.

If an IP data packet is forwarded via a 'security association', the actual IPsec security will be applied.

Security Association

A security association (SA) is the establishment of shared security information between two network entities. It serves as a basis for the use of IPsec and can be compared to a tunnel.

The SA specifies which security measures to use for a packet. SAs are established between sender and recipient. The following SA parameters are required:

- authentication method of the participants (pre-shared key or certificate)
- key algorithm to be used for the IPsec connection (see: Table 11 ⇨ 📄124)
- time after which another authentication is required (optional)
- time after which the IPsec key must be renewed (optional)

How Does an SA Work?

When using an SA the tunnel parameters must be defined. When a packet must be sent through a non-existing tunnel (SA), the print server establishes contact with the remote server.

In the so-called 'main mode' the print server sends its suggestions concerning the tunnel parameters. The remote server chooses one suggestion and sends it back.

Alternatively you can choose the 'aggressive mode' that offers almost the same functions but needs fewer packets. (The 'aggressive mode' is less secure and should only be used if the remote IP address is known.)

Afterwards, information for the authentication of the remote server and the agreement about a key (Diffie-Hellman algorithm) will be transferred.

Two different methods are used for authentication purposes.

- authentication via 'Pre-Shared Keys' (PSK) or a
- certificate-based authentication

After the print server and remote server have specified the SA parameters, the IP data packets that are to be encrypted will be sent by the SA together with the ESP protocol (or the AH protocol).

Moreover, 'Internet Key Exchange' (IKE) is used as a protocol for the key exchange or key management togehter with the 'Internet Security Association and Key Management Protocol' (ISAKMP).

IPsec Structure and Procedure

The kernel has two databases for the use of IPsec.

- Security Policy Database (SPD)
  The kernel refers to the SPD in order to decide if a particular IP data packet needs to be processed by IPSec or not. The SPD also contains entries that specify which IPsec SA and in what form an IPsec SA is to be used.

- Security Association Database (SAD)
  The SAD contains the keys for each IPSec SA.

The illustration shows the cooperation between SPD, SAD, and kernel while using IPsec SA with keys.
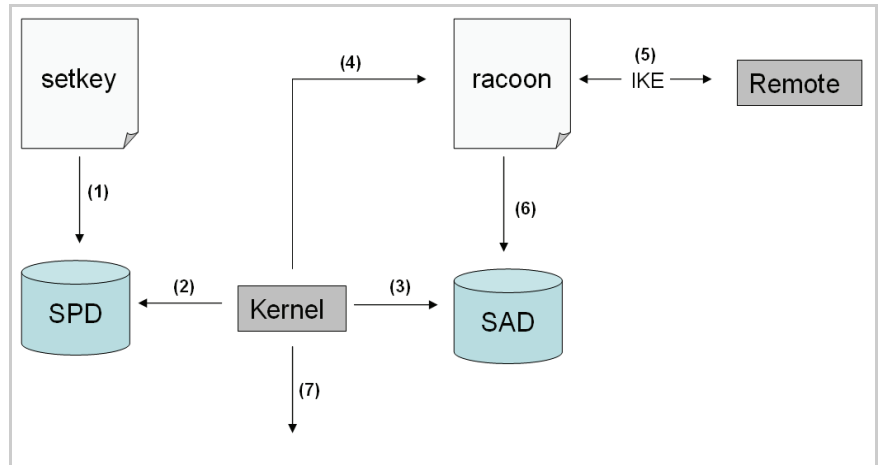
Fig. 20: IPsec procedure

(1) The administrator defines a policy in the SPD via 'setkey'.
(2) The kernel refers to the SPD to determine if IPsec can be used for an IP data packet.
(3) If a key is required for the IPsec-SA, the kernel will get the key from the SAD.
(4) If the SAD has no key, the kernel sends a request to 'racoon'.
(5) 'racoon' uses IKE to exchange keys with the remote server.
(6) 'racoon' writes the key to the SAD.
(7) The kernel is able to send IPsec data packets.

You can use manual keys or an IKE daemon (e.g. racoon) for authentication purposes. racoon provides the automatic key exchange between two hosts. The setup of a policy in the SPD is required in both cases.

When using manual keys, you must make entries in the SAD in order to provide the encryption algorithm and the keys for a secure communication with other hosts. When using an IKE daemon, the SAs are created automatically.

What is the Task of the Print Server?

The print server offers to ways to implement IPsec policies including SA.

- You can create an IPsec policy via the Print Server Homepage. An input mask assists you in defining the rules.

- Via the Print Server Homepage you can import IPsec policies as ready-made configuration files (racoon/setkey) to the print server.

Only one IPsec policy can be active at a time.

Please do not operate the print server with a dynamic IP address if you use IPsec.

What information do you need?

- 'How to Create IPsec Rules' ⇨ 🖹116
- 'How to Use IPsec Configuration Files' ⇨ 🖹126
- 'How to Define Exceptions' ⇨ 🖹129
- 'How to Enable IPsec Policies' ⇨ 🖹130

IP sec Area only accessible via SSL

The access to the IPsec area on the Print Server Homepage is protected via a secure SSL connection.

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 client, the certificate is not classed as 'trusted'. In this case, you will get an error message. Install the certificate on the client by means of a browser ⇨ 🖹109.

11.1 How to Create IPsec Rules

This section describes the creation of IPsec rules via the input mask of the Print Server Homepage.

Rule Structure

IPsec rules are composed of filters and actions.

Filter A filter must be defined to check the data traffic. The filter consists of the following elements:

- Local IP address
  The local IP address corresponds to the IP address of the print server. The existing IPv4 address of the print server will be used and cannot be changed at this point. IPv6 addresses can be defined via an address template.

- Remote IP address
  Addresses in the format IPv4 and IPv6 are supported. You can also specify IP address ranges. IP addresses and ranges can be stored in address templates and added to a rule.

- Services
  Specifies the services that are used by an IP data packet. A service includes the protocol to be used and its port. Several protocols can be summarized in one service template and stored using a freely definable name.

Action An action determines the measure to be taken if an IP data packet corresponds to the description of a filter. The following actions can be selected:

- Allow all (allow IP data packets)
- Drop all (block IP data packets)
- Use IPsec (forward IP data packets via an SA)

SA
If an IP data packet is forwarded via a 'Security Association' you must specify the SA parameters via an SA template. An SA template contains information about the authentication and the key exchange.

To exchange keys, parameters have been specified in the IKE template.

Rules and Priority

The priority of the rules is defined according to the following criteria.

Exclusiveness of the IP Addresses
Depending on the number of IP addresses contained in an 'address template' the following priority can be determined:

- unique IP address (e. g. 192.168.0.194)
- address ranges (e. g. 192.168.0.194/24 or 0.0.0.0/0)

Rule Numbers
Depending on the rule number the following priority can be determined:

- Based on their priority the rules are processed in the following order: from rule 1 (top) to rule 4 (buttom).
- If a rule can be applied, the corresponding action will be carried out. All other rules will be neglected.
- If no rule can be applied, the default rule will be used.

Examples

Example 1

<u>Target:</u>
Each participant in the company is allowed to print via the printer 'x' without any restrictions.
- Due to large print volumes the 'Sales' department is to be excluded.
- Due to sensitive customer data the 'Support' department will only be allowed to print via IPsec. The SA template 'Level 1' will be used for this purpose.

<u>Implementation concept:</u>

Rule	Active	Addresses Filter	Service Filter	Action	SA (Security Association)
1	x	Sales (IP range)	All services	Drop all	---
2	x	Support (IP range)	All services	Require IPsec	Level 1
3		---	---	Allow all	---
4		---	---	Allow all	---
Default		All IP addresses	All services	Allow all	---

Example 2

<u>Target:</u>
No participant in the company is allowed to print via the printer 'y'.
- The 'Sales' and 'Support' departments will be allowed to print.
- Due to sensitive data the Sales Manager is supposed to print via IPsec.
  The SA template 'Level 1' will be used for this purpose.
- The printer will be configured via IPsec by the 'Support' department only. The SA template
  'Level 2' will be used for this purpose.

<u>Implementation concept:</u>
- All relevant printing services are specified in the 'Printing' service filter.
- All relevant protocols for the administration are specified in the 'Configuring' service
filter.

Rule	Active	Addresses Filter	Service Filter	Action	SA (Security Association)
1	x	Director (IP)	Printing	Require IPsec	Level 1
2	x	Sales (IP range)	Printing	Allow all	---
3	x	Support (IP range)	Configuring	Require IPsec	Level 2
4	x	Support (IP range)	Printing	Allow all	---
Default		All IP addresses	All services	Drop all	---

What do you want to do?

☐ 'Creating IPsec Rules' ⇨ 🖹120

☐ 'Enabling IPsec Rules' ⇨ 🖹120

☐ 'Defining Address Templates' ⇨ 🖹120

☐ 'Defining Service Templates' ⇨ 🖹122

☐ 'Defining SA Templates' ⇨ 🖹123

☐ 'Defining IKE Templates' ⇨ 🖹124

Creating IPsec Rules

IP data packets can be filtered by address and log information and be assigned to an action. The assignment of filters and filter actions is done via rules.

Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – IPsec**.
3. *Select* **Edit rules**.
4. *Define the filters.*
   To do this, mark the templates to be used in the 'Address filter' and 'Service filter' lists.
5. *Mark the filter action to be used in the 'Action' list.*
6. *If you have chosen the 'Require IPsec' filter action you must also mark the 'Secutity Association (SA)' to be used.*
7. *Click* **Save**.

The settings are saved.

Enabling IPsec Rules

An IPsec policy is composed of several rules. The rules to be used must be enabled so that they can be taken into consideration within the IPsec policy. The activity is controlled by means of the check boxes on the left side of the rules.

Afterwards you must enable the entire IPsec policy for the rules to take effect; see: ⇨🗎130.

Defining Address Templates

Local and remote IP addresses can be defined in the address template. Addresses in the format IPv4 and IPv6 are supported.

3 address templates has been implemented by default. You can specify another 5 templates, if required.

The IPv4 address of the print server is always used as the local IPv4 address. The address is not shown in the template.

Please use static IP addresses only.

📩 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Edit rules***.*
4. *Select* **Edit address templates.**
5. *Specify the address template; see: Table 8* ⇨ 📄 *121.*
6. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 8: Address Template Parameters

Parameter	Description
Name	Name of the address template. *You can enter a maximum of 18 characters.*
Remote (IPv4)	Specifies remote IPv4 addresses or IPv4 address ranges. *Formats/Convention/Example* *- All IPv4 addresses = 0.0.0.0/0* *- IPv4 address = 192.168.0.1* *- IPv4 address range = 192.168.0.1/24* *(The notation of address ranges is done via the CIDR methodology.)*
Local (IPv6)	Specifies local IPv6 addresses or IPv6 address ranges. *Formats/Convention/Example* *- All IPv6 addresses = ::/0* *- IPv6 address = 0:0:0:0:0:FFFF:a.b.c.d* *- IPv6 address range = 0:0:0:0:0:FFFF:a.b.c.d/96* *(The notation of address ranges is done via the CIDR methodology.)*
Remote (IPv6)	Specifies remote IPv6 addresses or IPv6 address ranges. *Formats/Convention/Example* *- All IPv6 addresses = ::/0* *- IPv6 address = 0:0:0:0:0:FFFF:a.b.c.d* *- IPv6 address range = 0:0:0:0:0:FFFF:a.b.c.d/96* *(The notation of address ranges is done via the CIDR methodology.)*

Defining Service Templates

A service includes the protocol to be used and its port. Network activities based on this protocol can be added to the IPsec rule by means of a service template. Several services can be combined in a service template.

The Service-Template 'All services' has been implemented by default. You can specify another 3 templates, if required.

🖳 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Edit rules***.*
4. *Select* **Edit service templates.**
5. *Specify the service template; see: Table 9* ⇨📄*122.*
6. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 9: Service Template Parameters

Parameter	Description
Name	Name of the service template. *You can enter a maximum of 16 characters.*
All	Comprises all protocols.
ICMP	Internet Control Message Protocol
HTTP	Hypertext Transfer Protocol
SNTP	Simple Network Time Protocol
SNMP	Simple Network Management Protocol
IPP	Internet Printing Protocol
Socket printing	Socket printing
LPR	Line Printer Remote
ThinPrint	ThinPrint® enables the transmission of compressed and bandwidth-optimized print jobs within a network.

Defining SA Templates

An SA template contains information about the authentication as well as the key exchange between the print server and the remote server. You can create a maximum of 4 SA templates.

Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Edit rules***.*
4. *Select* **Edit SA templates.**
5. *Specify the SA template; see: Table 10* ⇨📄*123.*
6. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 10: SA Template Parameters

Parameter	Description
Name	Name of the IPsec template. *You can enter a maximum of 16 characters.*
Authentication type	Specifies the procedure for the authentication of the remote server. *Two procedures are available:* *- authentication via pre-shared key* *- authentication via certificates.* (For the installation of certificates into print servers; see: ⇨📄98.)
Verify certificate	Specifies the type of certificate required for the certificate-based authentication. *- Disabled: A self-signed certificate is sufficient for the authentication. (Upon delivery, a self-signed certificate is stored in the print server).* *- Enabled: A root certificate is required for the authentication.*
Pre-Shared Key	Specifies the Pre-Shared Key (PSK). *You need the key if the 'Pre-Shared Key' procedure has been selected as 'Authentication type'.* *You can enter a maximum of 16 characters.*
IKE	Specifies the template to be used for the automatic key exchange.

Defining IKE Templates

The IKE template contains the parameters to be used for the automatic key exchange.

The 'IKE Default' template has been implemented by default. You can specify another 3 templates, if required.

📔 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – IPsec**.
3. *Select* **Edit rules**.
4. *Select* **Edit SA templates.**
5. *Select* **Edit IKE templates.**
6. *Specify the IKE template; see: Table 11* ⇨ 📄 *124.*
7. *Click* **Save** *to confirm.*
↳ The settings are saved.

Table 11: IKE Template Parameters

Parameter	Description
Name	Name of the IKE template. *You can enter a maximum of 16 characters.*
- Phase 1 - IKE Phase 1 establishes a secure channel.	
Negotiation	Specifies the procedure for the negotiation of the encryption and authentication.
	- In the 'Main Mode' individual connections will be successively established for the individual steps (key exchange etc.).
	- In the 'Aggressive Mode' individual steps of the Main Mode will be summarized (faster but less secure).
	You can select several procedures. Only the most secure procedure will be applied. If a procedure fails, a less complicated (and therefore less secure) procedure will be used.
Diffie-Hellman group	Specifies the Diffie-Hellman group number for the creation of dynamically generated temporary keys. The keys are used during the negotiation.
Encryption algorithm	Specifies the encryption algorithm to be used during the negotiation.

Parameter	Description
Hash algorithm	Specifies the Hash algorithm to be used during the negotiation.
IKE SA lifetime	Specifies the duration of the IKE connection in seconds. When the IKE SA lifetime expires, a re-authentication is required. (optional) *(min. 600 sec / max. 4294967295 sec)*
- Phase 2 - **IKE phase 2 negotiates the encryption and integrity parameters used to secure the data packet to be transferred.**	
- Phase 2 - Encapsulation type	Specifies how the IP data packet is handled within the SA. The IPsec specification differentiates between the 'Transport Mode' and the 'Tunnel Mode'. - In the Transport Mode the IP data packet is encrypted. However, the IP header will be kept. - In the Tunnel Mode a complete IP data packet will be encapsulated in another packet and be given a new IP header. *NOTE: The Tunnel Mode cannot be selected via the selection list on the Printserver Homepage. Use a configuration file (racoon/setkey) instead.*
Diffie-Hellman group	Specifies the Diffie-Hellman group number for the creation of additional dynamically generated temporary keys. The keys are used during phase 2. (optional)
Encryption algorithm	Specifies the encryption code for phase 2.
Authentication algorithm	Specifies the Hash algorithm for phase 2.
With AH protocol	Specifies the use of the 'Authentication Header' protocol for the protection of the packet integrity and packet authentication. *AH uses the authentication header to authenticate the packet. In the IP data packet, the authentication header will be added after the IP header.*
IPsec SA lifetime	Specifies the duration of the IPsec SA connection in seconds. (When the IPsec SA lifetime expires, you have to renew the IPsec key. *(min. 600 sec / max. 4294967295 sec)*

11.2 How to Use IPsec Configuration Files

In order to prepare the print server for the IPsec procedure you must use the following configuration files for the configuration of SPD and SAD.

- 'setkey.conf' to change, add, or delete entries in SPD and SAD.

- 'racoon.conf' to configure the IKE daemon 'racoon' for the automatic key exchange.

Creating IPsec Configuration Files

When creating the configuration file 'racoon.conf' you must specify the reference to the print server certificates as follows:

Example

```
path certificate "/flash";

remote 192.168.0.1 {
        exchange_mode main;
certificate_type x509 "cert.pem" "pkey.pem";
verify_cert on;
        my_identifier asn1dn;
peers_identifier asn1dn;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method rsasig;
                dh_group modp1024;
        }
}

sainfo address 192.168.0.2 any address 192.168.0.1 any
{
        pfs_group modp768;
        encryption_algorithm 3des;
        authentication_algorithm hmac_md5;
        compression_algorithm deflate;
}
```

Detailed information about the creation of configuration files would go beyond the scope of this document. You will find more detailed information on the Internet.

Importing IPsec Configuration Files

You must load the files in the print server so that the values of configuration files 'setkey.conf' or 'racoon.conf' can be applied.

📭 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Load files***.*
4. *Click* **Browse***.*
5. *Select the configuration file.*
6. *Click* **Load***.*
7. *Click* **Save** *to confirm.*
↳ The settings of the configuration file will be saved.

Importing the Pre-Shared Key

If the authentication method 'Pre-Shared Key' is used for an SA (see: Table 10 ⇨🗎123) the pre-shared key must be saved in the print server.

📭 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Load files***.*
4. *Next to Preshared keys file click* **Browse…***.*
5. *Select the file.*
6. *Click* **Load***.*
7. *Click* **Save** *to confirm.*
↳ The pre-shared key is loaded.

Importing Certificates

If an authentication via certificates is used for the SA (see: Table 10 ⇨🗎123), you must save certificates in the print server. To save certificates; see: ⇨🗎98.

11.3 How to Define Exceptions

Network activities based on the protocols SLP, DHCP, FTP, and NetBIOS can be excluded from the filtering by the IPsec policy.

This ensures that specified network activities are permanently allowed and are not blocked by IPsec.

Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Edit rules***.*
4. *Enable the relevant protocols under 'IPsec exceptions'.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

If all FTP network activities are allowed (FTP = on), you must specify the 'Allow all' action in the default rule.

11.4 How to Enable IPsec Policies

After you have created IPsec policies via input mask or via configuration files and implemented them on the print server, you can enable a policy.

Test Mode We recommend using the test mode to access the device in case of a misconfiguration. In the test mode, IPsec remains active until the hard reboot of the device. IPsec is disabled after the hard reboot.

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

Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – IPsec**.
3. *Specify the IPsec policy to be used.*
   - **Use configured rules** *(use policy of the manually configured rules)*
   - **Use configuration files** *(use policy of the loaded configuration files)*
4. *Make sure that the* **test mode** *is on.*
5. *Tick* **IPsec**.
6. *Click* **Save** *to confirm. The setting is saved.*
   IPsec remains active until the device is hard rebooted.
7. *Check the access to the device.*

If you can no longer access the device, initiate a hard reboot of the device and modify the IPsec policy.

---

8. *Clear* **Test mode**.
9. *Click* **Save** *to confirm.*
   ↳ IP traffic will be allowed based on the rules defined in the IPsec policy.

---

12 Printer Status and Printer Messages

The print server can receive information and messages from connected printers and provide these messages/information in various forms. This chapter describes how to display and receive information.

- 'How to Display the Printer Status' ⇨ 🗎131

- 'How to Get Printer Messages via Email' ⇨ 🗎134

- 'How to Get Printer Messages via SNMP Traps' ⇨ 🗎136

- 'How to Display the Job History' ⇨ 🗎138

12.1 How to Display the Printer Status

There are many ways to keep yourself informed about the status of the printers which are administered via the print server.

The information that can be shown depends on the printer and print server models. As for print servers with several physical printer ports, the information is displayed separately for each port.

- ☐ 'Displaying the Printer Status and the Printer Display via the PRINTSERVER Homepage' ⇨ 🗎132

- ☐ 'Displaying the Printer Display via the PRINTSERVER-NetTool' ⇨ 🗎132

- ☐ 'Displaying the Printer Status via the PRINTSERVER-NetTool' ⇨ 🗎132

- ☐ 'Displaying the Printer Status via FTP' ⇨ 🗎133

Displaying the Printer Status and the Printer Display via the PRINTSERVER Homepage

📋 Proceed as follows:

1. Start the PRINTSERVER Homepage.

2. Select **Status – Printer Port**.

↳ The printer status and the printer display are displayed.

Displaying the Printer Display via the PRINTSERVER-NetTool

📋 Proceed as follows:

1. Start the PRINTSERVER-NetTool.

2. Select the printer/print server from the print server list.

3. Select **Actions – Printer Panel** *from the menu bar.*

↳ The printer display will be displayed.

Fig. 21: PRINTSERVER-NetTool - Printer Panel

Displaying the Printer Status via the PRINTSERVER-NetTool

The printer status can be viewed in the 'Port Status' column of the print server list. Follow these steps in order to get additional information about the printer status:

📋 Proceed as follows:

1. Start the PRINTSERVER-NetTool.

2. Double-click the print server in the print server list.
The **Properties** *dialog appears.*

3. Select **Status – Printer Port** *from the navigation bar.*

✤ The printer status will appear on the screen.

Displaying the Printer Status via FTP

The printer status is stored in the 'printerport' file of the print server. You can view the contents of the file on the screen via FTP.

📋 Proceed as follows:

1. Open an FTP connection to the print server:
   Syntax: ` ftp <IP Address>`
   Example: ` ftp 192.168.0.123`
2. Enter either the print server password or press ENTER if no password has been assigned.
3. Get the printer status from the print server:
   `get printerport`
4. Close the FTP connection:
   `quit`

12.2 How to Get Printer Messages via Email

You can get email notifications from the printers connected to the print server. You can define under which circumstances the printer will send a notification.

This allows up to two freely definable recipients to get information about the printer status, printer errors (such as Paper empty), the number of pages printed, or print jobs.

The information that can be shown depends on the connected printer model.

☑ A DNS server has been configured on the print server; see: ⇨📄65.

☑ SMTP parameters are configured on the print server; see: ⇨📄173.

☐ 'Configuring Email Notification via the PRINTSERVER Homepage' ⇨📄134

☐ 'Configuring Email Notification via the PRINTSERVER-NetTool' ⇨📄135

Configuring Email Notification via the PRINTSERVER Homepage

📇 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – Notification***.*
3. *Select* **Email Notification***.*
4. *Configure the parameters; see: Table 12* ⇨📄*135.*
5. *Click* **Save** *to confirm.*
↳ The settings are saved.

Configuring Email Notification via the PRINTSERVER-NetTool

📋 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server or printer in the print server list. The* **Properties** *dialog appears.*
3. *Select* **Configuration – Notification** *from the navigation bar.*
4. *Select* **Email Notification***.*
5. *Select the tab of the relevant recipient.*
6. *Configure the parameters; see: Table 12* ⇨▤*135.*
7. *Click* **OK** *to confirm.*

↳ The settings are saved.

Table 12: Parameters for Email Notification

Parameters	Description
Email active	Enables or disables email notification.
Mail recipient	Here, you can specify the email address of the recipient.
Accounting Job history, Time interval (h), Jobs	Here, you can specify if you want to receive a notification containing information about the number of print jobs processed by the print server. Notifications can be sent after a defined interval or after a defined number of print jobs. Valid numbers are 1 to 60 print jobs.
Accounting * (Page Counter, Time interval (h), Page interval)	Here, you can specify if you want to receive a notification containing information about the number of pages printed by the printer. Notifications can be sent after a defined interval or after a defined number of pages printed.
Printer error * (Paper empty, Paper jam, etc.)	Here, you can specify the type of printer error that will cause a notification.

* In the case of print servers with several physical printer ports, you must select the relevant port.

12.3 How to Get Printer Messages via SNMP Traps

You can get SNMP trap notifications from the connected printers. You can define under which circumstances the printer will send a notification.

This allows two freely definable recipients to get information about the printer status, printer errors (such as Paper empty), the number of pages printed, or print jobs.

The information that can be shown depends on the connected printer model.

☐ 'Enabling SNMP Trap Notification via the PRINTSERVER Homepage' ⇨ 136

☐ 'Enabling SNMP Trap Notification via the PRINTSERVER-NetTool' ⇨ 136

Enabling SNMP Trap Notification via the PRINTSERVER Homepage

Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Configuration – Notification**.
3. *Select* **SNMP Trap Notification**.
4. *Define the recipient via the IP address.*
5. *Configure the parameters; see: Table 13 ⇨ 137.*
6. *Click* **Save** *to confirm.*
↳ The settings are saved.

Enabling SNMP Trap Notification via the PRINTSERVER-NetTool

Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Double-click the print server or printer in the print server list. The* **Properties** *dialog appears.*

3. *Select* **Configuration – Notification***.*
4. *Select* **SNMP Trap Notification***.*
5. *Select the tab of the relevant recipient.*
6. *Define the recipient via the IP address.*
7. *Configure the parameters; see: Table 13* ⇨ 🖹 *137.*
8. *Click* **OK** *to confirm.*

↳ The settings are saved.

Table 13: Parameters for SNMP Trap Notification

Parameters	Description
IP address	Here, you can specify the IP address of the recipient to whom the SNMP traps will be sent.
Trap community	Here, you can specify the Trap community.
Authentication traps	Enables or disables the authentication traps.
Printer traps	Enables or disables the sending of traps in case of a printer error.
Printer error * (Paper empty, Paper jam, etc.)	Here, you can specify the type of printer error that will cause a notification.

* In the case of print servers with several physical printer ports, you must select the relevant port.

12.4   How to Display the Job History

You can get information about the print jobs that have been sent to the print server. 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 print server or printer is turned off or reset. The print jobs will not be deleted when the print server is restarted.

What do you want to do?

☐ 'Displaying the Job History via the PRINTSERVER Homepage'
   ⇨ 🗎138

☐ 'Displaying the Job History via the PRINTSERVER-NetTool'
   ⇨ 🗎138

Displaying the Job History via the PRINTSERVER Homepage

📥 Proceed as follows:

1. Start the PRINTSERVER Homepage.
2. Select **Status – Job History***.*
↳ The Job History is displayed.

Displaying the Job History via the PRINTSERVER-NetTool

📥 Proceed as follows:

1. Start the PRINTSERVER-NetTool.
*2. Double-click the print server in the print server 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. (Depending on the connected printer model)

Table 14: Job History – Status Information

Parameters	Description
Status	'Status' indicates the status of the network connection. The following statuses are possible: - 'Completed' means that the print server has completely forwarded the print job to the printer. - 'Pending' means that the print job has been accepted by the print server but that the data transfer has not yet started. - 'Processing' means that the print job has been transferred from the print server 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 print server has been restarted while the print job was processed.
Port	'Port' shows the port that is used for printing. (This parameter is only available for print server models with several physical printer ports.)
Name	'Name' refers to the name of the print jobs that are handled my means of the protocols HTTP, IPP, LPR, and LPD. The string starts with the identification number of the print job, followed by the host name of the device from which the print job has been spooled.
Protocol	'Protocol' indicates the protocol which has been used for transferring the print data.
Sender	In TCP/IP networks, 'Sender' specifies the sender of the print job.
Size	'Size' indicates the size (in KB) of the print job. The minimal size that is displayed is 1 KB.
Copies	'Pages' refers to the number of pages of the print job.
Creation time	'Creation time' specifies the time at which the print job was sent to the print server.
Duration	'Duration' indicates the time needed by the print server for processing the print jobs. The shortest duration that is displayed is 1 second.

13 Print Jobs and Print Data

This chapter contains information concerning the administration of print jobs and print data. You will learn how to load and assign print jobs directly to the print server, how to time print jobs, and how to modify and convert print data.

What information do you need?

- 'How to Define a Timeout for Taking on Print Jobs' ⇨ 🗎140
- 'How to Assign Print Jobs Directly' ⇨ 🗎141
- 'How to Modify Print Data' ⇨ 🗎143
- 'How to Convert Print Data' ⇨ 🗎145

13.1 How to Define a Timeout for Taking on Print Jobs

You can restrict print jobs to a certain period of time (timeout). If the spooler does not send any print job within the specified time frame, the connection between the print server and the spooler will be interrupted.

Benefits and Purpose

A timeout limits the duration of a connection and thus allows other connections to establish.

📇 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – General**.
3. *Enter the seconds after which the connection will be aborted into the* **Job receive timeout** *box. We recommend to set the value to '120'. If the value is set to '0', this function is disabled.*
4. *Click* **Save** *or* **OK** *to confirm.*
✎ The setting is saved.

13.2 How to Assign Print Jobs Directly

You can assign print jobs directly to the printers via the print server without having to open the file-specific application software.

The print file can be assign via the PRINTSERVER Homepage, the PRINTSERVER-NetTool, or via FTP.

The print file must be in a format that suits the printer. When a print file is downloaded to the print server, the file is automatically recognized as print file and printed.

Make sure that the logical printer does not convert data.

Assigning the Print File via the PRINTSERVER Homepage

🗂 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Actions – Download Area**.
3. *Select* **File Printing**.
4. *Select a logical printer from the list.*
5. *Click* **Browse...**.
6. *Select the print file.*
7. *Click* **Print**.
8. *(Enter the print server password, if necessary).*
↳ The print file is printed.

Assigning the Print File via the PRINTSERVER-NetTool

🗂 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*

---

2. *Mark the print servers in the print server list to which you want to download a print file.*

3. *Select* **Actions – Download – Print File** *from the menu bar. The* **File Download** *dialog appears.*

4. *Click* **Choose**.

5. *Select the print file.*

6. *In the case of password-protected print servers:*
   If the print servers displayed in the list are not password-protected, activate 'Ask for each password'.
   If the print servers displayed in the list are protected by different passwords, activate 'Ask for each password'.
   If the print servers displayed in the list are protected by the same password, activate 'Use this password' and enter the password.

7. *Click* **Start download**.

8. *Confirm the security query.*

9. *(Enter the print server password, if necessary).*

↳ The print file is printed.

13.3 How to Modify Print Data

The print server offers many filters in order to modify print data.

Filter Function 'Find and Replace'

You can edit print data using the filter 'Find and Replace'. For this purpose the print server scans incoming print data streams for specific patterns. As soon as such a pattern is found it will be automatically deleted or replaced by another previously defined pattern.

Benefits and Purpose

It may be useful to edit print data if there is no access to the original documents or if changes to the original files would be too laborious.

You can edit print data using the filter 'Find and Replace'. The filter functions can be configured by means of logical printers; see: 'Logical Printers (Filters)' ⇨🖹178.

Syntax

You can enter various patters into the boxes 'Find' and 'Replace'. Please pay attention to the following syntax:

- 256 characters can be used.

- You can define various patters. Use ';;' as separator. The first pattern that is defined by separators in the 'Find' string will be replaced by the first pattern that is defined by separators in the 'Replace' string.

- In the case of patterns with ASCII text, you can use clear text (depending on the printer driver, etc.)

- Patterns including escape sequences and control characters require special representation. Patterns for hexadecimal code (or other) must be entered as decimal code. In decimal code, each character is represented as three digits (triplets). Each triplet is preceded by a backslash '\'.

Example   In the data stream, the string 'white' is replaced by the string 'black' and the string 'cat' is replaced by the string 'dog'.

	ASCII	Decimal	Hexadecimal
Search	white;;cat	\119\104\105\116\101;;\099\097\116	77 68 69 74 65 63 61 74
Replace	black;;dog	\098\108\097\099\107;;\100\111\103	62 6C 61 63 6B 64 6F 67

Filter Function 'Job Start and Job End'

The print server allows the sending of start and end sequences before/after a print job. These sequences may consist of PRESCRIBE or ESC commands that trigger a form feed after the print job.

ESC commands consist of job start sequence '\027' followed by the actual control characters preceded by a backslash and written as a decimal. Job end sequence '\027 \012', for example, triggers a form feed after the print job. For more information, please look up the available ESC commands in your printer manual.

Configuration is done via logical printers; see: ⇨▤178.

13.4 How to Convert Print Data

The print server offers many filters in order to convert print data.

Filter Function 'HEX Dump Mode' (Hexadecimal + ASCII)

The print server supports the hex dump mode. The hex dump mode is used to search for errors in print data in order to detect communication problems between the computer and the printer.

The hex dump mode displays each character both as hexadecimal code and ASCII character code. Printer control commands are printed as hexadecimal values and do not influence the printout in any way. Configuration is done via logical printers; see: ⇨ 🖹178.

Filter Function 'LF / CR+LF'

Depending on the system, line breaks are coded differently. In order to get the desired result, the print server supports the conversion of print data from LF (Line Feed) to CR+LF (Carriage Return with Line Feed). Configuration is done via logical printers; see: ⇨ 🖹178.

14 Maintenance

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

14.1 How to Print a Service Page

You can print service pages. The service page contains a list of the service-relevant print server parameter values. lists all configurable parameters. The service page is available in English.

Printing the Service Page via the Status Button

Using the status button of the print server operating panel, you can print a service page with all current parameter values of the print server.

Proceed as follows:

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

↳ The service page and the current parameter values are 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. *Change to the directory in which you wish to save the file.*
2. *Open an FTP connection to the print server:*
   Syntax: `ftp <IP Address>`
   Example: `ftp 192.168.0.123`
3. *Enter an arbitrary user name.*
4. *Enter the print server password or press ENTER if no password has been assigned.*
5. *Transfer the service page from the print server 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.

14.2 How to Save Print Server Settings (Backup)

All print server settings (with the exception of passwords) are saved in the 'parameters' file.

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

You can edit the print server parameters using a text editor. Afterwards, the configured file can be downloaded to one or more print servers. The parameters included in the file will be taken over by the print servers.

What do you want to do?

☐ 'Saving the 'Parameters' File to the Client via the PRINTSERVER-NetTool' ⇨▤148

☐ 'Editing the 'Parameters' File using a Text Editor' ⇨▤149

☐ 'Downloading the 'Parameters' File to one or more Print Servers using the PRINTSERVER-NetTool' ⇨▤150

☐ 'Downloading the 'Parameters' File to a Print Server using the Print Server Homepage' ⇨▤151

Saving the 'Parameters' File to the Client via the PRINTSERVER-NetTool

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

Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Mark one or more print servers in the print server list.*
3. *Select* **Actions – Download –** Parameters *File from the menu bar. The* **Parameter Download** *dialog appears; see Fig. 22* ⇨▤*149.*
4. *Mark the printer server(s).*
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.
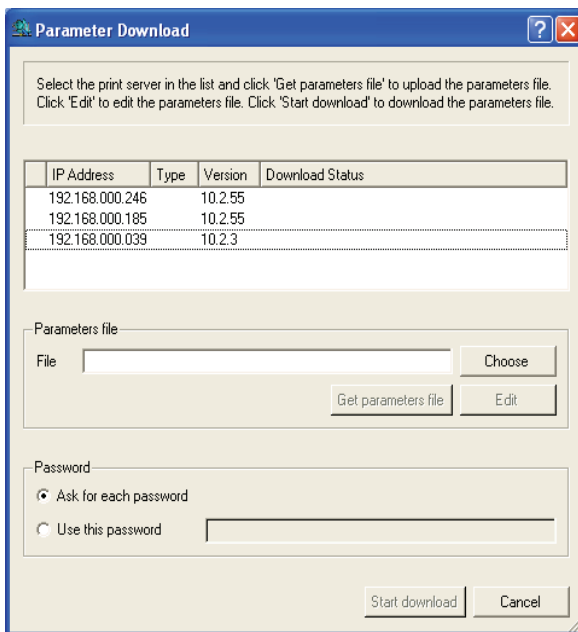
Fig. 22: PRINTSERVER-NetTool - Parameter Download

Editing the 'Parameters' File using a Text Editor

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

📋 Proceed as follows:

1. Start the PRINTSERVER-NetTool.
2. Select a print server from the print server list.
*3. Select **Actions – Download –** Parameters *File from the menu bar.*
   *The **Parameter Download** dialog appears; see Fig. 22 ⇨▤149.*
*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. The syntax and values can be obtained from the parameter list; see:* ⇨▤*209.*
9. *Save the file.*

Downloading the 'Parameters' File to one or more Print Servers using the PRINTSERVER-NetTool

You can configure one or more print servers using the 'parameters' file. For this purpose, the file is downloaded to the print server.

When downloading the 'parameters' file to several print servers, the parameter default settings 'IP address,' 'Host name,' and 'NetBIOS name' of the respective print server will be maintained. All other settings will be overwritten by those in the 'parameters' file.

Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Select one or more print servers from the print server list.*
3. *Select* **Actions – Download Parameters File** *from the menu bar.
   The* **Parameter Download** *dialog appears; see Fig. 22* ⇨▤*149.*
4. *Click* **Choose**.
   The **Parameter Download** *dialog appears.*
5. *Specify the 'parameters' file.*
6. *Click* **Open**.
7. *Decide on the password option:
   If the print server displayed in the list are not
   password-protected or protected by different passwords,
   activate* **Ask for each password**.
   *If the print servers 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 print servers displayed in the list. If you do not want to download the file to all print servers, you must close the dialog and only select the desired print servers from the print server list (see step 2).

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

↳ The 'parameters' file will be downloaded to the print server(s). The print server parameters will be configured in accordance with the file.

Downloading the 'Parameters' File to a Print Server using the Print Server Homepage

The PRINTSERVER Homepage can be used to configure a print server via the 'parameters' file. All previous print server settings will be overwritten by the 'parameters' file.

Proceed as follows:

1. *Start the PRINTSERVER 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 print server password, if necessary.*

↳ The 'parameters' file will be downloaded to the print server. The print server parameters will be configured in accordance with the file.

14.3 How to Reset Parameters to their Default Values

You can reset all print server parameters to their default values (factory default settings). Earlier settings will be deleted in this process. Installed certificates will not be deleted.

⚠

Since the IP address of the print server will be reset as well, the PRINTSERVER Homepage cannot be started or displayed after the reset.

You must reset the parameters, for example, if you want to use the print server in another network by changing the location of the printer. Before this change of location, you should reset the parameters to the default settings to install the print server in another network.

If a password has been set in the print server, the password has to be entered before resetting the parameters. No password is necessary if you reset the print server using the status button of the print server operating panel.

What do you want to do?

☐ 'Resetting Parameters via the PRINTSERVER Homepage' ⇨ 🖹153

☐ 'Resetting Parameters via the PRINTSERVER-NetTool' ⇨ 🖹153

☐ 'Resetting Parameters via an FTP Connection' ⇨ 🖹153

☐ 'Resetting Parameters using the Status Button' ⇨ 🖹154

Resetting Parameters via the PRINTSERVER Homepage

Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Actions – Default Settings***.*
3. *Click* **Default Settings***.*
ↆ The parameters are reset.

Resetting Parameters via the PRINTSERVER–NetTool

Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Select a print server from the print server list.*
3. *Select* **Actions – Default Settings** *from the menu bar.*
4. *Click* **Finish***.*
ↆ The parameters are reset.

Resetting Parameters via an FTP Connection

Proceed as follows:

1. *Open an FTP connection to the print server:*
   Syntax: `ftp <IP Address>`
   Example: `ftp 192.168.0.123`
2. *Enter either the print server password or press ENTER if no password has been assigned.*
3. *Reset the parameters:*
   `quote SITE RESET`
4. *Close the FTP connection:*
   `quit`
5. *As for internal print server models, turn the printer off and back on.*
   As for external print server models, disconnect and reconnect the power socket on the print server or turn the print server off and back on.
ↆ The parameters are reset.

Resetting Parameters using the Status Button

The reset process comprises three different steps.

- In the first step, the print server is forced into reset mode. The parameters are reset in this mode.

- The second step involves restarting the printer or the print server.

- In the third step, a status page is printed. The status page can be used to check whether the parameters were successfully reset. (Note: It is not possible to print a status page via a GDI printer.)

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 print server will go into BIOS mode. In this case you need to start the reset process again.

These three steps are illustrated in the following. Internal and external print server models each have their own processes, which are illustrated separately. The illustrations may vary slightly from your device model.

Before starting the reset process, disconnect the network cable from the print server in order to avoid the distracting flashing Link LED. (Does not apply to WLAN print server models.)

Resetting Internal Print Servers

[Phase 1] Print Server Reset

Turn the printer off.

Press the status button of the print server and keep it pressed.
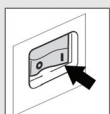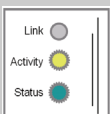
Turn the printer on.

Wait until the Activity- and Status-LED start blinking simultaneously.
The Reset Mode is activate.
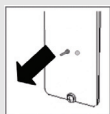
Release the status button for about 2 seconds.

The LEDs blink alternatingly.
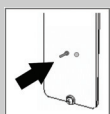
Press the status button once again and keep it pressed.

The LEDs blink simultaneously.

After few seconds only the Activity-LED blinks consistently.

Release the status button.

[Phase 2] Device Restart

Turn the printer off.
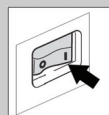
Turn the printer on.

[Phase 3] Status Check
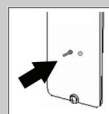
Press the status button for a short time.

Resetting External Print Servers

[Phase 1] Print Server Reset
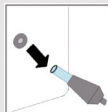
Turn the printer off / Disconnect the power socket
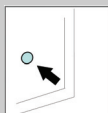
Press the status button and keep it pressed.
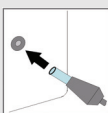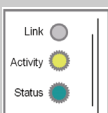
Turn the printer on / Reconnect the power socket

Wait until the Activity- and Status-LED start blinking simultaneously.
The Reset Mode is activate.
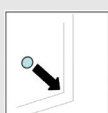
Release the status button for about 2 seconds.

The LEDs blink alternatingly.
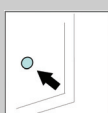
Press the status button once again and keep it pressed.

The LEDs blink simultaneously.
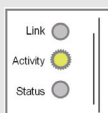
After few seconds only the Activity-LED blinks consistently.
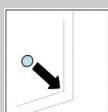
Release the status button.

[Phase 2] Device start
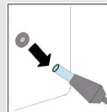
Turn the printer off / Disconnect the power socket
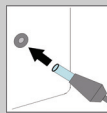
Turn the printer on / Reconnect the power socket

[Phase 3] Status Check
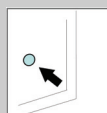
Press the status button for a short time.

* Depending on the print server model, the print server is disconnected via the power switch or by removing the power cable.

14.4 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 some functions do not work properly and if has released a new software version with new functions or bug fixes.

Check the currently installed software version of your print server. The version number can be found in the print server list of the PRINTSERVER-NetTool. You can also start the PRINTSERVER Homepage and select **Status – General**.

Where Do I Find the Update Files?

You can download the current software files from the website of the manufacturer. Different update files are available depending on your print server model.

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

Update Types

A print server 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 print server.

- With a dynamic update, polling is performed each time the print server is restarted 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 print server via FTP.

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

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

Requirements

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

☑ All print jobs are finished.

What do you want to do?

☐ 'Standard Update via the PRINTSERVER Homepage' ⇨ 🖹158

☐ 'Standard Update via the PRINTSERVER-NetTool' ⇨ 🖹159

☐ 'Standard Update via FTP' ⇨ 🖹160

☐ 'Dynamic Update via the PRINTSERVER Homepage' ⇨ 🖹160

☐ 'Dynamic Update via the PRINTSERVER-NetTool' ⇨ 🖹162

☐ 'Dynamic Update via FTP' ⇨ 🖹162

☐ 'Perform an Update to more than one Print Server' ⇨ 🖹163

Standard Update via the PRINTSERVER Homepage

🗗 Proceed as follows:

1. Start the PRINTSERVER 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 print server is restarting.

Standard Update via the PRINTSERVER-NetTool

🔳 Proceed as follows:

1. Start the PRINTSERVER-NetTool.
2. Select a print server from the print server list.
3. Select **Actions – Firmware Update – Standard Update** *from the menu bar. The* **update** *dialog appears; see Fig. 23 ⇨ 📄159.*
4. Click **Choose***.*
5. Select the update file.
6. Click **Start update***.*
7. Confirm the security query.
↳ The update is executed. The print server is restarting.
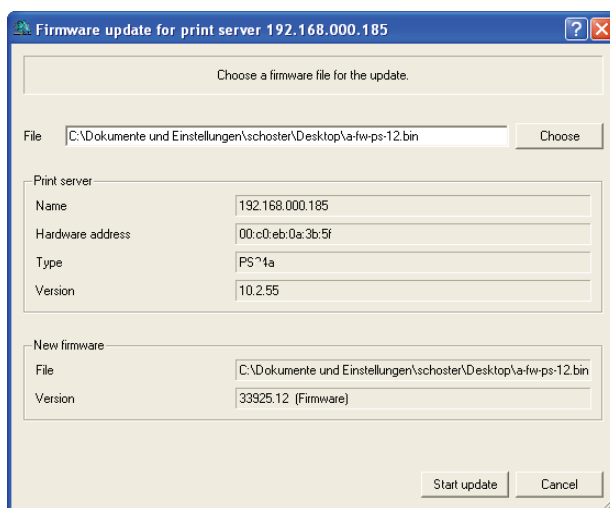
Fig. 23: PRINTSERVER-NetTool - Standard Update

Standard Update via FTP

You can perform a standard update 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 print server:*
   Syntax: `ftp <IP address of the print server>`
   Example: `ftp 192.168.0.123`
3. *Enter an arbitrary user name.*
4. *Enter either the print server password or press ENTER if no password has been assigned.*
5. *Switch to binary mode:*
   `bin`
6. *Send the update file to the print server:*
   Syntax: `put <name of update file> binfile`
   Example: `put a-fw-ps-12.bin binfile`
7. *Close the FTP connection:*
   `quit`

Dynamic Update via the PRINTSERVER 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 print server is set up as 'user' on the file server.

📋 Proceed as follows:

1. *Start the PRINTSERVER 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.*
   Syntax: `ftp://<file server IP address>/`

```
<Software file name>
```
Example: `ftp://192.168.0.100/a-fw-ps-12.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/a-fw-ps-12.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 print server verifies the version of the software files. If the print server detects a higher version, this version will be installed automatically on the print server.
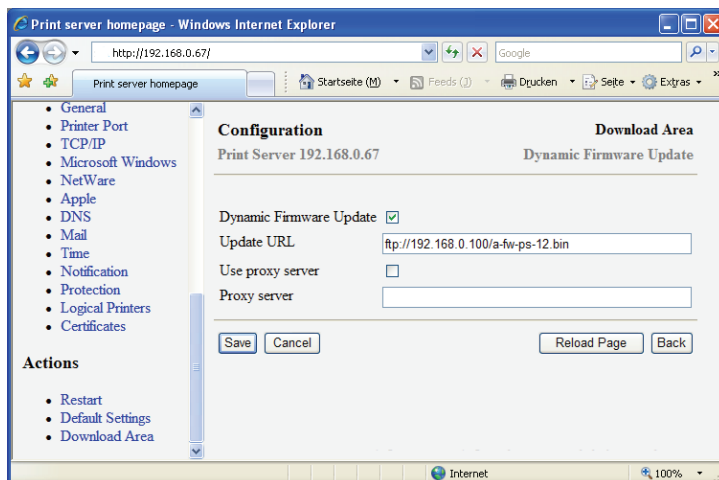
Fig. 24: PRINTSERVER Homepage - Dynamic Update

Dynamic Update via the PRINTSERVER-NetTool

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

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

📁 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Select a print server from the print server 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/a-fw-ps-12.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/a-fw-ps-12.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 print server verifies the version of the software files. If the print server detects a higher version, this version will be installed automatically on the print server.

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' ⇨ 📄34.

Perform an Update to more than one Print Server

The PRINTSERVER-NetTool allows you to carry out an update to more than one print server.

Requirements

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

▣ Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Select the print servers from the print server list.*
3. *Select* **Actions – Firmware Update from the menu bar.** *The* **Dynamic Update** *dialog appears; see Fig. 24* ⇨ 📄 *161.*
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 print servers by right-clicking the print server.*
8. *If one single password is used for all print servers, select* **Use this password** *and enter the password.*
9. *Click* **Start update***.*
10. *Confirm the security query.*
↳ The update is executed. The print servers are restarted.
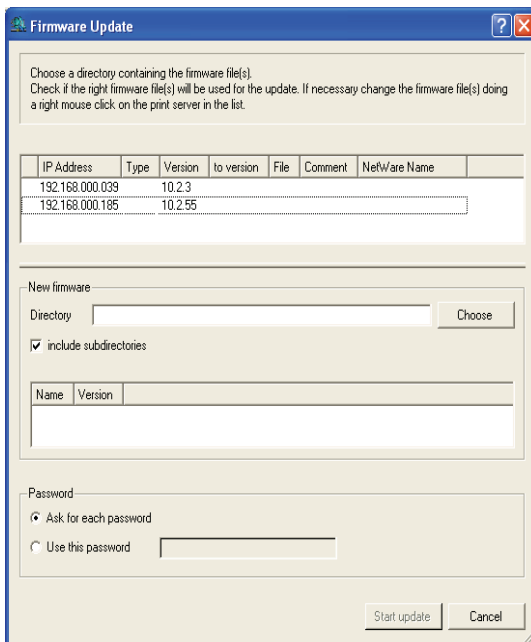
Fig. 25: PRINTSERVER-NetTool - Update

14.5　How to Restart the Print Server

The print server can be restarted manually. A restart is usually not necessary.

Restarting the Print Server using the PRINTSERVER Homepage

📂 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Actions – Restart**.
3. *Click* **Restart Print Server**.
↳ The print server is restarting.

Restarting the Print Server via the PRINTSERVER-NetTool

📂 Proceed as follows:

1. *Start the PRINTSERVER-NetTool.*
2. *Select a print server from the print server list.*
3. *Select* **Actions – Restart** *from the menu bar.*
   The **Restart print server** *dialog appears.*
4. *Click* **Finish**.
↳ The print server is restarting.

15 Supported Network Protocols

Print servers support a multitude of protocols. This chapter explains to you which protocols you can use, how to configure them and which print server features can be activated by means of these protocols.

Depending on your network type and printing requirements, you will need different protocols to operate the print server. We recommend disabling all protocols in the print server that you do not need.

If you have disabled a protocol, all functions based on this protocol are no longer available.

What information do you need?

- 'HTTP' ⇨🖹167
- 'TCP/IP' ⇨🖹167
- 'IPv6' ⇨🖹169
- 'NetBIOS/WINS' ⇨🖹170
- 'POP3' ⇨🖹172
- 'SMTP' ⇨🖹173
- 'SNTP' ⇨🖹175
- 'SNMP' ⇨🖹175

15.1 HTTP

HTTP (Hypertext Transfer Protocol) is a protocol for data transfer. HTTP requires a reliable transport protocol for communication purposes. TCP is used in virtually all cases.

The print server needs HTTP for the data transfer of the PRINTSERVER Homepage and the PRINTSERVER Print Monitor.

If you have disabled HTTP, all functions based on this protocol are no longer available. The PRINTSERVER Homepage or printing via HTTP using the PRINTSERVER Print Monitor will no longer be available.

Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – Protection***.*
3. *Tick/clear* **HTTP***.*
4. *Click* **Save** *or* **OK** *to confirm.*
   ꙅ The setting is saved.

15.2 TCP/IP

'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 establishs 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 print server into a TCP/IP network.

If you have disabled TCP/IP, all functions based on this protocol are no longer available. This means that, for example, the PRINTSERVER Homepage or FTP will no longer be available.

Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – TCP/IP***.*
3. *Configure the TCP/IP parameters; see: Table 15* ⇨▤*168.*
4. *Click* **Save** *or* **OK** *to confirm.*
↳ The settings are saved.

Table 15: TCP/IP Parameters

Parameters	Description
TCP/IP	Enables/disables TCP/IP
IP Address	IP address of the print server
Subnet Mask	Subnet mask of the print server
Gateway	Gateway address of the print server
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 Print Server (Upon delivery, the default name is displayed)
Contact person	Freely definable description
Location	Freely definable description

Parameters	Description
DHCP BOOTP ARP/PING ZeroConf	Enables/disables the protocols 'DHCP', 'BOOTP', 'ARP/PING', and 'ZeroConf'. Protocols offer various possibilities to save the IP address in the print server. (See: 'Saving the IP Address in the Print Server' ⇨ 📄15). We recommend disabling these options once an IP address has been assigned to the print server.

15.3 IPv6

You can integrate the print server into an IPv6 network and configure several IPv6 settings.

Requirements   ☑ The print server is connected to a network that supports IPv6.

📂 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – IPv6***.*
3. *Configure the IPv6 parameter; see: Table 16 ⇨ 📄169.*
4. *Click* **Save** *or* **OK** *to confirm.*
↳ The settings are saved.

Table 16: IPv6 Parameters

Parameter	Description
IPv6	Enables/disables the IPv6 functionality of the print server.
IPv6 address	Defines a print server IPv6 unicast address assigned manually in the format n:n:n:n:n:n:n:n. *Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.*

Parameter	Description
Router	Defines the IPv6 unicast address of the router. The print server sends his 'Routers Solicitations' (RS) to this router.
Prefix length	Defines the length of the subnet prefix for the IPv6 address. (The value 64 is preset.) *Address ranges are indicated by prefixes. The prefix length (Number of used bits) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/' .*
Automatic configuration	Enables/disables the automatic assignment of the IPv6 address for the print server.

15.4 NetBIOS/WINS

'NetBIOS' (Network Basic Input Output System) allows you to address a client in Microsoft Windows networks not only via a unique TCP/IP address but also via a unique NetBIOS name.

Benefits and Purpose

'WINS' (Windows Internet Naming Service) is a system for the dynamic resolution of NetBIOS names. WINS works similar to DNS and is also dynamic. If a new host enters the network, its name will automatically be registered with the WINS server. The client registers the NetBIOS name of the computer as well as the domain name and the name of the registered users and user groups.

To use this service, you must configure a couple of Microsoft Windows parameters such as the NetBIOS name, the NetBIOS domain, and the WINS server.

📋 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – Microsoft Windows**.
3. *Configure the parameters; see: Table 17* ⇨📄*171.*
4. *Click* **Save** *or* **OK** *to confirm.*
↳ *The settings are saved.*

Table 17: Microsoft Windows Parameters

Parameters	Description
NetBIOS	Enables/disables peer-to-peer printing
NetBIOS Name	Print Server Name Appears in the relevant workgroup or domain
NetBIOS domain	Name of an existing workgroup or domain
NetBIOS refresh every	Time interval (in minutes) for updating the NetBIOS parameters
WINS registration	Enables/disables the WINS services
WINS via DHCP	If you have enabled 'WINS via DHCP,' you can enter the IP address of the WINS server via DHCP. If 'WINS via DHCP' is disabled, you can enter the IP address of the WINS server manually.
Primary WINS server	IP address of the primary WINS server
Secondary WINS server	IP address of the secondary WINS server

15.5 POP3

'POP3' (Post Office Protocol Version 3) is a transfer protocol that a client can use to fetch emails from a mail server.

Benefits and Purpose

POP3 is used in print servers to administer print servers via email; see: ⇨ 🖹36.

Requirements

☑ A DNS server has been configured on the print server; see: ⇨ 🖹65.

📑 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – Mail – POP3***.*
3. *Configure the POP3 parameters; see: Table 18 ⇨ 🖹172.*
4. *Click* **Save** *or* **OK** *to confirm.*
↳ The settings are saved.

Table 18: POP3 Parameters

Parameters	Description
POP3	Enables/disables the POP3 support.
Server name	Defines the name of the POP3 server.
User name	Defines the name used by the print server to log on to the POP3 server.
Security	Here, you can select an authentication method (SSL, APOP).
Check mail every	Here, you specify the time interval (in minutes) for retrieving emails from the POP3 server.
Server port	Specifies the port of the POP3 server. Default: 110. When using SSL, specify port 995.
Password	Defines the password used by the print server to log on to the POP3 server.
Delete read messages	Here, you can enables/disables the automatic deletion of read emails.

Parameters	Description
Ignore mail exceeding	Here, you can specify the maximum email size (in KB) to be accepted by the print server. (0 = unlimited)

15.6 SMTP

SMTP (Simple Mail Transfer Protocol) is a protocol that controls the sending of emails in networks.

Benefits and Purpose

SMTP is needed in the print server to administer the print server via email (see: ⇨📄36) and get printer information via email (see: ⇨📄134).

Requirements

☑ A DNS server has been configured on the print server; see: ⇨📄65.

📂 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – Mail – SMTP***.*
3. *Configure the SMTP parameters; see: Table 19 ⇨📄173.*
4. *Click* **Save** *or* **OK** *to confirm.*
↳ The settings are saved.

The PRINTSERVER Homepage offers an alternative access to the SMTP input mask. The SMTP input mask can also be found under the menu item 'Configuration' - 'Notification' - 'Email Notification'.

Table 19: SMTP Parameters

Parameters	Description
Server name	IP address or Host name of the SMTP server

Parameters	Description
Server port	Defines the port number used by the ISD to send emails to the SMTP server. (Default = 25)
TLS	Enables or disables TLS. The TLS protocol serves to encrypt the transmission between the print server and the SMTP server.
Sender name	Here, you can specify the email sender name to be used by the print server. If no sender name is specified, the default name of the print server will be used.
Signature	Here, you can specify the signature to be used in an email generated by the print server. The print server name, serial number and IP address are used as default values. You can enter a maximum of 128 characters.
Use POP3 settings	Here, you can specify whether the POP3 settings for authentication shall be used or whether you want to configure your own parameters.
SMTP Authentication (User name, Password)	Here, you can specify the user name and password for the SMTP authentication.

15.7 SNTP

SNTP (Simple Network Time Protocol) is a simplified version of the NTP. NTP (Network Time Protocol) is a protocol for synchronizing the clocks of computer systems in networks.

Benefits and Purpose

SNTP is needed in the print server to control the device time of the print server via a time server in networks; see: 'How to Configure the Device Time' ⇨ 🖹67.

📑 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – Time***.*
3. *Configure the SNTP parameters; see: Table 20* ⇨ 🖹*175.*
4. *Click* **Save** *or* **OK** *to confirm.*

↳ The settings are saved.

Table 20: SNTP Parameters

Parameters	Description
SNTP	Enables/disables the use of a time server.
Time server	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	The time zone is used to equalize the difference between the Greenwich Mean Time or UTC (Universal Time Coordinate) of the time server and the local time.

15.8 SNMP

'SNMP (Simple Network Management Protocol) has become the standard protocol for the administration and monitoring of network elements. SNMP is used for providing and transferring management information within the network.

The SNMP architecture is based on one or more management stations and several network elements with one or more implemented network management agents. SNMP is used for communication between the management stations and the agents.

SNMP allows you to read and edit management information provided by the network elements. The collection of management information of a device is called MIB.

Private MIB of the Print Server

As an agent, the print server provides the standard 'MIB-II' and a 'private MIB' (Management Information Base). All print server parameters and status information are saved in the 'private MIB'. The 'private MIB' is saved in the print server on delivery and can be installed immediately. On the PRINTSERVER LIBRARY CD you will find a formal description of the private MIB objects. If there is no PRINTSERVER LIBRARY CDincluded in the delivery, please consult your retailer or printer manufacturer.

Benefits and Purpose

The print server parameters can be queried and configured by a management tool, such as OpenView or TransView, by means of the SNMP protocol. In case of an error, such as 'Paper empty', the print server automatically sends an error message, the so-called trap, to pre-defined IP address.

In order to receive SNMP traps, you must configure the IP address and enable the traps; see: 'How to Get Printer Messages via SNMP Traps' ⇨🖹136.

Requirements

When using SNMP, make sure that:

☑ The TCP/IP protocol is installed on any client intended for printing.

☑ The print server is connected to the network and the printer.

☑ The print server is known to the network via its IP address; see: ⇨🖹15.

16 Additional Features

Some print server models have additional features that go beyond normal print server features. This chapter describes scenarios, backgrounds, and methods that can extend the features of the print server.

Which features will be supported depends on your printer sever model.

16.1 Logical Printers (Filters)

What Are Logical Printers?

Logical printers are pre-installed filters that are assigned to a print object. The filter contains information about the print data.

The print data that is received by the print server will be interpreted and processed depending on the filter settings. This way, print data flows can be manipulated, converted, and sent via defined TCP/IP ports and printer ports.

Logical printers can be used to adapt the print server to various printing needs and networks. All print server models have eight logical printers.

Functions of Logical Printers

The following functions can be used via logical printers:

- The **printer port** of print server models with several physical printer ports (COM1, USB1, etc.) is defined via the logical printer.

- The logical printer defines which **TCP/IP port** is used to send the print data.

- Depending on the system, line breaks are coded differently. In order to get the desired result, the print server supports the conversion of print data from LF (Line Feed) to **CR+LF** (Carriage Return with Line Feed).

- The print server supports the **hex dump mode**. The hex dump mode is used to search for errors in print data in order to detect communication problems between the computer and the printer. The hex dump mode displays each character both as hexadecimal code and ASCII character code. Printer control commands are printed as hexadecimal values and do not influence the printout in any way.

- The print server allows the sending of **start** and **end sequences** before/after a print job. These sequences may consist of PRESCRIBE or ESC commands that trigger a form feed after the print job; see: 'How to Modify Print Data' ⇨🖹143.

- The print server supports a function called **Search** and **Replace**. This allows you to search for strings within the print data sent to the print server and to replace the strings, if necessary; see: 'How to Modify Print Data' ⇨ 🖹143.

Preset Functions of Print Servers with One Port

The following functions of logical printers (no. 1-8) are preset for print servers that have a physical printer port.

Logical Printer	Preset Function	Preset TCP/IP Port
1	Default setting	9100
2	Conversion of Line Feed (LF) to Carriage Return with Line Feed (CR+LF)	9101
3	Not assigned	9102
4	Printing of a banner page when the LPD protocol is used	9103
5	Enables the Hex dump mode	9104
6	Not assigned	9105
7	Not assigned	9106
8	Not assigned	9107

Preset Printer Ports of Print Servers with Several Printer Ports

The following printer ports of the logical printers (no. 1-8) are preset for print servers that have several physical printer ports.

Physical Printer Ports	Logical Printer	TCP/IP Port	Preset Printer Port
	1	9100	USB1
	2	9101	USB2
2 X	3	9102	USB3
	4	9103	USB4
Note: You can connect a hub to the USB port 2. In this case, five printers can be administered via USB 1 through 5 by means of the TCP/IP ports	5	9104	USB5
	6	9105	USB1
	7	9106	USB1
	8	9107	USB1

Physical Printer Ports	Logical Printer	TCP/IP Port	Preset Printer Port
	1	9100	LPT1
1 X	2	9101	USB1
	3	9102	USB2
1 X	4	9103	USB3
	5	9104	USB4
Note: You can connect a hub to the USB port. In this case, four printers can be administered via USB 1 through 4 by means of the TCP/IP ports	6	9105	LPT1
	7	9106	LPT1
	8	9107	LPT1

Physical Printer Ports	Logical Printer	TCP/IP Port	Preset Printer Port
	1	9100	LPT1
1 X	2	9101	LPT2
	3	9102	LPT3
3 X	4	9103	COM1
	5	9104	LPT1
	6	9105	LPT1
	7	9106	LPT1
	8	9107	LPT1

Physical Printer Ports	Logical Printer	TCP/IP Port	Preset Printer Port
	1	9100	USB1
	2	9101	USB2
3 X	3	9102	USB3
	4	9103	USB1
	5	9104	USB1
	6	9105	USB1
	7	9106	USB1
	8	9107	USB1

How to Use Logical Printers

In order to use the logical printers in an ideal way, you must configure the logical printer with the desired function. Then you must assign the logical printer to a print object. (This procedure can also take place in reversed order.)

What do you want to do?

☐ 'Configuring the Logical Printers' ⇨ 📄182

☐ 'Assigning Logical Printers' ⇨ 📄183

Configuring the Logical Printers

You can adapt the assigned functions and printer ports to your needs.

📑 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – Logical Printer.**
3. *Change the desired parameters, see: Table 21* ⇨ 🗎 *182.*
4. *Click* **Save** *or* **OK** *to confirm.*
↳ The setting is saved.

Table 21: Settings of the Logical Printers

Parameters	Description
Start Sequences / End Sequences	Depending on the application, you might have to configure the logical printer. These sequences may consist of PRESCRIBE or ESC commands. ESC commands consist of job start sequence '\027' followed by the actual control characters preceded by a backslash and written as a decimal. Job end sequence '\027 \012', for example, triggers a form feed after the print job. For more information, please look up the available ESC commands in your printer manual.
Search/ Replace	Using 'Find' and 'Replace,' you can look for strings in the data sent to the print server and replace them with new strings. Wildcards and truncations cannot be used. The string can consist of max. 256 characters.
Hex dump mode	Enables/disables the hex dump mode. The hex dump mode is mainly used to search for errors in print data. The hex dump mode displays each character both as hexadecimal code and ASCII character code. Printer control commands are printed as hexadecimal values and do not influence the printout in any way.
CR + LF	Enables/disables the conversion from line feed (LF) to carriage return with line feed (LF+CR).
Banner page	Enables/disables the printing of a banner page when the LPD protocol is used.
Banner page mode	Defines the format in which the banner page will be printed. (ASCII)

Parameters	Description
TCP/IP Port	TCP/IP port in accordance with the logical printer. The following default values apply: no. 1 = 9100 no. 2 = 9101 no. 3 = 9102 no. 4 = 9103 no. 5 = 9104 no. 6 = 9105 no. 7 = 9106 no. 8 = 9107
Printer Port	Defines the port used by the logical printer for printing. (This parameter is only available for print server models with several physical printer ports.)

Assigning Logical Printers

Depending on your system, logical printers may be addressed in various ways. The assignment often takes place during the print server installation; see: 'Print Server Installation' ⇨ 🖹40.

Table 22: Addressing Logical Printers in Systems

System	Syntax
Windows	In Windows networks, you may use the corresponding TCP/IP ports instead of the logical printers; see 'TCP/IP Port' ⇨ 🖹206.
FTP	In the case of an FTP print data transfer, the logical printers are addressed with 'lp1' through 'lp8'. Example: put <file name> lp1

16.2 ThinPrint® (Print Data Compression)

What is ThinPrint®?

The ThinPrint® technology enables the transmission of compressed and bandwidth-optimized print jobs within a network. Implementing '.print Clients' in print servers enables the reception and decompression of compressed print data.

Basic Functions

Print jobs are compressed using the server component of the .print technology, the so-called '.print Engine'. Depending on the environment, this software module will be installed on the application server or a central print server. The server sends the compressed print data to the print server with the implemented '.print Client'. The print server then decompresses the print data, transferring it to the respective printer.

What do you want to do?

☐ 'Addressing Print Servers in ThinPrint® Environments' ⇨▤184

☐ 'Configuring the ThinPrint® Port' ⇨▤185

☐ 'Controlling the Bandwidth' ⇨▤185

☐ 'Using .print AutoConnect' ⇨▤186

☐ 'Receiving Encrypted ThinPrint® Data' ⇨▤187

Addressing Print Servers in ThinPrint® Environments

You must use the following syntax if you want to address the print server in ThinPrint® environments:

Syntax:

```
<IP address or host name of the print server>:
<number of the logical printer>#<arbitrary name>
```

Example:

```
192.168.0.123:1#IC0001FF
```

Printing via LPR is not possible.

Configuring the ThinPrint® Port

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

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

📋 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – ThinPrint®**.
3. *Enter the port number into the* **ThinPrint® port** *box.*
4. *Click* **Save** *or* **OK** *to confirm.*
✎ The setting is saved.

Controlling the Bandwidth

The bandwidth describes the capacity of a data connection. The bandwidth of the print server 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 print server (client side).

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

📋 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – ThinPrint®**.
3. *Tick* **Bandwidth**.
4. *Enter the desired bandwidth.*
5. *Click* **Save** *or* **OK** *to confirm.*

↳ The setting is saved.

Using .print AutoConnect

.print AutoConnect is a tool within the .print technology for the automatic creation of print objects. The print objects are created on the basis of defined templates without the need to automatically load the printer drivers.

Printers can be combined in printer groups and printer locations on the basis of so-called printer classes. A name table translation (Dynamic Printer Matrix) simplifies the creation of classes and the assignment of printers.

In the case of several drivers we recommend the assignment of the appropriate printer drivers via the printer class. This assignment can be set up accordingly in the printer configuration on the .print client.

📑 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – ThinPrint®***.*
3. *Configure the parameters; see: Table 23 ⇨📄186.*
4. *Click* **Save** *or* **OK** *to confirm.*

↳ The setting is saved.

Table 23: ThinPrint® AutoConnect Parameters

Parameter	Description
ID	The ID clearly identifies the printers for the ThinPrint® server.
Printer	The printer name is bound to the ID and gives the print object a description for a better differentiation.
Class	Printers with compatible drivers can be arranged in one class.
Driver	Specifies the printer driver for the embedded printer.

Receiving Encrypted ThinPrint® Data

A secure connection during the transfer of print jobs between the ThinPrint® server and the print server is guaranteed by means of an SSL encryption. The ThinPrint® server requests a certificate from the print server. By means of this certificate, the ThinPrint® server checks whether the print server is authorized to receive the print data.

If encryption was enabled on the ThinPrint® server, you must install a certificate from a corresponding Certification Authority both on the ThinPrint® server and the print server.

To authorize the print server to receive encrypted print data, proceed as follows:

- Create a certificate request; see: 'How to Create a Certificate Request for CA Certificates' ⇨🖹102.

- Save the CA certificate; see: 'How to Save CA Certificates in the Print Server' ⇨🖹104.

16.3 WLAN (Wireless Local Area Network)

What is WLAN?

WLAN is a radio technology that allows you to establish wireless connections between network components. The WLAN technology is defined as a standard of the IEEE 802.11 family.

If your print server supports WLAN, you can operate the print server wirelessly in the network. The print server has additional parameters that are described in the following.

WLAN Settings

Communication Modes

The communication mode (the operating mode) defines the network structure in which the print server will be installed. Two modes are available:

- In the 'Ad-Hoc' mode, the print server communicates directly with another WLAN client (peer-to-peer).

- The 'infrastructure' mode is suitable for setting up large wireless networks with several devices in different rooms. Communication between the devices is done via an access point which is connected to the network. The access point can be protected by encryption or authentication.

SSID

The ID of a wireless network is referred to as SSID (Service Set Identifier) or network name. Each wireless LAN has a configurable SSID in order to clearly identify the wireless network. The SSID is configured in the access point of a Wireless LAN. Each device (PC, print server, etc.) that is intended to have access to the wireless network must be configured using the same SSID.

Channel (Frequency Range)

The product uses the 2.4 GHz ISM band. A channel has a bandwidth of 22 MHz. The distance between two neighboring channels is 5 MHz.

Neighboring channels overlap, which can lead to interferences. If several WLANs are operated in a small radius, a distance of at least five channels should exist between two channels.

Channel 3 is preset.

Keep yourself informed about national provisions regarding the use of WLAN products and only use authorized channels.

Roaming Roaming refers to the use of end devices (such as print servers) or just to the use of the participants' identity between two networks. This setting is primarily used for the interaction with CISCO Hot Spots.

The transmitting power of the print server can be configured via the 'dBm' paramter.

Security Settings

Make sure that no unauthorized user logs on to the Wireless LAN and that no one has access to the Internet or network resources. Your print server offers several security mechanisms.

Standard	Mechanism	
	Encryption	Authentication
WEP	WEP (Open System / Shared Key)	---
WEP+EAP	WEP (Open System)	EAP (TLS / MD5 / LEAP / TTLS / PEAP / FAST)
WPA (Personal Mode)	TKIP/MIC	PSK
WPA2 (Personal Mode)	AES-CCMP	PSK
WPA (Enterprise Mode)	TKIP/MIC	EAP (TLS / MD5 / LEAP / TTLS / PEAP / FAST)
WPA2 (Enterprise Mode)	AES-CCMP	EAP (TLS / MD5 / LEAP / TTLS / PEAP / FAST)

WEP WEP (Wired Equivalent Privacy) is an encryption method according to IEEE 802.11 on the basis of the RC4 encryption algorithm. WEP offers mechanisms for data encryption and authentication. WEP uses a key to encrypt the entire communication. As for encrypted access points, the same WEP key must be used for the access point and the print server.

Some access points convert WEP keys that are entered as ASCII text into arbitrary hexadecimal values. In this case, the WEP keys for the access point and the print server do not match. It is therefore recommended to use hexadecimal WEP keys.

WPA /WPA2 In contrast to WEP, WPA (Wi-Fi Protected Access) offers enhanced mechanisms for exchanging keys. The exchange key is only used at the beginning of a session. Afterwards a session key is used. The key is regenerated periodically. The WPA mechanism requires an authentication at the beginning of a connection.

In the 'Personal Mode' authentication is done via the Pre Shared Key (PSK). The PSK is a password with 8–63 alphanumerical characters. The 'Enterprise Mode' uses the EAP authentication method.

An individual 128 bit key is used for data encryption after the authentication. The following two encryption methods can be distinguished:

- TKIP (Temporal Key Integrity Protocol) for WPA
- AES (Advanced Encryption Standard) for WPA2

Authentication You can check the identity of a device or user by means of an authentication method before they gain access to resources in the network. The print server offers different variants of EAP (Extensible Authentication Protocol) as authentication method. For further information; see: 'Print Server Network Authentication' ⇨ 🖹87.

Print Server and Network Settings

The factory default settings of the print server are described in the following.

Mode:	ad-hoc
SSID:	wlsetup
Channel:	3

You can find the current print server settings on the status page. To print a status page, press the status button of the print server.

Decide in which network structure you want to operate the print server. Familiarize yourself with the current settings of your wireless network. The following questions will help you:

- Which communication mode is used in the network?
  (Ad-Hoc / Infrastructure)

- Which SSID is used in the network?

- Does the network use some kind of encryption?
  - Which type of key is used?
  - What is the key called?

- Which authentication method is used?
  (Open System / Shared Key / EAP)
  - Shared Key: What is the key called?
  - EAP-TLS / TTLS: Where is the root certificate stored?
  - EAP-MD5 / LEAP: What user name and password is used for the print server as user of the RADIUS server?
  - EAP-PEAP/FAST: Which Variants are Configured?

Installing the Print Server in WLAN

☑ The current network settings are known.

☑ The print server is connected to a printer and the mains supply;
see: 'Hardware Installation Guide'.

☑ The PRINTSERVER-NetTool is installed on the client; see: ⇨📄27.

☑ The client can set up a wireless connection.

📂 Proceed as follows:

1. *In order to communicate with the print server, you must adapt the wireless network settings of your computer to the current settings of the print server.*

2. *Start the PRINTSERVER-NetTool and find the print server in the print server list; see: ⇨📄27.*

3. *Select the print server from the print server list.*

4. *Select* **Installation – Wireless Wizard** *from the menu bar. The Wireless Wizard is started.*

5. *Follow the instructions of the Wireless Wizard.*

6. *Enter the IP address manually or select a method for the automatic assignment of IP addresses.*

7. *Alternatively, the Wizard expects you to enter a temporary IP address.*
   The temporary IP address is needed for configuration purposes. It does not have to be identical to the target IP address. The temporary IP address must be within the address range of the configuration PC. Example:
   - PC IP = 192.168.100.001 / subnet mask = 255.255.255.000
   - print server IP = 192.168.100.002 / subnet mask = 255.255.255.000

8. *Select the communication mode:*
   'Ad-Hoc' to operate the print server 'Peer to Peer'.
   'Infrastructure' to operate the print server within a network with an access point.

9. *Enter the SSID:*
   Enter a freely definable name if you want to operate the print server in the 'Ad-Hoc' mode.
   Enter the SSID of the access point if you want to operate the print server in the 'Infrastructure' mode.

10. *Select a WLAN security mode and follow the instructions.*

11. *Check your entries and click* **Finish**. *The settings are saved and the print server is restarted.*

12. Adapt the WLAN settings of your computer to the current settings of the print server.

13. Select **Find New** *from the* **Search** *menu of the PRINTSERVER-NetTool and find the print server in the print server list.*

14. Carry out the print server software installation on your PC. For further information; see: 'Print Server Installation' ⇨ 🖹 *40.*

Troubleshooting

If the print server is not displayed in the print server list, print a status page and verify the data; see: 'Printing the Status Page via the Status Button' ⇨ 🖹 62.

In the event of incorrect entries, reset the print server parameters and repeat the installation; see: 'How to Reset Parameters to their Default Values' ⇨ 🖹 152.

16.4 IPv6 (Printing in IPv6 Networks)

You can integrate the print server into an IPv6 network. The print server supports printing in Windows systems via LPD.

What are the Advantages of IPv6?

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

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

What is the Structure of an IPv6 Address?

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

Each field is separated by a colon (:).
<u>Example:</u> `fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4`

Leading zeros in a field can be omitted.
<u>Example:</u> `fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4`

An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used. However, the use of two colons can be used only once in an address.
<u>Example:</u> `fe80 :                    : 10 : 1000 : 1a4`

As a URL in a Web browser, an IPv6 address must be enclosed in brackets. This prevents port numbers from being mistakenly regarded as part of an IPv6 address.
<u>Example:</u> `http://[2001:608:af:1::100]:443`

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

Which Types of IPv6 Addresses are available?

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

- Unicast addresses can be routed globally. These addresses are unique and therefore unambiguous. A packet that is sent to a unicast address will only arrive to the interface that is assigned to this address. Unicast addresses have the prefixes '2' or '3'.

- Anycast addresses are assigned to more than one interface. This means that a data packet that is sent to this address will arrive at various devices. The syntax of anycast addresses is the same as the one of unicast addresses. The difference is that anycast addresses choose one interface out of many.
  A packet that is dedicated to an anycast address arrives at the nearest interface (in line with the router metrics). Anycast addresses are only used by routers.

- Multicast addresses allow you to send data packets to different interfaces at the same time without a proportional increase of the bandwidth. A multicast address can be recognized by the prefix 'ff'.

What do you want to do?

☐ 'Saving IPv6 Addresses' ⇨📄196

☐ 'Displaying IPv6 Addresses' ⇨📄196

☐ 'Configuring IPv6 Settings' ⇨📄197

☐ 'Printing in IPv6 Networks using the Print Server' ⇨📄198

Saving IPv6 Addresses

For information about the automatic assignment of IPv6 addresses; see: ⇨📄20.

Assigning IP Addresses manually

You can assign a unicast address to the print server manually.

📒 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – IPv6**.
3. *Tick* **IPv6.**
4. *Enter the IPv6 unicast address into the* **IPv6 address** *box.*
5. *Click* **Save** *or* **OK** *to confirm.*

↳ The setting is saved.

Displaying IPv6 Addresses

The IPv6 addresses that are saved in the print server can be displayed.

Requirements

☑ The print server is connected to a network that supports IPv6.

☑ The 'IPv6' parameter has been enabled in the print server.

📒 Proceed as follows:

1. *Start the PRINTSERVER Homepage.*
2. *Select* **Status – IPv6**.

↳ The IPv6 addresses are displayed.

Configuring IPv6 Settings

You can configure several IPv6 settings.

Requirements   ☑ The print server is connected to a network that supports IPv6.

📑 Proceed as follows:

1. *Start the PRINTSERVER Homepage or start the PRINTSERVER-NetTool and double-click the print server in the print server list.*
2. *Select* **Configuration – IPv6**
3. *Configure the IPv6 parameter.*
4. *Click* **Save** *or* **OK** *to confirm.*

↳ The settings are saved.

Table 24: IPv6 Parameters

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

Printing in IPv6 Networks using the Print Server

In Windows systems, you can print via LPD and use a print server that was addressed via IPv6.

———————

Windows 95 and Windows 98 are not supported.

———————

Requirements

☑ Service Pack 1 or Service Pack 2 is installed for Windows XP.

☑ In the case of Windows 2000 and Windows 2003 you need to make certain adjustments. Contact the manufacturer of your operating system for further information.

☑ On the Windows system, the element 'TCP/IP Version 6' is installed and enabled under 'Network Properties'.

Procedure

Follow these steps if you want to print:

☐ Installing the Windows Component 'Print Services for Unix' on the Client

☐ Adding an 'LPR Port' to an Installed Printer

Installing the Windows Component 'Print Services for Unix' on the Client

Proceed as follows:

1. *Start the dialog* **Network Connections** *on your Windows client. (Start --> Settings --> Network Connections)*

2. *Select* **Advanced – Optional Networking Components** *from the menu bar. The Windows Optional Networking Components Wizard is started.*
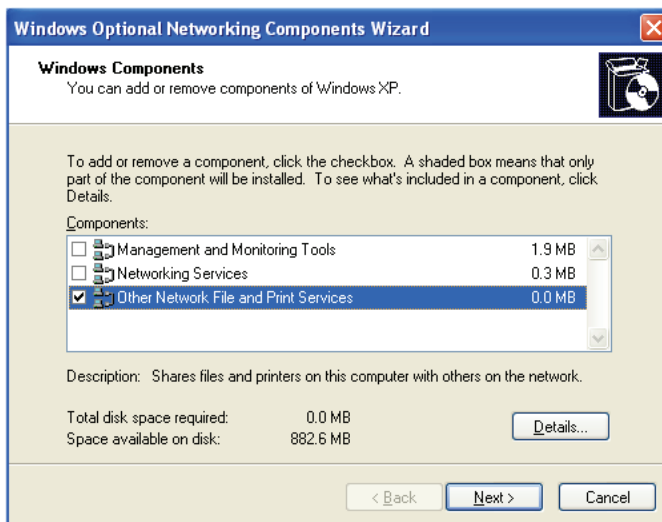
Fig. 26: Windows – Optional Networking Components

3. *Tick* **Other Network File and Print Services***.*
4. *Click* **Details***. The subcomponents of* **Other Network File and Print Services** *are displayed.*
5. *Install and enable the subcomponent* **Print Services for Unix***.*
↳ **LPR Port** is displayed in the **Printer Ports** dialog.

Adding an 'LPR Port' to an Installed Printer

🖅 Proceed as follows:

1. *Start the* **Printers and Faxes** *dialog on your Windows client. (Start --> Settings --> Printers and Faxes)*
2. *Mark the relevant printer.*
3. *Select* **File – Properties** *from the menu bar. The* **Properties** *dialog appears.*
4. *Select the* **Ports** *tab.*
5. *Click* **Add***. The* **Printer Ports** *dialog appears.*
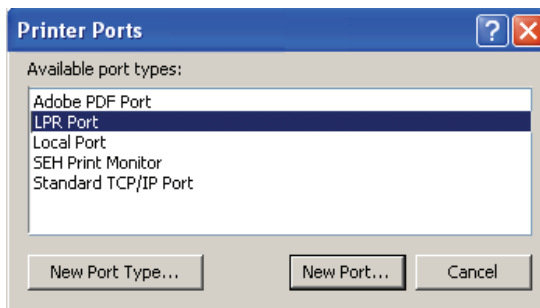
Fig. 27: Windows – Printer Ports

6. *Mark* **LPR Port.**
7. *Click* **New Port***. The* **Add LPR compatible printer** *dialog appears.*
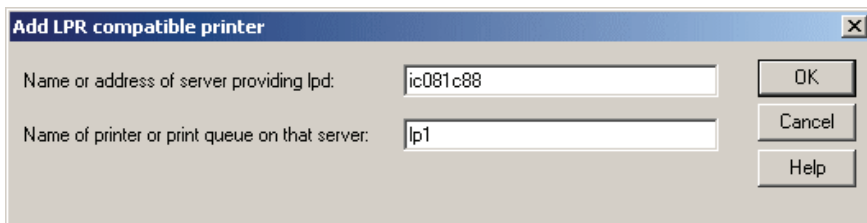
Fig. 28: Windows – Add LPR Compatible Printer

8. *Enter the DNS name or the IP address of the print server.*

Some applications do not support the direct entry of IPv6 addresses. Use the name resolution instead. Make sure that the relevant IPv6 entries have been configured in the DNS system. Enter the host name or the complete domain name of the print server.

9. *Enter the name of the printer or the print queue on the server.*
10. *Click* **OK***.*
↳ An LPR port is added to the selected printer.

17 Appendix

The appendix contains a glossary, the print server parameter list, notes about the print server models and the index lists of this document.

What information do you need?

- 'Glossary' ⇨ 🖹202
- 'Notes concerning the Print Server Models' ⇨ 🖹208
- 'Parameter List' ⇨ 🖹209
- 'List of Figures' ⇨ 🖹234
- 'Index' ⇨ 🖹235

17.1 Glossary

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

Manufacturer-Specific Software Solutions

- 'PRINTSERVER Print Monitor' ⇨📄203

- 'PRINTSERVER Printer Wizard' ⇨📄203

- 'PRINTSERVER- NetTool' ⇨📄203

Network Technology

- 'Default Name' ⇨📄203

- 'Hardware Address' ⇨📄203

- 'IP Address' ⇨📄204

- 'Print Server Name' ⇨📄205

- 'Gateway' ⇨📄205

- 'Host Name' ⇨📄205

- 'Subnet Mask' ⇨📄206

- 'TCP/IP Port' ⇨📄206

PRINTSERVER Print Monitor

The PRINTSERVER Print Monitor is an specific extension for the printing service of a Windows operating system. The software ensures the transfer of unencrypted and encrypted (SSL/TLS) print data from the client to the print server by means of direct TCP/IP ports. The PRINTSERVER Print Monitor can be installed and configured on every client intended for printing. The Print Monitor supports 32-bit systems.

PRINTSERVER Printer Wizard

The PRINTSERVER Printer Wizard is a self-extracting program that helps to install a network printer via a print server in Windows networks. The tasks of the PRINTERSERVER Printer Wizard include:

- installation of the PRINTSERVER Print Monitor
- printer driver installation
- installation of print server and printer
- setting up the printer
- printing a test page

PRINTSERVER-NetTool

The software PRINTSERVER-NetTool has been developed for the administration of network devices within a predefined network.

Default Name

see: 'Print Server Name' ⇨ 📄205

Hardware Address

The print server is addressable by means of its world-wide unique hardware address. This address is commonly referred to as the 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.

Hardware Address

00:c0:eb:00:01:ff

Manufacturer
ID

Device
number
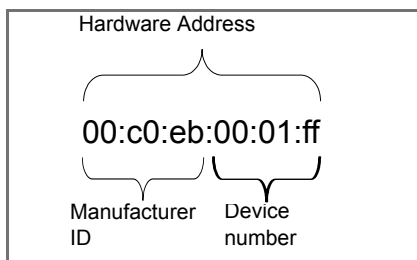
The hardware address is found on the PRINTSERVER Homepage, in the PRINTSERVER-NetTool, the status page, the housing of the print server, or on the print server card.

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

Operating system	Representation	Example
Windows	Hyphen	00-c0-eb-00-01-ff

IP Address The IP address is a fundamental prerequisite for the communication within a network. Each network that uses the TCP/IP protocol requires a unique addressing of its end devices.

• IP addresses of the version IPv4 of the Internet protocol consist of four digits between 0 and 255 that are separated by periods.

• IP addresses of the version IPv6 of the Internet protocol consist of eight hexadecimal numbers that are separated by colons.

In order to be reachable in a TCP/IP network, the print server needs an IP address that is used only once in the network; see: 'Saving the IP Address in the Print Server' ⇨🖹15.

Print Server Name
The print server name (default 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.

Default name

IC0001ff

Device number
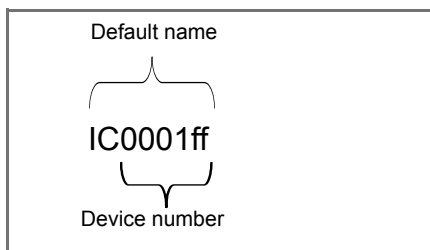
Gateway
Using a gateway, you can address IP addresses from external networks. If you wish to use a gateway, you can configure the relevant parameter via the PRINTSERVER Homepage or the PRINTSERVER-NetTool.

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

The assignment is carried out either in the 'hosts' file or on the DNS or WINS server. The 'hosts' file is an internal system file in which the assignment of the host names to the IP addresses is saved.

<u>Syntax:</u> `<IP address> <host name>`

<u>Example:</u> `192.168.0.123 IC0001FF`

The 'hosts' file is located in the 'windows' directory in Windows networks. In other operating systems, such as AS/400 for example, the name of the assignment file may differ.

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 print server is configured not to use subnetworks by default. If you wish to use a subnetwork, you can configure the relevant parameter via the PRINTSERVER Homepage or the PRINTSERVER-NetTool.

TCP/IP Port

During the transfer of files between two computers, addressing with the IP address alone is generally not sufficient. In addition to the IP address, a port number (TCP/IP port) is used. This number defines the computer memory area that is reserved for a specific communications connection. The combination of an IP address and a port number is unique for every communications connection and is defined as a socket.

TCP/IP Ports with LPD Protocol

If the LPD protocol is used for transferring print data, the corresponding data packet contains the pre-configured TCP/IP port 515. The transferred print data is saved to the memory area corresponding to the port number and then processed.

TCP/IP Ports Without LPD Protocol

If the LPD protocol is not available, as in the case of Windows 98 networks, you must configure the TCP/IP port yourself. To do this, you must install a printer port and enter the port number. In this case, such a port may also be called a direct printer port.

TCP/IP Ports and Logical Printers

The TCP/IP port corresponds to that of the logical printers. The following TCP/IP ports are preset in your print server via the logical printers.

Logical Printer	1	2	3	4	5	6	7	8
TCP/IP Port	9100	9101	9102	9103	9104	9105	9106	9107

17.2 Notes concerning the Print Server Models

This section contains individual information about the print server models described in this documentation.

- 'WLAN Models' ⇨ 🖹208

- 'Production Date of the Print Server' ⇨ 🖹208

WLAN Models

In the case of print server models with WLAN support, the menu item 'Authentication' can be found in the menu 'WLAN'.

Production Date of the Print Server

The production date of your print server model can be found in the serial number. The serial number can be obtained from the status page. You can print a status page by pressing the status button for a short time.

```
                  Serial number

           xxxyyyymmxxxxx

              Year   Month
```
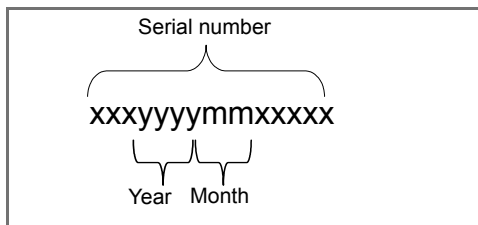
17.3 Parameter List

This chapter gives an overview of all available print server parameters. Each print server model has its own parameters, sorted by topics. The parameter list gives details about the functions and values of the individual parameters.

Table 25: Parameter List - General

Parameters	Value	Description
info_txt [Dealer]	max. 64 characters [a-z, A-Z, 0-9, _, -]	Defines the name of the dealer or supplier. *This description is freely definable.*
info_url [Dealer URL]	max. 64 characters [a-z, A-Z, 0-9, _, -]	Defines the name of the dealer or supplier. *This description is freely definable.*
language [Print server language]	en = English de = German fr = French es = Spanish it = Italian pt = Portuguese jp = Japanese cn = Chinese simplified zh = Chinese traditional kr = Korean	Defines the language of the print server.
sp_mode [Status page mode]	Auto ASCII DATAMAX ZPL	Defines the data format in which the status page is printed. *The data formats ASCII, DATAMAX (label printer), and ZPL (label printer) are available.* *The preset 'Auto mode' automatically uses the appropriate data format.*

Parameters	Value	Description
tp_port [ThinPrint® port]	1 - 65535 [5 characters, 0-9]	Defines the ThinPrint® port number. *The port number of the print server must be identical to the port number that was defined for the ThinPrint® server.*
tp_bandwidth [Bandwidth]	on/off	Enables/disables the bandwidth value of the ThinPrint® port (client side).
tp_bandwidthval [Bandwidth]	1600 - 1000000 [7 characters, 0-9]	Defines the bandwidth in bit/second (bit/s) used to decrease the bandwidth limit on the ThinPrint® port (client side).
job_rcvtmout [Job receive timeout]	1 - 9999 [4 characters, 0-9] 0 = no timeout	Specifies the timeout (in seconds) for receiving print jobs. *If the spooler does not send any print job within the timeout period, the connection between the print server and the spooler will be interrupted. If the value is set to 0, this function is disabled. If you want to use the timeout option, we recommend using the value '120'.*
eth_conf [Ethernet settings]	0 = Auto 1 = 10BaseT/FL HALF 2 = 10BaseT/FL FULL 3 = 100BaseFX/TX HALF 4 = 100BaseFX/TX FULL 5 = 1000BaseT/SX	Defines the network speed of the print server. *'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 26: Parameter List – WLAN

Parameters	Value	Description
wifi_mode [Mode]	1 = infrastructure mode 2 = Ad-Hoc mode	Defines the communication mode. *The communication mode defines the network structure in which the print server will be installed.*
wifi_channel [Channel]	1 ~ 14	Defines the channel to which the entire data communication will be transmitted. *The channel (frequency range) should be changed if interferences emerge. Channels 1 through 14 are available. Keep yourself informed about national provisions regarding the use of WLAN products and only use authorized channels.*
wifi_name [SSID]	max. 64 characters [a-z, A-Z, 0-9, _, -]	Defines the SSID. *The ID of a wireless network is referred to as SSID (Service Set Identifier) or network name. Each wireless LAN has a configurable SSID in order to clearly identify the wireless network.*
wifi_encrypt [Encryption]	0 = none 1 = WEP (Open System) 2 = WEP (Shared Key) 3 = WPA (TKIP) 4 = WPA (AES) 5 = WPA2 (TKIP) 6 = WPA2 (AES)	Defines the encryption method to be used.
wifi_keyid [WEP key used]	0 = none 1 = wifi_wepkey 2 = wifi_wepkey2 3 = wifi_wepkey3 4 = wifi_wepkey4	Specifies the ID of the currently used WEP key.
wifi_wepkey wifi_wepkey2 wifi_wepkey3 wifi_wepkey4 [WEP Key]	The max. number of characters depends on the selected model. 64 ASCII = 5 64 HEX = 10 128 ASCII = 13 128 HEX = 26	Defines the WEP key used. Four WEP keys are available. *You can enter the following characters: - Hexadecimal = 0-9, a-f, A-F - ASCII = 0-9, a-z A-Z*
wifi_psk [PSK]	8 - 63 characters	Defines the Pre Shared Key (PSK) for Wi-Fi Protected Access (WPA).

Parameters	Value	Description
wifi_roaming [Roaming]	on/off	Enables/disables the optional use of roaming. *Roaming refers to the use of end devices (such as print servers) or just to the use of the participants' identity between two networks. This setting is primarily used for the interaction with CISCO Hot Spots.*
wifi_dbm2roam [dBm]	1 - 999	Defines the transmitting power in dBm. *dBm is a unit of expression of power level in decibels with reference to a power of 1 milliwatt.*

Table 27: Parameter List – Printer Port

Parameters	Value	Description
pp*_ecp [ECP mode]	on/off	Enables/disables the ECP mode of external print server models. *The ECP (Enhanced Capability Port) mode can be used for quick and compressed data transfer.*
pp*_fast [Fast mode]	on/off	Enables/disables the fast mode of external print server models. *Using the fast mode, the print server speed can be increased. With older printer models, it is recommended to disable the fast mode.*
pp*_port_mode [Port mode]	0 = Unidirectional 1 = Bidirectional	Specifies the communication mode between the print server and the printer.
pp4_baudrate [Baud rate]	150 / 300 / 600 / 1200 / 1800 / 2400 / 3600 / 4800 /7200 / 9600 / 19200 / 38400 / 57600 / 115200	Specifies the baud rate for data transfer.
pp4_parity [Parity]	none even odd	Specifies the parity bit for the detection of incorrectly transmitted bit sequences (parity check). *none = no parity check* *even = even parity check* *odd = odd parity check*
pp4_databits [Data bits]	5 ~ 8	Specifies how many data bits will be transferred in one data packet.
pp4_stopbits [Stop bits]	1 ~ 2	Defines the stop bit. *Stop bits mark the end of a data transfer unit and allow the recipient of a data transfer to synchronize the data flow.*
pp4_flowcontrol [Flow control]	none xon (xon/xoff) dsr (DSR/DTR) both	Defines the handshake procedure to control the data flow between print server and printer. *none = handshake is disabled* *xon = software handshake is enabled* *dsr = hardware handshake is enabled* *both = software and hardware handshake are enabled*

* Port number of the print server (e.g. LPT 1-3, COM1 or USB 1-5)

Table 28: Parameter List – TCP/IP

Parameters	Value	Description
tcpip [TPC/IP]	on/off	Enables/disables the TCP/IP protocol. *If you have disabled TCP/IP, all functions based on this protocol are no longer available. This means that, for example, the PRINTSERVER Homepage or FTP will no longer be available.*
ip_addr [IP Address]	valid IP address	Defines the IP address of the print server.
ip_mask [Subnet mask]	valid IP address	Defines the subnet mask of the print server.
ip_gate [Gateway]	valid IP address	Defines the gateway address of the print server.
ip_dhcp [DHCP]	on/off	Enables/disables the DHCP protocol.
ip_bootp [BOOTP]	on/off	Enables/disables the BOOTP protocol.
ip_auto [ARP/PING]	on/off	Enables/disables the IP address assignment via ARP/PING.
ip_set_by [IP Address]	0 = Unknown 1 = SNMP (NetTool) 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 Homepage	Shows the applied method for the IP address assignment.
ip_auto_gate [Multicast router as gateway]	on/off	Enables/disables the automatic entry of a found multicast router as gateway address. *If disabled, the gateway address has to be entered manually.*

Parameters	Value	Description
ip_zconf [ZeroConf]	on/off	Enables/disables the automatic verification of an IP address conflict via ZeroConf. *ZeroConf describes a procedure for the automatic assignment of IP addresses.*
ipv6 [IPv6]	on/off	Enables/disables the IPv6 functionality of the print server.
ipv6_addr [IPv6 address]	n:n:n:n:n:n:n:n.	Defines a print server IPv6 unicast address assigned manually. *Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.*
ipv6_gate [Router]	n:n:n:n:n:n:n:n.	Defines the IPv6 unicast address of the router. The print server sends his 'Routers Solicitations' (RS) to this router.
ipv6_plen [Prefix length]	0 - 64	Defines the length of the subnet prefix for the IPv6 address. (The value 64 is preset.) *Address ranges are indicated by prefixes. The prefix length (Number of used bits) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/' .*
ipv6_auto [Automatic configuration]	on/off	Enables/disables the automatic assignment of the IPv6 address for the print server.
sys_name [Host name]	max. 64 characters	Defines the host name of the print server.
sys_descr [Description]	max. 128 characters	Defines a free description (of the print server).
sys_contact [Contact person]	max. 64 characters	Defines a free description (of a contact person).
sys_location [Location]	max. 64 characters	Defines a free description (of the location of the device).

Table 29: Parameter List - IPsec

Parameter	Value	Description
ipsec [IPsec]	on/off	Enables/disables the use of IPsec. *(Pay attention to the IPsec test mode.)*
ipsec_testmode [Test mode]	on/off	Enables/disables the IPsec test mode. *We recommend using the test mode to access the device in case of a misconfiguration. In the test mode, IPsec remains active until the hard reboot of the device. IPsec is disabled after the hard reboot.*
ipsec_config	0 = Use configured rules 1 = Use configuration files	Specifies the way in which IPsec policies are added to the print server.
ipsec_dhcp [DHCP]	on/off	Enables/disables the filtering of DHCP network activities by the IPsec policy. *- on = activity is always allowed* *- off = activity is filtered via IPsec*
ipsec_netbios [NetBIOS]	on/off	Enables/disables the filtering of NetBIOS network activities by the IPsec policy. *- on = activity is always allowed* *- off = activity is filtered via IPsec*
ipsec_slp [SLP]	on/off	Enables/disables the filtering of SLP network activities by the IPsec policy. *- on = activity is always allowed* *- off = activity is filtered via IPsec*
ipsec_slp [FTP]	on/off	Enables/disables the filtering of FTP network activities by the IPsec policy. *- on = activity is always allowed* *- off = activity is filtered via IPsec* *If all FTP network activities are allowed (FTP = on), you must specify the 'Allow all' action in the default rule.*
ipsec_def_action [*action of the default rule*]	0 = Allow all 1 = Drop all	As specified in the IPsec default rule, this is the action to be carried out if a data packet matches the description of a filter.
ipsec_rule1_enabled ipsec_rule2_enabled ipsec_rule3_enabled ipsec_rule4_enabled [Rule 1-4]	on/off	Enables/disables the IPsec rules.

Parameter	Value	Description
ipsec_rule1_iaddr_tmpl ipsec_rule2_iaddr_tmpl ipsec_rule3_iaddr_tmpl ipsec_rule4_iaddr_tmpl [Address filter]	0 = --- 1 = Address Template 1 2 = Address Template 2 3 = Address Template 3 4 = Address Template 4 5 = Address Template 5 6 = Address Template 6 7 = Address Template 7 8 = Address Template 8	Specifies the filter within an IPsec rule for the IP traffic via a template. *cp. parameter 'iaddr_tmpl1_name'*
ipsec_rule1_iserv_tmpl ipsec_rule2_iserv_tmpl ipsec_rule3_iserv_tmpl ipsec_rule4_iserv_tmpl [Service filter]	0 = --- 1 = Service Template 1 2 = Service Template 2 3 = Service Template 3 4 = Service Template 4	Specifies the filter within an IPsec rule for protocols and services via a template. *cp. parameter 'iserv_tmpl1_name'*
ipsec_rule1_ipsec_tmpl ipsec_rule2_ipsec_tmpl ipsec_rule3_ipsec_tmpl ipsec_rule4_ipsec_tmpl [Security association (SA)]	0 = --- 1 = SA Template 1 2 = SA Template 2 3 = SA Template 3 4 = SA Template 4	Specifies the parameters of the 'Security Association' via a template. *cp. parameter 'ipsec_tmpl1_name'*
ipsec_rule1_action ipsec_rule2_action ipsec_rule3_action ipsec_rule4_action [Action]	0 = Allow all 1 = Drop all 2 = Require IPsec	As specified within the IPsec rule, this is the action to be carried out if a data packet matches the description of a filter.
iaddr_tmpl1_name iaddr_tmpl2_name iaddr_tmpl3_name iaddr_tmpl4_name iaddr_tmpl5_name iaddr_tmpl6_name iaddr_tmpl7_name iaddr_tmpl8_name [Name]	max. 18 characters [a-z, A-Z, 0-9, _, -]	Name of the address template. The template is used for filtering the IP traffic. *Local and remote IP addresses can be defined in the address template.* *Addresses in the format IPv4 and IPv6 are supported.*
iaddr_tmpl1_ip_remote iaddr_tmpl2_ip_remote iaddr_tmpl3_ip_remote iaddr_tmpl4_ip_remote iaddr_tmpl5_ip_remote iaddr_tmpl6_ip_remote iaddr_tmpl7_ip_remote iaddr_tmpl8_ip_remote [Remote (IPv4)]	- IPv4 address - IPv4 address range - All IPv4 addresses = 0.0.0.0/0	Specifies a remote IPv4 address or an IPv4 address range for an address template. *The notation of address ranges is done via the CIDR methodology, e.g. 192.168.0.1/24.*

Parameter	Value	Description
iaddr_tmpl1_ip6_local iaddr_tmpl2_ip6_local iaddr_tmpl3_ip6_local iaddr_tmpl4_ip6_local iaddr_tmpl5_ip6_local iaddr_tmpl6_ip6_local iaddr_tmpl7_ip6_local iaddr_tmpl8_ip6_local [Local (IPv6)]	- IPv6 address - IPv6 address range - All IPv6 addresses = ::/0	Specifies a local IPv6 address or an IPv6 address range for an address template. *The notation of address ranges is done via the CIDR methodology.*
iaddr_tmpl1_ip6_remote iaddr_tmpl2_ip6_remote iaddr_tmpl3_ip6_remote iaddr_tmpl4_ip6_remote iaddr_tmpl5_ip6_remote iaddr_tmpl6_ip6_remote iaddr_tmpl7_ip6_remote iaddr_tmpl8_ip6_remote [Remote (IPv6)]	- IPv6 address - IPv6 address range - All IPv6 addresses = ::/0	Specifies a remote IPv6 address or an IPv6 address range for an address template. *The notation of address ranges is done via the CIDR methodology.*
iserv_tmpl1_name iserv_tmpl2_name iserv_tmpl3_name iserv_tmpl4_name [Name]	max. 16 characters [a-z, A-Z, 0-9, _, -]	Name of the service template. *The template is used for filtering the IP traffic by services and protocols.*
iserv_tmpl1_services iserv_tmpl2_services iserv_tmpl3_services iserv_tmpl4_services [Services]	ALL, ICMP, HTTP, SNMP, SNTP, IPP, Socket printing, LPR, ThinPrint	Specifies the elements of the service filter. *Several protocols can be combined in a service.*
ipsec_tmpl1_name ipsec_tmpl2_name ipsec_tmpl3_name ipsec_tmpl4_name [Name]	max. 16 characters [a-z, A-Z, 0-9, _, -]	Name of the IPsec template. The IPsec template specifies the parameters of a 'Security Association'.
ipsec_tmpl1_certificate ipsec_tmpl2_certificate ipsec_tmpl3_certificate ipsec_tmpl4_certificate [Authentication type]	1 = Certificates 0 = Pre-Shared Key	Specifies the procedure for the authentication of the remote server. *Two procedures are available: - authentication via pre-shared key - authentication via certificates.*
ipsec_tmpl1_verify ipsec_tmpl2_verify ipsec_tmpl3_verify ipsec_tmpl4_verify [Verify certificate]	on/off	Specifies the type of certificate required for the certificate-based authentication. *Disabled: A self-signed certificate is sufficient for the authentication. Enabled: A root certificate is required for the authentication.*

Parameter	Value	Description
ipsec_tmpl1_psk ipsec_tmpl1_psk ipsec_tmpl1_psk ipsec_tmpl1_psk [Pre-Shared Key]	max. 16 characters	Specifies the Pre-Shared Key (PSK). *You need the key if the 'Pre-Shared Key' procedure has been selected as 'Authentication type'.*
ipsec_tmpl1_key _exchange ipsec_tmpl2_key _exchange ipsec_tmpl3_key _exchange ipsec_tmpl4_key _exchange [IKE]	0 = --- 1 = IKE template 'IKE Default' 2 = IKE template 2 3 = IKE template 3 4 = IKE template 4	Specifies the template to be used for the IKE (automatic key exchange) within a SA. *cp. parameter 'ipsec_key_exchange1_name'* *The 'IKE Default' template has been implemented by default. You can specify another three IKE templates, if required.*
ipsec_key_exchange 1_name ipsec_key_exchange 2_name ipsec_key_exchange 3_name ipsec_key_exchange 4_name [Name]	max. 16 characters [a-z, A-Z, 0-9, _, -]	Name of the IKE template.
ipsec_key_exchange 1_modes ipsec_key_exchange 2_modes ipsec_key_exchange 3_modes ipsec_key_exchange 4_modes [Negotiation]	main, aggressive	Specifies the procedure for the negotiation of the encryption and authentication. - In the 'Main Mode' individual connections will be successively established for the individual steps (key exchange etc.). - In the 'Aggressive Mode' individual steps of the Main Mode will be summarized (faster but less secure). *You can select several procedures. Only the most secure procedure will be applied. If a procedure fails, a less complicated (and therefore less secure) procedure will be used.*

Parameter	Value	Description
ipsec_key_exchange 1_dh_group ipsec_key_exchange 2_dh_group ipsec_key_exchange 3_dh_group ipsec_key_exchange 4_dh_group [Diffie-Hellman group]	1 = modp768 2 = modp1024 3 = modp1536 4 = modp2084 5 = modp3072 6 = modp4096 7 = modp6144 8 = modp8192	Specifies the Diffie-Hellman group number for the creation of dynamically generated temporary keys. The keys are used during the negotiation.
ipsec_key_exchange1 _encryption_algo_ph1 ipsec_key_exchange2 _encryption_algo_ph1 ipsec_key_exchange3 _encryption_algo_ph1 ipsec_key_exchange4 _encryption_algo_ph1 [Encryption algorithm]	0 = des 1 = 3des 2 = aes	Specifies the encryption algorithm to be used during the negotiation.
ipsec_key_exchange 1_hash_algo_ph1 ipsec_key_exchange 2_hash_algo_ph1 ipsec_key_exchange 3_hash_algo_ph1 ipsec_key_exchange 4_hash_algo_ph1 [Hash algorithm]	0 = md5 1 = sha1	Specifies the Hash algorithm to be used during the negotiation.
ipsec_key_exchange1_li fetime_ph1 ipsec_key_exchange2_li fetime_ph1 ipsec_key_exchange3_li fetime_ph1 ipsec_key_exchange4_li fetime_ph1 [IKE SA lifetime]	min. 600 sec max. 4294967295 sec	Specifies the duration of the IKE connection in seconds. When the IKE SA lifetime expires, a re-authentication is required.

Parameter	Value	Description
ipsec_key_exchange1_ encapsulation_mode ipsec_key_exchange2_ encapsulation_mode ipsec_key_exchange3_ encapsulation_mode ipsec_key_exchange4_ encapsulation_mode [Encapsulation type]	0 = Transport mode	Specifies how the IP data packet is handled within the SA. The IPsec specification differentiates between the 'Transport Mode' and the 'Tunnel Mode'. - In the Transport Mode the IP data packet is encrypted. However, the IP header will be kept. - In the Tunnel Mode a complete IP data packet will be encapsulated in another packet and be given a new IP header. *NOTE: The Tunnel Mode cannot be selected via the selection list on the Printserver Homepage. Use a configuration file (racoon/setkey) instead.*
ipsec_key_exchange1_ pfs_group ipsec_key_exchange2_ pfs_group ipsec_key_exchange3_ pfs_group ipsec_key_exchange4_ pfs_group [Diffie-Hellman group]	0 = --- 1 = modp768 2 = modp1024 3 = modp1536 4 = modp2084 5 = modp3072 6 = modp4096 7 = modp6144 8 = modp8192	Specifies the Diffie-Hellman group number for the creation of additional dynamically generated temporary keys. The keys are used during phase 2.
ipsec_key_exchange1_ encryption_algo_ph2 ipsec_key_exchange2_ encryption_algo_ph2 ipsec_key_exchange3_ encryption_algo_ph2 ipsec_key_exchange4_ encryption_algo_ph2 [Encryption algorithm	3des = 3des des = des aes = aes des_iv64 = des64 des_iv32 = des32 null_enc = none	Specifies the encryption algorithm for phase 2. *You can select several procedures. If the remote party also offers several procedures, the procedure that was listed first with the communication partner will be used.*
ipsec_key_exchange 1_auth_algo_ph2 ipsec_key_exchange 2_auth_algo_ph2 ipsec_key_exchange 3_auth_algo_ph2 ipsec_key_exchange 4_auth_algo_ph2 [Authentication algorithm]	hmac_md5 = md5 hmac_sha1 = sha1 non_auth = none	Specifies the Hash algorithm for phase 2. *You can select several procedures. If the remote party also offers several procedures, the procedure that was listed first with the communication partner will be used.*

Parameter	Value	Description
ipsec_key_exchange 1_with_ah ipsec_key_exchange 2_with_ah ipsec_key_exchange 3_with_ah ipsec_key_exchange 4_with_ah [With AH protocol]	on/off	Specifies the use of the 'Authentication Header' protocol for the protection of the packet integrity and packet authentication. *AH uses the authentication header to authenticate the packet. In the IP data packet, the authentication header will be added after the IP header.*
ipsec_key_exchange 1_lifetime_ph2 ipsec_key_exchange 2_lifetime_ph2 ipsec_key_exchange 3_lifetime_ph2 ipsec_key_exchange 4_lifetime_ph2 [IP SA lifetime]	min. 600 sec max. 4294967295 sec	Specifies the duration of the IPsec SA connection in seconds. When the IPsec SA lifetime expires, you have to renew the IPsec key.

Table 30: Parameter List - Microsoft Windows

Parameters	Value	Description
netbios [NetBIOS]	on/off	Enables/disables peer-to-peer printing.
netbios_name [NetBIOS Name]	max. 15 characters	Defines the print server name which appears in the relevant workgroup or domain.
netbios_domain [NetBIOS Domain]	max. 15 characters	Defines the name of an existing workgroup or domain.
netbios_time [NetBIOS refresh]	max. 4 characters; [0-9] 0-9999	Defines the time interval (in minutes) after which the NetBIOS parameters will be refreshed.
wins [WINS registration]	on/off	Enables/disables the WINS registration.
wins_dhcp [WINS via DHCP]	on/off	Enables/disables the automatic entry of the IP address of a WINS server via DHCP. *If the option is enabled, the IP address of the WINS server is entered via DHCP. If the option is disabled, you can enter the IP address of the WINS server manually.*
wins_primary [Primary WINS server]	valid IP address	Defines the IP address of the primary WINS server.
wins_seconary [Secondary WINS server]	valid IP address	Defines the IP address of the secondary WINS server. *The secondary WINS server is used if the primary WINS server is not available.*

Table 31: Parameter List – DNS

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

Table 32: Parameter List – SNTP

Parameters	Value	Description
sntp [SNTP]	on/off	Enables/disables the use of a time server.
sntp_server [Time server]	max. 255 characters	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.* ** Additional abbreviations can be found in the menu item 'Configuration' --> 'Time'.*	The time zone is used to equalize the difference between the Greenwich Mean Time or UTC (Universal Time Coordinate) of the time server and the local time, including country-specific particularities such as Daylight Saving Time. *Enter the abbreviation for your local time zone as parameter value.*

Table 33: Parameter List - Notification

Parameters	Value	Description
nf*_mail_mask1 nf*_mail_mask2 [Printer error]	Paper jam = 1 Paper empty = 2 Toner low = 4 Cover open = 8 Toner empty = 16 Cassette not ready = 32 Warming up = 64 Offline = 128 Engine error = 256 No select = 512 Service call = 16384 Miscellaneous error = 32768	Defines the printer errors of which recipient 1 or 2 is informed by email. *The email contains information about the printer error.* *Each code represents a message.* *By adding these codes, several printer errors can be indicated at once.* *Not all print server models support all printer error messages.*
nf_mail_addr1 nf_mail_addr2 [Mail recipient]	valid email address	Defines the email address of the recipient to which the emails will be sent. *The emails contain information about the printer error. You can define 1 or 2 recipients.*
nf_mail_pr1 nf_mail_pr2 [Email active] [Email active]	on/off	Enables/disables the email notification for recipient 1 or 2.
nf_mAccHist1 nf_mAccHist2 [Job history] [Job History]	on/off	Enables/disables the email notification for recipient 1 or 2. *The emails contain information about the number of print jobs processed by the print server.*
nf_mAccHistTime1 nf_mAccHistTime2 [time interval]	max. 4 characters; [0-9] 0-9999	Defines the time interval (in hours) in which an email will be sent to recipient 1 or 2.
nf_mAccHistCnt1 nf_mAccHistCnt2 [Jobs]	max. 2 characters; [0-9] 1-60	Defines the number of print jobs after which an email will be sent to recipient 1 or 2.
nf*_mAccPCnt1 nf*_mAccPCnt2 [Page counter] [Page counter]	on/off	Enables/disables the email notification for recipient 1 or 2. *The emails contain information about the number of printed pages of a printer.*

Parameters	Value	Description
nf*_mAccPCntTime1 nf*_mAccPCntTime2 [time interval]	max. 4 characters; [0-9] 0-9999	Defines the time interval (in hours) in which an email will be sent to recipient 1 or 2. *The emails contain information about the number of printed pages of a printer.*
nf*_mAccPCntCnt1 nf*_mAccPCntCnt2 [page interval]	max. 4 characters; [0-9] 0-9999	Defines after how many printed pages an email will be sent to recipient 1 or 2. *The emails contain information about the number of printed pages.*
nf*_trap_mask1 nf*_trap_mask2	Paper jam = 1 Paper empty = 2 Toner low = 4 Cover open = 8 Toner empty = 16 Cassette not ready = 32 Warming up = 64 Offline = 128 Engine error = 256 No select = 512 Service call = 16384 Miscellaneous error = 32768	Defines the printer errors of which recipient 1 or 2 is informed by a trap. *A trap contains information about the printer error.* *Each code represents a message.* *By adding these codes, several printer errors can be indicated at once.* *Not all print server models support all printer error messages.*
nf_trap_ip1 nf_trap_ip2 [IP Address]	valid IP address	Defines the IP address of the recipient to which the traps will be sent. *The traps contain information about the printer error. You can define 1 or 2 recipients.*
nf_trap_com1 nf_trap_com2 [Trap community]	max. 15 characters	Defines the Trap community of recipient 1 or 2.
nf_trap_aut1 nf_trap_aut2 [Authentication traps]	on/off	Enables/disables the sending of traps containing authentication information for recipient 1 or 2.
nf_trap_pr1 nf_trap_pr2 [Printer traps]	on/off	Enables/disables the sending of traps for selected printer errors for recipient 1 or 2.

* Port number of the print server (e.g. LPT 1-3, COM1 or USB 1-5)

Table 34: Parameter List – SMTP

Parameters	Value	Description
nf_smtp_srv [Server name]	max. 255 characters	Defines the name of the SMTP server.
nf_smtp_port [Server port]	max. 5 characters	Defines the port number used by the print server to send emails to the SMTP server. (Default = 25)
nf_smtp_user [User name]	max. 255 characters	Defines the name used by the print server to connect to the SMTP server.
nf_smtp_pwd [Password]	max. 255 characters	Defines the password the print server uses to connect to the SMTP server.
nf_smtp_sndr [Sender name]	max. 255 characters	Defines the email sender name to be used by the print server.
nf_smtp_ssl [TLS]	on/off	Enables/disables TLS. *The TLS protocol serves to encrypt the transmission between the print server and the SMTP server.*
nf_smtp_asp3 [Use POP3 settings]	on/off	Enables/disables the option for using the parameters 'User name' and 'Password' from the POP3 settings for authentication.
nf_smtp_sign [Signature]	max. 128 characters	Defines the signature to be contained in an email generated by the print server.

Table 35: Parameter List – POP3

Parameters	Value	Description
nf_pop3 [POP3]	on/off	Enables/disables the POP3 support.
nf_pop3_srv [Server name]	max. 255 characters	Defines the name of the POP3 server.
nf_pop3_poll [Check mail every]	max. 4 characters; [0-9] 0-9999	Defines the time interval (in minutes) for retrieving emails from the POP3 server.
nf_pop3_port [Server port]	max. 5 characters default = 110 SSL = 995	Defines the port used by the print server for receiving emails. When using SSL, enter 995 as port number.

Parameters	Value	Description
nf_pop3_user [User name]	max. 255 characters	Defines the name used by the print server to log on to the POP3 server.
nf_pop3_pwd [Password]	max. 255 characters	Defines the password the print server uses to log on to the POP3 server.
nf_pop3_secure [Security]	0 = off (no security) 1 = APOP 2 = SSL	Defines an authentication method.
nf_pop3_mdel [Delete read messages]	on/off	Enables/disables the automatic deletion of read emails on the server.
nf_pop3_limit [Ignore mail exceeding]	max. 4 characters; [0-9] 0-9999 0 = unlimited	Defines the maximum email size (in kbyte) to be accepted by the print server.

Table 36: Parameter List – Protection

Parameters	Value	Description
passwd [Password]	max. 16 characters	Defines the password for the authorization to change print server 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	Enables/disables the password demand for print server 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 print server 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.*

Parameters	Value	Description
http [HTTP]	on/off	Enables/disables the HTTP protocol on the print server. *If the HTTP protocol is disabled, those functions that are based on the protocol will not be available (e.g. the PRINTSERVER Homepage cannot be started).*

Table 37: Parameter List – EAP Authentication

Parameters	Value	Description
eap_auth_type [Authentication]	<u>Print Server with WLAN</u> 1 = Open System 2 = Shared Key 3 = EAP-MD5/LEAP 4 = EAP-TLS 5 = EAP-TTLS 6 = PEAP 7 = EAP-FAST <u>Print Server without WLAN</u> 1 = not defined 2 = not defined 3 = EAP-MD5/LEAP 4 = EAP-TLS 5 = EAP-TTLS 6 = PEAP 7 = EAP-FAST	Defines the authentication method that is used to identify devices or users in the network.
eap_auth_name [User name]	max. 64 characters	Defines the name of the print server as saved in the authentication server (RADIUS).
eap_auth_pwd [Password]	max. 64 characters	Defines the password of the print server as saved in the authentication server (RADIUS).
eap_auth_ anonymous_name [Anonymous name]	max. 64 characters	Defines the anonymous name for the unencrypted part of the EAP authentication methods TTLS, PEAP, and FAST.

Parameters	Value	Description
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	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	Defines the kind of external authentication for the EAP authentication methods PEAP and FAST.

Table 38: Parameter List – Dynamic Update

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

Table 39: Parameter List – Logical Printer

Parameters	Value	Description
lp*_prt_port [Printer port]	depends on the print server model	Defines the port used by the logical printer for printing. *This parameter is only available for print server models with several physical printer ports.*
lp*_tcp_port [TCP/IP port]	max. 4 characters; [0-9] 0-9999	Defines the TCP/IP port of the relevant logical printer.
lp*_mode [Banner page mode]	ASCII	Defines the format in which the banner page will be printed.
lp*_job_start [Job start]	max. 256 characters	Defines a start sequence. *Depending on the application, you might have to configure the logical printer. These sequences may consist of PRESCRIBE or ESC commands. ESC commands consist of job start sequence '\027' followed by the actual control characters preceded by a backslash and written as a decimal. Job end sequence '\027 \012', for example, triggers a form feed after the print job. For more information, please look up the available ESC commands in your printer manual.*
lp*_job_end [Job end sequence]	max. 256 characters	Defines an end sequence. *(see above)*
lp*_search [Search]	max. 256 characters *no wildcard or truncations*	Defines a string which is searched for in the data sent to the print server. *Using 'Find' and 'Replace,' you can look for strings in the data sent to the print server and replace them with new strings.*
lp*replace [Replace]	max. 256 characters *no wildcard or truncations*	Defines the string which is replaced in the data sent to the print server. *(see above)*
lp*_crlf [CR + LF]	on/off	Enables/disables the conversion from line feed (LF) to carriage return with line feed (LF+CR).
lp*_banner [Banner page]	on/off	Enables/disables the printing of a banner page or when the LPD protocol is used.

Parameters	Value	Description
lp*_hexdump [Hex dump mode]	on/off	Enables/disables the hex dump mode. *The hex dump mode is used to search for errors in print data. The hex dump mode displays each character both as hexadecimal code and ASCII character code. Printer control commands are printed as hexadecimal values and do not influence the printout in any way.*
lp*_prt_name [Printer]	max. 32 characters [a-z, A-Z, 0-9, _, -]	Specifies the printer name for the ThinPrint® AutoConnect feature. *The printer name is bound to the ID and gives the print object a description for a better differentiation.*
lp*_prt_class [Class]	max. 7 characters [a-z, A-Z, 0-9]	Specifies classes for the ThinPrint® AutoConnect feature. *Printers with compatible drivers can be arranged in one class.*
lp*_prt_driver [Driver]	max. 64 characters [a-z, A-Z, 0-9, _, -]	Specifies printer drivers for embedded printers for the ThinPrint® AutoConnect feature.

* Number of the logical printer (1–8)

17.4 List of Figures

17.5 Index

V

Version Number 58

W

WEP (Wired Equivalent Privacy) 189
WINS 170
Wireless Wizard 33
Wizard 33
WPA/WPA2 190
Write Protection 81

Z

ZeroConf 16