



Printserver

User Manual
Windows / macOS

printserver ONE



Manufacturer & Contact

SEH Computertechnik GmbH
Südring 11
33647 Bielefeld
Deutschland
Phone: +49 (0)521 94226-29
Fax: +49 (0)521 94226-99
Support: +49 (0)521 94226-44
Email: info@seh.de
Web: <https://www.seh-technology.com>



Document

Typ: User manual
Titel: printserver ONE User Manual | Windows / macOS
Version: 1.0 | 2021-04

Legal Information

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

The original manual is the German version of this document and shall govern. All non-German versions of this document are translation of the original manual.

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

These products include 'open source software'.

For detailed information, visit <https://www.seh-technology.com>.

© 2021 SEH Computertechnik GmbH

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

Content

1. General Information	1
1.1 Your Print Server	1
1.2 Documentation	1
1.3 Support and Service	4
1.4 Your Safety	5
1.5 First Steps	6
1.6 Finding the Print Server (Determining the IP Address)	6
2. Printing in Windows	8
2.1 How to Set Up Socket Printing	8
2.2 How to Set Up LPD/LPR Printing	10
2.3 How to Set Up IPP Printing	12
2.4 How to Configure Encrypted Printing	13
3. Printing in macOS	16
3.1 How to Set Up IPP Printing	16
3.2 How to Set Up LPD Printing	17
4. Administration Methods	19
4.1 Administration via SEH Product Manager	19
4.2 Administration via Print Server Homepage	22
4.3 Administration via FTP/FTPS Connection	24
4.4 Administration via Email	25
5. Network Settings	30
5.1 How to Configure IPv4 Parameters	30
5.2 How to Configure IPv6 Parameters	31
5.3 How to Adapt the Network Speed	34
5.4 How to Configure the DNS	34
5.5 How to Configure Bonjour	35
5.6 How to Use SNMP	36
5.7 How to Configure POP3 and SMTP	37
6. Port Settings	40
6.1 How to Enable PJJ	40
6.2 How to Enable 1284.4/MLC	40
6.3 How to Define the Communication Mode	41
7. Device Settings	42
7.1 How to Configure the Language of the Device	42
7.2 How to Configure the Device Time	42
7.3 How to Determine a Description	43

8. Print Server Status Information	44
8.1 How to View Status Information	44
8.2 What Status Information is Shown?	44
8.3 How to Print a Status Page	45
9. Print Jobs and Print Data	47
9.1 How to Define a Timeout for Taking on Print Jobs	47
9.2 How to Assign Print Jobs Directly	47
9.3 How to Modify Print Data	48
9.4 How to Convert Print Data?	49
9.5 How to Use Logical Printers (Filter Functions)?	50
10. Printer Status and Printer Messages	54
10.1 How to View the Printer Status	54
10.2 How to Get Additional Printer Information	54
10.3 How to Get Printer Messages via Email	55
10.4 How to Get Printer Messages via SNMP Trap	56
10.5 How to View the Job History	57
11. Security	59
11.1 How to Define a Password for the Print Server (Read/Write Protection)	59
11.2 How to Disable the HTTP Access (Protection against Viruses)	60
11.3 How to Protect Printers against Unauthorized Access (IP Sender Control)	60
12. Certificate Management	62
12.1 How to View Certificates	63
12.2 How to Create a Self-Signed Certificate	64
12.3 How to Create a Certificate Request for a Requested Certificate	66
12.4 How to Save a Requested Certificate in the Print Server	67
12.5 How to Save a PKCS12 Certificate in the Print Server	67
12.6 How to Save CA Certificates in the Print Server	68
12.7 How to Delete Certificates	69
13. Network Authentication	70
13.1 How to Configure EAP-MD5	70
13.2 How to Configure EAP-TLS	72
13.3 How to Configure EAP-TTLS	73
13.4 How to Configure PEAP	74
13.5 How to Configure EAP-FAST	76

14. Maintenance	78
14.1 How to Secure the Print Server Parameters (Backup)	78
14.2 Load parameter file via the SEH Product Manager	79
14.3 How to Reset Parameters to their Default Values	80
14.4 How to Perform an Update	81
14.5 How to Restart the Print Server	85
15. Additional Feature – ThinPrint®	86
15.1 How to Define the ThinPrint Port	86
15.2 How to Define the Bandwidth	87
15.3 How to Use ThinPrint AutoConnect	88
15.4 How Does the Print Server Receive Encrypted Data?	89
16. Additional Feature – Internet Protocol Security (IPsec)	90
16.1 How to Create IPsec Rules	94
16.2 How to Use IPsec Configuration Files	103
16.3 How to Define Exceptions	105
16.4 How to Enable IPsec Policies	106
17. Appendix	107
17.1 Glossary	107
17.2 Parameter List	110
17.3 Troubleshooting	143
17.4 Index	144

1 General Information



This chapter contains information concerning the device and the documentation as well as notes about your safety. You will learn how to benefit from your print server and how to operate the device properly.

1.1 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.

Supported Systems

Print servers have been designed for the use in the following systems:

- Microsoft Windows (32/64-Bit; Windows 10 or higher, Server 2012 R2 or higher)
- macOS (10.14.x or higher)



Important:

This document describes the usage in Windows / macOS environments.

1.2 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. System-specific instructions for the following systems:

- Windows
- macOS



PDF

Quick Installation Guide

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



Scope and Content

For information on the software version of your print server, refer to the version number displayed in the device list next to the print server in the SEH Product Manager.

Due to the multitude of supported operating systems, instructions are described exemplarily. The respective concept can be transferred to other versions of the operating system.

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 a quick overview of technical matters and background information; see: ⇒ [107](#).

Symbols and Conventions

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

Table1: Conventions within the documentation

Symbol / Convention	Description
 WARNING Warning	A warning contains important information that must be heeded. Non-observance may lead to malfunctions.
 Important: Important informations	These notes contain crucial information for failure-free operation.
 Tip	Recommendations and beneficial advice
✓ Requirement	Requirements that must be met before you can begin the action.
1. <i>Select...</i> 2. ...	Step-by-step instructions
↳ Result	Outcome of a performed action
□ Option	A square marks procedures and options that you can choose.
• Numeration	Listing
⇒ 	The arrow marks a reference to a page within this document. In the PDF file, you can jump to this page by clicking the symbol.
Bold	Established terms (of buttons or menu items, for example) are set in bold.
Courier	Command lines are set in 'Courier' font.
'Proper names	Proper names are put in inverted commas.

1.3 Support and Service

SEH Computertechnik GmbH offers extensive Support.

If you have any questions, please contact us.



Monday through Thursday
Friday

8:00 a.m. to 4:45 p.m.

8:00 a.m. to 15:15 p.m.



+49 (0)521 94226-44



support@seh.de

Customers from the United States of America (USA) and Canada please contact North American Support:



Monday – Friday

9:00 am – 5:00 pm (EST/EDT)



+1-610-943-3226



support@sehtechnology.com

All information and downloads regarding your product are available on our website:



<https://www.seh-technology.com>



1.4 Your Safety

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

Intended Use

Print servers are used in TCP/IP networks and are designed for use in office environments. They are used for direct integration of printers in office environments.

Improper Use

All uses of the device that do not comply with the functionalities described in the documentation are regarded as improper use.

Safety Regulations

Before commissioning the print server, read and follow the safety instructions in the 'Quick Installation Guide'. A printed version of this document is included in the scope of delivery.

Warnings

Before starting the initial setup of the UTN server, read and observe the safety regulations in the 'Installation Guide'. This document is enclosed in the packaging in printed form.



WARNING

Warning!

Liability and Guarantee

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

Modifications to the Device and Repairs

It is not allowed to make modifications to the hardware and software or to try to repair the device. If your device needs to be repaired, contact our support ⇒ [4](#).

1.5 First Steps

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

1. *Read and observe the security regulations in order to avoid damages to people and devices; see: ⇒ [5](#).*
2. *Carry out the hardware installation. The hardware installation comprises the connection of the printserver to the network and the mains supply; see: 'Quick Installation Guide'.*
3. *Make sure that the print server has an IP configuration which is suitable for your network; see: ⇒ [6](#).*
4. *Configure your clients for printing via the print server, see: Windows ⇒ [8](#)/macOS ⇒ [16](#).*
↳ Via the print server you can print to the printers connected.

1.6 Finding the Print Server (Determining the IP Address)

Why IP Addresses?

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

How Does the Print Server Obtain Its IP Configuration?

Print servers are shipped without IP configuration. Once the print server is connected to the network, it automatically receives an IP configuration via the boot protocols BOOTP or DHCP. If this is not the case, the print servers seeks a ZeroConf IP address from the ZeroConf address range (169.254.0.0/16).

How to Find The Print Server in the Network (Determining the IP Address)

The SEH Product Manager is a software tool developed by SEH Computertechnik GmbH for the administration of SEH print servers. By means of this tool you can find the print server's IP address, as described below.



WARNING

The SEH Product Manager only works in IPv4 networks. In IPv6-only networks only the Print Server Homepage (⇒ 19) can be accessed to administrate the print server.

The client, printer and print server must be assigned to the same local network segment for the initial configuration.

1. Download the installation file for the SEH Product Manager from the homepage of the SEH Computertechnik GmbH:

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



2. Start the installation file.
3. Select the desired language.
4. Follow the installation routine.
The SEH Product Manager will be installed on your client.
5. Start the SEH Product Manager on your client.
↳ The SEH Product Manager searches the network for existing print servers and displays them in the 'device list'.

If the print server has received an IP configuration via the boot protocols BOOTP or DHCP, you can identify it with the help of its type designation. If you are using several print servers of the same type, identify the print server using its hardware address. You can find the hardware address in the type plate at the bottom of the print server.

If the print server has assigned itself an IP address via ZeroConf from the address range (169.254.0.0/16) which is reserved for ZeroConf, it will be displayed in the device list, too (A print server with a ZeroConf IP address can only be found when the device is in the same network segment). Assign a new IP configuration to the print server, see below.



For more information on the SEH Product Manager, see: 'Administration via SEH Product Manager' ⇒ 19.

2 Printing in Windows



This chapter describes printing via the print server in Windows.

The print server embeds a printer into the network. In order to print via the print server, the printers connected to the print server must be set up as printers on the client system.



Important:

The following descriptions show how printers are set up in Windows 10. The menu navigation in other Windows systems may vary. For more information, please read the printer setup instructions in your Windows user manual.

2.1 How to Set Up Socket Printing

Socket printing is carried out by means of direct TCP/IP ports.

Procedure

Follow these steps if you want to print:

- 'Setting up the Printer on the Client' ⇒ 8

Setting up the Printer on the Client

Requirements

- ✓ The print server is connected to the network and the printer; see: Quick Installation Guide.
- ✓ The print server and the printer are turned on.
- ✓ The print server has a suitable IP configuration, see: ⇒ 6.
- ✓ You know the print server's current IP address; see: ⇒ 6.

1. Open the **Start** menu.
2. Select **Settings**.
*The **Settings** dialog appears.*
3. Select **Devices**.
*The **Devices** dialog appears.*
4. Select **Printers & Scanners**.
*The **Printers & Scanners** dialog appears.*

5. Select **Add a printers or scanners**.
Printers and scanners are searched for.
6. Scroll down to the end of the result list and select **The printer that I want isn't listed**.
*The **Add printer** dialog appears.*
7. Tick **Add a local printer or network printer with manual settings**.
8. Tick **Create a new port**.
9. From the list **Type of port**, select **Standard TCP/IP Port**.
10. Click **Next**.
11. In the **Hostname or IP address** box, enter the IP address of the print server.

**Important:**

Omit leading zeros from the IP address!

12. Enter a description into the **Port name** box.
13. Untick **Query the printer and automatically select the driver to use**.
14. Click **Next**.
15. (In the area **Device Type**, tick **Standard**.)
16. (Select **Generic Network Card** from the list.)
17. (Click **Next**.)
18. From the list **Manufacturer and Printers**, select the printer model.
19. Click **Next**.
20. Enter a description into the **Printer name** box.
21. Click **Next**.
The printer is being installed.
22. Tick **Do not share this printer**.
23. Click **Next**.
24. Click **Print a test page**.
The test page is printed.
25. Click **Finish**.
↳ The printer is set up on the client. If you print via the printer you have set up, the print job will be printed on the printer connected to the print server.

2.2 How to Set Up LPD/LPR Printing

When using the printing protocol Line Printer Daemon/Line Printer Remote-Protokoll (LPD/LPR), printing is done via a TCP/IP connection.

Mode of Operation

LPD/LPR consists of two components:

- Line Printer Daemon (LPD) refers to the process which receives print jobs from the LPR client. LPD runs on the print server. Thus the print server is called LPD server.
- Line Printer Remote (LPR) is the term for the process which sends print jobs to a printer or respectively to a print queue. The client (PC, etc.) which sends the print job is the LPR client and must be equipped with the required software.

Procedure

Follow these steps if you want to print:

- 'Activating LPR on the Client' ⇒ 10.
- 'Setting up the Printer on the Client' ⇒ 11.

Activating LPR on the Client

1. In the taskbar, enter 'Programs and Features' into the search box. The search results are displayed.
2. In the search results, select **Turn Windows features on or off**. The **Windows Features** dialog appears.
3. Under **Print and Document Services** activate **LPR Port Monitor**.
4. Click **OK** to confirm.
↳ LPR is activated on the client.

Setting up the Printer on the Client

Requirements

- ✓ The print server is connected to the network and the printer; see: Quick Installation Guide.
- ✓ The print server and the printer are turned on.
- ✓ The print server has a suitable IP configuration, see: ⇨ 6.
- ✓ You know the print server's current IP address; see: ⇨ 6.

1. Open the **Start** menu.
2. Select **Settings**.
The **Settings** dialog appears.
3. Select **Devices**.
The **Devices** dialog appears.
4. Select **Printer & Scanners**.
The **Printer & Scanners** dialog appears.
5. Select **Add a printers or scanners**.
Printers and scanners are searched for.
6. Scroll down to the end of the result list and select **The printer that I want isn't listed**.
The **Add printer** dialog appears.
7. Tick **Create a new port**.
8. From the list **Type of port**, select **Standard TCP/IP Port**.
9. Into the **Address** box, enter the IP address of the print server.



Important:

Omit leading zeros from the IP address!

10. Enter a description into the **Port name** box.
11. Untick **Query the printer and automatically select the driver to use**.
12. Click **Next**.
13. (In the area **Device Type**, tick **Standard**.)
14. (Select **Generic Network Card** from the list.)
15. (Click **Next**.)
16. From the list **Manufacturer and Printers**, select the printer model.
17. Click **Next**.
18. Enter a description into the **Printer name** box.
19. Click **Next**.
The printer is being installed.
20. Click **Print a test page**.
The test page is printed.
21. Click **Finish**.
↳ The printer is set up on the client.

2.3 How to Set Up IPP Printing

In IPP (Internet Printing Protocol) the print data is transmitted via HTTP to the printer. When printing via IPP, the print server is addressed via a Uniform Resource Identifier (URI). The syntax of the URI looks as follows:

```
http://<IP address>:631/ipp/<logical printer>
```

Requirements

- ✓ The print server is connected to the network and the printer; see: Quick Installation Guide.
- ✓ The print server and the printer are turned on.
- ✓ The print server has a suitable IP configuration, see: ⇒ 6.
- ✓ You know the print server's current IP address; see: ⇒ 6.

1. Open the **Start** menu.
2. Select **Settings**.
*The **Settings** dialog appears.*
3. Select **Devices**.
*The **Devices** dialog appears.*
4. Select **Printers & Scanners**.
*The **Printers & Scanners** dialog appears.*
5. Select **Add a printers or scanners**.
Printers and scanners are searched for.
6. Scroll down to the end of the result list and select **The printer that I want isn't listed**.
*The **Add printer** dialog appears.*
7. Tick **Select a shared printer by name**.
8. Into the **Select a shared printer by name** box, enter the print server's IP address and the socket number for IPP printing. If necessary, enter the name of the logical printer (lp1–lp8):
`http://<IP address>:631/ipp/<logical printer>`



Important:

Omit leading zeros from the IP address!

9. Click **Next**.
*The **Add Printer Wizard** appears.*
10. From the list **Manufacturer and Printers**, select the printer model.
11. To confirm click **OK**.
The printer is being installed.
12. Click **Next**.
13. Print a test page.
14. Click **Finish**.
 - ↳ The printer is set up on the client. If you print via the printer you have set up, the print job will be printed on the printer connected to the print server.

2.4 How to Configure Encrypted Printing

You can encrypt the print data that is sent to the print server from the client.

Mode of Operation

The communication between client and print server is encrypted via SSL/TLS. In this process, the print server is addressed via a Uniform Resource Identifier (URI). The syntax of the URI looks as follows:

```
https://<IP address>:443/ipp/<logical printer>
```

For authentication a print server certificate is required. The 'Common name' box of the print server certificate must contain the print server's IP address.

Procedure

In order to encrypted printing, proceed as follows:

- Create a self-signed certificate in the print server. Into the 'Common name' box, enter the IP address of the print server. Omit leading zeros from the IP address. See: 'How to Create a Self-Signed Certificate' ⇒ 64.
- Save the print server certificate on the client from which you want to print; see: ⇒ 8.
- On the client, create a printer for the printer connected to the print server; see: ⇒ 15.

You must observe the following instructions in the indicated order. If this procedure is not adhered to, the printer connected to the print server cannot be set up as printer on the client.

Saving the Print Server Certificate on the Client

The print server certificate can be saved on the client via the webbrowser Microsoft Edge .

Requirements

- ✓ You have administrative rights on the client.
 - ✓ Microsoft Edge is installed on the client. (It is installed by default in Windows 10.)
1. *In the taskbar, enter 'Microsoft Edge' into the search box. The search results are displayed.*
 2. *In the search results, right click on **Microsoft Edge**. The context menu appears.*
 3. *Select **Run as administrator**. A security query appears.*
 4. *Confirm the security query by clicking **Yes**. Microsoft Edge starts.*

5. Open an encrypted connection to the print server: To do this, enter 'https://' and the IP address of the print server as the URL.
Example: `https://10.168.1.234`
The following message appears: **Your connection isn't private.**
6. Click **Advanced**.
7. Click **Continue to this website (not recommended)**.
8. In the address bar, click **Not secure**.
The popup **Your connection to this site isn't secure** appears.
9. Click **Certificates (not valid)**.
10. Click **Copy to file**.
The **Certificate Export Wizard** appears.
11. Click **Next**.
12. Select **Base-64 encoded X.509 (.CER)**.
13. Click **Next**.
14. Save the certificate file.
15. Click **Finish**.
16. In the taskbar, enter 'Manage computer certificates' into the search box.
The search results are displayed.
17. In the search results, right click on **Manage computer certificates**.
The context menu appears.
18. Select **Run as administrator**.
A security query appears.
19. Click **Yes** to confirm.
The certificate dialog appears.
20. From the list, select **Trusted Root Certification Authorities**.
21. Right click and select **All Task**.
22. Click **Import**.
The **Certificate Import Wizard** starts.
23. Click **Next**.
24. Click **Next** to confirm the certificate store.
25. Click **Finish**.
A success message appears.
26. Confirm the success notification by clicking **OK**.
27. Close the certificate dialog by clicking **OK**.
↳ The print server certificate is installed on the client.

Setting up the Printer on the Client

Requirements

- ✓ The print server is connected to the network and the printer; see: Quick Installation Guide.
- ✓ The print server and the printer are turned on.
- ✓ The print server has a suitable IP configuration, see: ⇨ 6.
- ✓ You know the print server's current IP address; see: ⇨ 6.

1. Open the **Start** menu.
2. Select **Settings**.
*The **Settings** dialog appears.*
3. Select **Devices**.
*The **Add printers & scanners** dialog appears.*
4. Select **Add a printers or scanners**.
Printers and scanners are searched for.
5. Scroll down to the end of the result list and select **The printer that I want isn't listed**.
*The **Add printer** dialog appears.*
6. Tick **Select a shared printer by name**.
7. Into the **Select a shared printer by name** box, enter the print server's IP address and the socket number for IPP printing. If necessary, enter the name of the logical printer (lp1–lp8):
`https://<IP address>:443/ipp/<logical printer>`



WARNING

In the URI, enter the IP address exactly as it is written in the file 'Common name' of the print server certificate. Omit leading zeros in both cases. Otherwise the print server cannot be addressed.

8. Click **Next**.
*The **Add Printer Wizard** appears.*
9. From the list **Manufacturer and Printers**, select the printer model.
10. To confirm click **OK**.
The printer is being installed.
11. Click **Next**.
12. Print a test page.
13. Click **Finish**.
↳ The printer is set up on the client. If you print via the printer you have set up, the print job will be printed on the printer connected to the print server. The print data is transmitted in an encrypted way.

3 Printing in macOS



This chapter describes printing via the print server in macOS.

The print server embeds non-network-ready printers into the network. In order to print via the print server, the printers connected to the print server must be set up as printers on the client system. This is done using the System Preferences.



Important:

The following descriptions show how printers are set up in macOS (10.14 or higher). The menu navigation in other macOS systems may vary. For more information, please read the printer setup instructions in your macOS manual.

3.1 How to Set Up IPP Printing

In IPP (Internet Printing Protocol) the print data is transmitted via HTTP to the printer. Print data can be transmitted via IPP in an encrypted or unencrypted way.

When printing via IPP, the print server is addressed via a Uniform Resource Identifier (URI). The URI syntax is as follows:

Transmission of unencrypted print data:

```
ipp://<IP address>:631/ipp/<logical printer (lp1-lp8)>
```

Transmission of encrypted print data:


```
ipp://<IP address>:443/ipp/<logical printer (lp1-lp8)>
```

The URIs are split into parts and entered via the system dialog.

Requirements

- ✓ The print server is connected to the network and the printer; see: Quick Installation Guide.
- ✓ The print server and the printer are turned on.
- ✓ The print server has a suitable IP configuration, see: ⇒ 6.
- ✓ You know the print server's current IP address; see: ⇒ 6.
- ✓ Only for the transmission of encrypted print data:
A certificate is installed in the print server; see: ⇒ 62.

1. Open the **System Preferences**.
2. Click **Printers & Scanners**.


3. Click the  icon.
The **Add** dialog appears.
4. Click **IP**.
5. Into the **IP Address** box, enter the IP address or host name of the print server (with leading zeros).
Optional: Add the port number.
Syntax: <IP address or host name>:<port number>
- Port number 443 = encrypted printing.
- Port number 631 = unencrypted printing.
6. From the **Protocol** list, select **Internet Printing Protocol - IPP**.
7. Into the **Queue** box, enter 'ipp/' and a logical printer (lp1 - lp8).
Syntax: ipp/<logical printer (lp1-lp8)>
Alternatively, leave the box empty, then the logical printer no. 1 will be used automatically.
8. Enter freely definable names for **Name** and **Location**.
9. From the **Use** list, select the printer driver.
10. Click **Add**.
The setting up dialog appears.
11. Configure the printer options.
12. Click **OK** to confirm.
↳ The printer is set up on the client. If you print via the printer you have set up, the print job will be printed on the printer connected to the print server.

3.2 How to Set Up LPD Printing

When using the printing protocol Line Printer Daemon, printing is done via a TCP/IP connection.

Requirements

- ✓ The print server is connected to the network and the printer; see: Quick Installation Guide.
- ✓ The print server and the printer are turned on.
- ✓ The print server has a suitable IP configuration, see: ⇒ 6.
- ✓ You know the print server's current IP address; see: ⇒ 6.

1. Open the **System Preferences**.
2. Click **Printers & Scanners**.
3. Click the  icon.
The **Add** dialog appears.
4. Click **IP**.
5. Into the **IP Address** box, enter the IP address or host name of the print server (with leading zeros).
6. From the **Protocol** list, select **Select Line Printer Daemon - LPD**.
7. Enter a logical printer (lp1 - lp8) into the **Queue** box.
Alternatively, leave the box empty, then the logical printer no. 1 will be used automatically.
8. Enter freely definable names for **Name** and **Location**.
9. From the **Use** list, select the printer driver.

10. Click **Add**.
The Setting up dialog appears.
11. *Configure the printer options.*
12. Click **OK** to confirm.
 - ↳ The printer is set up on the client. If you print via the printer you have set up, the print job will be printed on the printer connected to the print server.

4 Administration Methods




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.

4.1 Administration via SEH Product Manager

The SEH Product Manager is a software tool developed by SEH Computertechnik GmbH for the administration of SEH print servers.

**Important:**

The SEH Product Manager only works in IPv4 networks. In IPv6-only networks only the Print Server Homepage (⇒ 22) can be accessed to administrate the print server.

Mode of Operation

The software is installed on all clients from which print servers are to be administrated and managed on the network.

After the SEH Product Manager is started, the network will be scanned for connected print servers. The network range to be scanned is freely definable. All print servers found will be displayed in the 'device list'.

You can modify the device list and adapt it to your individual needs. You can select the print servers in the device list and configure them.

If a task can be performed using the SEH Product Manager, this will be described in the corresponding chapters.

Installation

In order to use the SEH Product Manager, the program must be installed on a computer with Windows / macOS operating system. The SEH Product Manager installer can be found on the SEH Computertechnik GmbH website:

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



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


- ✓ Windows 7 or higher
- ✓ The Installation can only be carried out by users with administrative rights.

The installation file is available as ‘*.dmg’ for macOS systems.

- ✓ macOS 10.12.x or higher
- ✓ The Installation can only be carried out by users with administrative rights.
- ✓ You know the administrator password.

1. *Start the installation file.*
2. *Follow the installation routine.*

Program Start

You can identify the SEH Product Manager by its icon: . The SEH Product Manager can be started with the usual mechanisms of your operating system.

Structure

After the program start you will see the main dialog with the following elements.

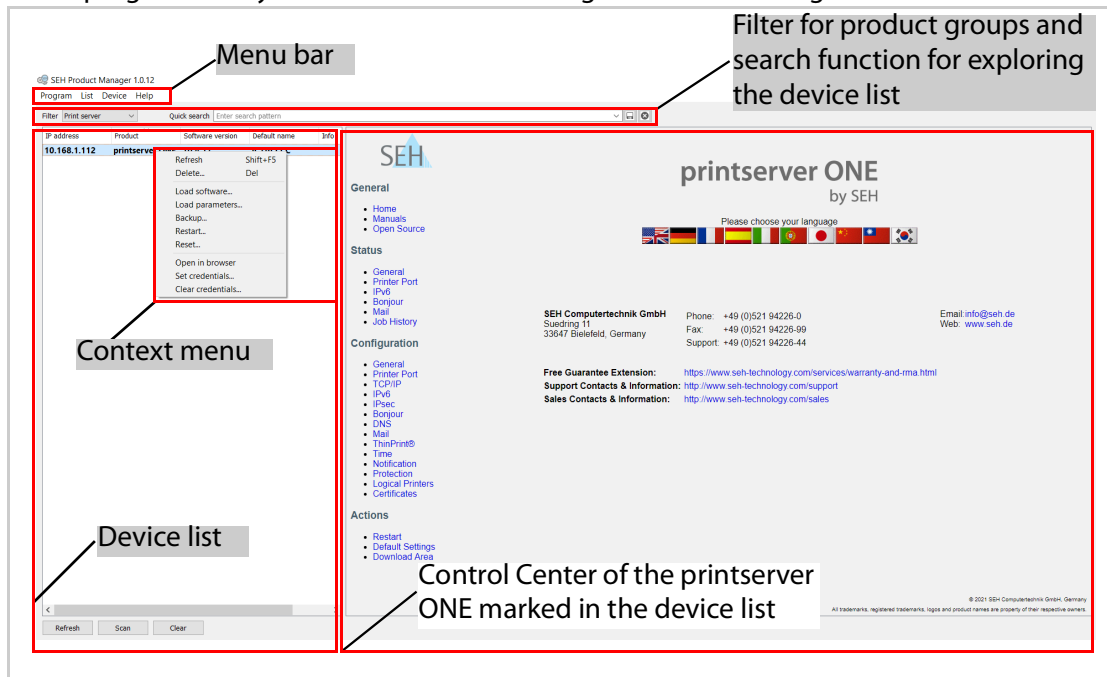




Fig. 1: SEH Product Manager- Main dialog

Calling the user interface of a print server

Select a print server in the device list to access the print server's user interface.

By default, the user interface is displayed to the right of the device list. Most configurations of the print server are performed using the user interface.

The print server's user interface can be opened in an Internet browser using the SEH Product Manager as the Printserver Homepage; see  .

Functionality and configuration of the user interface and the Print Server Homepage are identical. The functions and configurations described in the next chapters are therefore explained using the user interface of the SEH Product Manager.

Detailed information on how to use the SEH Product Manager can be found in the Online Help. To start the Online Help, select **Help – Online Help** from the menu bar.

4.2 Administration via Print Server Homepage

Functionalities

The print server has a user interface, the Print Server Homepage , which can be opened in an Internet browser (Microsoft Edge, Mozilla Firefox, Safari).

The print server can be configured and monitored via the Print Server Homepage .

Requirements

- ✓ The print server is connected to the network, printer and the mains voltage.
- ✓ The print server has a suitable IP configuration, see: ⇒ 6.

Starting the Print Server Homepage

1. *Open your browser.*
2. *Enter the IP address of the print server as the URL.*
 - ↳ The Printserver Homepage **is displayed in the browser.**



Important:

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

You can also start the Print Server Homepage via the software tool 'SEH Product Manager'.

1. *Select the print server in the device list.*
2. *Select **Actions – Launch Browser** from the menu bar.*
 - ↳ The Print Server Homepage **is displayed in the browser.**

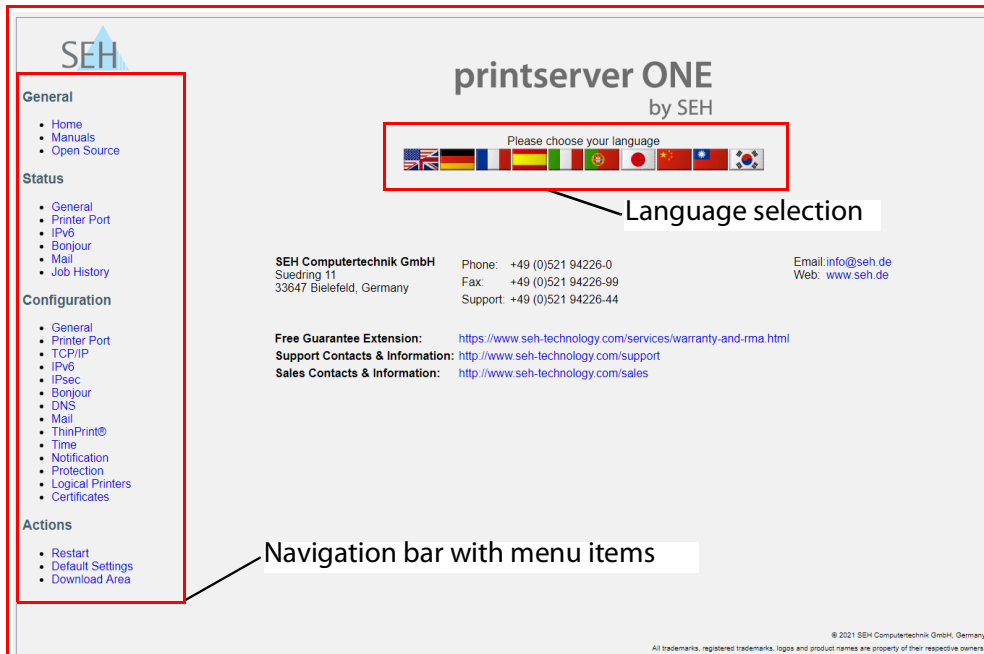


Fig. 2: printserver Control Center

Structure of the Print Server 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 Print Server Homepage via **General – Home**. Simply select the relevant flag. You will also see the contact information of the manufacturer.

Clicking the **General – Manuals** link brings you to the SEH Computertechnik GmbH homepage. Here, you can download the latest manuals as *.pdf files.

Right-click in the user interface of the print server home page to open the context menu. Using the context menu, you can navigate between pages and reload pages.

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

The appearance of the Print Server Homepage depends on the print server model and software version.

4.3 Administration via 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/TLS (FTPS)

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

We recommend using SSL/TLS so that unencrypted user names, passwords, and data cannot be read by unauthorized persons.

Configuring Parameters via 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.

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 the enter key 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: ⇒ ¶110.
 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.

Which Functions Are Supported?

An FTP/FTPS connection allows you to

- print a status page ⇒ ¶45
- print a service page ⇒ ¶45
- configure the printserver parameters ⇒ ¶22
- 'reset the print server parameters to their default settings' ⇒ ¶80
- 'query the printer status' ⇒ ¶44

- 'carry out updates' ⇒ 81

4.4 Administration via Email

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

- ✓ A DNS server has been configured on the print server, see: ⇒ 34.
- ✓ In order to receive emails, the print server must be set up as user with its own email address on a POP3 server.
- ✓ POP3 and SMTP parameters have been configured on the print server; see: ⇒ 37.

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.

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' ⇒ 26.*
 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	sends the status page of the print server
	get servicepage	sends the service page of the print server
	get parameters	sends the parameter list of the print server
	get jobhistory	sends the job history
	get pagecounter	sends the number of printed pages
	set parameters	sends parameters to the print server The syntax and values can be obtained from the parameter list, see: ⇒ 110. Parameter and value must be entered into the email body; see: ⇒ 26.
	print	Prints the email (text only).
	printa	Prints the first attachment of an email.
	print attachment	See: 'printa'
	update ps	Carries out an automatic update using the software that is attached to the email.
	clean mailqueue	Empties the email printer queue and deletes all entries from the mailbox.

Commands	Option	Description
[ack] (optional)	–	sends an acknowledgment back to the sender
[<Com- ment>] (optional)	–	Freely definable text for descriptions.

The following applies for the instructions:

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

**Important:**

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: ⇨ 59), you also need a password. Enter the password into the first line of the email body. Note the following syntax:

```
password: <password>
```

Parameter Changes

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

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

The syntax and values can be obtained from the parameter list, see: ⇨ 110.

Example 1

This email causes the print server to send the parameter list to the sender of the email.

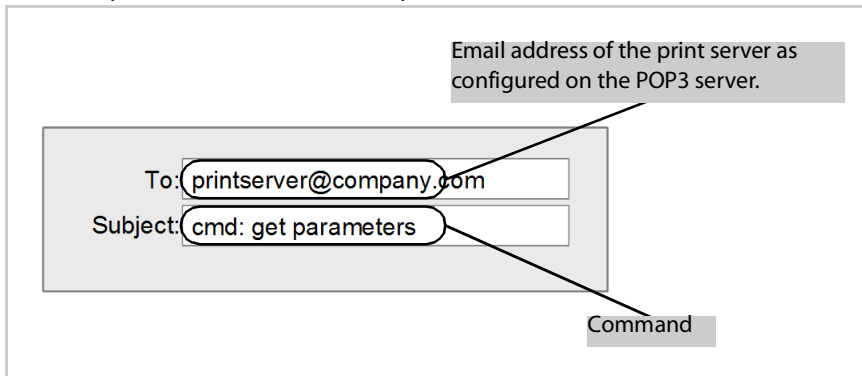


Fig. 3: Administration via Email - Example 1

Example 2

This e-mail causes the printer to print the e-mail attachment. The sender also receives an acknowledgment of receipt by the print server.

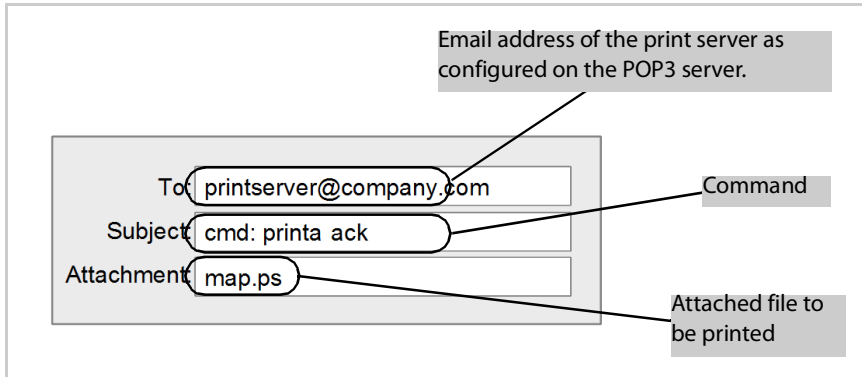


Fig. 4: Administration via Email - Example 2

5 Network Settings



You can define various settings for an ideal integration of the print server into a network. This chapter explains which network protocols and settings are supported by the print server.

5.1 How to Configure IPv4 Parameters

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

The boot protocols DHCP and BOOTP belong to the TCP/IP protocol family. You can define various IPv4 parameters for an ideal integration of your print server into a TCP/IP network. For further information about the IP configuration, see: ⇒ 6.

Configuring IPv4 Parameters via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – TCP/IP** in the user interface of the print server homepage.
4. Configure the TCP/IP parameters; ⇒ table 2 30.
5. Click **Save** to confirm.
↳ The settings are saved.

Table 2: TCP/IP Parameters

Parameters	Description
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, it will be attempted to automatically enter the address of the found multicast router as gateway address. If disabled, the gateway address has to be entered manually.
Host name	Host Name of the print server
Contact person	Freely definable description

Parameters	Description
Location	Freely definable description
DHCP BOOTP ZeroConf	Enables/disables the protocols 'DHCP', 'BOOTP', and 'ZeroConf'. Protocols offer various possibilities to save the IP address in the print server. We recommend disabling these options once an IP address has been assigned to the print server.

5.2 How to Configure IPv6 Parameters

You can integrate the print server into an IPv6 network.

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

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 (:).

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

Leading zeros in a field can be omitted.

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

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

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

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

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

**Important:**

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'.

Configuring IPv6 Settings via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Click **Configuration – IPv6** in the user interface of the print server homepage.
4. Configure the IPv6 parameters; ⇨ table 3 33.
5. Click **Save** to confirm.
↳ The settings are saved.

Table 3: IPv6 Parameters

Parameters	Description
IPv6	Enables/disables the IPv6 functionality of the print server.
IPv6 address	<p>Defines a print server IPv6 unicast address assigned manually in the format n:n:n:n:n:n:n.</p> <p>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.</p>
Router	Defines the IPv6 unicast address of the router. The print server sends its 'Router Solicitations' (RS) to this router.
Prefix length	<p>Defines the length of the subnet prefix for the IPv6 address. The value 64 is preset.</p> <p>Address ranges are indicated by prefixes. The prefix length (number of bits used) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/'.</p>
Automatic configuration	Enables/disables the automatic assignment of the IPv6 address for the print server.

5.3 How to Adapt the Network Speed

Network communication is done via three direction-oriented transmission methods between two equal data stations. Simplex, half duplex and full duplex.



Important:

The network speed can only be adjusted for a connection via cable (Ethernet).

Duplex Mode

The print server is able to recognize the duplex mode used in the Ethernet and to automatically adjust to it.

The 'Auto' mode is preset. There is also the possibility to manually adjust the setting of the desired duplex mode.



WARNING

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.

Adapting the Speed via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – General** in the user interface of the print server homepage.
4. Select the desired setting from the **Ethernet settings** list.
5. Click **Save** to confirm.
↳ The setting will be saved.

5.4 How to Configure the DNS

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

Benefits and Purpose

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

Configuring DNS via the SEH Product Manager

Requirements

- ✓ A DNS server is available in the network.
- 1. *Start the SEH Product Manager.*
- 2. *Select the print server in the device list.*
The printserver homepage appears.
- 3. *Select **Configuration – DNS** in the user interface of the print server homepage.*
- 4. *Configure the DNS parameters; ⇨ table 4 35.*
- 5. *Click **Save** to confirm.*
↳ The settings are saved.

Table 4: DNS parameters

Parameters	Description
DNS	Enables/disables the name resolution via a DNS server.
Domain name	Defines the domain name of an existing DNS server.
Primary DNS server	Defines the IP address of the primary DNS server.
Secondary DNS server	Defines the IP address of the secondary DNS server. The secondary DNS server is used if the first one is not available.

5.5 How to Configure Bonjour

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

The print server uses Bonjour to:

- check the IP address assigned via ZeroConf (⇨ 6).
- match host names and IP addresses
- announce its Bonjour services (printing services, Printserver Homepage)

Configuring Bonjour via the SEH Product Manager

1. *Start the SEH Product Manager.*
2. *Select the print server in the device list.*
The printserver homepage appears.


3. Select **Configuration – Bonjour** in the user interface of the print server homepage.
4. Configure the Bonjour parameters; ⇒ table 5  36.
5. Click **Save** to confirm.
 - ↳ The settings are saved.

Table 5: Bonjour Parameters

Parameters	Description
Bonjour	Enables/disables Bonjour.
Bonjour name	<p>Defines the Bonjour name of the print server.</p> <p>The print server uses this name for its Bonjour services. If no Bonjour name is entered, the default name will be used (printer name@lCxxxxxx).</p> <p>You can enter a maximum of 63 characters. The name must not start with an underscore.</p>

5.6 How to Use SNMP

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

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


Private MIB of the Print Server

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.

Benefits and Purpose

The print server parameters can be queried and configured by a management tool by means of the SNMP protocol.

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: ⇒  6.



For more information, read the manual of your SNMP management tool.

5.7 How to Configure POP3 and SMTP

You must configure the protocols POP3 and SMTP on the TPR so that the notification service (⇒ 37) and the administration via email (⇒ 25) will work properly.

POP3

'POP3' (Post Office Protocol Version 3) is a transfer protocol that a client can use to fetch emails from a mail server. POP3 is used in print servers to administer print servers via email; see: ⇒ 25.

SMTP

'SMTP' (Simple Mail Transfer Protocol) is a protocol that controls the sending of emails in networks. SMTP is used in print servers to administer print servers via email (see: ⇒ 25) and to send printer information via email (see: ⇒ 55).

Configuring POP3 via the SEH Product Manager

Requirements

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

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – Mail** in the user interface of the print server homepage.
4. Configure the POP3 parameters; ⇒ table 6 37.
5. Click **Save** to confirm.
↳ The settings are saved.

Table 6: POP3 Parameters

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

Parameters	Description
User name	Defines the user name used by the print server to log on to the POP3 server.
Security	Defines the authentication method (APOP/SSL/TLS).
Check mail every	Defines the time interval (in minutes) for retrieving emails from the POP3 server.
Server port	Defines the port used by the print server for receiving emails. The port number 110 is preset. When using SSL/TLS, enter 995 as port number.
Password	Defines the password used by the print server to log on to the POP3 server.
Delete read messages	Enables/disables the automatic deletion of read emails.
Ignore mail exceeding	Defines the maximum email size (in KByte) to be accepted by the print server. (0 = unlimited)

Configuring SMTP via the SEH Product Manager

Requirements

- ✓ The print server is set up as user with its own email address on a POP3 server.
- 1. Start the SEH Product Manager
- 2. Select the print server in the device list.
The *printserver homepage* appears.
- 3. Select **Configuration - Mail - SMTP** in the user interface of the print server homepage.
- 4. Configure the SMTP parameters; ⇒ table 7 39.
- 5. Click **Save** to confirm.
 - ↳ The settings are saved.



The SMTP input mask can also be found under **Configuration – Notification – Email Notification**.

Table 7: SMTP Parameters

Parameters	Description
Server name	Defines the SMTP server via the IP address or the host name. The host name can only be used if a DNS server was configured beforehand.
Server port	Defines the port number used by the print server to send emails to the SMTP server. The port number 25 is preset. When using SSL/TLS, enter 995 as port number.
TLS	Enables/disables TLS. The TLS protocol serves to encrypt the transmission between the print server and the SMTP server.
Sender name	Defines the email address used by the print server to send emails. <u>Note:</u> Very often the name of the sender and the user name are identical.
Signature	Defines the signature to be contained 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. A signature created by the sender allows the recipient to verify the identity of the sender and to make sure that the email was not modified.
Use POP3 settings	Defines whether the POP3 settings for the authentication shall be used or whether different login data (user name and password) shall be used.
User name	Defines the user name used by the print server to log on to the SMTP server.
Password	Defines the password used by the print server to log on to the SMTP server.

6 Port Settings



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

6.1 How to Enable PJJ

With PJJ (Print Job Language) commands you can get additional printer information such as detailed status information, printer panel readings or printed pages statistics.

Which information (if any) will be displayed depends on the degree in which the printers can interpret PJJ commands. Refer to the manual of your printer for further information.

The print server recognizes if a printer supports PJJ and displays this in the SEH Product Manager under **Status – Printer Port** in the **Printer emulation** parameter.



Important:

The option '1284.4/MLC' may not be enabled at the same time

Enabling PJJ via SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – Printer Port** in the user interface of the print server homepage.
4. Tick **PJJ** for the relevant printer port.
5. Click **Save** to confirm.
↳ The setting will be saved.

6.2 How to Enable 1284.4/MLC

IEEE 1284.4 defines a transport protocol for a point-to-point link between a client application and a printer or MFP. One physical link allows you to use several logical channels. These channels allow you to simultaneously and independently exchange different data.

Benefits and Purpose

1284.4/MLC optimizes the bidirectional functionality of external interfaces. Using 1284.4/MLC, you can get more detailed printer status information.



Important:

The option 'PJI' may not be enabled at the same time.

Enabling 1284.4/MLC via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – Printer Port.** in the user interface of the print server homepage.
4. Tick **1284.4/MLC.**
5. Click **Save** to confirm.
↳ The setting will be saved.

6.3 How to Define the Communication Mode

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

The following communication modes are available:

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

Defining the Communication Mode via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – Printer Port.** in the user interface of the print server homepage.
4. Select the desired mode from the **Port mode** list.
5. Click **Save** to confirm.
↳ The setting will be saved.

7 Device Settings



You can configure the device time and the device language for the print server and specify a description. This chapter describes the device settings.

7.1 How to Configure the Language of the Device

You can set the device language of the print server. The status information are displayed in the device language. The print server supports the following languages:

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

Configuring the Device Language via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – General** in the user interface of the print server homepage.
4. Select the desired language from the **Print server language** list.
5. Click **Save** to confirm.
 - ↳ The settings are saved.

7.2 How to Configure the Device Time

You can control the device time of the print server via a time server (SNTP server) in the network. A time server synchronizes the time of devices within a network. In the print server, the time server is defined via the IP address or the host 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 (⇒ 57) '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.

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.

Configuring the Device Time via the SEH Product Manager

Requirements

- ✓ A time server is integrated into the network.
- 1. *Start the SEH Product Manager.*
- 2. *Select the print server in the device list.*
The printserver homepage appears.
- 3. *Select **Configuration – Time** in the user interface of the print server homepage.*
- 4. *Click **SNTP**.*
- 5. *Into the **Time server** box, enter the IP address or the host name of the time server*
(The host name can only be used if a DNS server was configured beforehand.)
- 6. *Select the code for your local time zone from the **Time zone** list.*
- 7. *Click **Save** to confirm.*
↳ The settings are saved.

7.3 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 SEH Product Manager

1. *Start the SEH Product Manager.*
2. *Select the print server in the device list.*
The printserver homepage appears.
3. *Select **Configuration – General** in the user interface of the print server homepage.*
4. *Enter freely definable names for **Description** and **Dealer**.*
5. *Into the **Dealer URL** box, enter the website of your print server retailer or seller.*
6. *Click **Save** to confirm.*
↳ The data is saved.

8 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.



The LEDs of the print server show its status. Please refer to the 'Quick Installation Guide' for detailed information.

8.1 How to View Status Information

You can view print server status information.

Viewing Status Information via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. In the user interface of the print server homepage, select the desired menu item under the **Status** category.
↳ The status information is shown.

8.2 What Status Information is Shown?

This chapter gives an overview of the print server status information. Different status information is available depending on your print server model.

General Status

The **General** page shows status information, such as the name of the print server, the hardware address, and 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.

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 on the Print Server Homepage.)

Bonjour Status

The **bonjour** page displays the bonjour name. As for print servers with several physical printer ports, the bonjour name is displayed separately for each port.

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. From the 65th print job onwards the FIFO method (first-in, first-out) is applied. 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: ⇨table 11 57.

8.3 How to Print a Status Page

You can print status pages. The pages are available in English.

Status Page

A status page contains important, basic print server information such as the print server type, MAC address, etc.

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.

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 the enter key 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 Button

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

1. *Press the button for a short time.*
↳ The status page is printed.

9 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.

9.1 How to Define a Timeout for Taking on Print Jobs

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

Benefits and Purpose

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

Defining a Timeout via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – General** in the user interface of the print server homepage.
4. Enter the time frame in seconds after which the connection will be aborted into the **Job receive timeout** box.
We recommend to set the value to '120'. (0 s = off)
5. Click **Save** to confirm.
↳ The setting will be saved.

9.2 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 assigned via the SEH Product Manager.

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.



Important:

Make sure that the logical printer does not convert data (e.g. ASCII to PostScript), see: ⇨ 50.

Assigning the Print File via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Actions – Download Area** in the user interface of the print server homepage.
4. Select **File Printing**.
5. Select a logical printer from the list.
6. Click **Browse / Choose File**.
7. Select the print file.
8. Click **Print**.
9. (Enter the print server password, if necessary.)
↳ The print file is printed.

9.3 How to Modify Print Data

The print server offers several filter functions for the subsequent editing of print data.

Filter Function 'Find and Replace'

You can use the filter function 'Find and Replace' to edit print data subsequently. 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: ⇨ 50.

Syntax

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

- 256 characters can be used.
- You can define various patterns. Use the double semicolon ';' 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 (e.g. Postscript or PCL) 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

The string 'white' is to be replaced by the string 'black' and the string 'cat' is to be replaced by 'dog' in the print data.

	ASCII	Decimal	Hexadecimal
Search	white;;c at	\119\104\105\116\101;;\09 9\097\116	77 68 69 74 65 63 61 74
Replac e	black;;d og	\098\108\097\099\107;;\10 0\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: ⇒ 50.

9.4 How to Convert Print Data?

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

Filter Function 'ASCII / PostScript'

The print server supports the conversion of print data from ASCII to PostScript format. Configuration is done via logical printers, see: ⇒ 50.

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: ⇒ 50.

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: ⇒ 50.

9.5 How to Use Logical Printers (Filter Functions)?

What Are Logical Printers?

Logical printers are pre-installed filters that are assigned to a print object. The filter contains information about the use of 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 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 printing of a **banner page** if the LPD protocol is used. ASCII or PostScript can be used to display the banner page.
- The print server supports the conversion of print data from **ASCII** to **PostScript** format.
- The print server supports the printing of **binary PostScript** files.

- The print server allows the sending of **start** and **end sequences** before/after a print job. These sequences may e.g. consist of PRESCRIBE or ESC commands that trigger a form feed after the print job, see: 'How to Modify Print Data' ⇨ 48.
- The print server supports a **Search and Replace** function. 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' ⇨ 48.

Preset Functions of Print Servers.

Logical Printer	Preset Function	Preset TCP/IP Port
1	Default settings	9100
2	Conversion of Line Feed (LF) to Carriage Return with Line Feed (CR+LF)	9101
3	Conversion of ASCII into PostScript data	9102
4	Printing a banner page in Novell networks or if 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

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.)

Configuring Logical Printers via the SEH Product Manager

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

1. *Start the SEH Product Manager.*
2. *Select the print server in the device list.
The printserver homepage appears.*
3. *Select **Configuration – Logical Printer** in the user interface of the print server homepage.*

4. Change the desired parameters, ⇒ table 8 52.
5. Click **Save** to confirm.
 - ↳ The setting will be saved.

Table 8: Settings of the Logical Printers

Parameters	Description
Start Sequences / End Sequences	Depending on the application, you might have to configure the logical printer.
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 or lost 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 if the LPD protocol is used.
ASCII/Post-Script	Enables/disables the conversion of ASCII into PostScript data.
Banner page mode	Defines the format (ASCII or PostScript) in which the banner page will be printed.
TCP/IP Port	TCP/IP port in accordance with the logical printer. The following default values apply: No. 1 = 9100No. 5 = 9104 No. 2 = 9101No. 6 = 9105 No. 3 = 9102No. 7 = 9106 No. 4 = 9103No. 8 = 9107

Parameters	Description
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.
Binary Post-Script	Enables/disables the printing of binary PostScript files. 'Binary PostScript' should be enabled if binary PostScript files are to be printed in heterogeneous networks.

Assigning Logical Printers

Depending on your system, logical printers may be addressed in various ways. The assignment is done when you create printers on the client for the printers connected to the print server (⇒ 11). In Windows, the respective TCP/IP ports are used instead of the logical printers. In macOS, logical printers are addressed with 'lp1' through 'lp8'.

10 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.

10.1 How to View the Printer Status

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

Displaying the Printer Status and the Printer Display via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Status – Printer Port** in the user interface of the print server homepage.
↳ The printer status and the printer display are displayed.

View 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.

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 the enter key if no password has been assigned.
3. Get the printer status from the print server:
get printerport
4. Close the FTP connection:
quit

10.2 How to Get Additional Printer Information

With PJJ (Print Job Language) commands you can get additional printer information via the print server, such as detailed status information, printer panel readings or printed pages statistics. To use PJJ, see: ⇒ 40.

10.3 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 prompt a notification.

This allows up to two 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 sent depends on the connected printer model.

Configuring Email Notifications via the SEH Product Manager

Requirements

- ✓ A DNS server has been configured on the print server, see: ⇒ 34.
 - ✓ SMTP parameters are configured on the print server; see: ⇒ 36.
1. Start the SEH Product Manager.
 2. Select the print server in the device list.
The printserver homepage appears.
 3. Select **Configuration – Notification** in the user interface of the print server homepage.
 4. Select **Email Notification**.
 5. Configure the notification parameters; ⇒ table 9 55.
 6. Click **Save** to confirm.
 - ↳ The settings are saved.

Table 9: Parameters for Email Notification

Parameters	Description
Email active	Enables/disables the email notification for recipient 1 or 2.
Email recipient	Defines the email address of the recipient.
Accounting - Job history, time interval (h), jobs	Enables/disables the sending of 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)	Enables/disables the sending of 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.

Parameters	Description
Printer error - Paper empty, Paper jam, etc.	Define the type of printer error that will cause a notification.

10.4 How to Get Printer Messages via SNMP Trap

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

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



Important:

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

Enabling SNMP Trap Notifications via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – Notification** in the user interface of the print server homepage.
4. Select **SNMP Trap Notification**.
5. Configure the notification parameters; ⇒ table 10 56.
6. Click **Save** to confirm.
↳ The settings are saved.

Table 10: Parameters for SNMP Trap Notification

Parameters	Description
IP address	Defines the IP address of the recipient.
Trap community	Defines the trap community of the recipient.
Authentication traps	Enables/disables the sending of authentication traps.
Printer traps	Enables/disables the sending of traps in case of an error.

Parameters	Description
Printer error - Paper empty, Paper jam, etc.	Defines the printer errors that will cause a notification.

10.5 How to View the Job History

Information on the print jobs handled by the print server are registered and shown in the job history.

A maximum of 64 print jobs are displayed. From the 65th print job onwards the FIFO method (first-in, first-out) is applied. 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.

Depending on the connected printer model, the following information is shown in the job history:

Table 11: Job History - Status Information

Parameters	Description
No.	Number of the print job.
Status	<p>Status of the print connection. The following statuses are possible:</p> <p>'Pending' means that the print job has been accepted by the print server but that the data transfer has not yet started.</p> <p>'Processing' means that the print job has been transferred from the print server to the printer.</p> <p>'Processing stopped' means that the data transfer to the printer was interrupted. This can occur if, for example, the printer ran out of paper. If the printer error is fixed, data transfer will be resumed.</p> <p>'Completed' means that the print server has completely forwarded the print job to the printer.</p> <p>'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.</p>
Protocol	Protocol used to transfer the print data.
Name	Job names of print jobs using 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.

Parameters	Description
Sender	Sender of the print job (in TCP/IP networks).
Size	Size (in kB) of the print job.
Pages	Number of pages of the print job.
Creation time	Time at which the print job has been sent to the print server.
Duration	The time (in seconds) needed by the print server for processing the print job.

**Important:**

A time server (⇒ 42) must be configured on the print server so that the date and time can be displayed correctly. If no time server is configured, the time stamp corresponds to the default time.

Displaying the Job History via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Status – Job History** in the user interface of the print server homepage.
↳ The job history is displayed.

11 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.

11.1 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

In addition, you can protect the display of parameters with a password too. For this purpose, the parameter **Access control** must be enabled. If this parameter is enabled, a password must be entered when opening the SEH Product Manager.

Defining the Password via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration - Protection** in the user interface of the print server homepage.
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 **Save** to confirm.
↳ The settings are saved.

11.2 How to Disable the HTTP Access (Protection against Viruses)

HTTP (Hypertext Transfer Protocol) is a protocol for the transfer of data. The print server needs HTTP for the data transfer of the Print Server Homepage.

Benefits and Purpose

The print server cannot be attacked directly by viruses. Attacks to open ports (e.g. port 80 / HTTP) 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.

Disabling HTTP via the SEH Product Manager

1. *Start the SEH Product Manager.*
2. *Select the print server in the device list.
The printserver homepage appears.*
3. *Select **Configuration - Protection** in the user interface of the print server homepage.*
4. *Clear **HTTP**.*
5. *Click **Save** to confirm.*
↳ The setting will be saved.

11.3 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 print.

Benefits and Purpose

The 'IP Sender Control' allows you to protect printers and sensitive data against 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.



WARNING

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 SEH Product Manager

1. *Start the SEH Product Manager*
2. *Select the print server in the device list.*
The printserver homepage appears.
3. *Select **Configuration - Protection** in the user interface of the print server homepage.*
4. *Into the **IP sender** box, enter the IP addresses or host names of authorized clients.*
(The host name can only be used if a DNS server was configured beforehand.)
5. *Click **Save** to confirm.*
↳ The settings are saved.

12 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: ⇒ 13.
- check the identity of the print server in the network; see: ⇒ 70.
- authenticate the print server if the connection is encrypted via SSL/TLS (HTTPS).
- administer the print server via an FTPS connection; see: ⇒ 24.
- allow for a certificate-based authentication of the remote server in the case of IPsec; see: ⇒ 97.
- to encrypt ThinPrint data; see: ⇒ 89.



Important:

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 ⇒ 59.

Which Certificates are available?

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

- Upon delivery, a self-signed certificate (the so-called **default certificate**) is stored in the print server. It is recommended that you replace the default certificate by a self-signed certificate or requested certificate as soon as possible.
- **Self-signed certificates** have a digital signature that has been created by the print server.
- A **requested certificate** is created by a certification authority (CA) for the print server on the basis of a certificate request.
- **CA certificates** are certificates that have been issued for a certification authority (CA). They are used for verifying certificates that have been issued by the respective certification authority.

- **PKCS#12** certificates are used to save private keys and their respective certificates and to protect them by means of a password.

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

- 1 print server certificate, i.e. 1 self-signed certificate or 1 requested certificate or 1 PKCS#12 certificate
- 1–8 CA certificates

12.1 How to View Certificates

Certificates installed in the print server and certificate requests can be displayed and viewed.

Displaying the Print Server Certificate via the SEH Product Manager

Requirements

- ✓ A certificate request has been created or a client certificate is installed in the print server.
1. *Start the SEH Product Manager.*
 2. *Select the print server in the device list.*
The printserver homepage appears.
 3. *Select **Configuration – Certificates** in the user interface of the print server homepage.*
 4. *Select **Print server certificate**.*
 - ↳ The certificate respectively certificate request is displayed.

Displaying the CA certificate via the SEH Product Manager

Requirements

- ✓ A CA certificate is installed in the print server.
- 1. *Start the SEH Product Manager.*
- 2. *Select the print server in the device list.*
The printserver homepage appears.
- 3. *Select **Configuration – Certificates** in the user interface of the print server homepage.*
- 4. *Select **CA certificates**.*
- 5. *For the desired certificate select **Show**.*
 - ↳ The CA certificate is displayed.

12.2 How to Create a Self-Signed Certificate

Creating Self-Signed Certificates via the SEH Product Manager

Requirements

- ✓ A print server certificate must not be already installed in the print server. To delete a print server certificate, see: ⇒ 69.
- 1. *Start the SEH Product Manager.*
- 2. *Select the print server in the device list.*
The printserver homepage appears.
- 3. *Select **Configuration – Certificates** in the user interface of the print server homepage.*
- 4. *Select **Print server certificate**.*
- 5. *Enter the relevant parameters; ⇒ table 12 64.*
- 6. *Click **Create self-signed certificate**.*
 - ↳ The certificate will be created and installed.

Table 12: 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. <i>You can enter a maximum of 64 characters.</i>

Parameters	Description
Email address	Specifies an email address. <i>You can enter a maximum of 40 characters.</i> <i>(Optional entry)</i>
Organization name	Specifies the company that uses the print server. <i>You can enter a maximum of 64 characters.</i>
Organizational unit	Specifies the department or subsection of a company. <i>You can enter a maximum of 64 characters.</i> <i>(Optional entry)</i>
Location	Specifies the locality where the company is based. <i>You can enter a maximum of 64 characters.</i>
State name	Specifies the state in which the company is based. <i>You can enter a maximum of 64 characters.</i> <i>(Optional entry)</i>
Country	Specifies the country in which the company is based. Enter the two-digit country code according to ISO 3166. Examples: DE = Germany, GB = Great Britain, US = USA
SAN (multi-domain)	
Issued on	Specifies the date from which on the certificate is valid.
Expires on	Specifies the date from which on the certificate becomes invalid.
RSA key length	Defines the length of the RSA key used: <ul style="list-style-type: none">- 1024 bit (fast encryption and decryption)- 2048 bit (standard encryption and decryption)- 4096 bit (slow encryption and decryption)

12.3 How to Create a Certificate Request for a Requested Certificate

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



Important:

After the creation of a certificate request, no print server certificate can be installed until the requested certificate has been saved in the print server.

Creating a Certificate Request via the SEH Product Manager

Requirements

- ✓ A print server certificate must not be already installed in the print server. To delete a print server certificate, see: ⇒ 69.
 - ✓ A certificate request must not already be created. To delete the certificate request, see: ⇒ 69.
1. *Start the SEH Product Manager.*
 2. *Select the print server in the device list.*
The printserver homepage appears.
 3. *Select **Configuration – Certificates** in the user interface of the print server homepage.*
 4. *Select **Print server certificate**.*
 5. *Enter the required parameters, ⇒ table 12 64.*
 6. *Click **Create certificate request**.*
The creation of the certificate request is in progress.
 7. *Save the request as text file.*
 8. *Send the text file as certificate request to a certification authority.*
- When the requested certificate has been received, it must be saved in the print server; see: ⇒ 67.

12.4 How to Save a Requested Certificate in the Print Server

A certificate which is issued by a certification authority for the print server can be used in the print server.

Saving a Requested Certificate via the SEH Product Manager

Requirements

- ✓ A certificate request has been created at an earlier date; see: ⇒ 66.
 - ✓ The certificate must be in 'base64' format.
1. *Start the SEH Product Manager.*
 2. *Select the print server in the device list.*
The printserver homepage appears.
 3. *Select **Configuration – Certificates** in the user interface of the print server homepage.*
 4. *Select **Print server certificate**.*
 5. *Click **browse/ select file**.*
 6. *Specify the requested certificate.*
 7. *Click **Load Certificate**.*
 - ↳ The requested certificate is saved in the print server.

12.5 How to Save a PKCS12 Certificate in the Print Server

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

Saving a PKCS#12 certificate via SEH Product Manager

- ✓ A print server certificate must not be already installed in the print server. To delete a print server certificate, see: ⇒ 69.
 - ✓ The certificate must be in 'base64' format.
1. *Start the SEH Product Manager.*
 2. *Select the print server in the device list.*
The printserver homepage appears.
 3. *Select **Configuration – Certificates** in the user interface of the print server homepage.*
 4. *Select **Print server certificate**.*
 5. *Click **Load certificate (pkcs12 format)**.*
 6. *Click **browse/ select file**.*
 7. *Enter the certificate.*
 8. *Enter the password.*

9. Click **Load PKCS12**.

↳ The PKCS#12 certificate is saved in the print server.

12.6 How to Save CA Certificates in the Print Server

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

Up to 8 CA certificates can be saved in the print server. Thus multi-level public key infrastructures (PKIs) are supported.



Important:

If you use the authentication method 'EAP-TLS' (⇒ 672), you must install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) in the print server and specify it for the authentication method; see: ⇒ 69.

Saving CA Certificates via the SEH Product Manager

Requirements

✓ The certificate must be in 'base64' format.

1. *Start the SEH Product Manager.*
2. *Select the print server in the device list.*
The printserver homepage appears.
3. *Select **Configuration – Certificates** in the user interface of the print server homepage.*
4. *Select **CA certificates**.*
5. *Click **Durchsuchen / Datei auswählen**.*
6. *Specify the CA certificate.*
7. *Click **Load CA certificate**.*
↳ The CA certificate is saved in the print server.

12.7 How to Delete Certificates



Important:

Do not delete the certificate (CA/self-signed/PKCS#12) if only HTTPS is defined as the permitted connection type for the web access to the Printserver Homepage. If the certificate is deleted, the Printserver Homepage can no longer be reached via SSL/TLS (HTTPS). In this case, use a non-encrypted connection.

Deleting a Print Server certificate or Certificate Request via the SEH Product Manager

Requirements

- ✓ A certificate request has been created or a client certificate is installed in the print server.
- 1. *Start the SEH Product Manager.*
- 2. *Select the print server in the device list.*
The printserver homepage appears.
- 3. *Select **Configuration – Certificates** in the user interface of the print server homepage.*
- 4. *Select **Print server certificate**.*
- 5. *Click **Delete certificate**.*
 - ↳ The certificate respectively certificate request is deleted.

Deleting CA Certificates via the SEH Product Manager

Requirements

- ✓ A CA certificate is installed on the print server.
- 1. *Start the SEH Product Manager.*
- 2. *Select the print server in the device list.*
The printserver homepage appears.
- 3. *Select **Configuration – Certificates** in the user interface of the print server homepage.*
- 4. *Select **CA certificates**.*
- 5. *For the desired certificate select **Show**.*
The CA certificate is displayed.
- 6. *Click **Delete**.*
 - ↳ The certificate is deleted.

13 Network Authentication



By means of 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, they must authenticate themselves in the network. After the authentication was successful, the access to the network will be freed.

What is EAP?

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

What is RADIUS?

RADIUS (Remote Authentication Dial-In User Service) is an authentication and account management system that validates user login information and grants access to the desired resources. The print server supports various EAP authentication methods in order to authenticate itself in a protected network.

13.1 How to Configure EAP-MD5

Benefits and Purpose

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

Mode of Operation

EAP-MD5 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 must then be enabled on the print server and the user name and password need to be entered.

Enabling EAP-MD5 via the SEH Product Manager

Requirements

- ✓ The print server is defined as user (with user name and password) on a RADIUS server.
- 1. *Start the SEH Product Manager.*
- 2. *Select the print server in the device list.*
The printserver homepage appears.
- 3. *Select **Configuration - Protection** in the user interface of the print server homepage.*
- 4. *Select **Authentication**.*
- 5. *Select **EAP-MD5** 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 **Save** to confirm.*
 - ↳ The settings are saved.

13.2 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.

Mode of Operation

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.



Important:

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: ⇒ 80.

Procedure

- Create a certificate request on the print server; see: ⇒ 66.
- Create a certificate using the certificate request and the authentication server (RADIUS).
- Install the requested certificate on the print server; see: ⇒ 67.
- Install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the print server; see: ⇒ 68.
- Enable the authentication method 'EAP-TLS' on the print server.
- 'Enabling EAP-TLS via the SEH Product Manager' ⇒ 72

Enabling EAP-TLS via the SEH Product Manager

1. *Start the SEH Product Manager.*
2. *Select the print server in the device list.
The printserver homepage appears.*
3. *Select **Configuration - Protection** in the user interface of the print server homepage.*

4. Select **Authentication**.
5. Select **EAP-TLS** from the **Authentication** list.
6. Click **Save** to confirm.
 - ↳ The settings are saved.

13.3 How to Configure EAP-TTLS

Benefits and Purpose

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

Mode of Operation

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 and MS-CHAPv2) are supported. This process is also referred to as 'inner authentication'.

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

Enabling EAP-TTLS via the SEH Product Manager

Requirements

- ✓ The print server is defined as user (with user name and password) on a RADIUS server.
- 1. *Start the SEH Product Manager.*
- 2. *Select the print server in the device list.*
The printserver homepage appears.
- 3. *Select **Configuration - Protection** in the user interface of the print server homepage.*
- 4. *Select **Authentication**.*
- 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 CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the print server; see: 'How to Save CA Certificates in the Print Server' ⇒ ¶68. While configuring the authentication, via **CA certificates – EAP authentication** select the root CA certificate.*
- 9. *Click **Save** to confirm.*
 - ↳ The settings are saved.

13.4 How to Configure PEAP

Benefits and Purpose

The 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.

Mode of Operation

In the case of PEAP, an encrypted TLS (Transport Layer Security) channel is established between the print server and the RADIUS server (as is the case for EAP-TTLS, see ⇒ ¶73). 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.

Enabling PEAP via SEH Product Manager

Requirements

- ✓ The print server is defined as user (with user name and password) on a RADIUS server.
- 1. *Start the SEH Product Manager.*
- 2. *Select the print server in the device list.
The printserver homepage appears.*
- 3. *Select **Configuration - Protection** in the user interface of the print server homepage.*
- 4. *Select **Authentication**.*
- 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 CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the print server; see: 'How to Save CA Certificates in the Print Server' ⇒ 68. While configuring the authentication, via **CA certificates – EAP authentication** select the root CA certificate.*
- 9. *Click **Save** to confirm.*
 - ↳ The settings are saved.

13.5 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.

Mode of Operation

EAP-FAST uses (as in the case of EAP-TTLS ⇒ 73) 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 authentication of the print server as well as the delivery of the PACs.

Enabling EAP-FAST via the SEH Product Manager

Requirements

- ✓ The print server is defined as user (with user name and password) on a RADIUS server.
- 1. *Start the SEH Product Manager.*
- 2. *Select the print server in the device list.
The printserver homepage appears.*
- 3. *Select **Configuration - Protection** in the user interface of the print server homepage.*
- 4. *Select **Authentication**.*
- 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 **Save** to confirm.*
 - ↳ The settings are saved.

14 Maintenance



A number of maintenance activities can be carried out on the print server. This chapter contains information on securing and resetting the parameter values. You will also learn how to carry out a restart and a device update.

14.1 How to Secure the Print Server Parameters (Backup)

All parameter values of the print server (exception: passwords) are saved in the 'parameters' file. You can save the parameters file as backup copy on your local client. This allows you to get back to a stable configuration status at any time.

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

Saving the Parameters File to the Client via the SEH Product Manager

1. Start the SEH Product Manager.
 2. Select one or more print servers in the device list.
 3. Right click to call up the context menu and select **Backup**.
 4. Select the location where the parameter file is to be saved.
 5. Click **Next**.
 6. Enter the password if a password is required and then click **Commit**.
 7. Click **Commit** directly if no password is configured.
 8. Select the compatible devices.
 9. Click **Backup** to save the parameter files.
- ↳ The parameters are saved.



If you want to change parameters, you can open the file directly in a text editor in order to edit the parameter values; see: ⇨ [78](#).

Editing the Parameters File

Using a text editor, you can edit the parameter values in the parameters file. You can open the parameters file in a text editor with the usual mechanisms of your operating system.

Requirements

- ✓ The parameters file has been saved on the client; see: ⇨ [78](#).
- ✓ A text editor is installed on the client.

**Important:**

Only change the parameter values. Other changes (layout, etc.) will render the parameters file unusable for the print server.

1. *Open the parameter file with a text editor.*
2. *Edit the parameters file. For information on the parameter values, see: 'Parameter List' ⇨ 110.*
3. *Save the parameters file.*
4. *Close the text editor.*
5. *Load the changed parameters file onto a print server.*
 - 'Load parameter file via the SEH Product Manager' ⇨ 79.

14.2 Load parameter file via the SEH Product Manager

All previous print server settings will be overwritten.

1. *Start the SEH Product Manager.*
2. *Select one or more printserver in the device list.*
3. *Right click to call up the context menu and select **Load parameters**.*
4. *Click **Choose** and select the parameter file.*
5. *Click **Next**.*
6. *Select the compatible devices.*
7. *Click **Upload** to load the parameter file.*
 - ↳ The parameter values are applied.

14.3 How to Reset Parameters to their Default Values

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



Important:

If you reset the parameters, the IP address of the print server may change and the connection to the Print Server Homepage may be terminated.

When is Resetting Recommended?

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.



By means of the button of the print server operating panel you can reset the parameters without entering the password.

Resetting Parameters via the SEH Product Manager

1. Start the SEH Product Manager.
2. Select one or more print server in the device list.
3. Right click to call up the context menu and select **Default settings**.
4. Select the compatible devices.
5. Click **Default settings**.
6. Click **OK** to confirm the security query.
 - ↳ The parameters are reset.

Resetting Parameters via an FTP Connection

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 the enter key if no password has been assigned.
3. Reset the parameters:


```
quote SITE RESET
```
4. Close the FTP connection:


```
quit
```
5. Interrupt the power supply of the print server. To do this, disconnect the power supply from the print server and then reconnect it.
 - ↳ The parameters are reset.

Resetting the Parameters via the Button

Using the button you can reset the print server's parameter values to their default setting.

1. *Press and hold the button for 5 seconds.*

↳ The parameters are reset and the print server is restarted.

14.4 How to Perform an Update

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

What Happens during an Update?

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

When is an Update recommended?

You should update your print server if some functions do not work properly and if a new software with new functions or bug fixes has been released by SEH Computertechnik GmbH .

Check the currently installed software and firmware version of your print server. The version number can be found in the device list of the *SEH Product Manager*.

Where do I Find the Update Files?

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

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



Important:

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

Update possibilities

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

- In the case of a standard update, the update file is downloaded manually from a server or a data medium and saved in the 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 update file has been stored on the specified file server. If this is the case, the update file is automatically saved in the print server via FTP.



Important:

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.

Standard Update via SEH Product Manager

Requirements

- ✓ All print jobs are finished.
 - ✓ All required update files are located in one directory.
1. Start the *Print Server Homepage*.
 2. Select the *print server in the device list*.
 3. Right click to call up the context menu and select **Load software**.
 4. Select the *software file*.

5. Click **Next**.
6. Select the compatible devices.
7. Click **Next** to load the update file.
 - ↳ The update is executed. The print server is restarting.

Standard Update via FTP

You can do a standard update on your print server via an FTP connection.

Requirements

- ✓ The print server has a suitable IP configuration, see: ⇒ 6.
 - ✓ You know the print server's current IP address; see: ⇒ 6.
 - ✓ All print jobs are finished.
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 the enter key if no password has been assigned.
 5. Switch to binary mode:
bin
 6. Send the update file to the print server:
Syntax: put <update file name> binfile
Example: put d-sys-ps-10.4.16.bin
 7. Close the FTP connection:
quit

Configure Dynamic Update via SEH Product Manager

Specify a directory on the file server for automatic (dynamic) updates. The directory contains the current update files. If the print server restarts, it checks if a new update file was put into the directory. If this is the case, the print server will be updated automatically.

Requirements

- ✓ All print jobs are finished.
 - ✓ The update files are in a directory.
 - ✓ The file server on which the update files are stored either uses the 'anonymous login' or the print server is set up as 'user' on the file server.
1. *Start the SEH Product Manager.*
 2. *Select the print server in the device list.*
The printserver homepage appears.
 3. *Select **Actions – Download Area** in the user interface of the print server homepage.*
 4. *Select **Dynamic Firmware Update**.*
 5. *Click **Dynamic Firmware Update**.*
 6. *In the **Update URL** box, specify the IP address of the file server on which the new updates files are to be stored.*
Syntax: ftp://<IP address of the file server>/
<software file name>
Example: ftp://192.168.0.100/d-sys-ps-10.4.16.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://192.168.0.100/d-sys-ps-10.4.16.bin
 7. *If you use a proxy server, tick **Use proxy** and enter the IP address of the proxy server.*
 8. *Click **Save** to confirm.*
↳ The settings are saved.

14.5 How to Restart the Print Server

If the print server is in an undefined state, the it can also be rebooted manually.

Restarting the Print Server using the SEH Product Manager

1. *Start the SEH Product Manager*
2. *Select on or more print server in the device list.*
3. *Right click to call up the context menu and select **Restart**.*
4. *Select the compatible devices.*
5. *Select **Restart**.*
 - ↳ The print server is restarting.

15 Additional Feature – ThinPrint®



Print servers are equipped with a ThinPrint feature. This chapter describes how to use the print server in a ThinPrint environment.

What is ThinPrint®?

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

Mode of Operation

Print jobs are compressed using the server component **ThinPrint Engine**. The server sends the compressed print data to a device on which a **ThinPrint Client** is implemented, e.g. the print server. The ThinPrint client then decompresses the print data and transfers it to any printer.



Important:

The settings described here refer to the client-side (print server). Information about the installation, configuration and administration of the ThinPrint environment can be found in the ThinPrint documentation at <http://www.thinprint.com>. How to Address the Print Server in a Thin-Print Environment?

Use the following syntax 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
```

15.1 How to Define the ThinPrint Port

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

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

Configuring the ThinPrint Port via SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – ThinPrint®** in the user interface of the print server homepage.
4. Into the **ThinPrint® port** box, enter the port number.
5. Click **Save** to confirm.
↳ The setting will be saved.

15.2 How to Define 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).



Important:

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.

Configuring the Bandwidth via SEH Product Manager

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – ThinPrint®** in the user interface of the print server homepage.
4. Tick **Bandwidth**.
5. Enter the desired bandwidth (bit/s).
6. Click **Save** to confirm.
↳ The setting will be saved.

15.3 How to Use ThinPrint AutoConnect

ThinPrint AutoConnect is a tool within the ThinPrint technology for the automatic creation of print objects. The printer 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 ThinPrint client.

Configuring AutoConnect via SEH Product Manager


1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – ThinPrint®** in the user interface of the print server homepage.
4. Configure the AutoConnect parameters; ⇒ table 13  88.
5. Click **Save** to confirm.
↳ The setting will be saved.

Table 13: ThinPrint AutoConnect parameters

Parameters	Description
ID	The ID clearly identifies the printers for the ThinPrint server.
printer	Defines the printer name. The printer name is purely a description and is used to distinguish the printers.
Class	Printers with compatible drivers can be arranged in one class.
Driver	Specifies the printer driver for the embedded printer.

15.4 How Does the Print Server Receive Encrypted 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/TLS 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 an encryption was enabled on the ThinPrint server, you must install a certificate from a corresponding Certification Authority (CA) 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: ⇒ [66](#).
- Save the requested certificate; see: ⇒ [67](#).

16 Additional Feature – Internet Protocol Security (IPsec)



To defend against threats against 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 14: Components of an IPsec policy

Component	Description
Filter list	<p>A filter list contains one or several filters.</p> <p>A filter is the description of</p> <ul style="list-style-type: none"> - IP traffic (IP address / IP address range) and - protocols and services that are used.

Component	Description
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: <ul style="list-style-type: none"> - Allow IP data packet, - Block IP data packet, - 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 (⇒ table 18 101)
- 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 together with the 'Internet Security Association and Key Management Protocol' (ISAKMP).

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.

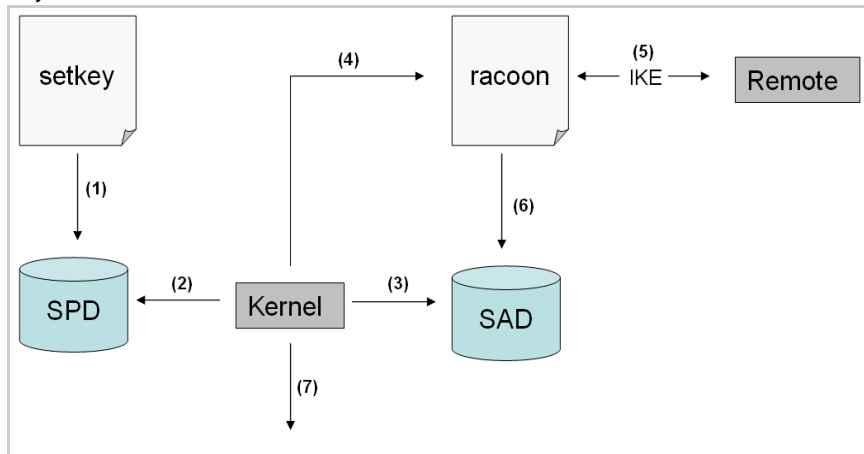


Fig. 5: IPsec procedure

- (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 method 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 two 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 Printserver Homepage you can import IPsec policies as ready-made configuration files (racoon/setkey) to the print server.



Important:

Only one IPsec policy can be active at a time



WARNING

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

IP sec Area only accessible via SSL

The access to the IPsec area on the Printserver Homepage is protected via a secure SSL connection. URLs that require an SSL/TLS connection start with 'https'. During a so-called 'handshake', the client asks for a certificate via a browser.

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 using a browser in order to make the certificate known to the client. For more information, refer to the documentation of your browser and operating system.

16.1 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 packet)
- Drop all (block IP data packet)
- Use IPsec (forward IP data packet 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.

Exclusivity of 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 from top to bottom.
- 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

Target:

- 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.

Implementation concept:

Rule	Active	Address 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	---

Rule	Active	Address filter	Service filter	Action	SA (Security Association)
Standard rule		Remote IP address	All services	Allow all	---

Example 2

Target:

- 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.

Implementation concept:

- 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	Address 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	---
Standard rule		Remote IP address	All services	Drop all	---

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.

1. Start the Print Server Homepage.
2. Start the SEH Product Manager.
3. Select the print server in the device list.
The printserver homepage appears.
4. Select **Configuration – IPsec** in the user interface of the print server homepage.
5. Select **Edit rules**.
6. Define the filters.
To do this, select the templates to be used in the 'Address filter' and 'Service filter' lists.
7. Select the filter action to be used in the 'Action' list.
8. If you have chosen the 'Require IPsec' filter action, you must also select the 'Security Association (SA)' to be used.
9. 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.



Important:

Afterwards you must enable the entire IPsec policy for the rules to take effect; see: ⇨ 106.

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 are 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.



Important:

Please use static IP addresses only.

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – IPsec** in the user interface of the print server homepage.
4. Select **Edit rules**.
5. Select **Edit address templates**.
6. Define the address template; ⇒ table 15 98.
7. Click **Save** to confirm.
↳ The settings are saved.

Table 15: Address Template Parameters

Parameters	Description
Name	Name of the address template <i>You can enter a maximum of 18 characters.</i>
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 <i>The notation of address ranges is done using the CIDR methodology.</i>
Local (IPv6)	Specifies local IPv6 addresses or IPv6 address ranges. Formats/Convention/Example: All IPv6 addresses = ::/0 IPv6 address = 0:0:0:0:FFFF:a.b.c.d IPv6 address range = 0:0:0:0:FFFF:a.b.c.d/96 <i>The notation of address ranges is done using the CIDR methodology.</i>
Remote (IPv6)	Specifies remote IPv6 addresses or IPv6 address ranges. Formats/Convention/Example: All IPv6 addresses = ::/0 IPv6 address = 0:0:0:0:FFFF:a.b.c.d IPv6 address range = 0:0:0:0:FFFF:a.b.c.d/96 <i>The notation of address ranges is done using the CIDR methodology.</i>

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' comprises all protocols and is implemented by default. You can specify another 3 templates, if required.


1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – IPsec** in the user interface of the print server homepage.
4. Select **Edit rules**.
5. Select **Edit service templates**.
6. Define the service template; ⇒ table 16  99.
7. Click **Save** to confirm.
↳ The settings are saved.

Table 16: Service Template Parameters

Parameters	Description
Name	Name of the service template <i>You can enter a maximum of 16 characters.</i>
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 specify up to 4 templates, if required.

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – IPsec** in the user interface of the print server homepage.
4. Select **Edit rules**.
5. Select **Edit SA templates**.
6. Define the SA template; ⇒ table 17 100.
7. Click **Save** to confirm.
↳ The settings are saved.

Table 17: SA Template Parameters

Parameters	Description
Name	Name of the IPsec template <i>You can enter a maximum of 16 characters.</i>
Authentication type	Specifies the procedure for the authentication of the remote server. Two procedures are available: - authentication via pre-shared key - authentication via certificates <i>For the installation of certificates on print servers; see: ⇒ 62.</i>
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'. <i>You can enter a maximum of 16 characters.</i>
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.

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The *printserver homepage* appears.
3. Select **Configuration – IPsec** in the user interface of the print server homepage.
4. Select **Edit rules**.
5. Select **Edit SA templates**.
6. Select **Edit IKE templates**.
7. Define the IKE template; ⇒ table 18 101.
8. Click **Save** to confirm.
↳ The settings are saved.

Table 18: IKE Template Parameters

Parameters	Description
Name	Name of the IKE template <i>You can enter a maximum of 16 characters.</i>
- Phase 1 - <i>IKE Phase 1 establishes a secure channel.</i>	
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.
Cipher algorithm	Specifies the encryption algorithm to be used during the negotiation.

Parameters	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) <i>min. 600 s / max. 4294967295 s</i>
- Phase 2 -	
<i>IKE phase 2 negotiates the encryption and integrity parameters used to secure the data packet to be transferred.</i>	
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)
Cipher 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. <i>AH uses the authentication header to authenticate the packet. In the IP data packet, the authentication header will be added after the IP header.</i>
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. <i>min. 600 s / max. 4294967295 s</i>

16.2 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 rrasig;
        dh_group modp1024;
    }
}
```



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.

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – IPsec** in the user interface of the print server homepage.
4. Select **Load files**.
5. Click **Browse / Choose File**.
6. Select the configuration file.
7. Click **Load**.
8. 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 (⇒table 17 ¶100) the pre-shared key must be saved in the print server.

1. *Start the SEH Product Manager.*
2. *Select the print server in the device list.*
The printserver homepage appears.
3. *Select **Configuration – IPsec** in the user interface of the print server homepage.*
4. *Select **Load files**.*
5. *Next to 'Preshared keys file' click **Browse / Choose File**.*
6. *Select the file.*
7. *Click **Load**.*
8. *Click **Save** to confirm.*
↳ The pre-shared key is loaded.

Importing Certificates

If an authentication via certificates is used for an SA (⇒table 17 ¶100), you must save certificates in the print server. To save certificates; see: ⇒ ¶67.

16.3 How to Define Exceptions

Network activities based on the protocols SLP, DHCP, Bonjour, 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.

1. *Start the SEH Product Manager.*
2. *Select the print server in the device list.*
The printserver homepage appears.
3. *Select **Configuration – IPsec** in the user interface of the print server homepage.*
4. *Select **Edit rules**.*
5. *Enable the relevant protocols under 'IPsec exceptions'!*
6. *Click **Save** to confirm.*
↳ The settings are saved.



Important:

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

16.4 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.



WARNING

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

1. Start the SEH Product Manager.
2. Select the print server in the device list.
The printserver homepage appears.
3. Select **Configuration – IPsec** in the user interface of the print server homepage.
4. Specify the IPsec policy to be used.
5. **Use configured rules**
(use policy from the manually configured rules)
6. **Use configuration files**
(use policy of the loaded configuration files)
7. Make sure that the **Test mode** is enabled.
8. Tick **IPsec**.
9. Click **Save** to confirm.
The setting will be saved. IPsec is enabled until the next hard reboot.
10. Check the access to the device.



Important:

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

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

17 Appendix



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

17.1 Glossary

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

Manufacturer-Specific Software Solutions

- 'SEH Product Manager' ⇒ 108

Network Technology

- 'Default Name' ⇒ 107
- 'Gateway' ⇒ 108
- 'Hardware Address' ⇒ 108
- 'Host Name' ⇒ 108
- 'IP Address' ⇒ 109
- 'MAC Address' ⇒ 109
- 'Subnet Mask' ⇒ 109
- 'Print server name' ⇒ 109
- 'TCP/IP Port' ⇒ 110

Default Name

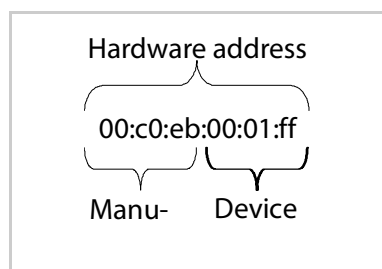
See: 'Print server name' ⇒ 109.

Gateway

Using a gateway, you can address IP addresses from other networks. If you wish to use a gateway, you can configure the relevant parameter via the Print Server Homepage or the SEH Product Manager.

Hardware Address

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



The hardware address is found on the housing of the print server, on the Print Server Homepage, in the SEH Product Manager, or on the status page.

The use of separators within the hardware address depends on the platform. In Windows / Mac are used.

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.

SEH Product Manager

The software ISEH Product Manager has been developed by SEH Computertechnik GmbH for the administration of SEH network devices within a predefined network.

IP Address

The IP address is a unique address for every node in your network, i.e., an IP address may appear only once in your local network. The address must be saved in the print server to make sure that it can be addressed within the network.

MAC Address

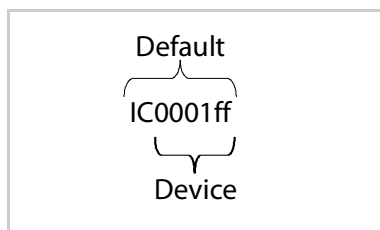
See: 'Hardware Address' ⇒ 108.

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 gateway, you can configure the relevant parameter via the Print Server Homepage or the SEH Product Manager.

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.



The default name can be found on the Printserver Homepage or in the SEH Product Manager.

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 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 Parameter List

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

- 'Parameter List - IPv4' ⇒ 111
- 'Parameter List - IPv6' ⇒ 113
- 'Parameter List - Network Speed' ⇒ 114
- 'Parameter List - HTTP' ⇒ 114
- 'Parameter List - HTTP' ⇒ 114
- 'Parameter List - DNS' ⇒ 115
- 'Parameter List - Bonjour' ⇒ 115
- 'Parameter List - POP3' ⇒ 115
- 'Parameter List - SMTP' ⇒ 117
- 'Parameter List - Device Settings' ⇒ 118
- 'Parameter List - Device Time' ⇒ 118
- 'Parameter List - Print Server Status Information' ⇒ 119
- 'Parameter List - Print jobs and data' ⇒ 119
- 'Parameter List - Port Settings' ⇒ 119
- 'Parameter List - Logical Printers' ⇒ 120

- 'Parameter List - Printer Notifications' ⇒ 122
- 'Parameter List - Security' ⇒ 126
- 'Parameter List - Network Authentication' ⇒ 126
- 'Parameter List - IPsec' ⇒ 128
- 'Parameter List - Dynamic Update' ⇒ 141
- 'Parameter List - ThinPrint®' ⇒ 142

To view the current parameter values of your print server, see: ⇒ 78.

Table 19: Parameter List - IPv4

Parameters	Value	Default	Description
ip_addr [IP address]	valid IP address	169.254. 0.0/16	Defines the IP address of the print server.
ip_mask [Subnet mask]	valid IP address	255.255. 0.0	Defines the subnet mask of the print server.
ip_gate [Gateway]	valid IP address	0.0.0.0	Defines the gateway address of the print server.
ip_dhcp [DHCP]	on/off	on	Enables/disables the DHCP protocol.
ip_bootp [BOOTP]	on/off	on	Enables/disables the BOOTP protocol.
ip_zconf [ZeroConf]	on/off	on	Enables/disables the ZeroConf (Zero Configuration Networking) protocol.

Parameters	Value	Default	Description
ip_set_by [IP address]	0–12 [1–2 characters; 0–9] <i>0 = Unknown</i> <i>1 = SNMP (Net-Tool)</i> <i>2 = BOOTP</i> <i>3 = DHCP</i> <i>4 = PING</i> <i>5 = not defined</i> <i>6 = ZeroConf</i> <i>7 = Parameters file</i> <i>8 = not defined</i> <i>9 = not defined</i> <i>10 = not defined</i> <i>11 = not defined</i> <i>12 = HTTP website</i>		Shows the method used for the IP address assignment.
ip_auto_gate [Multicast router as gateway]	on/off	on	Enables/disables the automatic entry of a found multicast router as gateway address. <i>If disabled, the gateway address has to be entered manually.</i>
sys_name [Host name]	max. 64 characters [a–z, A–Z, 0–9]	[Default name]	Defines the host name of the print server.
sys_contact [Contact person]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Freely definable description of the contact person.
sys_location [Location]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Freely definable description of the device location.

Table 20: Parameter List - IPv6

Parameters	Value	Default	Description
ipv6 [IPv6]	on/off	on	Enables/disables the IPv6 functionality of the print server.
ipv6_addr [IPv6 address]	n:n:n:n:n:n:n	::	Defines a print server IPv6 unicast address assigned manually in the format n:n:n:n:n:n:n. <i>Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.</i>
ipv6_gate [Router]	n:n:n:n:n:n:n	::	Defines the IPv6 unicast address of the router. The print server sends its 'Router Solicitations' (RS) to this router.
ipv6_plen [Prefix length]	0-64 [1-2 characters; 0-9]	64	Defines the length of the subnet prefix for the IPv6 address. <i>Address ranges are indicated by prefixes. The prefix length (number of bits used) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/.'</i>
ipv6_auto [Automatic configuration]	on/off	on	Enables/disables the automatic assignment of the IPv6 address for the print server.

Table 21: Parameter List - Network Speed

Parameters	Value	Default	Description
eth_conf [Ethernet settings]	0-5 [1 characters; 0-5] 0 = automatic 1 = 10BaseT/FL half-duplex 2 = 10BaseT/FL full-duplex 3 = H100BaseFX/ TX half- duplex 4 = 100BaseFX/T X full duplex 5 = 1000Ba- seT/SX	0	Defines the network speed of the print server. <i>'Auto' means that the network speed is recognized automatically. If the speed is set manually, it must be match that of the other network devices.</i>

Table 22: Parameter List - HTTP

Parameters	Value	Default	Description
http [HTTP]	on/off	on	Enables/disables the HTTP protocol on the print server. Note: If the HTTP protocol is disabled, functions that are based on the protocol will not be available (e.g. the Print Server Homepage cannot be started).

Table 23: Parameter List - DNS

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

Table 24: Parameter List - Bonjour

Parameters	Value	Default	Description
bonjour [Bonjour]	on/off	on	Enables/disables the Bonjour service.
pp*_rdzv_name [Bonjour name]	max. 63 characters [a-z, A-Z, 0-9]	[blank]	Defines the Bonjour name of the print server.

Table 25: Parameter List - POP3

Parameters	Value	Default	Description
nf_pop3 [POP3]	on/off	off	Enables/disables the POP3 functionality.

Parameters	Value	Default	Description
nf_pop3_srv [Server name]	max. 255 characters	[blank]	Defines the POP3 server via the IP address or the host name. <i>The host name can only be used if a DNS server was configured beforehand.</i>
nf_pop3_port [Server port]	1–65535 [1–5 characters; 0–9]	110	Defines the port of the POP3 server used by the print server for receiving emails. <i>When using SSL/TLS, enter 995 as port number.</i>
nf_pop3_user [User name]	max. 255 characters	[Default name]	Defines the name used by the print server to log on to the POP3 server.
nf_pop3_pwd [Password]	max. 255 characters	[blank]	Defines the password used by the print server to log on to the POP3 server.
nf_pop3_secure [Security]	0–2 [1 characters; 0–2] <i>0 = off (no security)</i> <i>1 = APOP</i> <i>2 = SSL/TLS</i>	0	Defines an authentication method.
nf_pop3_poll [Check mail every]	0–9999 [1–4 characters; 0–9]	1	Defines the time interval (in minutes) for retrieving emails from the POP3 server.
nf_pop3_limit [Ignore mail exceeding]	0–9999 [1–4 characters; 0–9] <i>0 = unlimited</i>	0	Defines the maximum email size (in Kbyte) to be accepted by the print server.
nf_pop3_mdel [Delete read messages]	on/off	on	Enables/disables the automatic deletion of read emails on the POP3 server.

Table 26: Parameter List - SMTP

Parameters	Value	Default	Description
nf_smtp_srv [Server name]	max. 255 characters	[blank]	Defines the SMTP server via the IP address or the host name. <i>The host name can only be used if a DNS server was configured beforehand.</i>
nf_smtp_port [Server port]	1–65535 [1–5 characters; 0–9]	25	Defines the port number used by the print server to send emails to the SMTP server.
nf_smtp_user [User name]	max. 255 characters	[blank]	Defines the user name used by the print server to log on to the SMTP server.
nf_smtp_pwd [Password]	max. 255 characters	[blank]	Defines the password used by the print server to log on to the SMTP server.
nf_smtp_ssl [TLS]	on/off	off	Enables/disables TLS. <i>The TLS protocol serves to encrypt the transmission between the print server and the SMTP server.</i>
nf_smtp_sndr [Sender name]	max. 255 characters	[Default name]	Defines the email address used by the print server to send emails. Note: Very often the name of the sender and the user name are identical.
nf_smtp_sign [Signature]	max. 128 characters	[Default-Name\r\nSerial:<serial number>\r\nIpAddress: <[IP address>]	Defines the signature to be contained in an email generated by the print server.
nf_smt-p_asp3 [Use POP3 settings]	on/off	off	Takes over the parameters 'User name' and 'Password' from the POP3 settings to log on to the SMTP server.

Table 27: Parameter List - Device Settings

Parameters	Value	Default	Description
language [Print server language]	en, de, fr, es, it, pt, jp, cn, zh, kr	en	Defines the language of the print server. <i>en= English</i> <i>de= German</i> <i>fr= French</i> <i>es= Spanish</i> <i>it= Italian</i> <i>pt= Portuguese</i> <i>jp= Japanese</i> <i>cn= Chinese, simplified</i> <i>zh= Chinese, traditional</i> <i>kr= Korean</i>
sys_descr [Description]	max. 128 characters [a-z, A-Z, 0-9]	[blank]	Freely definable description of the contact person.
info_txt [Dealer]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Freely definable name of a dealer or supplier.
info_url [Dealer URL]	max. 64 characters [a-z, A-Z, 0-9, _ , - , .]	[blank]	Freely definable URL of a dealer or supplier.

Table 28: Parameter List - Device Time

Parameters	Value	Default	Description
sntp [SNTP]	on/off	on	Enables/disables the use of a time server (SNTP).
sntp_server [Time server]	max. 255 characters [a-z, A-Z, 0-9, _ , - , .]	[blank]	Defines a time server via the IP address or the domain name. <i>The host name can only be used if a DNS server was configured beforehand.</i>

Parameters	Value	Default	Description
time_zone [Time zone]	UTC, GMT, EST, EDT, CST,CDT, MST, MDT, PST, PDT, etc.	WET/WES T (EU)	The time zone is used to equalize the difference between the time received over the time server and the local time.

Table 29: Parameter List - Print Server Status Information

Parameters	Value	Default	Description
sp_mode [Status page mode]	Auto ASCII PostScript DATAMAX Citizen-Z	Auto	Defines the data format in which the status page is printed. <i>The data formats ASCII, PostScript, DATAMAX (label printer), and Citizen-Z (label printer) are available.</i> <i>The preset 'Auto' mode automatically uses the appropriate data format.</i>

Table 30: Parameter List - Print jobs and data

Parameters	Value	Default	Description
job_rcvmtout [Job receive timeout]	1-9999 [4 characters, 0-9] <i>0 = no timeout</i>	0	Defines the time (seconds) after which the connection to the spooler is closed if no print job is sent to the print server. <i>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'.</i>

Table 31: Parameter List - Port Settings

Parameters	Value	Default	Description
pp*_1284_4 [1284.4 / MLC]	on/off	off	Enables/disables the 1284.4/MLC protocol. <i>You can use 1284.4/MLC to obtain enhanced printer status information.</i>

Parameters	Value	Default	Description
pp*_pjl [PJL]	on/off	off	Enables/disables the PJL (Print Job Language) compatibility. <i>Printers supporting PJL forward enhanced printer information to the print server, if the parameter is enabled.</i>
pp*_ecp [ECP mode]	on/off	off	Enables/disables the ECP mode. <i>The ECP mode (Enhanced Capabilities Port) can be used for quick and compressed data transfer.</i>
pp*_port_ mode [Port mode]	0–2 [1 characters; 0–2] <i>0= unidirectional</i> <i>1= bidirectional</i>	0	Specifies the communication mode between the print server and the printer.

Table 32: Parameter List - Logical Printers

Parameters	Value	Default	Description
lp1_tcp_port ~	0–9999 [1–4 characters; 0–9]	9100 9101	Defines the TCP/IP port of the logical printer.
lp8_tcp_port [TCP/IP port]		~ 9108	
lp1_mode ~ lp8_mode [Banner page mode]	ASCII PostScript	ASCII	Defines the format in which the banner page is printed.
lp1_job_start ~ lp8_job_start [Job start]	max. 256 characters	[blank]	Defines a start sequence. <i>Depending on the application, you might have to configure the logical printer. For further information; see: ⇒ 51.</i>

Parameters	Value	Default	Description
lp1_job_end ~ lp8_job_end [Job end]	max. 256 characters	[blank]	Defines an end sequence. <i>Depending on the application, you might have to configure the logical printer. For further information; see: ⇒ 51.</i>
lp1_search ~ lp8_search [Search]	max. 256 characters [no wildcard or truncations]	[blank]	Defines a string which is searched for in the data sent to the print server. <i>Using 'Find' and 'Replace,' you can look for strings in the data sent to the print server and replace them with new strings.</i>
lp1_replace ~ lp8_replace [Replace]	max. 256 characters [no wildcard or truncations]	[blank]	Defines the string which is replaced in the data sent to the print server. <i>Using 'Find' and 'Replace,' you can look for strings in the data sent to the print server and replace them with new strings.</i>
lp1_crlf ~ lp8_crlf [CR + LF]	on/off	off	Enables/disables the conversion from line feed (LF) to carriage return with line feed (LF+CR).
lp1_banner ~ lp8_banner [Banner page]	on/off	off	Enables/disables the printing of a banner page if the LPD protocol is used.
lp1_ascii_ps ~ lp8_ascii_ps [ASCII/Post-Script]	on/off	off	Enables/disables the conversion of ASCII into PostScript data.

Parameters	Value	Default	Description
lp1_hexdump ~ lp8_hexdump [Hex dump mode]	on/off	off	Enables/disables the hex dump mode. <i>The hex dump mode is used to search for errors in print data.</i>
lp1_binary_ps ~ lp8_binary_ps [Binary PostScript]	on/off	off	Enables/disables the printing of binary PostScript files. <i>Enable this option if binary PostScript files are to be printed in heterogeneous networks.</i>

Table 33: Parameter List - Printer Notifications

Parameters	Value	Default	Description
nf_mail_pr1 nf_mail_pr2 [Email active]	on/off	off	Enables/disables the email notification for recipient 1 or 2.
nf_mail_addr1 nf_mail_addr2 [Email recipient]	valid email address	[blank]	Defines the email address of the recipient for notifications.
nf_mAccHist1 nf_mAccHist2 [Job History]	on/off	off	Enables/disables the sending of emails containing information on how many prints jobs were handled by the print server to recipient 1 or 2.

Parameters	Value	Default	Description
nf_mAccHist- Time1 nf_mAccHist- Time2 [time interval]	0–9999 [1–4 characters; 0–9]	0	Defines the time interval (in hours) with which an email containing information on how many prints jobs were handled by the print server (job history) is sent.
nf_mAc- cHistCnt1 nf_mAc- cHistCnt2 [Jobs]	1–60 [1–2 characters; 0–9]	60	Defines the number of print jobs after which an email containing information on how many prints jobs were handled by the print server (job history) is sent to recipient 1 or 2.
nf*_mAc- cPCnt1 nf*_mAc- cPCnt2 [Page counter]	on/off	off	Enables/disables the sending of emails containing the number of pages printed by the print server to recipient 1 or 2.
nf*_mAc- cPCntTime1 nf*_mAc- cPCntTime2 [time interval]	0–9999 [1–4 characters; 0–9]	0	Defines the time interval (in hours) with which an email containing information on how many pages were printed by the printer (page counter) is sent to recipient 1 or 2.
nf*_mAc- cPCntCnt1 nf*_mAc- cPCntCnt2 [page inter- val]	0–9999 [1–4 characters; 0–9]	0	Defines the number of pages after which an email containing information on how many pages were printed by the printer (page counter) is sent to recipient 1 or 2.

Parameters	Value	Default	Description
nf*_mail_mas k1	0 = none 1 = paper jam	0	<p>Defines the printer errors of which recipient 1 or 2 is informed by email.</p> <p><i>The email contains information about the printer error. Each code represents a message. By defining more than one code, several printer errors can be indicated at once.</i></p> <p>Note: Not all print server models support all printer error messages.</p>
nf*_mail_mas k2	2 = Paper empty		
[Printer error]	4 = toner low		
	8 = printer open		
	16 = toner empty		
	32 = cassette not ready		
	64 = warming up		
	128 = offline		
	256 = engine error		
	512 = no select		
	1024 = paper low		
	16384 = call customer service		
	32768 = miscellaneous error		
nf_trap_ip1 nf_trap_ip2 [IP address]	valid IP address	[blank]	Defines the SNMP trap address of the recipient.
nf_trap_com 1 nf_trap_com 2 [Trap community]	max. 15 characters [a-z, A-Z, 0-9]	[blank]	Defines the SNMP trap community of the recipient.

Parameters	Value	Default	Description
nf_trap_aut1 nf_trap_aut2 [Authentication traps]	on/off	off	Enables/disables the sending of traps containing authentication information.
nf_trap_pr1 nf_trap_pr2 [Printer traps]	on/off	off	Enables/disables the sending of traps for selected printer errors (⇒ 125) for recipient 1 or 2.
nf*_trap_mas k1 nf*_trap_mas k2 [Printer error]	0 = none 1 = paper jam 2 = Paper empty 4 = toner low 8 = printer open 16 = toner empty 32 = cassette not ready 64 = warming up 28 = offline 256 = engine error 512 = no select 124 = paper low 16384 = call customer service 32768 = miscellaneous error	0	<p>Defines the printer errors of which recipient 1 or 2 is informed by a trap.</p> <p><i>A trap contains information about the printer error. Each code represents a message. By defining more than one code, several printer errors can be indicated at once.</i></p> <p>Note: Not all print server models support all printer error messages.</p>

Table 34: Parameter List - Security

Parameters	Value	Default	Description
passwd [Password]	max. 16 characters [a-z, A-Z, 0-9]	[blank]	Defines the password that is needed to authorize print server parameter changes.
access_control [Access control]	on/off	off	Enables/disables the password demand for seeing print server parameters. <i>This parameter only makes sense if a password was set at an earlier stage; see above.</i>
ip1_sender ~ ip8_sender [IP sender]	max. 255 characters [The use of wild-cards (*) is possible to authorize sub-networks, for example.]	[blank]	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.

Table 35: Parameter List - Network Authentication

Parameters	Value	Default	Description
eap_auth_type [Authentication]	1-7 [1 characters; 1-7] <i>1 = not defined</i> <i>2 = not defined</i> <i>3 = EAP-MD5</i> <i>4 = EAP-TLS</i> <i>5 = EAP-TTLS</i> <i>6 = EAP-PEAP</i> <i>7 = EAP-FAST</i>	1	Defines the authentication method that is used to identify devices or users in the network.

Parameters	Value	Default	Description
eap_auth_name [User name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the name of the print server as saved in the authentication server (RADIUS).
eap_auth_pwd [Password]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the password of the print server as saved in the authentication server (RADIUS).
eap_auth_external [EAP- (PEAP/FAST) options]	0-5 [1 characters; 0-5] <i>0 = none</i> <i>1 = PEAP LABEL 0</i> <i>2 = PEAP LABEL 1</i> <i>3 = PEAP VER 0</i> <i>4 = PEAP VER 1</i> <i>5 = FAST INLINE PROVISIONING</i>	0	Defines the kind of external authentication for the EAP authentication methods TTLS, PEAP, and FAST.
eap_auth_inner [Inner Authenticat- ion]	0-8 [1 characters; 0-8] <i>0 = none</i> <i>1 = MS-CHAP</i> <i>2 = MS-CHAPv2</i> <i>3 = PAP</i> <i>4 = CHAP</i> <i>5 = EAP-MD5</i> <i>6 = EAP-MS-CHAP</i> <i>7 = EAP-MS- CHAPv2</i> <i>8 = EAP-TLS</i>	0	Defines the kind of inner authentication for the EAP authentication methods TTLS, PEAP, and FAST.

Parameters	Value	Default	Description
eap_auth_anonymous_name [Anonymous name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the anonymous name for the unencrypted part of the EAP authentication methods TTLS, PEAP, and FAST.

Table 36: Parameter List - IPsec

Parameters	Value	Default	Description
ipsec [IPsec]	on/off	off	Enables/disables the use of IPsec.
ipsec_test-mode [Test mode]	on/off	on	Enables/disables the IPsec test mode. <i>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.</i>
ipsec_config	0-1 [1 characters; 0-1] <i>0=Use manually configured rules</i> <i>1=Use configuration files</i>	1	Specifies the way in which IPsec policies are added to the print server.
ipsec_bonjour [Bonjour]	on/off <i>on = activity is always allowed</i> <i>off = activity is filtered via IPsec</i>	off	Enables/disables the filtering of Bonjour network activities by the IPsec policy.

Parameters	Value	Default	Description
ipsec_dhcp [DHCP]	on/off <i>on = activity is always allowed</i> <i>off = activity is fil- tered via IPsec</i>	off	Enables/disables the filtering of DHCP network activities by the IPsec policy.
ipsec_slp [FTP]	on/off <i>on = activity is always allowed</i> <i>off = activity is fil- tered via IPsec</i>	off	Enables/disables the filtering of FTP network activities by the IPsec policy. <u>Note:</u> If all FTP network activities are allowed (FTP = on), you must specify the 'Allow all' action in the default rule.
ipsec_netbios [NetBIOS]	on/off <i>on = activity is always allowed</i> <i>off = activity is fil- tered via IPsec</i>	off	Enables/disables the filtering of NetBIOS network activities by the IPsec policy.
ipsec_slp [SLP]	on/off <i>on = activity is always allowed</i> <i>off = activity is fil- tered via IPsec</i>	off	Enables/disables the filtering of SLP network activities by the IPsec policy.
ipsec_rule1_e nabled ~ ipsec_rule4_e nabled [Rule 1–4]	on/off	off	Enables/disables the IPsec rules.

Parameters	Value	Default	Description
ipsec_rule1_i addr_tmpl ~	0–8 [1 character; 0–8] 0=---	0	Specifies the filter within an IPsec rule for the IP traffic via an address template. <i>See parameter 'iaddr_tmpl1_name' ⇒ 131.</i>
ipsec_rule4_i addr_tmpl [Address filter]	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		
ipsec_rule1_i serv_tmpl ~	0–4 [1 character; 0–4] 0=---	0	Specifies the filter within an IPsec rule for protocols and services via a service template. <i>See parameter 'iserv_tmpl1_name' ⇒ 132.</i>
ipsec_rule4_i serv_tmpl [Service filter]	1=Service template 1 2=Service template 2 3=Service template 3 4=Service template 4		

Parameters	Value	Default	Description
ipsec_rule1_action ~ ipsec_rule4_action [Action]	0–2 [1 character; 0–2] <i>0 = Allow all</i> <i>1 = Drop all</i> <i>2 = IPsec require</i>	2	As specified within the IPsec rule, this is the action to be carried out if a data packet matches the description of a filter.
ipsec_rule1_ipsec_tmpl ~ ipsec_rule4_ipsec_tmpl [Security association (SA)]	0–4 [1 character; 0–4] <i>0 = ---</i> <i>1 = SA template 1</i> <i>2 = SA template 2</i> <i>3 = SA template 3</i> <i>4 = SA template 4</i>	0	Specifies the parameters of the 'Security Association' via an SA template. <i>See parameter 'ipsec_tmpl1_name' ⇒ 133.</i>
ipsec_def_action [Action of the default rule]	0–1 [1 character; 0–1] <i>0 = Allow all</i> <i>1 = Drop all</i>	0	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.
iaddr_tmpl1_name ~ iaddr_tmpl8_name [Name]	max. 18 characters [a–z, A–Z, 0–9, _ , -] <i>iaddr_tmpl1_name</i> <i>=</i> <i>all IP addresses</i> <i>iaddr_tmpl2_name</i> <i>=</i> <i>all IPv4 addresses</i> <i>iaddr_tmpl3_name</i> <i>=</i> <i>all IPv6 addresses</i>	iaddr_tmpl1_name iaddr_tmpl2_name iaddr_tmpl3_name	Name of the address template The template is used for filtering the IP traffic. <i>Local and remote IP addresses can be defined in the address template. Addresses in the format IPv4 and IPv6 are supported.</i>

Parameters	Value	Default	Description
iaddr_tmpl1_ip_remote ~ iaddr_tmpl8_ip_remote [Remote (IPv4)]	0.0.0.0/0 valid IPv4 address valid IPv4 address range <i>0.0.0.0/0 = all IPv4 addresses</i>	0.0.0.0/0	Specifies a remote IPv4 address or an IPv4 address range for an address template. <i>The notation of address ranges is done via the CIDR methodology (e.g. 192.168.0.1/24).</i>
iaddr_tmpl1_ip6_local ~ iaddr_tmpl8_ip6_local [Local (IPv6)]	::/0 valid IPv6 address valid IPv6 address range <i>::/0 = all IPv6 addresses</i>	::/0	Specifies a local IPv6 address or an IPv6 address range for an address template. <i>The notation of address ranges is done via the CIDR methodology (e.g. 192.168.0.1/24).</i>
iaddr_tmpl1_ip6_remote ~ iaddr_tmpl8_ip6_remote [Remote (IPv6)]	::/0 IPv6 address IPv6 address range <i>::/0 = all IPv6 addresses</i>	::/0	Specifies a remote IPv6 address or an IPv6 address range for an address template. <i>The notation of address ranges is done via the CIDR methodology (e.g. 192.168.0.1/24).</i>
iserv_tmpl1_name ~ iserv_tmpl4_name [Name]	max. 16 characters [a-z, A-Z, 0-9, _, -]	iserv_tmpl1_name = all services	Name of the service template. <i>The template is used for filtering the IP traffic by services and protocols.</i>

Parameters	Value	Default	Description
ipsec_tmpl1_name ~ ipsec_tmpl4_name [Name]	max. 16 characters [a-z, A-Z, 0-9, _ , -]		Name of the SA template. <i>The template specifies the parameters of a 'Security Association'.</i>
ipsec_tmpl1_certificate ~ ipsec_tmpl4_certificate [Authentication type]	0-1 [1 character; 0-1] <i>0 = pre-shared key</i> <i>1 = certificates</i>	1	Specifies the procedure for the authentication of the remote server.
ipsec_tmpl1_verify ~ ipsec_tmpl4_verify [Verify certificate]	on/off <i>off = self-signed certificate suffices</i> <i>on = CA root certificate is required.</i>	off	Specifies the type of certificate required for the certificate-based authentication.
ipsec_tmpl1_psk ~ ipsec_tmpl4_psk [Pre-Shared Key]	max. 16 characters		Specifies the Pre-Shared Key (PSK). <i>You need the key if the 'Pre-Shared Key' procedure has been selected as 'Authentication type'.</i>

Parameters	Value	Default	Description
ipsec_tm- pl1_key_ex- change ~ ipsec_tm- pl4_key_ex- change [IKE]	0-4 [1 character; 0-4] 0=--- 1=IKE template 'IKE Default' 2=IKE template 2 3=IKE template 3 4=IKE template 4	0	Specifies the template to be used for the IKE (automatic key exchange) within a SA. <i>See parameter 'ipsec_key_exchange1_name' ⇒ ¶134.</i> <i>The 'IKE Default' template has been implemented by default. You can specify another 5 templates, if required.</i>
ipsec_key_ex- change1_na me ~ ipsec_key_ex- change4_na me [Name]	max. 16 characters [a-z, A-Z, 0-9, _, -]	ipsec_key _ex- change1_ name = IKE Default	Name of the IKE template
ipsec_key_ex- change1_- modes ~ ipsec_key_ex- change4_- modes [Negotiation]	main aggressive	main	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). <i>(Both security methods can also be used in combination.) Only the most secure procedure will be applied. If a procedure fails, a less complicated (and therefore less secure) procedure will be used.</i>

Parameters	Value	Default	Description
ipsec_key_exchange1_dh_group ~ ipsec_key_exchange4_dh_group [Diffie-Hellman group]	1–8 [1 character; 1–8] <i>1 = modp768</i> <i>2 = modp1024</i> <i>3 = modp1536</i> <i>4 = modp2084</i> <i>5 = modp3072</i> <i>6 = modp4096</i> <i>7 = modp6144</i> <i>8 = modp8192</i>	2	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_algorithm1 ~ ipsec_key_exchange4_encryption_algorithm1 [Encryption algorithm]	0–2 [1 character; 0–2] <i>0 = DES</i> <i>1 = 3DES</i> <i>2 = AES</i>	1	Specifies the encryption algorithm to be used during the negotiation.
ipsec_key_exchange1_hash_algorithm1 ~ ipsec_key_exchange4_hash_algorithm1 [Hash algorithm]	0–1 [1 character; 0–1] <i>0 = MD5</i> <i>1 = SHA-1</i>	1	Specifies the hash algorithm to be used during the negotiation.

Parameters	Value	Default	Description
ipsec_key_exchange1_lifetime_ph1 ~ ipsec_key_exchange4_lifetime_ph1 [IKE SA lifetime]	600-4294967295 [3 characters; 0-9]		Specifies the duration of the IKE connection in seconds. When the IKE SA lifetime expires, a re-authentication is required.
ipsec_key_exchange1_encapsulation_mode ~ ipsec_key_exchange4_encapsulation_mode [Encapsulation type]	0-1 [1 character; 0-1] <i>0 = transport mode</i> <i>1 = tunnel mode</i>	0	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 Print Server Homepage. Use a configuration file (racoon/setkey) instead.

Parameters	Value	Default	Description
ipsec_key_exchange1_pfs_group ~	0–8 [1 character; 0–8] 0 = --- 1 = <i>modp768</i>	ipsec_key_ex-change1_pfs_group p = 0	Specifies the Diffie-Hellman group number for the creation of additional dynamically generated temporary keys. The keys are used during phase 2.
ipsec_key_exchange4_pfs_group	2 = <i>modp1024</i> 3 = <i>modp1536</i> 4 = <i>modp2084</i>	ipsec_key_ex-change2_pfs_group p = 1	
[Diffie-Hellman group]	5 = <i>modp3072</i> 6 = <i>modp4096</i> 7 = <i>modp6144</i> 8 = <i>modp8192</i>	ipsec_key_ex-change3_pfs_group p = 1 ipsec_key_ex-change4_pfs_group p = 1	

Parameters	Value	Default	Description
ipsec_key_exchange1_encryption_algorithm_ph2	3des des aes des_iv64 ~	ipsec_key_exchange1_encryption_algorithm_ph2 = 3des,des,aes	Specifies the encryption algorithm for phase 2. <i>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.</i>
ipsec_key_exchange4_encryption_algorithm_ph2 [Encryption algorithm]	des_iv32 / null_enc [Multiple algorithms can be defined using a comma-separated list.]	ipsec_key_exchange2_encryption_algorithm_ph2 = aes ipsec_key_exchange3_encryption_algorithm_ph2 = aes ipsec_key_exchange4_encryption_algorithm_ph2 = aes	<i>3des = 3DES des = DES aes = AES des_iv64 = DES 64 des_iv32 = DES 32 null_enc = none</i>

Parameters	Value	Default	Description
ipsec_key_exchange1_auth_algo_ph2 ~ ipsec_key_exchange4_auth_algo_ph2 [Authentication algorithm]	hmac_md5 hmac_sha1 non_auth [Multiple algorithms can be defined using a comma-separated list.]	ipsec_key_exchange1_auth_algo_ph2 = hmac_md5, hmac_sha1 ipsec_key_exchange2_auth_algo_ph2 = hmac_sha1 ipsec_key_exchange3_auth_algo_ph2 = hmac_sha1 ipsec_key_exchange4_auth_algo_ph2 = hmac_sha1	Specifies the hash algorithm for phase 2. <i>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.</i> <i>hmac_md5= MD5</i> <i>hmac_sha1= SHA-1</i> <i>non_auth= none</i>

Parameters	Value	Default	Description
ipsec_key_exchange1_with_ah ~ ipsec_key_exchange4_with_ah [With AH protocol]	on/off	off	Specifies the use of the 'Authentication Header' protocol for the protection of the packet integrity and packet authentication. <i>AH uses the authentication header to authenticate the packet. In the IP data packet, the authentication header will be added after the IP header.</i>
ipsec_key_exchange1_lifetime_ph2 ~ ipsec_key_exchange4_lifetime_ph2 [IKE SA lifetime]	600–4294967295 [1–10 characters; 0–9]		Defines the time interval in seconds after which the IPsec key of an IPsec SA connection is renewed.
iserv_tmpl1_services ~ iserv_tmpl4_services [Services]	ALL ICMP HTTP SNMP SNTP IPP Socket printing LPR ThinPrint	iserv_tmpl1_services = ALL [blank]	Specifies the elements of the service filter. <i>Several protocols can be combined in a service.</i>

Table 37: Parameter List - Dynamic Update

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

Table 38: Parameter List - ThinPrint®

Parameters	Value	Default	Description
tp_port [ThinPrint® port]	1–65535 [1–5 characters; 0– 9]	4000	Defines the TCP port used by the print server for communicating with the ThinPrint® server. <i>The port number of the print server must be identical to the port number that was defined on the ThinPrint server.</i>
tp_bandwidth [Bandwidth]	on/off	off	Enables/disables the bandwidth functionality of the ThinPrint® port (print server side).
tp_bandwidthval [Bandwidth]	1600–1000000 [1–7 characters; 0– 9]	256000	Defines the bandwidth in bit/second (bit/s) used to decrease the bandwidth limit on the ThinPrint® port (print server side).
lp1_prt_name ~ lp8_prt_name [Printer]	max. 32 characters [a-z, A-Z, 0-9, _, -]	[blank]	Defines the printer name for the ThinPrint AutoConnect feature.
lp1_prt_class ~ lp8_prt_class [Class]	max. 7 characters [a-z, A-Z, 0-9, _, -]	[blank]	Defines the printer class name for the ThinPrint AutoConnect feature.
lp1_prt_driver ~ lp8_prt_driver [Driver]	max. 64 characters [a-z, A-Z, 0-9, _, -]	[blank]	Defines the printer driver for the ThinPrint AutoConnect feature.

17.3 Troubleshooting

This chapter describes some problems and their solutions.

Problem

- 'A connection to the Print Server Homepage cannot be established' ⇒ 143
- 'The password is no longer available' ⇒ 143

A connection to the Print Server Homepage cannot be established

Eliminate possible error sources. First of all, check:

- the cabling connections,
- the print server's IP configuration (⇒ 6), and
- the proxy settings of your browser.

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

- 'HTTP' (Hypertext Transfer Protocol) is deactivated. Reset Parameters to their default values ⇒ 80.
- The access is protected via SSL/TLS (HTTPS) ⇒ 69.
- The access is protected via SSL/TLS (HTTPS) and you deleted the certificate required (CA/self-signed/PKCS#12). Reset the parameter values of the print server to their default settings to get access ⇒ 80. Previous settings will be deleted.
- The password protection is enabled ⇒ 59.

The password is no longer available

The access to the Print Server Homepage can be protected by a password ⇒ 59. If the password is no longer available, you can reset the parameter values of the print server to their default settings to get access ⇒ 80. Previous settings will be deleted.

17.4 Index

A

- Access control 59
- Address template 97
- Administration methods 19
- ASCII 50
 - Print as PostScript 52
- Authentication 70
- AutoConnect 88

B

- Backup 78
- Bandwidth 87
- Banner page 50
- Bidirectional Communication 41
- Binary PostScript 50
- Bonjour 35
- Button 81
 - Print status page 46

C

- CA certificate 62
- Carriage Return with Line Feed (CR+LF) 50
- Certificate 62
- Certification authority 62
- Certification authority (CA) 62
- Communication mode
 - Bidirectional 41
 - Unidirectional 41
- Configuration parameter. See Parameters
- Contact 4

D

- Default certificate 62
- Default name 109
- Default settings 80
- Description 43
- Device number 109
- DNS 34
- Download
 - Parameters file 24, 78
 - Status page 45
- Downloads 4

- Duplex mode 34
- Dynamic update 82

E

- EAP-FAST 76
- EAP-MD5 70
- EAP-TLS 72
- EAP-TTLS 73
- Email
 - Administration 25
 - Commands 26
 - Notification 55
- Encrypted printing 13
- ESC 49, 51
- Extensible Authentication Protocol (EAP) 70

F

- Factory default settings 80
- Filter Function
 - Find and replace 48
- Filter function 48, 50
 - ASCII/PostScript 49
 - HEX dump mode 49
 - Job Start and Job End 49
 - LF / CR+LF 50
- Filter Settings 50
- Find and Replace 51
- Firmware update 81
- FTP 24
 - Configuring parameters 24
 - Print status page 45
 - Update 83
- FTPS 24

G

- Gateway 30, 108
- Guarantee 5

H

- Hardware address 44
- Hex dump mode 50
- Host name 108

- I**
- IEEE 802.1x 70
- IEEE1284.4 40
- IKE template 101
- Improper Use 5
- Intended Use 5
- Internet Printing Protocol (IPP) 12, 16
 - Printing 12, 16
- Internet Protocol Security, see IPsec
- IP address 6, 109
- IP sender control 60
- IP-Adresse
 - Saving 6
- IPsec 90
 - Address template 97
 - Configuration file 103
 - Exceptions 105
 - IKE template 101
 - Policy 90, 106
 - Rule 94, 97
 - SA template 100
 - Security association (SA) 91
 - Service template 99
 - Test mode 106
- IPv6 31
- J**
- Job history 45, 57
- L**
- Language 42
- LF print as LF+CR 51, 52
- Liability 5
- Line Feed (LF) 50
- Line Printer Daemon (LPD) 10, 16
- Logical 110
- Logical printers 50, 110
- M**
- MIB 36
- N**
- Network Protocols 30
- Network speed 34
- Notification
 - Email 55
 - SNMP traps 56
- P**
- Parameter values 80
- Parameters 110
 - Backup 78
 - Configuration via
 - Email 25
 - FTP 24
 - Download 78
 - File 78
 - Reset 80
 - Values 78
- Parameters file 24
- Password 59
- PEAP 74
- PJL 40
- PKCS#12 63, 67
- POP3 37
- Port
 - Mode 41
- PRESCRIBE 49, 51
- Print data
 - Conversion 49
 - Modify 48
 - Subsequent editing 48
- Print Job Language (PJL) 40, 54
- Print jobs
 - Assignment 47
 - Restrict the acceptance to a certain period of time 47
 - Status 45
 - Timeout 47
 - View 57
- Print server
 - Description 43
 - Language setting 42

- Reset 80
- restart 85
- Security 59
- Print server homepage 22
- Printer
 - Adaptation 50
 - Information 44, 54
 - Status information 44
 - View Status 54
- Printer messages
 - E-Mail 55
 - SNMP trap 56
- Printing
 - Encryption 13
 - Line Printer Daemon (LPD) 10, 16
 - Status page 46
- Printing method
 - Internet Printing Protocol 12, 16
 - Line Printer Daemon (LPD) 10, 16
 - Socket printing
 - 64-bit systems 8
- Private MIB 36
- Product information 4
- Protection 59
 - Against unauthorized parameter modifications 59
 - Read protection 59
 - Write protection 59
- Protocol
 - HTTP 60
 - IPv6 31
 - POP3 37
 - SMTP 37
 - SNMP 36
 - SNTP 42
 - TCP/IP 30
- Public Key 62
- R**
- Read protection 59
- Remote Authentication Dial-In User Service (RADIUS) 70
- Repairs 5
- Requested certificate 62
- Reset 80
- Restart 85
- S**
- SA template 100
- Safety regulations 5
- Secure printing 13
- Security association 91, 94
- SEH Product Manager 22
- Self-signed certificate 62
- Service template 99
- Signature 62
- SMTP 37
- SNMP 36
 - Traps 56
- SNTP server 42
- Socket 110
- Socket printing 8
 - 64-bit systems 8
- Software update 81
- Standard update 82
- Status
 - Bonjour 45
 - General 44
 - IPv6 45
 - Job history 45
 - Mail 45
 - POP3 45
 - Print server 44
 - Printer 54
 - Printer port 44
 - SMTP 45
- Status page 45
 - Download 45
 - Print 45
- Subnet mask 30, 109

T

TCP/IP 30

Test mode 106

ThinPrint

Client 86

Engine 86

ThinPrint® 86

AutoConnect 88

Bandwidth 87

Port 86

Printer class 88

SSL/TLS encryption 89

Time of the device 42

Time server 42

Time stamp 42

Time zone 43

Timeout 47

U

Unidirectional communication 41

Update 81

automatic 82

dynamic 82

standard 82

via Email 25

UTC 43

V

Version number 44

Viruses 60

W

Warnings 5

Website 4

Write protection 59