SEH

Intelligent Spooling Device

ISD400 / ISD410

User Manual

Manufactured by:
SEH Computertechnik GmbH
Suedring 11
33647 Bielefeld
Germany
Phone: +49 (0)521 94226-29
Fax: +49 (0)521 94226-99
Support: +49 (0)521 94226-44
Email: info@seh.de
Web: http://www.seh.de

Document:
Type: User Manual
Title: ISD400 / ISD410
Version: 1.1

Online Links to important Internet Resources:

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

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

This product uses 'Open Source Software'. For further information, please contact http://www.seh.de.
The product documentation gives you valuable information about your product.
Keep the documentation for further reference during the life cycle of the product.

Table of Contents

1 General Information

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

What information do you need?

- 'ISD400 / ISD410' ⇨🗎6
- 'Documentation' ⇨🗎9
- 'Support and Service' ⇨🗎12
- 'Your Safety' ⇨🗎13
- 'First Steps' ⇨🗎14
- 'Switching on/off the ISD' ⇨🗎15

1.1 ISD400 / ISD410

Purpose

The ISD was developed to spool and manage print jobs and to handle print queues.

In complex networks with high volumes of data traffic and in large-scale structures, the ISD can substantially relieve server load and remove strain from the network. This results in better performance and enhanced system stability.

The ISD adds server qualities to the printing in peer-to-peer networks. Enhanced transparency, higher performance and the central management of all print processes result in maximum efficiency and very little time required for maintenance and system updates.

The ISD is able to accept print jobs from various operating systems and to forward them to the printer via Socket, LPD, or IPP.

Features

- Central, efficient management of all print jobs and queues in the network
- Many print job management options: Prioritizing, deleting, halting, re-routing to alternative queues, etc.
- Many queue management options: Setting up balance and copy queues, blocking queues, etc.
- Quick, simple Installation: network printers are automatically detected, printer drivers can be automatically installed using Point and Print functionality, etc.
- Location-independent management via browser
- Simple initial configuration using the front panel display and control panel
- Comprehensive security options:
  - access control for configuration menus and queues,
  - web page encryption using HTTPs (TLS/SSL), certificates
  - Certificate management
  - Session management
  - support of the Windows Active Directory
  - IPsec support
- Automatic error notification via email
- With integrated DHCP/DNS functionality to automatically assign the IP address in networks without DHCP/DNS server
- Seamless integration in all Windows environments: MS Domain support.
- With integrated ThinPrint .print Client v7.0 and ThinPrint SSL encryption
- IPv6 support
- Additionally, the ISD410 comes with an integrated RAID system. The integrated RAID system increases the reliability and availability of the ISD410. All data will be saved redundantly to two hard disks.

Supported Network Protocols

- Application Level: HTTP, SNMP, DHCP
- Client to ISD: LPD, SMB, Socket, IPP, ThinPrint
- ISD to Printer: Socket, LPD, IPP

Procedure and Basic Functions

The ISD can be installed, configured, and managed quickly and easily. You will need an IP address to connect the ISD to the network. The IP address can be obtained automatically via DHCP or manually via the keys at the front of the device. The entire installation, configuration, and administration of the ISD and the connected network printers is done via a web interface (ISD Control Center).

All print servers and network printers that are available in the network will be detected automatically by search mechanisms during the installation procedure and will be made available as completely configured print queues.

If required, the drivers that are needed for printing purposes can be installed automatically to the connected Windows clients by means of the Microsoft feature Point-and-Print. To do this, the drivers must be stored to the ISD beforehand.

1.2 Documentation

Structure of the Documentation

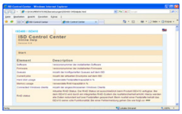
The ISD documentation consists of the following documents:

PDF

User Documentation
Detailed description of the ISD configuration and administration. (This document)
You will find the PDF file at www.seh.de or on the ISD hard disk (see: 'Service Area' ⇨ 🗎12).

Printed PDF

Quick Installation Guide
Information about security, hardware installation, and the initial operation procedure.
You will find the PDF file at www.seh.de or on the ISD hard disk (see: 'Service Area' ⇨ 🗎12).



HTML

Online Help (ISD Control Center)
The Online Help contains detailed information about how to use the ISD Control Center.

HTML

Online Help (SEH ISD Manager)
The Online Help contains detailed information about how to use the software tool 'SEH ISD Manager'.

Scope and Content

This document describes the entire functional range of the ISD. Access to the administration interface (ISD Control Center) is restricted to different user groups. Many instructions in this document require admin rights for the ISD Control Center.

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: ⇨🗎148.

Symbols and Conventions

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

Table 1: Conventions within the documentation

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

1.3 Support and Service

Service Area

The service area is a defined memory area on the ISD hard disk. The service area contains the ISD documentation and the installation files for the ISD tools. The service area can be displayed via the ISD Control Center.

Proceed as follows:

1. *Start the ISD Control Center ⇨ 🗎 16.*
2. *Select* **Manuals & Tools**.

↳ The service area is displayed.

Support

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

🕐	Monday through Thursday
	Friday
		from 8:00 a.m. to 4:45 p.m. and
		from 8:00 a.m. to 3:15 p.m. (CET)

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

Current Services

The following services can be found on the website www.isd.info.

ISD Portal
SEH
Startpage
Products
Service
Support
News
Where to buy?
About SEH
German
English
News
Channel: Keep Saving With TPGs!
Channel: Prices Stay Low!
Trade Shows & Events: SEH in London at DSEi
Review: Citrix iForum in Singapore
Tech?Update!: Cloud Computing
follow us @
twitter
DSEi
Channel: Keep Saving With TPGs!
Channel: Prices Stay Low!
Trade Shows & Events: SEH in London at DSEi

Welcome at the SEH ISD Portal!

Here you find all information about our print spool appliances of the ISD400 series!

Good news for our distributors and dealers in Europe: Our TPG ThinPrint .print Gateways are available at a special price for another month! Including the latest version of the ThinPrint .print Client, the TPGs decompress and decrypt all print jobs... mehr »

From May to June we made our European distributors and dealers happy by reducing the prices of three top SEH print servers. Now we are pleased to announce that we will make this price reduction permanent for the products: PS03a, the print... mehr »

From September 8 to 11, this year's Defense Systems & Equipment International 2009 (DSEi) will see the SEH Technology UK debut at this largest trade show for defense and security solutions worldwide. DSEi is an important platform for decision... mehr »

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

1.4 Your Safety

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

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

Intended Use

The ISD400 / ISD410 was developed to spool and manage print jobs in TCP/IP networks. The ISD has been designed for use in office environments.

Improper Use

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

Safety Regulations

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

Warnings

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

⚠

Warning!

1.5 First Steps

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

☞ Proceed as follows:

1. *Read and observe the security regulations in order to avoid damages to people and devices ⇨🗎13.*
2. *Carry out the hardware installation. The hardware installation comprises the connection of the ISD to the network and the power supply; see: 'Quick Installation Guide'.*
3. *Switch on the ISD; see: 'Quick Installation Guide' or ⇨🗎15.*
4. *Make sure that an IP address is stored in the ISD; see: 'Defining IPv4 Parameters Manually via the Front of the Device' ⇨🗎38.*
5. *Start the ISD Control Center ⇨🗎16.*
6. *Log on as Admin ⇨🗎17.*
7. *Carry out a Quick Setup ⇨🗎48.*
   The Quick Setup includes the configuration of TCP/IP parameters and queues.
8. *Define the role of the ISD within the network ⇨🗎50.*
9. *Install the printer drivers ⇨🗎60.*
10. *Configure the printer queues ⇨🗎80.*

↳ The ISD is operational.

1.6 Switching on/off the ISD

Booting / Switching on

☞ Proceed as follows:

1. *Press the power button* ⏻ *.*

↳ The system will boot

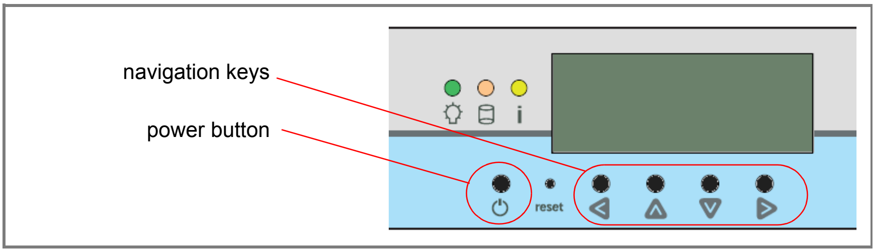


Fig. 1: ISD Device – Switching on/off the ISD

Shutting down / Switching off

Print jobs that are processed while the ISD shuts down cannot be completed. Print jobs that are stored in a queue will be completed when the device reboots.

☞ Proceed as follows:

1. *Press the button* ▽ *. The display shows:*

```
Shutdown
System
```

2. *Press the button* ▷ *. The display shows:*

```
Press V to
Shutdown System
```

3. *Press the button* ▽ *.*

↳ The system will shut down.

What Happens in the Case of a Power Failure?

When the ISD receives again the necessary power, it takes on the same status as before the power failure.

2 Administration Methods

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

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

What information do you need?

- 'Administration via the ISD Control Center' ⇨🗎16
- 'Administration via the SEH ISD Manager' ⇨🗎19
- 'Administration via the ISD Operating Panel' ⇨🗎22

2.1 Administration via the ISD Control Center

The ISD Control Center is a user interface for the administration of the ISD. The ISD Control Center is stored in the ISD and can be displayed on a PC by means of an Internet browser (Internet Explorer, Netscape, Firefox, Safari).

Requirements

☑ The ISD is connected to the network.

☑ The ISD has a valid IP address, see: ⇨🗎37.

Starting the ISD Control Center

Proceed as follows:

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

↳ The ISD Control Center will be displayed.

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

You can also start the ISD Control Center via the software tool 'SEH ISD Manager'. To start the ISD Control Center via the SEH ISD Manager, mark the ISD in the selection list and select **ISD – Homepage** from the menu bar.

Logging on to the ISD Control Center

After starting the ISD Control Center the 'Login' dialog appears. Access to the ISD Control Center is granted to the user profiles 'Any', 'User', and 'Admin'. You will also need a password.

The following describes access as 'Admin' with the default password.

Proceed as follows:

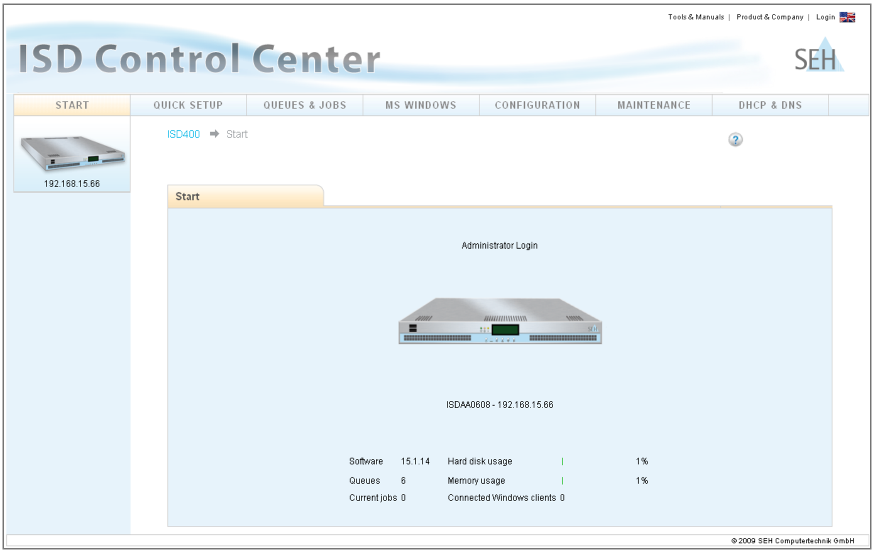
1. *Start the ISD Control Center.*
2. *Select 'Admin' from the* **Login account** *list.*
3. *Enter the password 'admin'.*
4. *Click* **Login** *to confirm.*

↳ The ISD Control Center shows the menu structure for the user profile 'Admin'.

Change the default password when you use the ISD in a real situation. For further information; see: ⇨🗎87.

Structure of ISD Control Center

The available menu items are located in the navigation bar (top). After selecting a menu item, the available submenu items are displayed on the left side. After selecting a submenu item, the corresponding page with its content is displayed.



ISDAA0608 - 192.168.15.66

Software 15.1.14
Queues 6
Current jobs 0
Hard disk usage 1%
Memory usage 1%
Connected Windows clients 0

Fig. 2: ISD Control Center - Administrator Login

The menu items refer to the configuration of the ISD. The menu items will be described in this document.

All administrative actions via the ISD Control Center require access as 'Admin'. For further information; see: ⇨🗎87.

2.2 Administration via the SEH ISD Manager

The SEH ISD Manager is a software that has been developed by SEH Computertechnik GmbH for a simple administration of the ISDs.

Basic Functions

After starting the SEH ISD Manager the ISDs can be added to the device list. You can mark and then monitor or configure the devices listed in the device list. You can modify the device list and adopt it to your individual needs.

Which Functions Are Supported?

The SEH ISD Manager offers the following features to assist you in your work:

- *Monitoring*: A status indicator monitors all the ISDs available in the network. The status indicator provides information about the utilized capacity, network configurations, Windows configurations, login status, set-up queues and printers, etc.
- *Backup Management*: The configuration settings of an ISD can be saved and maintained in an image file. The image files can be created and deleted at any time. Image files can also be manually or automatically backed up to the PC.
- *Update Management*: The Update Management function allows software to be simultaneously installed on one or more ISDs. The software can be a software update, a patch, a filter application or an image file.
- *Queues and printer drivers*: Queues and printer drivers installed on the ISDs can be combined and stored in a database on the PC. From here they can be easily forwarded to and installed on other ISDs.
- *Reboot*: One action is required to activate a restart on one or more ISDs.

User Rights

You will need certain user rights in order to carry out configurations via the SEH ISD Manager. When saving software, queues, and printer drivers to an ISD or carrying out a restart, you will be prompted to enter the password for the user profile 'Admin'. For further information; see: ⇨🗎87.

Installation and Program Start

In order to use the SEH ISD Manager, the program must be installed on a computer with a Windows operating system.

You will find the SEH ISD Manager installation file at www.seh.de or on the ISD hard disc. (see: 'Service Area' ⇨🗎12).

Proceed as follows:

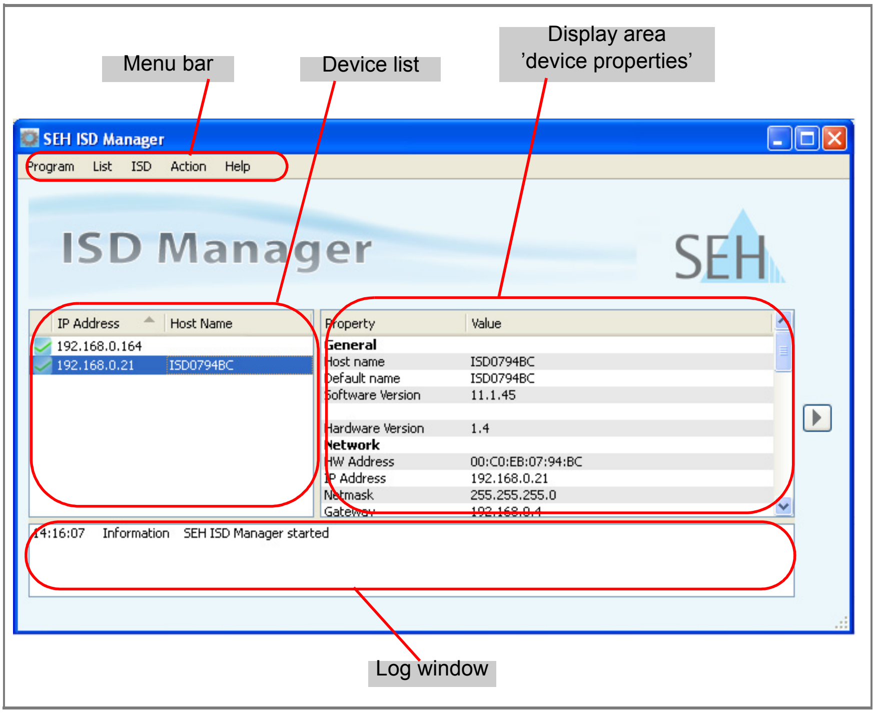
1. *Start the SEH ISD Manager installation file.*
2. *Follow the installation routine.*

↳ The SEH ISD Manager will be installed on the system.

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

Structure of the SEH ISD Manager

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



IP Address	Host Name
192.168.0.164	
192.168.0.21	ISD0794BC

Property	Value
General	
Host name	ISD0794BC
Default name	ISD0794BC
Software Version	11.1.45
Hardware Version	1.4
Network	
HW Address	00:C0:EB:07:94:BC
IP Address	192.168.0.21
Netmask	255.255.255.0
Gateway	192.168.0.1

```
14:16:07    Information    SEH ISD Manager started
```

Fig. 3: SEH ISD Manager - Main Dialog

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

2.3 Administration via the ISD Operating Panel

The ISD operating panel is located at the front of the device. Use the navigation keys to carry out different tasks.

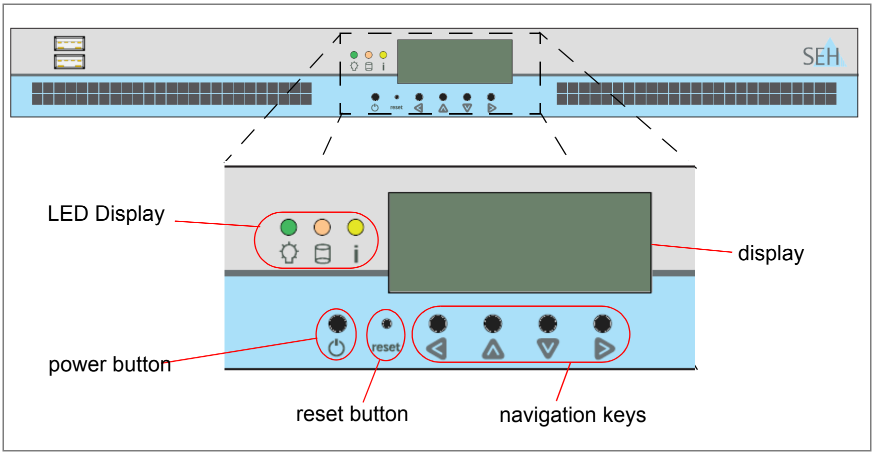


Fig. 4: ISD Device - Operating Panel with Navigation Keys

Which Functions Are Supported?

The navigation keys of the ISD operating panel allow you to

- 'Switching on/off the ISD' ⇨🗎15
- 'Getting Information' ⇨🗎35
- 'Defining IPv4 Parameters Manually via the Front of the Device' ⇨🗎38
- 'Defining IPv4 Parameters via DHCP using the Front of the Device' ⇨🗎39
- 'Resetting the ISD Parameters' ⇨🗎112
- 'Resetting the Password' ⇨🗎113
- 'Hard Rebooting the ISD via the Device Front' ⇨🗎116

You can protect the operating panel against unauthorized access by means of a 4-digit PIN. The administrator defines the PIN on the ISD Control Center. If the operating panel is protected, you must enter the PIN via the navigation keys; see: ⇨🗎91.

3 Printing Methods

The ISD supports a number of printing methods. It all depends on how the print data is sent from the client to the printer. This chapter gives a short overview.

The print data is sent from the client to the printers via the ISD. The print data stream can be divided into two ways:

- The print data is sent from the client to the ISD
  (This setting will be configured on the PC client while setting up printers).
- The print data is sent from the ISD to the printer
  (The queue type specifies which protocol is used to send the print data from the ISD to the printer. Queues will be created on the ISD via the ISD Control Center.)

What information do you need?

- 'LPD Printing' ⇨🗎23
- 'Socket Printing' ⇨🗎24
- 'IPP Printing' ⇨🗎26
- 'Windows Printing (SMB/CIFS)' ⇨🗎27

3.1 LPD Printing

The ISD supports printing via the LPD (Line Printer Daemon) protocol. During LPD printing the print data is sent to the IP address of the printer by means of the LPR port.

ISD ⇨ Printer

Every queue created during the Quick Setup automatically supports LPD printing. This means that a queue that is configured on the ISD sends print data to the assigned printer via LPD. For further information; see: Table 13 ⇨🗎69.

Client ⇨ ISD

In order to use LPD, the port name for the configuration of the client must be identical to the queue name on the ISD.

3.2 Socket Printing

When socket printing is used, the print data will be sent from the client to the ISD via direct TCP/IP ports. The ISD receives the print data and routes it to the printers.

Procedure

Follow the instructions to make use of socket printing:

□ 'Preparing the Client for Socket Printing' ⇨🗎24.

□ 'Preparing the Queue for Socket Printing' ⇨🗎25

Preparing the Client for Socket Printing

As far as socket printing is concerned, a printer port must be added to every client intended for printing. You can use the printing service of a Windows operating system or the SEH Print Monitor to configure printer ports on the clients.

The SEH Print Monitor is an SEH-specific extension. It ensures, amongst others, the transfer of print data from the client to the ISD by means of direct TCP/IP ports. In conjunction with the ISD, only connections via the HTTP protocol are available. You can choose between unencrypted (HTTP port 80) and encrypted connections (HTTP port 443).

Encrypted connections can be additionally secured by means of an authentication. For authentication purposes you must install the certificate of the ISD to the client; see: ⇨🗎99.

Installing the SEH Print Monitor

You will find the SEH Print Monitor installation file at www.seh.de or on the ISD hard disc. (see: 'Service Area' ⇨🗎12).

Proceed as follows:

1. *Start the SEH Print Monitor installation file.*
2. *Follow the installation routine.*

↳ The SEH Print Monitor will be installed to your system.

Creating Printer Ports

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

☞ Proceed as follows:

1. *Click 'Start' > 'Settings' > 'Printers and Faxes'.*
2. *Select* **File – Add Printer** *from the menu bar.*
   The 'Add Printer Wizard' appears.
3. *Click* **Next**.
4. *Tick* **Local printer attached to this computer**.
5. *Click* **Next**.
6. *Tick* **Create a new port**.
7. *Select 'SEH Print Monitor' from the* **Type of port** *list.*
8. *Click* **Next**.
   The dialog **SEH TCP/IP Port Configuration** *appears.*
9. *Specify the ISD via the IP address or host name.*
10. *Follow the program.*

↳ The printer port will be added to the client.

Preparing the Queue for Socket Printing

Every queue created on the ISD during the Quick Setup supports socket printing. A TCP/IP port from the range 9100 to 9107 is additionally assigned to the queues.

☞ Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS – Print Sockets**.
3. *Assign available queues to the TCP/IP ports.*
4. *Click* **Save** *to confirm.*

↳ The setting is saved.

3.3 IPP Printing

The IPP (Internet Printing Protocol) provides printing services via a network. IPP is based on HTTP 1.1. Bidirectional functions have been added to allow status queries and notifications.

In a client/server system, print data can be transmitted via IPP in an encrypted or unencrypted way. Every queue created during the Quick Setup automatically supports IPP. For further information; see: Table 13 ⇨🗎69.

In the case of IPP printing, the IPP device will be addressed via a Uniform Resource Identifier (URI). The syntax of the URI looks as follows:

ISD ⇨ Printer

Transmission of unencrypted data

```
http://<ip-address>:631/ipp/<logical printer>
ipp://<ip-address>/ipp/<logical printer>
```

Transmission of encrypted data

```
https://<ip-address>/ipp/<logical printer>
```

<ip-address> = IP address or host name of the end device*
<logical printer> = logical printer (lp1 - lp8) **

* The syntax describes an application scenario where the print data is sent from the ISD to an SEH print server.

** The logical printer defines the printer port to which the print data is sent. If no logical printer is defined, the logical printer no. 1 will be used automatically.

Client ⇨ ISD

Transmission of unencrypted data

```
ipp://<ip-address>/printers/<my_queue>
http://<ip-address>:631/printers/<my_queue>
```

Transmission of encrypted data

```
https://<ip-address>/printers/<my_queue>
```

<ip-address> = IP address or host name of the ISD
<my_queue> = queue name on the ISD

3.4 Windows Printing (SMB/CIFS)

Windows printing is based on the protocols SMB and CIFS. SMB (Server Message Block) describes the exchange of data between computers in a network.

CIFS (Common Internet File System) describes an extended version of SMB. CIFS is based on NBT (NetBIOS over TCP/IP) and SMB and offers (amongst the sharing of files and printers) additional services.

The ISD supports the protocols used by Windows and thus offers additional functions.

SMB printing is almost exclusively used by Microsoft operating systems. It is based on the SMB protocol, today regarded as the preferred protocol for communicating and sharing files and resources on a network. In order to integrate the ISD in a Microsoft environment; see: 'The ISD in Microsoft Networks' ⇨🗎50.

One major advantage of SMB printing in client/server environments is its central driver management capability (Point and Print). This method is used to store printer drivers centrally on the ISD. If a client establishes a connection to a printer on the ISD, the client will find the suitable driver on the ISD. The driver will then be automatically installed on the client. In order to use Point and Print, see: ⇨🗎60.

4 Status Information

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

What information do you need?

- 'How to Get Information via the ISD Control Center' ⇨🗎28
- 'How to Get Information via Email or SNMP Traps' ⇨🗎33
- 'How to Get Information via the SEH ISD Manager' ⇨🗎34
- 'Which Information Do I Get via the Device Front?' ⇨🗎35

4.1 How to Get Information via the ISD Control Center

You can view the current configuration status of the ISD via the ISD Control Center. Additionally you can view and analyze the print volume in the network. You can view current and completed print jobs.

What do you want to do?

□ 'Displaying Basic Information' ⇨🗎29

□ 'Displaying Status Information' ⇨🗎29

□ 'Displaying MS Windows Network Information' ⇨🗎31

□ 'Displaying Queues' ⇨🗎31

□ 'Displaying Current Print Jobs' ⇨🗎32

□ 'Displaying the Job History' ⇨🗎32

□ 'Displaying Advanced Status Information' ⇨🗎33

Displaying Basic Information

After the login, basic information of the ISD will be displayed on the 'Start' page. In addition to the user profile, the host name, and the IP address you will get the following information:

Table 2: Basic Information

Parameters	Description
Software	Version number of the installed software
Queues	Number of configured print queues on the ISD
Current jobs	Number of current print jobs on the ISD
Hard disk usage	Used hard drive capacity
Memory usage	Used RAM capacity
Connected Windows clients	Number of connected Windows clients
RAID status	Current RAID status. (The RAID function is only available for the ISD410.)

Displaying Status Information

Detailed status information can be found on the 'Maintenance' page.

☞ Proceed as follows:

1. *Select* **MAINTENANCE - Status**.

↳ The status information is displayed.

Table 3: Status Information

Parameters	Description
Device	
Default name	Default name of the ISD
Host name	Host name of the ISD
Date	Current date
Time	Current time

Parameters	Description
Uptime	Period of time during which the ISD is operational
Serial number	Serial number of the ISD
Software	Version number of the installed software
Hardware version	Hardware version of the ISD
Network	
Hardware address	Hardware address of the ISD (MAC address)
IP address	IPv4 address of the ISD
Subnet mask	Subnet mask
Gateway	Gateway address of the ISD. A gateway is used to ensure communication between the ISD and devices in other subnets.
Primary DNS server	IP address of the primary DNS server
Secondary DNS server	IP address of the secondary DNS server. The secondary DNS server is used if the first one is not available.
DNS domain name	Domain name of the DNS server
MS Windows	
NetBIOS name	NetBIOS name of the ISD
NetBIOS workgroup	Name of the NetBIOS workgroup
WINS server	IP address or host name of the WINS server
Printer administrator	Local user that has the right to install printer drivers and carry out global printer settings.
Hard Disk *(only ISD400)*	
Model	Name of the hard disk model
Capacity	Complete hard disk capacity
Used	Used hard disk space
RAID *(only ISD410)*	
Model	Name of the RAID system
Status	Current RAID status.
Capacity	Complete hard disk capacity
Used	Used hard disk space
Disk	Hard disk number
Model (Disk)	Name of the hard disk model
Serial (Disk)	Serial number of the hard disk

Parameters	Description
Status (Disk)	Status of the hard disk

Displaying MS Windows Network Information

Detailed information about the Windows network settings can be found on the 'MS Windows' page.

Proceed as follows:

1. *Select* **MS WINDOWS – Network Settings***.*

↳ The Windows network settings are displayed.

Table 4: MS Windows Information

Parameters	Description
Host / NetBIOS name	NetBIOS name of the ISD. The NetBIOS name is identical to the host name.
WINS server	IP address or host name of the WINS server
Workgroup	Name of the NetBIOS workgroup
(Active Directory) Domain name	Domain name within the Active Directory
Password server	IP address or host name of the password server.
Server role	Role of the ISD within the network environment
Status	Membership within a domain

Displaying Queues

Detailed information about the created queues can be found on the 'Queues' page.

Proceed as follows:

1. *Select* **QUEUES & JOBS – Queues***.*

↳ The queues are displayed.

Table 5: Queues Information

Parameters	Description
Description	Freely definable description of the queue.
Location	Freely definable description of the printer location.
IP address	IP address of the connected printer.
State	Status of the queue
Jobs	Number of current print jobs

Displaying Current Print Jobs

You can display the current print jobs. You get details such as the name, size, or status of the print job.

Proceed as follows:

1. *Select* **QUEUES & JOBS – Current Jobs**.

↳ The active print jobs are shown.

The print jobs that are displayed can be edited. Editing means the deleting, halting, and prioritizing of print jobs as well as moving print jobs to different queues. To edit a print job click the name of the queue.

Displaying the Job History

You can view the completed print jobs in the Job History. You get details such as the name or size of the print job.

Proceed as follows:

1. *Select* **QUEUES & JOBS – Job History**.

↳ The Job History is displayed.

Displaying Advanced Status Information

Via the Diagnostics area you can display the following status information.

- network information
- memory information
- task information

Proceed as follows:

1. *Select* **MAINTENANCE - Diagnostic***.*
2. *Select the* **Advanced Status** *tab.*

↳ The advanced status information is display.

4.2 How to Get Information via Email or SNMP Traps

You can get notifications as emails or SNMP traps from the ISD. You can define which event or type of notification will cause the ISD to send a notification.

Voraussetzung

☑ The notification service has been configured; see: ⇨🗎46.

In addition, the ISD can send the following information to the recipients of the notification service:

- number of failed login attempts to the ISD Control Center; see: ⇨🗎90
- Log Files; see: ⇨🗎111
- Information about Hardware, Cups and Samba; see: ⇨🗎111

4.3 How to Get Information via the SEH ISD Manager

The SEH ISD Manager allows you to get an overview of the entire ISD status information.

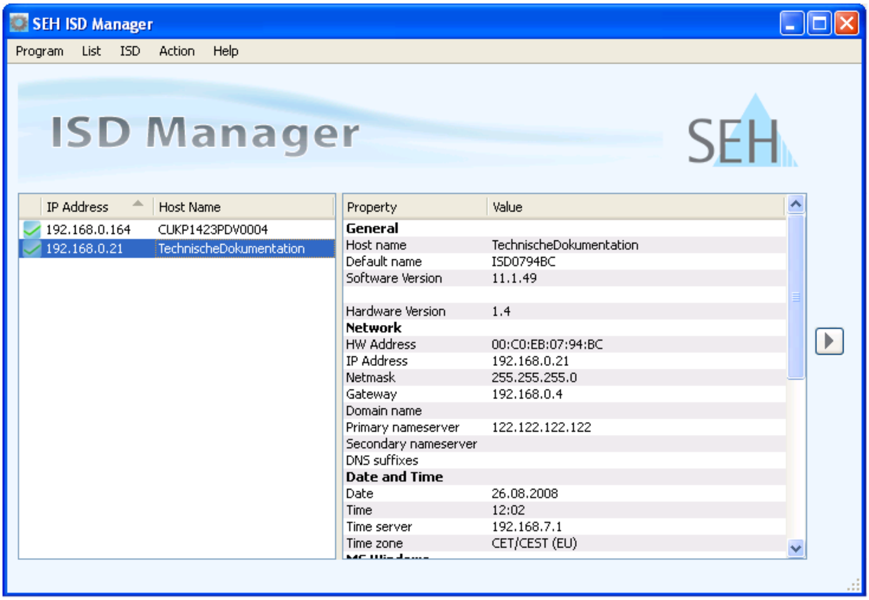
Requirements

☑ The SEH ISD Manager is installed on the PC; see: ⇨🗎19.

Proceed as follows:

1. *Start the SEH ISD Manager* ⇨🗎*20.*
2. *Add the ISD to the list.*
   - Select **List - Add ISD***.*
   - Define the ISD via the IP address or host name.
   - Click **OK** *to confirm.*
3. *Make sure that the device properties are displayed in the main dialog.*
4. *Double-click the ISD in the list.*

↳ The entire ISD status information is shown.



IP Address	Host Name
192.168.0.164	CUKP1423PDV0004
192.168.0.21	TechnischeDokumentation

Property	Value
General	
Host name	TechnischeDokumentation
Default name	ISD0794BC
Software Version	11.1.49
Hardware Version	1.4
Network	
HW Address	00:C0:EB:07:94:BC
IP Address	192.168.0.21
Netmask	255.255.255.0
Gateway	192.168.0.4
Domain name	
Primary nameserver	122.122.122.122
Secondary nameserver	
DNS suffixes	
Date and Time	
Date	26.08.2008
Time	12:02
Time server	192.168.7.1
Time zone	CET/CEST (EU)

Fig. 5: SEH ISD Manager – Status Information

4.4 Which Information Do I Get via the Device Front?

You can get information via the LEDs at the device front.

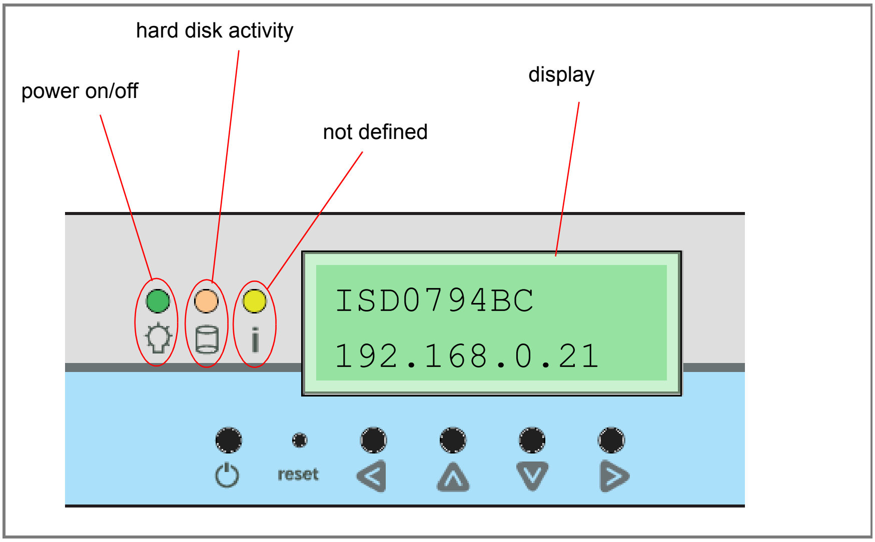
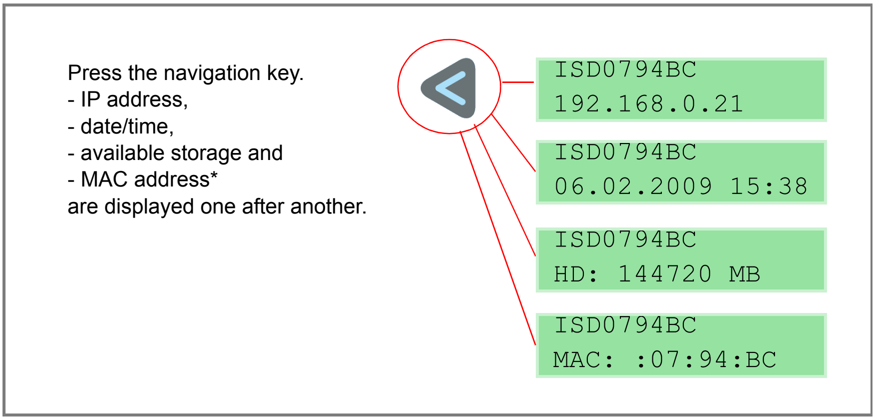


Fig. 6: ISD Device - LEDs

You can get information via the display at the device front.



Press the navigation key.
- IP address,
- date/time,
- available storage and
- MAC address*
are displayed one after another.

Fig. 7: ISD Device – Display

* The display only shows the last six digits of the MAC address. For further information; see: ⇨ 🗎150.

5 Network and Device Settings

You can configure the device time, DNS, host name, etc. on the ISD. This chapter describes the network and device settings.

What information do you need?

- 'How to Configure IPv4 Parameters?' ⇨🖹37
- 'How to Configure IPv6 Parameters' ⇨🖹40
- 'How to Configure DNS' ⇨🖹43
- 'How to Define the Host Name' ⇨🖹44
- 'How to Configure the Device Time' ⇨🖹44
- 'How to Use the Notification Service' ⇨🖹46
- 'How to Use the Quick Setup' ⇨🖹48

Please use the Quick Setup for the initial configuration of the ISD.

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.

You can define various parameters (IP, netmask, gateway) for an ideal integration of the ISD into a TCP/IP network. You can assign the TCP/IP parameter manually or have it assigned automatically via DHCP (Dynamic Host Configuration Protocol). The manually assignment is default. You can define the parameters via the operating panel at the front of the device or via the ISD Control Center.

What do you want to do?

□ 'Defining IPv4 Parameters Manually via the Front of the Device' ⇨🖹38

□ 'Defining IPv4 Parameters via DHCP using the Front of the Device' ⇨🖹39

□ 'Defining IPv4 Parameters via the ISD Control Center' ⇨🖹39

Defining IPv4 Parameters Manually via the Front of the Device

Use the navigation keys at the front of the device to assign the TCP/IP parameters manually.

Proceed as follows:

1. *Select ▲. The display shows:*

```
 IP Setup   >
 Cancel     <
```

2. *Select ▶. The display shows the current IP configuration ('Manual' or 'DHCP'):*

```
 IP Configuration
 Manual
```

3. *Select* **Manual** *via ▲ or ▼ and press ▶ to confirm.*
   The display shows:

```
 IP Address
000.000.000.000
```

4. *Enter the IP address.*
   Use ◀ ▶ to navigate to individual numerical values within the IP address. You can change the numerical values via ▲▼.
5. *Press ▶ to confirm. The display shows:*

```
 Netmask
000.000.000.000
```

6. *Enter the netmask.*
7. *Press ▶ to confirm. The display shows:*

```
 Gateway
000.000.000.000
```

8. *Enter the gateway.*
9. *Press ▶ to confirm. The display shows:*

```
 > Apply
 < Back
```

10. *Press ▶ to confirm. The display shows:*

```
 Applying Network
 Settings ...
```

↳ The settings are saved.

Defining IPv4 Parameters via DHCP using the Front of the Device

Requirements

☑ An active DHCP server is integrated into the network.

Use the navigation keys at the front of the device to assign the TCP/IP parameters via DHCP.

Proceed as follows:

1. *Select ▲. The display shows:*

```
IP Setup  >
Cancel    <
```

2. *Select ▶. The display shows the current IP configuration ('Manual' or 'DHCP'):*

```
IP Configuration
Manual
```

3. *Select* **DHCP** *via ▲ or ▼ and press ▶ to confirm.*
   The display shows:

```
> Apply
< Back
```

4. *Press ▶ to confirm.*

↳ The settings are saved.

Upon booting DHCP will be applied automatically. TCP/IP parameters are assigned by a DHCP server.

Defining IPv4 Parameters via the ISD Control Center

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION - IPv4**.
3. *Enter the TCP/IP parameters manually or enable the* **DHCP** *option; see: Table 6 ⇨ 🗎 40.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 6: Parameter - IPv4

Parameters	Description
IP address	IP address of the ISD (e.g. 192.168.0.21)
Subnet mask	Subnet mask of the ISD
Gateway	Gateway address of the ISD. A gateway is used to ensure communication between the ISD and devices in other subnets.
DHCP	Enables/disables ’DHCP’. TCP/IP parameters can be assigned automatically to the ISD via DHCP. This requires a reboot after the DHCP activation.

5.2 How to Configure IPv6 Parameters

You can integrate the ISD into an IPv6 network.

Benefits and Purpose

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

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

What is the Structure of an IPv6 Address?

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

Each field is separated by a colon (:).
Example: `fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4`

Leading zeros in a field can be omitted.
Example: `fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4`

An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used. However, the use of two colons can be used only once in an address.
Example: `fe80 :                                : 10 : 1000 : 1a4`

As a URL in a Web browser, an IPv6 address must be enclosed in brackets. This prevents port numbers from being mistakenly regarded as part of an IPv6 address.
Example: `http://[2001:608:af:1::100]:443`

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

Which Types of IPv6 Addresses are available?

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

- Unicast addresses can be routed globally. These addresses are unique and therefore unambiguous. A packet that is sent to a unicast address will only arrive to the interface that is assigned to this address. Unicast addresses have the prefixes '2' or '3'.
- Anycast addresses are assigned to more than one interface. This means that a data packet that is sent to this address will arrive at various devices. The syntax of anycast addresses is the same as the one of unicast addresses. The difference is that anycast addresses choose one interface out of many.
  A packet that is dedicated to an anycast address arrives at the nearest interface (in line with the router metrics). Anycast addresses are only used by routers.

- Multicast addresses allow you to send data packets to different interfaces at the same time without a proportional increase of the bandwidth. A multicast address can be recognized by the prefix 'ff'.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION – IPv6***.*
3. *Configure the IPv6 parameters; see: Table 7 ⇨🗎42.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 7: Parameter - IPv6

Parameters	Description
IPv6	Enables/disables the IPv6 functionality of the ISD
IPv6 address	Defines a manually assigned IPv6 Unicast address in the n:n:n:n:n:n:n:n. format for the ISD. *Each 'n' describes the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.*
Router	Defines the IPv6 unicast address of the router. The ISD sends its 'Router Solicitations' (RS) to this router.
Prefix length	Defines the length of the subnet prefix for the IPv6 address. (The value 64 is preset.) *Address ranges are specified by prefixes. The prefix length (number of used bits) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/'.*
Automatic configuration	Enables/disables the automatic configuration of IPv6 addresses for the ISD.
IPv6 addresses	Displays the automatically configured IPv6 addresses.
IPv6 routing table	The IPv6 routing table is created automatically on the basis of the current IPv6 configuration of the ISD. When IPv6 packages are forwarded, the routing table of the ISD is searched for an entry that matches the IPv6 target address most.

5.3 How to Configure 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 ISD.

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.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION – DNS***.*
3. *Configure the DNS parameters; see: Table 8 ⇨🗎43.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 8: Parameter - DNS

Parameters	Description
Domain name	Domain name of an existing DNS server (e.g. company.de)
Primary DNS server	IP address of the primary DNS server. (e.g. 192.168.0.21)
Secondary DNS server	IP address of the secondary DNS server. (The secondary DNS server is used if the primary DNS server is not available.)
Domain search list	Suffixes for the domain search list. (e.g. soft.seh.de) Multiple entries are to be separated by blanks.

5.4 How to Define the Host Name

You can define a host name for the ISD. The host name is an alias for an IP address. Upon delivery, the default name is displayed. You can find the host name on the ISD Control Center, in the SEH ISD Manager or the display at the front of the device.

Benefits and Purpose

The host name uniquely identifies the ISD in the network and makes it easier to remember.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION – Time & Host name***.*
3. *Enter the host name. (max. 63 characters)*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

5.5 How to Configure the Device Time

The device time can be configured manually or via a time server. A time server is a computer networking device that reads the actual time from a reference clock and distributes this information to its clients. The time server is defined via the IP address or the host name.

An active time server overrides the manually defined time.

UTC & Time Zone

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

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 can be handled by means of the 'Time zone' parameter.

Benefits and Purpose

Once the device time is configured, all print jobs that are handled by the ISD will get a time stamp. Date and time are then displayed under Job History. The device time is also required for automatic backups.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION - Time & Host name***.*
3. *Enter date and time or use a time server; see see: Table 9 ⇨ 🗎 45.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 9: Parameters - Time

Parameters	Description
Default name	Default name of the ISD
Host name	Host name of the ISD (max. 63 characters)
Date	Date in the format: 'dd.mm.yyyy' (e.g. 23.05.2007)
Time	Time in the 24 hours format: 'hh:mm' (e.g. 16:36)
Time server	IP address or host name of the time server (e.g. 'ntp1.ptb.de'). The 'ntp' protocol is used.
Time zone	The time zone is used to equalize the difference between the Greenwich Mean Time or UTC (Universal Time Coordinate) of the time server and the local time.

5.6 How to Use the Notification Service

You can get notifications as emails or SNMP traps from the ISD. You can define which event or type of notification will cause the ISD to send a notification.

Benefits and Purpose

By means of notifications, the recipient (usually the administrator) will be immediately informed about errors and warnings irrespective of his/her location.

In addition, the ISD can send the following information to the recipients of the notification service:

- number of failed login attempts to the ISD Control Center; see: ⇨🗎90
- Log Files; see: ⇨🗎111
- Information about Hardware, Cups and Samba; see: ⇨🗎111

In order to use the notification service you must configure the SMTP parameters or SNMP traps on the ISD.

☞ Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION - Notification**.
3. *Configure the parameters; see: Table 10 ⇨🗎46.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

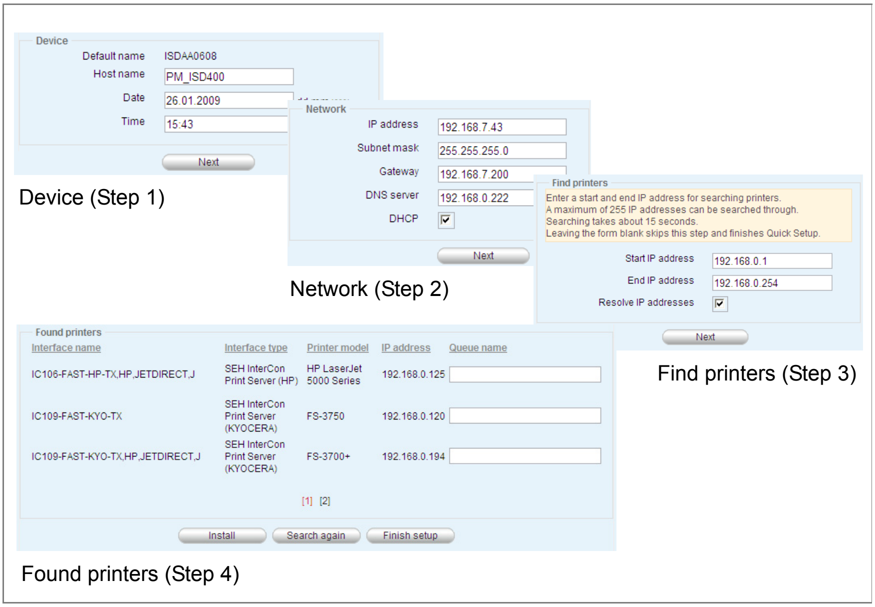
Table 10: Parameter - Notification

Parameters	Description
Email	
Server name	IP address or host name of the SMTP server. (e.g. 192.168.0.21)
Server port	Defines the port number used by the ISD to send emails to the SMTP server. (Default = 25)

Parameters	Description
TLS	Enables/disables TLS. The TLS protocol serves to encrypt the transmission between the ISD and the SMTP server.
Authentication (Login)	Enables/disables the authentication method between the ISD and the SMTP server.
User name	Defines the name used by the ISD during the authentication with the SMTP server.
Password	Defines the password used by the ISD during the authentication with the SMTP server.
Sender name	Defines the email sender name to be used by the ISD. (Default = ISD Default Name).
Recipient	Defines the email address of the recipient (e.g. people@company.com)
Notification level	The notification level specifies which types of notification are sent. The following levels are available: Disabled Disables the 'notification' feature. No notifications will be sent. Errors only Only system errors will be sent. (e.g. 'Unable to connect to spool server') Warnings and errors System errors or warnings will be sent. (e.g. 'Password for user *admin* changed) All messages All types of notification will be sent (e.g. 'Print queue created').
SNMP traps	
IP address	IP address or host name of the SNMP server (e.g. 192.168.0.21).
Trap community	Defines the recipient as a trap community (e.g. public)
Notification level	The notification level specifies which types of notification are sent. The following levels are available: Disabled Disables the 'notification' feature. No notifications will be sent. Errors only Only system errors will be sent. (e.g. 'Unable to connect to spool server') Warnings and errors System errors or warnings will be sent. (e.g. 'Password for user *admin* changed) All messages All types of notification will be sent. (e.g. 'Print queue created')

5.7 How to Use the Quick Setup

The Quick Setup assists you with the initial configuration of the ISD. The Quick Setup contains four steps in order to set up necessary parameters and queues on the ISD.



Device

Default name ISDAA0608

Host name PM_ISD400

Date 26.01.2009

Time 15:43

Device (Step 1)

Network

IP address 192.168.7.43

Subnet mask 255.255.255.0

Gateway 192.168.7.200

DNS server 192.168.0.222

DHCP ☑

Network (Step 2)

Find printers

Enter a start and end IP address for searching printers.
A maximum of 255 IP addresses can be searched through.
Searching takes about 15 seconds.
Leaving the form blank skips this step and finishes Quick Setup.

Start IP address 192.168.0.1

End IP address 192.168.0.254

Resolve IP addresses ☑

Find printers (Step 3)

Found printers

Interface name	Interface type	Printer model	IP address	Queue name
IC106-FAST-HP-TX,HP,JETDIRECT,J	SEH InterCon Print Server (HP)	HP LaserJet 5000 Series	192.168.0.125	
IC109-FAST-KYO-TX	SEH InterCon Print Server (KYOCERA)	FS-3750	192.168.0.120	
IC109-FAST-KYO-TX,HP,JETDIRECT,J	SEH InterCon Print Server (KYOCERA)	FS-3700+	192.168.0.194	

Found printers (Step 4)

Fig. 8: ISD Control Center – Quick Setup

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUICK SETUP***.*
3. *Enter the host name and the device time.*
4. *Click* **Next***.*
5. *Enter the TCP/IP parameters or enable the* **DHCP** *option.*
6. *Click* **Next***.*
7. *Define search parameters for the search for printers in the network. You can search a maximum of 255 IP addresses.*
8. *Click* **Next***.*
   The number of the printers found is displayed.

9. *Click* **OK** *to confirm.*
   The printer list is displayed.
10. *Assign names to the queues (that are not resolved via DNS) in the* **Queue name** *column.*
    Note the following conventions:
    - letters, numbers, hyphens and underscores are allowed
    - no space characters are allowed
    - no more than 32 characters (Windows 98 max. 15 characters)
11. *Click* **Install***. The names of the queues appear dimmed in the column* **Queue name***.*
12. *Click* **Finish setup** *to confirm.*

➥ The settings are saved.

For a fast configuration we recommend assigning printer drivers via 'Point and Print'; see: ⇨🗎60.
To configure additional DNS settings; see: ⇨🗎43.
To define a time server, see: ⇨🗎44.

6 The ISD in Microsoft Networks

The ISD can be integrated into Windows networks. The ISD can take over and implement several Windows-based functions. This chapter describes how to ideally integrate the ISD into a Windows network.

Windows networking is a set of protocols and services that allow Windows machines to communicate to provide facilities such as file and printer sharing and work group and domain browsing.

SMB (Server Message Block) is used to grant Windows systems access to resources of UNIX-based systems and vice versa. SMB is used to implement the Windows directory service Active Directory Service.

CIFS (Common Internet File System) describes an extended version of SMB. CIFS is based on NBT (NetBIOS over TCP/IP) and SMB and offers (amongst the sharing of files and printers) additional services.

The ISD supports the protocols used by Windows and thus offers additional functions.

What information do you need?

- 'How to Implement the ISD into the Active Directory' ⇨🗎51
- 'How to Use an NTLM Authentication' ⇨🗎53
- 'How to Define the Printer Administrator' ⇨🗎54
- 'How to Define the ISD as a Stand-Alone Server' ⇨🗎55
- 'How to Configure the Local User Management' ⇨🗎55
- 'How to Configure Additional Windows Settings' ⇨🗎59

6.1 How to Implement the ISD into the Active Directory

What is ADS?

The Active Directory Service (ADS) is the directory service of the Microsoft Windows 2000 and Windows 2003 server. A directory service allows for efficient management of users, groups, printers, and other resources available on the network.

Administrators, for example, may use the ADS to define consistent access rights applying to the entire network. Centrally managing the access rights allows for a user and group based access management.

Benefits and Purpose

By embedding the ISD into the Active Directory Service, an existing user management can be used to control the access to print resources efficiently.

Requirements

☑ The ISD was entered with a type A resource record (IPv4 address of the host) on the used DNS server.

Procedure

Follow the instructions to embed the ISD into an ADS:

□ Define the DNS server in the network; see: ⇨🗎43.

□ Define a time server, see: ⇨🗎44.

□ Define the ISD as a member of a domain; see: ⇨🗎51.

□ Define a printer administrator, see: ⇨🗎54.

Defining the ISD as Member of a Domain

☞ Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MS WINDOWS***.*
3. *Click* **Change***.*
4. *Mark the option* **Domain member***.*
5. *Click* **Next***.*
6. *Mark the option* **Join an Active Direcory domain***.*
7. *Click* **Next***.*

8. *Configure the network options; see: Table 11* ⇨🗎*52.*
9. *Click* **Next***.*
10. *Create a computer account for the ISD on the domain controller. To do this, you need administrator rights for the domain controller. Enter* **Administrator account** *and* **Password***.*

↳ The successful integration of the ISD into the Active Directory is confirmed.

Table 11: Networking Options - Member of an Active Directory

Parameters	Description
NetBIOS name	The ISD host name is used as NetBIOS name.
Active Directory domain name	Domain name. *Use the complete Active Directory domain name, e.g. 'MYDOMAIN.MYCOMPANY.COM' or 'thisdomain.local'*
Workgroup name	Name of the workgroup. *Usually, this is the NetBIOS domain name.*
Password server	IP address or host name of the password server. *Usually, this is the Windows domain controller.* *Multiple entries are to be separated by blanks.*
WINS server	IP address or host name of the WINS server (optional) *A WINS server must be specified to allow the communication between participants of different network segments.*

After embedding the ISD into the ADS, you must define the 'printer administrator' to grant administrative access from the Windows PC to the ISD.

6.2 How to Use an NTLM Authentication

NTLM authentication means that users will be authenticated by means of the 'Active Directory' or the 'NT 3.5x/4.0' domain controller.

Procedure

Follow the instructions to prepare for an NTLM authentication:

☐ Define the DNS server in the network; see: ⇨🗎43.

☐ Define a time server, see: ⇨🗎44.

☐ Define the use of the NTLM authentication; see: ⇨🗎53.

☐ Define a printer administrator, see: ⇨🗎54.

Defining the NTLM Authentication

☞ Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MS WINDOWS***.*
3. *Click* **Change***.*
4. *Mark the option* **Domain member***.*
5. *Click* **Next***.*
6. *Mark the option* **Use NTLM authentication***.*
7. *Click* **Next***.*
8. *Configure the network options; see: Table 12 ⇨🗎53.*
9. *Click* **Next***.*
10. *Create a computer account for the ISD on the domain controller. To do this, you need administrator rights for the domain controller. Enter* **Administrator account** *and* **Password***.*

↳ The settings are saved.

Table 12: Networking Options - Domain member (NTLM)

Parameters	Description
NetBIOS name	The ISD host name is used as NetBIOS name.
NetBIOS domain name	NetBIOS domain name

Parameters	Description
Password server	Password server *Enter '*' for the automatic search for the password server.*
WINS server	IP address or host name of the WINS server (optional) *A WINS server must be specified to allow the communication between participants of different network segments.*

After embedding the ISD into the ADS, you must define the 'printer administrator' to grant administrative access from the Windows PC to the ISD.

6.3 How to Define the Printer Administrator

In order to administer the ISD in an ADS environment (see: ⇨🖹51), you must create a Windows-specific account; the so-called 'printer administrator'. The printer administrator is selected from the directory service of the created 'users'.

Benefits and Purpose

The printer administrator is needed to install printer drivers in Windows networks and to change global printer settings. Without a printer administrator the administrative access to the ISD from a Windows PC is disabled.

Requirements

☑ The ISD is embedded into the ADS; see: ⇨🖹51.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MS WINDOWS – Printer Admin***.*
3. *Manually enter a* **user** *or a* **group**
   (- syntax for groups: '@DomainGroup')
   (- syntax for users: 'DomainUser')
   or select **Select account from list***.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

6.4 How to Define the ISD as a Stand-Alone Server

The ISD can be used as a stand-alone server in the network and can be equipped with an independent user administration. The printing services offered by the ISD will only be used by those users who have been authenticated by the local user management.

Procedure

Follow the instructions to prepare the ISD for a local authentication:

□ Define the ISD as a stand-alone server; see: ⇨🗎55.

□ Configure the local user management; see: ⇨🗎55.

Defining the ISD as a Stand-Alone Server

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MS WINDOWS***.*
3. *Click* **Change***.*
4. *Mark the option* **Stand-Alone server***.*
5. *Click* **Next***.*
6. *Enter a 'workgroup'.*
7. *Enter the IP address of the WINS server.*
8. *Click* **Next***.*

↳ The network settings will be adapted.

6.5 How to Configure the Local User Management

In the case of the local user management, users are created and equipped with passwords. Several users can be united in local groups.

Benefits and Purpose

The local user management is needed for the distribution of access rights if the ISD is used a stand-alone server. If the ISD is embedded into an ADS, the local user management can be used to generate additional access rights. The users are authenticated both by the ADS and the local user management.

The local user management is done via the ISD Control Center.

What do you want to do?

- □ 'Creating Users' ⇨🖹56
- □ 'Deleting Users' ⇨🖹56
- □ 'Changing the User Password' ⇨🖹57
- □ 'Assigning Users to a Group' ⇨🖹57
- □ 'Creating Groups' ⇨🖹57
- □ 'Deleting Groups' ⇨🖹58

Creating Users

Proceed as follows:

1. *Select* **MS WINDOWS – Local Users & Groups.**
2. *Select* **Create user***.*
3. *Enter the user name and password.*
   You cannot use system names (root, LP, sys, users...) as user and group names.
4. *Confirm the password.*
5. *Click* **Create***.*

↳ The setting is saved.

Deleting Users

Proceed as follows:

1. *Select* **MS WINDOWS – Local Users & Groups.**
2. *Mark a user in the list.*
3. *Select* **Delete user***.*

↳ The setting is saved.

Changing the User Password

☞ Proceed as follows:

1. *Select* **MS WINDOWS – Local Users & Groups.**
2. *Mark a user in the list.*
3. *Select* **Change password.**
4. *Enter a password.*
5. *Confirm the password.*
6. *Click* **Save** *to confirm.*

↳ The setting is saved.

Assigning Users to a Group

☞ Proceed as follows:

1. *Select* **MS WINDOWS – Local Users & Groups.**
2. *Mark a user in the list.*
3. *Select* **Set group membership***.*
4. *Assign the groups to the user.*
5. *Click* **Save** *to confirm.*

↳ The setting is saved.

Creating Groups

☞ Proceed as follows:

1. *Select* **MS WINDOWS – Local Users & Groups.**
2. *Select* **Local groups***.*
3. *Select* **Create group***.*
4. *Enter a group name.*
5. *Click* **Create***.*

↳ The setting is saved.

Deleting Groups

Proceed as follows:

1. *Select* **MS WINDOWS - Local Users & Groups.**
2. *Select* **Local groups***.*
3. *Select a group from the list.*
4. *Select* **Delete group***.*

↳ The setting is saved.

6.6 How to Configure Additional Windows Settings

You can configure additional Windows-specific settings.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MS WINDOWS – Miscellaneous.**
3. *Configure the required settings.*
4. *Click* **Save** *to confirm.*

↳ The setting is saved.

- *Backup share*:
  Allow access to backup images on the ISD via SMB.
- *Machine account*:
  Manual creation of a user account for the ISD if the ISD cannot be authenticated by a Windows 2000/2003 domain controller in the case of a configured NTLM authentication.
- *(Un)publish all installed queues in AD*:
  Enables/disables the display of queues in the Active Directory.
- *LDAP signing*:
  Enables an LDAP authentication.
- *NetBIOS name resolution file*:
  Allows to define lmhosts entries. lmhosts (LAN manager hosts) defines the assignment of IP addresses to NetBIOS names.
- *Disable domain user and group enumeration*:
  Disables the domain user and group enumeration. This increases the performance in large domains. You must enter the printer administrator manually.

7 Printer Driver Management

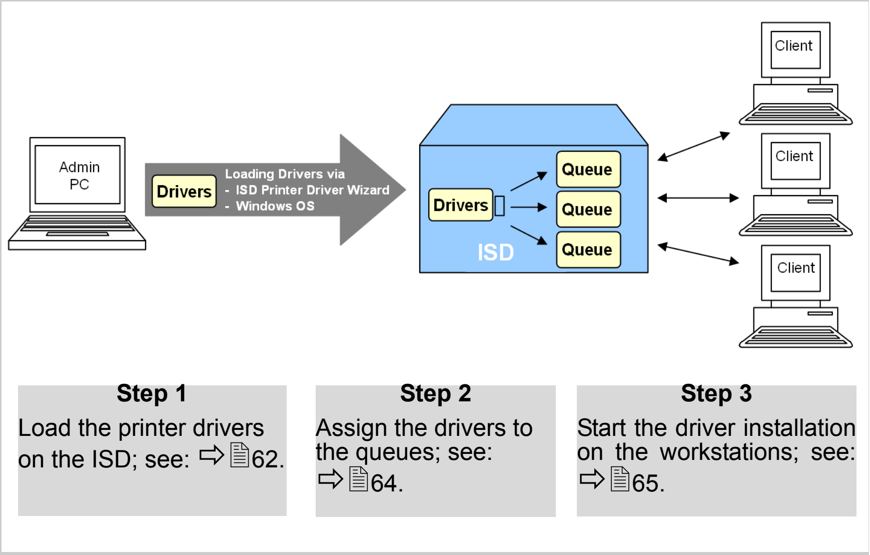
The ISD has a central printer driver management. This chapter describes how to distribute printer drivers with minimal effort.

In order to be able to print you must install the required printer driver on all workstations.

Point and Print

In heterogeneous Microsoft networks the automatic printer driver installation via 'Point and Print' is the most efficient way to load the drivers to the individual workstations. In addition you can centrally configure and manage driver settingsZudem lassen sich auch Treibereinstellungen (e.g. duplex, paper trays, etc.) or updates.

The ISD supports the Point-and-Print function developed by Microsoft for the central management of printer drivers. Store all required printer drivers on the ISD. The drivers will then be downloaded automatically to the individual workstations, if required.



Step 1
Load the printer drivers on the ISD; see: ⇨ 🗎62.

Step 2
Assign the drivers to the queues; see: ⇨ 🗎64.

Step 3
Start the driver installation on the workstations; see: ⇨ 🗎65.

Fig. 9: Point and Print

What information do you need?

- 'How to Save Printer Drivers on the ISD' ⇨🗎62
- 'How to Assign Printer Drivers to Queues' ⇨🗎64
- 'How to Initiate the Driver Installation on the Workstation (Point and Print)' ⇨🗎65
- 'How to Distribute Printer Drivers to several ISDs' ⇨🗎66
- 'How to Distribute Queues and Printer Drivers' ⇨🗎67

7.1 How to Save Printer Drivers on the ISD

The printer drivers can be saved to the ISD using the ISD Printer Driver Wizard or the Windows operating system.

ISD Printer Driver Wizard

The ISD Printer Driver Wizard simplifies the storing of printer drivers on the ISD by combining the required files for the installation and management of a printer driver. This package will then be loaded to the ISD. You will find the ISD Printer Driver Wizard at www.seh.de or on the ISD hard disk (see: 'Service Area' ⇨🗎12).

32-Bit / 64-Bit Version

The driver version to be loaded on the ISD by the ISD Printer Driver Wizard depends on the system on which the Wizard is installed.

- If you use a 64-Bit system the Wizard can only load 64-Bit drivers on the ISD.
- If you use a 32-Bit system the Wizard can only load 32-Bit drivers on the ISD.

The other driver version can be installed via Windows mechanisms (Remote Procedure Call, RPC).

For each operating system (used by the workstation) you must store the individual printer drivers on the ISD.

Universal Printer Driver

In heterogeneous networks, the use of UPD drivers (Universal Printer Driver) may be advisable. UPD drivers support various printer models of one printer manufacturer and are compatible with a number of operating systems. The ISD Printer Driver Wizard supports the installation of UPD drivers.

What do you want to do?

□ 'Saving Printer Drivers via the ISD Printer Driver Wizard' ⇨🗎63

□ 'Saving UPD Drivers via the ISD Printer Driver Wizard' ⇨🗎63

□ 'Saving Printer Drivers via the Windows Operating System' ⇨🗎64

Saving Printer Drivers via the ISD Printer Driver Wizard

The ISD Printer Driver Wizard helps you to install printer drivers on the ISD.

Requirements

☑ The ISD Printer Driver Wizard is installed on a Windows PC.

☑ You have administrative rights for the Windows PC.

☑ The current user of the Windows PC is specified as 'Printer Administrator' on the ISD; see: ⇨🗎54.

Proceed as follows:

1. *Start the ISD Printer Driver Wizard on the Windows PC.*
   (Start → Programs → SEH Computertechnik GmbH → ISD Printer Driver Wizard)
2. *Select the* **Printer Driver Installation** *mode.*
3. *Follow the installation routine.*

↳ The printer driver is saved on the ISD.

Saving UPD Drivers via the ISD Printer Driver Wizard

The ISD Printer Driver Wizard helps you to install UPD drivers on the ISD. When saving a UPD driver, a queue for the relevant printer will be created on the ISD.

Requirements

☑ The ISD Printer Driver Wizard is installed on a Windows PC.

☑ You have administrative rights for the Windows PC.

☑ The current user of the Windows PC is specified as 'Printer Administrator' on the ISD; see: ⇨🗎54.

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

Proceed as follows:

1. *Start the ISD Printer Driver Wizard on the Windows PC.*
   (Start → Programs → SEH Computertechnik GmbH → ISD Printer Driver Wizard)
2. *Select the* **Queue and Printer Driver Installation** *mode.*
3. *Follow the installation routine.*

↳ UPD driver and queue will be saved on the ISD.

Saving Printer Drivers via the Windows Operating System

The following description refers to the configuration in Windows 7. Depending on your Windows system, the menu navigation can vary.

Requirements

☑ You have administrative rights for the Windows PC.

☑ The current user of the Windows PC is specified as 'Printer Administrator' on the ISD; see: ⇨🗎54.

Proceed as follows:

1. *Start the Windows PC.*
2. *Enter the IP address of the ISD into the start menu search box.*
   Syntax: \\<IP address of the ISD>
   The connection will be established.
3. *Mark the ISD.*
4. *Select* **Server Properties...** *from the shortcut menu.*
   The dialog **Print Server Properties** *opens.*
5. *Select the* **Drivers** *tab.*
6. *Click* **Add**.
   The Add Printer Driver Wizard is started.
7. *Follow the installation routine.*

↳ The printer driver is saved on the ISD.

7.2 How to Assign Printer Drivers to Queues

Via the ISD Control Center you can assign Windows printer drivers to queues.

Requirements

☑ Windows printer drivers are stored on the ISD; see: ⇨🗎62.

☑ Queues are created on the ISD; see: ⇨🗎72.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MS WINDOWS - Drivers**.
3. *Mark the queues you want to assign a printer driver to.*

4. *Select a printer driver from the 'Available' list.*
5. *Click* **OK***.*

↳ The settings are saved.

7.3 How to Initiate the Driver Installation on the Workstation (Point and Print)

This section describes the final step of 'Point and Print'. In this step the assigned printer driver will be installed automatically on the workstation.

ℹ The following description refers to the configuration in Windows 7. Depending on your Windows system, the menu navigation can vary.

Requirements

☑ The workstation must be part of the domain; see: ⇨🗎50.

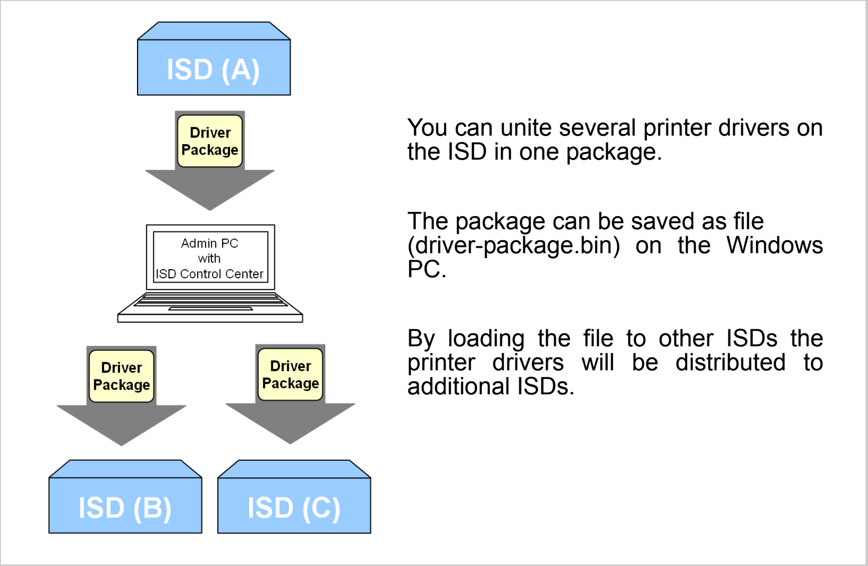
☞ Proceed as follows:

1. *Start the workstation.*
2. *Enter the IP address of the ISD into the start menu search box.*
   Syntax: \\<IP address of the ISD>
   The connection will be established.
3. *Mark the queue.*
4. *Select* **Connect...** *from the shortcut menu.*

↳ The printer driver will be saved on the workstation.

7.4 How to Distribute Printer Drivers to several ISDs

It is usually a great effort if printer drivers must be distributed to several ISDs in large networks. The ISD Control Center offers the following solution for an effective distribution of the printer drivers.



You can unite several printer drivers on the ISD in one package.

The package can be saved as file (driver-package.bin) on the Windows PC.

By loading the file to other ISDs the printer drivers will be distributed to additional ISDs.

Fig. 10: Distribution of printer driver packages

Requirements

☑ Windows printer drivers are stored on the ISD; see: ⇨🗎62.

Proceed as follows:

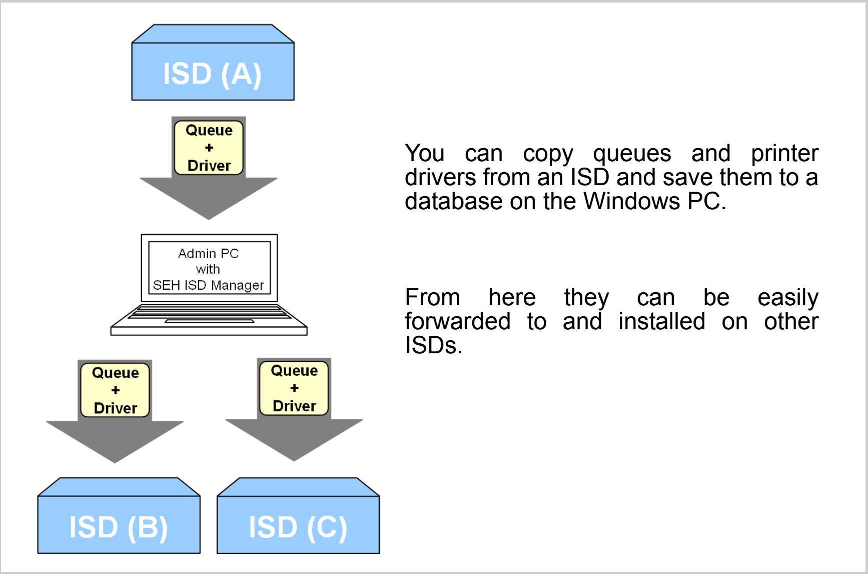
1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MS WINDOWS – Drivers***.*
3. *Click* **Create driver package***.*
4. *Select the printer drivers from the 'Available drivers' list.*
5. *Click* **Create***.*
   The file 'driver-package.bin' will be created on the ISD.
6. *Click* **Download driver package***.*
7. *Save the file 'driver-package.bin' on the Windows PC.*
8. *Start the ISD Control Center of the ISD that will get the drivers from the package.*

9. *Install the file 'driver-package.bin'; see: 'How to Uninstall/Install Software Modules' ⇨🗎109.*

↳ The drivers will be installed on the ISD.

7.5 How to Distribute Queues and Printer Drivers

It is usually a great effort if queues and printer drivers must be distributed to several ISDs in large networks. The SEH ISD Manager offers the following solution for an efficient distribution of queues and printer drivers.



You can copy queues and printer drivers from an ISD and save them to a database on the Windows PC.

From here they can be easily forwarded to and installed on other ISDs.

Fig. 11: Distribution of queues and printer drivers

Requirements

☑ Queues and Windows printer drivers are stored on the ISD; see: ⇨🗎62.

☑ The SEH ISD Manager is installed on the PC; see: ⇨🗎19.

Duplicating Queues and Drivers

Copy queues and printer drivers to the database of the SEH ISD Manager.

Proceed as follows:

1. *Start the SEH ISD Manager.*
2. *Mark the ISD in the list.*
3. *Select* **Action – Duplicate Queues and Drivers** *from the menu bar.*
4. *Mark the queues and drivers to be duplicated.*
   Via the option 'Select assigned drivers automatically' you can automatically select all drivers assigned to a queue.
5. *Click Save.*

↳ The selected queues and drivers will be copied to the database.

Installing Queues and Drivers

Install the queues and drivers to one or more ISD(s).

Proceed as follows:

1. *Start the SEH ISD Manager.*
2. *Mark the ISDs in the list.*
3. *Select* **Action – Install Queues and Drivers** *from the menu bar.*
4. *Click* **Select***.*
5. *Mark the queues and drivers to be installed.*
   Via the option 'Select assigned drivers automatically' you can automatically select all drivers assigned to a queue.
6. *Click* **OK***.*
7. *Click* **Install***.*

↳ The selected queues and drivers will be installed on the ISD(s).

For further information; see: 'Administration via the SEH ISD Manager' ⇨🗎19 and the Program Online Help.

8 Print Queues

The ISD offers numerous features for the management of queues. This chapter provides an overview.

The ISD offers a central and efficient management of queues. You can create a large number of queues on the ISD. The queues use different protocols to send the print data. You can also create queues with special functions.

Table 13: Queue Types

Queue Type	Description
Socket/ HP JetDirect	The queue supports printing via direct TCP/IP ports. During socket printing, the ISD acts as network connection for a printer which is independent of a client. The ports can be installed on the client with the aid of the SEH Print Monitor. When creating the queue, the printer will be specified by its IP address or host name. You must also specify the TCP/IP port.
LPD	The queue supports printing via the LPD (Line Printer Daemon) protocol. During LPD printing the print data is sent to the IP address of the printer by means of the LPR port. When creating the queue, the printer will be specified by its IP address or host name. You must also specify the ’remote device’. (Note: In the case of SEH print servers, the remote device is defined via the logical printer lp1 - lp8).
IPP	The queue supports printing via the IPP (Internet Printing Protocol) protocol. When the queue is created, the IPP device will be specified via the device URI (Uniform Device Identificator); see: Table 15 ⇨ 🗎72.
Balance queue	The balance queue is a virtual queue that represents a group of printers and that distributes the print jobs according to the availability of the printers. For further information; see: ⇨ 🗎75.
Copy queue	The copy queue is a virtual queue that represents a group of printers. The copy queue copies incoming print jobs and automatically sends them to the group members. The print job will then be printed on several printers. For further information; see: ⇨ 🗎74.

What information do you need?

- 'How to Find Queues in the Network' ⇨🗎71
- 'How to Create a Queue (Socket/LPD/IPP)' ⇨🗎72
- 'How to Create a Copy Queue' ⇨🗎74
- 'How to Create a Balance Queue' ⇨🗎75
- 'How to Modify a Queue' ⇨🗎76
- 'How to Define Queue Settings (Drivers/TCP Port/ThinPrint®)' ⇨🗎76
- 'How to Delete a Queue' ⇨🗎77
- 'How to Test a Queue (Printing a Test Page)' ⇨🗎77
- 'How to Enable/Disable a Queue' ⇨🗎78
- 'How to Reject/Allow Print Jobs' ⇨🗎78
- 'How to Assign a Filter Application to a Queue' ⇨🗎79

8.1 How to Find Queues in the Network

The ISD Control Center offers an automatic methode for finding network printers in the network.

During the Quick Setup all network printers and print servers that are available in the network will be identified via automatic detection routines and displayed as queues. To use the Quick Setup, see: ⇨🗎48.

You can also use the detection routine when creating queues.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS - Create Queue***.*
3. *Configure the parameters* **Queue name**, **Description**, *and* **Location***.*
4. *Click* **Next***.*
5. *Select* **Search Network Printer** *from the list.*
6. *Configure the parameters; see: Table 14 ⇨🗎71.*
7. *Click* **Next***.*

↳ The ISD searches the defined network range via SNMP and displays the detected printers and print servers in a list.

If a device is selected, the printing method (TCP/IP socket, or LPD) will be assigned automatically depending on the network card.

Table 14: Queue search parameters

Parameters	Description
Start IP address	Defines the start IP address of the network range for the search for printers in the network. You can search a maximum of 255 IP addresses.
End IP address	Defines the end IP address of the network range.
Resolve IP addresses	Enables/disables the name resolution via a DNS server.
Select from database	Displays the search result from the network scans.

8.2 How to Create a Queue (Socket/LPD/IPP)

Queues can be created automatically or manually.

Creating Queues Automatically

During the Quick Setup all network printers and print servers that are available in the network will be identified via automatic detection routines and displayed as queues. To use the Quick Setup, see: ⇨🗎48.

Creating Queues Manually

Printers and print servers that are not detected automatically or that have been installed at a later date, can be added manually.

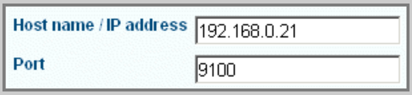
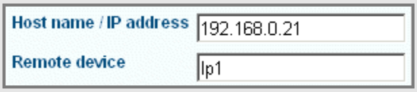
Proceed as follows:

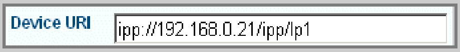
1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS – Create Queue***.*
3. *Configure the parameters; see: Table 15 ⇨🗎72.*
4. *Click* **Next***.*
5. *Select the queue type.*
6. *Click* **Next***.*
7. *Enter the settings of the connected printer.*
8. *Click* **Next***.*
9. *Click* **OK** *to confirm.*

↳ The settings are saved.

Table 15: Parameter – Queue

Parameters	Description
Create Queue - Step 1	
Queue name	Queue Name Note the following conventions: - letters, numbers, hyphens and underscores are allowed - no space characters are allowed - do not use more than 32 characters (Windows 98 max. 15 characters)
Description	Printer description (optional)
Location	Printer location (optional)
Create Queue - Step 2	
Queue type	Defines the queue type; see: ⇨🗎69.

Parameters	Description
Create Queue - Step 3 *The parameters that are displayed depend on the chosen queue type.*	
Socket/ HP JetDirect	Description: Host name or IP address as well as port of the printer / print server. Example*:  Host name / IP address: 192.168.0.21 Port: 9100 Syntax*: `<hostname>:port number`
LPD	Description: Host name or IP address of the printer / print server. You must also specify the ’remote device’. (Note: In the case of SEH print servers, the remote device is defined via the logical printer lp1 - lp8**). Example*:  Host name / IP address: 192.168.0.21 Remote device: lp1 Syntax*: `<hostname>/<logical printer>`

IPP	Description:
	When IPP is used, the devices will be identified by the device URI (Uniform Device Identificator).
	
	Example*:
	
	Device URI: ipp://192.168.0.21/ipp/lp1
	
	Syntax*:
	Transmission of unencrypted data
	`http://<ip-address>:631/ipp/<logical printer>`
	`ipp://<ip-address>/ipp/<logical printer>`
	
	Transmission of encrypted data
	`https://<ip-address>/ipp/<logical printer>`
	
	<ip-address> = IP address or host name of the end device
	<logical printer> = logical printer (lp1 - lp8) **

Balance Queue	Defines the queues that are members of the ’balance queue’.
Copy Queue	Defines the queues that are members of the ’copy queue’.

Parameters	Description
Search Network Printer	Defines an address range that is searched for connected printers. You can search a maximum of 255 IP addresses. Search results from the network scans will not be deleted and can be displayed via ’Select from data base’.

* Example and syntax describe an application scenario where the print data is sent from the ISD to an SEH print server. If you use an end device (printer, print server, etc.) of a different manufacturer, you will need a different syntax. For further information, contact the manufacturer of the end device.

** The logical printer defines the printer port to which the print data is sent. If no logical printer is defined, the logical printer no. 1 will be used automatically.

8.3 How to Create a Copy Queue

You can copy print jobs and print them to several printers at a time. To this purpose a so-called copy queue is configured on the ISD.

The copy queue copies an incoming print job and automatically sends it to the previously configured queues. The print job will then be printed on several printers. When creating the copy queue, you must specify the queues involved.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS – Create Queue***.*
3. *Configure the parameters* **Queue name**, **Description**, *and* **Location***.*
4. *Click* **Next***.*
5. *Select* **Copy Queue** *as queue type.*
6. *Click* **Next***.*
7. *Select the queues that are to automatically receive copies of print jobs from the copy queue.*
8. *Click* **Next***.*
9. *Click* **OK** *to confirm.*

↳ The copy queue will be created on the ISD.

8.4 How to Create a Balance Queue

The balance queue is a virtual queue that represents a group of printers and that distributes the print jobs according to the availability of the printers. When creating the balance queue, you must specify the queues involved.

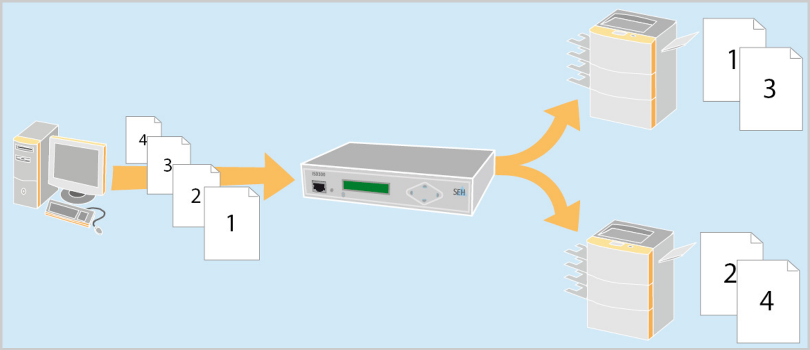


Fig. 12: Balance Queue

Benefits and Purpose

The balance queue helps you to distribute print jobs to the available printers. Large print jobs can be processed faster even if one of the involved printing systems becomes unavailable.

When creating the balance queue, you must specify the queues involved.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS – Create Queue***.*
3. *Configure the parameters* **Queue name**, **Description**, *and* **Location***.*
4. *Click* **Next***.*
5. *Select* **Balance Queue** *as queue type.*
6. *Click* **Next***.*
7. *Select the queues that are part of the balance queue.*
8. *Click* **Next***.*
9. *Click* **OK** *to confirm.*

↳ The copy queue will be created on the ISD.

8.5 How to Modify a Queue

You can change the queue properties later on.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Modify** *for the relevant queue.*
4. *Configure the parameters; see: Table 15 ⇨ 72.*
5. *Click* **Next**.
6. *Select the queue type.*
7. *Click* **Next**.
8. *Enter the settings of the connected printer.*
9. *Click* **Next**.
10. *Click* **OK** *to confirm.*

↳ The settings are saved.

8.6 How to Define Queue Settings (Drivers/TCP Port/ThinPrint®)

You can define the queue settings. This way, Windows drivers, TCP ports, and ThinPrint® parameters can be reassigned or changed.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Settings** *for the relevant queue.*
4. *Define the settings.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

8.7 How to Delete a Queue

You can delete a queue.

ℹ All print jobs that are assigned to the queue will also be deleted.

☞ Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Settings** *for the queue to be deleted.*
4. *Mark 'Delete queue' in the* **Actions** *list.*
5. *Click* **OK** *to confirm.*

↳ The queue will be deleted.

8.8 How to Test a Queue (Printing a Test Page)

You can print a test page to check the queue and printer.

☞ Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Settings** *from the list.*
4. *Mark 'Print ASCII test page' or 'Print PostScript test page' in the* **Actions** *list.*
5. *Click* **OK** *to confirm.*

↳ The test page is printed.

8.9 How to Enable/Disable a Queue

You can disable a queue and process the pending print jobs at a later stage. The incoming print jobs will then be collected in a queue and processed one after the other once the queue has been activated.

Benefits and Purpose

It makes sense to interrupt a queue if the connected printer is temporarily unavailable or the printing is to take place outside office hours so that employees will not be disturbed by noise emissions.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Settings** *for the relevant queue.*
4. *Mark 'Start' or 'Stop' in the* **Actions** *list.*
5. *Click* **OK** *to confirm.*

↳ The setting is saved.

8.10 How to Reject/Allow Print Jobs

You can define a queue in such a way that it rejects print jobs. Incoming print jobs will not be accepted. Print jobs contained in the queue will be processed.

Benefits and Purpose

It makes sense to interrupt print jobs if the connected printer will be temporarily unavailable due to maintenance activities.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Settings** *for the relevant queue.*
4. *Mark 'Reject jobs' or 'Accept jobs' in the* **Actions** *list.*
5. *Click* **OK** *to confirm.*

↳ The setting is saved.

8.11 How to Assign a Filter Application to a Queue

The ISD supports specific, printing related software solutions provided by third parties (e.g. barcode printing). This way the ISD can be adapted to individual environments and requirements in an ideal way.

Requirements

☑ The filter application is installed on the ISD. To install a filter application on the ISD; see: ⇨🗎109.

☞ Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Settings** *for the relevant queue.*
4. *Select* **Filter.**
5. *Mark a filter in the 'Available' list.*
6. *Click* **Add**.
7. *Click* **OK** *to confirm.*

↳ The settings are saved.

9 Print Jobs

The ISD offers numerous features for the management of print jobs. This chapter provides an overview.

The ISD offers a central and efficient management of print jobs.

What information do you need?

- 'How to Delete Print Jobs' ⇨🗎80
- 'How to Hold/Restart Print Jobs' ⇨🗎81
- 'How to Prioritize Print Jobs' ⇨🗎81
- 'How to Move Jobs to other Queues' ⇨🗎82
- 'How to Store Jobs in a Queue' ⇨🗎82
- 'How to Manage Print Jobs in the Repository' ⇨🗎83

9.1 How to Delete Print Jobs

You can delete the print jobs in a queue.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Jobs** *from the list.*
4. *Mark a print job.*
5. *Select the action* **Delete** *from the 'Select an action' list.*
6. *Click* **OK** *to confirm.*

↳ The print job is deleted.

The action **Delete all** deletes all print jobs within a queue.

9.2 How to Hold/Restart Print Jobs

You can hold and restart the processing of print jobs.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Jobs** *from the list.*
4. *Mark a print job.*
5. *Select the action* **Hold**, **Release** , *or* **Restart** *from the 'Select an action' list.*
6. *Click* **OK** *to confirm.*

↳ The print job will be stopped or restarted.

9.3 How to Prioritize Print Jobs

You can manually move print jobs within a queue in order to process print jobs faster.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Jobs** *from the list.*
4. *Mark a print job.*
5. *Select the action* **Move to top** *from the 'Select an action' list.*
6. *Click* **OK** *to confirm.*

↳ The print job will be given priority.

9.4 How to Move Jobs to other Queues

If a print job is within a queue whose printer is not operational, the print job can be moved to a different queue.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Jobs** *from the list.*
4. *Mark a print job.*
5. *Select a queue from the 'Move jobs to queue' list.*
6. *Click* **OK** *to confirm.*

↳ The print job will be moved to the selected queue.

9.5 How to Store Jobs in a Queue

You can store print jobs in a queue. The print file will be stored in a queue and can be printed easily at any time.

Benefits and Purpose

Storing print jobs in a queue reduces network traffic because frequent files do not need to be sent again and again.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Jobs** *from the list.*
4. *Select* **Job Storing**.
5. *Mark the option* **Keep printed jobs in the queue**.
6. *Click* **Save** *to confirm.*

↳ The settings are saved.

9.6 How to Manage Print Jobs in the Repository

The repository is a defined area on the hard disk of the ISD. You can store print jobs in the repository. Print jobs will be loaded and stored in the repository either directly or via a queue.

If required, a print file (print job) can be selected from the repository and can be assigned to a queue for printing.

Benefits and Purpose

Storing print jobs in the repository reduces network traffic because frequent files do not need to be sent again and again.

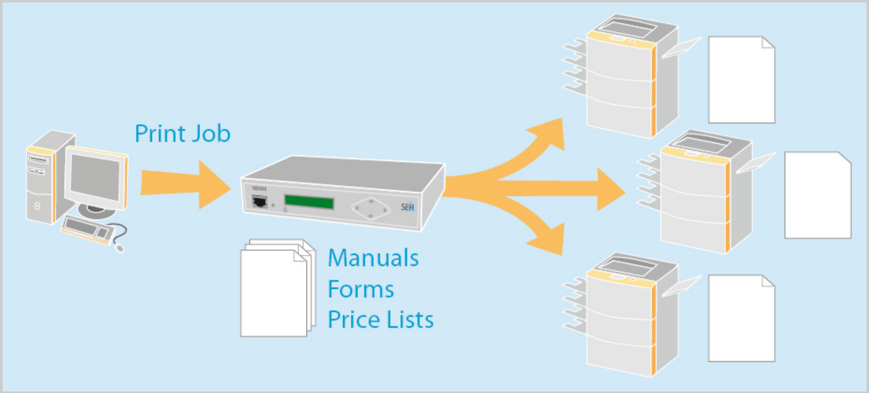


Fig. 13: Repository

What do you want to do?

- □ 'Loading Print Jobs to the Repository via a Queue' ⇨🗎84
- □ 'Uploading Print Files Directly to the Repository' ⇨🗎84
- □ 'Printing Files from the Repository' ⇨🗎84
- □ 'Deleting Files from the Repository' ⇨🗎85

Loading Print Jobs to the Repository via a Queue

The print jobs contained in a queue can be stored automatically to a repository.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Jobs** *from the list.*
4. *Select* **Job Storing.**
5. *Mark the option* **Store printed jobs in the repository**.
6. *Click* **Save** *to confirm.*

↳ All jobs that are printed via the queue will be stored in the repository.

Uploading Print Files Directly to the Repository

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS – Repository**.
3. *Click* **Browse...** *in the* **Add file** *window.*
4. *Select the print file.*
5. *Click* **Add**.

↳ The print file will be stored in the repository.

Printing Files from the Repository

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS – Repository**.
3. *Mark a print file.*
4. *Select a queue from the list.*
5. *Click* **Print**.

↳ The file will be printed via the selected queue.

Deleting Files from the Repository

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS – Repository***.*
3. *Mark a print file.*
4. *Click* **Delete***.*

↳ The file will be deleted.

10 Security

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

What information do you need?

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

- 'How to Control the Access to the ISD Control Center' ⇨🖹87
- 'How to Control the Access to the ISD Operating Panel' ⇨🖹91
- 'How to Control the Access to Queues' ⇨🖹93
- 'How to Use Certificates Correctly' ⇨🖹94
- 'How to Block Ports' ⇨🖹102

More security-related topics from other chapters:

- Encrypted ThinPrint® print data; see: ⇨🖹122.
- Encrypted print data for IPP printing; see: ⇨🖹26.
- Encrypted print data for socket printing; see:⇨🖹24
- User Management via the Windows Active Directory; see ⇨🖹50.
- Protect the ISD via Internet Protocol Security (IPsec); see ⇨🖹128.

10.1 How to Control the Access to the ISD Control Center

You can protect the administrative access to the ISD Control Center by user profiles.

User Profiles

Access to the ISD Control Center is granted to the user profiles 'Any', 'User', and 'Admin'. You will also need a password. The table shows which access rights are assigned to the different user profiles.

Table 16: User Profiles

User Profile	Access rights	Password
Any	- calling status information about queues and print jobs	*no password required*
User	- calling status information about queues and print jobs - managing own print jobs, e.g. deleting, halting print jobs, changing priority *(These access rights are defined by the administrator.)*	user *(default)*
Admin	- calling status information - setting up and administrating queues - deleting, halting, and changing priority of all print jobs - installation, configuration, and maintenance of the ISD	admin *(default)*

User name and password are transferred in an unencrypted way during the login. You can use certificates for an encrypted connection (SSL); see: ⇨🗎94.

Failed Login Attempts

Failed login attempts are logged and can be displayed. The admin can receive information about the failed login attempts, if necessary.

Session Timeout

Session timeout means that the connection to the ISD Control Center will be terminated for security reasons after a period of inactivity.

What do you want to do?

- □ 'Changing the Password of a User Profile' ⇨🗎88
- □ 'Defining Access Rights for the User Profile 'User'' ⇨🗎89
- □ 'Getting Information about Failed Login Attempts' ⇨🗎90
- □ 'Defining the Session Timeout' ⇨🗎90

Changing the Password of a User Profile

Upon delivery the ISD has the passwords listed in the table; see: 'User Profiles' ⇨🗎87.

Change the default passwords when you use the ISD in a real situation.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION - Password***.*
3. *Under* **Login account***, select the user profile of which you want to change the password.*
4. *Enter the current password into the* **Old password** *box.*
   (Only required if the password of the user profile 'Admin' will be changed.)
5. *Enter the new password in the* **New password** *box.*
   (4 to 30 characters [a-z, A-Z, 0-9])
6. *Repeat the passwords.*
7. *Click* **Save** *to confirm.*

↳ The setting is saved.

If the password is no longer available, it can be reset by means of the ISD operating panel; see ⇨🗎113. To protect the ISD operating panel against unauthorized access; see ⇨🗎91.

Defining Access Rights for the User Profile 'User'

The user profile 'User' specifies the access rights for handling print jobs. The administrator determines

- who (what user)
- can execute certain actions (e.g. deleting, halting, etc.)

print jobs.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION - Access Rights***.*
3. *Tick the desired options; see: Table 17 ⇨ 89.*
4. *Click* **Save** *to confirm.*

↳ The setting is saved.

Table 17: Parameter - Access Rights

Parameters	Description
Rights apply to all hosts	Specifies the hosts (users) for which the access rights apply. enabled: The rights apply to all hosts. All print jobs can be managed by all users. disabled: The rights only apply to the sender host of the respective print job. Users can only manage their own print jobs.
Prioritize	Allows to change the priority of print jobs within a queue.
Move jobs to other queues	Allows to move print jobs between queues.
Delete all jobs	Allows to delete all print jobs.
Hold/Release jobs	Allows to hold and release print jobs.
Print jobs from repository	Allows to print jobs from the repository.

Getting Information about Failed Login Attempts

You can view the log containing the failed login attempts.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION - Session Management***.*

↳ The log is displayed.

If required, a freely definable number of failed login attempts will result in an automatic notification via email.

Requirements

☑ The notification service has been configured; see: ⇨🗎46.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION - Session Management***.*
3. *Tick* **Notification***.*
4. *In the* **Failed login attempts** *box, enter the number of failed login attempts that will result in a notification.*
5. *Click* **Save** *to confirm.*

↳ The setting is saved.

Defining the Session Timeout

Session timeout means that the connection to the ISD Control Center will be terminated for security reasons after a period of inactivity. The user will be logged out and has to log on again. Set the time period for the session timeout.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION - Session Management***.*
3. *Tick* **Session Timeout***.*
4. *Enter the interval (in minutes) into the* **Period** *box.*
5. *Click* **Save** *to confirm.*

↳ The setting is saved.

10.2 How to Control the Access to the ISD Operating Panel

You can protect the operating panel at the front of The ISD against unauthorized access by means of a 4-digit PIN. The administrator defines the PIN via the ISD Conrol Center.

If the operating panel is protected, you must enter the PIN via the navigation keys. The control panel will be protected again after each operation.

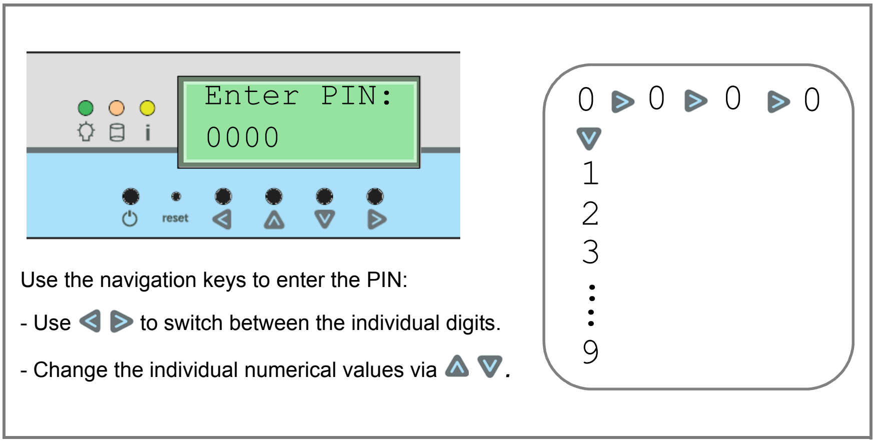
What do you want to do?

□ 'Entering the Panel Lock PIN' ⇨🗎92

□ 'Setting the Panel Lock PIN' ⇨🗎92

Entering the Panel Lock PIN

If the control panel is protected, the message ‘Enter PIN’ will appear when the navigation keys are pressed.



Use the navigation keys to enter the PIN:

- Use ◁ ▷ to switch between the individual digits.

- Change the individual numerical values via △ ▽.

Fig. 14: ISD Device – Panel Lock

If the PIN is no longer available, it can be reset by means of the ISD Control Center; see ⇨🗎92. To protect the ISD Control Center against unauthorized access; see ⇨🗎87.

Setting the Panel Lock PIN

The PIN is preset to '0000'. Using these default settings, the control panel is not protected.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION – Password***.*
3. *Enter the* **PIN***.*
4. *Confirm by clicking* **Save***.*

↳ The setting is saved.

10.3 How to Control the Access to Queues

You can control and restrict the access to the queues and their related printers to certain clients.

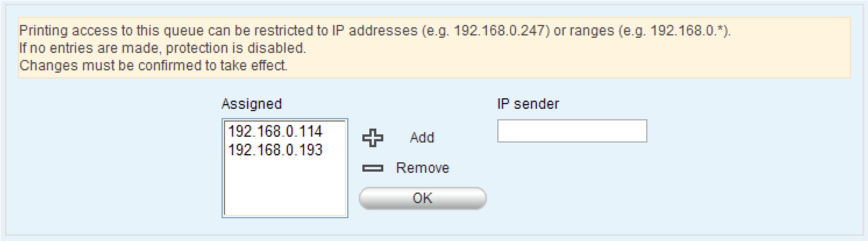
To enable the IP sender access control, you must enter the IP addresses of the clients into an IP sender list. The queue will only accept print jobs from clients specified in the list. The use of wildcards (*) allows you to define subnetworks and to authorize these subnetworks for accessing queues.

Once an IP sender has been defined, all undefined clients lose their authorization to print via the queue. The IP sender access control cannot control access via SMB.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS.**
3. *Select* **Settings***.*
4. *Select* **Protection***.*
5. *Enter the IP address in the* **IP sender** *box.*
6. *Click* **Add***.*
7. *Confirm your entries.*

↳ The settings are saved.



Printing access to this queue can be restricted to IP addresses (e.g. 192.168.0.247) or ranges (e.g. 192.168.0.*).
If no entries are made, protection is disabled.
Changes must be confirmed to take effect.

Assigned
192.168.0.114
192.168.0.193

IP sender

Fig. 15: ISD Control Center – Queue Access Control

10.4 How to Use Certificates Correctly

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

What are Certificates?

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

Benefits and Purpose

The use of certificates allows for various security mechanisms. Use certificates on the ISD

- to receive encrypted ThinPrint print data; see: ⇨🗎126.
- to receive encrypted print data when using HTTPs printing (TCP/IP); see: ⇨🗎24.
- to authenticate the ISD/client if the administrative access to the ISD Control Center is protected via HTTPs (SSL); see: ⇨🗎99.
- to allow for a certificate-based authentication of the remote server in the case of IPsec; see: ⇨🗎128.

If you want to use certificates, it is advisable to protect the administrative access to the ISD Control Center by a password so that the certificate on the ISD cannot be deleted by unauthorized persons; see: ⇨🗎87.

Which Certificates are available?

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

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

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

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

Upon delivery, a certificate (the so-called **default certificate)** is stored in the ISD. It is recommended that you replace the default certificate by a self-signed certificate or CA certificate as soon as possible.

What do you want to do?

□ 'Creating a Self-Signed Certificate' ⇨🗎96

□ 'Creating a Certificate Request for CA Certificates' ⇨🗎97

□ 'Saving the CA Certificate in the ISD' ⇨🗎98

□ 'PKCS12 Saving the Certificate on the ISD' ⇨🗎98

□ 'Deleting Certificates' ⇨🗎99

□ 'Installing Certificates on Windows Clients' ⇨🗎99

Creating a Self-Signed Certificate

If a self-signed certificate or a CA certificate has already been saved in the ISD, the content of this certificate will be displayed. In this case you have to delete the existing certificate first; see: ⇨🗎99.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE - Certificates***.*
3. *Enter the relevant parameters, see: Table 18 ⇨🗎96.*
4. *Mark the option* **Self-signed certificate***.*
5. *Click* **Create***.*

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

Table 18: Certificate Features

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 ISD to allow a clear assignment of the certificate to the ISD. You can enter a maximum of 64 characters.
Email address	Specifies an email address. You can enter a maximum of 40 characters. (Optional Entry)
Organization name	Specifies the company that uses the ISD. You can enter a maximum of 64 characters.
Organizational unit	Specifies the department or subsection of a company. You can enter a maximum of 64 characters. (Optional Entry)
Locality name	Specifies the locality where the company is based. You can enter a maximum of 64 characters.
State name	Specifies the state in which the company is based. You can enter a maximum of 64 characters. (Optional Entry)
Country name	Specifies the country in which the company is based. Enter the two-digit country code according to ISO 3166. Examples: DE = Germany, GB = Great Britain, US = USA
Issued on	Specifies the date after which the certificate is valid.
Expires on	Specifies the date after which the certificate is invalid.

Creating a Certificate Request for CA Certificates

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

If a self-signed certificate or a CA certificate has already been saved in the ISD, the content of this certificate will be displayed. In this case you have to delete the existing certificate first; see: ⇨🗎99.

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

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE - Certificates***.*
3. *Enter the relevant parameters, see: Table 18 ⇨🗎96.*
4. *Select* **Create certificate request***.*
5. *Click* **Create***.*
   The creation of the certificate request is in progress. This may take a few minutes.
6. *Confirm your entries.*
7. *Save the request as text file.*
8. *Send the text file as certificate request to a certification authority.*

When the CA certificate has been received, it must be saved in the ISD; see: 'Saving the CA Certificate in the ISD' ⇨🗎98.

Saving the CA Certificate in the ISD

Requirements

☑ The certificate must be in base 64 format.

☞ Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE – Certificates***.*
3. *Click* **Browse...***.*
4. *Specify the CA certificate.*
5. *Click* **Load***.*
6. *Confirm your entries.*

↳ The CA certificate is saved in the ISD.

PKCS12 Saving the Certificate on the ISD

Certificates with the PKCS12 format are used to save private keys and their respective certificates and to protect them by means of a password.

Requirements

☑ The certificate must be in base 64 format.

☞ Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE – Certificates***.*
3. *Select* **Load certificate (PKCS#12 format)***.*
4. *Click* **Browse...***.*
5. *Enter the certificate.*
6. *Enter the password.*
7. *Click* **Load***.*
8. *Confirm your entries.*

↳ The PKCS12 certificate is saved in the ISD.

Deleting Certificates

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE - Certificates**
3. *Click* **Delete**.

↳ The certificate is deleted.

Installing Certificates on Windows Clients

Why do I need Certificates on the Client?

The following cases require a certificate on the client:

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

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

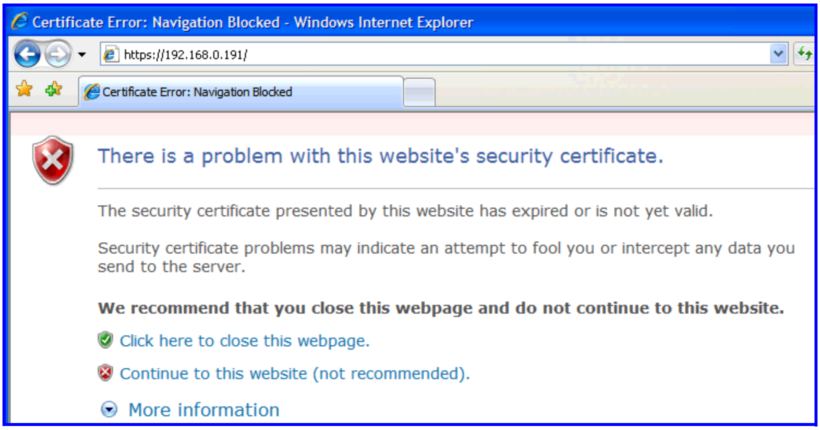
If a certificate is unknown to the Windows client, the certificate is not classed as 'trusted'. In this case, you will get an error message. Install the certificate on the Windows client using a browser in order to make the certificate known to the client.

Example

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

Proceed as follows:

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


Certificate Error: Navigation Blocked - Windows Internet Explorer

https://192.168.0.191/

Certificate Error: Navigation Blocked

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

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

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

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

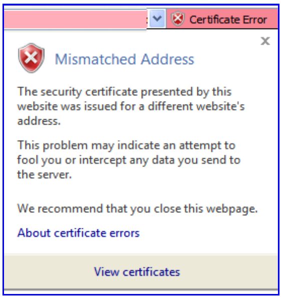
Click here to close this webpage.

Continue to this website (not recommended).

More information

Fig. 16: Internet Explorer – Security Alert

2. *Click* **Continue to this website**.
   A note (certificate error) is displayed.


Certificate Error

Mismatched Address

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

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

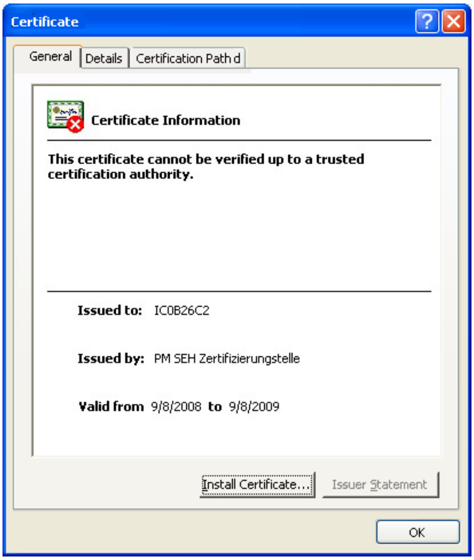
We recommend that you close this webpage.

About certificate errors

View certificates

Fig. 17: Internet Explorer – Alert

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



Certificate Information

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

Issued to: IC0B26C2

Issued by: PM SEH Zertifizierungstelle

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

Fig. 18: Internet Explorer – Certificate

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

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

10.5 How to Block Ports

You can block the access to ports on the ISD.

Benefits and Purpose

Port attacks directly address the relevant services or protocols and take advantage of their weak points. The blocking of ports protects the ISD against attacks.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **CONFIGURATION – Port Blocking**.
3. *Mark the ports to be blocked.*
4. *Click* **Save** *to confirm.*

↳ The setting is saved.

If you block a port, all TCP services that use this port will be disabled.

Table 19: TCP Services and Ports

Service name	Port
Discard	TCP 9
SMB - NETBIOS-SSN - MICROSOFT-DS	 TCP 139 TCP 445
LPR	TCP 515
ThinPrint®	Freely definable (default: TCP 4000)
IPP	TCP 631
HTTP(s) Printing - HTTP - HTTPS	 TCP 80 TCP 443
Socket (RAW) Printing	TCP 9100 - 9107
SNMP	UDP 163
Service Location Protocol	Multicast Port 427

11 Maintenance

A number of maintenance activities can be carried out on the ISD. This chapter contains information about the backup management and the implementation of software modules. You will also learn how to carry out a restart and a device update.

What information do you need?

- 'How to Manage Backup Images' ⇨🖹104
- 'How to Restart the ISD' ⇨🖹115
- 'How to Uninstall/Install Software Modules' ⇨🖹109
- 'How to Use the Diagnostics Function' ⇨🖹111
- 'How to Reset ISD Parameters to their Default Values' ⇨🖹112
- 'How to Reset the Passwort' ⇨🖹113
- 'How to Carry out an Update' ⇨🖹114
- 'How to Restart the ISD' ⇨🖹115

11.1 How to Manage Backup Images

You can save an ISD's configuration settings to an image. The image files can be created manually or automatically. The image files can additionally be saved to the PC.

The image file name contains the creation date (yyyy-mm-dd format) and the host name of the ISD. You can save up to seven images in the ISD. The oldest images will be deleted automatically, if needed. (First in - First Out)

What does a Backup Image contain?

A Backup Image contains the following:

- drivers and queues
- ISD-specific settings
  (e.g. TCP/IP settings, port lockings, etc.)
- settings related to the user management
  (user profile, access rights, and passwords)
- DNS and DHCP settings

Benefits and Purpose

If required, you can use an image to implement a system restore in real time. You can also use images to quickly pass on configuration settings to other ISDs.

The SEH ISD Manager supports backup management with advanced features. For further information; see: 'Administration via the SEH ISD Manager' ⇨🗎19.

What do you want to do?

□ 'Creating a Backup Image manually' ⇨🗎105

□ 'Creating a Backup Image automatically' ⇨🗎105

□ 'Deleting Backup Images' ⇨🗎106

□ 'Storing a Backup Image on a Local Computer' ⇨🗎106

□ 'Installing Backup Images on the ISD' ⇨🗎106

Creating a Backup Image manually

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE - Backup***.*
3. *Click* **Create now***.*

↳ The backup image is stored on the ISD.

Creating a Backup Image automatically

You can create automatic backups in defined time intervals. To do this, you must define the weekday and time range in which the backup will start. (24 hour format; e.g. 22-02)

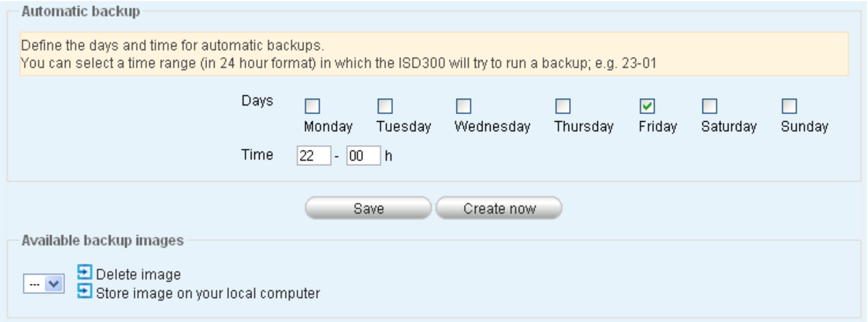
Requirements

☑ The device time has been configured correctly on the ISD; see: ⇨ 🗎44.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE - Backup***.*
3. *Mark the days, on which a backup image is to be created.*
4. *Enter the time range.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.



Automatic backup

Define the days and time for automatic backups.
You can select a time range (in 24 hour format) in which the ISD300 will try to run a backup; e.g. 23-01

Days: ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☑ Friday ☐ Saturday ☐ Sunday

Time: 22 - 00 h

Fig. 19: ISD Control Center - Backup

Deleting Backup Images

Image files that are no longer needed should be deleted from the ISD.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE - Backup**.
3. *Mark the image in the list* **Available backup images.**
4. *Select* **Delete image**.

↳ The backup image will be deleted.

Storing a Backup Image on a Local Computer

Image files should be copied to a local computer in regular intervals.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE - Backup**.
3. *Mark the image in the list* **Available backup images.**
4. *Select* **Store image on your local computer**.
5. *Choose a location and click* **Save**.

↳ The backup image is stored on the local computer.

Installing Backup Images on the ISD

A backup image can be copied from a local computer (location) to the ISD at any time.

The procedure for loading an image to the ISD is identical to the installation of software modules. For further information; see: 'How to Uninstall/Install Software Modules' ⇨🗎109.

11.2 How to Use the RAID Function

The ISD410 comes with an integrated RAID system. The integrated RAID system increases the reliability and availability of the ISD410. All data will be saved redundantly to two hard disks. Should one of the hard disks fail, the ISD410 will remain fully operational.

The RAID function is only available for the ISD410. All required settings are preconfigured.

What do you want to do?

- □ 'ISD Displaying the RAID Status' ⇨🗎107
- □ 'Verifying ISD Hard Disks' ⇨🗎108
- □ 'ISD Hard Disks Rebuilding Data Synchrony' ⇨🗎108

ISD Displaying the RAID Status

The RAID status is displayed in the ISD Control Center on the 'Statusinfo' page.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE – Status**.

↳ The RAID status will be displayed.

Table 20: RAID Status

Parameters	Description
OK	The RAID system works perfectly
Rebuilding	Rebuilds the data synchrony
Initializing	Initialization of the hard disks
Verifying	Checks the hard disks for redundancy
Migrating	Adoption of changed RAID settings
Degraded	Missing data synchrony of the hard disks
Inoperable	Hard disk is not recognized

The status 'Degraded' or 'Inoperable' describes an incorrect behaviour of a hard disk in the ISD. Please contact the SEH support team.

When statuses change, you can get notifications via email or SNMP traps. To configure automatic notifications, see: ⇨🗎33.

Verifying ISD Hard Disks

You can check the hard disks in the ISD for redundancy.

☞ Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* MAINTENANCE - RAID*.*
3. *Mark the option* Verify*.*
4. *Click* Next*.*
5. *Click* Verify*.*

↳ The hard disks of the ISD will be verified.

ISD Hard Disks Rebuilding Data Synchrony

The hard disks of the ISD are monitored by a RAID system; see: RAID Status ⇨🗎107. If the hard disk of the ISD does not work properly, you may have to exchange the hard disk. Please contact the SEH support team.

The 'Rebuild' function is implemented in the ISD Control Center to synchronize an exchanged hard disk with a faultless hard disk.

Only use the 'Rebuild' function after consultation with the SEH support team.

11.3 How to Uninstall/Install Software Modules

You can install different kinds of software modules to the ISD. A software module can be, for example:

- a software file (see: 'Update' ⇨🗎114)
- a 3rd party software (see: 'Filter Application' ⇨🗎127)
- an image file (see: 'Backup' ⇨🗎106)

By means of the SEH ISD Manager you can install a software module to several ISDs at a time. For further information; see: 'Administration via the SEH ISD Manager' ⇨🗎19.

What do you want to do?

□ 'Installing Software Modules' ⇨🗎109

□ 'Uninstalling Software Modules' ⇨🗎110

Installing Software Modules

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE – Software**.
3. *Mark the option* **Install software**.
4. *Click* **Next**.
5. *Click* **Browse...**.
6. *Select the software file.*
7. *Click* **Next**.
   The file is downloaded to the ISD.
8. *Click* **Next**.
   The software module will be installed on the ISD.
9. *Confirm your entries.*

↳ The software module will be installed. If required, the ISD will restart automatically to activate the software module.

Uninstalling Software Modules

You can uninstall software modules from the ISD.

☞ Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE - Software**.
3. *Mark the option* **Remove software**.
4. *Click* **Next**.
5. *Mark the module that is to be deleted from the* **Available ressources** *list.*
6. *Click* **Delete**.
7. *Confirm your entries.*

↳ The software module will be uninstalled.

11.4 How to Use the Diagnostics Function

The Diagnostics function is divided into three tabs that allow for a detailed verification of the ISD system.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* MAINTENANCE – Diagnostics*.*
3. *Select a tab.*

Log Files

The tab allows you to:

- view, filter, update and delete log entries
- save log entries as a compressed file (support.tar)
- send log entries to a mail recipient

Advanced Status

The tab contains:

- network information
- memory information
- task information

Expert Mode

You can configure certain settings (e.g. Cups, Samba, Kernel, etc.) via the Expert Mode. The Expert Mode is undocumented and can only be used after consultation with the SEH support team.

These settings can only be configured by qualified admins and after consultation with the SEH support team. Incorrect settings may result in a misbehavior of the system.

11.5 How to Reset ISD Parameters to their Default Values

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

ℹ

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

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

You can reset the parameters via the device front.

☞ Proceed as follows:

1. *Press 2 x ▽. The display shows:*

   ```
    Default Settings
    Press >
   ```

2. *Press the button ▷. The display shows:*

   ```
    Press V to
   Reset Parameters
   ```

3. *Press the button ▽.*

↳ The parameters are reset.

11.6 How to Reset the Passwort

You can protect the administrative access to the ISD Control Center by means of a password; see: ⇨🗎87. If the password is no longer available, it can be reset.

This is done via the ISD operating panel at the front of the device.

Proceed as follows:

1. *Press 3 x ▽. The display shows:*

   ```
    Password Reset
    Press >
   ```

2. *Press the button ▷. The display shows:*

   ```
    Press V to
   Reset Password
   ```

3. *Press the button ▽.*

↳ The password will be reset.

11.7 How to Carry out an Update

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

What Happens during an Update?

In the course of an update, the existing software will be overwritten and replaced by a new version. The parameter default settings of the device remain unchanged.

When Is an Update Recommended?

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

Check the installed software version on the ISD. The version number can be found in the ISD Control Center.

Where Do I Find the Update Files?

You can download the current software files at www.seh.de.

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

An update is carried out by installing the software files to the ISD. The procedure is identical to the installation of software modules. To carry out a update; see: 'Installing Software Modules' ⇨🗎109.

11.8 How to Restart the ISD

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

By means of the SEH ISD Manager you can carry out a reboot of several ISDs at a time.

What do you want to do?

□ 'Rebooting the ISD via the ISD Control Center' ⇨🗎115

□ 'Rebooting the ISD via the SEH ISD Manager' ⇨🗎115

□ 'Hard Rebooting the ISD via the Device Front' ⇨🗎116

Rebooting the ISD via the ISD Control Center

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **MAINTENANCE – Restart**.
3. *Click* **Restart**.

↳ The ISD will be rebooted.

Rebooting the ISD via the SEH ISD Manager

You can carry out a reboot for one or several ISDs at a time.

Proceed as follows:

1. *Start the SEH ISD Manager* ⇨🗎*19.*
2. *Mark the ISDs in the list.*
3. *Select* **Action – Reboot** *from the menu bar. A password prompt appears.*
4. *Enter the password and click* **OK** *to confirm. (optional)*

↳ The ISDs will be rebooted.

Hard Rebooting the ISD via the Device Front

A hard reboot (also known as a cold reboot or cold start) is when power to the ISD is cycled (turned off and then on).

Restart

Insert a sharp item (e.g. a paper clip) into the hole and press the reset button.

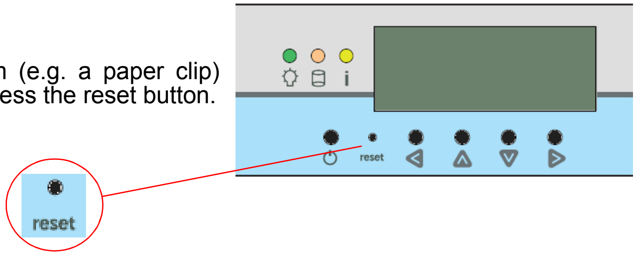


Fig. 20: ISD Device – ISD reboot

12 Additional Features

In addition to the basic features of print spooling, the ISD offers further useful functions. This chapter describes the available functions and how they can be used efficiently.

What information do you need?

- 'How to Use the ISD as DHCP Server' ⇨🗎118
- 'How to Use the ISD as DNS Server' ⇨🗎120
- 'How to Use the ISD as ThinPrint® Gateway' ⇨🗎122
- 'How to Use Filter Applications' ⇨🗎127

12.1 How to Use the ISD as DHCP Server

The ISD comes with an integrated DHCP server. DHCP servers are used for the automatic assignment of IP addresses within a network.

Benefits and Purpose

DHCP (Dynamic Host Configuration Protocol) provides clients with network configuration. The main information to be provided is the IP address. To this purpose, the client sends its request for an IP address to the network. A 'qualified' DHCP server answers this request and the client obtains its IP address.

The functional range of the DHCP server that is included in the delivery was planned for small to medium corporate network as well as branch and remote offices.

Procedure

Follow the instructions to make use of DHCP in your network:

□ 'Configuring the DHCP Server' ⇨🗎118

□ 'Starting/Stopping the DHCP/DNS Server' ⇨🗎121

Configuring the DHCP Server

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **DHCP & DNS***.*
3. *Select* **Configure DHCP server***.*
4. *Configure the parameters; see: Table 21 ⇨🗎119.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

If the DNS/DHCP server is switched on, the changes will become effective after the reboot of the DNS/DHCP server. Select **Apply Changes** from the **DHCP & DNS** menu.

Table 21: Parameter - DHCP Server

Parameters	Description
Address ranges	
Start IP address End IP address	The network ranges define the upper and lower limit of the IP addresses to be assigned. Specify the ranges via a 'Start IP address' and an 'End IP address'. Up to four ranges can be specified. Note: The network ranges must be within the maximum IP range. This range is specified by the gateway.
Fixed IP addresses	
- MAC Address - IP Address - Hostname	Static IP addresses and host names can be assigned to a maximum of ten hosts via the DHCP server. The hosts are specified by the MAC address.
DHCP options *These settings apply to all specified IP ranges and hosts.* *Multiple server addresses are to be separated by commas.*	
Lease time	A lease time is the length of time that a DHCP server specifies that a client computer can use an assigned IP address. Can be defined as hours or minutes. Select 'infinite' for an unlimited validity.
Subnet mask	Defines the subnet mask that is assigned to a client together with the IP address.
Broadcast address	Broadcast address
Default routers	IP address of the default router
DNS servers	IP address of the DNS server
DNS domain name	Defines the DNS domain name that is assigned to the clients for the DNS host name resolution.
GMT Time offset	Time zone adjustment in seconds
NTP servers	IP address of the NTP time server
SMTP servers	IP address of the SMTP server
POP3 servers	IP address of the POP3 server
WINS servers	IP address of the WINS server
NetBIOS node type	The node type defines the strategy to be used for the name resolution (b-node, p-node, m-node, h-node).

You can view the lease information of the DHCP server. Select **View leases file.**

12.2 How to Use the ISD as DNS Server

The ISD comes with an integrated DNS server. DNS (Domain Name System) is a service that translates domain names into IP addresses. Using DNS, names can be assigned to IP addresses and vice versa.

Benefits and Purpose

DNS is very helpful in particular since names are retained a lot easier than multiple digits numbers, i.e. Smith's PC instead of 192.168.0.231. In addition, DNS allows for more flexibility since names may be assigned independent of IP addresses, therefore, enabling names to be changed or assigned to a different IP address at any time.

The functional range of the DNS server that is included in the delivery was planned for small to medium corporate network as well as branch and remote offices.

Procedure

Follow the instructions to make use of the DNS service:

□ 'Configuring the DNS Server' ⇨🗎120

□ 'Starting/Stopping the DHCP/DNS Server' ⇨🗎121

Configuring the DNS Server

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin.'*
2. *Select* **DHCP & DNS**.
3. *Select* **Configure DNS server**.
4. *Configure the parameters; see: Table 22* ⇨🗎*121.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

If the DNS/DHCP server is switched on, the changes will become effective after the reboot of the DNS/DHCP server. Select **Apply Changes** from the **DHCP & DNS** menu.

Table 22: Parameter - DNS Server

Parameters	Description
Master DNS servers	IP address of the master DNS server. *All requests to the ISD that cannot be answered locally or by the servers for local domains are forwarded to the master server. Up to 300 answers from the master servers are cached by the ISD.*
Forward Zones	IP address and domain name of a local DNS server (e.g. localdomain 192.168.22.11). *All requests to local domains served by other local DNS servers can be forwarded to this local DNS servers. This option can be used to keep network traffic away from external master servers.*
Master Zones	DNS request to domains specified here are not forwarded to other servers. If the request cannot be resolved locally, the requesting client receives an error message.

Starting/Stopping the DHCP/DNS Server

After the DHCP or DNS settings have been configured, the DHCP/DNS server can be started.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **DHCP & DNS**.
3. *Click* **Start/Stop Server**.

↳ The DHCP/DNS server is started/stopped.

In order to start the server during the system boot automatically, enable the **Yes** option and click **Save**.

12.3 How to Use the ISD as ThinPrint® Gateway

The ISD comes with an integrated ThinPrint® client.

What is ThinPrint®?

The ThinPrint® technology enables the transmission of compressed and bandwidth-optimized print jobs within a network. Used as ThinPrint® gateway, the ISD can receive and decompress print jobs that have been compressed by means of ThinPrint®.

As ThinPrint® gateway the ISD supports the ThinPrint functions 'AutoConnect' and 'Connection Service'.

The ISD also supports the ThinPrint® SSL encryption of print data. This way the ISD can unencrypt encrypted print jobs and send them to the relevant printer.

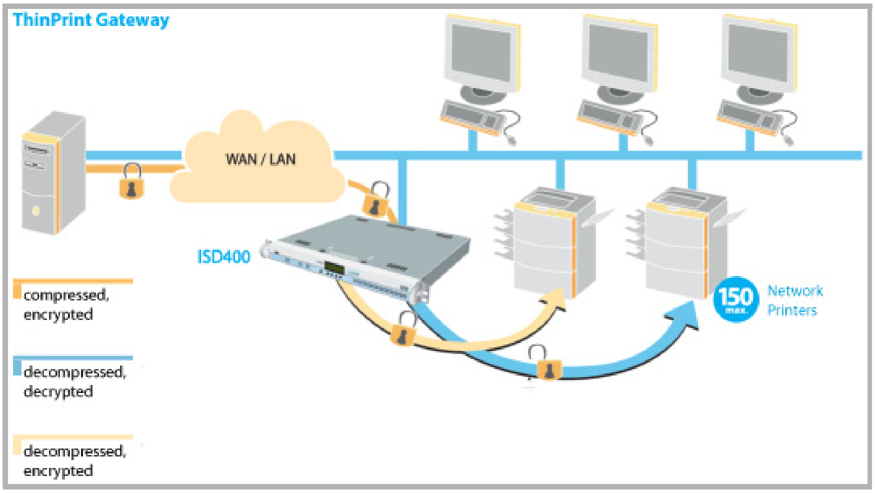


Fig. 21: ISD as ThinPrint® Gateway

What do you want to do?

- □ 'Configuring ThinPrint® Parameters' ⇨🗎123
- □ 'Using the ThinPrint® Connection Service' ⇨🗎125
- □ 'Receiving Encrypted ThinPrint® Data' ⇨🗎126

Configuring ThinPrint® Parameters

In order for the ISD to communicate with the ThinPrint® server (.print Engine) via a port and to receive print jobs, you must adapt various parameters.

ThinPrint® Port Number

In ThinPrint® environments, printing is done to a TCP/IP port via a socket connection. The port number of the ISD must be identical to the port number that was defined for the ThinPrint® server. Port 4000 is preset. You can change the port number, if necessary.

Bandwidth

Bandwidth describes the capacity of a data connection. The bandwidth of the ISD 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 ISD (client side).

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

Printer ID

Print jobs are sent from the ThinPrint® server to the ISD. After the decompression of the print jobs, the ISD forwards the data to the printers. The print jobs are assigned via a printer ID. A large number of network printers can be connected to the ThinPrint® port which is defined via the ISD.

.print AutoConnect

.print AutoConnect is a tool within the .print technology for the automatic creation of print objects. The print objects are created on the basis of defined templates without the need to automatically load the printer drivers.

Printers can be combined in printer groups and printer locations on the basis of so-called printer classes. A name table translation (Dynamic Printer Matrix) simplifies the creation of classes and the assignment of printers.

In the case of several drivers we recommend the assignment of the appropriate printer drivers via the printer class. This assignment can be set up accordingly in the printer configuration on the .print client.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS – ThinPrint®***.*
3. *Configure the parameters; see: Table 23 ⇨🗎124.*
4. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 23: Parameter – ThinPrint®

Parameters	Description
ThinPrint® port	ThinPrint® port number *(allowed entry: 1 - 65535 | default = 4000)*
Bandwidth	Enables/disables the bandwidth value of the ThinPrint® port (client side). The bandwidth is indicated in bit/second (bit/s). *(allowed entry: 1600 - -1000000 | default = 25600)*
Default queue	Defines the default queue. ThinPrint® print jobs without ID are redirected to the default queue. Print jobs with ID that have not been assigned or that are outside the range will not be accepted.
ID	The ID clearly identifies the printers for the ThinPrint® server. *(allowed entry: 1 - 65536)*
Class	Printers with compatible drivers can be arranged in one class. You can also define a printer class if you want to use the .print AutoConnect feature.
Driver	Printer driver for the embedded printer. You can also define a printer class if you want to use the .print AutoConnect feature.

Using the ThinPrint® Connection Service

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

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

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

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

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **QUEUES & JOBS – ThinPrint®***.*
3. *Select* **Connection Service***.*
4. *Configure the parameters; see: Table 24 ⇨🗎125.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 24: Parameter – ThinPrint® Connection Service

Parameters	Description
Connection Service	Enables/disables the .print Connection Service
Connection Server	IP address of the server on which the Connection Service is installed.
Port	Port number used by the ISD to communicate with the Connection Service (default = 4001)
Client ID	Client ID as stored in the database of the Connection Service. The client ID is needed by the Connection Service to forward print jobs to the ISD.

Parameters	Description
Keep alive	Interval (in seconds) for refreshing the connection to the Connection Service. The value has to be lower or equal than the 'KeepAliveTO' parameter of the .print Connection Service (server side). *(allowed entry: 30 - 180 | default = 60)*
Authentication key	Authentication key as stored in the database of the Connection Service.
Connection retry	Interval (in seconds) for connection retries if the Connection Service is not reachable. *(allowed entry: 5 - 6000 | default = 300)*

Receiving Encrypted ThinPrint® Data

A secure connection during the transfer of print jobs between ThinPrint® (server or Connection Service) and the ISD is guaranteed by means of an SSL encryption.

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

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

- Create a certificate request; see: 'Creating a Certificate Request for CA Certificates' ⇨🗎97.
- Save the CA certificate; see: 'Saving the CA Certificate in the ISD' ⇨🗎98.

12.4 How to Use Filter Applications

The ISD supports specific, printing related software solutions provided by third parties (e.g. barcode printing). This way the ISD can be adapted to individual environments and requirements in an ideal way.

Procedure

Follow the instructions to make use of filter applications:

□ Install a filter application on the ISD; see: 'How to Uninstall/Install Software Modules' ⇨🗎109.

□ Assign the filter application to a queue; see: ⇨🗎79.

13 Internet Protocol Security (IPsec)

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

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 25: Components of an IPsec policy

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

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

Security Association

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

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

- authentication method of the participants (pre-shared key or certificate)
- key algorithm to be used for the IPsec connection (see: Table 29 ⇨🗎141)
- 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 ISD establishes contact with the remote server.

In the so-called 'main mode' the ISD 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 ISD and remote server have specified the SA parameters, the IP data packets that are to be encrypted will be sent by the SA together with the ESP protocol (or the AH protocol).

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

IPsec Structure and Procedure

The kernel has two databases for the use of IPsec.

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

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

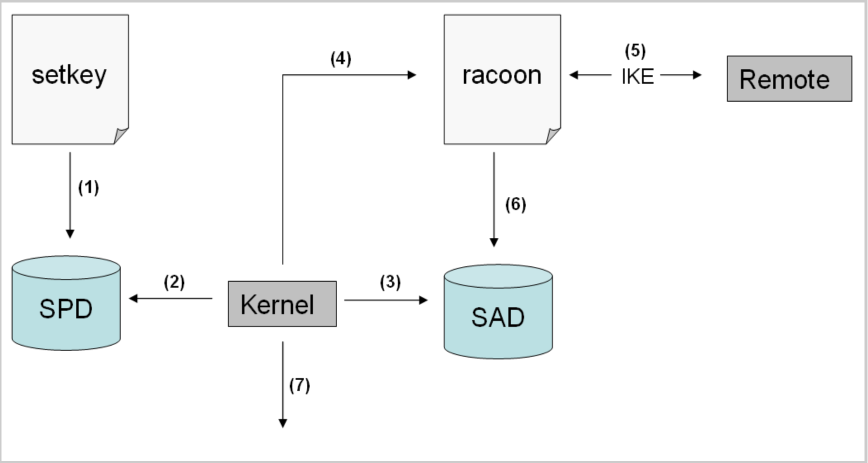


Fig. 22: IPsec Procedure

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

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

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

Tasks of the ISD

The ISD offers to ways to implement IPsec policies including SA:

- You can create an IPsec policy via the ISD Control Center. An input mask assists you in defining the rules.
- Via the ISD Control Center you can import IPsec policies as ready-made configuration files (racoon/setkey) to the ISD.

Only one IPsec policy can be active at a time.

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

What information do you need?

- 'How to Create IPsec Rules' ⇨🗎133
- 'How to Use IPsec Configuration Files' ⇨🗎142
- 'How to Define Exceptions' ⇨🗎145
- 'How to Enable IPsec Policies' ⇨🗎146

13.1 How to Create IPsec Rules

This section describes the creation of IPsec rules via the input mask of the ISD Control Center.

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 ISD. The existing IPv4 address of the ISD will be used and cannot be changed at this point. IPv6 addresses can be defined via an address template.
- *Remote IP address:* Addresses in the format IPv4 and IPv6 are supported. You can also specify IP address ranges. IP addresses and ranges can be stored in address templates and added to a rule.
- *Services:* Specifies the services that are used by an IP data packet. A service includes the protocol to be used and its port. Several protocols can be summarized in one service template and stored using a freely definable name.

Action

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

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

SA

If an IP data packet is forwarded via a 'Security Association' you must specify the SA parameters via an SA template. An SA template contains information about the authentication and the key exchange. To exchange keys, parameters have been specified in the IKE template.

Rules and Priority

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

Exclusiveness of the IP Addresses

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

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

Rule Numbers

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

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

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

What do you want to do?

□ 'Creating IPsec Rules' ⇨🗎136

□ 'Enabling IPsec Rules' ⇨🗎136

□ 'Defining Address Templates' ⇨🗎136

□ 'Defining Service Templates' ⇨🗎138

□ 'Defining SA Templates' ⇨🗎139

□ 'Defining IKE Templates' ⇨🗎140

Creating IPsec Rules

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

☞ Proceed as follows:

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

↳ The settings are saved.

Enabling IPsec Rules

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

ℹ

Afterwards you must enable the entire IPsec policy for the rules to take effect; see: ⇨🗎146.

Defining Address Templates

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

Three address templates are implemented by default. You can specify another twelve templates, if required.

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

Please use static IP addresses only.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin.'*
2. *Select* **Configuration – IPsec**.
3. *Select* **Edit rules**.
4. *Select* **Edit address templates.**
5. *Specify the address template; see: Table 26* ⇨🗎*137.*
6. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 26: Address Template Parameters

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

Defining Service Templates

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

The service template 'All services' comprises all protocols and is implemented by default. You can specify another twelve templates, if required.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Edit rules***.*
4. *Select* **Edit service templates.**
5. *Select the number of the template to be edited from the selection list in the path.*
6. *Specify the service template; see: Table 27 ⇨🗎138.*
7. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 27: Service Template Parameters

Parameter	Description
Name	Name of the service template. *You can enter a maximum of 16 characters.*
ICMP	Internet Control Message Protocol
HTTP	Hypertext Transfer Protocol
HTTPs	Hypertext Transfer Protocol secure
SNTP	Simple Network Time Protocol
SNMP	Simple Network Management Protocol
IPP	Internet Printing Protocol
Socket printing	Socket printing
LPR	Line Printer Remote

Parameter	Description
ThinPrint	ThinPrint® enables the transmission of compressed and bandwidth-optimized print jobs within a network.
SMB	Server Message Block

Defining SA Templates

An SA template contains information about the authentication as well as the key exchange between the ISD and the remote server.

You can specify twelve templates, if required.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Edit rules***.*
4. *Select* **Edit SA templates.**
5. *Select the number of the template to be edited from the selection list in the path.*
6. *Specify the SA template; see: Table 28 ⇨🗎139.*
7. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 28: SA Template Parameters

Parameter	Description
Name	Name of the IPsec template. *You can enter a maximum of 16 characters.*
Authentication type	Specifies the procedure for the authentication of the remote server. *Two procedures are available:* *- authentication via pre-shared key* *- authentication via certificates.* (For the installation of certificates on the ISD; see: ⇨🗎94.)

Parameter	Description
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 ISD).* - *Enabled: A root certificate is required for the authentication.*
Pre-Shared Key	Specifies the Pre-Shared Key (PSK). *You need the key if the ’Pre-Shared Key’ procedure has been selected as ’Authentication type’.* *You can enter a maximum of 16 characters.*
IKE	Specifies the template to be used for the automatic key exchange.

Defining IKE Templates

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

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

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Edit rules***.*
4. *Select* **Edit SA templates.**
5. *Select* **Edit IKE templates.**
6. *Select the number of the template to be edited from the selection list in the path.*
7. *Specify the IKE template; see: Table 29 ⇨🗎141.*
8. *Click* **Save** *to confirm.*

↳ The settings are saved.

Table 29: IKE Template Parameters

Parameter	Description
Name	Name of the IKE template. *You can enter a maximum of 16 characters.*
	- Phase 1 - **IKE Phase 1 establishes a secure channel.**
Negotiation	Specifies the procedure for the negotiation of the encryption and authentication. - In the ’Main Mode’ individual connections will be successively established for the individual steps (key exchange etc.). - In the ’Aggressive Mode’ individual steps of the Main Mode will be summarized (faster but less secure). *You can select several procedures. Only the most secure procedure will be applied. If a procedure fails, a less complicated (and therefore less secure) procedure will be used.*
Diffie-Hellman group	Specifies the Diffie-Hellman group number for the creation of dynamically generated temporary keys. The keys are used during the negotiation.
Encryption algorithm	Specifies the encryption algorithm to be used during the negotiation.
Hash algorithm	Specifies the Hash algorithm to be used during the negotiation.
IKE SA lifetime	Specifies the duration of the IKE connection in seconds. When the IKE SA lifetime expires, a re-authentication is required. (optional) *(min. 600 sec / max. 4294967295 sec)*
	- Phase 2 - **IKE phase 2 negotiates the encryption and integrity parameters used to secure the data packet to be transferred.**
- Phase 2 - Encapsulation type	Specifies how the IP data packet is handled within the SA. The IPsec specification differentiates between the ’Transport Mode’ and the ’Tunnel Mode’. - In the Transport Mode the IP data packet is encrypted. However, the IP header will be kept. - In the Tunnel Mode a complete IP data packet will be encapsulated in another packet and be given a new IP header. *NOTE: The Tunnel Mode cannot be selected via the selection list of the ISD Conrol Center. Use a configuration file (racoon/setkey) instead.*

Parameter	Description
Diffie-Hellman group	Specifies the Diffie-Hellman group number for the creation of additional dynamically generated temporary keys. The keys are used during phase 2. (optional)
Encryption algorithm	Specifies the encryption code for phase 2.
Authentication algorithm	Specifies the Hash algorithm for phase 2.
With AH protocol	Specifies the use of the ’Authentication Header’ protocol for the protection of the packet integrity and packet authentication. *AH uses the authentication header to authenticate the packet. In the IP data packet, the authentication header will be added after the IP header.*
IPsec SA lifetime	Specifies the duration of the IPsec SA connection in seconds. When the IPsec SA lifetime expires, you have to renew the IPsec key. *(min. 600 sec / max. 4294967295 sec)*

13.2 How to Use IPsec Configuration Files

In order to prepare the ISD 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.

What do you want to do?

□ 'Creating IPsec Configuration Files' ⇨🗎143

□ 'Importing IPsec Configuration Files' ⇨🗎144

□ 'Importing the Pre-Shared Key' ⇨🗎144

□ 'Importing Certificates' ⇨🗎144

Creating IPsec Configuration Files

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

Example

```
path certificate "/etc/isd";

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

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

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

Importing IPsec Configuration Files

You must load the files to the ISD so that the values of configuration files 'setkey.conf' or 'racoon.conf' can be applied.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin.'*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Load files***.*
4. *Click* **Browse***.*
5. *Select the configuration file.*
6. *Click* **Load***.*
7. *Click* **Save** *to confirm.*

↳ The settings of the configuration file will be saved.

Importing the Pre-Shared Key

If the authentication method 'Pre-Shared Key' is used for an SA (see: Table 28 ⇨🗎139) the pre-shared key must be saved in the ISD.

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin.'*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Load files***.*
4. *Next to Preshared keys file click* **Browse...***.*
5. *Select the file.*
6. *Click* **Load***.*
7. *Click* **Save** *to confirm.*

↳ The pre-shared key is loaded.

Importing Certificates

If an authentication via certificates is used for the SA (see: Table 28 ⇨🗎139), you must save certificates in the ISD. To save certificates; see: ⇨🗎94.

13.3 How to Define Exceptions

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

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

Proceed as follows:

1. *Start the ISD Control Center with the user profile 'Admin'.*
2. *Select* **Configuration – IPsec***.*
3. *Select* **Edit rules***.*
4. *Enable the relevant protocols under 'IPsec exceptions'.*
5. *Click* **Save** *to confirm.*

↳ The settings are saved.

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

13.4 How to Enable IPsec Policies

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

Test Mode

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

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

Proceed as follows:

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

If you can no longer access the device, initiate a hard reboot (⇨🗎115) of the device and modify the IPsec policy.

8. *Deactivate the* **Test mode***.*
9. *Click* **Save** *to confirm.*

↳ IP traffic will be allowed based on the rules defined in the IPsec policy.

14 Appendix

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

What information do you need?

14.1 Glossary

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

What information do you need?

Manufacturer-Specific Software Solutions

- 'ISD Control Center' ⇨🗎149
- 'SEH ISD Manager' ⇨🗎149
- 'SEH Print Monitor' ⇨🗎149
- 'ISD Printer Driver Wizard' ⇨🗎149

Network Technology

- 'Hardware Address' ⇨🗎150
- 'IP Address' ⇨🗎150
- 'Host Name' ⇨🗎151
- 'Gateway' ⇨🗎151
- 'Subnet Mask' ⇨🗎151
- 'Default Name' ⇨🗎151

ISD Control Center

The ISD Control Center is a user interface for the administration of the ISD. The ISD Control Center is stored in the ISD and can be displayed on a PC by means of an Internet browser (Internet Explorer, Netscape, Firefox, Safari).

SEH ISD Manager

The SEH ISD Manager is a software application developed by SEH Computertechnik GmbH to simplify the administration of ISDs. The SEH ISD Manager offers the following functions to assist you in various operations:

- Monitoring
- Backup and Update Management
- Queues and Driver
- Reboot

SEH Print Monitor

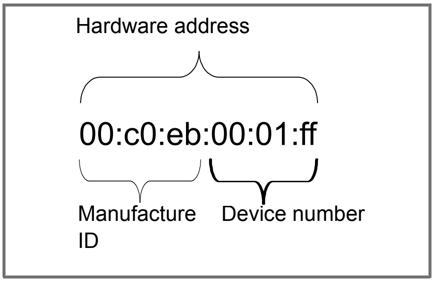
The SEH Print Monitor is an SEH-specific extension for the printing service of a Windows operating system. The software ensures the transfer of unencrypted and encrypted (SSL/TLS) print data from the client to the ISD by means of direct TCP/IP ports. The SEH Print Monitor can be installed and configured on every client intended for printing.

ISD Printer Driver Wizard

The SEH ISD Printer Driver Wizard simplifies storing all required printer drivers to ISD. It collects all required files for installing and managing a certain printer driver. This packet can simply be uploaded to an ISD.

Hardware Address

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



The hardware address is found on the housing, the SEH ISD Manager, or the ISD Control Center.

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

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

IP Address

The IP address is the unique address of each node in a network, i.e. an IP address may occur only once on a local network. The system administrator usually assigns the IP address. The address must be saved in the ISD to make sure that it can be addressed within the network.

Host Name

The host name is an alias for an IP address. The host name uniquely identifies the ISD in the network and makes it easier to remember. The host name is found on the ISD Control Center, the SEH ISD Manager or on the display at the device front.

Gateway

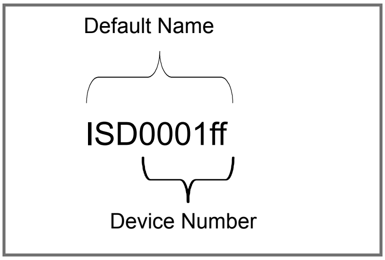
Using a gateway, you can address IP addresses from external networks. If you wish to use a gateway, you can configure the relevant parameter via the ISD Control Center.

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 ISD is configured not to use subnetworks by default. If you wish to use a subnetwork, you can configure the relevant parameter via the ISD Control Center.

Default Name

The default name consists of three letters 'ISD' and the device number. The device number consists of the last six numbers of its hardware address.



The default name is found on the ISD Control Center.

14.2 List of Tables

14.3 List of Figures

14.4 Index