my Secure Network Device

File Access Server mySND-120

User Manual

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

Scan this QR code (meCard) using your smart phone.

Document:
Type: User Manual
Title: my Secure Network Device
Version: 1.0

Online Links to Important Websites:

Support Contacts & Information:	http://www.seh-technology.com/support
Sales Contacts & Information:	http://www.seh-technology.com/sales
Downloads:	http://www.seh-technology.com/services/downloads/mySND.html

InterCon is a registered trademark of SEH Computertechnik GmbH.

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

Table of Contents

1 General Information. 5
1.1 mySND 6
1.2 Documentation. 7
1.3 Support and Service 9
1.4 Your Safety 10
1.5 First Steps 11
1.6 Saving the IP Address in the SND Server 12

2 Administration Methods 16
2.1 Administration via the mySND Control Center 17
2.2 Administration via the InterCon-NetTool 20
2.3 Administration via Email 22
2.4 Administration via the Reset Button of the Device 24

3 Network Settings 25
3.1 How to Configure IPv4 Parameters 25
3.2 How to Configure IPv6 Parameters 28
3.3 How to Configure the DNS 30
3.4 How to Configure SNMP 31
3.5 How to Configure POP3 and SMTP 32
3.6 How to Configure Bonjour 36

4 Device Settings 38
4.1 How to Determine a Description 38
4.2 How to Configure the Device Time 39
4.3 How to Use the Notification Service 40

5 Media Management and Access Settings 42
5.1 How to Manage User Accounts (Access Control) 42
5.2 How to Prepare Removable Media 47
5.3 How to Configure the Media assignment 48
5.4 How to Configure File Filters 50
5.5 How to Configure the Automatic File Transfer 53

6 Working with the mySND File Browser 57
6.1 How to Use the mySND File Browser. 57
6.2 How to Display Files in the mySND File Browser. 60
6.3 How to Select Files. 61
6.4 How to Sort Files. 62
6.5 How to Search Files 63
6.6 How to Store Files on a Client 64
6.7 How to Email Files via the mySND File Browser. 64
6.8 How to Rename Files. 65
6.9 How to Delete Files 66

7 Security 68
7.1 How to Define the Encryption Level for SSL/TLS Connections. 69
7.2 How to Control the Access to the mySND File Browser and the mySND Control Center 70
7.3 How to Manage Sessions. 72
7.4 How to Enable/Disable the USB Port. 73
7.5 How to Control the Access to the SND Server (TCP Port Access Control) 74
7.6 How to Use Certificates Correctly. 76
7.7 How to Use Authentication Methods 84

8 Maintenance 91
8.1 How to Secure the SND Parameters (Backup) 91
8.2 How to Reset the SND Parameters to their Default Values 93
8.3 How to Perform an Update. 96
8.4 How to Restart the SND Server 97

9 Appendix. 98
9.1 Glossary 99
9.2 Parameter List 102
9.3 Troubleshooting. 119
9.4 List of Figures. 122
9.5 Index. 123

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 SND Server and how to operate the device properly.

What information do you need?

- 'mySND' ⇨🗎6
- 'Documentation' ⇨🗎7
- 'Support and Service' ⇨🗎9
- 'Your Safety' ⇨🗎10
- 'First Steps' ⇨🗎11
- 'Saving the IP Address in the SND Server' ⇨🗎12

1.1 mySND

Purpose

mySND (my Secure Network Device) is used to safely deploy files within the network. Files from a non-network-enabled SD card and a non-network-enabled USB mass storage device (e.g. USB stick, hard drive, etc.) can be made available to several network participants. To do this, the SD card is inserted into the integrated network-enabled SD card reader. Alternatively, the USB mass storage device is connected to the USB port of the SND Server.

The file is accessed via the 'mySND File Browser'. The administration of the SND Server is done via the 'mySND Control Center'.

System Requirements

SND Server have been designed for the use in TCP/IP-based networks.

The mySND File Browser and the mySND Control Center can only be used if your browser software accepts cookies and if JavaScript is enabled.

Supported browsers:

- Mozilla Firefox (version 3 or later)
- Google Chrome
- Internet Explorer (version 7 or later)
- Safari

A screen resolution of at least 1024 x 768 pixels is required.

Procedure and Basic Functions

After embedding the SND Server into the network, you must configure the administrator account and additional user accounts. Access data, privileges and file filters are assigned to each account. The SD cards and user accounts are then linked to each other via media assignments.

After connecting a removable media, the users authenticate themselves in the mySND File Browser. The access to the files and the work with files (downloading files, sending files, etc.) depends on the assigned account properties and media assignments.

1.2 Documentation

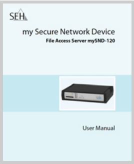
Please note the following names in this documentation:

- SD card → removable medium
- USB mass storage device → removable media

Since the File Access Server mySND-120 provides the mySND feature, it is called SND Server.

Structure of the Documentation

The mySND documentation consists of the following documents:



PDF

User Manual

Detailed description of the mySND configuration and administration.

Printed PDF

Quick Installation Guide

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

HTML

Online Help

The Online Help contains detailed information about how to use the 'mySND File Browser' and the 'mySND 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: ⇨🗎99.

Symbols and Conventions

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

Table 1: Conventions within the documentation

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

1.3 Support and Service

Support

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

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

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

Current Services

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

In unseren Screencasts erfahren Sie alles Wissenswerte über unsere Produkte. Schauen Sie doch mal rein!

- Anwendungsszenarien und Beispiele für den Einsatz von SEH-Produkten
- Sicher Drucken im Netz mit SEH-Produkten
- Druckerspezifische Lösungen, Druckkostenkontrolle, Netzwerkdruckmanagement und mehr

SEH ist Sponsor der Biologischen Station Gütersloh/Bielefeld e.V.
In diesem Jahr haben wir uns entschlossen, keine Weihnachtsgeschenke an unsere…

Tech?Update!: Virtualisierung und die Perspektive von SEH
Der Begriff "Virtualisierung" ist in der IT-Welt in aller Munde, weil er mit…

SEH in der Fachpresse: Funkschau testet myUTN-80 Dongleserver
Dirk Jarzyna hat für das Magazin Funkschau unseren myUTN-80 Dongleserver…

SEH zum ersten Mal bei der Citrix Synergy Barcelona
Citrix Ready-Partner SEH zeigt

- current firmware/software
- current tools
- current documentation
- current product information
- product data sheets
- 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. SEH Computertechnik GmbH will not accept any liability for loss of data, property damages and consequential damages resulting from the non-observance of the mentioned safety regulations and warnings.

Intended Use

The SND Server is operated in TCP/IP networks. mySND is used for the secure deployment of data on non-network-enabled SD cards and USB mass storage devices for several network participants. The SND Server has been designed for use in office environments.

Improper Use

All uses of the device that do not comply with the mySND 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 SND Server, please note the safety regulations in the 'Quick Installation Guide'. The Quick Installation Guide is enclosed in the packaging.

Warnings

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

⚠

Warning!

Data Backup (Backup)

To prevent data loss and/or data corruption on the respective removable medium and consequential damages, we strongly recommend you to make a backup copy of your data on a different storage medium before the initial operation, data access and data processing. Keep the storage medium with the backup copy in a safe place.

Disclaimer

SEH Computertechnik GmbH will not be liable for loss of data and/or data corruption, consequential damages or data recovery.

1.5 First Steps

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

Proceed as follows:

1. *Read and observe the security regulations in order to avoid damages to people and devices; see: ⇨🗎10.*
2. *Carry out the hardware installation. The hardware installation comprises the connection of the SND Server to the network, removable media and the mains supply; see: 'Quick Installation Guide'.*
3. *Make sure that an IP address is stored in the SND Server; see: ⇨🗎12.*
4. *Configure the administrator account and additional user accounts; see: ⇨🗎42.*
5. *Create a media assignment for the SD cards; see: ⇨🗎48.*
6. *(Optional) Enable the USB port; see: ⇨🗎73.*
7. *Authenticate yourself in the mySND File Browser; see: ⇨🗎57.*

↳ The access to the files and the work with files are possible.

1.6 Saving the IP Address in the SND Server

Why IP Addresses?

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

How Does the SND Server Obtain IP Addresses?

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

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

Once the SND Server has automatically received an IP address via a boot protocol, you can save a freely definable IP address in the SND Server. The assigned IP address of the SND Server can be determined and modified via the software tool 'InterCon-NetTool'; see: ⇨🗎20.

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

Automatic Methods of IP Address Assignments

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

Manual Methods of IP Address Assignments

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

ZeroConf

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

You can use the domain name service of Bonjour for the name resolution of the IP address; see: ⇨🗎36.

BOOTP

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

Requirements

☑ The 'BOOTP' parameter has been enabled, see: ⇨🗎25.

☑ A BOOTP server is available in the network.

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

DHCP

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

Requirements

☑ The 'DHCP' parameter has been enabled, see: ⇨🗎25.

☑ A DHCP server is available in the network.

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

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

Auto Configuration (IPv6 Standard)

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

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

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

Requirements

☑ The 'IPv6' parameter has been activated.

☑ The 'Automatic configuration' parameter has been activated.

To configure the assignment of IPv6 addresses, see: ⇨🗎28.

InterCon-NetTool

The InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices. The IP Wizard of the InterCon-NetTool helps you to configure the TCP/IP parameters, e.g. the IP address. You can manually enter the desired IPv4 address and save it in the SND Server using the IP Wizard. To configure an IPv4 address via the InterCon-NetTool, see: ⇨🗎26.

mySND Control Center

You can manually enter the desired IPv4 address and save it in the SND Server using the mySND Control Center IP Wizard.

- To configure an **IPv4** address via the mySND Control Center, see: ⇨🗎25.
- To configure an **IPv6** address via the mySND Control Center, see: ⇨🗎28.

ARP/PING

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

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

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

The 'arp' command is used for editing the ARP table. The 'ping' command sends a data packet containing the IP address to the hardware address of the SND Server. When receiving the data packet, the SND Server permanently saves its IP address.

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

Requirements

☑ The 'ARP/PING' parameter has been enabled, see: ⇨🗎25.

Edit the ARP table:
Syntax: `arp -s <IP address> <hardware address>`
Example: `arp -s 192.168.0.123  00-c0-eb-00-01-ff`

Assign a new IP address to the SND Server:
Syntax: `ping <IP address>`
Example: `ping 192.168.0.123`

2 Administration Methods

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

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

What information do you need?

- 'Administration via the mySND Control Center' ⇨🗎17
- 'Administration via the InterCon-NetTool' ⇨🗎20
- 'Administration via Email' ⇨🗎22
- 'Administration via the Reset Button of the Device' ⇨🗎24

2.1 Administration via the mySND Control Center

Which Functions Are Supported?

The mySND Control Center comprises all features for the administration and monitoring of the SND Server.

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

The access to the mySND Control Center is controlled by means of user accounts (⇨🗎42). Users authenticate themselves via a user name and a password. Only users with administrator privilege have access to the mySND Control Center.

Start and Login

The login to the SND server is session-based. Up to 16 users can be logged on to the SND server at the same time. For further information; see: ⇨🗎72.

Requirements

☑ The SND Server is connected to the network and the mains voltage.

☑ The SND Server has a valid IP address.

☑ The used user account has administrator privileges; see: ⇨🗎42.

The user account 'Admin' and the password 'admin' have been configured by default. Change the password when you use the SND server in a real situation; see: ⇨🗎42.

Proceed as follows:

1. *Open your browser.*
2. *Enter the IP address of the SND Server as the URL.*
   The login page appears.
   If the login page is not displayed, check the proxy settings of your browser.
3. *Enter the user name and password of a user account.*
4. *Click* **Login***.*
   The mySND File Browser will be displayed in the browser.
5. *Click* **Control Center***.*

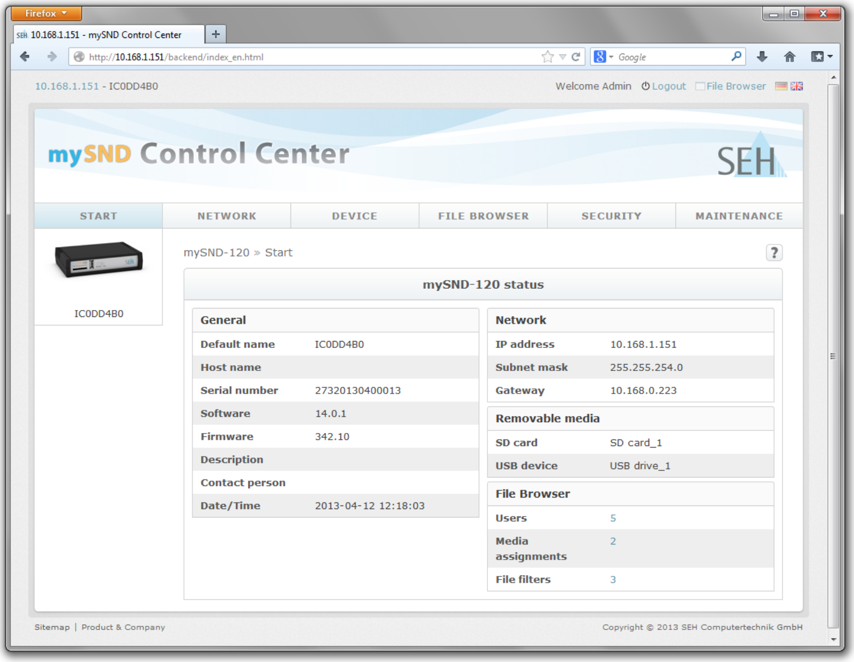
↳ The mySND Control Center will be displayed in the browser.

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

Proceed as follows:

1. *Highlight the SND Server in the device list.*
2. *Select* **Actions – Launch Browser** *from the menu bar.*
   The login page appears.
3. *Enter the user name and password of a user account.*
4. *Click* **Login***.*
   The mySND File Browser will be displayed.
5. *Click* **Control Center***.*

↳ The mySND Control Center will be displayed in the browser.



mySND-120 status

General	
Default name	IC0DD4B0
Host name	
Serial number	27320130400013
Software	14.0.1
Firmware	342.10
Description	
Contact person	
Date/Time	2013-04-12 12:18:03

Network	
IP address	10.168.1.151
Subnet mask	255.255.254.0
Gateway	10.168.0.223

Removable media	
SD card	SD card_1
USB device	USB drive_1

File Browser	
Users	5
Media assignments	2
File filters	3

Fig. 1: Starting the mySND Control Center

Structure of the mySND Control Center

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

Important information (IP address, host name, user account) is displayed at the top. The IP address allows you to directly go to the login page. The menu item **File Browser** allows you to go to the pane with the same name.

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

You can choose your language by clicking the relevant flag.

All other menu items refer to the configuration of the SND Server. You will find a description of the menu items in the Online Help of the SND Server. To start the Online Help, click the **?** icon.

Logout

Up to 16 users can be logged on to the SND server at the same time. If this number is reached, further logins will fail. Log off in order to allow other users to access the SND server.

Proceed as follows:

1. *Click* **Logout**.

↳ The login page appears. You have successfully logged out.

2.2 Administration via the InterCon-NetTool

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

Mode of Operation

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

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

Installation

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

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

Proceed as follows:

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

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

Program Start

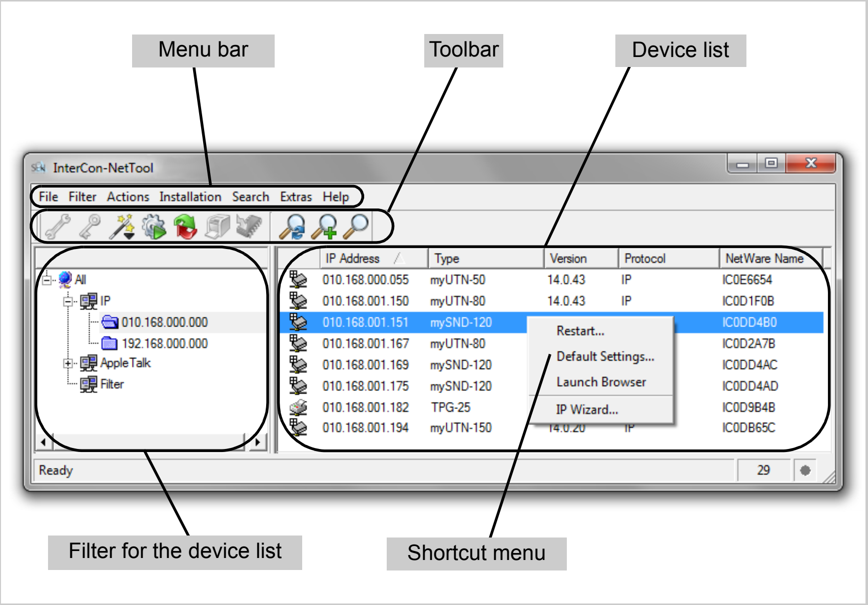
To start the program, double-click the InterCon-NetTool icon . The icon is found on the desktop or the Windows start menu.

(Start → Programs → SEH Computertechnik GmbH → InterCon-NetTool)

The settings of the InterCon-NetTool are saved in the 'InterCon-NetTool.ini' file. This file is stored in the user folder of the user that is currently logged in.

Structure of the InterCon-NetTool

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



IP Address	Type	Version	Protocol	NetWare Name
010.168.000.055	myUTN-50	14.0.43	IP	IC0E6654
010.168.001.150	myUTN-80	14.0.43	IP	IC0D1F0B
010.168.001.151	mySND-120			IC0DD4B0
010.168.001.167	myUTN-80			IC0D2A7B
010.168.001.169	mySND-120			IC0DD4AC
010.168.001.175	mySND-120			IC0DD4AD
010.168.001.182	TPG-25			IC0D9B4B
010.168.001.194	myUTN-150	14.0.20	IP	IC0DB65C

Fig. 2: InterCon-NetTool - Main Dialog

Which Functions Are Supported?

Using the InterCon-NetTool, you can:

- 'assign an IPv4 address to the SND Server' ➪🗎26
- 'restart the SND Server' ➪🗎97
- 'reset the parameter values of the SND Server to their default settings' ➪🗎93
- call the login page to start the 'mySND File Browser' ➪🗎57 and the 'mySND Control Center' ➪🗎17
- 'switch from the BIOS mode to the default mode' ➪🗎119

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

2.3 Administration via Email

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

Functionalities

An email allows you to

- send SND Server status information
- define SND Server parameters or
- perform an update on the SND Server.

Requirements

☑ A DNS server has been configured on the SND Server; see: ⇨🗎30.

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

☑ POP3 and SMTP parameters have been configured on the SND Server; see: ⇨🗎32.

Sending Instructions via Email

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

Proceed as follows:

1. *Open an email program.*
2. *Write a new email.*
3. *Enter the SND Server address as recipient.*
4. *Enter an instruction into the subject line; see: 'Syntax and Format of an Instruction' ⇨🗎22.*
5. *Send the email.*

↳ The SND Server receives the email and carries out the instruction.

Syntax and Format of an Instruction

Note the following syntax for instructions in the subject line:

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

The following commands are supported:

Commands	Option	Description
[<command>]	get status	sends the status page of the SND Server
	get parameters	sends the parameter list of the SND Server
	set parameters	sends parameters to the SND Server. The syntax and values can be obtained from the parameter list, see: ⇨🗎102. Parameter and value must be entered into the email body; see: ⇨🗎23.
	update SND	Carries out an automatic update using the software that is attached to the mail.
	help	Sends a page with information about the administration via email.
[<comment>]		Freely definable text for descriptions.

The following applies for the instructions:

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

Security with TAN

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

Parameter Changes

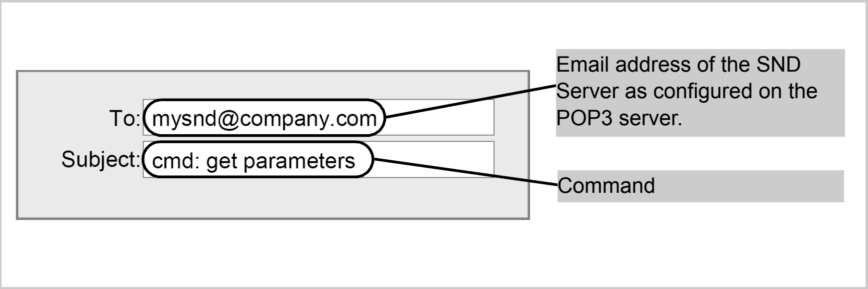
Parameter changes are integrated into the email body with the following syntax:

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

The syntax and values can be obtained from the parameter list, see: ⇨🗎102.

Example 1

This email causes the SND Server to send the parameter list to the sender of the email.



To: mysnd@company.com

Subject: cmd: get parameters

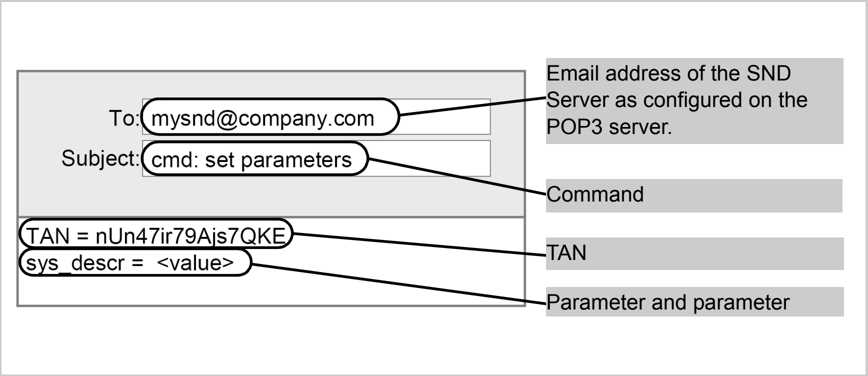
Email address of the SND Server as configured on the POP3 server.

Command

Fig. 3: Administration via Email - Example 1

Example 2

This email configures the parameter 'Description' on the SND Server.



To: mysnd@company.com

Subject: cmd: set parameters

TAN = nUn47ir79Ajs7QKE

sys_descr = <value>

Email address of the SND Server as configured on the POP3 server.

Command

TAN

Parameter and parameter

Fig. 4: Administration via Email - Example 2

2.4 Administration via the Reset Button of the Device

LEDs, the reset button and various ports can be found on the SND Server. These components are described in the 'Quick Installation Guide'.

Using the reset button you can reset the SND Server's parameter values to their default setting; see: ⇨🗎93.

3 Network Settings

You can define various settings for an ideal integration of the SND Server into a TCP/IP network. This chapter explains which network settings are supported by the SND Server.

What information do you need?

- 'How to Configure IPv4 Parameters' ⇨🗎25
- 'How to Configure IPv6 Parameters' ⇨🗎28
- 'How to Configure the DNS' ⇨🗎30
- 'How to Configure SNMP' ⇨🗎31
- 'How to Configure POP3 and SMTP' ⇨🗎32
- 'How to Configure Bonjour' ⇨🗎36

3.1 How to Configure IPv4 Parameters

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

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

What do you want to do?

□ 'Configuring IPv4 Parameters via the mySND Control Center' ⇨🗎25

□ 'Configuring IPv4 Parameters via the InterCon-NetTool' ⇨🗎26

Configuring IPv4 Parameters via the mySND Control Center

☞ Proceed as follows:

1. *Start the mySND Control Center.*

2. *Select* **NETWORK - IPv4***.*
3. *Configure the IPv4 parameters; see: Table 2* ⇨🗎*26.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Table 2: IPv4 Parameters

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

Configuring IPv4 Parameters via the InterCon-NetTool

Requirements

☑ The InterCon-NetTool is installed on the client, see: ⇨🗎20.

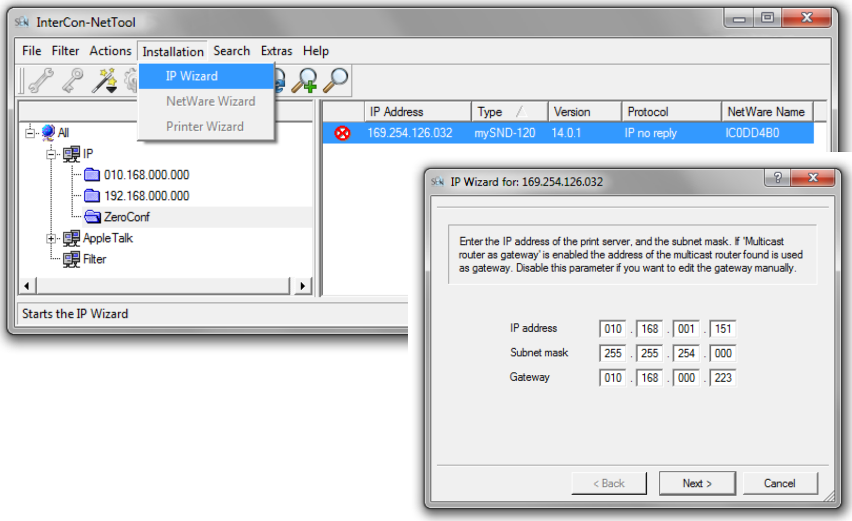
☑ The network scan via Multicast has been enabled in the InterCon-NetTool.

☑ The router in the network forwards multicast requests.

Proceed as follows:

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

↳ The settings will be saved.



IP Address	Type	Version	Protocol	NetWare Name
169.254.126.032	mySND-120	14.0.1	IP no reply	IC0DD4B0

Starts the IP Wizard

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

IP address	010 . 168 . 001 . 151
Subnet mask	255 . 255 . 254 . 000
Gateway	010 . 168 . 000 . 223

Fig. 5: InterCon-NetTool - IP Wizard

3.2 How to Configure IPv6 Parameters

You can integrate the SND Server into an IPv6 network.

What are the Advantages of IPv6?

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

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

What is the Structure of an IPv6 Address?

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

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

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

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

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

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 mySND Control Center.*
2. *Select* **NETWORK – IPv6***.*
3. *Configure the IPv6 parameters; see: Table 3 ⇨🗎29.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Table 3: IPv6 Parameters

Parameters	Description
IPv6	Enables/disables the IPv6 functionality of the SND Server.

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

3.3 How to Configure the DNS

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

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 mySND Control Center.*
2. *Select* **NETWORK – DNS***.*
3. *Configure the DNS parameters; see: Table 4 ⇨🗎31.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Table 4: DNS Parameters

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

3.4 How to Configure SNMP

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

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

SNMPv1

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

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

SNMPv3

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

Proceed as follows:

1. *Start the mySND Control Center.*

2. *Select* **NETWORK - SNMP***.*
3. *Configure the SNMP parameters; see: Table 5 ⇨🗎32.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Table 5: SNMP Parameters

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

3.5 How to Configure POP3 and SMTP

You must configure the protocols POP3 and SMTP and email limits on the SND Server so that the notification service (⇨🗎40), the administration via email (⇨🗎22), the automatic file transfer (⇨🗎53) and the sending of files in the mySND File Browser (⇨🗎64) will work properly.

POP3

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

SMTP

'SMTP' (Simple Mail Transfer Protocol) is a protocol that controls the sending of emails in networks. SMTP is required in the SND Server to administer the SND Server via email, to operate the notification service and to transfer files automatically and send them from the mySND File Browser.

> The encryption and signing of emails via S/MIME is only possible for the administration via email and the notification service.

Email Limits

For the automatic file transfer (⇨🗎53) and the file sending in the mySND File Browser (⇨🗎64) you must define the maximum number of files and the total file size. This allows you to adhere to size restrictions for attachments that are set by the email provider.

What do you want to do?

- □ 'Configuring POP3' ⇨🗎33
- □ 'Configuring SMTP' ⇨🗎34
- □ 'Defining Email Limits' ⇨🗎36

Configuring POP3

Requirements

☑ The SND Server is set up as user with its own email address on a POP3 server.

☞ Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **NETWORK - Email***.*
3. *Configure the POP3 parameters; see: Table 6* ⇨🗎*34.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Table 6: POP3 Parameters

Parameters	Description
POP3	Enables/disables the POP3 functionality.
POP3 - Server name	Defines the POP3 server via the IP address or the host name. *The host name can only be used if a DNS server was configured beforehand.*
POP3 - Server port	Defines the port used by the SND Server for receiving emails. The port number 110 is preset. When using SSL/TLS, enter 995 as port number.
POP3 - Security	Defines the authentication method to be used (APOP/SSL/TLS). When using SSL/TLS, the cipher strength is defined via the encryption level ⇨🖹69.
POP3 - Check mail every	Defines the time interval (in minutes) for retrieving emails from the POP3 server.
POP3 - Ignore mail exceeding	Defines the maximum email size (in Kbyte) to be accepted by the SND Server. *(0 = unlimited)*
POP3 - User name	Defines the user name used by the SND Server to log on to the POP3 server.
POP3 - Password	Defines the password used by the SND Server to log on to the POP3 server.

Configuring SMTP

Requirements

☑ The SND Server is set up as user with its own email address on an SMTP server.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **NETWORK – Email.**
3. *Configure the SMTP parameters; see: Table 7 ⇨🖹35.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Table 7: SMTP Parameters

Parameters	Description
SMTP - Server name	Defines the SMTP server via the IP address or the host name. *The host name can only be used if a DNS server was configured beforehand.*
SMTP - Server port	Defines the port number used by the SND Server to send emails to the SMTP server. The port number 25 is preset.
SMTP - TLS	Enables/disables TLS. *The security protocol TLS (Transport Layer Security) is used to encrypt the transmission between the SND Server and the SMTP server. The cipher strength is defined via the encryption level* ⇨ 🗎*69.*
SMTP - Sender name	Defines the email address used by the SND Server to send emails. <u>Note:</u> Very often the name of the sender and the user name are identical.
SMTP - Login	Enables/disables the SMTP authentication for the login.
SMTP - User name	Defines the user name used by the SND Server to log on to the SMTP server.
SMTP - Password	Defines the password used by the SND Server to log on to the SMTP server.
SMTP - Security (S/MIME)	Enables/disables the encryption and signing of emails via S/MIME. <u>Note:</u> Only emails from the administration and the notification service can be encrypted and signed.
SMTP - Signing emails	Defines the signing of emails. *A signature created by the sender allows the recipient to verify the identity of the sender and to make sure that the email was not modified. An S/MIME certificate is required for the signing of emails* ⇨ 🗎76.
SMTP - Full encryption	Defines the encryption of emails. *Only the recipient can open and read the encrypted email. An S/MIME certificate is required for the encryption* ⇨ 🗎76.
SMTP- Attach public key	Sends the public key together with the email. Many email clients require the public key to be attached in order to view the emails.

Defining Email Limits

📂 Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **NETWORK - Email**.
3. *Configure the email limits; see: Table 8 ⇨🗎36.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Table 8: Email Limits

Parameters	Description
SMTP - Total file size limit	Defines the total size limit (in kB) of the files that are sent via email during the file transfer via the mySND File Browser (⇨🗎64) and the automatic file transfer (⇨🗎53). *If the defined value is exceeded, the remaining files will be sent in additional emails during the automatic file transfer.*
SMTP - Maximum number of files	Defines the maximum number of files that are sent via email during the file transfer via the mySND File Browser (⇨🗎64) and the automatic file transfer (⇨🗎53). *If the defined value is exceeded, the remaining files will be sent in additional emails during the automatic file transfer.*

3.6 How to Configure Bonjour

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

The SND Server uses the following Bonjour functions:

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

When checking the IP address assigned via ZeroConf (see: 'ZeroConf' ⇨🗎13) the SND Server sends a query to the network. If the IP address is no longer available in the network, the SND Server receives an answer. The SND Server then sends another query with a different IP address. If the IP address is available, it is saved in the SND Server.

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

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

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **NETWORK - Bonjour***.*
3. *Configure the Bonjour parameters; see: Table 9 ⇨🗎37.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Table 9: Bonjour Parameters

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

4 Device Settings

You can configure descriptions, the device time and the notification service on the SND Server. This chapter describes these device settings.

What information do you need?

- 'How to Determine a Description' ⇨🗎38
- 'How to Configure the Device Time' ⇨🗎39
- 'How to Use the Notification Service' ⇨🗎40

4.1 How to Determine a Description

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

Proceed as follows:

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

↳ The data is saved.

4.2 How to Configure the Device Time

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

Benefits and Purpose

If the time server is enabled, the date and time of the last change will be displayed in the mySND File Browser according to the time set on the SND Server.

UTC

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

Time zone

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

Requirements

☑ A time server is integrated into the network.

Proceed as follows:

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

↳ The settings will be saved.

4.3 How to Use the Notification Service

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

The following message types are possible:

- The status email periodically informs the recipient about the status of the SND Server and the connected removable media.
- The event notification informs you about a specific event on the SND Server via email or SNMP trap. The event can be:

  - The connection or disconnection of removable media to/from the SND Server.

  - The restart of the SND Server.

What do you want to do?

☐ 'Configuring the sending of status emails' ⇨🗎40

☐ 'Configuring event notifications via email' ⇨🗎41

☐ 'Configuring event notifications via SNMP traps' ⇨🗎41

Configuring the sending of status emails

Requirements

☑ SMTP parameters have been configured on the SND Server, see: ⇨🗎32.

☑ A DNS server has been configured on the SND Server; see: ⇨🗎30.

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

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **DEVICE - Notification***.*
3. *Enter the recipient into the* **Email address** *box.*
4. *Tick* **Status email***.*

5. *Specify the sending interval in the* **Status notification time** *area.*
6. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Configuring event notifications via email

Requirements

☑ SMTP parameters have been configured on the SND Server, see: ⇨📄32.

☑ A DNS server has been configured on the SND Server; see: ⇨📄30.

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

☞ Proceed as follows:

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

↳ The settings will be saved.

Configuring event notifications via SNMP traps

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

☞ Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **DEVICE – Notification**.
3. *In the* **SNMP traps** *area, specify the recipients via the IP address and the community.*
4. *Tick the options with the desired message types in the* **Notifications** *area.*
5. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

5 Media Management and Access Settings

This chapter describes how to restrict the access to the SND Server, how to use removable media on the device and how to configure the file access.

The access control on the SND server is handled via the user management. All user accounts can access the USB mass storage devices. The access to an SD card only takes place via user accounts that are assigned to this card. Exception: User accounts with administrator privilege can access all SD cards.

Displayed file types are determined by the file filter that is assigned to the user account.

Optionally you can configure an automatic file transfer.

What information do you need?

- 'How to Manage User Accounts (Access Control)' ⇨🗎42
- 'How to Prepare Removable Media' ⇨🗎47
- 'How to Configure the Media assignment' ⇨🗎48
- 'How to Configure File Filters' ⇨🗎50
- 'How to Configure the Automatic File Transfer' ⇨🗎53

5.1 How to Manage User Accounts (Access Control)

The access to the SND Server is controlled by means of user accounts. You will need a user name and a password to get access to the program.

The user account 'Admin' and the password 'admin' have been configured by default. Change the password when you use the SND Server in a real situation.

In addition to the predefined administrator account you can create 4 additional user accounts. If this number is reached, you must delete a user account before you can define a new one.

Login

A user account allows for multiple logins, i.e. the account can be used by a single user or by a group of users. Up to 16 users can be logged on to the SND Server simultaneously. For further information; see: ⇨🗎72

When logging in, the password is transmitted in plain text. We recommend setting up a secure connection (SSL/TLS); see: ⇨🗎70.

Rights

Each account will be equipped with rights for the work with files in the mySND File Browser and the administrative access (mySND Control Center).

Only system administrators should have access to the mySND Control Center because this is where security-related settings can be configured.

File Filters

File types displayed in the mySND File Browser are determined by the file filter assigned. The file filter 'All files' is configured by default. To configure additional file filters; see: ⇨🗎50.

Enabling/Disabling Accounts

You can enable/disable a user account. This allows you to temporarily restrict the user access without having to delete or reconfigure the user account.

What do you want to do?

- □ 'Adding a User Account' ⇨🗎44
- □ 'Editing a User Account' ⇨🗎45
- □ 'Deleting a User Account' ⇨🗎46
- □ 'Enabling/Disabling a User Account' ⇨🗎46

Adding a User Account

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **FILE BROWSER – User management***.*
3. *Define the desired credentials in the* **Add user** *area; see: Table 10 ⇨🗎44.*
4. *Tick the options with the desired rights; see: Table 10 ⇨🗎44.*
5. *Select the desired file filter; see: Table 10 ⇨🗎44.*
6. *Click* **Save** *to confirm.*

↳ The settings will be saved.

Table 10: User Account Parameters

Parameters	Description
Credentials	
User name	Defines the name for the user account in order to log on to the SND Server. *(The name of the administrator account cannot be changed.)*
Password	Defines the password for the user account in order to log on to the SND Server.
Retype	Re-entry of the password
Email address	Defines the email address suggestions for the automatic file transfer (⇨🗎40).
Rights	
Administration	Enables/disables the administrative access to the SND Server. All connected removable media can be displayed (no media assignment required). *Only system administrators should have access to the mySND Control Center because this is where security-related settings can be configured.* *(The option cannot be disabled for the administrator account.)*
Rename/Delete files	Enables/disables the feature for renaming and deleting files in the mySND File Browser.

Parameters	Description
Download files	Enables/disables the download feature in the mySND File Browser.
Email files	De-/aktiviert die E-Mail-Funktion im mySND File Browser.
Set/Clear archive bit	Enables/disables the archive bit feature in the mySND File Browser.
File access	
File filters	Defines a file filter for the user account. After logging on to the mySND File Browser, only files of the file types defined in the filter will be displayed. For further information; see: ⇨🗎50.

Editing a User Account

You can modify the settings of an existing user account.

⚠

Do not edit user accounts that are currently used by the SND Server. These accounts are marked with a green dot in the 'User status' table.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – User management***.*
3. *Click the* 🔧 *icon in the* **User status** *table for the user account to be modified.*
   The **Edit user** *dialog appears.*
4. *Make the desired modifications; see: Table 10 ⇨🗎44.*
5. *Click* **Save** *to confirm.*

↳ The settings will be saved.

Deleting a User Account

Do not delete user accounts that are currently used by the SND Server. These accounts are marked with a green dot in the 'User status' table.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – User management***.*
3. *Click the* 🗑 *icon in the* **User status** *table for the user account to be deleted.*
4. *Confirm the security query by clicking* **Delete***.*

↳ The user account will be deleted.

Enabling/Disabling a User Account

Do not disable user accounts that are currently used by the SND Server. These accounts are marked with a green dot in the 'User status' table.

The administrator account cannot be disabled.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – User management***.*
3. *Click the* 🔧 *icon in the* **User status** *table for the user account to be modified.*
   The **Edit user** *dialog appears.*
4. *Enables/disables the option in front of the user account name.*
5. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

5.2 How to Prepare Removable Media

For a removable medium to be used on the SND Server, it must have the 'FAT32', 'FAT16' or 'FAT12' file system. You can format the removable medium on the SND Server accordingly. In the process a partition will be created spanning the entire removable medium.

Whether formatting is required, is displayed in the mySND Control Center under the 'Media preparation' menu item in the 'Media status' table.

To facilitate the identification of a removable medium, assign a freely definable name.

What do you want to do?

□ 'Formatting a Removable Medium' ⇨🗎47

□ 'Renaming a Removable Medium' ⇨🗎48

Formatting a Removable Medium

Requirements

☑ A removable medium is connected to the SND Server.

⚠

During the formatting process, all data on the removable medium will be permanently lost.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER - Media preparation***.*
3. *Select the device type from the* **Removable medium** *list.*
4. *Enter a freely definable name into the* **Device name** *box.*
5. *Click* **Formatting***.*

↳ The removable medium will be formatted. This may take a few minutes.

Renaming a Removable Medium

Requirements

☑ A removable medium is connected to the SND Server.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – Media preparation**.
3. *Select the device type from the* **Removable medium** *list.*
4. *Enter a freely definable name into the* **Device name** *box.*
5. *Click* **Rename***.*

↳ The removable medium will be renamed.

5.3 How to Configure the Media assignment

In order to restrict the access to SD cards on the SND Server, SD cards are assigned to user accounts. Only user accounts that are assigned to the SD card can access the removable medium via the mySND File Browser.

SD cards without media assignment can be used on the SND Server only with administrator privilege (⇨🗎42).

Media assignments (along with file filters ⇨🗎50) reduce the risk of feeding unwanted data via the SND Server into the network.

We recommend disabling the USB port in order to further reduce the risk of feeding unwanted files into the network via the SND Server (⇨🗎73).

SD cards are identified via their device ID. Up to 16 media assignments can be configured.

What do you want to do?

□ 'Establishing a Media Assignment' ⇨🗎49

□ 'Editing a Media Assignment' ⇨🗎49

□ 'Deleting a Media Assignment' ⇨🗎50

Establishing a Media Assignment

Requirements

☑ The SD card for which a media assignment is to be established, is connected to the SND Server.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – Media assignment***.*
3. *Enter a freely definable name into the* **Assignment name** *box.*
4. *In the* **Users** *area, enable the user accounts that are allowed to use the SD card.*
5. *Click* **Save** *to confirm.*

↳ The settings will be saved.

Editing a Media Assignment

You can modify the settings of an existing media assignment.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – Media assignment***.*
3. *Click the* 🔧 *icon in the* **Media assignment status** *table for the media assignment to be edited.*
   The **Edit media assignment** *dialog appears.*
4. *Enter a freely definable name into the* **Assignment name** *box.*
5. *In the* **Users** *area, enable the user accounts that are allowed to use the SD card.*
6. *Click* **Save** *to confirm.*

↳ The settings will be saved.

Deleting a Media Assignment

After the deletion of a media assignment, the access to the corresponding SD card via the mySND File Browser is only possible with administrator privilege (⇨🖹42).
If a file transfer for the media assignment was configured, it will also be deleted.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – Media assignment***.*
3. *Click the* 🗑 *icon in the* **Media assignment status** *table for the media assignment to be deleted.*
4. *Confirm the security query by clicking* **Delete***.*

↳ The media assignment will be deleted.

5.4 How to Configure File Filters

You can determine what file types will be displayed in the mySND File Browser for a certain user account. Define a file filter (⇨🖹51) and assign it to a user account (⇨🖹42).

This allows you to restrict the file access for the users.

The file filter 'All files' is defined by default and cannot be edited or deleted. You can freely define 4 additional file filters. If this number is reached, you must delete a file filter before you can define a new one.

On the SND Server, file types are defined by their file extension. Changing the file extension on a different device (PC, etc.) can lead to the fact that unwanted files will be fed into the network via the SND Server.

What do you want to do?

- □ 'Adding a File Filter' ⇨🗎51
- □ 'Editing File Filters' ⇨🗎51
- □ 'Deleting the File Filter' ⇨🗎52

Adding a File Filter

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – File filter.**
3. *Enter a freely definable name into the* **Filter name** *box.*
4. *In the* **Accessible file types** *box, define the file types that will be displayed in the mySND File Browser. Enter the file extension:*
   - Schema: .<Extension>
   - File types without extension will be defined by a dot.
   - Multiple entries are to be separated by blanks.
5. *Click* **Save** *to confirm.*

↳ The settings will be saved.

Editing File Filters

You can modify the settings of an existing file filter.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – File filter.**
3. *Click the* 🔧 *icon in the* **File filter status** *table for the file filter to be modified.*
4. *Enter a freely definable name into the* **Filter name** *box.*
5. *In the* **Accessible file types** *box, define the file types that will be displayed in the mySND File Browser. Enter the file extension:*
   - Schema: .<Extension>
   - File types without extension will be defined by a dot.
   - Multiple entries are to be separated by blanks.
6. *Click* **Save** *to confirm.*

↳ The settings will be saved.

Deleting the File Filter

After the deletion of a file filter, all user accounts to which this file filter was assigned to can longer view files in the mySND File Browser. Assign a new file filter to these user accounts (⇨🖹45).

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER - File filter***.*
3. *Click the* 🗑 *icon in the* **File filter status** *table for the file filter to be deleted.*
4. *Confirm the security query by clicking* **Delete***.*

↳ The file filter is deleted.

5.5 How to Configure the Automatic File Transfer

The automatic file transfer via email can be triggered when connecting removable media to the SND Server.

The files are transferred without encryption.

Transfer Method

The method for the automatic file transfer is determined by the removable medium.

SD cards:

- card-specific transfer
(One transfer is set up per SD card.)
- The automatic file transfer can only be set up for SD cards with media assignment.
- 1 recipient per SD card

USB mass storage devices:

- device-independent transfer
(For all USB mass storage devices an overall transfer will be set up.)
- 2 recipients

Recipients

The recipients are freely definable. If you defined email addresses for the user accounts, these email addresses will be suggested as recipients.

Content

Files from a specified folder will be transferred. The content from subfolders will not be transferred. Only defined file types will be transferred.

Limits

Up to 10 files or 5000 kB can be sent in one email per default. If the defined value is exceeded, the remaining files will be sent in additional emails. You can modify these limits, see: ⇨🗎36.

Archive Bit

Optionally, transferred files are marked by the archive bit ✓. Marked files will not be resent when the removable medium is reconnected to the SND Server. Remove the archive bit to resend files, for example after a failed send attempt.

No archive bit can be set with read-only removable media.

Enable/Disable the Transfer

You can enable/disable automatic file transfers. This allows you disable transfers without having to delete and reconfigure the file transfer.

What do you want to do?

- □ 'Configuring File Transfers' ⇨🗎54
- □ 'Editing File Transfers' ⇨🗎55
- □ 'Enabling/Disabling File Transfers' ⇨🗎55
- □ 'Setting/clearing the archive bit' ⇨🗎56

Configuring File Transfers

Requirements

☑ (only for SD cards) A media assignment was configured for the SD card; see: ⇨🗎48.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER - File transfer***.*
3. *Select the device type from the* **Removable medium** *list.*
4. *Select the SD card from the list. (ony for SD cards)*
5. *Enter the email address of the addressee into the* **Recipient** *box.*
6. *In the* **Source folder** *box, enter the path to the source directory on the removable medium.*
7. *In the* **File types** *box, define the file types to be transferred by their file extension.*
   - Schema: .<Extension>
   - File types without extension will be defined by a dot.
   - Multiple entries are to be separated by blanks.
8. *Clear* **Set archive bit.** *(Optional)*
9. *Click* **Save** *to confirm.*

↳ The settings will be saved.

Editing File Transfers

You can modify the settings of an existing file transfer.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – File transfer**.
3. *Click the* 🔧 *icon in the* **File transfer status** *table for the file transfer to be edited.*
4. *Select the SD card from the list. (ony for SD cards)*
5. *Enter the email address of the addressee into the* **Recipient** *box.*
6. *In the* **Source folder** *box, enter the path to the source directory on the removable medium.*
7. *In the* **Accessible file types** *box, define the file types to be transferred by their file extension.*
   - Schema: .<Extension>
   - File types without extension will be defined by a dot.
   - Multiple entries are to be separated by blanks.
8. *Tick/clear* **Set archive bit**. *(Optional)*
9. *Click* **Save** *to confirm.*

↳ The settings will be saved.

Enabling/Disabling File Transfers

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – File transfer**.
3. *Click the* 🔧 *icon in the* **File transfer status** *table for the file transfer to be disabled.*
4. *Clear* **Enable**.
5. *Click* **Save** *to confirm.*

↳ The settings will be saved.

Deleting File Transfers

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Click* **FILE BROWSER – File transfer***.*
3. *Click the* 🗑 *icon in the* **File transfer status** *table for the file transfer to be deleted.*
4. *Confirm the security query by clicking* **Delete***.*

↳ The file transfer is deleted.

Setting/clearing the archive bit

Requirements

☑ A removable medium is connected to the SND Server.

☑ Files are available on the removable medium.

☑ The user account used has the right to set and clear archive bits; see: ⇨🗎42.

Proceed as follows:

1. *Start the mySND File Browser.*
2. *Click* **SD** *or* **USB***.*
   The removable medium is selected.
3. *Select a folder.*
   The files are displayed.
4. *Select the files to be modified.*
5. *Select* **Set archive bit** *or* **Clear archive bit** *from the shortcut menu.*

↳ The archive bit is set/cleared.

6 Working with the mySND File Browser

🗎 The access to the removable media that are connected to the SND Server and the files stored on them is done via the mySND File Browser. This chapter describes how to access and work with files.

What information do you need?

- 'How to Use the mySND File Browser' ⇨🗎57
- 'How to Display Files in the mySND File Browser' ⇨🗎60
- 'How to Select Files' ⇨🗎61
- 'How to Sort Files' ⇨🗎62
- 'How to Search Files' ⇨🗎63
- 'How to Store Files on a Client' ⇨🗎64
- 'How to Email Files via the mySND File Browser' ⇨🗎64
- 'How to Delete Files' ⇨🗎66
- 'How to Rename Files' ⇨🗎65

6.1 How to Use the mySND File Browser

The mySND File Browser is the user interface for the file access. It shows the files saved on the removable medium that is connected to the SND Server.

The mySND File Browser is stored in the SND Server and can be displayed by means of a browser software (Internet Explorer, Firefox, Safari).

The access to the mySND File Browser is controlled by means of user accounts (⇨🗎42). Users authenticate themselves via a user name and a password.

Start and Login

The login to the SND server is session-based. Up to 16 users can be logged on to the SND server at the same time. For further information; see: ⇨🗎72.

Requirements

☑ The SND Server is connected to the network and the mains voltage.

☑ The SND Server has a valid IP address.

The user account 'Admin' and the password 'admin' have been configured by default. Change the password when you use the SND server in a real situation; see: ⇨🗎42.

Proceed as follows:

1. *Open your browser.*
2. *Enter the IP address of the SND Server as the URL.*
   The login page appears.
   If the login page is not displayed, check the proxy settings of the browser.
3. *Enter the user name and password of a user account.*
4. *Click* **Login***.*

↳ The mySND File Browser will be displayed in the browser.

You can also start the mySND File Browser via the software tool 'InterCon-NetTool'.

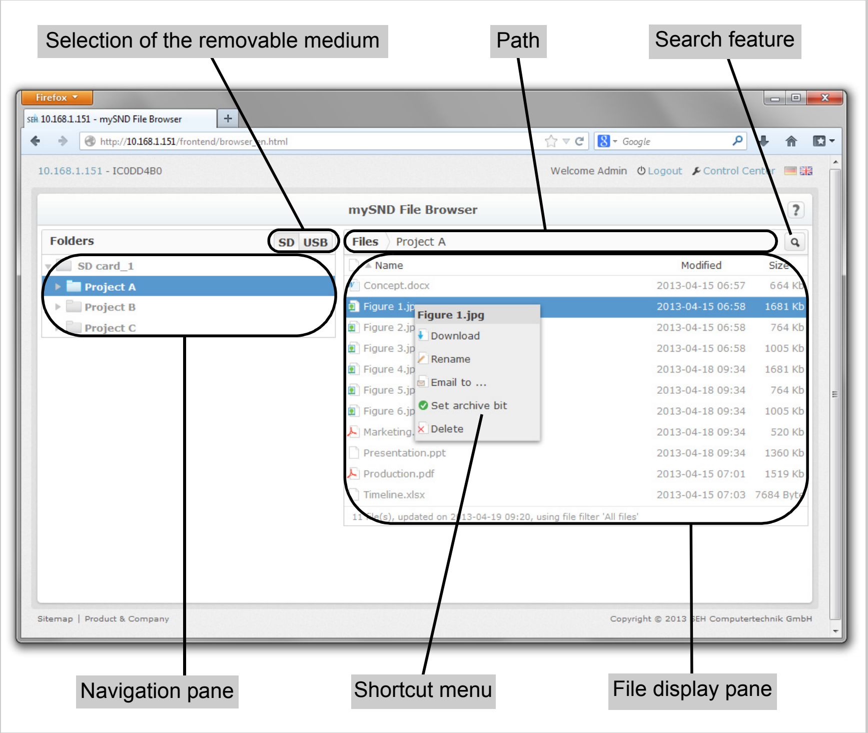
Proceed as follows:

1. *Highlight the SND Server in the device list.*
2. *Select* **Actions – Launch Browser** *from the menu bar.*
   The login page appears.
3. *Enter the user name and password of a user account.*
4. *Click* **Login***.*

↳ The mySND File Browser will be displayed.

Structure and Mode of Operation of the mySND File Browser

After the logging the mySND File Browser will be displayed with the following dialog items:



Name	Modified	Size
Concept.docx	2013-04-15 06:57	664 Kb
Figure 1.jp	2013-04-15 06:58	1681 Kb
Figure 2.jp	2013-04-15 06:58	764 Kb
Figure 3.jp	2013-04-15 06:58	1005 Kb
Figure 4.jp	2013-04-18 09:34	1681 Kb
Figure 5.jp	2013-04-18 09:34	764 Kb
Figure 6.jp	2013-04-18 09:34	1005 Kb
Marketing.	2013-04-18 09:34	520 Kb
Presentation.ppt	2013-04-18 09:34	1360 Kb
Production.pdf	2013-04-15 07:01	1519 Kb
Timeline.xlsx	2013-04-15 07:03	7684 Byt

11 file(s), updated on 2013-04-19 09:20, using file filter 'All files'

Fig. 6: mySND File Browser

The buttons for the selection of the removable medium (top left) determine from what removable medium the content will be displayed in the file display pane (right). The navigation pane (left) and the path (top) allow for the orientation and navigation on the removable medium. Working with files (e.g. download) is done via the corresponding button (top right) or the shortcut menu (right-click).

You can choose your language by clicking the relevant flag.

Important information (IP address, host name, user account) is displayed at the top. The IP address allows you to directly go to the login page.

The manufacturer's contact details and additional information regarding the product are displayed under **Product & Company**.

Users with administrator privileges can click **Control Center** to go to the pane with the same name. The **Sitemap** provides administrators with an overview of and direct access to all pages of the mySND Control Center.

Logout

Up to 16 users can be logged on to the SND server at the same time. If this number is reached, further logins will fail. Log off in order to allow other users to access the SND server.

Proceed as follows:

1. *Click* **Logout***.*

↳ The login page appears. You have successfully logged out.

Detailed information about the work with the mySND File Browser can be found in the following chapters or in the SND Server Online Help. To start the Online Help, click the **?** icon.

6.2 How to Display Files in the mySND File Browser

In the mySND File Browser, files will be displayed that are stored on a removable medium that is connected to the SND Server.

Displayed file types are determined by the file filter that is defined for the user account used; see: ⇨🗎50.

Requirements

☑ A removable medium is connected to the SND Server.

☑ Files are available on the removable medium.

Proceed as follows:

1. *Start the mySND File Browser.*
2. *Click* **SD** *or* **USB***.*
   The removable medium is selected.

3. *Select a folder.*
   (To show or hide subfolders, click the triangular icon in front of the folder.)

↳ The file content will be displayed.

6.3 How to Select Files

To work with one or more files, you have to select the files.

What do you want to do?

□ 'Selecting a Single File' ⇨ 61

□ 'Selecting Consecutive Files' ⇨ 61

□ 'Selecting Non-Consecutive Files' ⇨ 62

Selecting a Single File

Requirements

☑ A removable medium is connected to the SND server.

☑ Files are available on the removable medium.

☞ Proceed as follows:

1. *Start the mySND File Browser.*
2. *Click* **SD** *or* **USB**.
   The removable medium is selected.
3. *Select a folder.*
   The files are displayed.
4. *Select the desired file.*

↳ The file is marked.

Selecting Consecutive Files

Requirements

☑ A removable medium is connected to the SND server.

☑ Files are available on the removable medium.

☞ Proceed as follows:

1. *Start the mySND File Browser.*

2. *Click* **SD** *or* **USB**.
   The removable medium is selected.
3. *Select a folder.*
   The files are displayed.
4. *Select the first file from your selection.*
5. *Keep the SHIFT key pressed and select the last file from your selection.*

↳ The files are marked.

Selecting Non-Consecutive Files

Requirements

☑ A removable medium is connected to the SND server.

☑ Files are available on the removable medium.

Proceed as follows:

1. *Start the mySND File Browser.*
2. *Click* **SD** *or* **USB**.
   The removable medium is selected.
3. *Select a folder.*
   The files are displayed.
4. *Windows/Linux: Keep the Alt Gr key pressed.*
   Mac: Keep the command key pressed.
5. *Select the individual files.*

↳ The files are marked.

6.4 How to Sort Files

You can sort the currently displayed files in the mySND File Browser by various criteria:

- name
- size
- change date
- file extension and
- archive bit

Requirements

☑ A removable medium is connected to the SND Server.

☑ Files are available on the removable medium.

Proceed as follows:

1. *Start the mySND File Browser.*
2. *Click* **SD** *or* **USB**.
   The removable medium is selected.
3. *Select a folder.*
   The files are displayed.
4. *Select the column heading to be sorted by.*

↳ The files displayed are sorted.
(The icon of an arrow in front of the column heading shows the sort order. To reverse the sort order, select the column heading again.)

6.5 How to Search Files

You can sort the currently displayed files in the mySND File Browser by freely definable criteria such as the file name.

Requirements

☑ A removable medium is connected to the SND Server.

☑ Files are available on the removable medium.

Proceed as follows:

1. *Start the mySND File Browser.*
2. *Click* **SD** *or* **USB**.
   The removable medium is selected.
3. *Select a folder.*
   The files are displayed.
4. *Click the icon* 🔍.
   The search field appears.
5. *Enter a search criterion into the search box.*

↳ The search result is displayed.

To end the search, click the ✕ icon.

6.6 How to Store Files on a Client

One or more files can be stored locally on your client. Several files are grouped in a zip file.

For performance reasons we recommend that you do not store more than 160 files in one download process.

Requirements

☑ A removable medium is connected to the SND Server.

☑ Files are available on the removable medium.

☑ The user account used has download privileges; see: ⇨🖹42.

☞ Proceed as follows:

1. *Start the mySND File Browser.*
2. *Click* **SD** *or* **USB**.
   The removable medium is selected.
3. *Select a folder.*
   The files are displayed.
4. *Select the desired files.*
   The Download button appears.
5. *Click* **Download**.
6. *Save the file selection to your local system by means of your browser.*

↳ The file selection is copied to your client.

6.7 How to Email Files via the mySND File Browser

You can send the files displayed in the mySND File Browser via email.

The files are transferred without encryption.

Limits

Up to 10 files or 5000 kB can be sent in one email per default. You can modify these limits, see: ⇨🖹36.

Requirements

☑ A removable medium is connected to the SND Server.

☑ Files are available on the removable medium.

☑ The user account used has email privileges; see: ⇨🗎42.

☑ SMTP parameters have been configured on the SND Server; see: ⇨🗎32.

☑ A DNS server has been configured on the SND Server; see: ⇨🗎30.

Proceed as follows:

1. *Start the mySND File Browser.*
2. *Click* **SD** *or* **USB***.*
   The removable medium is selected.
3. *Select a folder.*
   The files are displayed.
4. *Select the desired files.*
5. *Select* **Email to ...** *from the shortcut menu.*
   The **Email files** *dialog appears.*
6. *Enter the email address of the addressee into the* **Recipients** *box.*
7. *Define a subject. (Optional)*
8. *Click* **Send***.*

↳ The file selection is sent.

6.8 How to Rename Files

Files stored on a removable medium can be renamed via the mySND File Browser.

Files can only be renamed one after the other.

Requirements

☑ A removable medium is connected to the SND Server.

☑ Files are available on the removable medium.

☑ The user account used has renaming privileges; see: ⇨🗎42.

Do not change the file extension. Otherwise the file will become unusable or cannot be displayed in the mySND File Browser.

Proceed as follows:

1. *Start the mySND File Browser.*
2. *Click* **SD** *or* **USB***.*
   The removable medium is selected.
3. *Select a folder.*
   The files are displayed.
4. *Select the file to be renamed.*
5. *Select* **Rename** *from the shortcut menu.*
6. *Enter a new file name.*
7. *Press Enter.*

↳ The file is renamed.

6.9 How to Delete Files

Files stored on a removable medium can be deleted via the mySND File Browser.

Deleted files will be permanently lost.

Requirements

☑ A removable medium is connected to the SND Server.

☑ Files are available on the removable medium.

☑ The user account used has deleting privileges; see: ⇨🗎42.

Proceed as follows:

1. *Start the mySND File Browser.*
2. *Click* **SD** *or* **USB***.*
   The removable medium is selected.
3. *Select a folder.*
   The files are displayed.

4. *Select the files to be deleted.*
5. *Select* **Delete** *from the shortcut menu.*
6. *Confirm the security query by clicking* **Delete***.*

↳ The file selection is deleted.

7 Security

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

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

What information do you need?

- 'How to Define the Encryption Level for SSL/TLS Connections' ⇨🗎69
- 'How to Control the Access to the mySND File Browser and the mySND Control Center' ⇨🗎70
- 'How to Manage Sessions' ⇨🗎72
- 'How to Enable/Disable the USB Port' ⇨🗎73
- 'How to Control the Access to the SND Server (TCP Port Access Control)' ⇨🗎74
- 'How to Use Certificates Correctly' ⇨🗎76
- 'How to Use Authentication Methods' ⇨🗎84

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

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

- Web access to the mySND File Browser and the mySND Control Center: HTTPS (⇨🗎70)
- Email: POP3 (⇨🗎32)
- Email: SMTP (⇨🗎32)

In the case of POP3 and SMTP only the administration via email and the notification service will be encrypted. The automatic file transfer and the file transfer via the mySND File Browser are carried out without encryption.

Encryption Level

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

Cipher Suite

Each encryption level is a collection of so-called cipher suites. A cipher suite is a standardized sequence of four cryptographic algorithms that are used to establish a secure connection. Depending on their cipher strength (in bit), cipher suites are grouped to form an encryption level. Which cipher suites are supported by the SND Server, i.e. are part of an encryption level, depends on the protocol used (SSLv2, SSLv3, TLSv1).

Establishing Connections

When establishing a secure connection, a list of supported cipher suites is sent to the communicating party. A cipher suite is agreed upon that will be used later on. The strongest cipher suite that is supported by both parties will be used by default. If there is no cipher suite that is supported by both parties, no SSL/TLS connection will be established.

The communicating parties of the SND Server (e.g. browser) must support the cipher suites of the selected encryption level in order

to successfully establish a connection. When problems occur, select a different level or reset the SND Server parameters; see: ⇨🗎93.

The following encryption levels can be selected:

- **Compatible:** Cipher suites with an encryption of 40 to 256 bit will be used.
- **Low:** Only cipher suites with a low encryption of 56 bit will be used. (Fast connection)
- **Medium:** Only cipher suites with an encryption of 128 bit will be used.
- **High:** Only cipher suites with a strong encryption of 128 to 256 bit will be used. (Slow connection)

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY – SSL connections***.*
3. *Select the desired encryption level from the* **Encryption** *area.*
4. *Click* **Save & Restart** *to confirm.*
5. The setting will be saved.

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

7.2 How to Control the Access to the mySND File Browser and the mySND Control Center

You can restrict the web access to the SND Server.

What do you want to do?

□ 'Specifying the Permitted Web Connection Type' ⇨🗎71

□ 'Protecting the web access via password' ⇨🗎71

The mySND Control Center can also be protected by the SNMP security concept. The concept includes administration of user groups and access rights. For further information; see: 'How to Configure SNMP' ⇨🗎31.

Specifying the Permitted Web Connection Type

Types of Connection (HTTP/HTTPS)

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

If HTTPS is exclusively chosen as the connection type, the web access to the mySND File Browser and the mySND Control Center is protected by SSL/TLS. The cipher strength is defined via the encryption level ⇨🗎69.

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

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY – Device access**.
3. *Tick* **HTTP/HTTPS** *or* **HTTPS only** *in the* **Web** *area.*
4. *Click* **Save & Restart** *to confirm.*

↳ The setting will be saved.

Protecting the web access via password

The access to the mySND Control Center and the mySND File Browser is controlled by means of user accounts; see: ⇨🗎42.

7.3 How to Manage Sessions

A user account allows for multiple logins on the SND Server, i.e. the account can be used by a single user or by a group of users.

The login is session-based. Up to 16 sessions can be saved at the same time. This means that up to 16 users can be logged on to the SND Server at the same time.

If this number is reached, further logins will fail. Sessions are terminated and are available for new logins if a user logs out (⇨🗎60 and ⇨🗎19) or the session timeout expires. Administrators also have the possibility to terminate current sessions.

What do you want to do?

□ 'Configuring a Session Timeout' ⇨🗎72

□ 'Terminating Sessions' ⇨🗎73

Configuring a Session Timeout

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

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY – Device access***.*
3. *Tick* **Session Timeout***.*
4. *In the* **Session duration** *box, enter the time in seconds after which the timeout is to be effective.*

↳ The setting will be saved.

Terminating Sessions

Users whose sessions are terminated lose their access to the SND Server and are required to login again. Current actions (file download, etc.) will be stopped.

Requirements

- □ The SND Server is connected to the network and the mains voltage.
- □ The SND Server has a valid IP address.
- □ The used user account has administrator privileges; see: ⇨🗎42.

Proceed as follows:

1. *Open your browser.*
2. *Enter the IP address of the SND Server as the URL.*
   The login page appears.
3. *Enter the user name and password of a user account.*
4. *Click* **Sessions***.*
   The page **mySND sessions** *appears.*
5. *In the* **Current sessions** *table, click the* 🗑 *icon for the session to be terminated.*
6. *Confirm the security query by clicking* **End***.*

↳ The session is terminated.

7.4 How to Enable/Disable the USB Port

The USB port on the SND Server is disabled by default.

The media assignment allows you to control the access to the SD cards on the SND Server (⇨🗎48). Every user that is logged in can access a USB mass storage device.

If the USB port is not needed, we recommend disabling this interface for security reasons. This reduces the risk of feeding unwanted files into the network via the SND server.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY – Device access**.
3. *Tick/clear* **USB port** *in the* **Interfaces** *area.*

↳ The setting will be saved.

7.5 How to Control the Access to the SND Server (TCP Port Access Control)

TCP Port Access Control

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

Security Levels

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

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

Exceptions

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

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

Test Mode

The 'test mode' allows you to check the configured access protection. If the test mode is activated, access protection remains active until the SND Server is rebooted. After restarting, the protection is no longer effective.

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

Proceed as follows:

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

If the SND Server can no longer be reached using the mySND Control Center, restart the device; see: ⇨🗎97.

9. *Clear* **Test mode***.*
10. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved. The port access control is active. Access to the ports is restricted.

7.6 How to Use Certificates Correctly

The SND Server 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 in the SND Server

- to check the identity of the SND Server in the network; see: 'Configuring EAP-TLS' ⇨🗎85.
- to authenticate the SND Server/client if the access to the mySND File Browser and the mySND Control Center is protected via HTTPS (SSL/TLS); see: ⇨🗎71.

If you use certificates, you should only grant administrator privileges to administrators to prevent unauthorized persons from deleting certificates on the SND Server; see: ⇨🗎42.

Which Certificates are available?

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

- Upon delivery, a certificate (the so-called **default certificate**) is stored in the SND Server. It is recommended that you replace the default certificate by a self-signed certificate or CA certificate as soon as possible.
- **Self-signed certificates** have a digital signature that has been created by the SND Server.
- **CA certificates** are certificates that have been signed by a certification authority (CA).
- The authenticity of the CA certificate can be verified by means of a so-called **root certificate** issued by the certification

authority. The root certificate is stored on an authentication server in the network.

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

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

- 1 Self-signed certificate

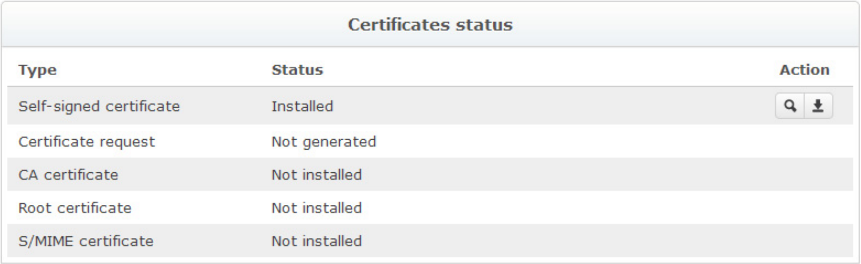
- 1 CA certificate or PKCS#12 certificate

- 1 Root certificate

- 1 S/MIME certificate

You can also generate a certificate request for a CA certificate. All certificates can be deleted separately. Existing certificates will be overridden when installing or generating new certificates.

A PKCS#12 certificate can only be installed if there are currently no certificate requests or CA certificates installed.



Certificates status

Type	Status	Action
Self-signed certificate	Installed	🔍 ⭳
Certificate request	Not generated	
CA certificate	Not installed	
Root certificate	Not installed	
S/MIME certificate	Not installed	

Fig. 7: mySND Control Center – Certificates

What do you want to do?

- □ 'Displaying Certificates' ⇨🗎78
- □ 'Creating a Self-Signed Certificate' ⇨🗎78
- □ 'Creating a Certificate Request for CA Certificates' ⇨🗎80
- □ 'Saving the CA Certificate in the SND Server' ⇨🗎80
- □ 'Saving the Root Certificate on the SND Server' ⇨🗎81
- □ 'Saving PKCS#12 Certificates on the SND Server' ⇨🗎82
- □ 'Saving the S/MIME Certificate on the SND Server' ⇨🗎82
- □ 'Deleting Certificates' ⇨🗎83

Displaying Certificates

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

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Select the certificate via the icon* 🔍.

↳ The certificate is displayed.

Creating a Self-Signed Certificate

ℹ

If a self-signed certificate has already been created on the SND Server, you must first delete the certificate; see: ⇨🗎83.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Click* **Self-signed certificate**.
4. *Enter the relevant parameters; see: Table 11* ⇨🗎*79.*
5. *Click* **Install**.

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

Table 11: Parameters for the Creation of Certificates

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

Creating a Certificate Request for CA Certificates

As a preparation for the use of a CA certificate, a certificate request that has to be sent to the certification authority can be created in the SND Server. The certification authority will then create a CA certificate on the basis of the certificate request. The certificate must be in base64 format.

If a certificate request has already been created on the SND Server, you must first delete the certificate request; see: ⇨🗎83.

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY – Certificates**.
3. *Click* **Certificate request**.
4. *Enter the required parameters, see: Table 11 ⇨🗎79.*
5. *Click* **Create a request**.
   The creation of the certificate request is in progress. This may take a few minutes.
6. *Click* **Save** *and save the request in a text file.*
7. *Click* **OK**.
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 SND Server; see: ⇨🗎80.

Saving the CA Certificate in the SND Server

If a CA certificate has already been installed on the SND Server, it will be overwritten.

Requirements

☑ A certificate request has been created at an earlier date; see: ⇨🗎80.

☑ The certificate must be in base64 format.

☞ Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Click* **CA certificate**.
4. *Click* **Browse**.
5. *Specify the CA certificate.*
6. *Click* **Install**.

↳ The CA certificate will be saved in the SND Server.

Saving the Root Certificate on the SND Server

The SND Server offers a number of authentication methods to verify its identity in a network. If you use the authentication method 'EAP-TLS' (⇨🗎85), you must install the root certificate of the authentication server (RADIUS) on the SND Server.

ℹ

If a root certificate has already been installed on the SND Server, it will be overwritten.

Requirements

☑ The certificate must be in base64 format.

☞ Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Click* **Root certificate**.
4. *Click* **Browse**.
5. *Specify the root certificate.*
6. *Click* **Install**.

↳ The root certificate is saved in the SND Server.

Saving PKCS#12 Certificates on the SND Server

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

If a PKCS#12 certificate has already been installed on the SND Server, it will be overwritten.

Requirements

☑ The certificate must be in base64 format.

☑ No certificate request may exist. To delete the certificate request, see: ⇨🗎83.

☑ No CA certificate may be installed. To delete a CA certificate, see: ⇨🗎83.

Proceed as follows:

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

↳ The PKCS12 certificate is saved on the SND Server.

Saving the S/MIME Certificate on the SND Server

S/MIME certificates (*.pem file) are used to sign and encrypt the emails that are sent by the SND Server in the course of the administration via email (⇨🗎22) and the notification service (⇨🗎40).

If an S/MIME certificate has already been installed on the SND Server, it will be overwritten.

Proceed as follows:

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

↳ The S/MIME certificate will be saved on the SND Server.

Deleting Certificates

Proceed as follows:

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

↳ The certificate is deleted.

7.7 How to Use Authentication Methods

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

What is IEEE 802.1x?

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

What is EAP?

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

What is RADIUS?

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

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

What do you want to do?

- □ 'Configuring EAP-MD5' ⇨🗎85
- □ 'Configuring EAP-TLS' ⇨🗎85
- □ 'Configuring EAP-TTLS' ⇨🗎86
- □ 'Configuring PEAP' ⇨🗎88
- □ 'Configuring EAP-FAST' ⇨🗎89

Configuring EAP-MD5

Benefits and Purpose

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

Mode of Operation

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

Requirements

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

Proceed as follows:

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

↳ The settings will be saved.

Configuring EAP-TLS

Benefits and Purpose

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

Mode of Operation

EAP-TLS describes a certificate-based authentication method via a RADIUS server. For this purpose, certificates are exchanged between the SND Server and the RADIUS server. An encrypted TLS connection between the SND Server and the RADIUS server is established in this process. Both RADIUS server and SND Server need a valid, digital certificate signed by a CA. The RADIUS server and the print server must validate the certificate. After the mutual authentication was successful, the access to the network will be freed.

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

ℹ

If you want to use the EAP-TLS authentication, you must observe the instructions below in the indicated order. If this procedure is not adhered to, the SND Server in the network may not be addressable. In this case you have to reset the SND Server parameters; see: ⇨🗎93.

Procedure

- Create a certificate request on the SND Server; see: ⇨🗎80.
- Create a CA certificate using the certificate request and the authentication server.
- Save the CA certificate on the SND Server; see: ⇨🗎80.
- Save the root certificate of the authentication server on the SND Server; see: ⇨🗎81.
- Enable the authentication method 'EAP-TLS' on the SND Server.

☞ Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY – Authentication***.*
3. *Select* **TLS** *from the* **Authentication method** *list.*
4. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Configuring EAP-TTLS

Benefits and Purpose

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

Mode of Operation

EAP-TTLS consists of two phases:

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

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

Requirements

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

☞ Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY – Authentication***.*
3. *Select* **TTLS** *from the* **Authentication method** *list.*
4. *Enter the user name and the password that are used for the configuration of the SND Server on the RADIUS server.*
5. *Select the settings intended to secure the communication in the TLS channel.*
6. *To make the connection more secure, you can also install the root certificate of the RADIUS server on the SND Server (⇨🗎81).*
7. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Configuring PEAP

Benefits and Purpose

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

Mode of Operation

In the case of PEAP (compare EAP-TTLS, see ⇨🗎86), an encrypted TLS (Transport Layer Security) channel is established between the SND Server and the RADIUS server. Only the RADIUS server authenticates itself on the SND Server using a certificate that was signed by a CA.

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

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

Requirements

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

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **SECURITY – Authentication**.
3. *Select* **PEAP** *from the* **Authentication method** *list.*
4. *Enter the user name and the password that are used for the configuration of the SND Server on the RADIUS server.*
5. *Select the settings intended to secure the communication in the TLS channel.*
6. *To make the connection more secure, you can also install the root certificate (⇨🗎81) of the RADIUS server on the SND Server.*
7. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

Configuring EAP-FAST

Benefits and Purpose

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

Mode of Operation

EAP-FAST uses (as in the case of EAP-TTLS, see ⇨🗎86) a channel in order to protect the data transfer. The main difference is that EAP-FAST does not require certificates for authentication purposes. (The use of certificates is optional).

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

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

EAP-FAST uses two methods to generate PACs:

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

Requirements

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

Proceed as follows:

1. *Start the mySND Control Center.*

2. *Select* **SECURITY – Authentication***.*
3. *Select* **FAST** *from the* **Authentication method** *list.*
4. *Enter the user name and the password that are used for the configuration of the SND Server on the RADIUS server.*
5. *Select the settings intended to secure the communication in the channel.*
6. *Click* **Save & Restart** *to confirm.*

↳ The settings will be saved.

8 Maintenance

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

What information do you need?

- 'How to Secure the SND Parameters (Backup)' ⇨🗎91
- 'How to Reset the SND Parameters to their Default Values' ⇨🗎93
- 'How to Perform an Update' ⇨🗎96
- 'How to Restart the SND Server' ⇨🗎97

8.1 How to Secure the SND Parameters (Backup)

All parameter values of the SND Server (exception: passwords) are saved in the ' <default name>_parameters' file.

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

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

What do you want to do?

□ 'Displaying Parameter Values' ⇨🗎92

□ 'Saving the Parameter File' ⇨🗎92

□ 'Loading the Parameter File to the SND Server' ⇨🗎92

Displaying Parameter Values

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **MAINTENANCE - Parameter backup**.
3. *Click the icon* 🔍.

↳ The current parameter values are displayed.

A detailed description of the parameters can be found in the 'Parameter List' ⇨ 🗎102.

Saving the Parameter File

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **MAINTENANCE - Parameter backup**.
3. *Click the icon* ⤓.
4. *Save the '<default name>_parameters.txt' file on a local system with the help of your browser.*

↳ The parameter file is copied and secured.

Loading the Parameter File to the SND Server

Proceed as follows:

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

↳ The parameter values in the file are applied to the SND Server.

8.2 How to Reset the SND Parameters to their Default Values

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

Resetting the SND Server may result in a change in the IP address and a loss of the connection to the mySND File Browser and the mySND Control Center.

When is Resetting Recommended?

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

What do you want to do?

☐ 'Resetting the Parameters via the mySND Control Center' ⇨🗎93

☐ 'Resetting Parameters via the InterCon-NetTool' ⇨🗎94

☐ 'Resetting the Parameters via the Reset Button' ⇨🗎94

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

Resetting the Parameters via the mySND Control Center

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **MAINTENANCE – Default settings**.
3. *Click* **Reset device to default settings**.
4. *Confirm the security query by clicking* **Reset**.

↳ The parameters are reset.

Resetting Parameters via the InterCon-NetTool

Proceed as follows:

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

↳ The parameters are reset.

Resetting the Parameters via the Reset Button

LEDs, the reset button and various ports can be found on the SND Server. These components are described in the 'Quick Installation Guide'.

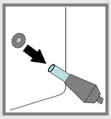
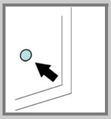
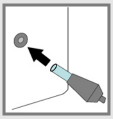
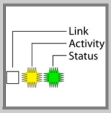
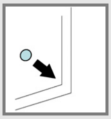
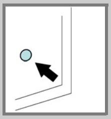
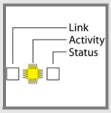
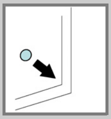
Using the reset button you can reset the SND Server's parameter values to their default setting. The reset process can be divided into two phases:

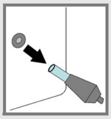
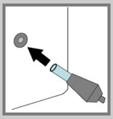
- During phase 1, the device is forced into the reset mode. During the reset mode, the parameters are reset.
- The second phase describes the restart of the device.

⚠

IMPORTANT: The reset mode is indicated by the synchronous blinking of the activity LED (yellow) and the status LED (green) and last for about five intervals.
You must release the reset button within this time frame, otherwise the device switches to the BIOS mode. If this happens, try the reset again.

The phases are described in the following:

[Phase 1] Reset	
	Switching off the SND Server (interrupt the power supply).
	Press and hold the reset button.
	Switching on the SND Server (establish the power supply).
	Wait until the activity LED and status LED blink synchronously. *The reset mode has been activated.*
	Release the reset button for about 2 seconds. *The LEDs blink alternatingly.*
	Press and hold the reset button again. *The LEDs blink synchronously.*
	*After a few seconds, only the activity LED will blink.*
	Release the reset button.

[Phase 2] Restart	
	Switching off the SND Server (interrupt the power supply).
	Switching on the SND Server (establish the power supply).

8.3 How to Perform an Update

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

What Happens during an Update?

In the course of an update, the existing firmware/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 functions do not work properly and if SEH Computertechnik GmbH has released a new software or firmware version with new functions or bug fixes.

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

Where Do I Find the Update Files?

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

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

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

Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **MAINTENANCE - Update**.
3. *Click* **Browse**.
4. *Select the update file.*
5. *Click* **Install**.

↳ The update is executed. The SND Server is restarting.

8.4 How to Restart the SND Server

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

What do you want to do?

□ 'Restarting the SND Server via the mySND Control Center' ⇨🗎97

□ 'Restarting the SND Server via the InterCon-NetTool' ⇨🗎97

Restarting the SND Server via the mySND Control Center

☞ Proceed as follows:

1. *Start the mySND Control Center.*
2. *Select* **MAINTENANCE - Restart**.
3. *Click* **Restart device**.
4. *Confirm the security query by clicking* **Restart**.

↳ The SND Server is restarting.

Restarting the SND Server via the InterCon-NetTool

☞ Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Highlight the SND Server in the device list.*
3. *Select* **Actions – Restart** *from the menu bar.*
4. *Click* **Finish**.

↳ The SND Server is restarting.

9 Appendix

The appendix contains a glossary, the parameter list of the SND Server, and the index lists.

What information do you need?

- 'Glossary' ⇨🗎99
- 'Parameter List' ⇨🗎102
- 'Troubleshooting' ⇨🗎119
- 'List of Figures' ⇨🗎122
- 'Index' ⇨🗎123

9.1 Glossary

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

What information do you need?

Manufacturer-Specific Software Solutions

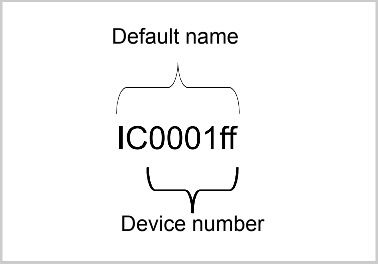
- 'mySND Control Center' ⇨🖹101
- 'mySND File Browser' ⇨🖹101
- 'InterCon-NetTool' ⇨🖹101

Network Technology

- 'Hardware Address' ⇨🖹100
- 'IP Address' ⇨🖹101
- 'Host Name' ⇨🖹100
- 'Gateway' ⇨🖹100
- 'Subnet Mask' ⇨🖹101
- 'Default Name' ⇨🖹99

Default Name

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



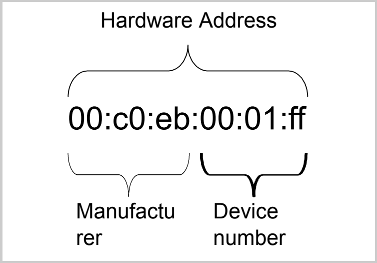
The default name can be found in the mySND Control Center or in the InterCon-NetTool.

Gateway

Using a gateway, you can address IP addresses from external networks. If you want to use a gateway, you can configure the relevant parameter in the SND Server via the mySND Control Center.

Hardware Address

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



The hardware address can be found on the housing or in the InterCon-NetTool.

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

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

Host Name

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

InterCon-NetTool

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

IP Address

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

mySND Control Center

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

mySND File Browser

The mySND File Browser is used to access files and to work with files (download, etc.). The mySND File Browser is stored in the SND Server and can be displayed by means of a browser software (Internet Explorer, Firefox, Safari).

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. By default, the SND Server is configured for the use without subnetworks. If you want to use a subnetwork, you can configure the relevant parameter in the SND Server via the mySND Control Center.

9.2 Parameter List

This section contains an overview of all the parameters of the SND Server. The parameter list provides details about the functions and values of the individual parameters.

What information do you need?

- 'Parameter List - IPv4' ⇨🖹103
- 'Parameter List – IPv6' ⇨🖹103
- 'Parameter List - DNS' ⇨🖹104
- 'Parameter List - SNMP' ⇨🖹104
- 'Parameter List - POP3' ⇨🖹106
- 'Parameter List - SMTP' ⇨🖹106
- 'Parameter List - Email Limits' ⇨🖹108
- 'Parameter List - Bonjour' ⇨🖹108
- 'Parameter List - Description' ⇨🖹109
- 'Parameter List - Date/Time' ⇨🖹109
- 'Parameter List - Notification' ⇨🖹109
- 'Parameter List - User Management' ⇨🖹111
- 'Parameter List - Media Assignment' ⇨🖹113
- 'Parameter List – File Filters' ⇨🖹113
- 'Parameter List - Automatic File Transfer' ⇨🖹114
- 'Parameter List - SSL Connections' ⇨🖹115
- 'Parameter List - Device Access' ⇨🖹116
- 'Parameter List - TCP port access' ⇨🖹116
- 'Parameter List - Authentication' ⇨🖹117

To view the current parameter values of your SND Server, see: 'Displaying Parameter Values' ⇨🖹92.

Table 12: Parameter List - IPv4

Parameters	Value	Default	Description
ip_dhcp [DHCP]	on/off	on	Enables/disables the DHCP protocol.
ip_bootp [BOOTP]	on/off	on	Enables/disables the BOOTP protocol.
ip_auto [ARP/PING]	on/off	on	Enables/disables the IP address assignment via ARP/PING.
ip_addr [IP address]	valid IP address	169.254.0.0/16	Defines the IP address of the SND Server.
ip_mask [Subnet mask]	valid IP address	255.255.0.0	Defines the subnet mask of the SND Server.
ip_gate [Gateway]	valid IP address	0.0.0.0	Defines the gateway address of the SND Server.

Table 13: Parameter List – IPv6

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

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

Table 14: Parameter List - DNS

Parameters	Value	Default	Description
dns [DNS]	on/off	on	Enables/disables the name resolution via a DNS server.
dns_primary [Primary DNS server]	valid IP address	0.0.0.0	Defines the IP address of the primary DNS server.
dns_secondary [Secondary DNS server]	valid IP address	0.0.0.0	Defines the IP address of the secondary DNS server. *The secondary DNS server is used if the primary DNS server is not available.*
dns_domain [Domain name (suffix)]	max. 64 characters [., a-z, A-Z, 0-9]	[blank]	Defines the domain name of an existing DNS server.

Table 15: Parameter List - SNMP

Parameters	Value	Default	Description
snmpv1 [SNMPv1]	on/off	on	Enables/disables SNMPv1.

Parameters	Value	Default	Description
snmpv1_ronly [Read-only]	on/off	off	Enables/disables the write protection for the community.
snmpv1_community [Community]	max. 64 characters [a-z, A-Z, 0-9]	public	Defines the name of the SNMP community. *The SNMP community is a basic form of access protection in which several participants with the same access rights are grouped together.*
snmpv3 [SNMPv3]	on/off	on	Enables/disables SNMPv3.
any_name [User name]	max. 64 characters [a-z, A-Z, 0-9]	anonymous	Defines the name of the SNMP user group 1.
any_pwd [Password]	8-64 characters [a-z, A-Z, 0-9]	[blank]	Defines the password of the SNMP user group 1.
any_hash [Hash]	md5 sha	md5	Specifies the hash algorithm of the SNMP user group 1.
any_rights [Access rights]	--- [None] readonly readwrite	readonly	Defines the access rights of the SNMP user group 1.
any_cipher [Encryption]	--- [None] aes des	---	Defines the encryption method of the SNMP user group 1.
admin_name [User name]	max. 64 characters [a-z, A-Z, 0-9]	admin	Defines the name of the SNMP user group 2.
admin_pwd [Password]	8-64 characters [a-z, A-Z, 0-9]	administrator	Defines the password of the SNMP user group 2.
admin_hash [Hash]	md5 sha	md5	Specifies the hash algorithm of the SNMP user group 2.
admin_rights [Access rights]	--- [None] readonly readwrite	readwrite	Defines the access rights of the SNMP user group 2.
admin_cipher [Encryption]	--- [None] aes des	---	Defines the encryption method of the SNMP user group 2.

Table 16: Parameter List - POP3

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

Table 17: Parameter List - SMTP

Parameters	Value	Default	Description
smtp_srv [Server name]	max. 128 characters	[blank]	Defines the SMTP server via the IP address or the host name. *The host name can only be used if a DNS server was configured beforehand.*

Parameters	Value	Default	Description
smtp_port [Server port]	1–65535 [1-5 characters; 0-9]	25	Defines the port number used by the SND Server to send emails to the SMTP server.
smtp_ssl [TLS]	on/off	off	Enables/disables TLS. *The security protocol TLS (Transport Layer Security) is used to encrypt the transmission between the SND Server and the SMTP server.*
smtp_sender [Sender name]	max. 128 characters	[blank]	Defines the email address used by the SND Server to send emails. *Very often the name of the sender and the user name are identical.*
smtp_auth [Login]	on/off	off	Enables/disables the SMTP authentication for the login.
smtp_usr [User name]	max. 128 characters	[blank]	Defines the user name used by the SND Server to log on to the SMTP server.
smtp_pwd [Password]	max. 128 characters	[blank]	Defines the password used by the SND Server to log on to the SMTP server.
smtp_sign [Security (S/MIME)]	on/off	off	Enables/disables the encryption and signing of emails via S/MIME. *Only emails from the administration and the notification service can be encrypted.*
smtp_encrypt [Full encryption] [Signing of emails]	on/off [off = sign, on = encrypt]	off	Defines the signing and encryption of emails.
smtp_attpkey [Attach public key]	on/off	on	Enables/disables the attachment of a public key to an email.

Table 18: Parameter List - Email Limits

Parameters	Value	Default	Description
autoSndMaxKb [Total file size limit]	100–10000 [3-5 characters; 0-9]	5000	Defines the total size limit (in kB) of the files that are sent via email during the file transfer via the mySND File Browser (⇨🗎64) and the automatic file transfer (⇨🗎53). *If the defined value is exceeded, the remaining files will be sent in additional emails during the automatic file transfer.*
autoSndMaxFiles [Maximum number of files]	1–100 [1-3 characters; 0-9]	10	Defines the maximum number of files that are sent via email during the file transfer via the mySND File Browser (⇨🗎64) and the automatic file transfer (⇨🗎53). *If the defined value is exceeded, the remaining files will be sent in additional emails during the automatic file transfer.*

Table 19: Parameter List - Bonjour

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

Table 20: Parameter List - Description

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

Table 21: Parameter List - Date/Time

Parameters	Value	Default	Description
ntp [Date/Time]	on/off	on	Enables/disables the use of a time server (SNTP).
ntp_server [Time server]	max. 64 characters [., a-z, A-Z, 0-9]	pool.ntp.org	Defines a time server via the IP address or the host name. *The host name can only be used if a DNS server was configured beforehand.*
ntp_tzone [Time zone]	UTC, GMT, EST, EDT, CST, CDT, MST, MDT, PST, PDT, etc.	CET/CEST (EU)	The time zone is used to equalize the difference between the time received over the time server and the local time, including country-specific particularities such as Daylight Saving Time.

Table 22: Parameter List - Notification

Parameters	Value	Default	Description
mailto_1 mailto_2 [Email address]	valid email address [max. 64 characters]	[blank]	Defines the email address of the recipient for notifications.
noti_dev_1 noti_dev_2 [medium connected/disconnected]	on/off	off	Enables/disables the sending of emails after a removable medium was connected to or disconnected from the SND server.

Parameters	Value	Default	Description
noti_pup_1 noti_pup_2 [Restart]	on/off	off	Enables/disables the sending of emails when the SND Server is restarted.
noti_stat_1 noti_stat_2 [Status email]	on/off	off	Enables/disables the periodical sending of a status email to recipient 1 or 2.

notistat_d
[Status notification time]
	al = daily
	mo = Monday
	tu = Tuesday
	we = Wednesday
	th = Thursday
	fr = Friday
	sa = Saturday
	su = Sunday
		al	Specifies the interval at which a status email is sent.

notistat_h [hh]	1 = 1. hour 2 = 2. hour 3 = 3. hour etc.	0	Specifies the time at which a status email is sent.
notistat_tm [mm]	0 = 00 minutes 1 = 10 minutes 2 = 20 minutes 3 = 30 minutes 4 = 40 minutes 5 = 50 minutes	0	Specifies the time at which a status email is sent.
trapto_1 trapto_2 [Trap target]	valid IP address	0.0.0.0	Defines the SNMP trap address of the recipient for notifications.
trapcommu_1 trapcommu_2 [Trap community]	max. 64 characters [a-z, A-Z, 0-9]	public	Defines the SNMP trap community of the recipient.
trappup [Restart]	on/off	off	Enables/disables the sending of SNMP traps when the SND Server is restarted.
trapdev [medium connected/disconnected]	on/off	off	Enables/disables the sending of SNMP traps after a removable medium was connected to or disconnected from the SND server.

Table 23: Parameter List - User Management

Parameters	Value	Default	Description
user_active_2 ~ user_active_5	on/off	off	Enables/disables the user account. *(The administrator account cannot be disabled.)*
user_name_2 ~ user_name_5 [User name]	max. 32 characters [a-z, A-Z, 0-9]	[blank]	Defines the name for the user account in order to log on to the SND server. *(The name of the administrator account cannot be changed.)*
user_pwd_1 ~ user_pwd_5 [Password]	max. 32 characters [a-z, A-Z, 0-9]	user_pwd_1 = admin user_pwd_2 ~ user_pwd_5 = [blank]	Defines the password for the user account in order to log on to the SND server.
user_email_1 ~ user_email_5 [Email address]	valid email address [max. 64 characters]	[blank]	Defines the email address suggestions for the automatic file transfer.
user_rAdm_2 ~ user_rAdm_5 [Administration]	on/off	off	Enables/disables the administrative access to the mySND Control Center. All connected removable media can be displayed. *Only system administrators should have access to the mySND Control Center because this is where security-related settings can be configured.* *(The option cannot be disabled for the administrator account.)*

Parameters	Value	Default	Description
user_rWr_1 ~ user_rWr_5 [Renaming/deleting files]	on/off	user_rWr_1 = on user_rWr_2 ~ user_rWr_5 = off	Enables/disables the feature for renaming and deleting files in the mySND File Browser.
user_rDl_1 ~ user_rDl_5 [Downloading files]	on/off	user_rDl_1 = on user_rDl_2 ~ user_rDl_5 = off	Enables/disables the download feature in the mySND File Browser.
user_rSd_1 ~ user_rSd_5 [Emailing files]	on/off	user_rSd_1 = on user_rSd_2 ~ user_rSd_5 = off	Enables/disables the email feature in the mySND File Browser.
user_rTog_1 ~ user_rTog_5 [Set/clear archive bit]	on/off	user_rTog_1 = on user_rTog_2 ~ user_rTog_5 = off	Enables/disables the archive bit feature in the mySND File Browser.
user_fFilter_1 ~ user_fFilter_5 [File filters]	0–5 [Number of one of the file filters defined on the SND Server: 0 = no files 1 = all files 2 = filter 2 3 = filter 3 4 = filter 4 5 = filter 5]	1	Defines a file filter for the user account. After logging on to the mySND File Browser, only files of the file types defined in the filter will be displayed.

Table 24: Parameter List - Media Assignment

Parameters	Value	Default	Description
sdCardCid_1 ~ sdCardCid_16 [Device ID]	hexadecimal digit [32 characters]	[blank]	Defines the device ID of an SD card for the unique identification on the SND Server and the assignment to the user accounts. *The device ID of an SD card connected to the SND Server is shown in the mySND Control Center.*
sdCardName_1 ~ sdCardName_16 [Assignment name]	max. 32 characters [a-z, A-Z, 0-9]	[blank]	Freely definable name for the media assignment.
sdCardUList_1 ~ sdCardUList_16 [User]	User account number [1–16; Multiple entries are to be separated by commas]	[blank]	Assigns one or more user accounts to the SD card. *Only assigned user accounts can access the SD card in the* mySND File Browser. *(Exception: Users with administrator privilege can access all removable media on the* SND Server.*)*

Table 25: Parameter List – File Filters

Parameters	Value	Default	Description
fFilter_name_2 ~ fFilter_name_5 [Filter name]	max. 32 characters [a-z, A-Z, 0-9]	[blank]	Freely definable name of the file filter. *The name of the file filter 'All files' cannot be changed.*
fFilter_2 ~ fFilter_5 [Accessible file types]	max. 64 characters [., a-z, A-Z, 0-9]	[blank]	Defines the file types displayed in the mySND File Browser by their file extension. - Schema: .<Extension> - File types without extension will be defined by a dot. - Multiple entries are to be separated by blanks. *The file types of the file filter 'All files' cannot be changed.*

Table 26: Parameter List – Automatic File Transfer

Parameters	Value	Default	Description
autoSndPDMedia	on/off	on	Enables/disables the automatic file transfer from USB mass storage devices.
autoSndPDRcp_1 autoSndPDRcp_2 [Recipient 1, Recipient 2]	valid email address [max. 64 characters]	[blank]	Defines the email address of the recipient for the automatic file transfer from USB mass storage devices.
autoSndPDDir [Source folder]	max. 64 characters [/, a-z, A-Z, 0-9]	/ [Root directory]	Defines the folder on USB mass storage devices from which the files will be transferred automatically. *The content from subfolders will not be transferred.*
autoSndPDExt [File types]	max. 32 characters [., a-z, A-Z, 0-9]	[blank]	Defines the file types that are transferred automatically from USB mass storage devices by their file extension. - Schema: .<Extension> - File types without extension will be defined by a dot. - Multiple entries are to be separated by blanks.
autoSNDPDaBit [Set archive bit]	on/off	on	Marks files that are transferred from USB mass storage devices by an archive bit. *Marked files will not be transferred again when the removable medium is reconnected to the SND server.* *No archive bit can be set with read-only USB mass storage devices.*
autoSndSDMedia_1 ~ autoSndSDMedia_16	on/off	on	Enables/disables the automatic file transfer from SD cards with media assignment.
sdCardAutoRcp_1 ~ sdCardAutoRcp_16 [Recipient]	valid email address [max. 64 characters]	[blank]	Defines the email address of the recipient for the automatic file transfer from SD cards with media assignment.

Parameters	Value	Default	Description
autoSndSDDir_1 ~ autoSndSDDir_16 [Source folder]	max. 64 characters [/, a-z, A-Z, 0-9]	/ [Root directory]	Defines the folder on SD cards from which the files will be transferred automatically. *The content from subfolders will not be transferred.*
autoSndSDExt_1 ~ autoSndSDExt_16 [File types]	max. 32 characters [., a-z, A-Z, 0-9]	[blank]	Defines the file types that are transferred automatically from SD cards. - Schema: .<Extension> - File types without extension will be defined by a dot. - Multiple entries are to be separated by blanks.
autoSndSDaBit_1 ~ autoSndSDaBit_16 [Set archive bit]	on/off	on	Marks files that are transferred from SD cards by an archive bit. *Marked files will not be transferred again when the removable medium is reconnected to the SND server.* *No archive bit can be set with read-only SD cards.*

Table 27: Parameter List - SSL Connections

Parameters	Value	Default	Description
security [Encryption]	1–4 [1 characters]	2	Defines the encryption level to be used for SSL/TLS connections. *1 = low (56 bit)* *2 = medium (128 bit)* *3 = high (128 - 256 bit)* *4 = compatible (40 - 256 bit)*

Table 28: Parameter List - Device Access

Parameters	Value	Default	Description
http_allowed [HTTP/HTTPS]	on/off	on	Defines the permitted type of connection (HTTP/HTTPS) to the mySND File Browser and the mySND Control Center. *If HTTPS is exclusively chosen as the connection type [http_allowed = off], the web access to the* mySND File Browser *and the* mySND Control Center *is protected via SSL/TLS.*
sessKeyTimer [Session timeout]	on/off	on	Enables/disables the termination of inactive sessions after the expiration of the defined session duration.
sessKeyTimeout [Session duration]	120–3600 [3–4 characters; 0-9]	600	Defines the time interval (in seconds) after which a session on the SND server is aborted for security reasons after a period of inactivity.
usbEnable [USB port]	on/off	off	Enables/disables the USB port on the SND Server.

Table 29: Parameter List - TCP port access

Parameters	Value	Default	Description
protection [Port access control]	on/off	off	Enables/disables the locking of the selected ports.
protection_test [Test mode]	on/off	on	Enables/disables the test mode. *The test mode allows you to test the parameters set using the access control. If the test mode is activated, the access protection remains active until the* SND Server *is rebooted.*

Parameters	Value	Default	Description
protection_level [Security level]	protec_tcp protec_all	protec_tcp	Specifies the port types to be locked: - TCP ports - all ports (IP ports)
ip_filter_on_1 ~ ip_filter_on_8 [IP address]	on/off	off	Enables/disables an exception from the port locking.
ip_filter_1 ~ ip_filter_8 [IP address]	valid IP address	[blank]	Defines elements that are excluded from port locking, using the IP address.
hw_filter_on_1 ~ hw_filter_on_8 [MAC address]	on/off	off	Enables/disables an exception from the port locking.
hw_filter_1 ~ hw_filter_8 [MAC address]	valid hardware address	00:00:00: 00:00:00	Defines elements that are excluded from port locking, using the hardware address.

Table 30: Parameter List – Authentication

Parameters	Value	Default	Description
auth_typ [Authentication method]	--- [None] MD5 TLS TTLS PEAP FAST	---	Defines the authentication method that is used to identify devices or users in the network.
auth_name [User name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the name of the SND Server as saved in the authentication server (RADIUS).
auth_pwd [Password]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the password of the SND Server as saved in the authentication server (RADIUS).

Parameters	Value	Default	Description

auth_extern [PEAP/EAP-FAST Options]	--- = none
	PLABEL0 = PEAPLABEL0
	PLABEL1 = PEAPLABEL1
	PVER0 = PEAPVER0
	PVER1 = PEAPVER1
	FPROV1 = FASTPROV1
		---	Defines the kind of external authentication for the EAP authentication methods TTLS, PEAP, and FAST.

auth_intern [Inner Authentication]	--- = none
	PAP = PAP
	CHAP = CHAP
	MSCHAP2 = MS-CHAPv2
	EMD5 = EAP-MD5
	ETLS = EAP-TLS
		---	Defines the kind of inner authentication for the EAP authentication methods TTLS, PEAP, and FAST.

auth_ano_name [Anonymous name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the anonymous name for the unencrypted part of the EAP authentication methods TTLS, PEAP, and FAST.
auth_wpa_addon [WPA add-on]	max. 255 characters [a-z, A-Z, 0-9]	[blank]	Specifies an optional WPA expansion.

9.3 Troubleshooting

This chapter describes some problems and their solutions.

Problem

- 'The SND Server indicates the BIOS mode' ⇨🗎119
- 'A connection to the mySND Control Center/mySND File Browser cannot be established.' ⇨🗎120
- 'The password is no longer available' ⇨🗎121

The SND Server indicates the BIOS mode

Possible Cause

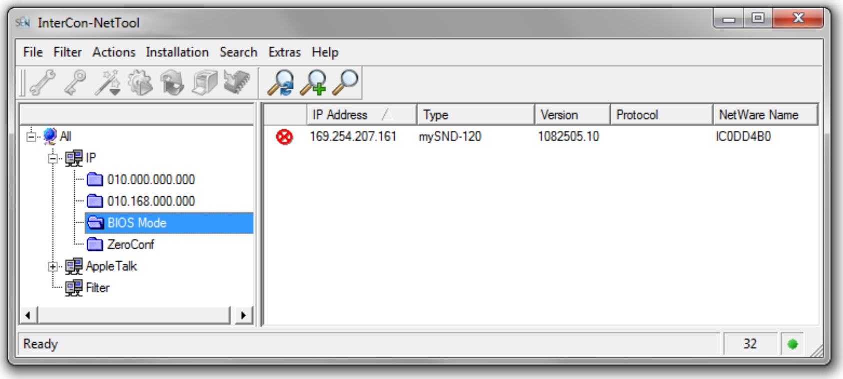
The SND Server switches to the BIOS mode if the firmware functions well but the software is faulty. This may happen in the case of an incorrect software update, for example. The SND Server indicates the BIOS mode if

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

⚠

The SND Server is not operational in the BIOS mode.

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



	IP Address	Type	Version	Protocol	NetWare Name
⊗	169.254.207.161	mySND-120	1082505.10		IC0DD4B0

Fig. 8: InterCon-NetTool – SND Server in BIOS Mode

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

Gehen Sie wie folgt vor:

1. *Start the InterCon-NetTool.*
2. *Highlight the SND Server in the device list.*
   You will find the *SND Server* **under the filter 'BIOS mode'.**
3. *Select* **Installation – IP Wizard** *from the menu bar.*
   The IP Wizard is started.
4. *Follow the instructions of the wizard in order to assign an IP address to the SND Server.*
   The IP address is saved.
5. *Carry out a software update on the SND Server; see: ⇨🗎96.*

↳ The software will be saved on the SND Server. The SND Server switches to the normal mode.

A connection to the mySND Control Center/mySND File Browser cannot be established.

Eliminate possible error sources. First of all, check:

- the cabling connections,

- the IP address of the SND Server (⇨🗎12) as well as

- the proxy settings of your browser.

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

□ The TCP port access control is enabled ⇨🗎74.

□ The access is protected via SSL/TLS (HTTPS) ⇨🗎71.

□ The cipher suites of the encryption level are not supported by the browser ⇨🗎69.

The password is no longer available

The access to the SND server is controlled by means of user accounts. You will need a user name and a password to get access to the program.

If the password is no longer available, you can reset the parameter values of the SND Server to their default settings to get access ⇨🗎93. Previous settings will be deleted.

9.4 List of Figures

Starting the mySND Control Center 18
InterCon-NetTool - Main Dialog 21
Administration via Email - Example 1 24
Administration via Email - Example 2 24
InterCon-NetTool - IP Wizard 27
mySND File Browser 59
mySND Control Center - Certificates 77
InterCon-NetTool – SND Server in BIOS Mode 119

9.5 Index

A

Address
  Hardware Address 100
  IP address 101
  MAC Address 100
Admin account 43
Archive bit 53
ARP/PING 15
Assign SD card 48
Authentication 84

B

Backup
  Data backup 10
  Parameters 91
Backup copy
  Data 10
  Parameters 91
Bonjour 36
BOOTP 13
Browser 6

C

CA certificate 76
Certificate 76
  create 78
  delete 83
  display 78
  Saving 80
Certificate request 80
Cipher Suite 69

D

Data backup 10
Default certificate 76
Default name 99
Default settings 93
Descriptions 38
Device number 99
DHCP 13
Disclaimer 11
DNS (Domain Name Service) 30
Documentation 7

E

EAP 84
EAP-FAST 89
EAP-MD5 85
EAP-TLS 85
EAP-TTLS 86
Email Limits 33
Enable/disable USB port 73
Encryption Level 69

F

File filters
  assign 43
  Configuring 50
File transfer (automatic) 53
Files
  delete 66
  display 60
  email 64
  rename 65
  search 63
  sort 62

G

Gateway 100

H

Hardware Address 100
Host name 100
Hotline 9
HTTP/HTTPS 71

I

IEEE 802.1x 84
Improper Use 10
Inactivity 72
Intended Use 10
InterCon-NetTool 20
  install 20
  IP Wizard 14
  Start 20
  Structure 21
IP address 101
  Saving 12
IPv4 25
IPv6 28

L

Login 43
  multiple 72

M

MAC Address 100
Maintenance 91
Media assignment 48
mySND (my Secure Network Device) 6
mySND Control Center 17
  Language 19
  login 17
  Start 17
  Structure 19
mySND File Browser 57
  delete feature 66
  Download 64
  File types 60
  Language 59
  login 58, 59
  renaming feature 65
  Search feature 63
  send email 64
  Sort feature 62
  Start 58
  Structure 59

N

Network Settings 25
Notification Service 40
Notification service
  Email 41
  SNMP trap 41
Notifications 40

P

Parameter file 91
Parameter list 102
Parameters
  default settings 93
  display 92
  Load 92
  Resetting 93
  Saving 92
Password 42
PEAP 88
POP3 32
Protection 68
Protocol
  BOOTP 13
  DHCP 13
  IPv4 25
  IPv6 28
  POP3 32
  SMTP 32
  SNMP 31
  SNTP 39
  SSL/TLS 69
Purpose 6

R

RADIUS 84
Removable medium 7
  format 47
  rename 48
Reset 93
Reset button 24, 94
Restart 97
Restrict file access

Disable USB port 73
File filters 50
Rights 43
Root certificate 76

S

S/MIME certificate 77
Security 68
Security level 74
Self-signed certificate 76
Session 72
exit 73
Time out 72
Session timeout 72
SMTP 32
SNMP trap 40
SNMPv1 31
SNMPv3 31
SSL/TLS connection 69
Subnet mask 101
Support 9
System Requirements 6

T

TCP port access control 74
TCP/IP 25
Test mode 74
Time of the device 39
Time server 39
Time zone 39
Types of connection 71
define 71

U

Update 96
User account 42
assign file filters 43
enable/disable 43
Rights 43
UTC 39

V

Version Number 96

Z

ZeroConf 13