

genuReSI

Installation and Configuration Manual

Version 1.18

^rgenua.

Edition: April 4, 2025 Revision: d35c544

Copyright ©2002–2025 genua GmbH. All rights reserved.

This product contains software based on the OpenBSD operating system.

genua GmbH Domagkstrasse 7 85551 Kirchheim/Munich Tel.: +49 89-991950-0 Fax : +49 89-991950-999

All trademarks and licenses indicated in the user manual are the property of their respective owners and are mentioned for information purposes only.

Registered trademarks of genua GmbH are listed on this website: https://kunde.genua.de/en/imprint/trademark.html

With kind regards,

genua GmbH

Contents **Genua**.

Contents

Pre	face		v
1	Main	tenance with the Rendezvous Concept	1
	1.1	The genua rendezvous concept	2
	1.2	Using the genuReSI Maintenance Application	3
2	Laun	ching the genuReSI Windows Application	5
	2.1	Installation Requirements	6
	2.2	Installation and Configuration	7
3	genu	ReSI for Maintainers	9
	3.1	Duties of the Maintainer	10
	3.2	Establishing/Terminating the Maintenance Connection	10
	3.3	Recording the Connection using RDP	11
	3.4	Data Exchange between Maintainer and Target System	12
	3.5	Configuration Updates	13
	3.6	Logging/History	14
	3.7	Local Settings	16
	3.8	Commands	18
	3.9	Plugins	19
	3.10	genuReSI Update	20
	3.11	genuReSI USB/Portable Mode	20
4	genu	ReSI for Operators	21
	4.1	Duties of the Operator	22
	4.2	Establishing/Terminating the Maintenance Connection	22
	4.3	Access Control at Runtime	24
	4.4	Recording the Connection with RDP and SSH	25

Genua. Contents

	4.5	Share Option	26
	4.6	Configuration Updates	27
	4.7	Logging/History	28
	4.8	Local Settings	30
	4.9	genuReSI Update	31
5	Adva	nced Configuration	33
	5.1	Configuration Files	34
	5.2	Role Management	35
	5.3	Using a Smart card	36
	5.4	Use with Firewall/NAT Gateway	39
	5.5	HTTP Proxy for SSH	40
	5.6	GUI Layout	41
	5.7	New Commands	42
6	STEF	27 via Rendezvous	43
	6.1	GUI Installation of the Loopback Adapter	44
	6.2	Command Line Installation of the Loopback Adapter	45
	6.3	IP Configuration	45
Inc	lex		49

Preface

About this Product

The genuReSI (Remote Secure Integration) Windows application offers a clear, easy-to-use interface for the configuration, administration and supervision of maintenance associations used within the Rendezvous maintenance concept.

Formatted Text

- Text: Console input or output, commands, filenames and path
- "Text": Text to be entered into GUI fields; names of icons, links, and external applications
- Key : Key on the keyboard or button in the GUI
- Menu \rightarrow Submenu: Menu path in the GUI

Warnings

Note: Notes provide additional information suitable for simplifying certain workflows or highlighting feature limitations.

!	Attention! The level Attention warns about minor security risks, minor or short-term disruption in operation.
!	Warning! The level Warning warns about major security risks, major or long- term disruptions of operation.
!	Danger! The level Danger warns about severe security risks, complete or permanent disruption in operation or permanent loss of data, if not observed.

Changes to the Manual

The manual is updated for every new release to reflect the changes to the software. It describes the respective current state of the genuReSI software.

Customer Portal of genua

Our customer portal can be reached under https://kunde.genua.de/en.html/. After you have logged in with your credentials, select Products \rightarrow genubox \rightarrow Maintenance App (genuReSI) in the main navigation to enter the customer support area of genubox and genuReSI.

Here you can access the Knowledge Base, Best Practices, Known Issues, Release Notes and Software Patches.

Feedback on the Manual

Your opinion is important to us. Please contact us if you require further information. Just send us an e-mail to: support@genua.de

^rgenua.

3

1

Chapter 1

Maintenance with the Rendezvous Concept

1.1	The genua rendezvous concept	2

1.2 Using the genuReSI Maintenance Application



1.1 The genua rendezvous concept

Figure 1.1: rendezvous concept

At the heart of the rendezvous concept is the rendezvous server (typically a genubox). This server can be located in the DMZ of the equipment manufacturer or service provider. A genubox operates as a firewall and VPN solution upstream of the equipment being maintained, isolating the equipment from the rest of the IT network.

The maintenance time frame is usually precisely defined. The **remote service provider** first establishes a VPN connection to the Rendezvous Box and must authenticate there. However, he cannot establish any direct connections to the customer network. The **operator** (an administrator from the customer network) must establish the connection between the rendezvous server and the service box. The connection between the maintainer and the object being maintained is then established via these two VPN tunnels. The maintainer can launch his software, authenticate with the machine being maintained, and start working.

The connection from the maintainer to the rendezvous server is established via SSH VPN.

After the maintenance work is finished, both the maintainer and the operator terminate the established connections.

Neither the maintainer nor the operator require deep knowledge of the system, since the entire rendezvous solution is configured centrally via the rendezvous server and a management system (genucenter).

1.2 Using the genuReSI Maintenance Application

Using the genuReSI (genua Remote Secure Integration) Windows application, the maintainer can establish the maintenance connection with a mouse click. This permits easy configuration and administration of the maintenance association via the easy-to-use GUI.

All sessions are logged. Depending on the configuration, they can also be recorded. This can be used for training purposes, for example.

The operator can also use genuReSI to enable the maintenance connection if he prefers a Windows application over the web-based GUI.

3

^rgenua.

^rgenua.

Chapter 2

Launching the genuReSI Windows Application

2.1	Installation Requirements	6
2.2	Installation and Configuration	7

5

2.1 Installation Requirements

- Configuration file <<u>config</u> name>.resi and the password that can be assigned to protect the configuration file. This is generated and made available on the genucenter by the equipment manufacturer or maintenance operator.
- Executable file ReSI.exe (the most recent version is available for download in the genua customer portal https://kunde.genua.de/en). Execute the file as a normal user to start genuReSI App. The app does not require installation or administrator privileges.

Note: genuReSI App is digitally signed by a genua certificate. The signature is automatically verified by Windows. Alternatively, you can verify the signature manually as follows:

- 1. Right click on the genuReSI app icon and navigate to Properties \rightarrow Digital Signatures.
- 2. Select the certificate genua GmbH and click on <u>Details</u>. In the General tab, information regarding the validity of the certificate is displayed.
- PC with a Windows OS that supports Microsoft .Net Framework version 4.8 and higher
- Microsoft .NET Framework version 4.8 and higher

Note: This version of the Microsoft .NET Framework is automatically installed with Windows 7 SP2 or higher. For older versions, the Client Profile may be downloaded in the Microsoft customer portal. Alternatively, you can use the external download link in the genua customer portal. Visit https://kunde.genua.de/en, log in and click on Downloads \rightarrow Releases \rightarrow Maintenance App 1.18 Release. The download link is in the genubox section.

2.2 Installation and Configuration

2.2.1 Installation genuReSI

Move the ReSI.exe file to the desired directory, for example:

C:\Users\<Username>\Desktop

on the genuReSI icon to launch the application.

Before starting, enter a configuration password to prevent unauthorized access. The password can also be saved by selecting "Save Password".



Figure 2.1: genuReSI Start Screen

- 1. Rendezvous connection/logging selection window
- 2. Main window
- 3. Toolbar

Meaning of the icons from left to right:

- Import configuration
- Settings
- History

7

2.2.2 Importing the Configuration

The corresponding dialog will be opened by any of the following: Via the File \rightarrow Import configuration menu, the link in the left window, the import button in the toolbar (second icon from the left), or the key combination Ctrl+1. Only applicable configuration files (*.resi) are shown here. Select the applicable configuration file and click on Open. If the configuration file is password protected, the password must be entered and confirmed with OK. If the configuration already exists, a message is displayed and the configuration can be renamed or canceled.

The imported configuration appears in the left window under **Maintenances / Service Boxes**. If multiple configurations are available, you have to import the other configuration files accordingly. The applicable configuration can be selected later in the left window.



Figure 2.2: Maintenances / Service Boxes

^rgenua.

Chapter 3

genuReSI for Maintainers

3.1	Duties of the Maintainer	10
3.2	Establishing/Terminating the Maintenance Connection	10
3.3	Recording the Connection using RDP	11
3.4	Data Exchange between Maintainer and Target System	12
3.5	Configuration Updates	13
3.6	Logging/History	14
3.7	Local Settings	16
3.8	Commands	18
3.9	Plugins	19
3.10	genuReSI Update	20
3.11	genuReSI USB/Portable Mode	20

9

3.1 Duties of the Maintainer

As the **maintainer**, you are responsible for establishing and terminating connections to the rendezvous server. The operator establishes the connection from the service box to the rendezvous server. Both connections must be established before the target system being maintained can be accessed. The configuration data is imported via the configuration file. It cannot be modified locally.

3.2 Establishing/Terminating the Maintenance Connection

The imported rendezvous connections are listed on the left side of the screen. Details about each connection are displayed on the right. After selecting the rendezvous connection, click on the <u>Connect</u> button to connect to the Rendezvous Box. If the Activate History menu item is enabled in the Settings, you may then enter a description for the connection (for logging).

🖧 Remote Maintenances / Service Boxes	▼ ậ 📮 rdp-a	issoc 🗙	vnc-assoc		
Search	× <u>•</u> <u>Ma</u>	intainer		Layout 📘 List	~
rdp-assoc					
vnc-assoc	Type Co	nnected	Address	hh:mm:ss C	onnect/Disconnect
	SSH	×	192.168.0.4	00:00:27	Connect
		6) ×	1	
	\odot		Please enter a chort comment about this Connection		
		Target Sy:	for your Connection-History	Target System Command	
		rdp-tar	Please enter a reason for the connect attempt		Autostart
		_			
			ОК		
		_			

Figure 3.1: Establishing the connection - Maintainer

Note: If an authorization via LDAP/Active Directory is configured for the connection, you may have to use a custom LDAP login name to access the Rendevous box. In this case, enter the LDAP login name at Settings \rightarrow SSH in the LDAP Loginname field.

Note: If the administrator configured the connection as a high availability setup with multiple Rendezvous Boxes, the additional drop-down menu **Automatic** is displayed under **Address**. If required, this menu allows the manual selection of a single Rendezvous Box from the setup to connect to the target system. Per default, a random Rendezvous Box is chosen.

If the connection has been established, this will be indicated with a check mark in the upper section (1) under "Connected". The "Disconnect" button can be used to terminate the connection to the rendezvous server.

In the lower section (2), the information displayed under Status indicates whether the operator has successfully established the connection from the rendezvous server to the genubox upstream of the machine being maintained. The name shown here is the name specified in the genucenter GUI for "Name for Maintainer". If nothing was entered in "Name for Maintainer", genuReSI displays the name of the connection. Press Ctrl + D to view additional technical details (port, local and remote IP) for the connection.

♀ Remote Maintenances / Service Boxes ▼	a vnc-assoc1 x ↓ vnc-assoc1		
Search 🗙	Maintainer		Layout 🚺 List 🗸
✓rdp-assoc1			
vnc-assoc I	Type Connected	Address	hh:mm:ss Connect/Disconnec
	Target Systems Stat	tus	Target System Command
	win-target1 2	E V RDP	V Execute Autostart

Figure 3.2: Window Layout

3.3 Recording the Connection using RDP

It is possible to record RDP, SSH, and VNC sessions, and to monitor active sessions (recording function). This must be started by the **operator**. The maintainer cannot control this. The camera icon for the connection indicates whether recording is configured.

In some cases, personal data of the maintainer may be affected by a recording. If this is the case, a privacy disclaimer informs you about how this personal data is acquired

and processed. The maintenance connection will be canceled if you do not agree to the disclaimer.

Target Systems	Status	Target System Command
rdp-target		RDP · Execute Autostart

Figure 3.3: Recording Connections

The status information for an established connection shows whether this session is being recorded or monitored. In our example, the session is being recorded and actively monitored, and the maintainer has access to the target system.

2017-08-21 14:31:26	💿 🛛 Maintainers: 🗗 alice	🖌 fred		
time left 56m 17s	monitored 🔤 operator, alice		e operator	

Figure 3.4: Session Recording Indicator

3.4 Data Exchange between Maintainer and Target System

The maintainer can upload data to the target system, or download data from the target system (also called the "Share Option"). This function must be started by the **operator**. The maintainer cannot control this. The exchange icon for the connection under Status indicates whether data exchange is configured (see figure 3.3).

Clicking on the icon opens the File Exchange Explorer. The data exchange is implemented using an RDP drive. The data is thus retained after terminating the session. File transfers are logged and the operator can also track them afterwards. If a virus scanner connected via ICAP has been configured for the Rendezvous Box, transferred files will be checked for malware automatically. The files will only be available after the virus scanner has approved them. The file transfer status displays more information about this process when necessary.

		Date	Туре	Size
p	2	4/05/2023 11:33:52	FILE	0 B
	2	4/05/2023 11:37:05	FILE	0 B
ls:				
C:\Users\Admin\Desktop\old_logo.bmp				
	2 15:	2 2 2 is:	24/05/2023 11:33:52 24/05/2023 11:37:05 is:	24/05/2023 11:33:52 FILE 24/05/2023 11:37:05 FILE s:

Figure 3.5: File Exchange Explorer

The upper window of the explorer displays all available objects. The lower window displays the current transfers. The menu provides icons for uploading and downloading, creating a new folder, and deleting objects. The displayed information does not update automatically by default, but it can be configured to do so. In addition, objects can be viewed as icons or in list format.

3.5 Configuration Updates

The maintainer needs a valid configuration file for the initial connection between genuReSI App and Rendezvous Box. Usually, this file is created by the administrator in the Central Management Station genucenter.

Once an active SSH connection to the Rendezvous Box is established, configuration changes are automatically transmitted and displayed with every genuReSI status check. Such changes can, e.g., add new connections. Therefore, there is no need to manually update configuration files, as long as the maintainer is able to connect to the Rendezvous Box with the latest configuration.

Alternatively, click Update Configuration in the title bar. genuReSI App checks for updates on every Rendezvous Box configured for SSH and updates the local configuration as required.

다. Remote Maintenances /	Service Boxes 🔻 🖡	✓ rdp-assoc1 ×		
Search	×	Maintainer		
HW Corp. 130				- List
✓ rdp-assoc1		T Considered	A	hh:mm:ss Connect/Disconnect
	(is) ChangesWindow There ar Details s	e changes in the maintainance configuration, w ee below.	×	00:03:59 Disconnect
	 Details 			arget System Command
	 Old Remote Maint Old Targetsystem 	enance: "HW Corp. 130" for Remote Maintenance "HW Corp. 130": win-tar	get1	 Execute Autostart
	➡ New Remote Mair New Targetsystem	tenance: PWC Corp. 1224 for Remote Maintenance "PWC Corp. 1224": win-	-target1	
다. Remote Maintenance	ОК			

Figure 3.6: Updated Configuration (Extended View)

3.6 Logging/History

Clicking on the **Logging** tab in the main window displays the genuReSI log data and the connections. The logging levels **Info**, **Debug**, and **Error** are available. The default logging level is Info.



Figure 3.7: Logging

To show the connection data for the recent connections (History), select the last icon in the toolbar: **History**. In the history window, the time frame for the connections can be defined and search text can be entered. The data can be saved to a local file so it can be included with a support request, for example, to assist with troubleshooting.

Filter					
	Date Select a date 15	.	Select a date 15		
	Text Search		×		
Who	Where	Why	Starttime	Endtime	Duration
Stefan Rinkes	Fernwartung Windows Server 2003 172.28.4.201 (SSH)		11/11/2016 1:26:41 PM	11/11/2016 1:26:43 PM	00:00:02
Stefan Rinkes	Fernwartung Windows Server 2003 172.28.4.201 (SSH)		11/11/2016 1:26:57 PM	11/11/2016 1:27:35 PM	00:00:38
Stefan Rinkes	Fernwartung Windows 8 172.28.4.201 (SSH)		11/11/2016 1:28:11 PM	11/11/2016 1:28:24 PM	00:00:13
Stefan Rinkes	Fernwartung Windows Server 2003 172.28.4.201 (SSH)		11/11/2016 1:28:34 PM	11/11/2016 1:30:26 PM	00:01:52
Stefan Rinkes	Fernwartung Windows Server 2003 172.28.4.201 (SSH)		11/11/2016 1:30:30 PM	11/11/2016 1:34:34 PM	00:04:04
Stefan Rinkes	ohne-recmote 172.28.4.201 (SSH)		11/11/2016 1:34:33 PM	11/11/2016 1:34:48 PM	00:00:15

Figure 3.8: Maintenance Connection History

3.7 Local Settings

A number of settings can be configured using the **Settings** icon in the toolbar:

• Application Settings:

General settings can be configured here, such as theme, activation of history and logging level.

• SSH:

SSH settings can be configured here, such as SSH forwarding and LDAP username, but also the network adapter for mapping addresses.

Plugins:

Installing/uninstalling plugins, see chapter 3.9.

• Smartcard:

File path to the smart card middleware.

• Commands: Definition of commands, see chapter 3.8.

• Roles:

Overview of available roles and settings.

Application Settings	Logging Level	Info ~
SSH SSH	Theme	Normal ~
Plugins	Icon Set	Bunt ~
Smartcard	VNC Client for Recmote	Use ReSI VNC Client
P Commands		RDP ~
	Register File Extension (*.resi)	\checkmark
Roles	Activate History	
About	Details View	or Ctrl + D in the main GUI)

Figure 3.9: Remote Maintainer Settings

3.8 Commands

Application Settings	Name 📥	Filename	Arguments	
SSH SSH	http	http://%HOST%:%PORT%		đ
Plugins	https	https://%HOST%:%PORT%		÷
Smartcard	RDP	mstsc	/v:%HOST%:%PORT%	di di
Commands				
Roles				
About				
-				
	Add			

Figure 3.10: Commands Settings

Various protocols can be used to access the maintained machine, such as RDP (Remote Desktop Protocol) from Microsoft or SSH (Secure Shell). Define the commands required for this from the **Commands** menu in the toolbar. RDP is always predefined. In our example, access via SSH using PuTTY was added. The commands defined here are available in the main window for an existing connection. They can be selected and started there. If **Autostart** is selected, these commands are automatically started with the rendezvous connection.

Name	Status		Command	1
windows-8		htt	itps v	Execute 🖌 Autostart
windows-7		Fir	refox http refox https	Execute Autostart
		htt	ttp	
		htt	itps	
		Pu	uTTY Plink	
		Pu	UTTY PUTTY	
		RD	DP	

Figure 3.11: Autostart Function

3.9 Plugins

Plugins make it easy for users to add features to their genuReSI setup. There are currently two types of plugins available: command and theme plugins.

Plugins are ZIP files containing a plugin info file and the files that the plugin requires. The current plugins, for example, are Firefox, OpenSSH, PuTTY, and UltraVNC. Always use the latest plugin version available. Please check that plugin and system architecture are identical (32 or 64 bit).

Application Settings	Searc	h	×					
SSH SSH		Installed		Name		Version		
Plugins Smartcard Commands	6	√	OpenSSH-X11			1.0	<u>License</u>	Ē
Roles			Installatio	n Complete		×		
				Installation Complete	Close	2		
	Add							

Plugins are installed/uninstalled via the Settings \rightarrow Plugins menu.

Figure 3.12: Plugins

Note: Follow these steps to use a VNC client made available as plugin.

- 1. Change to $\texttt{Edit} \ \rightarrow \ \texttt{Settings} \ \rightarrow \ \texttt{Application} \ \texttt{Settings}$
- 2. Deactivate the checkbox Use genuReSI VNC Client
- 3. Choose your client in the selection menu below.

Note: VNC connections are supported according to the Remote Framebuffer Protocol (RFC 6143).

3.10 genuReSI Update

genuReSI has an autoupdate feature: When the app is started, it automatically checks for updates of the ReSI.exe file. If a new version is available, the dialog box **Update Available** is displayed. Click Yes to install the update. After that, restart the genuReSI application.

The update installs the latest version of the ReSI.exe file. The previous version is stored as ReSI_old.exe.

The autoupdate feature is enabled by default. To disable the feature, navigate to Settings \rightarrow Application Settings and deactivate the checkbox Check for Updates on Start. All updates have to be triggered manually now.

Note: Do not forget to update plugins in use.

3.11 genuReSI USB/Portable Mode

To make the genuReSI application available on any computer, it can be installed on a USB stick and opened from there. USB mode can also be launched in read-only mode. In this case, all write operations are disabled. This means the configuration cannot be saved. Thus, you can first launch genuReSI and then immediately remove the USB stick.

^rgenua.

Chapter 4

genuReSI for Operators

4.1	Duties of the Operator	22
4.2	Establishing/Terminating the Maintenance Connection	22
4.3	Access Control at Runtime	24
4.4	Recording the Connection with RDP and SSH	25
4.5	Share Option	26
4.6	Configuration Updates	27
4.7	Logging/History	28
4.8	Local Settings	30
4.9	genuReSI Update	31

4.1 Duties of the Operator

As an **operator**, you are responsible for establishing and terminating the connection from the rendezvous server to the genubox upstream of the maintained target system. Without this connection, the maintainer **cannot** establish the maintenance connection. The operator also determines whether a connection should be recorded or monitored live if configured accordingly (usually via the genucenter Management Station). As long as rendezvous is configured to allow this, the operator can grant the maintainer control of the keyboard and mouse of the target system, and revoke that control.

The configuration data is imported via the configuration file. It cannot be modified locally.

The operator GUI can be accessed directly via the genucenter or locally via the genubox using a special operator login. It can also be accessed using genuReSI. The operator GUI is described in the manuals for genucenter/genubox. Installation and configuration are described in chapter 2.

4.2 Establishing/Terminating the Maintenance Connection

♣ Remote Maintenances / Service Boxes	▼ ậ 🛋 servicebox 🗙				
Search	× boperator			Layout	List ~
servicebox	Type Connected		Address	himmiss	Connect/Disconnect
	SSH X		192.168.0.6	00:00:00	Connect
	\sim				
	Maintenances	Remaining Time	Target Systems	Recordings Browser	Start/Stop

Figure 4.1: Establishing the Connection - Operator

The imported operator connections are listed on the left side of the screen. More details about each connection are listed on the right. After selecting the operator connection, click on the **Connect** button. This only establishes the SSH connection to the genubox. It does not start a maintenance connection!

Note: If an authorization via LDAP/Active Directory is configured for the connection, you may have to use a custom LDAP login name to access the Service box. In this case, enter the LDAP login name at Settings \rightarrow SSH in the LDAP Loginname field.

The available connections are displayed in the lower section of the main window. These can also be started with the **Start** button.

ିର୍ଦ୍ଧ Remote Maintenances / Service Boxes	▼					
Search	× boperator				Lavout III	liet v
✓ servicebox						
	Type Connected		Address		hh:mm:ss	Connect/Disconnec
	SSH 🗸	Starting FBZ 'rdp-assoc'	× 168.0.6		00:01:16	Disconnect
	Disk Usage Storage 9.84 GE Search for Remote Maintenance Maintenar rdp-assoc	Here you can configure if this session sho recorded and if file sharing is allowed. Options	v X	Target Systems	Recordings Browser	Start/Stop
	vnc-assoc			1 Vnc-target	Open	Start

Figure 4.2: Establishing the Connection

A camera icon next to the connection (under Forwardings) signals that recording has been configured. The explorer icon signals that the data exchange option is configured, and the access control icon that access control at runtime is enabled.

If the history is enabled (see chapter Settings), a reason for establishing the connection can be specified. The recording and share options can also be enabled in this window. The privileges to allow the maintainer to start the maintenance can be defined by activating the respective check boxes.

Once connections have been established, this will be visible in the upper section (1) under "Connected", indicating that the SSH session to the genubox upstream of the target system being maintained has been established. The connection to the genubox can be terminated with the **Disconnect** button. This does not affect maintenance connections.

^rgenua.

hh:mm:ss Connect/Disconn 00:00:28 Disconnect
00:00:28 Disconnect
Recordings Browser Start/Stop
Recordings Browser

Figure 4.3: Connections Overview

The lower section under Forwardings (2) shows whether the operator has enabled connections from the genubox to the machine being maintained, and which connections the operator has enabled. The status of the maintainer's connection is shown under Maintainer (3). The time window of a maintenance connection can be edited with a click on Remaining Time (4). Clicking on **Stop** allows the operator to terminate the connection from the genubox to the machine being maintained.

4.3 Access Control at Runtime

Carchin	×	Everybody Full Access		Everybody No Acces	
	Name	*	Connected	Access Rights	
Maintainer			×	ď	

Figure 4.4: Connections Overview

The operator can grant or revoke access to the target system keyboard and mouse at runtime as long as this option is enabled in the configuration. To modify these privileges, the operator

must click on the access control icon in the **Forwardings** section. The window shown in figure 4.4 appears. Clicking on the open padlock (in this case) allows the operator to revoke the maintainer's access to the mouse and keyboard. The padlock is closed when access is revoked. Clicking on the closed padlock opens it again and grants the maintainer access to the target system keyboard and mouse again.

4.4 Recording the Connection with RDP and SSH

It is possible to record RDP and SSH sessions and monitor active sessions (recording function). This must be started by the operator. The maintainer cannot control this. The camera icon for the connection indicates whether recording is configured (see figure 4.3).

If a connection with recording has been started, the operator can monitor the active session live by clicking on the camera icon. The blinking camera icon in the newly opened session window means that the session is currently being recorded. You can also see whether the maintainer is currently connected.



Figure 4.5: Recording in Active Session

Clicking on the **Open** button under Recordings Browser opens the window with the previously recorded sessions. These can be downloaded in raw format, converted to VP8 format, or deleted. Converted recordings can also be downloaded to the local workstation and viewed there.

Make sure to delete recordings that are no longer required in a timely manner to prevent using up available storage space.

8		8		8		
windows-8-11-33-07-2	23-10-2015 wir	ndows-8-11-50-23-11	-05-2016 windo	ws-8-11-56-25-11-	05-2016	

Figure 4.6: Downloading/Converting Recordings

4.5 Share Option

If the share option (data exchange) is enabled, the operator can click on the explorer icon to open the explorer for the operator. All files copied (upload and download) are displayed here. The operator can also download the files using the download icon in the toolbar.

File . 0 🖬 🕯	▲ _ O ♣ Auto-Refresh Interval _			
Date	Filename	Operation	State	Size
4/23/2015 7:39:51 PM	/beerkill.gif	upload	complete	1.59 MB



If a virus scanner connected via ICAP has been configured for the Rendezvous Box, transferred files will be checked for malware automatically. The files will only be available after the virus scanner has approved them. The file transfer status displays more information about this process when necessary.

Date	State		Filename	Maintainer	Operation	Size
05/03/2021 14:23:13	nfected	/eicar.com.txt		resimaintainer (Fernwarter ReSI)	Upload	68 B
05/03/2021 12:09:25		/main.txt		resimaintainer (Fernwarter ReSI)	Upload	18 B

Figure 4.8: Malware detected ("Infected")

4.6 Configuration Updates

The operator needs a valid configuration file for the initial connection between genuReSI App and Service Box. Usually, this file is created by the administrator in the Central Management Station genucenter.

Once an active SSH connection to the Service Box is established, configuration changes are automatically transmitted and displayed with every genuReSI status check. These configuration changes, e.g., additional connections, are usually also done via the genucenter. Therefore, there is no need to manually update configuration files, as long as the operator is able to connect to the Service Box with the latest configuration.

Note: Unlike the maintainer, the operator is not required to confirm changed configurations. The new configuration is immediately displayed in the operator view.

Alternatively, click Update Configuration in the title bar. genuReSI App checks for updates on every Rendezvous Box configured for SSH and updates the local configuration as required.

4.7 Logging/History



Figure 4.9: Logging

Clicking on the Logging tab in the main window displays the genuReSI log data and the connections. The logging levels Info, Debug, and Error are available.

To show the connection data for the recent connections (History), select the last icon in the toolbar: **History**. In the history window, the time frame for the connections can be defined and search text can be entered. The data can be saved to a local file so it can be included with a support request, for example, to assist with troubleshooting.

Filter	Date Select a date 15	-	Select a date 15		
	Text Search		×		
Who	Where	Why	Starttime	Endtime	Duration
Stefan Rinkes	Fernwartung Windows Server 2003 172.28.4.201 (SSH)		11/11/2016 1:26:41 PM	11/11/2016 1:26:43 PM	00:00:02
Stefan Rinkes	Fernwartung Windows Server 2003 172.28.4.201 (SSH)		11/11/2016 1:26:57 PM	11/11/2016 1:27:35 PM	00:00:38
Stefan Rinkes	Fernwartung Windows 8 172.28.4.201 (SSH)		11/11/2016 1:28:11 PM	11/11/2016 1:28:24 PM	00:00:13
Stefan Rinkes	Fernwartung Windows Server 2003 172.28.4.201 (SSH)		11/11/2016 1:28:34 PM	11/11/2016 1:30:26 PM	00:01:52
Stefan Rinkes	Fernwartung Windows Server 2003 172.28.4.201 (SSH)		11/11/2016 1:30:30 PM	11/11/2016 1:34:34 PM	00:04:04
Stefan Rinkes	ohne-recmote 172.28.4.201 (SSH)		11/11/2016 1:34:33 PM	11/11/2016 1:34:48 PM	00:00:15

Figure 4.10: History

The operator can open the current log file for an active connection using the **Logging** (book icon) button:

Maintenances	Remaining Time	Forwardings	Maintainer	Recordings Browser	Start/Stop
Fernwartung	59 Minutes	Fernwartung-vnc	✔ Fern Warter	Open	Stop

Figure 4.11: Logging Active Session

This is displayed in a separate window:

```
File OE
Nov 14 09:03:09 sri-box2 fbz[3]: Authenticated to 172.28.4.201 ([172.28.4.201]:22).
Nov 14 09:03:09 sri-box2 fbz[3]: rv_start: ready (requested by oparator)
Nov 14 09:03:10 sri-box2 fbz[3]: Maintainer srinkes connected
Nov 14 09:03:10 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: started
Nov 14 09:03:10 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: starting session for wsystem windows-8
Nov 14 09:03:10 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: maintainers have view-only rights
Nov 14 09:03:11 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: VNC server started
Nov 14 09:03:12 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: VNC proxy started
Nov 14 09:03:13 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: OSSD daemon started
Nov 14 09:03:14 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: RDP client started
Nov 14 09:03:14 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: starting session for wsystem windows-7
Nov 14 09:03:14 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: maintainers have view-only rights
Nov 14 09:03:15 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: VNC server started
Nov 14 09:03:16 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: VNC proxy started
Nov 14 09:03:17 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: OSSD daemon started
Nov 14 09:03:18 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: RDP client started
Nov 14 09:03:18 sri-box2 fbz[3]: recmote start [pid 9939, user oparator]: exit(0)
Nov 14 09:03:20 sri-box2 fbz[3]: xferd-archiver for wsys 2[35848]: started for fbz 'F\M-C\M-$rnwartung' and wsystem 'windows-8' (archiving is a
Nov 14 09:03:20 sri-box2 fbz[3]: xferd-service for wsys 2[37599]: waiting for requests
Nov 14 09:03:20 sri-box2 fbz[3]: User srinkes connected to file transfer service for wsystem 2 on port 7002
Nov 14 09:03:24 sri-box2 fbz[3]: xferd-archiver for wsys 7[5767]: started for fbz 'F\M-C\M-$rnwartung' and wsystem 'windows-7' (archiving is o'
Nov 14 09:03:24 sri-box2 fbz[3]: xferd-service for wsys 7[87836]: waiting for requests
Nov 14 09:03:24 sri-box2 fbz[3]: User srinkes connected to file transfer service for wsystem 7 on port 7007
Nov 14 09:03:34 sri-box2 fbz[3]: xferd-service for wsys 7[87836]: start upload of '/checksums.txt'
Nov 14 09:03:35 sri-box2 fbz[3]: xferd-service for wsys 7[87836]: terminating
Nov 14 09:03:35 sri-box2 fbz[3]: xferd-archiver for wsys 7[5767]: terminating
Nov 14 09:03:35 sri-box2 fbz[3]: fuser srinkes operator oparator host 127.0.0.2 port 12907 bytes 180+704 seconds 10.75
Nov 14 09:03:35 sri-box2 fbz[3]: User srinkes disconnected from file transfer service for wsystem 7 on port 7007
Nov 14 09:03:35 sri-box2 fbz[3]: xferd-archiver for wsys 7[27247]: started for fbz 'F\M-C\M-$rnwartung' and wsystem 'windows-7' (archiving is a
Nov 14 09:03:35 sri-box2 fbz[3]: xferd-service for wsys 7[41115]: waiting for requests
Nov 14 09:03:35 sri-box2 fbz[3]: User srinkes connected to file transfer service for wsystem 7 on port 7007
```

Figure 4.12: Log Data Output

4.8 Local Settings

A number of settings can be configured using the **Settings** icon in the toolbar:

• Application Settings:

General settings can be configured here, such as theme, activation of history and logging level.

• SSH:

SSH settings can be configured here, such as SSH forwarding and LDAP username, but also the network adapter for mapping addresses.

- Plugins: Installing/uninstalling plugins, see chapter 3.9.
- Smartcard:

File path to the smart card middleware.

• Commands: Definition of commands, see chapter 3.8.

• Roles:

Overview of available roles and settings.

Application Settings	Logging Level	Info ~
SSH SSH	Theme	Normal ~
Plugins	Icon Set	Bunt ~
Smartcard	VNC Client for Recmote	☑ Use ReSI VNC Client
P Commands		RDP 🗸
	Register File Extension (*.resi)	\checkmark
Roles	Activate History	
d About	Details View	(or Ctrl + D in the main GUI)

Figure 4.13: Settings

4.9 genuReSI Update

genuReSI has an autoupdate feature: When the app is started, it automatically checks for updates of the ReSI.exe file. If a new version is available, the dialog box **Update Available** is displayed. Click Yes to install the update. After that, you have to restart the ReSI application.

The update installs the latest version of the ReSI.exe file. The previous version is stored as ReSI_old.exe in the TEMP directory.

The autoupdate feature is enabled by default. To disable the feature, navigate to Settings \rightarrow Application Settings and deactivate the checkbox Check for Updates on Start. All updates have to be triggered manually now.

^rgenua.

^rgenua.

Chapter 5

Advanced Configuration

5.1	Configuration Files	34
5.2	Role Management	35
5.3	Using a Smart card	36
5.4	Use with Firewall/NAT Gateway	39
5.5	HTTP Proxy for SSH	40
5.6	GUI Layout	41
5.7	New Commands	42

5.1 Configuration Files

genuReSI configuration and log files are located in the respective user directories at AppData\Local\genua_GmbH and AppData\Roaming\ReSI. These directories should be included in any backups.

5.2 Role Management

ID:	0
Role:	Operator
Name:	Oper Ator
Loginname:	zieloperator
LDAP:	
Smartcard:	
Stop Connections when Smartcard i: removed	
PrivateKey:	 BEGIN RSA PRIVATE KEY MIIEowIBAAKCAQEAsSfsf0ql/ci+RsOwPdhamv4J3vjHRp5zGIA2a4Q9a15AMxUC iN0epLnhjRIQNtbUXSQB3bFLUvkiKnN4c98ncN96qe6MZPovTshsVQq1Dp8xx0ux FsJIIxvBa1TprnTw06hCzjYqOMnKoLVRCtmtijkMkJ81E+x6mme38UF3JHziCrxe hdtAdqV2/Q+m83ICRPbsUHSGH7M47px0naK2N4cvi9kNuNq6N8qN0A7jeZR18+ok oCHjrv6Uruq9UDHKUGQSGtQV/q+LaNWt8RkVhHm7zL62c0Xt2EA8/J2THArO7fGF RuT6FIJQyrosm59XD6VCfPtKR9ue/Np0Odje2QJDAQABAoIBAQCXLF93HC6cill8 5r6dd+ORgZkAycCbdZj5aluWEimrVqIoLdSU4ERHA0wC8QfvVBGyTYi+Go4RhwFt wk2Wa2YnvrzZ8/SMMqZDz/KrjFIAdojnGbI6g9OzI+WbMZgle/wXhRsDfKntSMR UsiOfsTFP/uF6iYME0MIfduMp3W5DuBGD0upCB5eAtvX5NSyQU/yKN122qOCUfKI QCLxCFKPQxs/B9F7L0qip2g2IQOaV8Spx/r0I6iiW39mMLvQ8jc5WoJg/ilqGUWI fSSR1zrD7MReASEHfRkVxfyR12UgJdCs7OxFuL0jG2xJaRQ4YbTYfIelCxNICQtP + U/tP01RA0GBAONTediRNYRq+Up8TSPJIQJTj85WsHMcanSOFmu8PRuq4iyT/bIN dfOK6h98UrfaxC4I62uWfyOHAdEgctJqd4570SHDW3yzImKoqrqyW3tyMEZHHM+W JJrxX58PyxZaiejZV+ZIBcRyBDxgrlGUdCTVVH5TYuJU4UGyHFe2tFIVAoGBAMeA awgHs0E8/Xn+NsGiVQtoo9KFPCthHhc2LqFAvd2RF0Y4I6FA/WpoS6WtLfS9Bhb0 fBI2o8QO5tfTzwYfIBaUhXtmq7U8r1dsrv2hqXsQsQeTHG8KaPG8Dv/uvF2C9L1B ILoRo9D6w3py5m99ewz5hhvC76vQxeGQpfOwwv61AoGAAmIKofGLvRkeAGDJMiAc ZXjYxhH0kZBXsVc2ynMnFNYqvsriWwHr3Zy0LZZRC6pYah9to1gVhxrQMxADB8+n Iy/HFnKEz/7UunIIMCLUgKvGw8XVEHwFSIaFORaiS16xmWZF3J0eqluDndppIIYo 3YX698QKAINfdR/X2jc7Q60CgYAb66kPEqTPu11xCVb4epOUaSykReIJ2OmxLfAQ uvLZM3kizsEx3DqbLcWlhIgsLFgx1j2V4rYcmIIO12KR5MFE57xWrOPTFY8kmR1U e<hsxz+pa7mzak33ru6cexl5s141lmw6hlkxi9xvuka5+y 1yr4njv1rbnphuvt28<="" li=""> gTyJEQKBgG7XeKQSAOer+x0tMVEAL3J4xHT3j5GaYUMPCAvfMoE+hj37bbYVfqYJ SeC4UN22Ne0RWZHUD8YxJOoxt9ImkZfOLCE+S+KVQFf5frY0Poi3owyWOJDtIhKE IG9RXqmHj8stnJnL/DsrMBBdDCW9qtN+qX+k3+b679S780HSyjF END RSA PRIVATE KEY </hsxz+pa7mzak33ru6cexl5s141lmw6hlkxi9xvuka5+y>
L2TP-Passphrase:	
	Canad

Figure 5.1: Role Management

The configuration files, including the roles (login name and private key), are usually created on the management system and do not have to be edited locally. If values such as the private key have to be changed, this can be done in the **Roles** menu in the toolbar. To do so, click on the role. This opens an edit window. Save the changes with the <u>Save</u> button. 'genua.

5.3 Using a Smart card

A smart card can be used to authenticate the operator and the maintainer.

5.3.1 PKCS#11 Module

Application Settings	PKCS#11 Module	C:\Windows\System32\cardos11_64.dll	
SSH SSH	Smartcard:	Description: CardOS API PKCS#11 Library Version: 2.20	
Plugins	Sinarcearea		Refresh
Smartcard			
H Commands		No Entries Refresh	
Roles			
About			

Figure 5.2: Selecting the PKCS Module

Enter the file path to your PKCS#11 middleware under Settings \rightarrow Smartcard in genuReSI. The file path can be found in the manual for your smart card software.

5.3.2 Smart Card Assignment

To support smart card authentication for a user, select the respective user under Settings \rightarrow Roles. Check the Smartcard box and then apply the changes by clicking on Save.

If existing connections should be stopped when the smart card is removed, check the **Stop Connections when Smartcard is removed** box as well.

<u>Note</u>:

This option can lead to problems with contact free smart cards, since these are only active during the first initialization and are then removed.

5.3.3 Assigning the Public Key in genucenter

Application Settings	PKCS#11 Module C:\Windows\System32\cardos11_64.dll	
SSH SSH	Description: CardOS API PKCS#11 Library Version: 2.20	
Plugins	Smartcard: 1234 (Gemplus USB SmartCard Reader 0)	
		Refres
Smartcard	Name	
Commands	🔎 2048 Bit RSA Public Key	Save as PEM
Roles		
About		
U About		

Figure 5.3: Smart Card Menu

The smart card public key must be known to the Rendezvous Box so you can authenticate using the smart card:

- 1. Export the public key of the user's smart card in the genuReSI App GUI at Settings \rightarrow Smartcard by clicking on Save as PEM.
- 2. Upload the public key in the genucenter:
 - (a) In the genucenter, navigate to either Rendezvous \rightarrow Operators \rightarrow <genuReSI user> or Rendezvous \rightarrow Maintainers \rightarrow <genuReSI user> in accordance with the user's designated function.
 - (b) In the Access via SSH section, activate the checkbox Enable SSH key login.
 - (c) Also, use **Upload file with key** to upload the exported public key.
 - (d) Save your changes and update the configuration of all participating systems.

Type Connected	Address	
SSH D	192.168.56.200	
Search for Target System	PIN for Smartcard Authentication to kasto- techniker@192.168.56.200	Com
S7-Steuer	Password	Firefox http
easy-71	Cancel OK	Firefox http
easy-137		Firefox http

5.3.4 Establishing the Connection

Figure 5.4: Smart Card PIN Entry

When establishing the connection, you will be asked for your smart card's PIN. After successfully entering it, you will have access to your connections.

5.4 Use with Firewall/NAT Gateway

5.4.1 SSH Forwarding

If your Rendezvous Box is located behind a firewall or a NAT gateway and is not directly reachable, you can set up SSH forwarding to enable the connection to the Rendezvous Box. On the firewall, a direct port forwarding rule that forwards SSH to the Rendezvous Box must be added.

Note: A maximum of 50 port forwardings is allowed per SSH connection.

Enter the IP address/hostname and/or the port for which forwarding is enabled in genuReSI under Settings \rightarrow SSH \rightarrow SSH Redirection.

5.5 HTTP Proxy for SSH

If it is not possible to set up static port forwarding for SSH to the Rendezvous Box, SSH can also be forwarded via an HTTP proxy.

You can either use the HTTP proxy saved in your Windows system or enter a different proxy. If the proxy requires authentication, enter your access data in the HTTP Proxy for SSH field in the following format.

Username:Password@IP address/Hostname:Port

5.6 GUI Layout

C	- I d rdp.assor X		
* Kemote Maintenances / Service Boxes			
Şearch	X Maintainer		Layout 📘 List 🗸
✓ rdp-assoc			
□ ssh-assoc	Type Connected	Address	hh:mm:ss Connect/Disconnect
	SSH 🗸	192.168.56.30	00:00:59 Disconnect
	Target Systems	Status	Target System Command
	win10rdp		RDP - Execute Autostart
	⊊ ssh-assoc ★		
	Maintainer		Layout 📘 List 🗸 🗸
	Type Connected	Address	hh:mm:ss Connect/Disconnect
	SSH 🗙	192.168.56.30	00:00:00 Connect
	\odot		
	Target Systems	Status	Target System Command
			PDP Y Everyte Autostart

Figure 5.5: GUI Layout

The genuReSI application uses what is known as a docking mechanism. This allows windows to be moved, docked to the editor frame, or even arranged across multiple screens (see https://docs.microsoft.com/en-us/visualstudio/ide/customizing-window-layouts-in-visual-studio, "Arrange and dock windows"). Thus, you can adjust and arrange the screen at your discretion.

5.7 New Commands

Internally, the rendezvous concept uses port forwardings to direct connections to the target system via the rendezvous server. In the **Commands** menu in the toolbar, commands can be defined to be executed on the target system. To do so, the syntax of the command must be known. The variables <code>%HOST%</code> and <code>%PORT%</code> designate the hostname and the port used. Windows environment variables are supported.

Example: PuTTY should be used to open an SSH connection on the target system. **Filename** defines where the putty.exe application is located on the local file system. Under **Arguments**, define the command -P %PORT% %HOST%, as PuTTY specifies the port with -P argument on the command line.

^rgenua.

Chapter 6

STEP7 via Rendezvous

6.1	GUI Installation of the Loopback Adapter	44
6.2	Command Line Installation of the Loopback Adapter	45
6.3	IP Configuration	45

To use the Siemens STEP7 protocol with rendezvous, we recommend adding a loopback adapter in Windows. The maintainer can do this directly via the genuReSI App GUI. Additionally, the installation can be performed via the command line, e.g., for an automatic installation with a centralized management tool.

6.1 GUI Installation of the Loopback Adapter

Note: Administrator privileges are required to install the Microsoft loopback adapter.

- 1. Start genuReSI App.
- 2. Navigate to Settings \rightarrow SSH.
- 3. In the section **Network Adapter for Mapping Addresses**, click on Install Loopback Driver. The loopback adapter will be installed.
- 4. In the drop-down menu, select the new loopback adapter as the **Network Adapter for Mapping Addresses**. The adapter will be used by genuReSI App now.
- 5. Click on (Close).
- 6. Continue with section 6.3

Application Settings	Network Adapter for Mapping Addresses	Microsoft Loopbackadapter für KM	-TEST ~
SSH SSH	SSH Debug		
Plugins	SSH Redirection	Redirection Host	Redirection Port
Smartcard	HTTP Proxy for SSH	No Proxy Use System Proxy Use own Proxy	
Commands		HTTP Proxy for SSH	
Roles	LDAP Loginname	Idap	
About			

Figure 6.1: genuReSI Loopback Adapter

6.2 Command Line Installation of the Loopback Adapter

Note: Administrator privileges are required to install the Microsoft loopback adapter.

Execute the genuReSI application with the parameter /install-loopback for an automated installation of the loopback adapter.

ReSI.exe /install-loopback

Continue with section 6.3.

6.3 IP Configuration

Once the connection is established, Windows will ask whether genuReSI may assign an IP address to the loopback adapter. Confirm with \underline{Yes} .



Figure 6.2: User Account Control

If the connection is established, the detailed view (switch to detailed view with Ctrl+D) will show the local IP address is set to 192.168.100.3. This IP address is entered by the admin **in advance** as the S7 address in the genucenter.

3311-035							
A Maint	tainer						Layout Eist
Type Conn	nected				Address		hh:mm:ss Connect/Disconne
SSH					192.168.56.30		00:00:29 Disconnect
Loc	cal Address	Local Port	Remote Address	Remote Port	Status	Target System Command	Start/Stop
				7002		PDP Y Everyte Autostart	Start

Figure 6.3: genuReSI with Active Connection

At this point, ipconfig also shows the IP address set by genuReSI:

Sthernet adapter LAN-Verbindung 5		
O		
Description	. Mieneest Leenbackadanten	
Physical Address	: 02-00-4C-4F-4F-50	
DHCP Enabled.		
Autoconfiguration Enabled	. Yes	
Link-local IPv6 Address	: fe80::ec58:2f73:5ea1:d3f6%20(Preferred)	
IPv4 Address	: 192.6.10.10(Preferred)	
Subnet Mask	: 255.255.255.255	
IPv4 Address	: <u>192.6_1.126(Tentative)</u>	
Subnet Mask	: 255.255.255.255	
Default Gateway	• • •	
	- $ -$	
DHGPV6 Glient DUID	: 00-01-00-01-18-10-76-05-E0-06-E6-C7-2C-08	
DNS Servers		
Not DIOC ough Tanin	·	



Once genuReSI is closed, the IP addresses are cleared again.

^rgenua.

Index **Genua**.

Index

Α

Advanced configuration	33
G	
genuReSI for Maintainers	9
genuReSI for Operators	21

L

Launching the genuReSI Windows	Applica-
tion	5

Μ

Maintenance	with the	rendezvous	concept
1			

Ρ

Product Overview

v

S

STEP7 via Rendezvous 43



About genua

genua GmbH is a German IT security specialist and has been securing networks and providing top-quality security solutions since the company was founded in 1992. Our business activities cover securing sensitive interfaces in both public authorities and industry, securely connecting highly critical infrastructure, reliably encrypting data communication over the Internet, providing remote maintenance systems for machines, plants and IT systems and providing remote access solutions for mobile employees and teleworkers. Our solutions are developed and produced in Germany and many companies and security-conscious authorities rely on solutions from genua to protect their IT.

genua is a member of the Bundesdruckerei Group.

genua GmbH, Domagkstrasse 7, 85551 Kirchheim, Germany tel +49 89 991950-0, info@genua.eu