genua.

genuReSI

Installation and Configuration Manual

Version 1.16

genua.

Edition: April 26, 2024

Revision: a232d46

Copyright ©2002–2024 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

Preface v

1 Maintenance with the Rendezvous Concept 1

1.1 The genua rendezvous concept 2

1.2 Using the genuReSI Maintenance Application 3

2 Launching the genuReSI Windows Application 5

2.1 Installation Requirements 6

2.2 Installation and Configuration 7

3 genuReSI for Maintainers 9

3.1 Duties of the Maintainer 10

3.2 Establishing/Terminating the Maintenance Connection 11

3.3 Recording the Connection using RDP 13

3.4 Data Exchange between Maintainer and Target System 14

3.5 Configuration Updates 15

3.6 Logging/History 16

3.7 Local Settings 18

3.8 Commands 20

3.9 Plugins 21

3.10 genuReSI Update 22

3.11 genuReSI USB/Portable Mode 22

4 genuReSI for Operators 23

4.1 Duties of the Operator 24

4.2 Establishing/Terminating the Maintenance Connection 25

4.3 Access Control at Runtime 28

4.4 Recording the Connection with RDP and SSH 29

genuReSI by genua GmbH. All rights reserved.

4.5 Share Option 31
4.6 Configuration Updates 32
4.7 Logging/History 33
4.8 Local Settings 36
4.9 genuReSI Update 38

5 Advanced Configuration 39
5.1 Configuration Files 40
5.2 Role Management 41
5.3 Using a Smartcard 42
5.4 Use with Firewall/NAT Gateway 45
5.5 HTTP Proxy for SSH 46
5.6 GUI Layout 47
5.7 New Commands 48

6 STEP7 via Rendezvous 49
6.1 GUI Installation of the Loopback Adapter 50
6.2 Command Line Installation of the Loopback Adapter 51
6.3 IP Configuration 52

Index 55

 genuReSI by genua GmbH. All rights reserved.

Preface

About this Product

The genuReSI (**Re**mote **S**ecure **I**ntegration) 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` → `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.

genuReSI by genua GmbH. All rights reserved.

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 → genubox → 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

genuReSI by genua GmbH. All rights reserved.

Chapter 1

Maintenance with the Rendezvous Concept

1.1 The genua rendezvous concept 2

1.2 Using the genuReSI Maintenance Application 3

genuReSI by genua GmbH. All rights reserved.

1.1 The genua rendezvous concept

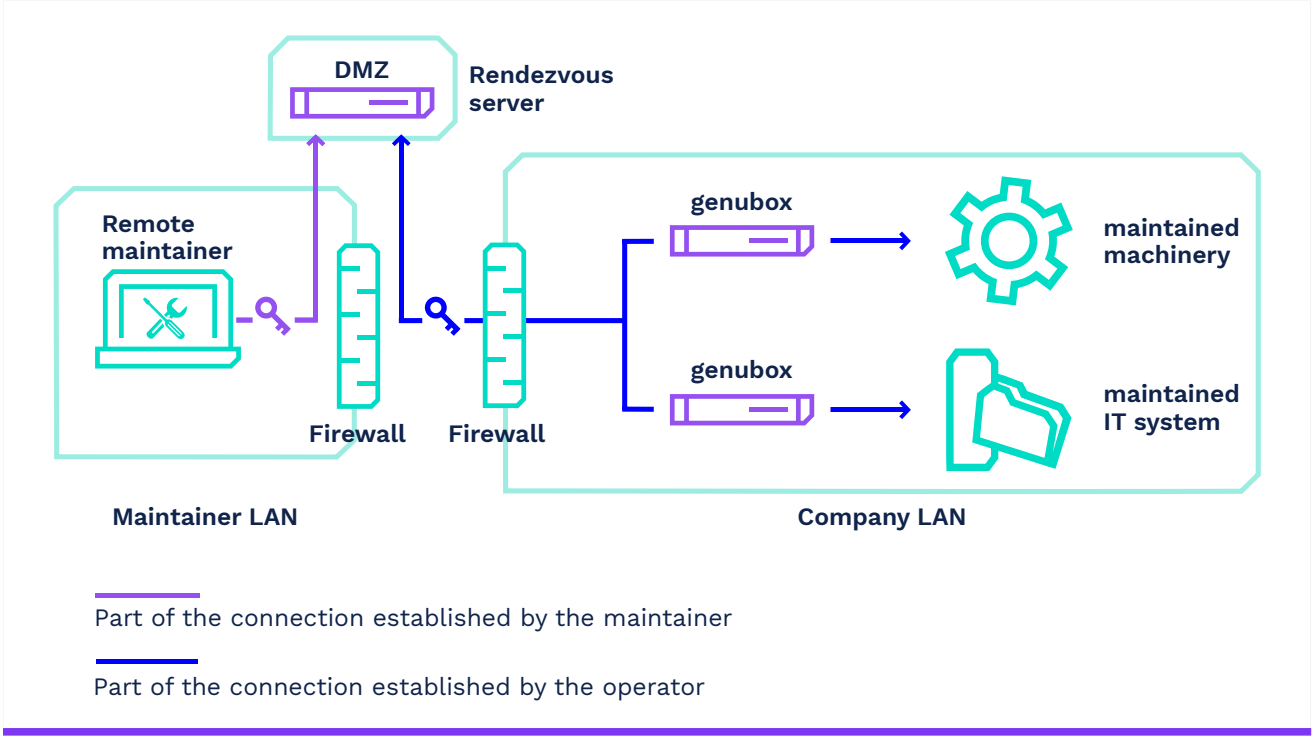

Figure 1.1: rendezvous concept

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 can be established either via SSH VPN or L2TP, depending on the customer's requirements.

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).

 genuReSI by genua GmbH. All rights reserved.

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.

genuReSI by genua GmbH. All rights reserved.

 genuReSI by genua GmbH. All rights reserved.

Chapter 2

Launching the genuReSI Windows Application

2.1 Installation Requirements 6

2.2 Installation and Configuration 7

genuReSI by genua GmbH. All rights reserved.

2.1 Installation Requirements

- Configuration file `<config 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 → Digital Signatures`.
  2. Select the certificate **genua GmbH** and click on Details. 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 → Releases → Maintenance App 1.16 Release`. The download link is in the **genubox** section.

genuReSI by genua GmbH. All rights reserved.

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”.

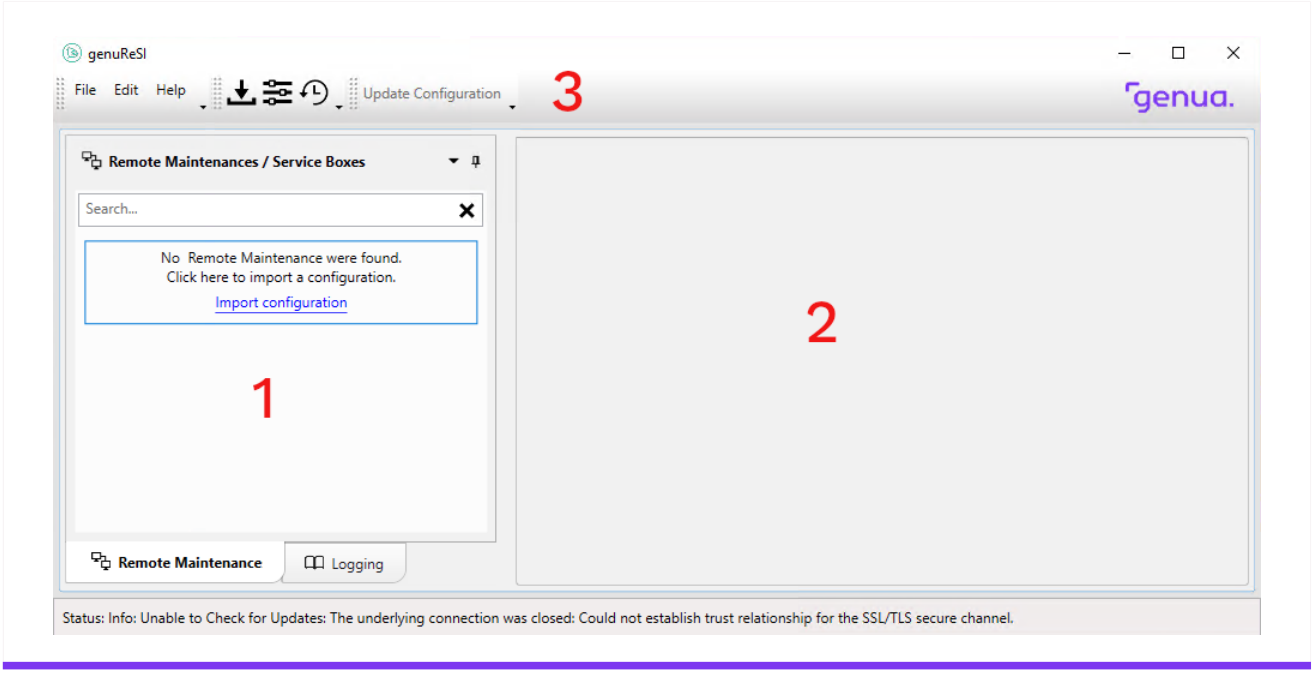

Figure 2.1: genuReSI Start Screen

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

Meaning of the icons from left to right:

- Import configuration
- Settings
- History

2.2.2 Importing the Configuration

The corresponding dialog will be opened by any of the following: Via the `File → 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+I. 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.

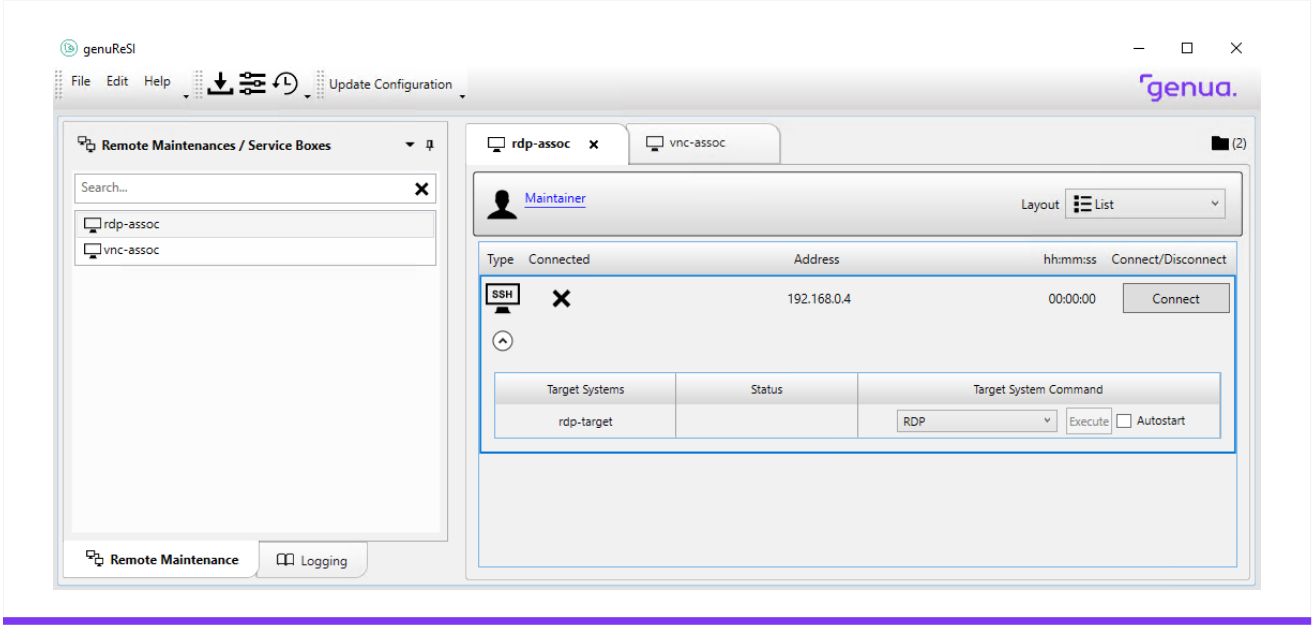

Figure 2.2: Maintenances / Service Boxes

genuReSI by genua GmbH. All rights reserved.

Chapter 3

genuReSI for Maintainers

3.1 Duties of the Maintainer 10
3.2 Establishing/Terminating the Maintenance Connection 11
3.3 Recording the Connection using RDP 13
3.4 Data Exchange between Maintainer and Target System 14
3.5 Configuration Updates 15
3.6 Logging/History 16
3.7 Local Settings 18
3.8 Commands 20
3.9 Plugins 21
3.10 genuReSI Update 22
3.11 genuReSI USB/Portable Mode 22

genuReSI by genua GmbH. All rights reserved.

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.

 genuReSI by genua GmbH. All rights reserved.

3.2 Establishing/Terminating the Maintenance Connection

The imported rendezvous connections are listed on the left side of the screen, and the connection methods (SSH or L2TP) for the connection are on the right. After selecting the rendezvous connection, click on the “Connect” 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).

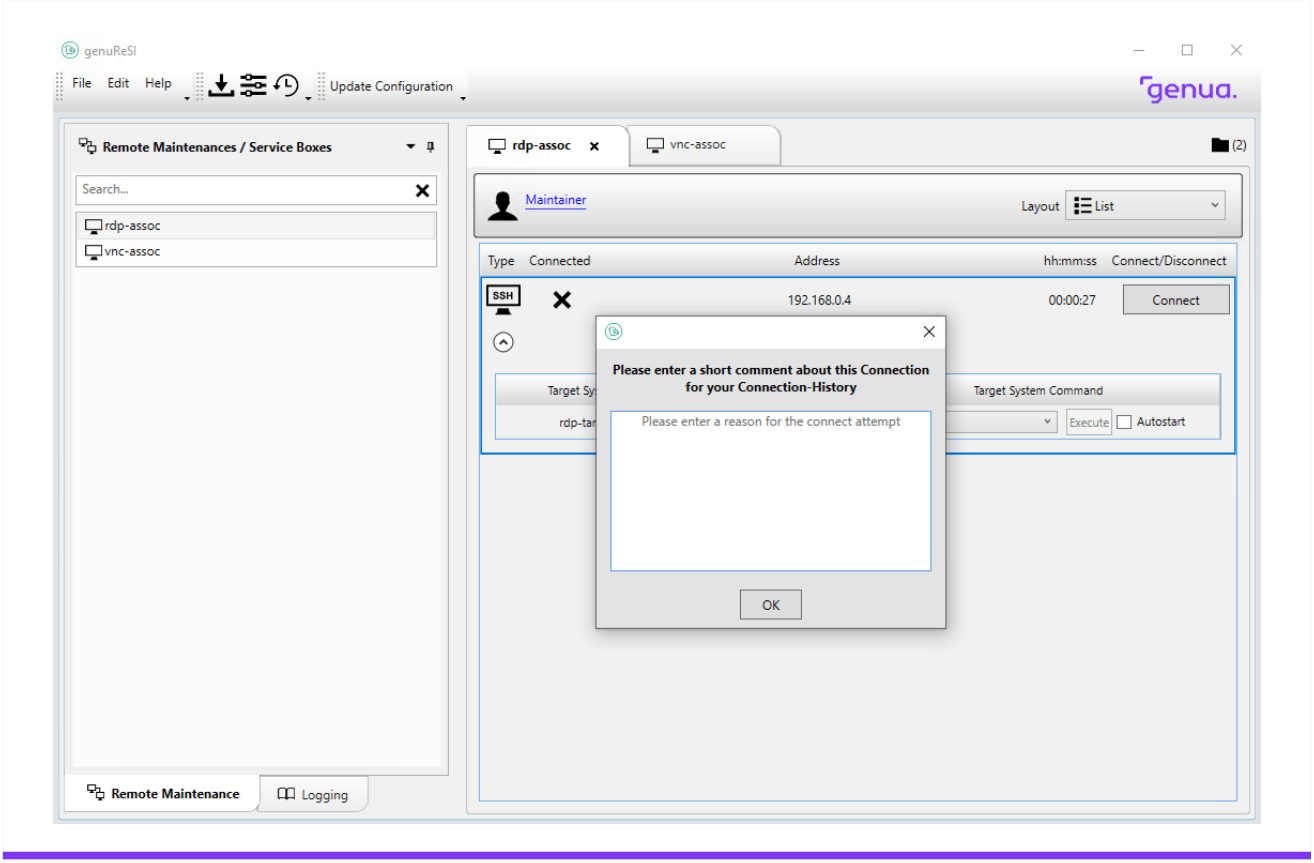

Figure 3.1: Establishing the connection – Maintainer

Note: If the administrator did configure 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 to manually select 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.

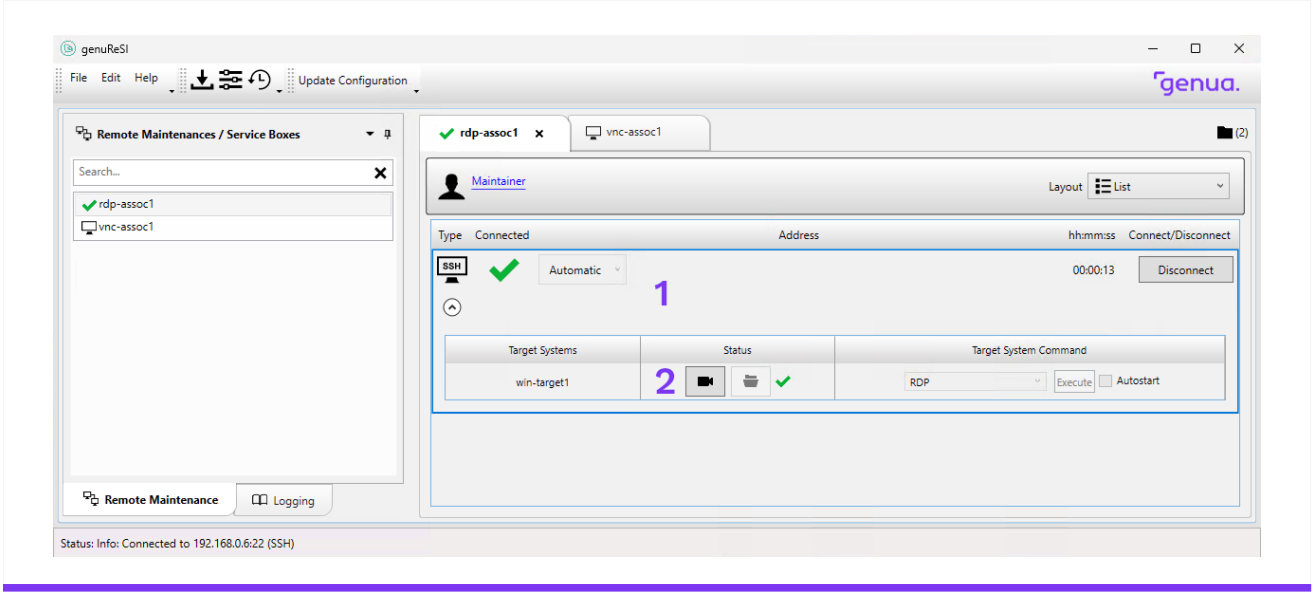

Figure 3.2: Window Layout

If **L2TP connections** are available, they will be selected and started accordingly. Other items that can be selected here are the default gateway and the preshared secret.

 genuReSI by genua GmbH. All rights reserved.

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.

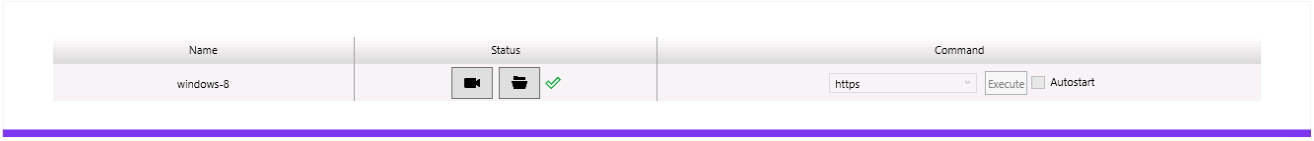

Figure 3.3: Recording Connections

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.

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.

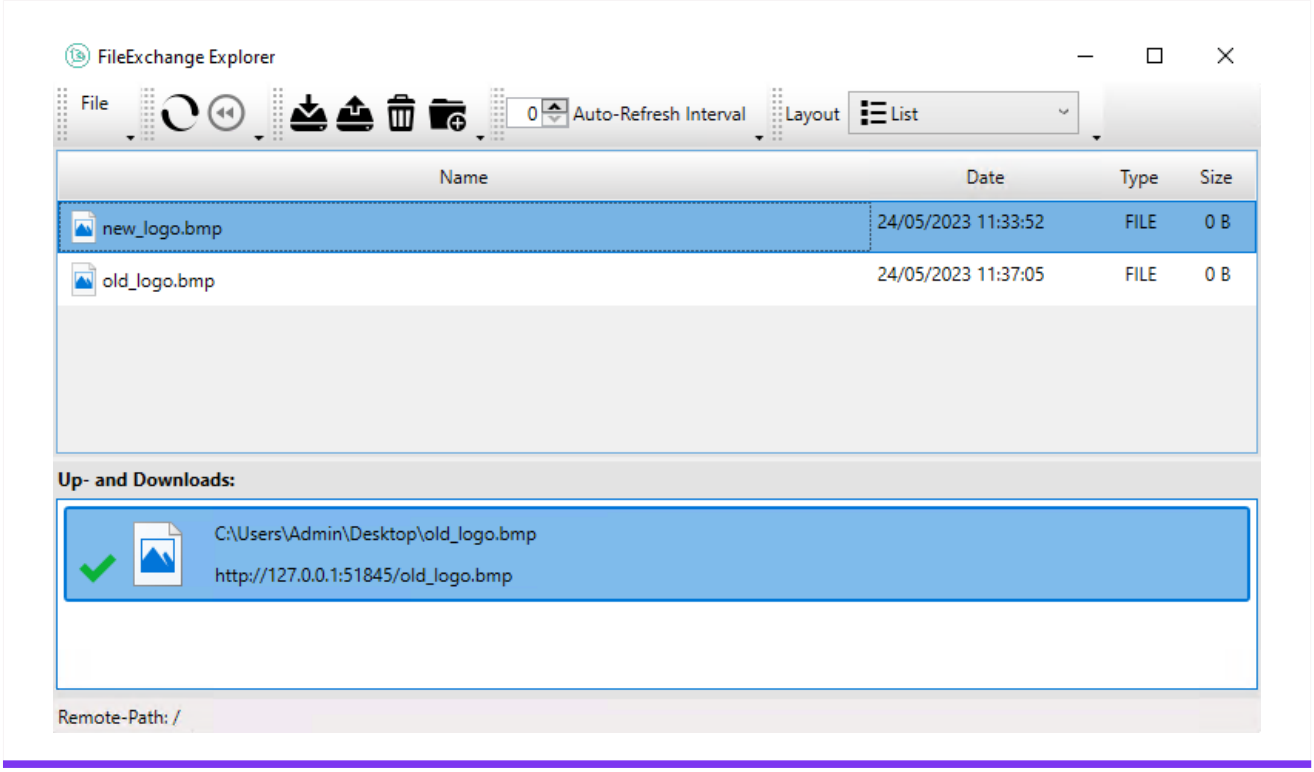

Figure 3.5: File Exchange Explorer

The upper window of the explorer shows all available objects. The lower window shows 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.

 genuReSI by genua GmbH. All rights reserved.

3.5 Configuration Updates

If an SSH connection to the Rendezvous Box has already been established, configuration changes are directly transmitted and displayed with every genuReSI status check. Changes like this add for example new connections. Usually they are done via Central Management Station genucenter. No configuration files have to be actively imported. This behavior is not currently supported for L2TP connections.

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.

genuReSI by genua GmbH. All rights reserved.

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.

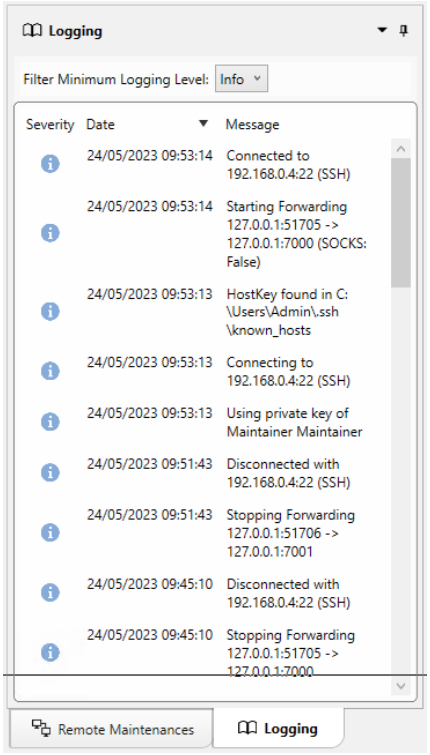

Figure 3.6: Logging

genuReSI by genua GmbH. All rights reserved.

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.

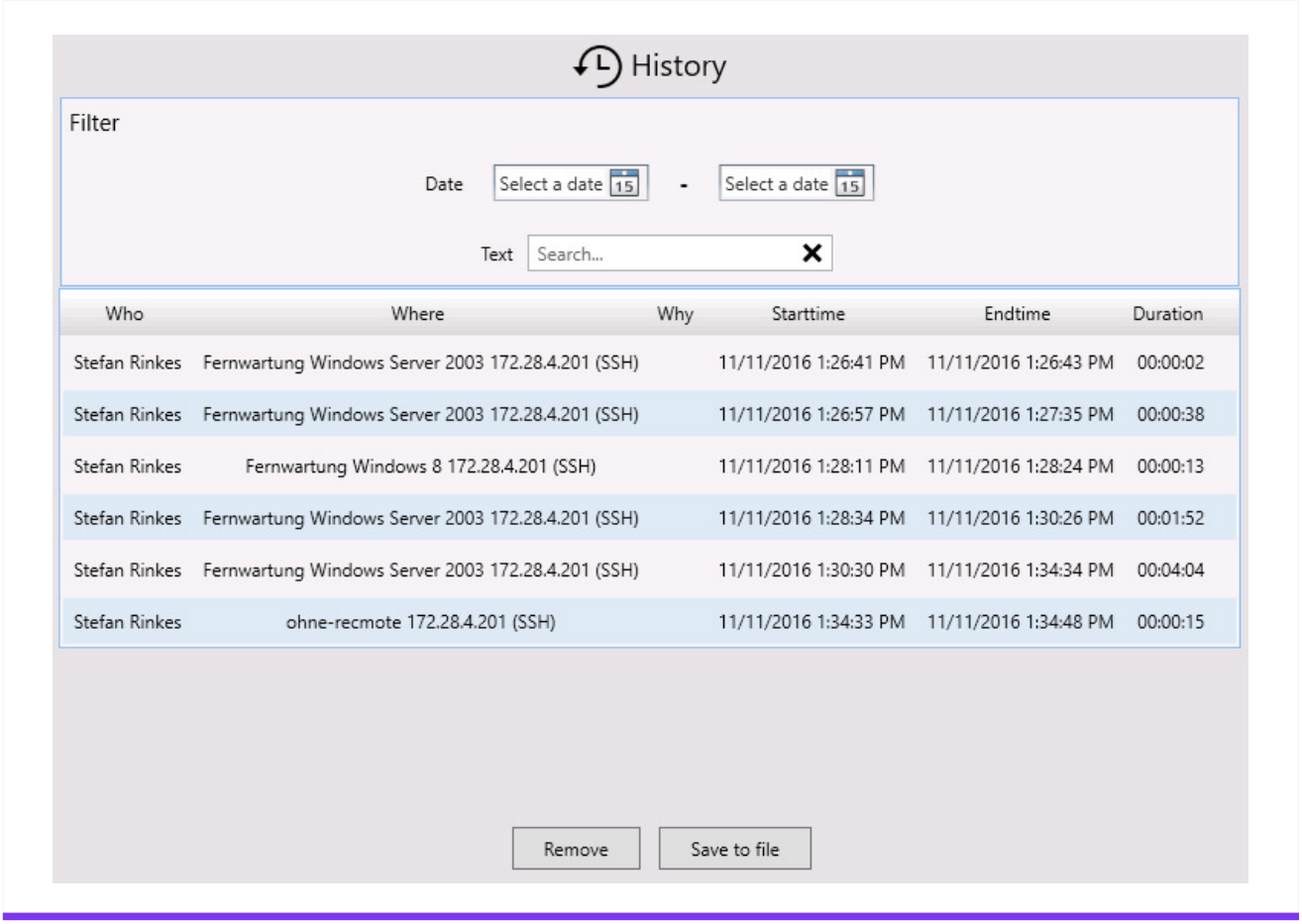

Figure 3.7: Maintenance Connection History

genuReSI by genua GmbH. All rights reserved.

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 smartcard middleware.
- **Commands**:
  Definition of commands, see chapter 3.8.
- **L2TP**:
  Definition of L2TP parameters.
- **Roles**:
  Overview of available roles and settings.

genuReSI by genua GmbH. All rights reserved.

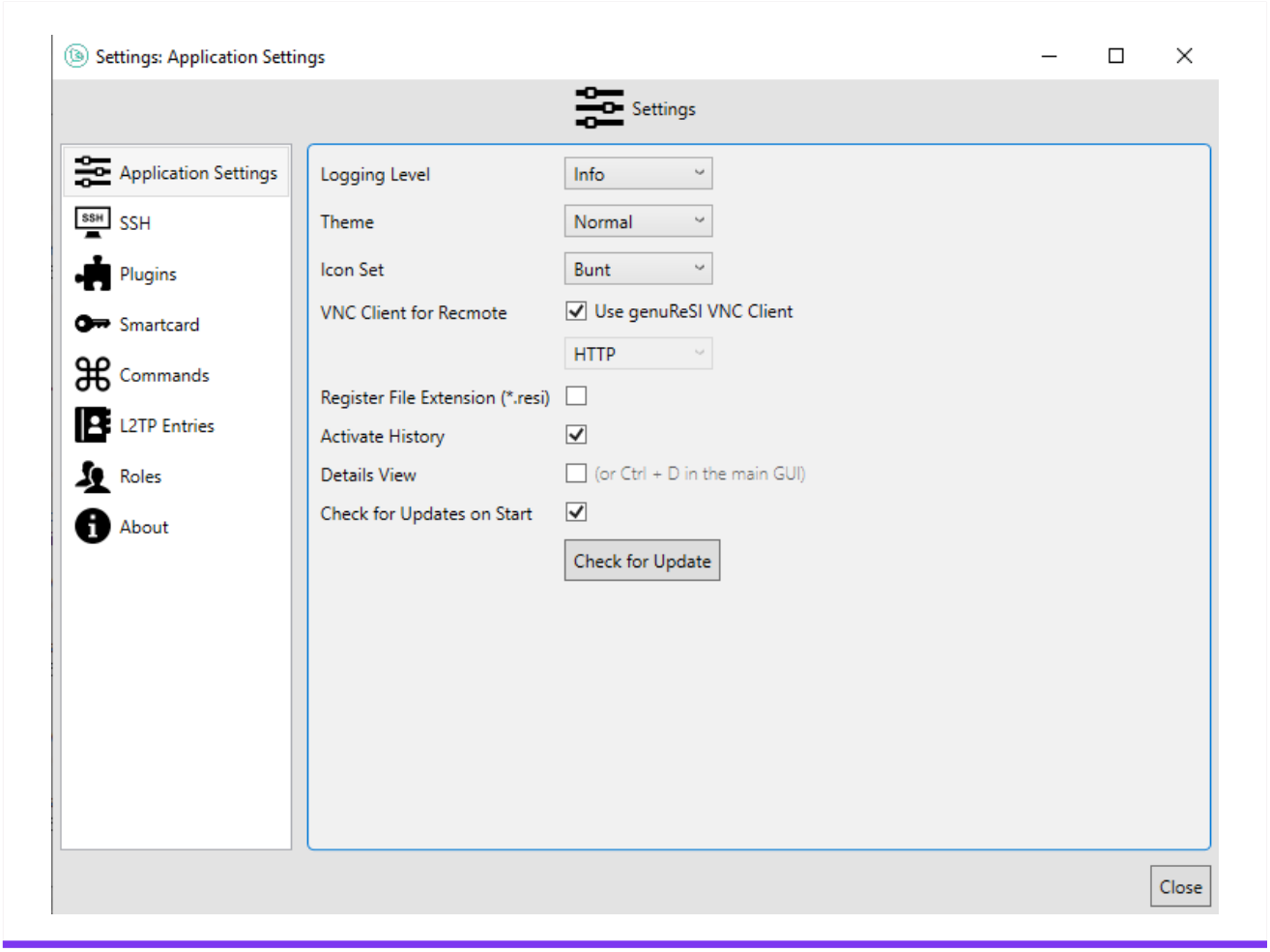

Figure 3.8: Maintainer Settings

genuReSI by genua GmbH. All rights reserved.

3.8 Commands

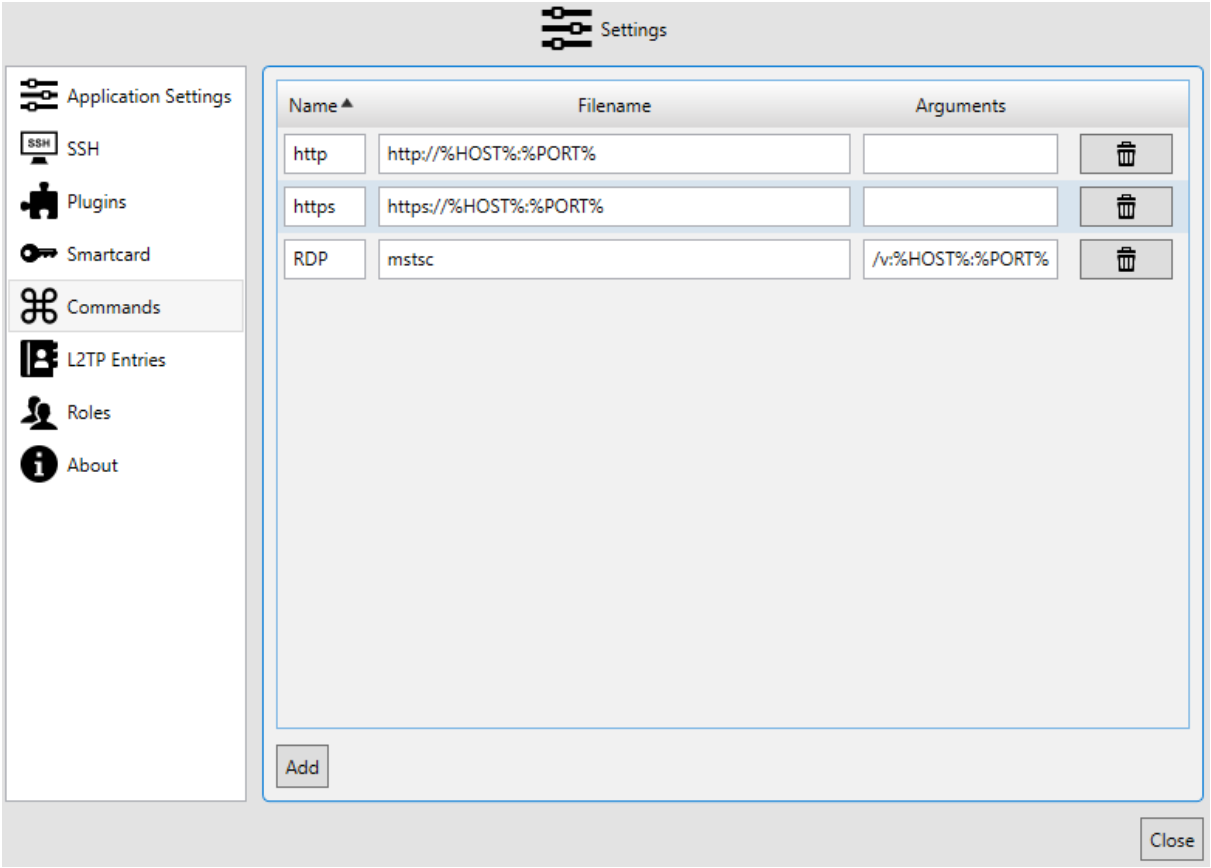

Figure 3.9: Commands Settings

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.

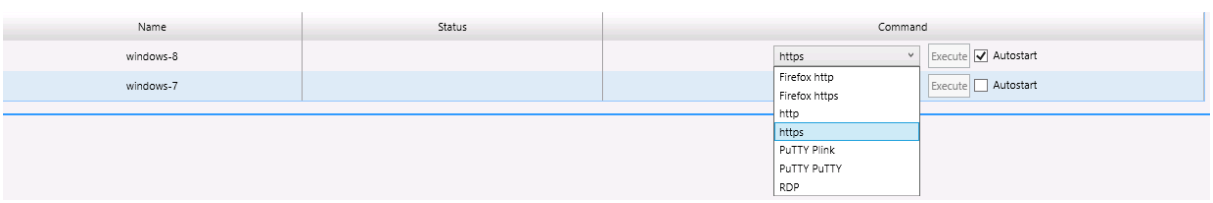

Figure 3.10: Autostart Function

genuReSI by genua GmbH. All rights reserved.

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).

Plugins are installed/uninstalled via the `Settings → Plugins` menu.

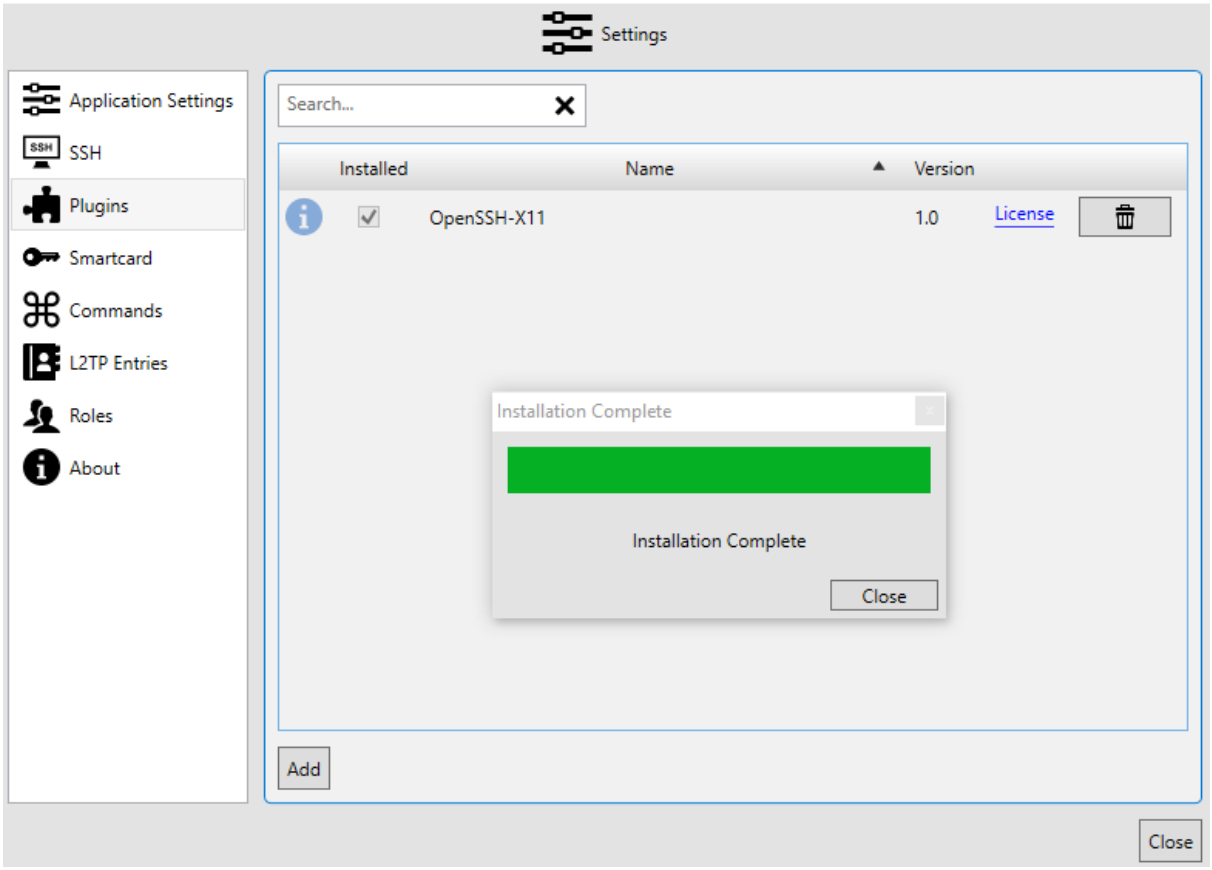

Figure 3.11: Plugins

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

1. Change to
   `Edit → Settings → Application 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` → `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.

genuReSI by genua GmbH. All rights reserved.

Chapter 4

genuReSI for Operators

4.1 Duties of the Operator 24
4.2 Establishing/Terminating the Maintenance Connection 25
4.3 Access Control at Runtime 28
4.4 Recording the Connection with RDP and SSH 29
4.5 Share Option 31
4.6 Configuration Updates 32
4.7 Logging/History 33
4.8 Local Settings 36
4.9 genuReSI Update 38

genuReSI by genua GmbH. All rights reserved.

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.

 genuReSI by genua GmbH. All rights reserved.

4.2 Establishing/Terminating the Maintenance Connection

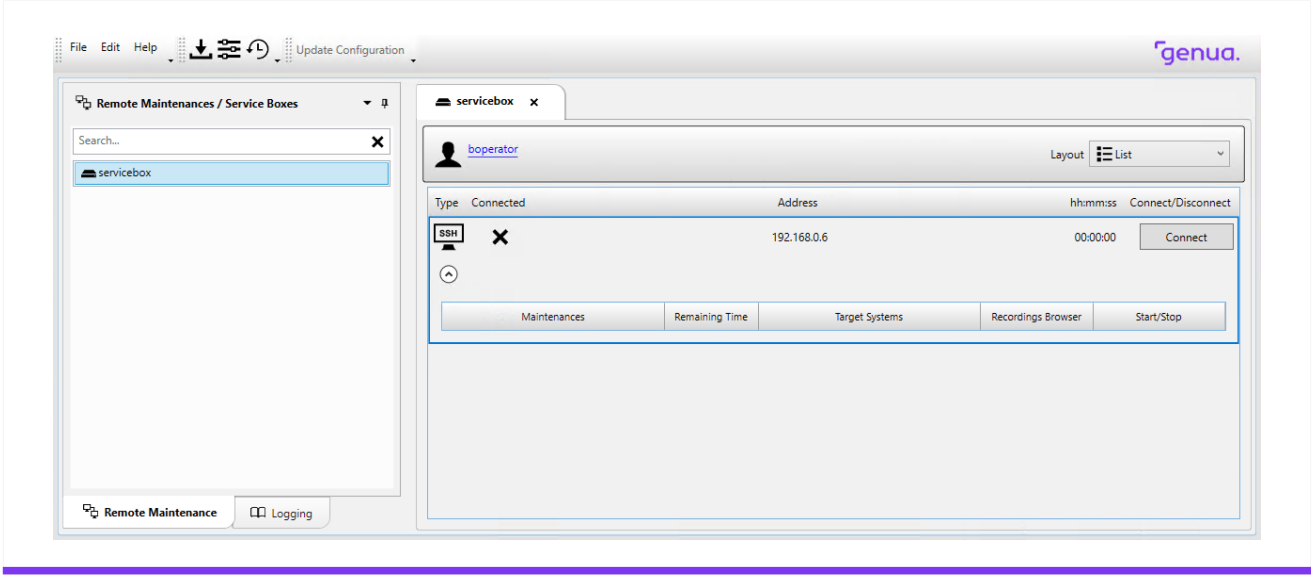

Figure 4.1: Establishing the Connection – Operator

The imported operator connections are listed on the left side of the screen, and the connection methods for the connection are 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!

genuReSI by genua GmbH. All rights reserved.

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

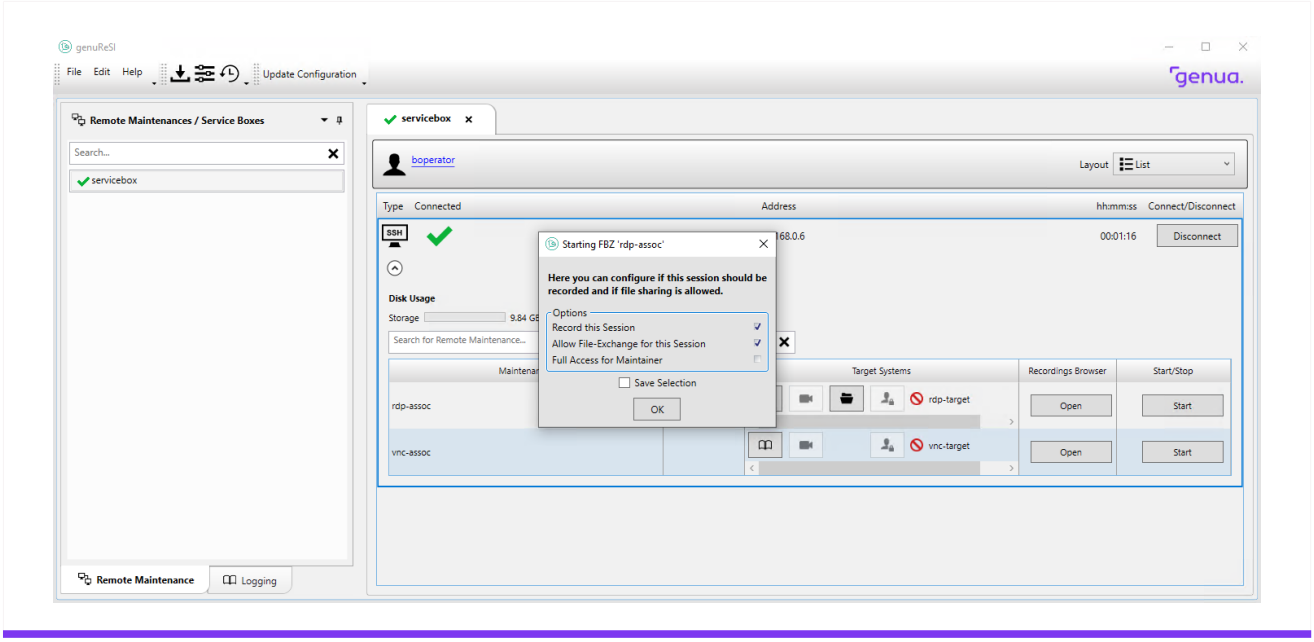

Figure 4.2: Establishing the Connection

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.

genuReSI by genua GmbH. All rights reserved.

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.

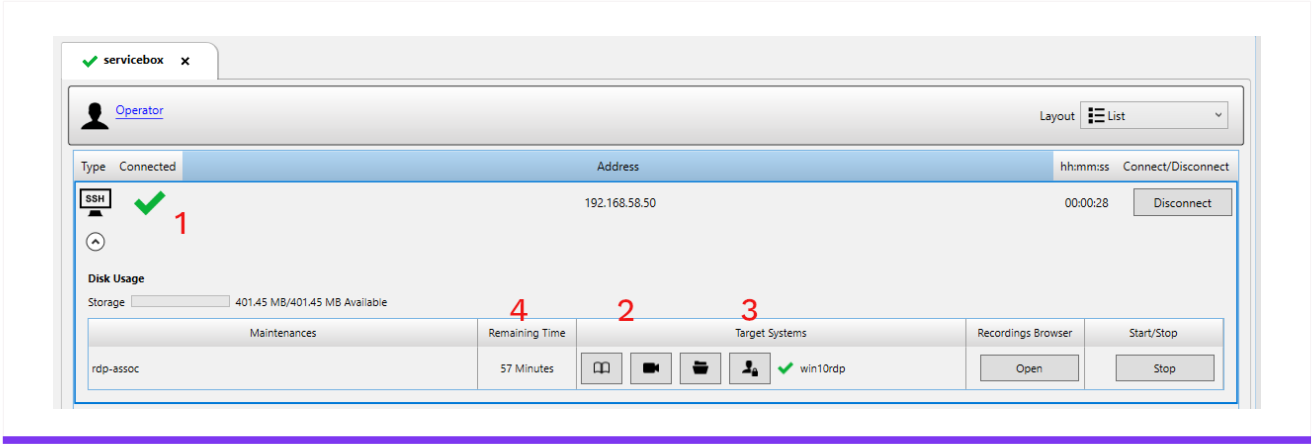

Figure 4.3: Connections Overview

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.

genuReSI by genua GmbH. All rights reserved.

4.3 Access Control at Runtime

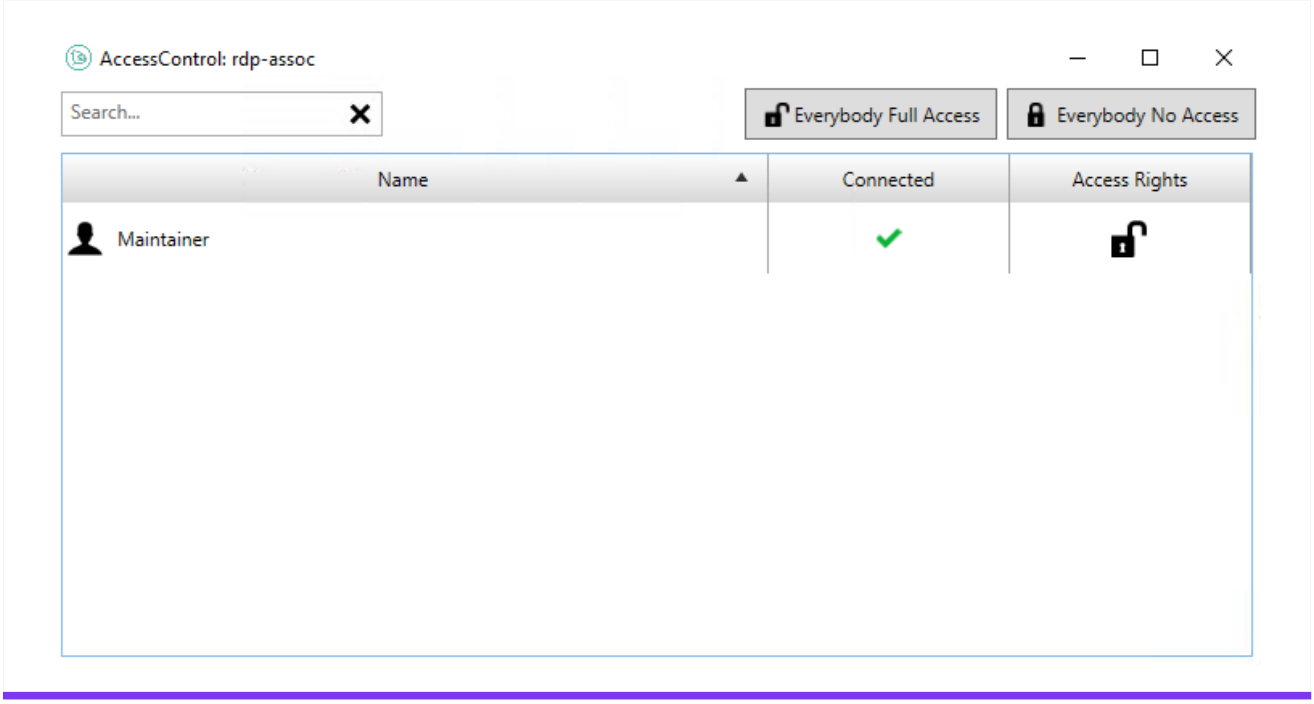

Figure 4.4: Connections Overview

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.

genuReSI by genua GmbH. All rights reserved.

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 filling up available storage space.

genuReSI by genua GmbH. All rights reserved.

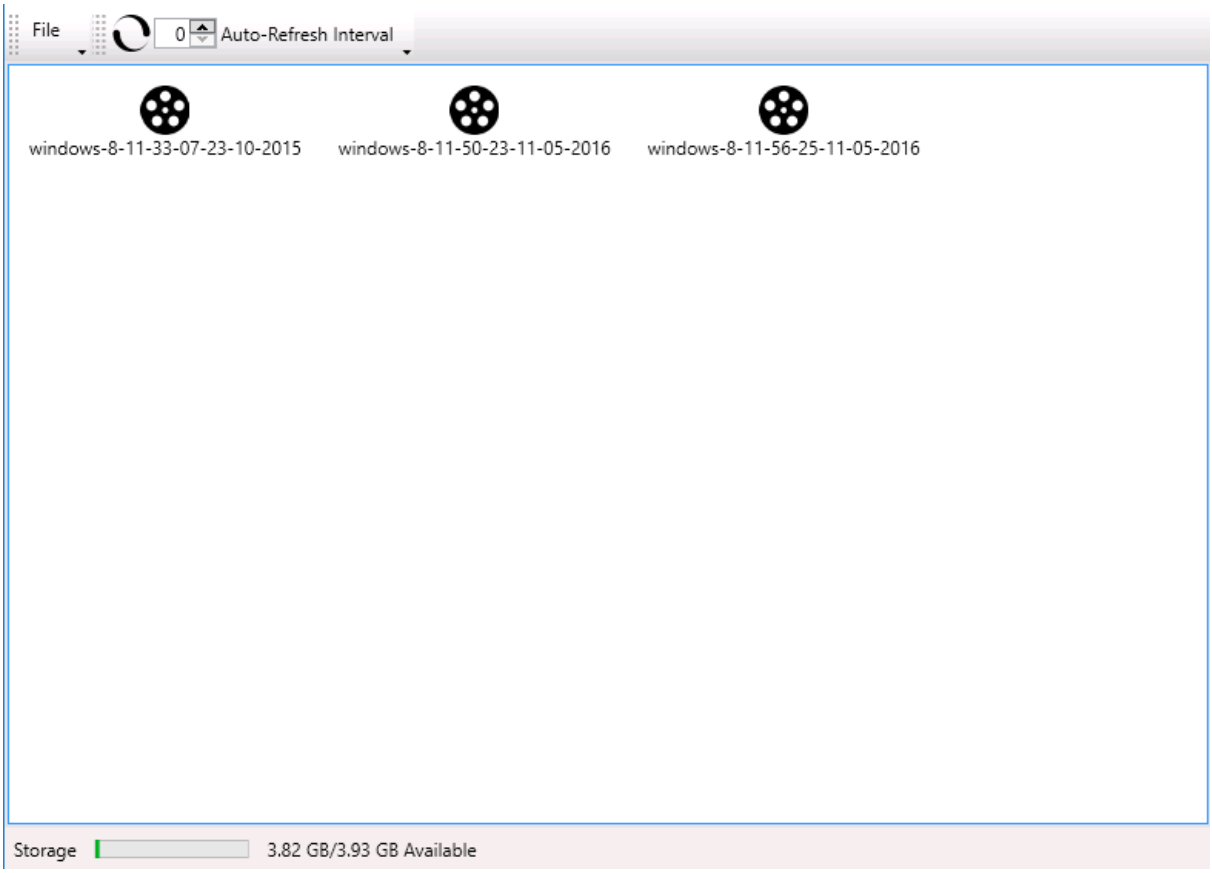

Figure 4.6: Downloading/Converting Recordings

 genuReSI by genua GmbH. All rights reserved.

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.

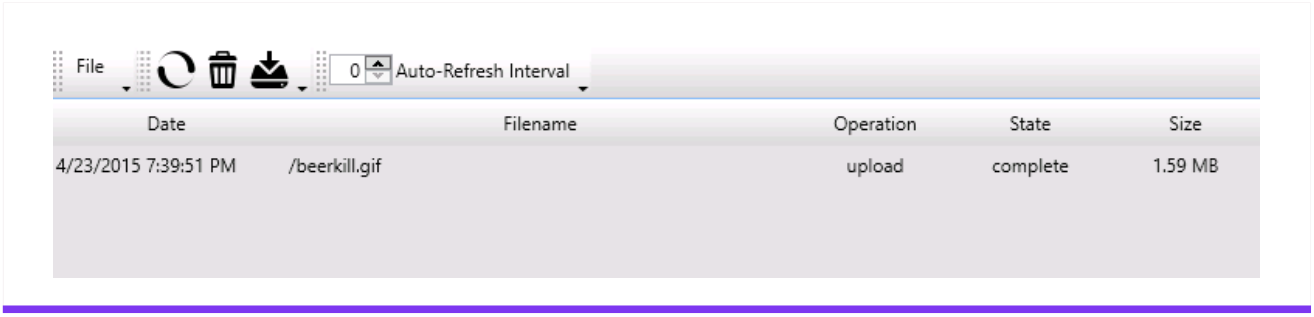

Figure 4.7: File Exchange

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.

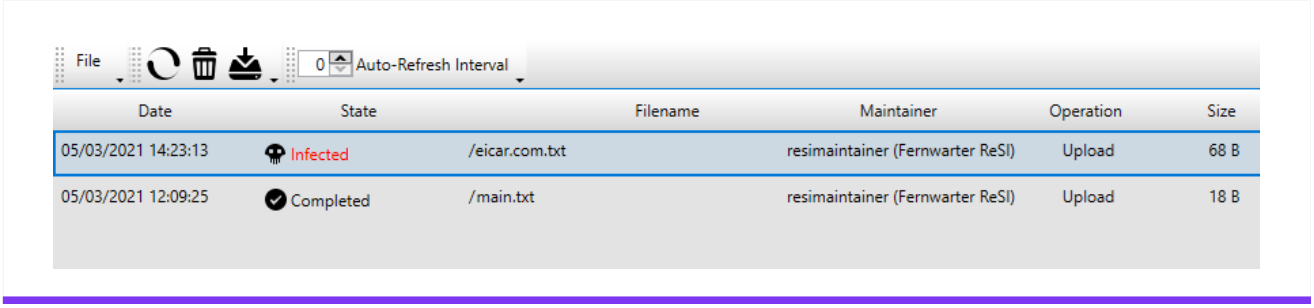

Figure 4.8: Malware detected (“Infected”)

genuReSI by genua GmbH. All rights reserved.

4.6 Configuration Updates

Configuration changes, e.g., adding new maintenance connections, are usually done via the Central Management Station genucenter. If an SSH connection to the genubox has already been established, configuration changes are directly transmitted and displayed with every genuReSI status check. No configuration files have to be actively imported.

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.

genuReSI by genua GmbH. All rights reserved.

4.7 Logging/History

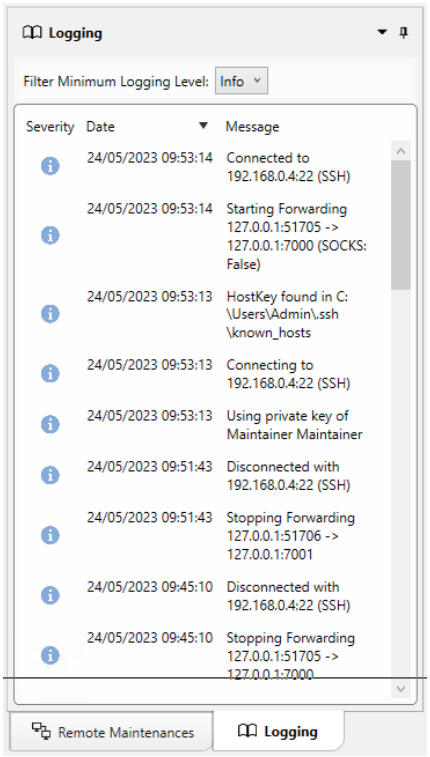

Figure 4.9: Logging

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.

genuReSI by genua GmbH. All rights reserved.

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.

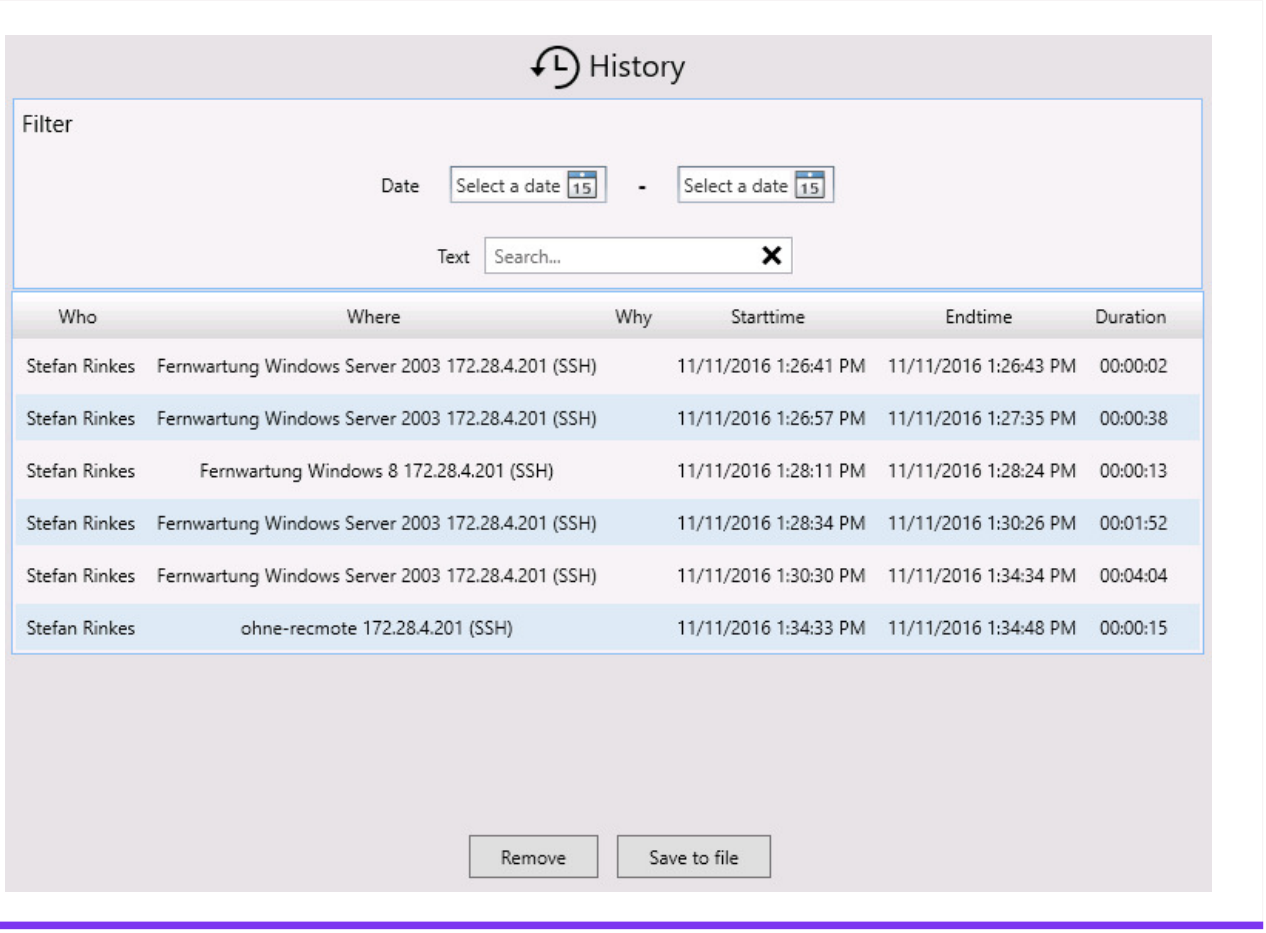

Figure 4.10: History

genuReSI by genua GmbH. All rights reserved.

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

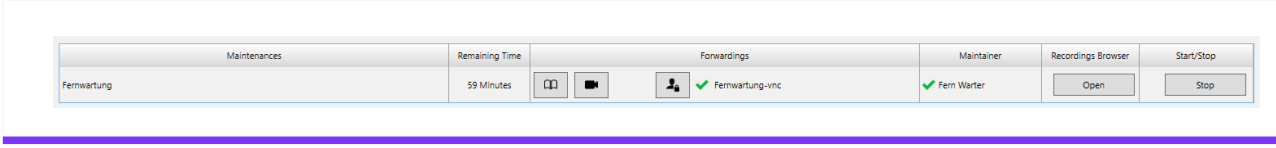

Figure 4.11: Logging Active Session

This is displayed in a separate window:

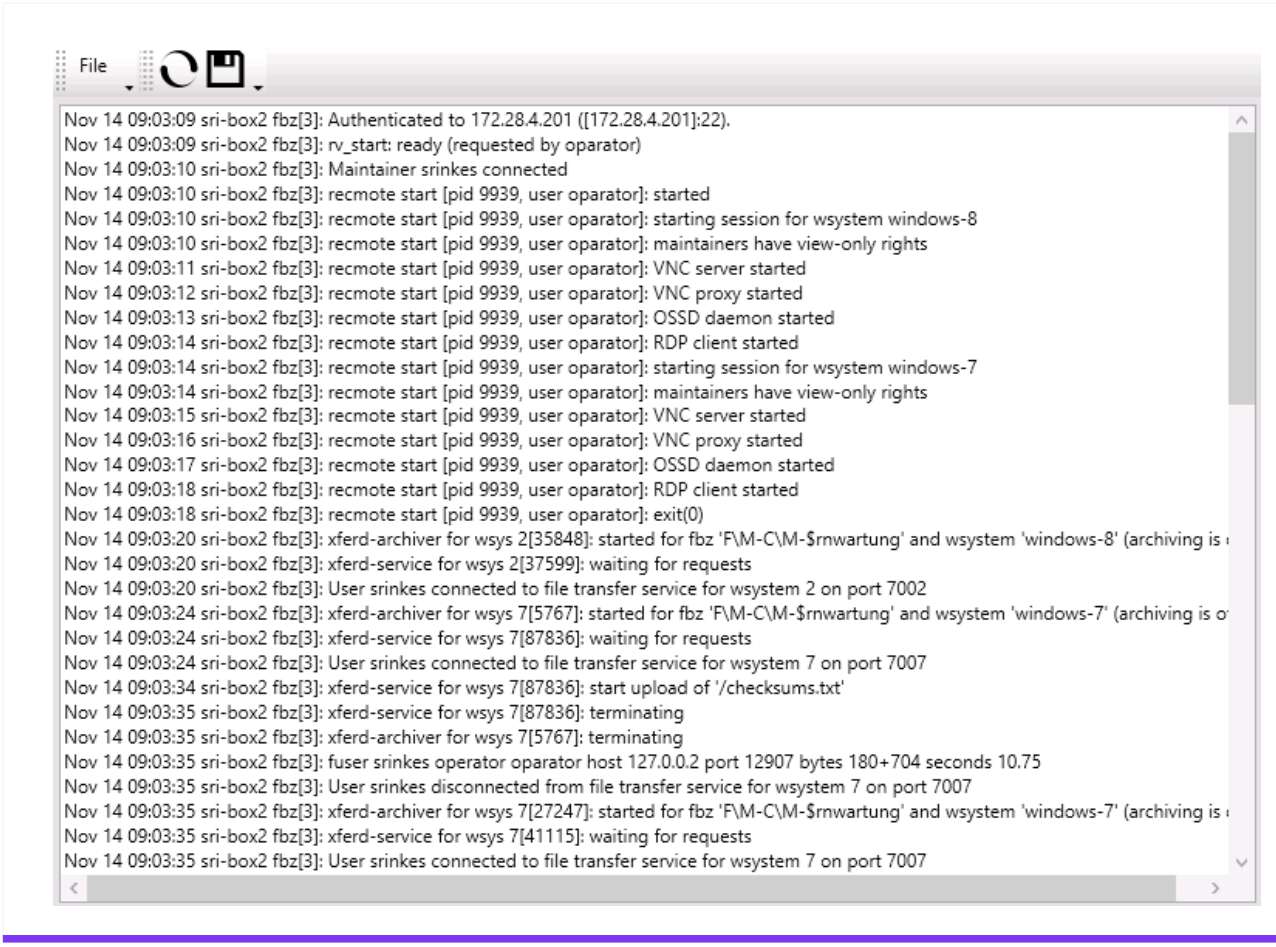

Figure 4.12: Log Data Output

genuReSI by genua GmbH. All rights reserved.

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 smartcard middleware.
- **Commands**:
  Definition of commands, see chapter 3.8.
- **L2TP**:
  Definition of L2TP parameters.
- **Roles**:
  Overview of available roles and settings.

 genuReSI by genua GmbH. All rights reserved.

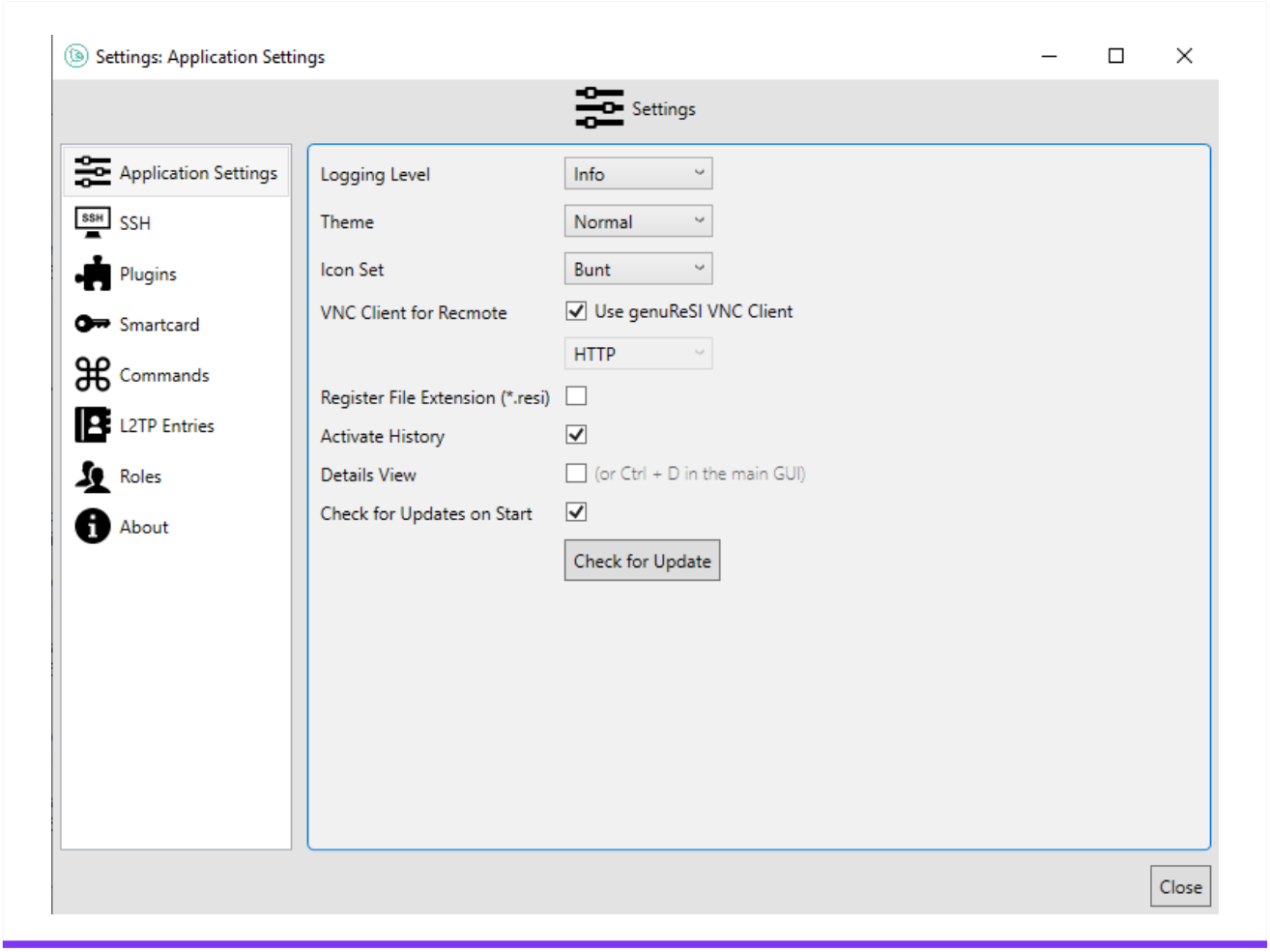

Figure 4.13: Settings

genuReSI by genua GmbH. All rights reserved.

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` → `Application Settings` and deactivate the checkbox **Check for Updates on Start**. All updates have to be triggered manually now.

genuReSI by genua GmbH. All rights reserved.

Chapter 5

Advanced Configuration

5.1 Configuration Files 40
5.2 Role Management 41
5.3 Using a Smartcard 42
5.4 Use with Firewall/NAT Gateway 45
5.5 HTTP Proxy for SSH 46
5.6 GUI Layout 47
5.7 New Commands 48

genuReSI by genua GmbH. All rights reserved.

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.

 genuReSI by genua GmbH. All rights reserved.

5.2 Role Management

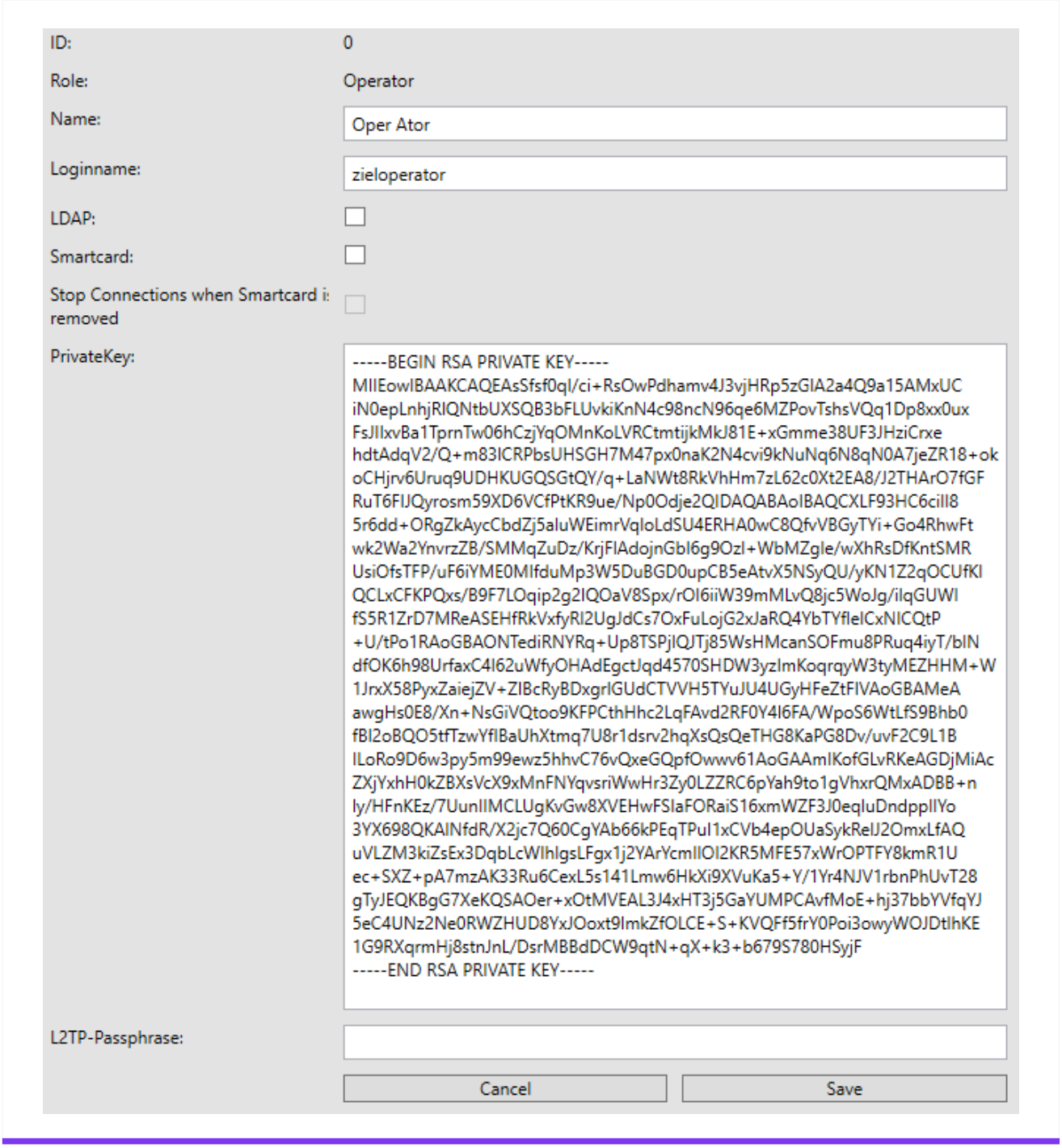

Figure 5.1: Role Management

The configuration files, including the roles (login name and private key/L2TP passphrase), are normally 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 desired role, which will open a window in edit mode. Save the changes with the **Save** button.

5.3 Using a Smartcard

A smartcard can be used to authenticate the operator and the maintainer.

5.3.1 PKCS#11 Module

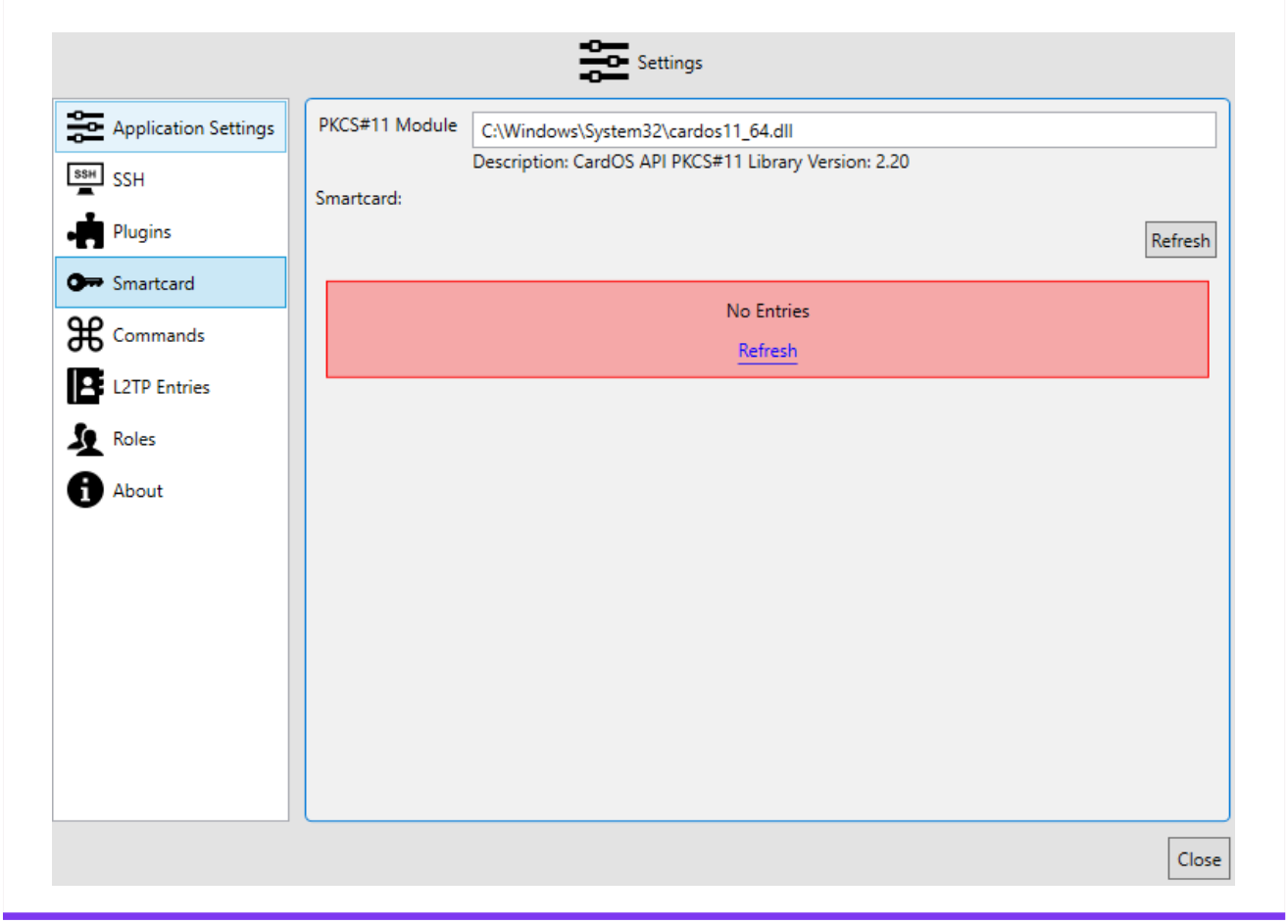

Figure 5.2: Selecting the PKCS Module

Enter the file path to your PKCS#11 middleware under `Settings` → `Smartcard` in genuReSI. The file path can be found in the manual for your smartcard software.

5.3.2 Smartcard Assignment

To support smartcard authentication for a user, select the respective user under `Settings` → `Roles`. Check the **Smartcard** box and then apply the changes by clicking on **Save**.

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

 genuReSI by genua GmbH. All rights reserved.

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

5.3.3 Assigning the Public Key in genucenter

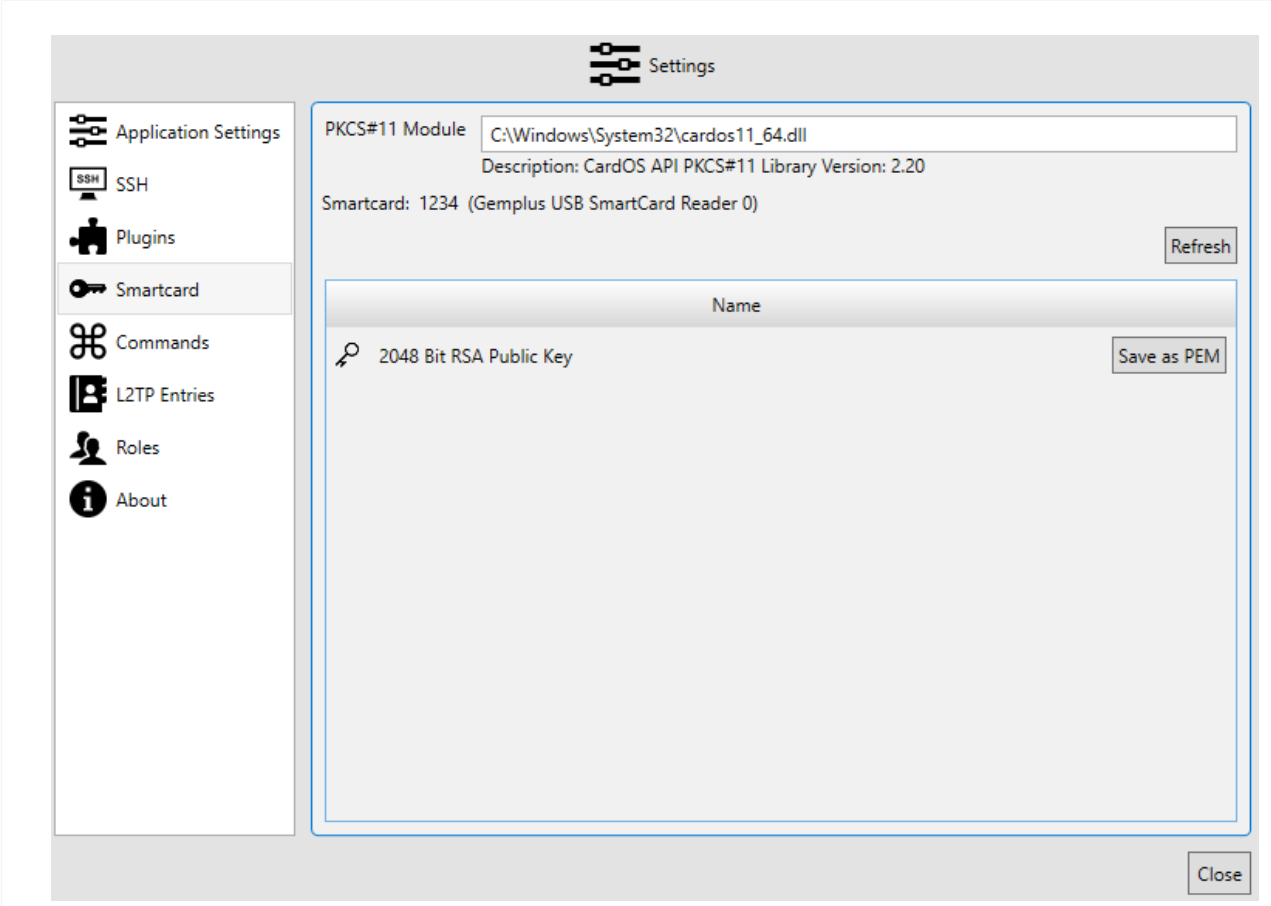

Figure 5.3: Smartcard Menu

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

1. Export the public key of the user's smartcard in the genuReSI App GUI at `Settings` → `Smartcard` by clicking on **Save as PEM**.
2. Upload the public key in the genucenter:
   (a) In the genucenter, navigate to either `Rendezvous` → `Operators` → `<genuReSI user>` or `Rendezvous` → `Maintainers` → `<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.

genuReSI by genua GmbH. All rights reserved.

5.3.4 Establishing the Connection

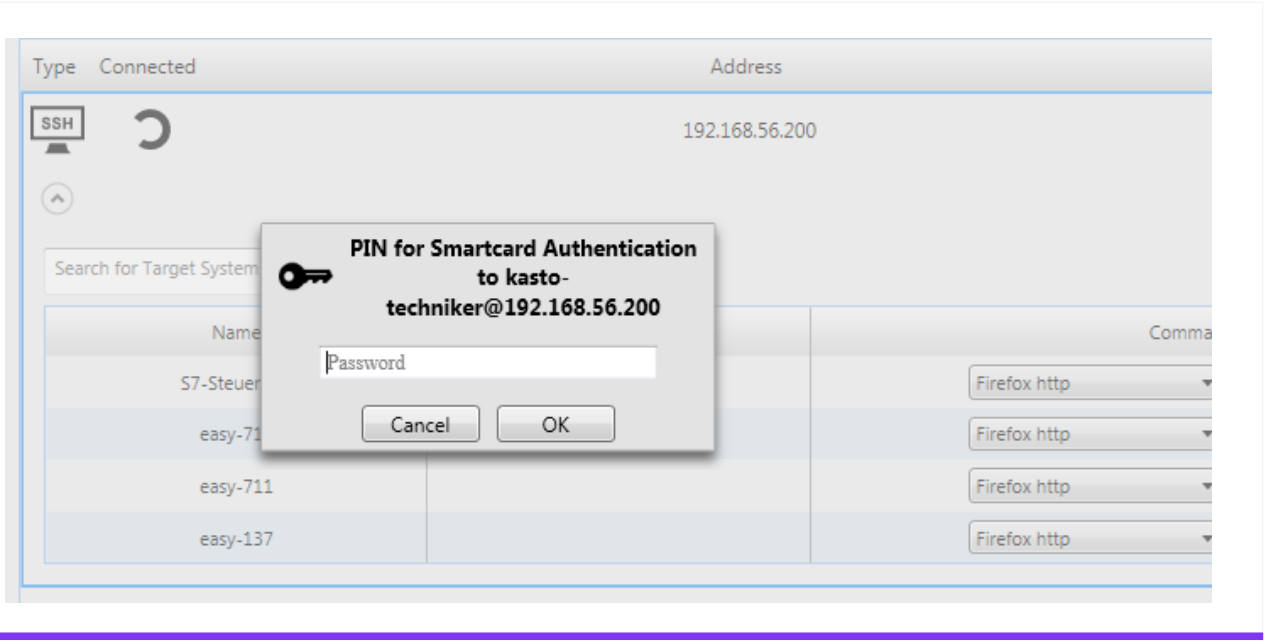

Figure 5.4: Smartcard PIN Entry

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

genuReSI by genua GmbH. All rights reserved.

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.

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

genuReSI by genua GmbH. All rights reserved.

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
```


genuReSI by genua GmbH. All rights reserved.

5.6 GUI Layout

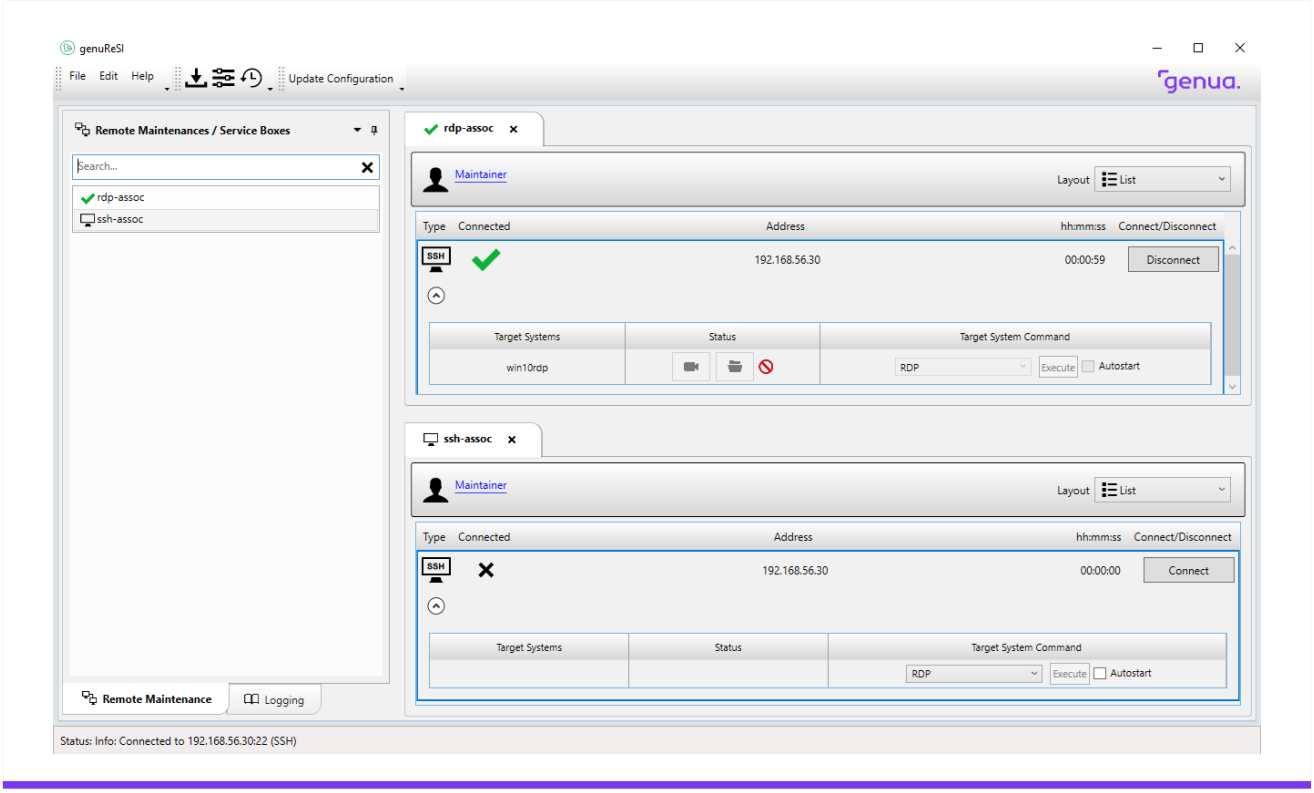

Figure 5.5: GUI Layout

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.

genuReSI by genua GmbH. All rights reserved.

5.7 New Commands

The rendezvous concept utilizes an internal mechanism called port forwarding, which directs connections to the trusted machine via the rendezvous server. In the **Commands** menu in the toolbar, commands can be defined to be executed on the target system (the machine being maintained). To do this, the command syntax of the command to be used must be known. The variables `%HOST%` and `%PORT%` designate the hostname and the port used. Windows environment variables are supported. **Example**: PuTTY should be used to open an SSH connection to the target system. Filename defines where on the local file system the `putty.exe` application is located. The command `-P %PORT% %HOST%` must be defined under Arguments, as the port is specified with `-P` using PuTTY via command line.

 genuReSI by genua GmbH. All rights reserved.

Chapter 6

STEP7 via Rendezvous

6.1 GUI Installation of the Loopback Adapter 50

6.2 Command Line Installation of the Loopback Adapter 51

6.3 IP Configuration 52

genuReSI by genua GmbH. All rights reserved.

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` → `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

 genuReSI by genua GmbH. All rights reserved.

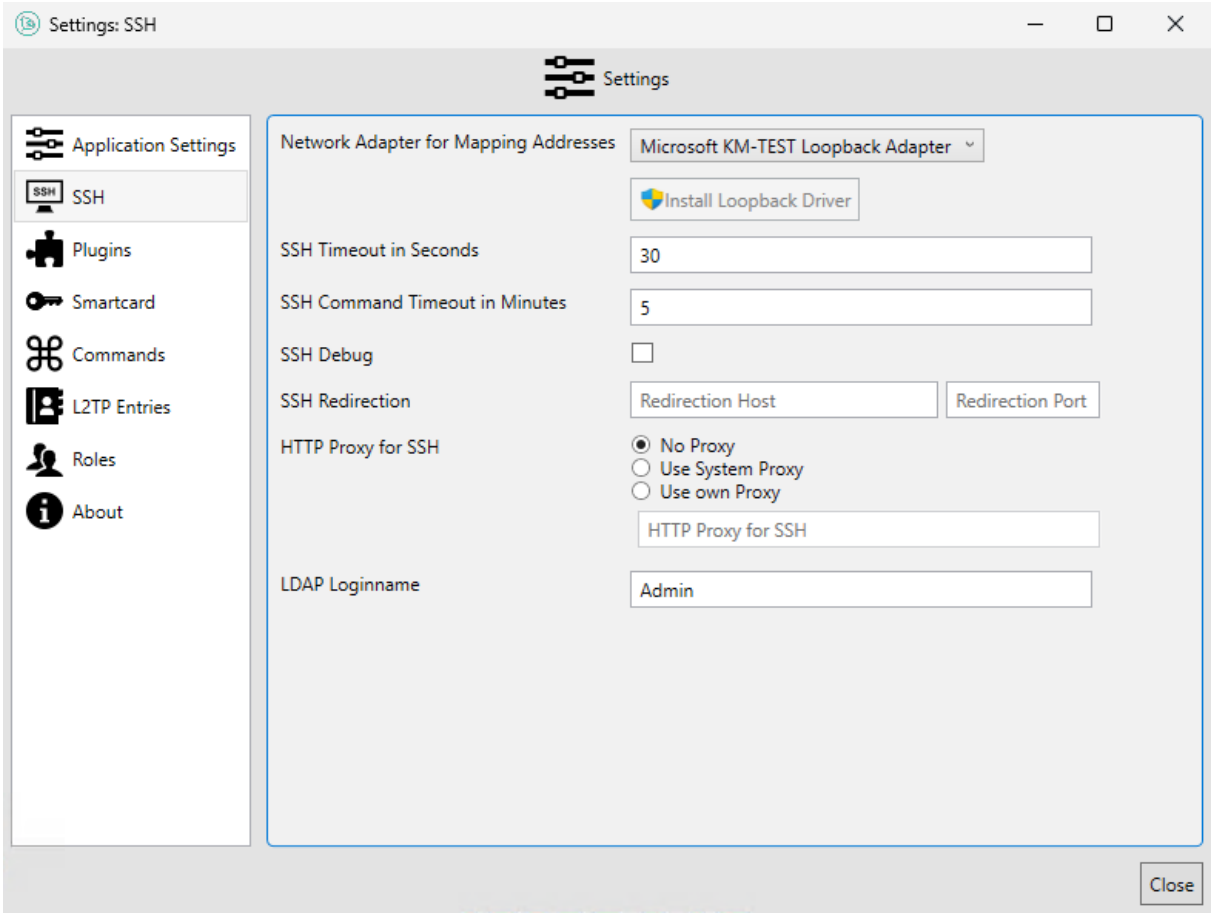

Figure 6.1: genuReSI Loopback Adapter

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 Yes.

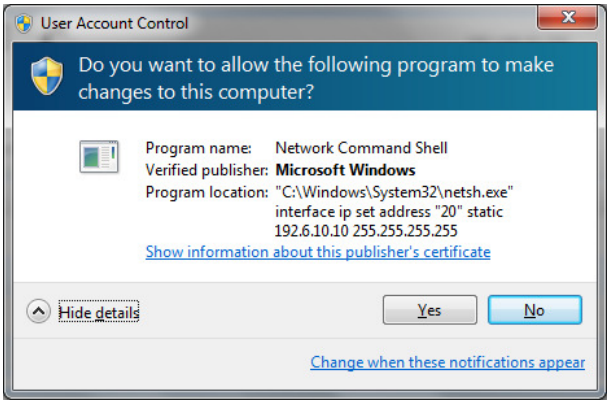

Figure 6.2: User Account Control

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.

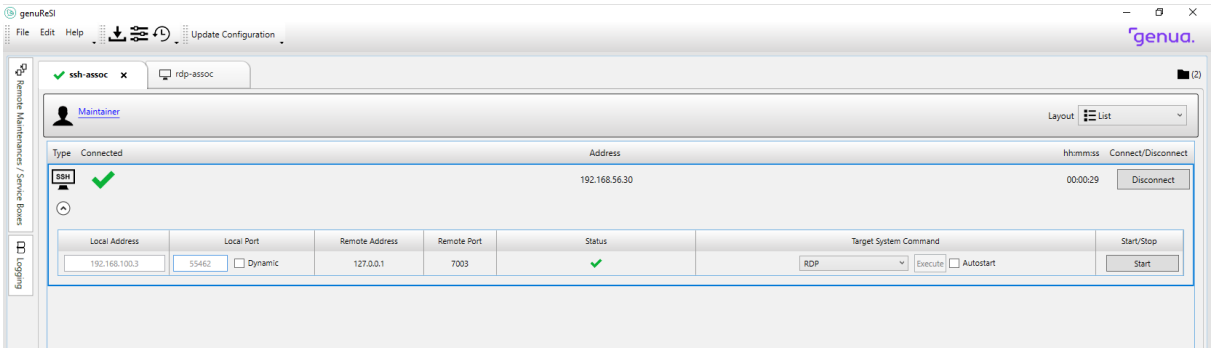

Figure 6.3: genuReSI with Active Connection

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

genuReSI by genua GmbH. All rights reserved.

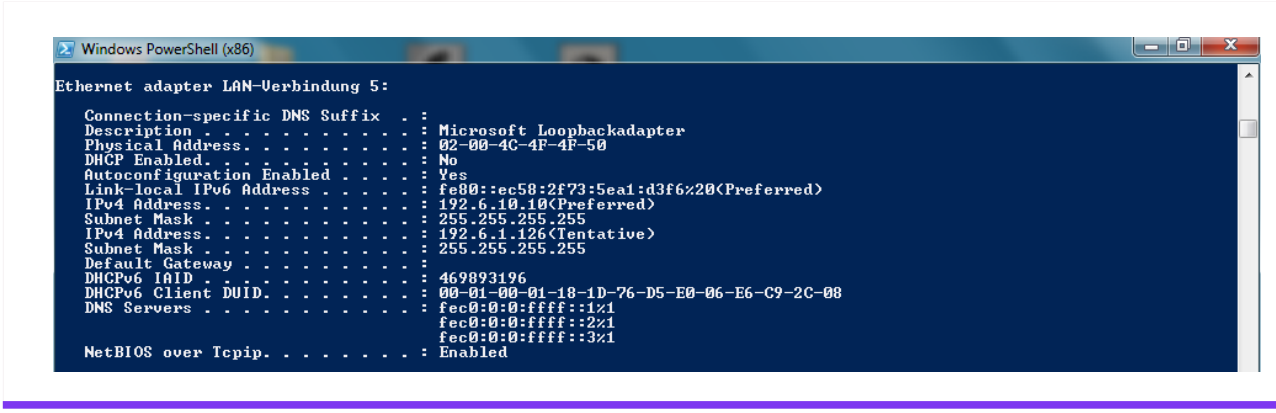

Figure 6.4: PowerShell with Mapping

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

genuReSI by genua GmbH. All rights reserved.

 genuReSI by genua GmbH. All rights reserved.

Index

A

Advanced configuration 39

G

genuReSI for Maintainers 9
genuReSI for Operators 23

L

Launching the genuReSI Windows Application 5

M

Maintenance with the rendezvous concept 1

P

Product Overview v

S

STEP7 via Rendezvous 49

genuReSI by genua GmbH. All rights reserved.

genua
A Bundesdruckerei Company

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