

genuReSI

Installations- und
Konfigurationshandbuch

Version 1.19

Ausgabe: 28. August 2025

Revision: 4af3cdb

Urheberrecht ©2002–2025 genua GmbH. Alle Rechte vorbehalten.

Dieses Produkt enthält Software auf Basis des OpenBSD-Betriebssystems.

genua GmbH
Domagkstraße 7
85551 Kirchheim b. München
Tel.: +49 89-991950-0
Fax : +49 89-991950-999

Alle im Handbuch angegebenen Marken und Lizenzen sind Eigentum der jeweiligen Inhaber und werden nur zu Informationszwecken erwähnt.

Die eingetragenen Marken der genua GmbH finden Sie hier:

<https://kunde.genua.de/impressum/warenzeichen.html>

Mit freundlichen Grüßen

Ihre genua GmbH

Inhaltsverzeichnis

Vorwort	v
1 Fernwartung mit dem Rendezvous-Konzept	1
1.1 Das Rendezvous-Konzept von genua	2
1.2 Einsatz der Fernwartungs-App genuReSI	4
2 Aufruf der Windows-App genuReSI	5
2.1 Installationsvoraussetzungen	6
2.2 Installation und Konfiguration	7
3 genuReSI für den Fernwarter	9
3.1 Aufgaben des Fernwarters	10
3.2 Aufbau/Abbau der Fernwartungsverbindung	10
3.3 Aufzeichnen der Verbindung bei RDP	11
3.4 Datenaustausch zwischen Fernwarter und Zielsystem	12
3.5 Konfigurationsupdates	13
3.6 Logging/History	14
3.7 Lokale Einstellungen	16
3.8 Befehle	18
3.9 Erweiterungen/Plugins	19
3.10 genuReSI Update	20
3.11 genuReSI USB/Portable Mode	20
4 genuReSI für den Operator	21
4.1 Aufgaben des Operators	22
4.2 Aufbau/Abbau der Fernwartungsverbindung	22
4.3 Zugriffskontrolle zur Laufzeit	25
4.4 Aufzeichnen der Verbindung bei RDP und SSH	25

4.5	Share-Option	26
4.6	Konfigurationsupdates	27
4.7	Logging/History	28
4.8	Lokale Einstellungen	30
4.9	genuReSI Update	31
5	Erweiterte Konfiguration	33
5.1	Konfigurationsdateien	34
5.2	Rollenverwaltung	35
5.3	Verwendung einer Smartcard	37
5.4	Verwendung mit Firewall/NAT-Gateway	40
5.5	HTTP Proxy für SSH	41
5.6	GUI-Gestaltung	42
5.7	Neue Befehle	43
6	STEP7 durch Rendezvous	45
6.1	GUI-Installation des Loopback-Adapters	46
6.2	Befehlsbasierte Installation des Loopback-Adapters	47
6.3	IP-Konfiguration	48
	Index	51

Vorwort

Über dieses Produkt

Die Windows-Applikation genuReSI (genua Remote Secure Integration) bietet eine übersichtliche und leicht zu bedienende Schnittstelle für Konfiguration, Verwaltung und Kontrolle von Fernwartungsbeziehungen im Rahmen des Rendezvous-Fernwartungskonzepts.

Konventionen zur Textdarstellung

- **Text**: Text für Konsolenein- und ausgaben, Befehle, Dateinamen und Pfade
- „Text“: In GUI-Felder einzugebender Text; Namen von Icons, Links und externen Programmen
- **Taste**: Taste auf der Tastatur oder Schaltfläche in der GUI
- **Menü** → **Untermenü**: Menüpfad in der GUI

Warnhinweise

Hinweis: Hinweise bieten zusätzliche Informationen, die den Betrieb erleichtern können oder bestimmte Einschränkungen bei einer Funktion aufzeigen.



Vorsicht! Die Stufe Vorsicht weist auf kleinere Sicherheitsrisiken, geringfügige oder kurzfristige Betriebsstörungen bei Nichtbeachtung hin.



Warnung! Die Stufe Warnung weist auf erhöhte Sicherheitsrisiken, gravierende oder längerfristige Betriebsstörungen bei Nichtbeachtung hin.



Gefahr! Die Stufe Gefahr weist auf gravierende Sicherheitsrisiken, vollständigen und dauerhaften Betriebsausfall oder dauerhaften Datenverlust bei Nichtbeachtung hin.

Änderungen im Handbuch

Das vorliegende Handbuch wird bei jedem neuen Software-Release an die Änderungen angepasst. Es beschreibt den jeweiligen Ist-Zustand der genuReSI-Software.

Kundenportal von genua

Sie erreichen unser Kundenportal unter <https://kunde.genua.de/>. Nachdem Sie sich mit Ihren Zugangsdaten angemeldet haben, gelangen Sie über die Hauptnavigation via **Produkte** → **genubox** → **Fernwartungs-App(genuReSI)** in den Supportbereich für genubox und genuReSI. Hier finden Sie unsere hilfreiche Knowledge Base, Best Practices, Known Issues, Release Notes und Software-Patches.

Feedback zum Handbuch

Ihre Meinung ist uns wichtig. Bitte zögern Sie nicht, uns Feedback zu geben, falls Ihnen in diesem Handbuch bspw. Informationen fehlen oder unklar erscheinen. Senden Sie uns dazu einfach eine E-Mail an: support@genua.de

Kapitel 1

Fernwartung mit dem Rendezvous-Konzept

1.1	Das Rendezvous-Konzept von genua	2
1.2	Einsatz der Fernwartungs-App genuReSI	4

1.1 Das Rendezvous-Konzept von genua

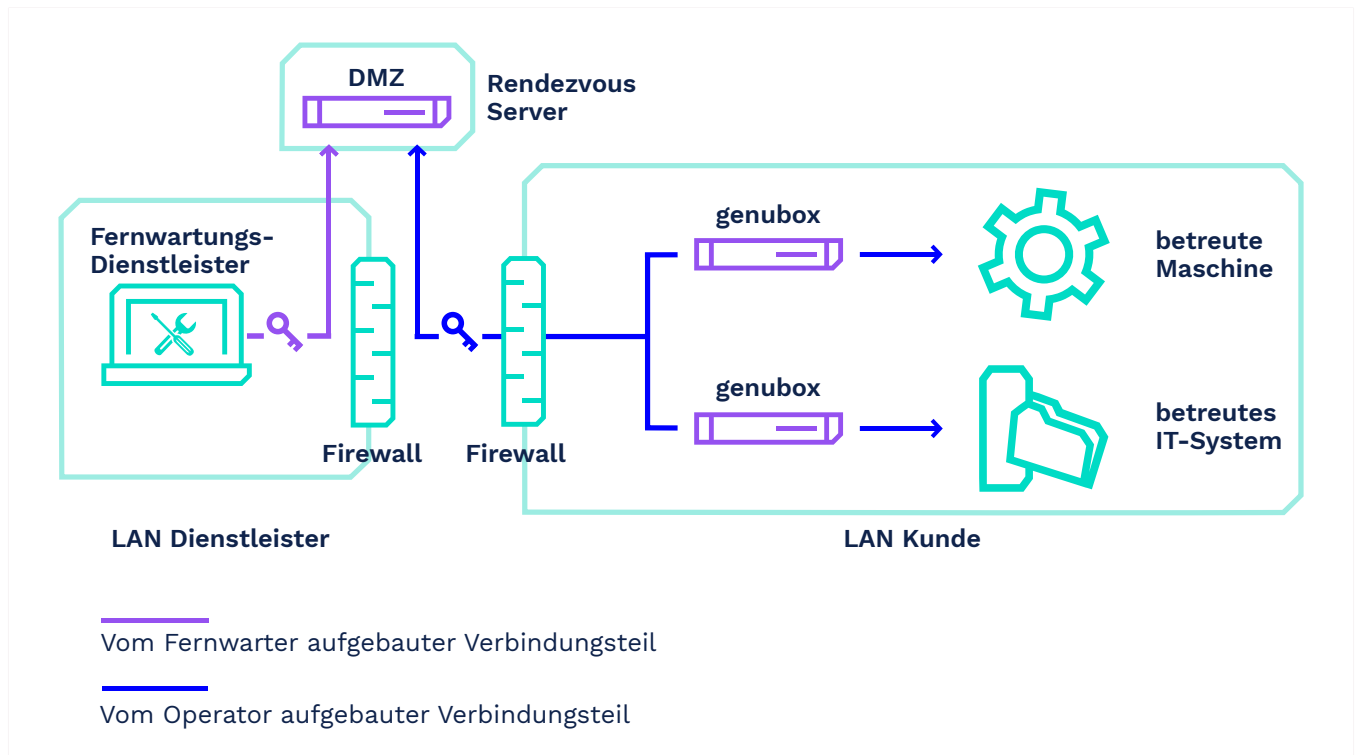


Abbildung 1.1: Rendezvous-Konzept

Das Herzstück des Rendezvous-Konzeptes ist der sogenannte Rendezvous-Server (typischerweise eine genubox). Dieser Server kann in der DMZ des Anlagenherstellers oder des Dienstleisters stehen. Vor der zu wartenden Anlage wird ebenfalls eine genubox als Firewall- und VPN- Lösung installiert, welche die Anlage vom restlichen IT-Netz isoliert.

Üblicherweise wird der Wartungszeitraum genau festgelegt, und der sogenannte **Fernwarter** baut zuerst eine VPN-Verbindung zur Rendezvousbox auf und muss sich dort authentisieren. Er kann aber keine direkte Verbindung zum Kundennetz aufbauen. Der sogenannte **Operator** (ein Administrator aus dem Kundennetz) muss die Verbindung zwischen dem Rendezvous-Server und der Servicebox aufbauen. Über diese beiden VPN-Tunnel wird jetzt die Verbindung zwischen Fernwarter und Wartungsobjekt aufgebaut. Der Fernwarter kann seine Wartungssoftware starten, sich falls erforderlich auf der zu wartenden Maschine authentisieren und mit den Arbeiten beginnen.

Die Verbindung vom Fernwarter zum Rendezvous-Server wird über SSH-VPN aufgebaut.

Nach Ende der Wartungsarbeiten beenden sowohl der Fernwarter als auch der Operator die aufgebauten Verbindungen.

Weder Fernwarter noch Operator benötigen tiefgehende Systemkenntnisse, da die gesamte Rendezvous-Lösung zentral über den Rendezvous-Server und ein Managementsystem (das genucenter) konfiguriert wird.

1.2 Einsatz der Fernwartungs-App genuReSI

Der Fernwarter kann die Wartungsverbindung über die Windows Applikation genuReSI (genua Remote Secure Integration) per Mausklick herstellen. Diese gestattet via leicht zu bedienender GUI die einfache Konfiguration und Verwaltung der Fernwartungsbeziehung.

Alle Sessions werden geloggt und können, je nach Konfiguration, sogar aufgezeichnet werden, um sie z. B. zu Schulungszwecken zu verwenden.

Optional kann genuReSI auch vom Operator zum Freischalten der Wartungsverbindung genutzt werden, wenn dieser eine Windows-Applikation der webbasierten GUI vorzieht.

Kapitel 2

Aufruf der Windows-App genuReSI

2.1	Installationsvoraussetzungen	6
2.2	Installation und Konfiguration	7

2.1 Installationsvoraussetzungen

- Die Konfigurationsdatei `<Config-Name>.resi` und das Passwort, das zum Schutz der Konfigurationsdatei vergeben werden kann (wird vom Anlagenhersteller bzw. Fernwartungsbetreiber auf dem genucenter erzeugt und zur Verfügung gestellt).
- Die ausführbare Datei `ReSI.exe` (neuester Download steht im Kundenportal unter <https://kunde.genua.de> zur Verfügung). Führen Sie die Datei als regulärer Benutzer aus, um genuReSI App zu starten. Das Programm benötigt weder eine Installation noch Administratorprivilegien.

Hinweis: genuReSI App ist digital mit einem Zertifikat von genua signiert. Die Signatur wird automatisch durch Windows geprüft. Alternativ prüfen Sie die Signatur manuell wie folgt:

1. Klicken Sie mit rechts auf das genuReSI App-Icon und navigieren Sie zu [Eigenschaften](#) → [Digitale Signaturen](#).
2. Wählen Sie das Zertifikat **genua GmbH** aus und klicken Sie auf [Details](#). Im Reiter **Allgemein** werden Informationen zur Gültigkeit der digitalen Signatur angezeigt.

- PC mit einem Windows-Betriebssystem, das Microsoft .NET Framework in der Version 4.8 oder höher unterstützt.
- Microsoft .NET Framework in der Version 4.8 oder höher.

Hinweis: Das entsprechende Microsoft .NET Framework wird ab Windows 7 SP2 automatisch installiert. Für frühere Versionen kann es direkt auf der Microsoft-Website heruntergeladen werden. Alternativ können Sie den externen Download-Link im genua-Kundenportal verwenden. Gehen Sie auf <https://kunde.genua.de>, melden Sie sich an und klicken Sie auf [Downloads](#) → [Releases](#) → [Fernwartungs-App 1.19 Release](#). Der Download-Link befindet sich im Abschnitt **genubox**.

2.2 Installation und Konfiguration

2.2.1 Installation genuReSI

Laden Sie die Datei **ReSI.exe** in das gewünschte Verzeichnis, beispielsweise

C:\Users\<Benutzername>\Desktop

Doppelklick auf das genuReSI-Icon wird die Applikation gestartet.

Vor dem Start müssen Sie noch ein Konfigurationspasswort angeben, um unbefugte Zugriffe zu verhindern. Das Passwort kann durch Ankreuzen von „Passwort speichern“ auch abgespeichert werden.

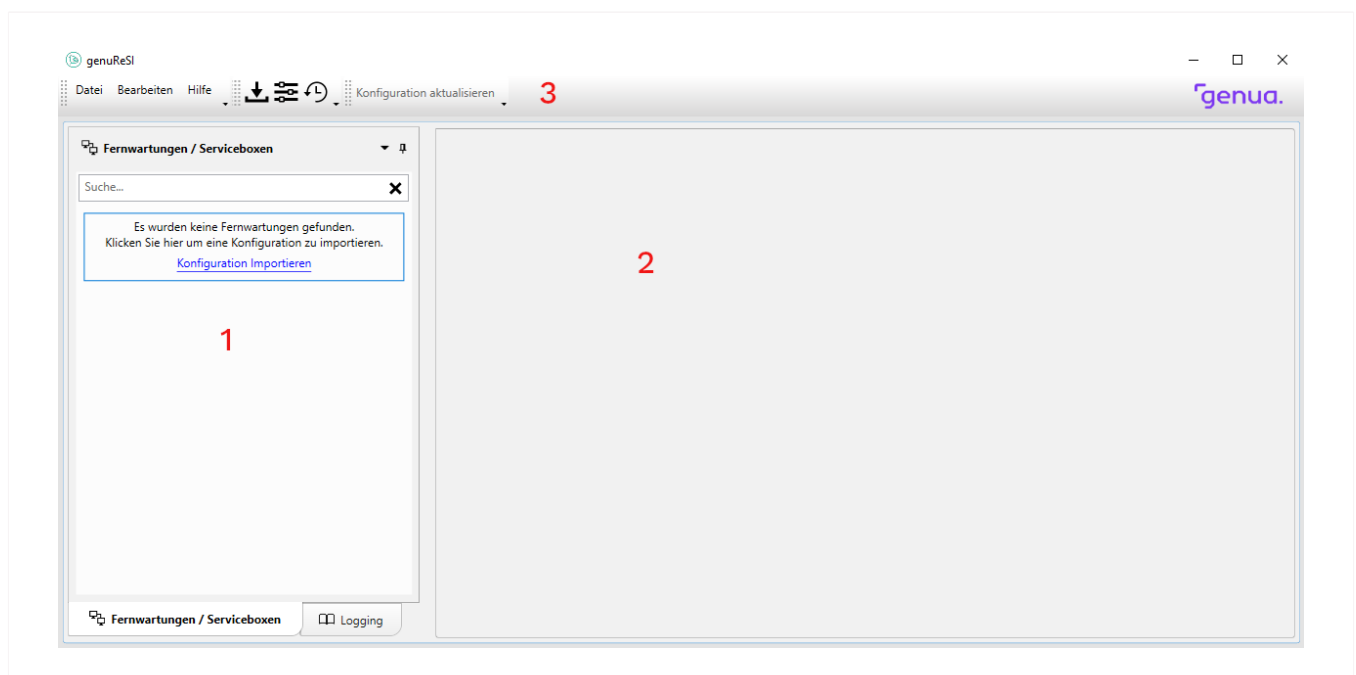


Abbildung 2.1: Startfenster genuReSI

1. Auswahlfenster Rendezvous-Verbindung/Logging
2. Hauptfenster
3. Toolbar

Bedeutung der Icons von links nach rechts:

- Konfiguration Importieren
- Einstellungen
- History

2.2.2 Importieren der Konfiguration

Über das Menü **Datei → Konfiguration Importieren**, den Link im linken Fenster, den Import-Button in der Toolbar (2. Icon von links) oder die Tastenkombination **Strg + I** öffnet sich der entsprechende Dialog. Hier werden nur passende Konfigurationsdateien (*.resi) angezeigt. Wählen Sie die passende Konfigurationsdatei und Klicken Sie auf **Öffnen**.

Ist die Konfigurationsdatei passwortgeschützt, muss das Passwort eingegeben und mit **OK** bestätigt werden. Existiert die Konfiguration schon, erscheint ein Hinweis und die Konfiguration kann umbenannt oder abgebrochen werden.

Im linken Fenster erscheint die importierte Konfiguration unter **Fernwartungen/Serviceboxen**. Sind mehrere Konfigurationen verfügbar, müssen Sie die weiteren Konfigurationsdateien entsprechend importieren, die passende Konfiguration kann später im linken Fenster ausgewählt werden.

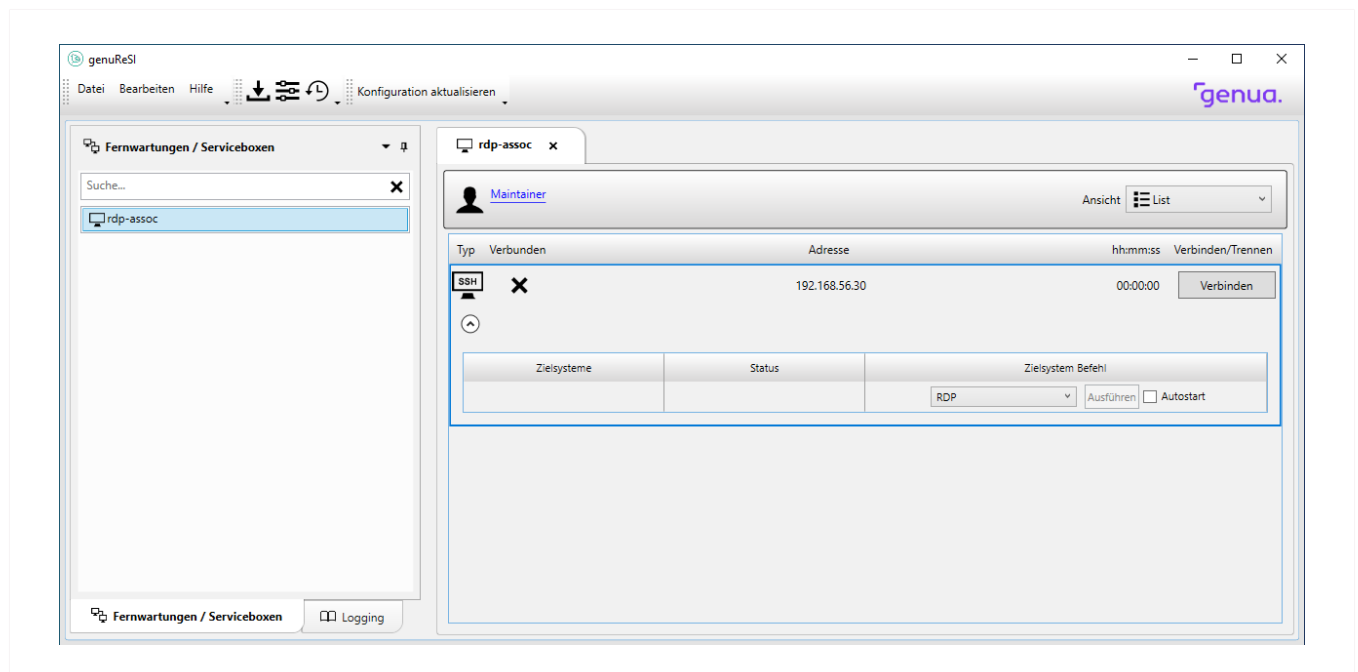


Abbildung 2.2: Fernwartungen / Serviceboxen

Kapitel 3

genuReSI für den Fernwarter

3.1	Aufgaben des Fernwarters	10
3.2	Aufbau/Abbau der Fernwartungsverbindung	10
3.3	Aufzeichnen der Verbindung bei RDP	11
3.4	Datenaustausch zwischen Fernwarter und Zielsystem	12
3.5	Konfigurationsupdates	13
3.6	Logging/History	14
3.7	Lokale Einstellungen	16
3.8	Befehle	18
3.9	Erweiterungen/Plugins	19
3.10	genuReSI Update	20
3.11	genuReSI USB/Portable Mode	20

3.1 Aufgaben des Fernwarters

Als **Fernwarter** sind Sie für den Auf- und Abbau der Verbindung zum Rendezvous-Server zuständig. Die Verbindung von der Servicebox zu Rendezvous-Server wird vom Operator aufgebaut. Erst nach dem Aufbau **beider Verbindungen** kann auf das zu wartende Zielsystem zugegriffen werden. Die Konfigurationsdaten werden über die Konfigurationsdatei importiert und können lokal nicht geändert werden.

3.2 Aufbau/Abbau der Fernwartungsverbindung

Im linken Bildschirmfenster stehen die importierten Rendezvous-Verbindungen zur Auswahl, im rechten Fenster werden Details zu jeder Verbindung angezeigt. Nach Auswahl der Rendezvous-Verbindung klicken Sie auf den Button **Verbinden**, um sich auf der Rendezvousbox einzuwählen. Ist unter **Einstellungen** der Menüpunkt **Aktiviere History** aktiviert, kann außerdem eine Beschreibung der Verbindung (für das Logging) angegeben werden.

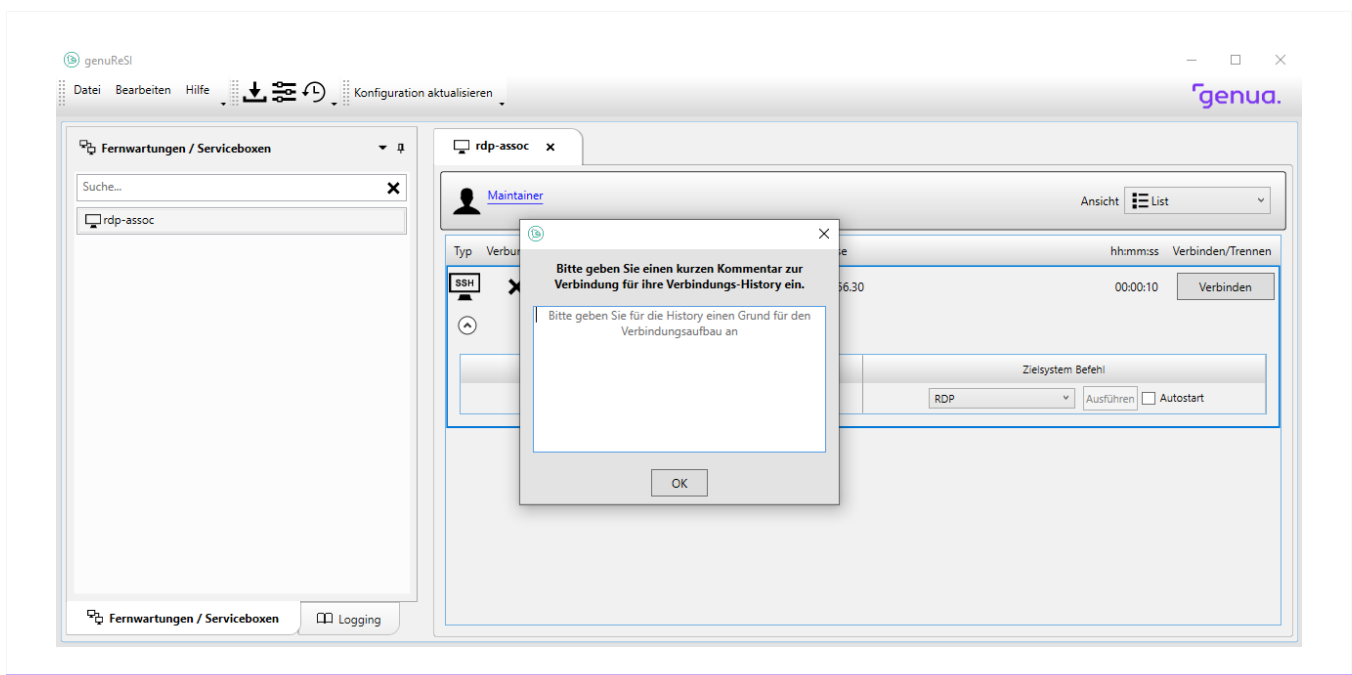


Abbildung 3.1: Verbindungsaufbau Fernwarter

Hinweis: Wenn für die Verbindung eine Autorisierung per LDAP/Active Directory konfiguriert ist, müssen Sie eventuell einen speziellen LDAP-Benutzernamen verwenden, um auf die Rendezvousbox zuzugreifen. Tragen Sie den LDAP-Benutzernamen in diesem Fall unter **Einstellungen** → **SSH** im Feld **LDAP Benutzername** ein.

Hinweis: Wenn der Administrator für die Verbindung ein High-Availability-Setup aus mehreren Rendezvousboxen konfiguriert hat, wird unter **Adresse** zusätzlich das Drop-down-Menü **Automatisch** angezeigt. Bei Bedarf können Sie über dieses Menü manuell eine bestimmte Rendezvousbox aus dem Setup auswählen, um sich darüber zum Zielsystem zu verbinden. Standardmäßig wird die Rendezvousbox zufällig ausgewählt.

Ist die Verbindung aufgebaut, wird dies im oberen Teil (1) unter „Verbunden“ mit dem Haken angezeigt, mit dem Button „Trennen“ kann die Verbindung zum Rendezvous-Server wieder abgebaut werden.

Im unteren Teil (2) wird bei Status angezeigt, ob die Verbindung vom Rendezvous-Server zur genubox vor der zu wartenden Maschine vom Operator erfolgreich aufgebaut wurde. Als Name wird hier der in der genucenter GUI mit „Name für Fernwarter“ angegebene Name angezeigt. Sollten Sie „Name für Fernwarter“ nicht angegeben haben, zeigt genuReSI den Namen der Verbindung an. Drücken Sie **Strg** + **D** um weitere technische Details (Port, Lokale und Remote IP) der Verbindung zu sehen.

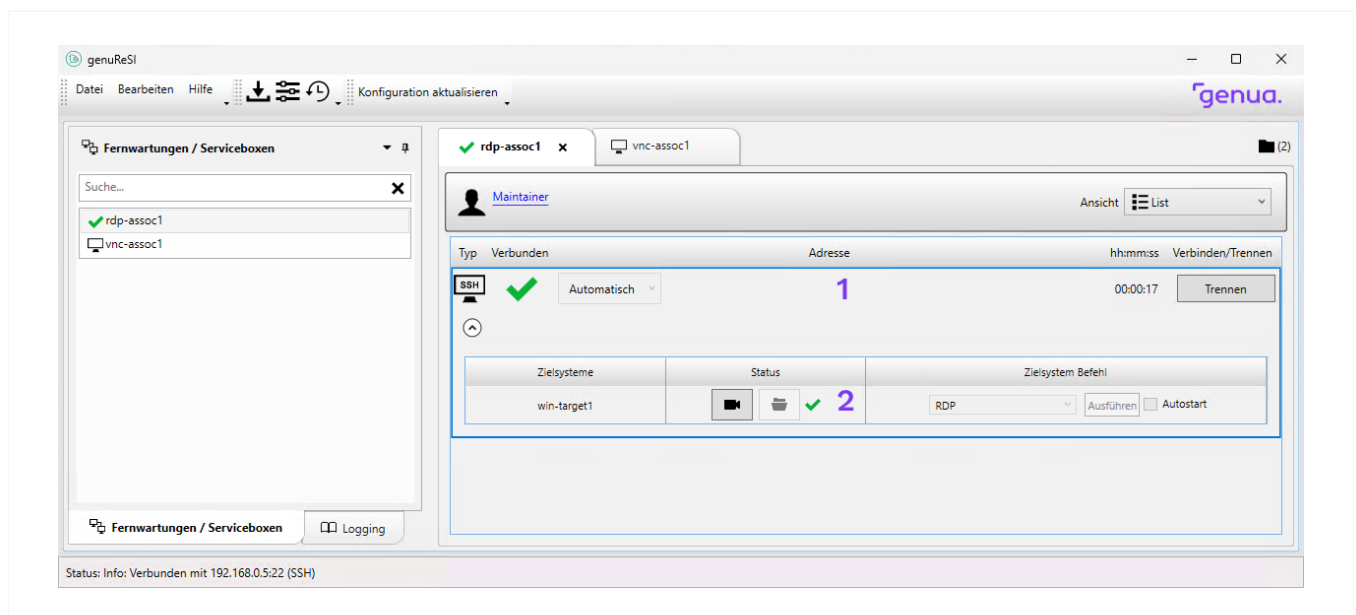


Abbildung 3.2: Fensteraufbau

3.3 Aufzeichnen der Verbindung bei RDP

Es besteht die Möglichkeit, RDP, SSH und VNC Sessions aufzuzeichnen und laufende Sessions mitzulesen (Recording-Funktion). Dies muss vom **Operator** gestartet werden, der Fernwarter kann dies nicht beeinflussen. Ob das Recording konfiguriert ist, kann anhand des Kamera-Icons bei der Verbindung festgestellt werden.

In manchen Fällen sind personenbezogene Daten des Fernwarters von der Fernwartungsaufzeichnung betroffen. In diesem Fall wird eine Datenschutz-Erklärung eingeblendet, die Sie dar-

über informiert, in welcher Form diese personenbezogenen Daten erfasst und verarbeitet werden. Stimmen Sie der Erklärung nicht zu, wird die Fernwartungsbeziehung abgebrochen.

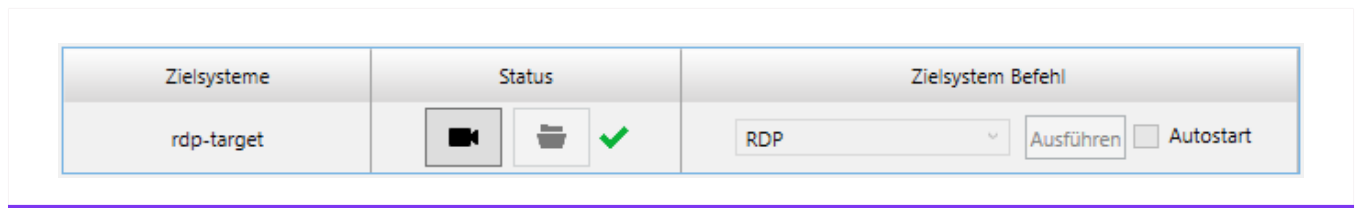


Abbildung 3.3: Mitschneiden von Verbindungen

In einer laufenden Verbindung wird anhand der Statusinformationen ersichtlich, ob diese Session mitgeschnitten oder mitgelesen wird (in unserem Beispiel wird die Session mitgeschnitten und aktiv mitgelesen, der Fernwarter hat Zugriff auf das Zielsystem).



Abbildung 3.4: Recordinganzeige in der Session

3.4 Datenaustausch zwischen Fernwarter und Zielsystem

Es besteht die Möglichkeit, Daten zum Zielsystem hochzuladen bzw. vom Zielsystem zum Fernwarter herunterzuladen (auch „Share-Option“ genannt). Diese Funktion muss vom **Operator** gestartet werden, der Fernwarter kann dies nicht beeinflussen. Ob der Datenaustausch konfiguriert ist, kann anhand des Exchange-Icons bei der Verbindung unter Status festgestellt werden (siehe Abbildung 3.3).

Klicken auf das Icon öffnet den File Exchange Explorer. Der Datenaustausch wird mittels eines RDP-Laufwerks ausgeführt, die Daten bleiben somit auch nach Beenden der Session erhalten. Dateiübertragungen werden geloggt und können vom Operator auch im Nachhinein nachvollzogen werden. Falls für die Rendezvousbox ein per ICAP angebundener Virens Scanner eingerichtet wurde, werden die übertragenen Dateien automatisch auf Schadsoftware geprüft und stehen erst nach Freigabe durch den Virens Scanner zur Verfügung. Bei Bedarf werden im Transferstatus weitere Informationen zu diesem Vorgang angezeigt.

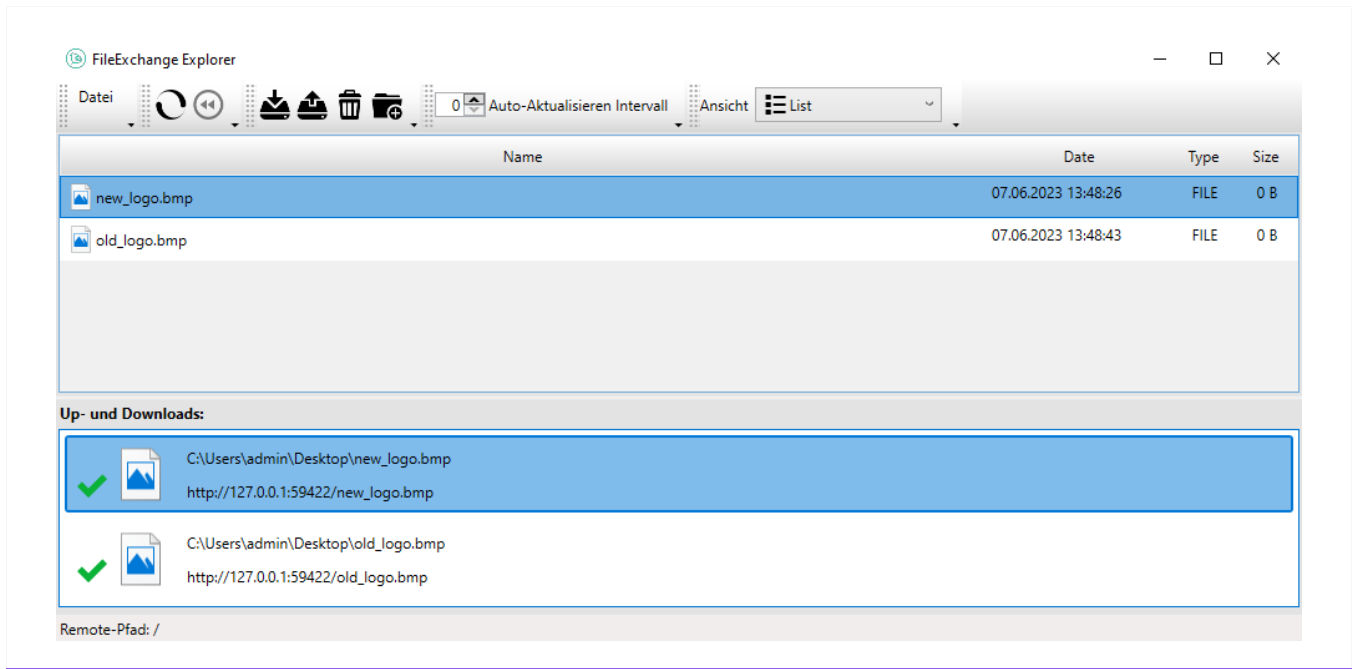


Abbildung 3.5: File Exchange Explorer

Im oberen Fenster des Explorers sind alle verfügbaren Objekte zu sehen, im unteren Fenster die aktuellen Übertragungen. Das Menü enthält Icons für den Up- bzw. Download, das Erstellen neuer Ordner sowie das Löschen von Objekten. Die automatische Anzeigenaktualisierung ist standardmäßig deaktiviert, dies lässt sich jedoch umstellen, außerdem können sowohl Objekte als auch Icons im Listenformat dargestellt werden.

3.5 Konfigurationsupdates

Für den initialen Aufbau der Verbindung von genuReSI App zur Rendezvousbox benötigt der Fernwarter eine gültige Konfigurationsdatei. Diese Datei wird in der Regel vom Administrator mithilfe der Central Management Station genucenter erstellt.

Besteht später eine aktive SSH-Verbindung zur Rendezvousbox, werden die nachfolgenden Konfigurationsänderungen bei jedem genuReSI-Statuscheck automatisch übertragen und angezeigt. Solche Änderungen betreffen z. B. neue Verbindungen. Solange sich der Fernwarter mit seiner aktuellen Konfiguration zur Rendezvousbox verbinden kann, braucht er deshalb keine weiteren Konfigurationsdateien aktiv einzulesen.

Alternativ klicken Sie in der Titelleiste auf [Konfiguration aktualisieren](#). genuReSI App prüft dann aktiv alle für SSH eingerichteten Rendezvousboxen auf Konfigurationsänderungen und aktualisiert bei Bedarf die vorhandenen Konfigurationen.

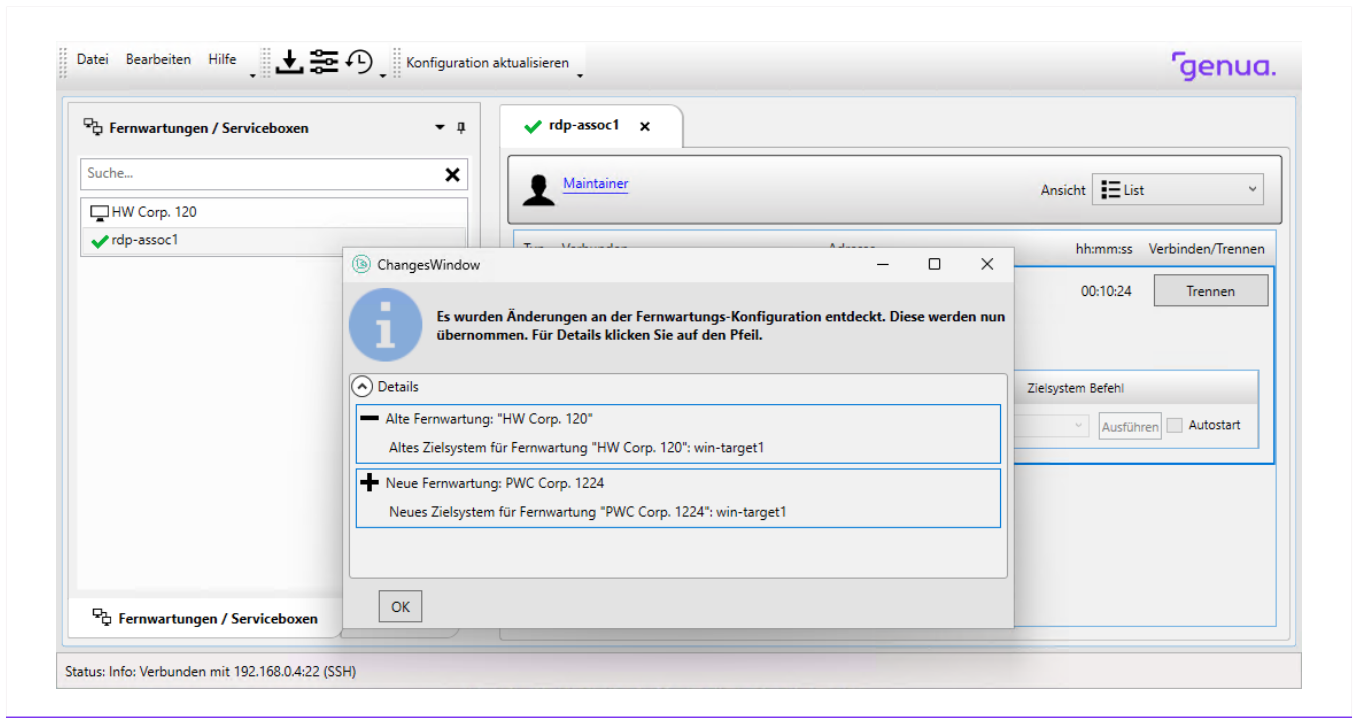


Abbildung 3.6: Aktualisierte Konfiguration (erweiterte Ansicht)

3.6 Logging/History

Wird im Hauptfenster der Reiter **Logging** angeklickt, werden die Logdaten von genuReSI und den Verbindungen angezeigt. Es stehen die LogLevel **Info**, **Debug** und **Error** zur Verfügung. Das StandardLogLevel ist Info.

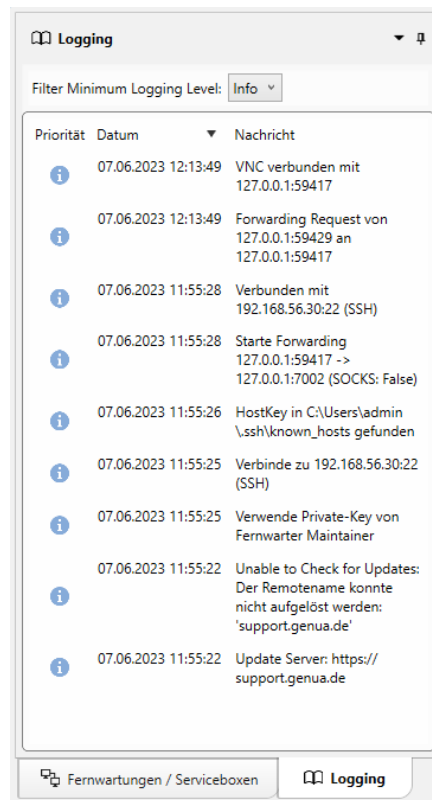
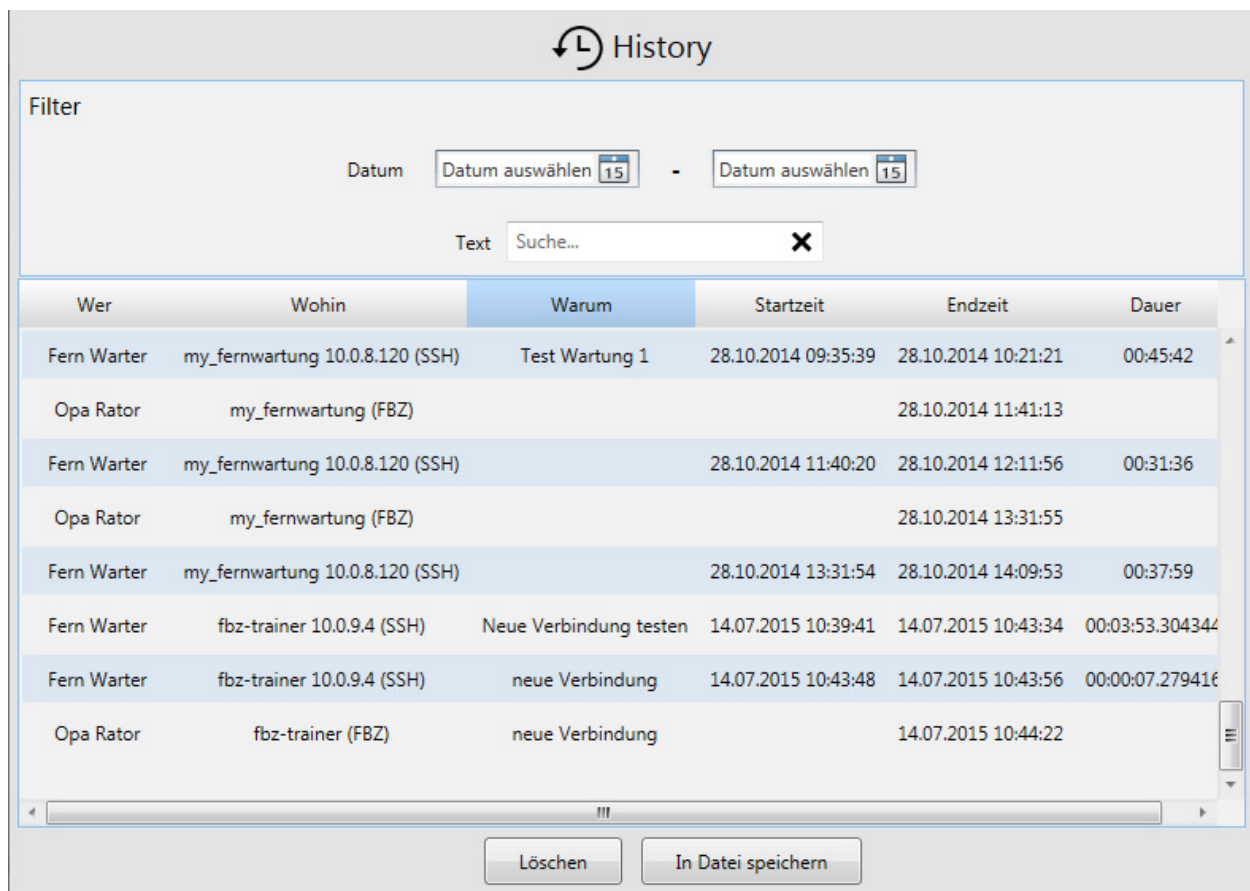


Abbildung 3.7: Logging Wartungsverbindungen

Um die Verbindungsdaten der letzten Verbindungen (History) anzuzeigen, wählen Sie in der Toolbar das letzte Icon **History**. Im History-Fenster kann sowohl der Zeitraum der Verbindungen definiert als auch ein Suchtext eingegeben werden. Die Daten können lokal in einer Datei gespeichert werden, um sie beispielsweise bei einer Supportanfrage zur besseren Fehleranalyse mitzuschicken.



Wer	Wohin	Warum	Startzeit	Endzeit	Dauer
Fern Warter	my_fernwartung 10.0.8.120 (SSH)	Test Wartung 1	28.10.2014 09:35:39	28.10.2014 10:21:21	00:45:42
Opa Rator	my_fernwartung (FBZ)			28.10.2014 11:41:13	
Fern Warter	my_fernwartung 10.0.8.120 (SSH)		28.10.2014 11:40:20	28.10.2014 12:11:56	00:31:36
Opa Rator	my_fernwartung (FBZ)			28.10.2014 13:31:55	
Fern Warter	my_fernwartung 10.0.8.120 (SSH)		28.10.2014 13:31:54	28.10.2014 14:09:53	00:37:59
Fern Warter	fbz-trainer 10.0.9.4 (SSH)	Neue Verbindung testen	14.07.2015 10:39:41	14.07.2015 10:43:34	00:03:53.304344
Fern Warter	fbz-trainer 10.0.9.4 (SSH)	neue Verbindung	14.07.2015 10:43:48	14.07.2015 10:43:56	00:00:07.279416
Opa Rator	fbz-trainer (FBZ)	neue Verbindung		14.07.2015 10:44:22	

Abbildung 3.8: History Wartungsverbindungen

3.7 Lokale Einstellungen

Über das Icon **Einstellungen** in der Toolbar können eine Vielzahl an Einstellungen vorgenommen werden:

- **Anwendungs-Einstellungen:**
Hier können allgemeine Einstellungen wie Thema, History-Aktivierung und Log Level vorgenommen werden.
- **SSH:**
Hier können SSH relevante Einstellungen zu SSH-Weiterleitung und LDAP vorgenommen werden, sowie die Netzwerkkarte für Mapping-Adressen ausgewählt werden.
- **Erweiterungen:**
Installation/Deinstallation von Plugins, siehe Kapitel 3.9.
- **Smartcard:**
Dateipfad zur Smartcard Middleware.
- **Befehle:**
Definition von Befehlen, siehe Kapitel 3.8.

- **Rollen:**
Übersicht verfügbarer Rollen und Einstellungen.

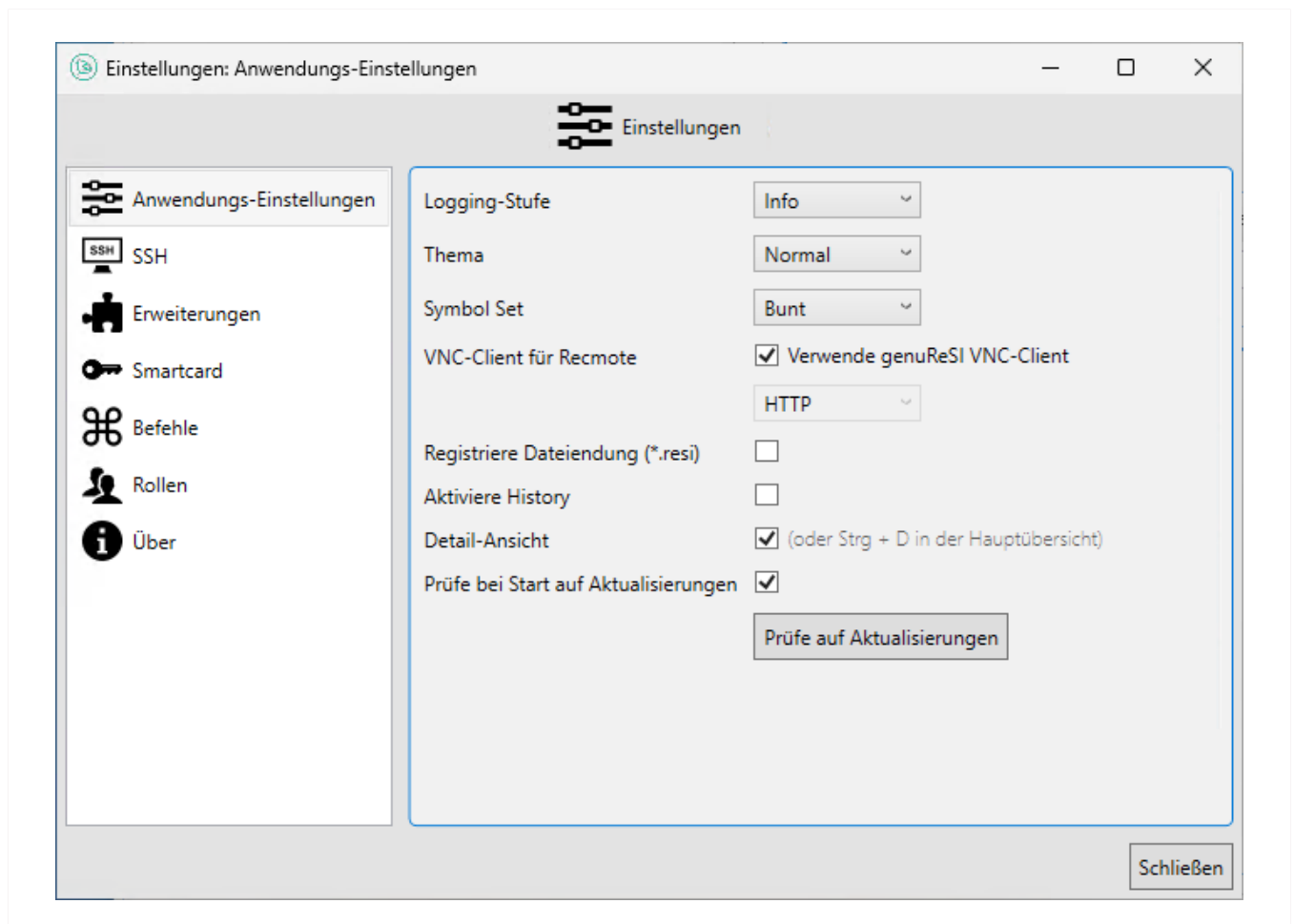


Abbildung 3.9: Einstellungen Fernwarter

3.8 Befehle

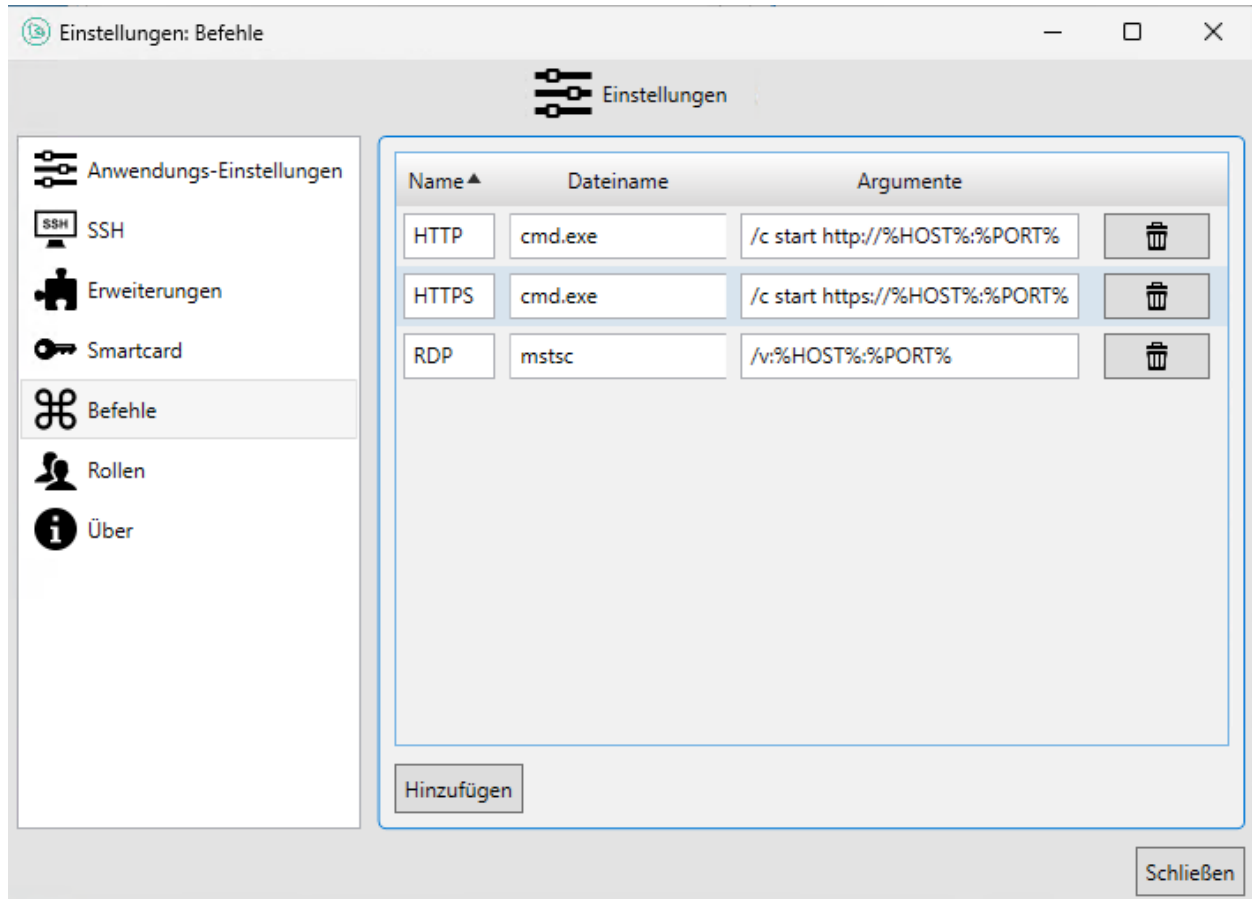


Abbildung 3.10: Einstellungen Befehle

Der Zugang zu der zu wartenden Maschine kann über verschiedene Protokolle erfolgen, z. B. über RDP (Remote Desktop Protocol) von Microsoft oder SSH (Secure Shell). Die dazu notwendigen Befehle werden im Menü **Befehle** der Toolbar definiert, vordefiniert ist immer RDP, in unserem Beispiel wurde der Zugang über SSH via PuTTY hinzugefügt. Die hier definierten Befehle stehen im Hauptfenster bei einer bestehenden Verbindung zur Verfügung und können dort ausgewählt und gestartet werden. Durch Anwählen von **Autostart** werden diese Befehle automatisch beim Starten der Rendezvous-Verbindung mitgestartet.

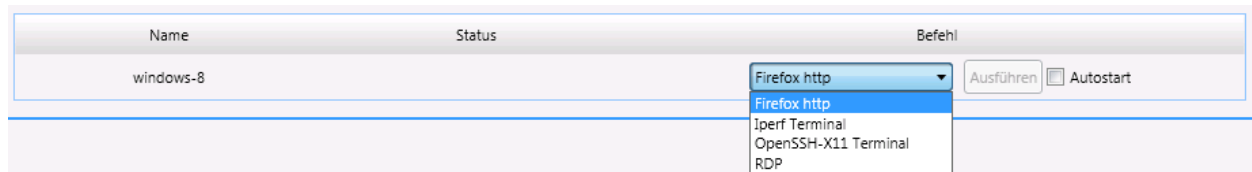


Abbildung 3.11: Autostart Funktion

3.9 Erweiterungen/Plugins

Um es Benutzern zu ermöglichen, einfach ihr genuReSI-Setup zu erweitern, gibt es sogenannte **Erweiterungen/Plugins**. Es sind derzeit zwei Arten von Plugins verfügbar, Command- und Theme-Plugins.

Plugins sind ZIP-Dateien, die eine Plugin-Info-Datei und die von dem Plugin benötigten Dateien beinhalten. Derzeit gibt es z. B. Firefox, OpenSSH, PuTTY oder UltraVNC als Erweiterungen. Verwenden Sie stets die neueste zur Verfügung gestellte Plugin-Version. Bitte achten Sie darauf, die zu ihrem System passende Programmarchitektur (32- oder 64-Bit) auszuwählen.

Installiert bzw. deinstalliert werden Erweiterungen über das Menü [Einstellungen](#) → [Erweiterungen](#).

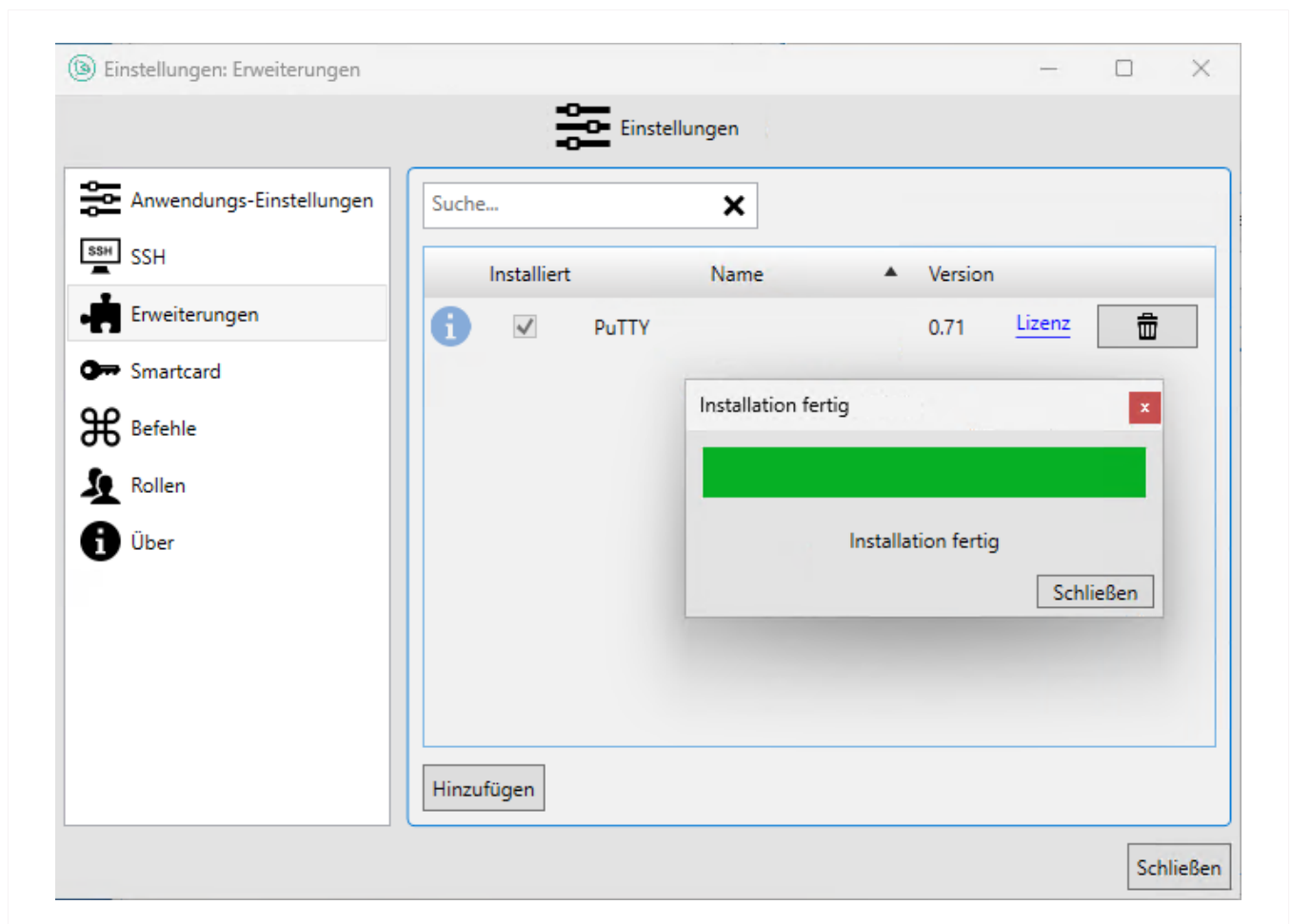


Abbildung 3.12: Erweiterungen

Hinweis: Um einen als Plugin zur Verfügung gestellten VNC-Client zu verwenden, müssen Sie zusätzlich folgende Anpassungen vornehmen:

1. Wechseln Sie in das Menü [Bearbeiten](#) → [Einstellungen](#) → [Anwendungs-Einstellungen](#).
2. Deaktivieren Sie die Checkbox **Verwende genuReSI VNC-Client**.
3. Wählen Sie im darunterstehenden Auswahlménü den gewünschten Client aus.

Hinweis: VNC-Verbindungen werden gemäß Remote Framebuffer Protocol (RFC 6143) unterstützt.

3.10 genuReSI Update

genuReSI verfügt über eine Autoupdate-Funktion: Wenn Sie die App starten, wird automatisch geprüft, ob eine neue Version der Datei [ReSI.exe](#) verfügbar ist. Falls eine neue Version vorliegt, erscheint das Dialogfeld **Update verfügbar**. Klicken Sie auf [Ja](#), wenn Sie das Update installieren möchten. Anschließend muss die Anwendung genuReSI neu gestartet werden.

Beim Update wird die aktuelle Version der Datei [ReSI.exe](#) installiert und die vorherige Datei als [ReSI_old.exe](#) im TEP-Verzeichnis abgelegt.

Die Autoupdate-Funktion ist standardmäßig aktiviert. Um die Funktion auszuschalten, gehen Sie im Menü auf [Einstellungen](#) → [Anwendungs-Einstellungen](#) und deaktivieren Sie die Checkbox **Prüfe bei Start auf Aktualisierungen**. Updates müssen dann manuell angestoßen werden.

Hinweis: Bitte denken Sie daran, auch verwendete Erweiterungen zu aktualisieren.

3.11 genuReSI USB/Portable Mode

Um die Anwendung genuReSI auf jedem Rechner verfügbar zu haben, kann sie auf einem USB-Stick installiert und von diesem gestartet werden. Der USB-Mode kann auch im Read-Only-Modus gestartet werden. Dann sind alle Schreib-Operationen deaktiviert. So kann beispielsweise die Konfiguration nicht gespeichert werden. Das erlaubt es, genuReSI einmal zu starten und dann den USB-Stick zu entfernen.

Kapitel 4

genuReSI für den Operator

4.1	Aufgaben des Operators	22
4.2	Aufbau/Abbau der Fernwartungsverbindung	22
4.3	Zugriffskontrolle zur Laufzeit	25
4.4	Aufzeichnen der Verbindung bei RDP und SSH	25
4.5	Share-Option	26
4.6	Konfigurationsupdates	27
4.7	Logging/History	28
4.8	Lokale Einstellungen	30
4.9	genuReSI Update	31

4.1 Aufgaben des Operators

Als **Operator** sind Sie für den Auf- und Abbau der Verbindung vom Rendezvous-Server zur genubox vor dem zu wartenden Zielsystem zuständig. Ohne diese Verbindung ist es dem Fernwarter **nicht** möglich, die Wartungsverbindung aufzubauen. Außerdem bestimmt der Operator, ob eine Verbindung aufgezeichnet oder live mitgelesen werden soll, wenn dies entsprechend konfiguriert ist (üblicherweise über die Managementstation genucenter). Der Operator kann, sofern Rendezvous so konfiguriert ist, den Zugriff des Fernwarters auf Keyboard und Maus des Zielsystems zur Laufzeit erteilen und wieder entziehen.

Die Konfigurationsdaten werden über die Konfigurationsdatei importiert und können lokal nicht geändert werden.

Der Zugriff auf die Operator-GUI kann sowohl direkt über das genucenter oder lokal über die genubox über einen speziellen Operator-Login erfolgen als auch über genuReSI. Die Bedienung der Operator-GUIs wird in den genucenter/genubox Handbüchern erläutert. Installation und Konfiguration erfolgt wie in Kapitel 2 beschrieben.

4.2 Aufbau/Abbau der Fernwartungsverbindung

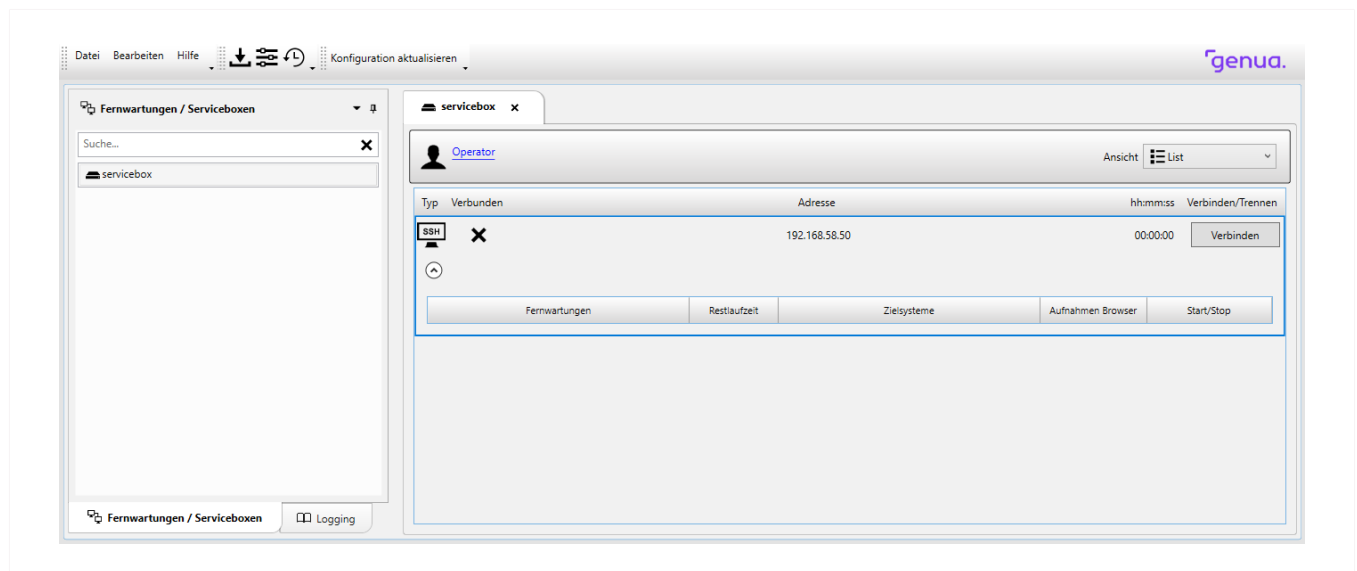


Abbildung 4.1: Aufbau der Verbindung / Operator

Im linken Bildschirmfenster stehen die importierten Operator-Verbindungen zur Auswahl, im rechten Fenster werden weitere Details dazu angezeigt. Nach Auswahl der Operator-Verbindung klicken Sie auf den Button **Verbinden**. Damit wird zuerst die SSH-Verbindung zur genubox aufgebaut, es wird noch keine Wartungsverbindung gestartet!

Hinweis: Wenn für die Verbindung eine Autorisierung per LDAP/Active Directory konfiguriert ist, müssen Sie eventuell einen speziellen LDAP-Benutzernamen verwenden, um auf die Servicebox zuzugreifen. Tragen Sie den LDAP-Benutzernamen in diesem Fall unter **Einstellungen** → **SSH** im Feld **LDAP Benutzername** ein.

Im unteren Teil des Hauptfensters werden die verfügbaren Verbindungen angezeigt, die mit dem Button **Start** ebenfalls gestartet werden können.

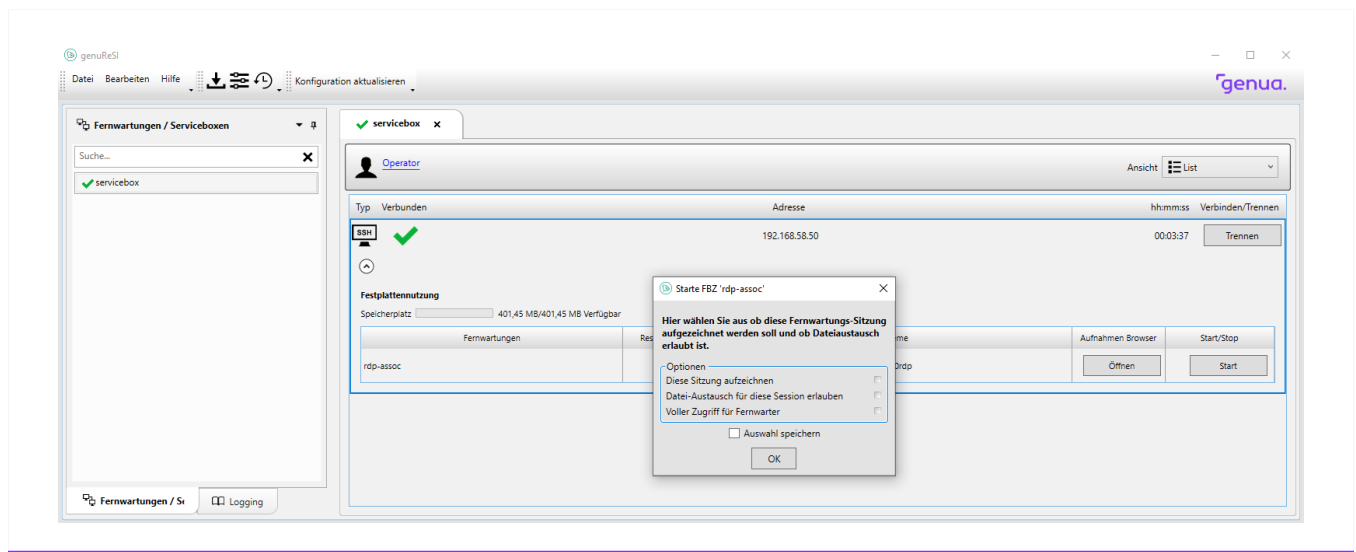


Abbildung 4.2: Aufbau der Verbindung

Ein Kamera-Icon neben der Verbindung (unter Forwardings) signalisiert, dass das Recording konfiguriert ist, das Explorer-Icon die konfigurierte Datenaustausch-Option und das Zugriffssteuerungs-Icon die Zugriffssteuerung zur Laufzeit.

Ist die History aktiviert (siehe Kapitel Einstellungen), kann ein Grund für den Aufbau angegeben werden. Außerdem werden in diesem Fenster durch Setzen der Aktivierungshaken das Recording und die Share-Option aktiviert, sowie die Rechte des Fernwarters zu Beginn der Fernwartung festgelegt.

Sind Verbindungen aufgebaut, wird im oberen Teil (1) unter „Verbunden“ angezeigt, dass die SSH-Session zur genubox vor dem zu wartenden Zielsystem etabliert ist. Mit dem Button **Trennen** kann die Verbindung zur genubox wieder abgebaut werden, Fernwartungsverbindungen bleiben davon unberührt.

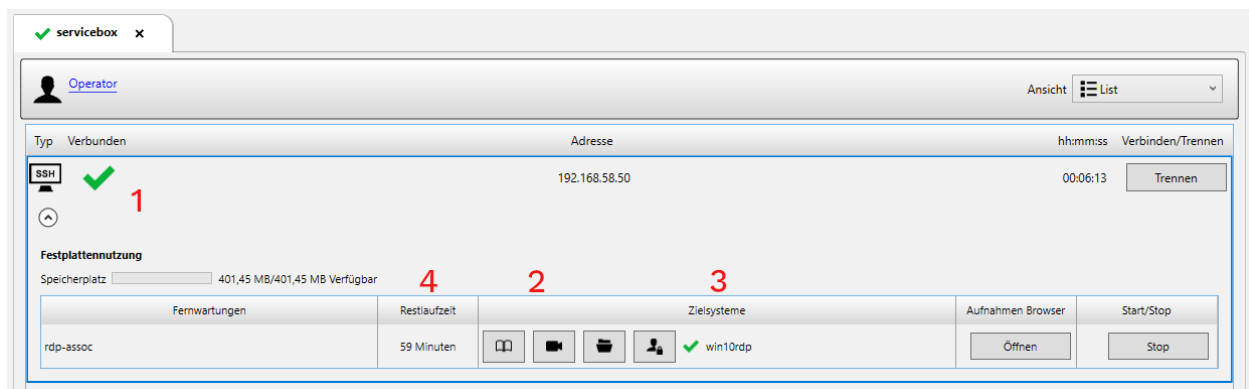


Abbildung 4.3: Übersicht Verbindungen

Im unteren Teil wird bei Forwardings (2) angezeigt, ob und welche Verbindungen von der genubox zur wartenden Maschine vom Operator freigeschaltet wurden. Unter Fernwartung (3) wird der Status der Wartungsverbinding des Fernwarters visualisiert. Durch einen Klick auf Restlaufzeit (4) kann das Zeitfenster der Fernwartung verändert werden. Mit Klicken auf **Stop** kann der Operator die Verbindung von genubox zur wartenden Maschine beenden.

4.3 Zugriffskontrolle zur Laufzeit

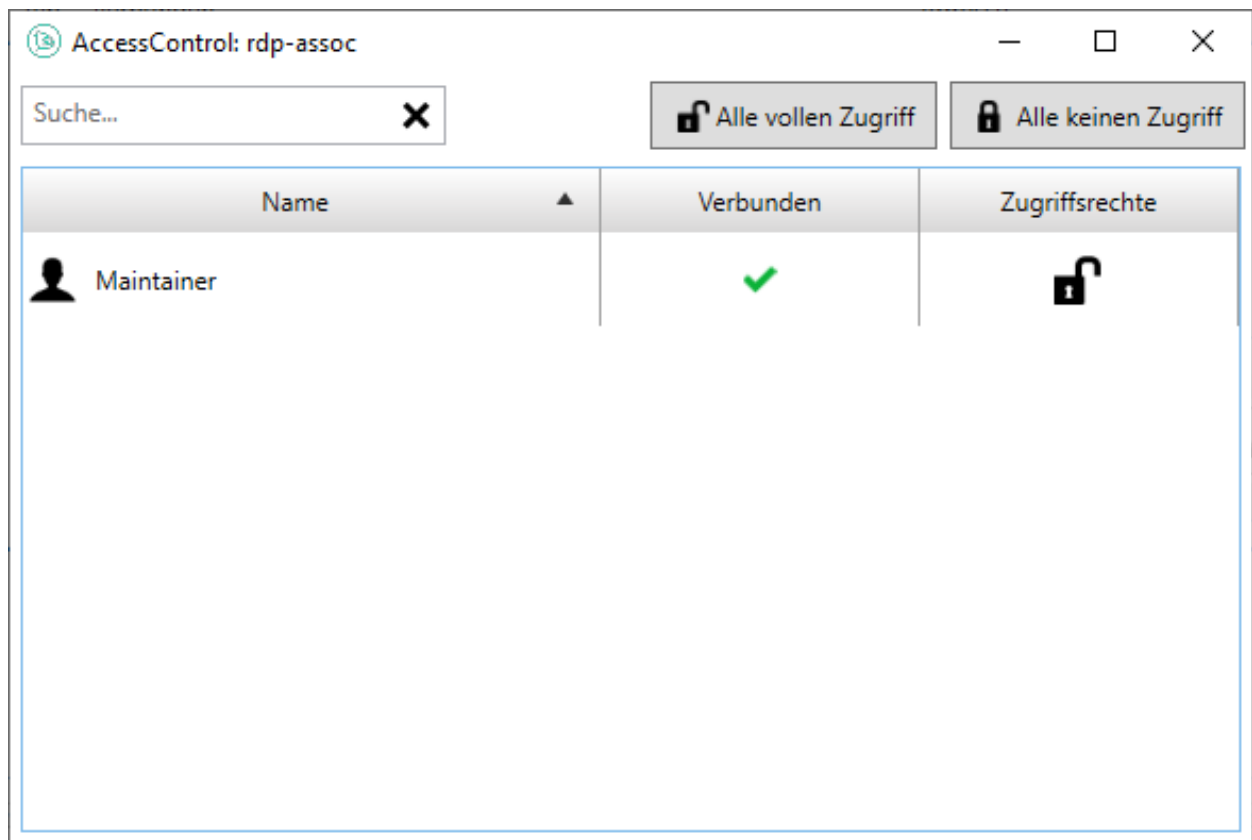


Abbildung 4.4: Übersicht Verbindungen

Der Operator kann dem Fernwarter, sofern diese Option in der Konfiguration vorgesehen ist, zur Laufzeit Zugriff zu Keyboard und Maus des Zielsystems geben oder entziehen. Um diese Rechte zu ändern, klickt der Operator auf das Zugriffskontrolle-Icon im Bereich **Forwardings**. Das in Abbildung 4.4 gezeigte Fenster erscheint. Mit einem Klick auf das in unserem Fall geöffnete Schloss kann der Operator dem Fernwarter den Zugriff auf Maus und Keyboard entziehen. Das Schloss erscheint bei entzogenem Zugriff geschlossen. Ein Klick auf das geschlossene Schloss öffnet es wieder und erlaubt dem Fernwarter erneut Zugriff auf Keyboard und Maus des Zielsystems.

4.4 Aufzeichnen der Verbindung bei RDP und SSH

Es besteht die Möglichkeit, RDP und SSH Sessions aufzuzeichnen und laufende Sessions mitzulesen (Recording-Funktion). Dies muss vom Operator gestartet werden, der Fernwarter kann dies nicht beeinflussen. Ob das Recording konfiguriert ist, kann anhand des Kamera-Icons bei der Verbindung festgestellt werden (siehe Abbildung 4.3).

Wurde eine Verbindung mit Recording gestartet, kann der Operator sich mit Klick auf das Kamera-Icon live auf die laufende Session aufschalten. In dem neu geöffneten Session-Window bedeutet das blinkende Kamera-Icon, dass die Session gerade aufgezeichnet wird, außerdem wird angezeigt, ob der Fernwarter gerade verbunden ist.

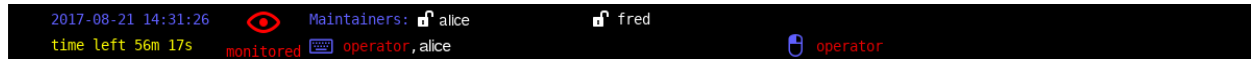


Abbildung 4.5: Aktives Recording in laufender Session

Wird auf den Button **Öffnen** unter Aufnahmen Browser geklickt, öffnet sich das Fenster mit den bereits aufgezeichneten Sessions. Diese können im Raw Format heruntergeladen, in VP8-Format konvertiert oder gelöscht werden. Konvertierte Aufnahmen können ebenfalls auf die lokale Workstation heruntergeladen und dort angesehen werden.

Achten Sie darauf, dass Aufnahmen, die nicht mehr benötigt werden, rechtzeitig gelöscht werden, damit der verfügbare Speicherplatz nicht komplett belegt wird.

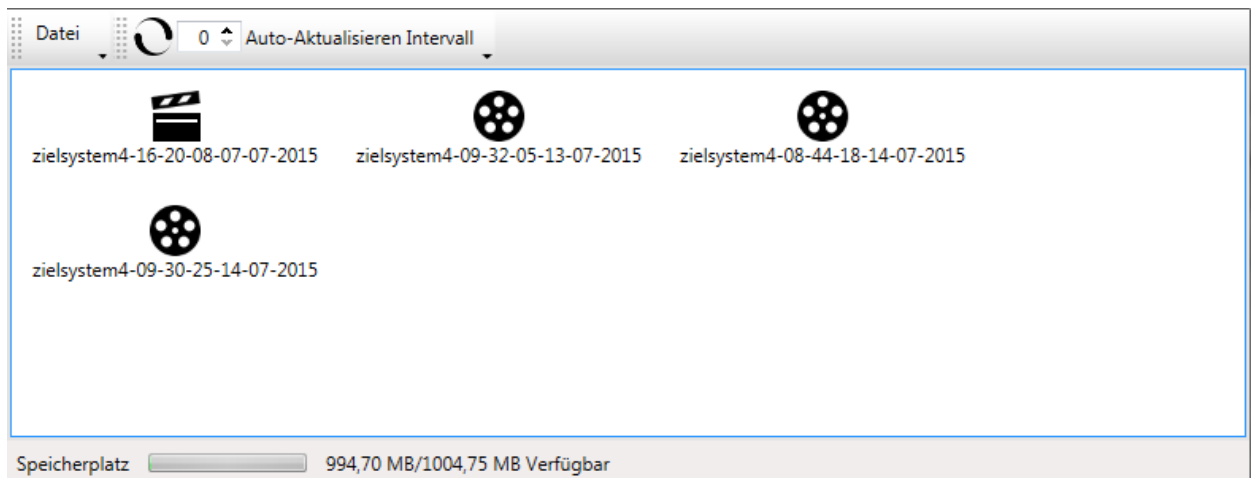
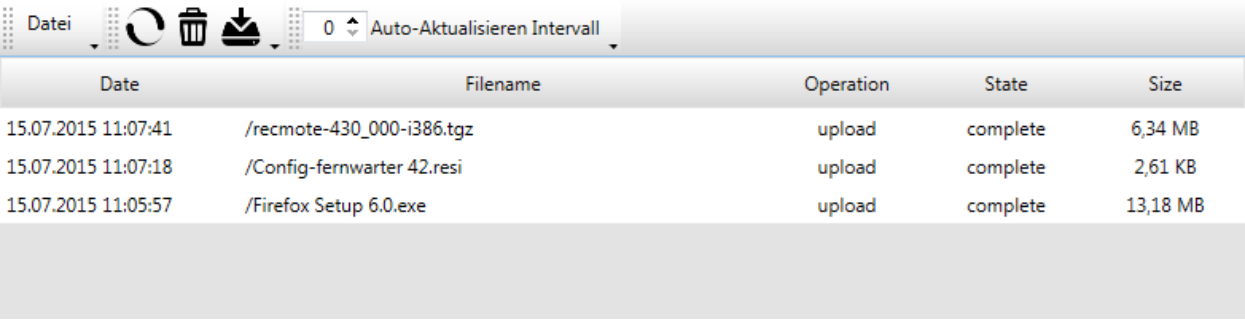


Abbildung 4.6: Download/Konvertierung von Aufnahmen

4.5 Share-Option

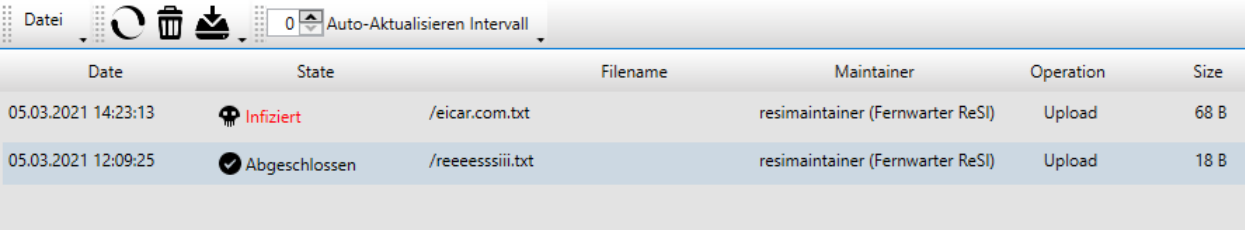
Ist die Share-Option (Datenaustausch) aktiviert, kann der Operator durch Klick auf das Explorer-Icon den Explorer für den Operator öffnen. Hier werden alle Dateien angezeigt, die kopiert wurden (Up- und Download), außerdem kann der Operator über das Download-Icon in der Menüzeile die Dateien herunterladen.



Date	Filename	Operation	State	Size
15.07.2015 11:07:41	/recmote-430_000-i386.tgz	upload	complete	6,34 MB
15.07.2015 11:07:18	/Config-fernwarter 42.resi	upload	complete	2,61 KB
15.07.2015 11:05:57	/Firefox Setup 6.0.exe	upload	complete	13,18 MB

Abbildung 4.7: Dateiaustausch

Falls für die Rendezvousbox ein per ICAP angebundener Virens Scanner eingerichtet wurde, werden die übertragenen Dateien automatisch auf Schadsoftware geprüft und stehen erst nach Freigabe durch den Virens Scanner zur Verfügung. Bei Bedarf werden im Transferstatus weitere Informationen zu diesem Vorgang angezeigt.



Date	State	Filename	Maintainer	Operation	Size
05.03.2021 14:23:13	Infiziert	/eicar.com.txt	resimaintainer (Fernwarter ReSI)	Upload	68 B
05.03.2021 12:09:25	Abgeschlossen	/reeesssiii.txt	resimaintainer (Fernwarter ReSI)	Upload	18 B

Abbildung 4.8: Malware gefunden („Infiziert“)

4.6 Konfigurationsupdates

Für den initialen Aufbau der Verbindung von genuReSI App zur Servicebox benötigt der Operator eine gültige Konfigurationsdatei. Diese Datei wird in der Regel vom Administrator mithilfe der Central Management Station genucenter erstellt.

Besteht später eine aktive SSH-Verbindung zur Servicebox, werden die nachfolgenden Konfigurationsänderungen bei jedem genuReSI-Statuscheck automatisch übertragen und angezeigt. Solche Änderungen erfolgen üblicherweise ebenfalls über das genucenter und betreffen z. B. neue Verbindungen. Solange sich der Operator mit seiner aktuellen Konfiguration zur Servicebox verbinden kann, braucht er deshalb keine weiteren Konfigurationsdateien aktiv einzulesen.

Hinweis: Im Unterschied zum Fernwarter braucht der Operator Konfigurationsänderungen nicht zu bestätigen. Alle Änderungen werden sofort in die Operatoransicht übernommen.

Alternativ klicken Sie in der Titelleiste auf [Konfiguration aktualisieren](#). genuReSI App prüft dann aktiv **alle** für SSH eingerichteten Rendezvousboxen auf Konfigurationsänderungen und aktualisiert bei Bedarf die vorhandenen Konfigurationen.

4.7 Logging/History

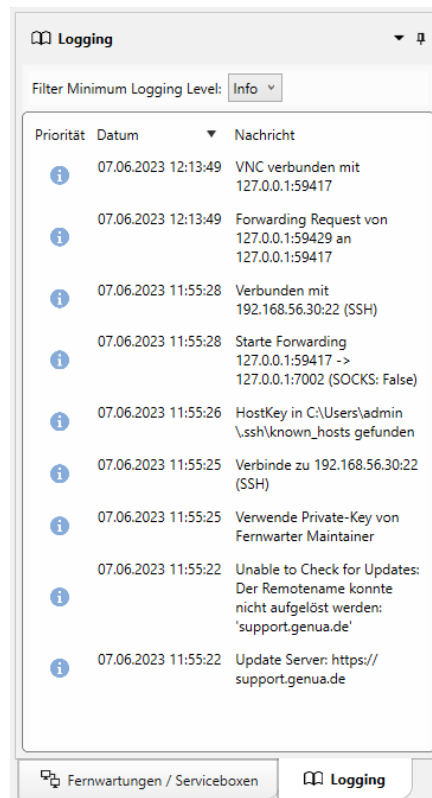
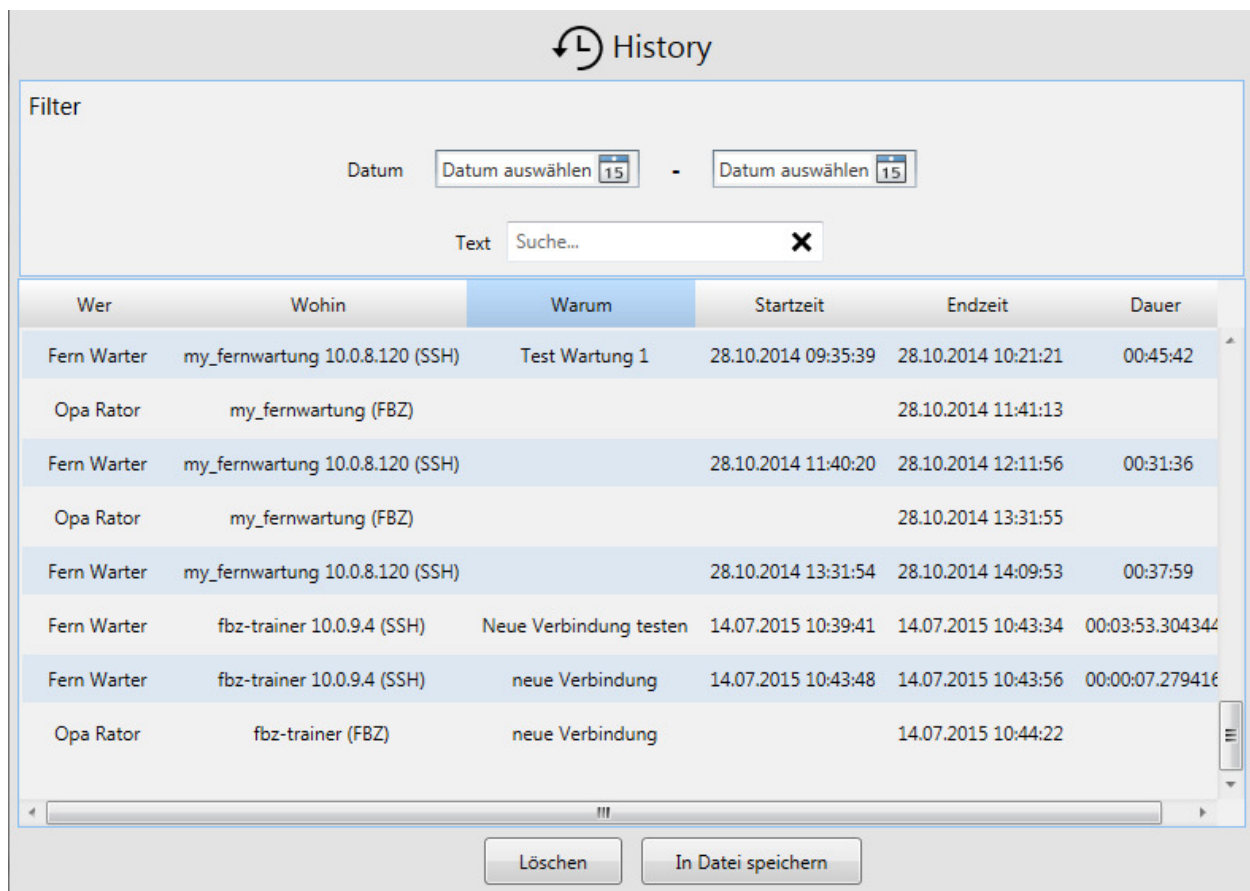


Abbildung 4.9: Logging

Wird im Hauptfenster der Reiter **Logging** angeklickt, werden die Logdaten von genuReSI und den Verbindungen angezeigt. Es stehen die LogLevel **Info**, **Debug** und **Error** zur Verfügung.

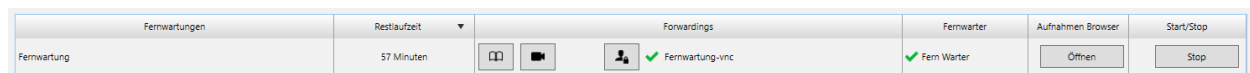
Um die Verbindungsdaten der letzten Verbindungen (History) anzuzeigen, wählen Sie in der Toolbar das letzte Icon **History**. Im History-Fenster kann sowohl der Zeitraum der Verbindungen definiert als auch ein Suchtext eingegeben werden. Die Daten können lokal in einer Datei gespeichert werden, um sie beispielsweise bei einer Supportanfrage zur besseren Fehleranalyse mitzuschicken.



Wer	Wohin	Warum	Startzeit	Endzeit	Dauer
Fern Warter	my_fernwartung 10.0.8.120 (SSH)	Test Wartung 1	28.10.2014 09:35:39	28.10.2014 10:21:21	00:45:42
Opa Rator	my_fernwartung (FBZ)			28.10.2014 11:41:13	
Fern Warter	my_fernwartung 10.0.8.120 (SSH)		28.10.2014 11:40:20	28.10.2014 12:11:56	00:31:36
Opa Rator	my_fernwartung (FBZ)			28.10.2014 13:31:55	
Fern Warter	my_fernwartung 10.0.8.120 (SSH)		28.10.2014 13:31:54	28.10.2014 14:09:53	00:37:59
Fern Warter	fbz-trainer 10.0.9.4 (SSH)	Neue Verbindung testen	14.07.2015 10:39:41	14.07.2015 10:43:34	00:03:53.304344
Fern Warter	fbz-trainer 10.0.9.4 (SSH)	neue Verbindung	14.07.2015 10:43:48	14.07.2015 10:43:56	00:00:07.279416
Opa Rator	fbz-trainer (FBZ)	neue Verbindung		14.07.2015 10:44:22	

Abbildung 4.10: History

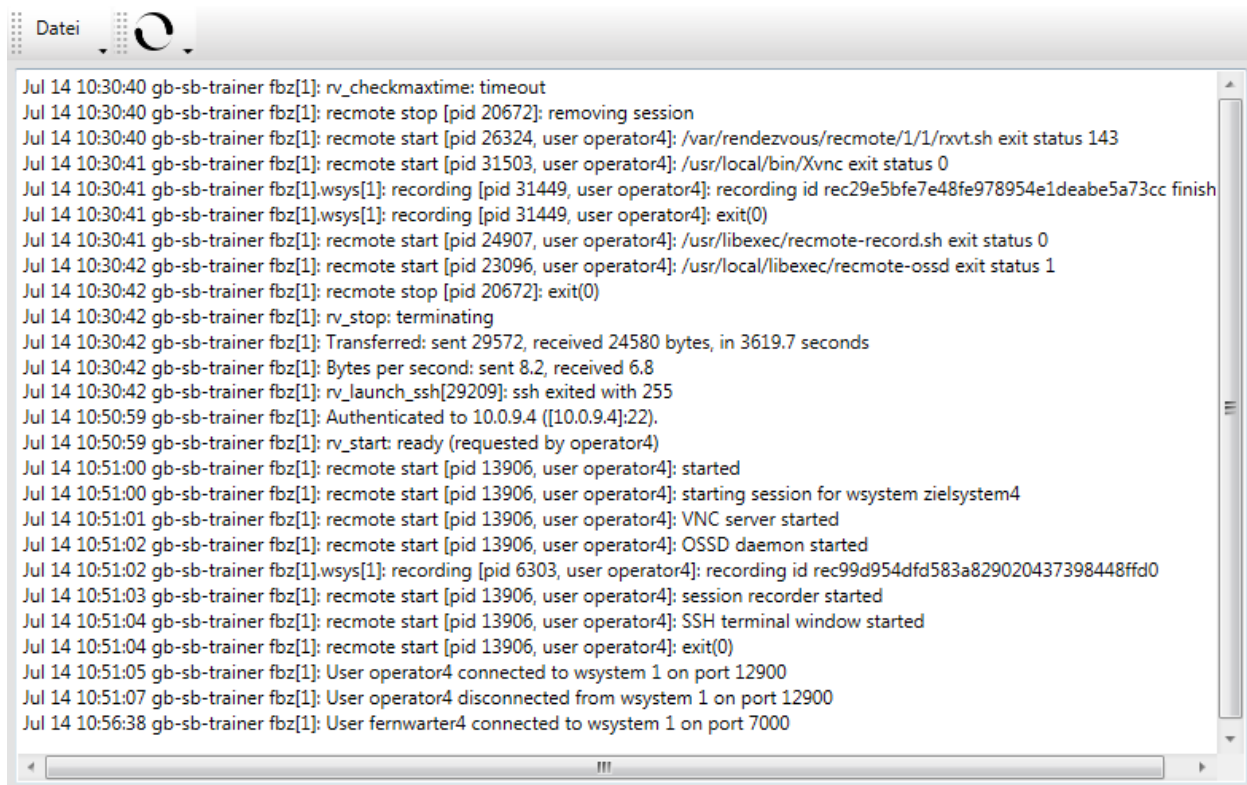
Bei einer laufenden Verbindung kann der Operator über den Button **Logging** (Buchsymbol) die aktuelle Logdatei öffnen:



Fernwartungen	Restlaufzeit	Forwardings	Fernwarter	Aufnahmen Browser	Start/Stop
Fernwartung	57 Minuten	   ✓ Fernwartung-vnc	✓ Fern Warter	 Öffnen	Stop

Abbildung 4.11: Logging laufende Session

Diese wird dann in einem separaten Fenster angezeigt:



```

Jul 14 10:30:40 gb-sb-trainer fbz[1]: rv_checkmaxtime: timeout
Jul 14 10:30:40 gb-sb-trainer fbz[1]: recmote stop [pid 20672]: removing session
Jul 14 10:30:40 gb-sb-trainer fbz[1]: recmote start [pid 26324, user operator4]: /var/rendezvous/recmote/1/1/rxvt.sh exit status 143
Jul 14 10:30:41 gb-sb-trainer fbz[1]: recmote start [pid 31503, user operator4]: /usr/local/bin/Xvnc exit status 0
Jul 14 10:30:41 gb-sb-trainer fbz[1].wsys[1]: recording [pid 31449, user operator4]: recording id rec29e5bfe7e48fe978954e1deabe5a73cc finish
Jul 14 10:30:41 gb-sb-trainer fbz[1].wsys[1]: recording [pid 31449, user operator4]: exit(0)
Jul 14 10:30:41 gb-sb-trainer fbz[1]: recmote start [pid 24907, user operator4]: /usr/libexec/recmote-record.sh exit status 0
Jul 14 10:30:42 gb-sb-trainer fbz[1]: recmote start [pid 23096, user operator4]: /usr/local/libexec/recmote-ossd exit status 1
Jul 14 10:30:42 gb-sb-trainer fbz[1]: recmote stop [pid 20672]: exit(0)
Jul 14 10:30:42 gb-sb-trainer fbz[1]: rv_stop: terminating
Jul 14 10:30:42 gb-sb-trainer fbz[1]: Transferred: sent 29572, received 24580 bytes, in 3619.7 seconds
Jul 14 10:30:42 gb-sb-trainer fbz[1]: Bytes per second: sent 8.2, received 6.8
Jul 14 10:30:42 gb-sb-trainer fbz[1]: rv_launch_ssh[29209]: ssh exited with 255
Jul 14 10:50:59 gb-sb-trainer fbz[1]: Authenticated to 10.0.9.4 ([10.0.9.4]:22).
Jul 14 10:50:59 gb-sb-trainer fbz[1]: rv_start: ready (requested by operator4)
Jul 14 10:51:00 gb-sb-trainer fbz[1]: recmote start [pid 13906, user operator4]: started
Jul 14 10:51:00 gb-sb-trainer fbz[1]: recmote start [pid 13906, user operator4]: starting session for wsystem zielsystem4
Jul 14 10:51:01 gb-sb-trainer fbz[1]: recmote start [pid 13906, user operator4]: VNC server started
Jul 14 10:51:02 gb-sb-trainer fbz[1]: recmote start [pid 13906, user operator4]: OSSD daemon started
Jul 14 10:51:02 gb-sb-trainer fbz[1].wsys[1]: recording [pid 6303, user operator4]: recording id rec99d954dfd583a829020437398448ffd0
Jul 14 10:51:03 gb-sb-trainer fbz[1]: recmote start [pid 13906, user operator4]: session recorder started
Jul 14 10:51:04 gb-sb-trainer fbz[1]: recmote start [pid 13906, user operator4]: SSH terminal window started
Jul 14 10:51:04 gb-sb-trainer fbz[1]: recmote start [pid 13906, user operator4]: exit(0)
Jul 14 10:51:05 gb-sb-trainer fbz[1]: User operator4 connected to wsystem 1 on port 12900
Jul 14 10:51:07 gb-sb-trainer fbz[1]: User operator4 disconnected from wsystem 1 on port 12900
Jul 14 10:56:38 gb-sb-trainer fbz[1]: User fernwarter4 connected to wsystem 1 on port 7000

```

Abbildung 4.12: Logdaten Output

4.8 Lokale Einstellungen

Über das Icon **Einstellungen** in der Toolbar können eine Vielzahl an Einstellungen vorgenommen werden:

- **Anwendungs-Einstellungen:**
Hier können allgemeine Einstellungen wie Thema, History-Aktivierung und Log Level vorgenommen werden.
- **SSH:**
Hier können SSH relevante Einstellungen zu SSH-Forwarding und LDAP vorgenommen werden, sowie die Netzwerkkarte für Mapping-Adressen ausgewählt werden.
- **Erweiterungen:**
Installation/Deinstallation von Plugins, siehe Kapitel 3.9.
- **Smartcard:**
Dateipfad zur Smartcard Middleware.
- **Befehle:**
Definition von Befehlen, siehe Kapitel 3.8.
- **Rollen:**
Übersicht verfügbarer Rollen und Einstellungen.

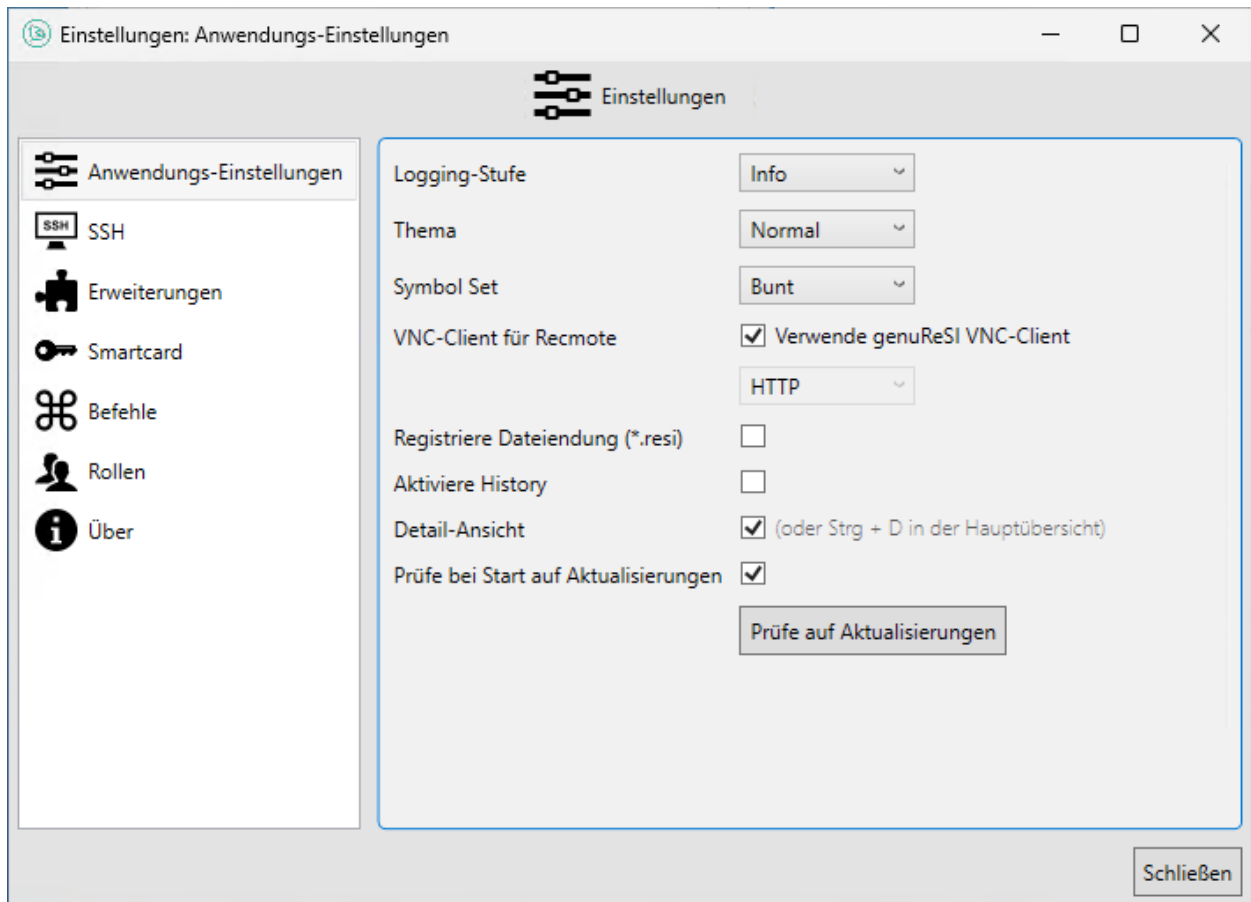


Abbildung 4.13: Einstellungen

4.9 genuReSI Update

genuReSI verfügt über eine Autoupdate-Funktion: Wenn Sie die App starten, wird automatisch geprüft, ob eine neue Version der Datei `ReSI.exe` verfügbar ist. Falls eine neue Version vorliegt, erscheint das Dialogfeld **Update verfügbar**. Klicken Sie auf **Ja**, wenn Sie das Update installieren möchten. Anschließend muss die Anwendung genuReSI neu gestartet werden.

Beim Update wird die aktuelle Version der Datei `ReSI.exe` installiert und die vorherige Datei als `ReSI_old.exe` im TEMP-Verzeichnis abgelegt.

Die Autoupdate-Funktion ist standardmäßig aktiviert. Um die Funktion auszuschalten, gehen Sie im Menü auf **Einstellungen** → **Anwendungs-Einstellungen** und deaktivieren Sie die Checkbox **Prüfe bei Start auf Aktualisierungen**. Updates müssen dann manuell angestoßen werden.

Kapitel 5

Erweiterte Konfiguration

5.1	Konfigurationsdateien	34
5.2	Rollenverwaltung	35
5.3	Verwendung einer Smartcard	37
5.4	Verwendung mit Firewall/NAT-Gateway	40
5.5	HTTP Proxy für SSH	41
5.6	GUI-Gestaltung	42
5.7	Neue Befehle	43

5.1 Konfigurationsdateien

genuReSI Konfigurations- und Logdateien befinden sich in den Verzeichnissen des jeweiligen Benutzers unter [AppData\Local\genua_GmbH](#) und [AppData\Roaming\ReSI](#). Diese Verzeichnisse sollten bei Backups mitgesichert werden.

5.2 Rollenverwaltung

ID:	0
Role:	Operator
Name:	Oper Ator
Loginname:	zieloperator
LDAP:	☐
Smartcard:	☐
Verbindungen Stoppen wenn Smartcard entfernt wird	☐
PrivateKey:	<pre>-----BEGIN RSA PRIVATE KEY----- MIIeowIBAAKCAQEAsSfst0ql/ci+RsOwPdhamv4J3vjHRp5zGIA2a4Q9a15AMxUC iN0epLnhjRIQNtbUXSQB3bFLUvkiKnN4c98ncN96qe6MZPovTshsVQq1Dp8xx0ux FsJlIxBa1TprnTw06hCzjYqOMnKoLVRCtmijkMkJ81E+xGmme38UF3JHzicrxe hdtAdqV2/Q+m83ICRPbsUHSQH7M47px0naK2N4cvi9kNuNq6N8qN0A7jeZR18+ok oCHjrv6Uruq9UDHKUGQSGtQY/q+LaNWt8RkVhHm7zL62c0Xt2EA8/J2THArO7fGF RuT6FIJQyrosm59XD6VCfPtKR9ue/Np0Odje2QIDAQABAoIBAQCXLF93HC6cill8 5r6dd+ORgZkAycCbdZj5aluWEimrVqloLdSU4ERHA0wC8QfVVBGyTYi+Go4RhwFt wk2Wa2YnvrzZB/SMMqZuDz/KrjFIAdojnGbl6g9Ozl+WbMZgle/wXhRsDfKntSMR UsiOfsTFP/uF6iYME0MlfdUmp3W5DuBGD0upCB5eAtvX5NSyQU/yKN1Z2qOCUfKI QCLxCFKPQxs/B9F7LOqip2g2IQOaV8Spx/rOI6iiW39mMLvQ8jc5WoJg/ilqGUWI f5SR1ZrD7MRASEHfRkVxfyRI2UgJdCs7OxFuLojG2xJaRQ4YbTYflelCxNICQtP +U/tPo1RAoGBAONTediRNYRq+Up8TSPjIJTj85WsHMcansOFmu8PRuq4iyT/blN dfOK6h98UrfaxC4I62uWfyOHAdEgctJqd4570SHDW3yzImKoqrqW3tyMEZHHM+W 1JrxX58PyxZaiejZV+ZIBcRyBDxgrIGUdCTVVH5TYuJU4UGyHFeZtFIVAoGBAMeA awgHs0E8/Xn+NsgivQtoo9KFPCthHhc2LqFAvd2RF0Y4I6FA/WpoS6WtLfS9Bhb0 fBI2oBQO5tftZwYfBaUhXtmq7U8r1dsrv2hqXsQsQeTHG8KaPG8Dv/uvF2C9L1B lLoRo9D6w3py5m99ewz5hhvC76vQxeGQpfOwww61AoGAAMIKofGLvRKeAGDjMiAc ZXjYxhH0kZBXsVcX9xMnFNyqvsriWwHr3Zy0LZZRC6pYah9to1gVhxrQMxADBB+n ly/HFnKEz/7UunllMCLUGKvGw8XVEHwFSLaFORaiS16xmWZF3J0eqluDndppIIYo 3YX698QKAINfdR/X2jc7Q60CgYAb66kPEqTPul1xCVb4epOUaSykRelJ2OmxLFAQ uVLZM3kiZsEx3DqbLcWihlgsLFgx1j2YArYcmllOI2KR5MFE57xWrOPTFY8kmR1U ec+SXZ+pA7mzAK33Ru6CexL5s141Lmw6HkXi9XVuKa5+Y/1Yr4NJV1rbnPhUvT28 gTyJEQKBgG7XeKQSAOer+xOtMVEAL3J4xHT3j5GaYUMPCAvfMoE+hj37bbYVfqYJ 5eC4UNz2Ne0RWZHUD8YxJOxt9ImkZfOLCE+S+KVQF5frY0Poi3owyWOJDthlKE 1G9RXqrmHj8stnJnL/DsrMBBdDCW9qtN+qX+k3+b679S780HSyJf -----END RSA PRIVATE KEY-----</pre>
L2TP-Passphrase:	
Abbrechen Speichern	

Abbildung 5.1: Rollenverwaltung

Normalerweise werden die Konfigurationsdateien inklusive der Rollen (Loginname und Private Key) auf dem Managementsystem erstellt und müssen lokal nicht editiert werden. Sollen Werte wie Private Key angepasst werden, kann dies über das Menü **Rollen** in der Toolbar erfolgen. Dazu die gewünschte Rolle anklicken und es öffnet sich ein Fenster im Bearbeitungsmodus. Die Änderung über den Button **Speichern** abspeichern.

5.3 Verwendung einer Smartcard

Es kann zur Authentisierung des Operators und des Fernwarters eine Smartcard verwendet werden.

5.3.1 PKCS#11 Modul

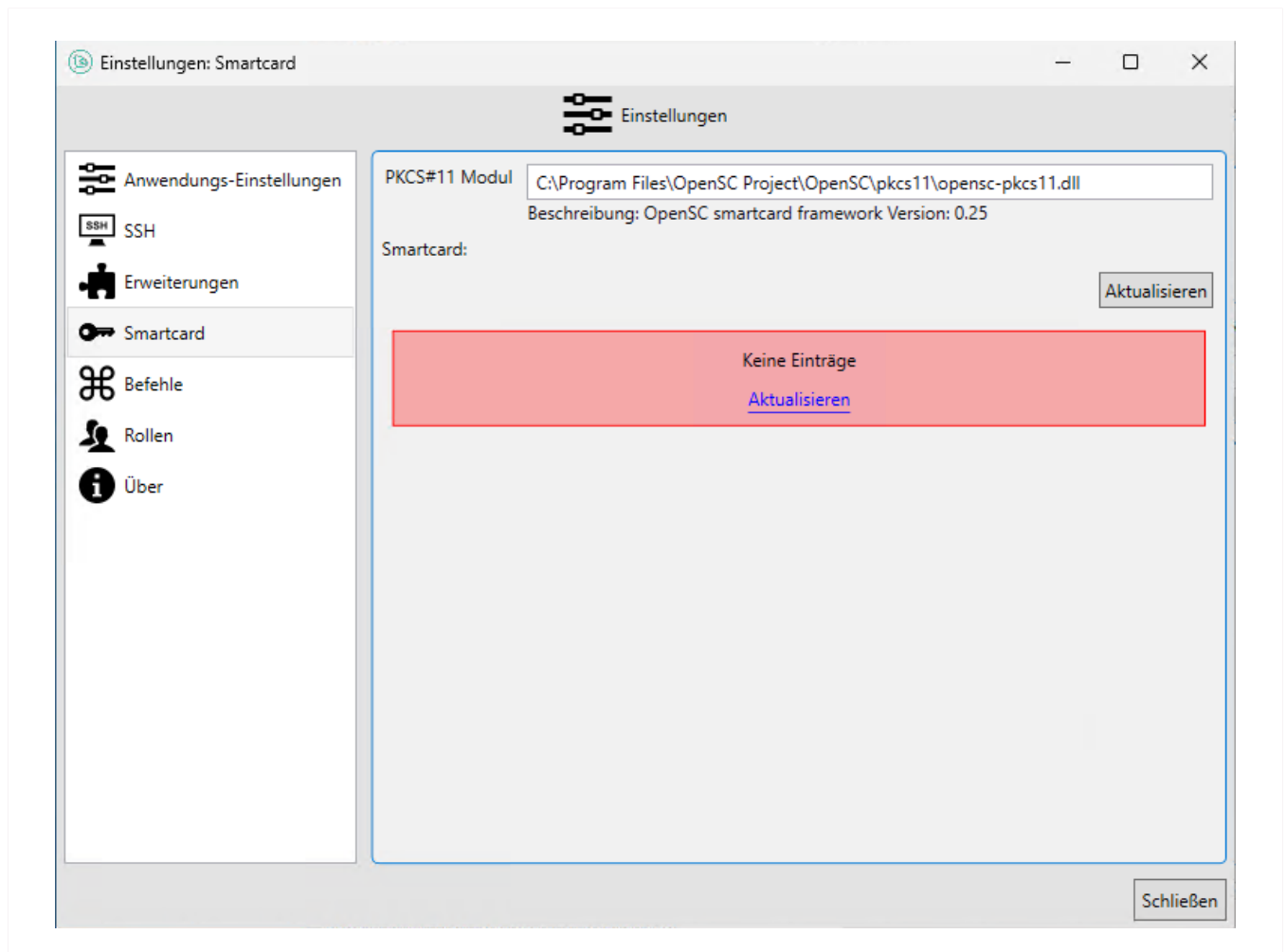


Abbildung 5.2: Auswahl des PKCS Moduls

Tragen Sie den Dateipfad zu Ihrer PKCS#11 Middleware unter [Einstellungen](#) → [Smartcard](#) der genuReSI ein. Den Dateipfad entnehmen Sie bitte dem Handbuch der von Ihnen verwendeten Smartcard-Software.

5.3.2 Smartcard-Zuweisung

Um die Smartcard-Authentisierung eines Benutzers zu ermöglichen, wählen Sie unter [Einstellungen](#) → [Rollen](#) den entsprechenden Benutzer aus. Aktivieren Sie die Checkbox **Smartcard** und übernehmen Sie die Änderungen anschließend mit einem Klick auf **Speichern**.

Sollen die bestehenden Verbindungen angehalten werden, sobald die Smartcard entfernt wird, aktivieren Sie zusätzlich die Checkbox **Verbindungen Stoppen wenn Smartcard entfernt wird**.

Hinweis:

Diese Option kann zu Problemen bei kontaktlosen Smartcards führen, da diese nur bei der ersten Initialisierung aktiv sind und anschließend entfernt werden.

5.3.3 Public Key im genucenter zuweisen

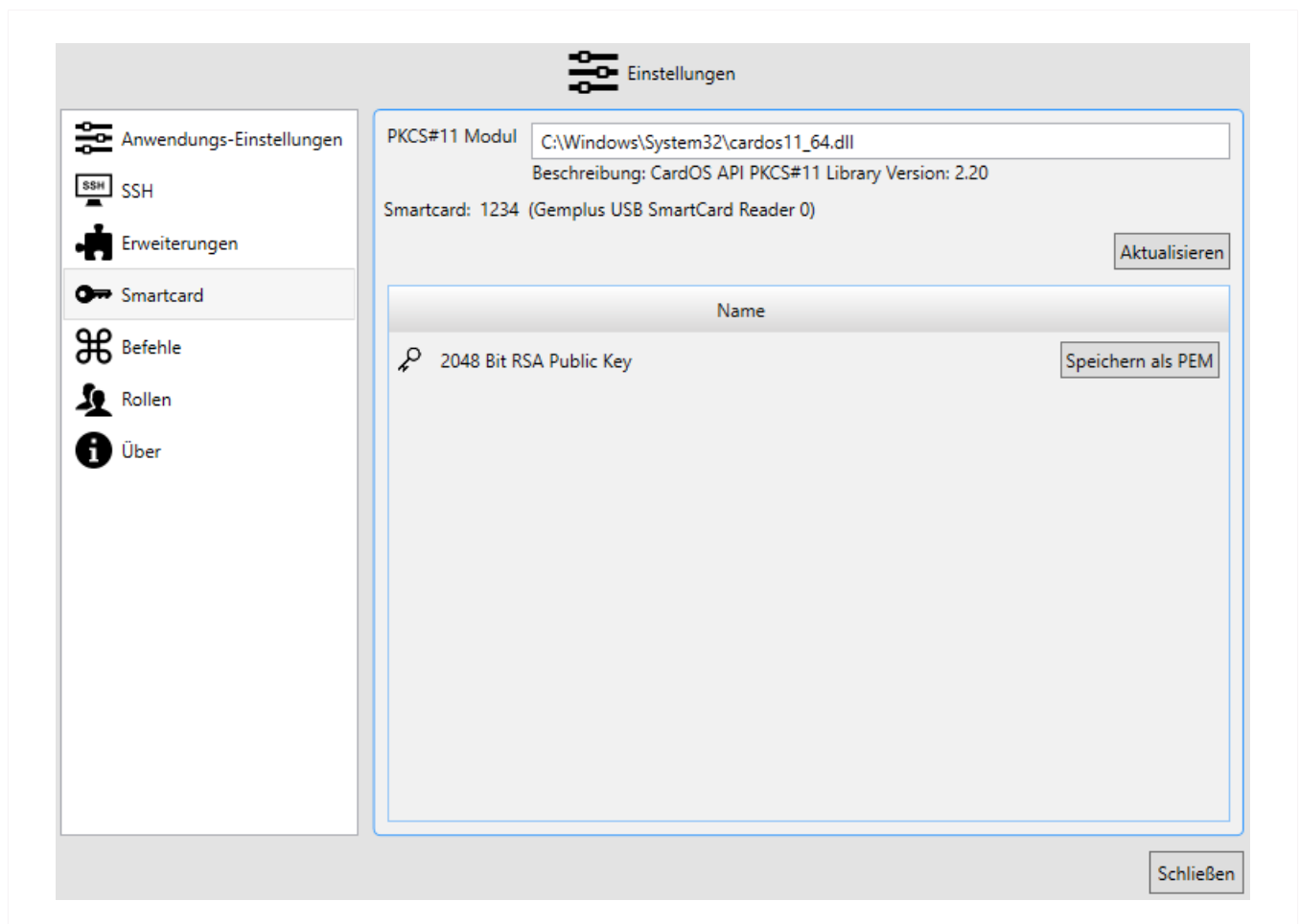


Abbildung 5.3: Smartcard Menü

Der Public Key der Smartcard muss der Rendezvousbox bekannt sein, damit Sie sich per Smartcard authentisieren können:

1. Exportieren Sie den Public Key der Smartcard des Benutzers in der genuReSI-App-GUI unter [Einstellungen](#) → [Smartcard](#) mit einem Klick auf [Speichern als PEM](#).
2. Laden Sie den Public Key im genucenter hoch:
 - (a) Navigieren Sie im genucenter je nach Funktion des Benutzers zu [Rendezvous](#) → [Operatoren](#) → [<genuReSI Benutzer](#) oder [Rendezvous](#) → [Fernwartler](#) → [<genuReSI Benutzer>](#).

- (b) Im Abschnitt **Zugriff per SSH** aktivieren Sie die Checkbox **Login mit SSH-Schlüssel aktivieren**.
- (c) Im gleichen Abschnitt laden Sie unter **Datei mit Schlüssel hochladen** den exportierten Public Key hoch.
- (d) Speichern Sie Ihre Änderungen und aktualisieren Sie die Konfiguration aller beteiligten Systeme.

5.3.4 Verbindung Aufbauen

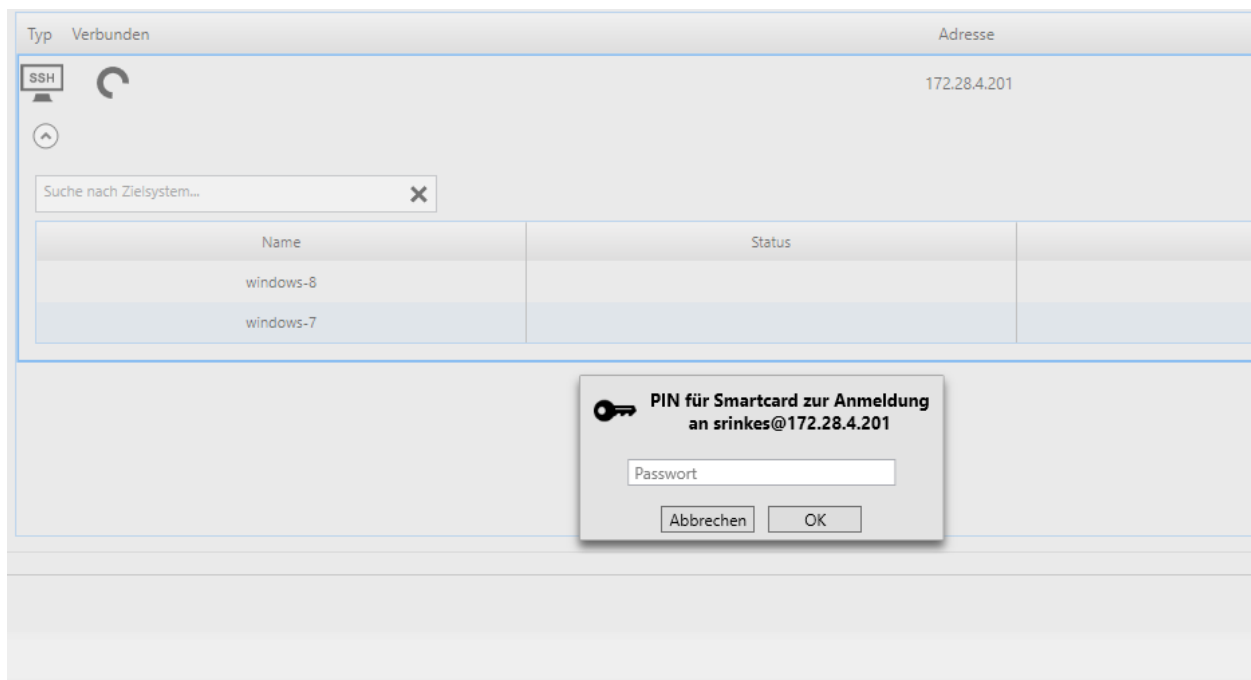


Abbildung 5.4: Smartcard PIN-Eingabe

Beim Aufbau der Verbindung werden Sie nach der PIN Ihrer Smartcard gefragt. Nach der erfolgreichen Eingabe haben Sie Zugriff auf Ihre Verbindungen.

5.4 Verwendung mit Firewall/NAT-Gateway

5.4.1 SSH Weiterleitung

Wenn sich Ihre Rendezvousbox hinter einer Firewall oder einem NAT-Gateway befindet und nicht direkt erreichbar ist, können Sie eine SSH-Weiterleitung einrichten, um die Verbindung zur Rendezvousbox zu ermöglichen. Auf der Firewall muss eine Regel zur direkten Port Weiterleitung angelegt werden, welche SSH auf die Rendezvousbox weiterleitet.

Hinweis: Pro SSH-Verbindung sind maximal 50 Port Forwardings erlaubt.

Tragen Sie in der genuReSI unter [Einstellungen](#) → [SSH](#) → [SSH Weiterleitung](#) die IP-Adresse/Hostname und/oder den Port ein, auf dem die Weiterleitung aktiviert ist.

5.5 HTTP Proxy für SSH

Sollte es nicht möglich sein eine feste Port Weiterleitung für SSH zur Rendezvousbox einzurichten, kann SSH auch über einen HTTP Proxy übertragen werden.

Sie können entweder den in Ihrem Windows System hinterlegten HTTP Proxy verwenden oder einen eigenen Proxy eintragen. Sollte der Proxy eine Authentisierung erfordern, geben Sie Ihre Zugangsdaten gemäß folgendem Muster in das Feld **HTTP Proxy für SSH** ein.

`Benutzer:Passwort@IP-Adresse/Hostname:Port`

5.6 GUI-Gestaltung

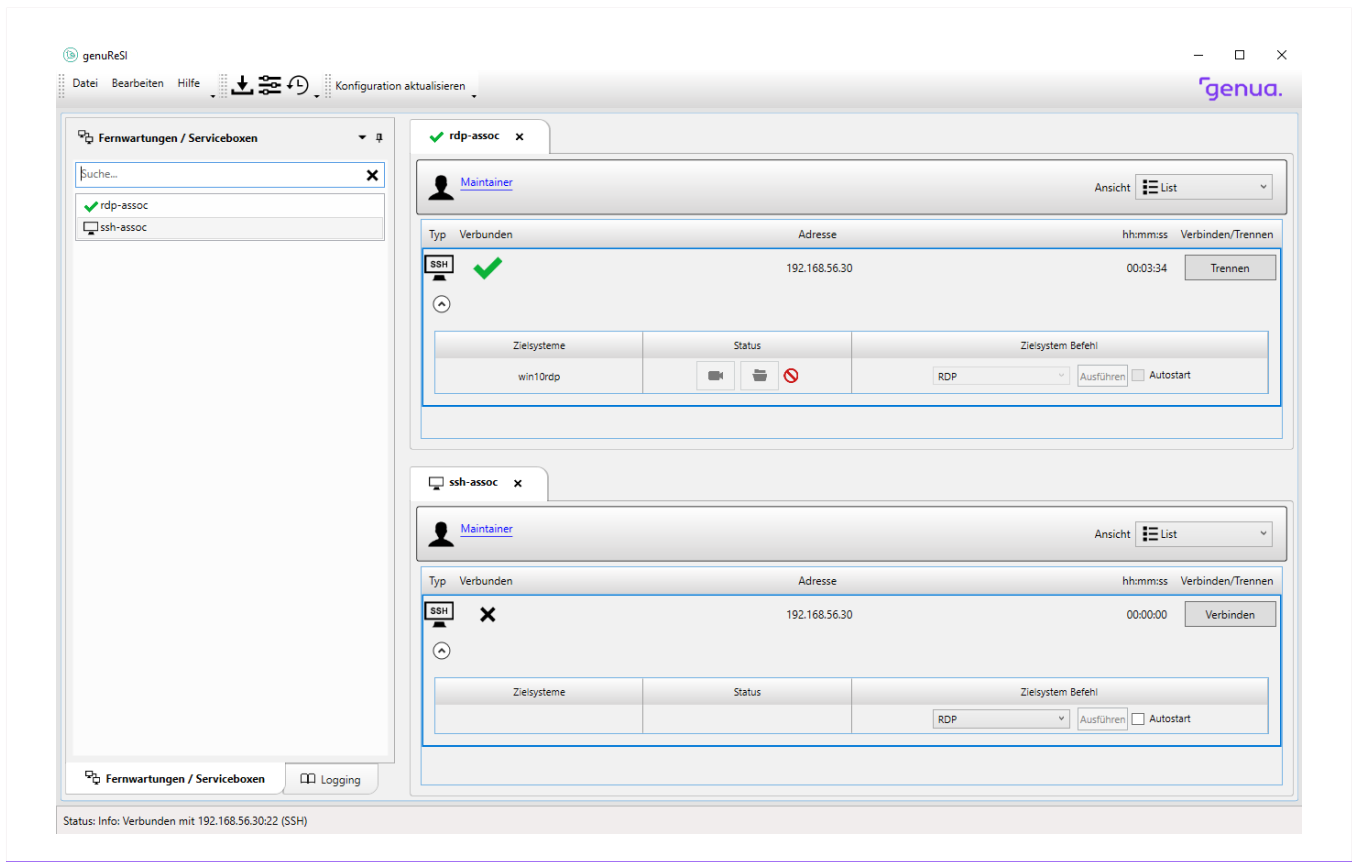


Abbildung 5.5: GUI Gestaltung

Die Anwendung genuReSI verwendet den sogenannten Dock Mechanismus. Damit können Fenster verschoben, am Bearbeitungsrahmen andockt oder auch auf verschiedenen Bildschirmen angeordnet werden (siehe <https://docs.microsoft.com/de-de/visualstudio/ide/customizing-window-layouts-in-visual-studio>, „Anordnen und Andocken von Fenstern“). Dadurch können Sie Ihren Bildschirm beliebig anpassen und gestalten.

5.7 Neue Befehle

Das Rendezvous-Konzept verwendet intern Port Forwardings, um Verbindungen über den Rendezvous-Server zum Zielsystem weiterzuleiten. Im Menü **Befehle** der Toolbar können Befehle definiert werden, die dann auf dem Zielsystem ausgeführt werden. Dazu muss die Befehlssyntax des zu verwendenden Befehls bekannt sein. Die Variablen **%HOST%** und **%PORT%** können für den Hostnamen und den benutzten Port eingesetzt werden. Windows Umgebungsvariablen werden unterstützt.

Beispiel: Auf dem Zielsystem soll via PuTTY eine SSH-Verbindung geöffnet werden. Unter **Dateiname** wird definiert, wo sich im lokalen Dateisystem die Datei **putty.exe** befindet. Unter **Argumente** muss der Befehl **-P %PORT% %HOST%** definiert werden, da PuTTY via Kommandozeile den Port mit **-P** anspricht.

Kapitel 6

STEP7 durch Rendezvous

6.1	GUI-Installation des Loopback-Adapters	46
6.2	Befehlsbasierte Installation des Loopback-Adapters	47
6.3	IP-Konfiguration	48

Um das Siemens STEP7 Protokoll mit Rendezvous zu nutzen, empfiehlt es sich, einen Loopback-Adapter in Windows anzulegen. Der Fernwarter kann dazu direkt die genuReSI-App-GUI nutzen. Zusätzlich besteht die Möglichkeit, die Installation über die Kommandozeile anzustoßen, etwa um eine automatische Installation mithilfe eines zentralen Verwaltungstools auszuführen.

6.1 GUI-Installation des Loopback-Adapters

Hinweis: Sie benötigen Administratorrechte, um den Microsoft Loopback-Adapter zu installieren.

1. Starten Sie genuReSI App.
2. Navigieren Sie zu [Einstellungen](#) → [SSH](#).
3. Im Abschnitt **Netzwerkkarte für Mapping-Adressen** klicken Sie auf [Installiere Loopback Treiber](#). Der Loopback-Adapter wird installiert.
4. Wählen Sie aus dem Drop-down-Menü den neu installierten Loopback-Adapter aus. Der Adapter wird nun von genuReSI App verwendet.
5. Klicken Sie auf [Schließen](#).
6. Fahren Sie fort mit Abschnitt 6.3

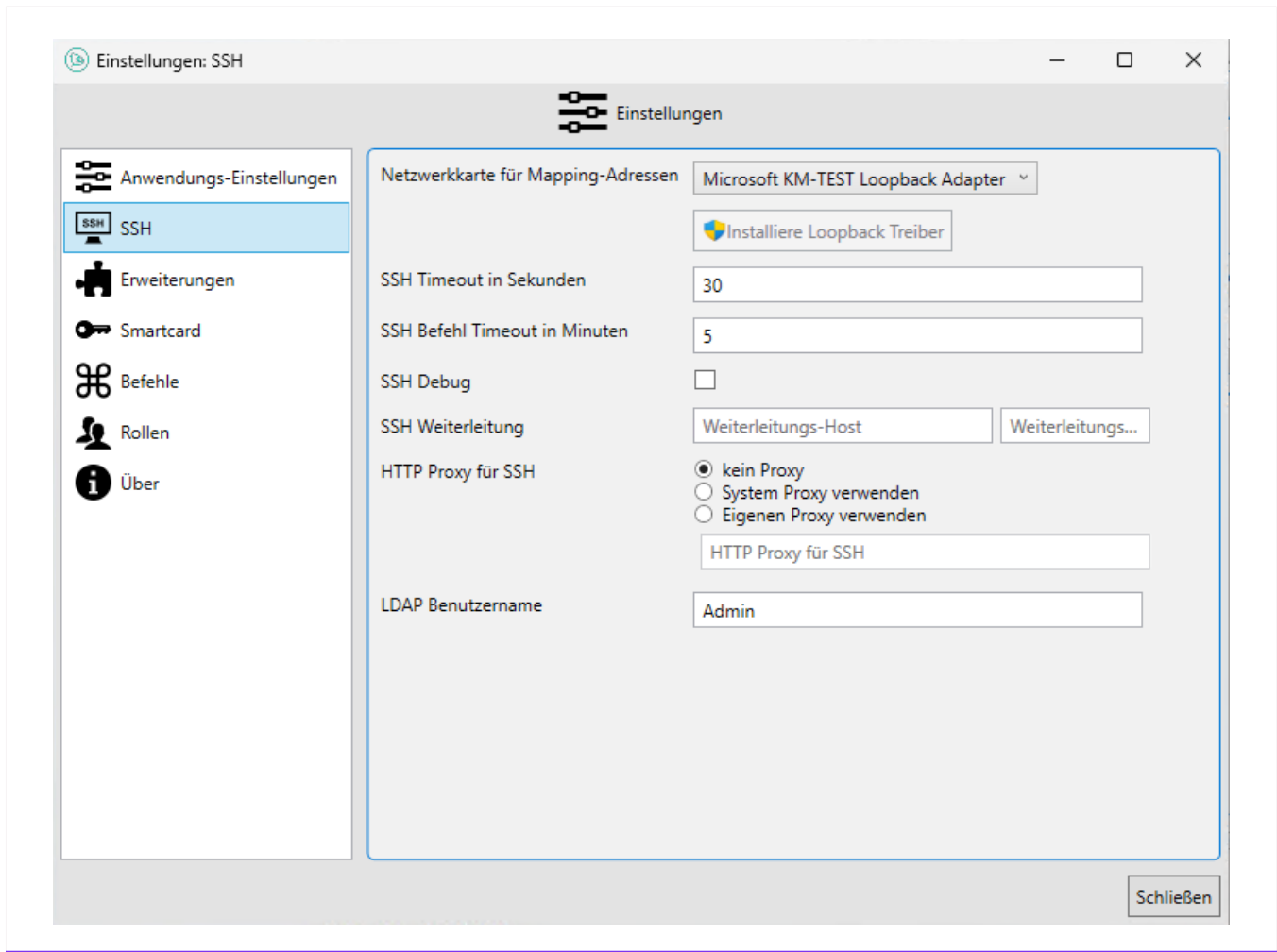


Abbildung 6.1: Loopback-Adapter in der genuReSI

6.2 Befehlsbasierte Installation des Loopback-Adapters

Hinweis: Das ausführende Programm benötigt Administratorrechte, um den Microsoft Loopback-Adapter zu installieren.

Rufen Sie die genuReSI-Applikation mit dem Parameter `/install-loopback` auf, um den Loopback-Adapter automatisch zu installieren:

```
ReSI.exe /install-loopback
```

Fahren Sie fort mit Abschnitt 6.3.

6.3 IP-Konfiguration

Sobald man die Verbindung herstellt, fragt Windows, ob genuReSI dem Loopback-Adapter eine IP zuweisen darf. Bestätigen Sie mit **Ja**.

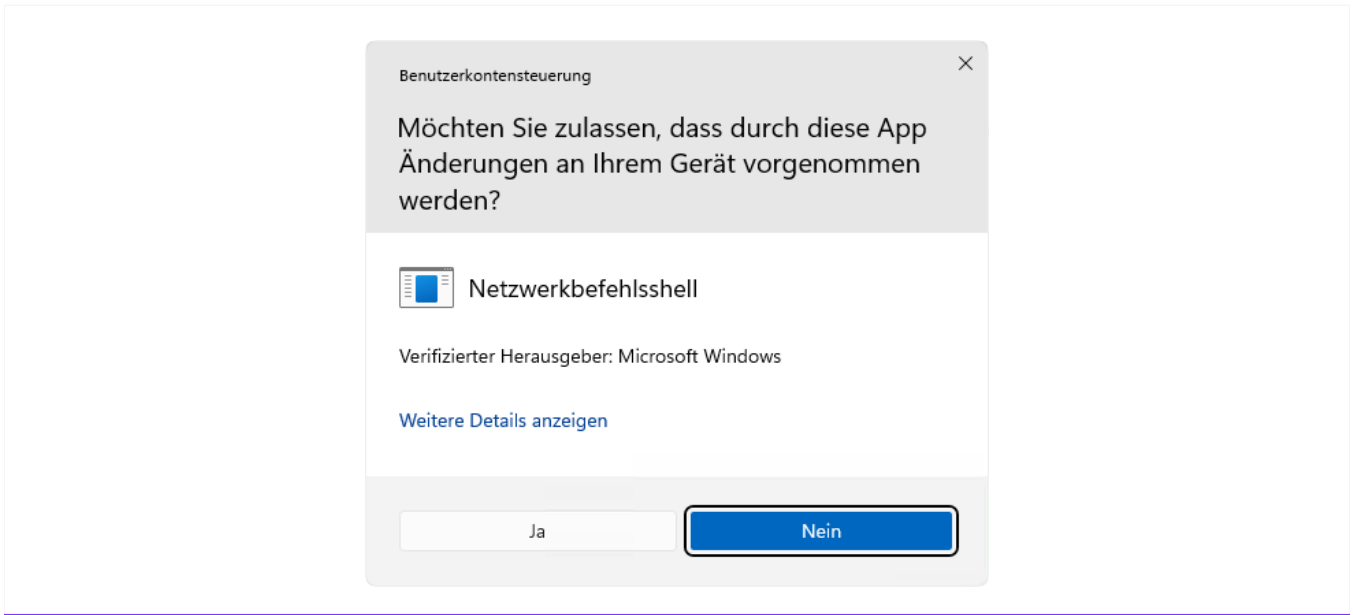


Abbildung 6.2: Benutzerkontensteuerung

Ist die Verbindung hergestellt, sieht man in der Detailansicht (Wechsel zur Detailansicht mit **Strg** + **D**), dass als Lokale Adresse die IP **192.168.100.3** eingestellt ist. Diese IP wird vom Administrator **vorher** am genucenter als S7-Adresse eingetragen.

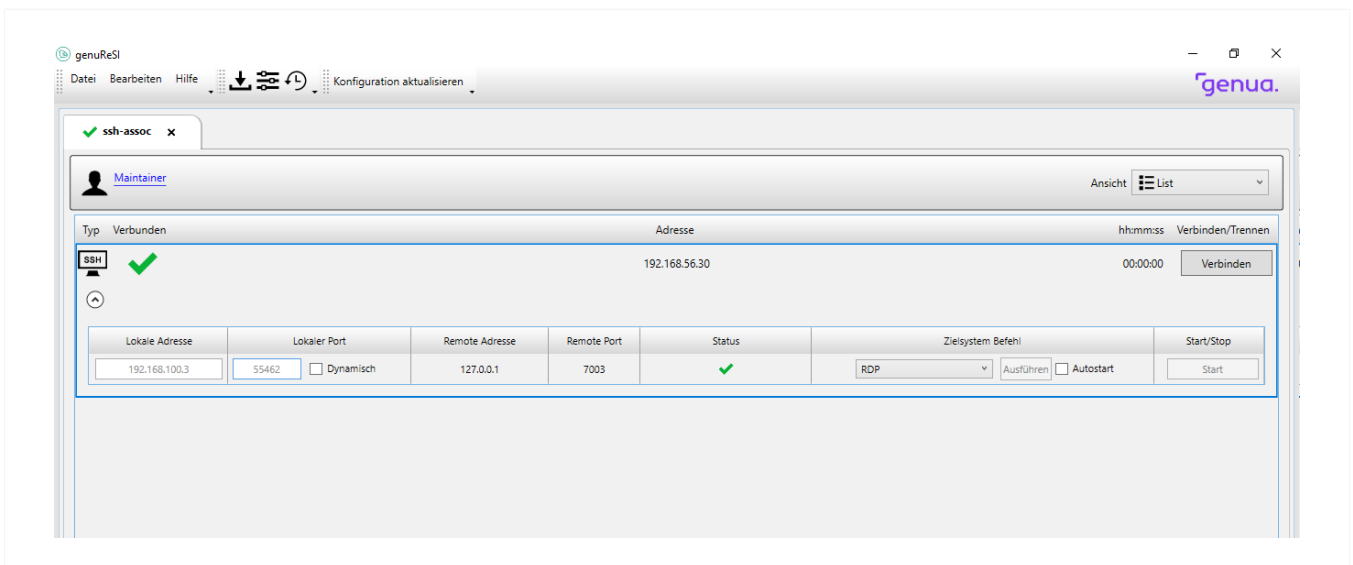


Abbildung 6.3: genuReSI mit aktiver Verbindung

Nun zeigt auch ipconfig die von genuReSI gesetzte IP:

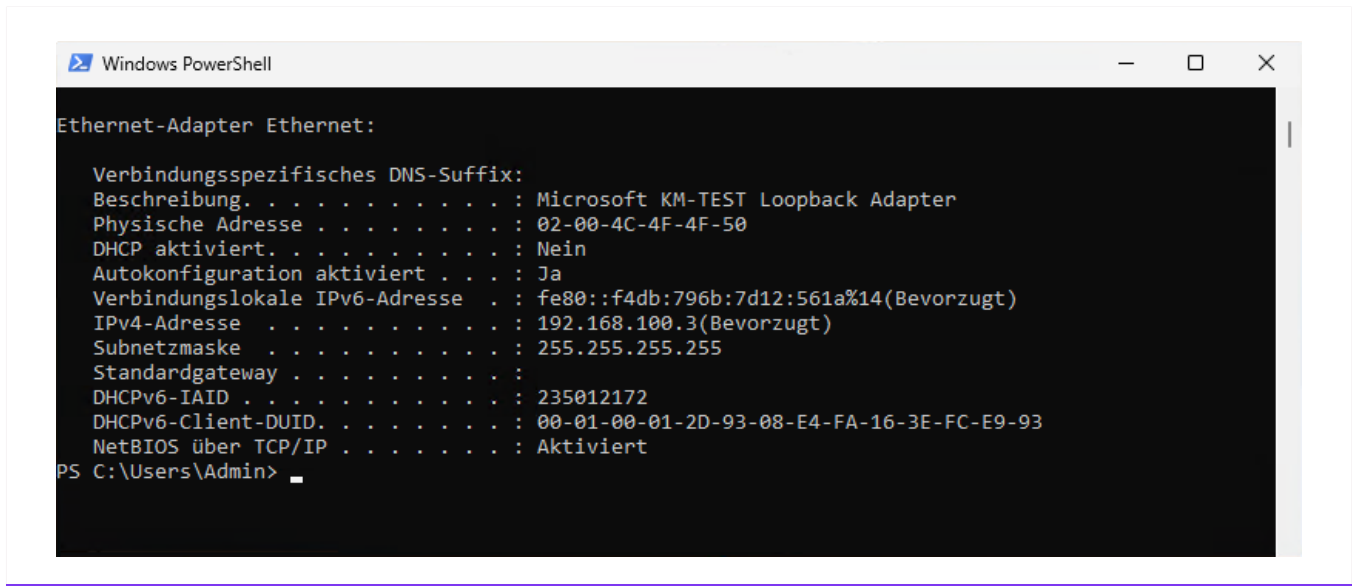


Abbildung 6.4: Powershell mit Mapping

Sobald genuReSI beendet wird, werden die gesetzten IPs wieder gelöscht.

Index

A

Aufruf der Windows-App genuReSI 5

E

Erweiterte Konfiguration 33

F

Fernwartung mit dem Rendezvous-Konzept
1

G

genuReSI für den Fernwarter 9

genuReSI für den Operator 21

P

Produktübersicht v

S

STEP7 durch Rendezvous 45

Über genua

Die genua GmbH ist ein deutscher Spezialist für IT-Sicherheit. Seit der Firmengründung 1992 beschäftigen wir uns mit der Absicherung von Netzwerken und bieten hochwertige Lösungen. Unser Leistungsspektrum umfasst die Absicherung sensibler Schnittstellen im Behörden- und Industriebereich bis hin zur Vernetzung hochkritischer Infrastrukturen. Des Weiteren bieten wir Lösungen für eine zuverlässig verschlüsselte Datenkommunikation via Internet an – einschließlich Fernwartung und Remote Access für Mitarbeiter im Home Office oder unterwegs.

Unsere Lösungen werden in Deutschland entwickelt und produziert. Viele Firmen und Behörden setzen auf Lösungen von genua zum Schutz ihrer IT. genua ist ein Unternehmen der Bundesdruckerei-Gruppe.

genua GmbH, Domagkstraße 7, 85551 Kirchheim bei München
tel +49 89 991950-0, info@genua.de