VisuNet RM Shell 5

Handbuch

Your automation, our passion.

PEPPERL+FUCHS

Es gelten die Allgemeinen Lieferbedingungen für Erzeugnisse und Leistungen der Elektroindustrie, herausgegeben vom Zentralverband Elektroindustrie (ZVEI) e. V. in ihrer neuesten Fassung sowie die Ergänzungsklausel: "Erweiterter Eigentumsvorbehalt".

Weltweit

Pepperl+Fuchs-Gruppe

Lilienthalstr. 200

68307 Mannheim

Deutschland

Telefon: +49 621 776 - 0

E-Mail: info@de.pepperl-fuchs.com

https://www.pepperl-fuchs.com

2024-01

2024-01

1 Historie des Handbuchs

Die folgenden Ausgaben des Handbuchs wurden veröffentlicht:

Version	Kommentare
Frühere	VisuNet RM Shell Version 5.5
11/2021	VisuNet RM Shell Version 5.6 • Zusätzliche Unterstützung des Pad-Ex® 01-Geräts • Zusätzliches Schnellmenü mit Statussymbolen • Benutzerdefiniertes VisuNet RM Shell-Hintergrundbild und Logo • Zusätzliche "Automatische Abmeldung“ für Administrator und Ingenieur • Zusätzliche Unterstützung von Add-ins für virtuelle RDP-Kanäle (PRO-Lizenz erforderlich)

2024-01

2 Einleitung

2.1 Hinweis

Diese manuelle Überarbeitung wurde mit VisuNet® RM Shell Version 5.6 veröffentlicht, deckt aber auch alle früheren Versionen von VisuNet RM Shell 5 ab.

2.2 Inhalt des Dokuments

Dieses Dokument beinhaltet Informationen, die Sie für den Einsatz Ihres Produkts in den zutreffenden Phasen des Produktlebenszyklus benötigen. Dazu können zählen:

- Produktidentifizierung
- Lieferung, Transport und Lagerung
- Montage und Installation
- Inbetriebnahme und Betrieb
- Instandhaltung und Reparatur
- Störungsbeseitigung
- Demontage
- Entsorgung

Hinweis!

Entnehmen Sie die vollständigen Informationen zum Produkt der weiteren Dokumentation im Internet unter www.pepperl-fuchs.com.

Hinweis!

Sie finden spezifische Geräteinformationen wie z. B. das Baujahr, indem Sie den QR-Code auf dem Gerät scannen. Alternativ geben Sie die Seriennummer in der Seriennummernsuche unter www.pepperl-fuchs.com ein.

Die Dokumentation besteht aus folgenden Teilen:

- vorliegendes Dokument
- Datenblatt

Zusätzlich kann die Dokumentation aus folgenden Teilen bestehen, falls zutreffend:

- EU-Baumusterprüfbescheinigung
- EU-Konformitätserklärung
- Konformitätsbescheinigung
- Zertifikate
- Control Drawings
- Betriebsanleitung
- Handbuch funktionale Sicherheit
- weitere Dokumente

2.3 Zielgruppe, Personal

Die Verantwortung hinsichtlich Planung, Montage, Inbetriebnahme, Betrieb, Instandhaltung und Demontage liegt beim Anlagenbetreiber.

Nur Fachpersonal darf die Montage, Inbetriebnahme, Betrieb, Instandhaltung und Demontage des Produkts durchführen. Das Fachpersonal muss die Betriebsanleitung und die weitere Dokumentation gelesen und verstanden haben.

Machen Sie sich vor Verwendung mit dem Gerät vertraut. Lesen Sie das Dokument sorgfältig.

2.4 Verwendete Symbole

Dieses Dokument enthält Symbole zur Kennzeichnung von Warnhinweisen und von informativen Hinweisen.

Warnhinweise

Sie finden Warnhinweise immer dann, wenn von Ihren Handlungen Gefahren ausgehen können. Beachten Sie unbedingt diese Warnhinweise zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden.

Je nach Risikostufe werden die Warnhinweise in absteigender Reihenfolge wie folgt dargestellt:

Gefahr!

Dieses Symbol warnt Sie vor einer unmittelbar drohenden Gefahr.

Falls Sie diesen Warnhinweis nicht beachten, drohen Personenschäden bis hin zum Tod.

Warnung!

Dieses Symbol warnt Sie vor einer möglichen Störung oder Gefahr.

Falls Sie diesen Warnhinweis nicht beachten, können Personenschäden oder schwerste Sachschäden drohen.

Vorsicht!

Dieses Symbol warnt Sie vor einer möglichen Störung.

Falls Sie diesen Warnhinweis nicht beachten, können das Produkt oder daran angeschlossene Systeme und Anlagen gestört werden oder vollständig ausfallen.

Informative Hinweise

Hinweis!

Dieses Symbol macht auf eine wichtige Information aufmerksam.

Handlungsanweisung

Dieses Symbol markiert eine Handlungsanweisung. Sie werden zu einer Handlung oder Handlungsfolge aufgefordert.

3 VisuNet RM Shell – ein Überblick

VisuNet Remote-Monitore (RMs) und Box Thin Clients (BTC) von Pepperl+Fuchs sind Thin-Client-Lösungen für Industrieanwendungen, die Bedienern eine vereinfachte, moderne Benutzerschnittstelle bieten. Die Firmware von RM, als VisuNet RM Shell (RM Shell) bezeichnet, ermöglicht es Anwendern, auf einfache Weise über Ethernet auf Anwendungen zuzugreifen, die auf einem Hostsystem (z. B. Arbeitsplatz-PC oder Server) laufen.

VisuNet RM Shell unterstützt die neuesten Versionen gängiger Remote-Protokolle wie RDP 10 oder VNC. Mit diesen Protokollen lassen sich RMs/BTCs auf einfache Weise in alle wichtigen Prozessleitsysteme integrieren – ungeachtet dessen, ob es sich dabei um virtuelle oder konventionelle, Workstation-basierte Setups handelt.

Darüber hinaus verfügt VisuNet RM Shell über eine maßgeschneiderte Benutzerschnittstelle, die nur die wichtigen Systemaspekte anzeigt, die für die Konfiguration des RM/BTC relevant sind. Dadurch wird die Integration eines RM/BTC in das Prozessleitsystem einfacher als je zuvor. Das Konfigurieren einer neuen RDP-Verbindung kann zum Beispiel in wenigen Schritten durchgeführt werden. Dies wird durch ein konsistentes, für die Touchscreen-Bedienung optimiertes Design aller Protokoll-Editoren erreicht.

VisuNet RM Shell trägt auch zur Erhöhung der Prozessstabilität bei. Sie sorgt für eine stabile Verbindung zum Host des Prozessleitsystems und für eine fehlerfreie Anzeige der Prozessbilder.

Mit der automatischen Verbindungsfunktion können RMs/BTCs so konfiguriert werden, dass sie automatisch eine Verbindung zu einem bestimmten Hostsystem herstellen, ohne dass der Anwender eingreifen muss. Während vorübergehend unterbrochene Verbindungen automatisch wieder hergestellt werden, können in VisuNet RM Shell Backup-Hosts definiert werden, mit denen sich ein RM/BTC automatisch verbindet, wenn ein Hostsystem ausfällt.

Zusätzlich zur Unterstützung von Remote-Protokollen bietet VisuNet RM Shell auch eine eingeschränkte Webbrowser-Funktion, die über einen optionalen professionellen Lizenzschlüssel aktiviert werden kann. Damit können feste Adressen für Webanwendungen wie beispielsweise webbasierte Manufacturing Execution Systems (MES) definiert werden. Anwender mit Administratorrechten können den Zugriff der Bediener auf diese vordefinierten Websites einschränken. Dies erhöht die Systemsicherheit und verringert das Risiko von Malware-Infiltration.

In diesem Handbuch werden die Merkmale und Funktionen von VisuNet RM Shell ausführlich beschrieben.

3.1 Aktualisieren der Architektur

Die RM Shell-Architektur besteht aus zwei Partitionen.

Die Hauptelemente von Partition C sind RM Shell sowie Gerätetreiber und Serviceanwendungen. Alle Komponenten basieren auf Windows 10 IOT LTSC 2019 oder Windows 10 IOT LTSB 2016.

Aktualisierungen zu Windows-Sicherheitspatches, funktionalen Aktualisierungen oder RM Shell-Sicherheitsaktualisierungen wirken sich auf Partition C aus. Nur einzelne Komponenten sind betroffen und werden je nach Aktualisierung überschrieben. Bei jedem Zurücksetzen auf die Werkseinstellungen werden alle Daten von Partition C überschrieben.

Die Aktualisierung der Werkseinstellungen ist ein eigenes Paket, das über Shell bereitgestellt und importiert wird.

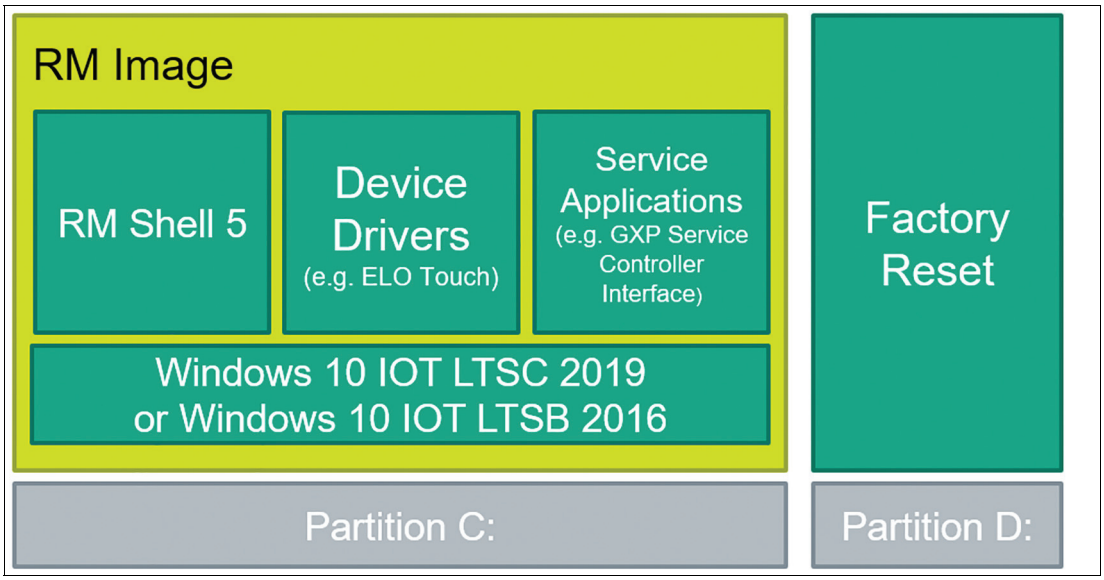


Abbildung 3.1 Architektur von RM Shell

3.2 Werksseitige Rückstellung

Mit Factory Reset Version 6.0 und höher steht die Image-Datei nicht mehr lokal auf Partition D zur Verfügung, wodurch Speicherplatz und Geschwindigkeit erhöht werden. Mit Factory Reset Version >6.0 und VisuNet RM Shell Version >5.3 ist es möglich, ein eigenes Backup Image zu erstellen. Wir empfehlen dringend, ein eigenes Backup Image zu erstellen und auf Ihrem Netzlaufwerk zu speichern.

Funktion	Beschreibung	Hinweise
Pepperl+Fuchs Factory Reset-Image	Verfügbar für jedes bestimmte Gerät. Die Pepperl+Fuchs-Grundeinstellungen werden auf Ihr Gerät angewendet. Mit Factory Reset 6.0 und höher wird die Image-Datei nicht mehr auf dem Gerät gespeichert.	Wenden Sie sich an Ihren lokalen Sales Support **Vorsicht!** Nach dem Anwenden des Pepperl+Fuchs Image muss das Gerät lokal eingerichtet werden! Der Assistent für den ersten Start von VisuNet RM Shell führt Sie durch die wichtigsten Schritte der Erstkonfiguration. Weitere Informationen finden Sie im Kapitel "Assistent für den ersten Start“ im Handbuch von VisuNet RM Shell.
Backup Image	Selbsterfasstes Backup Image, das nur auf demselben Gerät mit identischer Seriennummer angewendet werden kann. Das Backup Image kann verwendet werden, um einen bestimmten Zustand eines Geräts wiederherzustellen.	Muss vom Kunden im Voraus über VisuNet RM Shell Factory Reset oder VisuNet CC - Device Backup erfasst werden. **Anmerkung:** VisuNet CC kann das Gerät möglicherweise nicht finden, wenn nach der Aufnahme der Image-Datei Änderungen am Computernamen oder in den Netzwerkeinstellungen vorgenommen wurden.

3.3 Programmfunktionen

Funktion	Beschreibung	Hinweise
Betriebssystem	Basierend auf Microsoft® Windows® 10 IoT Enterprise LTSC 2019 oder Microsoft® Windows® 10 IoT Enterprise LTSB 2016	Verbesserte Funktion in RM Shell 5
Moderne, vereinfachte Benutzerschnittstelle	Touch-optimierte, moderne Benutzerschnittstelle	
Einfache Einrichtung	Für die intuitive Verwendung entworfen. Zusätzlich führt Sie ein Einrichtungsassistent bei der ersten Konfiguration eines RM durch die wichtigsten Schritte	Verbesserte Funktion in RM Shell 5
Automatische Verbindung	Ermöglicht die Konfiguration des RM für die automatische Verbindung mit Hostsystemen nach dem Start	
Erkennung von Verbindungsverlust	Der RM erkennt Netzwerkausfälle oder wenn ein Host nicht verfügbar ist	
Backup-Verbindung	Bei einem Netzwerk- oder Hostausfall kann ein RM automatisch eine Verbindung zu einem Backup-Hostsystem herstellen	

Funktion	Beschreibung	Hinweise
Zentrale Verwaltung aller RMs	RMs können zentral über VisuNet Control Center verwaltet und konfiguriert werden.	Optionale CC-Lizenzfunktion. Weitere Informationen finden Sie unter pepperl-fuchs.com/hmi
Remote-Protokolle und -Clients		
MS RDP	Neueste Version von Microsoft Remote Desktop Protocol	
VNC	VNC-Client, kompatibel mit mehreren VNC-Servern (z. B. TightVNC und UltraVNC)	
Eingeschränkter Webbrowser, basierend auf Internet Explorer	Schneller HTML-Browser, der Internet Explorer zum Rendern von Websites verwendet. Der Zugriff von Bedienern kann auf bestimmte Websites eingeschränkt werden.	Optionale PRO-Lizenzfunktion
Eingeschränkter Webbrowser, basierend auf Chrome	Schneller HTML5-Browser, der Google Chrome verwendet. Der Zugriff von Bedienern kann auf bestimmte Websites eingeschränkt werden.	Optionale PRO-Lizenzfunktion
Desktop Sharing	Zeigt den Desktop anderer RMs mit aktiviertem Desktop-Sharing-Server an	Optionale PRO-Lizenzfunktion
Raritan KVM	Der Client ermöglicht eine direkte Verbindung zum Raritan Dominion KX IV-101 KVM-over-IP-Switch	Optionale PRO-Lizenzfunktion
DRDC	Ermöglicht die Direktverbindung eines VisuNet Remote Monitors mit einem virtualisierten Emerson DeltaV-System	Optionale DRDC-Lizenzfunktion
Security		
Unified Write Filter	Unified Write Filter schützt das Laufwerk vor persistentem Speichern schädlicher Software	Neue Funktion in RM Shell 5
Scheduler	Ermöglicht die Verwendung des Unified Write Filter rund um die Uhr ohne Pufferüberlauf. Regelmäßige Neustarts können geplant werden, wenn das Gerät nicht verwendet wird	Neue Funktion in RM Shell 5
Unterstützung von Antivirensoftware	Administratoren können Virenschutzsoftware von Drittanbietern installieren. Windows Defender ist standardmäßig aktiviert	Neue Funktion in RM Shell 5
Dialogfeldfilter	Schließt Anwendungsfenster, die nicht in der Whitelist enthalten sind und blockiert den Benutzerzugriff auf das Dateisystem	Neue Funktion in RM Shell 5
Firewall	Die Windows-Firewall schützt RMs vor Netzwerkangriffen	
USB-Stick-Laufwerksperre	Die USB-Sperre verhindert den Zugriff auf Speichermedien wie USB-Sticks auf den RMs	
Aktualisierungen	Pepperl+Fuchs bietet regelmäßig Aktualisierungen in Form von Sicherheits-Patches und Funktionsaktualisierungen an.	Bitte suchen Sie regelmäßig nach Aktualisierungen oder lassen Sie sich über den Thin-Client-Software-Update-Service von Pepperl+Fuchs informieren.

2024-01

Funktion	Beschreibung	Hinweise
Sicherungsbild erfassen	Erfassen Sie Ihre individuellen Geräteeinstellungen des RM/BTC als Sicherungsbild und wenden Sie sie bei Bedarf wieder auf das Gerät an.	Neue Funktion von RM Shell 5.3 und höher und Factory Reset 6.0 **Anmerkung:** RM Shell 5.3 (oder höher) in Kombination mit Factory Reset 6.0 (oder höher) ist erforderlich.
Sicherungsbild anwenden	Wenden Sie die individuellen Geräteeinstellungen des RM/BTC an, die zuvor als Sicherungsbild erfasst wurden, und überschreiben Sie die vollständige Windows-Partition.	Neue Funktion von RM Shell 5.3 und höher und Factory Reset 6.0 **Anmerkung:** RM Shell 5.3 (oder höher) in Kombination mit Factory Reset 6.0 (oder höher) ist erforderlich.
Zusätzliche Sicherheitsfunktionen		
Sicherheitswarnungen	Pepperl+Fuchs überprüft alle Berichte zu **Sicherheitslücken,** die Produkte und Dienstleistungen von Pepperl+Fuchs betreffen.	Internetsicherheit und Berichterstellung, Abonnieren Sie unseren **RSS-Feed,** um über Informationen zur Cyber-Sicherheit von Pepperl+Fuchs auf dem Laufenden zu bleiben
Thin-Client-Software-Update-Service	Wir informieren Sie, wenn Sicherheits- oder Funktionsaktualisierungen verfügbar sind.	https://www.pepperl-fuchs.com/global/en/33314.htm
Erweiterte Funktionen		
Administratorzugriff auf Windows® Explorer	Ermöglicht Administratoren, Anwendungen von Drittanbietern zu installieren und erweiterte Systemeinstellungen anzupassen. Systeme können in die Domain integriert werden.	Neue Funktion in RM Shell 5
Reinigungsverriegelung	Ermöglicht die vorübergehende Sperrung der Eingabegeräte (z. B. Touchscreen) bei der Reinigung des Gerätes, um versehentliche Eingaben zu vermeiden	
Netzwerk-Testtools	Ein Satz Netzwerk-Testtools (z. B. Ping-Tool) bietet Unterstützung bei der Inbetriebnahme eines RM	
Task Switcher	Wechseln Sie zwischen mehreren Remote-Verbindungen und -Apps, die auf dem RM ausgeführt werden.	
Extended Desktop-Support für industrielle Box Thin Clients BTC	Remote-Profilverbindungen können verschiedenen Monitoren zugewiesen werden, die mit dem industriellen Box Thin Client BTC verbunden sind	
Wireless-LAN-Konfigurationsunterstützung	Wireless-LAN-Verbindungen können in RM Shell verwaltet werden (integrierter Wireless-LAN-Adapter erforderlich)	
Process Explorer	Ermöglicht es, einen RM zu diagnostizieren und zu überwachen, wie viel RAM, Speicher und CPU von lokalen Prozessen verwendet werden.	
Desktop Sharing-Server	Klonen Sie einen RM und zeigen Sie seinen Desktop auf anderen RMs an	

3.4 Lizenzierung

Bestellinformationen

Beim Kauf von RMs oder BTCs von Pepperl+Fuchs ist RM Shell bereits installiert und der Lieferumfang enthält RM Shell-Lizenzen.

Part.Nr.	Modellnummer
548289	VISUNET-RM-SHELL5-PRO
548294	VISUNET-RM-SHELL5-DRDC
548284	VISUNET-RM-SHELL5-CC

Hinweis!

Lizenz-Bundles

Informationen zu Lizenz-Bundles erhalten Sie bei Ihrem Pepperl+Fuchs-Vertreter vor Ort.

3.5 Standardkennwörter

Gerät/Funktion	Anwender	Kennwort
Werksseitige Rückstellung		VisuReset
Raritan KVM-over-IP-Switch DKX4-101	admin	raritan

3.6 Installation

Ein Assistent führt Sie durch die ersten Schritte der Installation von RM Shell. Nach Abschluss des Assistenten für den ersten Start wird RM Shell in der Rolle Bediener gestartet.

3.6.1 Einrichtungsassistent

Wenn Sie ein Gerät zum ersten Mal mit VisuNet RM Shell starten, wird der Einrichtungsassistent auf dem Bildschirm angezeigt. Dieser Assistent führt Sie durch die wichtigsten Schritte der Erstkonfiguration.

Konfigurieren Sie Ihre "Basic System Settings“ (grundlegende Systemeinstellungen) und klicken Sie auf **Next** (Weiter). Akzeptieren Sie "Terms and Conditions“ (Geschäftsbedingungen) im nächsten Fenster, um VisuNet RM Shell zu verwenden.

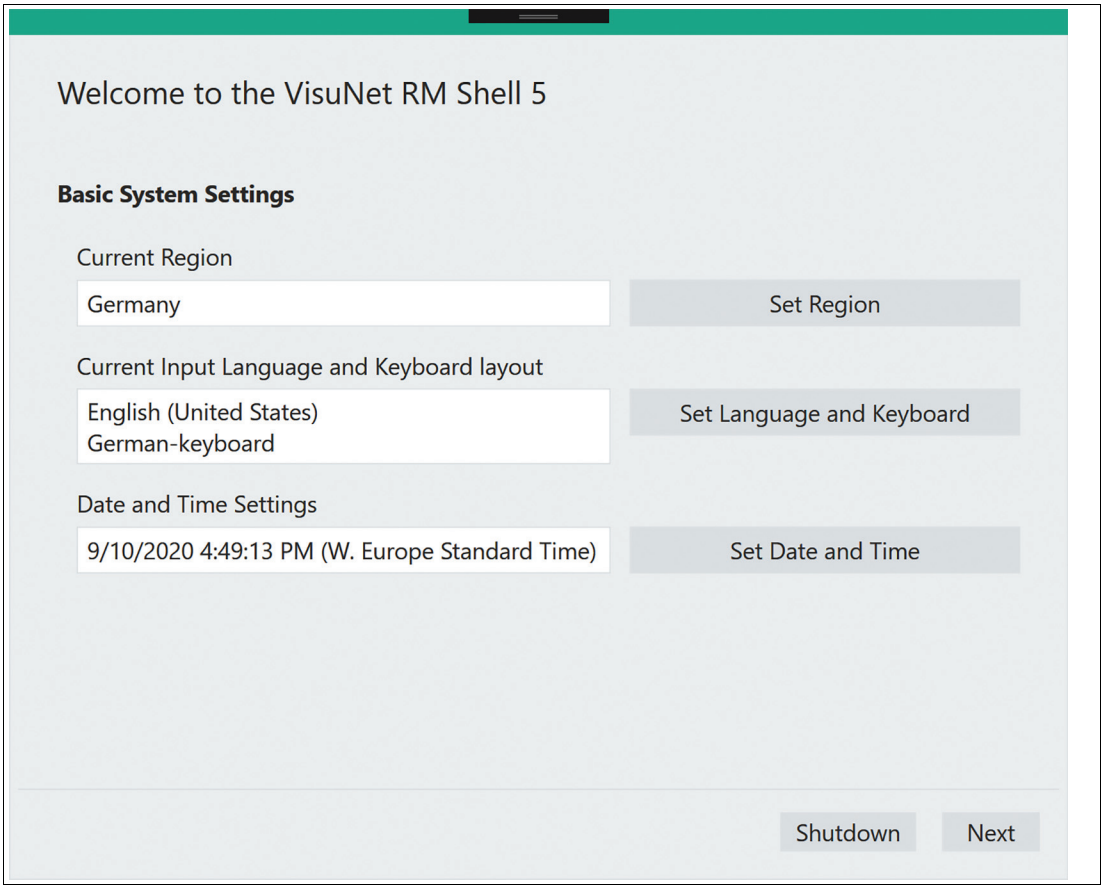


Abbildung 3.2

Wenn Ihr VisuNet RM Shell 5 auf Windows® 10 IoT Enterprise 2019 LTSC basiert, müssen Sie auch die folgenden Schritte ausführen:

Die richtige "Region“ festlegen

1. Klicken Sie auf **Set Region** (Region festlegen), um zu den erweiterten Microsoft®-Einstellungen zu gelangen.

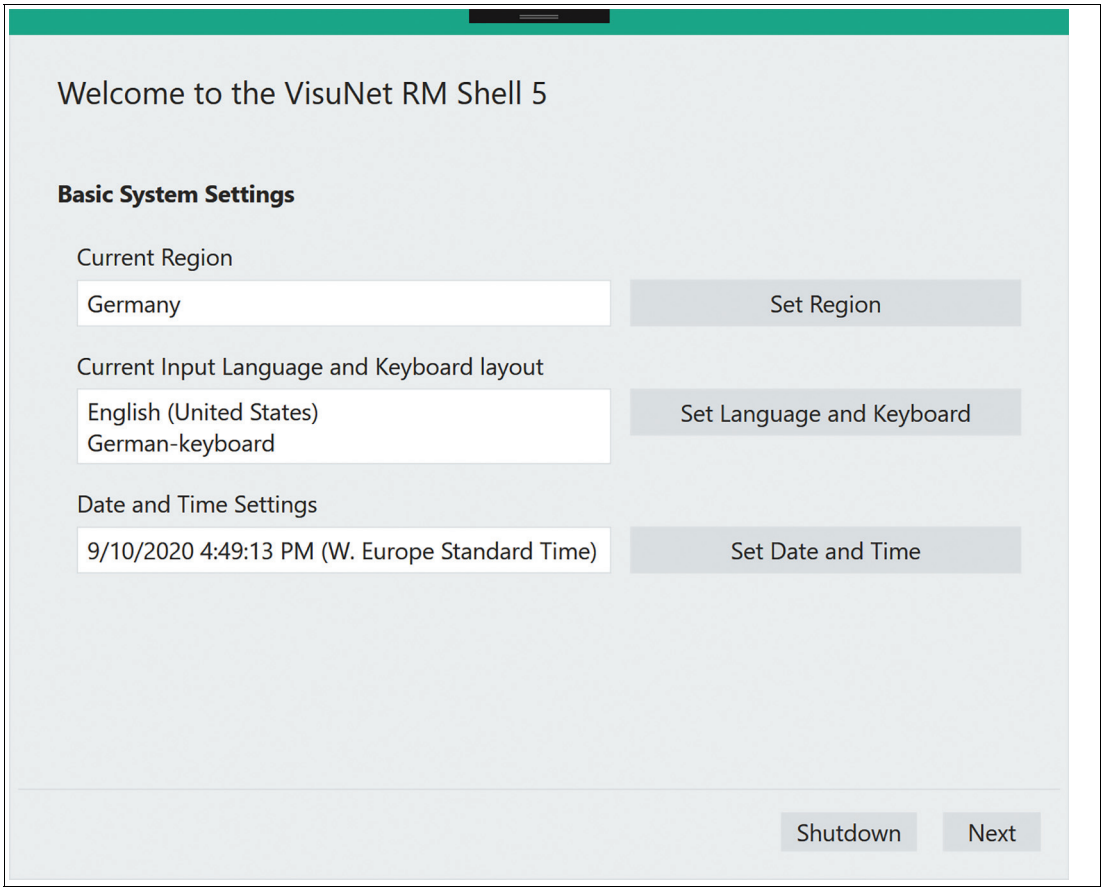


Abbildung 3.3

2. Navigieren Sie zur Registerkarte **Region** (Region) auf der linken Seite

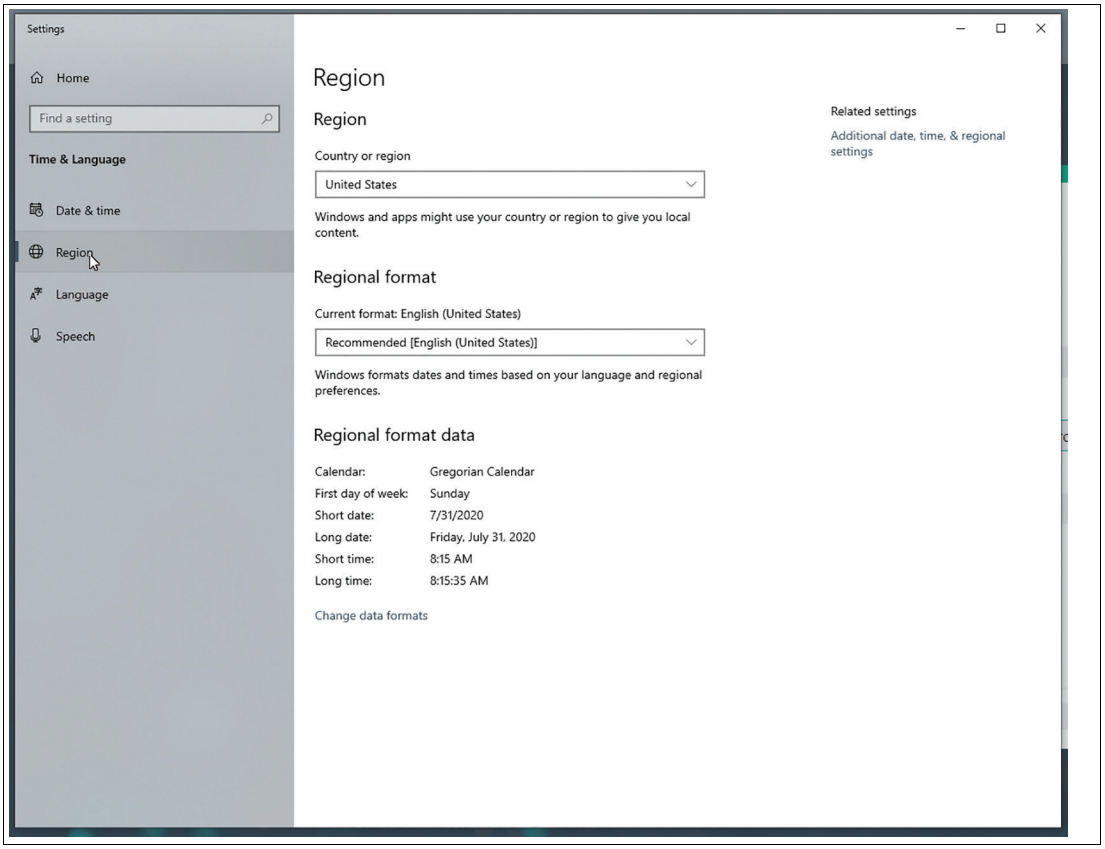


Abbildung 3.4

3. Wählen Sie die gewünschte Region aus der Dropdown-Liste aus.

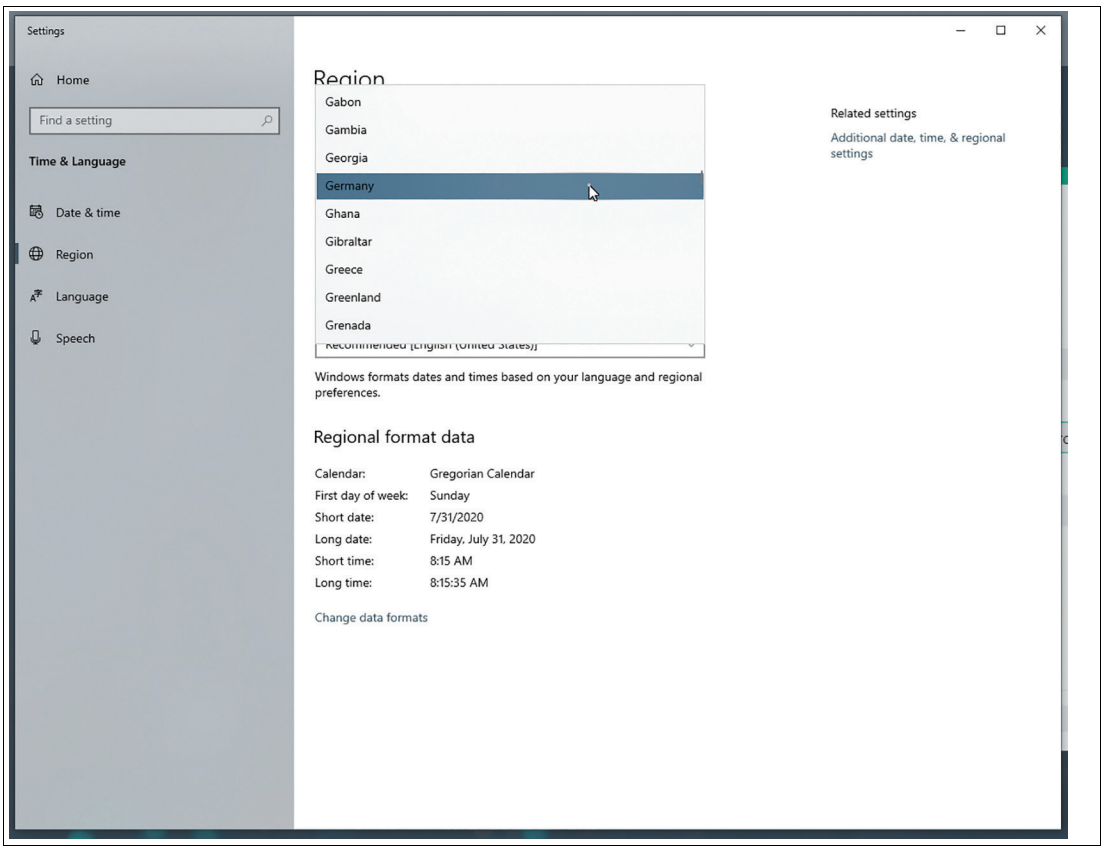


Abbildung 3.5

4. Schließen Sie das Dialogfeld.

"Keyboard Layout“ (Tastaturbelegung) hinzufügen

Klicken Sie auf **Set Language and Keyboard** (Sprache und Tastatur einstellen) (2.), um die erweiterten Microsoft®-Einstellungen einzugeben, und navigieren Sie dann zu **Language** (Sprache)

1. Wählen Sie die installierte Sprache **English (United States)** (Englisch (US)) aus und klicken Sie auf die Schaltfläche **Options** (Optionen):

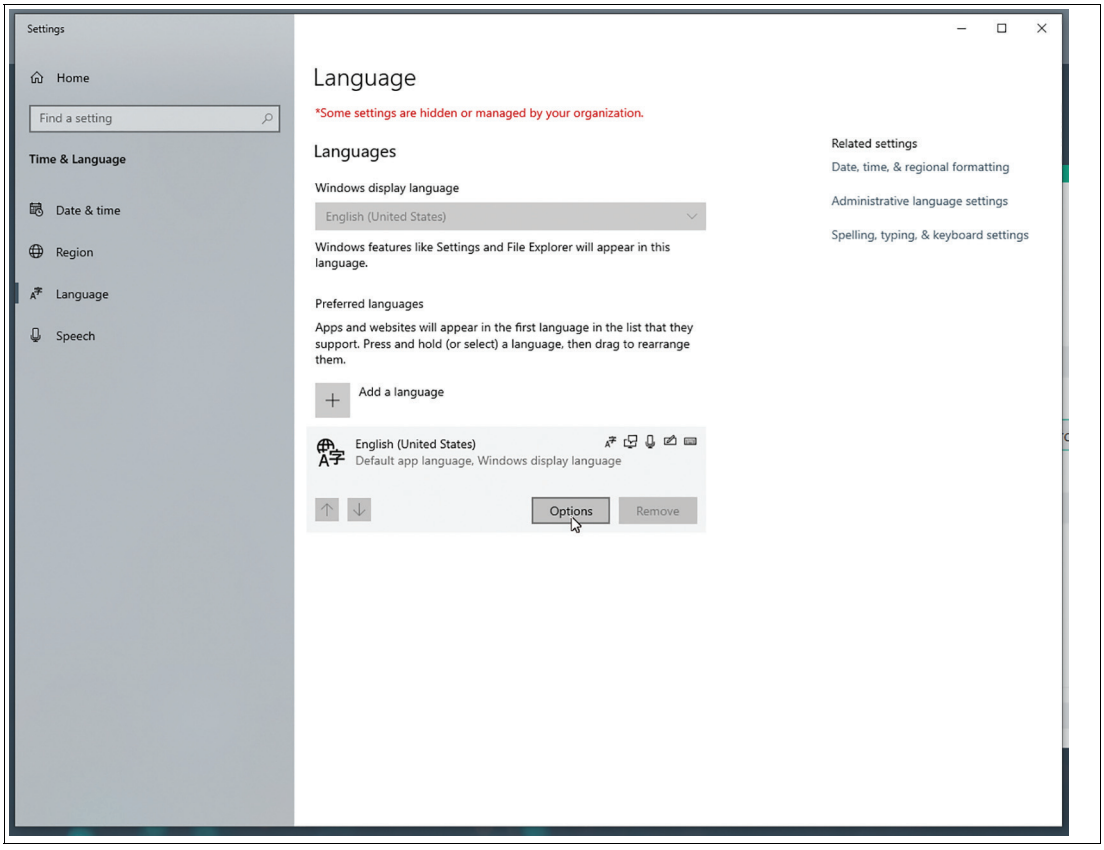


Abbildung 3.6

2. Klicken Sie im Abschnitt "Keyboards“ (Tastatur) auf die Schaltfläche **Add a keyboard** (Eine Tastatur hinzufügen)

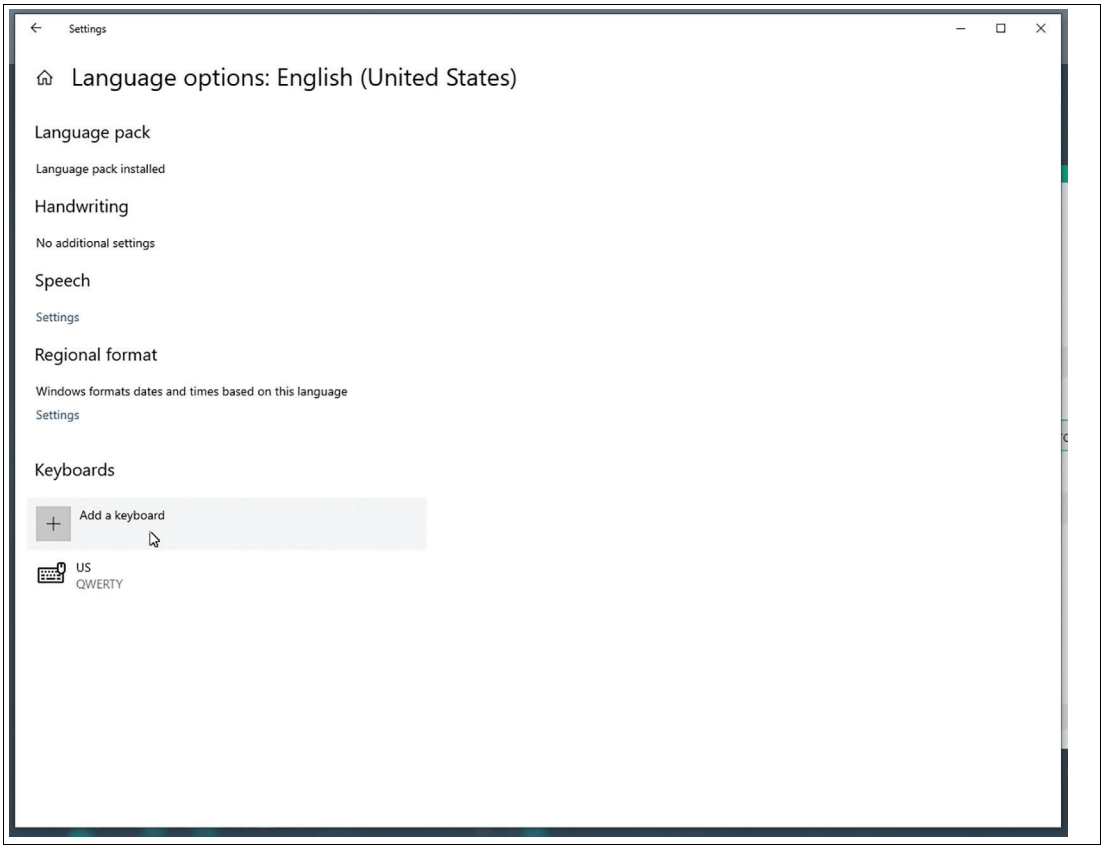


Abbildung 3.7

3. Wählen Sie die neue Tastaturbelegung aus:

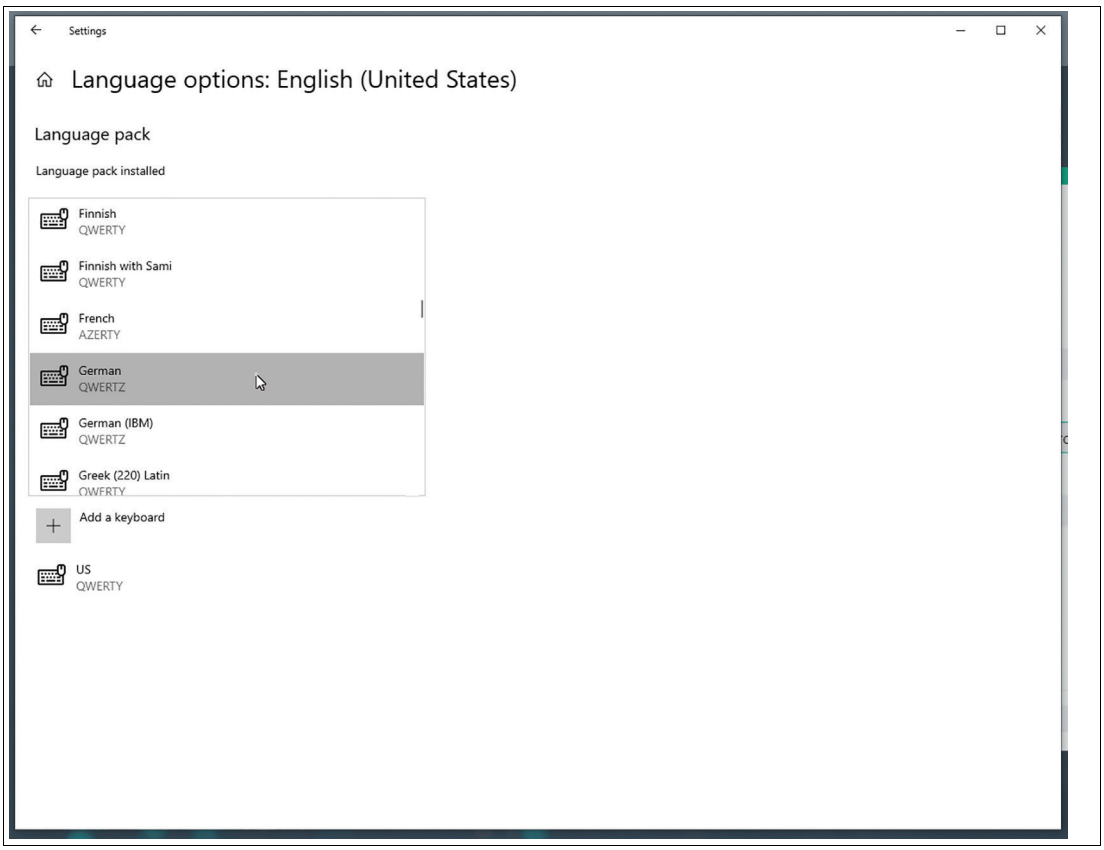


Abbildung 3.8

4. Entfernen Sie im letzten Schritt die US-Tastaturbelegung.

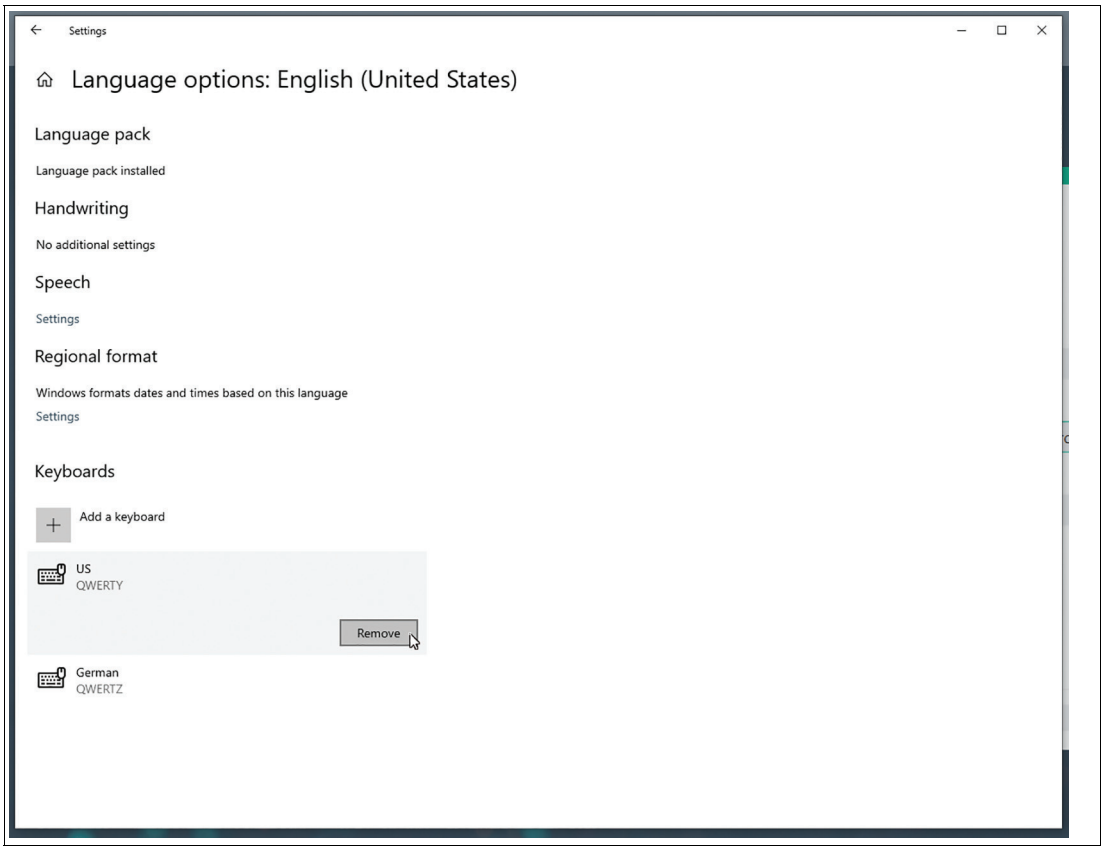


Abbildung 3.9

5. Schließen Sie das Dialogfeld.
6. Die Eingabesprache im Einrichtungsassistenten ändert sich nicht, da nur die Tastaturbelegung von dieser Änderung betroffen ist.

Der Assistent führt Sie durch die folgenden Schritte:

"Computer Name“ (Computername)

Ändert auch den Computernamen Ihres Windows®-Gerätes.

Der aktualisierte Computername wird erst nach einem Neustart angewendet.

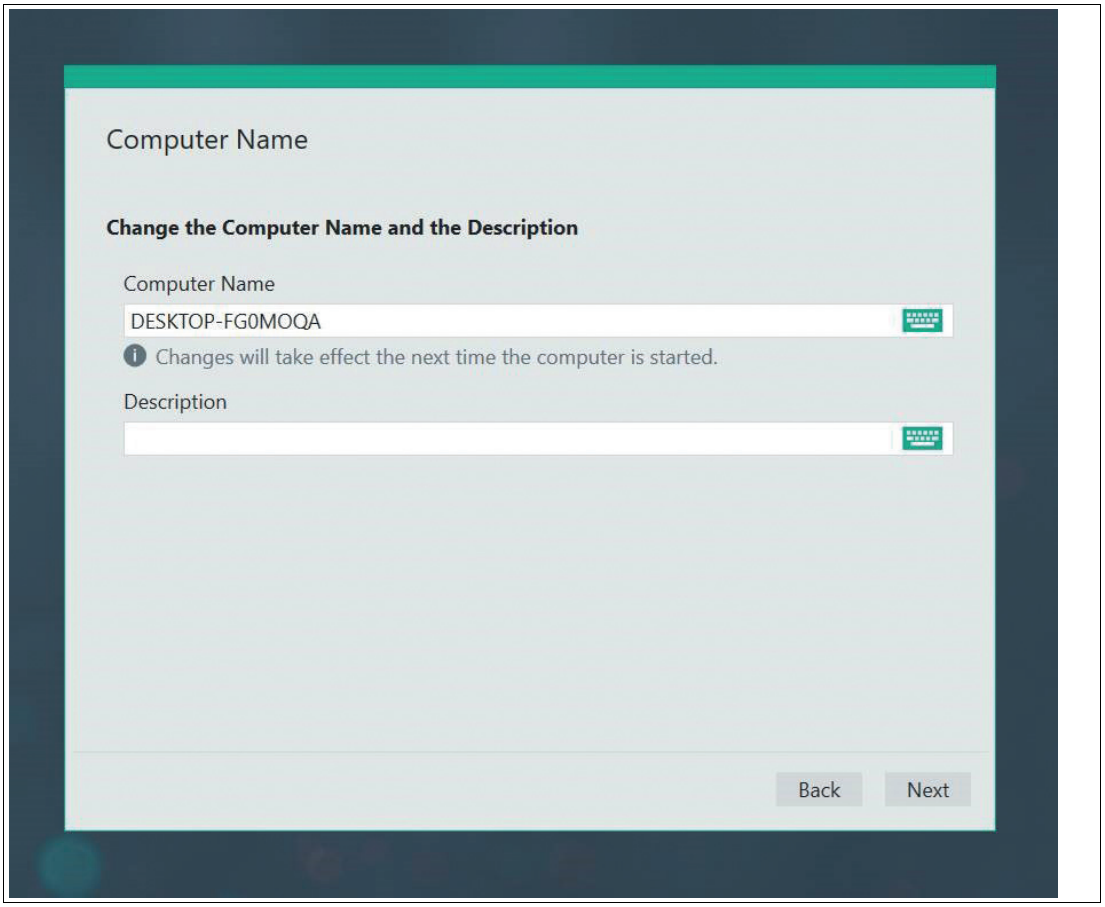


Abbildung 3.10 "Computer Name“ (Computername)

"Setup Network“ (Netzwerk einrichten)

Alle Informationen zur lokalen Hardware des RM-/BTC-Netzwerkadapters werden angezeigt.

Sie können den Netzwerkadapternamen entsprechend Ihren Bedürfnissen anpassen.

Verwenden Sie diese Option zum Aktivieren/Deaktivieren von "DHCP“ (Dynamic Host Configuration Protocol).

Mit "DHCP“ können Sie den RM/BTC ohne weitere manuelle Konfiguration in ein bestehendes Netzwerk integrieren. Einstellungen wie "IP Address“ (IP-Adresse), "Subnet Mask“ (Subnetzmaske), "Default Gateway“ (Standard-Gateway) und "DNS Server“ (DNS-Server) werden dem RM/BTC dann automatisch zugewiesen. Sie können jedoch alle diese Parameter manuell einrichten, indem Sie die Option "DHCP“ deaktivieren.

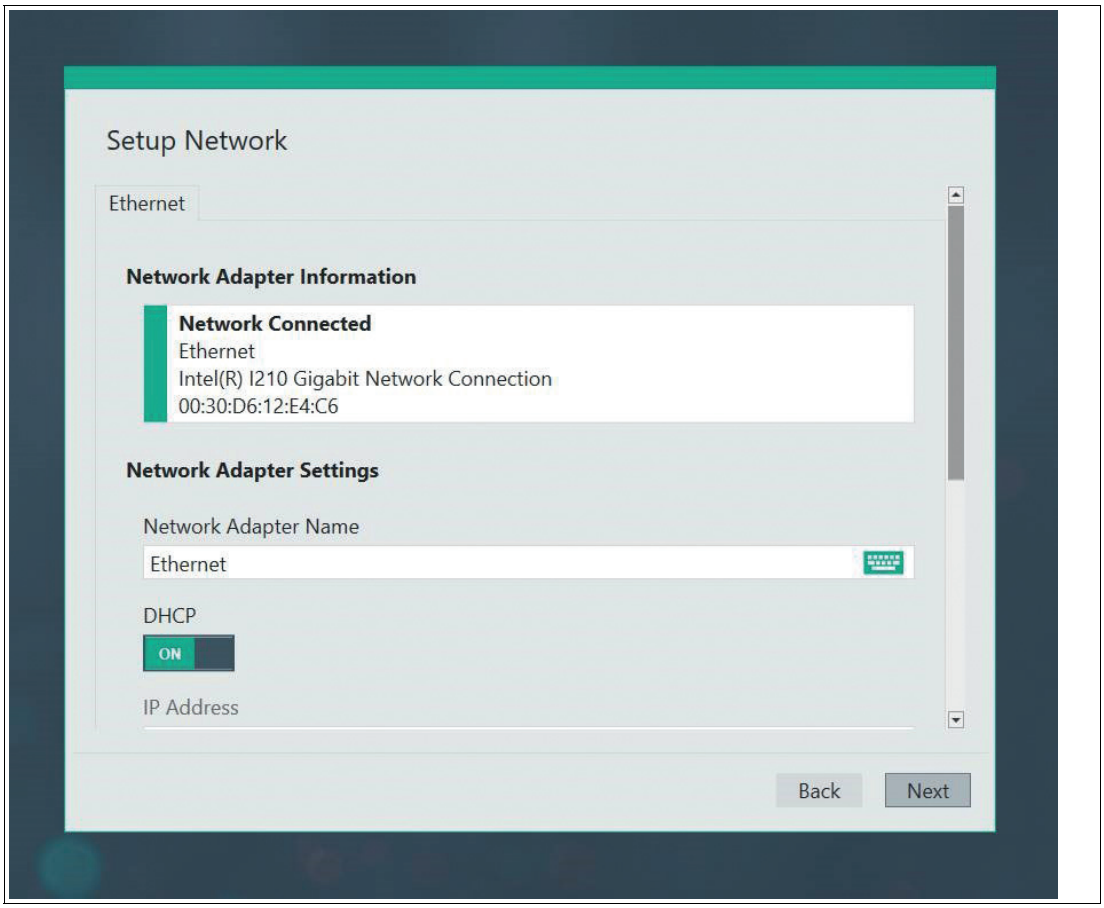


Abbildung 3.11 "Setup Network“ (Netzwerk einrichten)

"Setup Touchscreen“ (Einrichtung des Touchscreens)

Wählen Sie die richtigen Touch-Einstellungen aus, wenn Ihr RM über eine Touchscreen-Option verfügt. Weitere Informationen finden Sie im Abschnitt 7.13.

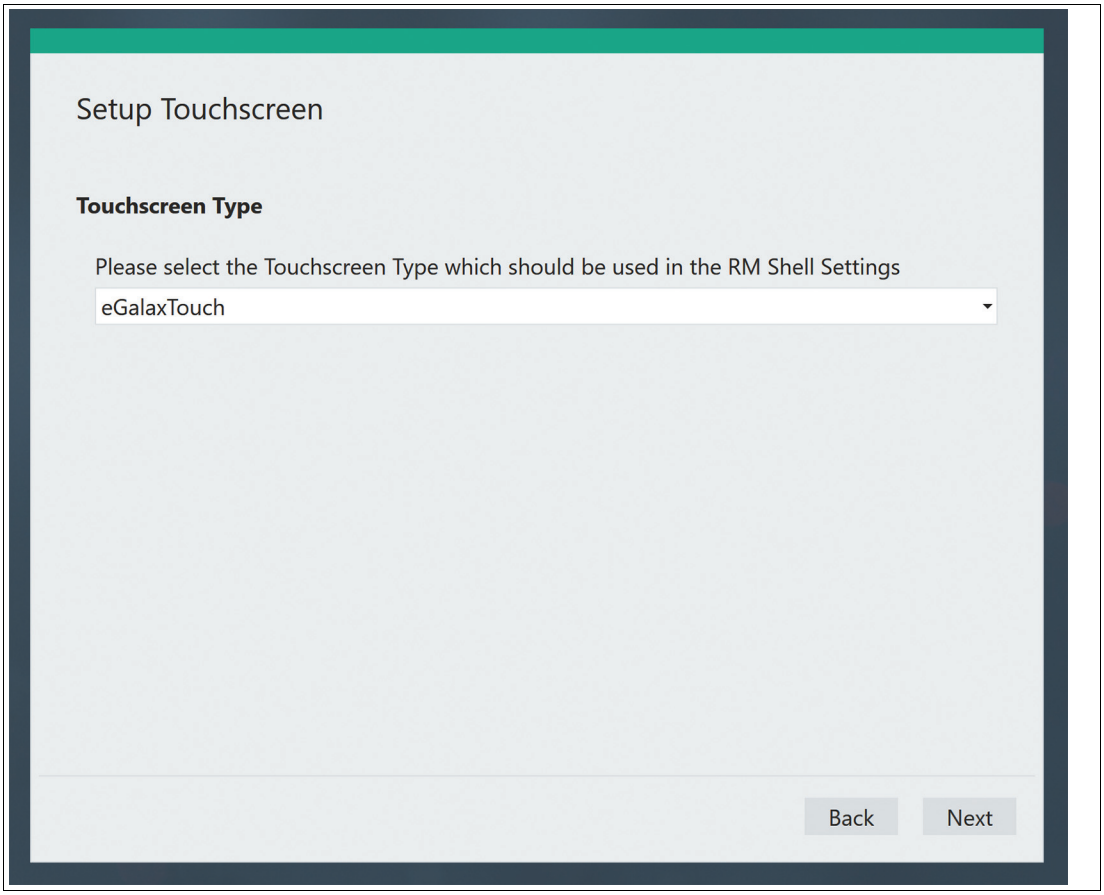


Abbildung 3.12

Password Settings (Kennwort-Einstellungen)

Engineer Password (Ingenieurskennwort): Es ist kein Standardkennwort festgelegt. Um ein Höchstmaß an Sicherheit zu gewährleisten, müssen die Benutzerrollen "Administrator“ und "Engineer“ (Ingenieur) kennwortgeschützt sein.

Administrator Password (Administratorkennwort): Es ist kein Standardkennwort festgelegt. Um ein Höchstmaß an Sicherheit zu gewährleisten, müssen die Benutzerrollen "Administrator“ und "Engineer“ (Ingenieur) kennwortgeschützt sein.

Windows Password (Windows-Kennwort): Greift auf das Windows®-Kennwort zu. Das Windows-Kennwort wird nur in verschlüsselter Form angezeigt.

Tipp

Es wird dringend empfohlen, das Windows-Kennwort zu ändern.

"Factory Reset Password“ (Kennwort zur werksseitigen Rückstellung): Ändern Sie das Kennwort für die werksseitige Rückstellung. Das Kennwort ist durch Punkte ausgeblendet und muss mindestens 6 Zeichen lang sein. Das Feld darf nicht leer sein.

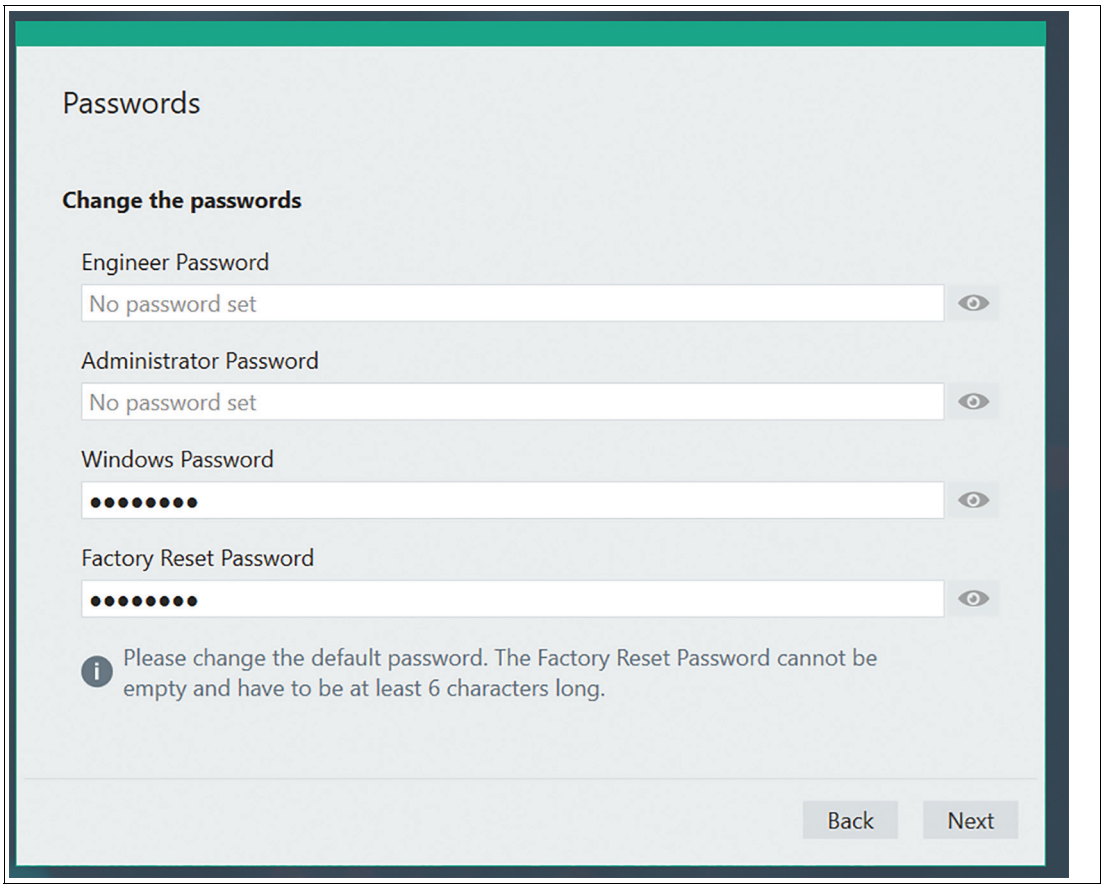


Abbildung 3.13 Password Settings (Kennwort-Einstellungen)

Hinweis!

Im Falle der Wiederherstellung eines Backup- oder Clone-Images oder wenn Sie das Kennwort in der Benutzerschnittstelle zur werksseitigen Rückstellung geändert haben, wird die Option "Factory Reset Password“ (Kennwort für die werksseitige Rückstellung) nicht angezeigt.

License Agreement (Lizenzvereinbarung)

Sie müssen der Lizenzvereinbarung zustimmen, damit Sie fortfahren können.

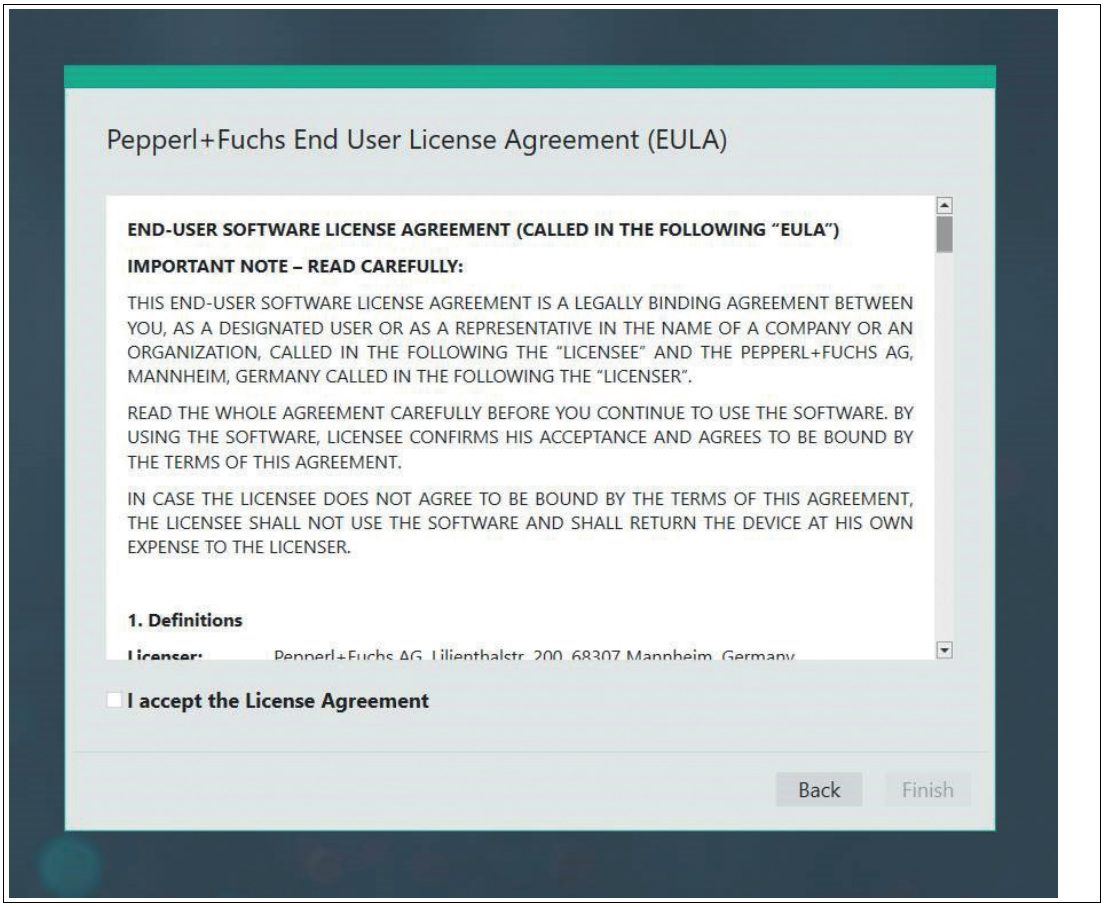


Abbildung 3.14 License Agreement (Lizenzvereinbarung)

Hinweis!

Richtige Informationen

Stellen Sie sicher, dass Sie in diesem Assistenten die richtigen Informationen angegeben haben. Die Informationen sollten für den Standort gültig sein, an dem VisuNet RM Shell installiert wird. Für die verschlüsselte Kommunikation und um eine zuverlässige Kommunikation zu gewährleisten, ist die richtige Zeit erforderlich.

Nach Abschluss des Einrichtungsassistenten wird VisuNet RM Shell in der Rolle "Operator“ (Bediener) gestartet. Wenn Sie weitere Einstellungen konfigurieren möchten, wechseln Sie zur Rolle "Administrator“.

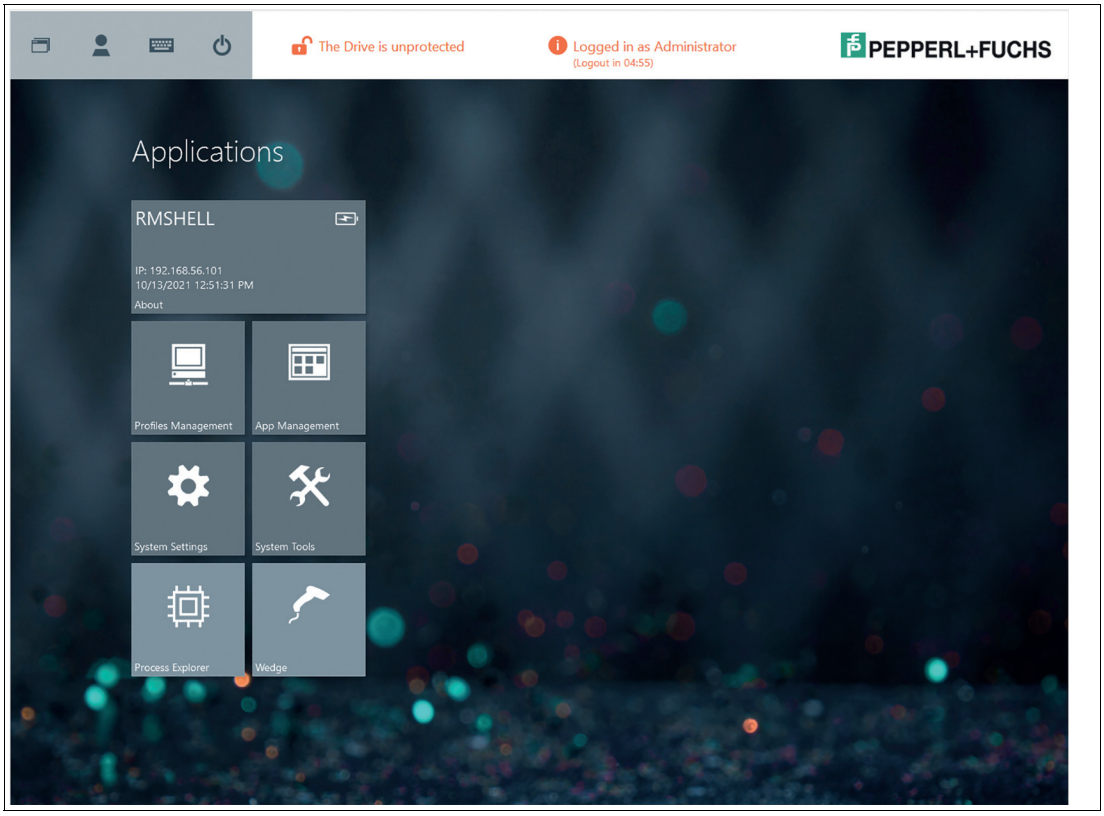


Abbildung 3.15

VisuNet RM Shell enthält keine vorab erstellten Verbindungsprofile. Aus diesem Grund ist die Profilliste leer, wenn Sie VisuNet RM Shell zum ersten Mal starten.

3.7 Benutzerrollen von VisuNet RM Shell

Das VisuNet RM Shell Sicherheitskonzept basiert auf 3 Benutzerrollen, die hierarchisch strukturiert sind. Jede Benutzerrolle hat unterschiedliche Rechte.

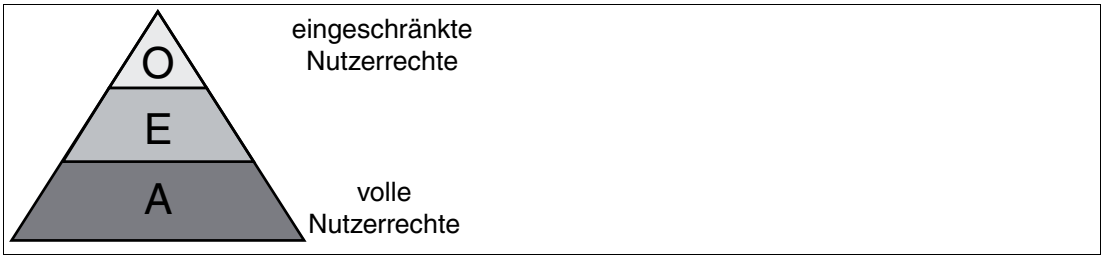


Abbildung 3.16 Das Konzept der Benutzerrechte: **O**(perator), **E**(ngineer) und **A**(dministrator)

Benutzerrolle	Beschreibung
Bediener (O)	Bediener sind Standardanwender. Sie können nur vordefinierte Profile ausführen. Bediener haben keinen Zugriff auf RM-Einstellungen.
Ingenieur (E)	Ingenieure sind für die Einrichtung und Integration von RM verantwortlich. Sie haben Zugriff auf Profile, Systemeinstellungen und Anwendungen (Erstellen, Bearbeiten und Löschen von Profilen).
Administrator (A)	Administratoren haben alle Rechte der Bediener und Ingenieure. Darüber hinaus können Administratoren auf Windows® Explorer zugreifen, um Anwendungen und Treiber von Drittanbietern zu installieren und erweiterte Einstellungen außerhalb von VisuNet RM Shell anzupassen.

Warnung!

Kennwortschutz!

Um ein Höchstmaß an Sicherheit zu gewährleisten, müssen die Benutzerrollen "Administrator“ und "Engineer“ (Ingenieur) kennwortgeschützt sein. Der Zugriff auf die Benutzerrollen Administrator und Ingenieur sollte nur Mitarbeitern gestattet werden, die mit der Verwaltung von Thin Clients vertraut sind. Es gibt keine werkseitig voreingestellte Kennworteinstellung für eine der Benutzerrollen.

Die Kennwörter können im Assistenten für den ersten Start festgelegt werden. In der Administratorrolle können die Kennwörter angepasst oder in den Sicherheitseinstellungen festgelegt werden

Hinweis!

Zusätzlicher Kennwortschutz mit optionaler automatischer Abmeldung der Anwender

Ingenieure und Administratoren werden abgemeldet, wenn das Gerät länger als der eingestellte Zeitraum inaktiv ist, wenn die automatische Anwenderabmeldung aktiviert ist.

Hinweis!

Kompatibilität von Drittanbieter-Software

VisuNet RM Shell ist für die Arbeit mit Software vorgesehen, die mit VisuNet-Geräten von Pepperl+Fuchs geliefert wird. Pepperl+Fuchs übernimmt keine Garantie für die Funktionalität von Drittanbieter-Software. Die Kunden sind dafür verantwortlich, die Kompatibilität mit Software von Drittanbietern sicherzustellen.

4 VisuNet RM Shell 5-Benutzerschnittstelle

Funktionen des Startbildschirms (Administratorrolle, nachdem einzelne Profile erstellt wurden)

Der Startbildschirm ist in 6 grundlegende Bereiche unterteilt:

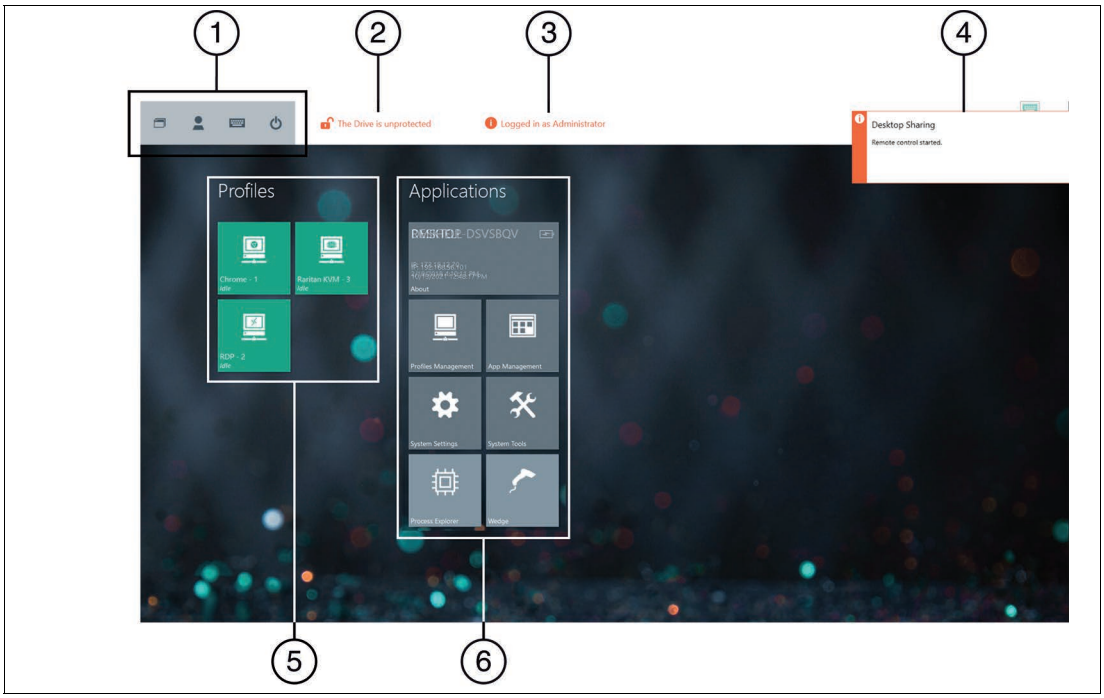


Abbildung 4.1 RM Shell 5-Startbildschirm

Nr.	Beschreibung
1	Systemfunktionen
2	Unified Write Filter-Status
3	Informationen zur Benutzerrolle
4	Aktuelle Meldungen
5	Profile
6	Anwendungen

1. Systemfunktionen

Symbol	Beschreibung
	RM Shell Task Switcher Mit dem RM Shell Task Switcher können Sie zwischen geöffneten Verbindungsprofilen und Anwendungen auf einem RM/BTC umschalten. Um den Task Switcher zu öffnen, klicken Sie auf das Symbol oder drücken Sie die Tastenkombination STRG+Alt+SCROLL auf der Tastatur. Der Task Switcher zeigt ein Fenster mit einer Übersicht über alle offenen Remote-Verbindungen und -Apps an. Sie können dann die Anwendung wechseln, indem Sie eine der angezeigten Remote-Verbindungen oder Apps auswählen. Mit den Zifferntasten 1 bis 9 können Sie innerhalb der Profile wechseln. Klicken Sie auf 0, um zum Startbildschirm von VisuNet RM Shell zurückzukehren.
	Benutzerrolle wechseln Wählen Sie zwischen Bediener, Ingenieur oder Administrator

2024-01

Symbol	Beschreibung
	Touchscreen-Tastatur Zeigt die Touchscreen-Tastatur auf dem Bildschirm an.
	Vorkonfigurierte Netzschalteroptionen wie z. B.: • Protect disk and restart (Festplatte schützen und neu starten) • Restart (Neustart) • Shutdown (Herunterfahren) (Für einige Geräte ist ein Strom Reset erforderlich, damit sie neu starten können) • Turn off display (Display ausschalten) Die Netzschalteroptionen können von den Benutzerrollen Ingenieur und Administrator festgelegt werden. Die Benutzerrolle "Operator“ (Bediener) darf nur die vorkonfigurierten Optionen durchführen.

2. Unified Write Filter-Status

In diesem Bereich des Startbildschirms wird angezeigt, ob der Unified Write Filter (einheitliche Schreibfilter) aktiviert ist. Weitere Informationen zum Unified Write Filter finden Sie unter siehe Kapitel 4.1.

3. Informationen zur Benutzerrolle

Wenn ein Administrator oder Ingenieur angemeldet ist, wird die angemeldete Benutzerrolle oben auf dem Startbildschirm angezeigt. Wenn ein Bediener angemeldet ist, werden diese Informationen nicht angezeigt.

4. Aktuelle Meldungen

In der oberen rechten Ecke des Startbildschirms werden aktuelle Fehlermeldungen oder Statusinformationen angezeigt, wenn bestimmte Ereignisse auftreten. Klicken Sie auf die aktuellen Meldungen, um sie zu entfernen. Die Meldungen werden nach 30 Sekunden automatisch ausgeblendet.

5. Profile

In diesem Abschnitt werden alle lokal erstellten Profile angezeigt. Jedes Profil wird durch eine Kachel dargestellt, die den Profiltyp (z. B. "RDP“, "VNC“), den Profilnamen (z. B. "RDP - 2“) und den Verbindungsstatus (z. B. "connected“ (verbunden), "disconnected“ (getrennt)) anzeigt.

Die folgenden Symbole geben die verschiedenen Profiltypen an:

RDP	
Desktop Sharing[1]	
VNC	

Web Browser URL (Webbrowser-URL) (Chrome)[1]	
Web browser URL (Webbrowser-URL) (IE)[1]	
Raritan KVM[1]	

1. PRO-Lizenz zum Entsperren der Funktion erforderlich

Profilstatusinformationen werden in der linken unteren Ecke der Profilkacheln angezeigt:

Status	Beschreibung	
Idle (Inaktiv)	Der anfängliche Status, nachdem ein Profil erstellt wurde	
Getrennt	Das Profil ist nicht mit einem Host verbunden	
Connected	Das Profil ist mit einem Host-PC verbunden. Es ist eine grüne Statusleiste oben in der Profil-Kachel sichtbar.	
Connection failed (Verbindung fehlgeschlagen)	Beim Versuch, eine Verbindung herzustellen, ist ein Fehler aufgetreten	
Auto connect (Automatische Verbindung)	Wenn die automatische Verbindung aktiviert ist, wird ein definiertes Profil automatisch mit einem Host verbunden. Die verbleibenden Sekunden vor dem nächsten Verbindungsversuch werden in der rechten oberen Ecke der Profilkachel angezeigt. Gleichzeitig ist eine animierte weiße Statusleiste über der Profilkachel sichtbar. Weitere Informationen zur automatischen Verbindung finden Sie unter siehe Kapitel 6.1.	

6. Anwendungen

In diesem Abschnitt werden alle Anwendungen angezeigt. Die Informationen und Funktionen, auf die in diesem Abschnitt zugegriffen werden kann, hängen von der angemeldeten Benutzerrolle ab:

Benutzerrolle	Beschreibung
Bediener	Zugriff auf Profile (wenn nicht durch eine vorkonfigurierte automatische Verbindung eingeschränkt). Kein Zugriff auf Systemeinstellungen oder Anwendungen.
Engineer	Zugriff auf Profile, Systemeinstellungen und Anwendungen (Erstellen, Bearbeiten und Löschen von Profilen).
Administrator	Uneingeschränkter Zugriff auf Profile, Systemeinstellungen, Anwendungen und Windows® Explorer.

4.1 Unified Write Filter

Der "Unified Write Filter“ (UWF, einheitlicher Schreibfilter) schützt das System vor einer persistenten Speicherung von Malware und Viren. Wenn der UWF aktiviert ist, wird die Systemfestplatte gesperrt und alle Systemänderungen werden nur im Cache gespeichert. Beim Neustart des Dateisystems wird der Cache gelöscht und die ursprüngliche Konfiguration wird erneut geladen.

Um eine Konfiguration dauerhaft zu speichern, müssen Sie den UWF deaktivieren und das System neu starten. Nach der Implementierung der Konfiguration aktivieren Sie den UWF und starten Sie den Computer erneut. Dadurch wird die persistente Speicherung der Konfiguration ausgelöst.

Vorsicht!

Rund-um-die-Uhr-Betrieb

Bei Rund-um-die-Uhr-Betrieb und aktiviertem UWF kann der Speicher des Systems knapp werden. Aktivieren Sie den automatischen Neustart.

Vorsicht!

Windows Swap File (Windows-Auslagerungsdatei)

Nachdem der Schreibfilter deaktiviert wurde, wird "Windows Swap File“ (Windows-Auslagerungsdatei) ebenfalls deaktiviert. Dadurch erhöht sich das Risiko, dass bei Rund-um-die-Uhr-Betrieb nicht genügend Speicher verfügbar ist, selbst wenn der UWF deaktiviert ist.

Die Auslagerungsdatei sollte daher nach dem Deaktivieren des Schreibfilters in den Windows®-Einstellungen wieder aktiviert werden.

Hinweis!

Anwenderzugriff auf den UWF

Nur Anwender, die als "Engineer“ (Ingenieur) oder "Administrator“ angemeldet sind, können den UWF aktivieren und deaktivieren.

Hinweis!

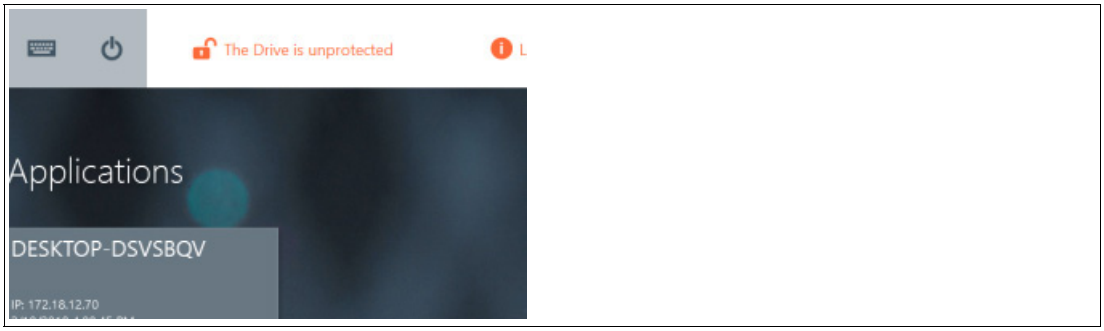
Software von Drittanbietern

Überprüfen Sie bei der Verwendung von Software von Drittanbietern (z. B. Antivirensoftware), ob die Software mit dem UWF kompatibel ist und keine großen Datenmengen auf die Festplatte schreibt.

Aktivieren und Deaktivieren des UWF

1. Klicken Sie auf das Netzsymbol in der oberen linken Ecke des VisuNet RM Shell-Startbildschirms.  .
2. Wählen Sie **Protect Disk and Restart** (Festplatte schützen und neu starten) bzw. **Unprotect Disk and Restart** (Festplattenschutz aufheben und neu starten) aus, um den UWF zu aktivieren bzw. zu deaktivieren.

   ↳ Nach dem Neustart wird die Änderung wirksam. Ein Symbol oben auf dem Startbildschirm zeigt an, ob der UWF aktiviert ist.



5 App "About“ (Info)

Die erste Kachel im Anwendungsbereich auf dem Startbildschirm ist die App "About“ (Info). Diese Kachel bietet Ihnen einen kurzen Überblick über Systeminformationen.

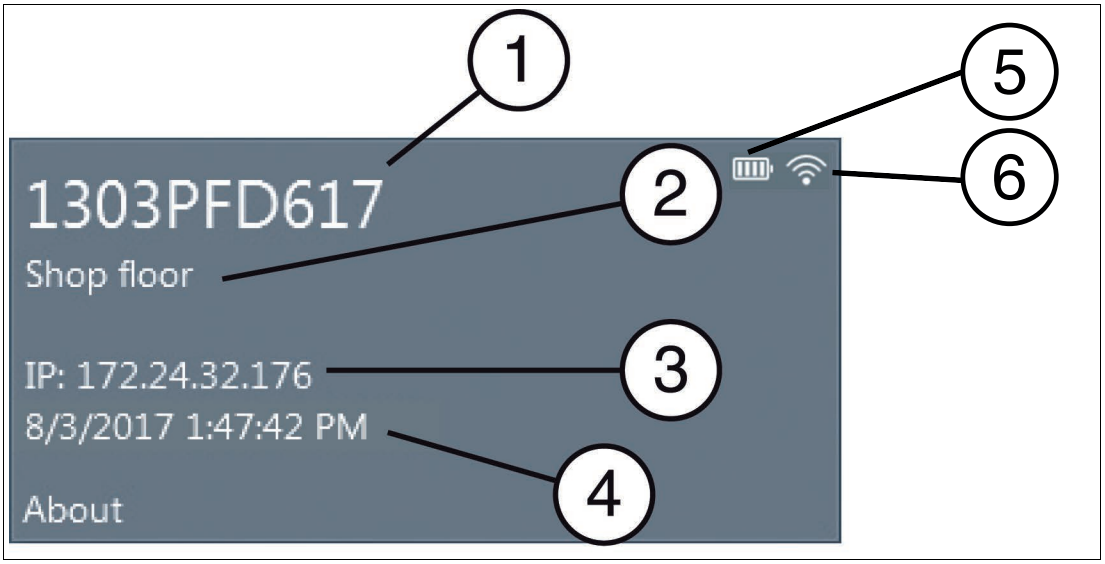


Abbildung 5.1 Die Kachel "About“ (Info) auf dem Startbildschirm

Nr.	Beschreibung
(1)	Computername des RM/BTC, siehe Kapitel 8.1
(2)	Beschreibung des RM/BTC, siehe Kapitel 8.1
(3)	IP-Adresse des RM/BTC, siehe Kapitel 8.8
(4)	Aktuelles Datum und Uhrzeit, siehe Kapitel 8.1
(5)	Batteriestatus (Status wird angezeigt, wenn Sie mit der Maus über das Symbol fahren)
(6)	Wi-Fi™-Status (nur verfügbar, wenn VisuNet RM Shell auf Pad-Ex® installiert ist)

Klicken Sie auf die Kachel "About“ (Info), um weitere Informationen aufzurufen.

Nachdem Sie auf die Kachel geklickt haben, werden in der Navigationsleiste 5 Untermenüs angezeigt:

- Pepperl+Fuchs SE – Dieses Untermenü enthält Informationen zur Pepperl+Fuchs Group
- DRDC information (DRDC-Informationen) – weitere Informationen finden Sie in unserem RM Shell DRDC-Handbuch unter pepperl-fuchs.com/hmi
- (Untermenü für GXP-spezifische Informationen),
- Hardware,
- Lizenzen, siehe Kapitel 5.2
- Software,
- Touch

5.1 Hardware

Dieses Untermenü enthält Informationen zu den integrierten Hardwarekomponenten ("Processor“ (Prozessor), "Chipset“ (Chipsatz), "Installed RAM“ (Installierter RAM), "Last boot up time“ (Letzte Startzeit)) und zu "Serial Number“ (Seriennummer) von VisuNet RM Shell.

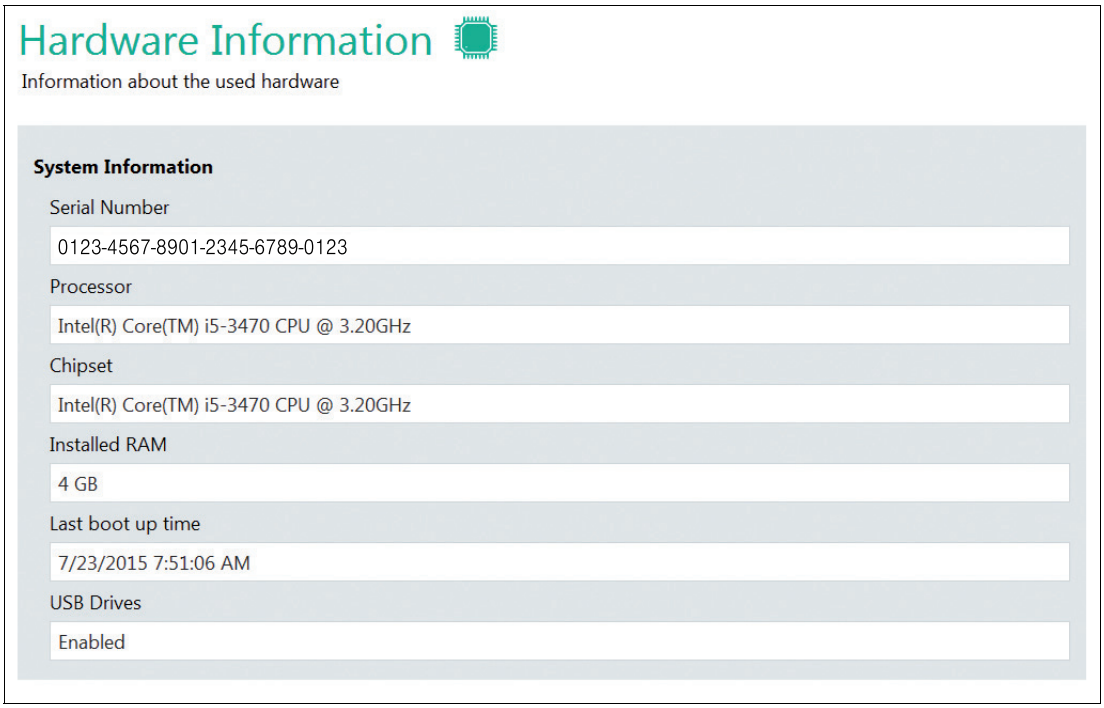


Abbildung 5.2 Informationen über die Systemhardware

5.2 Lizenzen und Nutzungsbedingungen

Dieses Untermenü enthält Lizenzinformationen zu RM Shell und Komponenten von Drittanbietern.

Weitere Informationen zur Pepperl+Fuchs Endbenutzer-Lizenzvereinbarung finden Sie unter siehe Kapitel 12.3.

5.3 Softwareinformation

Dieses Untermenü enthält Informationen zur "RM Shell“-Version, zum "Betriebssystem“ (Operating System), "Systemstatus“ (System Status) und den "geladenen Baugruppen“ (Loaded Assemblies).

Die aktuelle Version von VisuNet RM Shell kann bei der Aktualisierung der Firmware nützlich sein. Die anderen Informationen können für den technischen Support erforderlich sein.

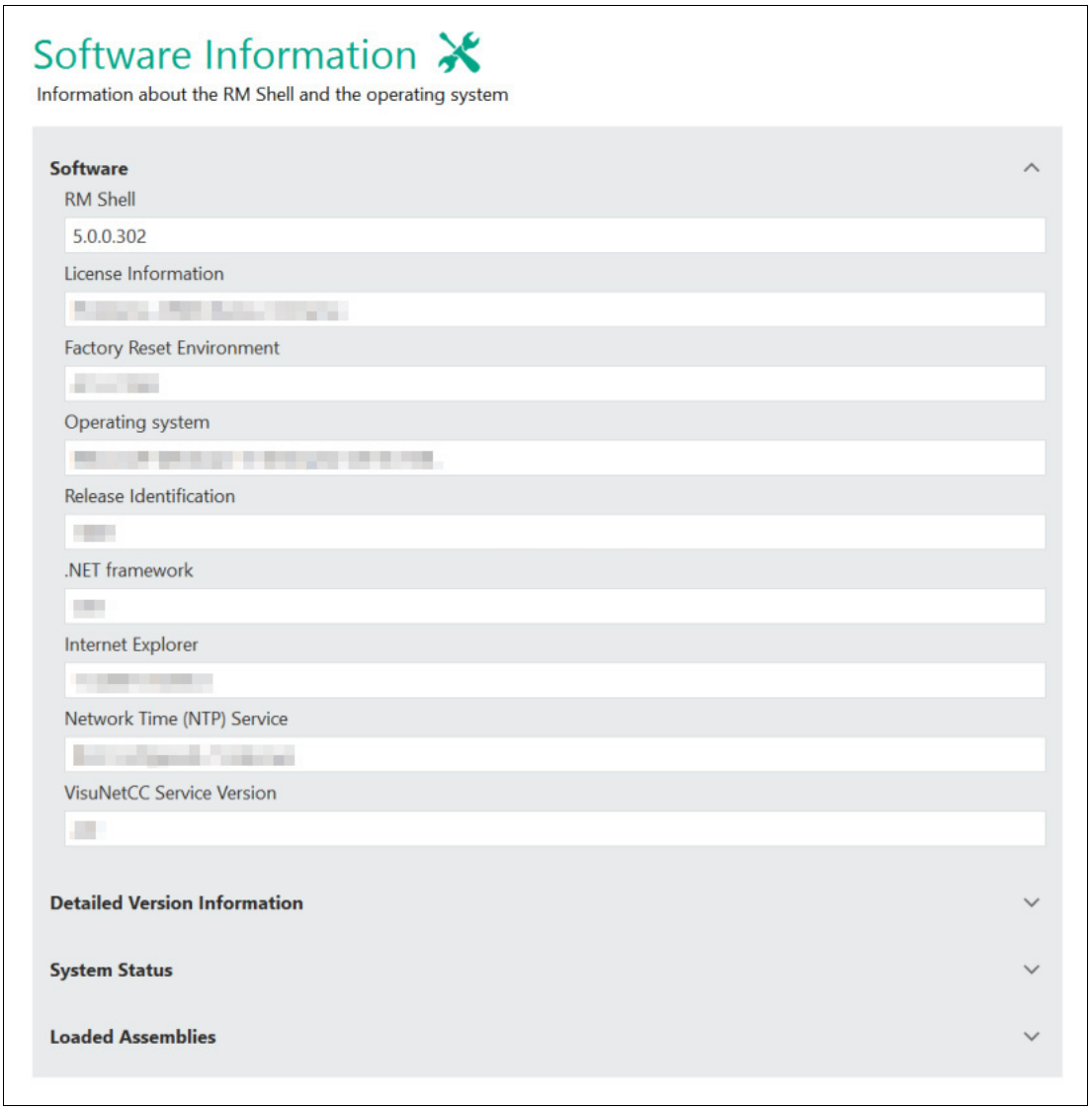


Abbildung 5.3 Software-Informationen

6 Profilverwaltungs-App

Erstellen und verwalten Sie entfernte "Connection Profiles“ (Verbindungsprofile) mit der App "Profiles Management“ (Profilverwaltung).

VisuNet RM Shell enthält keine vorab erstellten Verbindungsprofile. Aus diesem Grund ist die Profilliste leer, wenn Sie VisuNet RM Shell zum ersten Mal starten.

Hinweis!

Deaktivieren des Schreibfilters für die persistente Speicherung von Konfigurationen

Um Konfigurationsänderungen persistent zu speichern, deaktivieren Sie den Unified Write Filter (UWF). Nachdem Sie die Konfigurationsänderungen implementiert haben, aktivieren Sie den UWF erneut, um die Änderungen persistent zu speichern.

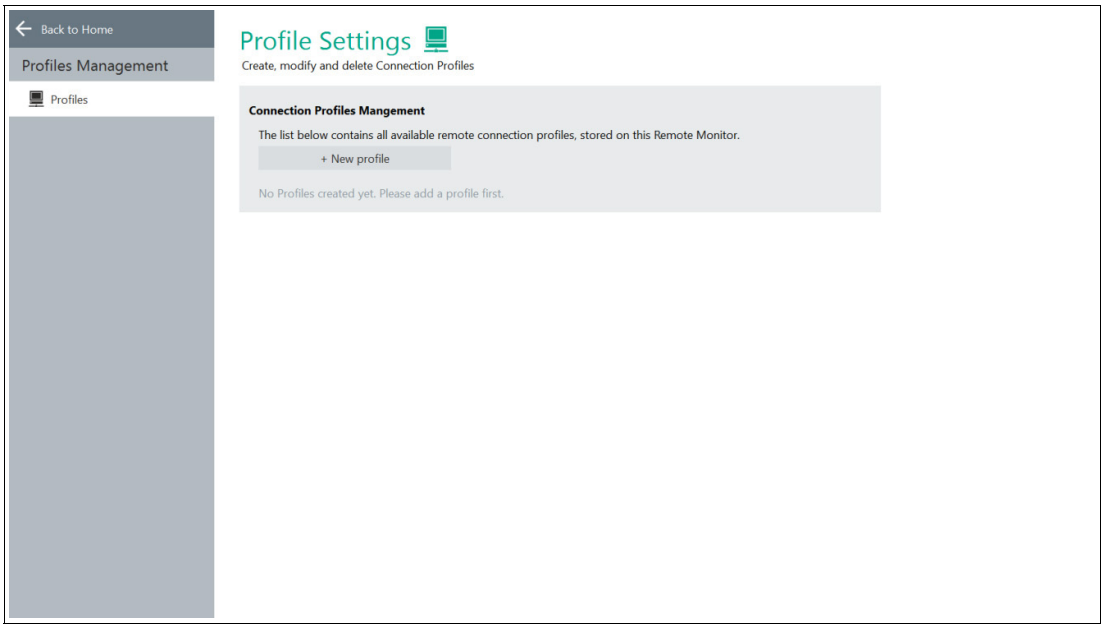
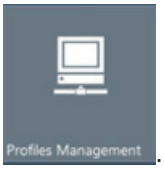


Abbildung 6.1 Startbildschirm Profilverwaltung. Zunächst ist die Profilliste leer.

Öffnen der Profilverwaltungs-App

1. Um die App "Profiles Management“ (Profilverwaltung) zu öffnen, klicken Sie auf dem Startbildschirm auf das entsprechende Symbol. 

.

Erstellen eines neuen Verbindungsprofils

1. Um ein neues Verbindungsprofil zu erstellen, klicken Sie auf + New profile.
2. Wählen Sie den gewünschten Verbindungstyp für das Profil aus, und klicken Sie auf **OK**. [1]

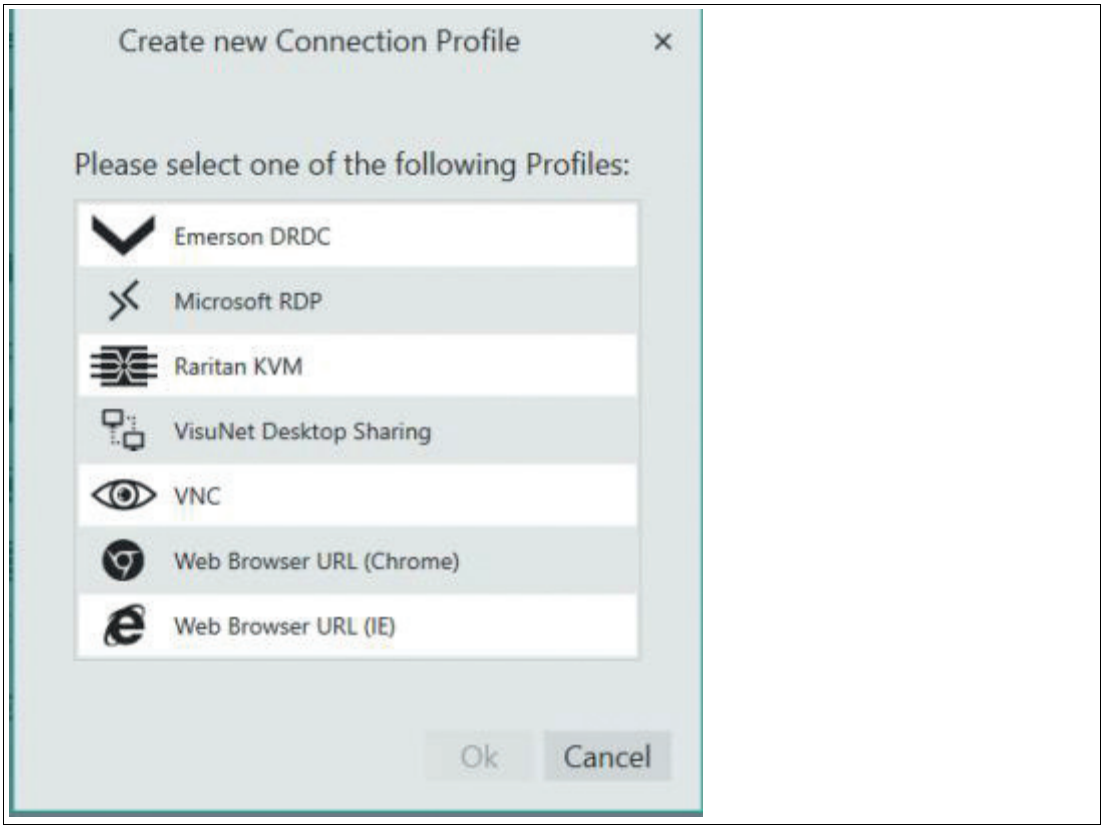


Abbildung 6.2 Das Dialogfenster "Create new Connection Profile“ (Neues Verbindungsprofil erstellen)

↳ Das ausgewählte Verbindungsprofil wird erstellt. Die Haupteinstellungen des neuen Profils werden geöffnet.

1. Webbrowser-, Raritan KVM- und VisuNet Desktop Sharing-Profile sind nur in der Pro-Version verfügbar

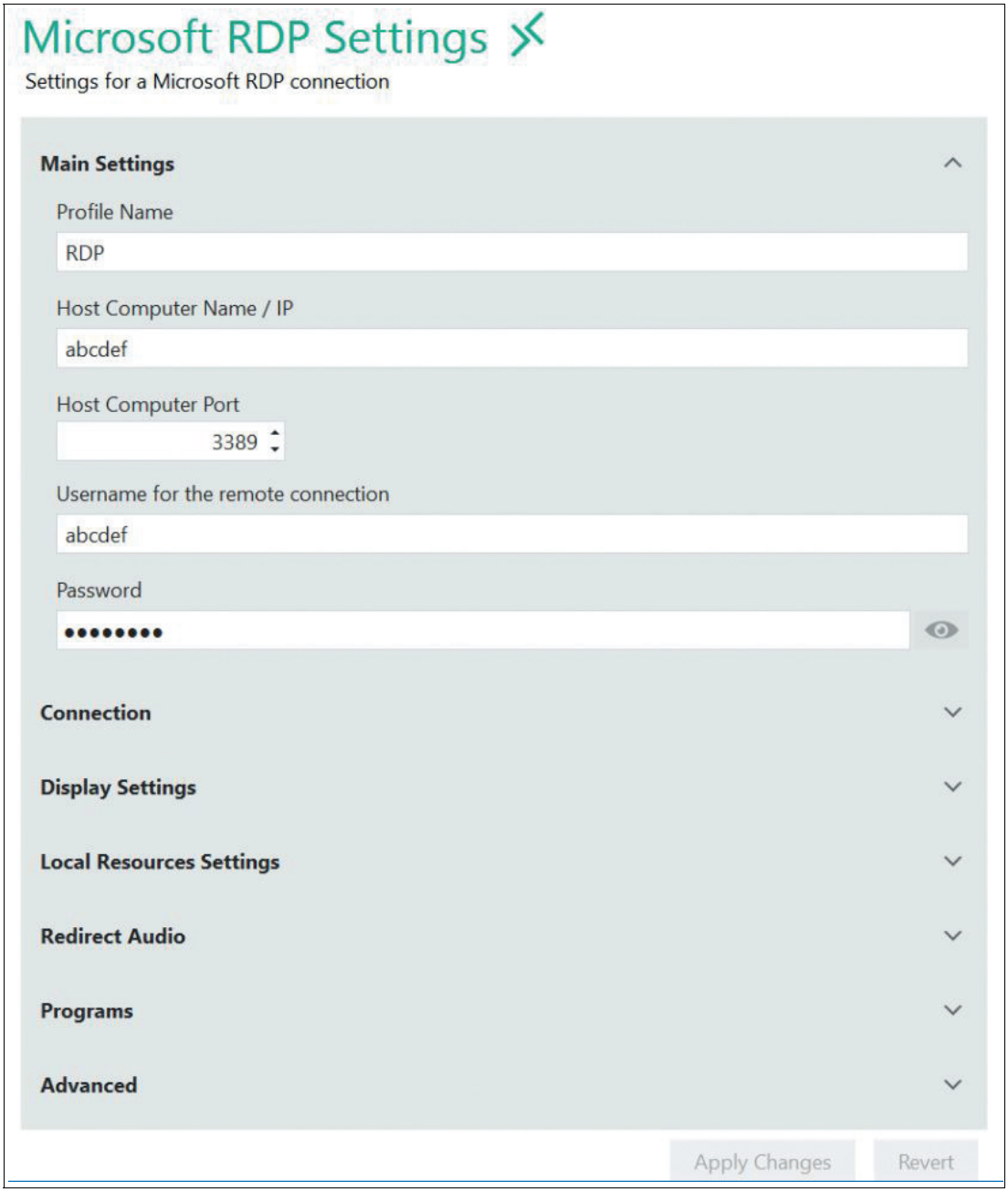


Abbildung 6.3 Die wichtigsten Einstellungen in einem Microsoft RDP-Profil

Bearbeiten der Profileinstellungen

1. Gehen Sie zu "Profile Settings“ (Profil-Einstellungen).
2. Um die Einstellungen eines Profils zu bearbeiten, doppelklicken Sie auf den gewünschten Profileintrag in der Liste der Profile oder klicken Sie auf .
3. Die Einstellungen variieren je nach dem gewählten Verbindungstyp. Nach der Bearbeitung der Einstellungen klicken Sie auf Apply Changes.

   ↳ Die Änderungen wurden gespeichert.

2024-01

Hinweis!

Verwenden Sie die Schaltfläche "Advanced“ (Erweitert), damit Sie zu den entsprechenden Windows®-Einstellungen weitergeleitet werden

Tipp

Verwenden Sie die zusätzliche Software VisuNet Control Center, um Profile einfach zu kopieren und einzufügen oder sogar ein Gerät mit unterschiedlichen Profilen und Profileinstellungen auf mehreren Geräten im Netzwerk zu klonen. Weitere Informationen zu VisuNet CC finden Sie unter pepperl.fuchs.com

6.1 Verbindungsfunktionen

Sie können für jedes Profil in der Profilliste 3 zusätzliche Funktionen einrichten.

- Auto Connect (Automatische Verbindung)
- Retry (Wiederholen)
- Backup Connection (Backup-Verbindung)

Die Funktion "Auto Connect“ (Automatische Verbindung)

Wenn Sie eine automatische Verbindung zu einem bestimmten Profil wünschen, verwenden Sie die Funktion "Auto Connect“ (Automatische Verbindung). RM Shell stellt automatisch nach einer voreingestellten Zeit eine Verbindung zum ausgewählten Profil her.

Einrichten der "Auto Connect“ (Automatische Verbindung)

1. Gehen Sie zu "Profile Settings“ (Profil-Einstellungen).
2. Klicken Sie zum Einrichten der automatischen Verbindung für ein Profil auf  .

   ↳ Das Dialogfenster "Connection Features“ (Verbindungsfunktionen) wird geöffnet.
3. Klicken Sie auf das Feld "Enable Auto Connect“ (Automatische Verbindung aktivieren).

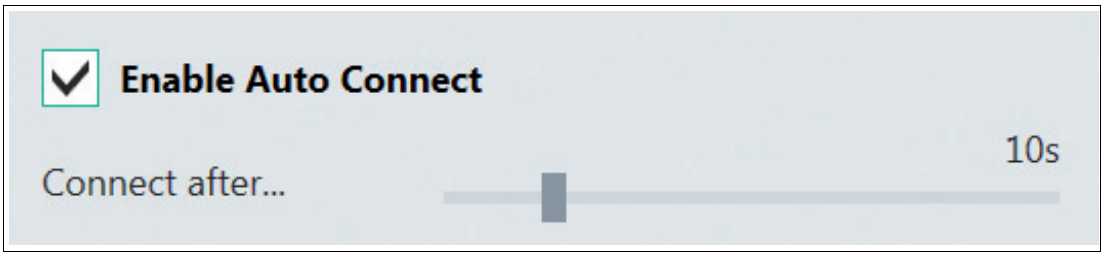


Abbildung 6.4 Optionen des automatischen Verbindungsaufbaus

4. Stellen Sie mit dem Schieberegler die Zeit ein, nach der VisuNet RM Shell automatisch eine Verbindung zum gewünschten Profil aufbaut.
5. Klicken Sie auf "OK“.

   ↳ Damit ist die automatische Verbindung vorkonfiguriert. Die Profilliste wird angezeigt.

Abbildung 6.5 Profil mit vorkonfigurierter automatischer Verbindung (wie in der Profilliste gezeigt): in diesem Beispiel stellt die VisuNet RM Shell nach 10 Sekunden automatisch eine Verbindung zum Profil "RD – 2“ her.

Hinweis!

Wenn Ihr Bediener nicht auf die RM Shell-Schnittstelle zugreifen soll, können Sie "Connect after...“ (Verbinden nach...) auf 0 Sekunden setzen. Das entsprechende Profil stellt sofort nach dem Booten des RM/BTC automatisch eine Verbindung her, ohne dass der RM Shell-Startbildschirm angezeigt wird.

Funktion "Retry“ (Wiederholen)

Falls die Verbindung zu einem Host verloren geht, versucht die Funktion "Retry“ (Wiederholen), die Verbindung zum Host wiederherzustellen. Sie können sowohl eine begrenzte Anzahl an Wiederholungen als auch die Zeit dazwischen angeben.

Einrichtung der Funktion "Retry“ (Wiederholen)

1. Gehen Sie zu "Profile Settings“ (Profil-Einstellungen).
2. Um die Funktion "Retry“ (Wiederholen) für ein Profil einzurichten, klicken Sie auf  .

   ↳ Das Dialogfenster "Connection Features“ (Verbindungsfunktionen) wird geöffnet.
3. Klicken Sie auf das Feld "Enable Retry“ (Wiederholen aktivieren).

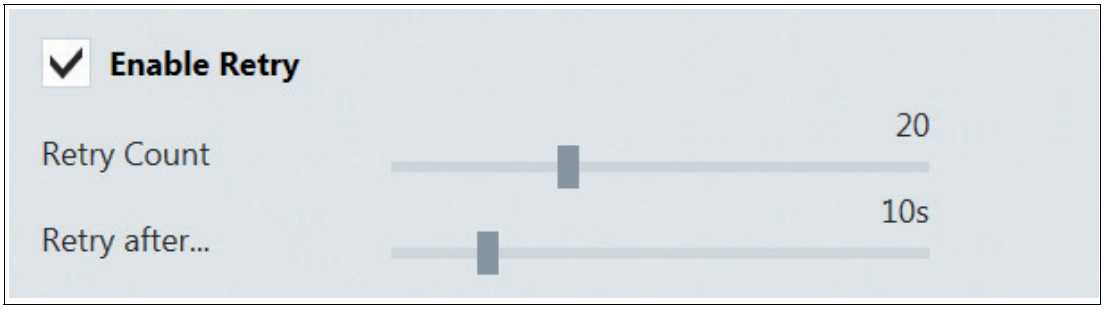


Abbildung 6.6 Wiederholungsoptionen

4. Verwenden Sie den Schieberegler "Retry Count“ (Anzahl Wiederholungen), um die Anzahl der Wiederholungen anzupassen.
5. Verwenden Sie den Schieberegler "Retry after...“ (Wiederholen nach...), um die Zeit zwischen den Wiederholungen anzupassen. Der Standardwert ist 10 Wiederholungen mit einer Pause von 10 Sekunden zwischen den einzelnen Wiederholungen.
6. Klicken Sie auf "OK“.

   ↳ Damit ist die Funktion "Retry“ (Wiederholen) eingerichtet. Die Profilliste wird angezeigt.

Funktion "Backup Connection“ (Backup-Verbindung)

Falls die Verbindung zum Host verloren geht und durch die Funktion "Retry“ (Wiederholen) nicht wieder hergestellt werden kann, können Sie ein anderes Profil als Backup einrichten.

Einrichtung der "Backup Connection“ (Backup-Verbindung)

1. Gehen Sie zu "Profile Settings“ (Profil-Einstellungen).
2. Zum Einrichten der Funktion "Backup Connection“ (Backup-Verbindung) für ein Profil klicken Sie auf  .

   ↳ Das Dialogfenster "Connection Features“ (Verbindungsfunktionen) wird geöffnet.
3. Klicken Sie auf das Feld "Enable Backup Connection“ (Backup-Verbindung aktivieren).

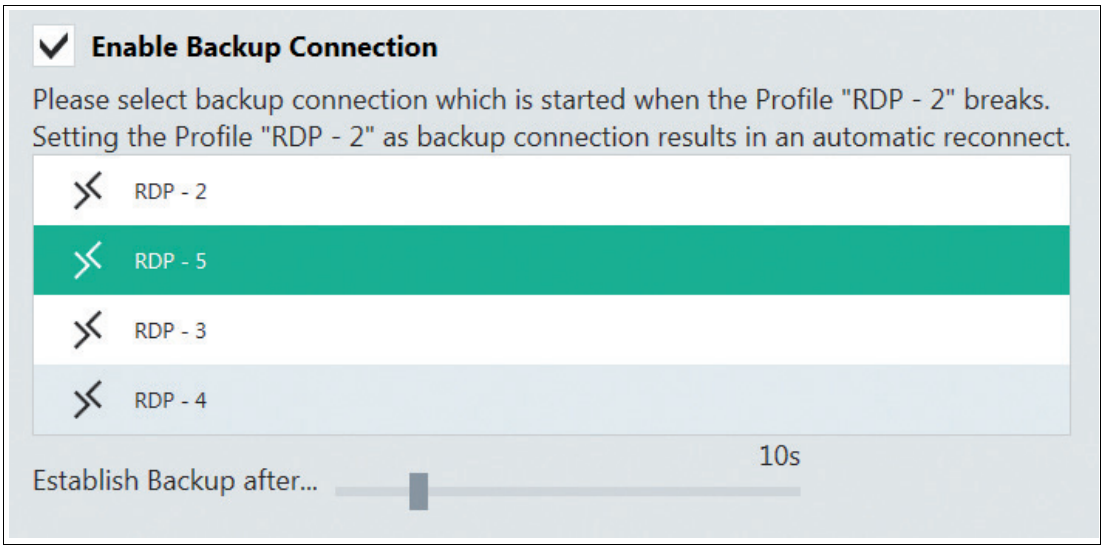


Abbildung 6.7 Backup-Verbindungsmöglichkeiten

4. Wählen Sie aus der Liste ein Backup-Profil aus, das gestartet wird, wenn die Verbindung mit dem ausgewählten Profil fehlschlägt.
5. Mit dem Schieberegler "Establish Backup after...“ (Backup herstellen nach...) stellen Sie die Zeit ein, nach der das Backup-Profil eine Verbindung zum Host herstellt.
6. Klicken Sie auf "OK“.

   ↳ Damit ist die Backup-Verbindung eingerichtet. Die Profilliste wird angezeigt.

Beispiel 1 – Kontinuierliche Verbindung zu einem bestimmten Host (über die Funktion "Backup Connection“ (Backup-Verbindung))

In diesem Beispiel stellt der RM/BTC automatisch eine Verbindung zu einem vordefinierten Host A her. Wenn die Verbindung fehlschlägt, versucht der RM/BTC kontinuierlich, die Verbindung zu Host A wiederherzustellen.

Anwendungsfall: Wenn Sicherheits- oder Software-Updates auf dem Hostsystem installiert sind und der Host neu gestartet werden muss, stellt diese Funktion sicher, dass der RM/BTC beim Neustart automatisch wieder eine Verbindung zum Host herstellt.

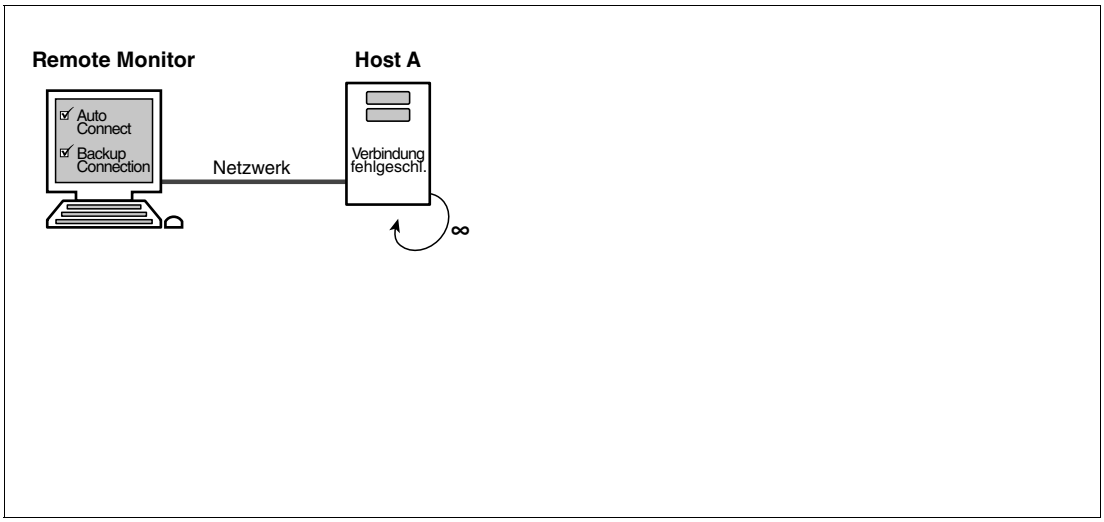
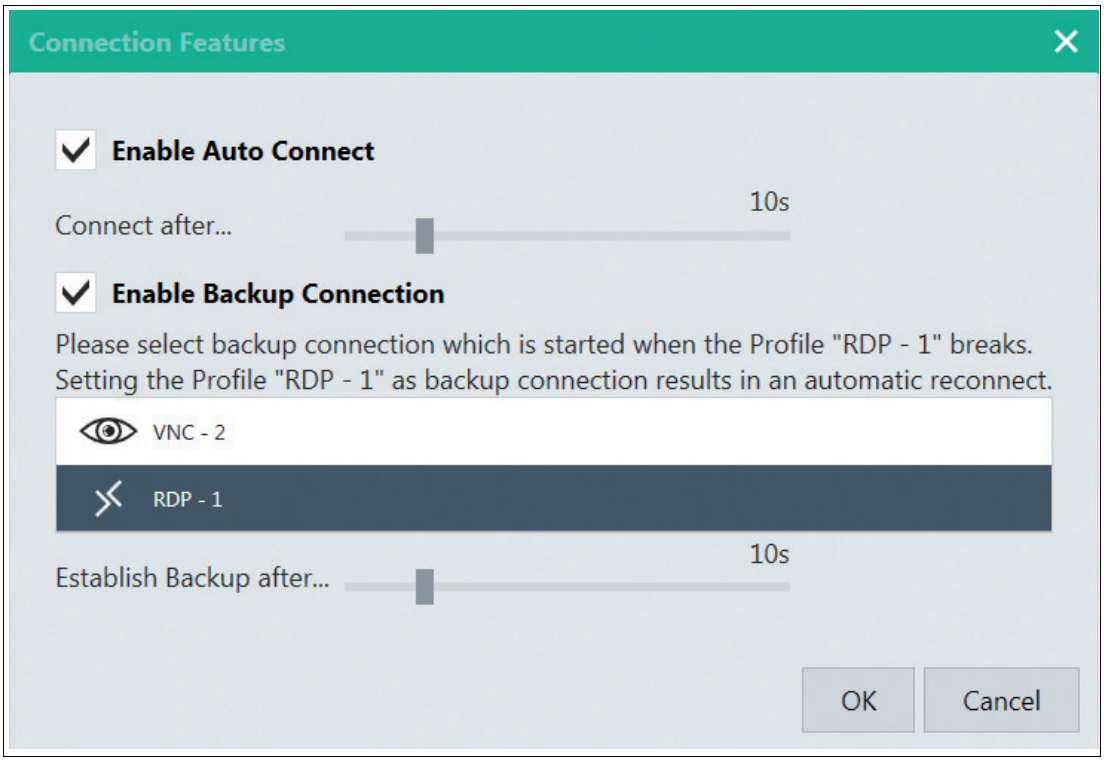


Abbildung 6.8 Beispiel 1: Unbegrenzte Anzahl von Wiederholungen zu einem bestimmten Host (mit der Funktion "Backup Connection (Backup-Verbindung)“

Einrichtung einer kontinuierlichen Verbindung zu einem bestimmten Host

1. Gehen Sie zur Profilverwaltung von RM Shell, wählen Sie das Profil, für das Sie unbegrenzte Verbindungswiederholungen einrichten möchten, aus und klicken Sie auf  .
2. Aktivieren Sie die Funktion "Auto Connect“ ("Automatische Verbindung“).
3. Stellen Sie mit dem Schieberegler die Zeit ein, nach der VisuNet RM Shell automatisch eine Verbindung zum angeforderten Profil aufbaut.
4. Aktivieren Sie die Funktion "Backup Connection“ (Backup-Verbindung).



5. Wählen Sie das gleiche Profil als Backup-Profil aus (in diesem Fall "RDP – 1“).
6. Klicken Sie auf "OK“, um die Änderungen zu speichern und zur Profilliste zurückzukehren.

Beispiel 2 – Kontinuierliche Verbindung zu mehr als einem Host (über die Funktion "Backup Connection“ (Backup Verbindung))

In diesem Beispiel stellt der RM/BTC automatisch eine Verbindung zu einem vordefinierten Host A her. Wenn die Verbindung fehlschlägt, versucht der RM/BTC nach einer vordefinierten Wartezeit, eine Verbindung zur Backup-Verbindung des Profils (in diesem Fall "Host B“) herzustellen. Wenn Host B ebenfalls nicht erreichbar ist, versucht der RM/BTC, eine Verbindung zur Backup-Verbindung des Profils von Host B (in diesem Fall "Host C“) herzustellen. Sie können ganz einfach "Schleifen“ für die Backup-Verbindungen Ihrer Profile definieren. In diesem Beispiel ist die Backup-Verbindung von Host C wieder Host A.

Anwendungsfall: Bei einer Infrastruktur mit redundanten Servern können Sie die RMs/BTCs so einrichten, dass sie eine Verbindung zu einem Backup-Server herstellen, wenn der Hauptserver ausfällt.

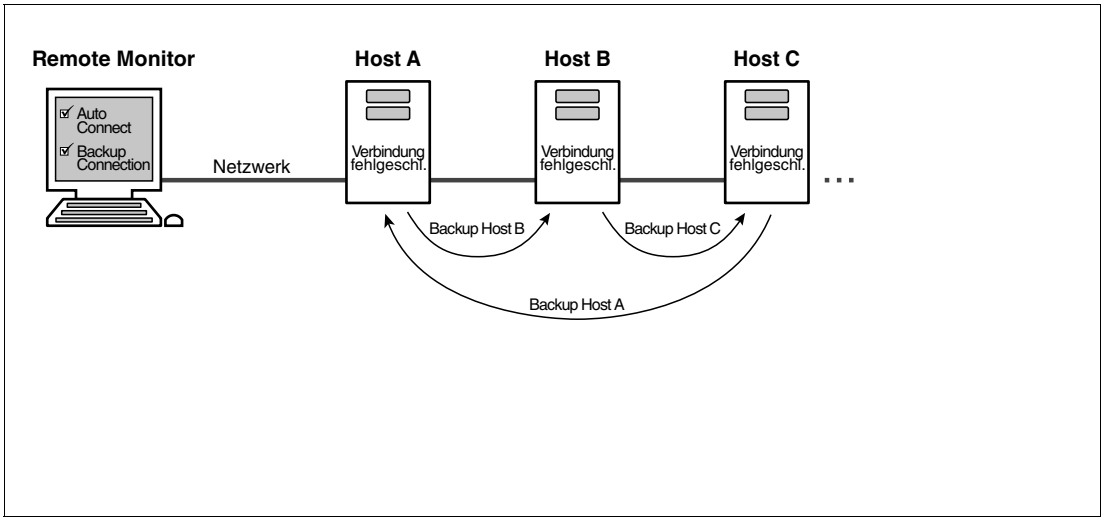
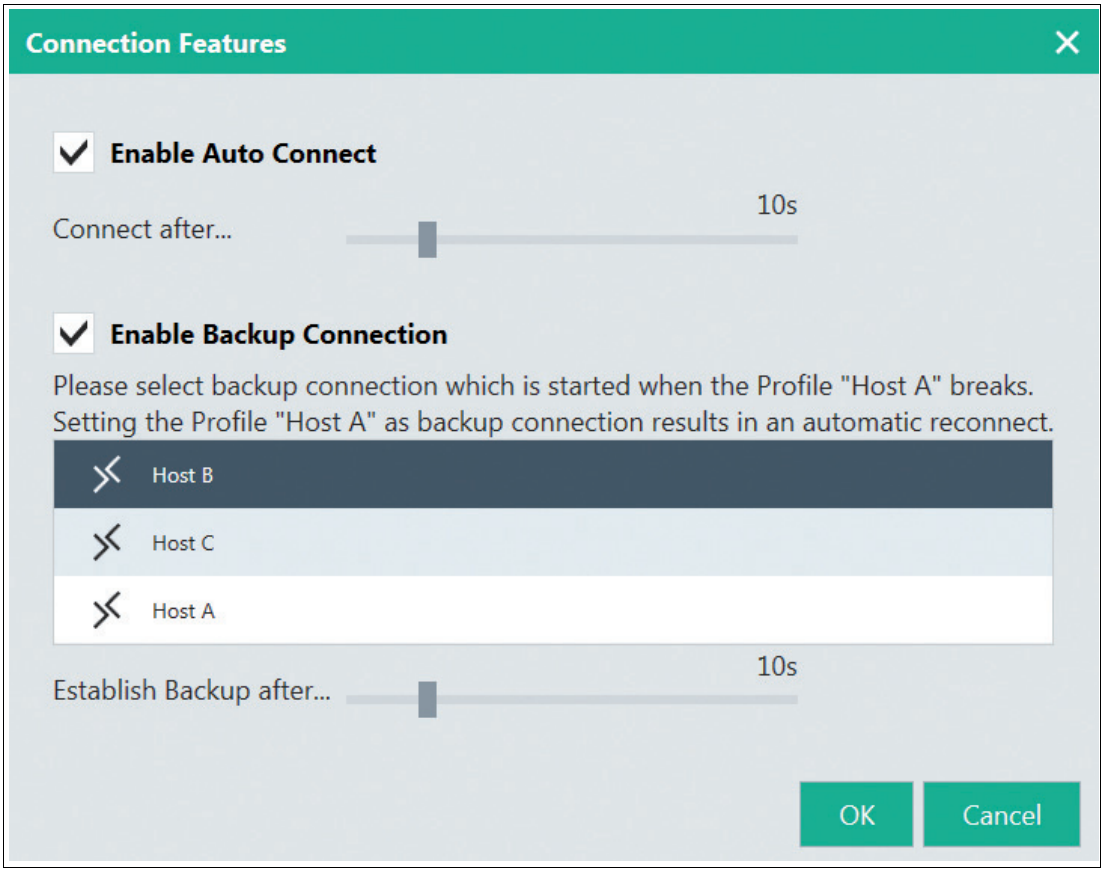


Abbildung 6.9 Beispiel 2: Unbegrenzte Anzahl von Wiederholungsversuchen für die Verbindung zu mehr als einem Host (über die Funktion "Backup Connection (Backup Verbindung)“)

Einrichtung einer kontinuierlichen Verbindung zu mehr als einem Host

1. Gehen Sie zur Profilverwaltung von RM Shell, wählen Sie das Profil, das Sie einrichten möchten (z. B. "Host A“) aus, und klicken Sie auf .
2. Aktivieren Sie die Funktion "Auto Connect“ ("Automatische Verbindung“).
3. Stellen Sie mit dem Schieberegler die Zeit ein, nach der RM Shell automatisch eine Verbindung zum angeforderten Profil aufbaut.
4. Aktivieren Sie die Funktion "Backup Connection“ (Backup-Verbindung).
5. Wählen Sie das erste Backup-Profil (in diesem Fall "Host B“) aus.



6. Klicken Sie auf "OK“, um die Änderungen zu speichern und zur Profilliste zurückzukehren.
7. Gehen Sie zur Profilverwaltung von RM Shell, wählen Sie das erste Backup-Profil, das Sie einrichten möchten (z. B. "Host B“) aus, und klicken Sie auf .
8. Aktivieren Sie die Funktion "Backup Connection“ (Backup-Verbindung).
9. Wählen Sie das zweite Backup-Profil (in diesem Fall "Host C“) aus.
10. Wiederholen Sie die obigen Schritte für alle Backup-Profile, die Sie einrichten möchten.
11. Definieren Sie als Backup-Profil für das "letzte“ Backup-Profil (in diesem Fall "Host C“) das ursprüngliche Profil (in diesem Fall "Host A“), um sicherzustellen, dass die Verbindungswiederherstellung erneut startet, wenn die Verbindung ausgefallen ist.
12. Klicken Sie auf "OK“, um die Änderungen zu speichern und zur Profilliste zurückzukehren.

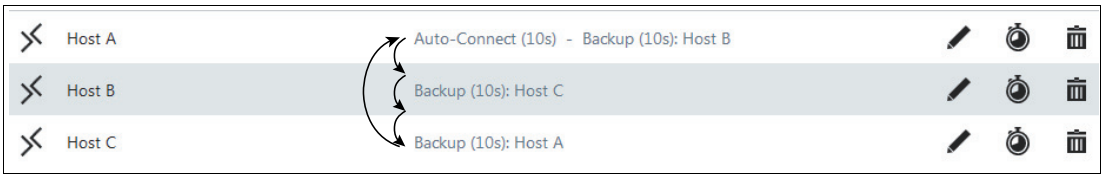


Abbildung 6.10 Profile mit Backup-Verbindungen

Beispiel 3 – Begrenzte Anzahl an Wiederholungsversuchen für die Verbindung zum gleichen Host (über die Funktion "Retry“ (Wiederholen))

In diesem Beispiel stellt der RM/BTC automatisch eine Verbindung zu einem vordefinierten Host A her. Wenn die Verbindung fehlschlägt oder verloren geht, versucht der RM/BTC dreimal, die Verbindung zu Host A wiederherzustellen. Wenn die Verbindung nicht wiederhergestellt werden kann, stellt der RM/BTC nach dem dritten Versuch keine Verbindung zu Host A her. Nach dem dritten Fehlversuch kehrt der Benutzer automatisch zum RM Shell-Startbildschirm zurück.

Anwendungsfall: Hier kann der Benutzer manuell eine alternative Verbindung wählen, wenn die Hauptverbindung zu Host A fehlgeschlagen ist.

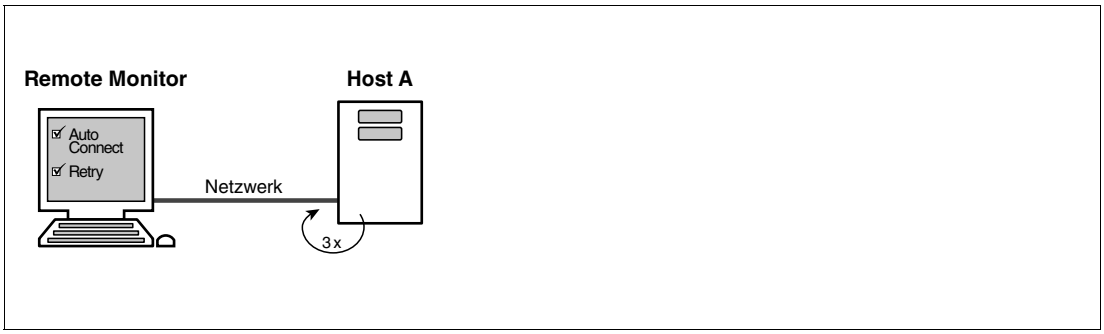


Abbildung 6.11 Beispiel 3: Begrenzte Anzahl von Wiederholungsversuchen für die Verbindung zum gleichen Host

Einrichtung einer begrenzten Anzahl an Wiederholungsversuchen für die Verbindung zum gleichen Host

1. Gehen Sie zur Profilverwaltung von RM Shell, wählen Sie das Profil, das Sie einrichten möchten, aus und klicken Sie auf  .
2. Stellen Sie mit dem Schieberegler die Zeit ein, nach der VisuNet RM Shell automatisch eine Verbindung zum angeforderten Profil aufbaut.
3. Aktivieren Sie die Funktion "Retry“ (Wiederholen).

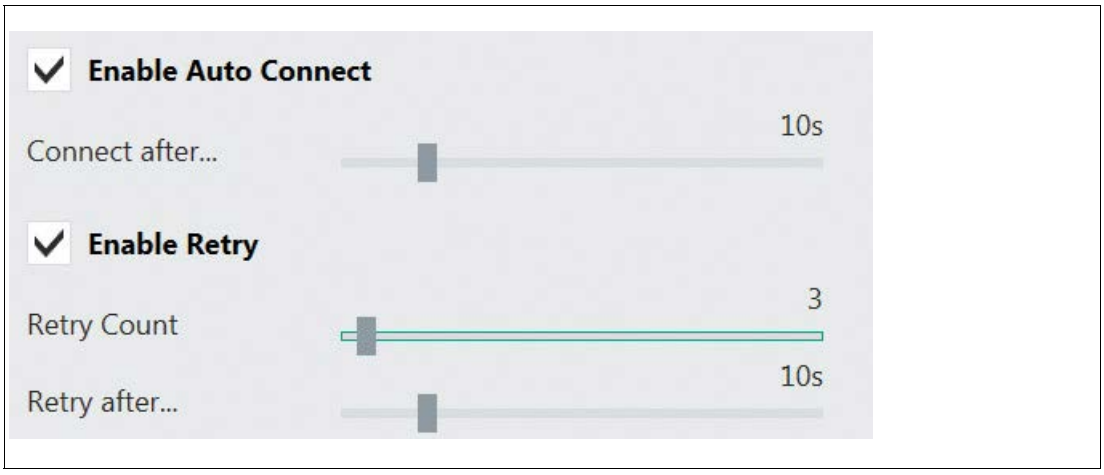


Abbildung 6.12 Entsprechende Einstellungen in VisuNet RM Shell (Profile settings – Connection features (Profileinstellungen – Verbindungsfunktionen))

4. Verwenden Sie den Schieberegler "Retry Count“ (Anzahl Wiederholungen), um die Anzahl der Wiederholungen anzupassen.

2024-01

5. Stellen Sie mit dem Schieberegler die Zeit ein, nach der VisuNet RM Shell automatisch versucht, die Verbindung zum Host wiederherzustellen.
6. Klicken Sie auf "OK", um die Änderungen zu speichern und zur Profilliste zurückzukehren.

6.2 RDP-Einstellungen

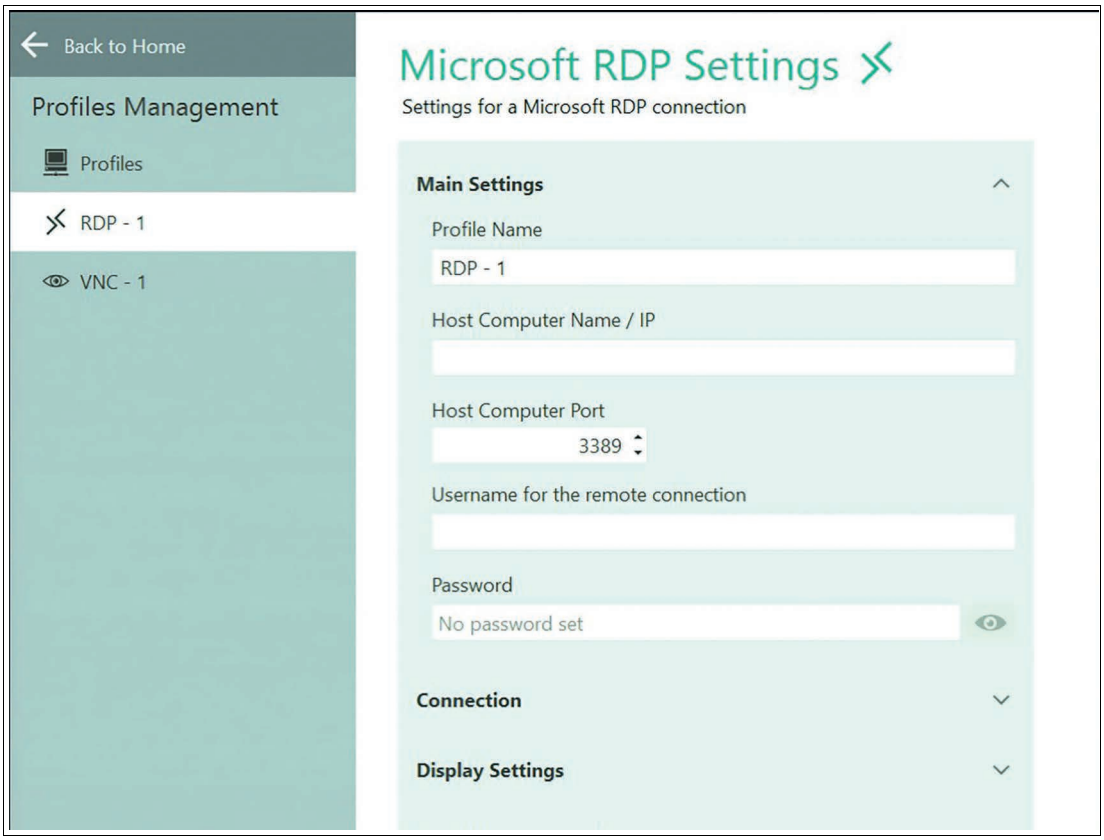
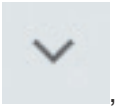


Abbildung 6.13

Die RDP-Einstellungen sind nach Typ gruppiert. Verwenden Sie das Symbol  , um die Abschnitte zu erweitern.

Main Settings (Grundlegende Einstellungen)

Option	Beschreibung
Profile Name (Profilname)	Ermöglicht Ihnen das Ändern des sichtbaren Namens des ausgewählten Profils.
Host Computer Name/IP (Name/IP-Adresse Host-Computer)	Dies kann der Netzwerkname für den Host oder seine IP-Adresse sein.
Host Computer Port (Port des Host-Computers)	Geben Sie den IP-Port des Hosts ein. Wir empfehlen die Verwendung der Standardeinstellung.
Username for remote connection (Benutzername für Remote-Verbindung)	Benutzername, der verwendet wird, um sich auf dem Host einzuloggen.
Kennwort	Kennwort, das benötigt wird, um sich auf dem Host einzuloggen.

Anschluss

Option	Beschreibung
Choose connection speed (Verbindungsgeschwindigkeit auswählen)	Hier wird nicht die Verbindungsgeschwindigkeit festgelegt, sondern die für diese Geschwindigkeit empfohlenen Einstellungen für die Benutzerschnittstelle (UI). Je nach gewählter Verbindungsgeschwindigkeit werden für den Host mehrere visuelle Effekte aktiviert oder deaktiviert. Die gewählte Geschwindigkeit kann möglicherweise die Leistung des RM/BTC beeinträchtigen.
Fast Disconnect Detection by sending Pings to Host Server (Schnelle Erkennung von Verbindungsunterbrechungen durch Senden von Pings an den Host-Server)	Wenn diese Option aktiviert ist, sendet der RM kontinuierlich Pings an den Host. Mögliche Verbindungsunterbrechungen werden viel schneller erkannt als üblich. Damit Sie diese Funktion verwenden können, muss der Host Pings akzeptieren.
Enable Auto-Reconnect of the RDP connection (disable Fast Disconnect Detection) (Automatische Wiederverbindung der RDP-Verbindung aktivieren (Fast Disconnect-Erkennung deaktivieren))	Aktivieren Sie diese Option, wenn Sie den integrierten RDP-Wiederverbindungsmechanismus nutzen möchten. Dieser Mechanismus versucht, eine Remote-Desktop-Verbindung wieder herzustellen, wenn sie gestört ist.
Send Keep Alive Telegrams to the RDP server (Senden von Keep-Alive-Telegrammen an den RDP-Server)	Diese Funktion erhält die Verbindung zwischen dem RM/BTC und dem Host aufrecht. Und zwar indem bei Inaktivität Nachrichten vom RM/BTC an den Host gesendet werden.
Enable Idle Timeout on the RDP server (Aktivieren von Idle-Timeout auf dem RDP-Server)	Aktivieren Sie diese Funktion, um ein Timeout zu aktivieren, nach dessen Ablauf bei Inaktivität der RM/BTC vom Host getrennt wird.
Enable Connect to Administrative Console Session ("Verbindung mit Administratorkonsolensitzung herstellen“ aktivieren)	Aktivieren Sie diese Einstellung, wenn Sie einen Server, der auf Windows® Server 2008 basiert, (mit oder ohne installiertem Terminal Server) per Fernzugriff verwalten möchten. Wenn Sie jedoch eine Verbindung herstellen, um einen auf Windows® Server 2008 basierten Server per Fernzugriff zu verwalten, auf dem der Rollendienst von Terminal Server nicht installiert ist, brauchen Sie den Schalter /admin nicht anzugeben. (In diesem Fall tritt mit oder ohne den Schalter /admin dasselbe Verbindungsverhalten auf.) Weitere Informationen finden Sie auf der folgenden Website: http://blogs.msdn.com/b/rds/archive/2007/12/17/changes-to-remote-administration-in-windows-server-2008.aspx
Block user from closing the connection (Anwender daran hindern, die Verbindung zu beenden)	Aktivieren Sie diese Option, um zu verhindern, dass ein Verbindungsfenster geschlossen wird.

Display Settings (Display-Einstellungen)

Option	Beschreibung
Fullscreen Mode (Vollbild-Modus)	Aktivieren Sie diese Option, um den Remote-Desktop in voller Größe anzuzeigen. Wenn Sie die Größe des Remote-Desktop-Bildschirms manuell konfigurieren möchten, deaktivieren Sie diese Option.
Remote Color Depth (Remote-Farbtiefe)	Wählen Sie die Farbtiefe der Remote-Desktop-Verbindung aus der Dropdown-Liste aus.

2024-01

Option	Beschreibung
Enable scale down of larger remote screens (Aktivieren der Skalierung bei größeren Remote-Bildschirmen)	Aktivieren Sie diese Option, um sicherzustellen, dass der gesamte Remote-Desktop im Client angezeigt wird, indem der Inhalt verkleinert wird.
Display connection bar (Verbindungsleiste anzeigen)	Aktivieren Sie diese Option, um die Verbindungsleiste am oberen Rand des Bildschirms anzuzeigen. Die Verbindungsleiste wird nach einigen Sekunden automatisch ausgeblendet. Sie wird eingeblendet, wenn Sie die Maus an den oberen Rand des Bildschirms bewegen.

Local Resources Settings (Einstellungen der lokalen Ressourcen)

Option	Beschreibung
Apply Windows® key combinations (Windows-Tastenkombinationen anwenden)	Wählen Sie eine der folgenden Optionen aus der Drop-Down-Liste aus • **On this computer (Auf diesem Computer)**: Die Windows®-Tastenkombinationen gelten immer für den lokalen Computer • **On the remote computer (Auf dem Remote-Computer)**: Die Windows®-Tastenkombinationen gelten für den Desktop des Remote-Computers • **Only when using full screen (Nur bei der Verwendung der vollen Bildschirmgröße)**: Die Windows®-Tastenkombinationen gelten nur für den Remote-Computer, wenn sich die Verbindung im Vollbildmodus befindet
Select local resources and devices that are used on the host (Lokale Ressourcen und Geräte auswählen, die auf dem Host verwendet werden)	Aktivieren Sie die lokalen Ressourcen und Geräte, die auf dem Host verfügbar sein sollen.

Redirect Audio (Audio umleiten)

Option	Beschreibung
Remote audio playback (Audio-Fernwiedergabe)	Geben Sie an, von welchem Gerät, von diesem Computer oder vom RM/BTC, Ton wiedergegeben werden soll. Standardmäßig ist der Ton deaktiviert.
Record local audio and send to remote computer (Lokale Audioaufnahmen aufzeichnen und an Remote-Computer senden)	Wenn Sie z. B. Ihre lokalen Mikrofonaufzeichnungen an den Server weiterleiten möchten

Hinweis!

Ein Speicherverlust in Microsoft® RDP kann zu "Out of Memory“ (Nicht genügend Speicher verfügbar) führen, wenn Audioumleitung und Rund-um-die-Uhr-Betrieb aktiviert sind. Es wird nicht empfohlen, diese Funktion zu aktivieren.

https://support.microsoft.com/en-ie/help/4019660/remote-desktop-connection-mstsc-exe-leaks-memory-when-you-play-a-sound

Programme

Option	Beschreibung
Start the following application on the remote computer (Folgende Anwendung auf den Remote-Computer starten)	Damit wird automatisch eine Anwendung auf dem Host-PC gestartet, nachdem sich der Anwender in der Sitzung angemeldet hat. Remote-Apps werden unter Windows Server 2008 und höher unterstützt. Wenden Sie sich an Ihren Systemadministrator, um Informationen zur Konfiguration von RDP-Remote-Apps zu erhalten.

Advanced (Erweitert)

Option	Beschreibung
Authentication	• Keine Authentifizierung des Servers • Die Server-Authentifizierung ist erforderlich und muss erfolgreich abgeschlossen werden, damit die Verbindung fortgesetzt werden kann • Versuch, den Server zu authentifizieren. Wenn die Authentifizierung fehlschlägt, wird der Anwender aufgefordert, die Verbindung abzubrechen oder ohne Server-Authentifizierung fortzufahren
Verwenden Sie den CredSSP (Credential Security Support Provider) für die Authentifizierung, falls verfügbar	Verwenden Sie diese Option für die Rückwärtsauthentifizierung mit einigen älteren RDP-Servern.
Aktivieren Sie den Client, um Doppelklicks zu erkennen und an den Server weiterzuleiten	Aktivieren Sie diese Option, damit die RM -Geräte Doppelklickereignisse erkennen, interpretieren und an den Remote-Host weiterleiten können.
Laden Sie systemweit installierte RDP-Plug-ins	Ermöglicht die Verwendung von auf dem System installierten und registrierten virtuellen RDP-Kanälen "Remote Desktop Services“ (PRO-Lizenz erforderlich)

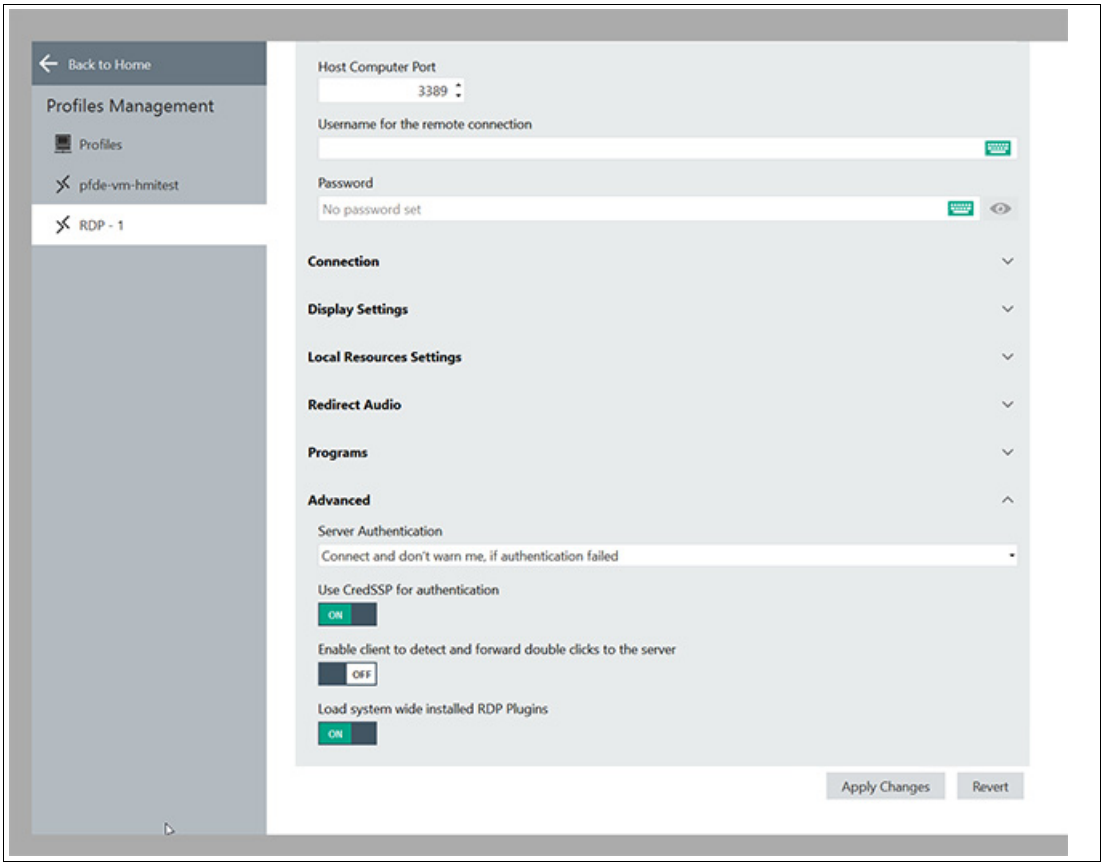


Abbildung 6.14

6.3 Raritan KVM-Einstellungen

In diesem Abschnitt wird die Konfiguration des Profils KVM-over-IP für Raritan KVM-over-IP-Switches beschrieben.

Hinweis!

VisuNet RM Shell 5.2 und höher wurde mit dem Raritan Dominion® KX IV-101 KVM-over-IP-Switch getestet und qualifiziert, der als Zubehör erhältlich ist (DKX4-101; #70118493). Eine separate Schnellinstallationsanleitung mit den Konfigurationsschritten für den Raritan Dominion® KX IV-101 KVM-over-IP-Switch ist online verfügbar (https://www.pepperl-fuchs.com/global/en/classid_2547.htm?view=productdetails&prodid=100044#documents).

Hinweis!

Für den KVM-over-IP-Client muss eine VisuNet RM Shell PRO-Lizenz freigeschaltet werden.

KVM-Profileinstellungen

Wenn der Raritan-Switch konfiguriert ist, kann ein neues KVM-Verbindungsprofil in VisuNet RM Shell 5.2 und höher erstellt werden. Mit diesem Profil kann eine Verbindung zu dem Host-PC hergestellt werden, der mit dem Raritan KVM-Switch verbunden ist.

Hinweis!

Stellen Sie sicher, dass der Raritan Dominion KVM-Switch ordnungsgemäß konfiguriert ist und dass DPA (Direct Port Access) aktiviert ist, bevor Sie ein Raritan KVM-Profil erstellen.

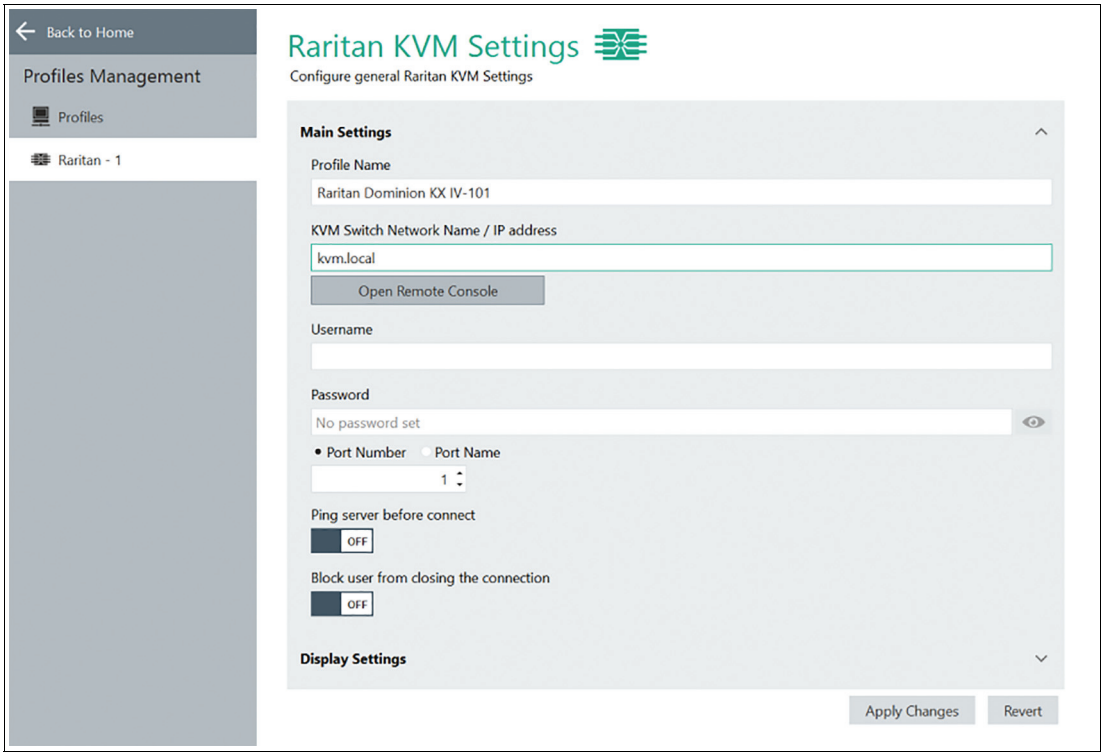


Abbildung 6.15 Raritan KVM-Einstellungen

General Settings (Allgemeine Einstellungen)

Option	Beschreibung
Profile Name (Profilname)	Name des KVM-Verbindungsprofils, das auf dem Startbildschirm angezeigt wird.
KVM Switch Network Name / IP address (Netzwerkname/IP-Adresse KVM-Switch)	Standardmäßig ist DHCP aktiviert. Stellen Sie sicher, dass Sie den folgenden Netzwerknamen verwenden, um die erste Verbindung einzurichten: **kvm.local** Weitere Informationen zu statischen IP-Adressen finden Sie im Raritan-Handbuch.
Username (Benutzername)	Benutzername, der auf dem Raritan KVM-Switch gespeichert ist, zu dem Sie eine Verbindung herstellen möchten. Standardbenutzer DKX4-101: **admin**
Kennwort	Kennwort des Benutzers, der auf dem Raritan KVM-Switch gespeichert ist, zu dem Sie eine Verbindung herstellen möchten. Standardkennwort DKX4-101: **raritan** (für Benutzer "admin“)
Port Number/Port Name (Portnummer/Portname)	Diese Einstellung kann auf Raritan KVM-over-IP-Switches mit mehreren Ports verwendet werden, um die Portnummer auszuwählen, zu der Sie eine Verbindung herstellen möchten.
Ping server before connect (Server vor der Verbindung pingen)	Überprüfen Sie mithilfe des Ping-Mechanismus, ob das Gerät verfügbar ist, bevor Sie eine Verbindung herstellen.
Block user from closing the connection (Anwender daran hindern, die Verbindung zu beenden)	Mit dieser Funktion wird die Funktion "Close“ (Schließen) aus der Verbindungsleiste entfernt. Bitte beachten Sie, dass diese Funktion den Anwender nicht daran hindert, die Verbindung über andere Client-Mechanismen zu schließen, z. B. über die Raritan Client-Menüleiste.

Display Settings (Display-Einstellungen)

Option	Beschreibung
Show the connection bar (Verbindungsleiste anzeigen)	Aktivieren Sie diese Option, um die Verbindungsleiste am oberen Rand des Bildschirms anzuzeigen. Die Verbindungsleiste wird nach einigen Sekunden automatisch ausgeblendet. Sie wird eingeblendet, wenn Sie die Maus an den oberen Rand des Bildschirms bewegen.

Nachdem Sie das Verbindungsprofil wie gewünscht konfiguriert haben, klicken Sie auf "Apply changes“ (Änderungen anwenden).

6.4 Einstellungen für VisuNet Desktop Sharing

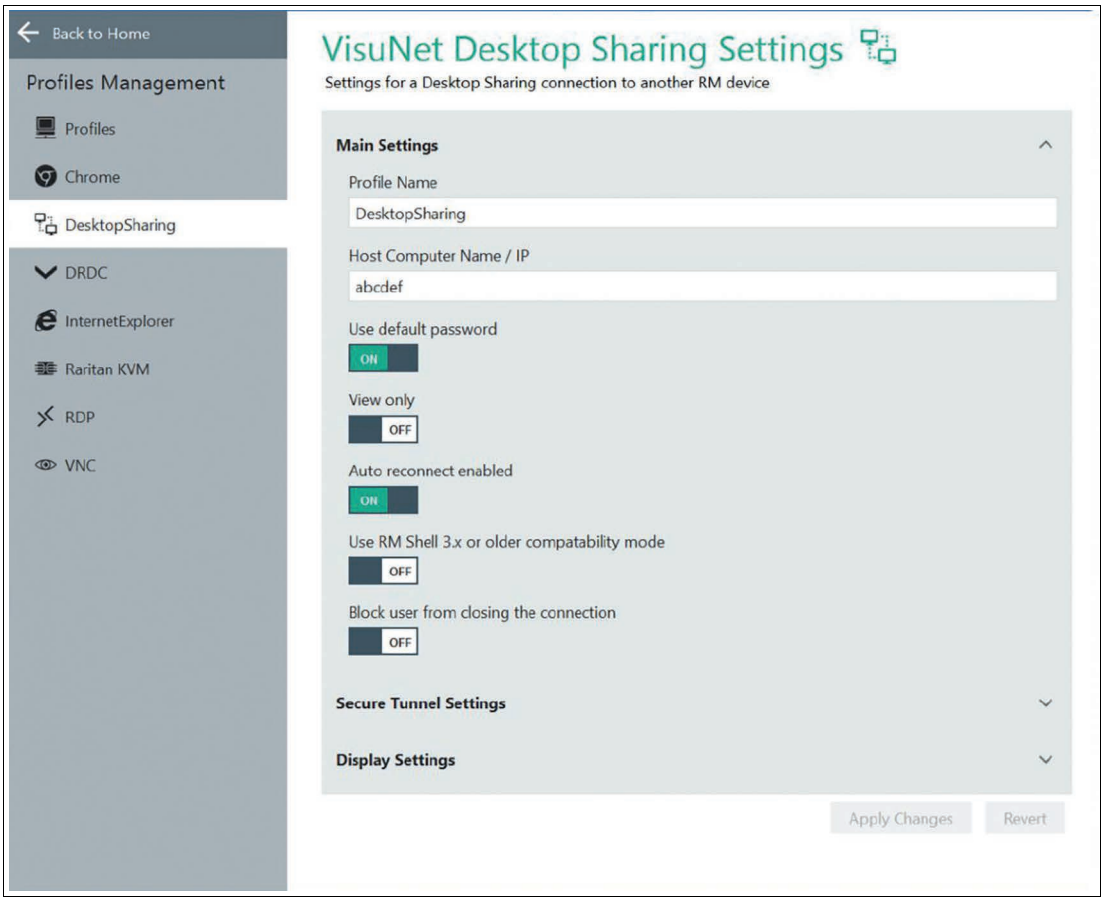


Abbildung 6.16

Main Settings (Grundlegende Einstellungen)

Option	Beschreibung
Profile Name (Profilname)	Ermöglicht Ihnen das Ändern des sichtbaren Namens des ausgewählten Profils.
Host Computer Name/IP (Name/IP-Adresse Host-Computer)	Geben Sie den Namen des Host-Computers oder die IP-Adresse des RM Masters ein. Wenn Sie Ihr eigenes Zertifikat für sicheres Tunnelsitzungs-Shadowing verwenden, müssen der Name des Hostcomputers und der gemeinsame Name des Zertifikats identisch sein.
Use default password (Standardkennwort verwenden)	Deaktivieren Sie diese Funktion, um Ihr eigenes Kennwort festzulegen.

Option	Beschreibung
View only (Nur ansehen)	Aktivieren Sie diese Funktion, um nur Lesezugriff zu erlauben. Wenn diese Option aktiviert ist, gibt es keine Mausfunktionalität und keine Tastatureingabe.
Auto reconnect enabled (Automatische Wiederverbindung aktiviert)	Aktivieren Sie diese Funktion, um die Verbindung zum RM Master automatisch wiederherzustellen, wenn die Verbindung unterbrochen wurde.
Use RM Shell 3.x or older compatibility mode (RM Shell 3.x oder älteren Kompatibilitätsmodus verwenden)	In einer älteren Version von RM Shell (Version 3.x) gibt es eine Funktion namens "Clone Display“ (Klonanzeige). Mit dieser Funktion können Sie auch einen Monitor spiegeln. Aktivieren Sie "Use RM Shell 3.x or older compatibility mode“ (RM Shell 3.x oder älteren Kompatibilitätsmodus verwenden), um einen RM Master mit RM Shell 3.x kompatibel mit RMs mit RM Shell 5 zu machen.
Block User from closing the connection (Benutzer daran hindern, die Verbindung zu beenden)	Aktivieren Sie diese Option, um zu verhindern, dass der Benutzer ein Verbindungsfenster öffnet.

Einstellungen für sicheren Tunnel

Option	Beschreibung
Enable Secure Tunnel (Sicheren Tunnel aktivieren)	Muss aktiviert sein, damit die Funktion Secure Tunnel Service (Sicherer Tunneldienst) verwendet werden kann
Secure Tunnel Port (Port für sicheren Tunnel)	Wir empfehlen die Verwendung des Standard-Tunnelports.
Accept embedded self-signed certificate only (Nur eingebettetes selbstsigniertes Zertifikat akzeptieren)	Wenn diese Option aktiviert ist, wird das in die RM Shell eingebettete Standardzertifikat akzeptiert. Wenn Sie Ihr eigenes Zertifikat verwenden, wird empfohlen, diese Funktion zu deaktivieren.
Ignore certificate name mismatch error (Fehler aufgrund von Zertifikatnamenskonflikt ignorieren)	Es wird dringend empfohlen, die Standardeinstellung "Off“ (Aus) beizubehalten
Ignore certificate chain error (Zertifikatkettenfehler ignorieren)	Es wird dringend empfohlen, die Standardeinstellung "Off“ (Aus) beizubehalten

Display Settings (Display-Einstellungen)

Option	Beschreibung
Screen stretching (Bildschirmdehnung)	Wählen Sie eine Option aus der Dropdown-Liste, um die Bildschirmdehnung zu wählen. 1. Resize the remote screen image to fill the local screen no matter what the actual aspect ratio is (Die Größe des Remote-Bildschirmdarstellung wird so angepasst, dass sie immer den lokalen Bildschirm füllt, unabhängig vom tatsächlichen Seitenverhältnis): Der Inhalt wird auf die Größe des lokalen Bildschirms gedehnt. Dies kann zu Verzerrungen des Inhalts führen. 2. Scale to as large an image as possible, but maintain the correct aspect ratio (Skalierung auf ein möglichst großes Bild, aber Beibehaltung des richtigen Seitenverhältnisses): Der Inhalt wird so groß wie möglich gedehnt, ohne Verzerrung des Seitenverhältnisses. Dies kann zu schwarzen Balken führen.
Cursor mode (Cursor-Modus)	Wählen Sie eine Option aus der Dropdown-Liste. • Track remote cursor locally (Remote-Cursor lokal verfolgen). • Let remote server deal with mouse cursor (Steuerung des Mauszeigers dem Remote-Server überlassen). • Don't show remote cursor (Remote-Cursor nicht anzeigen); Es wird kein Cursor angezeigt. Verwenden Sie "No cursor“ (Kein Cursor) als Cursor-Tracking-Modus.
Cursor tracking mode (Cursor-Tracking-Modus)	No cursor (Kein Cursor): Es steht kein Cursor zur Verfügung. Wählen Sie diese Option für den Cursor-Modus "Don't show remote cursor“ (Remote-Cursor nicht anzeigen). • Dot cursor (Punktcursor): Ein Punkt wird als Cursor verwendet. • Normal cursor (Normaler Cursor): Der Windows-Standardpfeil wird als Cursor verwendet. • Small cursor (Kleiner Cursor): Ein kleinerer Windows-Standardpfeil wird als Cursor verwendet.
Display the connection bar (Verbindungsleiste anzeigen)	Aktivieren Sie diese Option, um die Verbindungsleiste am oberen Rand des Bildschirms anzuzeigen. Die Verbindungsleiste wird nach einigen Sekunden automatisch ausgeblendet. Sie wird wieder eingeblendet, wenn Sie die Maus an den oberen Rand des Bildschirms bewegen.

Aufbau einer VisuNet Desktop Sharing-Verbindung mit aktiviertem sicherem Tunnel

Beim Aufbau einer VisuNet Desktop Sharing-Verbindung von einem Client (Gerät A) zu einem Host (Gerät B) müssen beide Geräte konfiguriert werden. Die Einstellungen können direkt an den Geräten in RM Shell oder per Fernzugriff über VisuNet Control Center vorgenommen werden.

1. Aktivieren Sie den VisuNet Desktop Sharing-Server in den Systemeinstellungen des Hosts (Gerät B). Der sichere Tunneldienst sowie die Verwendung des Standardzertifikats werden standardmäßig aktiviert.

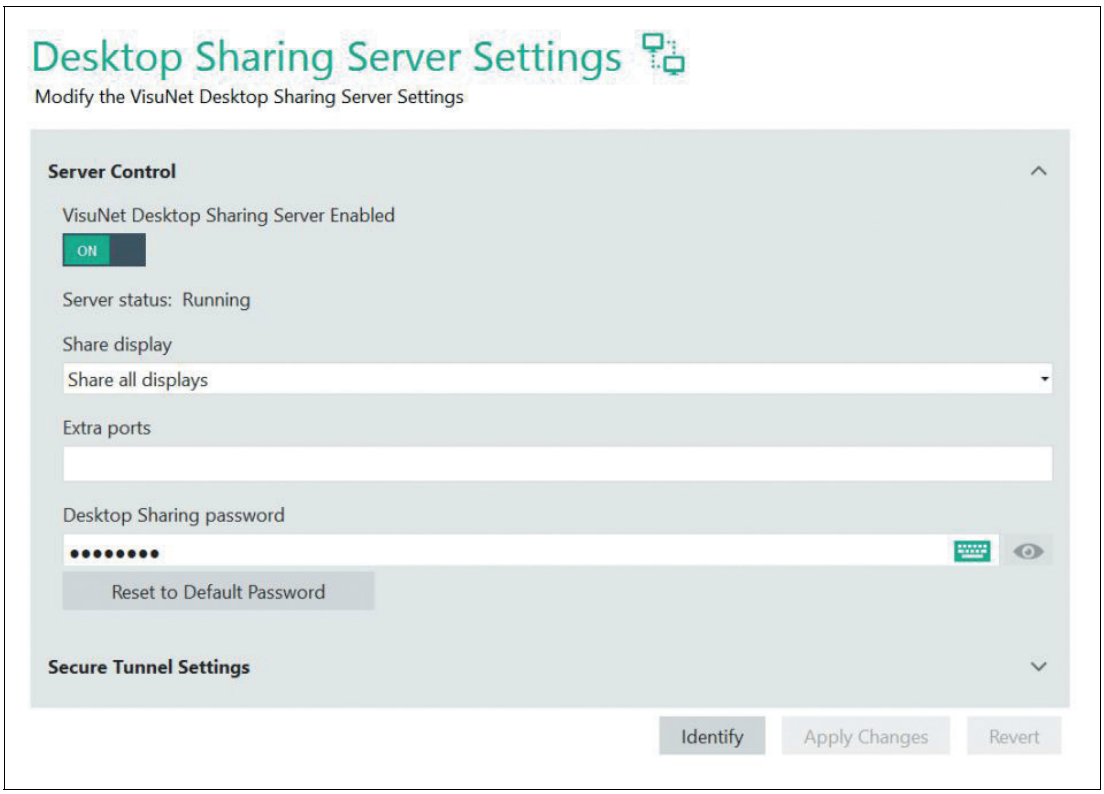


Abbildung 6.17

2. Laden Sie Ihr Zertifikat mit einem privaten Schlüssel von einem angeschlossenen USB-Gerät oder über den Ordner "Share“ im Netzwerk auf Ihr Host-Gerät B hoch. Die zusätzliche Software VisuNet Control Center kann zum Hochladen Ihres Zertifikats verwendet werden.
3. Öffnen Sie den "Certificate Import Wizard“ (Assistenten für den Import von Zertifikaten), indem Sie das Zertifikat mit Windows-Explorer öffnen. Befolgen Sie die Anweisungen. Speichern Sie das Zertifikat auf Ihrem lokalen Gerät.

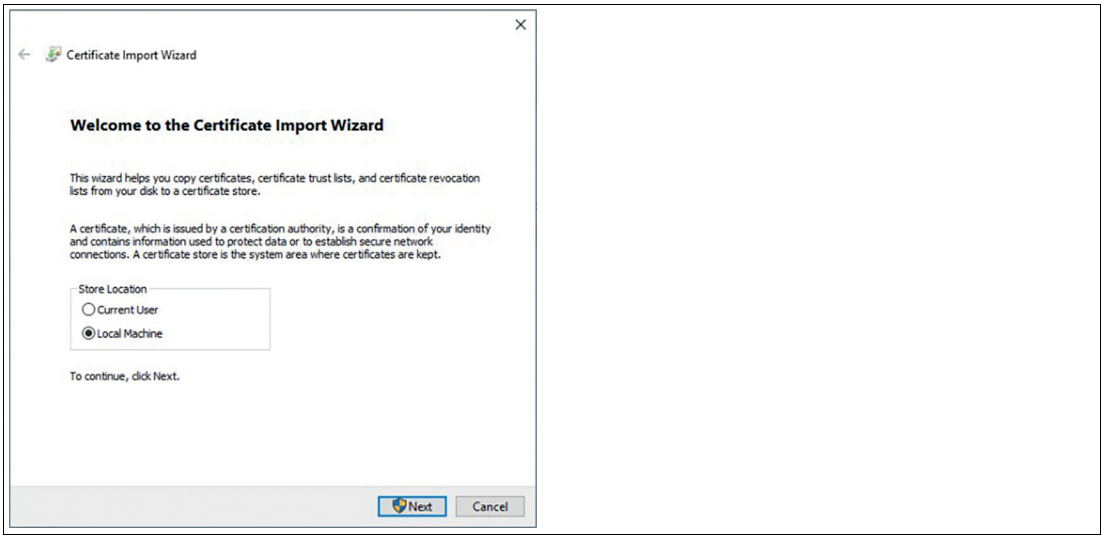


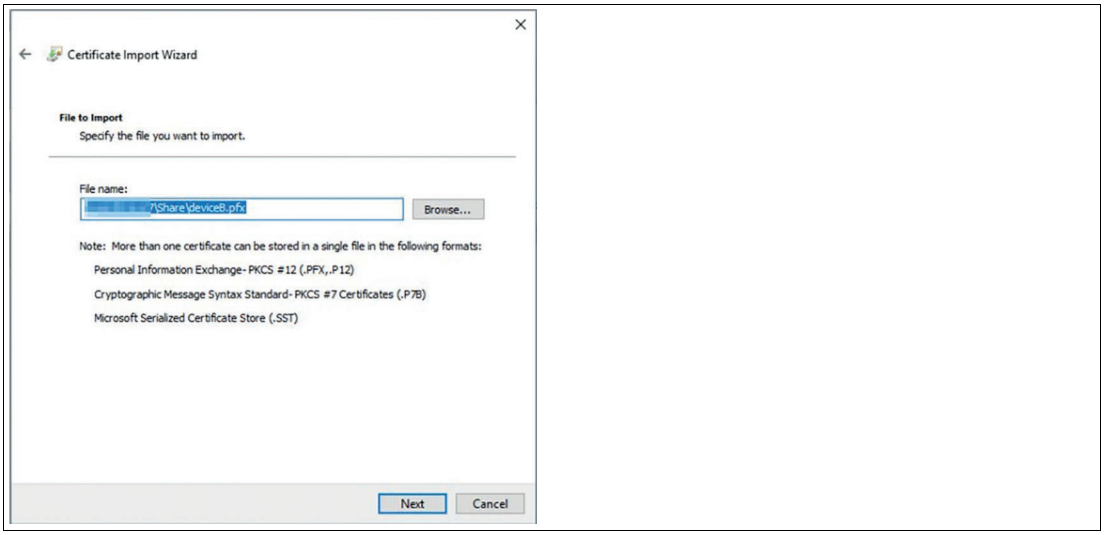
Abbildung 6.18

Vorsicht!

Security (Sicherheit)

Um die Sicherheit weiter zu erhöhen, ist es wichtig, für das Zertifikat den Namen des Host-Gerätes zu vergeben.

4. Importieren Sie die Datei auf das Host-Gerät B.



5. Geben Sie das Passwort ein. Das Kennwort wird vom Ersteller des Zertifikats festgelegt.

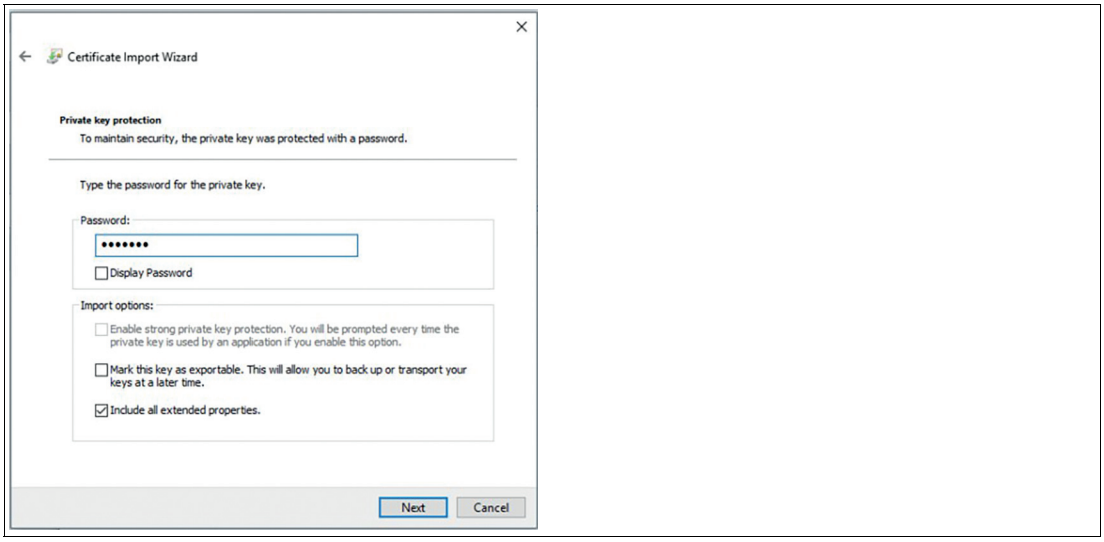


Abbildung 6.19

6. Wählen Sie den Speicher aus, in dem Ihr Zertifikat gespeichert werden soll.

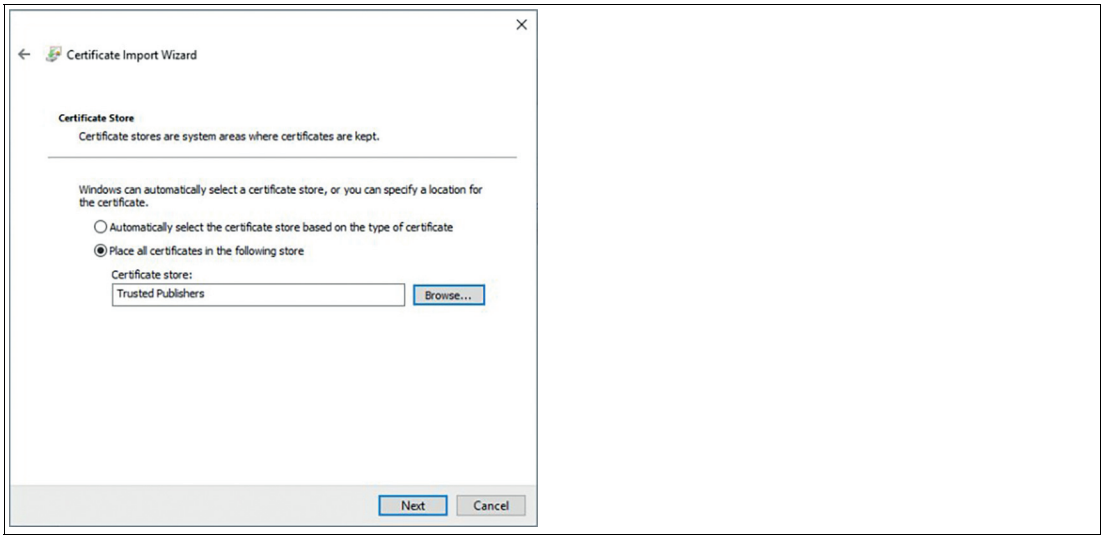


Abbildung 6.20

7. Überprüfen Sie die endgültigen Einstellungen und schließen Sie den Importvorgang ab, indem Sie auf "Finish“ (Fertig stellen) klicken.

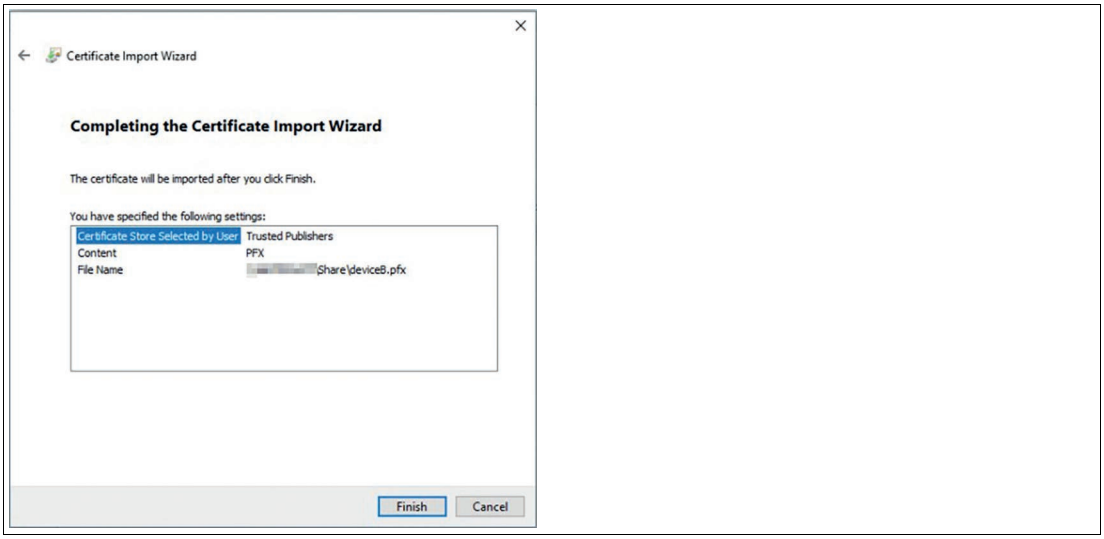


Abbildung 6.21

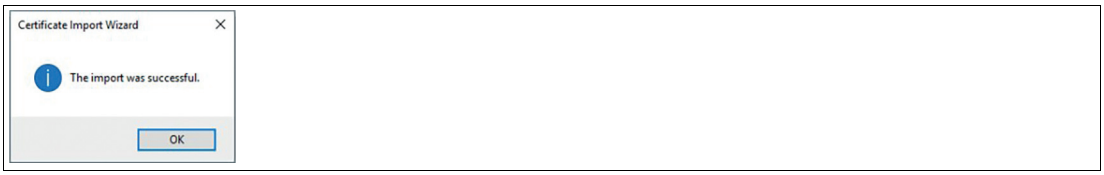


Abbildung 6.22

8. Aktualisieren Sie die Liste Ihrer Zertifikate und wählen Sie das importierte Zertifikat aus.

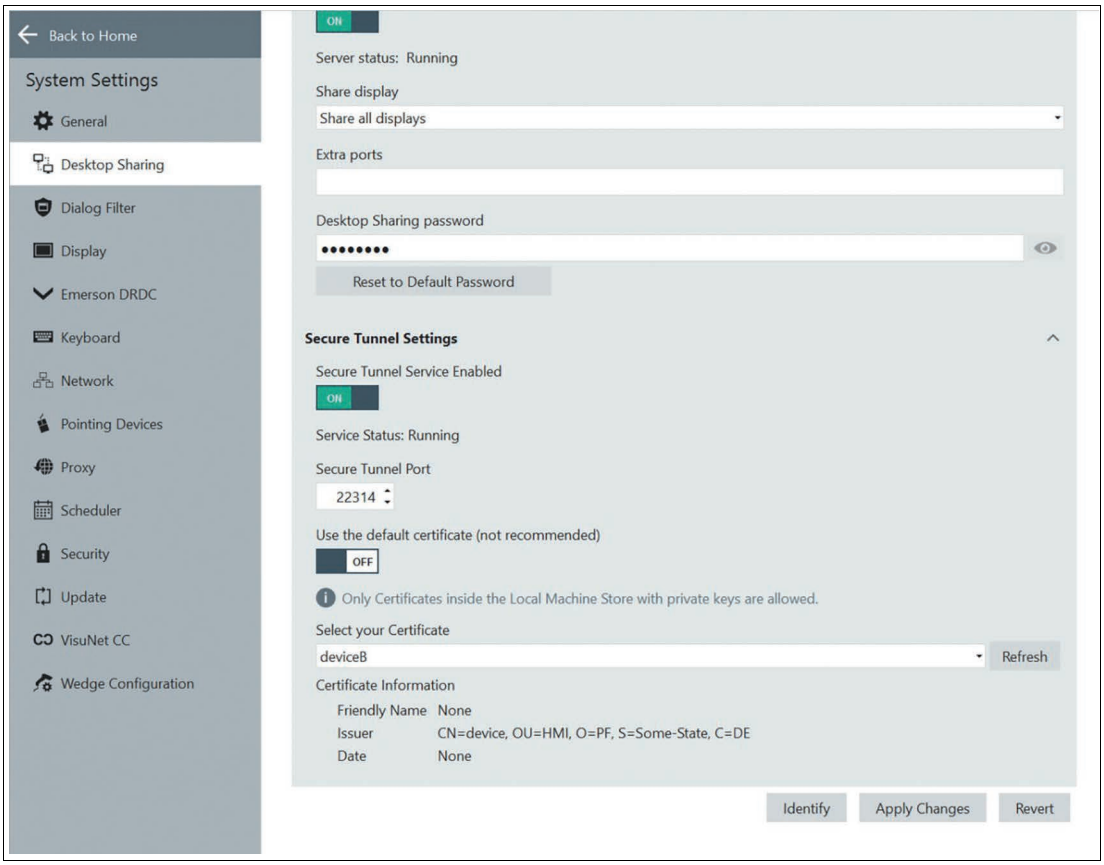


Abbildung 6.23

9. Um die Änderungen zu übernehmen, klicken Sie auf "Apply Changes“ (Änderungen anwenden).

Konfiguration von Client-Gerät A

Um eine unterbrechungsfreie Kette zu erstellen, fahren Sie nun mit der Konfiguration von Client-Gerät A fort und installieren Sie das Public-Key-Zertifikat (Root CA) auf dem Client-Gerät A.

1. Öffnen Sie das Zertifikat im Ordner Share per Doppelklick und öffnen Sie den Certificate Import Wizard (Assistenten für den Import von Zertifikaten), indem Sie auf "Install Certificate…“ (Zertifikat installieren...) klicken.

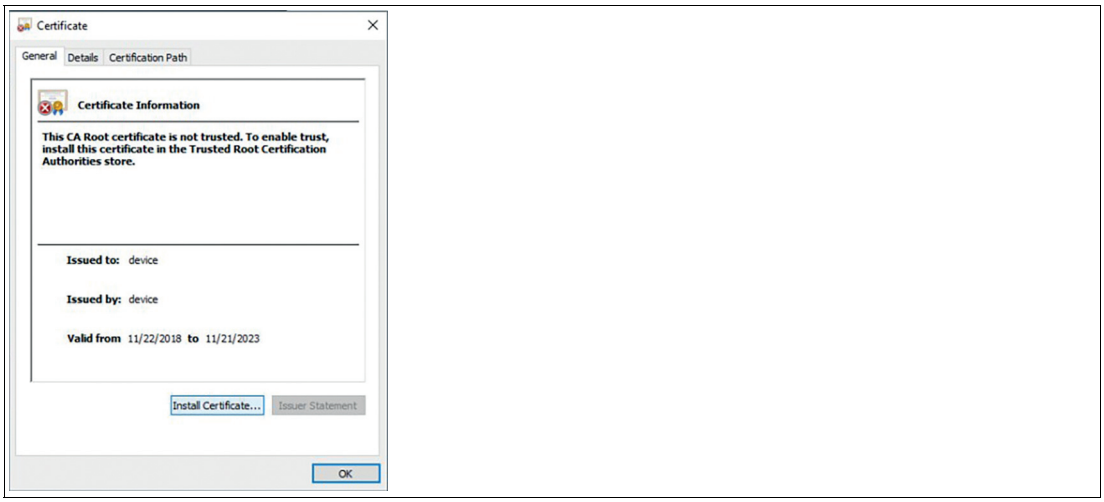


Abbildung 6.24

2. Befolgen Sie die Anweisungen des Importassistenten. Wählen Sie den Standort Ihres Geschäfts und den Zertifizierungsspeicher aus und klicken Sie auf "Next“ (Weiter), um fortzufahren.

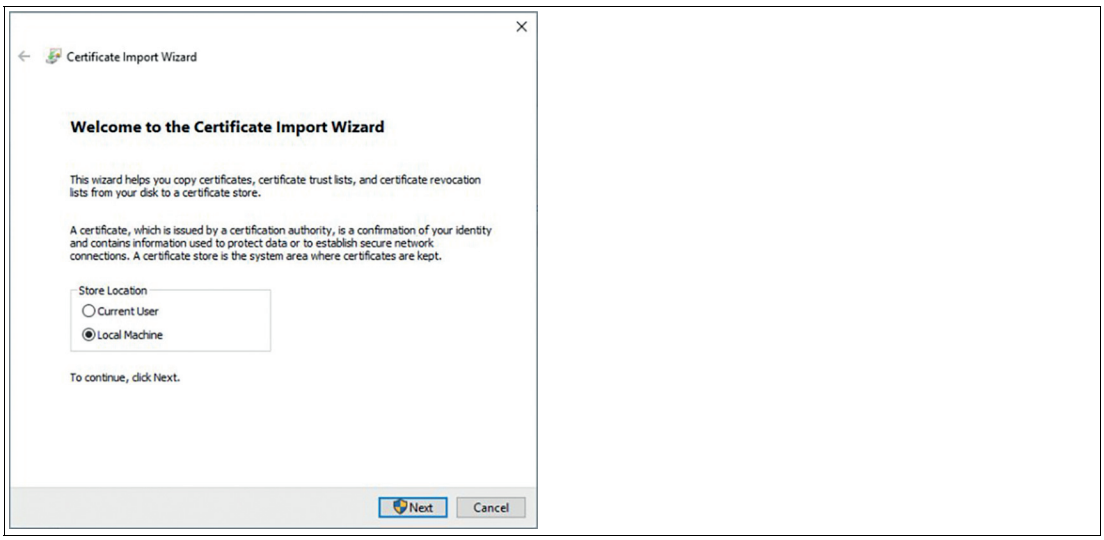


Abbildung 6.25

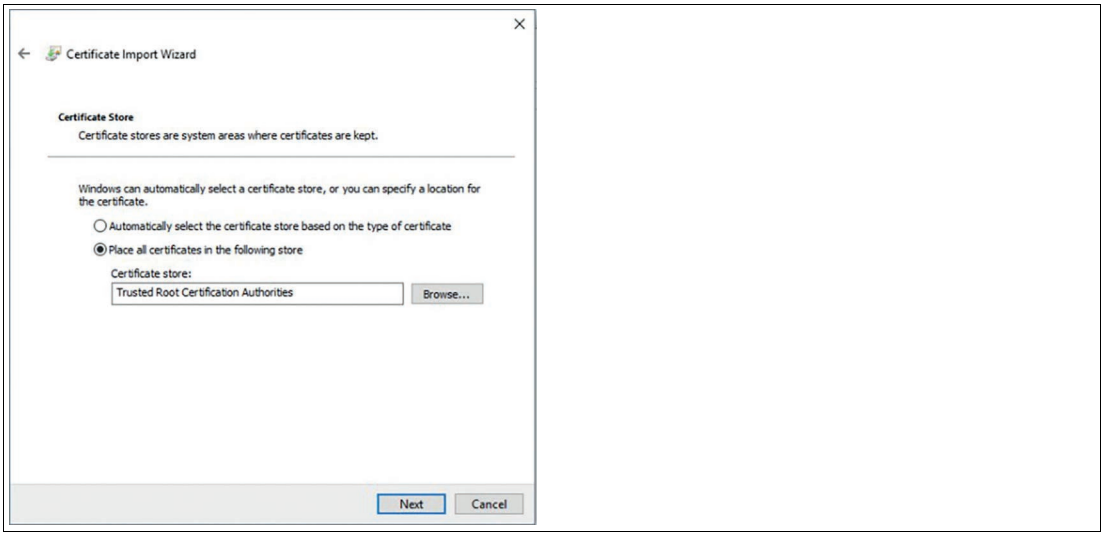


Abbildung 6.26

3. Bevor Sie den Import Ihres Zertifikats abschließen, können Sie die Spezifikationen Ihrer Einstellungen noch einmal überprüfen. Klicken Sie auf "Finish“ (Fertig stellen), um den Import abzuschließen.

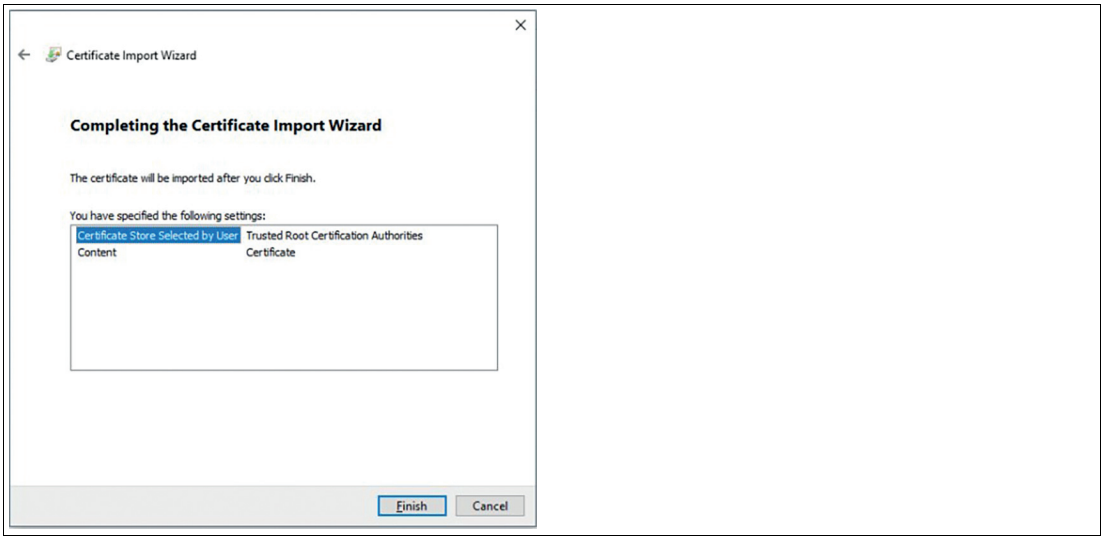


Abbildung 6.27

↳ Wenn Sie alle Implementierungen der Zertifikate erfolgreich abgeschlossen haben, wird keine Fehlermeldung angezeigt, wenn Ihre Fernüberwachung beginnt.

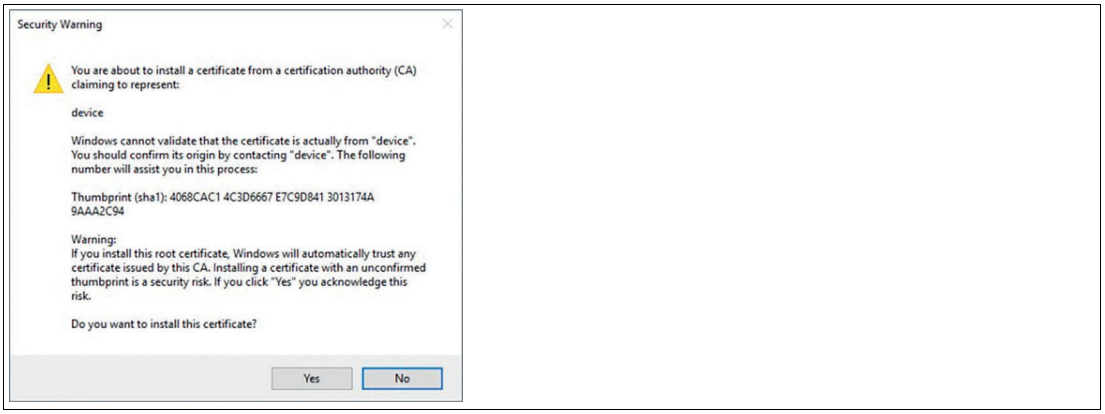


Abbildung 6.28

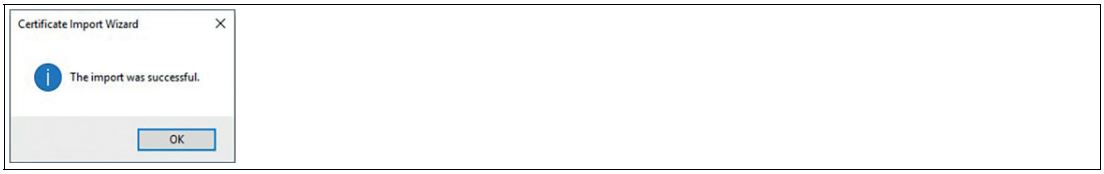


Abbildung 6.29

4. Erstellen Sie ein neues VisuNet Desktop Sharing-Profil auf Ihrem Client-Gerät

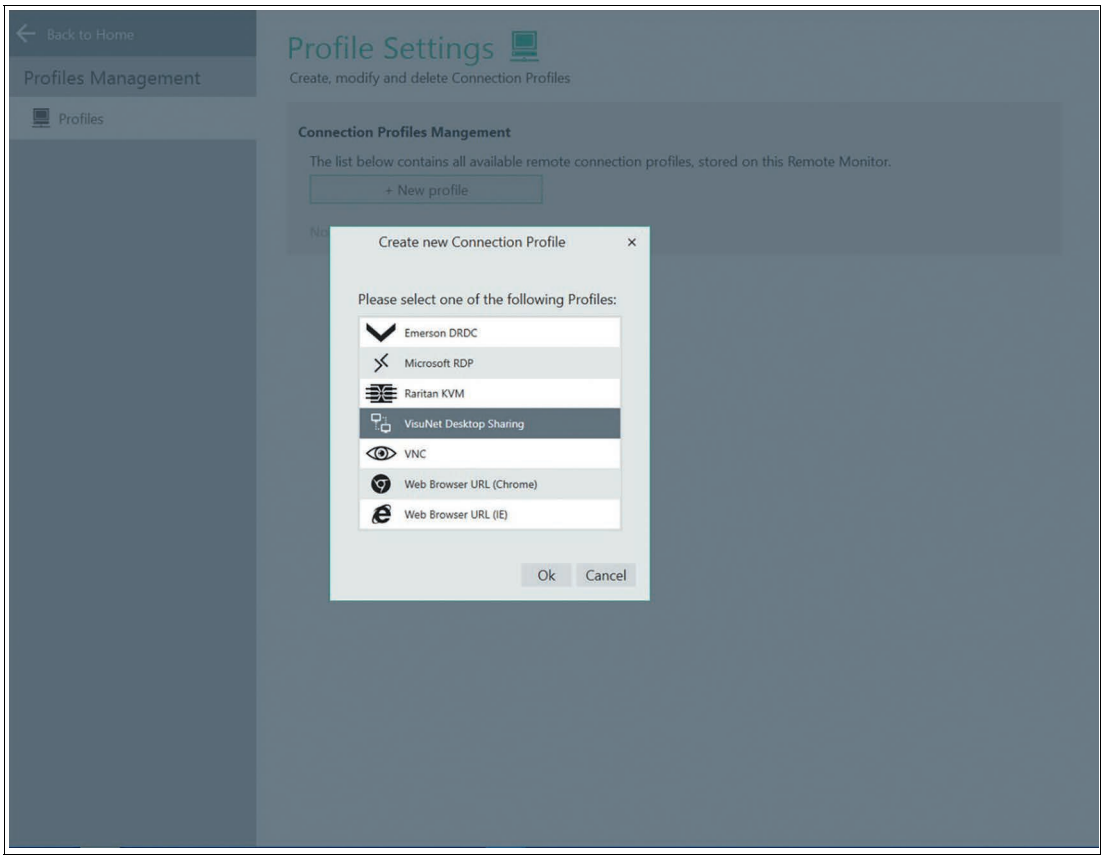


Abbildung 6.30

Vorsicht!

Beibehalten der Werkseinstellungen

Es wird dringend empfohlen, die Standardeinstellungen "ignoring certificate mismatch error“ (Fehler aufgrund von Zertifikatnamenskonflikt ignorieren) und "ignore certificate chain error“ (Zertifikatkettenfehler ignorieren) auf "Off“ (Aus) zu belassen.

5. Aktivieren Sie den sicheren Tunnel. Setzen Sie "Accept embedded self-signed certificate only“ (Nur eingebettetes selbstsigniertes Zertifikat akkzeptieren) auf "Off“ (Aus).

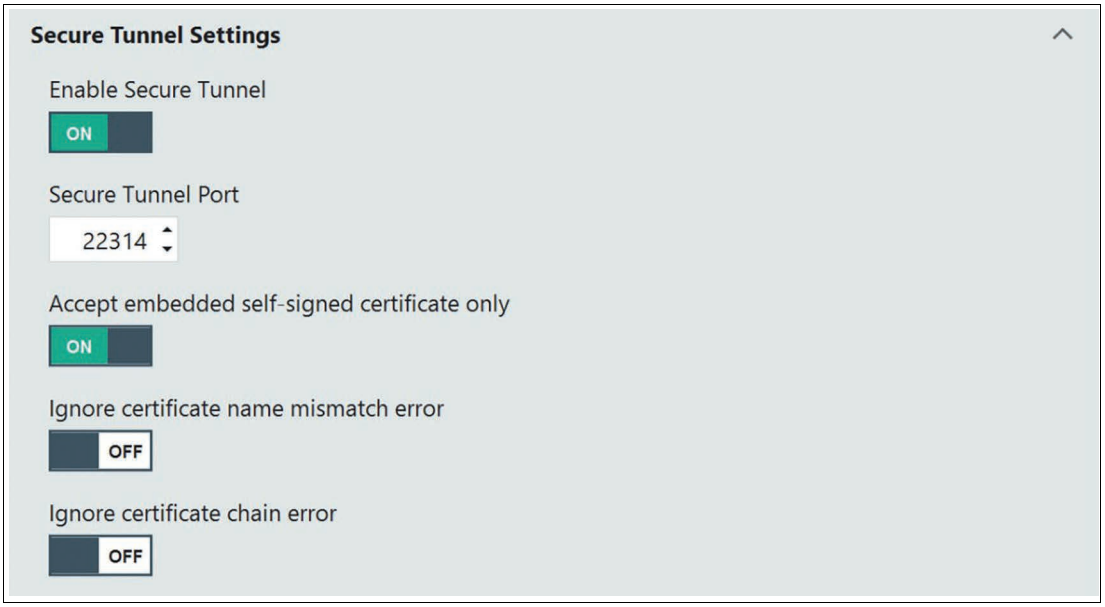


Abbildung 6.31

6.5 VNC-Einstellungen

RM Shell bietet einen integrierten VNC-Client. Dieser Client ist mit Standard-VNC-Serversoftware kompatibel. Er unterstützt auch viele einzigartige Funktionen, die spezifisch für UltraVNC- und TightVNC-Distributionen sind. Dazu gehört beispielsweise die sichere Kommunikation mit einem VNC-Server. Der VNC-Client unterstützt die Authentifizierung mittels UltraVNC NTLM (ms-logon) und bietet integrierte Unterstützung für Plugins für UltraVNC SecureVNC v2.3 und MSRC4 v1.2.2 DSM.

Dieser Abschnitt beschreibt die wichtigsten Einstellungen zum Einrichten einer VNC-Verbindung.

Main Settings (Grundlegende Einstellungen)

In diesem Abschnitt können Sie allgemeine Einstellungen wie Profilname, Host-Name/IP-Adresse und den Kennwortschutz einrichten.

Option	Beschreibung
Profile Name (Profilname)	Ermöglicht Ihnen das Ändern des sichtbaren Namens des ausgewählten Profils.
Host Computer Name/IP (Name/IP-Adresse Host-Computer)	Geben Sie den Namen des Host-Computers oder die IP-Adresse des Hosts im Netzwerk ein.
Host Computer Port (Port des Host-Computers)	Hier können Sie den Host-Port eingeben. Wir empfehlen die Verwendung der Standardeinstellung.
Password Type (Kennworttyp)	Wählen Sie die Art des Kennwortschutzes für die VNC-Verbindung.

Anschluss

In diesem Abschnitt können Sie die Verbindungsdetails konfigurieren.

Option	Beschreibung
Fast Disconnect Detection by sending Pings to the Host Server (Schnelle Erkennung von Verbindungsunterbrechungen durch Senden von Pings an den Host-Server)	Wenn diese Option aktiviert ist, sendet der RM/BTC kontinuierlich Pings an den Host. Mögliche Verbindungsunterbrechungen werden viel schneller erkannt als üblich.
Encoding (Kodierung)	Es stehen mehrere Kodierungsmethoden zur Verfügung. Beachten Sie, dass die gewählte Kodierung mit den VNC-Host-Einstellungen übereinstimmen muss.
Use CopyRect encoding (CopyRect-Kodierung verwenden)	Eine weitere Kodierungsmethode. Beachten Sie, dass die gewählte Kodierung mit den VNC-Host-Einstellungen übereinstimmen muss.
Use Cache encoding (Cache-Kodierung verwenden)	Verwenden Sie diese Option, um die Leistung zu verbessern. Durch die Verwendung der Cache-Kodierung kann die Fehlertoleranz beeinflusst werden.
View only (Nur ansehen)	Aktivieren Sie diese Option, um den VNC-Host-Bildschirm anzusehen. Es ist keine Interaktion über Maus oder Tastatur erlaubt.
Request shared session (Gemeinsame Sitzung anfordern)	Dadurch können mehrere Clients dieselbe VNC-Sitzung gemeinsam nutzen. Wenn diese Option nicht angegeben ist, kann jeweils nur ein Client mit einem VNC-Server verbunden werden. Wenn ein neuer, nicht gemeinsam genutzter Client verbunden ist, werden vorhandene Clients getrennt oder die neue Verbindung wird getrennt, je nachdem, wie der Server konfiguriert ist.
Remote input enabled (Remote-Eingabe aktiviert)	Um die Maus- und Tastatursteuerung des RM zu deaktivieren, während der VNC-Host auch Teile der RM-Funktionalität steuert, wählen Sie "Remote input enabled - off“ (Remote-Eingabe aktiviert - aus) aus.
Auto reconnect enabled (Automatische Wiederverbindung aktiviert)	Aktivieren Sie diese Option, um den integrierten Wiederherstellungsmechanismus von VNC zu nutzen. Dieser Mechanismus versucht ebenfalls, eine Verbindung wiederherzustellen, wenn sie gestört ist.
Block user from closing the connection (Anwender daran hindern, die Verbindung zu beenden)	Aktivieren Sie diese Option, um zu verhindern, dass ein Verbindungsfenster geschlossen wird.

Display Settings (Display-Einstellungen)

In diesem Abschnitt können Sie die Display-Einstellungen auswählen, wie beispielsweise Farbtiefe, Cursor-Modus (Änderungs-Nachverfolgungsmodus), Verhalten der Verbindungsleiste beim Anpassen des Bildschirms usw.

Option	Beschreibung
Color Depth (Farbtiefe)	Wählen Sie die gewünschte Farbtiefe der VNC-Verbindung aus der Dropdown-Liste aus.
Screen Stretching (Bildschirmdehnung)	Wählen Sie eine Option aus der Dropdown-Liste, um die Bildschirmdehnung zu wählen. 1. Resize the remote screen image to fill the local screen no matter what the actual aspect ratio is (Die Größe des Remote-Bildschirmdarstellung wird so angepasst, dass sie immer den lokalen Bildschirm füllt, unabhängig vom tatsächlichen Seitenverhältnis): Der Inhalt wird auf die Größe des lokalen Bildschirms gedehnt. Dies kann zu Verzerrungen des Inhalts führen. 2. Scale to as large an image as possible, but maintain the correct aspect ratio (Skalierung auf ein möglichst großes Bild, aber Beibehaltung des richtigen Seitenverhältnisses): Der Inhalt wird so groß wie möglich gedehnt, ohne Verzerrung des Seitenverhältnisses. Dies kann zu schwarzen Balken führen.
Scaling engine (Skalierungs-Engine)	Wählen Sie die gewünschte Skalierungs-Engine
Show the connection on following displays (Verbindung auf folgenden Displays anzeigen)	Wenn Sie erweiterte Desktop-Systeme oder BTC* verwenden, kann jedes Profil auf verschiedenen Displays angezeigt werden. Wählen Sie aus der Dropdown-Liste das Display aus, das das betreffende Profil anzeigt. Wählen Sie die Option "Expand over all display“ (Auf allen Displays erweitern) aus, wenn das Profilfenster auf allen Displays maximiert werden soll. Verwenden Sie die Schaltfläche "Identify Display“ (Display identifizieren), um die verschiedenen Displays zu identifizieren. Die Nummer des jeweiligen Displays wird auf jedem Monitor angezeigt.
Cursor Mode (Cursor-Modus)	Wählen Sie eine Option aus der Dropdown-Liste. • Track remote cursor locally (Remote-Cursor lokal verfolgen) (empfohlen) • Let remote server deal with mouse cursor (Steuerung des Mauszeigers dem Remote-Server überlassen) • Don't show remote cursor (Remote-Cursor nicht anzeigen): Es wird kein Cursor angezeigt. Verwenden Sie "No cursor“ (Kein Cursor) als Cursor-Tracking-Modus
Cursor Tracking Mode (Cursor-Tracking-Modus)	• No cursor (Kein Cursor): Es steht kein Cursor zur Verfügung. Wählen Sie diese Option für den Cursor-Modus "Don't show remote cursor“ (Remote-Cursor nicht anzeigen). • Dot cursor (Punktcursor): Ein Punkt wird als Cursor verwendet • Normal cursor (Normaler Cursor): Der Windows-Standardpfeil wird als Cursor verwendet • Small cursor (Kleiner Cursor): Ein kleinerer Windows-Standardpfeil wird als Cursor verwendet
Use custom compression (Benutzerdefinierter Komprimierung verwenden)	Die Komprimierung ist abhängig von der gewählten Kodierung. Verwenden Sie den Schieber, um die Komprimierungsrate auszuwählen.

Option	Beschreibung
Use JPG compression (JPG-Komprimierung verwenden)	Die Komprimierung ist abhängig von der gewählten Kodierung. Verwenden Sie den Schieber, um die Komprimierungsrate auszuwählen.
Display the connection bar (Verbindungsleiste anzeigen)	Aktivieren Sie diese Option, um die Verbindungsleiste am oberen Rand des Bildschirms anzuzeigen. Die Verbindungsleiste wird nach einigen Sekunden automatisch ausgeblendet. Sie wird eingeblendet, wenn Sie die Maus an den oberen Rand des Bildschirms bewegen.

Proxy Settings (Proxy-Einstellungen)

In diesem Abschnitt können Sie die Proxy-Einstellungen für die Proxy-Verbindung usw. festlegen, wie beispielsweise Proxy-Port, IP-Adresse, Benutzername und Kennwort.

Option	Beschreibung
Proxy Type (Proxy-Typ)	Wählen Sie einen der folgenden Proxy-Typen: • Direct connection (Direktverbindung) • SOCKS5 (no password) (SOCKS5 (kein Kennwort)) • HTTP proxy (no password) (HTTP-Proxy (kein Kennwort)) • UltraVNC repeater (UltraVNC-Repeater)
Proxy IP address (Proxy-IP-Adresse)	Geben Sie die Proxy-IP-Adresse ein
Proxy user name (Proxy-Benutzername)	Geben Sie den Proxy-Benutzernamen ein
Proxy password (Proxy-Kennwort)	Geben Sie das Proxy-Kennwort ein
Proxy port (Proxy-Port)	Wählen Sie den Proxy-Port aus

Advanced (Erweitert)

In diesem Abschnitt können Sie die erweiterten Einstellungen konfigurieren.

Option	Beschreibung
Show VNC Error Message Boxes (VNC-Fehlermeldungsfelder anzeigen)	Die Aktivierung dieser Option vereinfacht die Verfolgung von Fehlern. Es kann jedoch zu Konflikten mit der automatischen Wiederverbindungsfunktion kommen. Die Voreinstellung ist "Off“ (Aus).
Disable clipboard (Zwischenablage deaktivieren)	Diese Option ermöglicht Ihnen das Kopieren von Inhalten aus der Zwischenablage des VNC-Servers in die lokale RM/BTC-Zwischenablage. In der Standardeinstellung ist das Kopieren von Inhalten in die RM/BTC-Zwischenablage aktiviert ("Disable clipboard – off“ (Zwischenablage deaktivieren – aus))
Enable Ctrl + Alt + Del hotkey (Tastenkombination Strg+Alt+Entf aktivieren)	Aktivieren Sie diese Option, um den Anwendern die Verwendung der Tastenkombination Strg+Alt+Entf zu ermöglichen.
Capture hotkeys containing the Alt key or Windows key (Tastaturkürzel, die die Alt- oder Windows-Taste enthalten, erfassen)	Tastenkombinationen, die eine Alt- oder Windows-Taste enthalten, werden weitergeleitet. Z. B. Window+E für Explorer oder Alt+Tab für Taskwechsel.
DSM encryption plug-in (DSM-Verschlüsselungs-Plugin)	Wählen Sie eines der folgenden Verschlüsselungs-Plugins: • Plain connection, no encryption (Einfache Verbindung, keine Verschlüsselung) • Use MSRC4 DSM plug-in (MSRC4 DSM-Plugin verwenden) • Use SecureVNC DSM plug-in (SecureVNC DSM-Plugin verwenden)

2024-01

6.6 Webbrowser-Einstellungen (Chrome)

Der eingeschränkte Webbrowser ist ein integrierter HTML-Webbrowser in RM Shell, der auf Google Chrome basiert. Er ermöglicht den direkten Zugriff auf HTML-basierte Systeme (z. B. SCADA, MES, IP-Kameras usw.). Mit dem eingeschränkten Webbrowser können Sie einen Link zu einer Webadresse angeben, die auf dem Startbildschirm als Profil angezeigt wird. Im Gegensatz zu einem Standard-Webbrowser kann der Benutzer keine andere Adresse im eingeschränkten Webbrowser eingeben; er kann nur auf die konfigurierte Website zugreifen.

Hinweis!

Optionale Funktion, erfordert PRO-Lizenz zum Entsperren der Funktion.

General Settings (Allgemeine Einstellungen)

Option	Beschreibung
Connection name (Verbindungsname)	Name der Webverbindung, die auf dem Startbildschirm angezeigt wird.
URL that will be navigated to (URL, zu der navigiert wird)	Die URL, mit der das Web-Profil verknüpft werden soll.
Show URL (URL anzeigen)	Aktivieren Sie diese Option, um die URL unten links im Verbindungsfenster anzuzeigen.
Block user from closing the connection (Benutzer daran hindern, die Verbindung zu beenden)	Aktivieren Sie diese Option, um zu verhindern, dass der Benutzer ein Verbindungsfenster öffnet. (Dadurch wird die Schaltfläche "Close“ (Schließen) in der Verbindungsleiste ausgeblendet und Alt+F4 deaktiviert.)

Display Settings (Display-Einstellungen)

Option	Beschreibung
Show the Connection Bar (Verbindungsleiste anzeigen)	Aktivieren Sie diese Option, um die Verbindungsleiste am oberen Rand des Bildschirms anzuzeigen. Die Verbindungsleiste wird nach einigen Sekunden automatisch ausgeblendet. Sie wird eingeblendet, wenn Sie die Maus an den oberen Rand des Bildschirms bewegen.
Show the connection on following displays (Verbindung auf folgenden Displays anzeigen)	Wenn Sie erweiterte Desktop-Systeme oder Box Thin Clients von Pepperl+Fuchs verwenden, kann jedes Profil auf verschiedenen Displays angezeigt werden. Wählen Sie aus der Dropdown-Liste das Display aus, das das betreffende Profil anzeigt. Wählen Sie die Option "Expand over all display“ (Auf allen Displays erweitern) aus, wenn das Profilfenster auf allen Displays maximiert werden soll. Verwenden Sie die Schaltfläche "Identify Display“ (Display identifizieren), um die verschiedenen Displays zu identifizieren. Die Nummer des jeweiligen Displays wird auf jedem Monitor angezeigt.

6.7 Webbrowser-Einstellungen (Internet Explorer)

Der eingeschränkte Webbrowser ist ein integrierter HTML-Webbrowser in RM Shell, der auf Internet Explorer basiert. Er ermöglicht den direkten Zugriff auf HTML-basierte Systeme (z. B. SCADA, MES, IP-Kameras usw.). Mit dem eingeschränkten Webbrowser können Sie einen Link zu einer Webadresse angeben, die auf dem Startbildschirm als Profil angezeigt wird. Im Gegensatz zu einem Standard-Webbrowser kann der Benutzer keine andere Adresse im eingeschränkten Webbrowser eingeben; er kann nur auf die konfigurierte Website zugreifen.

Hinweis!

Optionale Funktion, erfordert PRO-Lizenz zum Entsperren der Funktion.

General Settings (Allgemeine Einstellungen)

Option	Beschreibung
Connection name (Verbindungsname)	Name der Webverbindung, die auf dem Startbildschirm angezeigt wird.
URL that will be navigated to (URL, zu der navigiert wird)	Die URL, mit der das Web-Profil verknüpft werden soll.
Show URL (URL anzeigen)	Aktivieren Sie diese Option, um die URL unten links im Verbindungsfenster anzuzeigen.
Show Message Box when Script errors detected (Meldungsfeld anzeigen, wenn Script-Fehler erkannt werden)	Aktivieren Sie diese Option, um Fehlermeldungen anzuzeigen.
Block user from closing the connection (Benutzer daran hindern, die Verbindung zu beenden)	Aktivieren Sie diese Option, um zu verhindern, dass der Benutzer ein Verbindungsfenster öffnet. (Dadurch wird die Schaltfläche "Close“ (Schließen) in der Verbindungsleiste ausgeblendet und Alt+F4 deaktiviert.)

Display Settings (Display-Einstellungen)

Option	Beschreibung
Show the Connection Bar (Verbindungsleiste anzeigen)	Aktivieren Sie diese Option, um die Verbindungsleiste am oberen Rand des Bildschirms anzuzeigen. Die Verbindungsleiste wird nach einigen Sekunden automatisch ausgeblendet. Sie wird eingeblendet, wenn Sie die Maus an den oberen Rand des Bildschirms bewegen.

7 App Management (Anwendungsverwaltung)

Mit App Management (Anwendungsverwaltung) können Administratoren Links zu Windows®-Tools .exe-Anwendungen wie Antivirensoftware oder Standardprogrammen wie Windows Media Player hinzufügen. Administratoren können dann eine Reihe von Einstellungen für jede Anwendung definieren und festlegen, welche Benutzerrollen Zugriff haben.

Hinweis!

Kompatibilität von Drittanbieter-Software

RM Shell ist für die Arbeit mit Software vorgesehen, die mit VisuNet-Geräten von Pepperl+Fuchs geliefert wird. Pepperl+Fuchs übernimmt keine Garantie für die Funktionalität von Drittanbieter-Software. Die Kunden sind dafür verantwortlich, die Kompatibilität mit Software von Drittanbietern sicherzustellen.

Hinweis!

Installieren von Antivirensoftware

Anweisungen zum Installieren von Antivirensoftware Siehe Kapitel 11.5.

Hinweis!

Whitelisting von Anwendungen

RM Shell verwendet einen Dialogfeldfilter, der automatisch alle Anwendungsfenster schließt, die nicht geöffnet werden dürfen. Wenn der Dialogfeldfilter aktiviert ist, müssen Sie möglicherweise Programme und Anwendungen auf die Whitelist setzen, damit die App ordnungsgemäß funktioniert. Anweisungen zum Whitelisting von Programmen siehe Kapitel 8.3.

Hinweis!

Maximale App-Größe

Die maximale Größe der installierten App muss 500 MB erweitern können. Kunden müssen beurteilen, ob App-Größen bis zu einem GB bei Windows Aktualisierungsprozessen Probleme verursachen. Wenn Ihre Apps/Programme eine höhere Leistung und mehr Speicher erfordern, empfehlen wir unsere VisuNet PCs.

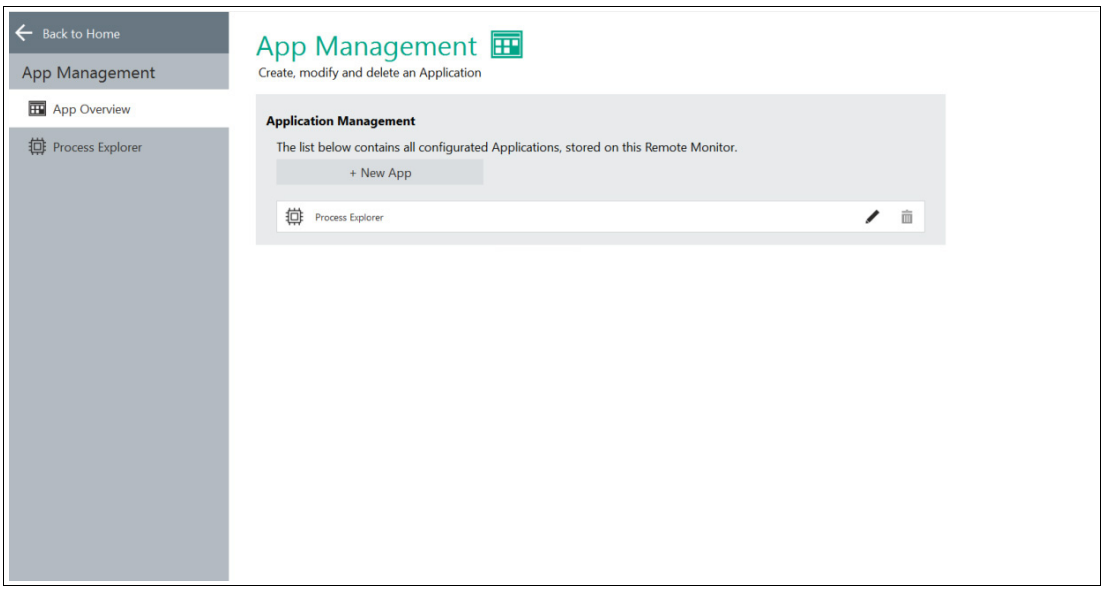


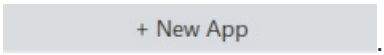
Abbildung 7.1 VisuNet RM Shell-Anwendungsverwaltung

Öffnen von App Management (Anwendungsverwaltung)

1. Um die Anwendungsverwaltung zu öffnen, klicken Sie auf dem Startbildschirm auf das entsprechende Symbol 

.

Erstellen einer App

1. Um eine App zu erstellen, klicken Sie auf 

.
2. Das Fenster "Generic App“ (Generische App) wird geöffnet. Auf diesem Bildschirm können Sie die folgenden Einstellungen festlegen:
   - **Name**: Wählen Sie einen Namen für die App aus oder verwenden Sie den automatisch generierten Namen.
   - **Application path** (Anwendungspfad): Geben Sie den Anwendungspfad manuell ein oder klicken Sie auf das Symbol am Ende des Felds, um danach zu suchen.
   - **Parameter**: Ermöglicht die Übergabe zusätzlicher Befehlszeilenparameter beim Starten der Anwendung. Geben Sie in diese Zeile nur die Parameter für die ausführbare Datei ein. Wenn Sie z. B. das Herunterfahren `shutdown /s /f /t 0` durchführen möchten, fügen Sie dieser Zeile nur `/s /f /t 0` hinzu.
   - **Allowed access** (Zulässiger Zugriff): Wählen Sie aus, welche Benutzerrollen auf die Anwendung zugreifen können.
   - **Autostart**: Startet die App automatisch nach dem Starten des RM/Box Thin Clients.
   - **Maximized** (Maximiert): Wenn diese Option aktiviert ist, wird das Anwendungsfenster beim Öffnen maximiert.
   - **Use default icon** (Standardsymbol verwenden): Wenn diese Option aktiviert ist, wird auf dem Bildschirm des Benutzers ein RM Shell-Standardsymbol angezeigt. Wenn diese Option deaktiviert ist, wird das Standardsymbol der Anwendung auf dem Bildschirm des Benutzers angezeigt.

2024-01

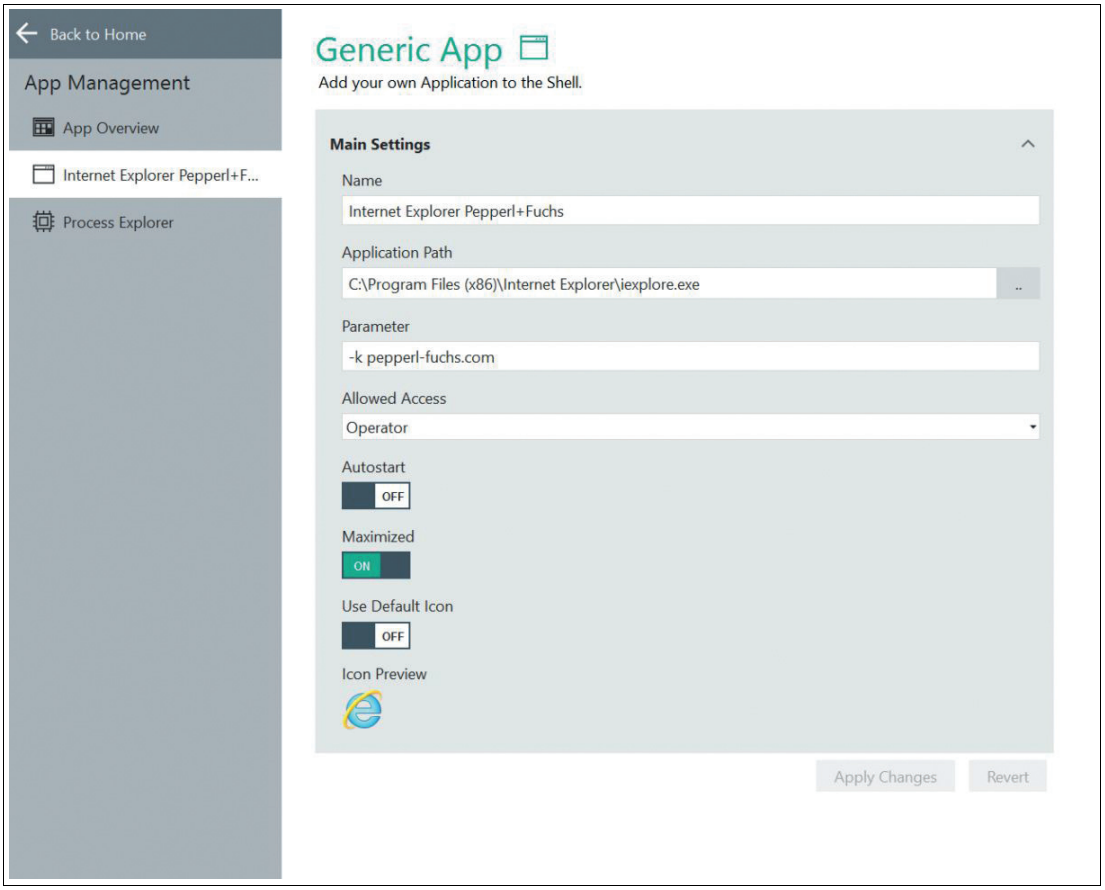


Abbildung 7.2 Im Fenster "Generic App“ (Generische App) können Sie Einstellungen für neue Apps festlegen und Einstellungen für vorhandene Apps anpassen.

↳ Die App wurde erstellt. Eine Kachel, die mit der Anwendung verknüpft ist, wird auf dem Startbildschirm des Benutzers im Bereich "Applications“ (Anwendungen) angezeigt.

Ändern von App-Einstellungen

1. Öffnen Sie App Management (Anwendungsverwaltung) und wählen Sie im Menü auf der linken Seite des Bildschirms die Option "App Overview“ (App-Übersicht) aus.
2. Klicken Sie auf das Symbol neben der Anwendung, die Sie ändern möchten.
3. Nachdem Sie die Einstellungen im angezeigten Fenster bearbeitet haben, klicken Sie auf "Apply changes“ (Änderungen anwenden).

   ↳ Die Änderungen wurden gespeichert.

7.1 App "Wedge“

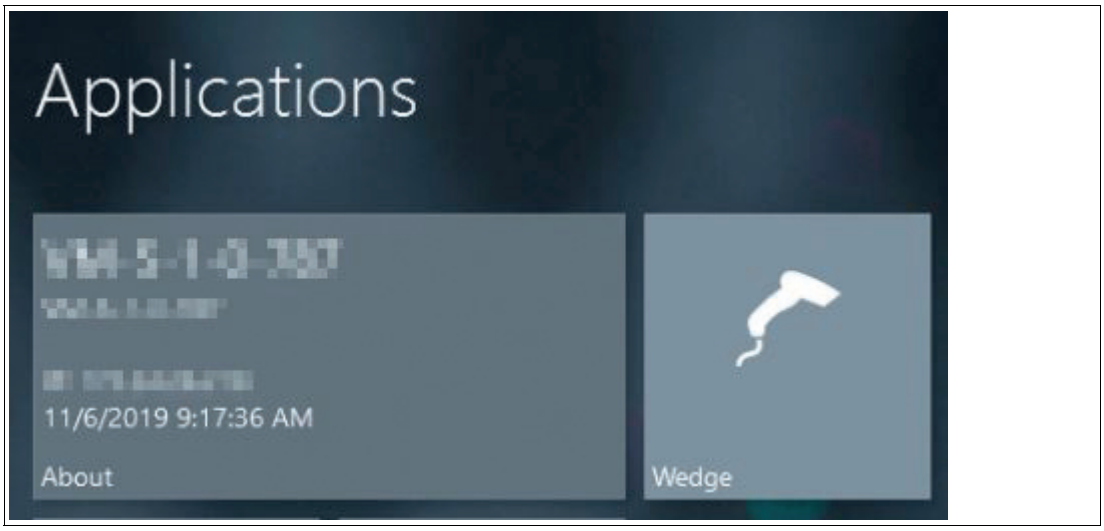


Abbildung 7.3 App "VisuNet RM Shell Wedge“

Die App "Wedge“ ist ein Tastaturemulationsprogramm, das Zeichenfolgen über den seriellen Port einliest und die entsprechenden Tastenkombinationen im RM simuliert. Diese werden dann an Ihren Host-PC gesendet. Die App ist speziell für den Anschluss von Pepperl+Fuchs-Barcodescannern (IDM Handheld 1D- und 2D-Codeleser) konzipiert. Sie ermöglicht die Verwendung eines an den seriellen Port angeschlossen Barcodescanners als Tastatureingabegerät in verschiedenen Anwendungen. Informationen zum Konfigurieren der Wedge-Einstellungen , siehe Kapitel 8.17.

Mit der App "Wedge“ können Benutzer außerdem überprüfen, ob ein Barcodescanner ordnungsgemäß an den seriellen Port angeschlossen und betriebsbereit ist. Die App "Wedge“ ist in allen drei Benutzerrollen verfügbar ("Operator“ (Bediener), "Engineer“ (Ingenieur) und "Administrator“).

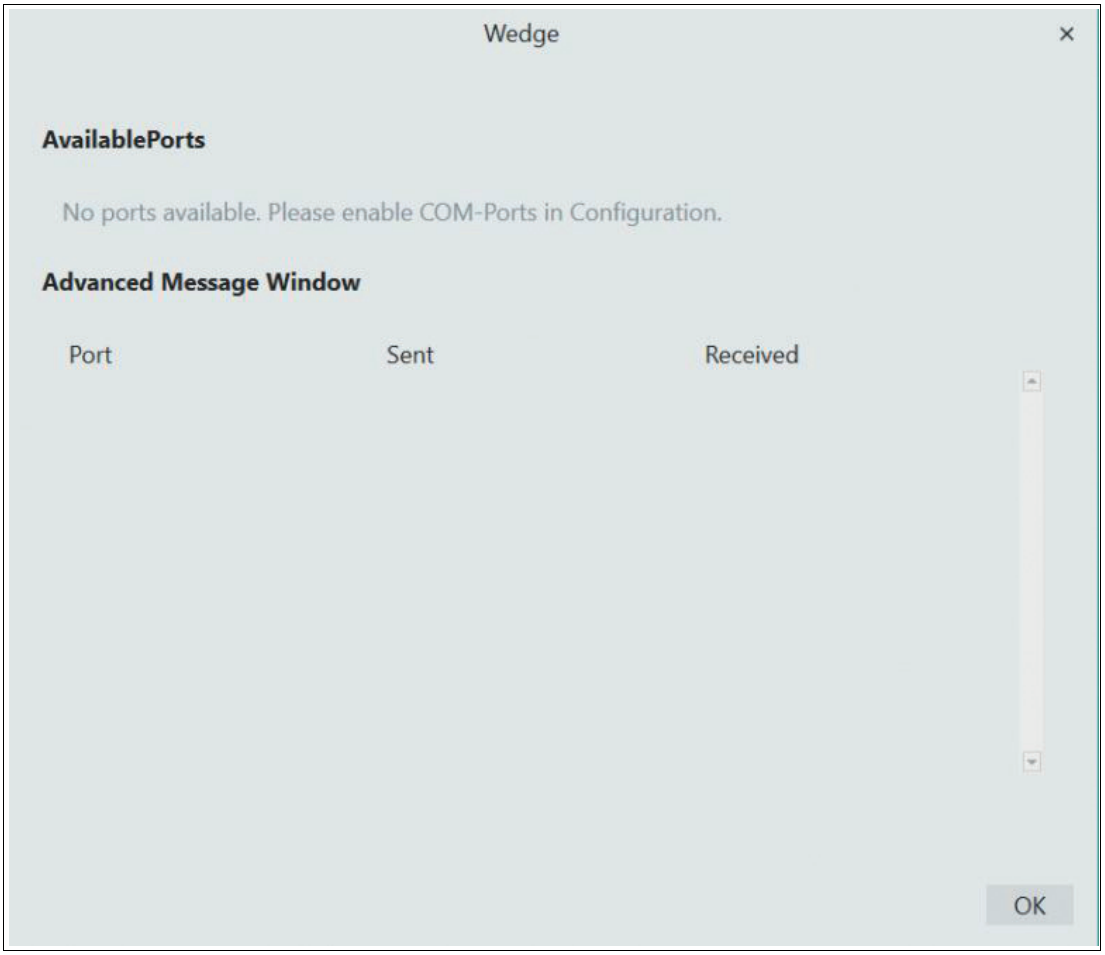


Abbildung 7.4

Hinweis!

Ab VisuNet RM Shell 5.5 ist es möglich, die App "Wedge“ vor dem Bediener zu verbergen. Nähere Informationen finden Sie im Abschnitt 7.16.

7.2 Process Explorer-App

Mit der Process Explorer-App können Sie mehrere Geräteparameter überwachen, einschließlich Speicher, Speichernutzung und CPU-Auslastung. Dieses Tool kann zur Diagnose und zum Testen von RM Shell verwendet werden. Die Benutzerrolle "Administrator“ kann festlegen, welche Benutzer in der App "App Management“ (Anwendungsverwaltung) darauf zugreifen können. Siehe Kapitel 7.

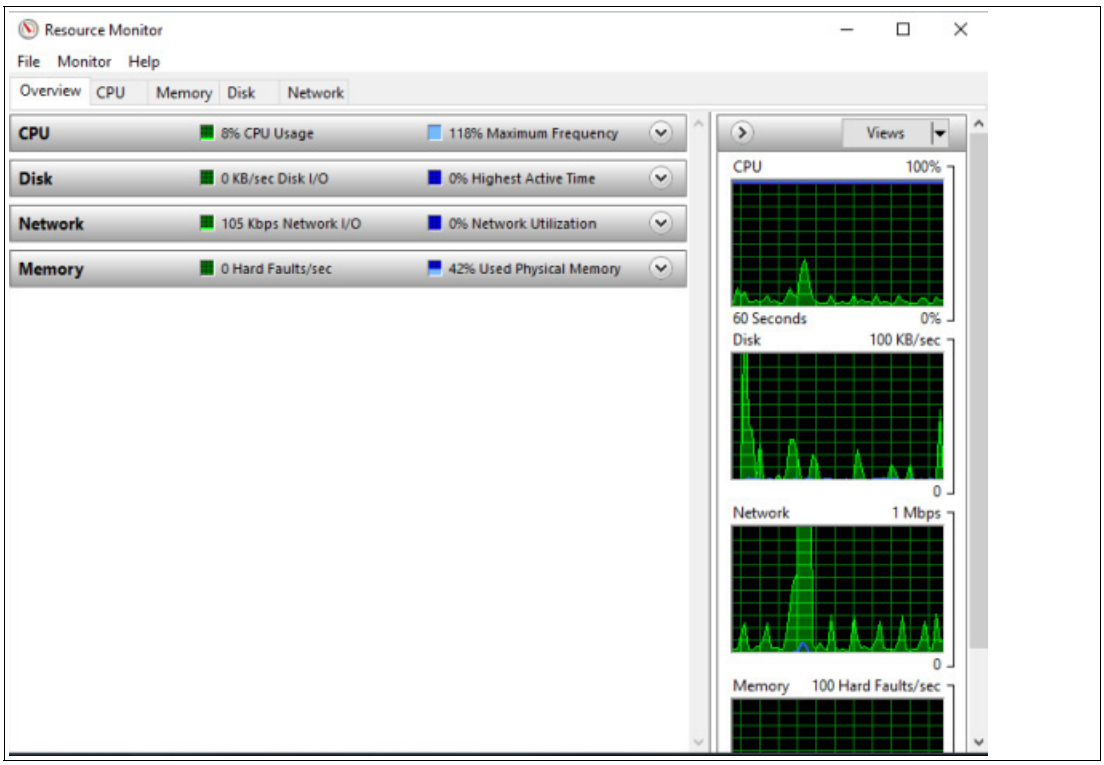


Abbildung 7.5 Process Explorer-Fenster

8 App "System Settings“ (Systemeinstellungen)

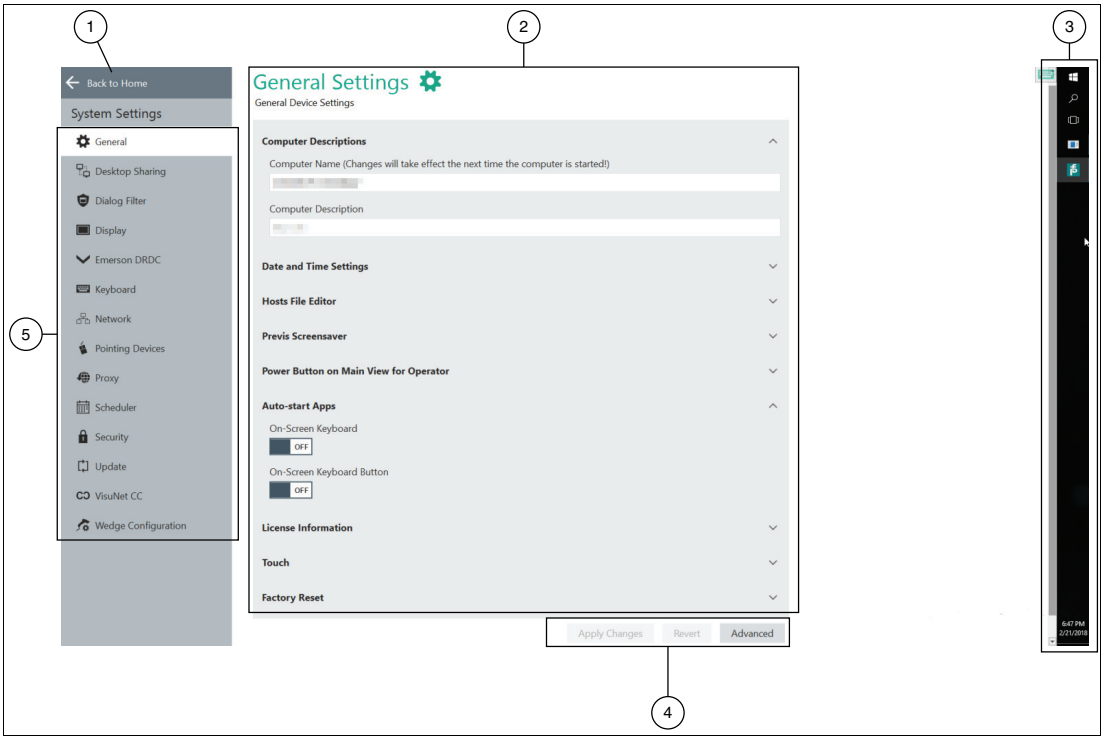


Abbildung 8.1 Bildschirmkomponenten der App "System Settings“ (Systemeinstellungen)

1	Zurück zum Startbildschirm
2	Startseite/Inhaltsseite
3	Windows® Explorer-Seitenleiste. Dieses Element ist nur für Anwender sichtbar, die als "Administrator“ angemeldet sind. Damit können Administratoren Software von Drittanbietern installieren und auf die Windows®-Systemsteuerung zugreifen, um erweiterte Einstellungen anzupassen.
4	• **Apply changes** (Änderungen anwenden): Schreibt geänderte Einstellungen auf den RM. • **Revert** (Zurücksetzen): Verwirft die geänderten Einstellungen und stellt die vorherigen Einstellungen wieder her. • **Advanced** (Erweitert): Nur für die Benutzerrolle Administrator sichtbar. Diese Schaltfläche öffnet zusätzliche Windows®-spezifische Dialogfenster für Einstellungen, die nicht in VisuNet RM Shell enthalten sind, aber möglicherweise für Administratoren nützlich sind.
5	Navigationsleiste mit allen Untermenüs. Jedes Untermenü wird im Folgenden ausführlich erläutert.

Hinweis!

Deaktivieren des Schreibfilters für die persistente Speicherung von Konfigurationen

Um Konfigurationsänderungen persistent zu speichern, deaktivieren Sie den Unified Write Filter (UWF). Nachdem Sie die Konfigurationsänderungen implementiert haben, aktivieren Sie den UWF erneut, um die Änderungen persistent zu speichern.

Hinweis!

Verwendung von Windows®-spezifischen erweiterten Einstellungen

Nachdem Sie die Einstellungen über die Windows®-spezifischen erweiterten Einstellungen geändert haben, müssen diese Einstellungen erneut in VisuNet RM Shell geladen werden, indem der aktuelle VisuNet RM Shell-Unterbildschirm einmal geändert wird.

Aufrufen der App "System Settings“ (Systemeinstellungen)

1. Rufen Sie die App "System Settings“ (Systemeinstellungen) auf, indem Sie auf das entsprechende Symbol auf dem Startbildschirm klicken 

.

Verwenden Sie diese App, um Ihre RM/BTC-Einstellungen zu verwalten. Das Untermenü "General Settings“ (Allgemeine Einstellungen) wird standardmäßig angezeigt, wenn Sie die App öffnen. Außerdem gibt es mehrere Untermenüs:

- **General**
  Legen Sie allgemeine Einstellungen wie Computerbeschreibung, Systemsprache, Datum und Uhrzeit, Previs-Bildschirmschoner, Konfiguration des Netzschalters und Lizenzinformationen fest. Siehe Kapitel 8.1.
- **Desktop Sharing**
  Verwalten Sie die Einstellungen für die Freigabe eines RM-Bildschirms. Siehe Kapitel 8.2.
- **Dialogfeldfilter**
  Fügen Sie Anwendungen einer Whitelist hinzu, um zu verhindern, dass sie vom Dialogfeldfilter geschlossen werden. Siehe Kapitel 8.3.
- **Anzeige**
  Verwalten Sie Display-Einstellungen wie Auflösung, Farbtiefe und Bildwiederholfrequenz. Siehe Kapitel 8.4.
- **Tastatur**
  Verwalten Sie Tastatureinstellungen wie Eingabesprache, Zeichenwiederholung und Mauszeiger-Blinken. Siehe Kapitel 8.7.
- **Network**
  Verwalten Sie Netzwerkeinstellungen wie Netzwerkadapter-Informationen und IP-Adresseinstellungen. Siehe Kapitel 8.8.
- **Pad-Ex**
  Verwalten Sie Ihre Pad-Ex-Einstellungen, indem Sie die Aktion für die Programmtaste oder die Drehsperre auswählen. Siehe Kapitel 8.9
- **Pointing Devices (Zeigegeräte)**
  Verwalten Sie Einstellungen für Zeigegeräte wie Empfindlichkeit oder Tastenverhalten des Zeigegerätes. Siehe Kapitel 8.10.
- **Proxy**
  Aktivieren Sie Proxy und verwalten Sie Proxy-Einstellungen. Siehe Kapitel 8.11.
- **Scheduler**
  Planen Sie regelmäßige Systemneustarts. So kann der Unified Write Filter kontinuierlich verwendet werden, ohne dass der Speicherpuffer überläuft. Siehe Kapitel 8.12.
- **Sicherheit**
  Richten Sie VisuNet RM Shell-Kennwörter ein und aktivieren Sie Firewalls. Siehe Kapitel 8.13.
- **Touch**
  Konfigurieren Sie Profile für die Berührungsempfindlichkeit. Dieses Untermenü wird nur angezeigt, wenn der verwendete RM mit dieser Option ausgestattet ist. Siehe Kapitel 8.14.
- **Update (Aktualisierung)**
  Aktivieren Sie Remote-Updates oder suchen Sie nach lokalen Updates. Siehe Kapitel 8.15.
- **VisuNet CC**
  Konfigurieren Sie VisuNet Control Center. Siehe Kapitel 8.16

2024-01

- **Wedge Configuration (Wedge-Konfiguration)**
  Verwalten Sie Einstellungen für die Wedge-Konfiguration wie Eingabezeichenverzögerung und Eingabemodus für Remote-Text. Definieren Sie zugeordnete Funktionen für HEX-Codes. Siehe Kapitel 8.17.

8.1 General Settings (Allgemeine Einstellungen)

Computer Descriptions (Computerbeschreibungen)

In diesem Abschnitt können Sie den Namen und die Beschreibung des lokalen RM/BTC bearbeiten und andere Domänen einbinden.

Funktion	Beschreibung
Computer Name (Computername)	Dieses Feld zeigt den aktuellen Computernamen des RM/BTC an. Um den Namen zu ändern, klicken Sie in das Feld und geben Sie einen neuen Namen ein. Die Änderungen werden wirksam, wenn der RM/BTC neu gestartet wird.
Computer Description (Computer-Beschreibung)	Dieses Feld enthält eine Beschreibung des RM/BTC. Sie können die Beschreibung bearbeiten, z. B. um zu beschreiben, wo sich der RM/BTC in Ihrem Produktprozess befindet (z. B. "Fertigungsbereich“). Die Beschreibung wird auf dem VisuNet RM Shell-Startbildschirm unter dem Computernamen auf der Kachel "About“ (Info) angezeigt. Um die Beschreibung zu bearbeiten, klicken Sie in das Feld und geben Sie eine Beschreibung ein.

Date and Time Settings (Datums- und Uhrzeiteinstellungen)

In diesem Abschnitt können Sie Datum und Uhrzeit der RMs/BTCs einrichten.

Die Datums- und Uhrzeiteinstellungen des RM/BTC müssen mit den Datums- und Uhrzeiteinstellungen des Hosts übereinstimmen.

Funktion	Beschreibung
Datum	Dieses Feld zeigt das aktuell definierte Datum an.
Zeit	Dieses Feld zeigt die aktuell definierte Zeit an.
Configure Date and Time (Datum und Uhrzeit konfigurieren)	Klicken Sie auf die Schaltfläche "Configure Date and Time“ (Datum und Uhrzeit konfigurieren), um Datum und Uhrzeit zu konfigurieren. Das Windows®-Dialogfenster für Datum und Uhrzeit wird geöffnet.
Configure Regional Settings (Regionale Einstellungen konfigurieren)	Klicken Sie auf die Schaltfläche "Configure Regional Settings“ (Regionale Einstellungen konfigurieren), um die regionalen Einstellungen zu konfigurieren. Das Windows®-Dialogfenster für Region und Sprache wird geöffnet.

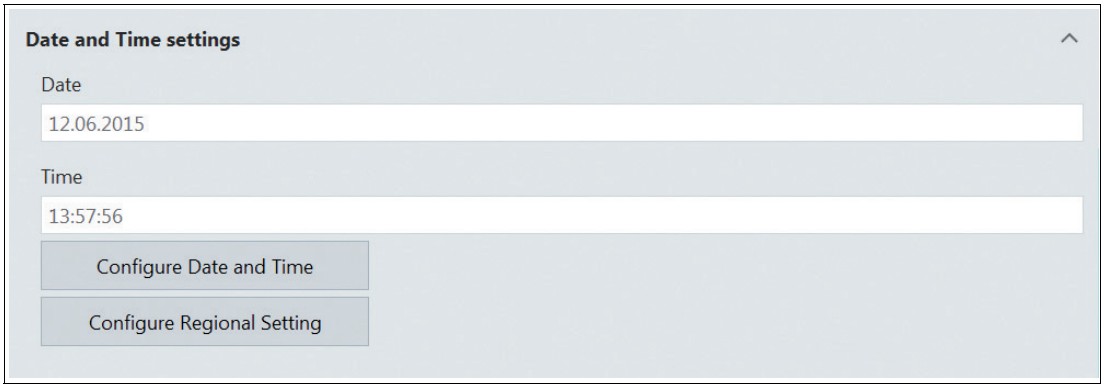


Abbildung 8.2 Allgemeine Einstellungen – Einstellungen für Datum und Uhrzeit

Vorsicht!

Zeitzone, Datum und Uhrzeit

Stellen Sie sicher, dass der RM/BTC mit der richtigen Zeitzone, dem richtigen Datum und der richtigen Uhrzeit eingerichtet ist. Verschlüsselte Kommunikationsprotokolle (z. B. die zwischen VisuNet RM Shell und VisuNet Control Center verwendeten) erfordern zwischen beiden Kommunikationspartnern synchronisierte Datums- und Uhrzeiteinstellungen. Der maximal mögliche Datums- und Zeitunterschied beträgt 12 Stunden.

License information (Lizenzinformationen)

In diesem Abschnitt finden Sie Informationen zur gegenwärtig verwendeten VisuNet RM Shell-Lizenz. Nur die Benutzerrolle "Administrator“ verfügt über die Rechte zum Anzeigen der Lizenzinformationen.

Funktion	Beschreibung
Applied Licenses (Angewendete Lizenzen)	Hier sehen Sie die eingegebenen Lizenzen Ihres Gerätes. Sie können diese auch löschen.
Add new license (Neue Lizenz hinzufügen)	Wenn Sie PRO-, DRDC- oder CC-Lizenzschlüssel erworben haben, geben Sie Ihre Lizenzschlüssel ein, um weitere Funktionen der VisuNet RM Shell PRO-, DRDC- oder VisuNet CC-Version zu aktivieren. Klicken Sie auf "Apply“ (Anwenden). Die Änderungen werden wirksam, wenn der RM/BTC neu gestartet wird.
License key (Lizenzschlüssel)	Wenn Sie PRO-Lizenzschlüssel erworben haben, geben Sie Ihre Lizenzschlüssel ein, um zusätzliche Funktionen der VisuNet RM Shell PRO-Version zu aktivieren. Klicken Sie auf "Apply“ (Anwenden). Die Änderungen werden wirksam, wenn der RM/BTC neu gestartet wird.

Abbildung 8.3 Allgemeine Einstellungen – Lizenzinformationen

Previs-Bildschirmschoner

In diesem Abschnitt werden die Einstellungen für den Previs-Bildschirmschoner beschrieben.

Previs ist ein Bildschirmschoner, der das permanente Nachleuchten oder Geisterbilder auf LC-Displays verhindert, wobei gleichzeitig das Prozessbild dargestellt wird. Die Prozessbilder bleiben sichtbar und Sie haben immer direkten Zugriff auf alle wichtigen Prozessinformationen.

Funktion	Beschreibung
Idle Time before starting (Leerlaufzeit vor dem Start)	Geben Sie die Zeitdauer der Inaktivität ein. Nach diesem Zeitfenster wird Previs gestartet. Wenn die Zeit auf 0 Min. eingestellt wird, ist der Bildschirmschoner deaktiviert.
Effect Intensity (Effektintensität)	Konfigurieren Sie die Intensität des Bildschirmschoners. Höhere Werte ermöglichen einen besseren Schutz gegen Einbrennen des Bildschirms.
PIN (nur numerische Zeichen!)	Mit der zusätzlichen PRO-Lizenz können Sie eine PIN festlegen, sodass nur berechtigte Personen das Gerät entsperren können.
Previs beim Start von Shell starten	Nach einem Neustart des Geräts muss jede Benutzerrolle die PIN eingeben, um das Gerät zu entsperren (PRO-Lizenz erforderlich).

Hinweis!

Um die PIN des Previs-Bildschirmschoners verwenden zu können, ist eine zusätzliche PRO-Lizenz erforderlich.

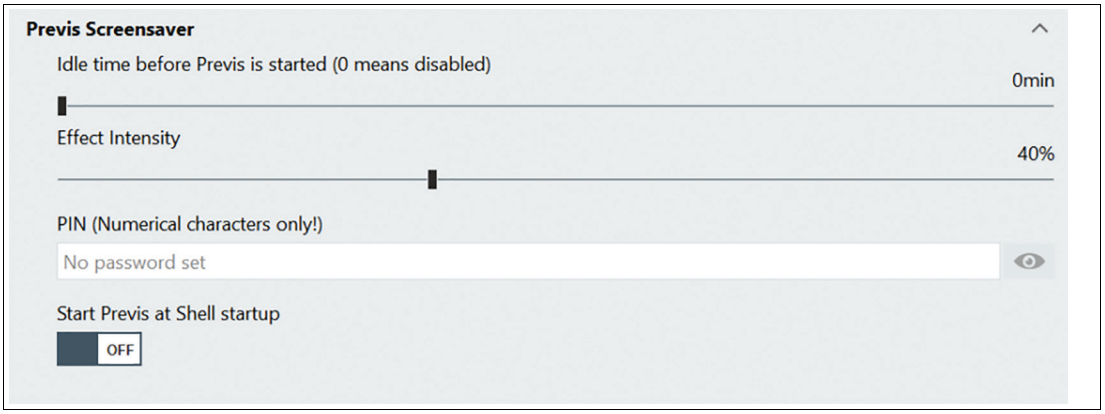


Abbildung 8.4 Allgemeine Einstellungen – Previs-Bildschirmschoner

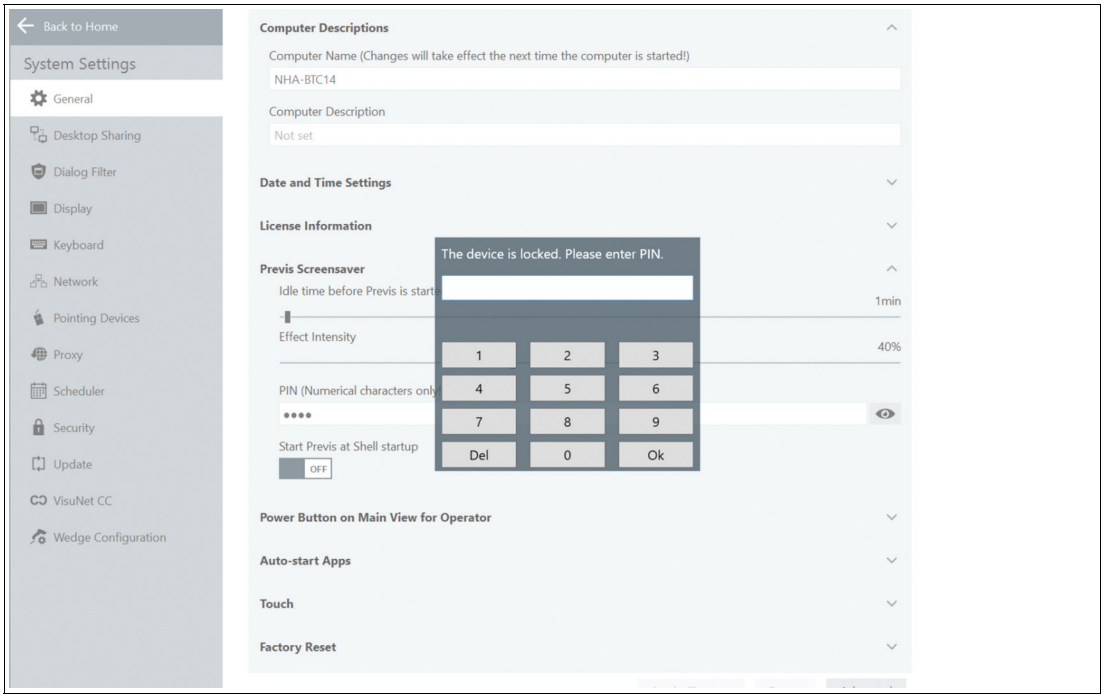


Abbildung 8.5 Geben Sie Ihr numerisches Kennwort über die Tastatur ein

Power Button on Main View for Operator (Netzschalter auf dem Hauptbildschirm für Bediener)

In diesem Abschnitt können Sie das Verhalten des Netzschalters, der sich in den Systemfunktionen auf dem Startbildschirm befindet, festlegen. Siehe Kapitel 4.

Der Netzschalter hat mehrere Funktionen, die für die Benutzerrolle "Operator“ (Bediener) eingerichtet werden können. Die Benutzerrolle "Operator“ (Bediener) darf nur die vorkonfigurierten Optionen durchführen.

Funktion	Beschreibung
Show "Restart“ Button (Schaltfläche "Neu starten“ anzeigen)	Aktiviert die Funktion "Restart“ (Neustart) im Menü "Power Button“ (Netzschalter) auf dem Startbildschirm. Wenn diese Funktion aktiviert ist, kann die Benutzerrolle "Operator“ (Bediener) den RM/BTC neu starten.
Show "Shutdown“ Button (Schaltfläche "Herunterfahren“ anzeigen)	Aktiviert die Funktion "Shutdown“ (Herunterfahren) im Menü "Power Button“ (Netzschalter) auf dem Startbildschirm. Wenn diese Funktion aktiviert ist, kann die Benutzerrolle "Operator“ (Bediener) den RM/BTC herunterfahren.
Show "Turn off display“ Button (Schaltfläche "Anzeige ausschalten“ anzeigen)	Aktiviert die Funktion "Turn off Display“ (Display ausschalten) im Menü "Power Button“ (Netzschalter) auf dem Startbildschirm. Wenn diese Funktion aktiviert ist, kann die Benutzerrolle "Operator“ (Bediener) die Anzeige ausschalten. Die Anzeige kann durch Bewegen des Zeigegeräts wieder eingeschaltet werden. Abhängig von der RM/BTC-Hardware schaltet diese Funktion möglicherweise die Hintergrundbeleuchtung bei einigen Geräten nicht aus, sondern schaltet nur den Bildschirm dunkel.

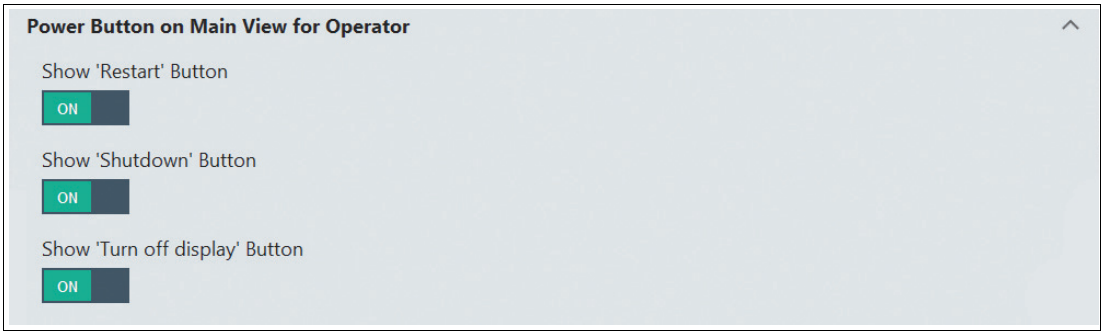


Abbildung 8.6 Allgemeine Einstellungen – Power-Schaltfläche auf der Startseite für Benutzer

Bildschirmtastatur-Einstellungen

In diesem Abschnitt können Sie konfigurieren, welche Apps sofort nach dem Starten von RM/BTC gestartet werden sollen.

Funktion	Beschreibung
Start On-Screen Keyboard with VisuNet RM Shell (Starten der Bildschirmtastatur mit VisuNet RM Shell)	Sorgt dafür, dass die Bildschirmtastatur beim Starten des RM/BTC direkt gestartet wird.
Start On-Screen Keyboard Button with VisuNet RM Shell (Starten der Bildschirmtastatur-Schaltfläche mit VisuNet RM Shell)	Zeigt eine schwebende Tastaturschaltfläche an, mit der die Bildschirmtastatur geöffnet wird.
Use Touch keyboard instead of On-Screen Keyboard (Verwenden der Touchscreen-Tastatur anstelle der Bildschirmtastatur)	Sorgt dafür, dass die Touchscreen-Tastatur beim Starten des RM/BTC direkt gestartet wird.

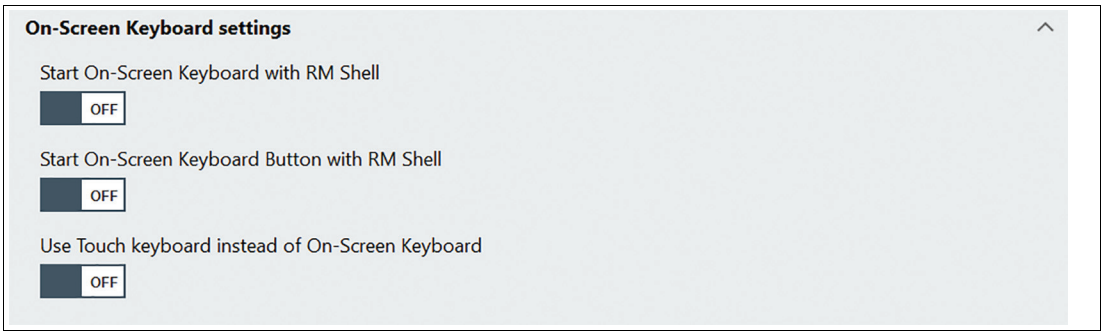


Abbildung 8.7 Bildschirmtastatur-Einstellungen

Schnellmenüeinstellungen

In diesem Abschnitt können Sie das schwebende Schnellmenü aktivieren oder deaktivieren.

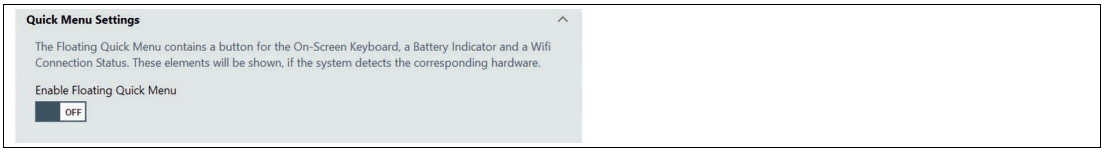


Abbildung 8.8

Abbildung 8.9

Das schwebende Menü kann nach Bedarf positioniert werden, indem Sie es einfach mit der Maus bewegen.

Klicken Sie auf das Symbol, um die Bildschirmtastatur oder weitere Informationen zum Akku-/WLAN-Status anzuzeigen.

Hintergrundbild und Logo

In diesem Abschnitt können Sie das Hintergrundbild und das Logo anpassen.

Um Ihr individuelles Hintergrundbild oder Logo hinzuzufügen, klicken Sie auf  .

Einstellungen der Hauptansicht

In diesem Abschnitt können Sie Funktionen für die Rolle "Operator“ (Bediener) ausblenden.

Funktion	Beschreibung
Hide System Tools from Operator (System-tools für Bediener ausblenden)	Die Kachel "System Tools“ (System-Tools) wird für die Rolle "Operator“ (Bediener) nicht mehr angezeigt.
Hide IP address from About Tile from Operator (IP-Adresse auf der Kachel "About“ (Info) für Bediener ausblenden)	Die IP-Adresse wird nicht mehr angezeigt.

Abbildung 8.10

Touch

In diesem Abschnitt können Sie den verwendeten Touchscreen-Typ auswählen. Wenn Ihr System nicht über einen Touchscreen verfügt, wählen Sie im Dropdown-Menü "None“ (Keinen) aus.

Hinweis!

Dies betrifft nicht die installierten Treiber, sondern nur die Benutzerschnittstelle.

Abbildung 8.11 Allgemeine Einstellungen – Touchscreen-Typ

Werksseitige Rückstellung

In diesem Abschnitt können Sie das System neu starten, indem Sie eine Image-Datei anwenden, wenn Sie VisuNet RM Shell 5.3 oder höher verwenden. Die Image-Dateien werden entweder von Pepperl+Fuchs bereitgestellt, oder Sie können Ihre eigene Image-Datei in einem früheren Schritt aufnehmen. Die Image-Dateien gelten nur für dasselbe Gerät mit derselben Seriennummer. Ausführliche Anweisungen zur werksseitigen Rückstellung finden Sie in siehe Kapitel 10

Funktion	Beschreibung
Reboot to Factory reset (Neustart mit werksseitiger Rückstellung)	Verwalten Sie die verfügbare Firmware für VisuNet RM Shell. Sie können eine Image-Datei aufnehmen oder anwenden.

8.2 Desktop Sharing

Funktion	Beschreibung
VisuNet Desktop Sharing Server Enabled (VisuNet Desktop Sharing-Server aktiviert)	Mit dieser Funktion wird der aktuelle RM/BTC als VisuNet RM Master eingerichtet. Die Funktion ermöglicht es anderen RMs/BTCs mit dem entsprechenden Desktop Sharing-Profil die Anzeige des RM-/BTC-Masters widerzuspiegeln. Für weitere Informationen siehe Kapitel 6.4.
Share display (Display freigeben)	Optionale Einstellung: Wenn der VisuNet RM Master über mehrere externe Displays verfügt (z. B. industrieller Box Thin Client BTC), können Sie auswählen, welches Display mit einem VisuNet RM Slave gemeinsam genutzt werden soll.
Desktop sharing password (Desktop Sharing-Kennwort)	Legen Sie Ihr eigenes Kennwort fest oder setzen Sie das Kennwort auf das Standardkennwort zurück.

Hinweis!

Die Desktop Sharing-Funktion wird auch für die Funktionalität "Session Shadowing“ (Sitzungs-Shadowing) in VisuNet Control Center verwendet. Diese Funktion muss aktiviert sein, damit das Shadowing eines RM/BTC über das Control Center möglich ist.

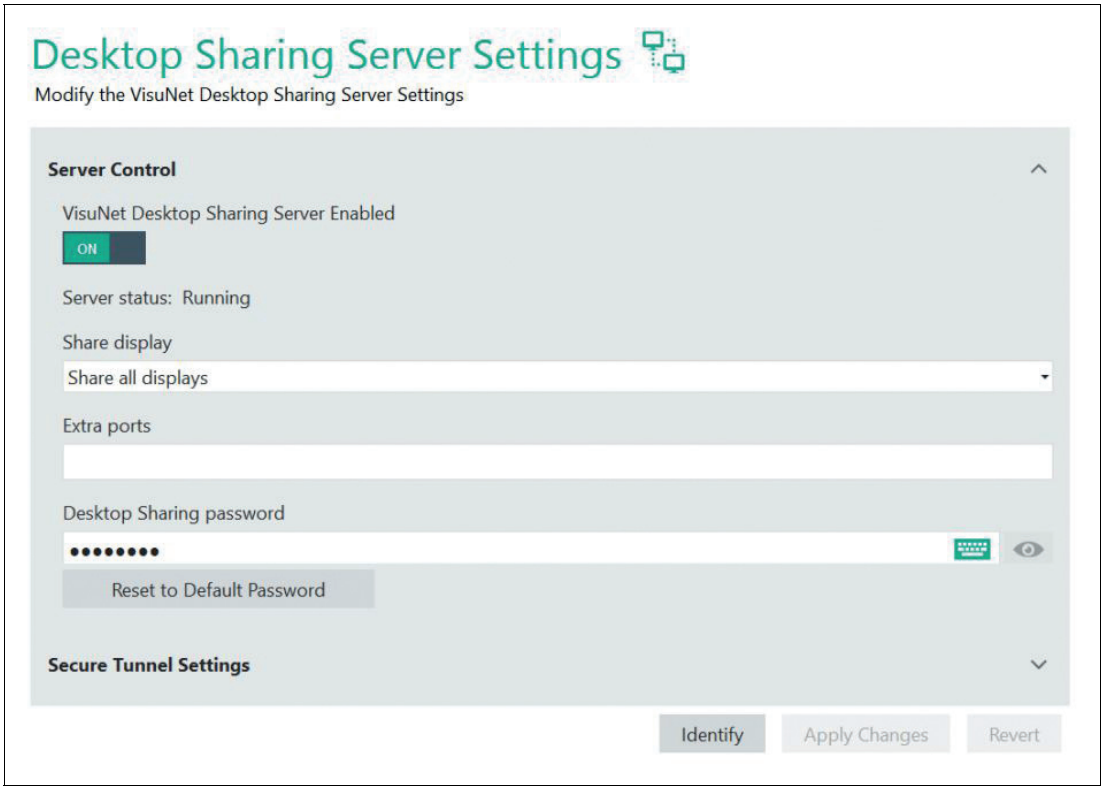


Abbildung 8.12 Desktop Sharing-Servereinstellungen

Wenn Sie das Sitzungs-Shadowing aktivieren, werden die Einstellungen für sicheren Tunnel ebenfalls standardmäßig aktiviert. Wir empfehlen, das Standardzertifikat nicht zu verwenden, sondern Ihr eigenes Zertifikat, um die Sicherheit noch weiter zu erhöhen.

Secure Tunnel Settings (Einstellungen für sicheren Tunnel)

Funktion	Beschreibung
Secure Tunnel Service Enabled (Sicherer Tunneldienst aktiviert)	Zusätzliche Erhöhung der Sicherheit
Service Status (Dienst-Status): Stopped	Rückmeldung der Einstellungen. Kontrollfunktion, ob der Dienst tatsächlich gestartet wurde.
Secure Tunnel Port (Port für sicheren Tunnel)	Wir empfehlen die Verwendung der Standardeinstellung.
Use the default certificate (Standardzertifikat verwenden) (nicht empfohlen)	Wir empfehlen, ein eigenes Zertifikat zu verwenden
Select your certificate (Zertifikat auswählen)	Laden Sie Ihr eigenes vertrauenswürdiges Root-Zertifikat hoch

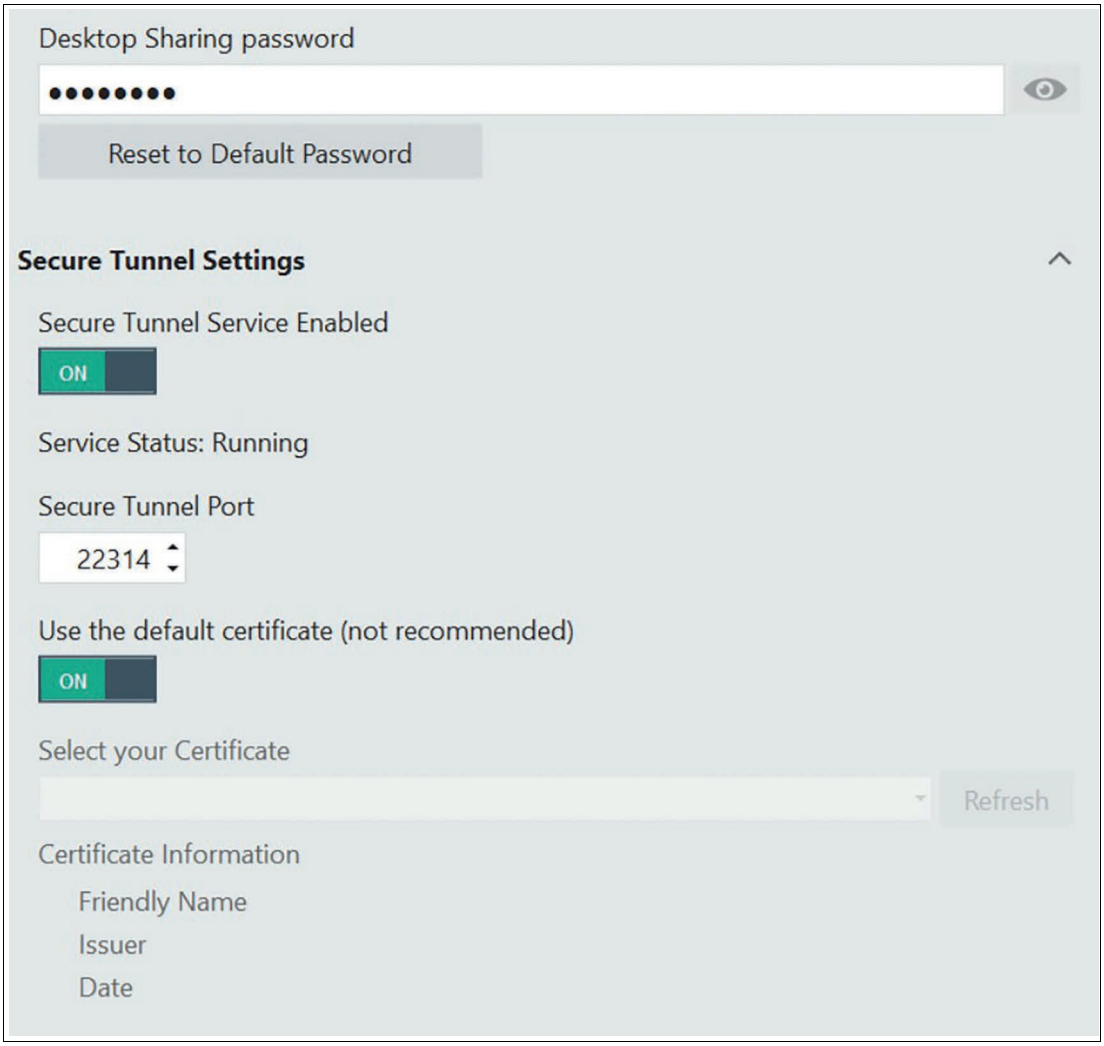
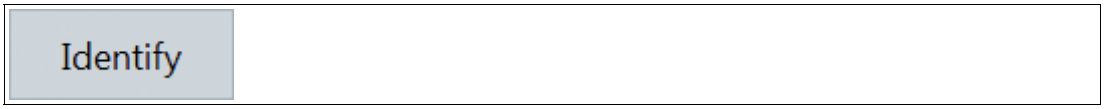


Abbildung 8.13 Einstellungen für sicheren Tunnel - wir empfehlen, Ihr eigenes Zertifikat hochzuladen

Weitere Informationen zum Hochladen Ihres eigenen Zertifikats siehe Kapitel 6.4.

Schaltfläche "Identify“ (Identifizieren)

Wenn Sie Systeme mit mehr als einem externen Display verwenden (z. B. erweiterte Desktop-Systeme, Pepperl+Fuchs-BTC), wird diese Schaltfläche angezeigt. Verwenden Sie die Schaltfläche, um die verschiedenen Anzeigen zu identifizieren. Die Nummer der jeweiligen Anzeige wird auf jedem Monitor angezeigt.



8.3 Dialogfeldfilter

Der Dialogfeldfilter schließt alle Anwendungsfenster, die nicht in der Whitelist enthalten sind, und verhindert, dass Benutzer auf das Dateisystem oder nicht autorisierte Programme zugreifen. In diesem Abschnitt kann der Administrator Prozesse und Anwendungsfenster auf die Whitelist setzen. Dadurch wird verhindert, dass sie durch den Dialogfeldfilter geschlossen werden. In der Administratorrolle ist der Dialogfeldfilter nicht aktiviert.

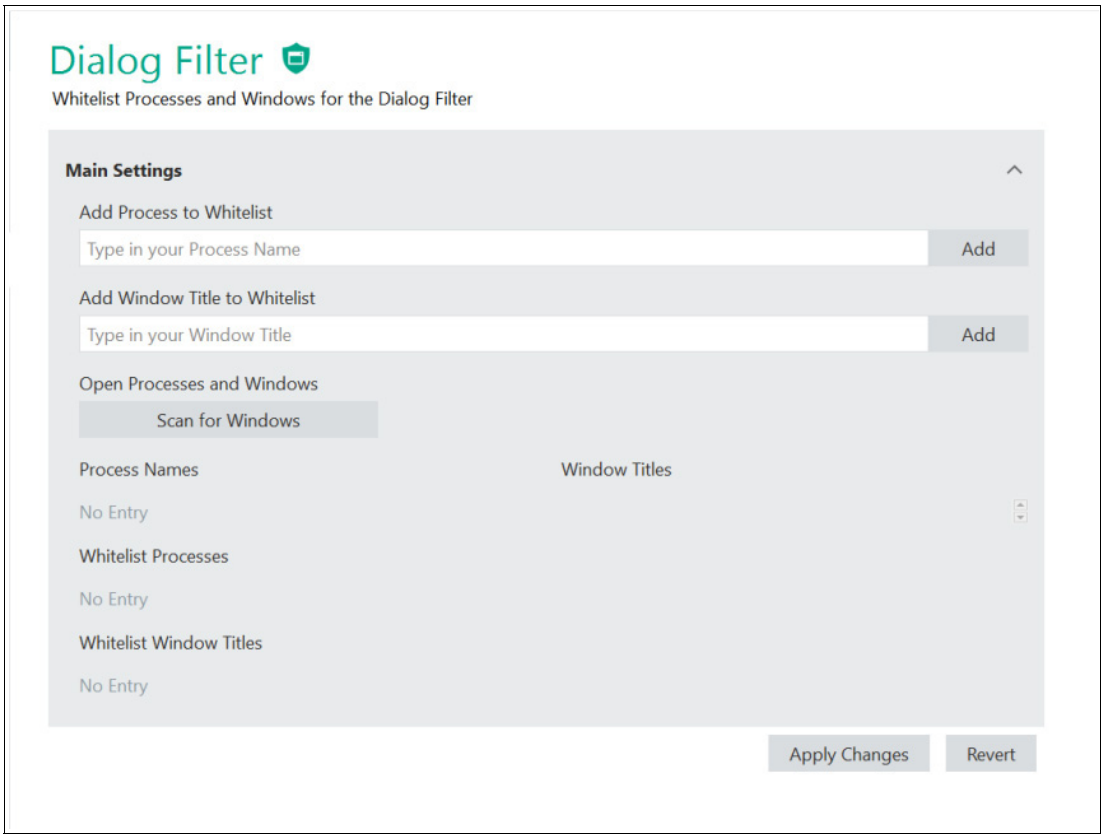


Abbildung 8.14 Dialogfeldfiltereinstellungen

Funktion	Beschreibung
Add Process to Whitelist (Prozess zu Whitelist hinzufügen)	Geben Sie den Namen eines Windows-Prozesses ein, um ihn der Whitelist hinzuzufügen. Fügen Sie beispielsweise "Explorer“ hinzu.
Add Window Title to Whitelist (Fenstertitel zu Whitelist hinzufügen)	Geben Sie den Prozessnamen so ein, wie er in einem Fenster angezeigt wird, um ihn der Whitelist hinzuzufügen. Fügen Sie beispielsweise "Internet Explorer“ hinzu.
Open Processes and Windows (Prozesse und Fenster öffnen)	Damit können Sie nach Prozessen suchen, die derzeit ausgeführt werden. Nachdem Sie auf "Scan for Windows“ (Nach Fenstern suchen) geklickt haben, wählen Sie einen Prozess für die Whitelist aus, indem Sie auf das Pluszeichen neben einem Prozess klicken.

2024-01

Abbildung 8.15

Alle Prozesse, die derzeit ausgeführt werden, können mit der Funktion "Scan for Windows“ (Nach Fenstern suchen) gesucht werden.

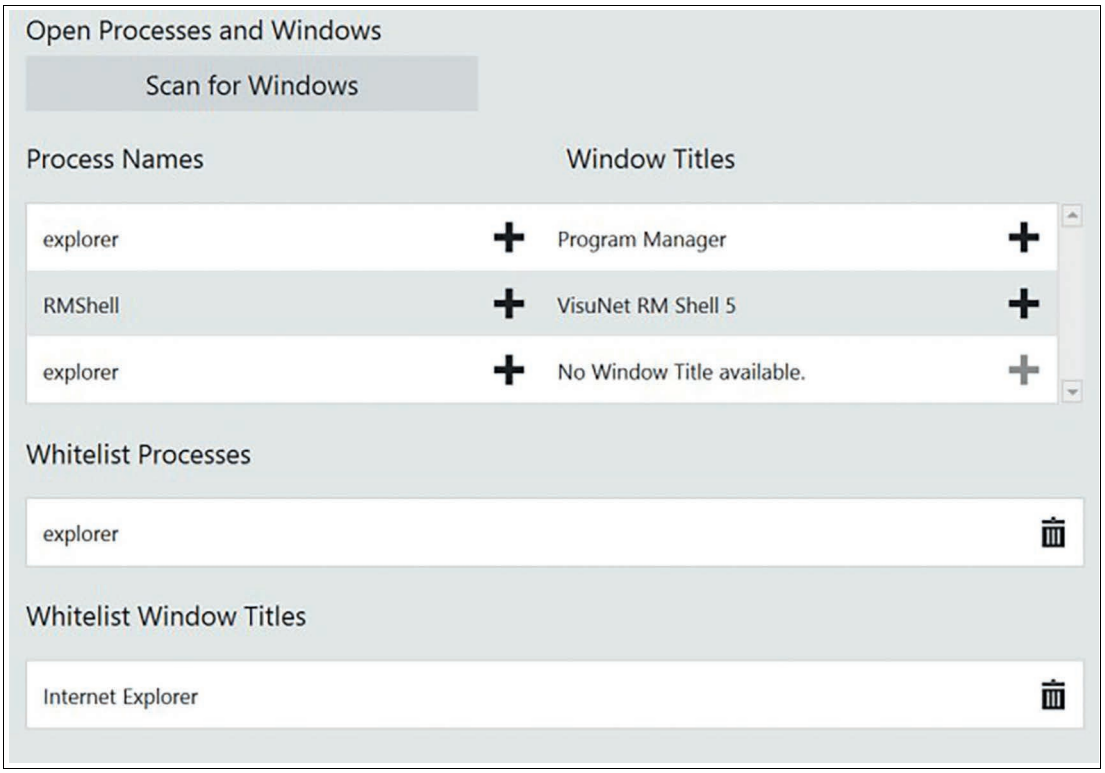


Abbildung 8.16

Scan for Windows (Nach Fenstern suchen)

Sucht alle Fenster, die in den letzten 60 Sekunden geöffnet waren. Die Suche wird im Hintergrund ausgeführt, auch wenn Sie zu einer anderen Seite navigieren. So können Sie Ihre allgemeinen Apps öffnen und alle erforderlichen Fenster und Prozesse scannen.

Klicken Sie auf ✚, um den gewünschten Prozess zur Whitelist hinzuzufügen. Fügen Sie einen Titel hinzu, um der Whitelist mit "Add Window Title to Whitelist“ (Fenstertitel zu Whitelist hinzufügen) einen Fenstertitel hinzuzufügen, der daraufhin im Fenster angezeigt wird.

8.4 Display Settings (Display-Einstellungen)

8.4.1 Konfigurieren eines einzelnen Monitors

Funktion	Beschreibung
Auflösung	Wählen Sie Resolution (Auflösung), Color Depth (Farbtiefe) und Refresh Frequency (Bildwiederholfrequenz) aus. Wählen Sie für optimale Ergebnisse die höchstmögliche native Auflösung.

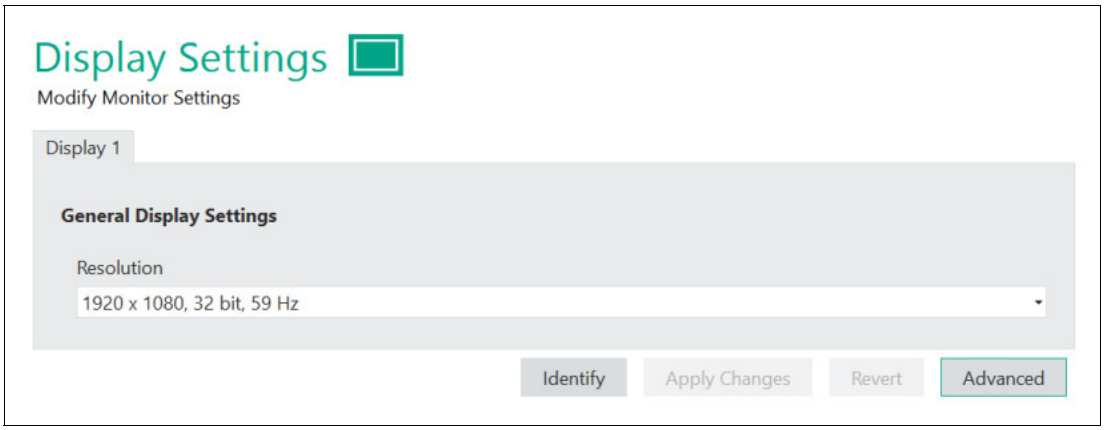


Abbildung 8.17 Display-Einstellungen

Hinweis!

Wir empfehlen die Verwendung der Standardeinstellungen.

8.4.2 Konfigurieren mehrerer Monitore

Wenn Sie einen Box Thin Client mit mehreren Monitoren verwenden, wird jeder Monitor in der Ansicht "Display Settings“ (Display-Einstellungen) als einzelne Registerkarte angezeigt.

Hinweis!

Monitornummerierung

Die in VisuNet RM Shell verwendete Monitornummerierung entspricht nicht den Zahlen in den Anzeigeeinstellungen von Windows®. Die Nummerierung in VisuNet RM Shell wird verwendet, um Profile der richtigen Bildschirmnummer zuzuweisen.

Mit der Schaltfläche "Identify“ (Identifizieren) können Sie die Display-Nummerierung der angeschlossenen Monitore überprüfen.

Um die Ausrichtung/Reihenfolge der angeschlossenen Monitore zu ändern, wechseln Sie zu "Advanced Settings“ (Erweiterte Einstellungen).

Im Fenster "Screen Resolution“ (Bildschirmauflösung) können Sie die Reihenfolge und Anordnung der angeschlossenen Monitore per Maus anpassen:

Neuanordnen angeschlossener Monitore

1. Ziehen Sie die Anzeige, die Sie neu anordnen möchten, mit der Maus und verschieben Sie sie an die neue Position.
2. Speichern Sie die Änderungen, indem Sie auf "Apply“ (Anwenden) klicken und das Fenster schließen.

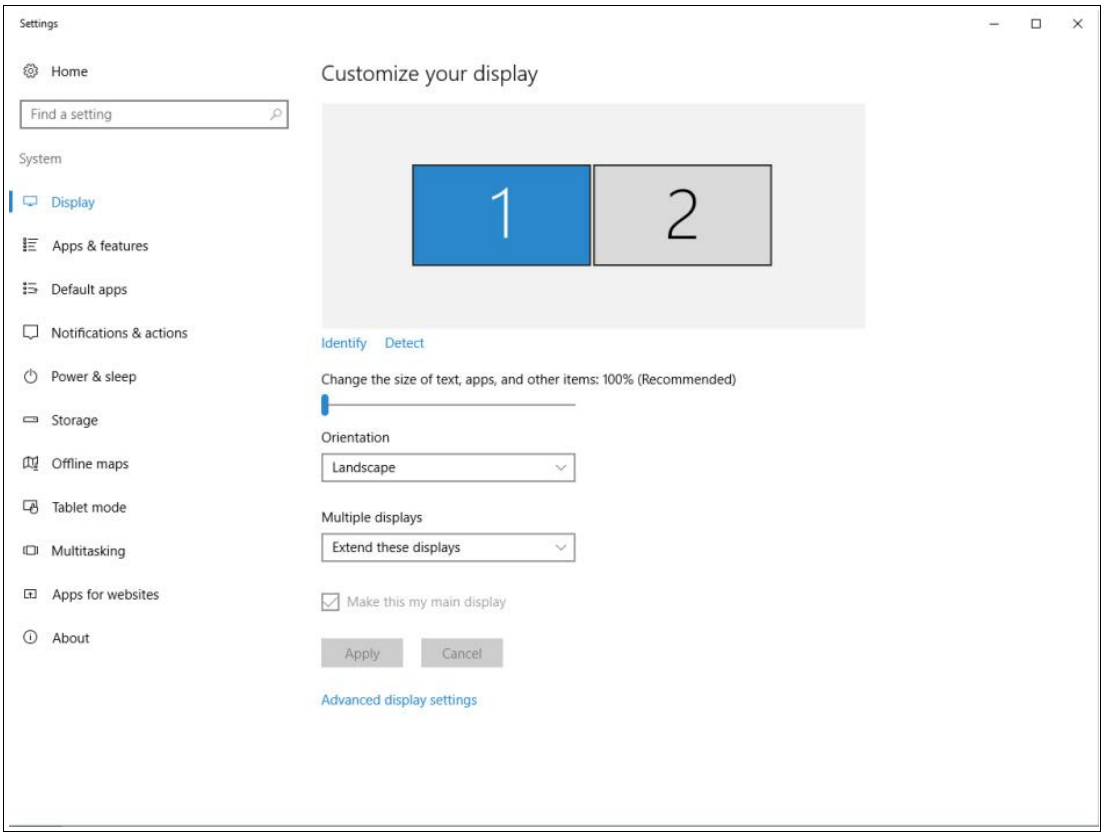


Abbildung 8.18 Neuanordnen mehrerer Monitore

Automatisches Ausrichten eines Setup mit vier Monitoren in einem quadratischen Layout

Funktion	Beschreibung
"Align Four-Monitor Setup“ (Setup mit vier Monitoren ausrichten)	Diese zusätzliche Funktion wird angezeigt, wenn vier Monitore mit den folgenden Anforderungen angeschlossen sind: • Identische Auflösung. • Alle Anzeigen sind im Querformat ausgerichtet. • Die Displays sind in einer annähernden 2x2-Anordnung angeordnet.

1. Erfüllen Sie die Anforderungen.
2. Klicken Sie auf "Align“ (Ausrichten), um automatisch eine genaue 2x2-Quad-Monitor-Anordnung einzurichten.

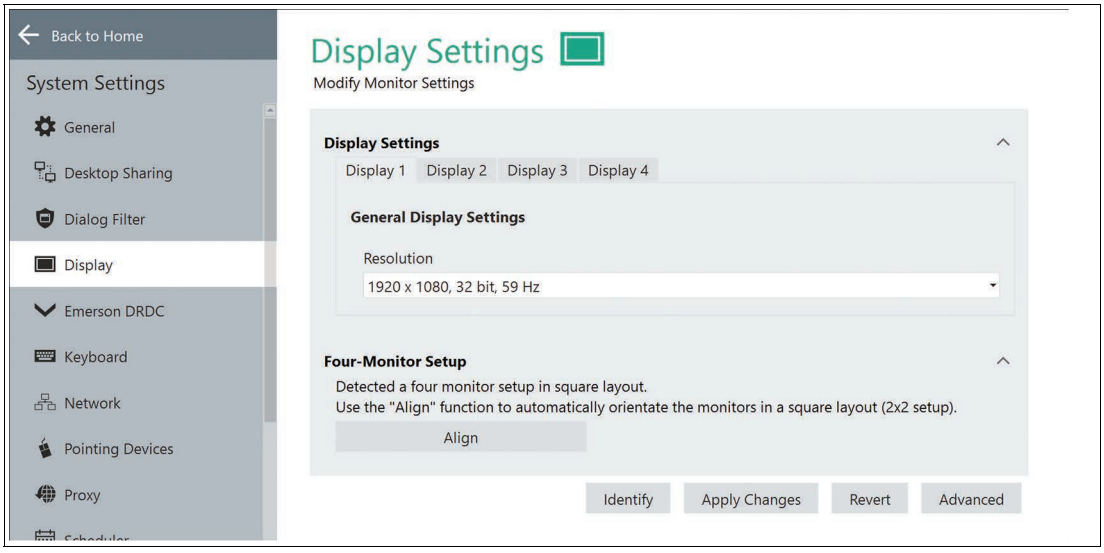


Abbildung 8.19

8.5 Emerson DRDC-Einstellungen

Mit "Emerson DRDC“ können Sie die Emerson DRDC-Einstellungen ändern.

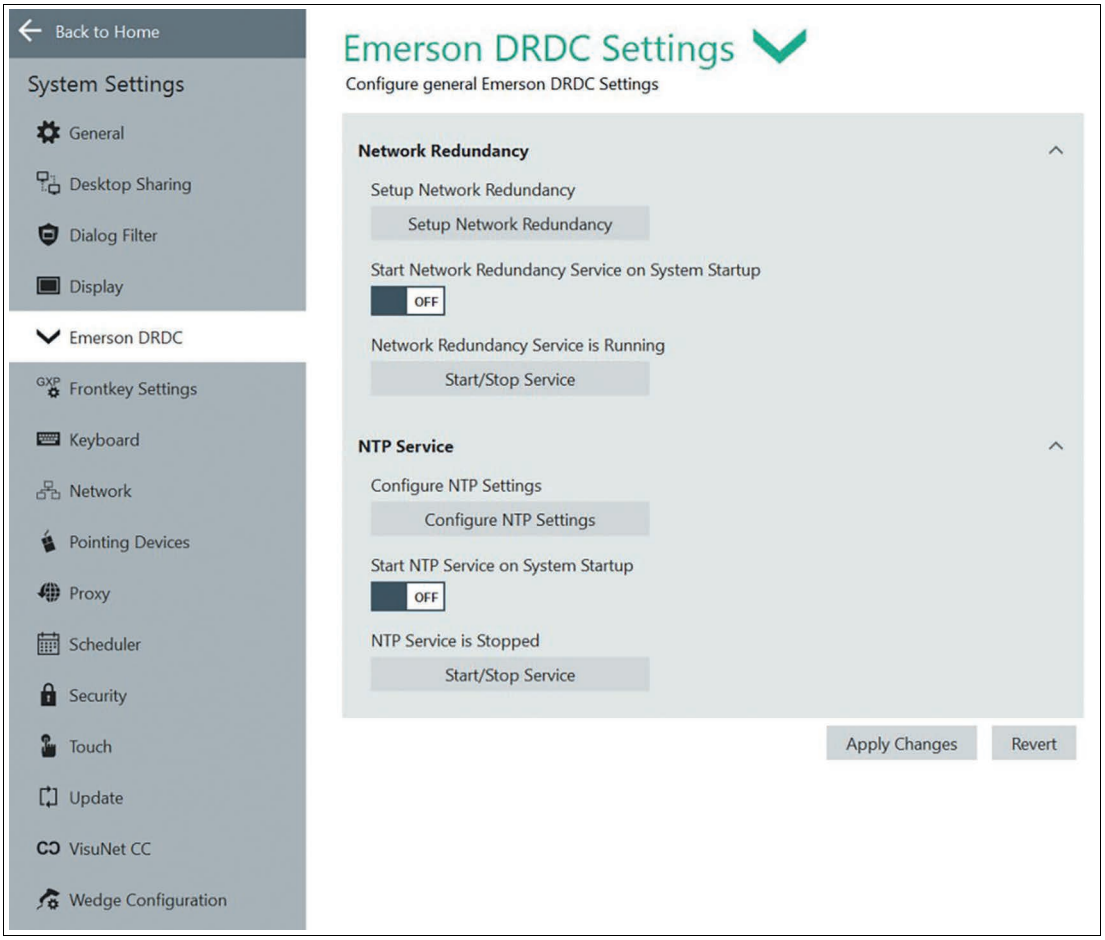


Abbildung 8.20

8.6 Fronttasten-Einstellungen

Hinweis!
Nur für VisuNet GXP-Geräte.

Navigieren Sie in der Navigationsleiste zu "frontkey settings“ (Fronttasten-Einstellungen).

Tasteneinstellungen

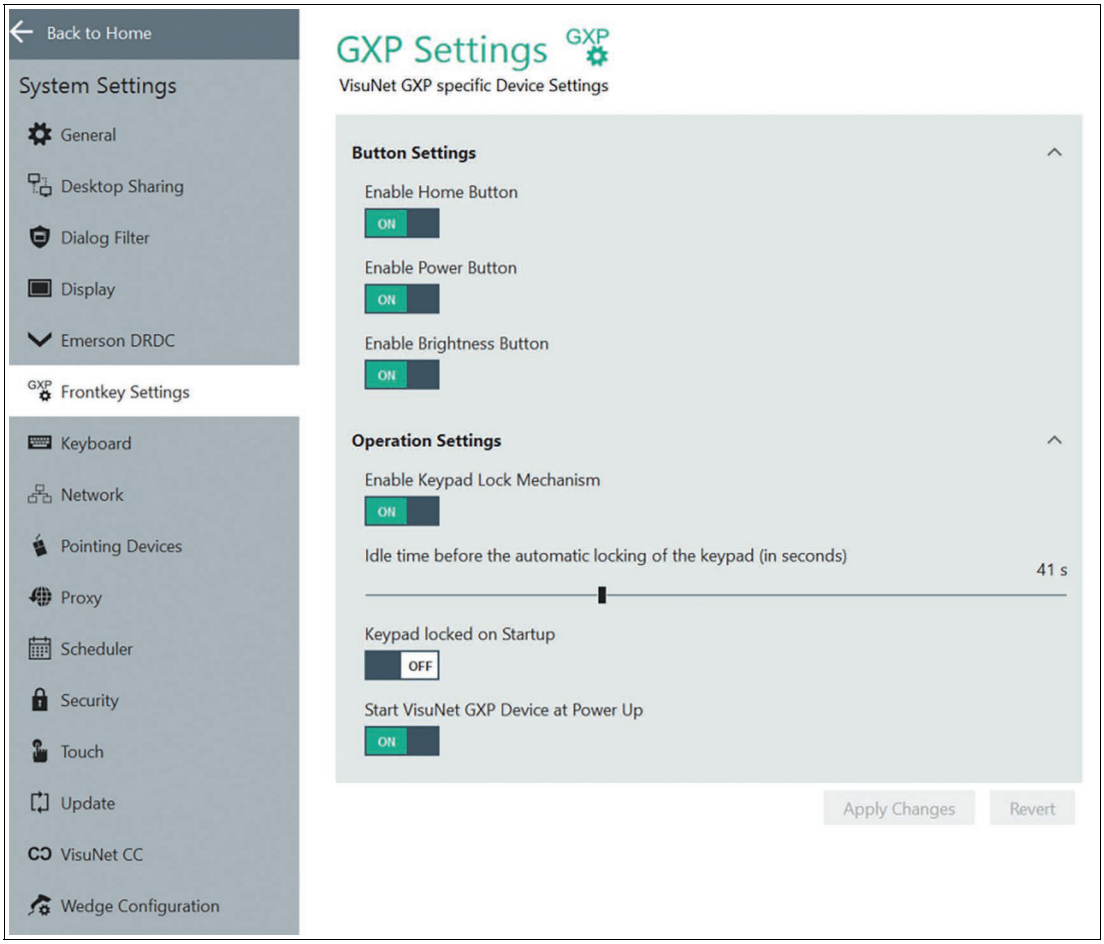


Abbildung 8.21

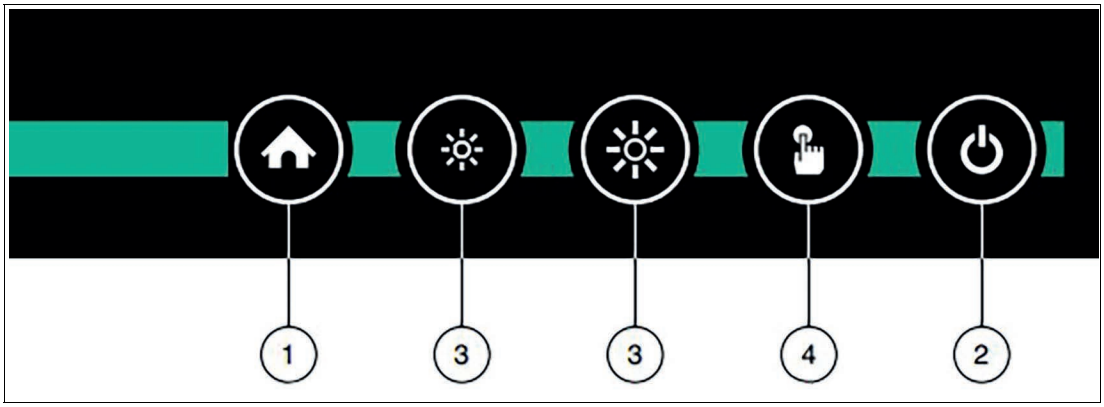


Abbildung 8.22

2024-01

PEPPERL+FUCHS

	Symbol	Beschreibung
1	Home	Konfigurierbare Fronttaste zum Aufruf einer bestimmten Funktion
2	Power	Konfigurierbarer Netzschalter (Herunterfahren, Neustart, Ruhezustand); Taste kann deaktiviert werden
3	Helligkeit	Verringert die Display-Helligkeit (dimmbar auf 0 %) bzw. erhöht die Display-Helligkeit
4	Touchscreen	Aktivieren/Deaktivieren des Touchscreens (z. B. zu Reinigungszwecken). Falls die Display-Einheit keinen integrierten Touchscreen aufweist, ist die Touchscreen-Taste deaktiviert.

Weitere Informationen zu Betrieb und Konfiguration finden Sie in unseren Handbüchern zu VisuNet-Display-Einheiten.

Bedienungseinstellungen

Sperren der Fronttasten:[1]

1. Aktivieren Sie die Tastensperre.
2. Stellen Sie die Leerlaufzeit vor der automatischen Tastensperre ein (in Sekunden), indem Sie mit dem Schieber einen Wert zwischen 1 Sekunde und 120 Sekunden einstellen.

↳ Die Tastensperre ist aktiviert.

Hinweis!

Wenn Sie eine beliebige Taste außer der Home-Taste drücken, wird die Animation zum Entsperren angezeigt.

Nach der eingestellten Leerlaufzeit werden die Fronttasten automatisch gesperrt. Um dies zu signalisieren, blinken alle LEDs dreimal.

Im Status der aktivierten Tastensperre können Sie festlegen, ob die Tastatur beim Einschalten oder nach der festgelegten Leerlaufzeit gesperrt werden soll.

1. Nur für Firmware Service Controller Version 1.3.2.231 und höher verfügbar. Das Update für Ihre TCU ist unter pepperl-fuchs.com verfügbar

8.7 Tastatureinstellungen

Input Language (Eingabesprache)

In diesem Abschnitt können Sie neue Tastaturlayouts hinzufügen, das Tastaturlayout konfigurieren und die Tastatur an Ihre spezifischen Sprachanforderungen anpassen.

Funktion	Beschreibung
Current Input Languages (Aktuelle Eingabesprachen)	In der Dropdown-Liste wird jedes Tastaturlayout angezeigt, das auf dem lokalen RM/BTC installiert ist. Um das Tastaturlayout auszuwählen, klicken Sie auf den Pfeil und wählen Sie das gewünschte Tastaturlayout aus.
Configure Input Languages (Eingabesprachen konfigurieren)	Um ein bestimmtes Tastaturlayout hinzuzufügen, klicken Sie auf die Schaltfläche "Configure Input Languages“ (Eingabesprachen konfigurieren). Ein Windows®-Dialogfenster wird geöffnet.

Abbildung 8.23 Tastatureinstellungen – Eingabesprache

Character Repeat (Zeichenwiederholung)

In diesem Abschnitt können Sie die Geschwindigkeit festlegen, mit der Zeichen wiederholt werden, wenn eine Taste gedrückt wird. Sie können dies durch Ändern der Wiederholungsverzögerung oder der Wiederholungsrate definieren.

Funktion	Beschreibung
Repeat Delay (Wiederholungsverzögerung)	Die Wiederholungsverzögerung ist die Zeitdauer, nach der ein Zeichen wiederholt wird, wenn Sie eine Taste gedrückt halten. Stellen Sie mit dem Schieberegler einen Wert zwischen einer kurzen und langen Verzögerung ein. Wenn die Wiederholverzögerung kurz ist, dauert es nur kurz, bis das Zeichen, dessen Taste gedrückt wird, wiederholt wird. Wenn die Wiederholverzögerung lang ist, dauert es länger, bis das Zeichen wiederholt wird.
Repeat Rate (Wiederholungsrate)	Die Wiederholungsrate ist die Rate, mit der ein Zeichen wiederholt wird, während Sie eine Taste gedrückt halten. Stellen Sie mit dem Schieberegler einen Wert zwischen einer niedrigen und hohen Wiederholungsrate ein. Wenn die Wiederholungsrate niedrig ist, wird das Zeichen langsamer wiederholt. Wenn die Wiederholungsrate hoch ist, wird das Zeichen schneller wiederholt.

Abbildung 8.24 Tastatureinstellungen – Zeichenwiederholung

2024-01

Cursor Blink (Mauszeiger-Blinken)

In diesem Abschnitt können Sie das Verhalten des Mauszeigers definieren.

Funktion	Beschreibung
Cursor Blink Enabled (Mauszeiger-Blinken aktiviert)	Diese Funktion aktiviert das Blinken des Mauszeigers. Wenn das Mauszeiger-Blinken deaktiviert ist, ist der Mauszeiger immer sichtbar.
Cursor Blink Rate (Mauszeiger-Blinkfrequenz)	Stellen Sie mit dem Schieberegler die Blinkfrequenz des Mauszeigers ein. Diese Option ist nicht verfügbar, wenn das Mauszeiger-Blinken deaktiviert ist.

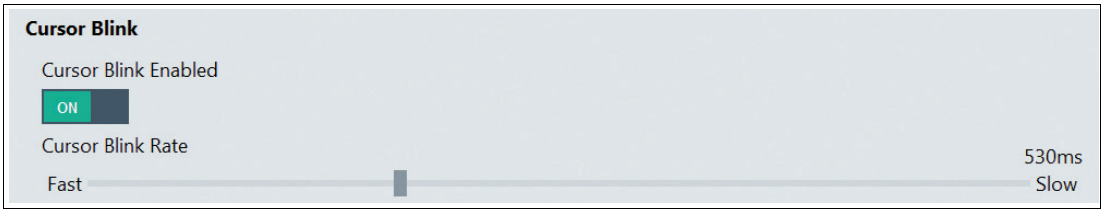


Abbildung 8.25 Tastatureinstellungen – Cursor-Blinken

8.8 Netzwerk

Network Adapter Information (Netzwerkadapter-Informationen)

In diesem Abschnitt finden Sie allgemeine Informationen zum Netzwerkadapter und zu den Netzwerkeinstellungen.

Funktion	Beschreibung
Network Adapter Information (Netzwerkadapter-Informationen)	Alle Informationen zur lokalen Hardware des RM-/BTC-Netzwerkadapters werden angezeigt.
Network Adapter Name (Netzwerkadaptername)	Sie können den Netzwerkadapternamen entsprechend Ihren Bedürfnissen anpassen.
DHCP	Verwenden Sie diese Option zum Aktivieren/Deaktivieren von DHCP (Dynamic Host Configuration Protocol). Mit DHCP können Sie RM/BTC ohne weitere manuelle Konfiguration in ein bestehendes Netzwerk integrieren. Einstellungen wie IP-Adresse, Subnetzmaske, Standard-Gateway und DNS-Server werden dem RM/BTC dann automatisch zugewiesen. Sie können jedoch alle diese Parameter manuell einrichten, indem Sie die DHCP-Option deaktivieren.

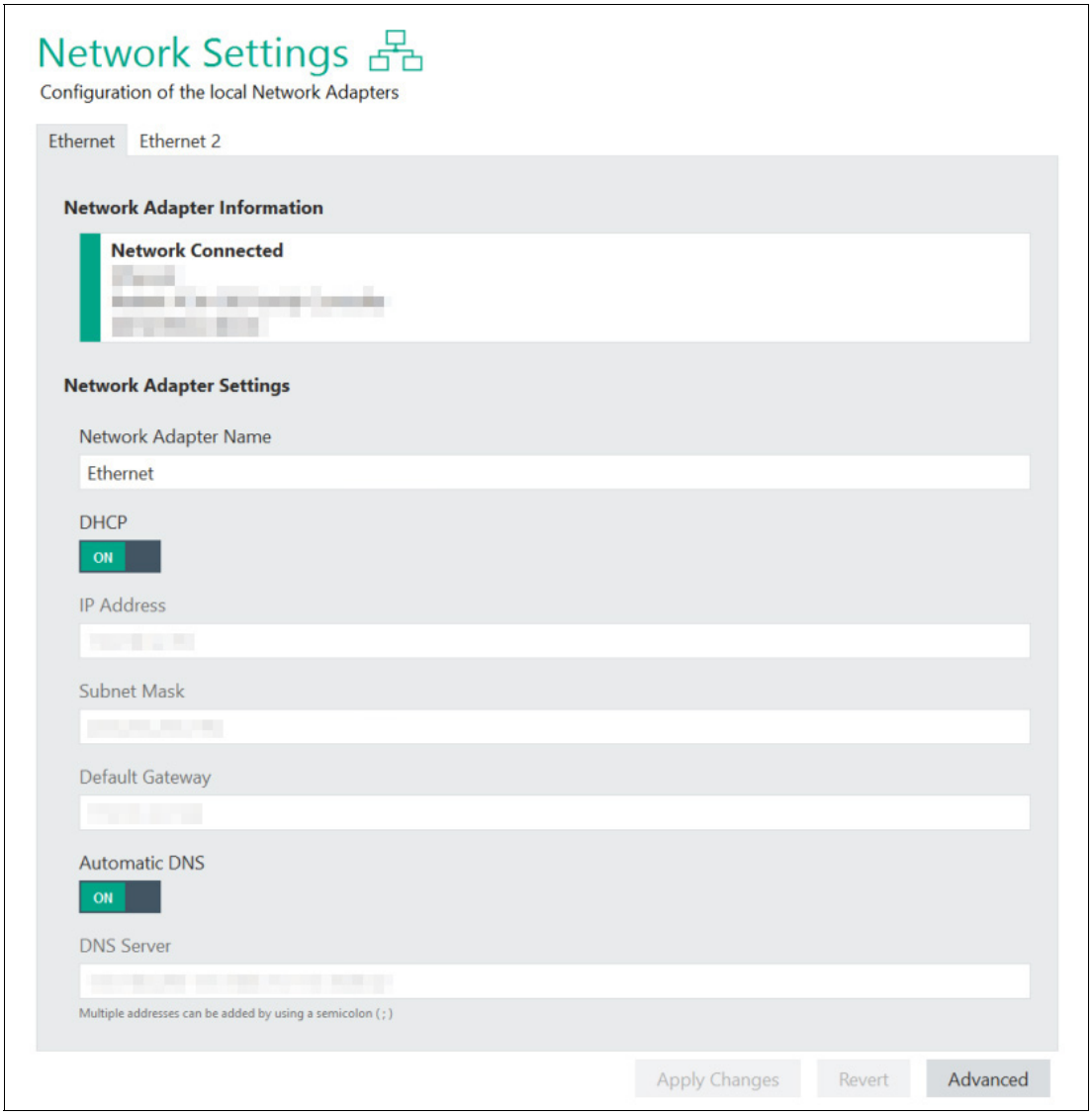


Abbildung 8.26 Netzwerkadapter-Informationen und Einstellungen

Hinweis!

Offene Netzwerkports

Die in RM Shell verwendeten offenen Netzwerkports sind im Anhang aufgeführt. Siehe Kapitel 12.1

Hinweis!

Advanced Settings (Erweiterte Einstellungen)

Erweiterte Einstellungen sind nur für Benutzer verfügbar, die mit der Administrator-Rolle angemeldet sind.

8.9 Pad-Ex®

Hinweis!

Gilt nur für industrielle Tablet Thin Client-Geräte mit Pad-Ex®.

Navigieren Sie in der Navigationsleiste zu "Pad-Ex“.

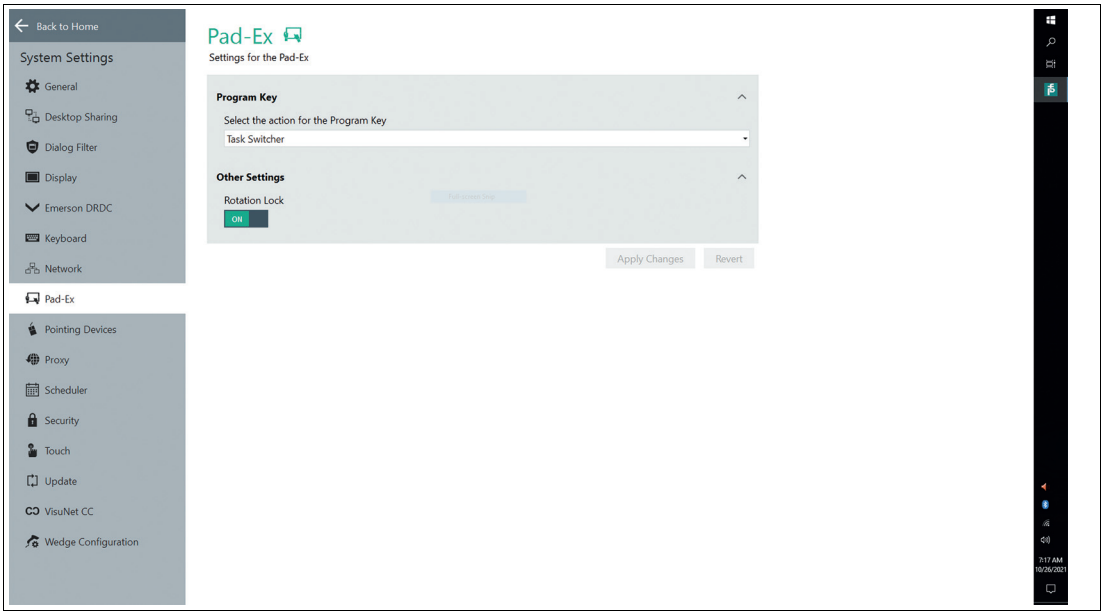


Abbildung 8.27

Einstellen der Programmtaste

1. Wählen Sie eine der folgenden Aktionen für Ihre Programmtaste aus

Funktion	Beschreibung
Keine	Keine Funktion
Task Switcher	Wechseln Sie zwischen mehreren Remote-Verbindungen und -Apps, die auf dem RM ausgeführt werden.
Gerätesperre	Eingangssperre zum Sperren des Ein- und Ausgangs des Pad-Ex, um unbeabsichtigten Betrieb, z. B. während eines Transports, zu vermeiden

Andere Einstellungen

Funktion	Beschreibung
Drehsperre aktiviert	Werkseinstellung: Verhindert, dass sich der Bildschirm automatisch dreht, und verriegelt den Bildschirm in der aktuellen Ausrichtung.
Drehsperre deaktiviert	Stellen Sie den Schieber auf "Aus“ (Off), um die Drehsperre zu deaktivieren und das automatische Drehen des Bildschirms zu aktivieren.

8.10 Zeigegerät-Einstellungen

Hinweis!

Systemneustart

Das Ändern der Mauseinstellungen erfordert einen Neustart des Systems.

Pointing Device Sensitivity Settings (Zeigegerät-Empfindlichkeitseinstellungen)

In diesem Abschnitt können Sie den Mauszeiger und die Doppelklick-Geschwindigkeit einstellen.

Funktion	Beschreibung
Mouse Cursor Speed (Mauszeiger-Geschwindigkeit)	Stellen Sie mit dem Schieberegler die Geschwindigkeit des Mauszeigers ein.
Double Click Speed (Doppelklick-Geschwindigkeit)	Stellen Sie mit dem Schieberegler die Doppelklick-Geschwindigkeit ein. Richten Sie die Doppelklick-Geschwindigkeit im Bereich von 100 ms (schneller Doppelklick) bis 5000 ms (langsamer Doppelklick) ein.

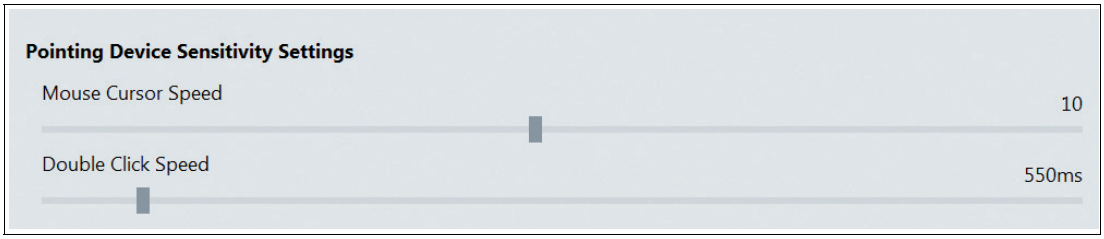


Abbildung 8.28 Einstellungen für Zeigegeräte – Empfindlichkeitseinstellung

Pointing Device Button Behavior (Zeigegerät-Tastenverhalten)

In diesem Abschnitt können Sie das Verhalten des Zeigegeräts einstellen.

Funktion	Beschreibung
Change Left and Right Keys (Vertauschen der linken und rechten Tasten)	Verwenden Sie diese Option, um zwischen den primären und sekundären Funktionen für die Maustasten umzuschalten. Aktivieren Sie diese Option, wenn Sie die rechte Taste für primäre Funktionen, wie Auswählen oder Ziehen von Objekten, verwenden möchten.
Hide Pointer While Typing (Zeiger während der Eingabe ausblenden)	Verwenden Sie diese Option zum Ausblenden des Zeigers während der Tastatureingabe.
Mouse Sonar (Maus-Sonar)	Verwenden Sie diese Option, um die Position des Mauszeigers auf dem Bildschirm anzuzeigen, indem Sie auf der Tastatur STRG/STRG drücken.

Abbildung 8.29 Einstellungen für Zeigegeräte – Verhalten von Tasten

Hinweis!

Advanced Settings (Erweiterte Einstellungen)

Erweiterte Einstellungen sind nur für Benutzer verfügbar, die mit der Administrator-Rolle angemeldet sind.

8.11 Proxy Settings (Proxy-Einstellungen)

In diesem Abschnitt können Sie die Verwendung eines Proxy-Servers aktivieren und Proxy-Server für verschiedene Kommunikationsprotokolle definieren.

Funktion	Beschreibung
Enable Proxy (Proxy aktivieren)	Mit dieser Option aktivieren/deaktivieren Sie die Verwendung eines Proxy-Servers.
Use the same proxy settings for all protocols (Die gleichen Proxy-Einstellungen für alle Protokolle verwenden)	Aktivieren Sie diese Option, um die gleichen Proxy-Einstellungen für alle Kommunikationsprotokolle zu verwenden. Wenn diese Option aktiviert ist, werden alle anderen Kommunikationsprotokolle deaktiviert/ausgegraut. Legen Sie die Proxy-Adresse und den Port fest, die Sie für alle Kommunikationsprotokolle verwenden möchten. Wenn diese Option deaktiviert ist, können Sie eine spezifische Proxy-Server-Adresse für jedes Kommunikationsprotokoll angeben.
Do not use proxy for following addresses (Keine Proxyserver für folgende Adressen verwenden)	Sie können eine Liste von Adressen definieren, für die kein Proxy-Server verwendet wird. Sie können mehrere Adressen, durch ein Semikolon getrennt, hinzufügen.
Ignore proxy server for local settings (Proxy-Server für lokale Einstellungen ignorieren)	Aktivieren Sie diese Option, wenn Sie nicht möchten, dass der Proxyserver für lokale Adressen verwendet wird.

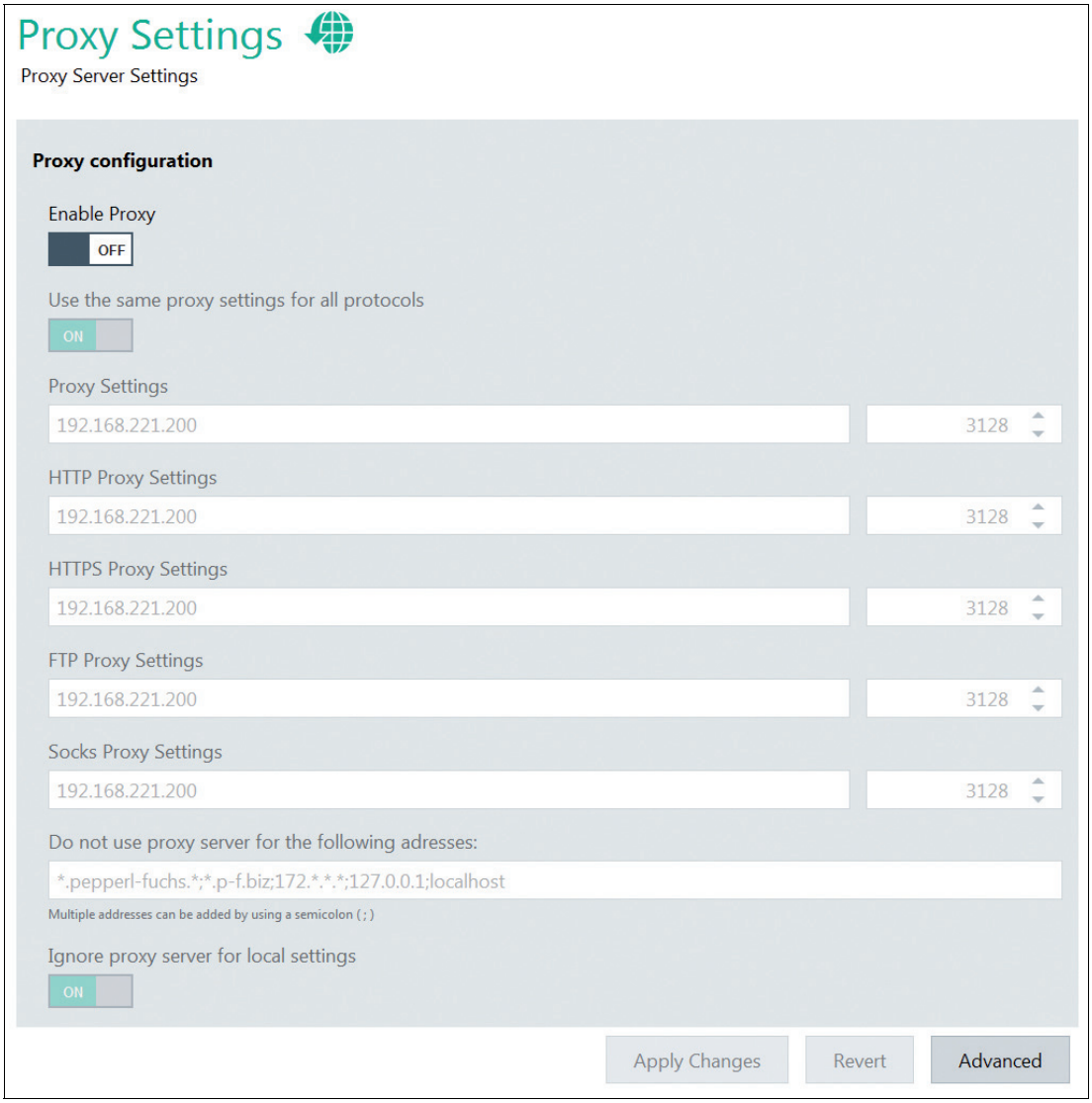


Abbildung 8.30 Proxy-Einstellungen

8.12 Scheduler

Es wird dringend empfohlen, den Scheduler zu aktivieren, wenn der Unified Write Filter aktiviert ist. Mit dem Scheduler können Sie regelmäßige Systemneustarts planen. Damit kann der Unified Write Filter kontinuierlich verwendet werden, ohne dass der Speicherpuffer überläuft.

Im Einstellungsmenü können Sie den Scheduler aktivieren oder deaktivieren, auswählen, wann und wie oft das System neu gestartet wird, und festlegen, wie lange das System vor dem Neustart im Leerlauf sein muss.

Das System wird erst neu gestartet, wenn die eingestellte Leerlaufzeit erreicht ist.

Abbildung 8.31 Scheduler-Einstellungen

Tipp

Wir empfehlen, den Scheduler rund um die Uhr zu aktivieren. Das System wird nur neu gestartet, wenn während der Leerlaufzeit kein Betrieb stattgefunden hat.

8.13 Sicherheit

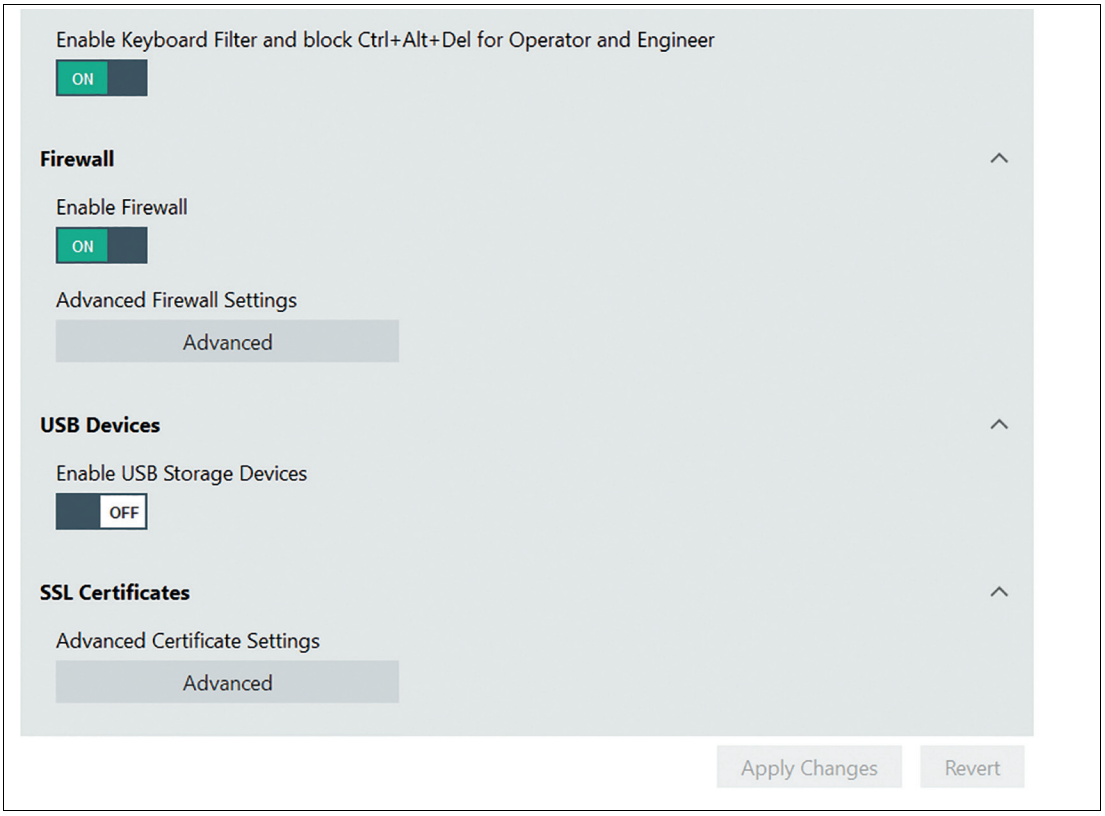


Abbildung 8.32

Hinweis!

Für Domänenbenutzer

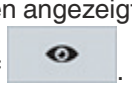
Der Filter muss deaktiviert werden, wenn das Gerät an eine Domäne übertragen wird und die automatische Windows®-Anmeldung nicht aktiviert ist.

Weitere Informationen finden Sie in der Anleitung. Siehe Kapitel 11.

VisuNet RM Shell und lokale Windows®-Benutzerkennwörter

In diesem Abschnitt können Sie Kennwörter für die Benutzerrollen Ingenieur und Administrator sowie für den lokalen Windows®-Benutzer festlegen.

Funktion	Beschreibung
VisuNet RM Shell-Kennwörter	
Engineer	Wenn Sie die Benutzerrolle "Engineer“ (Ingenieur) mit einem Kennwort schützen möchten, geben Sie ein Kennwort in das entsprechende Feld ein. Das eingegebene Kennwort wird nur in Form von Punkten angezeigt. Um das aktuelle Kennwort anzuzeigen, klicken Sie auf . Nachdem das Kennwort festgelegt wurde, können nur Benutzer, die das Kennwort kennen, sich mit der Benutzerrolle "Engineer“ (Ingenieur) anmelden.
Administrator	Wenn Sie die Benutzerrolle "Administrator“ mit einem Kennwort schützen möchten, geben Sie ein Kennwort in das entsprechende Feld ein. Das eingegebene Kennwort wird nur in Form von Punkten angezeigt. Um das aktuelle Kennwort anzuzeigen, klicken Sie auf . Nachdem das Kennwort festgelegt wurde, können nur Benutzer, die das Kennwort kennen, sich mit der Administrator-Benutzerrolle anmelden.

Funktion	Beschreibung
Local Windows® User (Lokaler Windows®-Benutzer)	Legen Sie das Kennwort für den lokalen Windows®-Benutzer fest oder ändern Sie es. Das eingegebene Kennwort wird nur in Form von Punkten angezeigt. Um das aktuelle Kennwort anzuzeigen, klicken Sie auf  .
Kennwort für die werksseitige Rückstellung	Ändern Sie das Kennwort für die werksseitige Rückstellung. Das Kennwort ist durch Punkte ausgeblendet und muss mindestens 6 Zeichen lang sein. Das Feld darf nicht leer sein.

Hinweis!

Das Windows®-Kennwort kann auch über die ursprünglichen Windows®-Einstellungen geändert werden. In diesem Fall wird die automatische Windows®-Anmeldung deaktiviert und der Windows®-Anmeldebildschirm wird angezeigt. Deshalb ist es unbedingt erforderlich, "Tastaturfilter und Strg+Alt+Entf“ zuzulassen.

Automatische Abmeldung des Anwenders

Mit dieser Einstellung können Sie die Funktion Automatische Abmeldung für die Rollen Administrator und Ingenieur aktivieren oder deaktivieren und festlegen, wie lange das System inaktiv sein muss, bevor die automatische Abmeldung erfolgt.

Ein Timer oben auf dem Startbildschirm zeigt an, wann die Abmeldung erfolgt, indem er die verstrichene Zeit anzeigt.

Hinweis!

Die automatische Abmeldung gilt nur für den Startbildschirm. Der Timer wird zurückgesetzt, sobald die Maus bewegt, eine Taste betätigt oder ein Klick erkannt wird.

Keyboard Filter Settings (Tastaturfiltereinstellungen)

Der Tastaturfilter ist standardmäßig aktiviert. Wenn Sie die Funktion Strg+Alt+Entf verwenden möchten, muss dieser Filter deaktiviert werden. Dies kann für die Integration von Systemdomänen nützlich sein, z. B. für die Abmeldefunktion.

Firewall

In diesem Abschnitt können Sie die Firewall-Einstellungen konfigurieren.

Funktion	Beschreibung
Firewall	Aktivieren/deaktivieren Sie diese Option, um die Windows®-Firewall auf dem RM zu aktivieren/deaktivieren.
Advanced Firewall Settings (Erweiterte Firewall-Einstellungen)	Klicken Sie auf "Advanced“ (Erweitert), um das Windows®-Dialogfenster für die Firewall-Einstellungen zu öffnen.

Abbildung 8.33 Sicherheitseinstellungen – Firewall

2024-01

USB Devices (USB-Geräte)

In diesem Abschnitt können Sie externe USB-Speichermedien (z. B. Speichersticks, externe Festplatten usw.) aktivieren oder deaktivieren.

Wenn die Option deaktiviert ist, kann der Anwender nicht auf externe USB-Geräte zugreifen, die mit dem RM verbunden sind. Die empfohlene voreingestellte Einstellung ist "OFF“ (AUS).

Abbildung 8.34 Sicherheitseinstellungen – USB-Geräte

SSL Certificates (SSL-Zertifikate)

In diesem Abschnitt können Sie die Microsoft-spezifischen erweiterten Zertifikateinstellungen bearbeiten.

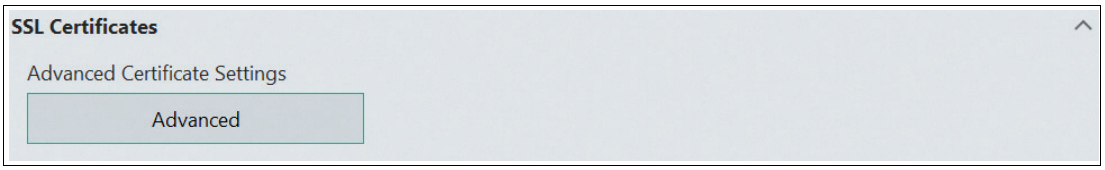


Abbildung 8.35 SSL certificates (SSL-Zertifikate) – Microsoft-spezifische Zertifikateinstellungen bearbeiten

8.14 Touch Settings (Touch-Einstellungen)

In diesem Menü können Sie die Touch-Einstellungen für VisuNet GXP ändern, wenn Ihr RM mit einer Touchscreen-Option ausgestattet ist. Wählen Sie im Dropdown-Menü die gewünschte Empfindlichkeitsstufe aus und klicken Sie auf die Schaltflächen "Calibrate“ (Kalibrieren), um Genauigkeit und Empfindlichkeit zu kalibrieren.

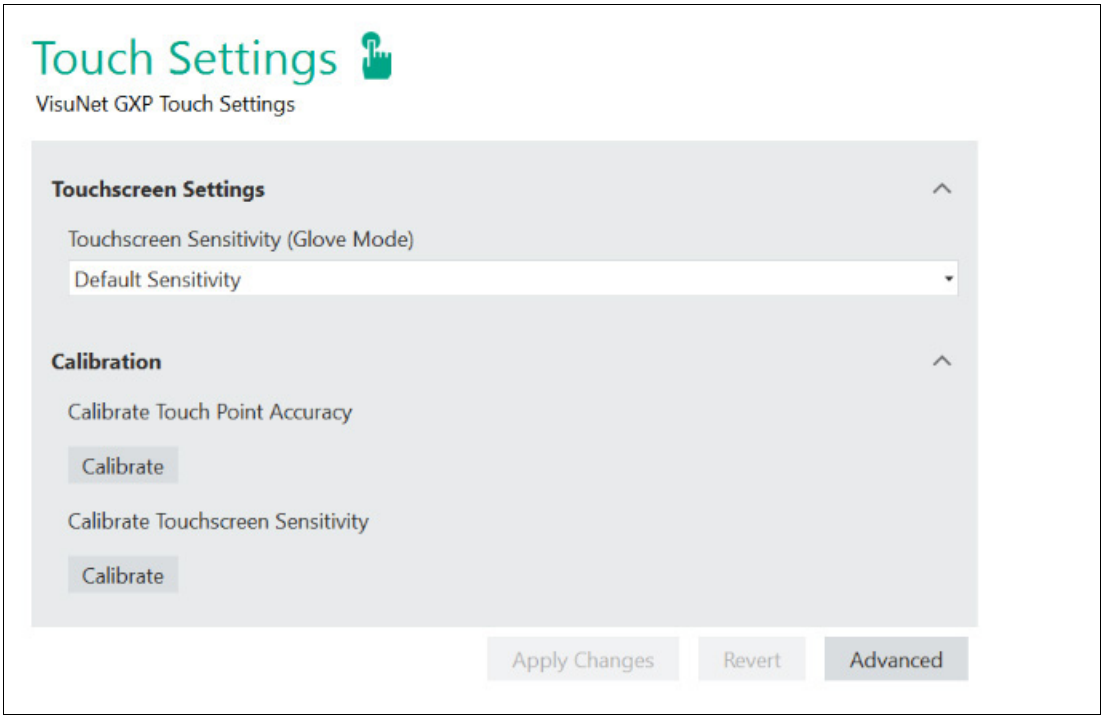


Abbildung 8.36 Touch-Einstellungen

8.15 Update (Aktualisierung)

In diesem Abschnitt können Sie die VisuNet RM Shell auf die neueste Version aktualisieren oder das Bereinigungssystem verwenden, um den Datenträger zu bereinigen. Das Untermenü "Update“ (Aktualisierung) ist nur für die Benutzerrolle "Administrator“ verfügbar.

Es gibt 3 Möglichkeiten, VisuNet RM Shell zu aktualisieren:

- Aktualisierung über ein lokales Gerät (z. B. USB-Stick)
- Aktualisierung über eine Netzwerkfreigabe
- Aktualisierung über VisuNet CC (Einzelgerät oder Aktualisierung mehrerer Geräte mit dem Assistenten für Firmware-Aktualisierungen)

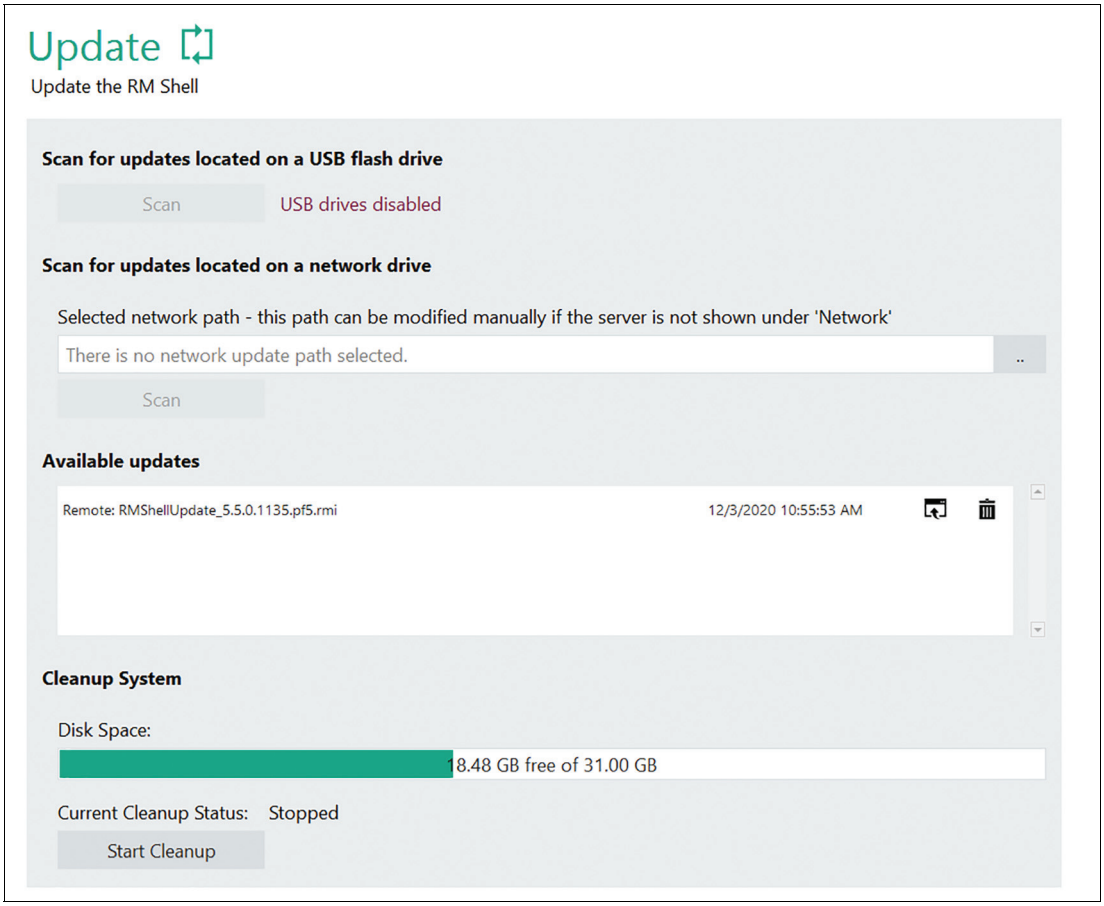


Abbildung 8.37 Systemeinstellungen: Update

Aktualisierung über ein lokales Gerät (USB-Stick)

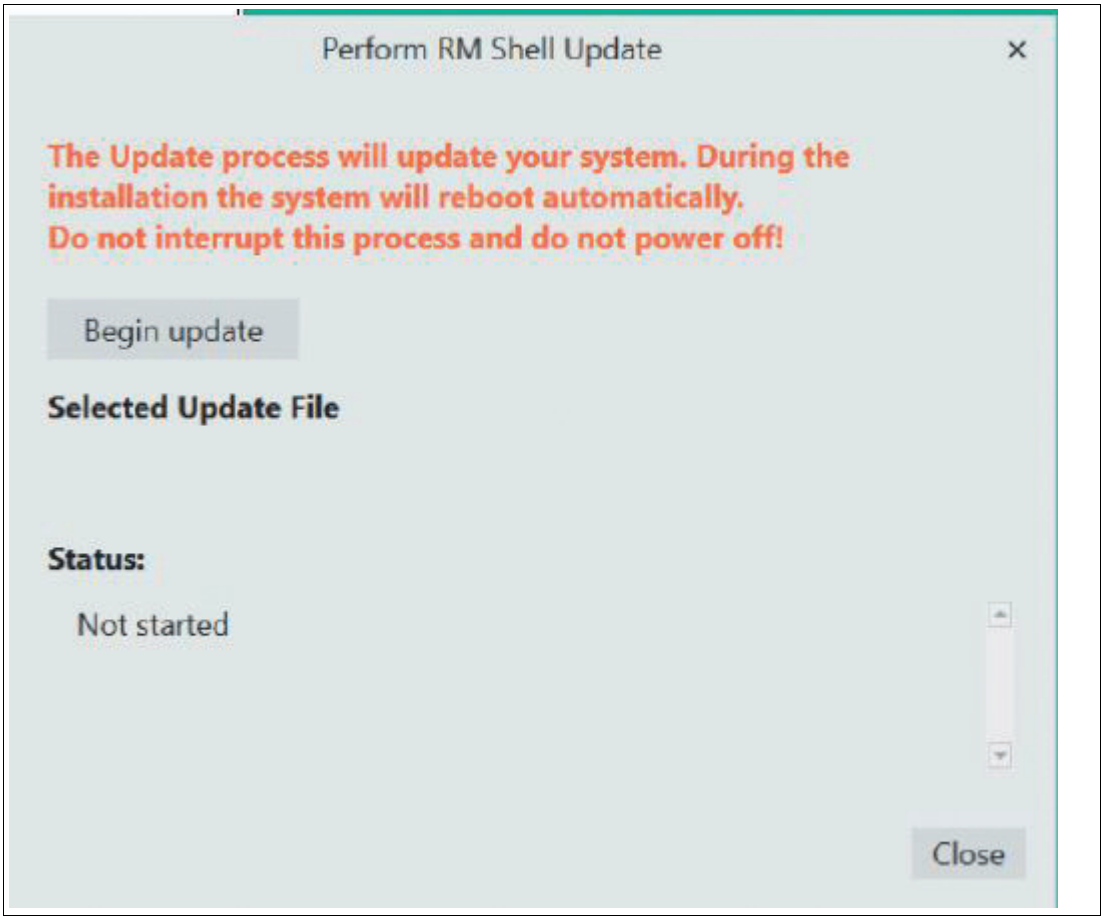
Sie können die VisuNet RM Shell aktualisieren, indem Sie ein lokales Gerät (USB-Stick) mit den aktuellen Aktualisierungsdateien verwenden.

Aktualisierung über ein lokales Gerät

1. Verbinden Sie das lokale Gerät mit dem RM.
2. Klicken Sie im Abschnitt "Find update“ (Update suchen) auf Scan.

   ↳ VisuNet RM Shell sucht nach lokalen Geräten, die mit dem RM verbunden sind. Die gescannte Aktualisierungsdatei wird im Abschnitt "Available updates“ (Verfügbare Updates) angezeigt. Der Name des lokalen Geräts wird als Präfix angezeigt.
3. Wählen Sie das gewünschte Update aus, indem Sie auf klicken.

   ↳ Das Dialogfenster "Begin Update“ (Mit Update beginnen) wird geöffnet.



4. Klicken Sie auf Begin update, um mit der Installation des Updates zu beginnen.

   ↳ Der Update-Installationsprozess wird gestartet. Während der Installation wird der RM zweimal neu gestartet.

Aktualisierung über eine Netzwerkfreigabe

1. Erstellen Sie einen Freigabeordner für das Update.
2. Öffnen Sie den Pfad und durchsuchen Sie den ausgewählten Ordner nach dem verfügbaren Update.

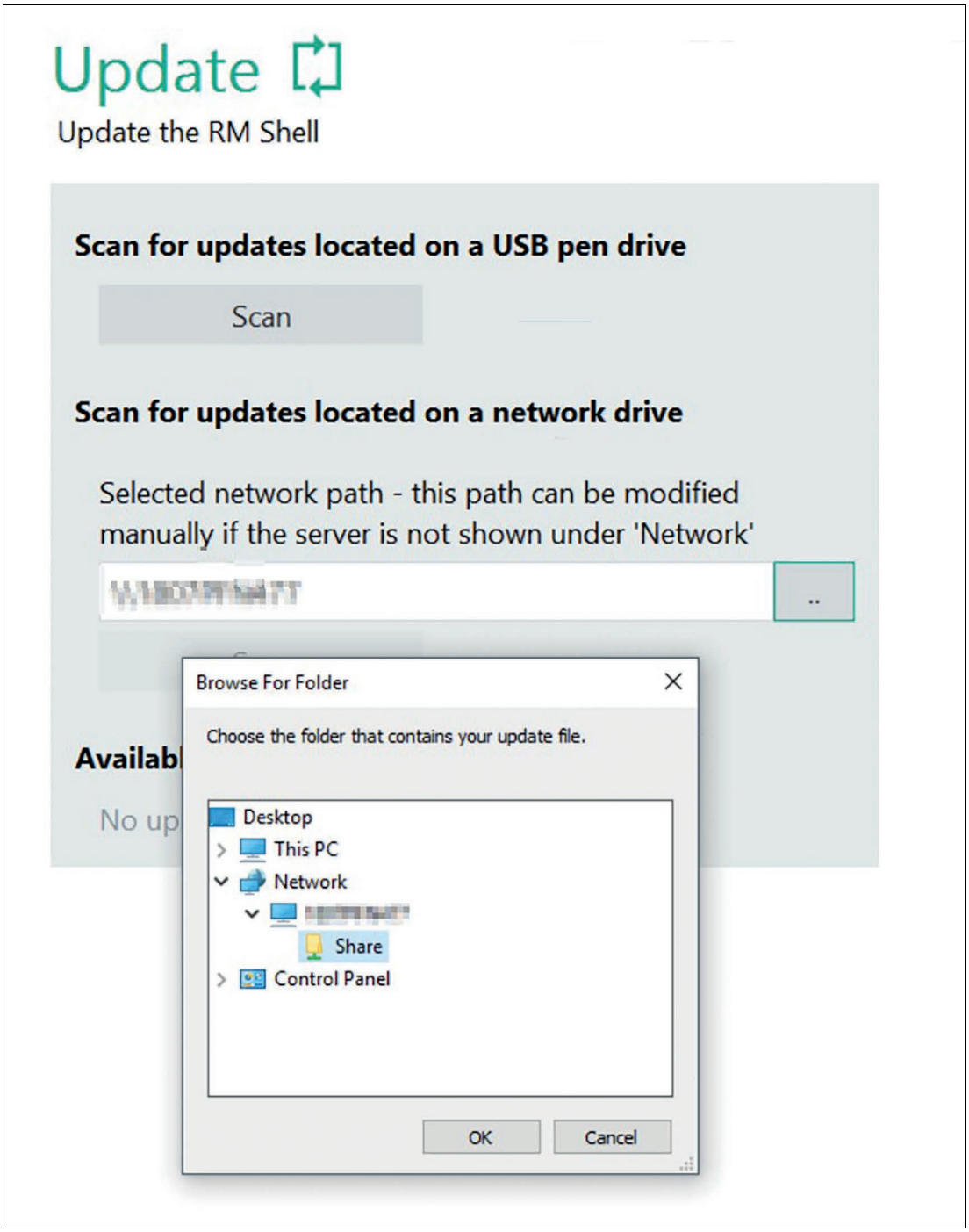


Abbildung 8.38

3. Das verfügbare Update wird nun in der Liste angezeigt.
4. Klicken Sie auf "Begin Update“ (Update starten), um die Installation zu starten.

2024-01

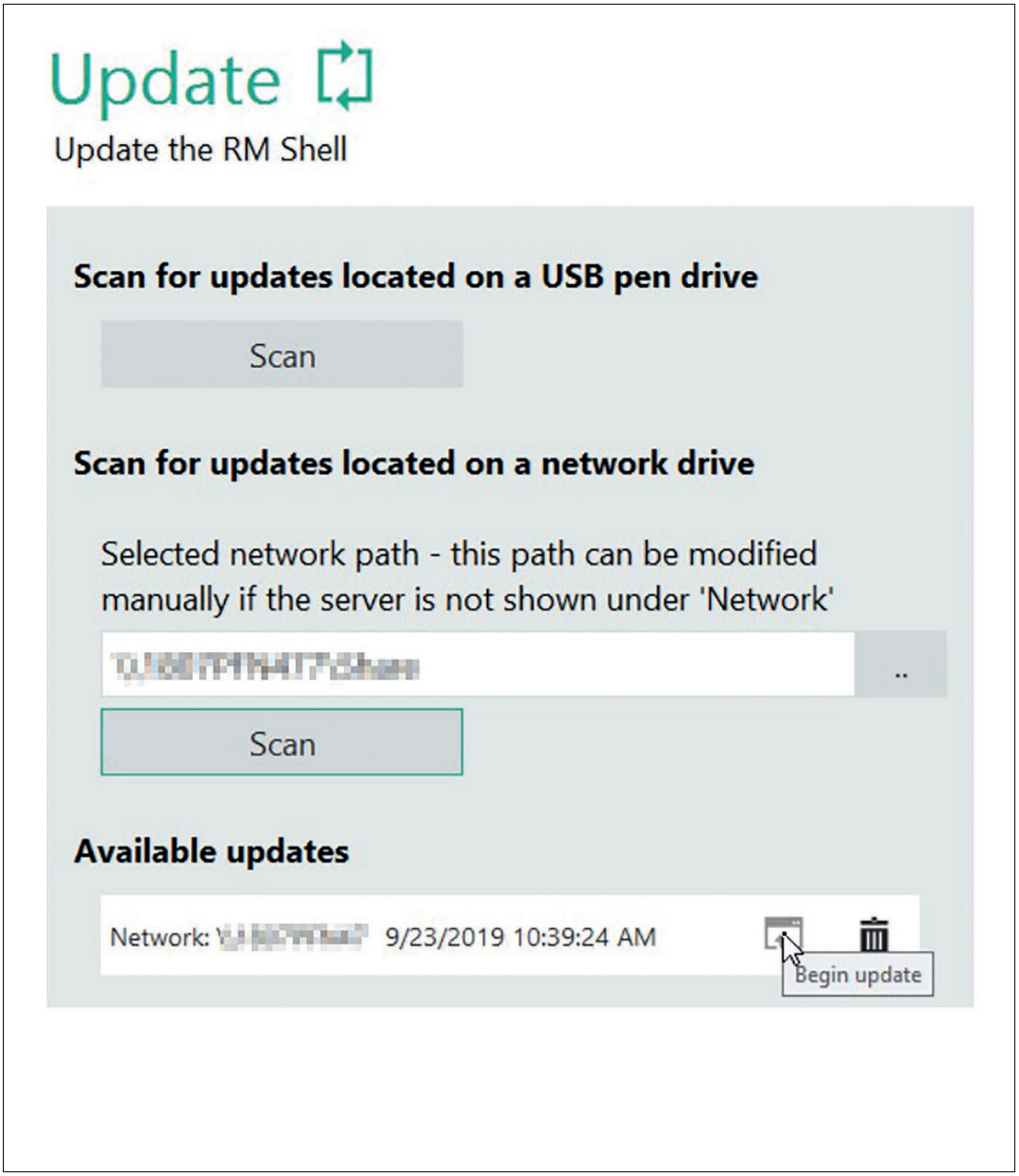


Abbildung 8.39

Weitere Informationen zur Durchführung einer Aktualisierung über VisuNet Control Center finden Sie im VisuNet CC-Handbuch.

Bereinigungssystem

Durch die Bereinigung Ihres Geräts wird Speicherplatz freigemacht und die Leistung verbessert, indem temporäre Dateien gelöscht und die Größe des WinSxS-Ordners verringert wird. Ab VisuNet RM Shell Version 5.5.0 wird der verfügbare Speicherplatz visualisiert.

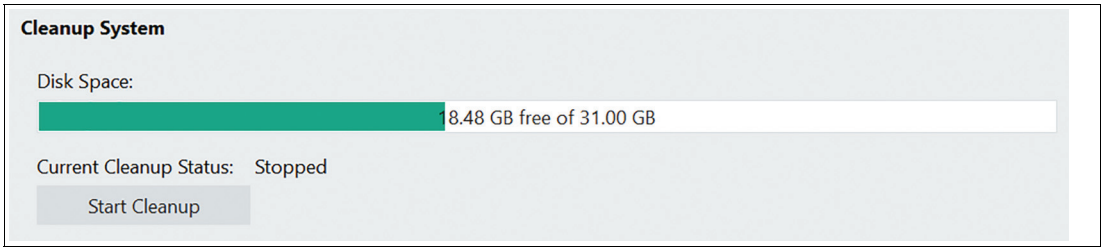


Abbildung 8.40

Hinweis!

Der Bereinigungsprozess kann mehrere Stunden dauern. Während dieser Zeit kann das Gerät verwendet werden, möglicherweise ist es aber langsamer. Es wird empfohlen, den Assistenten zur Datenträgerbereinigung nur dann auszuführen, wenn der Speicherplatz knapp wird.

Hinweis!

Wenn Ihr Speicher nach der Bereinigung des Datenträgers immer noch nicht für Updates oder die Installation von Software von Drittanbietern ausreicht, empfehlen wir, Ihr Gerät auf die Werkseinstellungen mit Version > 6.0 zu aktualisieren, die unter www.pepperl-fuchs.com verfügbar ist. Durch das angepasste Partitionsdesign des neuesten Updates hat sich der verfügbare Speicherplatz deutlich erhöht.

8.16 VisuNet CC-Einstellungen

Hinweis!

Für die Verwendung von VisuNet Control Center ist eine zusätzliche Lizenz erforderlich. Weitere Informationen zu VisuNet CC finden Sie online unter pepperl-fuchs.com

Sie können die VisuNetCC-Konnektivität aktivieren/deaktivieren und einige der entsprechenden Einstellungen für die Zeitüberschreitung von Verbindungen konfigurieren. Die vorkonfigurierten Einstellungen werden als Standardwerte betrachtet. Es wird nicht empfohlen, diese zu ändern, es sei denn, es treten Probleme auf. Für langsame Verbindungen innerhalb des Netzwerks empfehlen wir, das Zeitlimit für Öffnen/Schließen zu erhöhen.

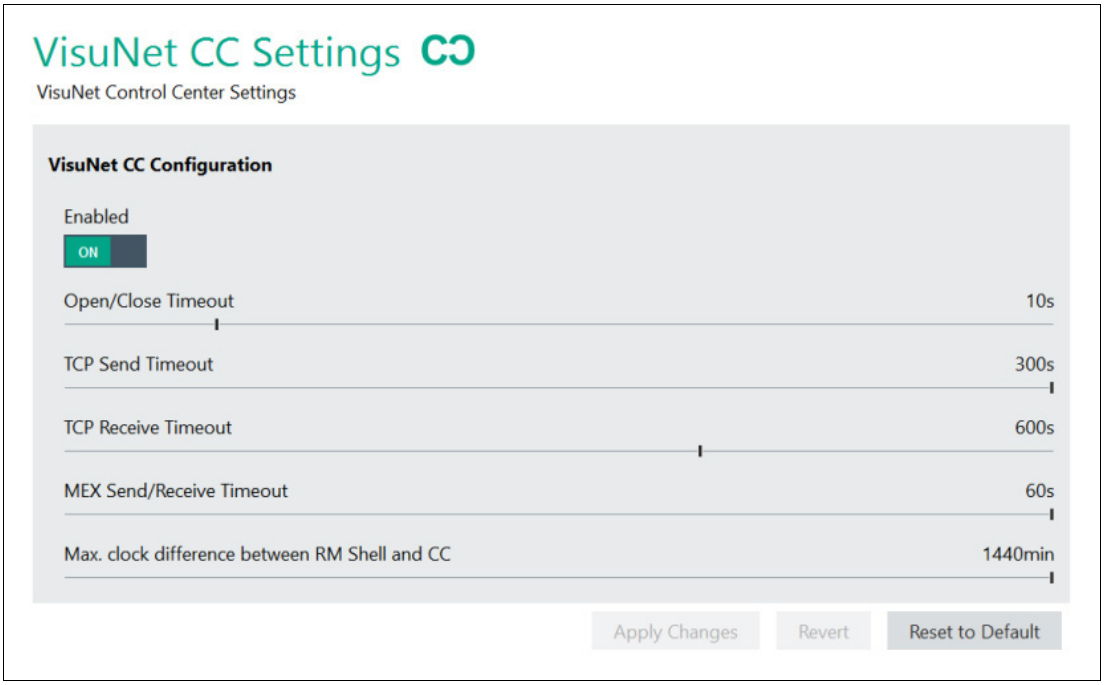


Abbildung 8.41 VisuNet CC-Einstellungen

8.17 Wedge Konfiguration für Scanner mit serieller Schnittstelle

General Settings (Allgemeine Einstellungen)

Funktion	Beschreibung
Input Character Delay (Eingabe-Zeichenverzögerung)	Konfigurieren Sie mit dem Schieberegler die Verzögerung: • 0 ms: keine Zeichenverzögerung • 200 ms: größte Verzögerung
Remote Text Input Mode (Eingabemodus für Remote-Text)	Es können verschiedene Modi zur Übersetzung der eingehenden Daten der seriellen Schnittstelle verwendet werden: • Der Tastatureingabesimulationsmodus (Standard und empfohlen) verwendet die Windows® Input Simulator-Funktion, um Zeichen als einzelne Tastatureingaben zu senden. Dieser Modus ist auf Tastaturzeichen beschränkt und bietet eingeschränkte Möglichkeiten, Sonderzeichen zu senden. • Im Modus Alt+ASCII werden Zeichen mithilfe der Simulation ALT+ASCII gesendet. Dieser Modus unterstützt Sonderzeichen, kann jedoch Probleme mit RDP-Verbindungen haben.
Blenden Sie die App "Wedge“ für den Bediener der Hauptansicht aus.	Bei Aktivierung dieser Funktion wird dem Bediener die App "Wedge“ nicht angezeigt.

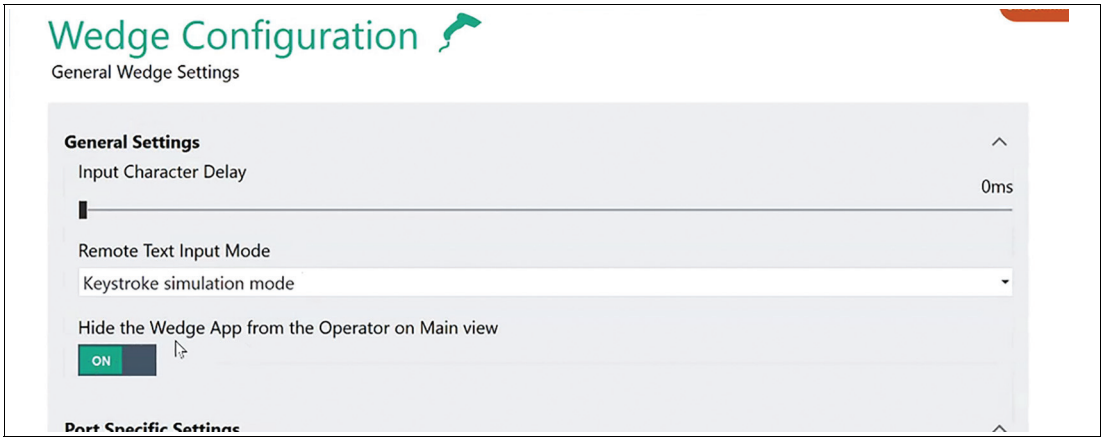


Abbildung 8.42 S2K-Wedge-Konfiguration: Allgemeine Einstellungen

Portspezifische Einstellungen

Wählen Sie den seriellen Port, an dem der Barcode-Scanner angeschlossen ist, und konfigurieren Sie ihn, indem Sie auf die entsprechende Registerkarte klicken.

Abbildung 8.43 COM-Port-Auswahl (in diesem Beispiel ist COM1 ausgewählt)

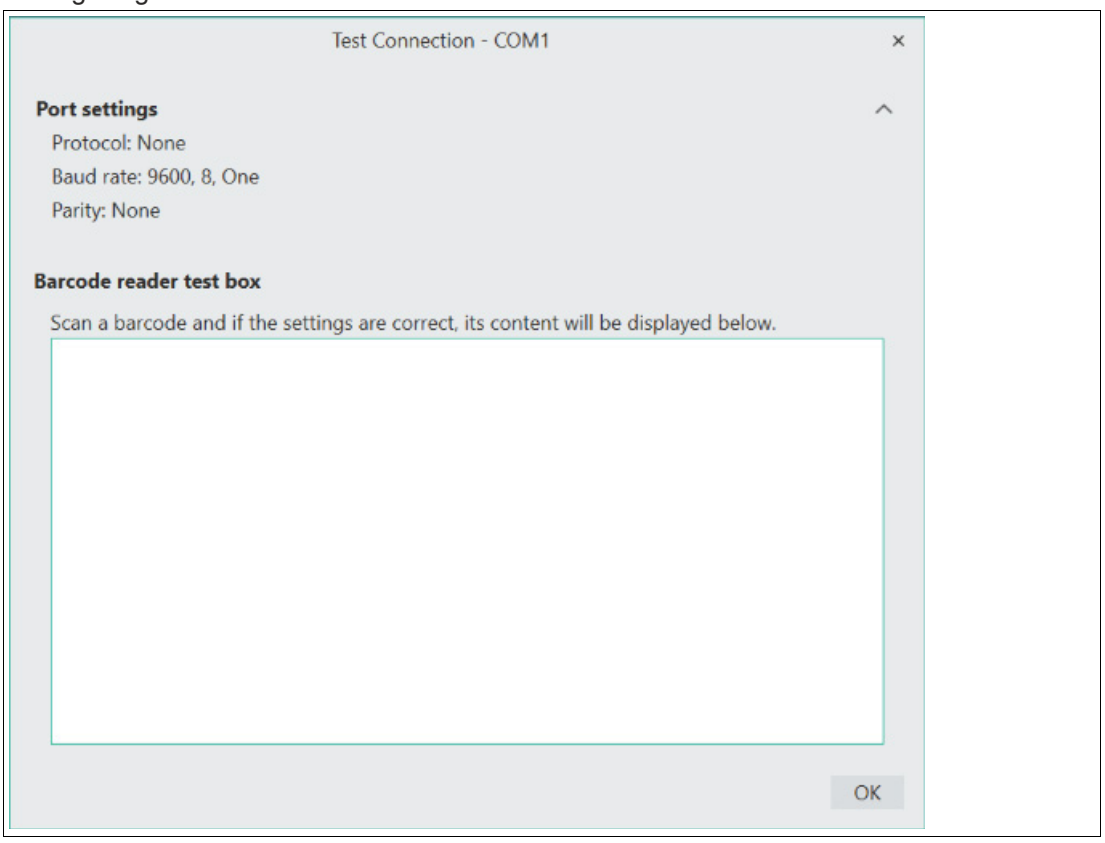
Testen der Verbindung

Um zu testen, ob ein PSCAN-Gerät ordnungsgemäß eingerichtet und angeschlossen ist, verwenden Sie die Funktion "Test connection“ (Verbindung testen).

Testen der COM-Port--Verbindung

1. Wählen Sie die Registerkarte des COM-Ports aus, den Sie testen möchten.
2. Klicken Sie auf Test Barcode reader.

   ↳ Das Fenster "Test Connection“ (Verbindung testen) wird geöffnet. Im Abschnitt "Port Settings“ (Port-Einstellungen) werden alle Einstellungen des entsprechenden COM -Ports angezeigt:



3. Scannen Sie mit dem PSCAN-Gerät einen Barcode.

   ↳ Wenn alle Einstellungen korrekt vorgenommen wurden, wird der Inhalt des Barcodes im Feld "Barcode reader test box“ (Testbox Barcode-Lesegerät) angezeigt.

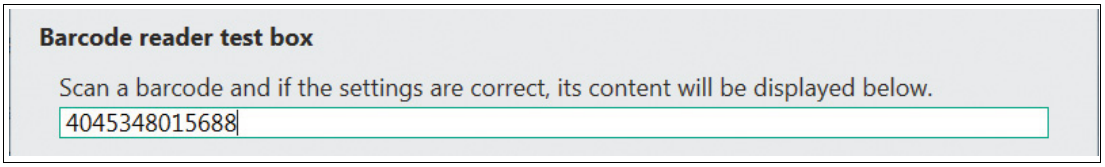


Abbildung 8.44 Scannertestfeld

4. Um den Test zu beenden, klicken Sie auf OK.

   Es werden alle Ports angeboten, die dem Betriebssystem bekannt sind, einschließlich derjenigen, die bereits von anderen Programmen belegt sind.

Funktion	Beschreibung
Protokoll	Diese Dropdown-Liste gibt das Protokoll an, das zur Datenübertragung verwendet wird.
Stop Bits	Stellen Sie hier die Anzahl der Stoppbits ein. Normalerweise wird ein Stoppbit verwendet.
Data Bits	Wählen Sie hier die Anzahl der Datenbits. Zulässige Werte sind 5, 6, 7 und 8. Normalerweise werden 8 Datenbits verwendet.
Baud Rate	Wählen Sie die Datenübertragungsgeschwindigkeit. Die Standardeinstellung für den Barcodescanner ist 9600 Baud.
Parity	Dieses Kontrollkästchen gibt an, ob das Paritätsprüfbit berechnet werden sollen, und wenn ja, wie.
Auto Connect (Automatische Verbindung)	Wenn diese Option aktiviert ist, öffnet VisuNet RM Shell automatisch den seriellen Port und stellt eine Verbindung zum Barcodescanner her, wenn der RM (neu) gestartet wird.
Visible on Operation screen (Auf dem Betriebsbildschirm sichtbar)	Wenn diese Option aktiviert ist, wird der serielle Port in der App "VisuNet Wedge“ sichtbar als serieller Port dargestellt.

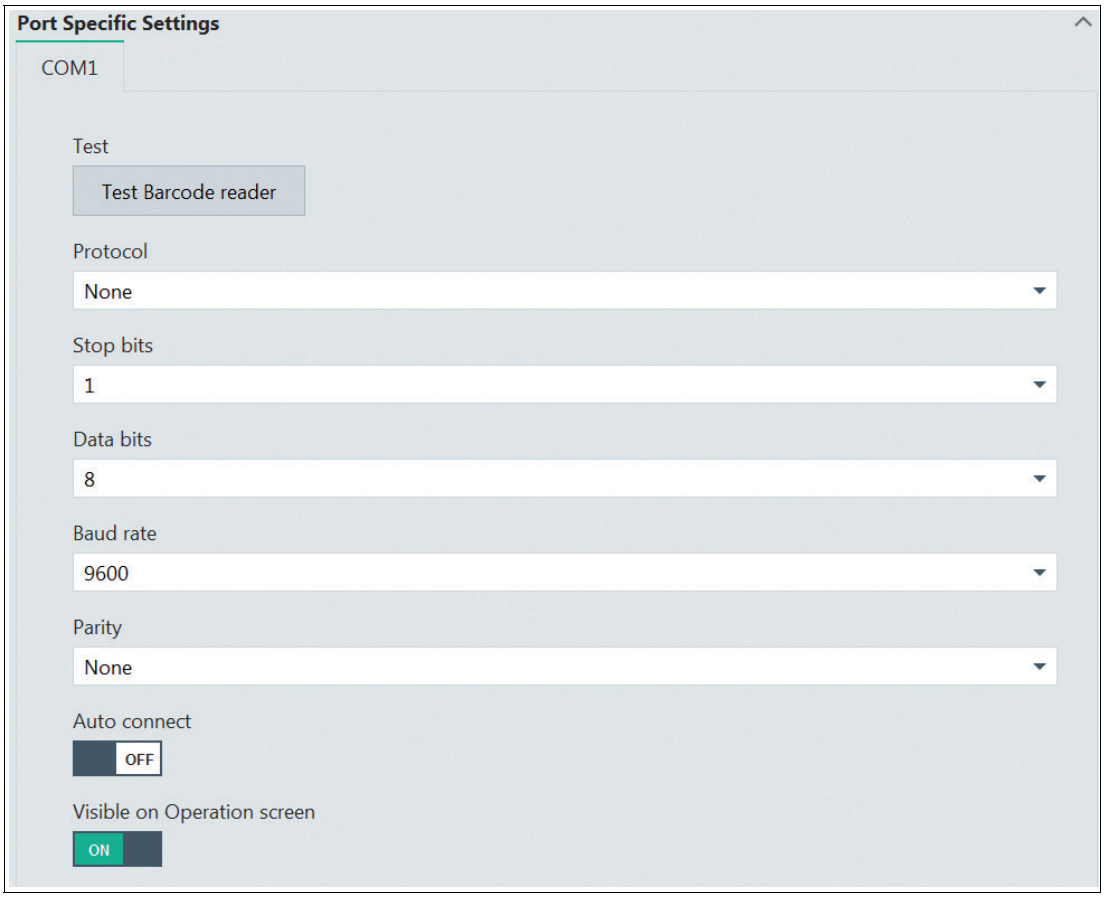


Abbildung 8.45 Wedge-Konfiguration – Portspezifische Einstellungen

2024-01

PEPPERL+FUCHS

Function Key Emulation (Funktionstastenemulation)

Die Zeichenfolgen des seriellen Ports werden entsprechend der Zuordnungstabelle in Tastenanschläge umgewandelt. Auf diese Weise können Sie eine Tastatureingabe mit dem Barcodescanner emulieren und die Eingaben an Ihren Host-PC senden. Die Zeichenfolgen bestehen aus tatsächlichen Inhalten und – abhängig von den gescannten Barcodes – aus sogenannten Steuerzeichen. Steuerzeichen enthalten keine Inhalte, sondern lösen verschiedene Aktionen aus. Im Abschnitt "Function Key Emulation“ (Funktionstastenemulation) können Sie mithilfe der Dropdown-Liste verschiedene Aktionen für die einzelnen Steuerzeichen konfigurieren.

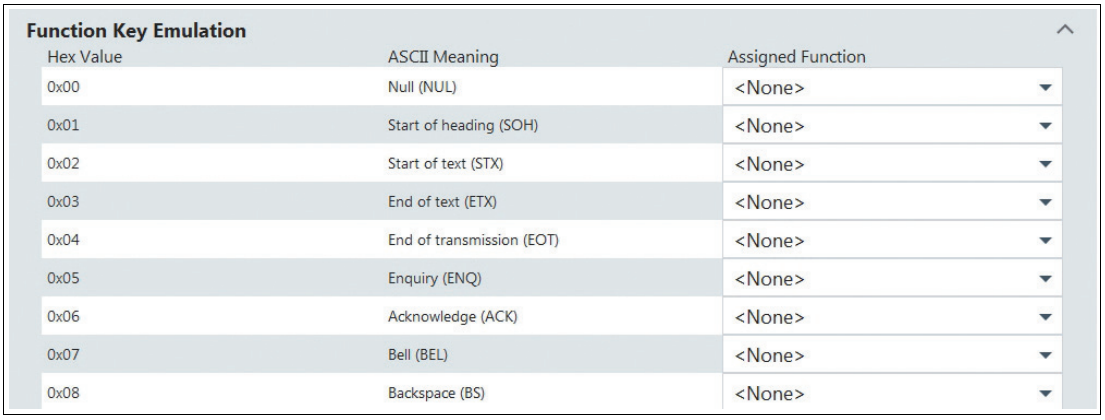


Abbildung 8.46 Wedge-Konfiguration – Funktionstastenemulation

9 App "System Tools“ (System-Tools)

Aufrufen der App "System Tools“ (System-Tools)

1. Rufen Sie die App "System Tools“ (System-Tools) auf, indem Sie auf das entsprechende Symbol auf dem Startbildschirm klicken 

.

Beim Aufrufen der App "System Tools“ (System-Tools) beginnen Sie immer mit dem Untermenü "Clean Lock“ (Reinigungsverriegelung). Es gibt mehrere zusätzliche Untermenüs:

9.1 Clean Lock (Reinigungsverriegelung)

In diesem Untermenü können Sie alle Ihre Eingabegeräte (wie Tastatur, Touchscreen, Touchpad usw.) zum Zweck der Reinigung verriegeln. Dadurch wird der RM vor versehentlichen Eingaben während des Reinigungsvorgangs geschützt.

Stellen Sie mit dem Schieberegler die Zeitdauer ein, für die die Eingabegeräte gesperrt werden.

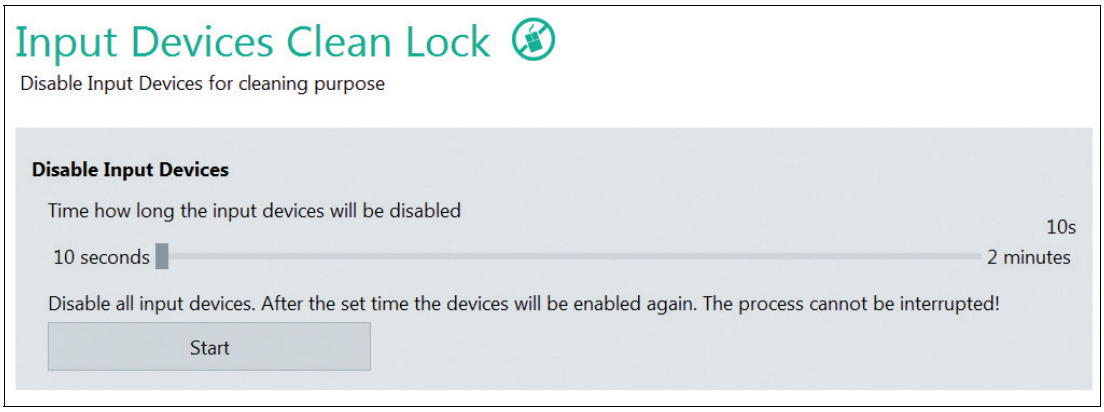


Abbildung 9.1 System-Tools – Einstellungen für die Reinigungsverriegelung

Hinweis!

Es ist möglich, die System Tools App im Bedienermodus über "General Settings“ (Allgemeine Einstellungen) auszublenden. Nähere Informationen finden Sie im Abschnitt 7.1.

9.2 Network Adapter Information (Netzwerkadapter-Informationen)

In diesem Untermenü finden Sie alle Informationen über die Netzwerkadapter-Hardware des lokalen RM.

Die Farbe der Leiste vor dem Netzwerkadapternamen zeigt den Status der Verbindung:

grün	Der Netzwerkadapter ist verbunden.
orange	Der Netzwerkadapter ist nicht verbunden, oder es ist ein Fehler aufgetreten.

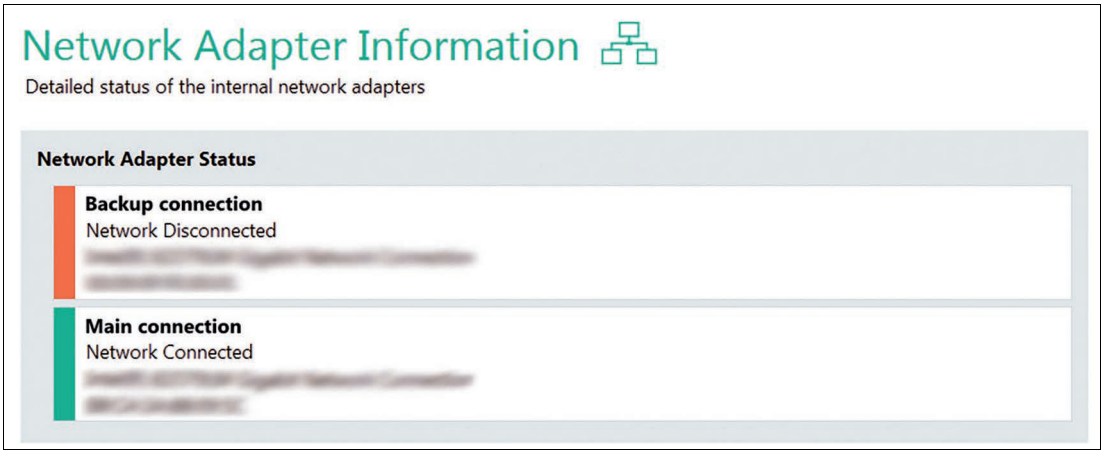


Abbildung 9.2 Systemwerkzeuge: Informationen zum Netzwerkadapter

9.3 Netzwerk-Tool NSLookup

Mit Network NSLookup Tool (Netzwerk–Tool NSLookup) können Sie den Domänennamen einer IP-Adresse oder die IP-Adresse eines Domänennamens überprüfen.

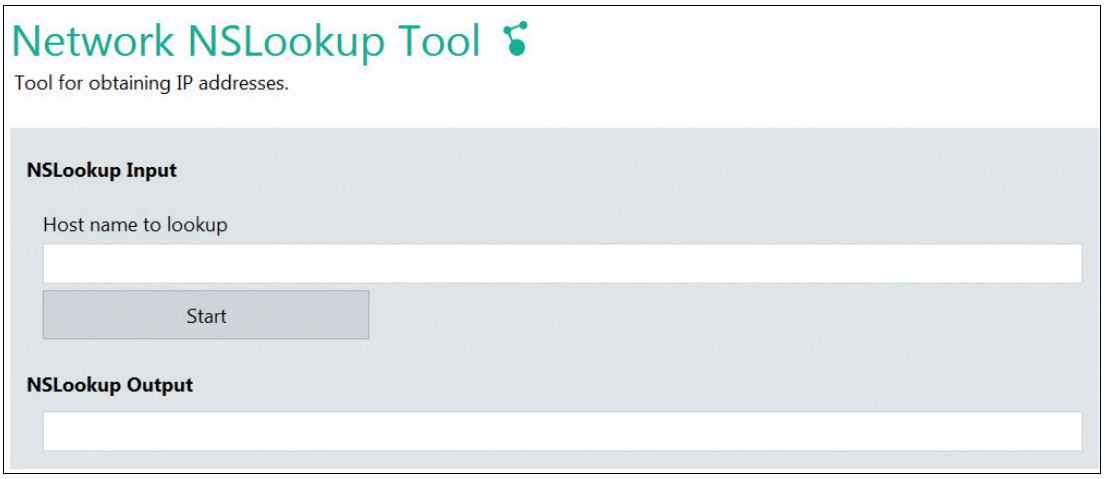


Abbildung 9.3 Network NSLookup Tool (Netzwerk-Werkzeug "NSLookup“)

Überprüfen eines Domänennamens

1. Geben Sie in das Feld "Host name to lookup“ (Hostname für Suche) die IP-Adresse ein.
2. Klicken Sie auf "Start“.

↳ Der entsprechende Domänenname wird im Feld "NSLookup Output“ (NSLookup-Ausgabe) angezeigt.

Überprüfen einer IP-Adresse

1. Geben Sie in das Feld "Host name to lookup“ (Hostname für Suche) den Domänennamen ein.
2. Klicken Sie auf "Start“.

↳ Die entsprechende IP-Adresse wird im Feld "NSLookup Output“ (NSLookup-Ausgabe) angezeigt.

9.4 Network Ping Tool (Netzwerk-Ping-Werkzeug)

In diesem Untermenü können Sie die Netzwerkeinstellungen testen und beispielsweise prüfen, ob der Host über Ethernet erreichbar ist.

Geben Sie im Bereich "Ping Input“ (Ping-Eingabe) die IP-Adresse oder den Computernamen des Computers ein, den Sie pingen möchten, und klicken Sie auf "Start“.

Im Bereich "Ping Status“ (Ping-Status) werden detaillierte Informationen zur Netzwerkverbindung angezeigt.

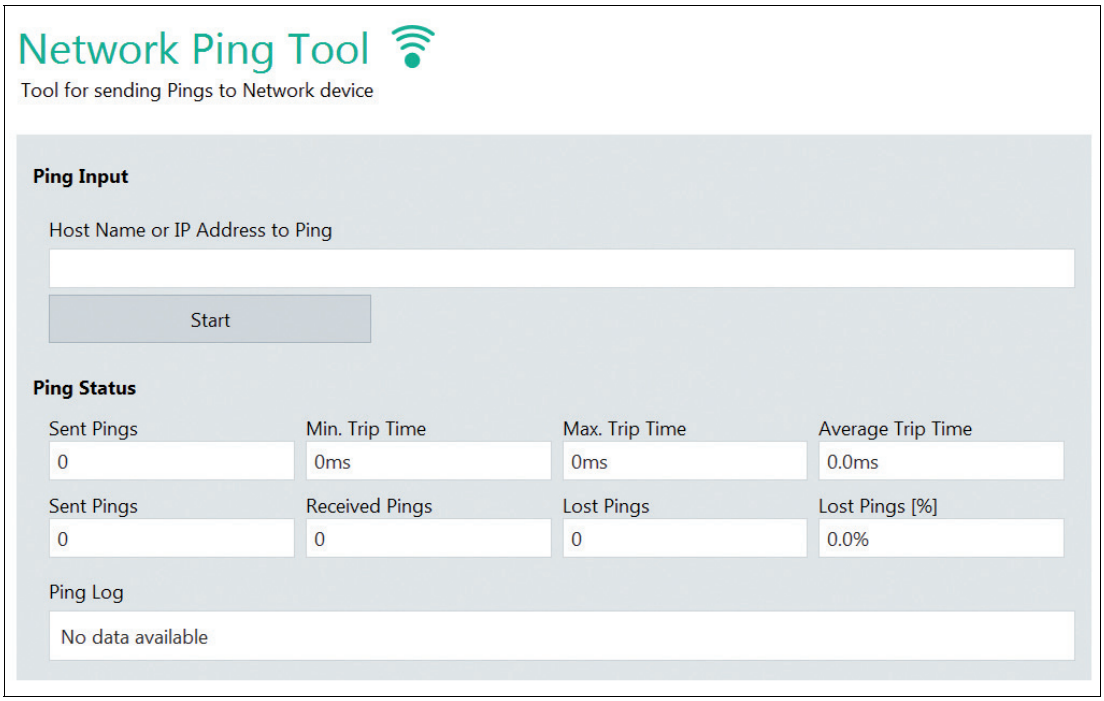


Abbildung 9.4 Systemwerkzeuge – Netzwerk-Ping-Werkzeug

10 Werksseitige Rückstellung

Hinweis!

Um Image-Dateien anwenden und erfassen zu können, ist VisuNet RM Shell Version 5.3 oder höher erforderlich.

Für die werksseitige Rückstellung bei einem Gerät mit resistivem Touchscreen müssen zusätzlich eine Tastatur und eine Maus verwendet werden.

Suchen Sie die derzeit installierte Firmware-Versionsnummer im VisuNet RM Shell-Factory Reset-Menü "Device Info“ (Geräteinfo).

Tipp

Verwenden Sie die zusätzliche Software VisuNet Control Center, um Image-Dateien einfach zu erfassen und auf mehrere kompatible Geräte innerhalb des Netzwerks anzuwenden. Weitere Informationen zu VisuNet CC finden Sie unter www.pepperl-fuchs.com.

Eingabe der werksseitigen Rückstellung über VisuNet RM Shell

1. Wechseln Sie im Hauptbildschirm von "Users“ (Anwender) zu "Administrator“.
2. Klicken Sie auf "System Settings“ (Systemeinstellungen).
3. Navigieren Sie zur Registerkarte "General“ (Allgemein).
4. Erweitern Sie den Abschnitt "Factory Reset“ (Werksseitige Rückstellung).

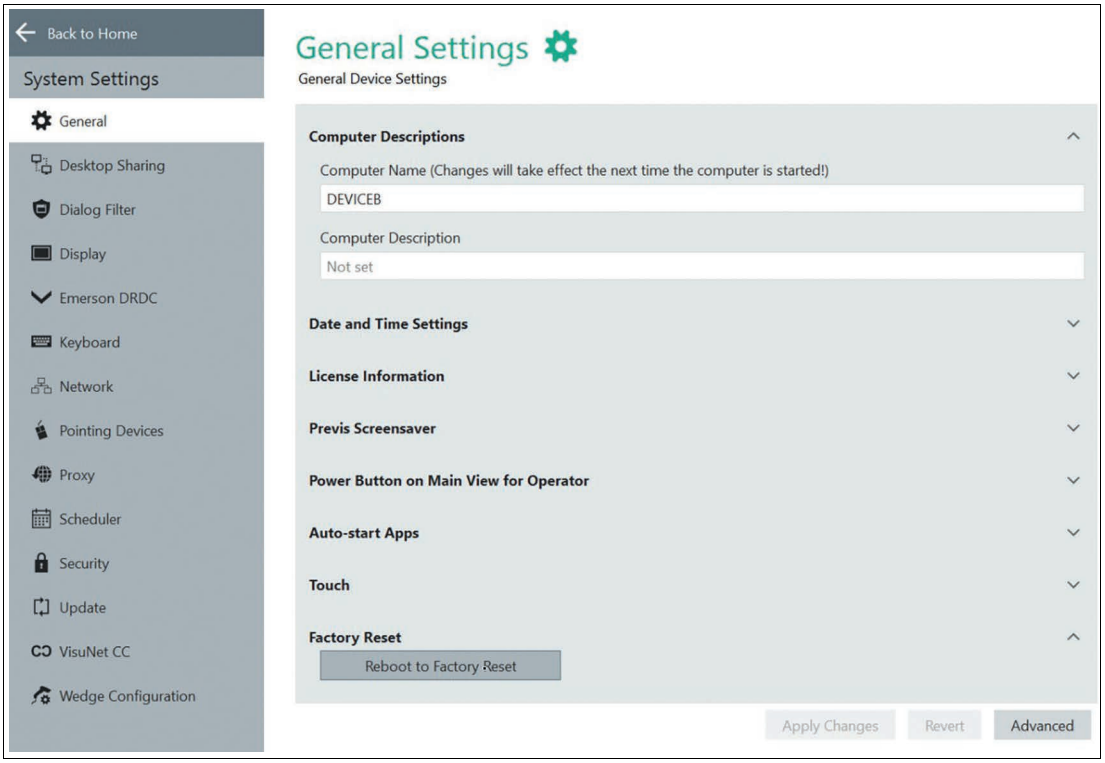


Abbildung 10.1

Factory System-Eingabe, wenn RM Shell abgestürzt ist

1. Schalten Sie das Gerät vollständig aus.
2. Schalten Sie das Gerät wieder ein. Drücken Sie während der ersten Startsequenz wiederholt die Taste "F9“.
3. Wenn ein Menü auf blauem oder schwarzem Hintergrund angezeigt wird, drücken Sie nicht mehr auf die Taste "F9“.

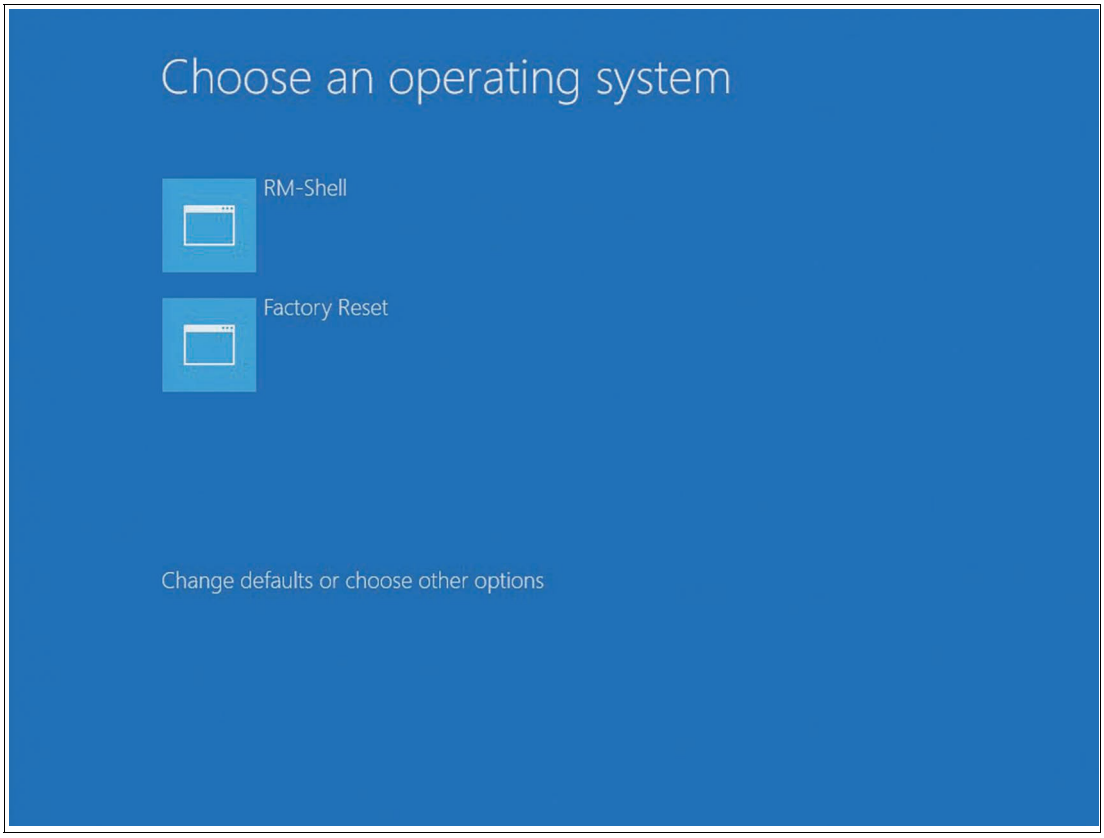


Abbildung 10.2

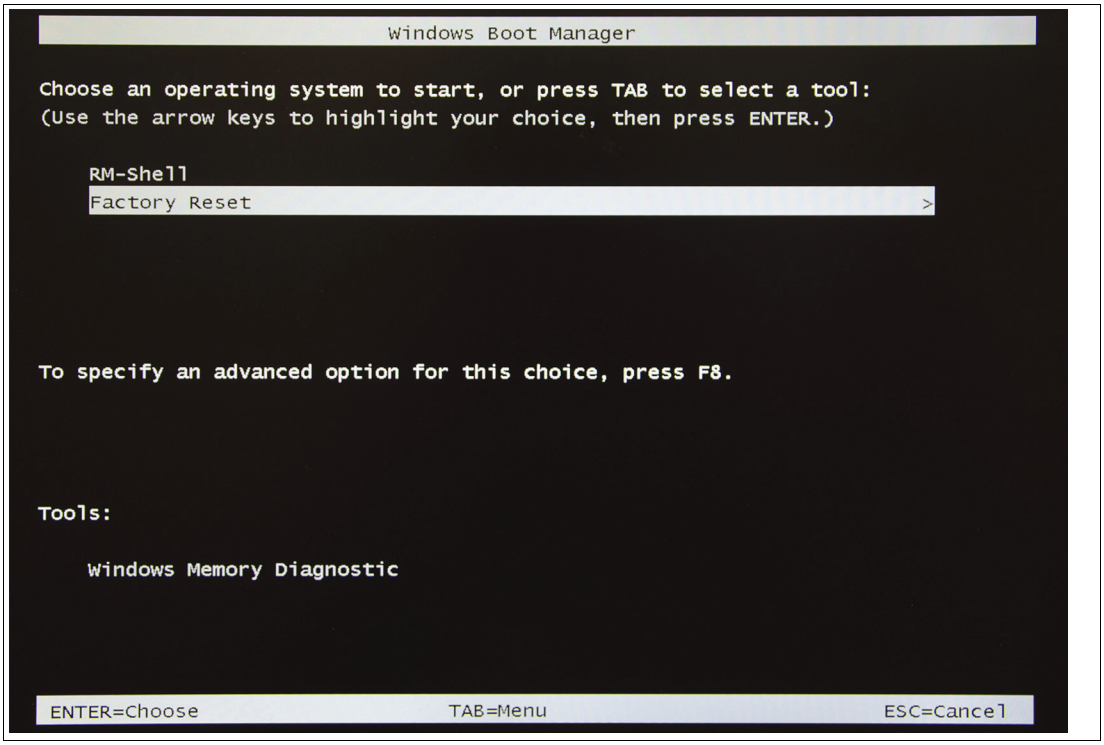


Abbildung 10.3

Anmelden bei VisuNet RM Shell Factory Reset Management

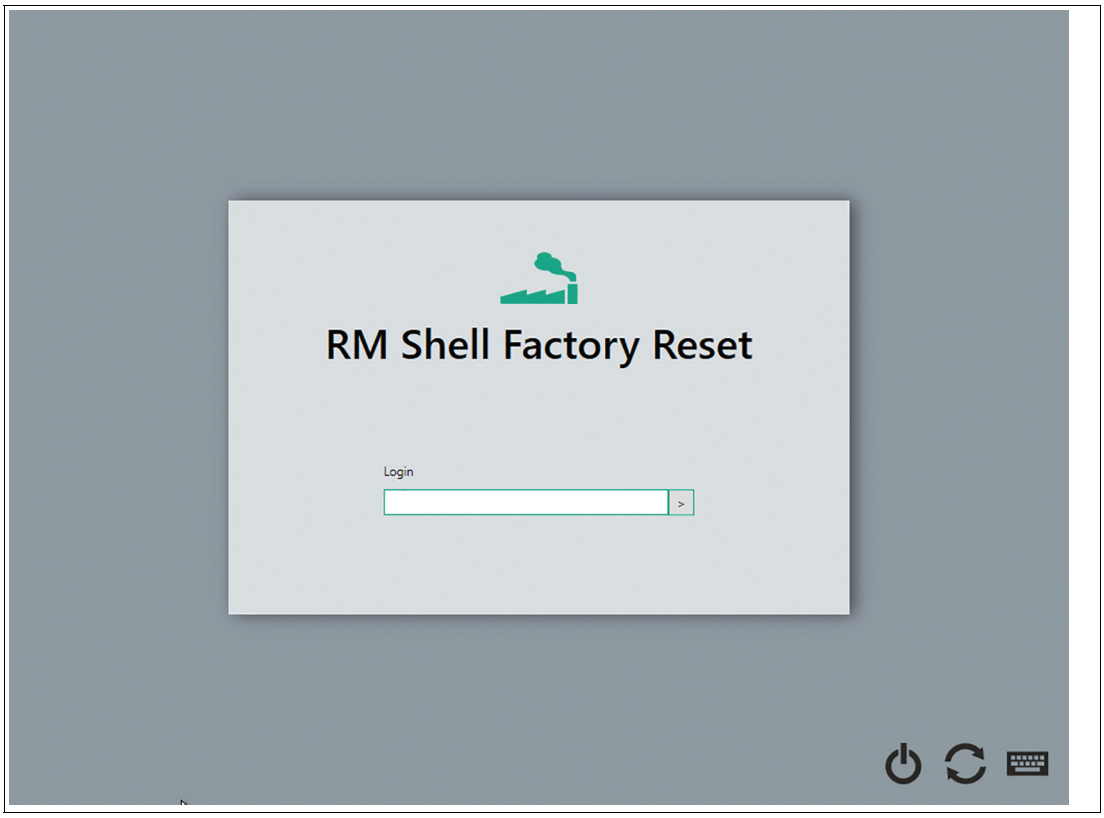


Abbildung 10.4

↳ Verwenden Sie das Standard-Anmeldekennwort **VisuReset**, um sich beim RM Factory Reset Management-Tool anzumelden.

Hinweis!

Öffnen Sie die Bildschirmtastatur, indem Sie auf  klicken. Es kann mehrere Sekunden dauern, bis die Bildschirmtastatur geöffnet wird.

10.1 Kennwort ändern

Standard-Anmeldekennwort ändern

Nach der Anmeldung werden Sie sofort aufgefordert, das Standard-Anmeldekennwort zu ändern.

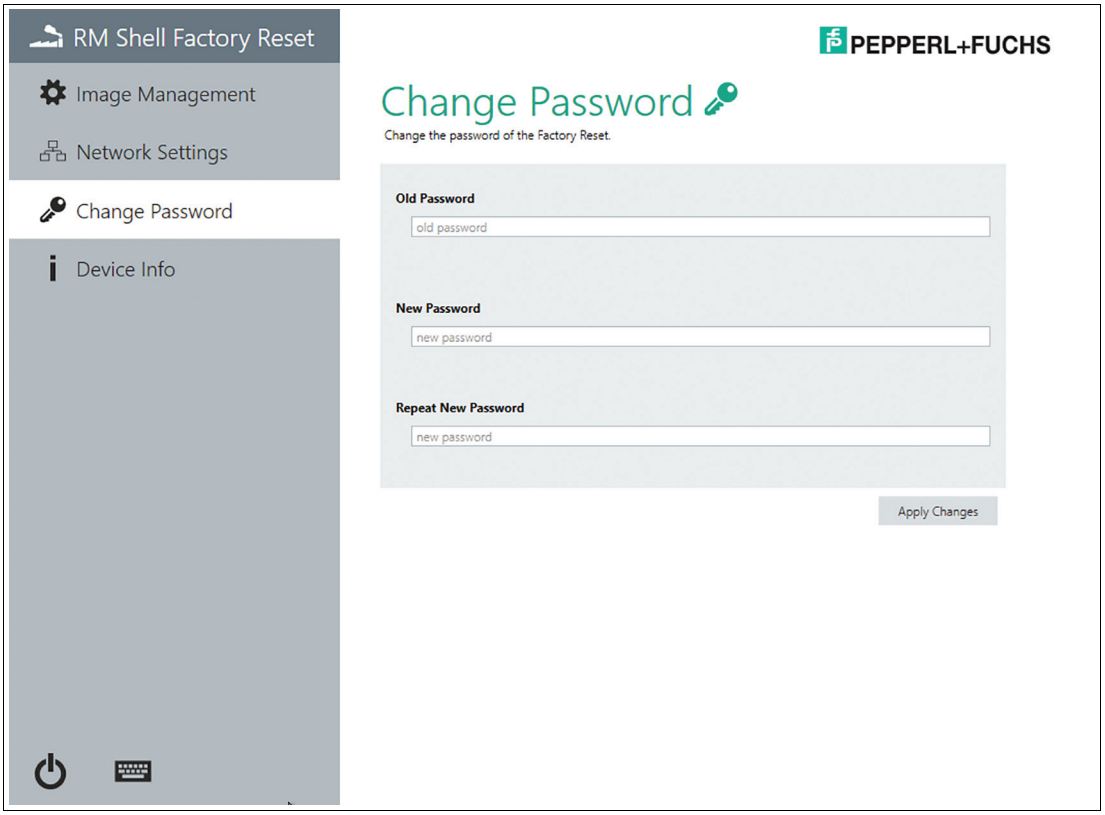


Abbildung 10.5

Hinweis!

Um ein Höchstmaß an Sicherheit zu gewährleisten, muss das Kennwort mindestens 6 Zeichen lang sein.

Das Kennwort kann jederzeit angepasst werden. Bei Abweichungen beim Ändern des Kennwortes werden Sie durch kurze orangefarbene Anmerkungen informiert.

10.2 Image File Management (Image-Datei-Management)

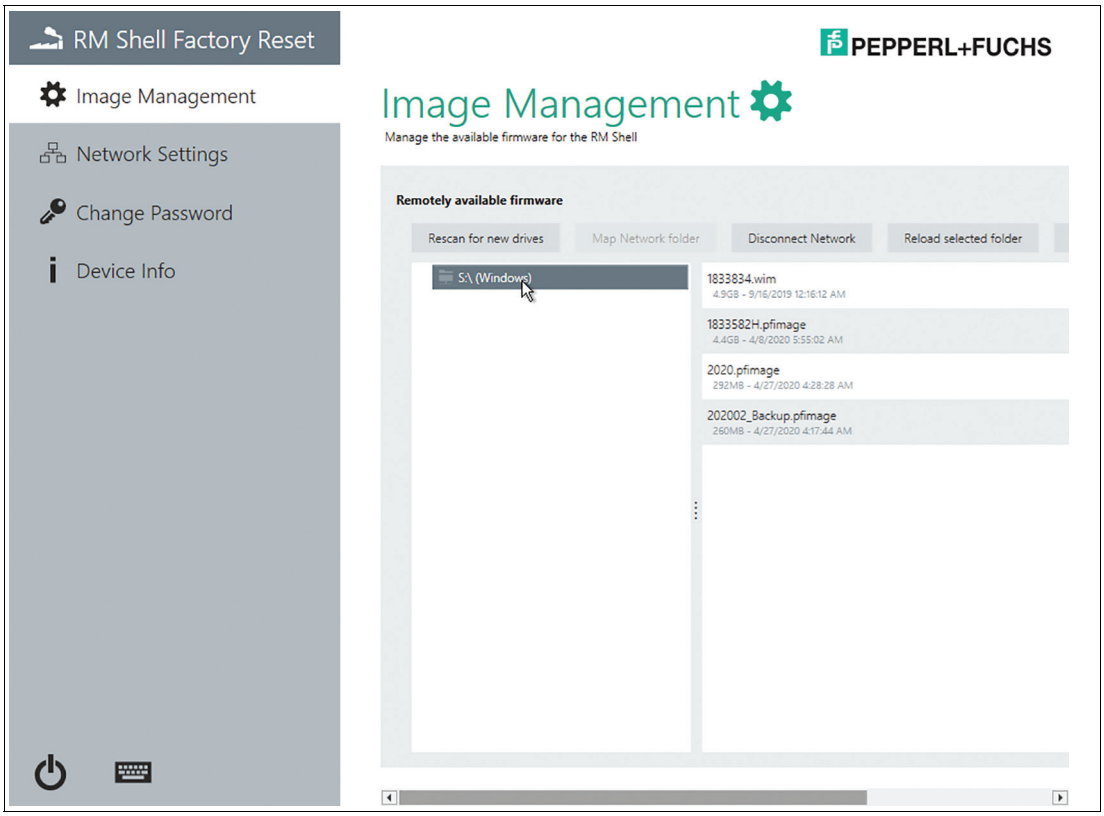


Abbildung 10.6

In diesem Untermenü können Sie die verfügbare Firmware für VisuNet RM Shell verwalten.

Erneut nach neuen Laufwerken suchen	Mit dieser Option wird nach angeschlossenen USB-Flash-Speicherlaufwerken gesucht. USB-Flash-Laufwerke können direkt zur Übertragung von Image-Dateien verwendet werden.
Netzwerkordner zuordnen	Um ein Image anzuwenden oder eine Image-Datei aufzunehmen, wählen Sie zuerst den Netzwerkordner aus. Die Image-Datei wird entweder auf den RM/BTC angewendet, mit dem das Netzwerk verbunden ist, oder das Image des RM/BTC wird erfasst und im Netzwerkordner gespeichert.
Netzwerk trennen	Es kann nur ein Netzwerkordner zugeordnet werden. Um eine Verbindung zu einem anderen Pfad herzustellen, müssen Sie zuerst die bestehende Pfadverbindung trennen.
Ausgewählten Ordner neu laden	Wenn während der Verbindung Aktualisierungen oder Änderungen im verbundenen Ordner vorgenommen wurden, verwenden Sie diese Schaltfläche, um die Daten neu zu laden.
Backup Image erfassen	Ordnen Sie zunächst einen Netzwerkordner zu, der im RM/BTC-Netzwerk verfügbar ist. Die Geräteeinstellungen des RM/BTC werden als Backup Image erfasst und im ausgewählten Netzwerkordner gespeichert. Diese Sicherung kann nur auf dasselbe Gerät/Gerät mit derselben Seriennummer angewendet werden. **Achtung:** Für jede Image-Datei sind ca. 7 GB Speicherplatz erforderlich. Dies hängt vom verwendeten Festplattenspeicher der Geräte ab. Stellen Sie sicher, dass die betreffende Netzwerkfreigabe über ausreichend Speicherplatz verfügt. Der Erfassungsprozess dauert je nach Netzwerkgeschwindigkeit etwa 30 Minuten.

Hinweis!

Weitere Informationen zu den verfügbaren Image-Dateien finden Sie in Kapitel 2.1.

Backup Image erfassen

1. Wählen Sie die **Netzwerkfreigabe** aus, mit der die "Image-Dateien“ übertragen werden. Stellen Sie sicher, dass die Netzwerkfreigabe über ausreichend Speicherplatz verfügt (~ 7 GB sind für jede Image-Datei erforderlich)
2. Legen Sie den Namen der Image-Datei fest und fahren Sie mit dem Aufnahmevorgang fort.

Abbildung 10.7

Backup Image oder offizielles Pepperl+Fuchs Image anwenden

1. Wählen Sie die Netzwerkfreigabe aus, mit der die Image-Dateien übertragen werden.
2. Wählen Sie die Image-Dateien aus, die Sie anwenden möchten. Sie können entweder eine Image-Datei anwenden, die zuvor von Ihrem RM/BTC mit derselben Seriennummer/demselben Gerät aufgenommen wurde, oder ein offizielles Pepperl+Fuchs Image, das für jeden spezifischen RM oder BTC verfügbar ist.
Wenden Sie sich an Ihren lokalen Vertriebssupport, wenn Sie das offizielle Pepperl+Fuchs Image anwenden möchten.

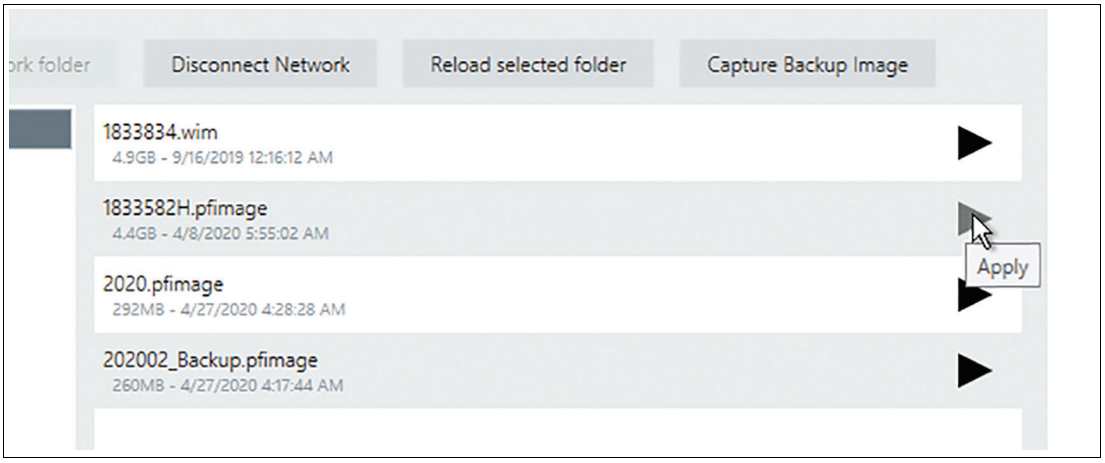


Abbildung 10.8

3. Klicken Sie auf "Apply“ (Anwenden), um die ausgewählte Firmware anzuwenden.

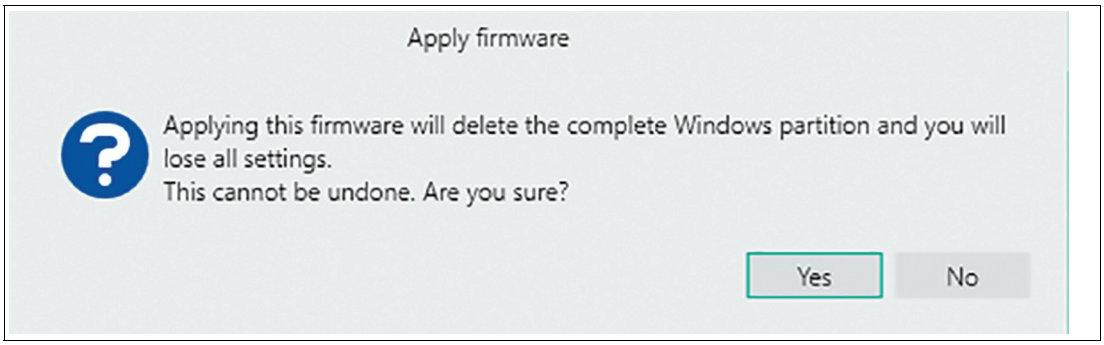


Abbildung 10.9

4. Nachdem Sie auf **Yes** (Ja) geklickt haben, wird die vollständige Windows®-Partition gelöscht, und die ausgewählte Image-Datei wird auf Ihr Gerät angewendet. Der Anwendungsvorgang dauert etwa 15 Minuten. Das System wird neu gestartet, nachdem die Image-Datei angewendet wurde.

10.3 Netzwerkeinstellungen

In diesem Abschnitt finden Sie allgemeine Informationen zu den Netzwerkeinstellungen.

Verwenden Sie diese Option zum Aktivieren/Deaktivieren von DHCP (Dynamic Host Configuration Protocol). Mit DHCP können Sie RM/BTC ohne weitere manuelle Konfiguration in ein bestehendes Netzwerk integrieren. Einstellungen wie IP-Adresse, Subnetzmaske, Standard-Gateway und DNS-Server werden dem RM/BTC automatisch zugewiesen. Sie können jedoch alle diese Parameter manuell einrichten, indem Sie die DHCP-Option deaktivieren.

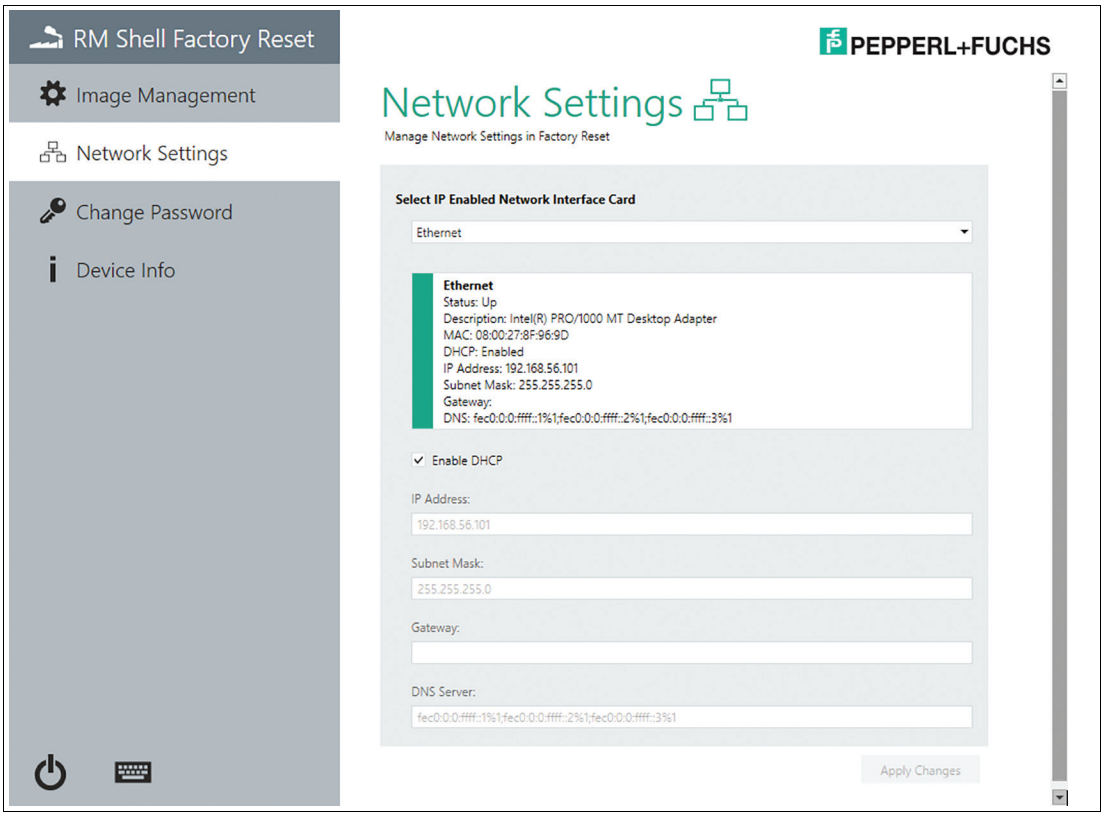


Abbildung 10.10

10.4 Geräteinformationen

Dieses Untermenü enthält Informationen zu "Factory Reset Version“ (auf die Werkseinstellungen zurückgesetzte Version), "Device Description“ (Gerätebeschreibung), "Installed Image File“ (installierte Image-Datei), "Compatible Images“ (kompatible Images), "Partitions“ (Partitionen) und "Licenses“ (Lizenzen).

Die Informationen sind nützlich, wenn Sie die Firmware aktualisieren, bzw. können für den technischen Support notwendig sein.

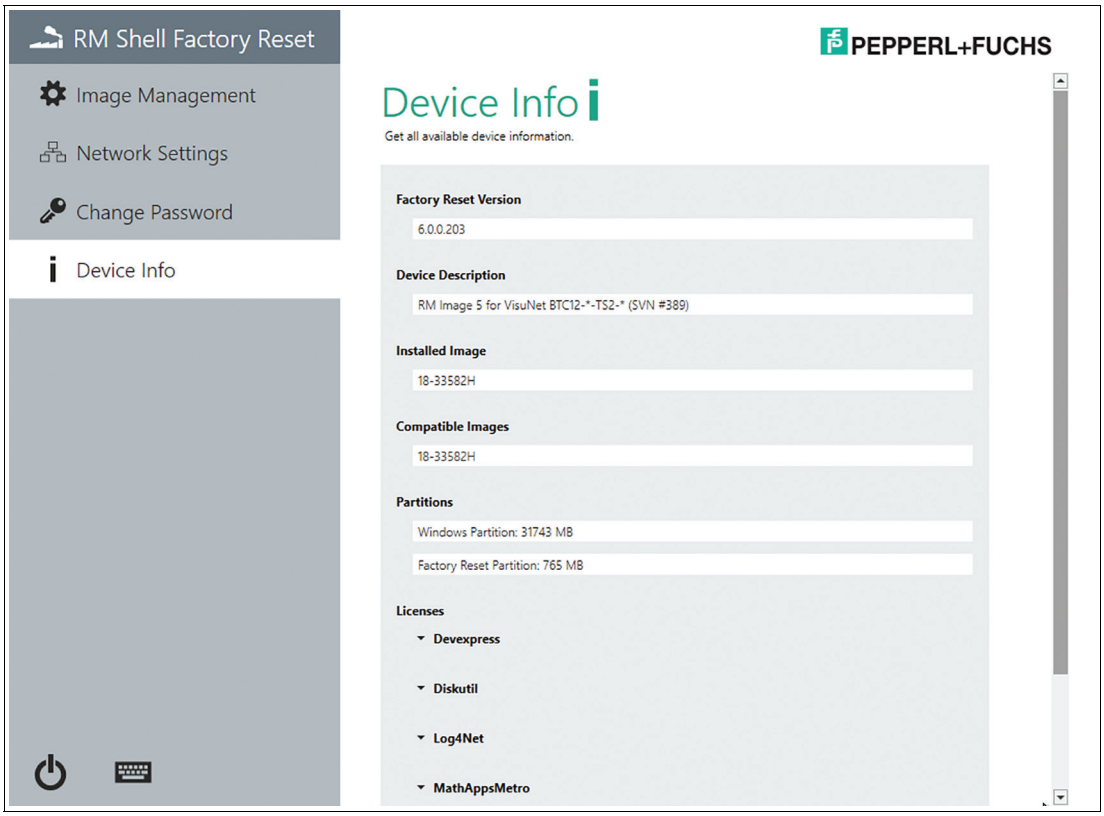


Abbildung 10.11

11 Anleitungen

11.1 Verbinden eines RM/BTC mit einem PC über RDP

Hinweis!

In diesem Kapitel wird beschrieben, wie ein RM/BTC unter Microsoft Windows mit einem PC über RDP verbunden wird.

Um die Kommunikation zwischen einem RM/BTC und einem PC sicherzustellen, müssen beide Geräte Teil desselben Netzwerkes und Subnetzes sein. Wenn Sie beide Geräte in einem Netzwerk mit einem DHCP-Server verwenden, gibt der DHCP-Server die IP-Adressen automatisch aus.

Für den Anschluss eines RM/BTC an einen PC empfiehlt Pepperl+Fuchs, die Konfiguration in 2 Schritten durchzuführen:

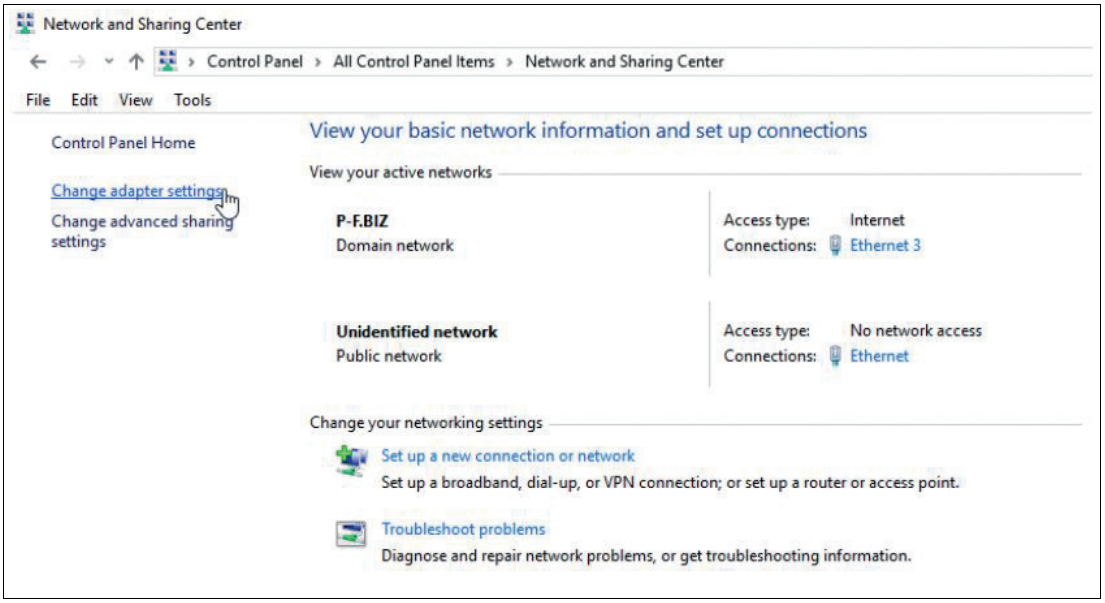
- Schritt 1: PC-Konfiguration
  - Manuelle Zuweisung der IP-Adresse
  - Aktivierung der RDP-Serverfunktion
- Schritt 2: RM/BTC-Konfiguration
  - Manuelle Zuweisung der IP-Adresse
  - Erstellung eines RDP-Profils

Schritt 1: PC-Konfiguration

Manuelles Zuweisen der IP-Adresse des PCs

1. Öffnen Sie "Network and Sharing Center“ (Netzwerk- und Freigabecenter) in der Taskleiste, indem Sie erst auf  und dann auf "Network and Sharing Center“ (Netzwerk- und Freigabecenter) klicken.

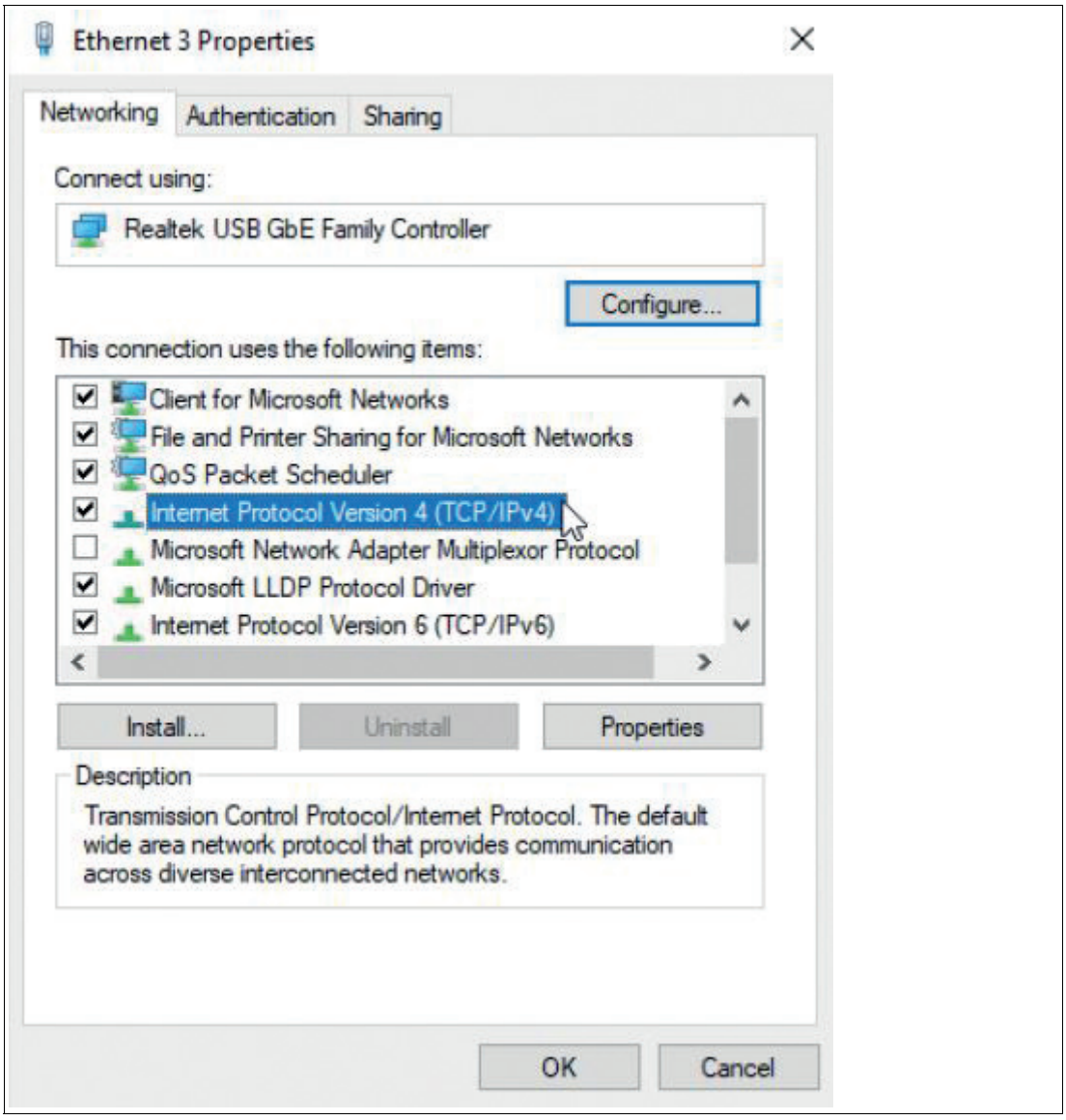
   ↳ Das Fenster "Network and Sharing Center“ (Netzwerk- und Freigabecenter) wird geöffnet.



2. Wählen Sie in der Navigationsleiste "Change adapter settings“ (Adaptereinstellungen ändern) aus.

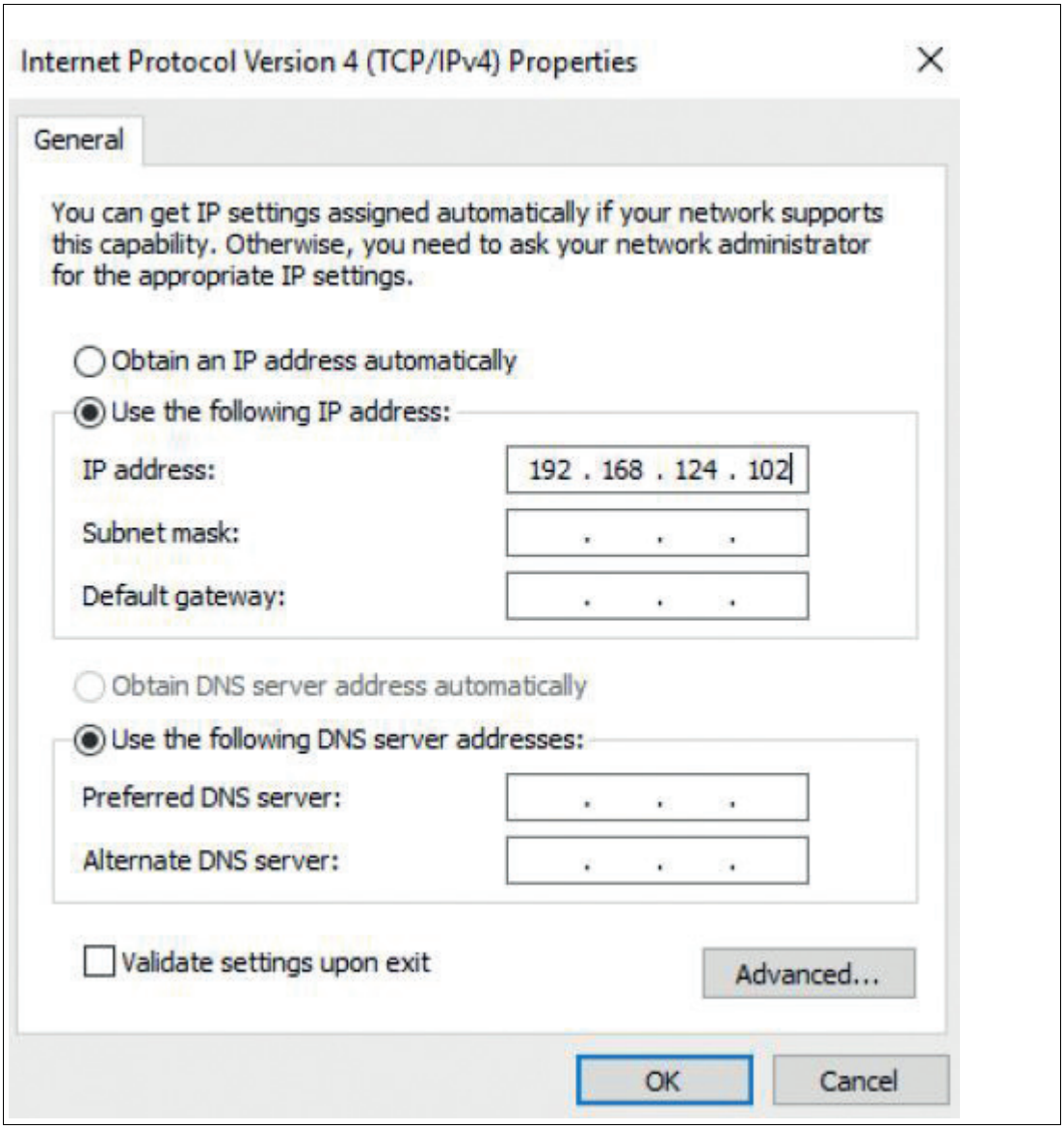
3. Suchen Sie nach der Netzwerkverbindung, die die Hardware-Komponente Ihres physischen Netzwerkanschlusses anzeigt. Die Hardware-Komponente des physischen Netzwerkanschlusses ist an ihrem Namen in der dritten Zeile erkennbar (z. B. "Intel(R) 82579LM...“)
4. Klicken Sie mit der rechten Maustaste auf die Netzwerkverbindung und wählen Sie "Properties“ (Eigenschaften) aus.

   ↳ Das Fenster "Local Area Connection Properties“ (Eigenschaften von LAN-Verbindung) wird geöffnet.



5. Heben Sie in der Liste "This connection uses the following items“ (Diese Verbindung verwendet die folgenden Elemente) die Option "Internet Protocol Version 4 (TCP/IPv4)“ (Internetprotokoll Version 4 (TCP/IPv4)) hervor.
6. Klicken Sie auf "Properties“ (Eigenschaften).

   ↳ Das Fenster "Internet Protocol Version 4 (TCP/IPv4) Properties“ (Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)) wird geöffnet.

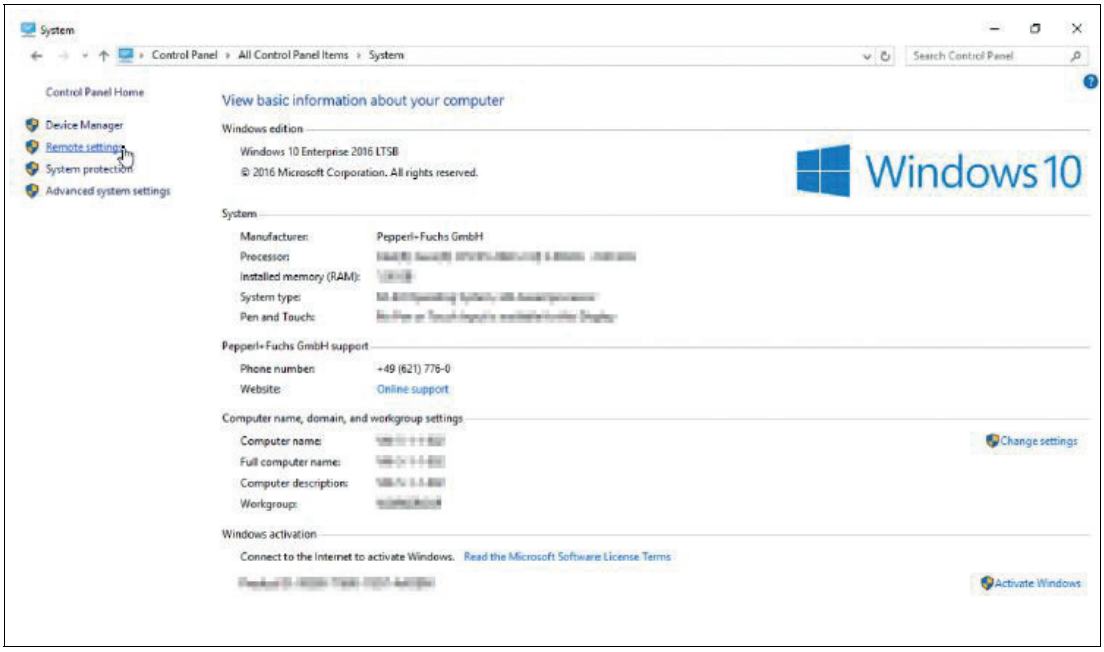


7. Wählen Sie die Option "Use the following IP address“ (Folgende IP-Adresse verwenden) aus und geben Sie eine statische IP-Adresse ein (z. B. "192.168.124.102“).
8. Klicken Sie auf "OK“, um die Änderungen zu bestätigen.
9. Schließen Sie das "Network and Sharing Center“ (Netzwerk- und Freigabecenter).

Aktivieren der RDP-Serverfunktion

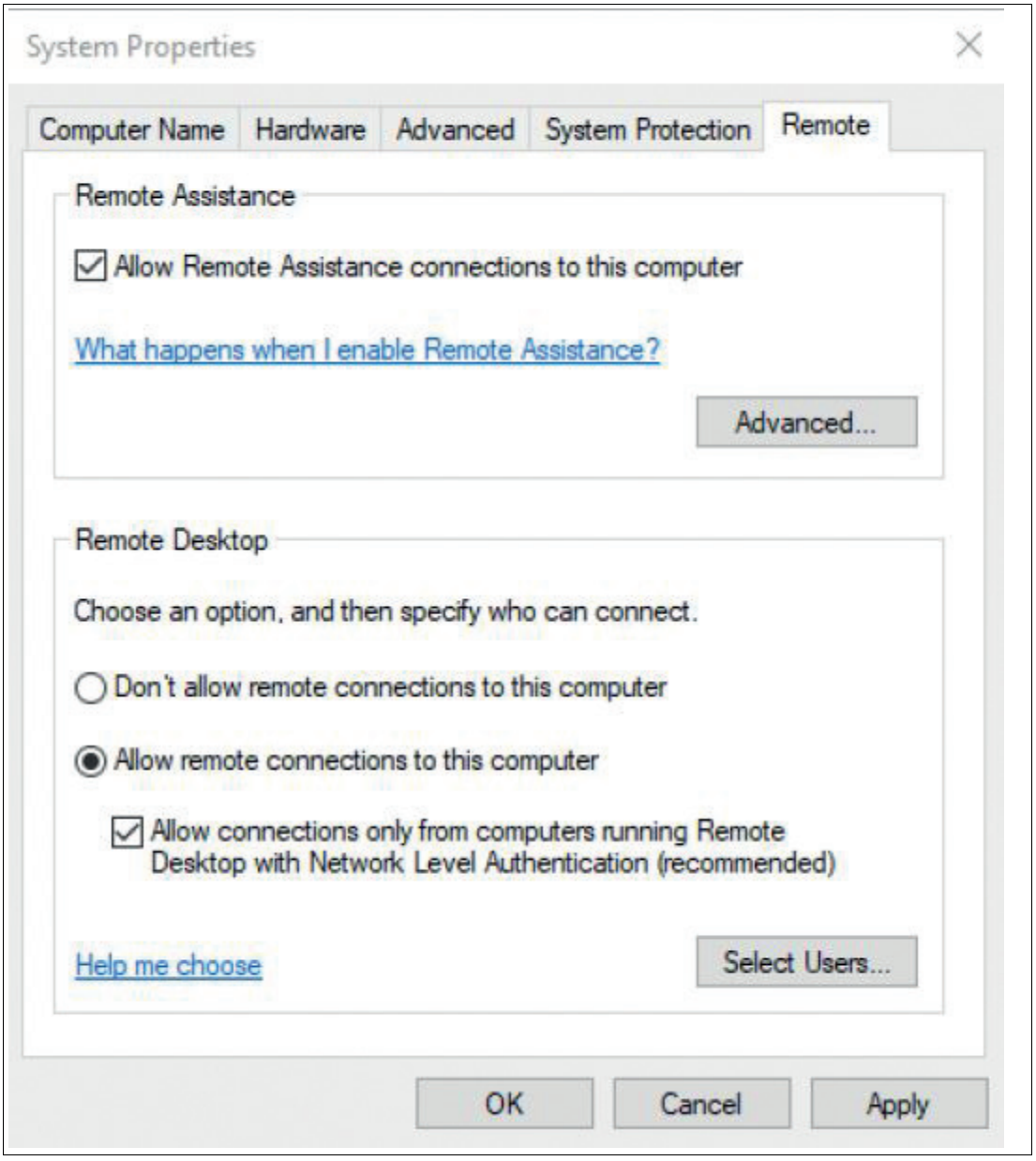
1. Öffnen Sie das Startmenü, klicken Sie mit der rechten Maustaste auf "Computer“ und wählen Sie "Properties“ (Eigenschaften) aus.

   ↳ Das Systembedienfeld wird geöffnet.



2. Klicken Sie auf "Remote settings“ (Remote-Einstellungen).

   ↳ Das Dialogfeld "System properties“ (Systemeigenschaften) wird geöffnet.



3. Wählen Sie die Option "Remote connections to this computer“ (Remote-Verbindungen zu diesem Computer) aus.

Hinweis!

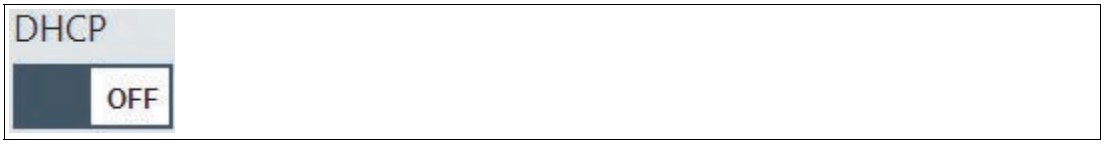
Es wird empfohlen, die zusätzliche Standardauthentifizierung auf Netzwerkebene "Network Level Authentication“ aktiviert zu lassen

4. Klicken Sie auf "OK“.
5. Schließen Sie das Systembedienfeld, um die Änderungen zu bestätigen.

Schritt 2: RM/BTC-Konfiguration

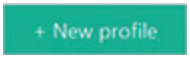
Manuelles Zuweisen der IP-Adresse des RM/BTC

1. Melden Sie sich bei RM/BTC Shell als Administrator an.
2. Starten Sie die App "System Settings“ (Systemeinstellungen)
3. Wählen Sie das Untermenü "Network“ (Netzwerk) aus.
4. Wenn mehrere Netzwerkadapter verfügbar sind, wählen Sie den Netzwerkadapter mit dem Status "Network connected" (Netzwerk verbunden) (grün) aus.
5. Deaktivieren Sie die Option DHCP.



6. Geben Sie in das Feld "IP address“ (IP-Adresse) eine IP-Adresse ein, die sich in den letzten drei Ziffern von der IP-Adresse unterscheidet, die dem PC zugewiesen ist (z. B. "192.168.124.101“).
7. Geben Sie in das Feld "Subnet Mask“ (Subnetzmaske) 255.255.255.0 ein.
8. Klicken Sie auf "Apply Changes“ (Änderungen übernehmen), um die Änderungen zu bestätigen.

Erstellen eines entsprechenden RDP-Profils

1. Wenn Sie nicht angemeldet sind, melden Sie sich bei RM Shell als Administrator an.
2. Starten Sie die App "Profiles Management“ (Profilverwaltung).
3. Erstellen Sie ein neues Profil, indem Sie auf 

klicken.
4. Wählen Sie "Microsoft RDP“ aus und klicken Sie auf "OK“.

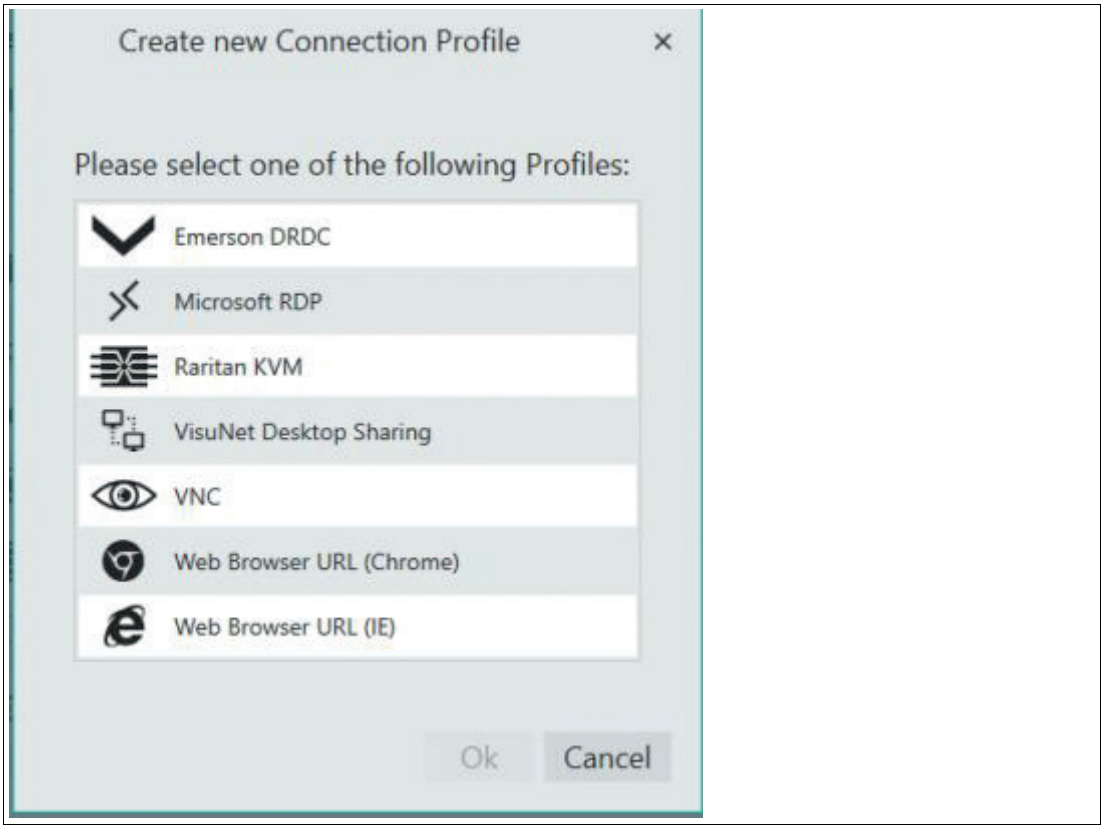


Abbildung 11.1 Das Dialogfenster "Create new Connection Profile“ (Neues Verbindungsprofil erstellen)

↳ Das RDP-Profil wird erstellt. Die Haupteinstellungen des neuen Profils werden geöffnet.

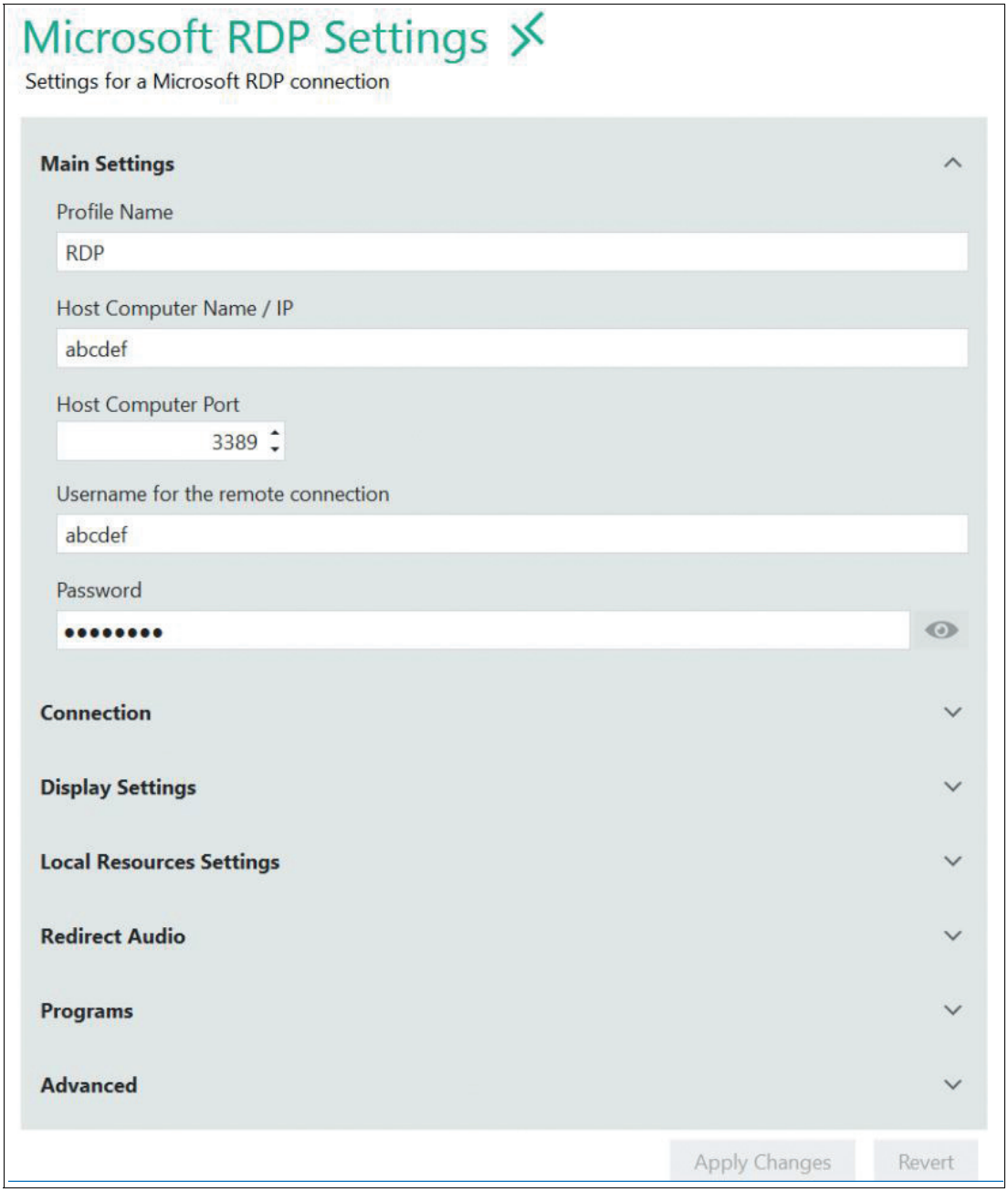


Abbildung 11.2 Die wichtigsten Einstellungen in einem Microsoft RDP-Profil

5. Geben Sie unter "Profile Name“ (Profilname) einen entsprechenden Namen für das aktuelle Verbindungsprofil ein.
6. Geben Sie unter "Host Computer/IP“ (Host-Computer/IP) die IP-Adresse ein, die Sie zuvor in der PC-Konfiguration eingegeben haben ("192.168.124.102“).
7. Optional: Bearbeiten Sie die anderen Einstellungen. Klicken Sie nach der Bearbeitung auf Apply Changes.

   ↳ Das neue Profil wird erstellt.
8. Kehren Sie zum Startbildschirm zurück.

   ↳ Das neue RDP-Profil ist jetzt im linken Profilbereich des Startbildschirms verfügbar.

11.2 Erhöhen von RDP-Reaktivität und -Leistung

Die Leistung und Reaktivität einer Windows RDP-Verbindung kann mit der neuesten Protokollversion RDP 8.0 erhöht werden. RDP 8.0 wurde mit Microsoft Windows Server 2012 und Windows 8 eingeführt.

Für Systeme, auf denen Windows 7 Service Pack 1 (SP1) oder Windows Server 2008 R2 Service Pack 1 (SP1) ausgeführt wird, wird ein offizielles RDP-Update von Microsoft bereitgestellt, mit dem RDP 8 auf diesen Systemen installiert werden kann.

Wenn Sie ein Hostsystem haben, auf dem Windows 7 SP1 oder Windows Server 2008 R2 SP1 ausgeführt wird, installieren Sie den RDP8-Patch, damit Sie von den Leistungsverbesserungen profitieren können.

Weitere Informationen finden Sie im offiziellen Artikel der Microsoft Knowledge Base, der die Installationsschritte detailliert beschreibt: https://support.microsoft.com/en-us/kb/2592687

11.3 Konfigurieren der automatischen Abmeldung von der Sitzung (Sitzungs-Timeout) mit RDP

Um Computerressourcen auf Ihrem Hostsystem zu speichern, ist es manchmal nützlich, eine automatische Abmeldung zu konfigurieren, wenn innerhalb eines bestimmten Zeitraums keine Benutzereingabe erfolgt ist.

Wenn Sie eine Zeitüberschreitung für inaktive RDP-Sitzungen einrichten möchten, können Sie diese über eine Richtlinie auf Ihrem Windows-Hostsystem konfigurieren.

Führen Sie die folgenden Konfigurationsschritte auf Ihrem Hostsystem aus, um eine automatische Abmeldung für eine inaktive Sitzung zu aktivieren:

Konfigurieren einer automatischen Abmeldung

1. Öffnen Sie Group Policy Editor (Gruppenrichtlinieneditor) über `cmd -> gpedit.msc`.
2. Navigieren Sie zu `Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\` (Computerkonfiguration\Richtlinien\Verwaltungsvorlagen\Windows-Komponenten\Remote Desktop Services\Remote Desktop-Sitzungs-Host\Sitzungszeitlimit\)
3. Öffnen Sie die Einstellung `Set time limit for active but idle Remote Desktop Services Sessions` (Zeitlimit für aktive, aber im Leerlauf befindliche Remote Desktop Services-Sitzungen festlegen), setzen Sie es auf `Enabled` (Aktiviert) und wählen Sie das Zeitlimit aus der Dropdown-Liste aus. Schließen Sie alle Fenster, indem Sie auf `OK` klicken.
4. Führen Sie `cmd` aus und geben Sie den Befehl `gpupdate`, um die Richtlinie zu aktualisieren.

   ↳ Nachdem die Richtlinien des Hostsystems aktualisiert wurden, sollte die automatische Anmeldung mit gespeicherten Anmeldedaten funktionieren.

Weitere Informationen finden Sie im offiziellen Microsoft-Artikel, der die Konfigurationsschritte detailliert beschreibt: https://technet.microsoft.com/en-us/library/cc754272(v=ws.11).aspx

11.4 Konfigurieren eines Setups mit mehreren Monitoren (erweiterter Desktop) mit RDP und Box Thin Client BTC

Wenn Sie einen Box Thin Client BTC mit mehreren Monitoren verwenden, können Sie eine RDP-Verbindung über alle angeschlossenen Monitore hinweg ausdehnen. Die RDP-Verbindung verhält sich dann wie ein lokaler "erweiterter Desktop“.

Um eine RDP-Verbindung als Verbindung mit mehreren Monitoren zu konfigurieren, gehen Sie wie folgt vor:

Configuring a Multi-Monitor Connection with RDP and BTC (Konfigurieren einer Verbindung mit mehreren Monitoren mit RDP und BTC)

Hinweis!

Diese Funktion ist nur verfügbar, wenn mehrere Monitore an das Gerät angeschlossen sind.

1. Schließen Sie die anderen erforderlichen Monitore an.
2. Melden Sie sich an der Benutzerrolle `Engineer` (Ingenieur) oder `Administrator` an.
3. Öffnen Sie `Profile Management` (Profilverwaltung).
4. Wählen Sie die RDP-Verbindung aus, die Sie über alle angeschlossenen Monitore erweitern möchten, und aktivieren Sie die Funktion `Fullscreen Mode` (Vollbildmodus).
5. Wechseln Sie zum Abschnitt `Display Settings` (Display-Einstellungen) und ändern Sie die Funktion `Show the connection on the following displays` (Verbindung anzeigen auf den folgenden Anzeigen) in `Expand over all displays` (Auf allen Displays erweitern).
6. Übernehmen Sie die Änderungen.

Weitere Informationen finden Sie im offiziellen Microsoft-Artikel, der die Konfigurationsschritte detailliert beschreibt: https://technet.microsoft.com/en-us/library/cc754272(v=ws.11).aspx

Wichtig: Die RDP-Verbindung "Extended Desktop“ (erweitertes Desktop) kann nur für Hostsysteme hergestellt werden, auf denen Windows 7 Ultimate, Windows 7 Enterprise (und Windows Server 2008 R2 oder höher) ausgeführt wird. Diese Funktion wird von Windows 7 Professional nicht unterstützt! Siehe Microsoft Community Post: https://answers.microsoft.com/en-us/windows/forum/windows_7-networking/windows-7-remote-desktop-with-multi-monitor/6bf0d5e3-644f-404e-baaf-ff2085e1c2c2

Hinweis!

Um die physische Anordnung der angeschlossenen Monitore mit der RDP-Verbindung darzustellen, stellen Sie sicher, dass die Monitore auch in den Display-Einstellungen korrekt angeordnet sind. Im Kapitel "Display-Einstellungen“ wird beschrieben, wie eine Einrichtung mit mehreren Monitoren konfiguriert werden kann.

11.5 Installieren von McAfee Endpoint Security

Hinweis!

Kompatibilität von Drittanbieter-Software

RM Shell ist für die Arbeit mit Software vorgesehen, die mit VisuNet-Geräten von Pepperl+Fuchs geliefert wird. Pepperl+Fuchs übernimmt keine Garantie für die Funktionalität von Drittanbieter-Software. Die Kunden sind dafür verantwortlich, die Kompatibilität mit Software von Drittanbietern sicherzustellen.

Bevor Sie beginnen

Bevor Sie McAfee Endpoint Security installieren, besuchen Sie das McAfee Knowledge Center und überprüfen Sie die Software- und Hardwarekompatibilität: https://kc.mcafee.com/corporate/index?page=content&id=KB82761.

Anforderungen

- USB-Stick
- Zusätzlicher PC zum Herunterladen und Entpacken der Installationsdateien

2024-01

Schritt 1: Download

- Laden Sie die McAfee-Software auf einen separaten PC herunter und entpacken Sie die ZIP-Datei auf einem USB-Stick.

Schritt 2: Deaktivieren des Filters

- Deaktivieren Sie den Unified Write Filter auf Ihrem Remote-Monitor. Siehe Kapitel 4.1.

Schritt 3: Öffnen von General Settings (Allgemeine Einstellungen)

- Öffnen Sie General Settings (Allgemeine Einstellungen) in der Administratorrolle

Schritt 4: Öffnen von Windows Explorer

- Öffnen Sie den Windows-Explorer im Startmenü

Schritt 5: Installieren

- Schließen Sie den USB-Stick an Ihren Remote-Monitor an und navigieren Sie zu den Installationsdateien. Führen Sie die Datei **setupEP.exe** aus und befolgen Sie die Installationsanweisungen.

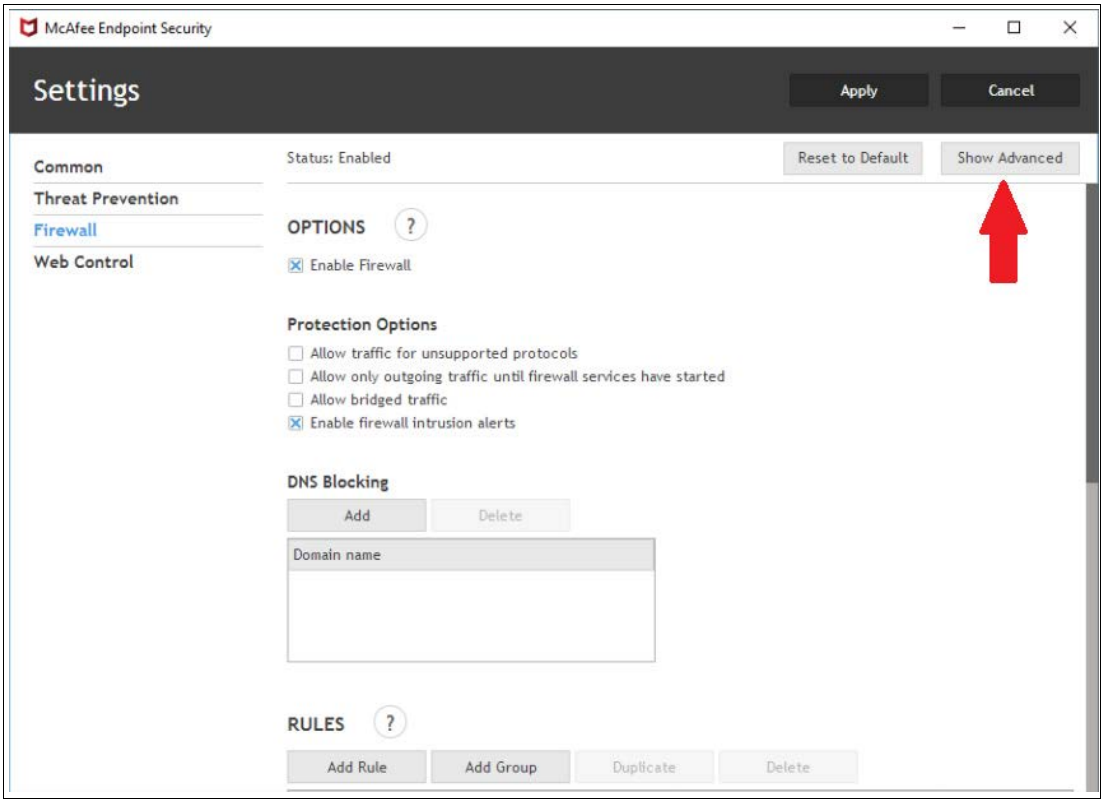
Schritt 6: Erstellen einer allgemeinen App

- Erstellen Sie eine allgemeine App für McAfee Endpoint Security. Dadurch wird ein Link zur Software auf dem Startbildschirm bereitgestellt. Siehe Kapitel 7

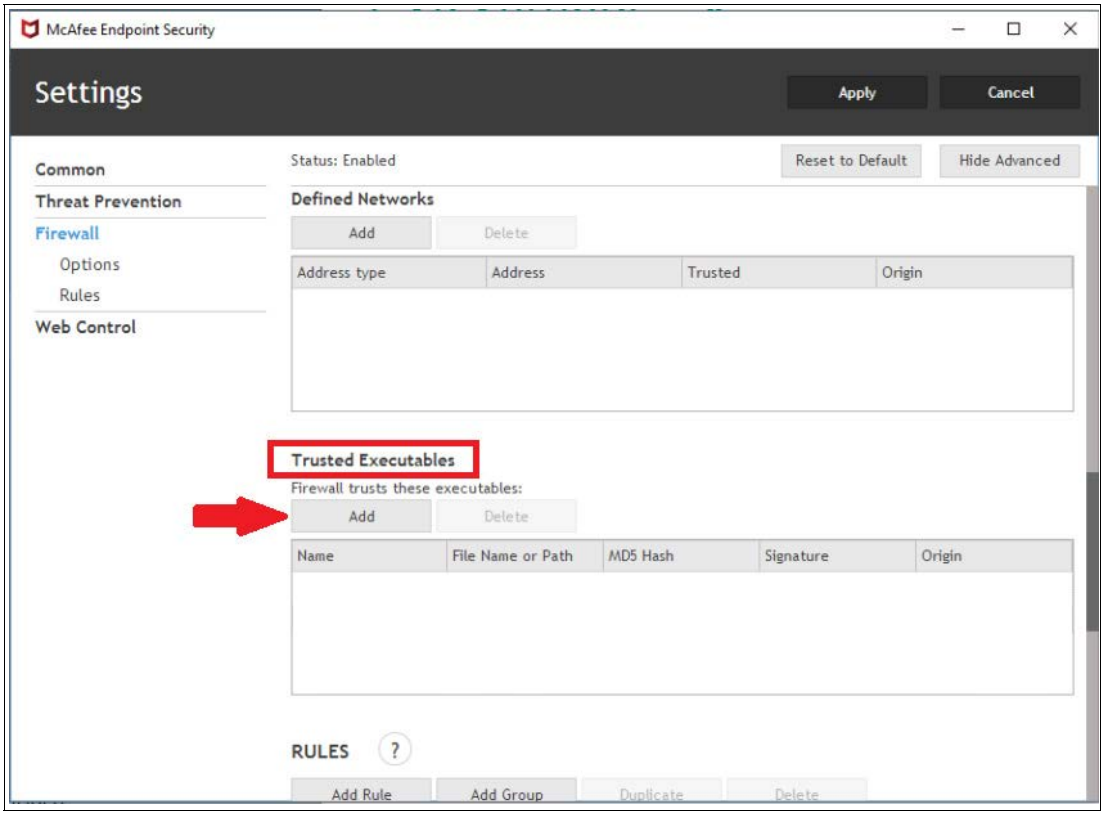
Schritt 7: Ändern der Firewall-Einstellungen

Wenn die Einrichtung abgeschlossen ist, müssen Sie der Firewall zwei Ausnahmeregeln hinzufügen. Dadurch wird gewährleistet, dass RM Shell optimal funktioniert.

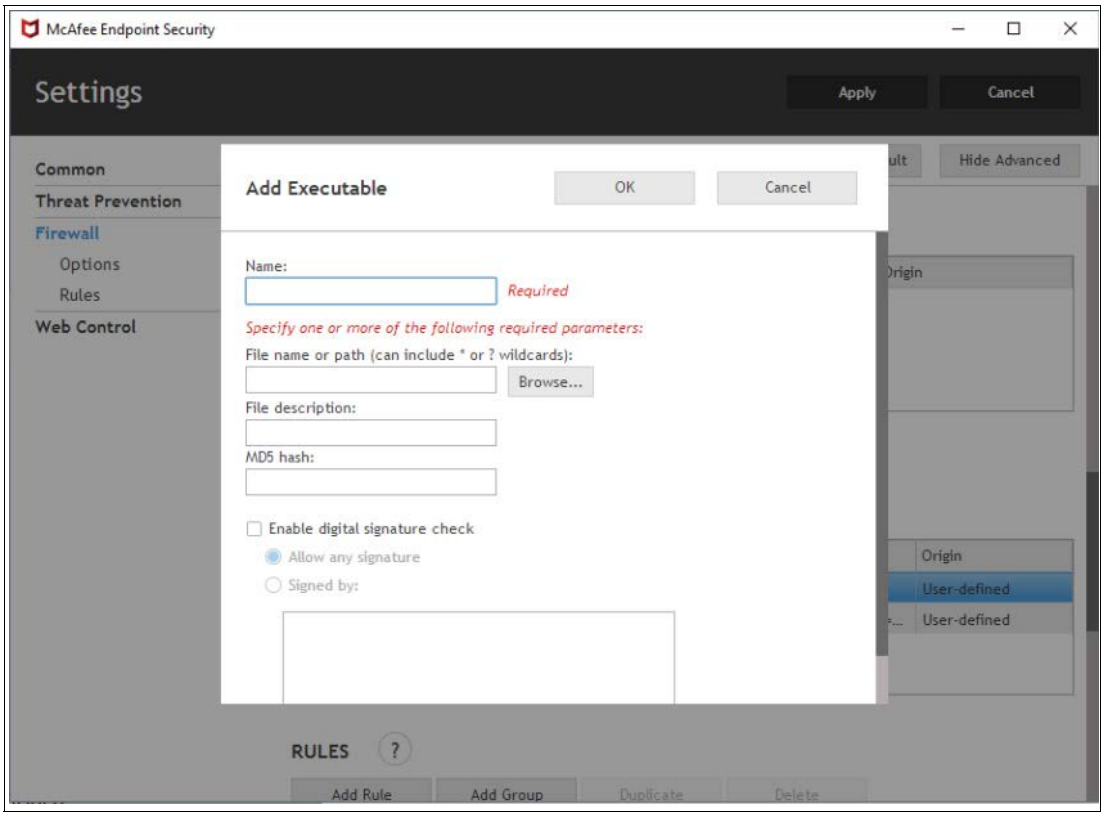
1. Öffnen Sie die Firewall-Einstellungen im McAfee-Programm und klicken Sie auf "Show Advanced“ (Erweiterte Funktionen anzeigen).



2. Blättern Sie nach unten, bis Sie "Trusted Executables“ (Vertrauenswürdige ausführbare Dateien) finden. Klicken Sie auf "Hinzufügen“ (Add).



↳ Das Menü "Add Executable“ (Ausführbare Datei hinzufügen) wird geöffnet.



3. Wählen Sie einen Namen für die Ausnahme aus.

2024-01

PEPPERL+FUCHS

4. Fügen Sie unter "File name or path“ (Dateiname oder Pfad) **tvnserver.exe** und **RMShell.exe** hinzu.
5. Diese Dateien finden Sie normalerweise unter:
   - C:\Programme\Pepperl+Fuchs\RMShell\RMShell.exe
   - C:\Programme\Pepperl+Fuchs\RMShell\Plugins\RMShell.DesktopSharing\Server\tvnserver.exe
6. Sie können auch zu diesen Dateien navigieren und sie über "Browse“ (Durchsuchen) hinzufügen.
7. Nachdem Sie die erforderlichen Parameter im Menü eingegeben haben, klicken Sie auf "Apply“ (Übernehmen).

11.6 Koppeln eines Bluetooth®-Gerätes

Die folgenden Anweisungen zeigen, wie ein Bluetooth®-Gerät in RM Shell gekoppelt wird. Als Beispiel dient ein Scanner ECOM Ident-Ex® 01. Weitere Informationen zu diesem Produkt finden Sie unter: https://www.ecom-ex.com/products/mobile-computing/reader-scanner-imager/ident-ex-01/

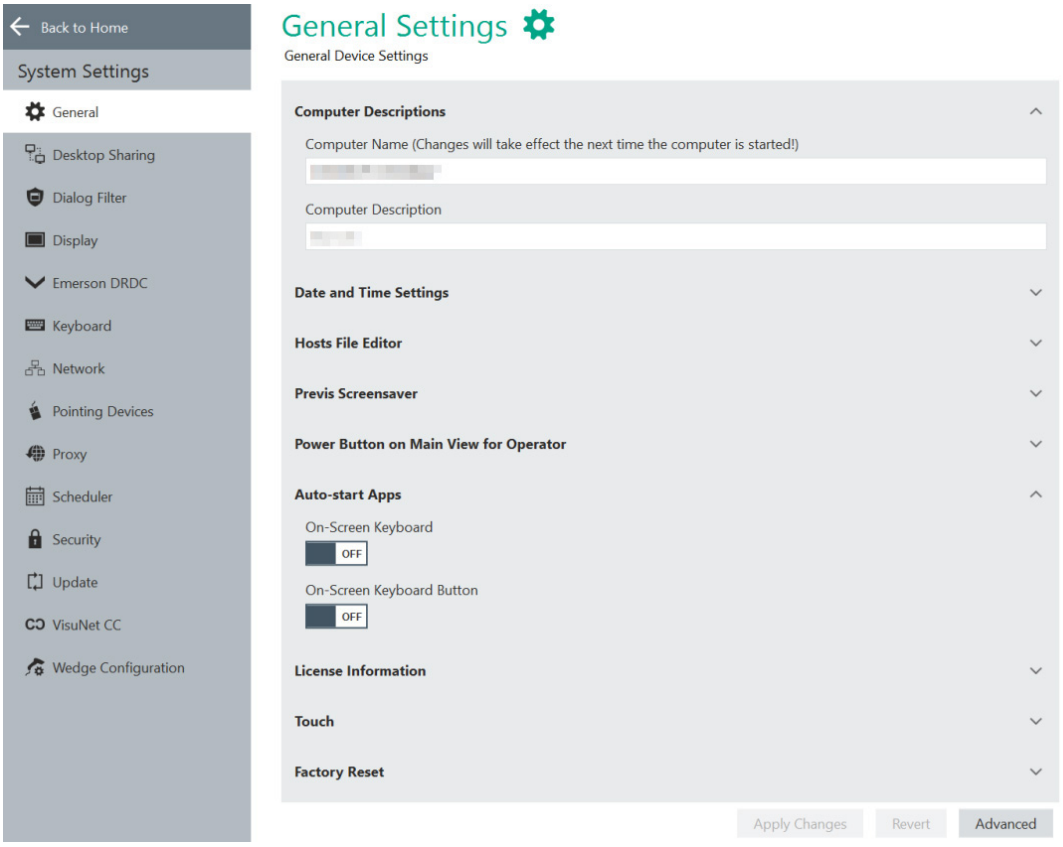
Hinweis!

Melden Sie sich als Administrator an

Sie müssen als Administrator angemeldet sein, damit Sie die folgenden Schritte ausführen können.

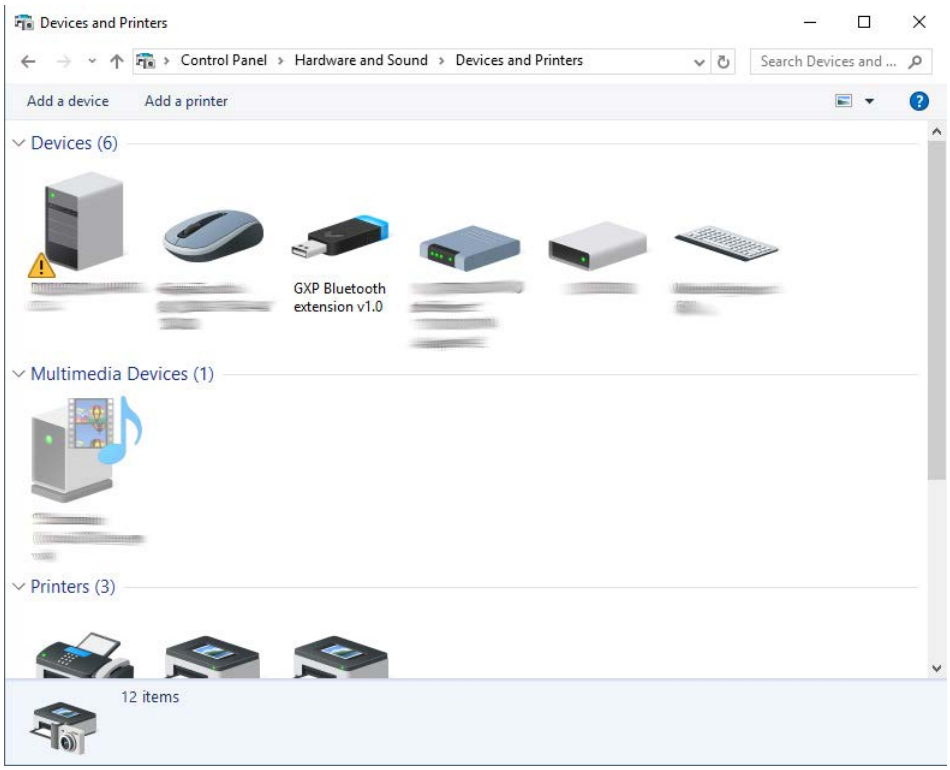
Koppeln eines Scanners ECOM Ident-Ex 01®

1. Schließen Sie einen Bluetooth-Dongle an die TCU/PCU an.
2. Navigieren Sie in der App "System Settings“ (Systemeinstellungen) zur Registerkarte "General“ (Allgemein).
3. Klicken Sie unten rechts auf dem Bildschirm auf die Schaltfläche "Advanced“ (Erweitert).

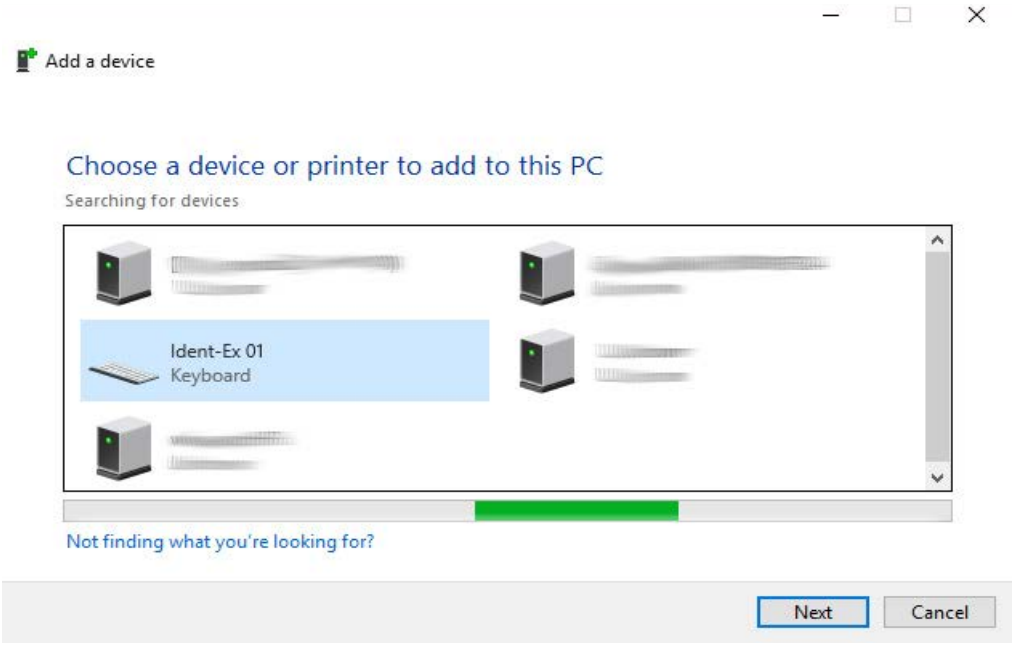


↳ Das Bedienfeld wird geöffnet.

4. Navigieren Sie zu "Hardware and Sound“ (Hardware und Sound) und anschließend zu "Devices and Printers“ (Geräte und Drucker).
5. Wählen Sie im Fenster "Drivers and Printers“ (Treiber und Drucker) die Option "Add a device“ (Gerät hinzufügen) aus.



6. Schalten Sie den Ident-Ex 01 ein. Nach einigen Sekunden wird der Scanner Ident-Ex 01 als Tastaturgerät angezeigt.
7. Wählen Sie das Gerät aus, und klicken Sie auf "Next“ (Weiter).



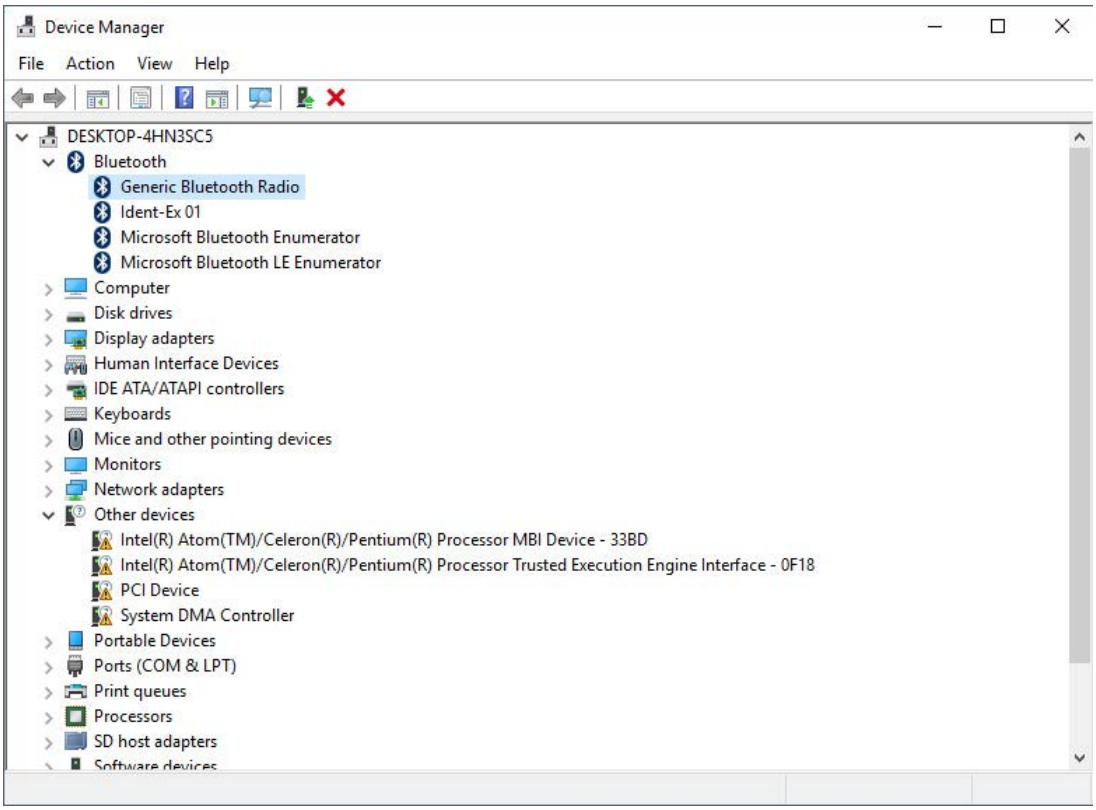
2024-01

PEPPERL+FUCHS

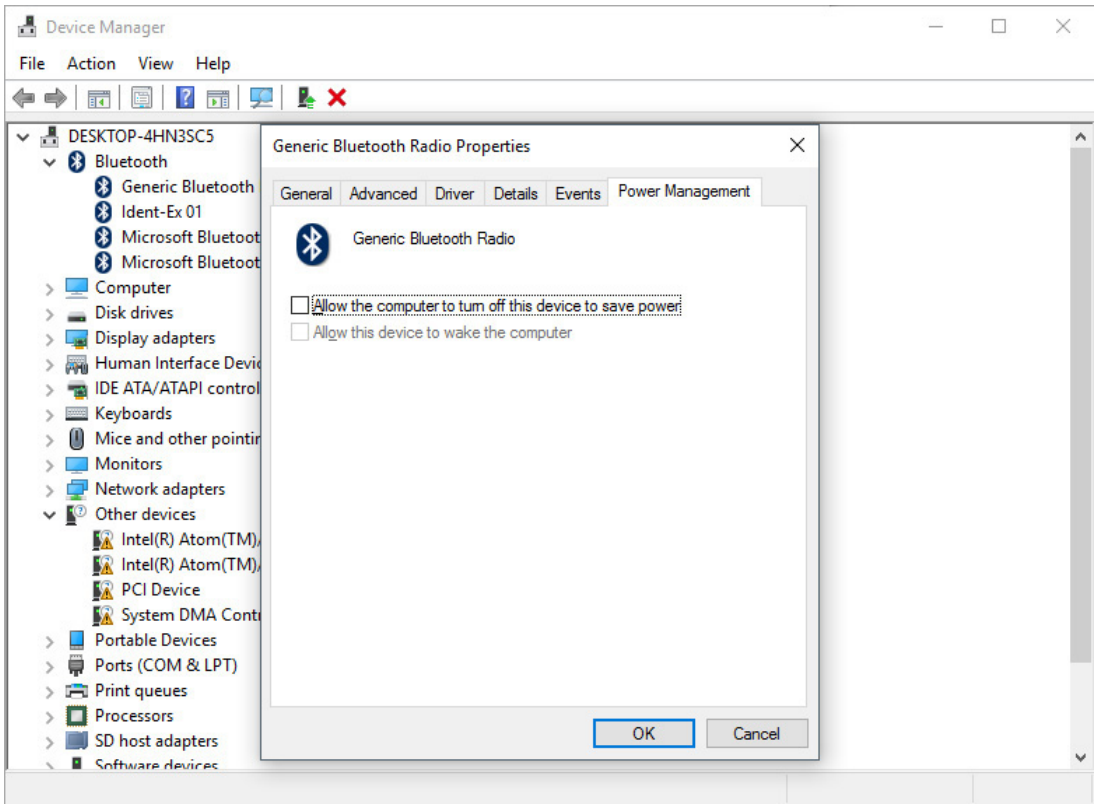
↳ Daraufhin wird das System mit dem Ident-Ex 01 gekoppelt. Nachdem das Gerät erfolgreich gekoppelt wurde, leuchtet die blaue LED-Anzeige auf dem Ident-Ex 01 auf.

8. Navigieren Sie in der Systemsteuerung zum Bereich "Hardware and Sound“ (Hardware und Sound). Wählen Sie unter "Device Manager“ (Geräte und Drucker) "Devices and Printers“ (Geräte-Manager) aus.

9. Klicken Sie mit der rechten Maustaste im Abschnitt "Bluetooth“ auf "Generic Bluetooth Radio“ (Generisches Bluetooth Radio).



10. Navigieren Sie zur Registerkarte "Power Management“ (Energieverwaltung) und deaktivieren Sie die Option "Allow the computer to turn off this device to save power“ (Computer kann das Gerät ausschalten, um Energie zu sparen).



↳ Das Gerät ist nun betriebsbereit.

Hinweis!

Wiederherstellen der Verbindung nach Neustart

Wenn die Verbindung zum Ident-Ex 01 nach einem Systemneustart oder nach dem Aus-/Einschalten des Scanners nicht automatisch wiederhergestellt wird, drücken Sie die SPP-Taste am Ident-Ex 01, bis die blaue Anzeige-LED wieder aufleuchtet.

11.7 Importieren von Hostzertifikaten

Importieren von Zertifikaten für RDP-Verbindungen

1. Passen Sie die Gruppenrichtlinieneinstellung des Hosts an.
2. Öffnen Sie "gpedit.msc“ (serverseitig), navigieren Sie zu (1) und deaktivieren Sie (2).

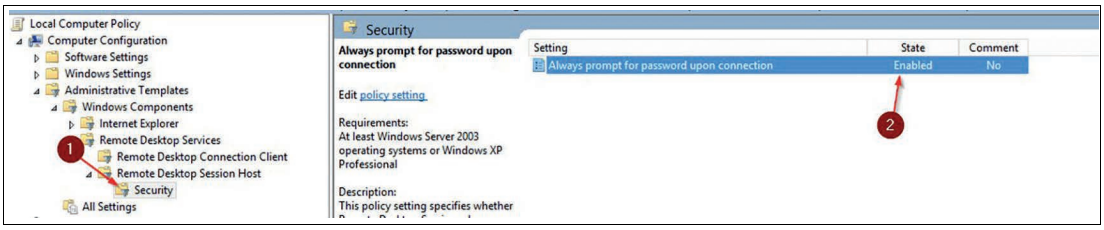


Abbildung 11.3

3. Importieren Sie Ihr Zertifikat.
4. Klicken Sie auf "View certificate“ (Zertifikat anzeigen) (1).

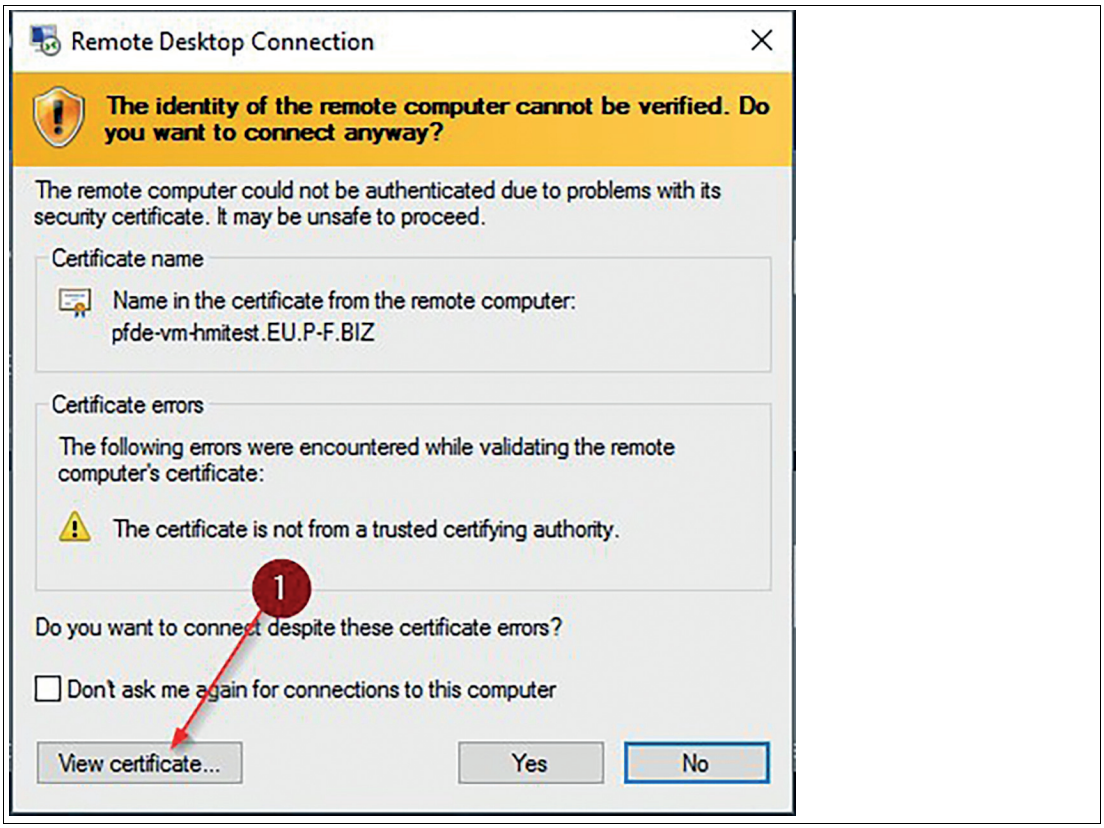


Abbildung 11.4

5. Klicken Sie auf "Install certificate“ (Zertifikat installieren) (2).

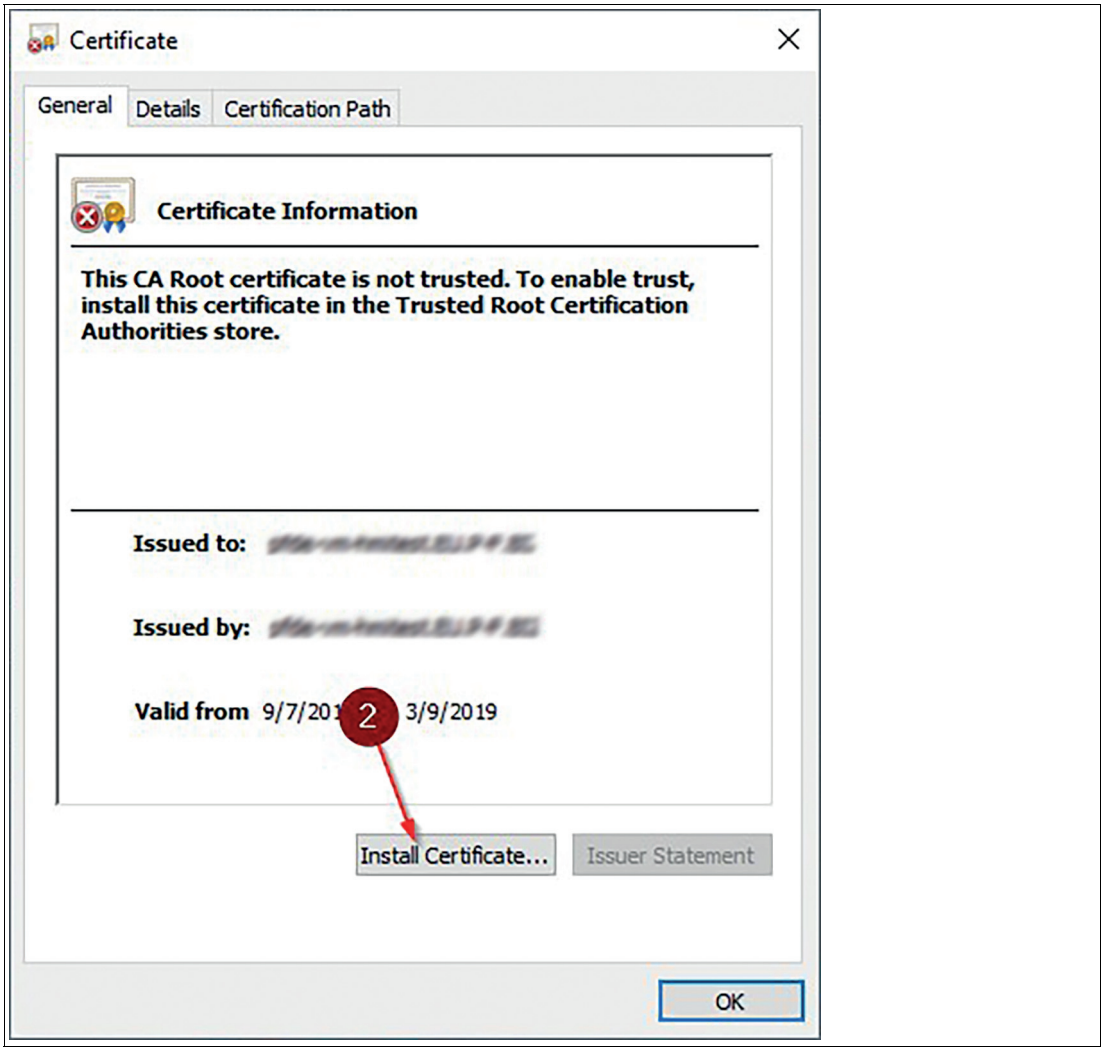


Abbildung 11.5

6. Befolgen Sie die Schritte des Assistenten für den Zertifikatimport
7. Wählen Sie "Local Machine“ (Lokaler Computer) (3) aus und klicken Sie auf "Next“ (Weiter) (4).

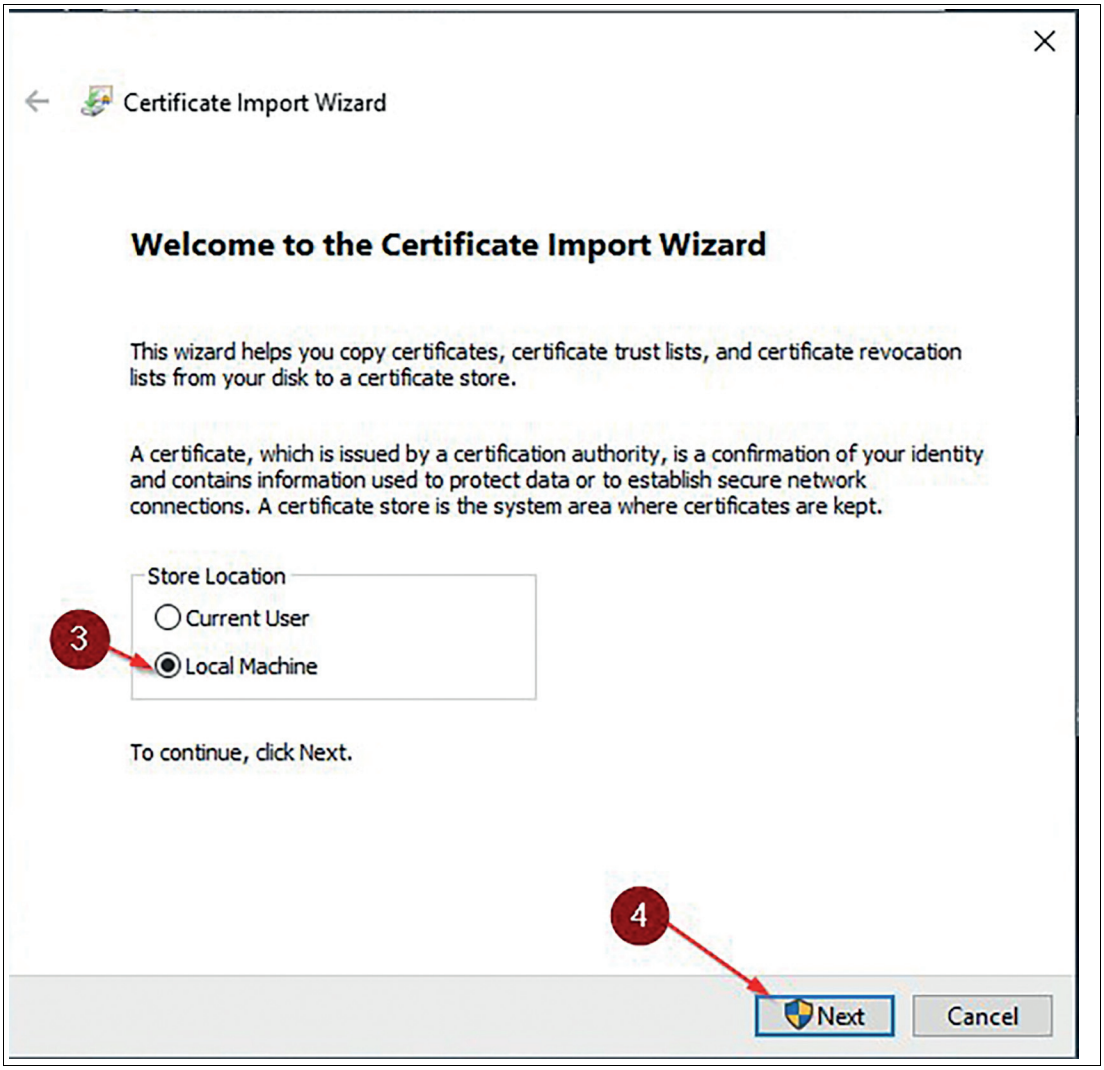


Abbildung 11.6

8. Wählen Sie Ihr eigenes Geschäft (5), (6), (7), (8) aus und klicken Sie auf "Next“ (Weiter) (9).

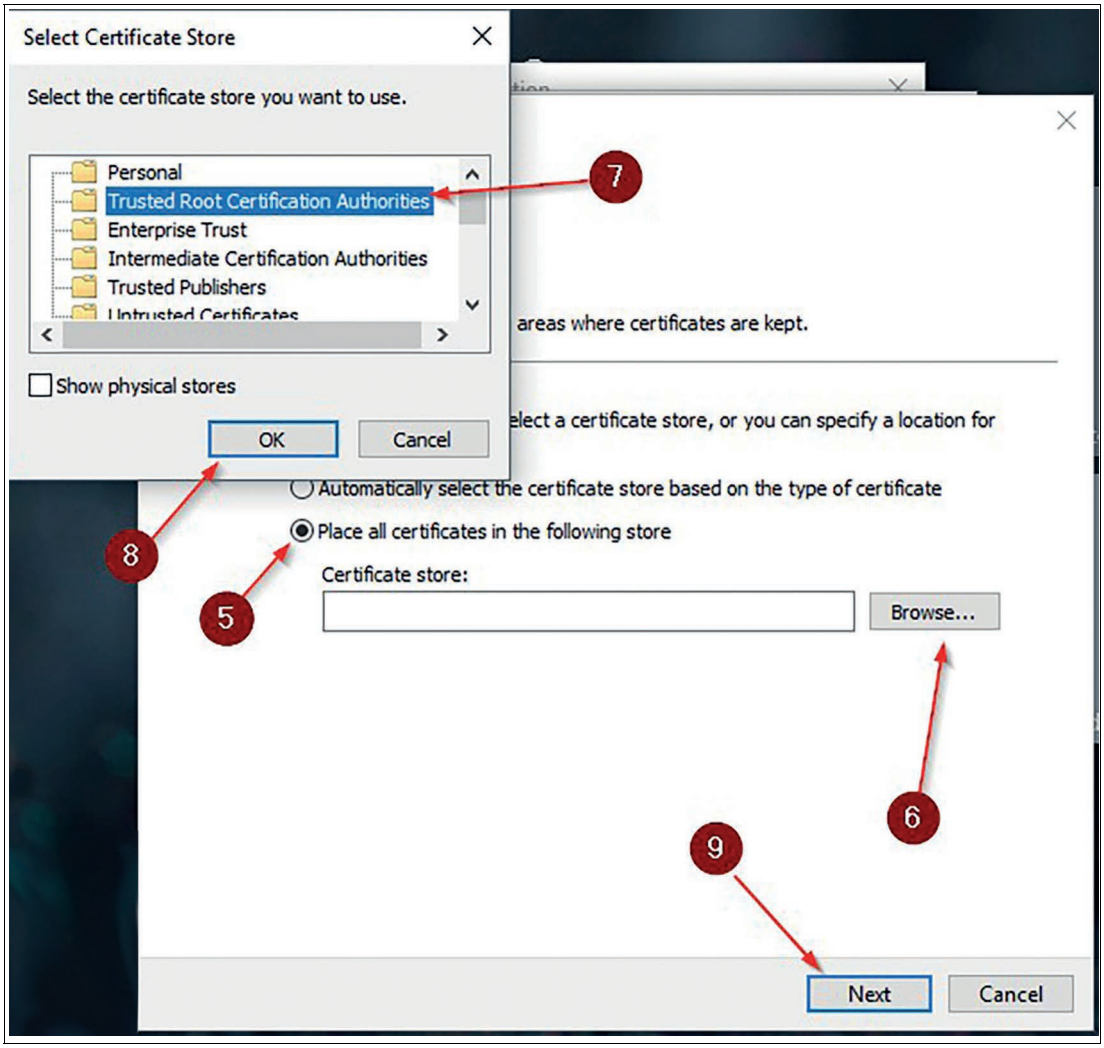


Abbildung 11.7

9. Nachdem Sie auf "Finish“ (Fertig stellen) geklickt haben, wird das Zertifikat importiert. Es sollte keine Zertifikatmeldung mehr angezeigt werden.

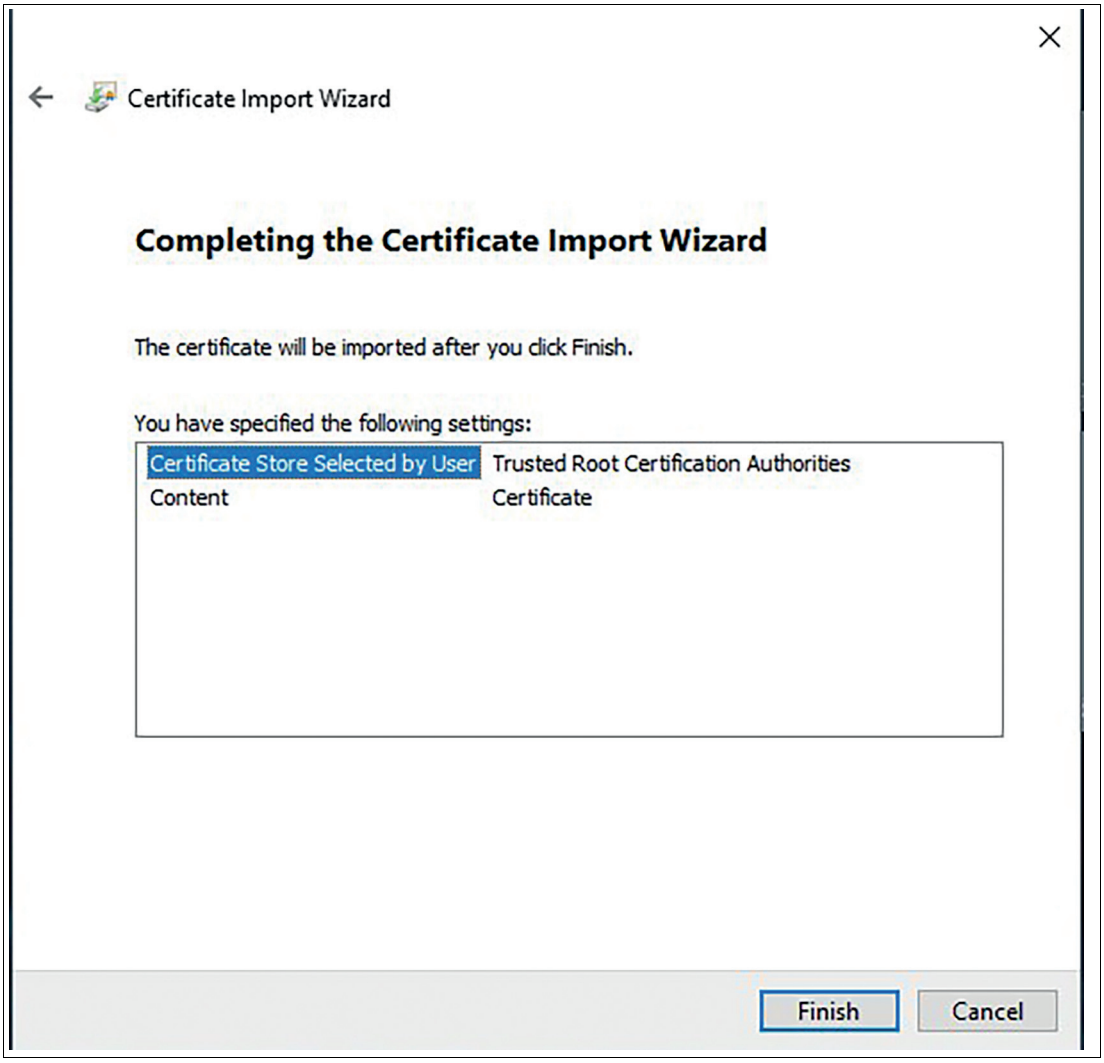


Abbildung 11.8

Integration einer Domäne

1. Melden Sie sich als Administrator an, öffnen Sie die Seite System Settings/Security (Systemeinstellungen/Sicherheit) und ändern Sie das Kennwort für "Local Windows User“ (Lokaler Windows-Benutzer).
2. Deaktivieren Sie "Keyboard Filter and block Ctrl+Alt+Del“ (Tastaturfilter und Strg+Alt+Entf sperren).
3. Wenden Sie die Einstellungen der Seite "Security“ (Sicherheit) an.
4. Klicken Sie auf System Settings (Systemeinstellungen)
5. Navigieren Sie zur Registerkarte General (Allgemein)
6. Erweitern Sie die erweiterten Windows-Einstellungen
7. Folgen Sie dem Pfad Control Panel > System and Security > System (Systemsteuerung > System und Sicherheit > System)
8. Klicken Sie auf "Change Settings“ (Einstellungen ändern)

Hinweis!

Wenn Sie "Change Settings“ (Einstellungen ändern) nicht öffnen können, deaktivieren Sie in "Local Group Policy Editor“ (Lokaler Gruppenrichtlinieneditor) die Option "Remove Properties from Computer icon context menu“ (Eigenschaften aus Kontextmenü für Computersymbole entfernen). Um den Local Group Policy Editor (Lokaler Gruppenrichtlinieneditor) zu öffnen, suchen Sie nach "gpedit.mcs“.

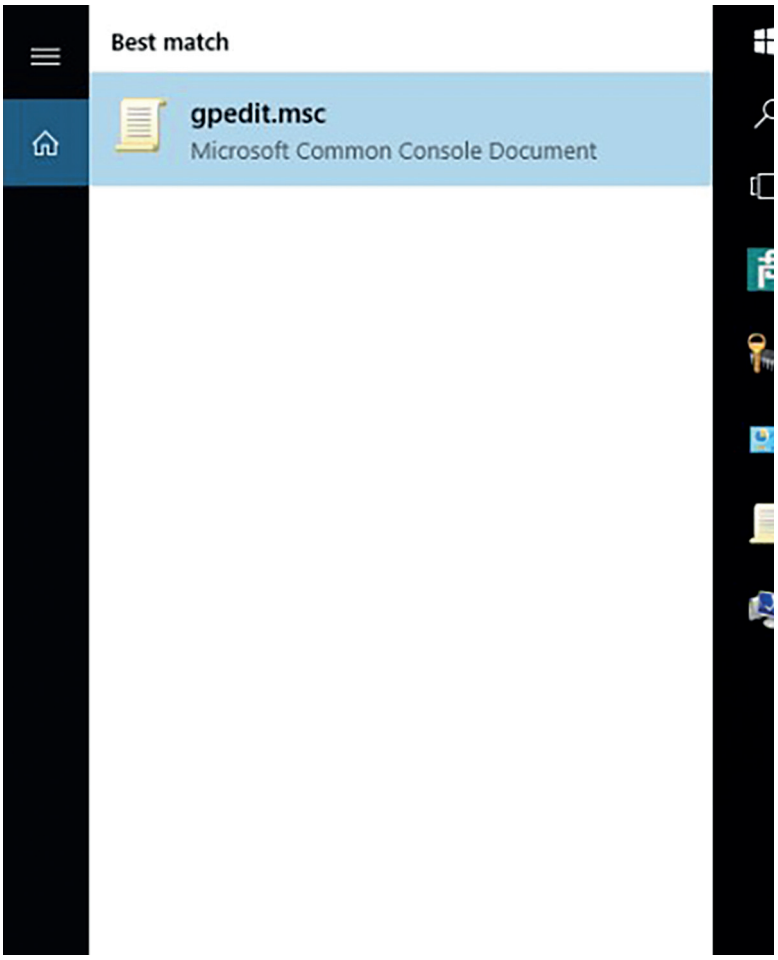


Abbildung 11.9

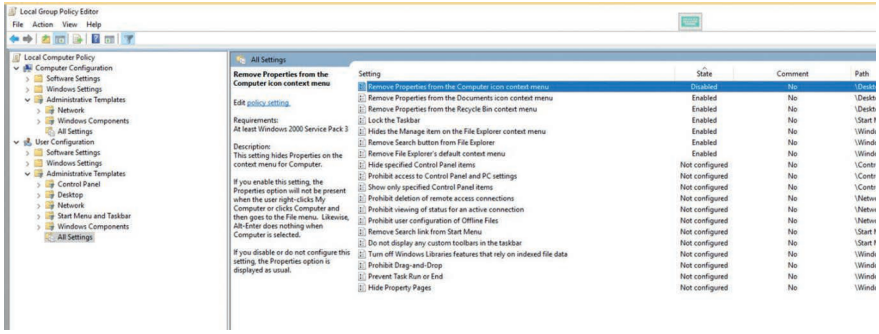


Abbildung 11.10

2024-01

PEPPERL+FUCHS

9. Verwenden Sie den folgenden Pfad: Local Computer Policy/User Configuration/Administrative Templates/Desktop/Remove Properties from the Computer icon context menu (Lokale Computerrichtlinie/Benutzerkonfiguration/Administrative Vorlagen/Desktop/Eigenschaften aus Kontextmenü für Computersymbole entfernen)
10. Wählen Sie Domäne aus und geben Sie den Domänennamen ein. Ein Berechtigungsfenster wird geöffnet. Geben Sie die Berechtigungsnachweise eines Domänenadministrators ein.

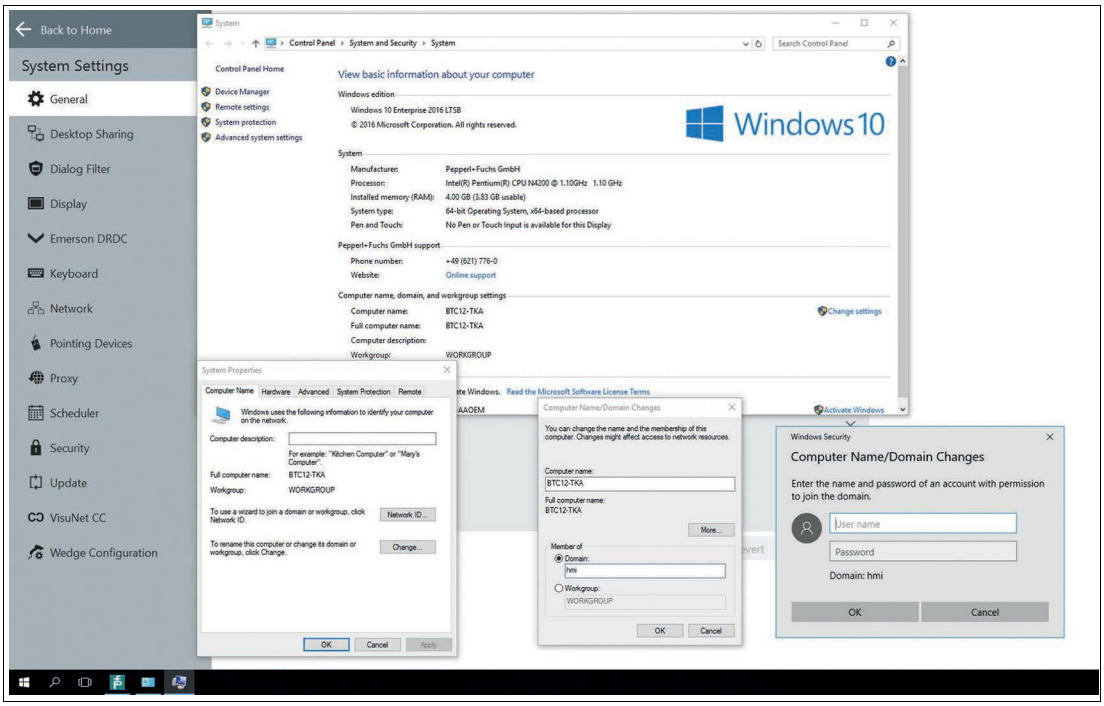


Abbildung 11.11

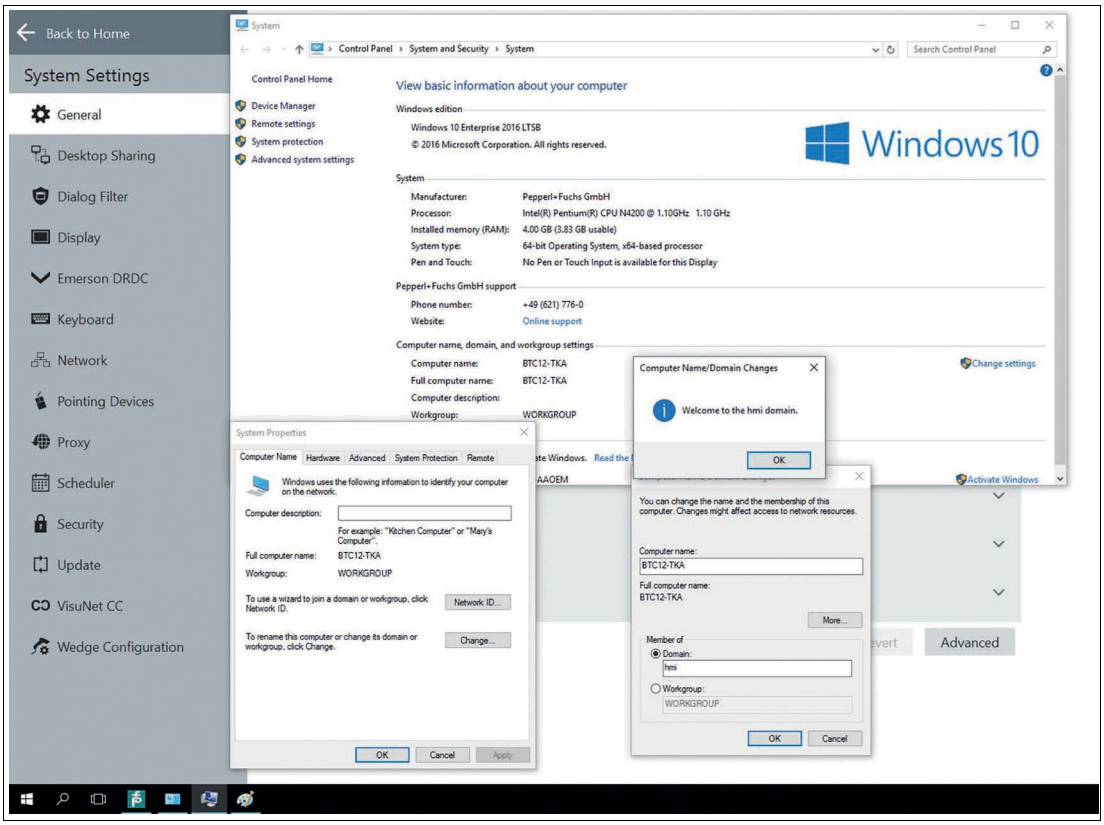


Abbildung 11.12

11. Starten Sie das Gerät neu
12. Nach dem Neustart müssen Sie die Berechtigungsnachweise für PFUser eingeben. Das Kennwort lautet VisuNetRMShell5. Bitte beachten Sie, dass Sie das lokale Konto verwenden müssen. Der Benutzer sollte wie folgt aussehen: .\PFUser
13. Fügen Sie der lokalen Administratorgruppe einen Domänenbenutzer hinzu. Öffnen Sie dazu lusrmgr.msc
14. Wechseln Sie zu Groups (Gruppen), klicken Sie mit der rechten Maustaste auf Administrators (Administratoren) und drücken Sie auf "Add to Group…“ (Zur Gruppe hinzufügen...).

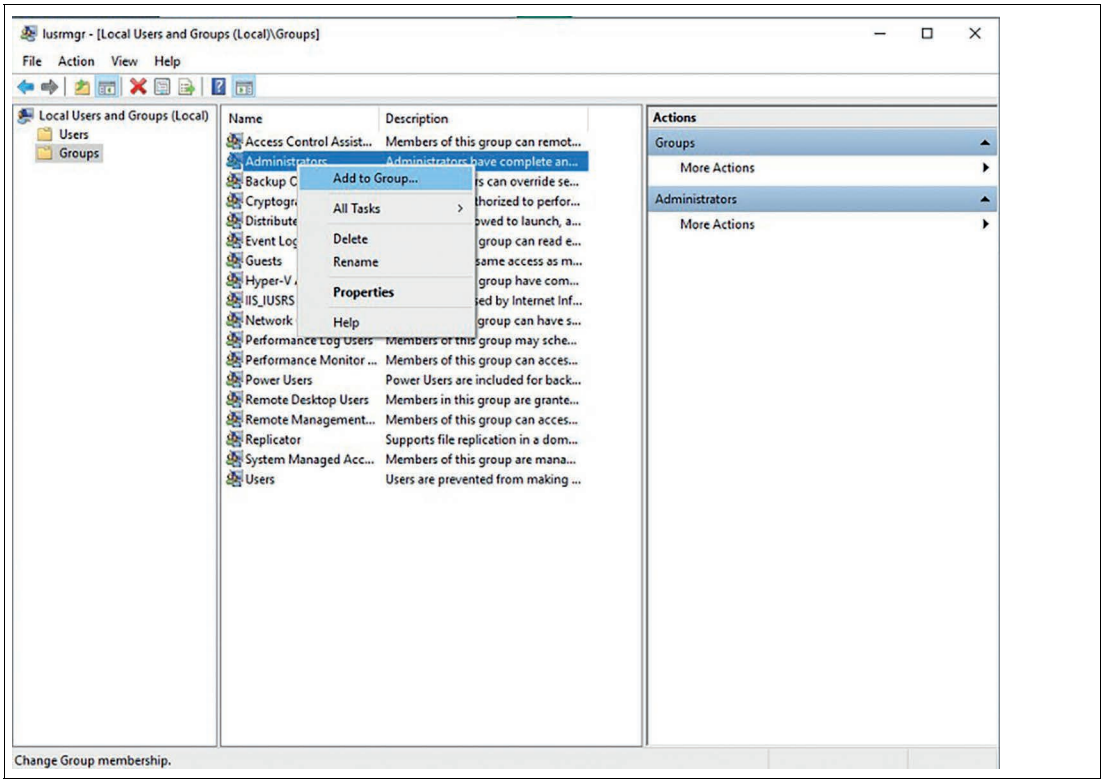


Abbildung 11.13

15. Geben Sie den Benutzernamen mit dem Domänenpräfix ein und klicken Sie auf "Check Names“ (Namen überprüfen), um den Namen zu überprüfen. Klicken Sie auf OK, um das Fenster zu schließen und die Einstellungen zu speichern.

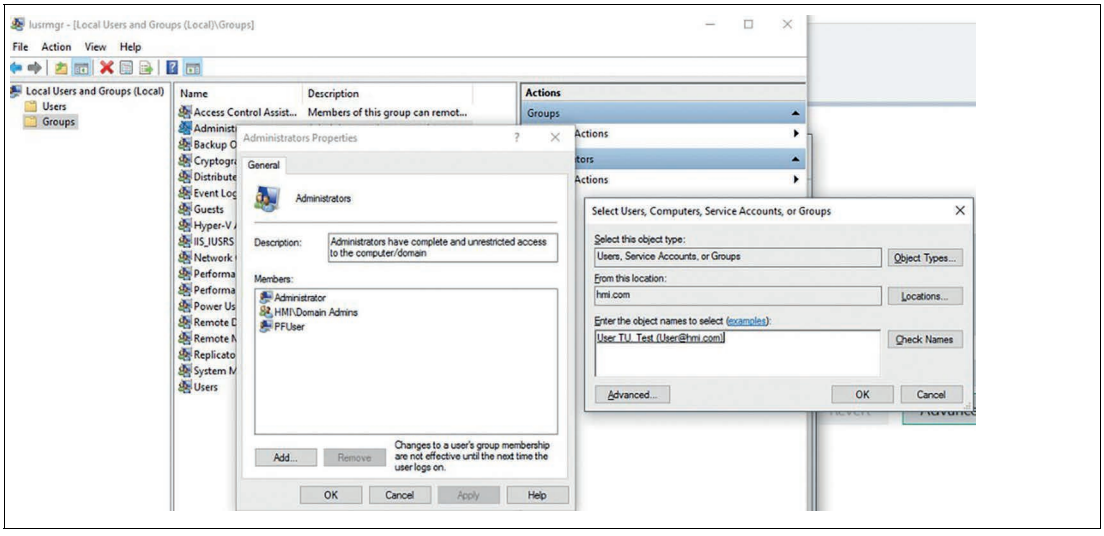


Abbildung 11.14

2024-01

16. Nun können Sie den Benutzer wechseln. In RM Shell können Sie "Strg+Alt+Entf“ für die schnelle Abmeldung aktivieren oder die Taskleiste für die normale Abmeldung verwenden.

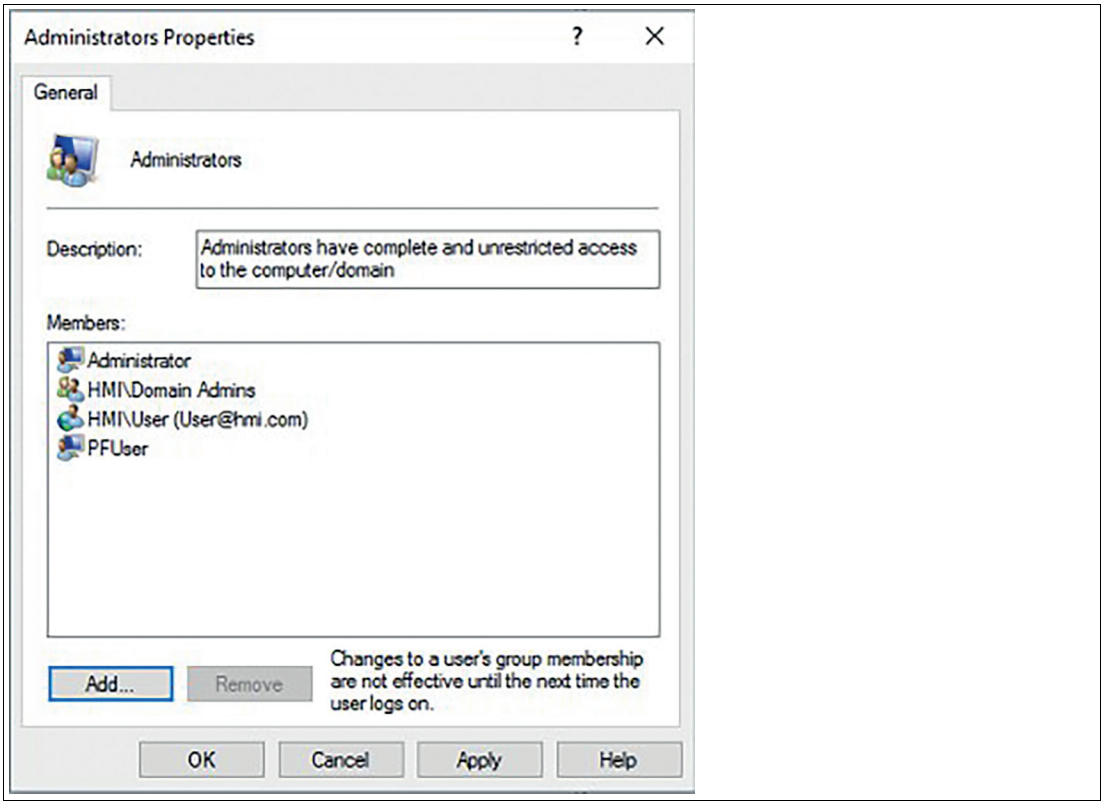


Abbildung 11.15

Hinweis!

Autologin (Automatische Anmeldung) wird standardmäßig deaktiviert. Es wird empfohlen, die Standardeinstellungen nicht zu ändern. Wenn Ihre Anwendung eine automatische Anmeldung erfordert, finden Sie weitere Informationen unter: https://support.microsoft.com/de-de/help/324737/how-to-turn-on-automatic-logon-in-windows.

11.8 TLS 1.0 aktivieren (für Raritan DKX2-101 oder ältere Webserver)

1. Öffnen Sie die Systemeinstellungen in der Administratorrolle.
2. Öffnen Sie den Gruppenrichtlinieneditor "gpedit.msc“.

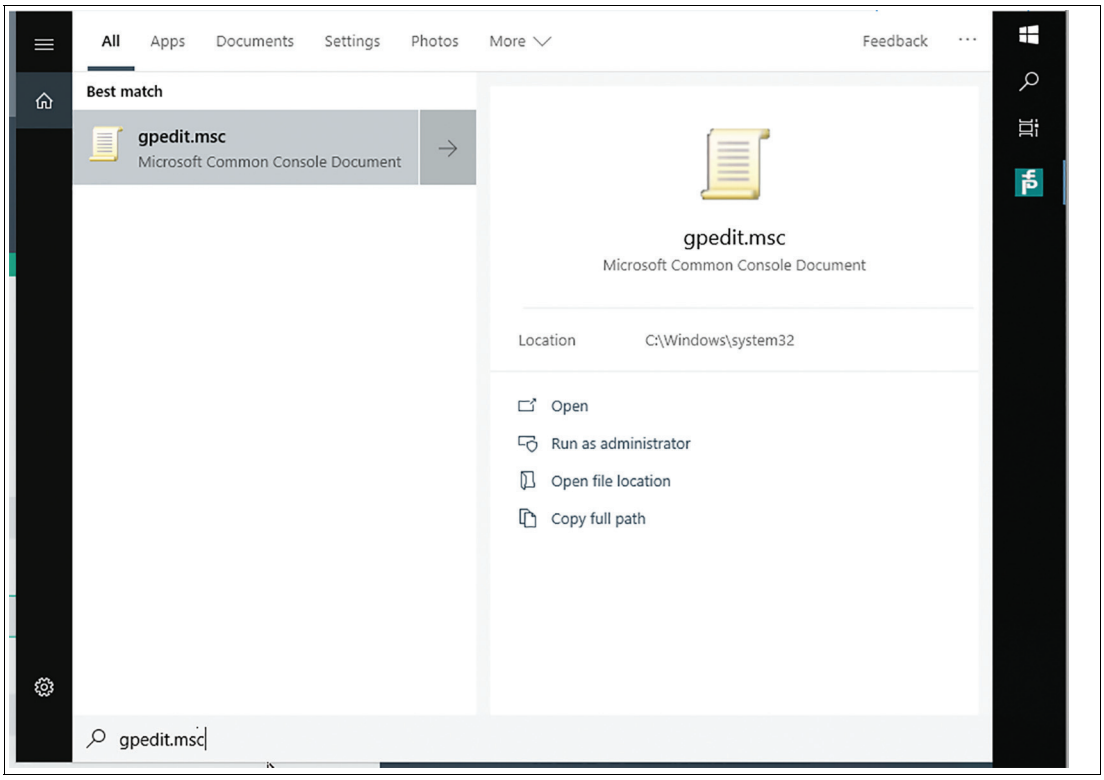


Abbildung 11.16

3. Navigieren Sie zu: Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> Turn off encryption support (Computerkonfiguration -> Verwaltungsvorlagen -> Windows-Komponenten -> Internet Explorer -> Internet-Systemsteuerung -> Erweitert -> Unterstützung für Verschlüsselung deaktivieren)
4. Wählen Sie "Turn off encryption support“ (Unterstützung für Verschlüsselung deaktivieren) und doppelklicken Sie, um das Dialogfeld zu öffnen.

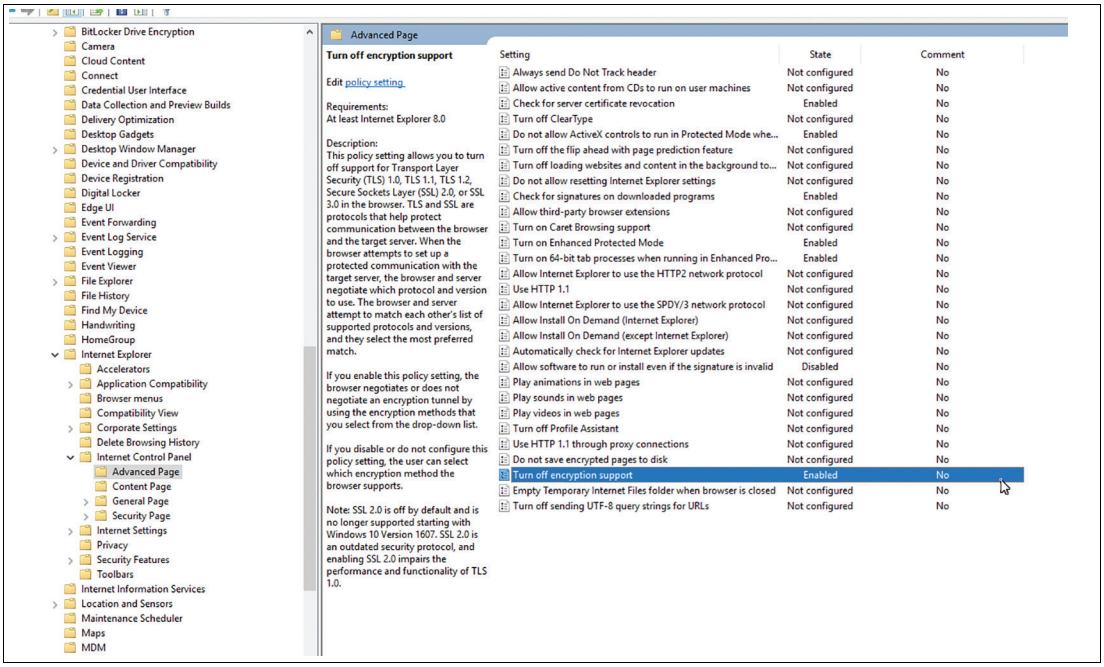


Abbildung 11.17

5. Wählen Sie TLS 1.0, TLS 1.1 und TLS 2.0.

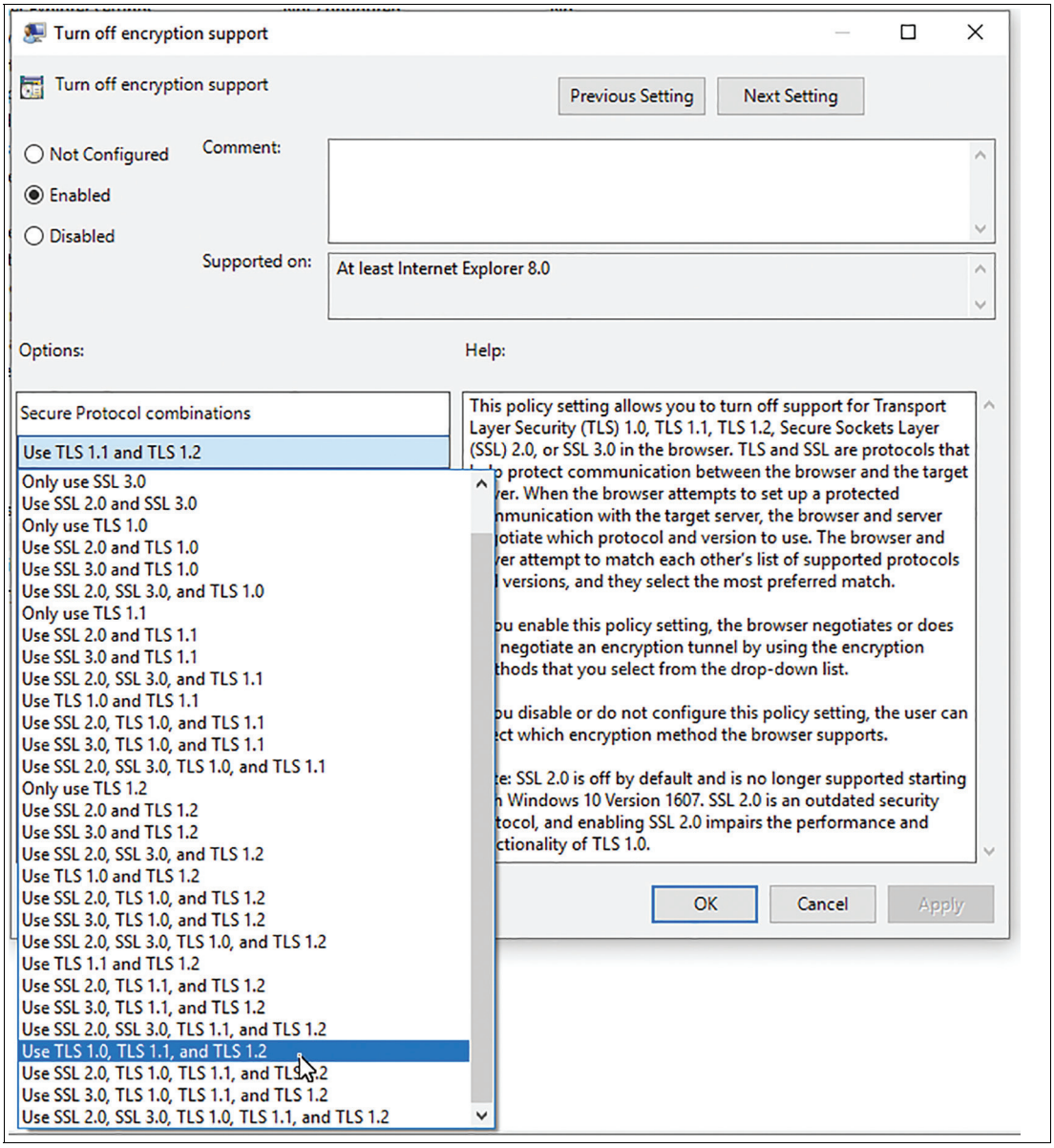


Abbildung 11.18

6. Schließen Sie das Fenster mit "OK“.
7. Starten Sie Shell neu.

11.9 VLAN-Tagging

Qualifiziert für die folgenden Geräte:

- BTC12
- BTC14
- VisuNet FLX
- VisuNet GXP (Generation 2020 mit Apollo Lake Prozessor)

Hinweis!

Installieren Sie bei Bedarf das Treiber-Update für die folgenden Geräte: BTC12, VisuNet FLX, VisuNet GXP (Generation 2020 mit Apollo Lake Prozessor) (Schritt 4 schlägt fehl). Die einzelnen Treiber-Updates sind online auf den Produktseiten der Geräte verfügbar.

Vorgehensweise

1. Melden Sie sich als Administrator an
2. Öffnen Sie System Settings (Systemeinstellungen)
3. Suchen Sie in der Windows®-Taskleiste nach "Windows PowerShell“ und öffnen Sie sie.

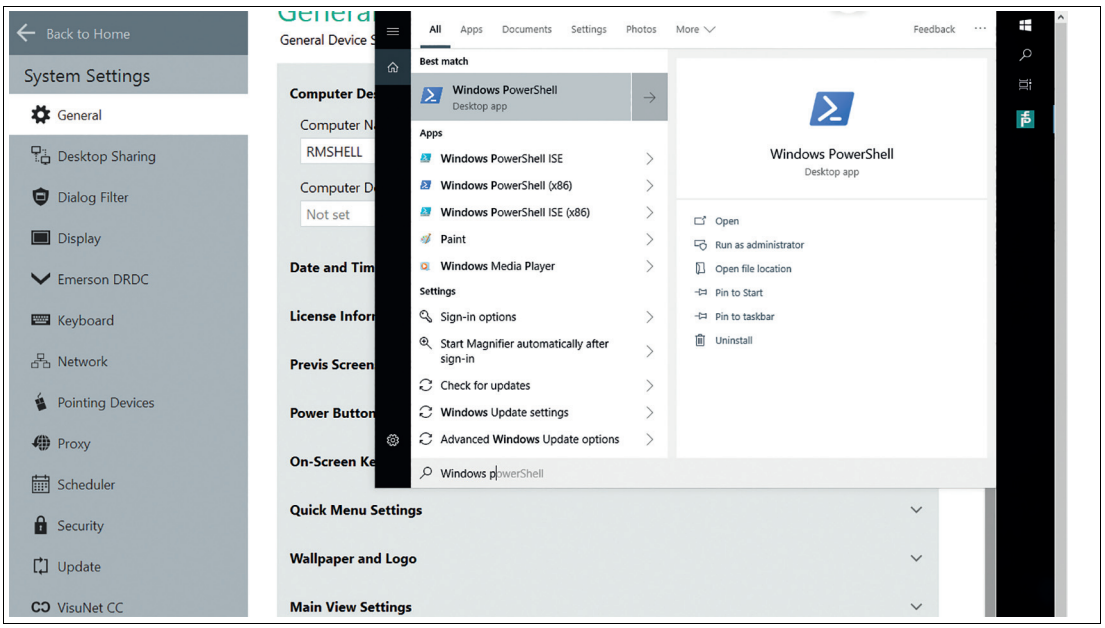


Abbildung 11.19

4. Laden Sie das erforderliche PowerShell-Modul mit: "Import-Module -Name 'C:\Program Files\Intel\Wired Networking\IntelNetCmdlets\IntelNetCmdlets'“.
5. Wenn dieser Schritt fehlschlägt, installieren Sie das online verfügbare Treiberpaket Ihres Geräts.
6. Sie können alle verfügbaren Netzwerkadapter auflisten mit: "Get-IntelNetAdapter“. Suchen Sie nach dem Netzwerkadapternamen, der das VLAN- Tag haben sollte.

Hinweis!

In der Regel haben die entsprechenden Ethernet-Adapter den Namen Ethernet oder Ethernet 2.

7. Jetzt können Sie folgenden Befehl ausführen: "Add-IntelNetVLAN -ParentName "<device name>" -VLANID "<vlanid>"“. Geben Sie für <Gerätename> den Netzwerkadapternamen des vorherigen Schritts und für <VLAN-ID> die gewünschte VLAN-ID ein.
8. **VLAN-Tag entfernen:**
9. Remove-IntelNetVLAN -ParentName "<Gerätename>" -VLANID "<VLAN-ID>"

11.10 NIC-Gruppierung

NIC-Gruppierung über Windows®-Implementierung:

Diese Option ist mit den NICs verschiedener Hersteller kompatibel, und für Geräte von Pepperl+Fuchs sind keine Treiber-Updates erforderlich, es gibt jedoch im Vergleich zu Intel-CMD-lets weniger Konfigurationsoptionen.

Diese Option wurde für alle Geräte von Pepperl+Fuchs auf Basis von Windows® 10 IoT 2019 LTSC mit mehreren Netzwerkadaptern einschließlich VisuNet GXP getestet (2020 Generation mit Apollo Lake Prozessor).

Vorgehensweise

1. Melden Sie sich als Administrator an
2. Öffnen Sie System Settings (Systemeinstellungen)
3. Suchen Sie in der Windows®-Taskleiste nach "Windows PowerShell“ und öffnen Sie sie.
4. Führen Sie den Befehl "Get-NetAdapter“ aus, um die Namen der Netzwerkadapter abzurufen.

   Hinweis!

   In der Regel haben die entsprechenden Ethernet-Adapter den Namen Ethernet oder Ethernet 2.

5. Führen Sie "New-NetSwitchTeam -Name "<Gruppenname>" -TeamMembers "<Netzwerkadaptername 1>", "<Netzwerkadaptername 2>"“ aus
6. Geben Sie für <Gruppenname> den Namen der Gruppe ein, die Sie konfigurieren möchten, und für <Netzwerkadaptername 1> und <Netzwerkadaptername 2> die Namen der Netzwerkadapter, die in Schritt 4 angezeigt wurden.
7. Nun sollte ein neuer Netzwerkadapter angezeigt werden, der konfiguriert werden kann.

Gruppierung entfernen:

Führen Sie "Remove- NetSwitchTeam -Name "<Gruppenname>"“ aus

NIC-Gruppierung über Intel CMDlets:

Für diese Option sind mehrere Gruppenmodi verfügbar, die aber für Intel NICs gelten.

Diese Option wurde für die folgenden Geräte von Pepperl+Fuchs getestet: BTC12, BTC14, VisuNet FLX.

Hinweis!

Installieren Sie das Treiber-Update für die folgenden Geräte BTC12 und VisuNet FLX. Die einzelnen Treiber-Updates sind online auf den Produktseiten der Geräte verfügbar. Für den BTC14 ist kein Treiber-Update erforderlich.

Vorgehensweise

1. Melden Sie sich als Administrator an
2. Öffnen Sie System Settings (Systemeinstellungen)
3. Suchen Sie in der Windows®-Taskleiste nach "Windows PowerShell“ und öffnen Sie sie.
4. Laden Sie das erforderliche PowerShell-Modul mit: "Import-Module -Name 'C:\Program Files\Intel\Wired Networking\IntelNetCmdlets\IntelNetCmdlets'“
5. Sie können alle verfügbaren Netzwerkadapter auflisten mit: "Get-IntelNetAdapter“. Suchen Sie nach den Namen der Netzwerkadapter, die Sie der Gruppe hinzufügen möchten.

   Hinweis!

   In der Regel haben die entsprechenden Ethernet-Adapter den Namen Ethernet oder Ethernet 2.

6. Führen Sie den folgenden Befehl aus, um eine neue Gruppe zu erstellen:
7. New-IntelNetTeam -TeamMemberNames "<Netzwerkadaptername 1>", "<Netzwerkadaptername 2>" -TeamMode AdapterFaultTolerance -TeamName "<Gruppenname>"
8. Geben Sie für <Netzwerkadaptername 1> und <Netzwerkadaptername 2> die Namen der Netzwerkadapter ein und für <Gruppenname> den Namen der Gruppe, die Sie erstellen möchten.
9. Es gibt weitere TeamModes (Gruppenmodi), die verwendet werden können. Siehe https://www.intel.de/content/www/de/de/support/articles/000032008/ethernet-products.html
10. Nun sollte ein neuer Netzwerkadapter angezeigt werden, der konfiguriert werden kann.

    Gruppierung entfernen:

    Führen Sie "Remove-IntelNetTeam -TeamName "<Gruppenname>"“ aus

12 Anhang

12.1 Offene Netzwerkports

Für die Kommunikation zwischen Control Center und RM Shell wird der TCP-Port 8023 verwendet.

Verwenden Sie zur Erkennung vorhandener RMs/BTCs (Scan) den UDP/TCP-Port 3702. https://en.wikipedia.org/wiki/WS-Discovery.

Für die NetBIOS-Auflösung ist kein DNS-Server vorhanden. Der UDP-Port 137 ist erforderlich. https://en.wikipedia.org/wiki/NetBIOS_over_TCP/IP

12.2 Shell friert auf dem RDP-Anmeldebildschirm ein

1. Navigieren Sie in "System Settings“ (Systemeinstellungen) zu "Touch“.

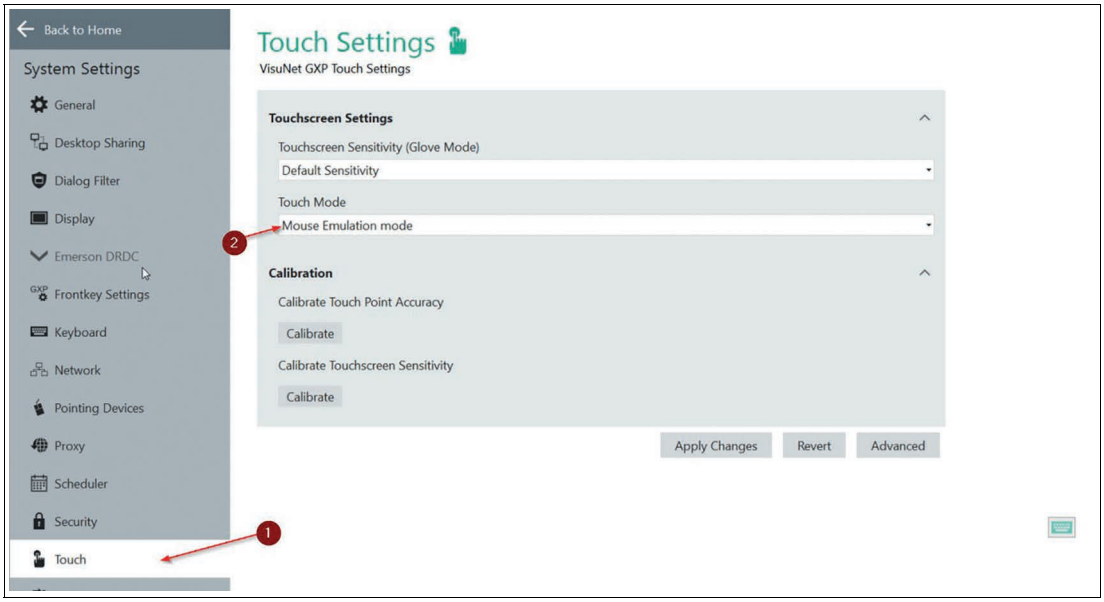


Abbildung 12.1

2. Wählen Sie unter "System Settings“ (Systemeinstellungen) auf der Registerkarte "Touch“ (1) die Option "Mouse Emulation mode“ (Mausemulationsmodus) (2) aus.

Hinweis!

Es wird empfohlen, das DRDC-Profil zu verwenden. Wenn Sie ein RDP-Profil verwenden, ist die Funktion "No Touch“ (Kein Touch) ein Windows-Fehler.

12.3 Pepperl+Fuchs SE Endbenutzer-Lizenzvereinbarung (End User License Agreement, EULA)

WICHTIGER HINWEIS – BITTE SORGFÄLTIG LESEN

DIESE ENDBENUTZER-LIZENZVEREINBARUNG IST EINE RECHTLICH BINDENDE VEREINBARUNG ZWISCHEN IHNEN ALS BESTIMMTEM BENUTZER ODER ALS VERTRETER IM NAMEN EINES UNTERNEHMENS ODER EINER ORGANISATION, IM FOLGENDEN "LIZENZNEHMER“ GENANNT, UND DER PEPPERL+FUCHS SE, MANNHEIM, DEUTSCHLAND, IM FOLGENDEN "LIZENZGEBER“ GENANNT.

LESEN SIE DIE GESAMTE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE WEITER VERWENDEN. DURCH DIE VERWENDUNG DER SOFTWARE BESTÄTIGT DER LIZENZNEHMER SEIN EINVERSTÄNDNIS UND STIMMT ZU, SICH AN DIE BEDINGUNGEN DIESER VEREINBARUNG ZU HALTEN.

FÜR DEN FALL, DASS SICH DER LIZENZNEHMER NICHT MIT DEN BEDINGUNGEN DIESER VEREINBARUNG EINVERSTANDEN ERKLÄRT, DARF DER LIZENZNEHMER DIE SOFTWARE NICHT VERWENDEN UND MUSS DAS GERÄT AUF EIGENE KOSTEN WIEDER AN DEN LIZENZGEBER ZURÜCKGEBEN.

1 - Definitionen

Lizenzgeber	Pepperl+Fuchs SE, Lilienthalstr. 200, 68307 Mannheim, Deutschland
Software	Bedeutet das bzw. die Softwareprogramm(e) des Lizenzgebers, einschließlich Microsoft-Software, die hiermit vom Lizenzgeber geliefert werden, und die dazugehörigen Informationen unter der Bezeichnung "VisuNet RM Shell 5“, die durch den Lizenzgeber mitgeliefert und bereits auf einem Gerät installiert wurden. Alle Updates für diese Software, für die der Lizenznehmer zum Erhalt berechtigt ist und die ihm vom Lizenzgeber zur Verfügung gestellt wurden, gelten für die Zwecke dieses Abkommens ebenfalls als Software.
Microsoft-Software	Bedeutet die MICROSOFT SOFTWARE LICENSE TERMS – WINDOWS 10, die den zusätzlichen Vertragsbedingungen unterliegen, wie auf dem Bildschirm "About“ (Info) von "VisuNet RM Shell 5“ beschrieben. Durch die Verwendung der Software ist der Lizenznehmer auch an die zusätzlichen Bedingungen der Microsoft-Software gebunden.
Gerät	Bedeutet alle Produkte des Lizenzgebers, auf denen die Software installiert ist.
Lizenz	Durch die Vergabe einer Lizenz gewährt der Lizenzgeber dem Lizenznehmer das Recht zur Nutzung der Software gemäß den Bedingungen in dieser EULA.

2 - Gegenstand der EULA

2.1 Der Lizenzgeber stellt die Software zur Verfügung, die den folgenden Geschäfts- und Nutzungsbedingungen für "VisuNet RM Shell 5“ unterliegt.

2.2 Ein Servicekontrakt für die Software ist nicht verfügbar.

3 - Gewährung der Lizenz

3.1 Nach Maßgabe der Bestimmungen und Bedingungen in dieser EULA gewährt der Lizenzgeber dem Lizenznehmer eine persönliche, nicht-exklusive und zeitlich nicht eingeschränkte Lizenz zur Nutzung der Software nach Maßgabe der folgenden Bestimmungen:

3.2 Der Lizenzgeber gewährt dem Lizenznehmer das Recht zur Verwendung der Software auf dem Gerät, auf dem sie an den Lizenznehmer geliefert wurde. Der Lizenznehmer darf die Software nur für diesen Nutzungszweck einsetzen.

3.3 Der Lizenznehmer ist berechtigt, eine Kopie der Software ausschließlich für Sicherungszwecke zu erstellen, vorausgesetzt, dass diese Kopie ganz klar mit allen Urheberrechtsvermerken und sonstigen Eigentumsvermerken in Bezug auf die ursprüngliche Kopie bezeichnet ist.

3.4 Der Lizenznehmer hat nur nach vorheriger schriftlicher Zustimmung des Lizenzgebers Anspruch auf Übertragung des Rechts zur Nutzung der Software auf einen Dritten, wenn die dritte Partei die Bedingungen dieser EULA akzeptiert und der Lizenznehmer keine Kopien der Software zurückbehält. Die Übertragung des Rechts zur Nutzung der Software darf nur zusammen mit dem Gerät erfolgen, auf dem die Software durch den Lizenzgeber installiert wurde.

4 - Lizenzbeschränkungen

4.1 Der Lizenznehmer ist in keiner Weise berechtigt, die Software oder Teile der Software zu ändern oder erweitern, und es dürfen keine Änderungen an der Software oder an von der Software abgeleiteten Produkte durchgeführt werden, außer nach vorheriger schriftlicher Zustimmung des Lizenzgebers.

4.2 Der Lizenznehmer ist in keiner Weise berechtigt, die Software oder Teile der Software, im Ganzen oder in Teilen zu dekompilieren, disassemblieren oder anderweitig rückzuentwickeln oder zu versuchen, auf den Quellcode der Software oder irgendwelche darin enthaltene Algorithmen, Konzepte, Techniken, Methoden oder Prozesse zuzugreifen oder diese abzuleiten.

4.3 Außer entsprechend den Bestimmungen in Abschnitt 3 ist der Lizenznehmer in keiner Weise berechtigt, Kopien der Software zu erstellen oder zu verbreiten, die Software zu vermieten, zu verleasen, zu verleihen oder eine Unterlizenzierung der Software durchzuführen oder die Software elektronisch von einem Gerät auf ein anderes oder über ein Netzwerk zu übertragen.

5 - Verletzung der Rechte Dritter

5.1 Für den Fall, dass ein wesentlicher Bestandteil der Software Gegenstand einer begründeten Klage Dritter wegen Copyright-, Patent- oder anderer Verstöße gegen Eigentumsrechte wird, wird der Lizenzgeber nach seiner Wahl entweder (i) die Software durch ein kompatibles, funktional gleichwertiges, keine Rechte verletzendes Software-Produkt ersetzen; (ii) die Software verändern oder eine andere Maßnahme ergreifen, sodass keine Rechte mehr verletzt werden; (iii) das Recht für den Lizenznehmer beschaffen, um die Software weiter zu nutzen; oder (iv), falls nach dem alleinigen Ermessen des Lizenzgebers keine der vorstehenden Alternativen billigerweise oder mit angemessenen Kosten und/oder Anstrengungen zur verfügbar ist, diese Lizenz beenden.

5.2 Die genannten Punkte stellen die gesamte Haftung des Lizenzgebers bezüglich der Ansprüche bei Urheberrechts- oder Patentverletzungen dar; des Weiteren, sofern in diesem Abschnitt nicht genannt, übernimmt der Lizenzgeber keine weitere Haftung gegenüber dem Lizenznehmer für irgendeinen Verlust oder Schaden oder eine Eigentumsrechtsverletzung gegen den Lizenznehmer durch Dritte, die sich aus oder im Zusammenhang mit einer etwaigen Behauptung oder Feststellung ergeben, dass die Nutzung der Software durch den Lizenznehmer gegen proprietäre oder Rechte an geistigem Eigentum verstößt.

6 - Eigentums- und Urheberrechte, Gefahrübergang

6.1 Die Lizenz gewährt dem Lizenznehmer die begrenzte Lizenz zur Nutzung der Software gemäß den Bedingungen dieser EULA.

6.2 Alle Ansprüche, Interessen und Rechte am geistigen Eigentum bezüglich der Software und alle damit verbundenen Dokumente sind und bleiben im Besitz des Lizenzgebers und/oder werden allein und ausschließlich durch diesen kontrolliert. Der Lizenzgeber behält sich alle Rechte an der lizenzierten Software vor, die nicht ausdrücklich in dieser EULA dem Lizenznehmer gewährt werden, einschließlich des nationalen und internationalen Urheberrechts.

6.3 Der Übergang der Gefahr zwischen Lizenzgeber und Lizenznehmer bezüglich der Software erfolgt zu dem Zeitpunkt, zu dem das Gerät, auf dem die Software installiert ist, an den Lizenznehmer ausgeliefert wird.

2024-01

7 - Beschränkte Gewährleistung und Haftungsausschluss

7.1 Der Lizenznehmer erkennt ausdrücklich an, dass die Nutzung der lizenzierten Software auf seine eigene Gefahr erfolgt. Der Lizenzgeber gibt keine Garantien oder andere Gewährleistungsansprüche, ob ausdrücklich oder stillschweigend, für die lizenzierte Software. Sie wird "wie besehen", ohne irgendwelche Gewährleistung, Bedingungen oder Bestimmungen, bereitgestellt, sofern in dieser EULA nicht anderweitig vereinbart.

7.2 Der Lizenzgeber gewährleistet, dass zum Zeitpunkt des Gefahrübergangs, wenn die Software in der Hard- und/oder Softwarekonfiguration installiert ist, in der sie an den Lizenznehmer ausgeliefert wurde, die Software in wesentlicher Übereinstimmung mit den Leistungen arbeitet, die in den zugehörigen Informationen beschrieben sind.

7.3 Mit Ausnahme der Bestimmungen in der vorgenannten beschränkten Gewährleistung schließt der Lizenzgeber alle anderen Garantien, ob ausdrücklich, stillschweigend oder anderweitig, aus, einschließlich der Gewährleistung der Handelsüblichkeit oder Eignung für einen bestimmten Zweck. Auch gewährleistet der Lizenzgeber nicht, dass die Software fehlerfrei ist oder ohne Unterbrechung arbeitet.

7.4 Keine zusätzlichen mündlichen oder schriftlichen Informationen oder Ratschläge durch den Lizenzgeber, seine Händler, Großhändler, Agenten oder Mitarbeiter stellen eine Garantie dar oder erweitern in irgendeiner Weise den Geltungsbereich der genannten Gewährleistung.

7.5 Lizenzgeber und Lizenznehmer stimmen darin überein, dass ein Fehler der Software vorliegt, wenn sie nicht über die oben festgelegten Qualitäten und Eigenschaften verfügt, wie in Abschnitt 7.2 zum Gefahrübergang beschrieben. Mängel der Software, die auf Seiten des Lizenznehmers erkannt wurden, können nur akzeptiert werden, wenn sie rekonstruierbar oder bewiesen sind.

7.6 Es liegt kein Fehler vor, wenn die Software auf anderer Hardware eingesetzt wird als auf dem Gerät, auf dem die Software installiert wurde. In den folgenden Fällen liegt ebenfalls kein Fehler vor:

- Schäden, die durch eine fehlerhafte oder fahrlässige Handhabung der Software entstehen, die nicht durch den Lizenzgeber verursacht werden,
- Schäden, die sich aus bestimmten externen Einflüssen ergeben, die nicht unter dieser EULA vorausgesetzt werden,
- jegliche Änderungen, die vom Lizenznehmer oder von Dritten vorgenommen werden, sowie alle daraus resultierenden Konsequenzen,
- Inkompatibilität der Software mit der Datenverarbeitungsumgebung des Lizenznehmers.

7.7 Falls irgendein Defekt vorliegt, ist der Lizenzgeber berechtigt, die Option zu wählen, die Behebung des Mangels nach seinem eigenen Ermessen durchzuführen, durch (a) Lieferung eines Ersatzes für die defekte Software, oder (b) Anbieten einer Nacherfüllung. Die Gewährleistungsfrist wird durch den Kaufvertrag des Geräts bestimmt.

8 - Haftungseinschränkungen

8.1 Die maximale Haftung des Lizenzgebers oder seiner leitenden Angestellten, Direktoren, Angestellten, Vertreter, Distributoren und Wiederverkäufer unter dieser Lizenz für alle Verluste oder Schäden, Kosten oder Verletzungen, entweder direkt, indirekt, zufällig oder sonstig, die sich aus der Verletzung jeglicher ausdrücklicher oder stillschweigender Gewährleistung, Bedingung oder Bestimmung, Vertragsverletzung, unerlaubter Handlung, Schadensersatzrecht oder anderen gesetzlichen Tatbeständen ergibt, die sich aus oder im Zusammenhang mit dieser EULA oder der Nutzung der Software ableiten lässt, ist beschränkt auf 10 % des vom Lizenznehmer bezahlten Einkaufpreises für das Gerät.

8.2 IN KEINEM FALL HAFTET DER LIZENZGEBER GEGENÜBER DEM LIZENZNEHMER ODER DRITTEN FÜR (A) GEWINNVERLUSTE, VERLUSTE VON EINNAHMEN, (B) INDIREKTE, ZUFÄLLIGE ODER FOLGESCHÄDEN, SELBST WENN KENNTNIS VON DER MÖGLICHKEIT SOLCHER BESTAND, (C) VERLUST VON DATEN ODER ALLEN ZUGEHÖRIGEN ANLAGENAUSFÄLLEN.

8.3 Die Beschränkung der Haftung gilt nicht, wenn der Lizenzgeber für vorsätzliche Pflichtverletzung oder grobe Fahrlässigkeit haftbar ist, unabhängig von den rechtlichen Grundlagen, oder wenn eine höhere Haftung nach zwingenden gesetzlichen Regelungen verlangt wird, wie beispielsweise, jedoch nicht beschränkt auf, durch das Produkthaftungsgesetz.

8.4 Es dürfen keine Maßnahmen oder Verfahren in Zusammenhang mit dieser EULA durch den Lizenznehmer mehr als drei Monate, nachdem die Ursache des Verfahrens auftritt, angestrengt werden.

9 - Software von Drittanbietern

Die Entwicklung von Teilen dieser Software basiert teilweise auf der Arbeit von Software von Dritten, für die Vermerke und/oder zusätzliche Bedingungen erforderlich sind, wie auf dem Bildschirm "About“ (Info) von "VisuNet RM Shell 5“ aufgeführt. Darüber hinaus enthält die Software Open Source-Softwareprogramme von Drittanbietern, die als unveränderte Kopien bereitgestellt werden. Eine Liste der enthaltenen Open Source Softwareprogramme, einschließlich der erforderlichen markanten Hinweise und der entsprechenden Lizenzbedingungen, finden Sie auch auf dem Info-Bildschirm der "VisuNet RM Shell 5“.

10 - Zusätzliche Funktionen der Software

Im Falle des Erwerbs von zusätzlichen Funktionen der Software stellt der Lizenzgeber dem Lizenznehmer einen Produktschlüssel zur Verfügung, der die Verwendung der zusätzlichen Funktionen auf dem Gerät autorisiert, auf dem sie an den Lizenznehmer ausgeliefert wurden; jede andere Verwendung des Produktschlüssels, insbesondere für andere Geräte, ist nicht zulässig.

11 - Geltendes Recht und Gerichtsstand

11.1 Die Gültigkeit, die Interpretation und die rechtlichen Auswirkungen dieser EULA werden geregelt und ausgelegt in Übereinstimmung mit dem Recht der Bundesrepublik Deutschland unter Ausschluss des deutschen Kollisionsrechts.

11.2 Die Kammern des Landgerichts Mannheim, Deutschland, sind allein zuständig bei eventuellen Streitfragen bezüglich dieser EULA. Jede Klage oder andere Verfahren bezüglich einer solchen Kontroverse werden in den genannten Gerichten in Mannheim und nicht anderswo verhandelt.

12 - Salvatorische Klausel und Inkonsistenzen

12.1 Sollte bezüglich einer Bestimmung in dieser EULA festgestellt werden, dass sie übermäßig umfassend, zweideutig oder anderweitig nicht durchsetzbar ist, dann wird diese Bestimmung neu formuliert, um ihren Geltungsbereich soweit erforderlich zu schmälern, um sie angemessen und durchsetzbar zu machen. Wenn der Geltungsbereich der Bestimmung nicht soweit eingeschränkt werden kann, dass die Bestimmung durchsetzbar wird, dann wird die Bestimmung aus dieser EULA entfernt.

12.2 In jedem Fall bleibt die übrige EULA in Kraft und behält ihre Gültigkeit.

12.3 Falls die Bedingungen dieser EULA in Konflikt mit den Inhalten der Microsoft-Software-Lizenzbedingungen stehen, haben die letzteren Vorrang in Bezug auf Microsoft-Software.

13 - Änderungen

Änderungen und Zusätze zu dieser EULA sind nur gültig, wenn sie schriftlich erfolgen und von beiden Parteien unterzeichnet sind; auf die Erfordernis der Schriftform kann nur schriftlich verzichtet werden.

Your automation, our passion.

Explosionsschutz

- Eigensichere Barrieren
- Signaltrenner
- Feldbusinfrastruktur FieldConnex®
- Remote-I/O-Systeme
- Elektrisches Ex-Equipment
- Überdruckkapselungssysteme
- Bedien- und Beobachtungssysteme
- Mobile Computing und Kommunikation
- HART Interface Solutions
- Überspannungsschutz
- Wireless Solutions
- Füllstandsmesstechnik

Industrielle Sensoren

- Näherungsschalter
- Optoelektronische Sensoren
- Bildverarbeitung
- Ultraschallsensoren
- Drehgeber
- Positioniersysteme
- Neigungs- und Beschleunigungssensoren
- Feldbusmodule
- AS-Interface
- Identifikationssysteme
- Anzeigen und Signalverarbeitung
- Connectivity

Pepperl+Fuchs Qualität
Informieren Sie sich über unsere Qualitätspolitik:

www.pepperl-fuchs.com/qualitaet

PEPPERL+FUCHS

www.pepperl-fuchs.com

/ DOCT-6044G