VisuNet RM Shell 5

Manual

Your automation, our passion.

PEPPERL+FUCHS

With regard to the supply of products, the current issue of the following document is applicable: The General Terms of Delivery for Products and Services of the Electrical Industry, published by the Central Association of the Electrical Industry (Zentralverband Elektrotechnik und Elektroindustrie (ZVEI) e.V.) in its most recent version as well as the supplementary clause: "Expanded reservation of proprietorship"

Worldwide

Pepperl+Fuchs Group

Lilienthalstr. 200

68307 Mannheim

Germany

Phone: +49 621 776 - 0

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

North American Headquarters

Pepperl+Fuchs Inc.

1600 Enterprise Parkway

Twinsburg, Ohio 44087

USA

Phone: +1 330 425-3555

E-mail: sales@us.pepperl-fuchs.com

Asia Headquarters

Pepperl+Fuchs Pte. Ltd.

P+F Building

18 Ayer Rajah Crescent

Singapore 139942

Phone: +65 6779-9091

E-mail: sales@sg.pepperl-fuchs.com

https://www.pepperl-fuchs.com

2022-02

2022-02

1 History of the Manual

The following editions of the manual have been released:

Version	Comments
Previous	VisuNet RM Shell version 5.5
11/2021	VisuNet RM Shell version 5.6 • Added Support for the Pad-Ex® 01 device • Added Quick Menu with status icons • Customized VisuNet RM Shell Wallpaper and Logo • Added "Auto Logout" for Administrator and Engineer • Added support of RDP virtual channel add-ins (requires PRO license)

2022-02

2 Introduction

2.1 Note

This manual revision was released with VisuNet® RM Shell version 5.6 but also covers all previous versions of VisuNet RM Shell 5.

2.2 Content of this Document

This document contains information required to use the product in the relevant phases of the product life cycle. This may include information on the following:

- Product identification
- Delivery, transport, and storage
- Mounting and installation
- Commissioning and operation
- Maintenance and repair
- Troubleshooting
- Dismounting
- Disposal

Note

For full information on the product, refer to the further documentation on the Internet at www.pepperl-fuchs.com.

The documentation comprises the following parts:

- This document
- Datasheet

In addition, the documentation may comprise the following parts, if applicable:

- EU-type examination certificate
- EU declaration of conformity
- Attestation of conformity
- Certificates
- Control drawings
- Instruction manual
- Other documents

2.3 Target Group, Personnel

Responsibility for planning, assembly, commissioning, operation, maintenance, and dismounting lies with the plant operator.

Only appropriately trained and qualified personnel may carry out mounting, installation, commissioning, operation, maintenance, and dismounting of the product. The personnel must have read and understood the instruction manual and the further documentation.

Prior to using the product make yourself familiar with it. Read the document carefully.

2.4 Symbols Used

This document contains symbols for the identification of warning messages and of informative messages.

Warning Messages

You will find warning messages, whenever dangers may arise from your actions. It is mandatory that you observe these warning messages for your personal safety and in order to avoid property damage.

Depending on the risk level, the warning messages are displayed in descending order as follows:

Danger!

This symbol indicates an imminent danger.

Non-observance will result in personal injury or death.

Warning!

This symbol indicates a possible fault or danger.

Non-observance may cause personal injury or serious property damage.

Caution!

This symbol indicates a possible fault.

Non-observance could interrupt the device and any connected systems and plants, or result in their complete failure.

Informative Symbols

Note

This symbol brings important information to your attention.

Action

1. This symbol indicates a paragraph with instructions. You are prompted to perform an action or a sequence of actions.

3 VisuNet RM Shell—An Overview

Pepperl+Fuchs VisuNet Remote Monitors (RMs) and Box Thin Clients (BTC) are industrial-grade thin-client solutions that provide a simplified, modern user interface for operators. The firmware of an RM, called VisuNet RM Shell, enables users to easily access applications that run on a host system (e.g., workstation PC or server) via Ethernet.

With VisuNet RM Shell, the latest versions of common remote protocols, such as RDP 10 or VNC are supported. With these protocols, the RMs / BTCs can be easily integrated into all major process control systems—whether they are virtualized or conventional workstation-based setups.

Further, VisuNet RM Shell has a tailored user interface, which only shows the important system aspects that are relevant for the configuration of the RM / BTC. This makes the integration of an RM / BTC into the process control system simpler than ever before. Configuring a new RDP connection, for example, can be done in a few steps. This is achieved via a consistent, touch-screen-optimized design across all protocol editors.

VisuNet RM Shell also helps increase process stability. It ensures a stable connection to the process control host system and an error-free display of the process pictures.

The auto-connect function can be used to configure RMs / BTCs in such a way that they automatically establish a connection to a designated host system, without any further intervention from the user. While temporarily interrupted connections are automatically re-established, backup hosts can be specified in VisuNet RM Shell to which an RM / BTC can automatically connect if a host system fails.

In addition to support for remote protocols, VisuNet RM Shell also offers a restricted web browser feature, which can be enabled via an optional professional license key. This allows fixed addresses to web applications like web-based Manufacturing Execution Systems (MES) to be defined. Users with administrator rights can restrict operator access to these pre-defined websites. This increases system security and reduces the risk of malware infiltration.

This manual describes the features and functions of VisuNet RM Shell in detail.

3.1 Update Architecture

The RM Shell architecture consists of two partitions.

The main elements of partition C are the RM Shell as well as Device Drivers and Service Applications. All components are based on Windows 10 IOT LTSC 2019 or Windows 10 IOT LTSB 2016.

Updates regarding Windows security patches, functional updates or RM Shell security updates effect partition C. Only single components are affected and will be overwritten depending on the update. Whenever a factory reset is performed all data of partition C will be overwritten.

The Factory Reset Update is an own package which will be provided and imported via Shell.

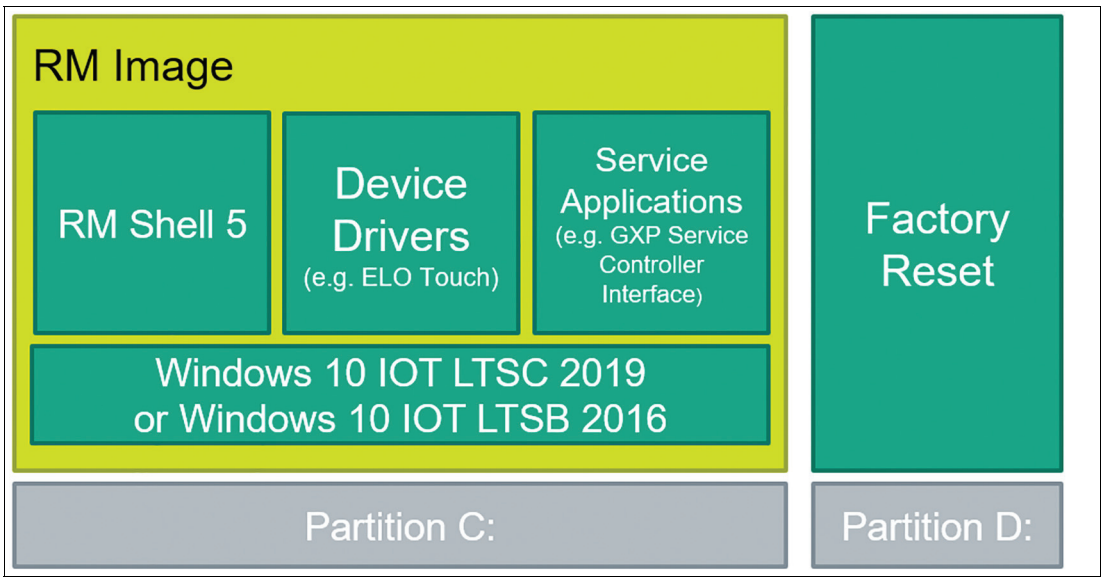


Figure 3.1 Architecture of the RM Shell

3.2 Factory Reset

With Factory Reset Version No. 6.0 and newer, the image file is no longer available locally on Partition D which increases the storage and speed. With Factory Reset Version >6.0 and VisuNet RM Shell version >5.3 it is possible to capture your own backup image. We strongly recommend creating your own backup image and store it on your network drive.

Feature	Description	Notes
Pepperl+Fuchs Factory Reset Image	Available for each-specific device. The Pepperl+Fuchs default settings are applied back to your device. With Factory Reset 6.0 and newer the image file will not be stored on the device anymore.	Get in contact with your local sales support **Caution!** After applying the Pepperl+Fuchs image, the setup of the device needs to be performed locally! The VisuNet RM Shell first start wizard will guide you through the most important initial configuration steps. Refer to the First Start Wizard Chapter in the VisuNet RM Shell manual for further information.
Backup Image	Own captured Backup Image, which can only be applied on the same device with the identical serial number. The backup image can be used to restore a specific state of a device.	Has to be captured by the customer in the VisuNet RM Shell Factory Reset or via VisuNet CC - Device Backup in advance. **Note:** VisuNet CC might not be able to find the device when changes of the computer name or the Network settings have been done after capturing the image file.

3.3 Program Features

Feature	Description	Notes
Operating system	Based on Microsoft® Windows® 10 IoT Enterprise LTSC 2019 or Microsoft® Windows® 10 IoT Enterprise LTSB 2016	Improved feature in RM Shell 5
Modern, simplified user interface	Touch-optimized, modern UI	
Easy Set-up	Designed to be used intuitive. Additional an initial setup wizard guides you through the most important steps when configuring an RM for the first time	Improved feature in RM Shell 5
Auto-connect	Allows you to configure the RM to automatically connect to host systems after startup	
Connection loss detection	The RM detects network failures or if a host is unavailable	
Backup connection	In case of a network or host failure, an RM can automatically connect to a backup host system	
Centralized management of all RMs	RMs can be managed and configured centrally via VisuNet Control Center.	Optional CC license feature. Please find further information at pepperl-fuchs.com/hmi
Remote Protocols and Clients		
MS RDP	Latest version of Microsoft Remote Desktop Protocol	

Feature	Description	Notes
VNC	VNC client, compatible with multiple VNC servers (e.g., TightVNC and UltraVNC)	
Restricted web browser, based on Internet Explorer	Fast HTML browser that uses Internet Explorer to render websites. Operators can be restricted to visiting only specified websites.	Optional PRO license feature
Restricted web browser, based on Chrome	Fast HTML5 browser that uses the Google Chrome. Operators can be restricted to visiting only specified websites.	Optional PRO license feature
Desktop Sharing	Displays the desktop of other RMs with enabled Desktop Sharing Server	Optional PRO license feature
Raritan KVM	Client allows you to directly connect to Raritan Dominion KX IV-101 KVM-over-IP-Switch	Optional PRO license feature
DRDC	Allows you to directly connect from a VisuNet Remote Monitor to a virtualized Emerson DeltaV system	Optional DRDC license feature
Security		
Unified write filter	Unified write filter Protects the drive from persistent storage of malicious software	New feature in RM Shell 5
Scheduler	Enables 24/7 use of unified write filter without buffer overflow. Periodic reboots can be planned to occur when device is not in use	New feature in RM Shell 5
Antivirus software support	Administrators can install third-party virus protection software. Windows defender is activated by default	New feature in RM Shell 5
Dialog filter	Closes application windows that are not whitelisted and blocks user access to the file system	New feature in RM Shell 5
Firewall	Windows firewall protects RMs from network attacks	
USB pen drive lock	USB lockdown prevents access of storage media like USB sticks on the RMs	
Updates	Pepperl+Fuchs provides regularly updates in terms of security patches and functional updates.	Please check for updates regularly or use our Thin Client Software Update Service to be informed by Pepperl+Fuchs.
Capture Backup Image	Capture your individual device settings of the RM/BTC as a backup image and apply when required back on to the device.	New feature of RM Shell 5.3 and newer, and Factory Reset 6.0 **Note:** RM Shell 5.3 (or newer) in combination with Factory Reset 6.0 (or newer) is required.
Apply Backup Image	Apply your individual device settings of the RM/BTC which were earlier captured as a backup image and overwrite the full windows partition.	New feature of RM Shell 5.3 and newer, and Factory Reset 6.0 **Note:** RM Shell 5.3 (or newer) in combination with Factory Reset 6.0 (or newer) is required.
Additional Security Features		

2022-02

Feature	Description	Notes
Security Alerts	Pepperl+Fuchs investigates all reports of **security vulnerabilities** affecting Pepperl+Fuchs products and services.	Cyber Security and Reporting, Subscribe to our **RSS feed** to stay updated on Cyber Security Information from Pepperl+Fuchs
Thin Client Software Update Service	Let us inform you when either security or functionality updates are available.	https://www.pepperl-fuchs.com/global/en/33314.htm
Advanced Features		
Administrator access to Windows® Explorer	Allows administrators to install third-party applications and adjust advanced system Settings. Systems can be integrated in the domain.	New feature in RM Shell 5
Clean lock	Allows you to temporarily lock the input devices (e.g., touchscreen) when cleaning the device to avoid accidental inputs	
Network test tools	A set of network test tools (e.g., ping tool) provide support while commissioning an RM	
Task Switcher	Switch between multiple remote connections and apps that are running on the RM.	
Extended desktop support for industrial Box Thin Client BTC	Remote profile connections can be assigned to different monitors that are connected to the industrial Box Thin Client BTC	
Wireless LAN configuration support	Wireless LAN connections can be managed in RM Shell (requires built-in wireless LAN adapter)	
Process explorer	Allows you to diagnose an RM and monitor how much RAM, storage, and CPU are being used by local processes.	
Desktop Sharing Server	Clone an RM and display its desktop on other RMs	

3.4 Licencing

Ordering Information

When purchasing Pepperl+Fuchs RMs or BTCs RM Shell is already installed and the scope of delivery includes RM Shell licenses.

Part No.	Model Number
548289	VISUNET-RM-SHELL5-PRO
548294	VISUNET-RM-SHELL5-DRDC
548284	VISUNET-RM-SHELL5-CC

Note

License Bundles

Contact your local Pepperl+Fuchs sales representative for information about license bundles.

3.5 Default Passwords

Device/Function	User	Password
Factory reset		VisuReset
Raritan KVM over IP Switch DKX4-101	admin	raritan

3.6 Installation

A Wizard guides you through the first steps of the installation of the RM Shell. After completing the First Start Wizard the RM Shell will be started in the Operator Role.

3.6.1 First Start Wizard

When you start a device with VisuNet RM Shell for the first time, the first-start wizard appears on your screen. This wizard guides you through the most important initial configuration steps.

Configure your "Basic System Settings" and click **Next**. Accept the "Terms and Conditions" on the next window to start using VisuNet RM Shell.

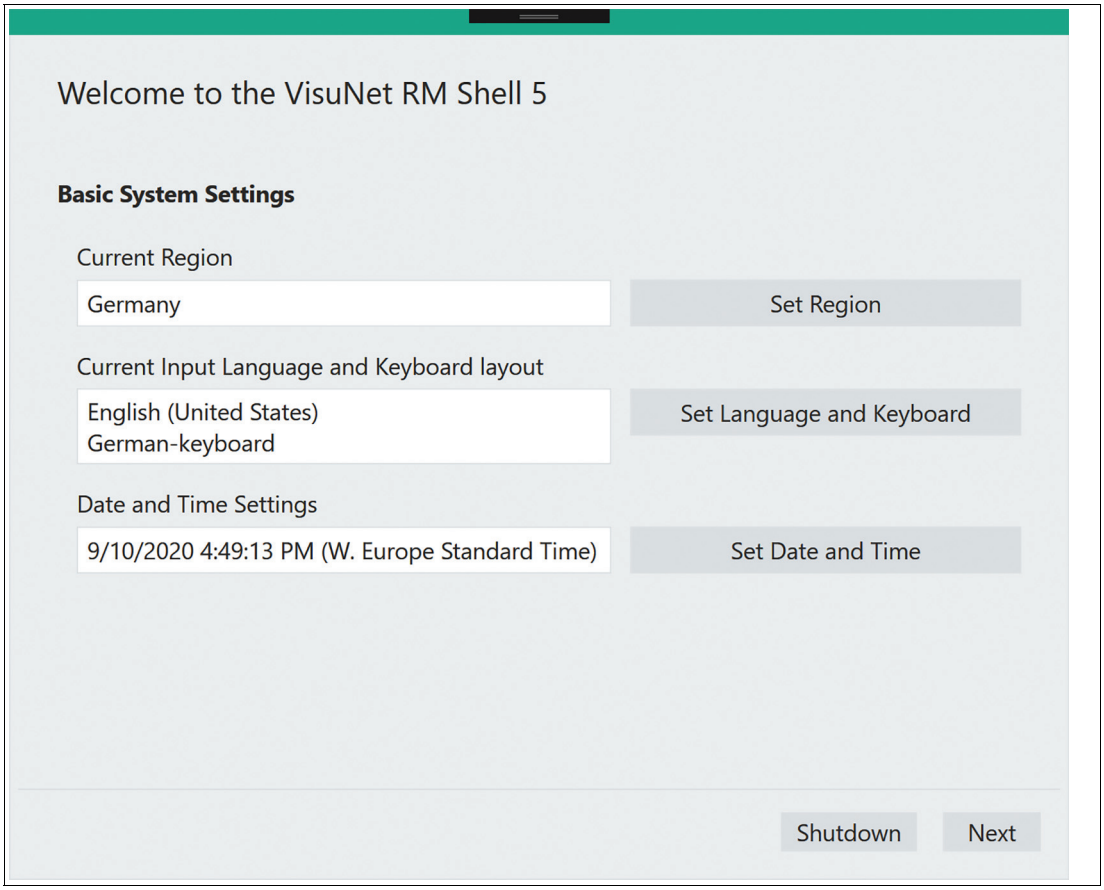


Figure 3.2

If your VisuNet RM Shell 5 is based on Windows® 10 IoT Enterprise 2019 LTSC, you also must perform the following steps:

Set the correct "Region"

1. Click **Set Region** to enter the advanced Microsoft® settings.

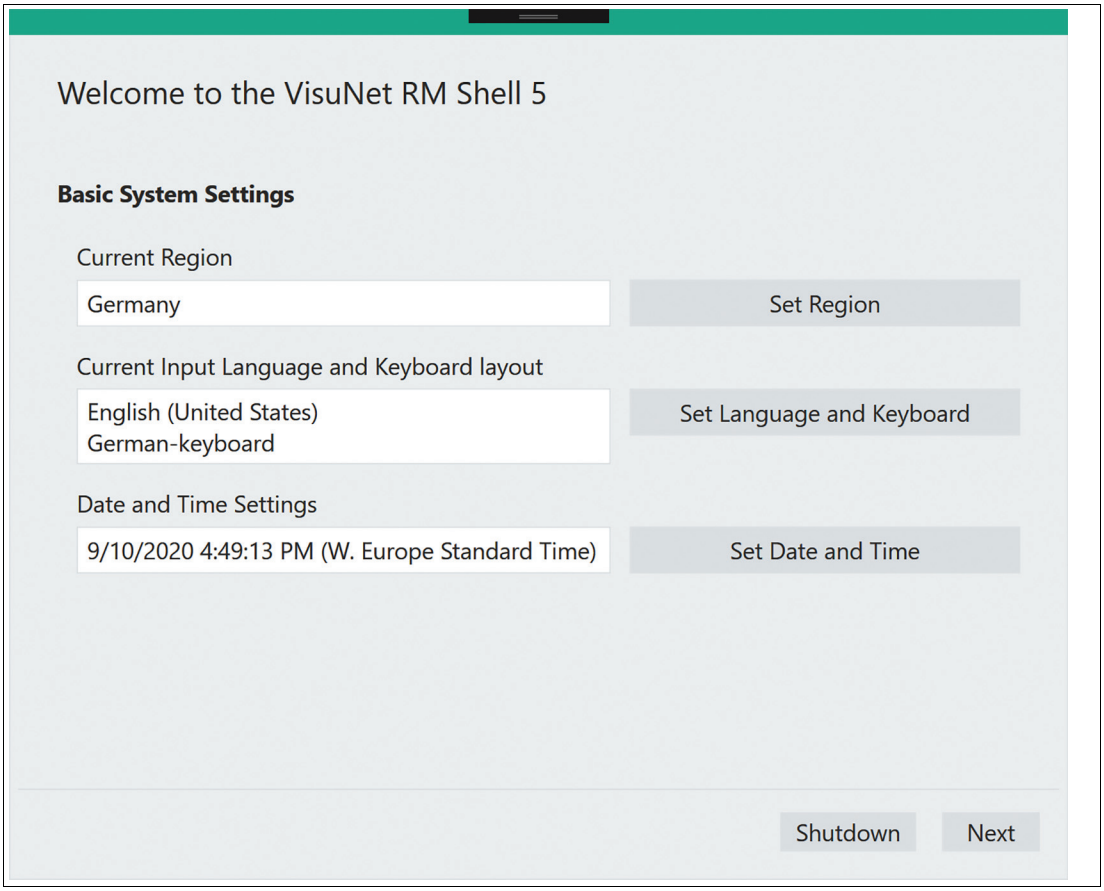


Figure 3.3

2. Navigate to the **Region** tab on the left side

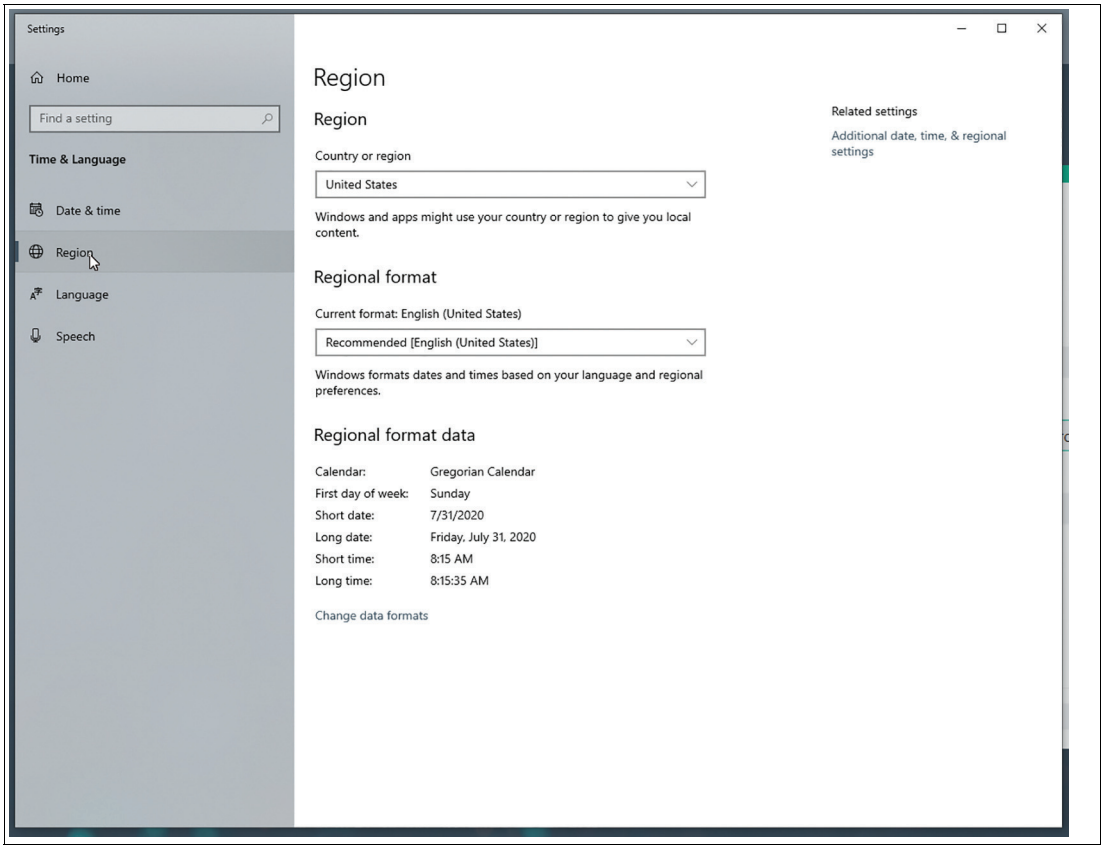


Figure 3.4

3. Pick the required "Region" from the drop-down list.

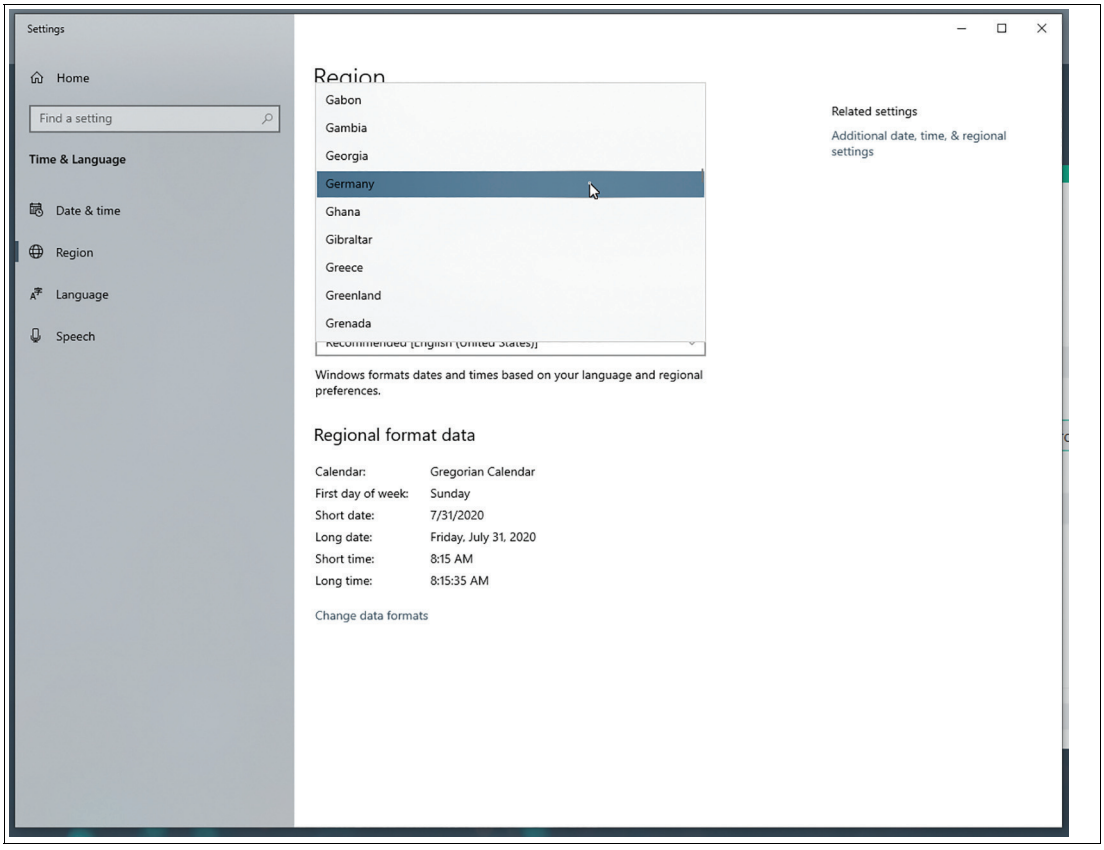


Figure 3.5

2022-02

4. Close the dialog.

Add "Keyboard Layout"

Click **Set Language and Keyboard** (2.) to enter the advanced Microsoft® settings, then navigate to **Language**

1. Select the installed language **English (United States)** and click the **Options** button:

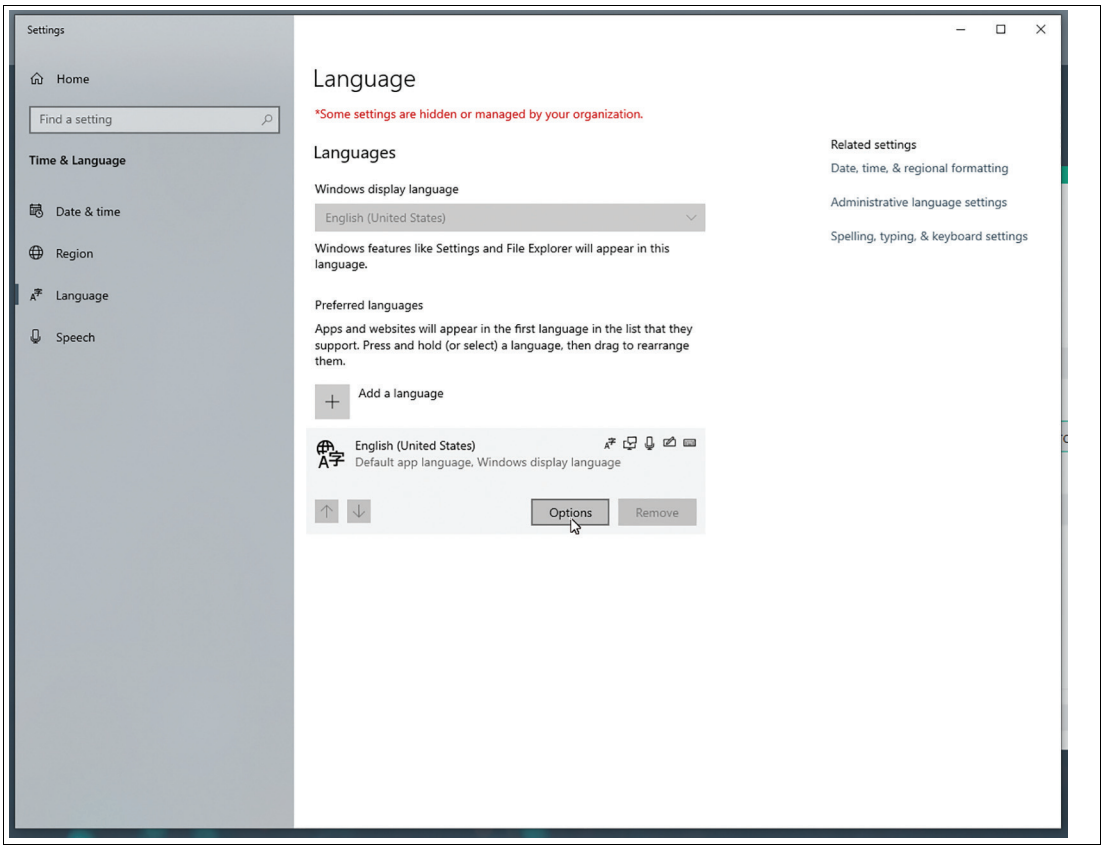


Figure 3.6

2. Under the "Keyboards" section, click the **Add a keyboard** button

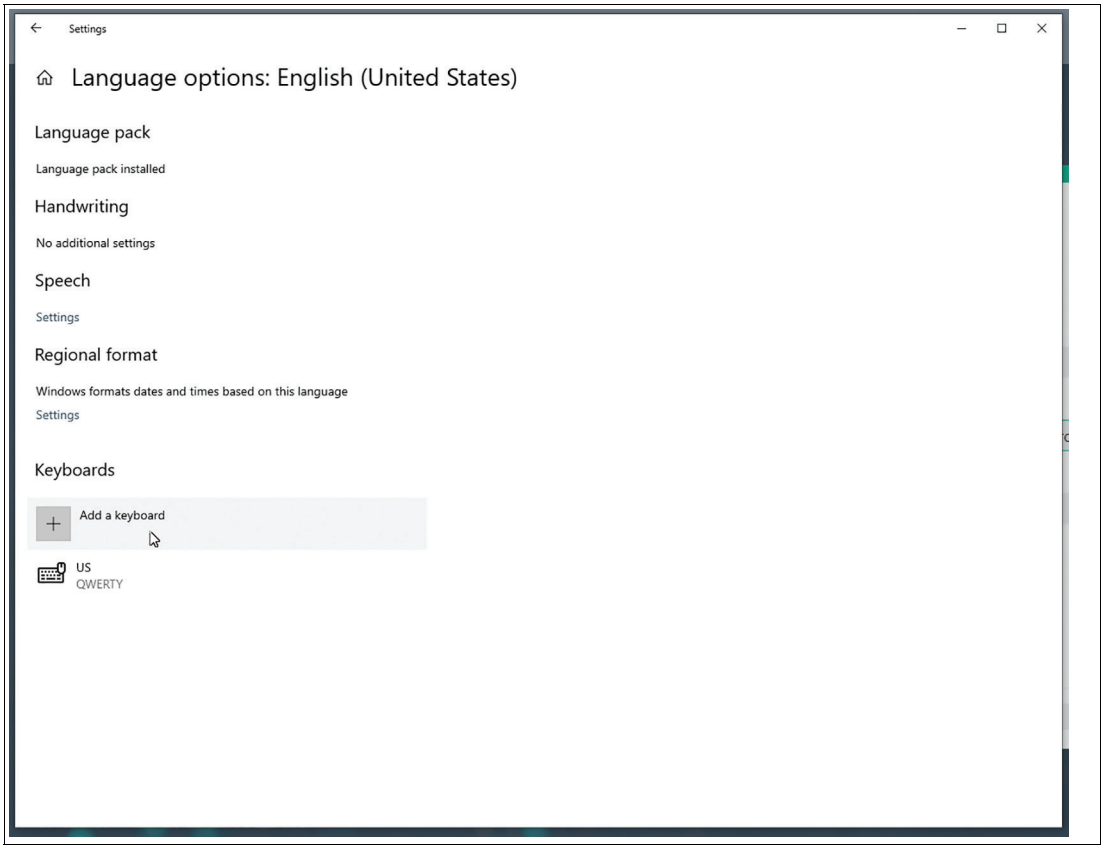


Figure 3.7

3. Select the new "Keyboard" layout:

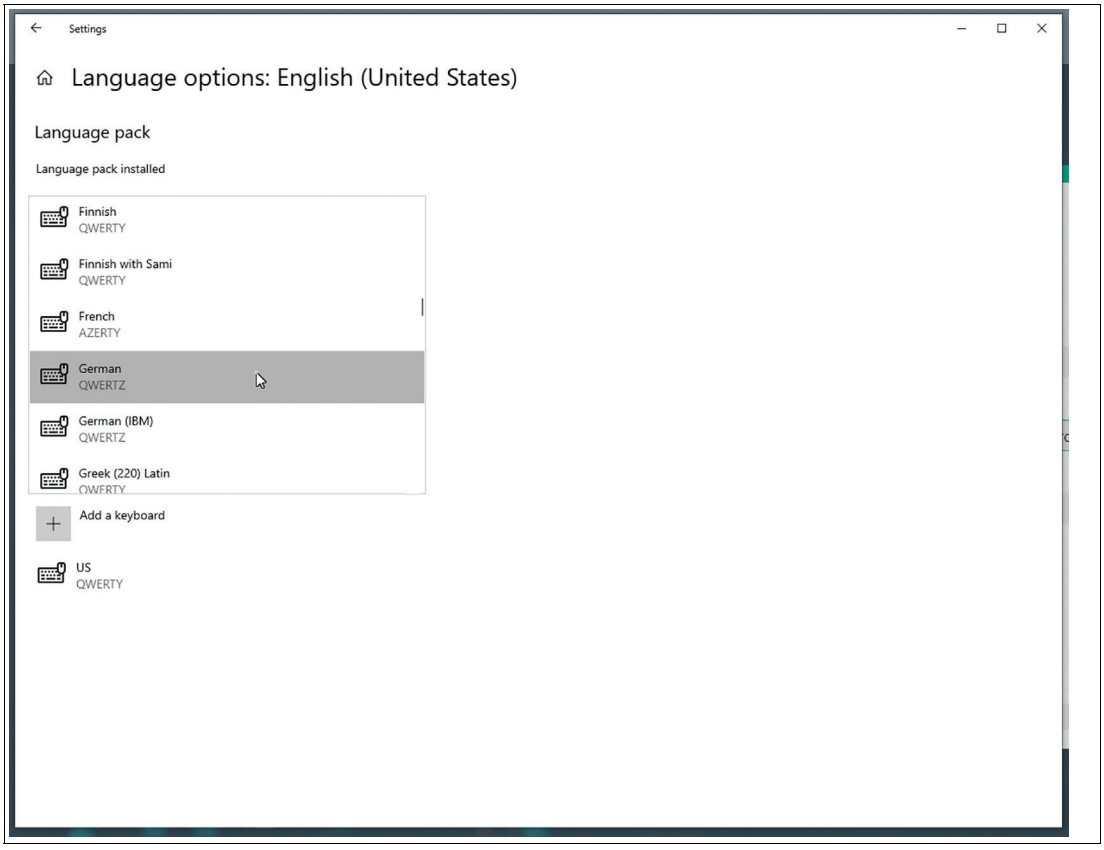


Figure 3.8

4. Remove the "US" keyboard layout in the last step.

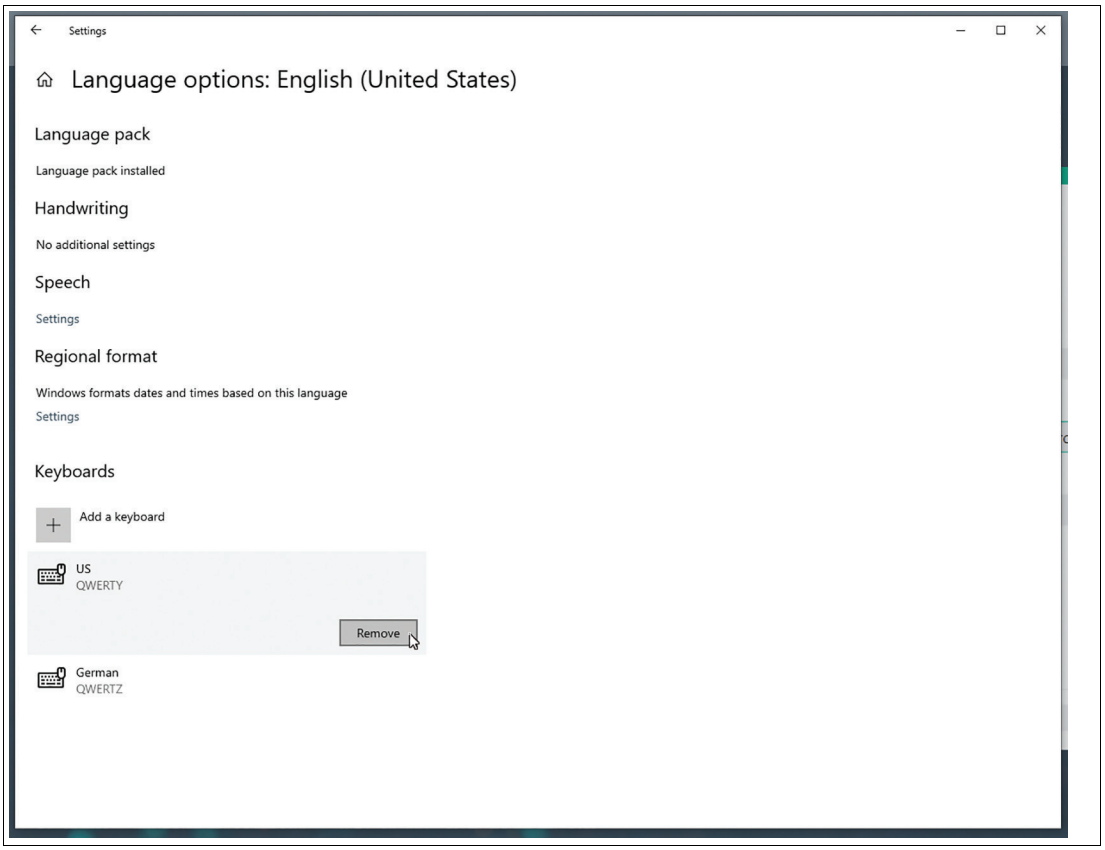


Figure 3.9

5. Close the dialog.
6. The input language in the First Start Wizard will not change, since only the keyboard layout is affected by this change.

The Wizard guides you through the following:

"Computer Name"

Changes the "Computer Name" of your Windows® device as well.

The updated "Computer Name" is only applied after a restart.

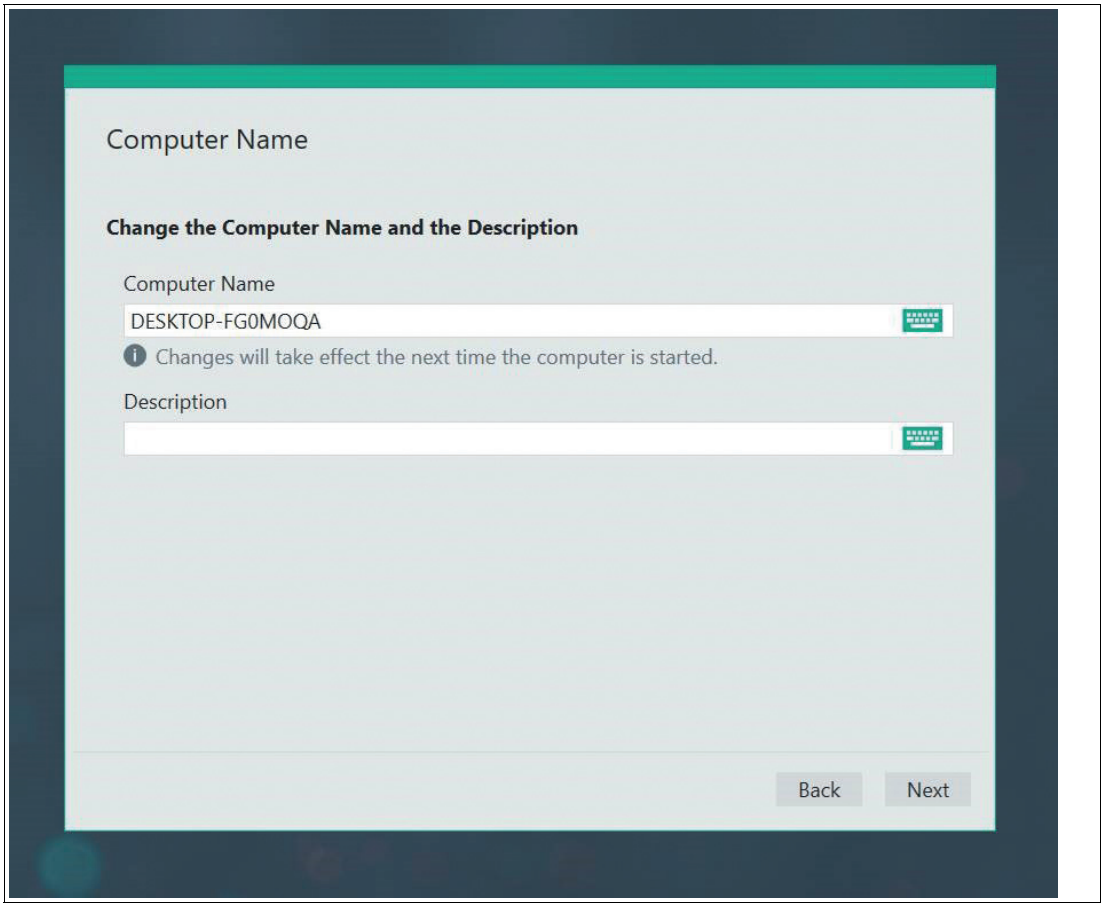


Figure 3.10 "Computer Name"

Setup "Network"

All information about the local RM / BTCs network adapter hardware is shown.

You can edit the network adapter name according to your needs.

Use this option to enable/disable "DHCP" (Dynamic Host Configuration Protocol).

With "DHCP", you can integrate the RM / BTC into an existing network without further manual configuration. Settings like "IP Address", "Subnet Mask", "Default Gateway", and "DNS Server" are addressed then assigned automatically to the RM / BTC. However, you can set up all these parameters manually by disabling the "DHCP" option.

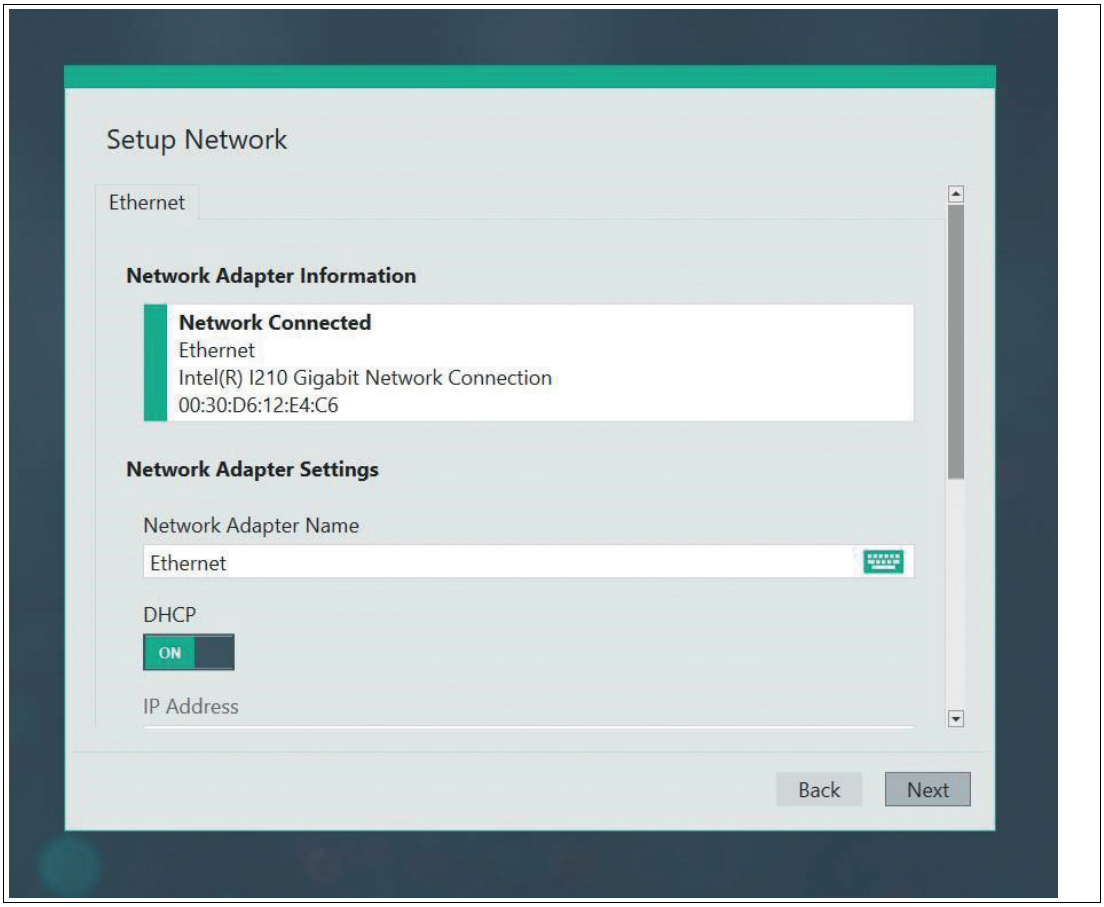


Figure 3.11 "Setup Network"

"Setup Touchscreen"

Select the right touch settings, if your RM is equipped with a touch screen option. For further information refer to chapter 7.13.

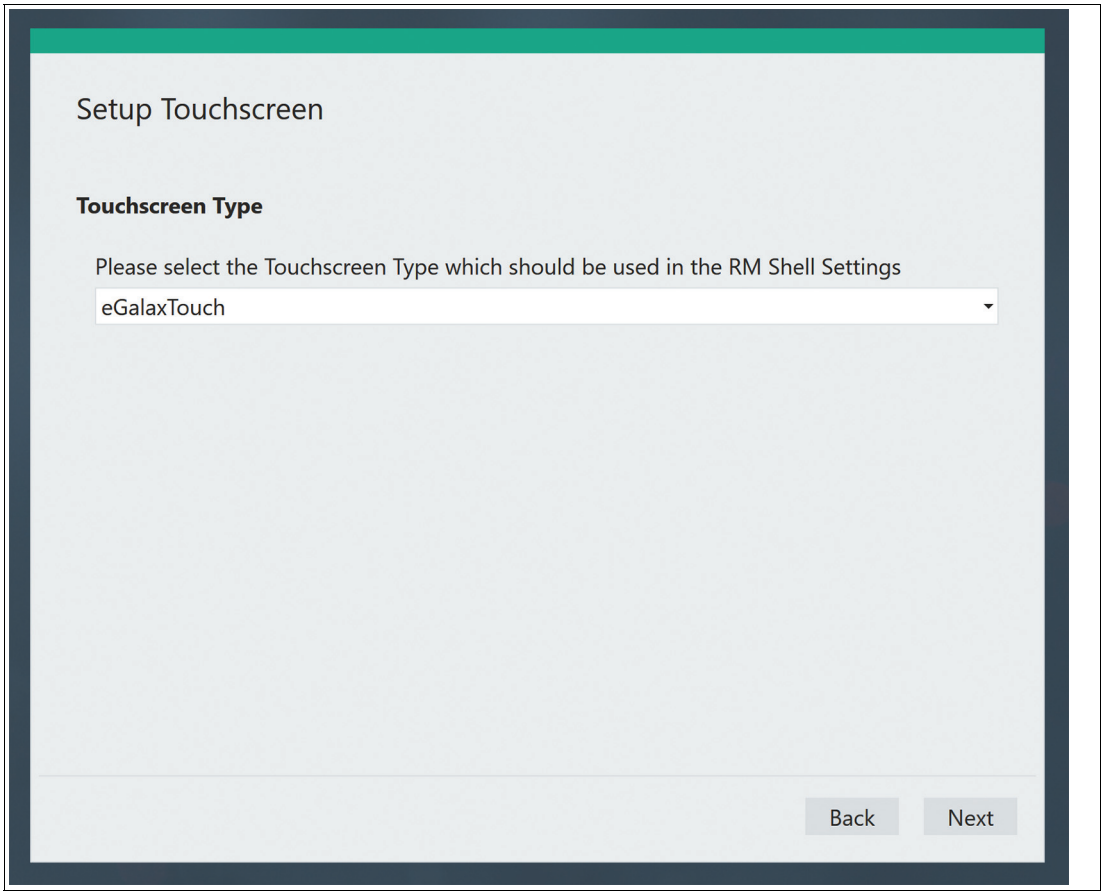


Figure 3.12

Password Settings

"Engineer Password": no default password is set. To ensure the highest level of security, the "Administrator" and "Engineer" user roles must be password protected.

"Administrator Password": no default password is set. To ensure the highest level of security, the "Administrator" and "Engineer" user roles must be password protected.

"Windows Password": accesses the Windows® password. The "Windows Password" is displayed in encrypted form only.

Tip

We highly recommend changing the "Windows Password".

"Factory Reset Password": Change the Factory Reset password. The password is hidden via dots and must have at least 6 characters. The field cannot be blank.

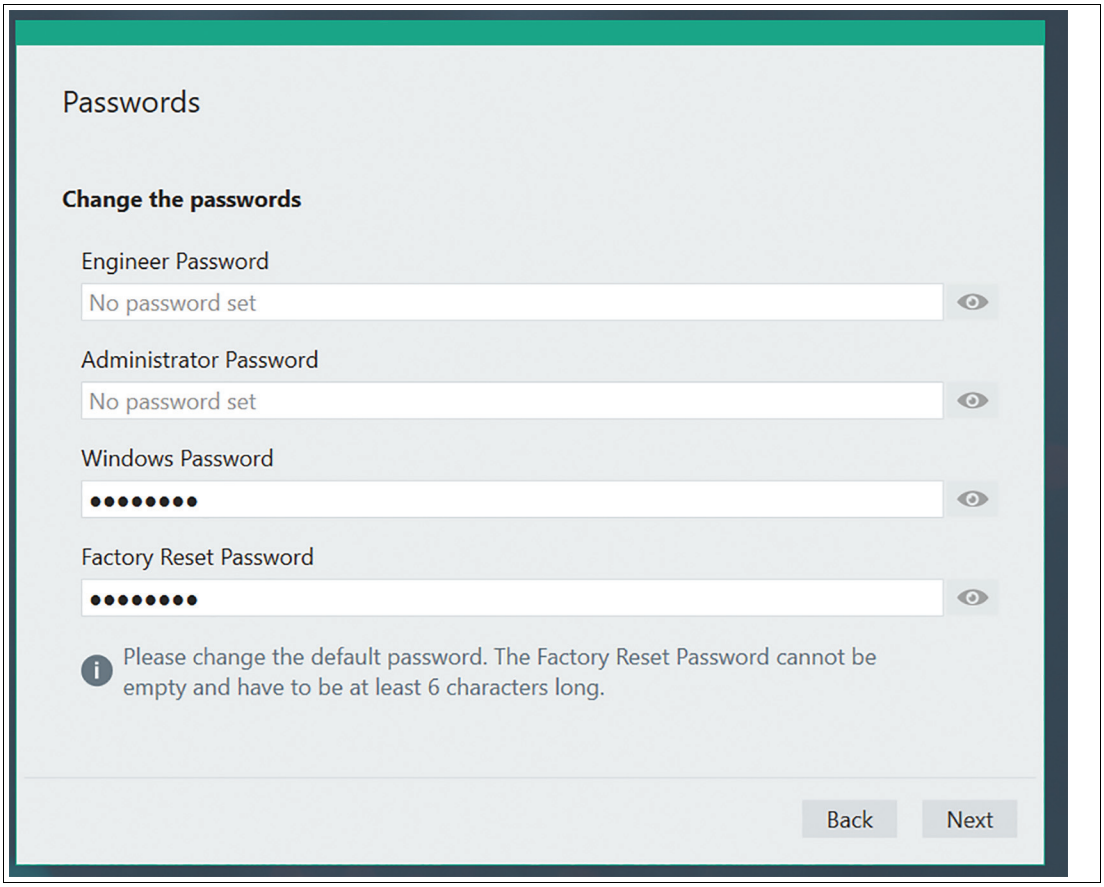


Figure 3.13 Password Settings

Note

In case of restoring a backup or clone image or if you changed the password in the Factory Reset UI the Factory Reset Password option will not appear.

License Agreement

You have to accept the "License Agreement" to proceed further.

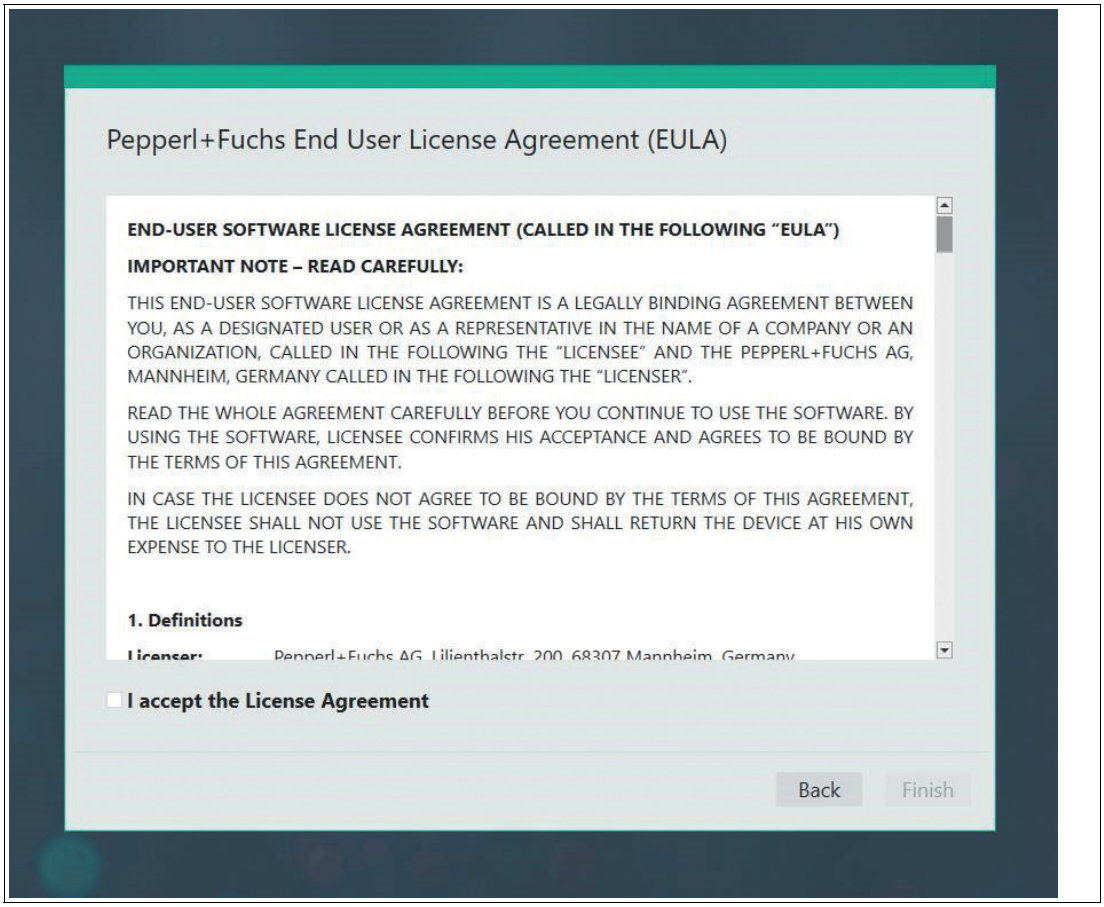


Figure 3.14 License Agreement

Note

Correct Information

Ensure that you set the correct information on this wizard. The information should be valid for the location where the VisuNet RM Shell will be installed. The correct time is required for encrypted communication and to ensure reliable communication.

After completing the First Starting Wizard, the VisuNet RM Shell will be started in the "Operator" role. To configure further settings switch to the "Administrator" role.

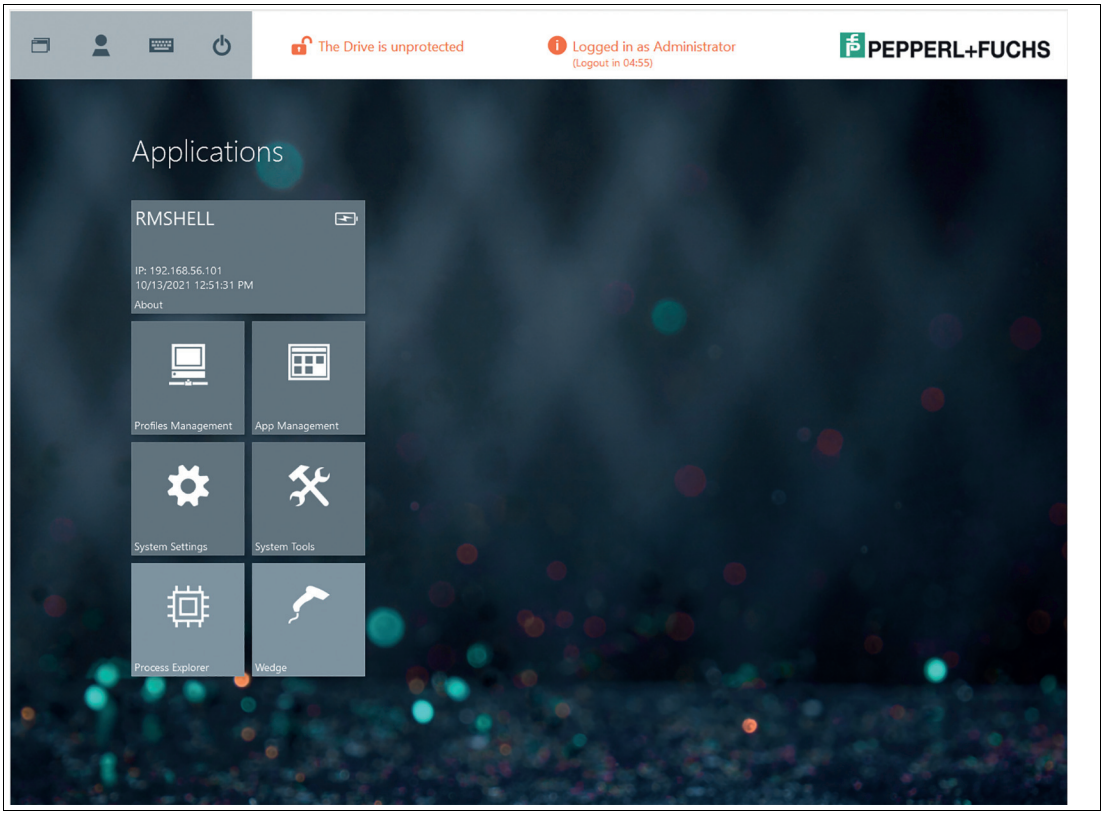


Figure 3.15

VisuNet RM Shell does not come with any pre-created connection profiles. For this reason, the profiles list is empty when you start VisuNet RM Shell for the first time.

3.7 VisuNet RM Shell User Roles

The VisuNet RM Shell security concept is based on 3 user roles that are structured hierarchically. Each user role has different rights.

Figure 3.16 Concept of user rights: **O**(perator), **E**(ngineer) and **A**(dministrator)

User Role	Description
Operator (O)	Operators are standard users. They can only execute predefined profiles. Operators have no access to RM settings.
Engineer (E)	Engineers are responsible for RM setup and integration. They have access to profiles, system settings, and applications (create, edit, and delete profiles).
Administrator (A)	Administrators have all rights of operators and engineers. In addition, administrators can access Windows® Explorer to install third-party applications and drivers and adjust advanced settings outside of VisuNet RM Shell.

Warning!

Password Protection!

To ensure the highest level of security, the Administrator and Engineer user roles must be password protected. Access to the Administrator and Engineer user roles should be permitted only to employees who are familiar with the administration of thin clients. There is no factory default password setting for any of the user roles.

The passwords can be set in the first start wizard. In the administrator role, the passwords can be adjusted or set in the Security Settings

Note

Additional Password Protection with optional User Auto Logout

Engineers and Administrators are logged out when the device is idle for longer than the set time frame if the User Auto Logout is enabled.

Note

Compatibility of Third-Party Software

VisuNet RM Shell is qualified to work with software that is shipped with Pepperl+Fuchs VisuNet devices. Pepperl+Fuchs does not guarantee the functionality of third-party software. Customers are responsible for ensuring compatibility with any third-party software.

2022-02

4 VisuNet RM Shell 5 User Interface

Home Screen Features (Administrator Role, after individual profiles have been created)

The home screen is divided into 6 basic areas:

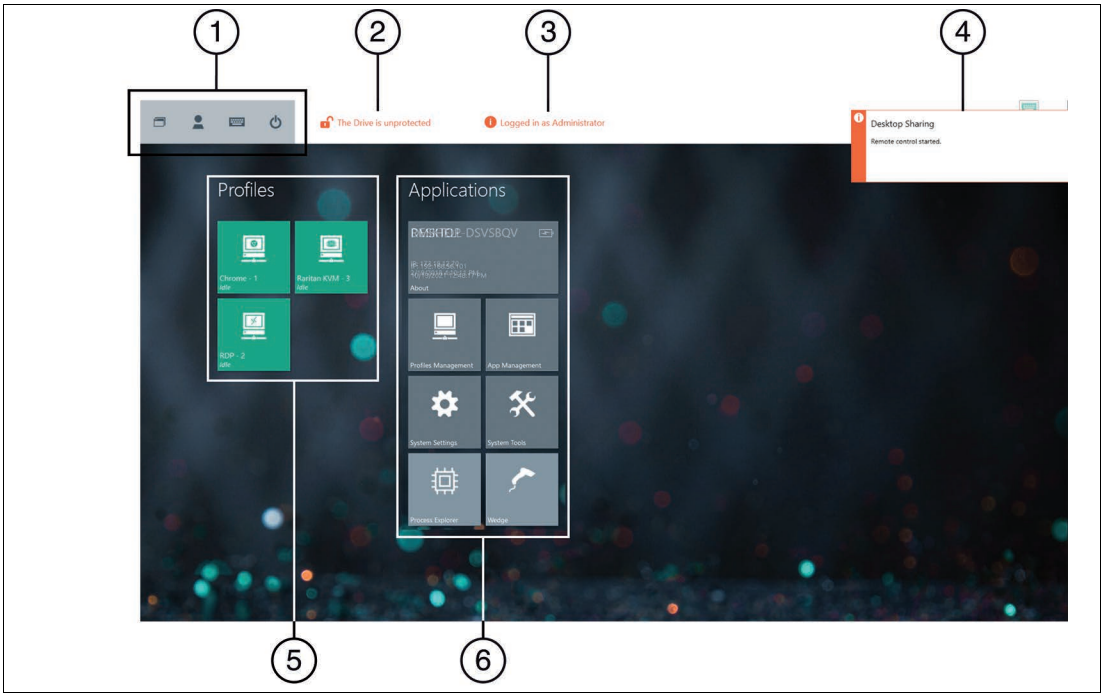


Figure 4.1 RM Shell 5 home screen

No.	Description
1	System functions
2	Unified write filter status
3	User-role information
4	Fly-in messages
5	Profiles
6	Applications

1. System Functions

Icon	Description
	RM Shell Task Switcher The RM Shell Task Switcher allows you to switch between open connection profiles and applications running on an RM / BTC. To open the Task Switcher, click the icon or press the hotkey CTRL+Alt+SCROLL on the keyboard. The Task Switcher shows a window overview of all open remote connections and apps. You can change the application by selecting one of the displayed remote connections or apps. Use the number keys 1 to 9 to switch within the profiles. Click 0 to return to the VisuNet RM Shell Home screen.
	Switch user role Choose between Operator, Engineer, or Administrator

Icon	Description
	Touchscreen keyboard Shows the touchscreen keyboard on the screen.
	Preconfigured power options, such as: • Protect disk and restart • Restart • Shutdown (Some devices need a power reset to be able to boot again) • Turn off display The power options can be set by the Engineer and Administrator user roles. The Operator user role is only allowed to run the preconfigured options.

2. Unified Write Filter Status

This area of the home screen indicates whether the unified write filter is enabled. For more information on the unified write filter, see chapter 4.1.

3. User-Role Information

When an Administrator or Engineer user is logged in, the signed-in user role is indicated at the top of the home screen. If an Operator user is logged in, this information is not displayed.

4. Fly-In Messages

At the top-right corner of the home screen, fly-in messages show error messages or status information when certain events occur. Click on the fly-in messages to make them disappear. The messages automatically disappear after 30 seconds.

5. Profiles

This section shows all profiles that have been created locally. Every profile is represented by a tile that displays the profile type (e.g., "RDP," "VNC"), profile name (e.g., "RDP - 2"), and connection status (e.g., "connected," "disconnected").

The following symbols indicate the different profile types:

RDP	
Desktop Sharing[1]	
VNC	
Web Browser URL (Chrome)[1]	

2022-02

Web browser URL (IE)[1]	
Raritan KVM[1]	

1. PRO license required to unlock feature

Profile status information is indicated at the bottom-left corner of each profile tile:

Status	Description	
Idle	Initial status after a profile has been created	
Disconnected	Profile is not connected to a host	
Connected	Profile is connected to a host PC. A green status bar at the top of the profile tile is visible.	
Connection failed	An error occurred while trying to establish a connection	
Auto connect	If auto connect is enabled, a defined profile connects automatically to a host. The seconds remaining before the next connection retry are counted down in the top-right corner of the profile tile. Simultaneously, an animated white status bar at the top of the profile tile is visible. For more information on auto connect, see chapter 6.1.	

6. Applications

This section shows all applications. The information and features that are accessible in this section vary based on the signed-in user role:

User Role	Description
Operator	Access to profiles (if not limited by a preconfigured auto connect). No access to system settings or applications.
Engineer	Access to profiles, system settings, and applications (create, edit, and delete profiles).
Administrator	Full access to profiles, system settings, applications, and Windows® Explorer.

4.1 Unified Write Filter

The "Unified Write Filter" (UWF) protects the system from persistent storage of malware and viruses. When the UWF is enabled, the system hard drive is locked down and all system changes are only cached. When rebooting the file system, the cache is deleted and the original configuration is loaded again.

To store a configuration persistently, you must disable the UWF and reboot the system. After you have implemented the configuration, enable the UWF and reboot again. This triggers the persistent storage of the configuration.

Caution!

24/7 Operation

During 24/7 operation and enabled UWF, the system can run out of memory. Activate the automatic restart.

Caution!

Windows Swap File

After deactivating the write filter, the "Windows Swap File" is also deactivated. This increases the risk of running out of memory in 24/7 operation, even when the UWF is disabled.

The swap file should therefore be reactivated in the Windows® settings after deactivating the write filter.

Note

User Access to UWF

Only users logged in as "Engineer" or "Administrator" can enable and disable the UWF.

Note

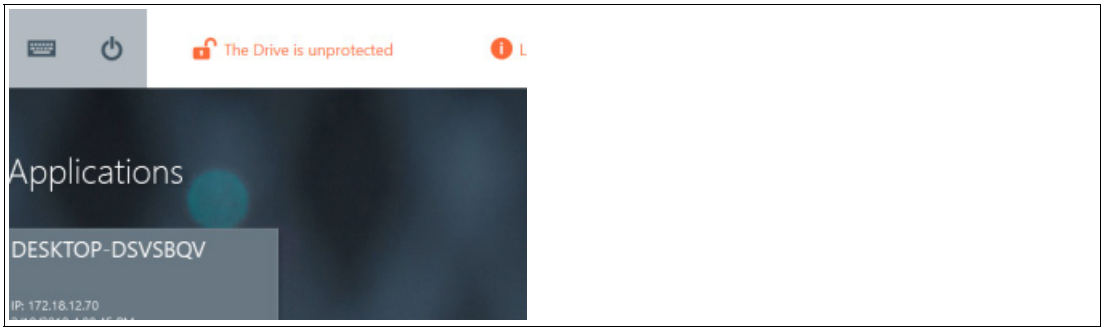
3rd Party Software

When using 3rd party software (e.g. antivirus software), verify if the software is compatible to the UWF and does not write large amounts of data onto the hard drive.

Enabling and Disabling the UWF

1. Click the "Power" icon at the top-left corner of the VisuNet RM Shell home screen.  .
2. Select **Protect Disk and Restart** to enable the UWF or **Unprotect Disk and Restart** to disable the UWF.

   ↳ After restart, the change will be in effect. An icon at the top of the home screen indicates whether the UWF is enabled.



2022-02

5 About App

The first tile in the application area on the home screen is the "About" app. This tile gives you a brief overview of system information.

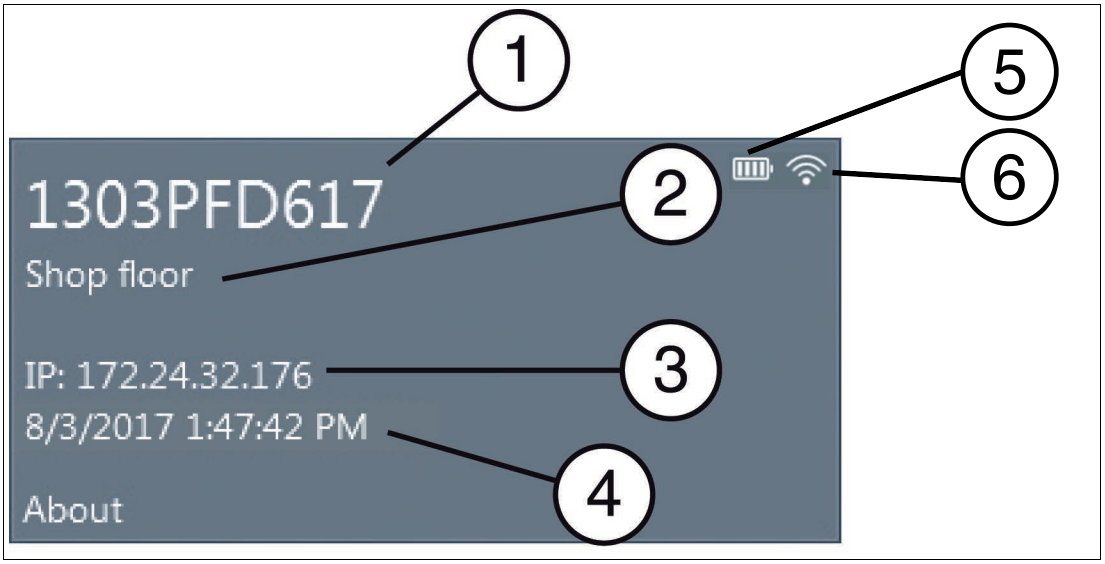


Figure 5.1 The "About" tile on the home screen

No.	Description
(1)	Computer name of the RM / BTC, see chapter 8.1
(2)	RM / BTC description, see chapter 8.1
(3)	IP address of the RM / BTC, see chapter 8.8
(4)	Current date and time, see chapter 8.1
(5)	Battery Status (Status indicated by hovering over the icon with your mouse)
(6)	Wi-Fi™ Status (only available for VisuNet RM Shell installed on Pad-Ex®)

For additional information, click the "About" tile.

After clicking the tile, you will see 5 submenus in the navigation bar:

- Pepperl+Fuchs SE – this submenu provides information on the Pepperl+Fuchs Group
- DRDC information - for further information refer to our VisuNet RM Shell DRDC manual at pepperl-fuchs.com/hmi
- (Submenu for GXP-specific information),
- Hardware,
- Licenses, see chapter 5.2
- Software,
- Touch

5.1 Hardware

This submenu provides information on the built-in "Hardware" components ("Processor", "Chipset", "Installed RAM", "Last boot up time") and the "Serial Number" of the VisuNet RM Shell.

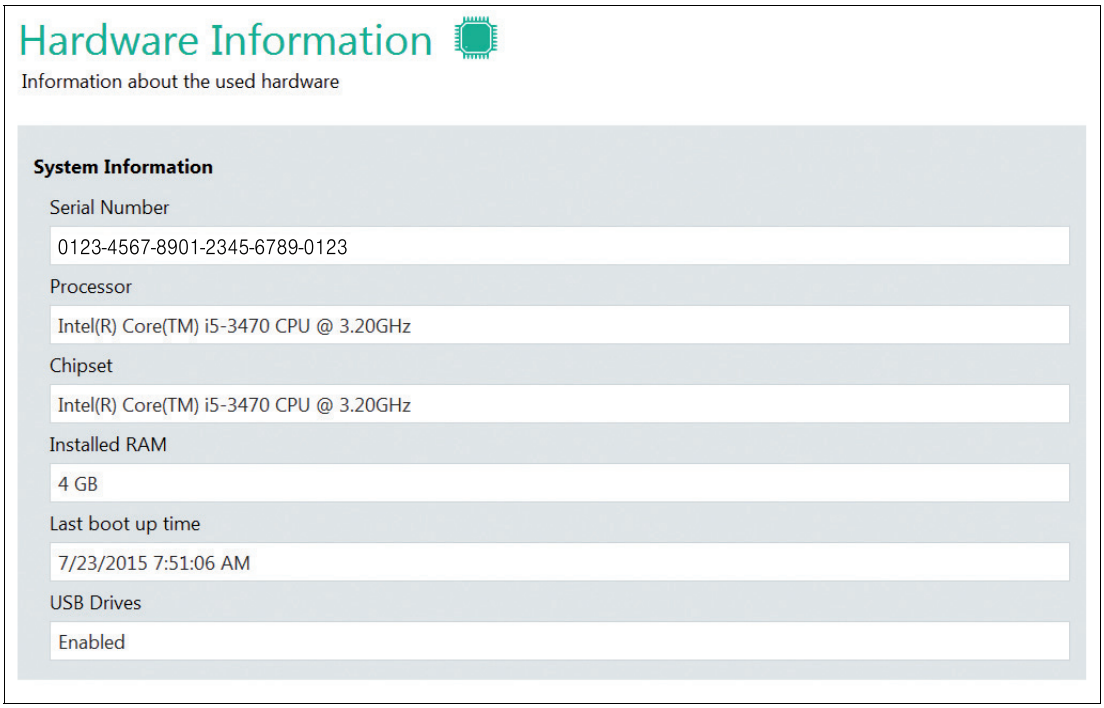


Figure 5.2 Information on the system hardware

5.2 Licenses and Terms of Use

This submenu provides license information for the RM Shell and third-party components.

For more information on the Pepperl+Fuchs End User License Agreement, see chapter 12.3.

5.3 Software Information

This submenu provides information on the "RM Shell" version, "Operating system", "System Status", and "Loaded Assemblies".

The current VisuNet RM Shell version can be useful when updating the firmware. The other information may be necessary for technical support.

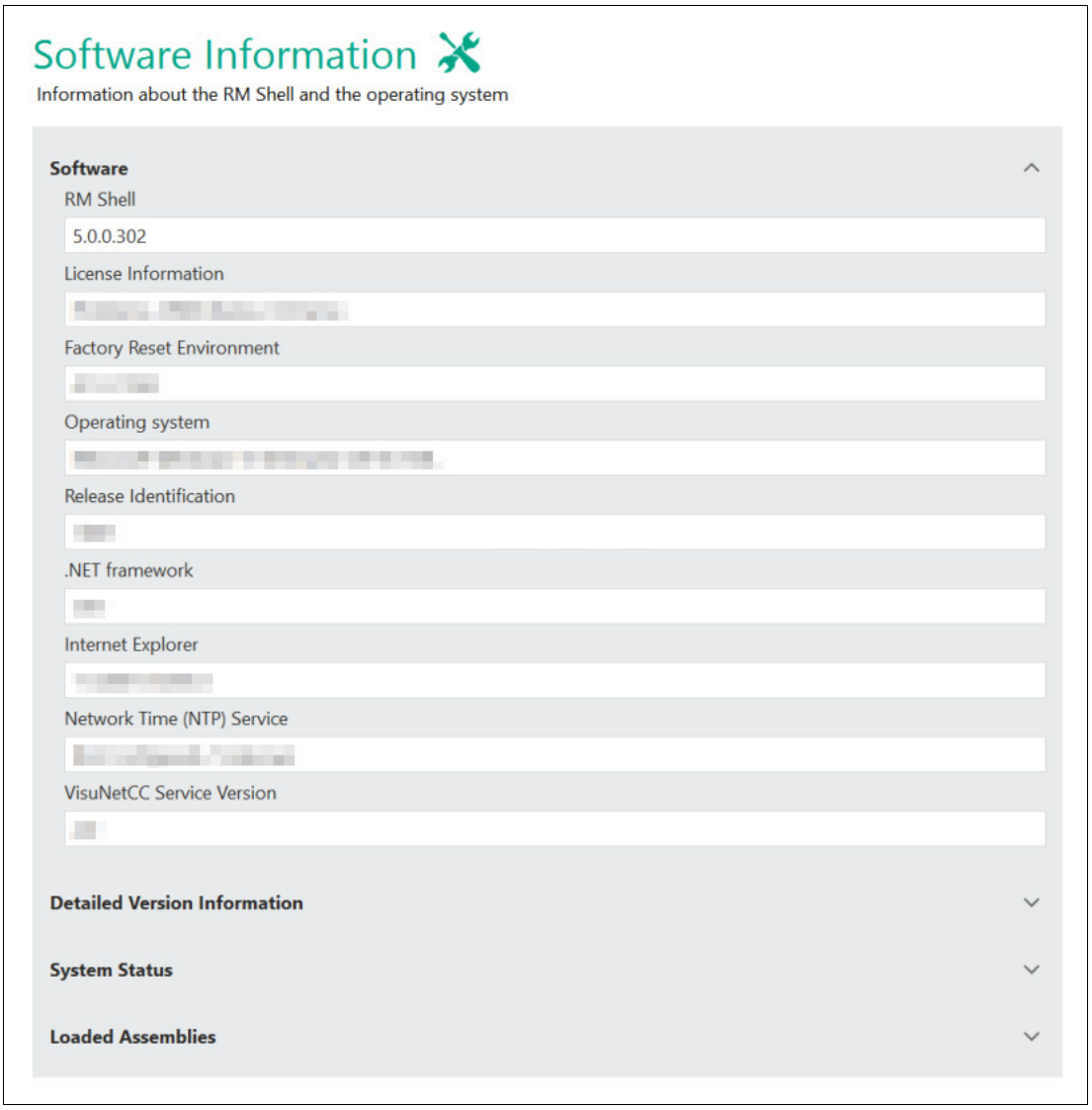


Figure 5.3 Software information

6 Profiles Management App

Create and manage remote "Connection Profiles" with the "Profiles Management" app.

VisuNet RM Shell does not come with any pre-created connection profiles. For this reason, the profiles list is empty when you start VisuNet RM Shell for the first time.

Note

Disable Write Filter for Persistent Storage of Configurations

To persistently store configuration changes, disable the unified write filter (UWF). Once you have implemented the configuration changes, enable the UWF again to persistently store the changes.

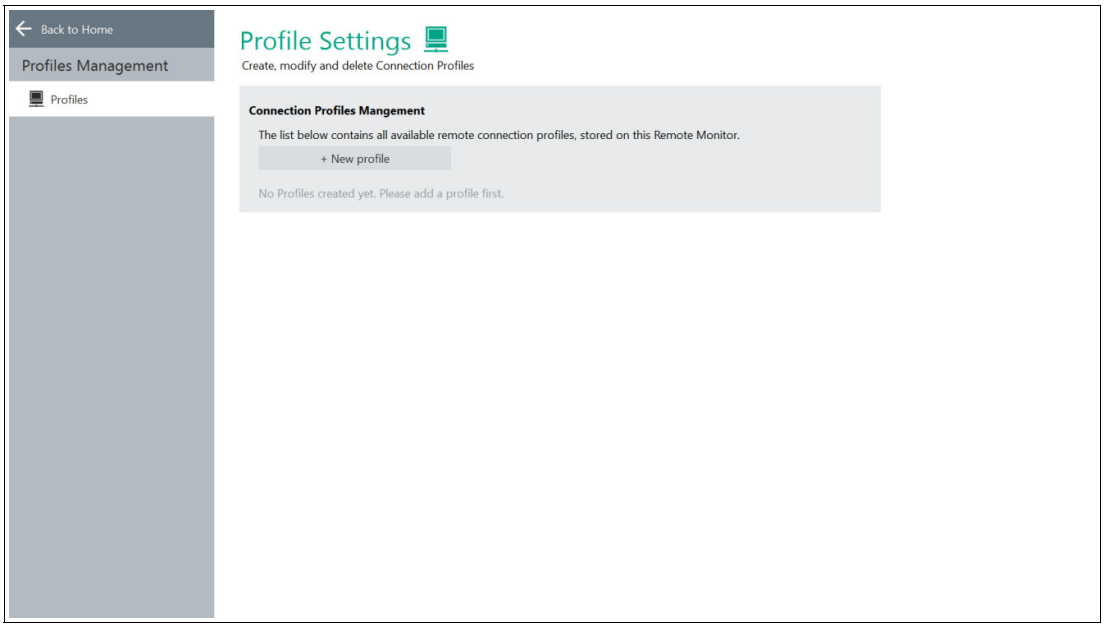


Figure 6.1 Profiles management home screen. Initially, the profiles list is empty.

Opening the Profiles Management App

1. To open the "Profiles Management" app, click the appropriate icon on the home screen.

.

Creating a New Connection Profile

1. To create a new connection profile, click + New profile.
2. Select your required connection "Profile" type and click **Ok**. [1]

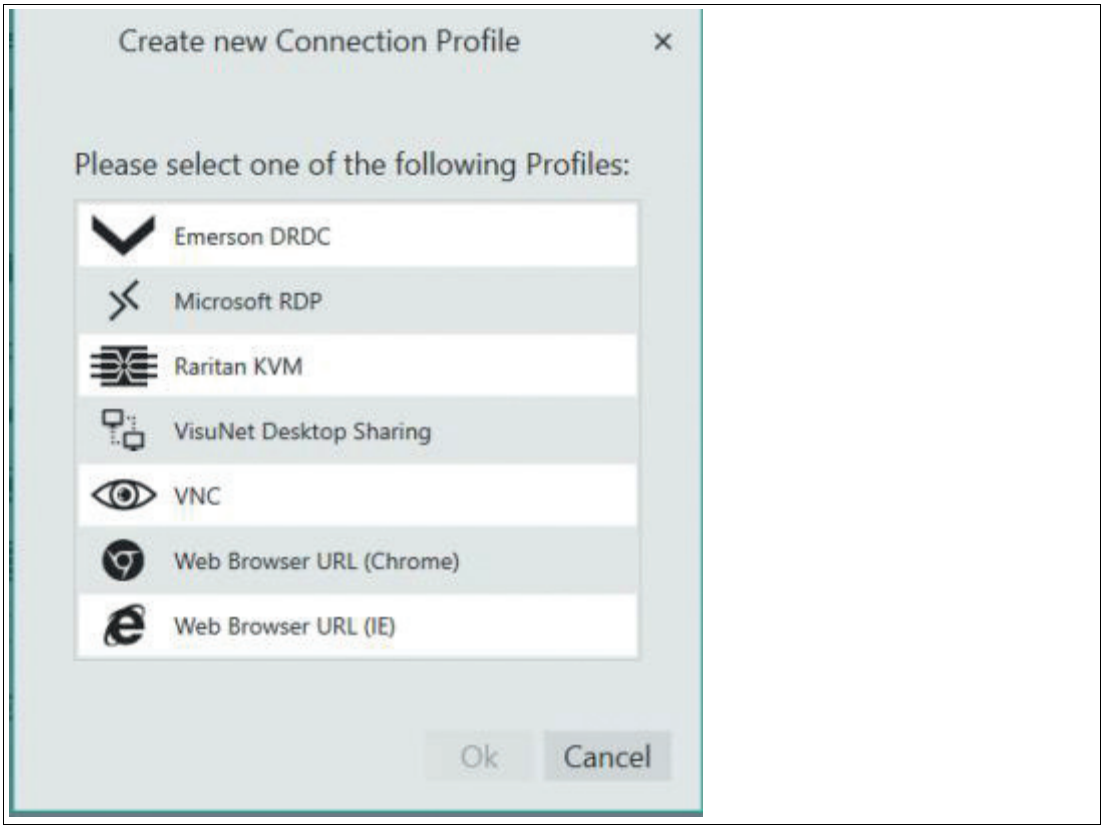


Figure 6.2 The "Create new Connection Profile" dialog box

↳ The selected connection profile has been created. The new profile's main settings open.

1. Web browser, Raritan KVM and VisuNet desktop sharing profiles are only available in the pro version

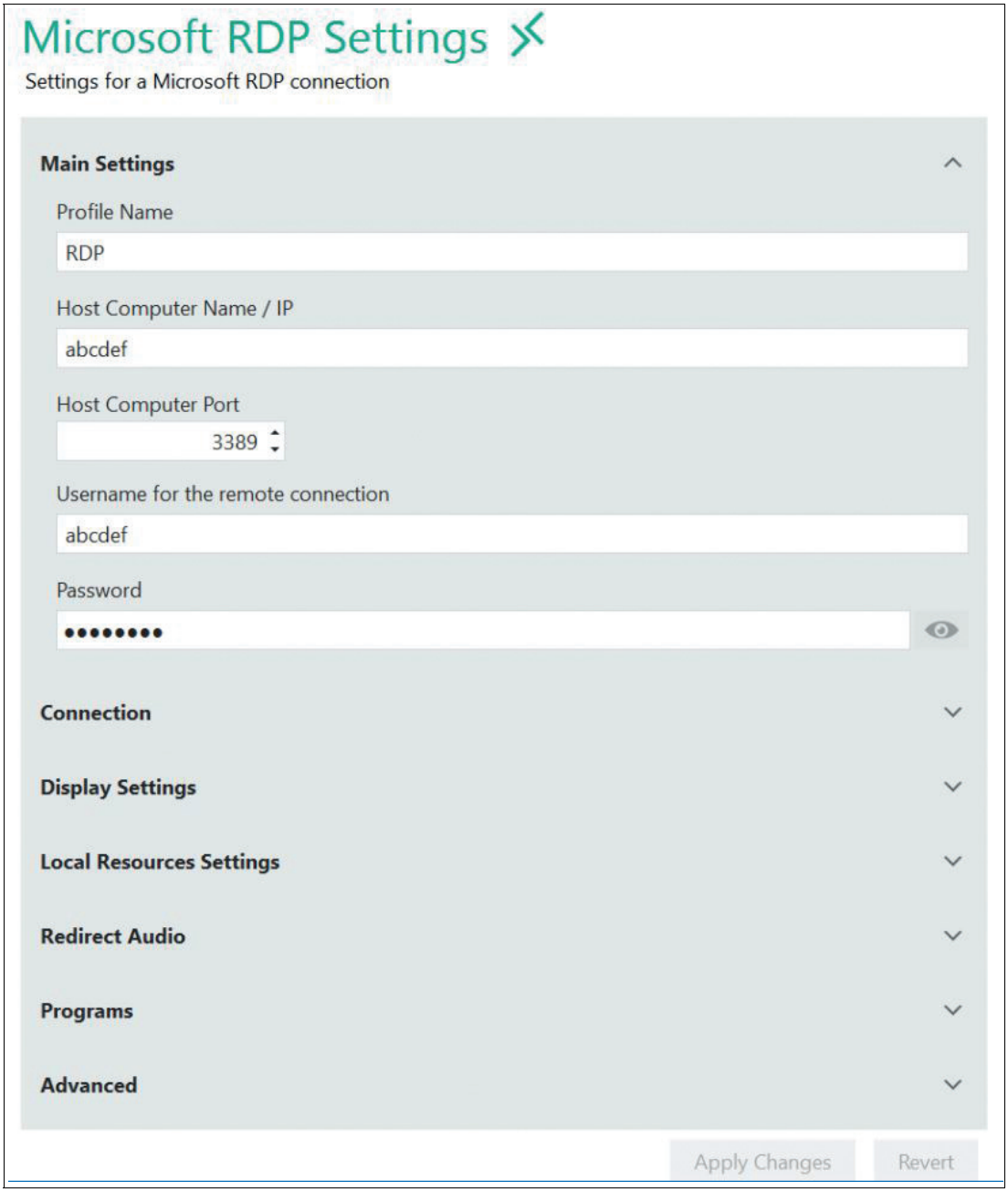


Figure 6.3 Main settings of a Microsoft RDP profile

Editing the Profile Settings

1. Go to "Profile Settings".
2. To edit the settings of a profile, double-click the requested profile entry in the profiles list or click  .
3. The settings vary according to the chosen connection type. After you have edited the settings, click Apply Changes.

   ↳ The changes have been saved.

2022-02

Note

Use the "Advanced" button to get forwarded to the corresponding Windows® Settings

Tip

Use the additional software VisuNet Control Center to easily copy and paste profiles or even clone one device with different profiles and profile settings to multiple devices within the network. Get further information of VisuNet CC at pepperl.fuchs.com

6.1 Connection Features

For each profile in the profiles list, you can set up 3 additional features.

- Auto Connect
- Retry
- Backup Connection

"Auto Connect" Feature

If you want an automatic connection to a specific profile, use the Auto Connect function. RM Shell establishes a connection to the selected profile automatically after a preconfigured time.

Setting up Auto Connect

1. Go to Profile Settings.
2. To set up the auto connect for a profile, click  .

   ↳ The "Connection Features" dialog box opens.
3. Check the "Enable Auto Connect" box.

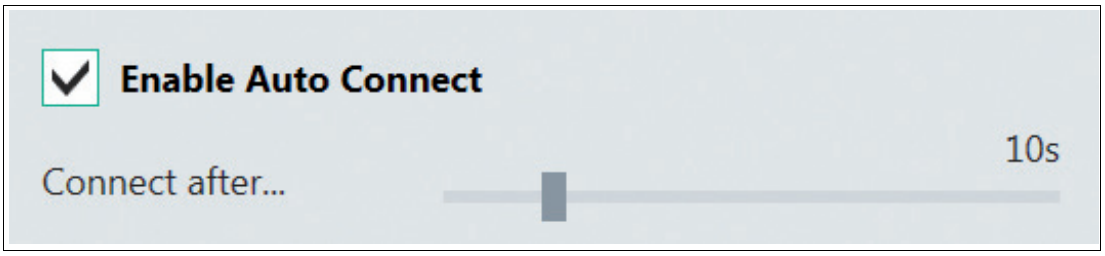


Figure 6.4 Auto connect options

4. Use the slider to adjust the time after which the VisuNet RM Shell automatically establishes a connection to the requested profile.
5. Click "OK."

   ↳ The auto connect has been preconfigured. The profiles list is shown.

Figure 6.5 Profile with preconfigured auto connect (as shown in the profiles list): in this example, VisuNet RM Shell automatically establishes a connection to the RD - 2 profile after 10 seconds.

Note

If you do not want your operator to access the RM Shell interface, you can set up "Connect after..." to 0 seconds. The corresponding profile will automatically connect immediately after booting the RM / BTC without showing the RM Shell home screen.

"Retry" Feature

In case a connection to a host gets lost, the "Retry" feature attempts to reconnect to the host. You can specify both a limited number of retries and the time between them.

Setting Up Retry Feature

1. Go to Profile Settings.
2. To set up the retry feature for a profile, click .

   ↳ The "Connection Features" dialog box opens.
3. Check the "Enable Retry" box.

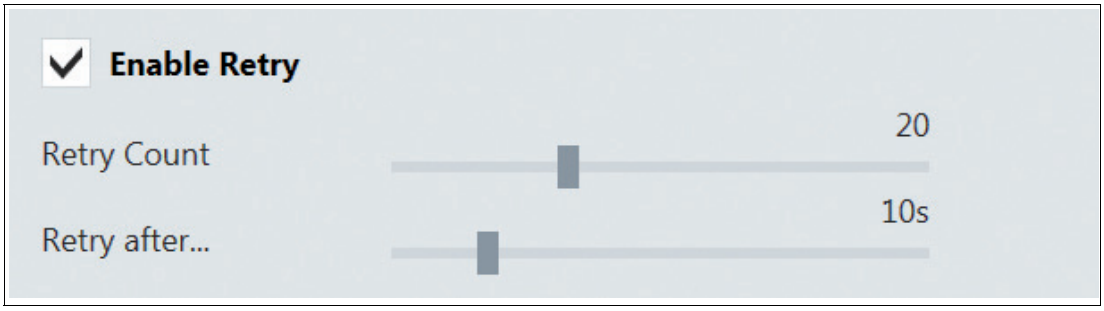


Figure 6.6 Retry options

4. Use the "Retry Count" slider to adjust the number of retries.
5. Use the "Retry after..." slider to adjust the time between retries. The default values are 10 retries with a 10 second break between each retry.
6. Click "OK."

   ↳ The retry feature has been set up. The profiles list is shown.

"Backup Connection" Feature

In case a connection to the host gets lost and cannot be reconnected by the "Retry" feature, you can set up another profile as a backup.

Setting Up Backup Connection

1. Go to Profile Settings.
2. To set up the backup connection feature for a profile, click  .

   ↳ The "Connection Features" dialog box opens.
3. Check the "Enable Backup Connection" box.

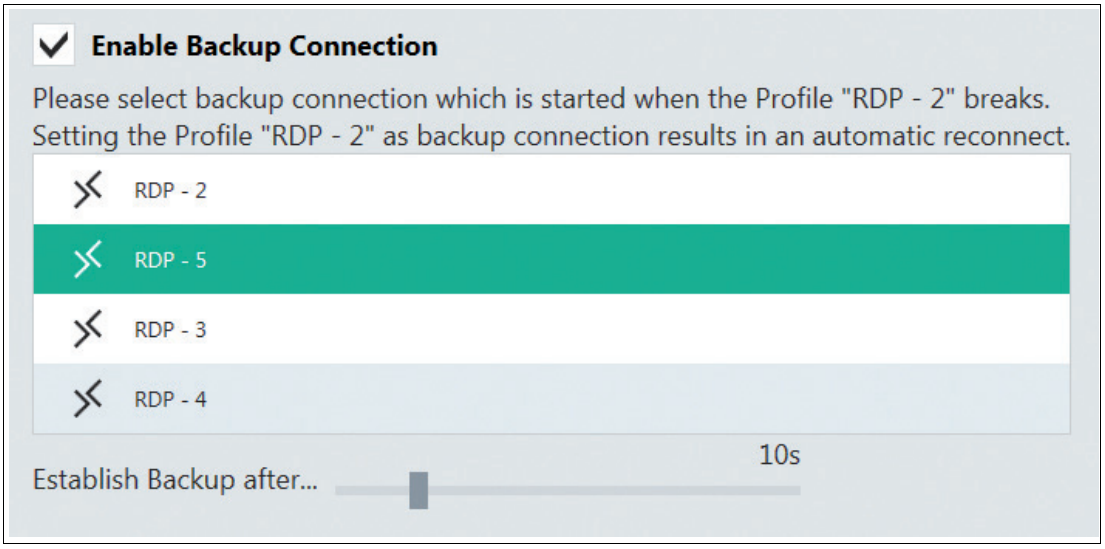


Figure 6.7 Backup connection options

4. Choose a backup profile from the list that will be started if the connection of the selected profile fails.
5. Use the "Establish Backup after..." slider to adjust the time before the backup profile connects to the host.
6. Click "OK."

   ↳ The backup connection has been set up. The profiles list is shown.

Example 1 – Connecting Continuously to a Specific Host (via "Backup Connection" feature)

In this example, the RM / BTC connects automatically to a predefined host A. If the connection fails, the RM / BTC will continuously try to reconnect to host A.

Use case: If security or software updates are installed on the host system and the host needs to be restarted, this function ensures that the RM / BTC automatically reconnects to the host when it is rebooted.

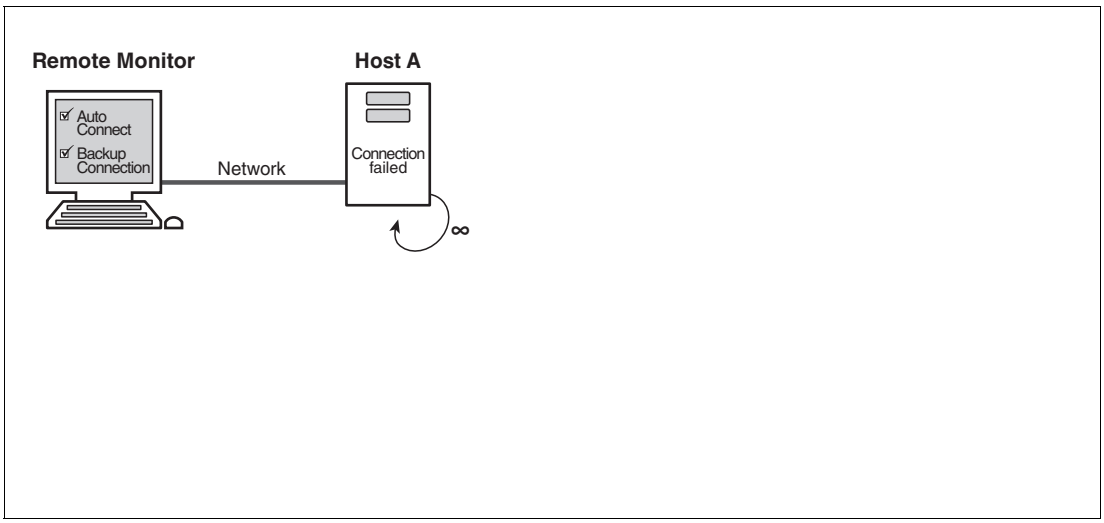
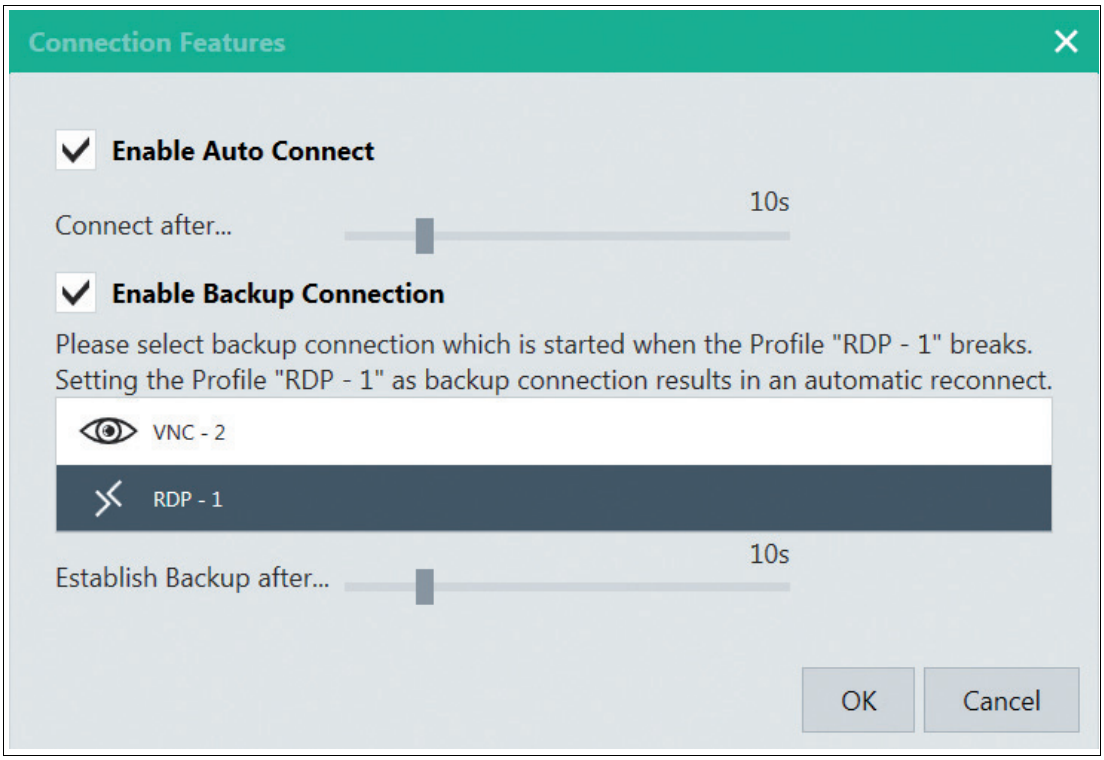


Figure 6.8 Example 1 - Unlimited number of retries to a specific host (with "Backup Connection" feature)

Setting Up a Continuous Connection to a Specific Host

1. Go to RM Shell's profile management, choose the profile you want to set to unlimited connection retries, and click .
2. Enable "Auto Connect" feature.
3. Use the slider to adjust the time after which VisuNet RM Shell automatically establishes a connection to the requested profile.
4. Enable the "Backup Connection" feature.



5. Choose the same profile as backup profile (in this case "RDP - 1").
6. To save the changes and return to the profiles list, click "OK."

Example 2 – Connecting Continuously to More Than One Host (via "Backup Connection" Feature)

In this example, the RM / BTC connects automatically to a predefined host A. If the connection fails, the RM / BTC will try to connect to the profile's backup connection (in this case, "host B") after a predefined waiting time. If host B is also not reachable, the RM / BTC will try to connect to the host B profile's backup connection (in this case, "host C"). You can easily create "loops" of backup connections for your profiles. In this example, the backup connection of host C is host A again.

Use case: If you have an infrastructure with redundant servers, you can set up the RMs / BTCs to connect to a backup server if the main server fails.

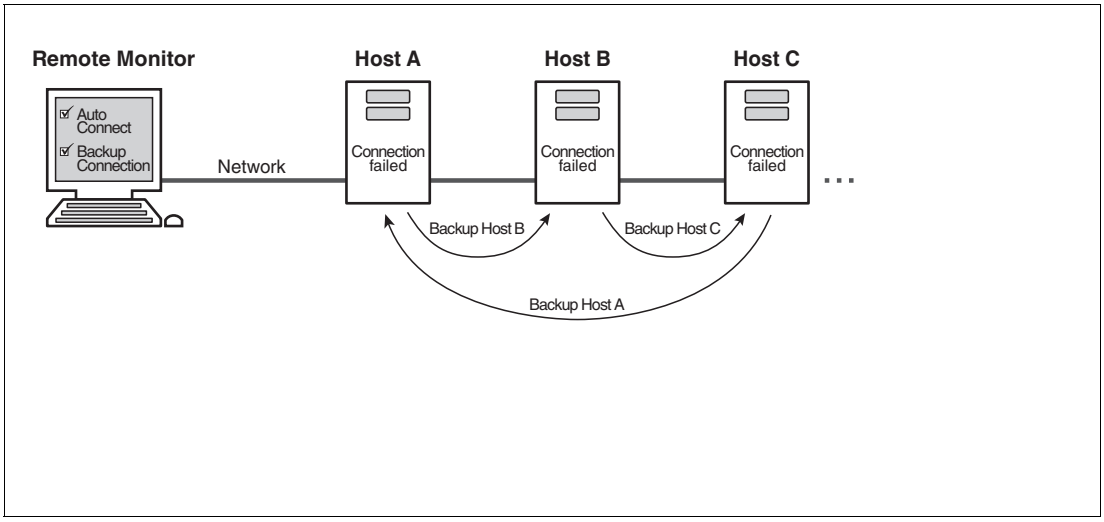
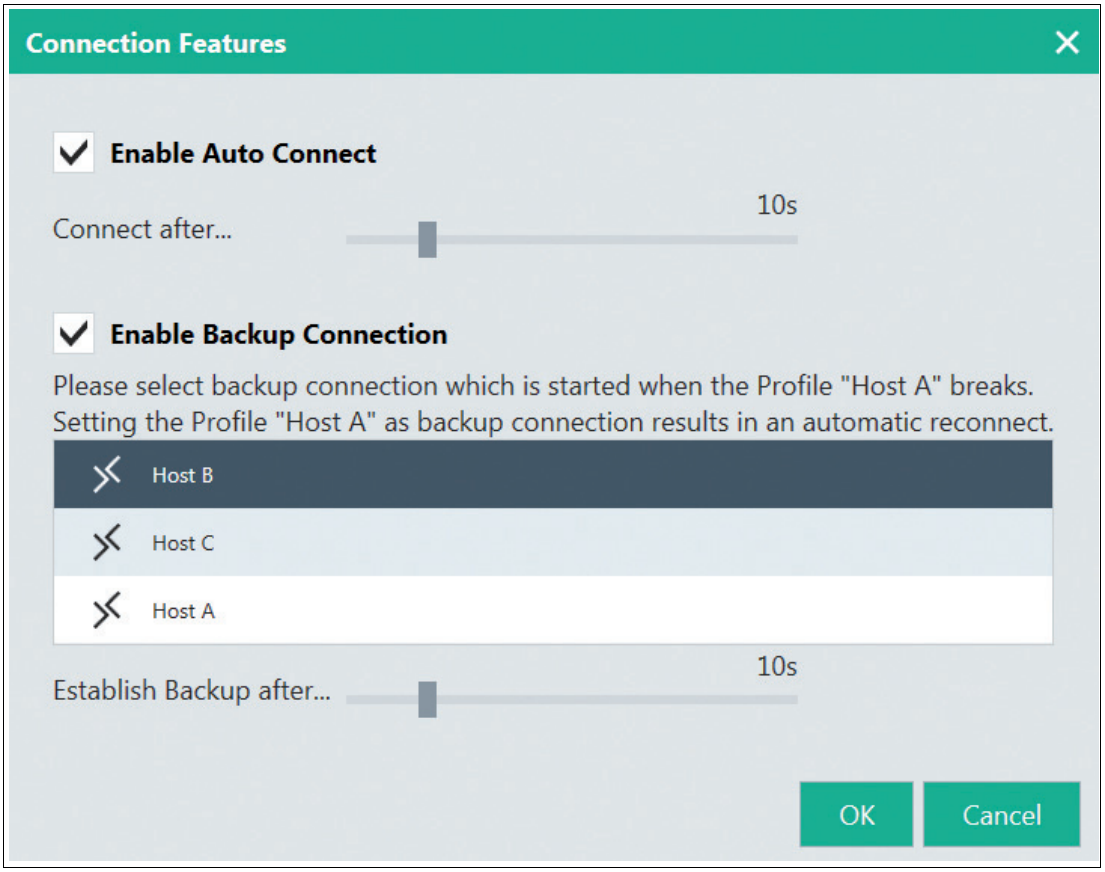


Figure 6.9 Example 2 - unlimited number of connection retries to more than one host (via "Backup Connection" feature)

Setting Up a Continuous Connection to More Than One Host

1. Go to RM Shell's profile management, choose the profile you want to set up (e.g., "host A"), and click .
2. Enable "Auto Connect" feature.
3. Use the slider to adjust the time after which RM Shell automatically establishes a connection to the requested profile.
4. Enable the "Backup Connection" feature.
5. Choose the first backup profile (in this case, "host B").



6. To save the changes and return to the profiles list, click "OK."
7. Go to RM Shell's profile management, choose the first backup profile you want to set up (e.g., "host B"), and click .
8. Enable the "Backup Connection" feature.
9. Choose the second backup profile (in this case, "host C").
10. Repeat the above steps for all backup profiles you want to set up.
11. For the "last" backup profile (in this case, "host C"), define the origin profile (in this case "host A") as backup profile to ensure that the connection retry starts over if the connection has failed.
12. To save the changes and return to the profiles list, click "OK."

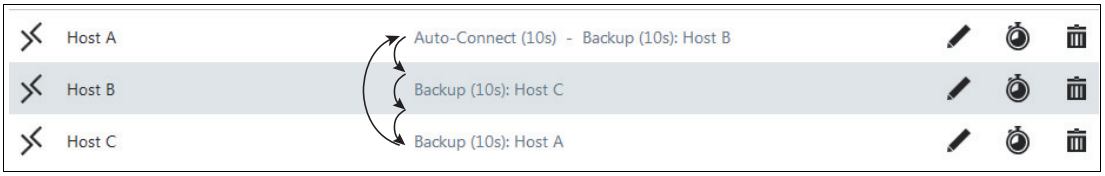


Figure 6.10 Profiles with backup connections

Example 3 – Limited Number of Connection Retries to the Same Host (via "Retry" Feature)

In this example, the RM / BTC connects automatically to a predefined host A. If the connection fails or gets lost, the RM / BTC will try to reconnect to host A 3 times. If the connection cannot be established, the RM / BTC will not connect to host A after the third retry. After the third retry fails, the user automatically returns to the RM Shell home screen.

Use case: This enables the user to manually select an alternative connection if the main connection to host A failed.

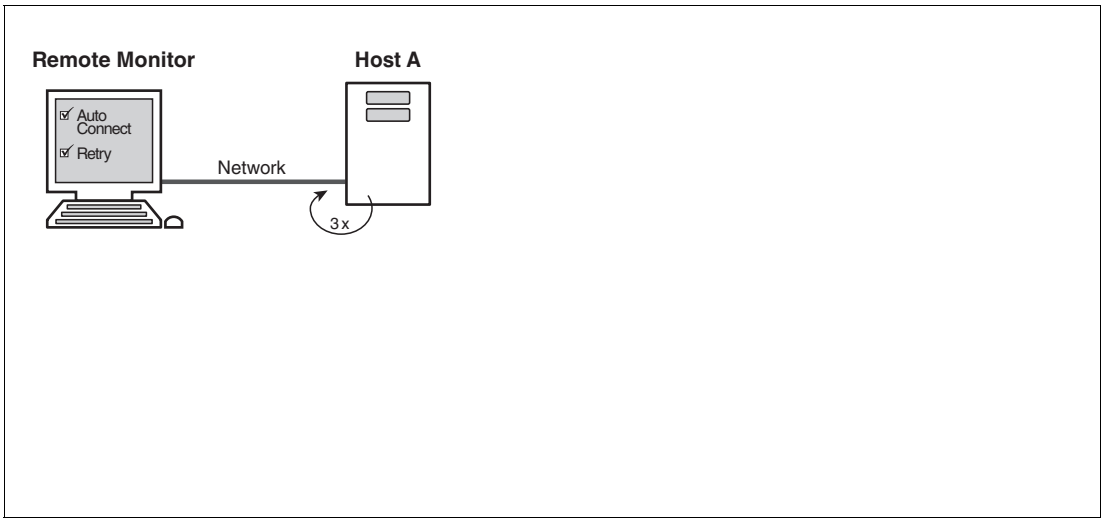


Figure 6.11 Example 3 - Limited number of connection retries to the same host

Setting Up Limited Number of Connection Retries to the Same Host

1. Go to RM Shell's profile management, choose the profile you want to set up, and click .
2. Use the slider to adjust the time after which VisuNet RM Shell automatically establishes a connection to the requested profile.
3. Enable the "Retry" feature.

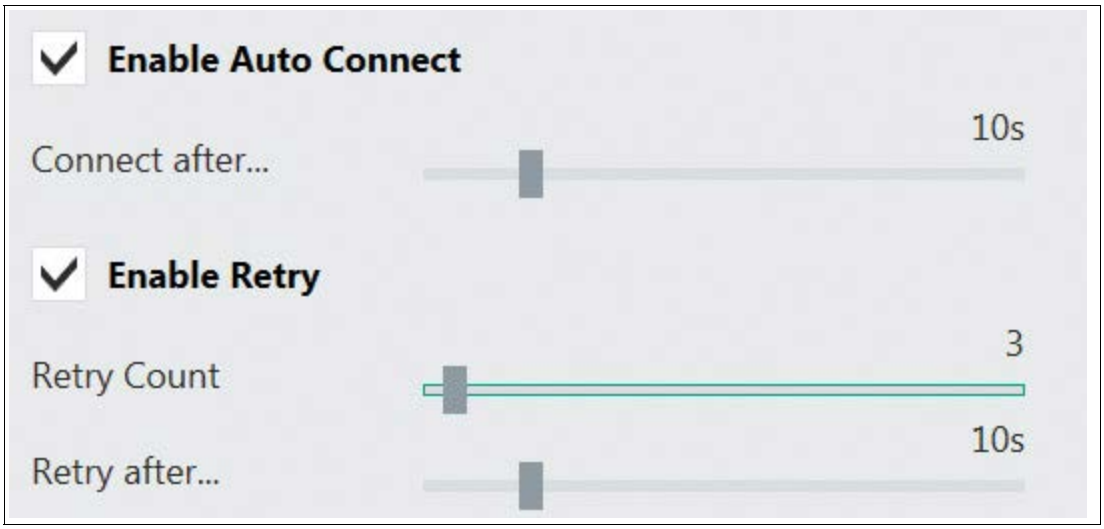


Figure 6.12 Corresponding settings in the VisuNet RM Shell (profile settings - connection features)

4. Use the "Retry Count" slider to adjust the number of retries.

2022-02

5. Use the slider to adjust the time after which VisuNet RM Shell automatically attempts to reconnect to the host.
6. To save the changes and return to the profiles list, click "OK."

6.2 RDP Settings

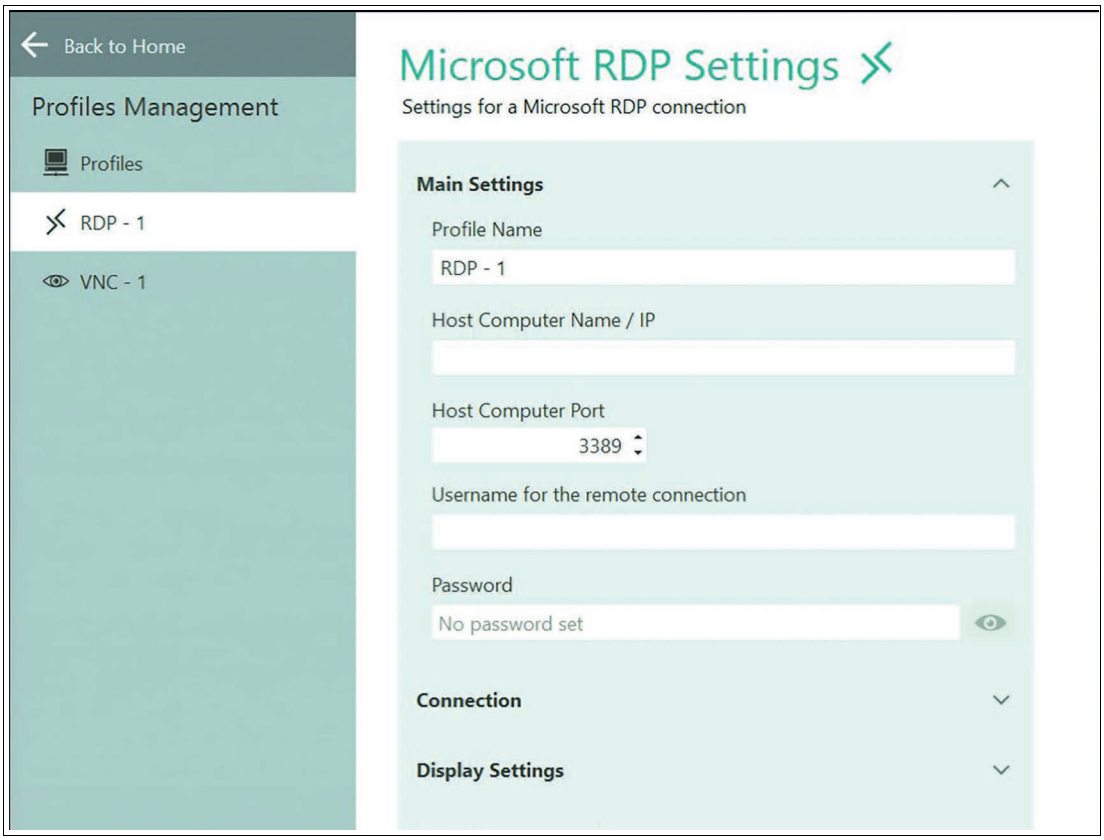


Figure 6.13

The RDP settings are grouped by type. Use the  icon to expand the sections.

Main Settings

Option	Description
Profile Name	Allows you to change the visible name of the selected profile.
Host Computer Name/IP	This can be the network name of the host or its IP address.
Host Computer Port	The port of the host. We recommend using the default setting.
Username for remote connection	Username that is used to log in to the host.
Password	Password that is needed to log in to the host.

Connection

Option	Description
Choose connection speed	This does not set the connection speed but the User Interface (UI) settings recommended for this speed. Several visual effects are activated or deactivated for the host, depending on the chosen connection speed. The chosen speed may diminish the performance of the RM / BTC.
Fast Disconnect Detection by sending Pings to Host Server	By enabling this option, the RM constantly sends pings to the host. Possible connection failures are detected much quicker than usual. To use this function, the host must accept pings.
Enable Auto-Reconnect of the RDP connection (disable Fast Disconnect Detection)	Enable this option to use the RDP's built-in connection recovery mechanism. This mechanism also tries to reestablish a remote desktop connection when it is disturbed.
Send Keep Alive Telegrams to the RDP server	This function keeps the connection between the RM / BTC and the host alive. It does this by sending messages from the RM / BTC to the host in case of inactivity.
Enable Idle Timeout on the RDP server	Enable this function to define the timeout inactivity period after which the RM / BTC is disconnected from the host.
Enable Connect to Administrative Console Session	Enable this setting when you want to remotely administer a Windows® Server 2008-based server (with or without Terminal Server installed). However, if you are connecting to remotely administer a Windows® Server 2008-based server that does not have the Terminal Server role service installed, you do not have to specify the /admin switch. (In this case, the same connection behavior occurs with or without the /admin switch.) For more details, please refer to following 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	Enable this option to prevent a connection window from being closed.

Display Settings

Option	Description
Fullscreen Mode	Enable this option to display the remote desktop in full size. If you want to set the remote desktop screen size manually, disable the option.
Remote Color Depth	Select the color depth of the remote desktop connection from the drop-down list.
Enable scale down of larger remote screens	Enable this option to ensure that the entire remote desktop is shown in the client by scaling the content down.
Display connection bar	Enable this option to show the connection bar at the top of the screen. The connection bar fades out automatically after a few seconds. It fades in when you move the mouse to the top of the screen.

Local Resources Settings

Option	Description
Apply Windows® key combinations	Select one of the following options from the drop-down list • **On this computer**: Windows® key combinations always apply to your local computer • **On the remote computer**: Windows® key combinations apply to the desktop of the remote computer • **Only when using full screen**: Windows® key combinations apply to the remote computer only when the connection is in full screen mode
Select local resources and devices that are used on the host	Enable the local resources and devices you wish to be available on the host.

Redirect Audio

Option	Description
Remote audio playback	Decide from which device whether this computer or on the RM / BTC Sound should be played back. Per default the sound is disabled.
Record local audio and send to remote computer	e.g. you want to forward your local microphone recordings to the server

Note

Memory Leak in Microsoft® RDP may cause "Out of Memory" when audio redirection and 24/7 operation is enabled. We do not recommend enabling this feature.

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

Programs

Option	Description
Start the following application on the remote computer	This will automatically start an application located on the host PC after the user has logged into the session. Remote Apps are supported on Windows Server 2008 and newer. Contact your System administrator on how to configure RDP Remote Apps.

Advanced

Option	Description
Authentication	• No authentication of the server • Server authentication is required and must complete successfully for the connection to proceed • Attempt authentication of the server. If authentication fails, the user is prompted with the option to cancel the connection or to proceed without server authentication
Use the Credential Security Support Provider (CredSSP) for authentication if available	Use this option for backwards authentication compatibility with some older RDP servers.

Option	Description
Enable client to detect and forward double-clicks to the server	Enable this option to allow the RM devices to detect, interpret, and forward double-click events to the remote host.
Load system-wide installed RDP Plugins	Allows using on the system installed and registered RDP "Remote Desktop Services virtual channels" (PRO license required)

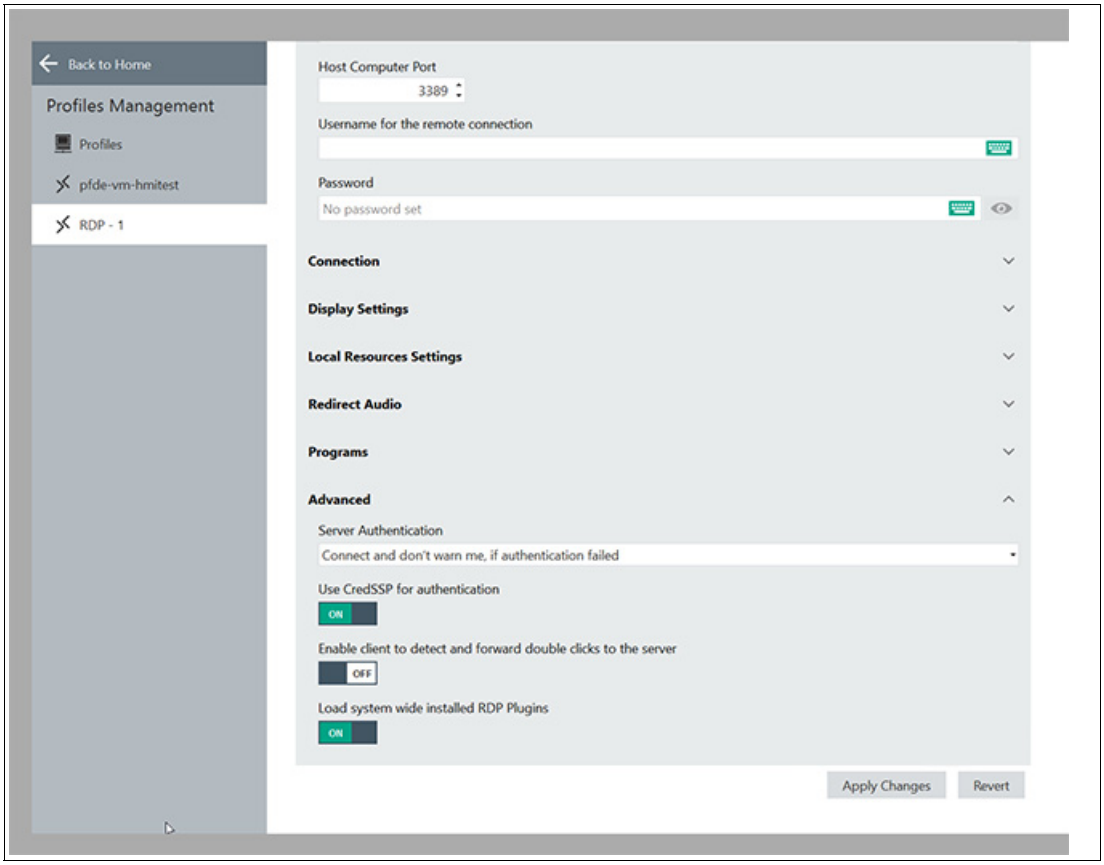


Figure 6.14

6.3 Raritan KVM Settings

This section describes the configuration of the KVM-over-IP profile for Raritan KVM-over-IP switches.

Note

The VisuNet RM Shell 5.2 and newer has been tested and qualified with the Raritan Dominion® KX IV-101 KVM-over-IP switch that is available as an accessory (DKX4-101; #70118493). A separate Quick Installation Guide with the configuration steps for the Raritan Dominion® KX IV-101 KVM-over-IP switch is available online (https://www.pepperl-fuchs.com/global/en/classid_2547.htm?view=productdetails&prodid=100044#documents).

Note

The KVM-over-IP client requires an VisuNet RM Shell PRO License to be unlocked.

KVM Profile Settings

When the Rartan switch is configured, a new KVM connection profile can be created in VisuNet RM Shell 5.2 and newer. This profile allows a connection to be established to the host PC that is connected to the Raritan KVM switch.

Note

Ensure that the Raritan Dominion KVM Switch is configured properly and that the Direct Port Access (DPA) is enabled before you create a Rartitan KVM profile.

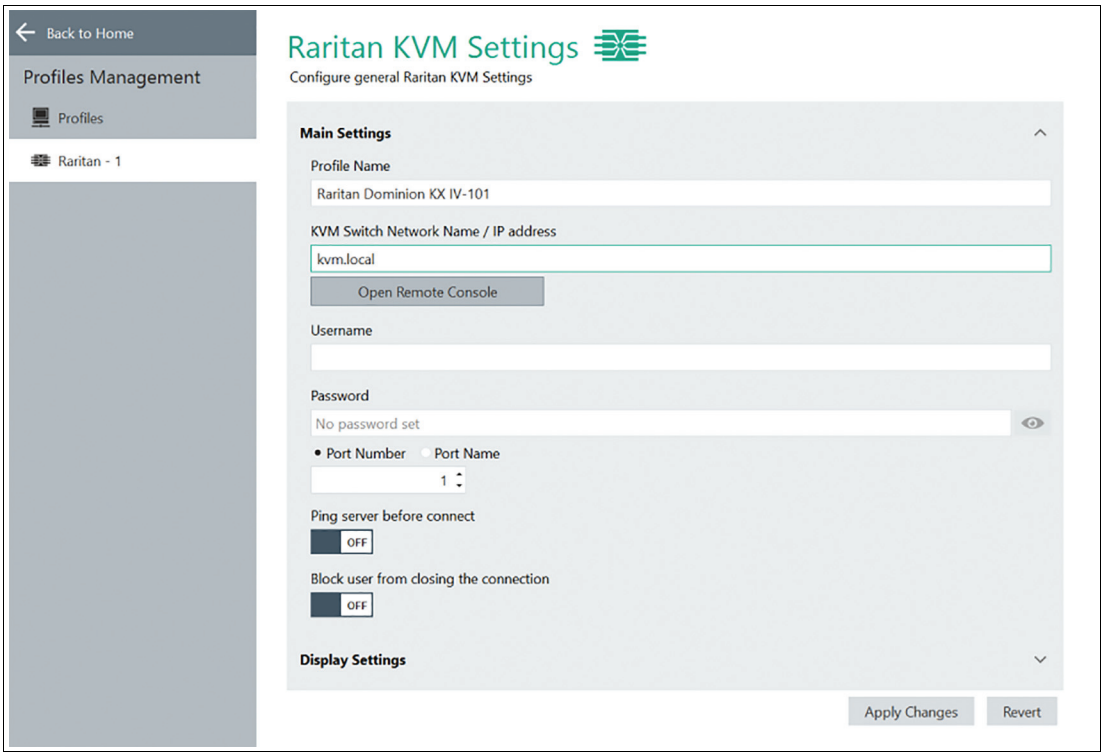


Figure 6.15 Raritan KVM Settings

General Settings

Option	Description
Profile Name	Name of the KVM connection profile that is presented on the home screen.
KVM Switch Network Name / IP address	Per default the DHCP is enabled. Ensure that you use the following Network Name to setup the first connection: **kvm.local** Refer to the Raritans manual if you require a static IP.
Username	User name that is stored on the Raritan KVM switch that you want to connect to. Default User DKX4-101: **admin**
Password	Password of the user that is stored on the Raritan KVM switch that you want to connect to. Default password DKX4-101: **raritan** (for user “admin”)
Port Number/Port Name	This setting can be used on Raritan multi-port KVM-over-IP switches to select the port number you want to connect to.
Ping server before connect	Use the ping mechanism to check whether the device is available before connecting.
Block user from closing the connection	This function removes the "Close" function from the connection bar. Note that this function does not stop the user from closing the connection via other client mechanisms, e.g., the Raritan client menu bar.

Display Settings

Option	Description
Show the connection bar	Enable this option to show the connection bar at the top of the screen. The connection bar fades out automatically after a few seconds. It fades in when you move the mouse to the top of the screen

After configuring the connection profile as desired, click "Apply Changes."

6.4 VisuNet Desktop Sharing Settings

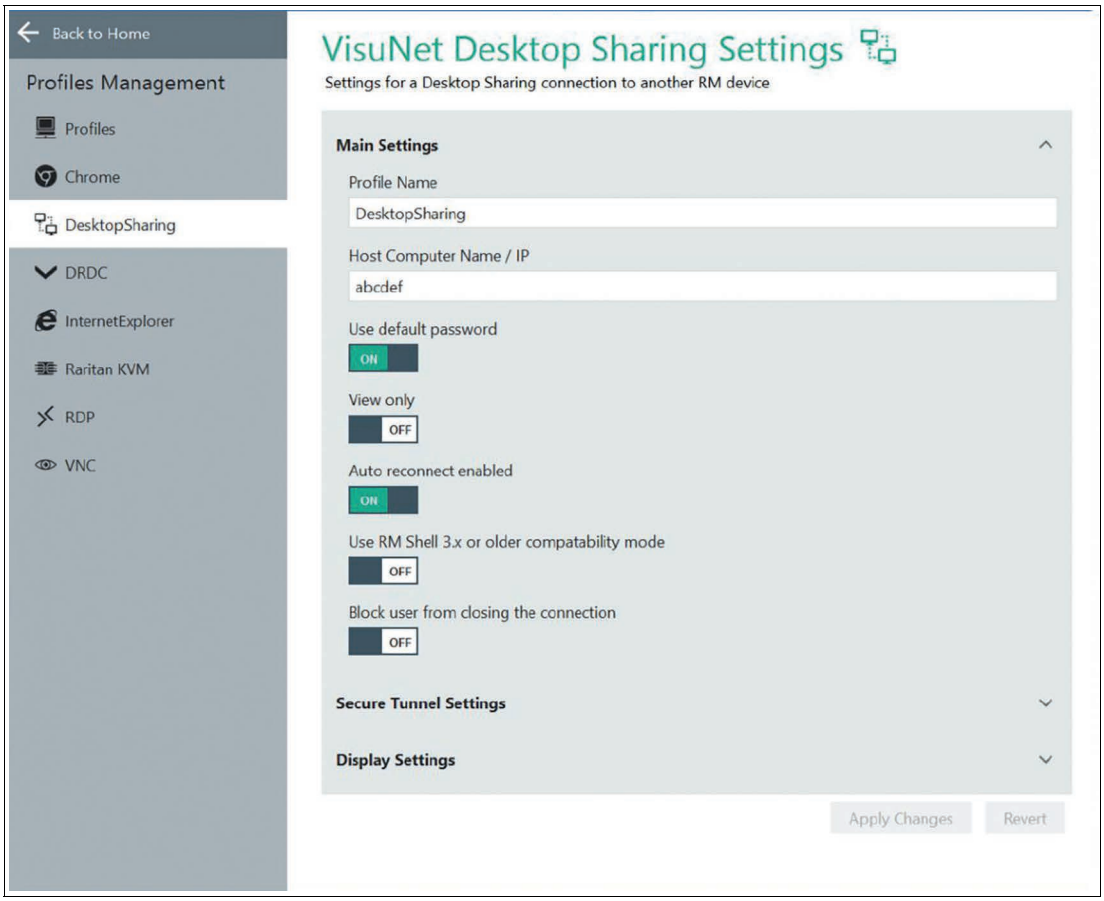


Figure 6.16

Main Settings

Option	Description
Profile Name	Allows you to change the visible name of the selected profile.
Host Computer Name / IP	Enter the host computer name or the IP address of the RM Master. If you use your own certificate for secure tunnel session shadowing the host computer name and the certificate common name need to be identical.
Use default password	Disable this function to set your own password.
View only	Enable this function to allow only reading access. If enabled, there is no mouse functionality or keyboard input.
Auto reconnect enabled	Enable this function to reconnect automatically to the RM Master if the connection is lost.

2022-02

Option	Description
Use RM Shell 3.x or older compatibility mode	In an older version of RM Shell (version 3.x), a feature called "Clone Display" exists. You can mirror a monitor with this feature, too. Enable the "Use RM Shell 3.x or older compatibility mode" to make an RM master with RM Shell 3.x compatible to RMs with RM Shell 5.
Block User from closing the connection	Enable this option to prevent the user from opening a connection window.

Secure Tunnel Settings

Option	Description
Enable Secure Tunnel	Needs to be enabled to use the secure tunnel service function
Secure Tunnel Port	We recommend to use the default Tunnel Port
Accept embedded self-signed certificate only	When enabled, the default certificate, which is embedded into the RM Shell, will be accepted. If you use your own certificate, we recommend to disable this function.
Ignore certificate name mismatch error	We highly recommend to remain the default “off” setting
Ignore certificate chain error	We highly recommend to remain the default “off” setting

Display Settings

Option	Description
Screen stretching	Select an option from the dropdown list to choose screen stretching. 1. Resize the remote screen image to fill the local screen no matter what the actual aspect ratio is: the content is stretched to the size of the local screen. This may lead to distortion of the content. 2. Scale to as large an image as possible, but maintain the correct aspect ration: the content will be stretched as large as possible without any distortion of the aspect ratio. This may lead to black bars.
Cursor mode	Select an option from the dropdown list. • Track remote cursor locally. • Let remote server deal with mouse cursor. • Do not show remote cursor; no cursor is shown. Use "no cursor" as cursor tracking mode.
Cursor tracking mode	No cursor: no cursor available. Select this option for cursor mode "Don't show remote cursor". • Dot cursor: a dot is used as cursor. • Normal cursor: standard Windows arrow is used as cursor. • Small cursor: a smaller standard Windows arrow is used as cursor.
Display the connection bar	Enable this option to show the connection bar at the top of the screen. The connection bar fades out automatically after a few seconds. It reappears when you move the mouse to the top of the screen.

Building up a VisuNet Desktop Sharing connection with Secure Tunnel enabled

When building up a VisuNet Desktop Sharing connection from a client (device A) to a host (device B), both devices need to be configured. The settings can be performed directly at the devices within RM Shell or remote via VisuNet Control Center.

1. Enable VisuNet Desktop Sharing Server in the System Settings of the host (device B). The Secure Tunnel Service as well as the use of the default certificate will be enabled per default.

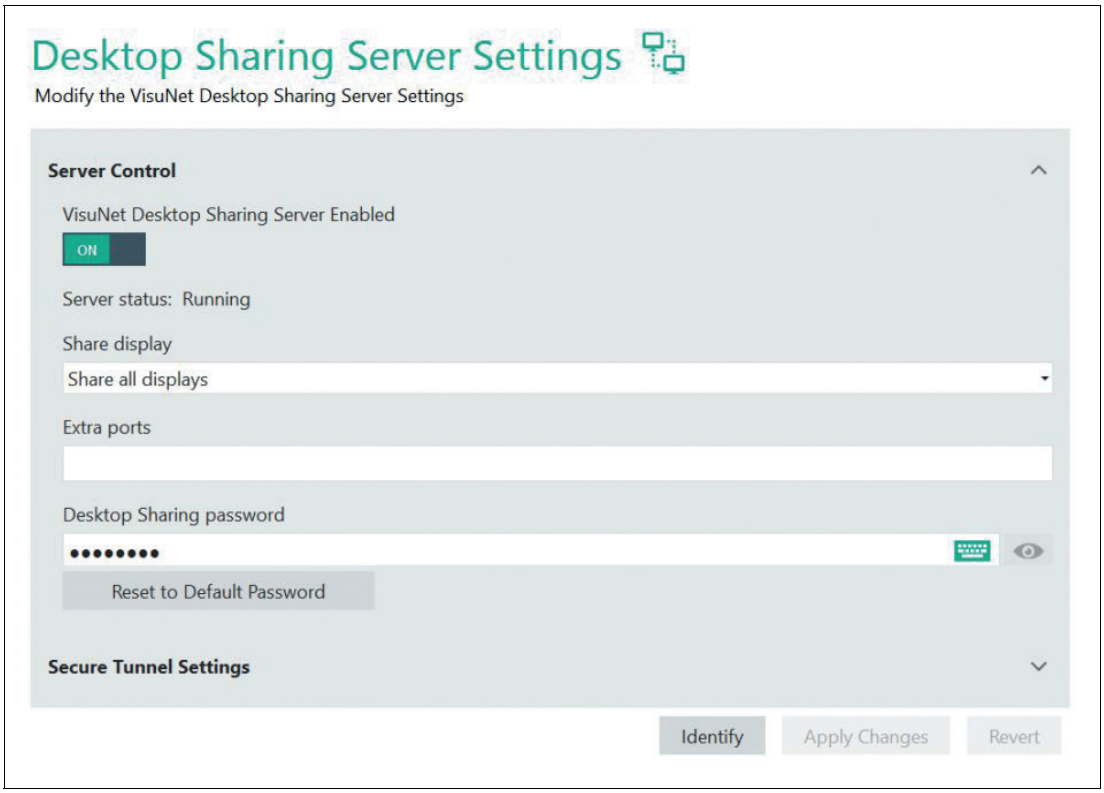


Figure 6.17

2. Upload your certificate with private key either from a connected USB device or via Share folder in the network to your host device B. The additional software VisuNet Control Center can be used to upload your certificate.
3. Open the Certficate Import Wizard by opening the certificate with the Windows explorer. Follow the guidance. Store the certificate on your local machine.

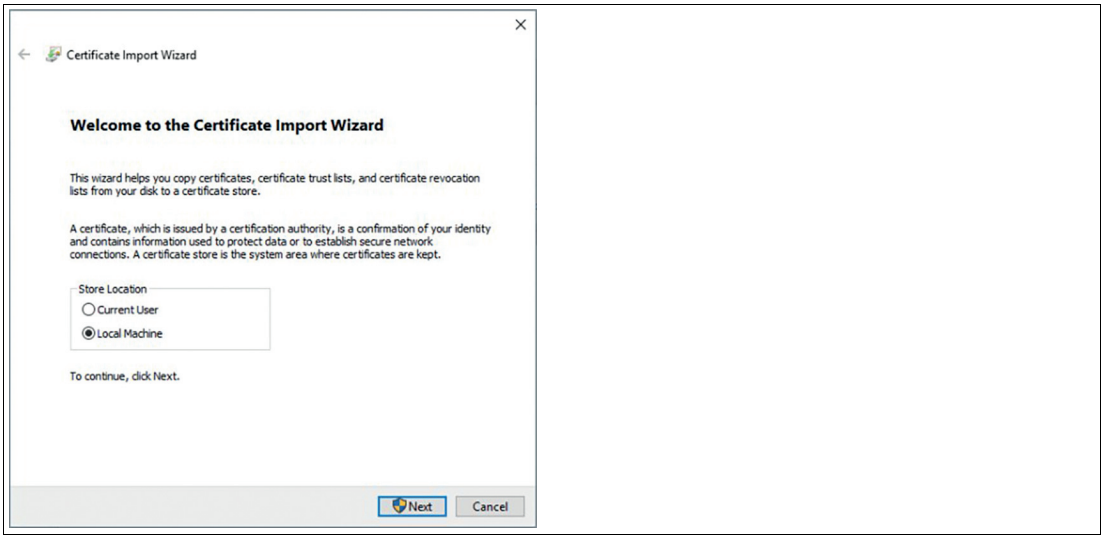


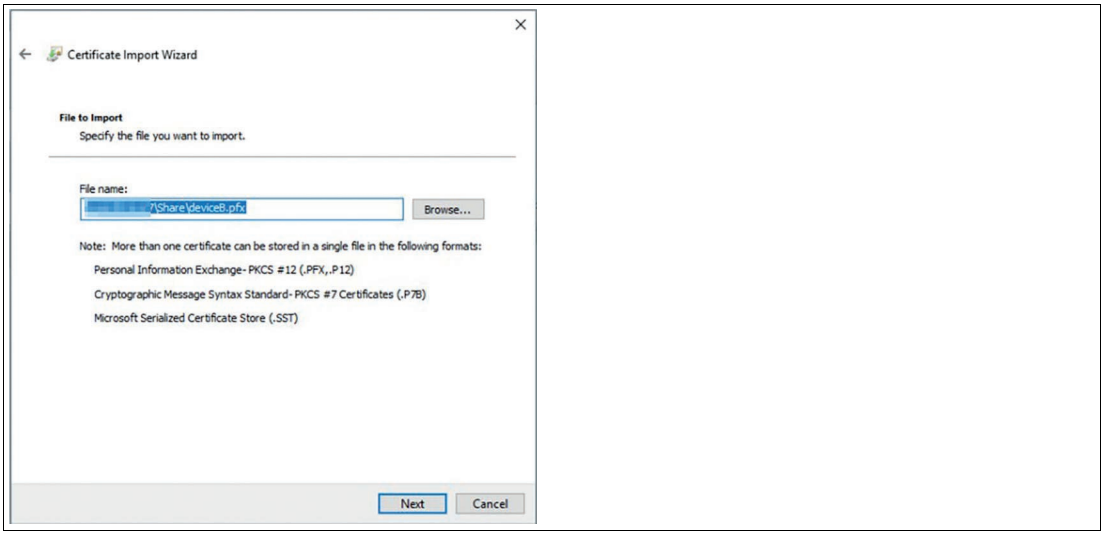
Figure 6.18

Caution!

Security

To further increase the security it is important to name the certificate the same name as your host device name.

4. Import the file to your host device B.



5. Enter the password. The password is set by the creator of the certificate.

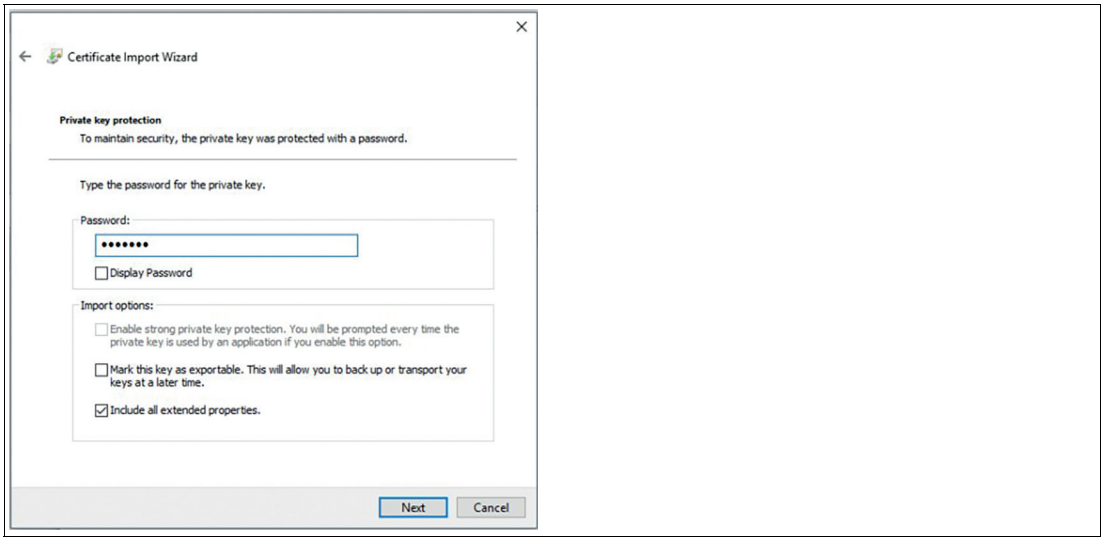


Figure 6.19

6. Choose the store your certificate should be stored in.

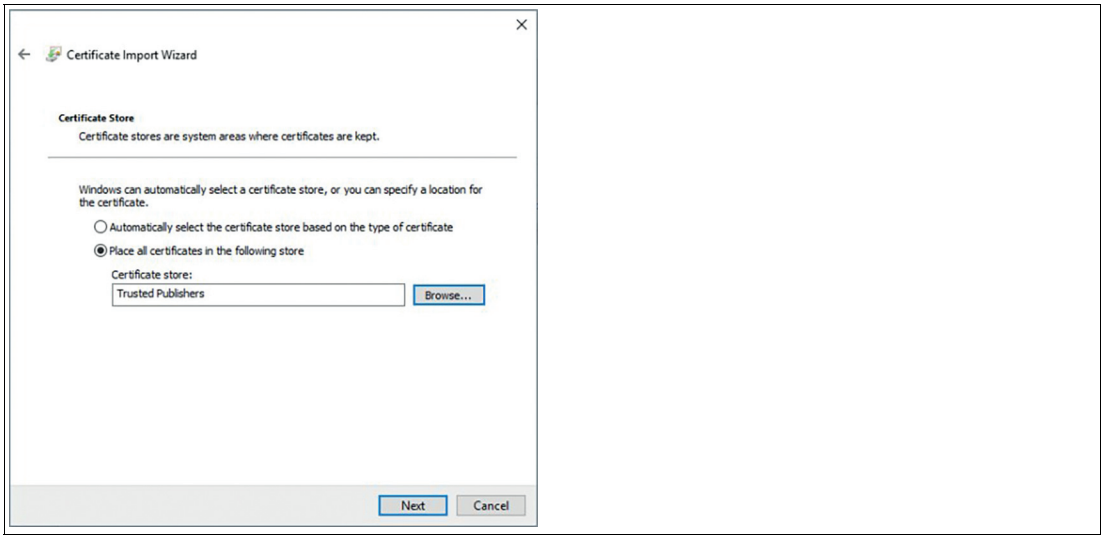


Figure 6.20

7. Check your final settings and finish the importing process by clicking “finish”.

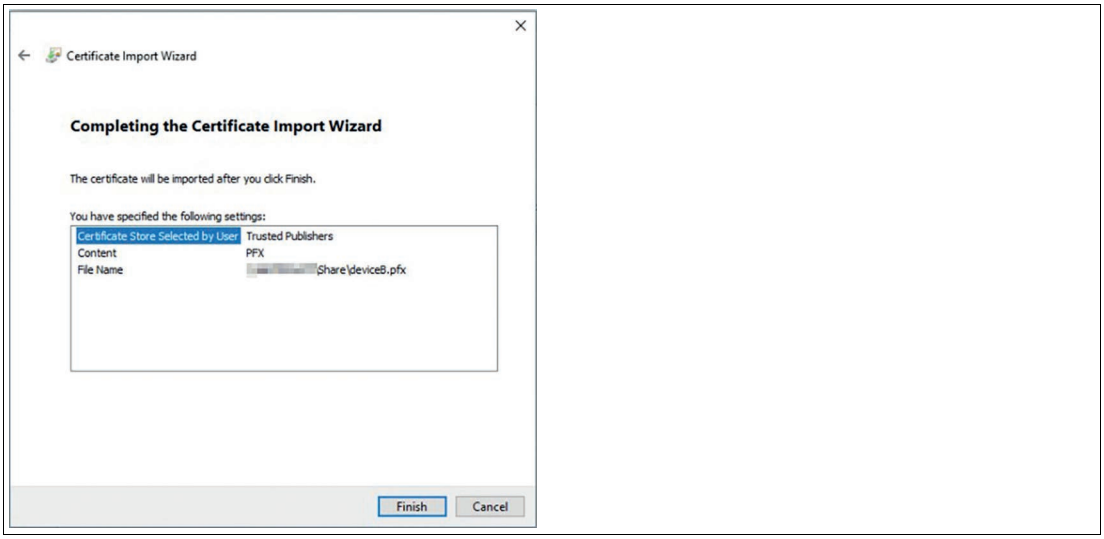


Figure 6.21

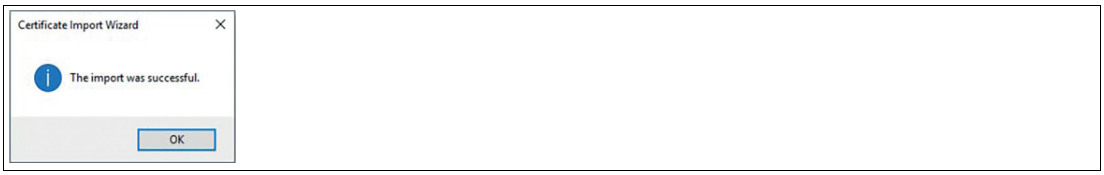


Figure 6.22

8. Refresh the list of your certificates and choose the imported certificate.

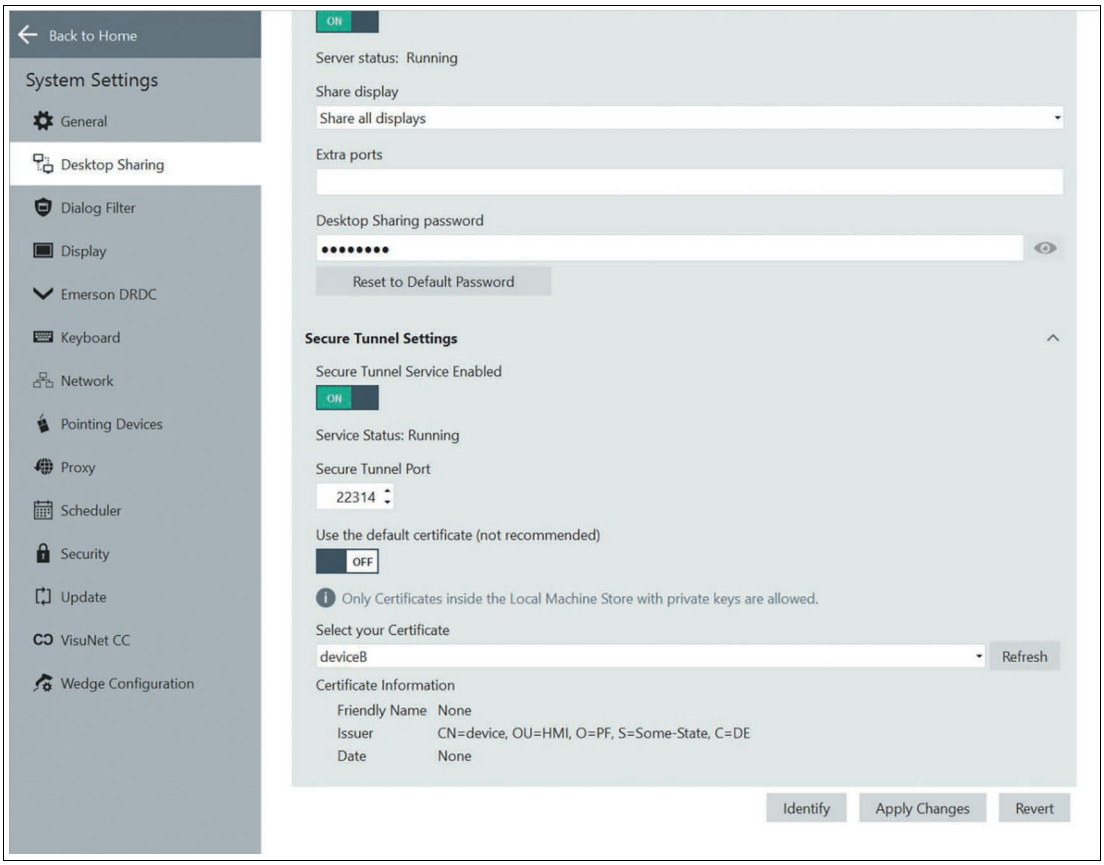


Figure 6.23

9. To save the changes, click "Apply Changes"

Configuration of client device A

To create an unbroken chain proceed now with the configuration of your client device A and install the public key certificate (root CA) on your client device A.

1. Open the certificate in the share folder via double click and open the Certificate Import Wizard by clicking “Install Certificate…”

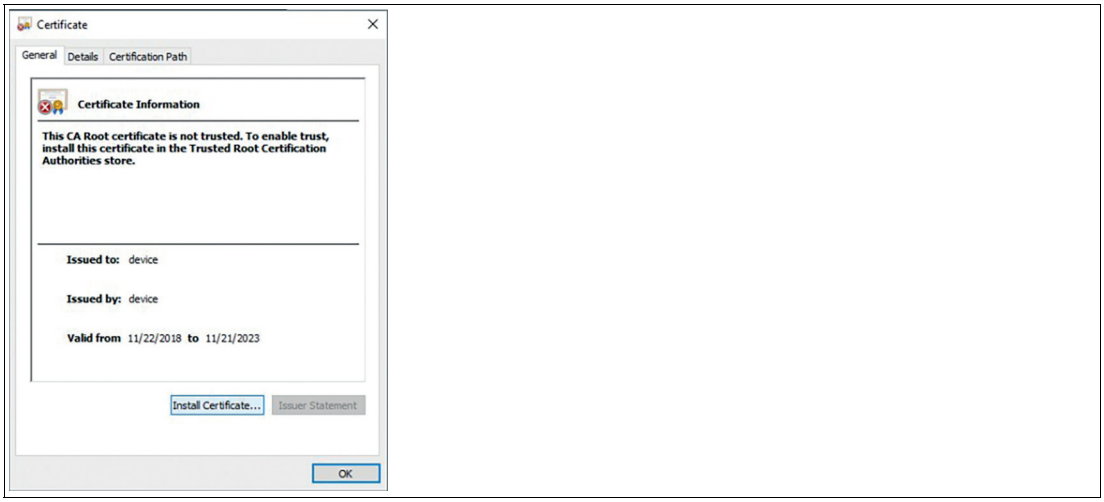


Figure 6.24

2. Follow the guided steps of the import wizard. Choose your store location and certification store and click "Next" to continue.

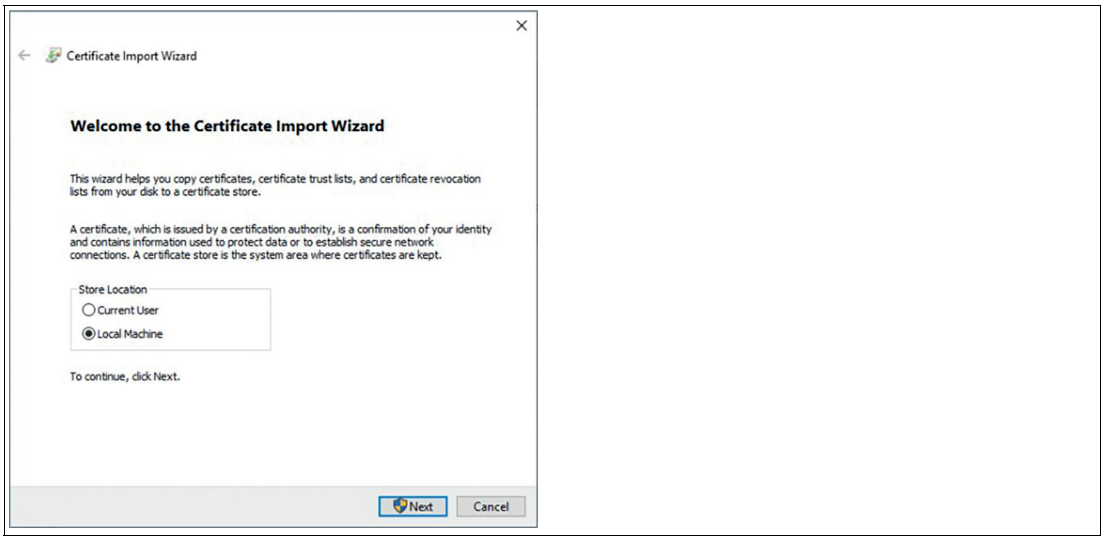


Figure 6.25

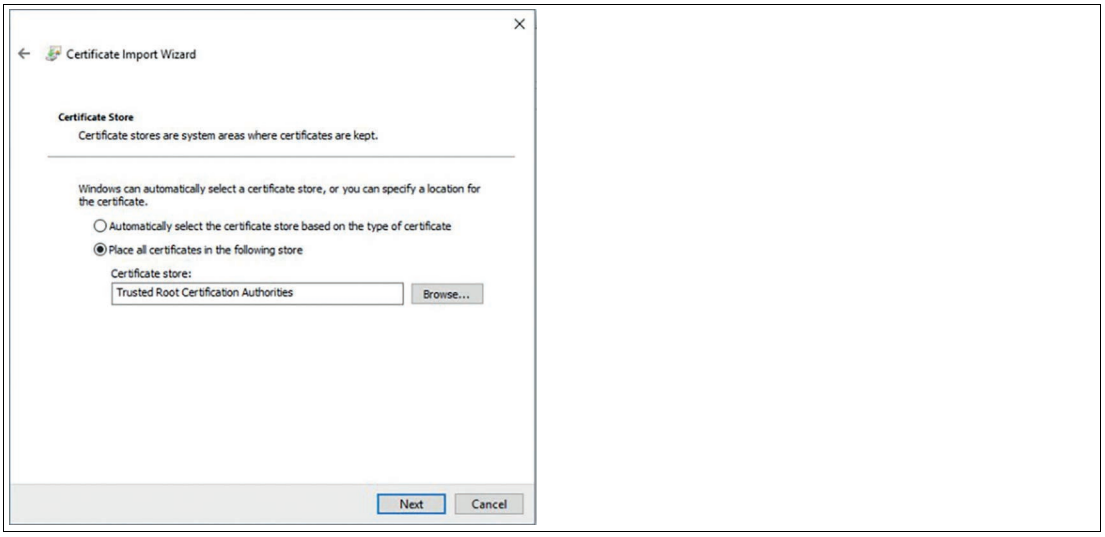


Figure 6.26

3. Before you complete the import of your certificate, you can double-check the specifications of your settings. Click "Finish" to complete your import.

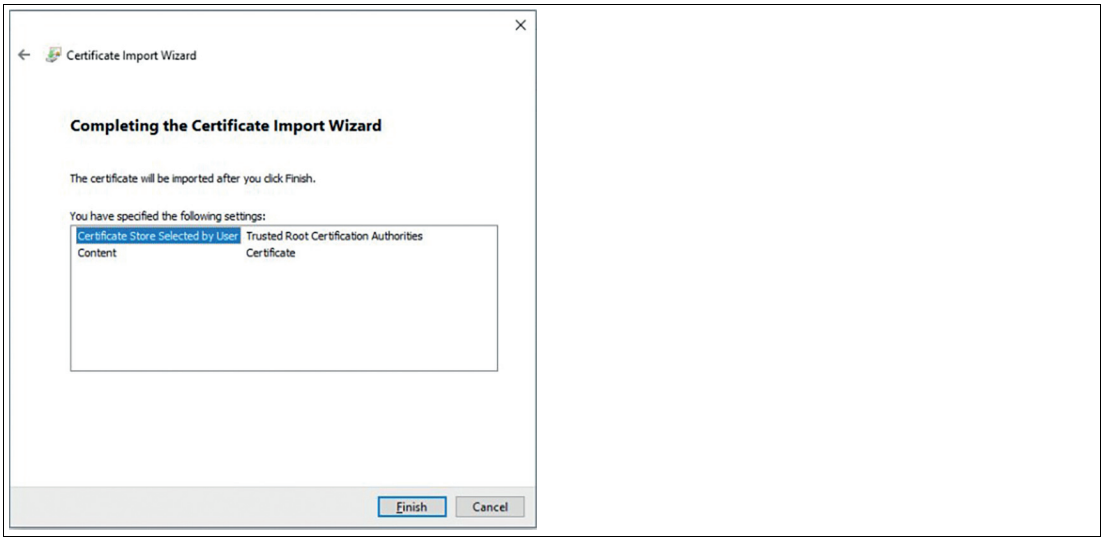


Figure 6.27

↳ If you completed all the implementations of the certificates successfully, no error message will appear when your remote observation starts.

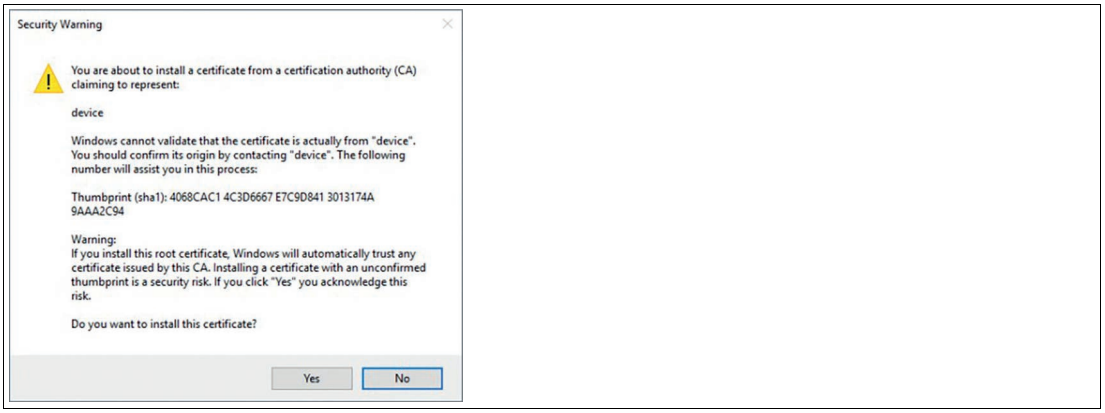


Figure 6.28

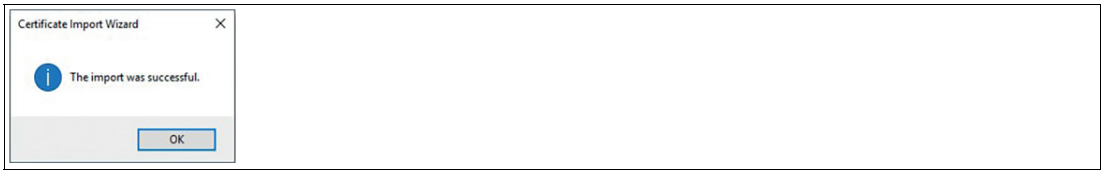


Figure 6.29

4. Create a new VisuNet Desktop Sharing Profile at your client device

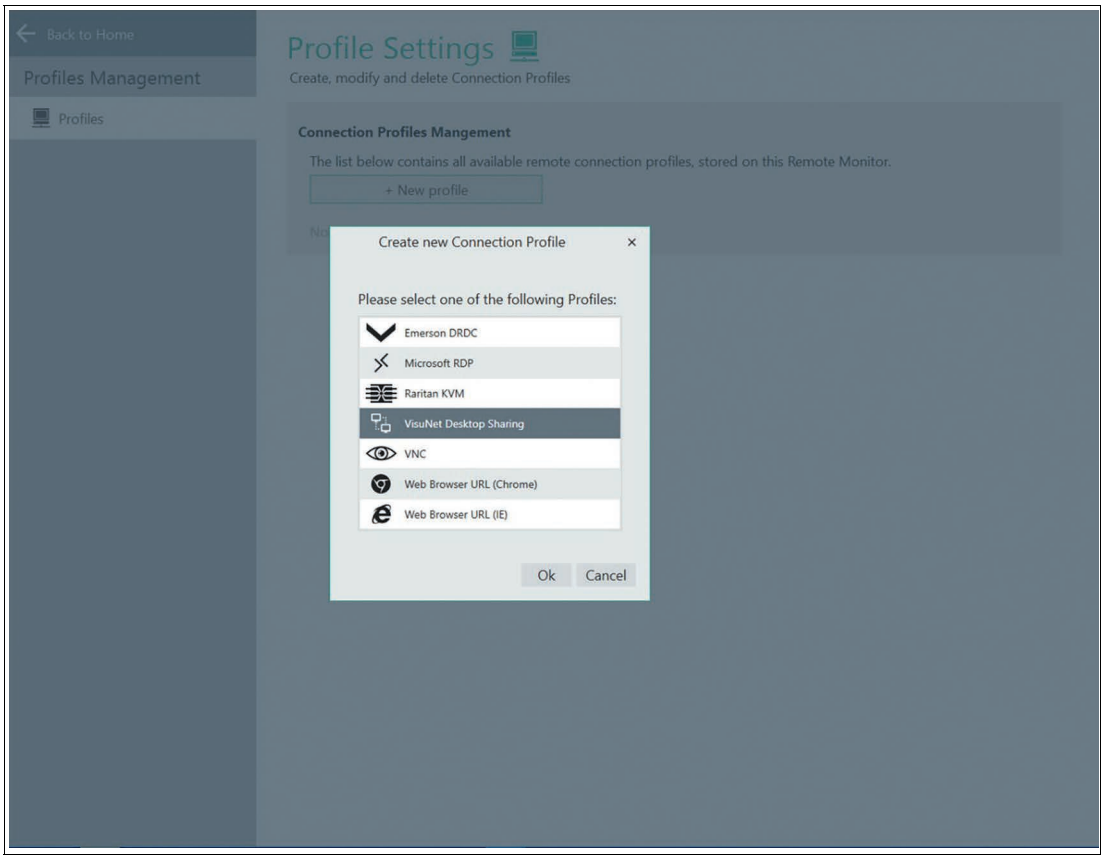


Figure 6.30

Caution!

Keep Default Settings

We highly recommend to remain the default settings of "ignoring certificate mismatch error" and "ignore certificate chain error" on "off".

5. Enable Secure Tunnel. Set “Accept embedded self-signed certificate only” to "off".

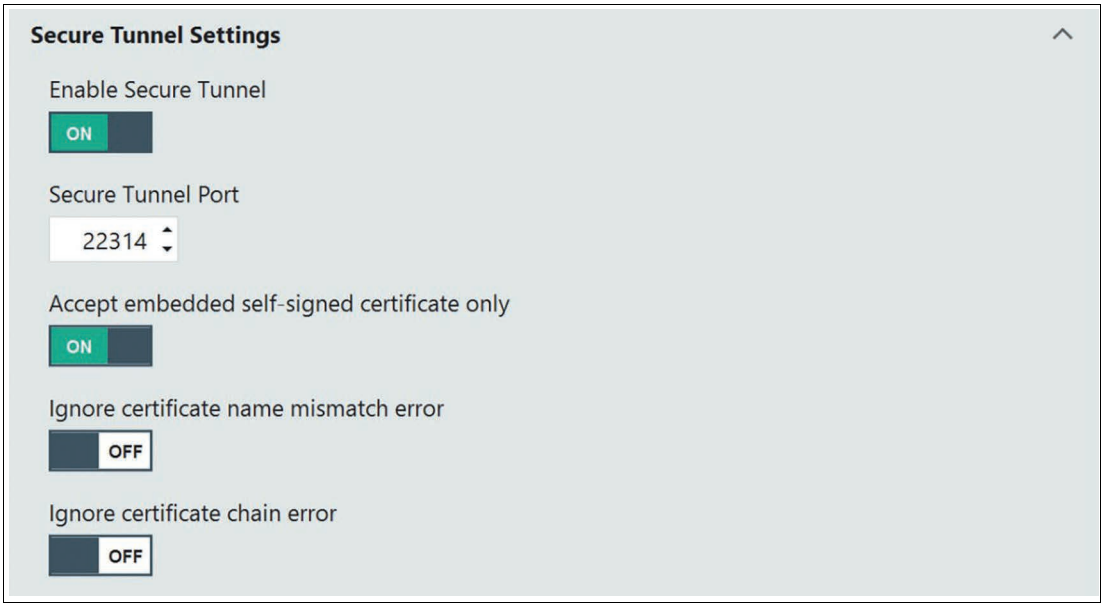


Figure 6.31

6.5 VNC Settings

RM Shell offers an embedded VNC client. This client is compatible with standard VNC server software. It also supports many unique features that are specific to UltraVNC and TightVNC distributions. This includes secure communication with a VNC server, for example. The VNC client supports UltraVNC NTLM (ms-logon) authentication and provides built-in support for UltraVNC SecureVNC v2.3 and MSRC4 v1.2.2 DSM plugins.

This section describes the core settings to set up a VNC connection.

Main Settings

In this section, you can set up general settings such as profile name, host name / IP address and password protection.

Option	Description
Profile Name	Allows you to change the visible name of the selected profile.
Host Computer Name / IP	Enter the host computer name or the IP address of the host in the network.
Host Computer Port	You can enter the port of the host. We recommend using the default setting.
Password Type	Choose the type of password protection for the VNC connection.

Connection

In this section, you can set up connection details.

Option	Description
Fast Disconnect Detection by sending Pings to the Host Server	When enabled, the RM / BTC constantly sends pings to the host. Possible connection failures will be detected much quicker than usual.
Encoding	There are several encoding methods available. Keep in mind that the chosen encoding must comply with the VNC host settings.
Use CopyRect encoding	Another encoding method. Keep in mind that the chosen encoding must comply with the VNC host settings.

Option	Description
Use Cache encoding	Use this option to improve the performance. Using cache encoding may affect the error tolerance.
View only	Enable this option to view the VNC host screen. No mouse or keyboard interaction is allowed.
Request shared session	This allows several clients to share the same VNC session. If this option is not set, only one client can be connected to the same VNC server. If a new, "non-shared" client is connected, existing clients will be disconnected or the new connection will be dropped, depending on the server's configuration.
Remote input enabled	To disable mouse and keyboard control of the RM while the VNC host also controls parts of RM functionality, select "Remote input enabled - off."
Auto reconnect enabled	Enable this option to use the VNC's built-in connection recovery mechanism. This mechanism also tries to reestablish a connection when it is disturbed.
Block user from closing the connection	Enable this option to prevent a connection window from being closed.

Display Settings

In this section, you can set up display settings such as color depth, cursor (tracking) mode, screen stretching behavior of the connection bar, etc.

Option	Description
Color Depth	Select the desired color depth of the VNC connection from the dropdown list.
Screen Stretching	Select an option from the dropdown list to choose screen stretching. 1. Resize the remote screen image to fill the local screen no matter what the actual aspect ratio is: the content is stretched to the size of the local screen. This may lead to distortion of the content. 2. Scale to as large an image as possible, but maintain the correct aspect ration: the content will be stretched as large as possible without any distortion of the aspect ratio. This may lead to black bars.
Scaling engine	Select the required scaling engine
Show the connection on following displays	If you use extended desktop systems or BTC*, every profile can be shown on different displays. From the dropdown list, select the display that shows the respective profile. Select "Expand over all display" if you want the profile window to be maximized over all displays. Use the "Identify Display" button to identify the different displays. The number of the respective display will be shown on each monitor.
Cursor Mode	Select an option from the dropdown list. • Track remote cursor locally (recommended) • Let remote server deal with mouse cursor • Don't show remote cursor: no cursor is shown. Use "no cursor" as cursor tracking mode
Cursor Tracking Mode	• No cursor: no cursor available. Select this option for cursor mode "Don't show remote cursor." • Dot cursor: a dot is used as cursor • Normal cursor: standard Windows arrow is used as cursor • Small cursor: a smaller standard Windows arrow is used as cursor

2022-02

Option	Description
Use custom compression	The compression depends on the selected encoding. Use the slider to select the compression rate.
Use JPG compression	The compression depends on the selected encoding. Use the slider to select the compression rate.
Display the connection bar	Enable this option to show the connection bar at the top of the screen. The connection bar fades out automatically after a few seconds. It fades in when you move the mouse to the top of the screen.

Proxy Settings

In this section, you can set up proxy settings such as proxy port, IP address, user name, password for the proxy connection, etc.

Option	Description
Proxy Type	Select one of the following proxy types: • Direct connection • SOCKS5 (no password) • HTTP proxy (no password) • UltraVNC repeater
Proxy IP address	Type in the proxy IP address
Proxy user name	Type in the proxy user name
Proxy password	Type in the proxy password
Proxy port	Select the proxy port

Advanced

In this section, you can set up advanced settings.

Option	Description
Show VNC Error Message Boxes	Enabling this option simplifies the error tracking. However, it may interfere with the auto reconnect function. The default setting is "off."
Disable clipboard	This option allows you to copy content from the VNC server clipboard to the local RM / BTC clipboard. In the default setting, copying content to the RM / BTC clipboard is enabled ("Disable clipboard - off")
Enable Ctrl + Alt + Del hotkey	Enable this option to allow users to use the Ctrl + Alt + Del hotkey.
Capture hotkeys containing the Alt key or Windows key	Key combinations containing an Alt or Windows key will be forwarded. E.g. Window+E for Explorer, or Alt+Tab for Task Switch.
DSM encryption plug-in	Select one of the following encryption plug-ins: • Plain connection, no encryption • Use MSRC4 DSM plug-in • Use SecureVNC DSM plug-in

6.6 Web Browser Settings (Chrome)

The restricted web browser is a built-in HTML web browser in RM Shell that is based on Google Chrome. It allows you to directly access HTML-based systems (e.g., SCADA, MES, IP Cameras, etc.). The restricted web browser allows you to specify a link to a web address that is presented on the home screen as a profile. In contrast to a standard web browser, operators cannot enter a different web address in the restricted web browser and can only access the configured website.

Note

Optional feature, requires PRO license to unlock feature.

General Settings

Option	Description
Connection name	Name of the web connection that is presented on the home screen.
URL that will be navigated to	The URL to which the web profile will be linked.
Show URL	Enable this option to show the URL at the bottom left of the connection window.
Block user from closing the connection	Enable this option to prevent the user from opening a connection window. (This hides the close button in the connection bar and disables Alt+F4)

Display Settings

Option	Description
Show the Connection Bar	Enable this option to show the connection bar at the top of the screen. The connection bar fades out automatically after a few seconds. It fades in when you move the mouse to the top of the screen.
Show the connection on following displays	If you use extended desktop systems or Pepperl+Fuchs box thin clients, every profile can be shown on different displays. From the dropdown list, select the display that shows the respective profile. Select "Expand over all display" if you want the profile window to be maximized over all displays. Use the "Identify Display" button to identify the different displays. The number of the respective display will be shown on each monitor.

6.7 Web Browser Settings (Internet Explorer)

The restricted web browser is a built-in HTML web browser in RM Shell that is based on Internet Explorer. It allows you to directly access HTML-based systems (e.g., SCADA, MES, IP Cameras, etc.). The restricted web browser allows you to specify a link to a web address that is presented on the home screen as a profile. In contrast to a standard web browser, operators cannot enter a different web address in the restricted web browser and can only access the configured website.

Note

Optional feature, requires PRO license to unlock feature.

General Settings

Option	Description
Connection name	Name of the web connection that is presented on the home screen.
URL that will be navigated to	The URL to which the web profile will be linked.
Show URL	Enable this option to show the URL at the bottom left of the connection window.
Show Message Box when Script errors detected	Enable this option to show error messages.
Block user from closing the connection	Enable this option to prevent the user from opening a connection window. (This hides the close button in the connection bar and disables Alt+F4)

Display Settings

Option	Description
Show the Connection Bar	Enable this option to show the connection bar at the top of the screen. The connection bar fades out automatically after a few seconds. It fades in when you move the mouse to the top of the screen.

7 App Management

App management allows administrators to add links to Windows® tools and .exe applications, such as antivirus software or standard programs like Windows Media Player. Administrators can then define a range of settings for each app and determine which user roles have access.

Note

Compatibility of Third-Party Software

RM Shell is qualified to work with software that is shipped with Pepperl+Fuchs VisuNet devices. Pepperl+Fuchs does not guarantee the functionality of third-party software. Customers are responsible for ensuring compatibility with any third-party software.

Note

Installing Antivirus Software

For instructions on installing antivirus software,See chapter 11.5.

Note

Whitelisting Applications

RM Shell uses a dialog filter that automatically closes all application windows that are not allowed to be opened. If the dialog filter is enabled, you may need to whitelist programs and applications in order for the app to operate properly. For instructions on whitelisting programs, see chapter 8.3.

Note

Maximum App Size

The maximum size of the installed App should need expand 500 MB. Customers need to evaluate if appsizes up to 1 GB lead to problems in the Windows updating process. If your apps/programs require higher performances and bigger storage we recommend our VisuNet PCs.

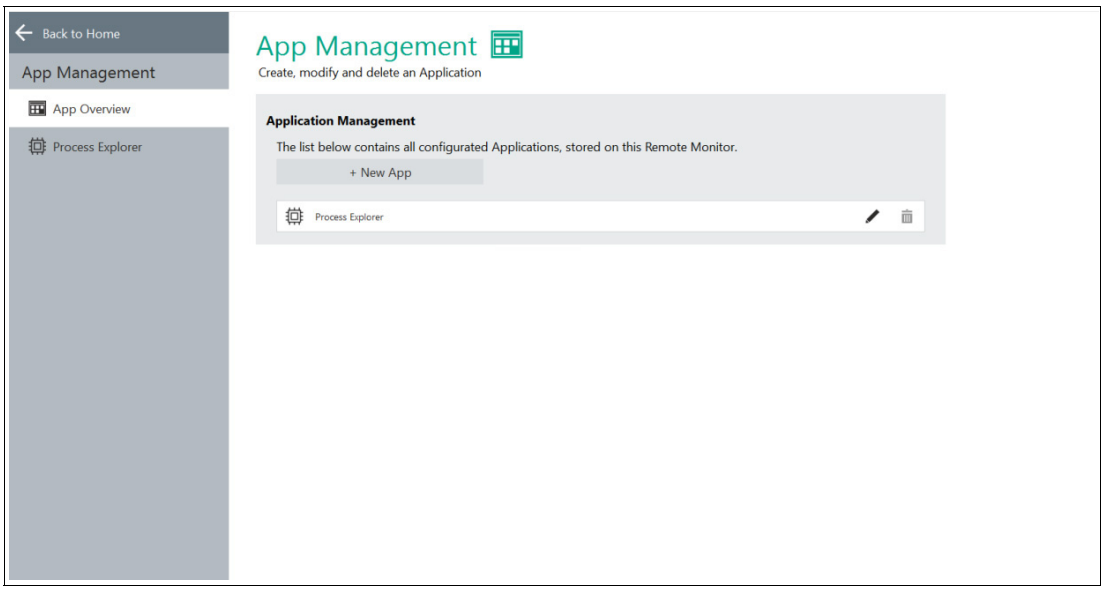
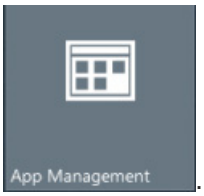


Figure 7.1 VisuNet RM Shell app management

2022-02

PEPPERL+FUCHS

Opening App Management

1. To open app management, click the appropriate icon on the home screen 

.

Creating an App

1. To create an app, click + New App.
2. The "Generic App" window appears. This screen allows you to determine the following settings:
   - **Name**: Choose a name for the app or use the name that is automatically generated.
   - **Application path**: Manually enter the application path or click the icon at the end of the field to browse.
   - **Parameter**: Allows additional command line parameters to be passed when starting the application. Only enter the parameters for the executable in this line. For example, when you want to perform `shutdown /s /f /t 0`, only add `/s /f /t 0` to this line.
   - **Allowed access**: Select which user roles can access the application.
   - **Autostart**: Starts app automatically after booting the RM / box thin client.
   - **Maximized**: When this option is turned on, the application window is maximized upon opening.
   - **Use default icon**: When this option is turned on, a default RM Shell icon appears on the user's screen. When this option is turned off, the application's standard icon appears on the user's screen.

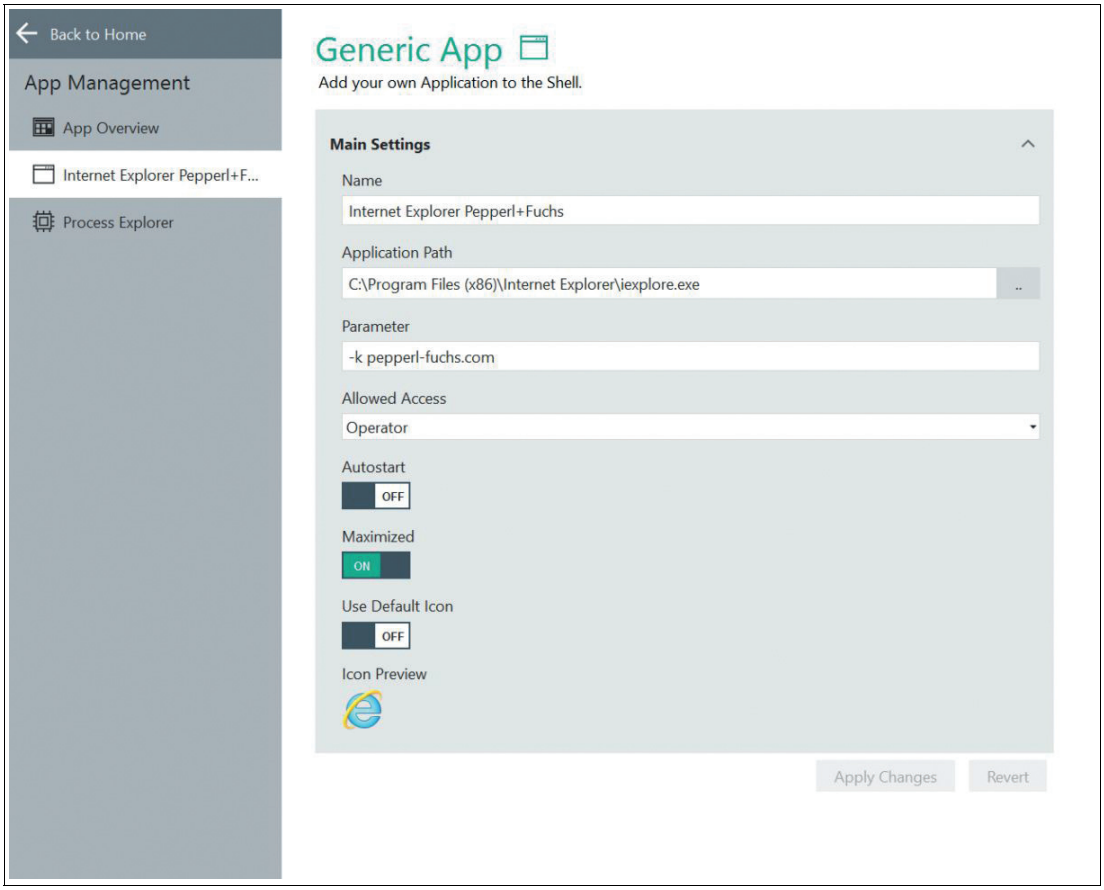


Figure 7.2 The "Generic App" window allows you to determine settings for new apps and adjust settings for existing apps.

↳ The app has been created. A tile that links to the app appears on the user's home screen in the "Applications" area.

Modifying App Settings

1. Open app management and select "App Overview" from the menu on the left side of the screen.
2. Click the icon that appears next to the app that you would like to modify.
3. After you edit the settings in the window that appears, click "Apply Changes."

   ↳ The changes have been saved.

7.1 Wedge App

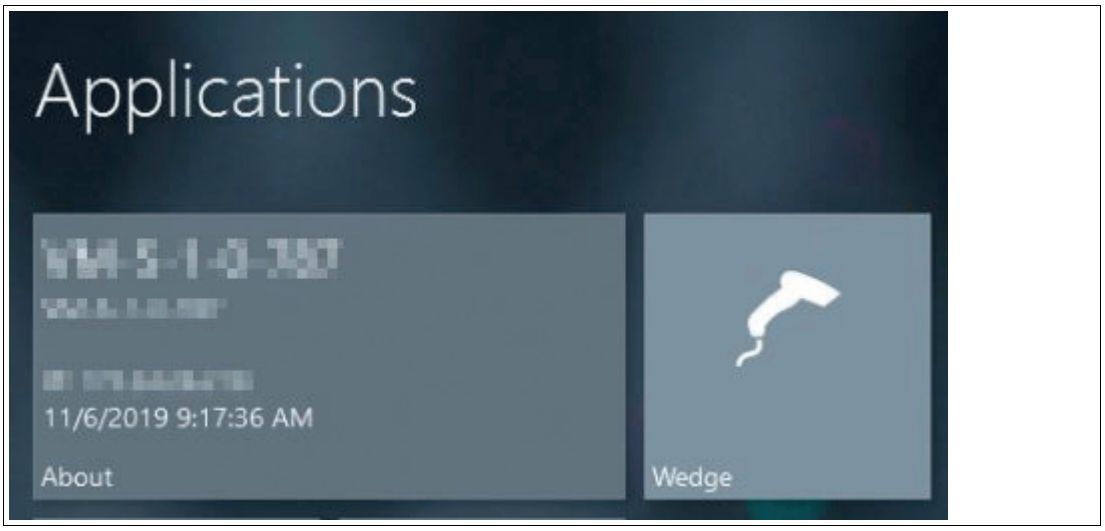


Figure 7.3 VisuNet RM Shell wedge app

The wedge app is a keyboard emulation program that reads character strings from the serial port and simulates the corresponding keystrokes on the RM. These are then sent to your host PC. The app is specially designed to connect Pepperl+Fuchs barcode scanners (IDM handheld 1-D and 2-D code readers). It allows a barcode scanner connected to the serial port to be used as a keyboard input device in various applications. For information on configuring the wedge settings, see chapter 8.17.

The wedge app also helps users check whether a barcode scanner is properly connected to the serial port and ready for use. The wedge app is available in all three user roles (Operator, Engineer, and Administrator).

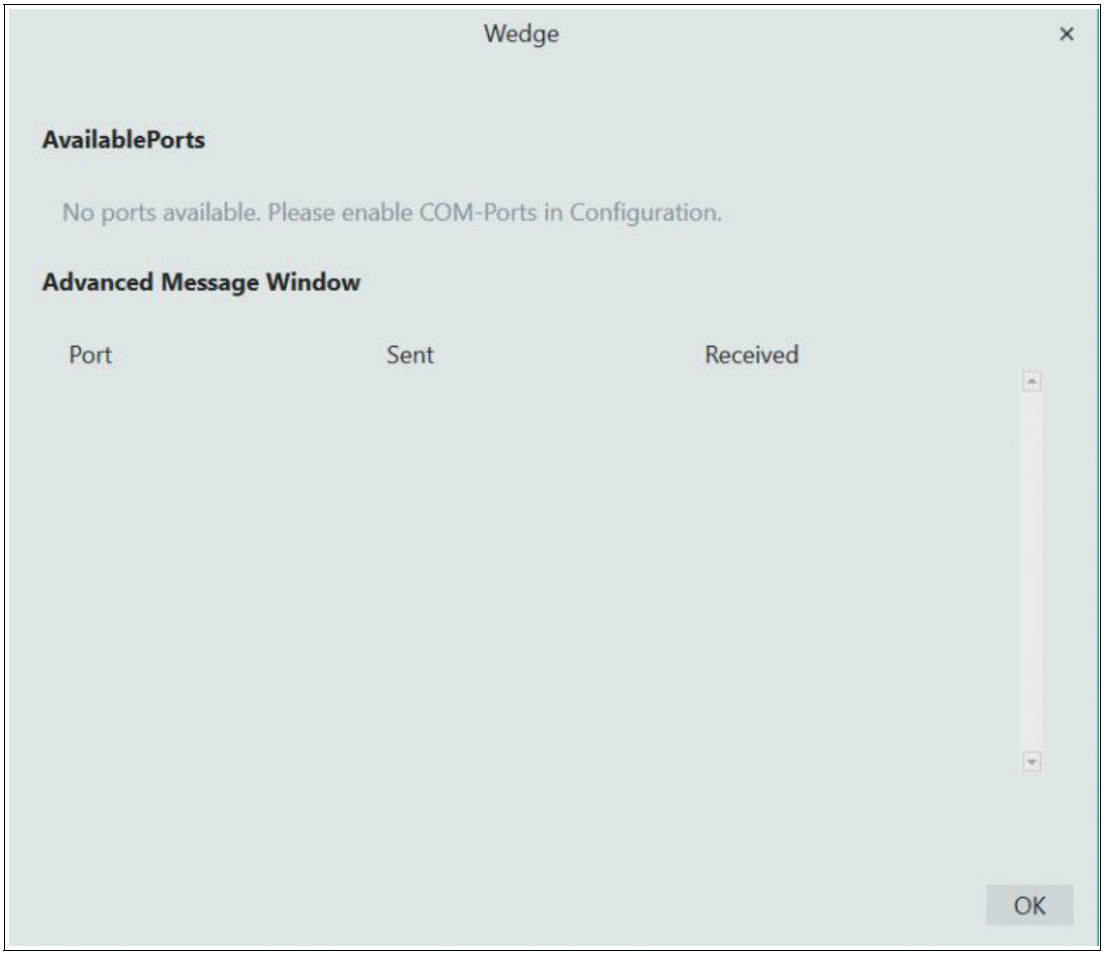


Figure 7.4

Note

From VisuNet RM Shell 5.5 on it is possible to hide the Wedge app from the Operator. Refer to Chapter 7.16 for further information.

7.2 Process Explorer App

The Process Explorer app allows you to monitor multiple device parameters, including memory, storage usage, and CPU load. This tool can be used to diagnose and test RM Shell. The Administrator user role can determine which users have access to it in the "app management" app. See chapter 7.

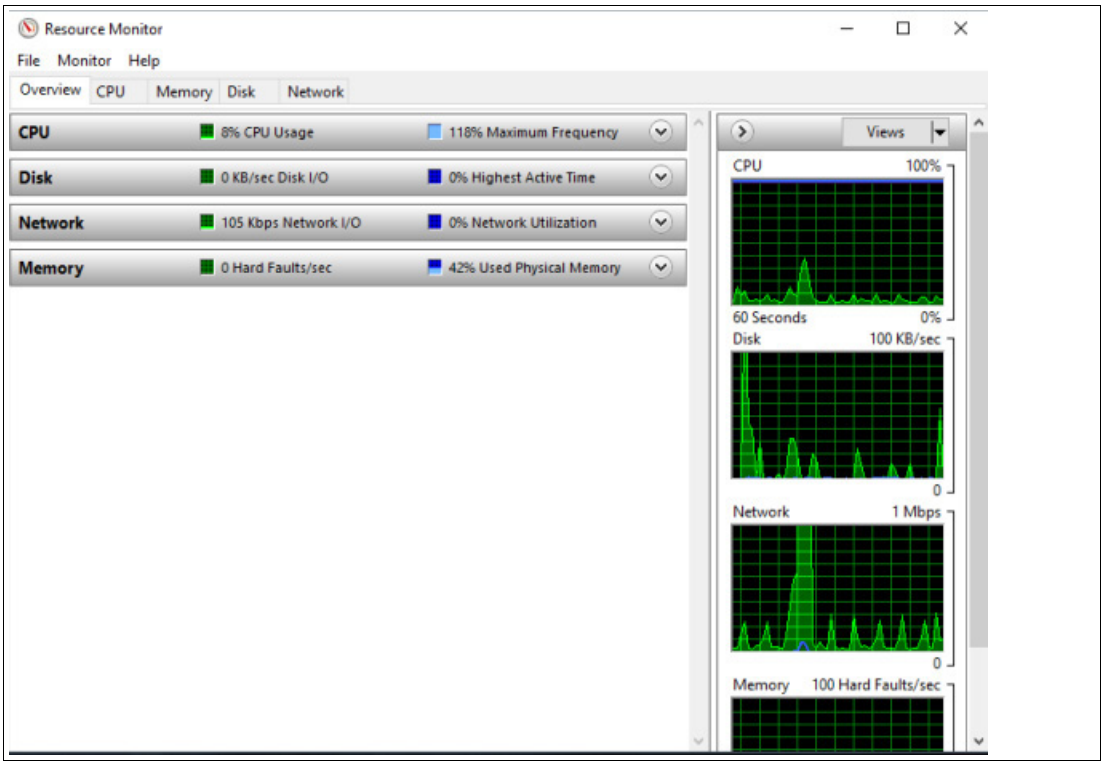


Figure 7.5 Process explorer window

8 System Settings App

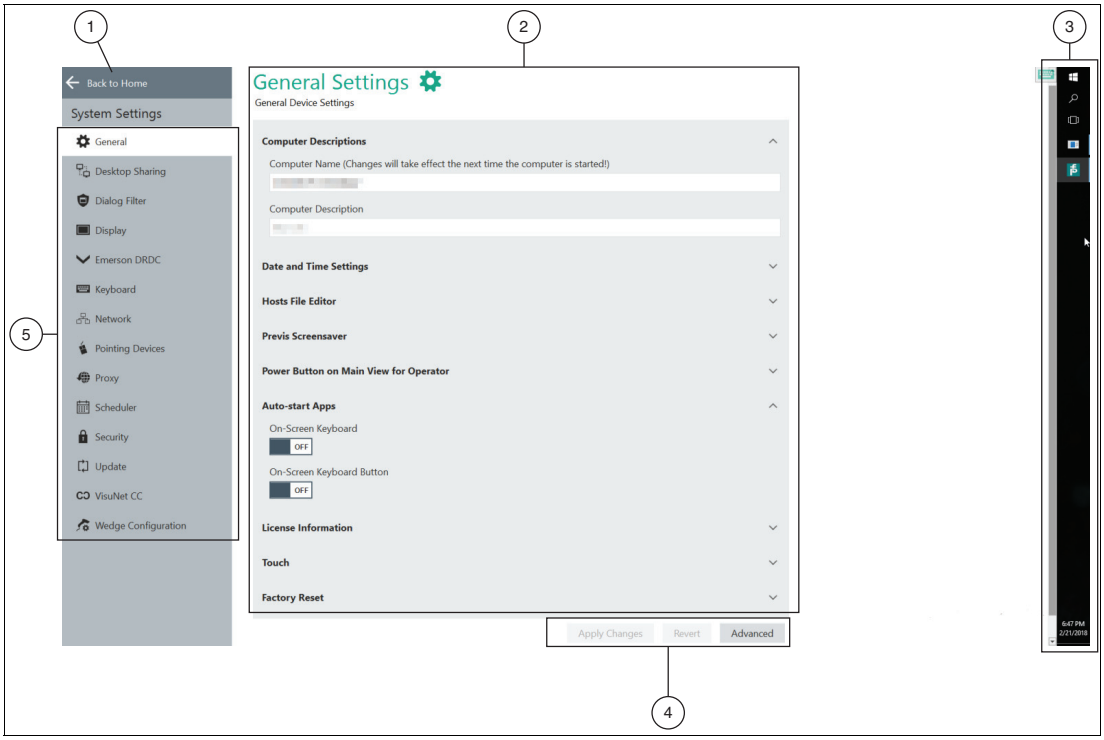


Figure 8.1 Components of the system settings app screen

1	Navigate back to home screen
2	Main Page / content page
3	Windows® Explorer sidebar. This element is only visible to users who are logged in as "administrator." This gives administrators the ability to install third-party software and access Windows® control center to adjust advanced settings.
4	• **Apply changes**: write changed settings to the RM. • **Revert**: discard changed settings and restore previous settings. • **Advanced**: Only visible for Administrator user role. This button opens additional Windows®-specific dialog boxes for settings that are not included in the VisuNet RM Shell but may be of use to Administrators.
5	Navigation bar with all submenus. Each submenu is explained in detail below.

Note

Disable Write Filter for Persistent Storage of Configurations

To persistently store configuration changes, disable the unified write filter (UWF). Once you have implemented the configuration changes, enable the UWF again to persistently store the changes.

Note

Working with Windows®-Specific Advanced Settings

After you change settings via the Windows®-specific Advanced Settings, reload these settings into the VisuNet RM Shell by changing the current VisuNet RM Shell subscreen once.

Entering System Settings App

1. To enter the system settings app, click the appropriate icon on the home screen

Use this app to manage your RM / BTC settings. The "General Settings" submenu is displayed by default when you open the app. Additionally, there are several other submenus:

- **General**
  Specify general settings such as computer description, system language, date and time, Previs screensaver, power button configuration, and license information. See chapter 8.1.
- **Desktop Sharing**
  Manage the settings for sharing the screen of an RM. See chapter 8.2.
- **Dialog Filter**
  Add applications to a whitelist to prevent them from being closed by the dialog filter. See chapter 8.3.
- **Display**
  Manage display settings such as resolution, color depth, and refresh frequency. See chapter 8.4.
- **Keyboard**
  Manage keyboard settings such as input language, character repeat, and cursor blink. See chapter 8.7.
- **Network**
  Manage network settings such as network adapter information and IP address settings. See chapter 8.8.
- **Pad-Ex**
  Manage your Pad-Ex settings as selecting the action for your program key or rotation lock. See chapter 8.9
- **Pointing Devices**
  Manage pointing device settings such as sensitivity or button behavior of the pointing device. See chapter 8.10.
- **Proxy**
  Enable proxy and manage proxy settings. See chapter 8.11.
- **Scheduler**
  Schedule periodic system reboots. This allows continuous use of the unified write filer without memory buffer overruns. See chapter 8.12.
- **Security**
  Set up VisuNet RM Shell passwords and enable firewalls. See chapter 8.13.
- **Touch**
  Configure touch sensitivity profiles. This submenu is only shown when the RM in use is equipped with this option. See chapter 8.14.
- **Update**
  Enable remote updates or scan for local updates. See chapter 8.15.
- **VisuNet CC**
  Configure VisuNet Control Center. See chapter 8.16
- **Wedge Configuration**
  Manage wedge configuration settings such as input character delay and remote text input mode. Define assigned functions for HEX codes. See chapter 8.17.

8.1 General Settings

Computer Descriptions

In this section, you can edit the name and description of the local RM / BTC and join other domains.

Function	Description
Computer Name	This field shows the current computer name of the RM / BTC. To edit the name, click in the field and enter a new name. The changes will take effect after the RM / BTC has been rebooted.
Computer Description	This field shows a description of the RM / BTC. You can edit the description, e.g., to describe where the RM / BTC is located in your product process (i.e., "Shop floor"). The description is shown on the VisuNet RM Shell home screen under the computer name on the About tile. To edit the description, click in the field and type.

Date and Time Settings

In this section, you can set up the RMs / BTCs' date and time.

The date and time settings of the RM / BTC must correspond with the date and time settings of the host.

Function	Description
Date	This field shows the currently defined date.
Time	This field shows the currently defined time.
Configure Date and Time	Click the "Configure Date and Time" button to configure the date and time. The Windows® "Date and Time" dialog box opens.
Configure Regional Settings	Click the "Configure Regional Setting" button to configure regional settings. The Windows® "Region and Language" dialog box opens.

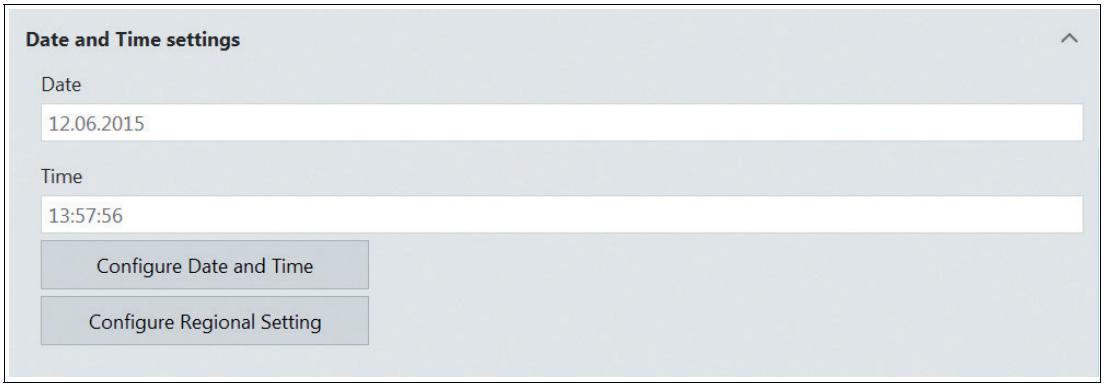


Figure 8.2 General settings - date and time settings

Caution!

Time Zone, Date, and Time

Ensure that the RM / BTC is set up with the correct time zone, date, and time. Encrypted communication protocols (e.g., those used between VisuNet RM Shell and VisuNet Control Center) require synchronized date and time settings between both communication partners. The maximum feasible date and time difference is 12 h.

License information

This section provides information about the VisuNet RM Shell license that you are currently using. Only the Administrator user role has the rights to see the license information.

Function	Description
Applied Licenses	Here you can see the entered licenses of your device. You are also able to delete them.
Add new license	If you purchased PRO, DRDC or CC license keys, enter your license keys to enable more features of the VisuNet RM Shell PRO, DRDC or VisuNet CC version. Click "Apply." Changes will take effect after the RM / BTC has been rebooted.
License key	If you purchased PRO license keys, enter your license keys to enable more features of the VisuNet RM Shell PRO version. Click "Apply." Changes will take effect after the RM / BTC has been rebooted.

Figure 8.3 General settings - license information

Previs Screensaver

In this section, you find the settings for the Previs screensaver.

Previs is a screensaver which prevents permanent image retention or image sticking on LC displays while presenting the process picture at the same time. Process pictures stay visible, and you still have direct access to all important process information.

Function	Description
Idle time before starting	Configure the time of inactivity. After this time frame, Previs will start. If the time is set to 0 min, the screensaver is disabled.
Effect Intensity	Configure the intensity of the screensaver. Higher values allow better protection against screen burn-in effects.
PIN (Numerical characters only!)	With the additional PRO license you are able to set a PIN so only authorized personal can unlock the device.
Start Previs at Shell startup	After a reboot or a new start of the device every user role has to enter the PIN to unlock the device (PRO license required).

Note

To be able to use the Previs Screensaver PIN function, an extra PRO license is required.

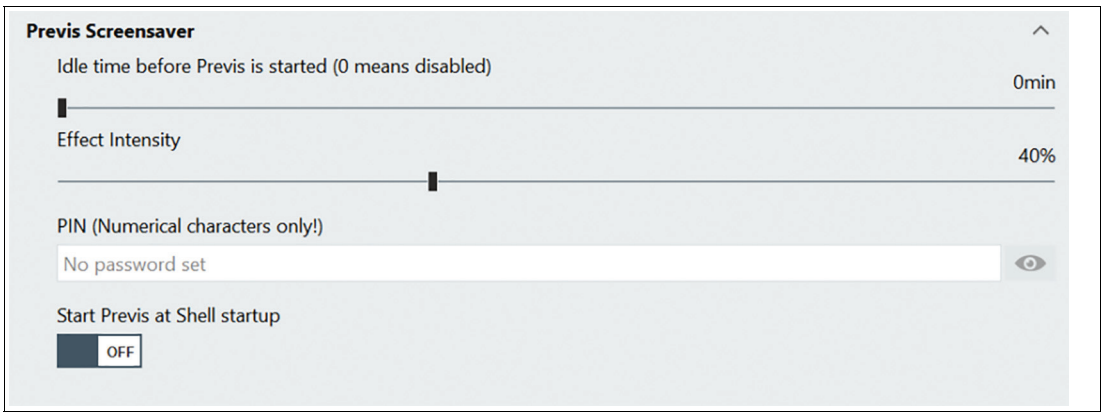


Figure 8.4 General settings - Previs screensaver

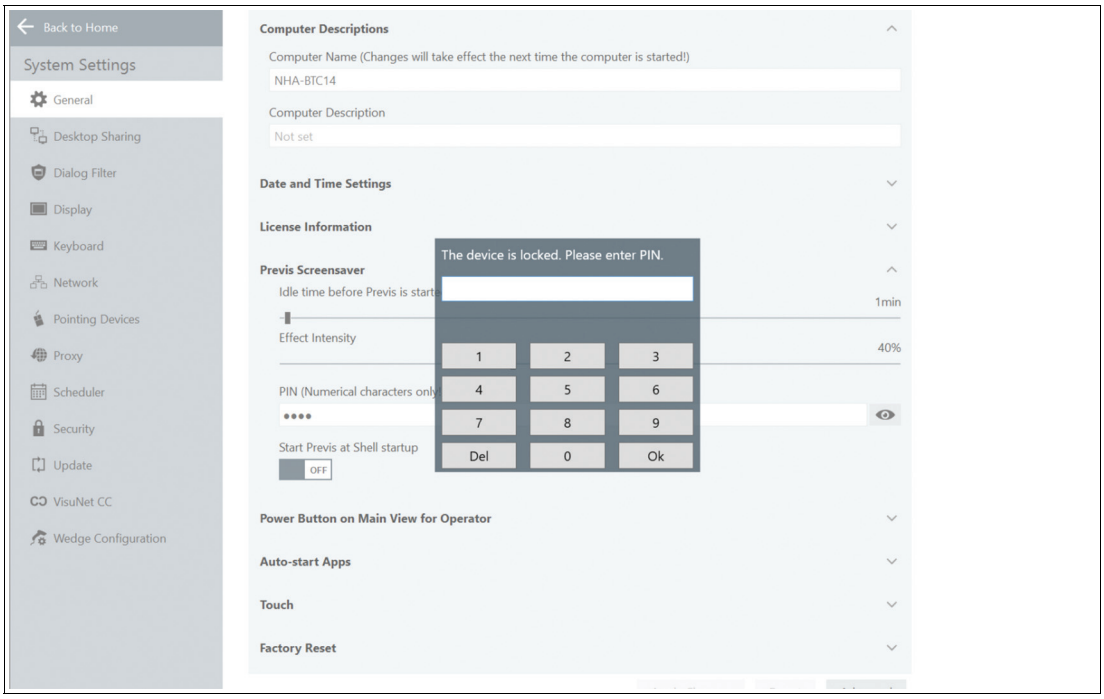


Figure 8.5 Unlock your numeric password with the keypad

Power Button on Main View for Operator

In this section, you can configure the power button behavior, which is located in the system functions on the home screen. See chapter 4.

The power button has several functions that can be set up for the Operator user role. The Operator user role is only allowed to run the preconfigured options.

Function	Description
Show "Restart" Button	Enables "restart" functionality in the power button menu on the home screen. If this functionality is enabled, the Operator user role is able to restart the RM / BTC.
Show "Shutdown" Button	Enables the "shutdown" functionality in the power button menu on the home screen. If this functionality is enabled, the Operator user role is able to shut down the RM / BTC.
Show "Turn off display" Button	Enables "turn off display" functionality in the power button menu on the home screen. If this functionality is enabled, the Operator user role is able to turn off the display. The display can be turned on again by moving the pointing device. Depending on the RM / BTC hardware, this function might not turn off the backlight of some devices but instead will only turn the screen black.

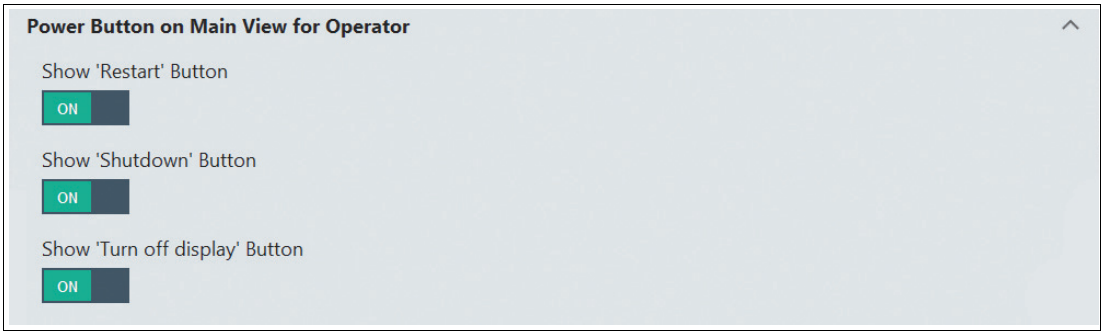


Figure 8.6 General settings - power button on home screen for operator

On-Screen Keyboard Settings

In this section, you can configure which apps start immediately after booting the RM / BTC.

Function	Description
Start On-Screen Keyboard with VisuNet RM Shell	Causes the on-screen keyboard to start right when the RM / BTC starts up.
Start On-Screen Keyboard Button with VisuNet RM Shell	Shows a dedicated floating keyboard button that opens the on-screen keyboard.
Use Touch keyboard instead of On-Screen Keyboard	Causes the Touch keyboard to start right when the RM/BTC starts up.

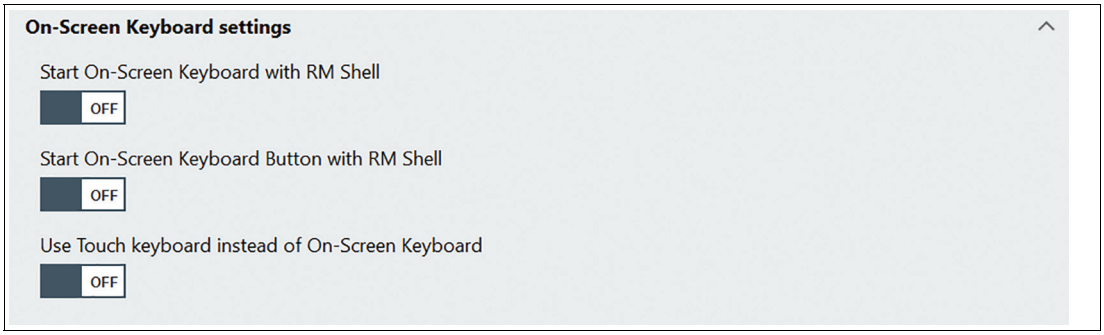


Figure 8.7 On-Screen Keyboard Settings

Quick Menu Settings

In this section you can enable or disable the floating quick menu.

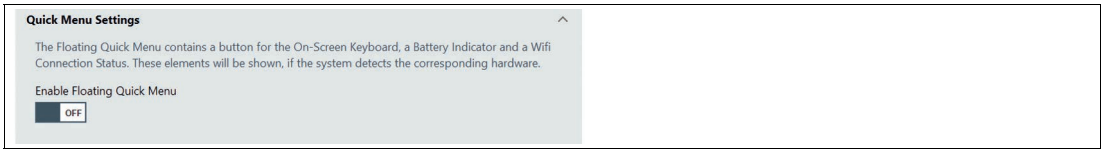


Figure 8.8

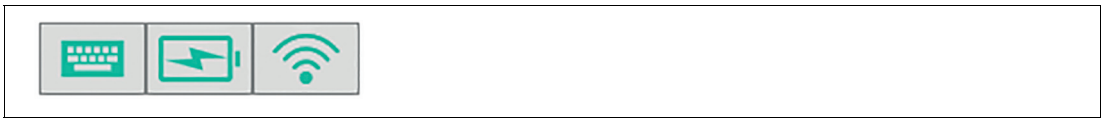


Figure 8.9

The floating menu can be located as required by easily moving the menu with your mouse.

Click the icon provides you the onscreen keyboard or further information on the battery/Wi-Fi status.

Wallpaper and Logo

In this Section you can customize your Wallpaper and Logo.

To add your individual Wallpaper or Logo click  .

Main View Settings

This section allows you to hide functions from the Operator role.

Function	Description
Hide System Tools from Operator	The System Tools Tile will not be visible for the Operator role anymore.
Hide IP address from About Tile from Operator	The IP address will not be visible anymore.

Figure 8.10

Touch

This section allows you to select the type of touch screen that you are using. If your system does not have a touch screen, select "none" from the drop-down menu.

Note

This does not affect the installed drivers, but only the UI.

Figure 8.11 General Settings - Touch Screen Type

Factory Reset

In this section, you can restart the system by applying an image file when using VisuNet RM Shell 5.3 or newer. The image files are either provided by Pepperl+Fuchs or you can capture your own image file in an earlier step. The image files are only applicable to the same device with the same serial number. For detailed instructions on performing a factory reset, see chapter 10

Function	Description
Reboot to Factory reset	Manage the available firmware for the VisuNet RM Shell. You can either capture or apply an image file.

8.2 Desktop Sharing

Function	Description
VisuNet Desktop Sharing Server Enabled	This function sets up the current RM / BTC as a VisuNet RM Master. The function allows other RMs / BTCs with the corresponding desktop sharing profile to mirror the RM / BTC Master's display. For more information, see chapter 6.4.
Share display	Optional setting: If the VisuNet RM Master has multiple external displays (e.g., industrial Box Thin Client BTC), you can select which display should be shared with a VisuNet RM Slave.
Desktop sharing password	Set your own Password or reset the password to the default password.

Note

The desktop sharing function is also used for the "Session Shadowing" functionality in VisuNet Control Center. This function must be enabled in order to "shadow" an RM / BTC with Control Center.

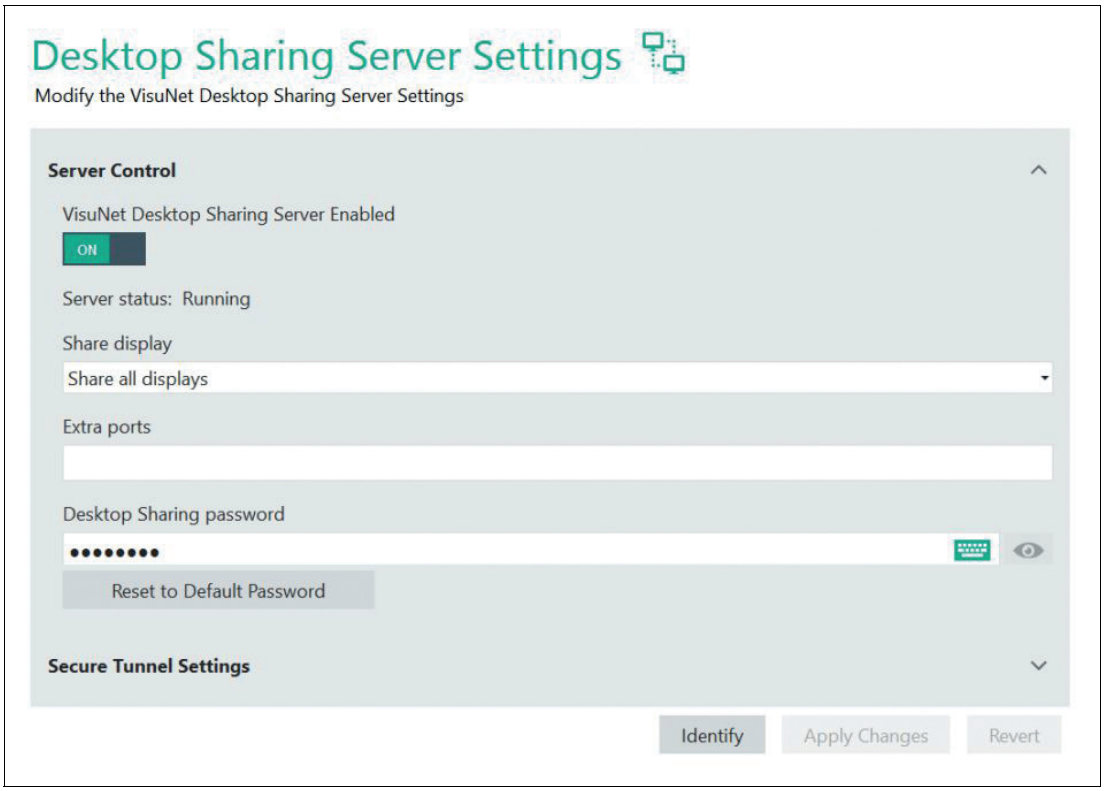


Figure 8.12 Desktop sharing server settings

If you enable the Session Shadowing, the Secure Tunnel Settings will be enabled per default as well. We recommend not to use the default certificate but your own certificate to increase the security even further.

Secure Tunnel Settings

Function	Description
Secure Tunnel Service Enabled	Further increase of the security
Service Status: Stopped	Feedback of the settings. Control function if Service really started.
Secure Tunnel Port	We recommend to use the default setting

2022-02

Function	Description
Use the default certificate (not recommended)	We recommend to use your own certificate
Select your certificate	Upload your own trusted root certificate

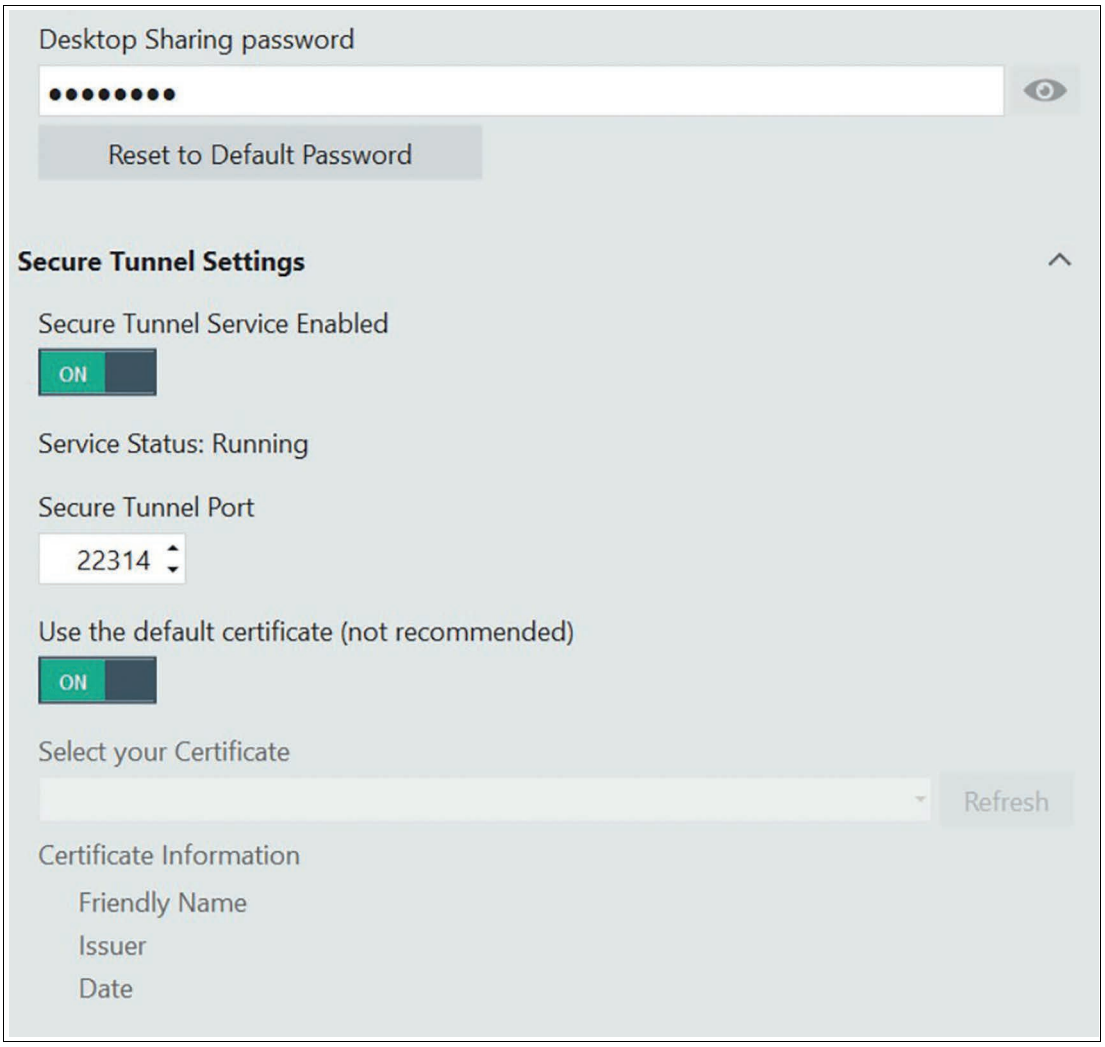
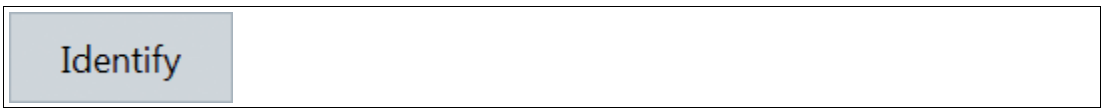


Figure 8.13 Secure Tunnel Settings - we recommend to upload your own certifcate

For further information on how to upload your own certificate, see chapter 6.4.

Identify Button

If you are using systems with more than one external display (e.g., extended desktop systems, Pepperl+Fuchs BTC), this button is shown. Use the button to identify the different displays. The number of the respective display is shown on each monitor.



8.3 Dialog Filter

The dialog filter closes all application windows that are not whitelisted and prevents users from accessing the file system or unauthorized programs. This section allows the administrator to whitelist processes and application windows. This prevents them from being closed by the dialog filter. In the administrator role the dialog filter is not activated.

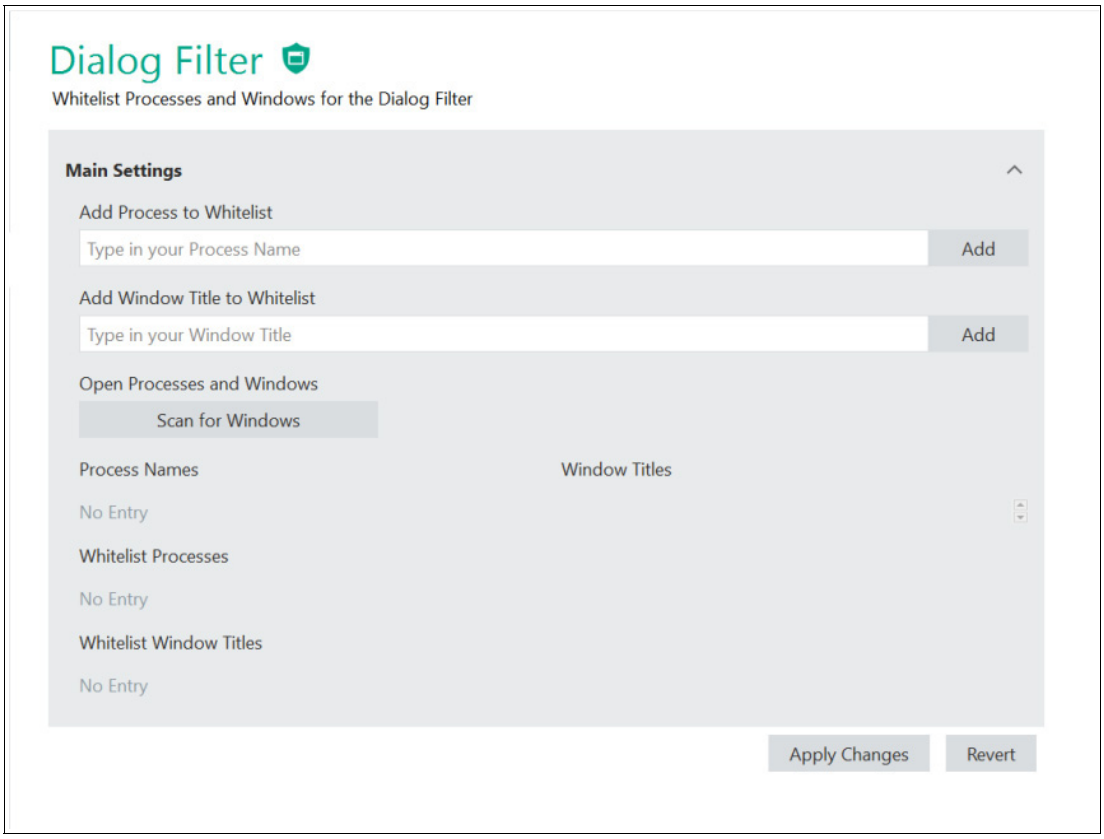


Figure 8.14 Dialog Filter Settings

Function	Description
Add Process to Whitelist	Type in the name of a Windows process to add it to the whitelist. For example, add "explorer."
Add Window Title to Whitelist	Type in the process name as it appears on a window to add it to the whitelist. For example, add "Internet Explorer."
Open Processes and Windows	This allows you to scan for processes that are currently running. After clicking "Scan for Windows," select a process to whitelist by clicking the "plus" icon next to a process.

Figure 8.15

All processes that are currently running can be found with the “Scan for Windows” function.

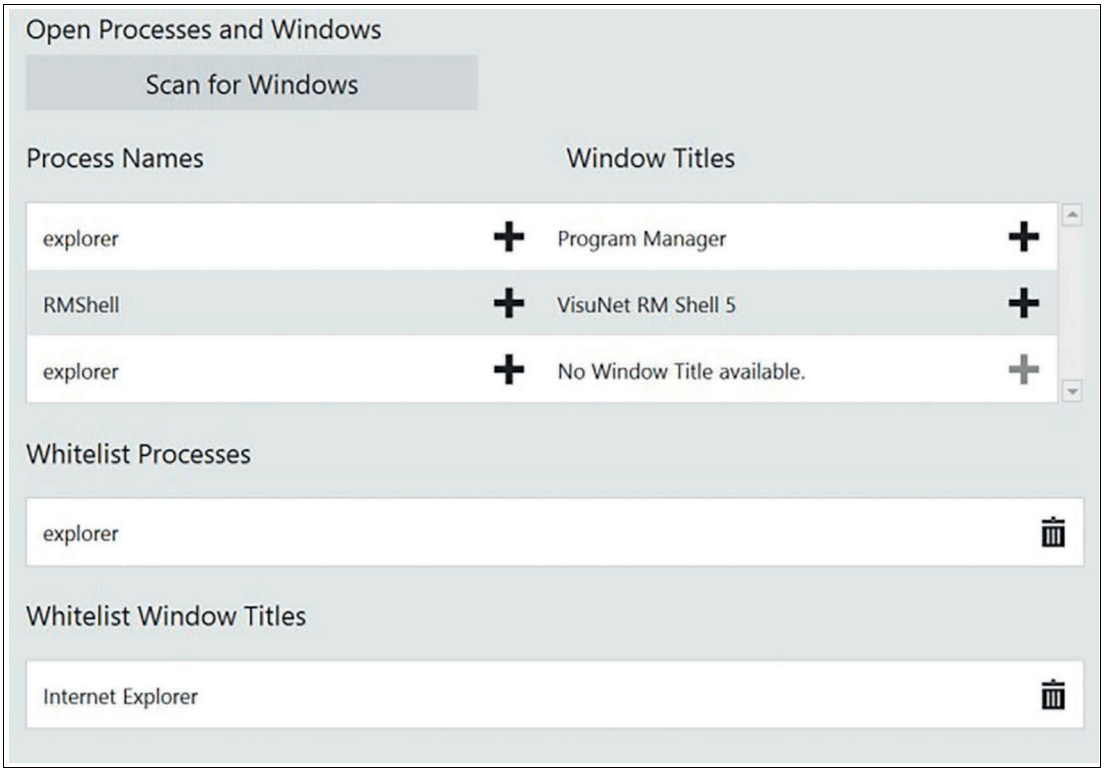


Figure 8.16

Scan for Windows

Scans all Windows which were open within in the last 60 seconds. It will run in the background even if you navigate to another page. This allows you to open your generic apps and scan all necessary windows and processes.

Click + to add the required process to the whitelist. Add a title to “add windows title to Whitelist” which will be appear on the window.

8.4 Display Settings

8.4.1 Configuring a Single Monitor

Function	Description
Resolution	Choose the resolution, color depth, and refresh frequency. For best results, choose the highest native resolution possible.

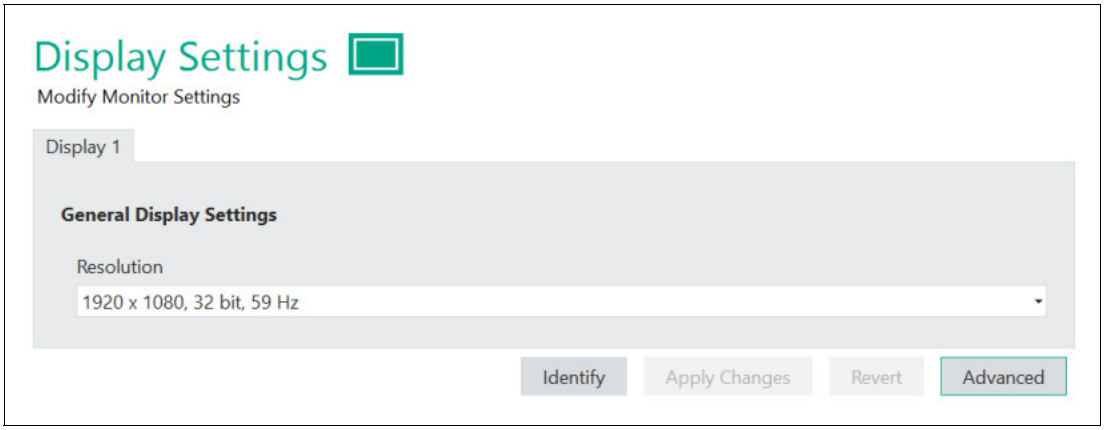


Figure 8.17 Display settings

Note

We recommend using the default settings.

8.4.2 Configuring Multiple Monitors

When you use a Box Thin Client with multiple monitors, each monitor is presented as an individual tab in the display settings view.

Note

Monitor Numbering

The monitor numbering used in VisuNet RM Shell does not correspond to the numbers in the Windows® display settings. Numbering in VisuNet RM Shell is used to assign profiles to the correct screen number.

The “Identify” button can be used to check the display numbering of the connected monitors.

To change the orientation/order of the connected monitors, enter the “Advanced” settings.

In the “Screen Resolution” window, you can arrange the order and arrangement of the connected monitors via mouse:

Rearranging Connected Monitors

1. Drag the display you want to rearrange via mouse and move it to the new position.
2. Save the changes by clicking "Apply" and close the window.

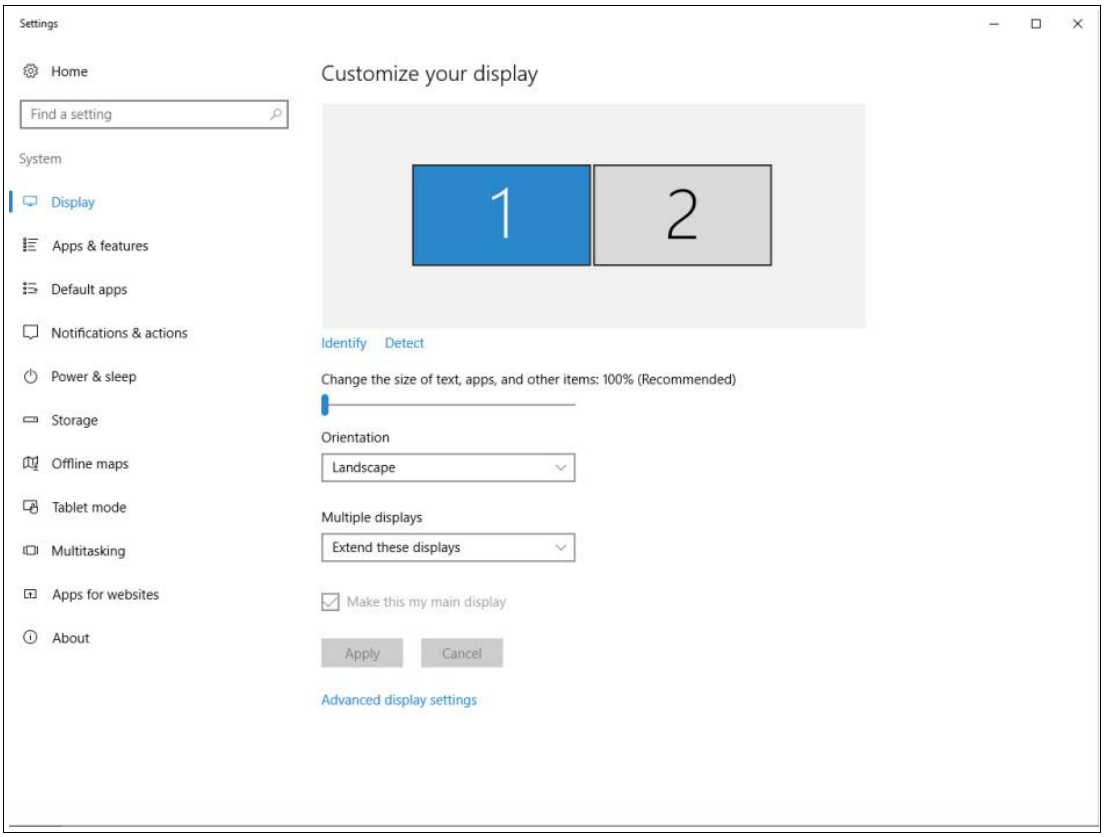


Figure 8.18 Rearranging multiple monitors

Automatically Align a Four-Monitor Setup in a Square Layout

Function	Description
Align Four-Monitor Setup	This additional feature shows up when 4 monitors with the following requirements are connected: • Identical resolution. • All displays are landscape-oriented. • The displays are arranged in a close-to-2x2-arrangement.

1. Fulfill the requirements.
2. Click "Align" to set up automatically an accurate 2x2 Quad-Monitor setup.

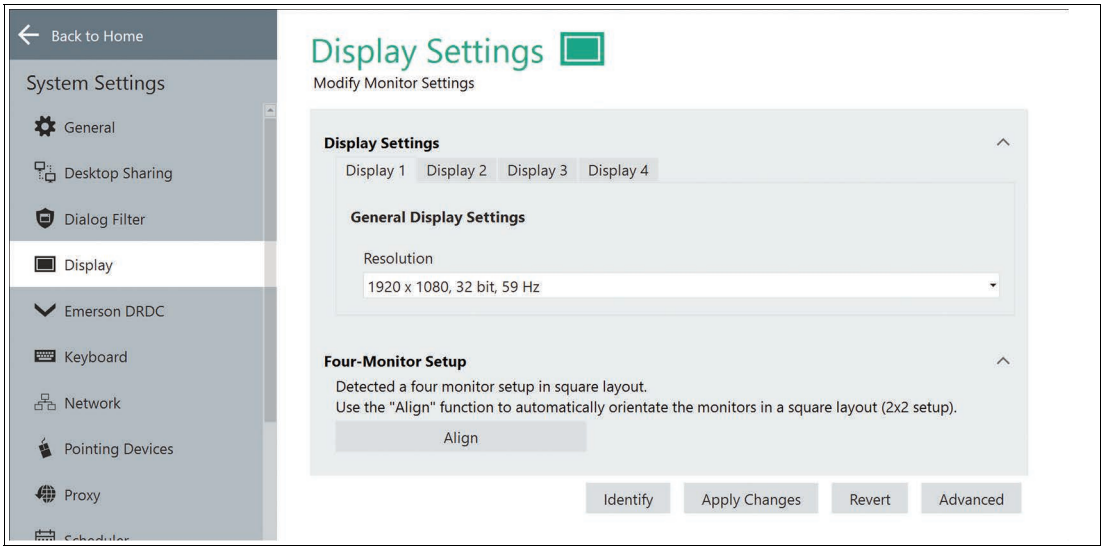


Figure 8.19

8.5 Emerson DRDC Settings

"Emerson DRDC" allows you to change the Emerson DRDC Settings.

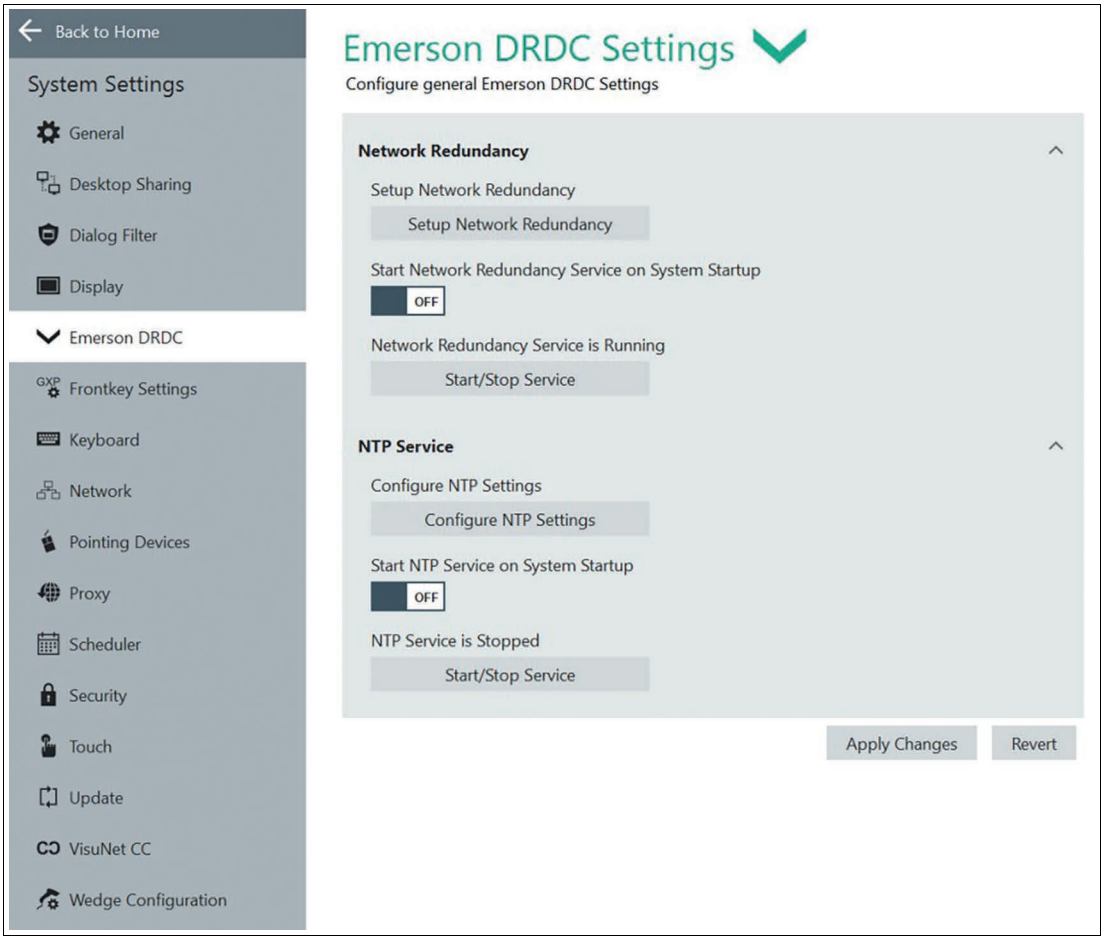


Figure 8.20

8.6 Frontkey Settings

Note

Only valid for VisuNet GXP devices.

Navigate to "frontkey settings" on the navigation bar.

Button Settings

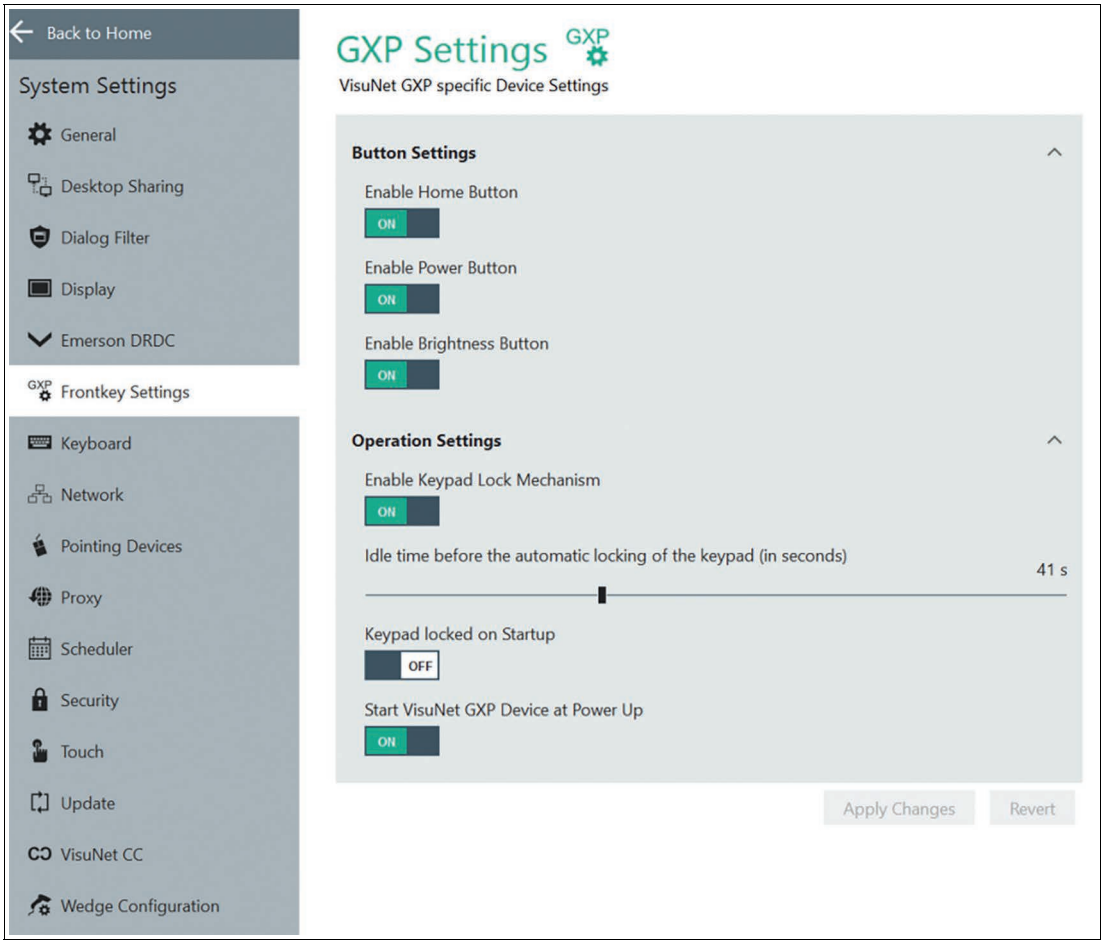


Figure 8.21

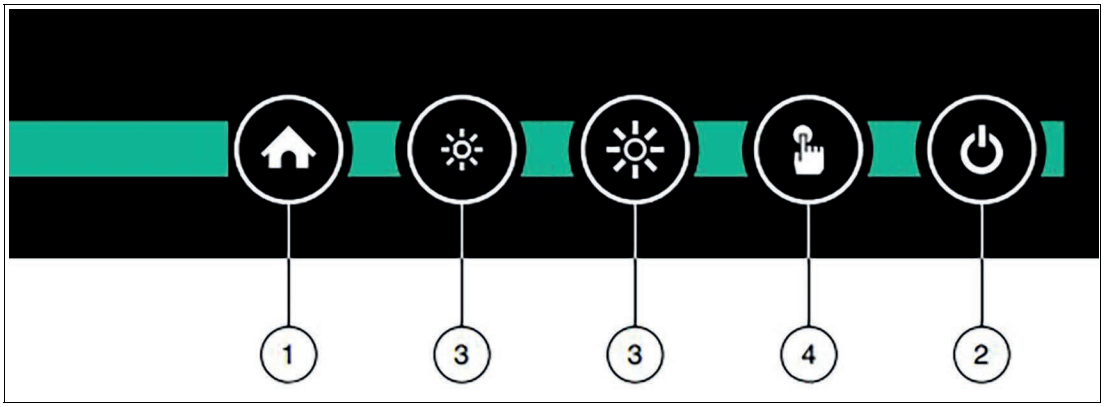


Figure 8.22

2022-02

	Button	Description
1	Home	Configurable front button to call a specified function
2	Power	Configurable power button (shutdown, restart, hibernate); button can be disabled
3	Brightness	Reduce display brightness (dimmable to 0%) or increase display brightness
4	Touch screen	Enable/disable touch screen (e.g. for cleaning purposes). If the display unit has no built-in touch screen, the touch screen button is disabled.

For further information regarding the operation and configuration refer to our VisuNet Display Unit manuals.

Operation Settings

Locking the front buttons:[1]

1. Enable the keypad lock mechanism.
2. Set the idle time before the automatic locking of the keypad (in seconds) by using the slider to adjust between 1 second ... 120 seconds.

↳ The keypad lock mechanism is activated.

Note

By pressing any button except the home button, the unlock animation is shown.

After the set idle time, the front buttons will be locked automatically. To signal this, all LEDs flash 3 times.

In the status of the enabled keypad lock mechanism you can decide whether the keypad should be locked on startup or after the set idle time.

1. Only available for Firmware Service Controller version 1.3.2.231 and newer. The update for your TCU is available at pepperl-fuchs.com

8.7 Keyboard Settings

Input Language

In this section, you can add new keyboard layouts, configure the keyboard layout, and customize the keyboard to your specific language needs.

Function	Description
Current Input Languages	The dropdown list shows every keyboard layout that is installed on the local RM / BTC. To choose the keyboard layout, click the arrow and select the preferred keyboard layout.
Configure Input Languages	To add a specific keyboard layout, click the "Configure Input Languages" button. A Windows® dialog box opens.

Figure 8.23 Keyboard settings - input language

Character Repeat

In this section, you can specify the speed at which characters will be repeated when you press a key. You can do this by changing the repeat delay or the repeat rate.

Function	Description
Repeat Delay	Repeat delay is the length of time after which a character will start repeating when you hold down a key. Use the slider to adjust between a short or long repeat delay. If the repeat delay is short, there will be a shorter period of time before the character being held down starts repeating. If the repeat delay is long, there will be a longer period of time before the character starts repeating.
Repeat Rate	Repeat rate is the rate at which a character will be repeated while you are holding down a key. Use the slider to adjust between a low or high repeat rate. If the repeat rate is low, the character will be repeated at a slower rate. If the repeat rate is high, the character will be repeated at a faster rate.

Figure 8.24 Keyboard settings - character repeat

2022-02

PEPPERL+FUCHS

Cursor Blink

In this section, you can specify the behavior of the cursor.

Function	Description
Cursor Blink Enabled	This function enables the blinking of the cursor. If you turn off cursor blink, the cursor will be constantly visible.
Cursor Blink Rate	Use the slider to adjust the blink rate of the cursor. This option is not available if cursor blink is disabled.

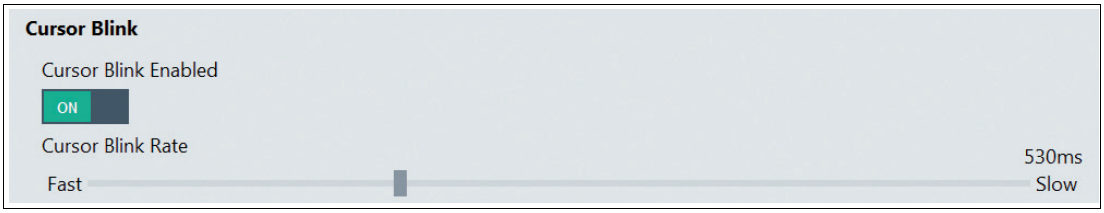


Figure 8.25 Keyboard settings - cursor blink

8.8 Network

Network Adapter Information

This section provides general information about the network adapter and network settings.

Function	Description
Network Adapter Information	All information about the local RM / BTC network adapter hardware is shown.
Network Adapter Name	You can edit the network adapter name according to your needs.
DHCP	Use this option to enable/disable DHCP (Dynamic Host Configuration Protocol). With DHCP, you can integrate the RM / BTC into an existing network without further manual configuration. Settings like IP Address, Subnet Mask, Default Gateway, and DNS Server are addressed then assigned automatically to the RM / BTC. However, you can set up all these parameters manually by disabling the DHCP option.

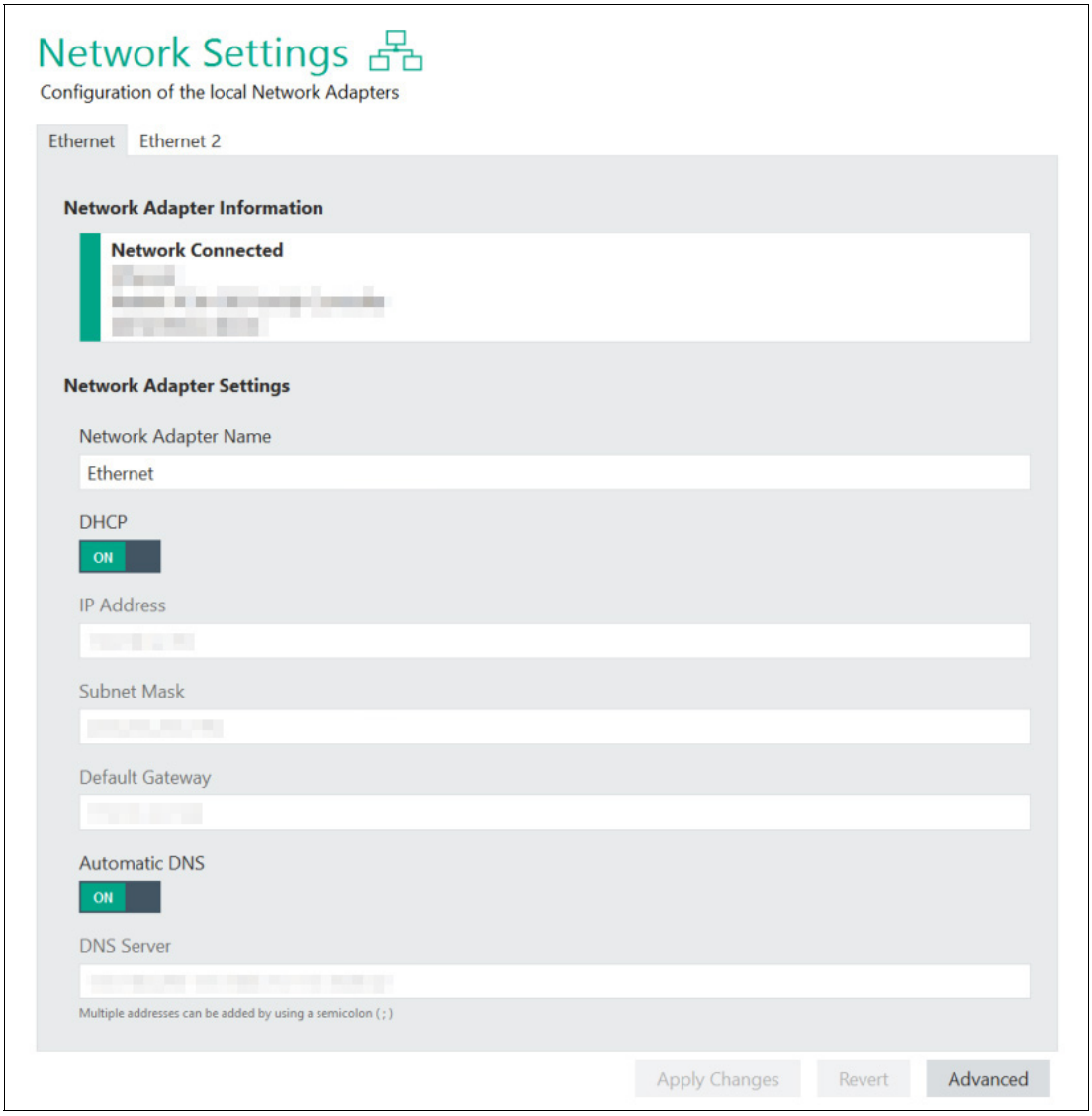


Figure 8.26 Network adapter information and settings

Note

Open Network Ports

The open network ports that are used in RM Shell are listed in the appendix. See chapter 12.1

Note

Advanced Settings

Advanced settings are only available for users who are logged in with the Administrator user role.

8.9 Pad-Ex®

Note

Only valid for Pad-Ex® Industrial Tablet Thin-Client devices.

Navigate to "Pad-Ex" on the navigation bar.

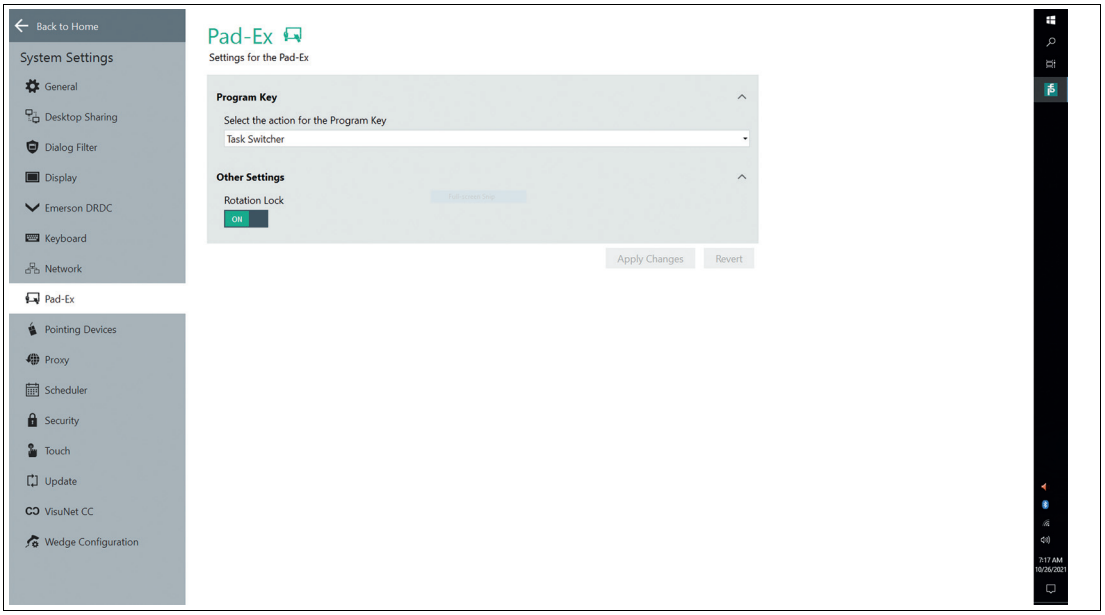


Figure 8.27

Setting the Program Key

1. Select one of the following actions for your program key

Function	Description
None	No function
TaskSwitcher	Switch between multiple remote connections and apps that are running on the RM.
DeviceLock	Input Lock that locks the input and output of the Pad-Ex to avoid unintentional operation e.g. during a transport

Other Settings

Function	Description
Rotation Lock enabled	Default setting This prevents your screen from automatically rotating and locks your screen in its current orientation.
Rotation Lock disabled r	Set the slider to "Off" to disable Rotation lock and enable automatic screen rotation.

8.10 Pointing Device Settings

Note

System Reboot

Changing the mouse settings requires a system reboot.

Pointing Device Sensitivity Settings

In this section, you can set up mouse cursor and double click speed.

Function	Description
Mouse Cursor Speed	Use the slider to adjust the speed of the mouse cursor.
Double Click Speed	Use the slider to adjust the double click speed. Use the range of 100 ms (fast double clicks) to 5000 ms (slow double clicks) to set up the double click speed.

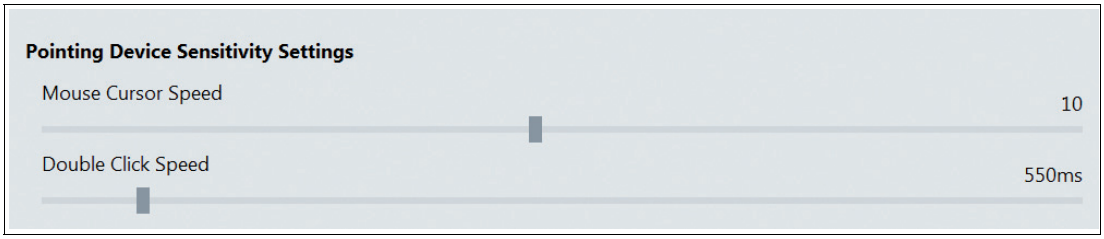


Figure 8.28 Pointing device settings - sensitivity settings

Pointing Device Button Behavior

In this section, you can specify the behavior of the pointing device.

Function	Description
Change Left and Right Keys	Use this option to switch between primary and secondary functions for the mouse buttons. Enable this option to use the right key for primary functions such as selecting or dragging objects.
Hide Pointer While Typing	Use this option to hide the pointer during keyboard input.
Mouse Sonar	Use this option to show the position of the pointer on the screen by pressing CTRL/STRG on the keyboard.

Figure 8.29 Pointing device settings - button behavior

2022-02

Note

Advanced Settings

Advanced settings are only available for users who are logged in with the Administrator user role.

8.11 Proxy Settings

In this section, you can enable the use of a proxy server and specify proxy servers for different communication protocols.

Function	Description
Enable Proxy	Use this option to enable/disable the use of a proxy server.
Use the same proxy settings for all protocols	Enable this option to use the same proxy settings for all communication protocols. If enabled, all other communication protocols are disabled/grayed out. Set the proxy address and the port you want to use for all communication protocols. If disabled, you can set a specific proxy address for each communication protocol.
Do not use proxy for following addresses	You can define a list of addresses that are excluded from the proxy server. Add multiple addresses by separating them with a semicolon.
Ignore proxy server for local settings	Enable this option if you do not want the proxy server to be used for local addresses.

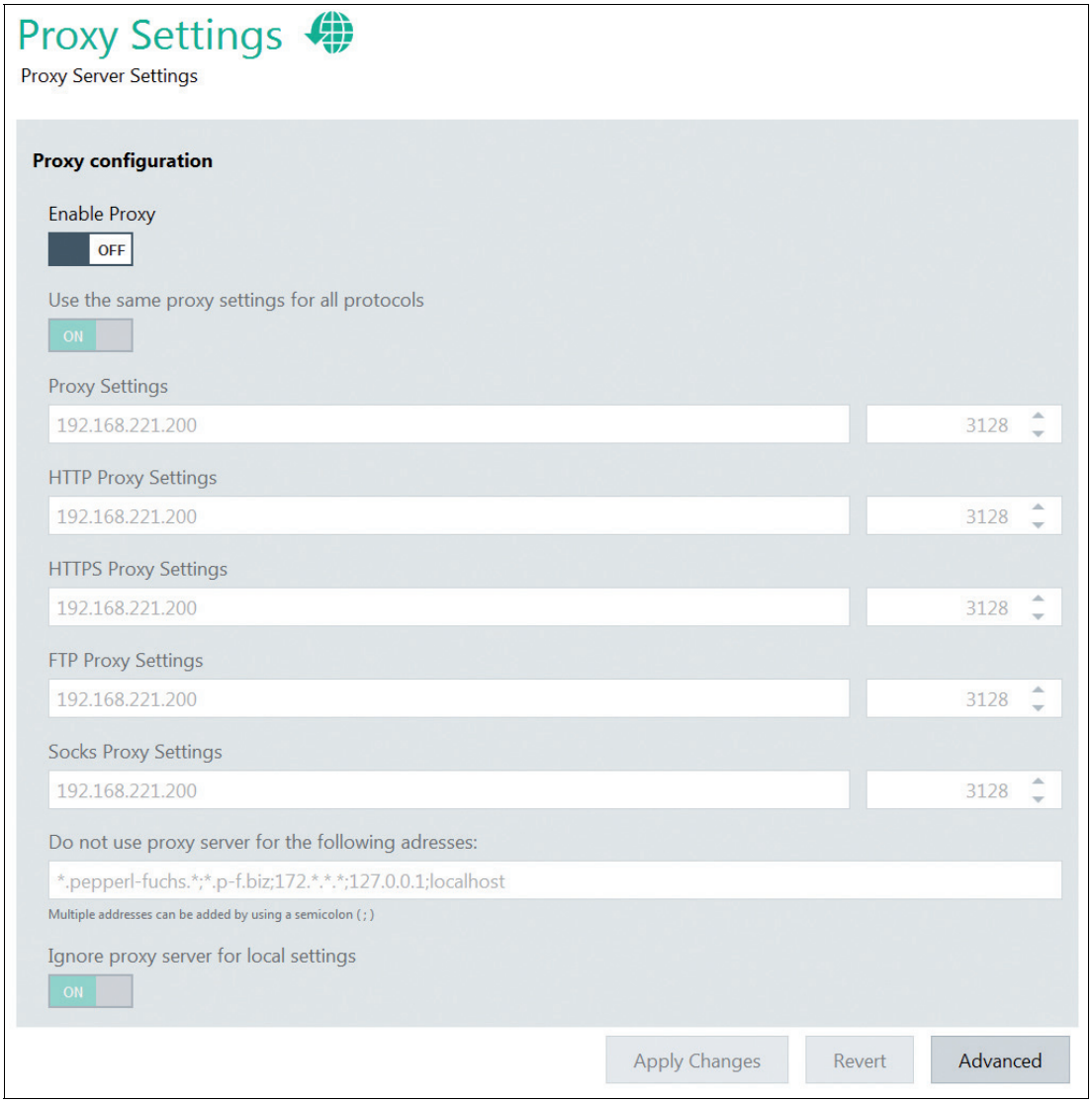


Figure 8.30 Proxy settings

8.12 Scheduler

We highly recommend to enable the scheduler when the unified writing filter is enabled. The scheduler allows you to schedule periodic system reboots. This enables continuous use of the unified write filter without memory buffer overruns.

In the settings menu, you can enable or disable the scheduler, select when and how frequently the system reboots, and choose how long the system must be idle before rebooting.

The system will only reboot when the set idle time is reached.

Figure 8.31 Scheduler settings

Tip

We recommend to enable the Scheduler in 24/7 operation. The system will only reboot when no operation has taken place for the period of the idle time.

8.13 Security

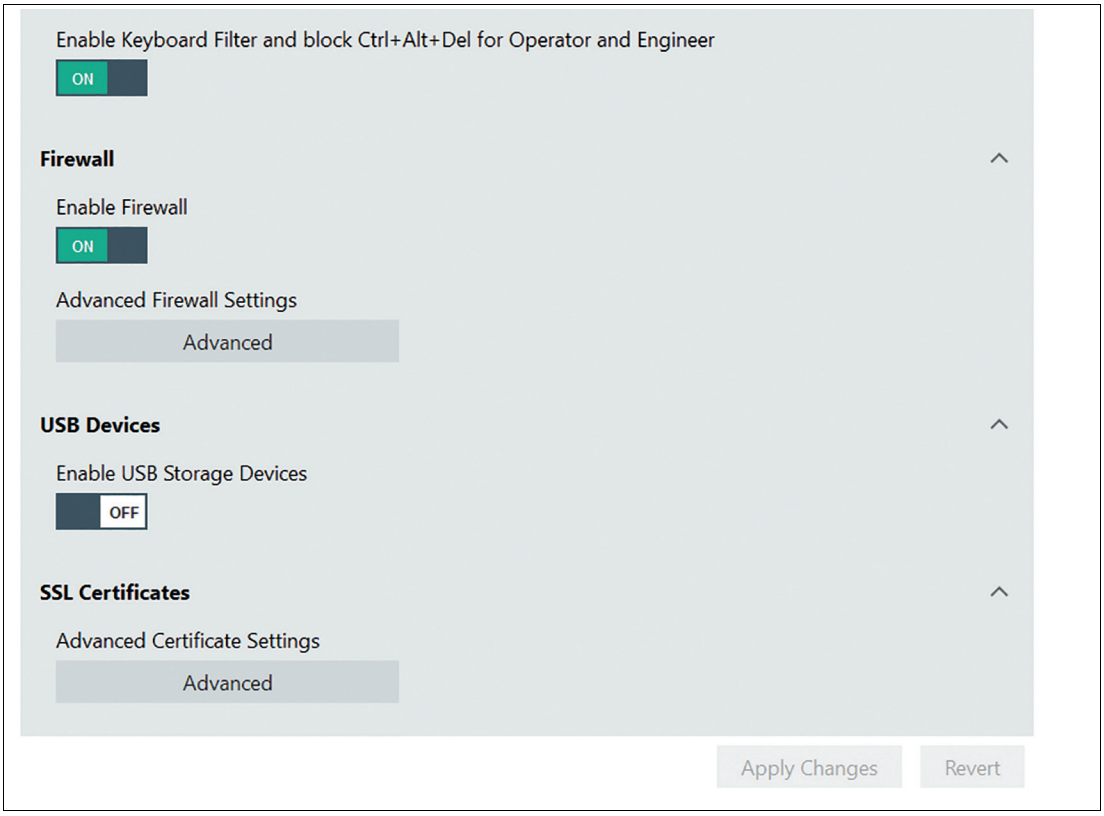


Figure 8.32

Note

For domain users

Filter must be disabled if the device is transferred to a domain and the Windows® autologin is not activated.

For further information refer to the How-To description. See chapter 11.

VisuNet RM Shell and Local Windows® User Passwords

In this section, you can set passwords for the Engineer and Administrator user roles and the local Windows® user.

Function	Description
VisuNet RM Shell Passwords	
Engineer	If you want to protect the Engineer user role with a password, enter a password into the Engineer field. The password is hidden via dots. To view the current password, click . Once the password is set, only users who know the password can log in to the Engineer user role.
Administrator	If you want to protect the Administrator user role with a password, enter a password into the Administrator field. The password is hidden via dots. To view the current password, click . Once the password is set, only users who know the password can log in to the Administrator user role.

Function	Description
Local Windows® User	Set or change the local Windows® user password. The password is hidden via dots. To view the current password, click .
Factory Reset Password	Change the Factory Reset password. The password is hidden via dots and must have at least 6 characters. The field cannot be blank.

Note

The Windows® password can also be changed via the original Windows® settings. In this case, the Windows® Auto-Login is deactivated and the Windows® login screen appears. Therefore it is mandatory to allow "the Keyboard Filter and ctrl+alt+delete".

User Auto Logout

This Setting allows you to enable or disable the function auto Logout for the administrator and engineer role and choose how long the system must be idle before the auto logout occurs.

A timer at the top of the home screen indicates when the logout will occur by displaying the time counted down.

Note

The Auto Logout works for the home screen only. The timer is reset as soon as the mouse is moved, keystrokes are made or a click is detected.

Keyboard Filter Settings

The keyboard filter is enabled per default. If you want to use the Ctrl+Alt+Del function, this filter must be disabled. This can be useful for system domain integration e.g. sign-out function.

Firewall

In this section, you can adjust the firewall settings.

Function	Description
Firewall	Enable/disable this option to activate/deactivate the Windows® firewall on the RM.
Advanced Firewall settings	Click "Advanced" to open the Windows® dialog box for firewall settings.

Figure 8.33 Security settings - firewall

USB Devices

In this section, you can enable or disable external USB storage devices (e.g., pen drives, external hard disks, etc.).

If the option is turned off, the user cannot access any external USB devices that are connected to the RM. The recommended default setting is "OFF."

Figure 8.34 Security settings - USB devices

SSL Certificates

In this section, you can edit the Microsoft-specific advanced certificate settings.

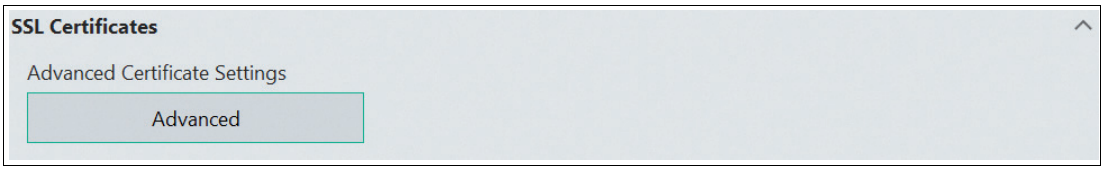


Figure 8.35 SSL certificates - edit Microsoft-specific certificate settings

8.14 Touch Settings

This menu allows you to change VisuNet GXP touch settings, if your RM is equipped with a touch screen option. Select the appropriate sensitivity level from the drop-down menu, and click the "Calibrate" buttons to calibrate accuracy and sensitivity.

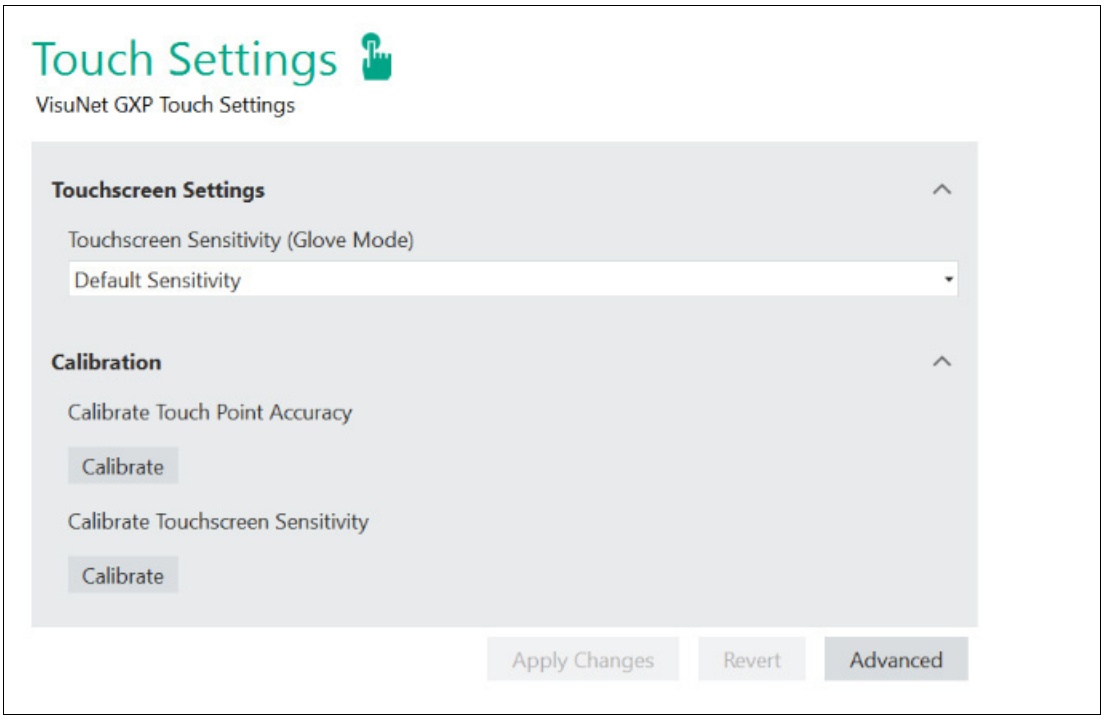


Figure 8.36 Touch settings

8.15 Update

In this section, you can update the VisuNet RM Shell to latest version or use the Cleanup System to clean up the disk. The update submenu is only available for the Administrator user role.

There are 3 ways to update the VisuNet RM Shell:

- Update via local device (e.g., USB flash drive)
- Update via network share
- Update via VisuNet CC (single device or update of multiple devices with the Update Firmware Wizard)

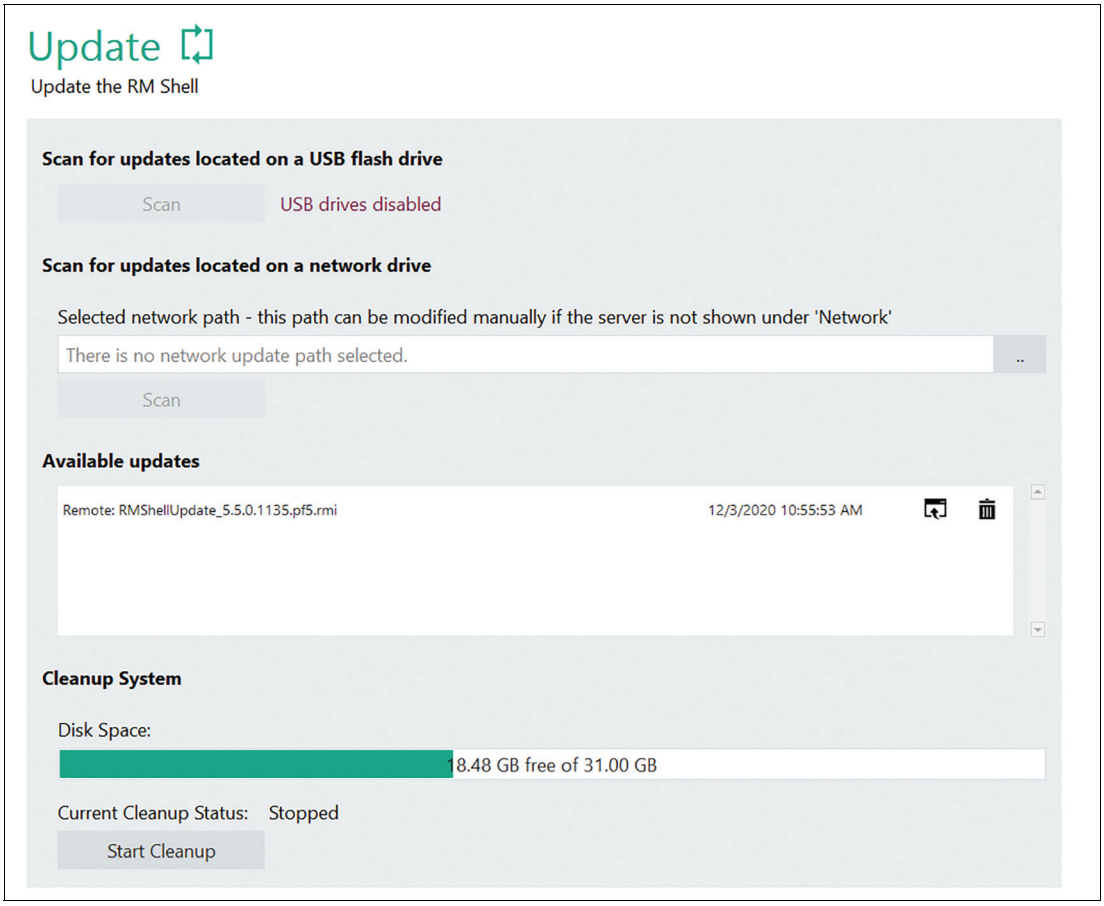


Figure 8.37 System settings: update

Updating via Local Device (USB flash drive)

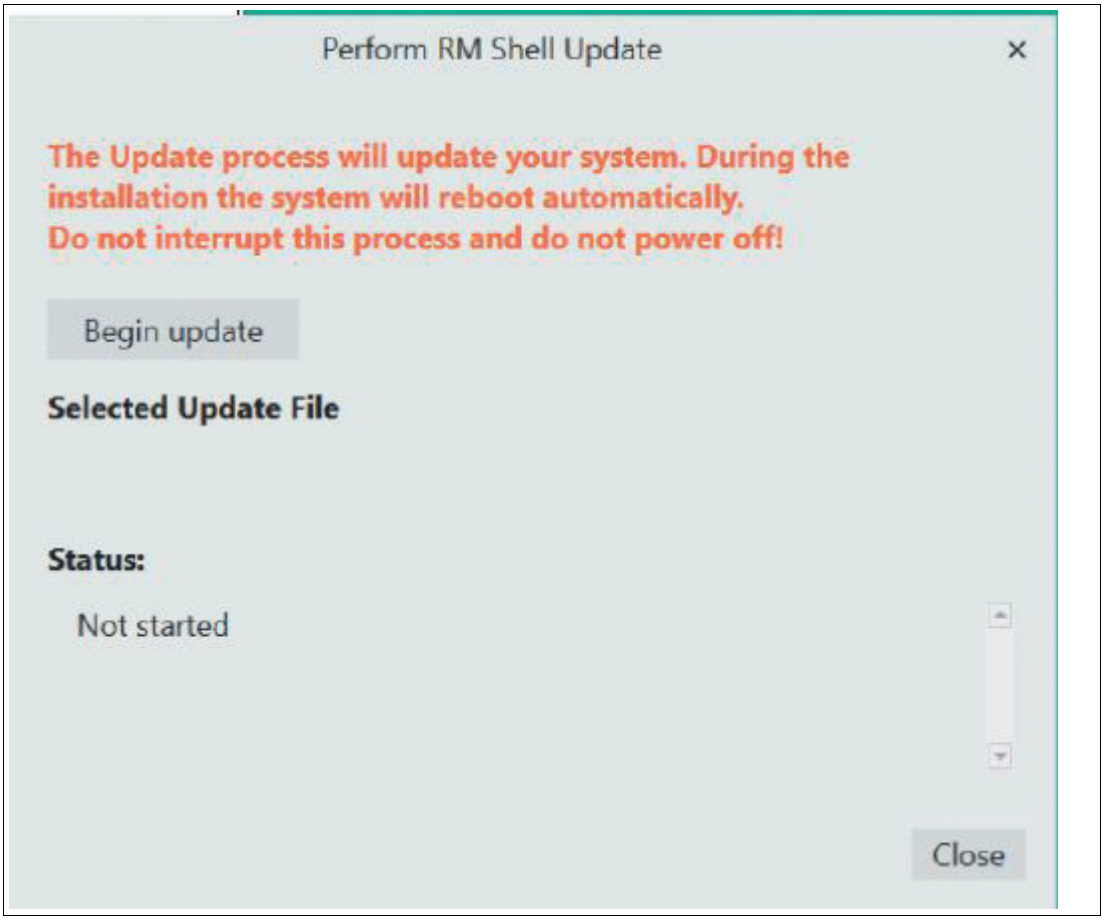
You can update the VisuNet RM Shell by using a local device (USB flash drive) with the current update files.

Updating via local device

1. Connect the local device to the RM.
2. In the "Find update" section, click Scan.

   ↳ VisuNet RM Shell scans for local devices connected to the RM. The scanned update file appears in the "Available updates" section. The local device's name is shown as prefix.
3. Choose the requested update by clicking .

   ↳ The "Begin update" dialog box opens.



4. To begin the update installation process, click Begin update.

   ↳ The update installation process starts. During the installation process, the RM reboots twice.

Updating via network share

1. Create a share folder to locate the update there.
2. Open the path and scan in the selected folder for the available update

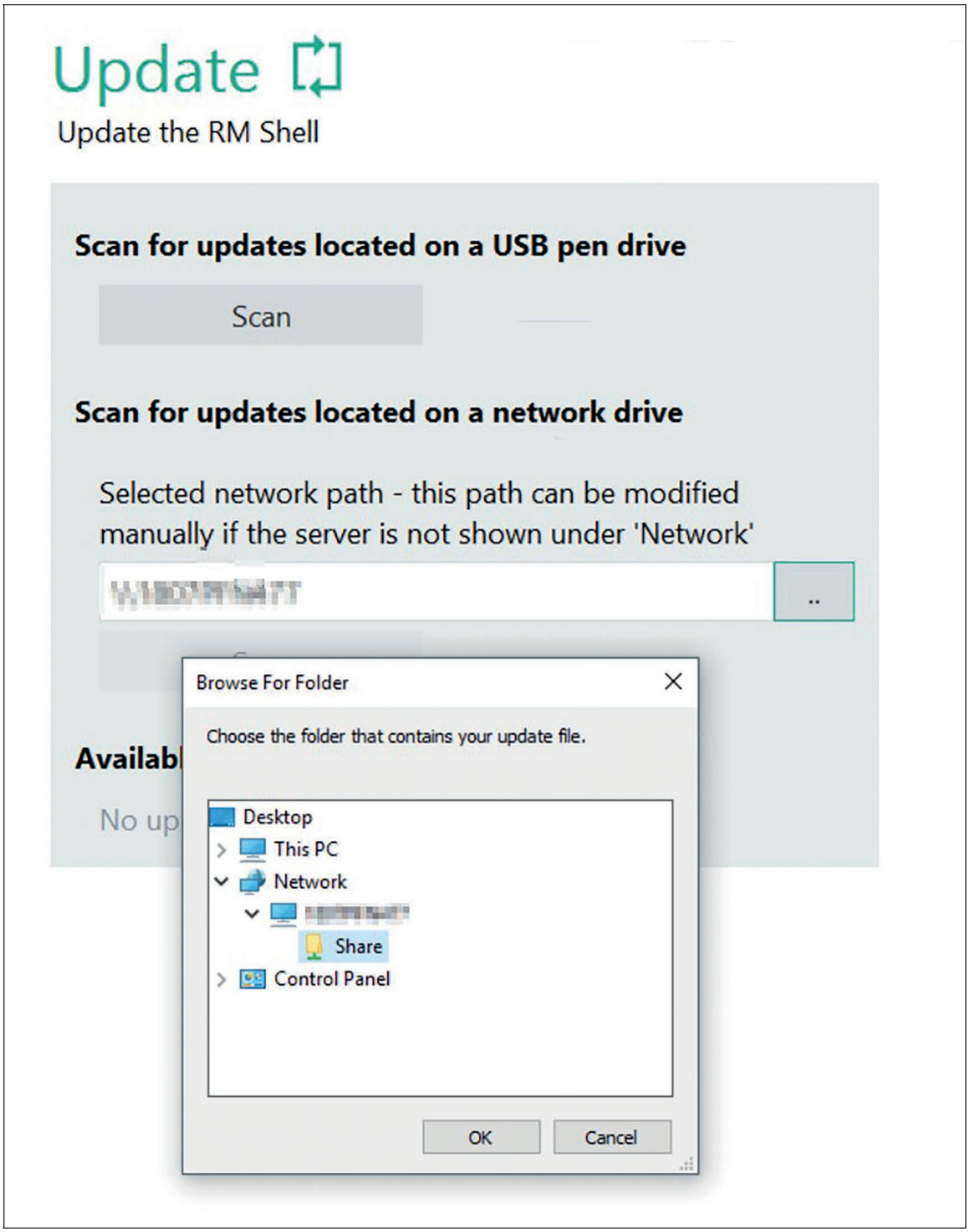


Figure 8.38

3. The available update appears in the list
4. Click “Begin Update” to start the installation.

2022-02

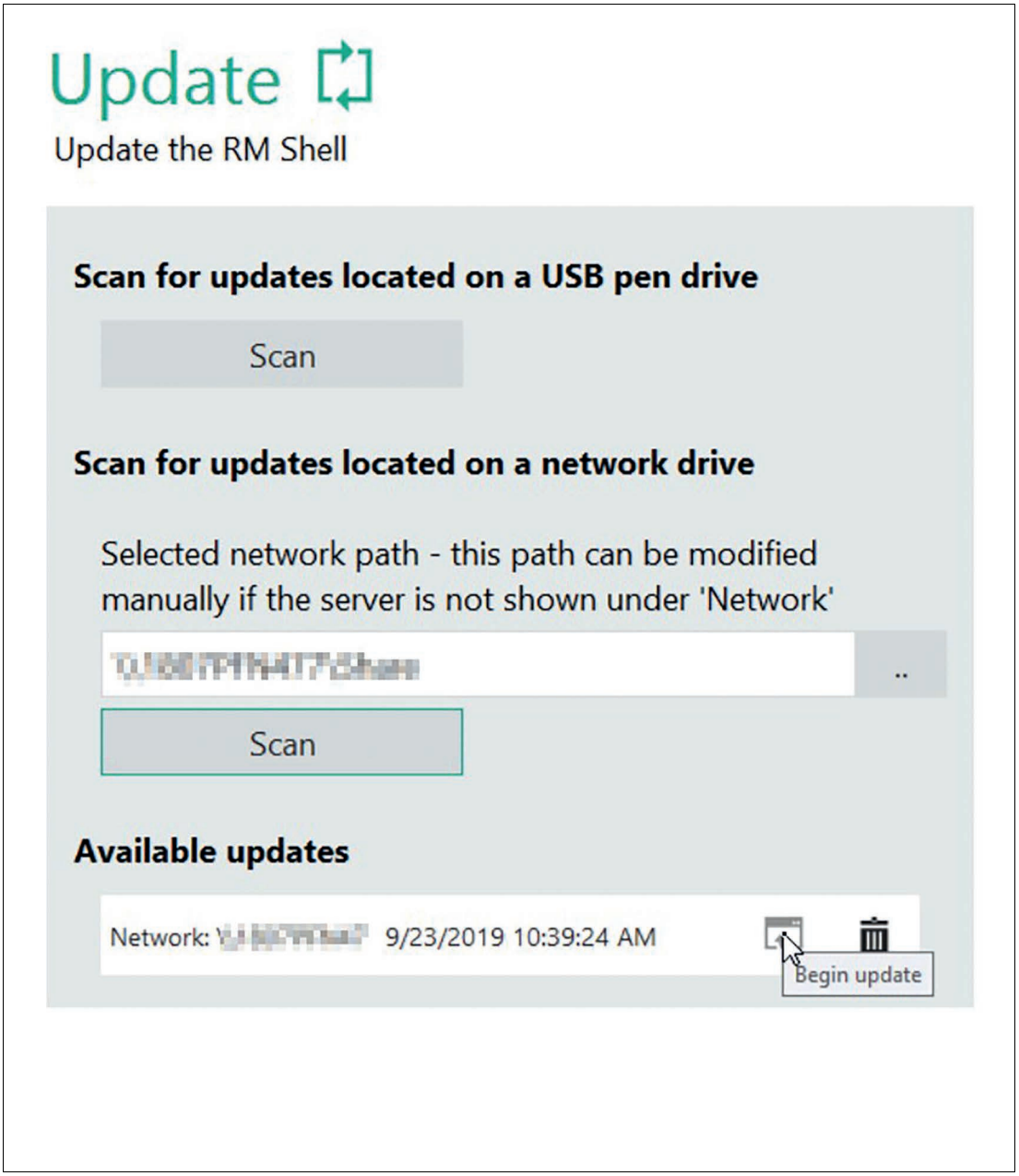


Figure 8.39

For further information on how to perform an update via VisuNet Control Center refer to the VisuNet CC manual.

Cleanup System

Cleaning your device frees up your drive space and helps it run better by deleting temporary files and reduce the size of the WinSxS folder. From VisuNet RM Shell version 5.5.0 on the available disk space is visualized.

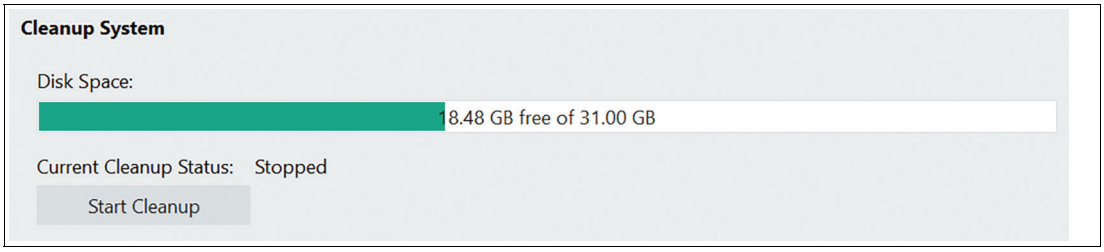


Figure 8.40

Note

The Cleanup process might run for several hours. During this time the device can be operated but might get slower. It is recommended to perform the Cleanup Disk Wizard only when the disk space is running low.

Note

If your storage after cleaning up the disk is still not sufficient for updates or installing 3rd party software we recommend updating your device with the latest factory reset version >6.0 available at www.pepperl-fuchs.com. Due to the adapted partition design of the latest update the available storage has increased considerably.

8.16 VisuNet CC Settings

Note

To use VisuNet Control Center an additional licence is required. Find more information of VisuNet CC online at: pepperl-fuchs.com

You have the ability to enable/disable VisuNetCC connectivity and configure some of the pertinent connection timeout settings. The preconfigured settings are considered the defaults. Changing them is not advised unless you are experiencing problems. For slow connections within the network we recommend to increase the open/close timeout.

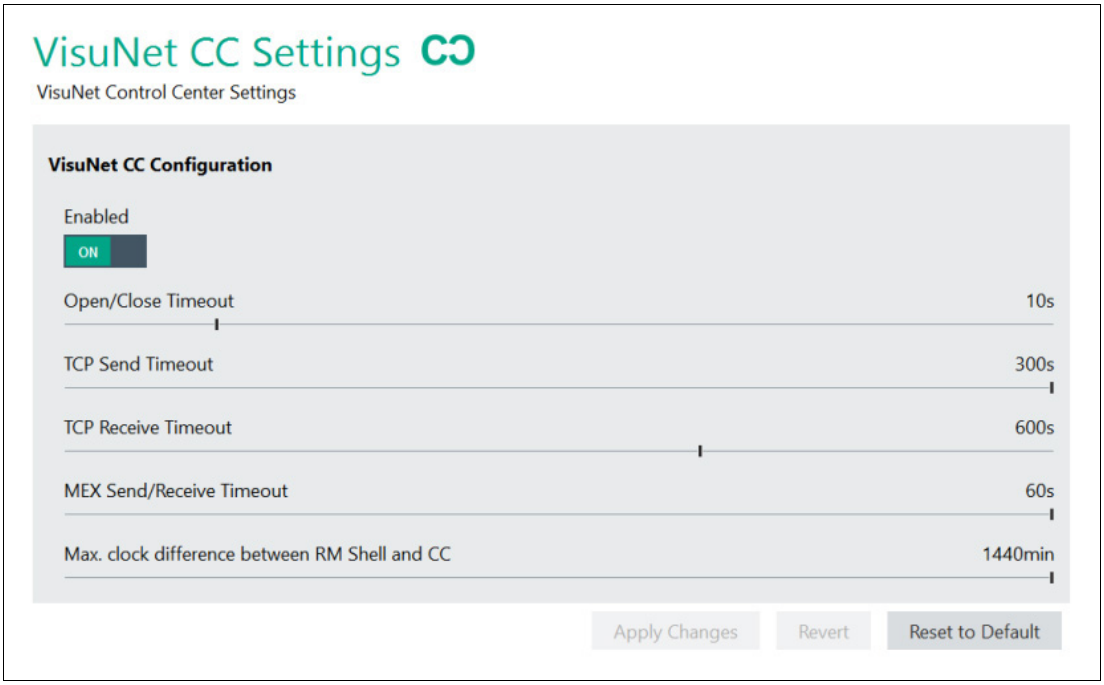


Figure 8.41 VisuNet CC settings

8.17 Wedge Configuration for Scanners With Serial Interface

General Settings

Function	Description
Input Character Delay	Use the slider to configure the delay: • 0 ms: no character delay • 200 ms: greatest delay
Remote Text Input Mode	Different modes for translating the incoming data of the serial interface can be used: • Keystroke simulation mode (default and recommended) uses Windows® Input Simulator functionality to send characters as single keystrokes. This mode is limited to keyboard characters and offers limited ability to send special characters. • Alt+ASCII mode sends characters using ALT+ASCII simulation. This mode supports special characters but may have issues with RDP connections.
Hide the Wedge App from the Operator on Main view	When activating this function, the Operator is not shown the Wedge App.

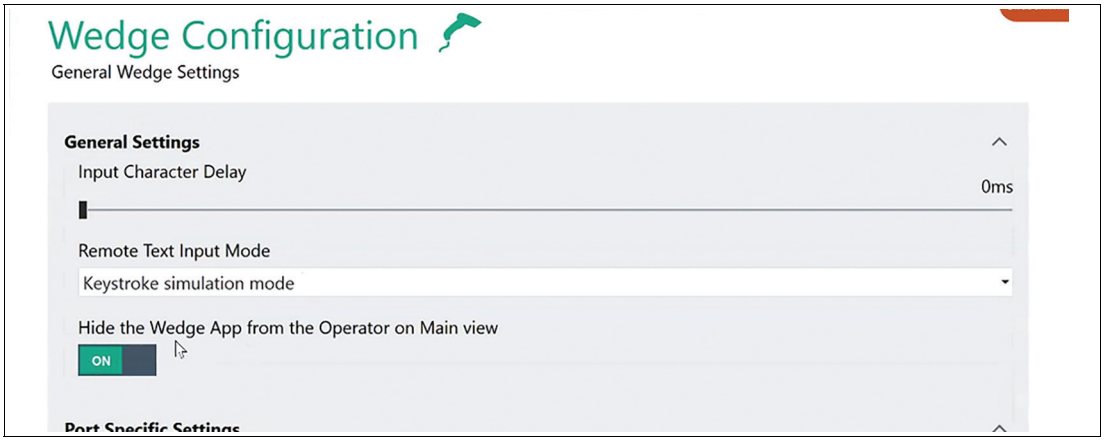


Figure 8.42 S2K Wedge configuration: general settings

Port Specific Settings

Choose the serial port that the barcode scanner is connected to and configure it by clicking the corresponding tab.

Figure 8.43 COM port selection (in this example COM1 is selected)

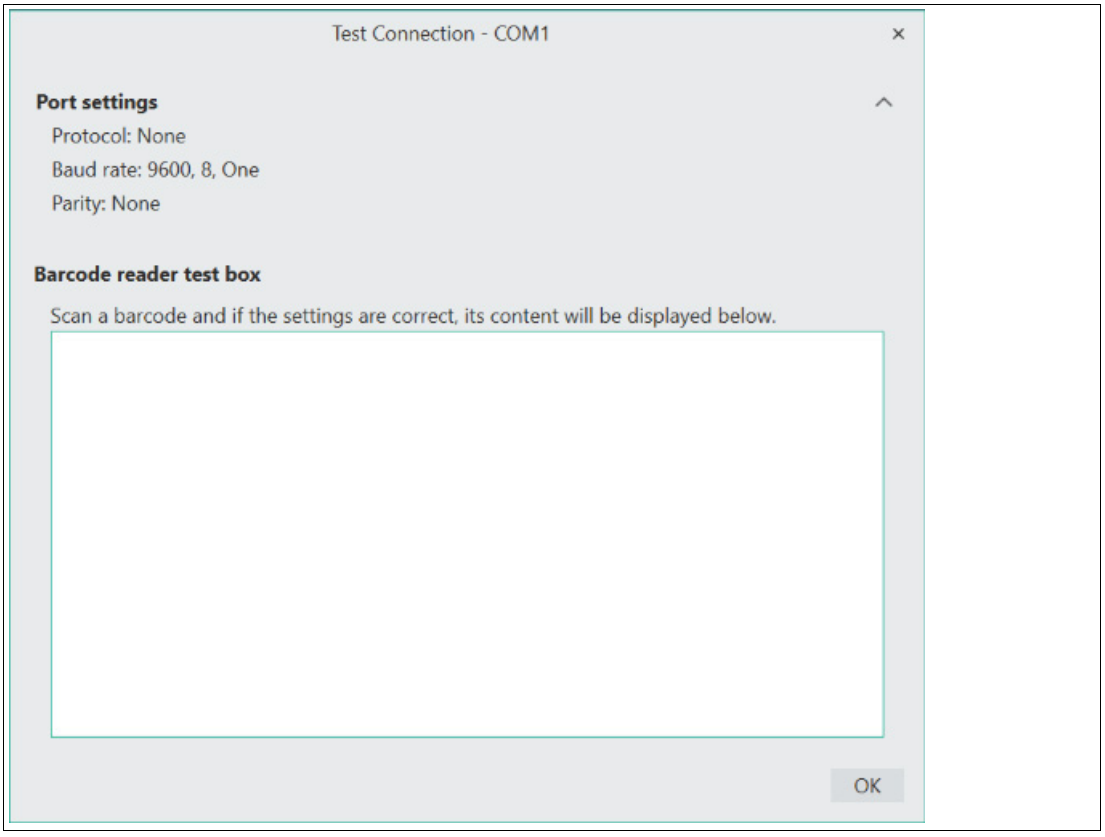
Test Connection

To test if a PSCAN device is set up and connected properly, use the "Test connection" functionality.

Testing the COM Port Connection

1. Choose the tab of the COM port that you want to test.
2. Click Test Barcode reader.

   ↳ The "Test Connection" window opens. In the "Port Settings" section, all settings of the corresponding COM port are shown:



3. Use your PSCAN device to scan a barcode.

   ↳ If all settings are set up properly, the barcode content is displayed in the "Barcode reader test box" field.

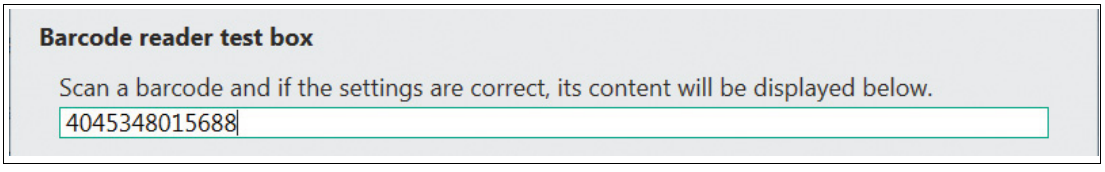


Figure 8.44 Scanner test box

4. To end the test, click OK.

All ports known to the operating system, including those already occupied by other programs, are offered.

Function	Description
Protocol	This dropdown list determines the protocol that is used to transfer data.
Stop Bits	Specify the number of stop bits here. There is usually one stop bit.
Data Bits	Choose the number of data bits here. 5, 6, 7 and 8 are permissible values. There are usually 8 data bits.
Baud rate	Choose the data transfer speed. The default setting for barcode scanner is 9600 baud.
Parity	This box specifies whether the parity check bit should be computed, and if so how.
Auto Connect	If enabled, the VisuNet RM Shell automatically opens the serial port and establishes a connection to the barcode scanner, if the RM is (re-)booted.
Visible on Operation screen	If enabled, the serial port is visible as a serial port in the VisuNet Wedge App.

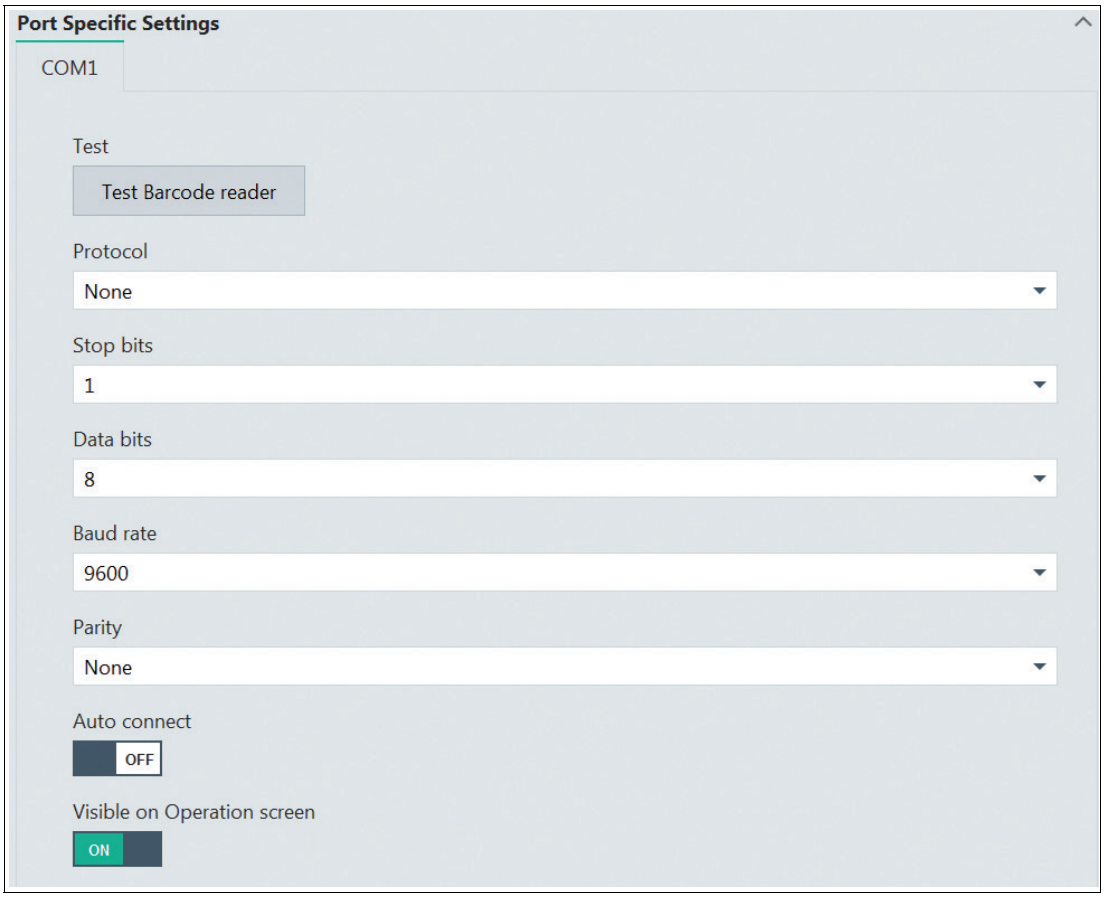


Figure 8.45 Wedge configuration - port specific settings

Function Key Emulation

The character strings from the serial port are transferred into keystrokes according to the mapping table. This allows you to emulate a keyboard input with the barcode scanner and to send the inputs to your host PC. The character strings consist of actual content and - depending on the barcodes you scan—so-called control characters. Control characters do not contain content but trigger various actions. In the function key emulation section, you can configure different actions for each control character by using the drop-down list.

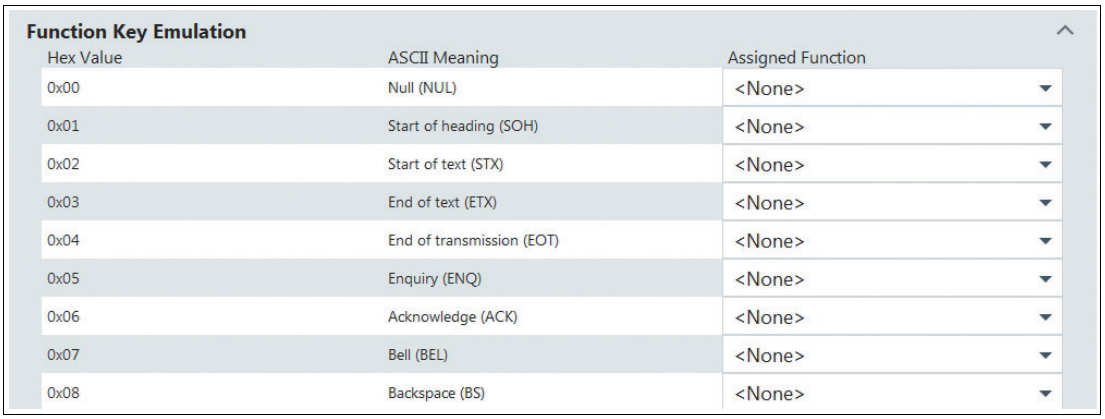


Figure 8.46 Wedge configuration - Function Key Emulation

9 System Tools App

Entering the System Tools App

1. To enter the system tools app, click the appropriate icon on the home screen 

.

When entering the System Tools app, you always start at the Clean Lock submenu. There are several additional submenus:

9.1 Clean Lock

In this submenu, you can lock all your input devices (such keyboard, touch screen, touch pad, etc.) for cleaning purposes. This protects the RM from accidental inputs during the cleaning process.

Use the slider to adjust the length of time that the input devices will be locked.

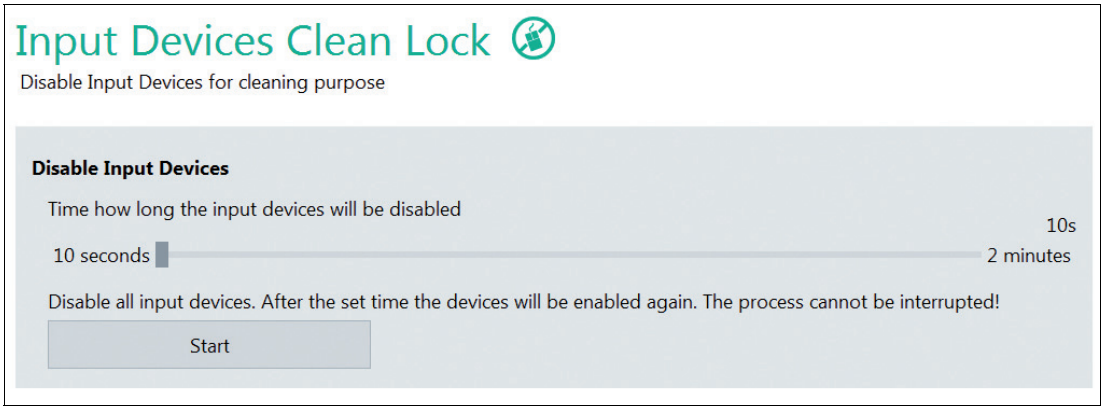


Figure 9.1 System tools - clean lock settings

Note

It is possible to hide the System Tools App in the Operator mode via General Settings. Refer to chapter 7.1.

9.2 Network Adapter Information

In this submenu, you can find all information on the network adapter hardware of the local RM.

The color of the bar in front of the network adapter's name indicates the status of the connection:

green	the network adapter is connected.
orange	the network adapter is not connected or an error occurred.

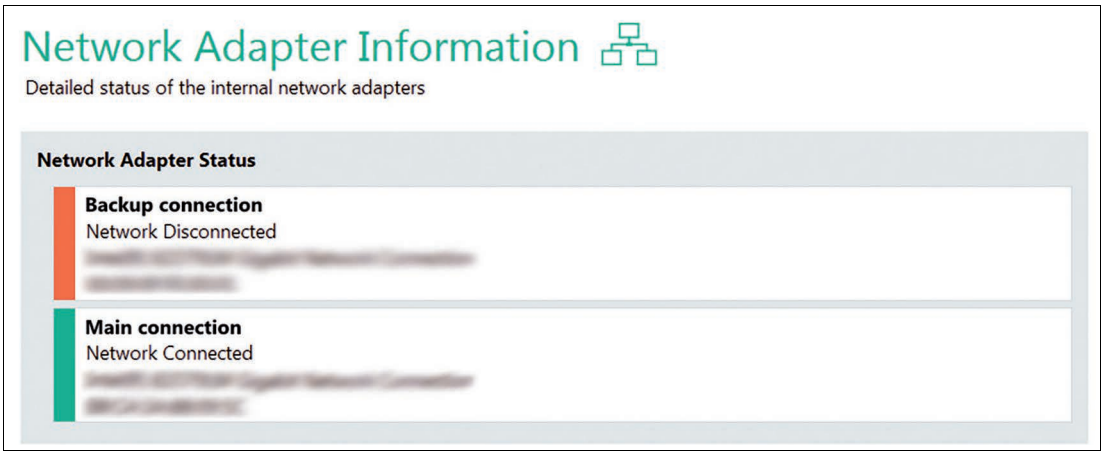


Figure 9.2 System tools: network adapter information

9.3 Network NSLookup Tool

With the Network NSLookup Tool, you can check the domain name of an IP address or the IP address of a domain name.

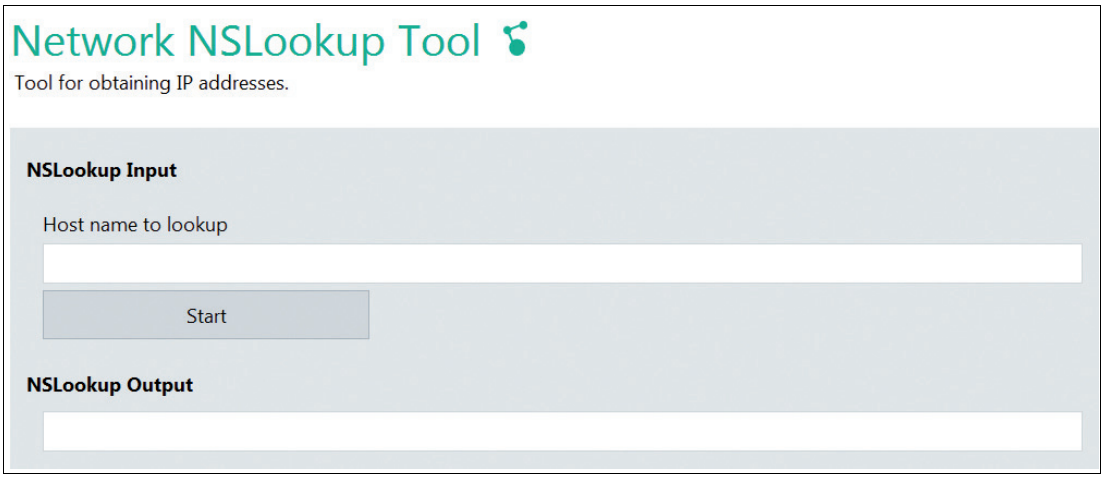


Figure 9.3 Network NSLookup Tool

Checking a domain name

1. In the "Host name to lookup" field, type in the IP address.
2. Click "Start."

↳ The corresponding domain name is displayed in the "NSLookup Output" field.

Checking an IP address

1. In the "Host name to lookup" field, type in the domain name.
2. Click "Start."

↳ The corresponding IP address is displayed in the "NSLookup Output" field.

9.4 Network Ping Tool

In this submenu, you can test the network settings and check, for instance, if the host is reachable via Ethernet.

In the ping input section, enter the IP address or computer name of computer that you would like to ping and click "Start."

The ping status section shows detailed information on the network connection.

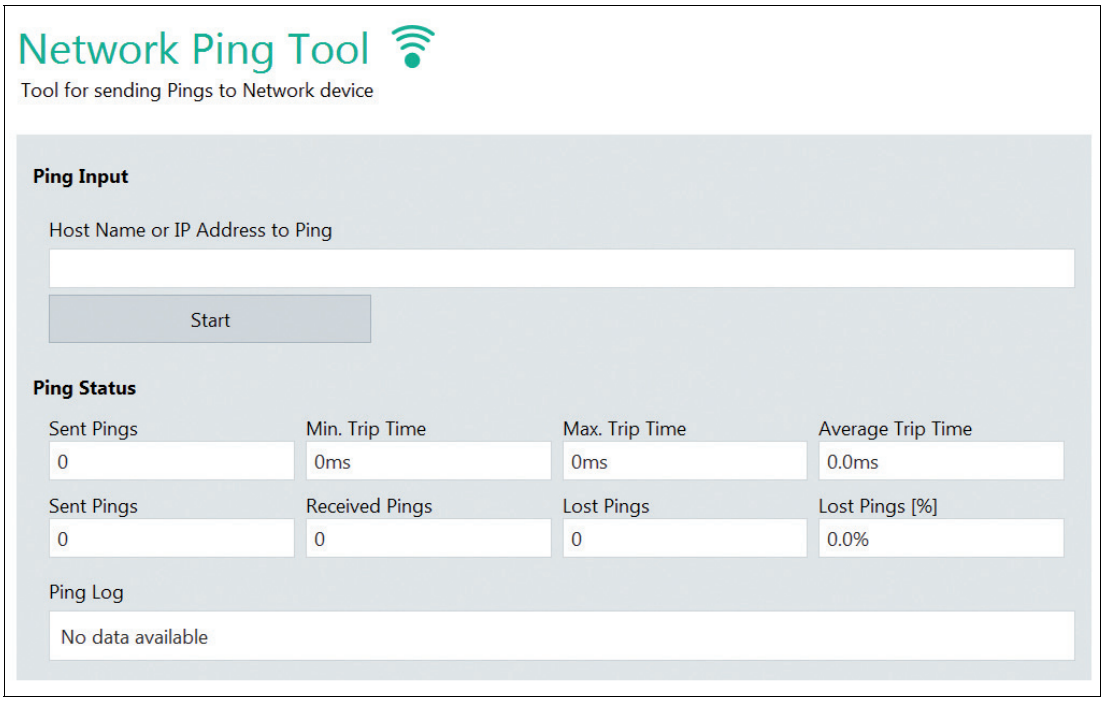


Figure 9.4 System tools - network ping tool

10 Factory Reset

Note

To be able to apply and capture image files, VisuNet RM Shell version 5.3 and newer is required.

Performing a factory reset for a device with resistive touch screen the additional use of a keyboard and mouse is required.

Find the currently installed firmware version number in the VisuNet RM Shell Factory Reset Menu "Device Info".

Tip

Use the additional software VisuNet Control Center to easily capture and apply image files to multiple compatible devices within the network. Get further information of VisuNet CC at www.pepperl-fuchs.com.

Enter the Factory Reset via VisuNet RM Shell

1. From the main screen, change "Users" to "Administrator".
2. Click "System Settings".
3. Navigate to the "General" tab.
4. Expand the "Factory Reset" section.

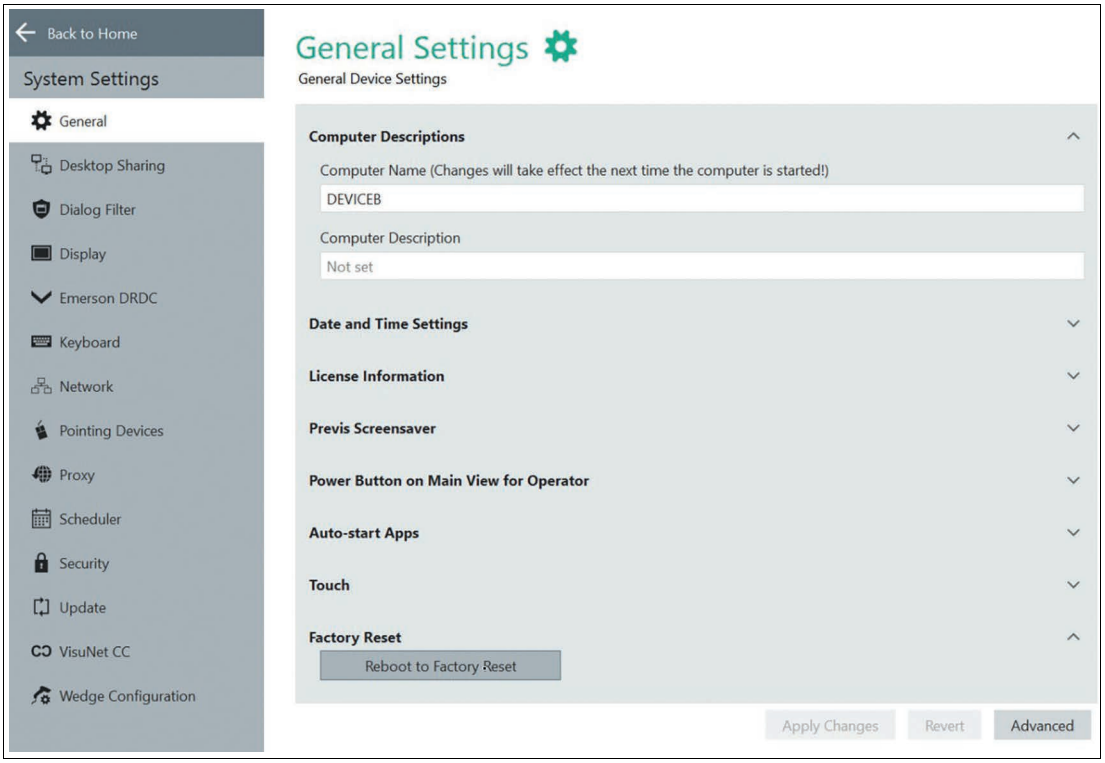


Figure 10.1

Enter the Factory System when the RM Shell is crashed

1. Power off the unit completely.
2. Power the unit back on. During the initial boot sequence, repeatedly press the "F9" key.
3. When you see a menu on a blue or black background, stop pressing the "F9" key.

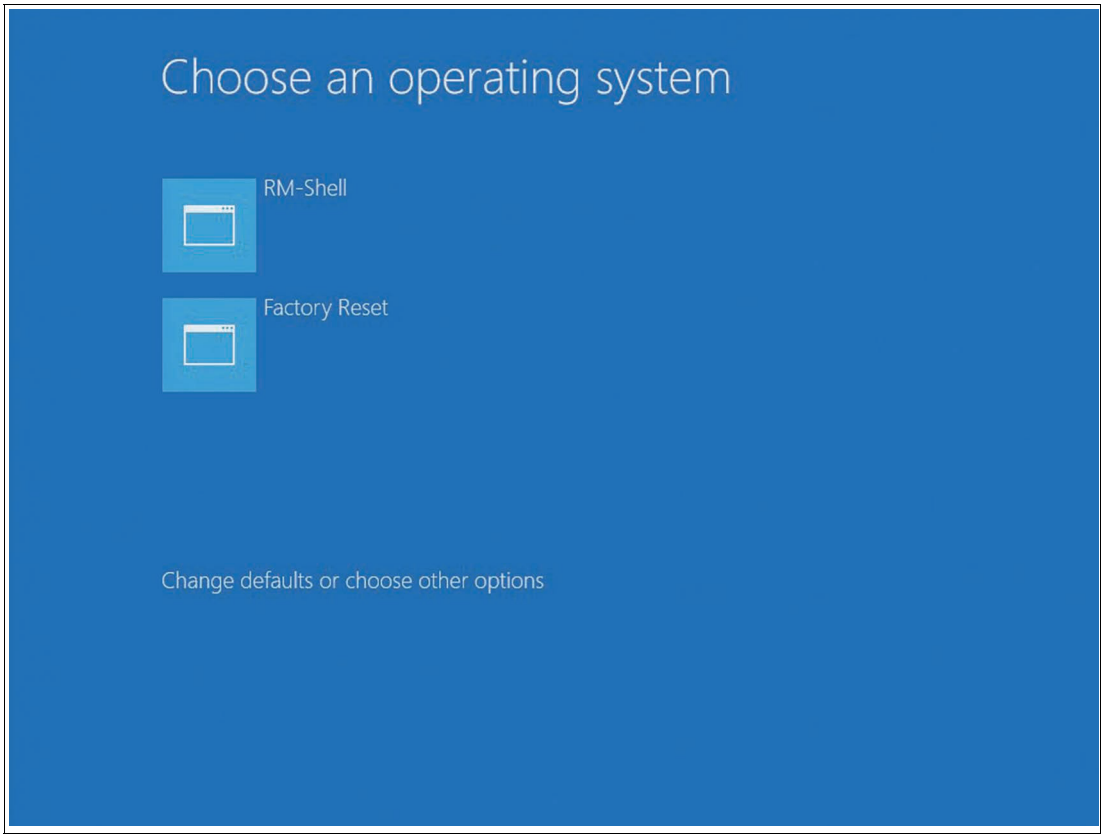


Figure 10.2

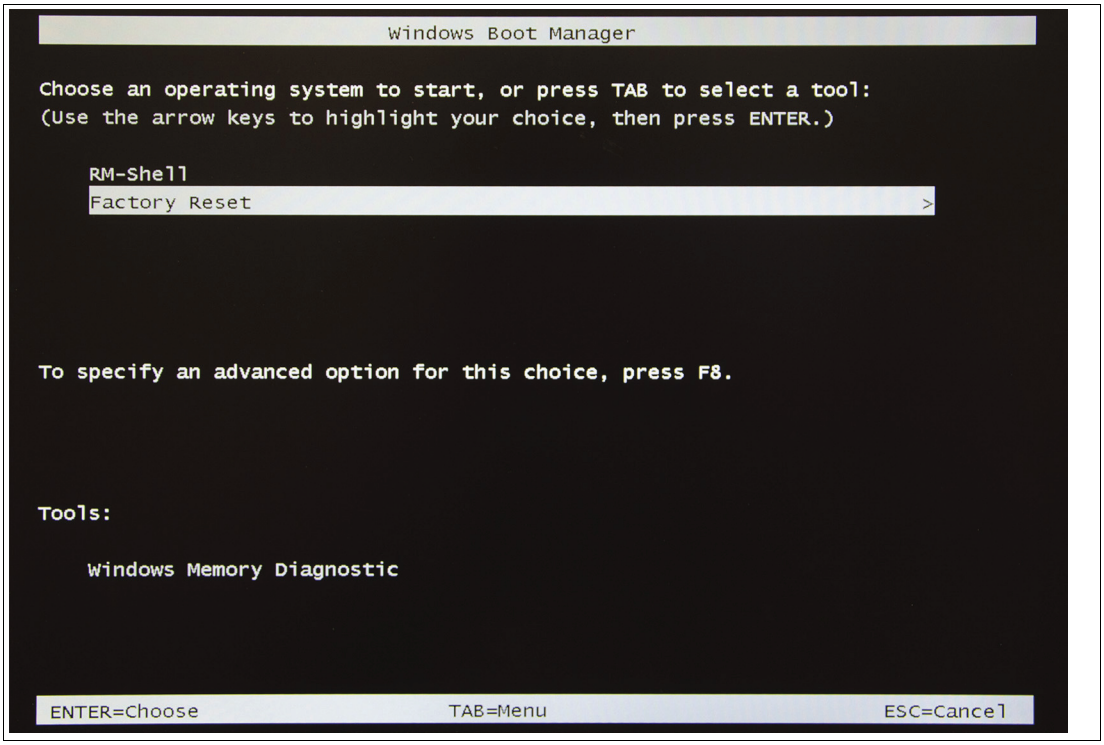

Windows Boot Manager
Choose an operating system to start, or press TAB to select a tool:
(Use the arrow keys to highlight your choice, then press ENTER.)
RM-Shell
Factory Reset
To specify an advanced option for this choice, press F8.
Tools:
Windows Memory Diagnostic
ENTER=Choose
TAB=Menu
ESC=Cancel

Figure 10.3

Login in to the VisuNet RM Shell Factory Reset Management

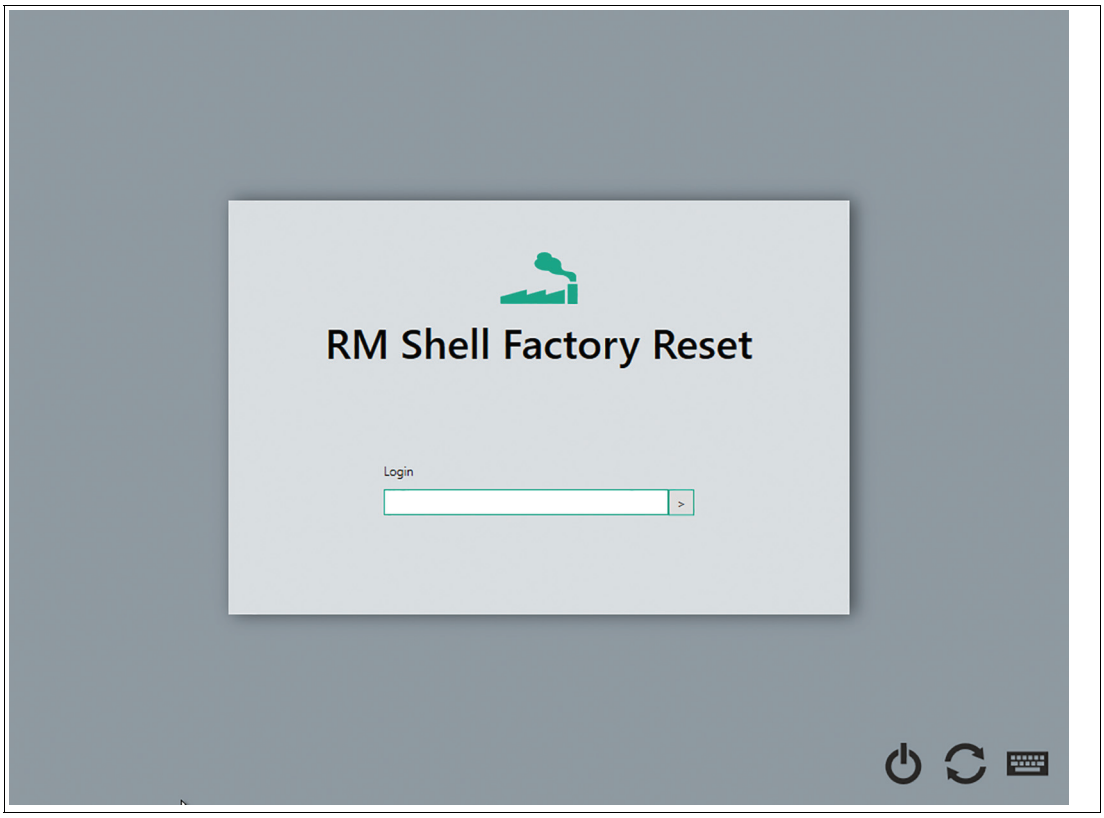


Figure 10.4

↳ Use the default Login password **VisuReset** to log in to the RM Factory Reset Management tool.

Note

Open the onscreen keyboard by clicking  . It might take up to several seconds until the onscreen keyboard opens.

10.1 Change Password

Change the default login password

After logging in you are immediately asked to change the default login password.

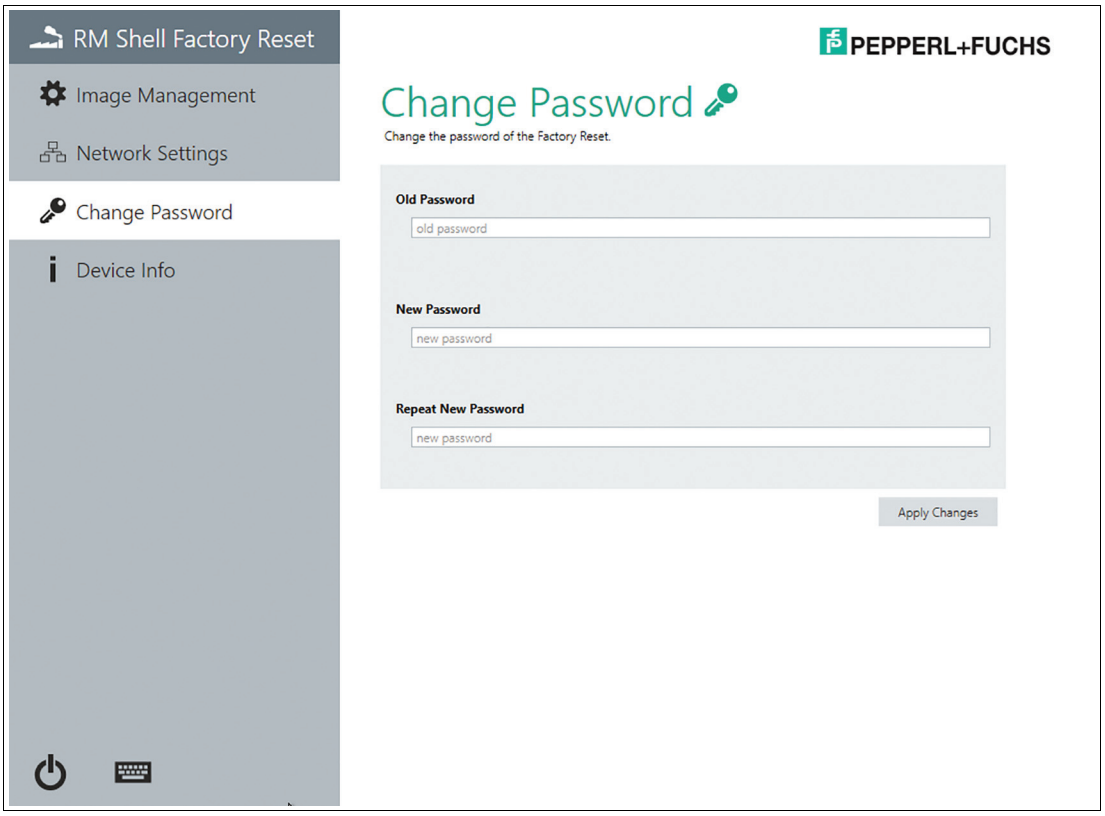


Figure 10.5

Note

To ensure the highest level of security, the password needs to be at least 6 characters long.

The password can be adjusted anytime required. You will be informed via brief notes in orange in the event of deviations while changing the password.

10.2 Image File Management

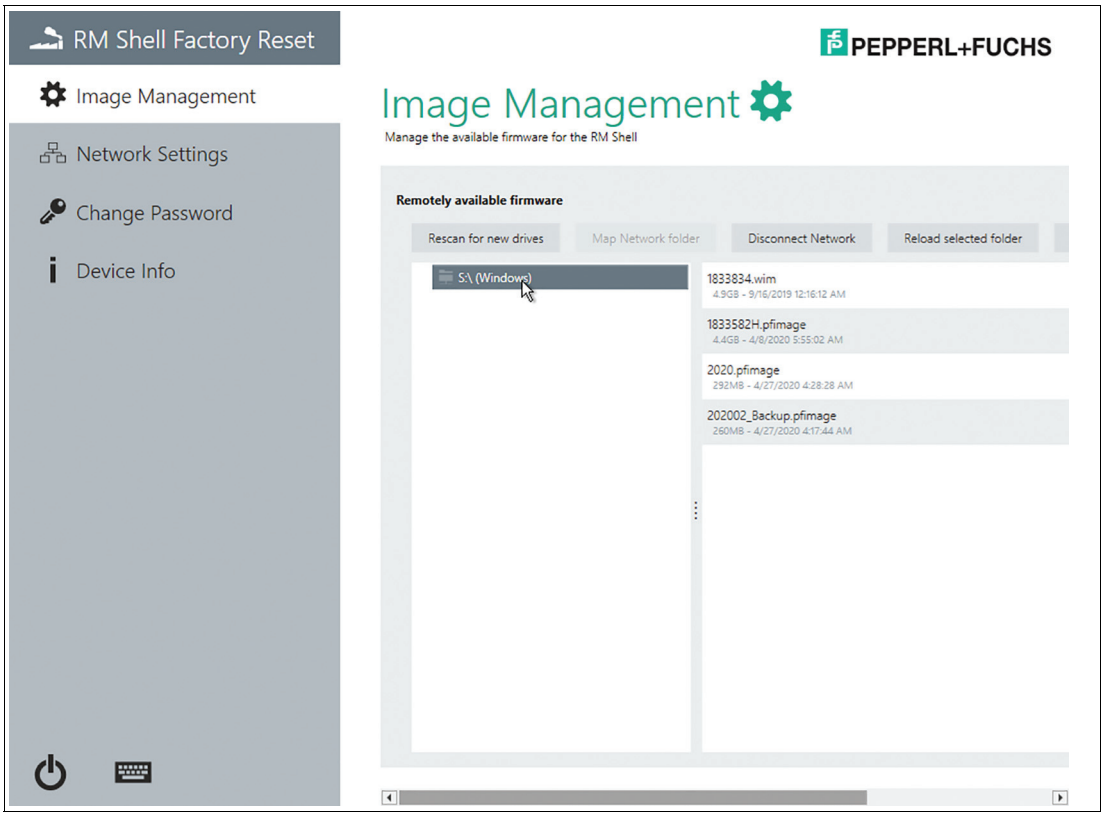


Figure 10.6

In this submenu you can manage the available firmware for the VisuNet RM Shell.

Rescan for new drives	Searches for connected USB flash memory drives. USB flash-drives can directly be used to transfer image files.
Map Network folder	To apply or capture an image file, select the network folder first. The image file is either applied on the RM/BTC from which the network is connected to or captures the image of the RM/BTC and stores it in the network folder.
Disconnect Network	Only one network folder can be mapped. To connect to another path, you must disconnect the existing path connection first.
Reload selected folder	If any updates or changes have been performed in the connected folder during the connection, use this button to reload the data.
Capture Backup Image	Map a network folder which is available inside the network of the RM/BTC first. The device settings of the RM/BTC are captured as a backup image and will be stored in the selected network folder. This backup can only be applied to the same device/device with the same serial number. **Attention:** For each image file about 7 GB storage is required. This depends on the used disk space of the devices. Make sure that the Net-work Share has enough storage. The capture process takes about 30 minutes, depending on the network speed.

Note

Refer to chapter 2.1 regarding the available image files.

2022-02

Capture Backup Image

1. Select the **Network Share**, which will be used to transfer the "Image Files". Make sure that the Network Share has enough storage (~ 7 GB are required for each image file)
2. Set the name for your image file and proceed with the capturing process.

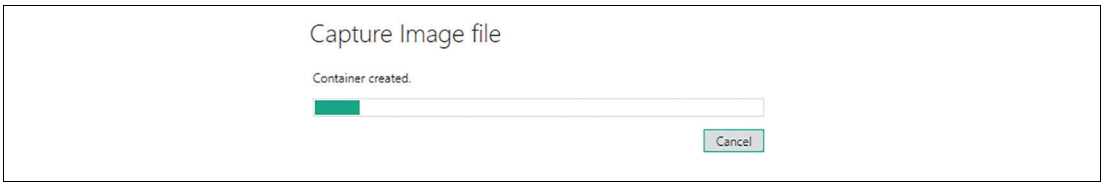


Figure 10.7

Apply Backup Image or an official Pepperl+Fuchs Image

1. Select the Network Share, which will be used to transfer the image files.
2. Choose the image files that you want to apply. You can either apply an image file which was earlier captured from your RM/BTC with the same serial number/same device or an official Pepperl+Fuchs image which is available for each specific RM or BTC.
Contact your local sales support if you would like to apply the official Pepperl+Fuchs image.

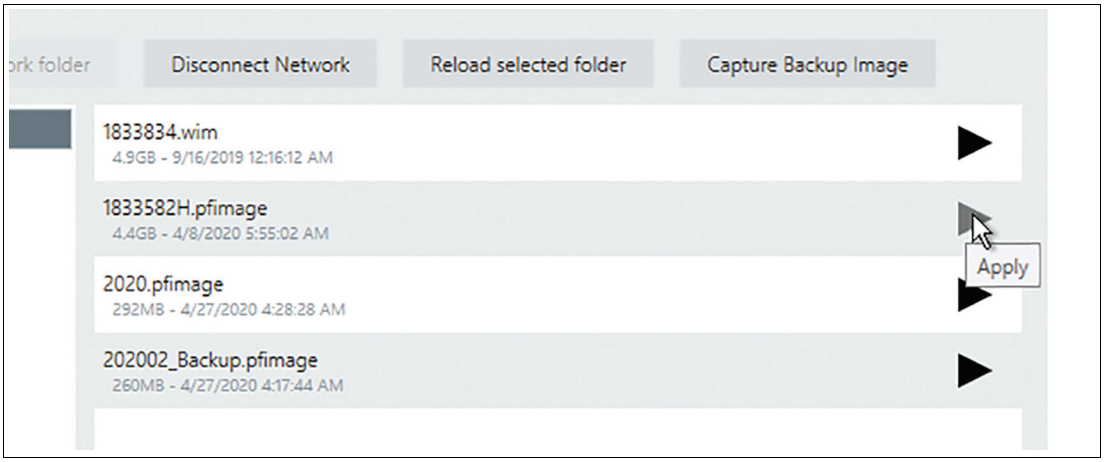


Figure 10.8

3. Click Apply to apply the selected firmware.

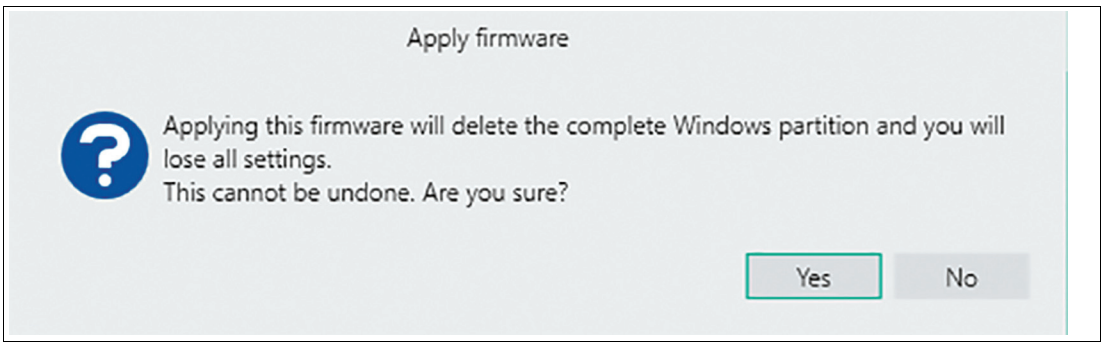


Figure 10.9

4. After clicking **Yes**, the complete Windows® partition will be deleted and the selected image file will be applied to your device. The apply process takes around 15 minutes. The system will reboot after the image file has been applied.

10.3 Network Settings

This section provides general information about the network settings.

Use this option to enable/disable DHCP (Dynamic Host Configuration Protocol). With DHCP, you can integrate the RM / BTC into an existing network without further manual configuration. Settings like IP Address, Subnet Mask, Default Gateway, and DNS Server are addressed and assigned automatically to the RM / BTC. However, you can set up all these parameters manually by disabling the DHCP option.

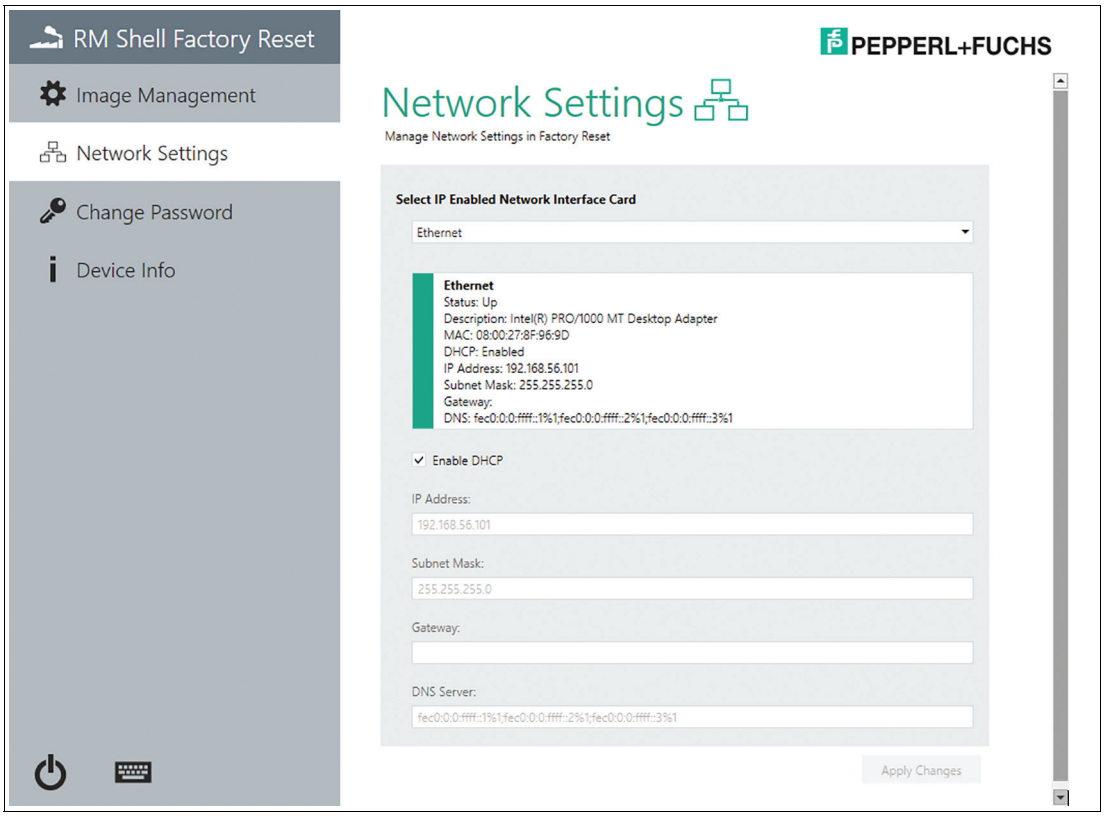


Figure 10.10

10.4 Device Info

This submenu provides information on the "Factory Reset Version", "Device Description", "Installed Image File", "Compatible Images", the "Partitions "and the "Licenses".

The information is useful when updating the firmware or may be necessary for technical support.

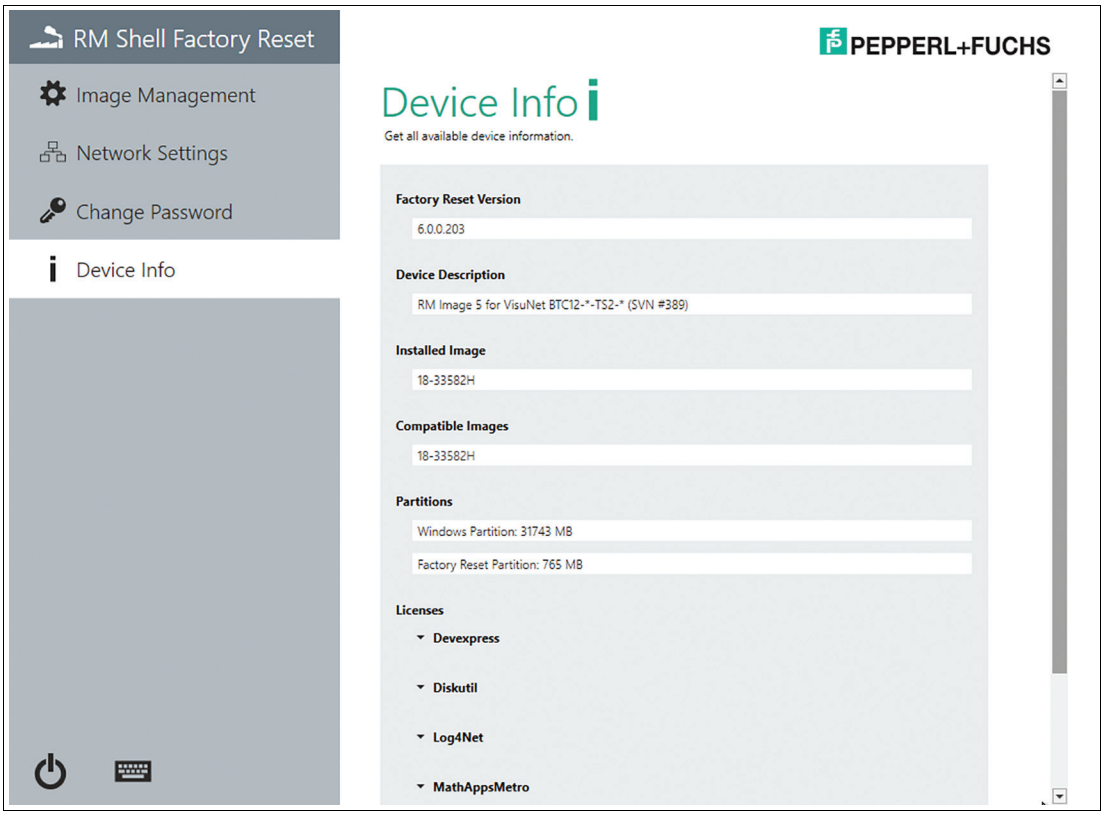


Figure 10.11

11 How-Tos

11.1 Connecting an RM / BTC with a PC via RDP

Note

This chapter describes how to connect an RM / BTC with a PC via RDP using Microsoft Windows.

To ensure communication between an RM / BTC and PC, both devices must be part of the same network and subnet. If you use both devices in a network with a DHCP server, the DHCP server issues the IP addresses automatically.

To connect an RM / BTC with a PC, Pepperl+Fuchs recommends that you do the configuration in 2 steps:

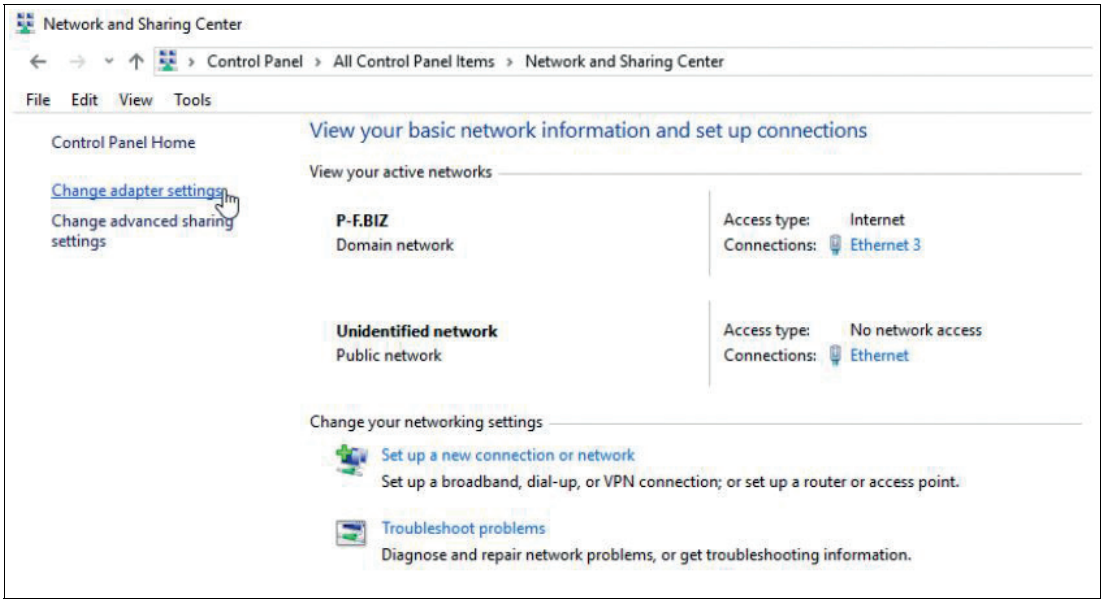
- Step 1: PC Configuration
  - Manual assignment of the IP address
  - Activation of the RDP Server Function
- Step 2: RM / BTC Configuration
  - Manual assignment of the IP address
  - Creation of an RDP profile

Step 1: PC Configuration

Assigning IP Address of the PC Manually

1. Open the "Network and Sharing Center" in the task bar by clicking  and click "Network and Sharing Center".

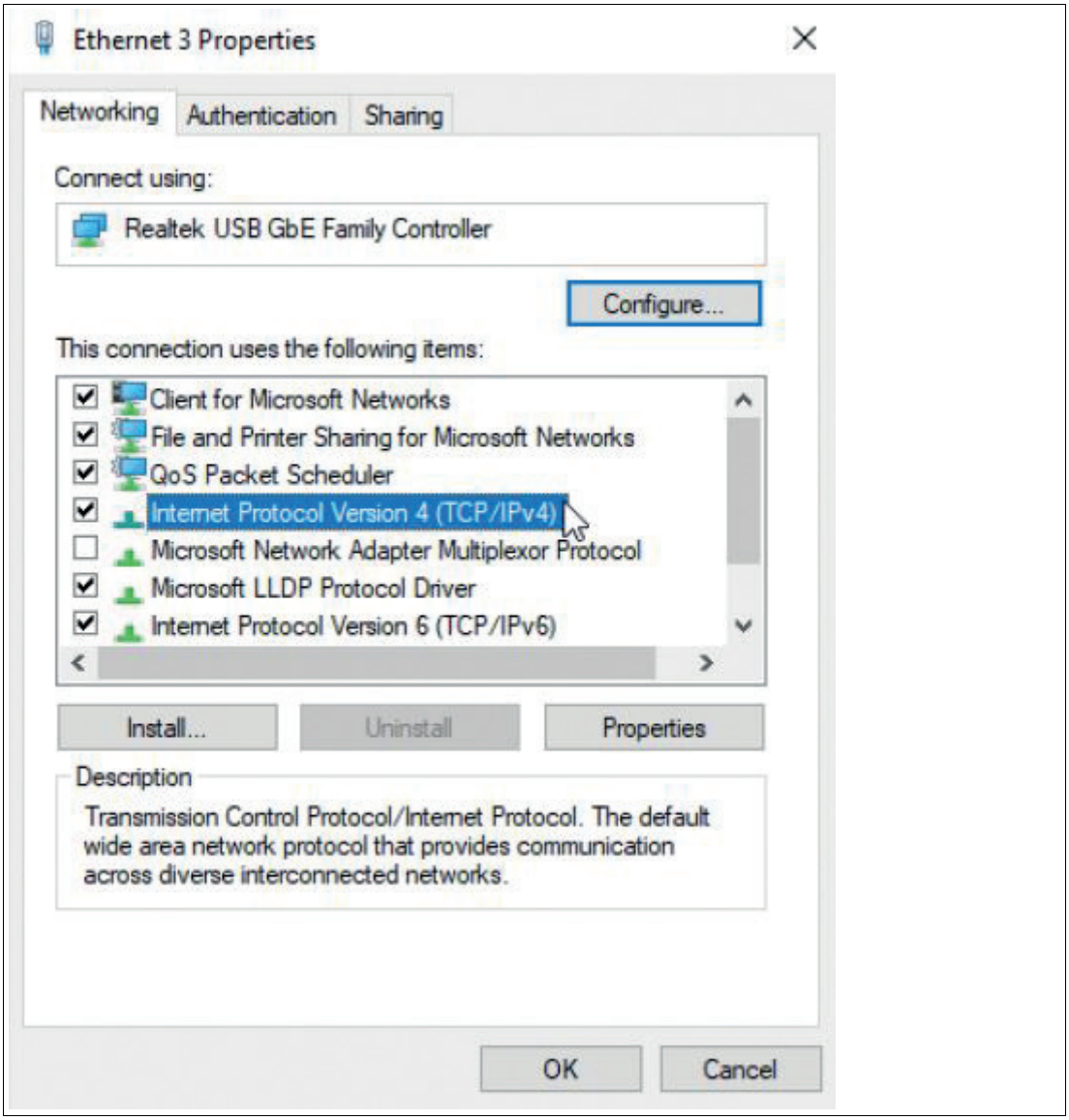
   ↳ The "Network and Sharing Center" window opens.



2. From the navigation bar, choose "Change adapter settings."
3. Search for the network connection that shows your physical network port hardware component. The physical network port hardware component is recognizable by its name in the third line (e.g., "Intel(R) 82579LM...")
4. Right-click on the network connection and choose "Properties".

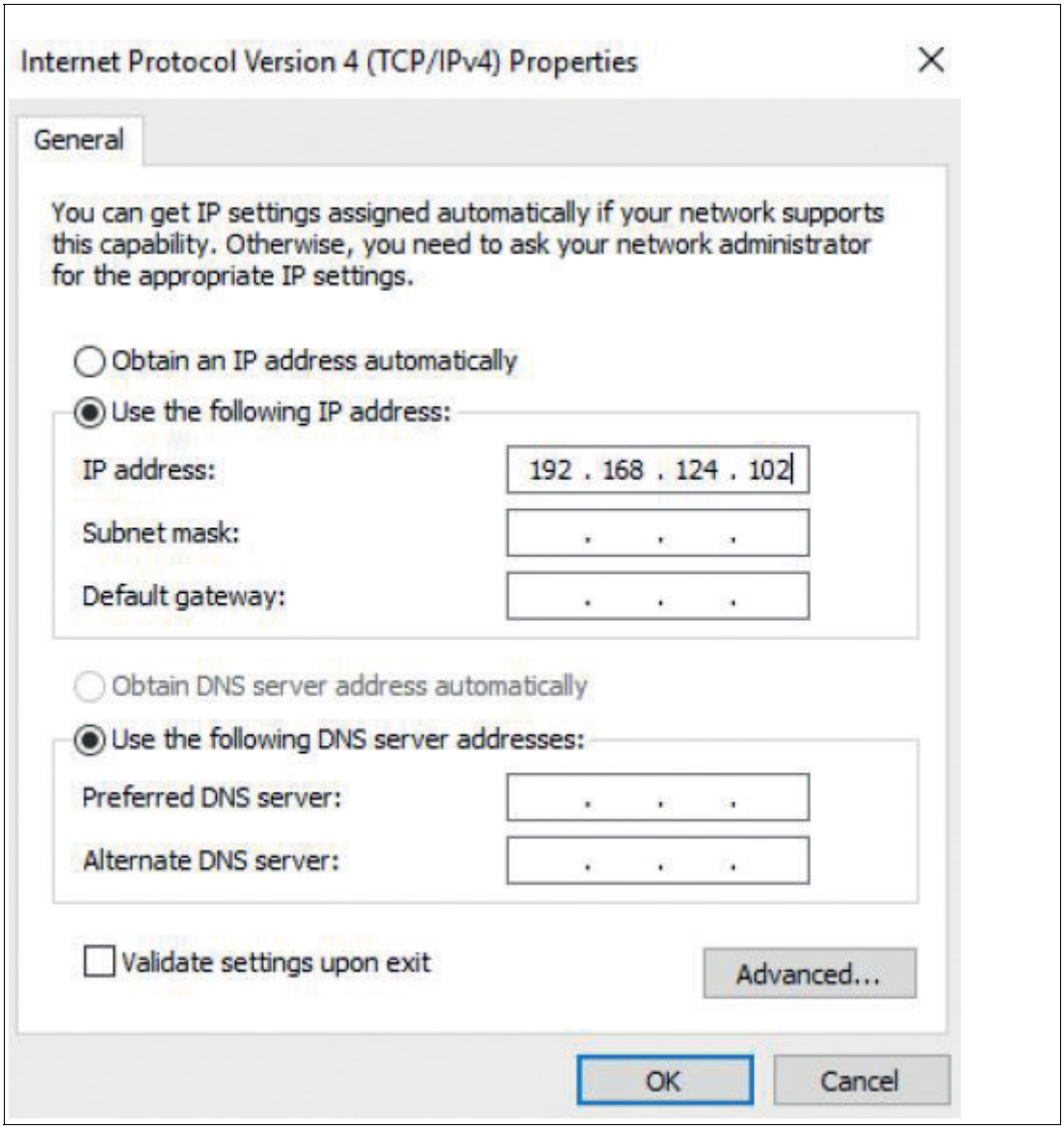
2022-02

↳ The "Local Area Connection Properties" window opens.



5. In the list "This connection uses the following items," highlight "Internet Protocol Version 4 (TCP/IPv4)".
6. Click "Properties."

↳ The "Internet Protocol Version 4 (TCP/IPv4) Properties" window opens.

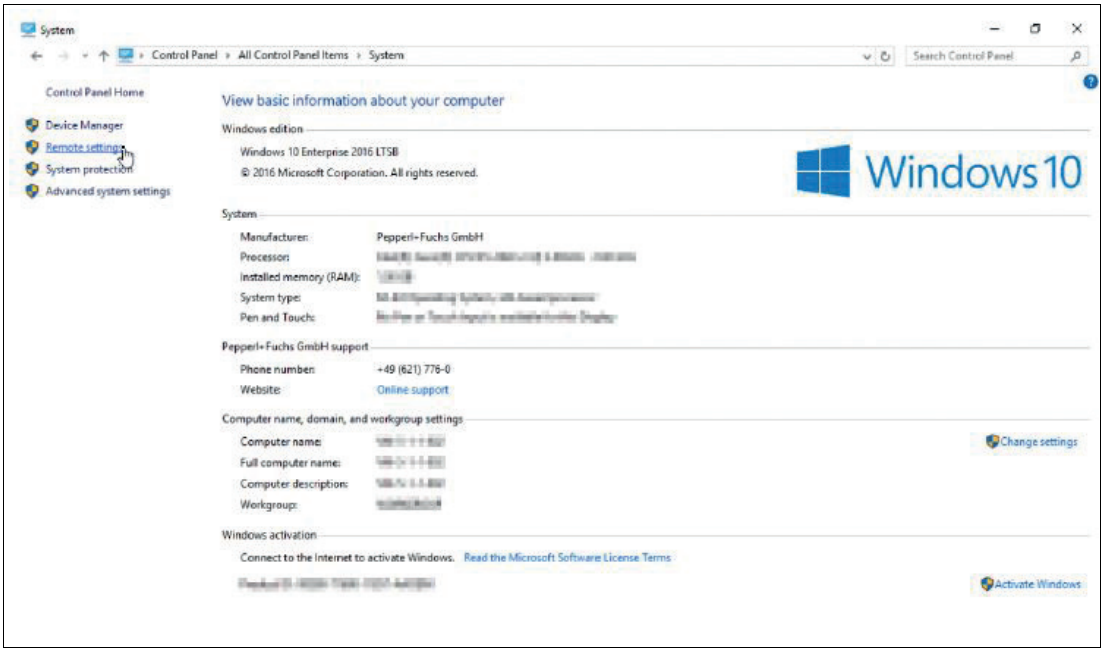


7. Choose the option "Use the following IP address" and type in a static IP address (e.g., "192.168.124.102").
8. To confirm the changes, click "OK."
9. Close the Network and Sharing Center.

Activating the RDP Server Function

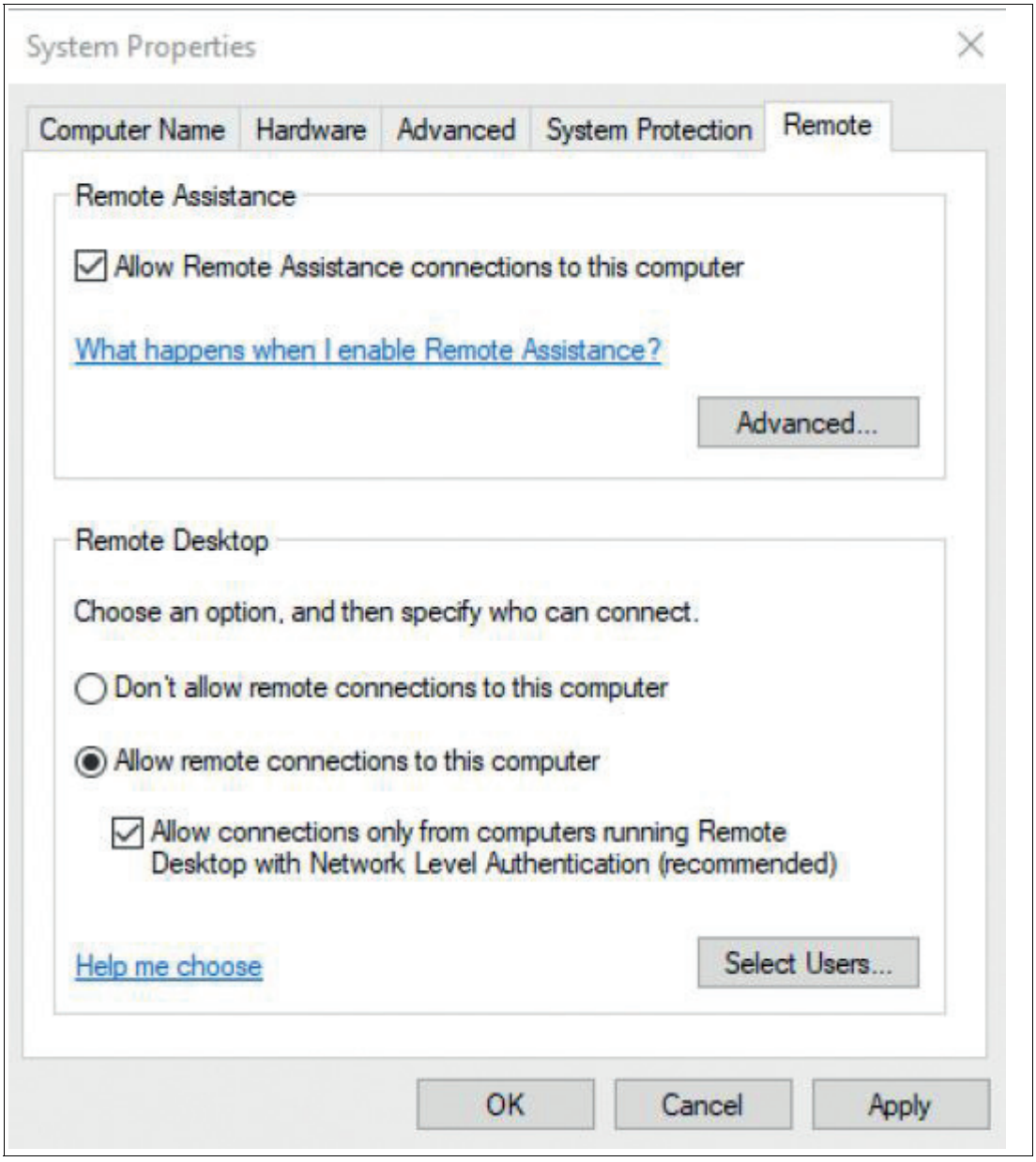
1. Open the start menu, right-click on "Computer" and choose "Properties."

   ↳ The system control panel opens.



2. Click on "Remote settings."

   ↳ The System properties dialog box opens.



3. Choose the option "remote connections to this computer"

Note

We recommend to leave the default additional "Network Level Authentication" enabled

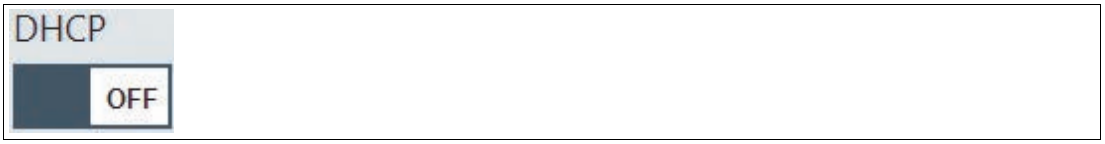
4. Click "OK."
5. To confirm the changes, close the system control panel.

2022-02

Step 2: RM / BTC Configuration

Assigning IP Address of the RM / BTC Manually

1. Log in to RM / BTC Shell as Administrator.
2. Start the System Settings App.
3. Select the submenu "Network."
4. If more than one network adapter is available, choose the network adapter with the status "Network connected" (green).
5. Disable the DHCP option.



6. In the IP address field, type an IP address that differs in the last 3 digits from the IP address that is assigned to the PC (e.g., "192.168.124.101").
7. In the Subnet Mask field, type 255.255.255.0.
8. To confirm the changes, click "Apply Changes."

Creating a Corresponding RDP Profile

1. If you are not logged in, log in to RM Shell as Administrator.
2. Start the Profiles Management app.
3. Create a new profile by clicking 

.
4. Select "Microsoft RDP," and click "OK."

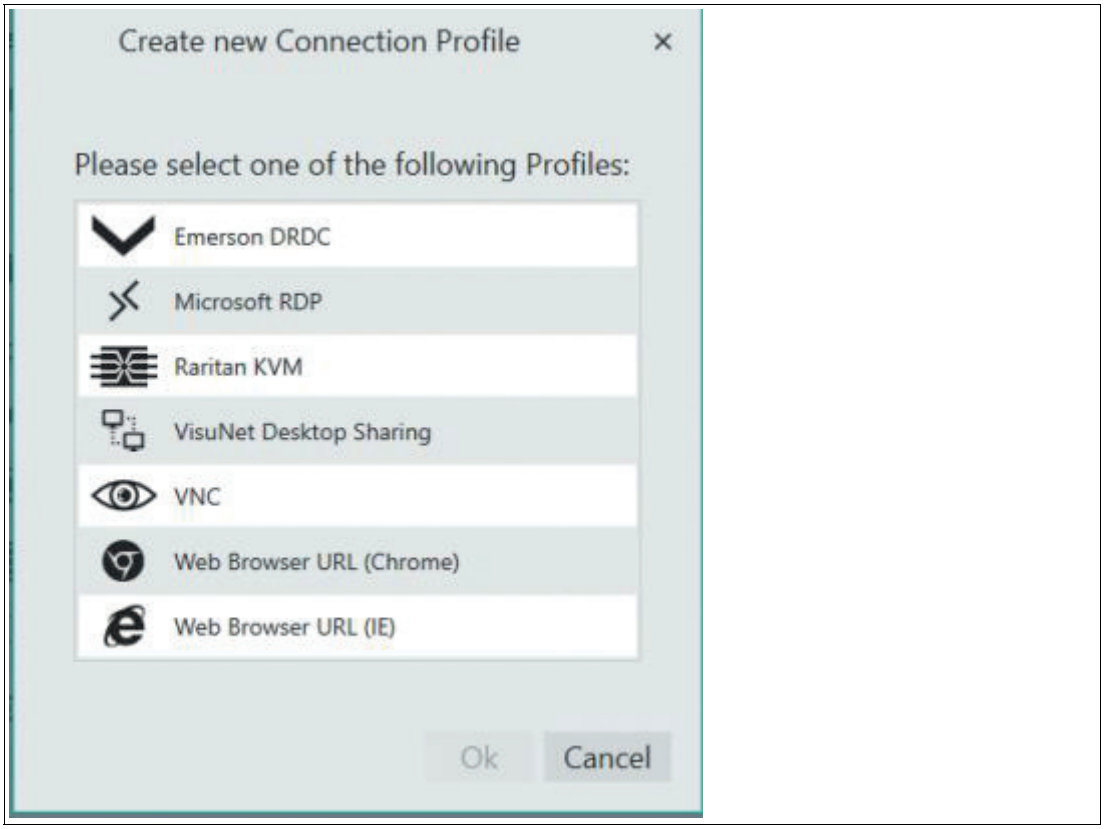


Figure 11.1 The "Create new Connection Profile" dialog box

↳ The RDP profile has been created. The new profile's main settings open.

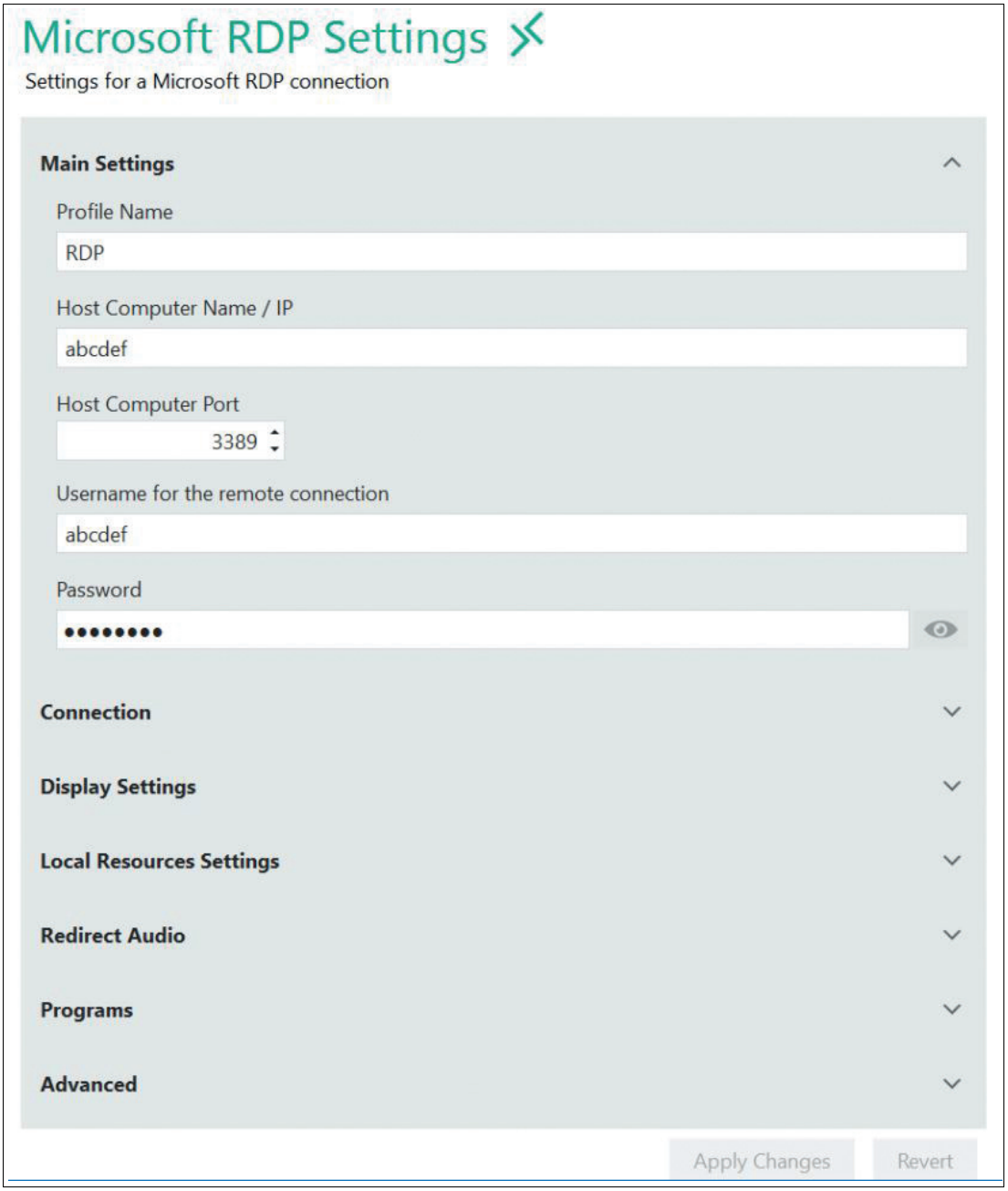


Figure 11.2 Main settings of a Microsoft RDP profile

5. In "Profile Name," type an appropriate name for the current connection profile.
6. In "Host Computer / IP," type the IP address that you have entered before in the PC configuration ("192.168.124.102").
7. Optional: edit the other settings. After editing, click Apply Changes.

   ↳ The new profile has been created.
8. Go back to the home screen.

   ↳ The new RDP profile is now available in the left profile section of the home screen.

11.2 Increasing RDP Reactivity and Performance

The performance and reactivity of a Windows RDP connection can be increased by using the latest protocol version RDP 8.0. RDP 8.0 was introduced with Microsoft Windows Server 2012 and Windows 8.

For systems running Windows 7 Service Pack 1 (SP1) or Windows Server 2008 R2 Service Pack 1 (SP1) an official RDP update is provided by Microsoft that allows to install RDP 8 on those systems.

If you have a host system running Windows 7 SP1 or Windows Server 2008 R2 SP1, please install the RDP8 patch to benefit from the performance improvements.

For further information, please read the official Microsoft knowledge base article that describes the installation steps in detail: https://support.microsoft.com/en-us/kb/2592687

11.3 Configuring Auto-Logoff from Session (Session Timeout) with RDP

To save computing resources on your host system, it is sometimes useful to configure an automated logoff when there has been no user input for a certain amount of time.

If you want to setup a timeout for idle RDP sessions, you can configure this via a policy on your Windows host system.

To enable an automated logoff for an idle session, please perform the following configuration steps on your host system:

Configuring An Auto-Logoff

1. Open Group Policy Editor via `cmd -> gpedit.msc`.
2. Navigate to `Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\`
3. Open setting `Set time limit for active but idle Remote Desktop Services Sessions`, set it to `Enabled`, and select the time limit from the dropdown list. Close all windows by clicking `OK`.
4. Run `cmd` and enter the command `gpupdate` to update your policy.

   ↳ After the host system policies have been updated, the auto-login with saved credentials should work.

For further information, please read the official Microsoft article that describes the configuration steps in detail: https://technet.microsoft.com/en-us/library/cc754272(v=ws.11).aspx

11.4 Configuring a Multi-Monitor (Extended Desktop) Setup with RDP and Box Thin Client BTC

When you use a Box Thin Client BTC with multiple monitors, you can stretch one RDP connection across all connected monitors. The RDP connection will then behave like a local “extended desktop.”

To configure an RDP connection as multi-monitor connection, please proceed with the following steps:

2022-02

Configuring a Multi-Monitor Connection with RDP and BTC

Note

This function is only available when multiple monitors are connected to the device.

1. Connect the further required monitors.
2. Login in to user role `Engineer` or `Administrator`.
3. Open `Profile Management`.
4. Select the RDP connection that you want to expand across all connected monitors and enable the feature `Fullscreen Mode`.
5. Go to section `Display Settings` and change the feature `Show the connection on the following displays` to `Expand over all displays`.
6. Apply the changes.

For further information, read the official Microsoft article that describes the configuration steps in detail: https://technet.microsoft.com/en-us/library/cc754272(v=ws.11).aspx

Important: The “Extended Desktop” RDP connection can only be established to host systems that run Windows 7 Ultimate, Windows 7 Enterprise, (and Windows Server 2008 R2 or newer). This feature is not supported by Windows 7 Professional! See 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

Note

To reflect the physical arrangement of your connected monitors with the RDP connection, ensure that the monitors are also correctly arranged in the display settings. Refer to the chapter “Display Settings” to check how a multi-monitor setup can be configured.

11.5 Installing McAfee Endpoint Security

Note

Compatibility of Third-Party Software

RM Shell is qualified to work with software that is shipped with Pepperl+Fuchs VisuNet devices. Pepperl+Fuchs does not guarantee the functionality of third-party software. Customers are responsible for ensuring compatibility with any third-party software.

Before You Get Started

Before installing McAfee Endpoing Security, visit McAfee's Knowledge Center to check software and hardware compatibility: https://kc.mcafee.com/corporate/index?page=content&id=KB82761.

Requirements

- USB flash drive
- Additional PC to download and unzip the installation files

Step 1: Download

- Download the McAfee software on a separate PC and unpack the zip file onto a USB flash drive.

Step 2: Disable Filter

- Disable the unified write filter on your remote monitor. See chapter 4.1.

Step 3: Open General Settings

- Open the general settings in the administrator role

Step 4: Open Windows Explorer

- Open Windows explorer in the start menu

Step 5: Install

- Plug the USB flash drive into your remote monitor and navigate to the installation files. Execute the **setupEP.exe** file and follow the installation instructions.

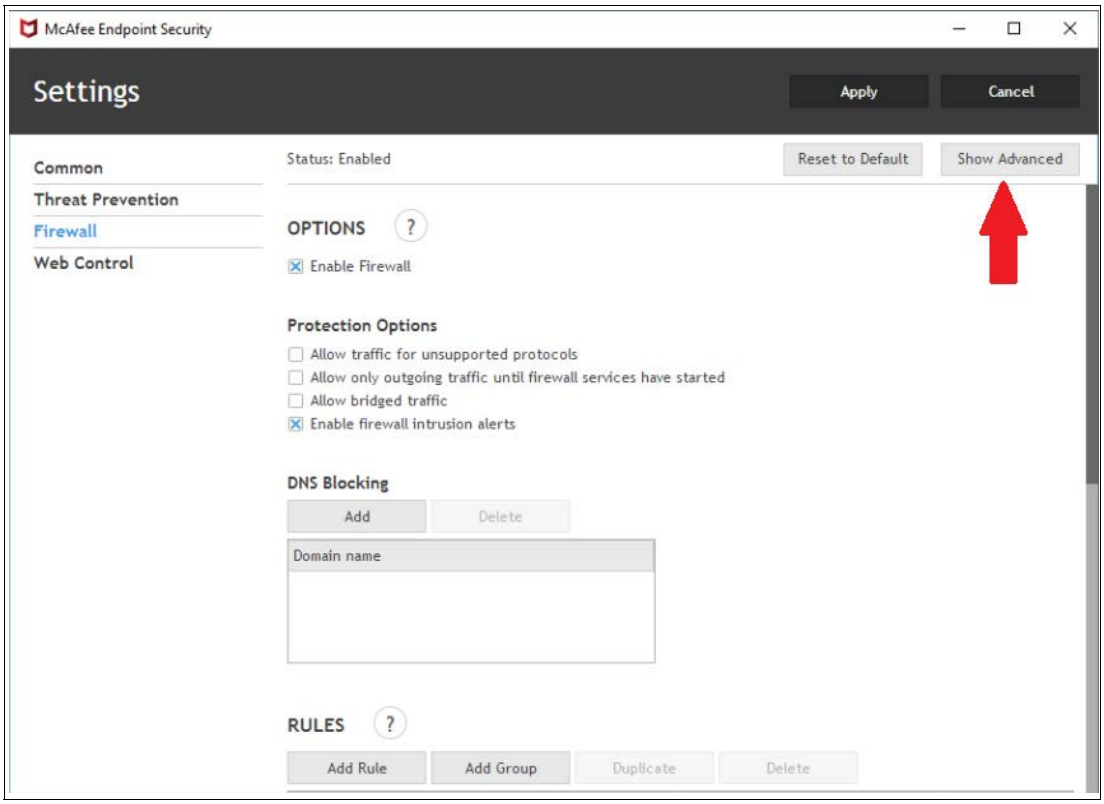
Step 6: Create Generic App

- Create a generic app for McAfee Endpoint Security. This will provide a link to the software on the home screen. See chapter 7

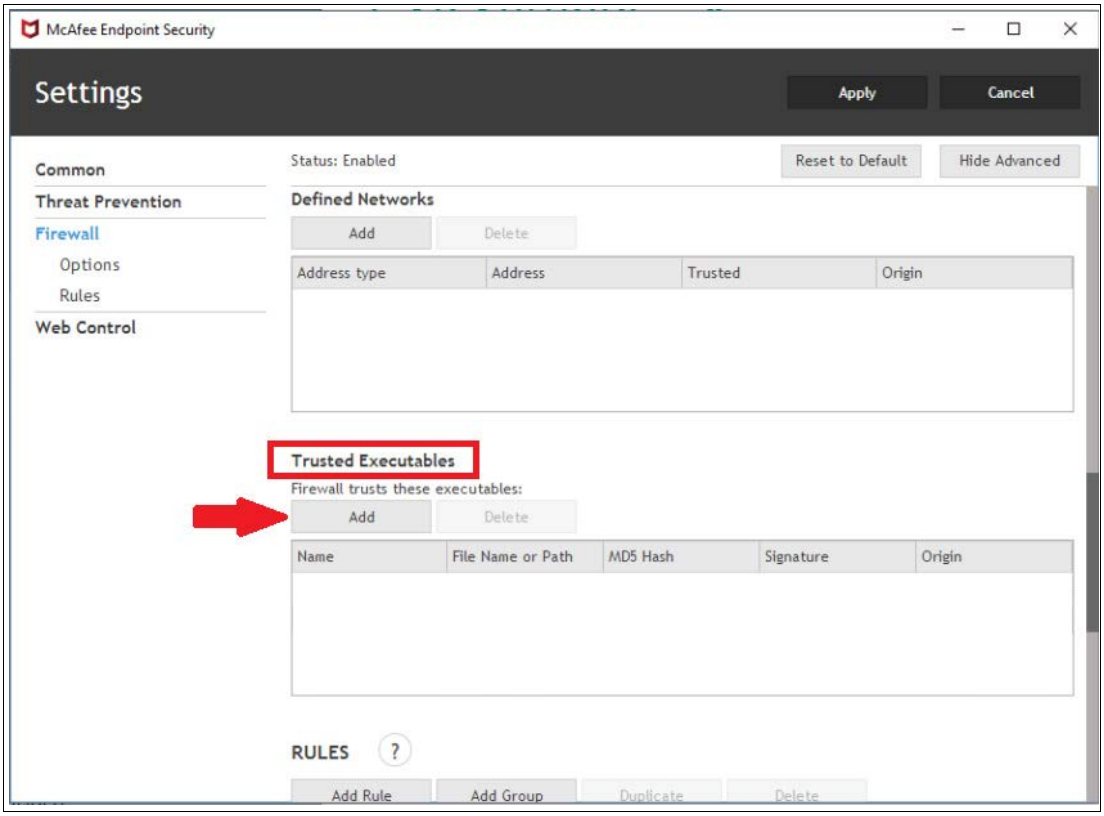
Step 7: Change Firewall Settings

Once setup is complete, you must add two exception rules to the Firewall. This will allow RM Shell to function properly.

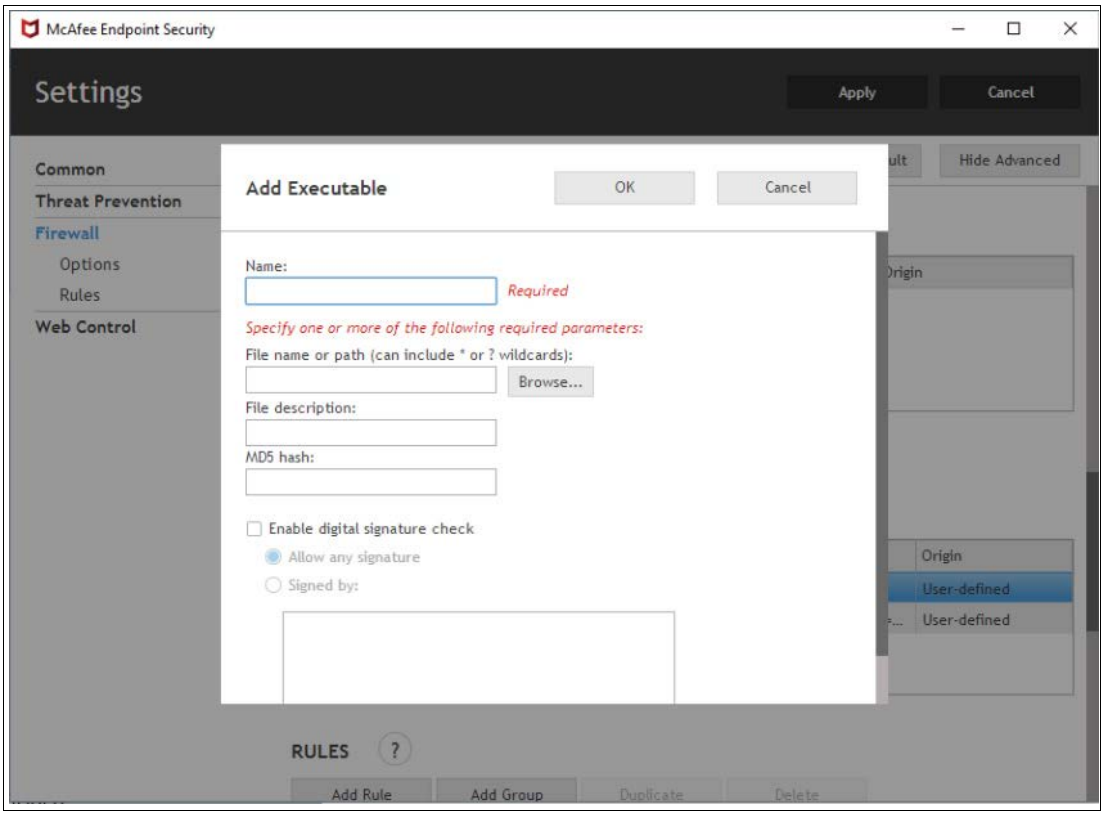
1. Open the firewall settings in the McAfee program and click "Show Advanced."



2. Scroll down until you find "Trusted Executables." Click "Add."



↳ The "Add Executable" menu will open.



3. Choose a name for the exception.
4. Under "File name or path," add **tvnserver.exe** and **RMShell.exe**.
5. This files can normally be found under:

- C:\Program Files\Pepperl+Fuchs\RMShell\RMShell.exe
- C:\Program Files\Pepperl+Fuchs\RMShell\Plugins\RMShell.DesktopSharing\Server\tvn-server.exe

6. You can also navigate to these files and add them via "Browse."
7. Once you have filled in the required parameters on the menu, click "Apply."

11.6 Pairing a Bluetooth® Device

The below instructions demonstrate how to pair a Bluetooth® device in RM Shell. An ecom Ident-Ex® 01 scanner is used as an example. For more information about this product, see: https://www.ecom-ex.com/products/mobile-computing/reader-scanner-imager/ident-ex-01/

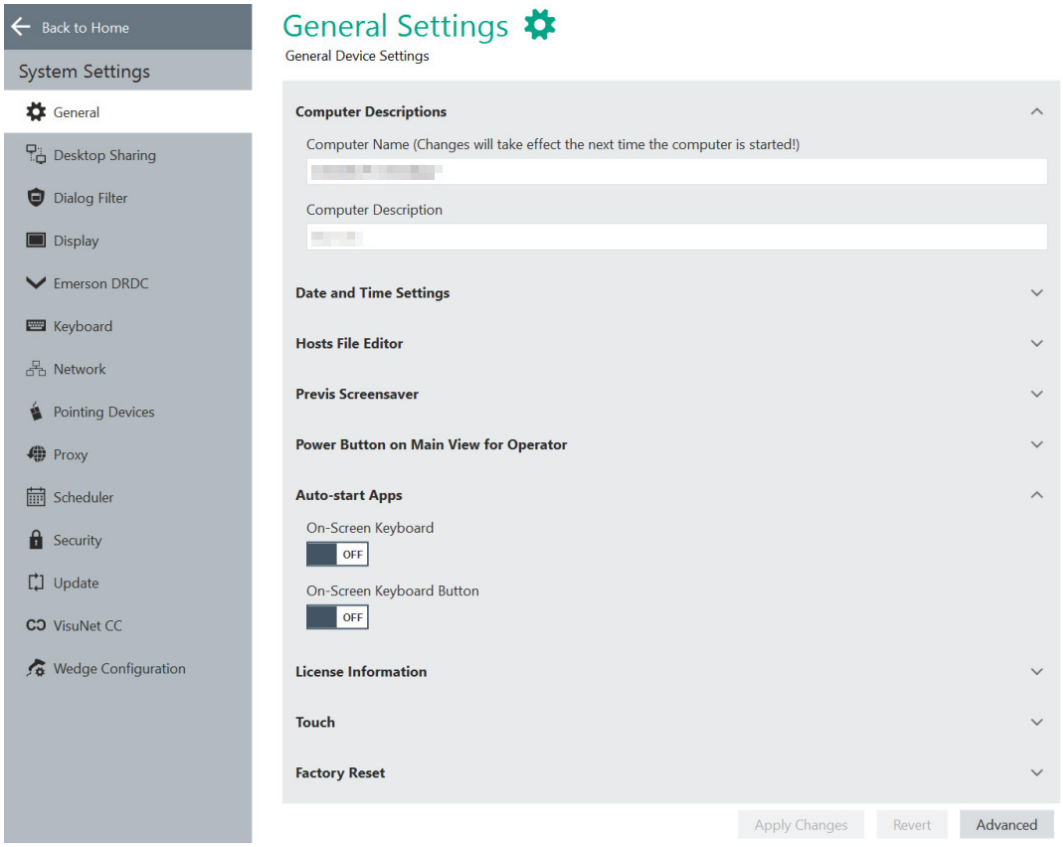
Note

Log in as Administrator

You must be logged in as Administrator in order to perform the following steps.

Pairing an ecom Ident-Ex 01® Scanner

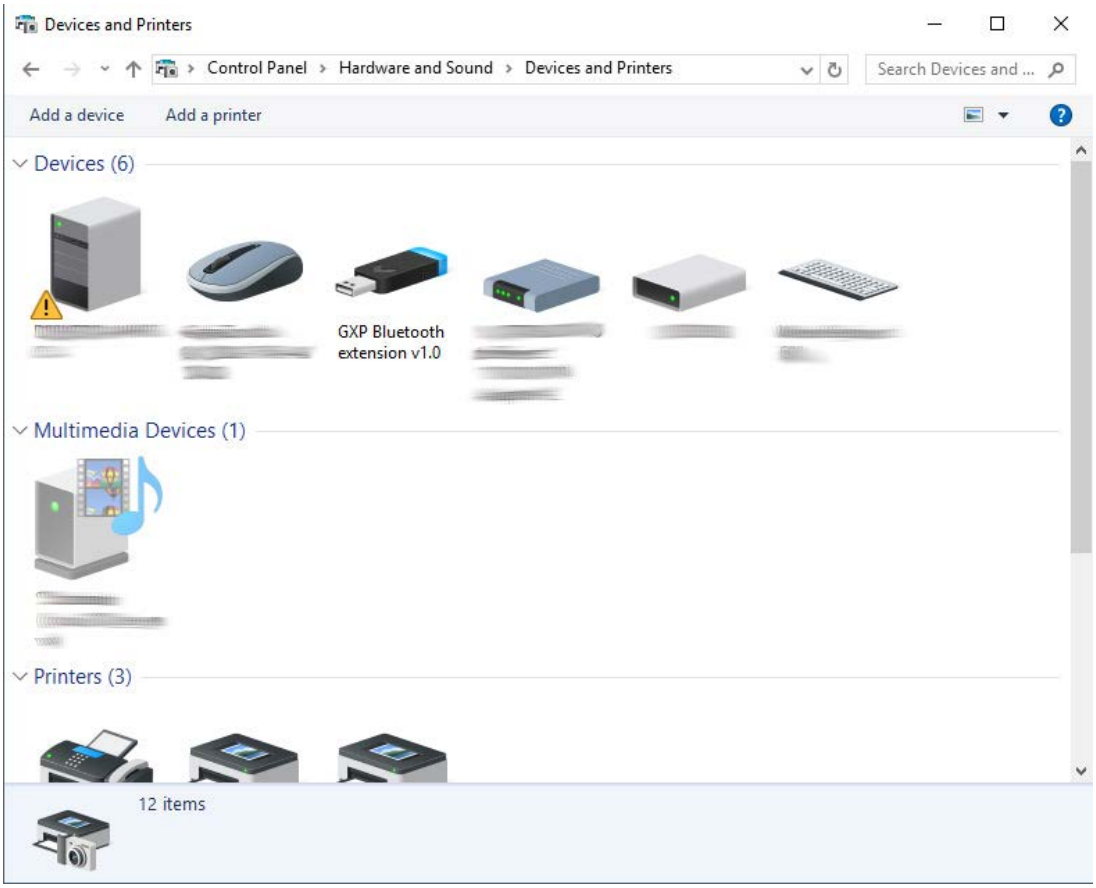
1. Connect a bluetooth dongle to the TCU/PCU.
2. Navigate to the "General" tab in the "System Settings" app.
3. Click the "Advanced" button at the bottom-right corner of the screen.



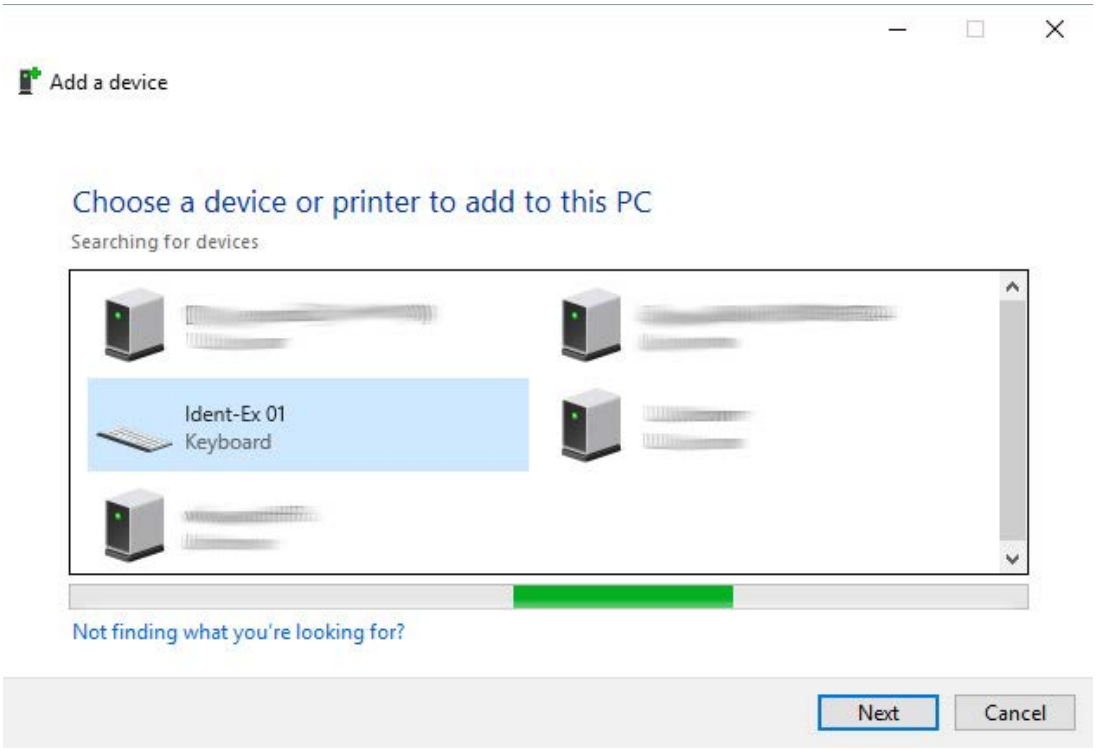
↳ The control panel will open.

4. Navigate to "Hardware and Sound," then "Devices and Printers."
5. Select "Add a device" in the "Drivers and Printers window.

2022-02



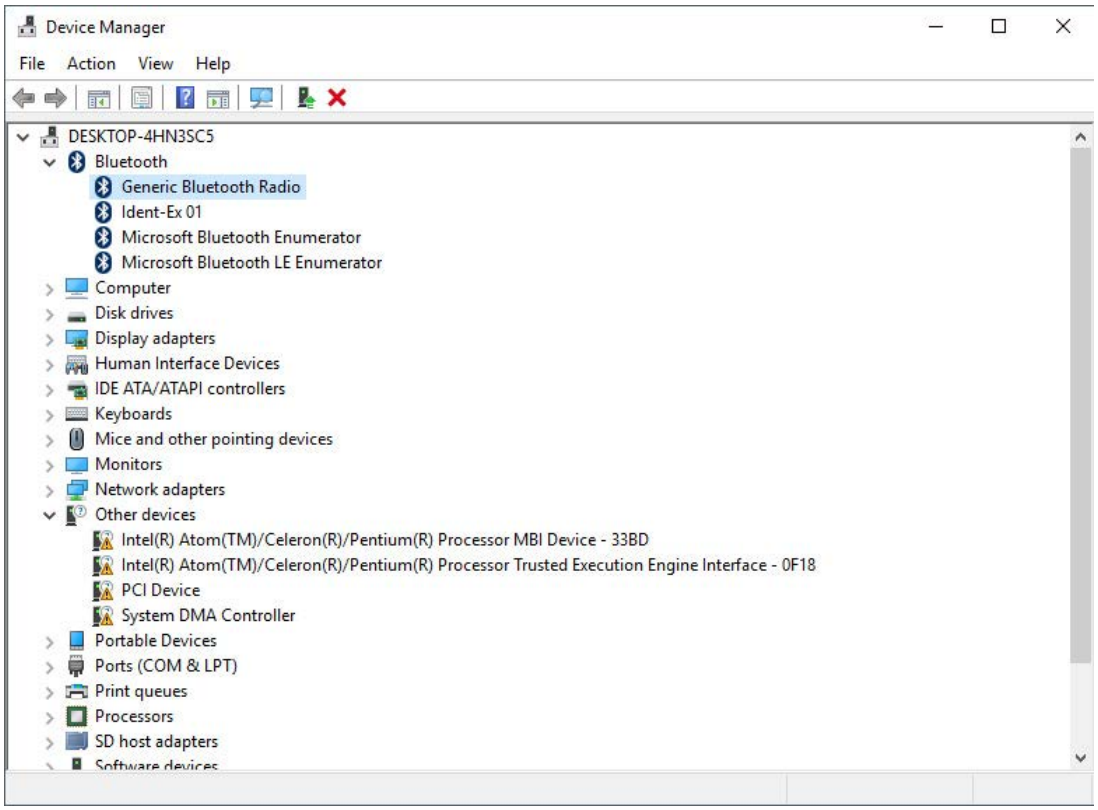
6. Turn on the Ident-Ex 01. After a few seconds, the Ident-Ex 01 scanner will appear as a keyboard device.
7. Select the device and click "Next."



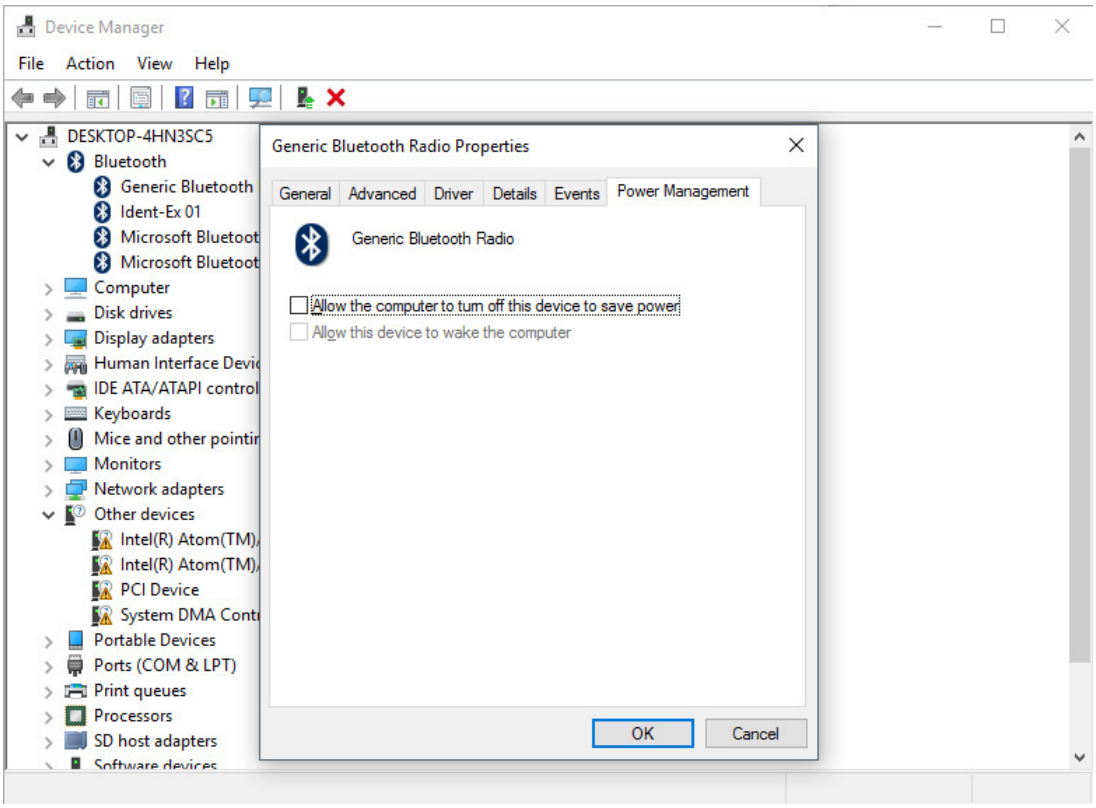
↳ The system will then pair with the Ident-Ex 01. After the device has been paired successfully, the blue LED indicator on the Ident-Ex 01 will turn on.

8. Navigate back to the "Hardware and Sound" section of the control panel. Select the "Device Manager" under "Devices and Printers."

9. Right click on "Generic Bluetooth Radio" under the "Bluetooth" section.



10. Navigate to the "Power Management" tab and uncheck the option "Allow the computer to turn off this device to save power."



↳ The device is now ready for operation.

Note

Reestablishing Connection after Reboot

If a connection to the Ident-Ex-01 is not automatically reestablished after a system reboot or the scanner has been turned off/on, press and hold the SPP button on the Ident-Ex 01 until the blue indicator LED turns on again.

11.7 Importing Host Certificates

Importing certificates for RDP connections

1. Adjust the Group Policy Setting of the host.
2. open “gpedit.msc” (server side), navigate to (1) and disable (2).

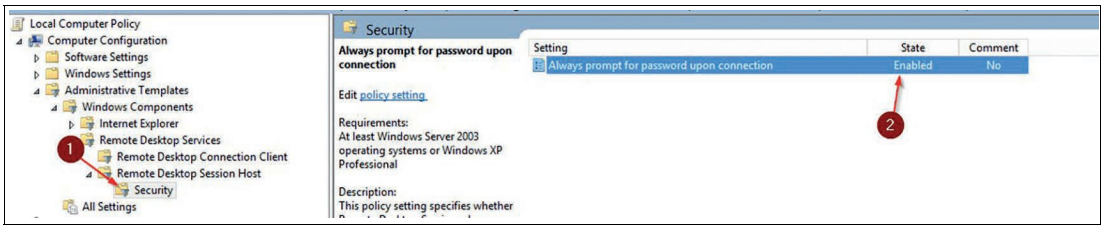


Figure 11.3

3. Import your certificate.
4. Click “View certificate” (1).

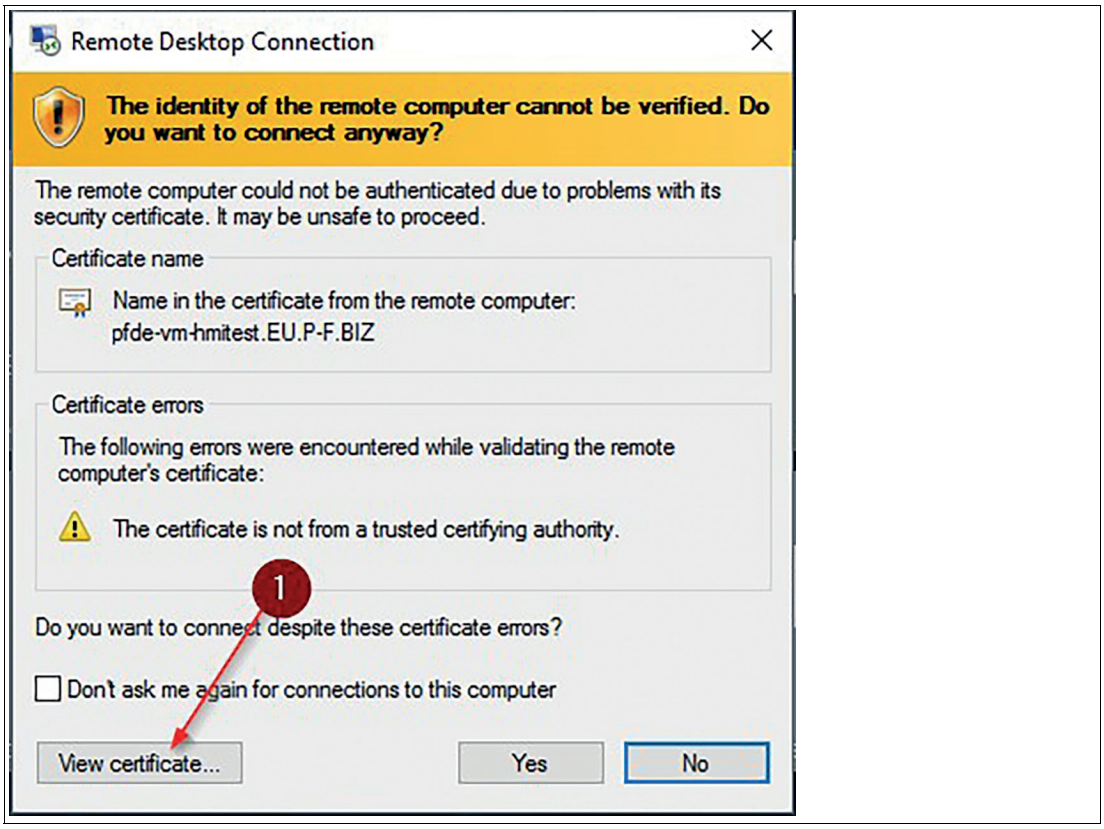


Figure 11.4

5. Click “Install certificate” (2)

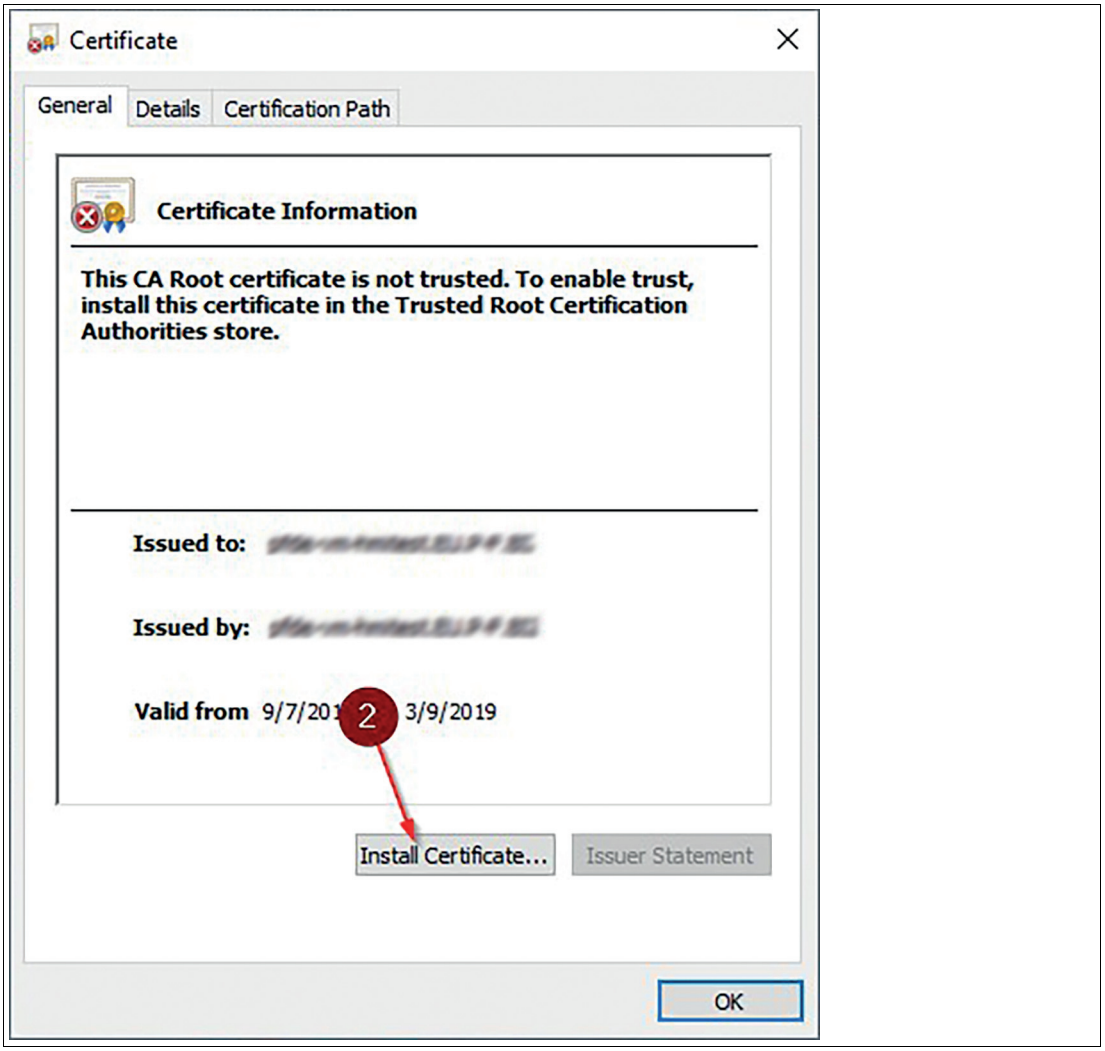


Figure 11.5

6. Follow the steps of the Certificate import Wizard
7. Select “Local Machine” (3) and click “Next” (4)

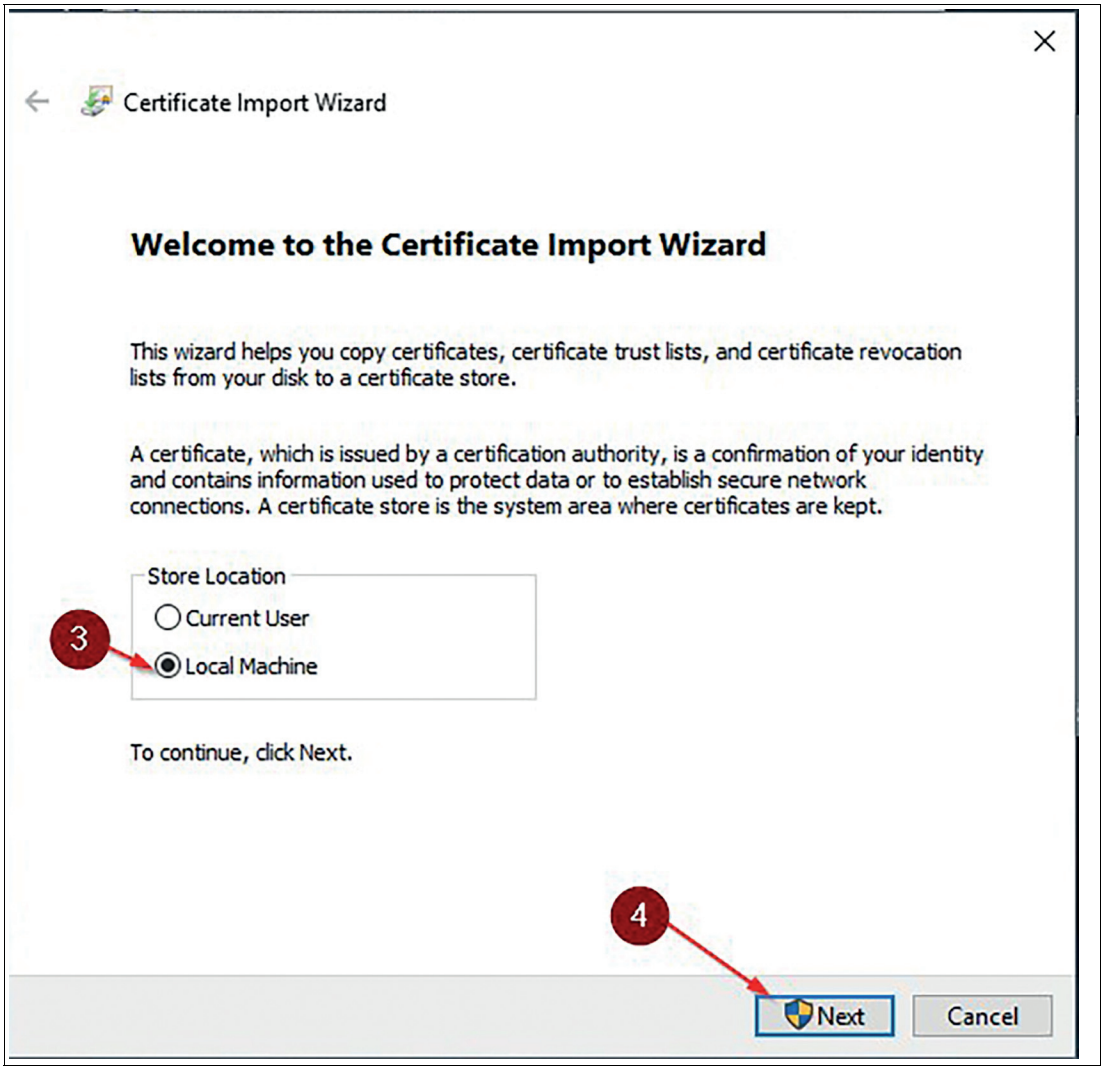


Figure 11.6

8. Select your own store (5), (6), (7), (8) and click “Next” (9).

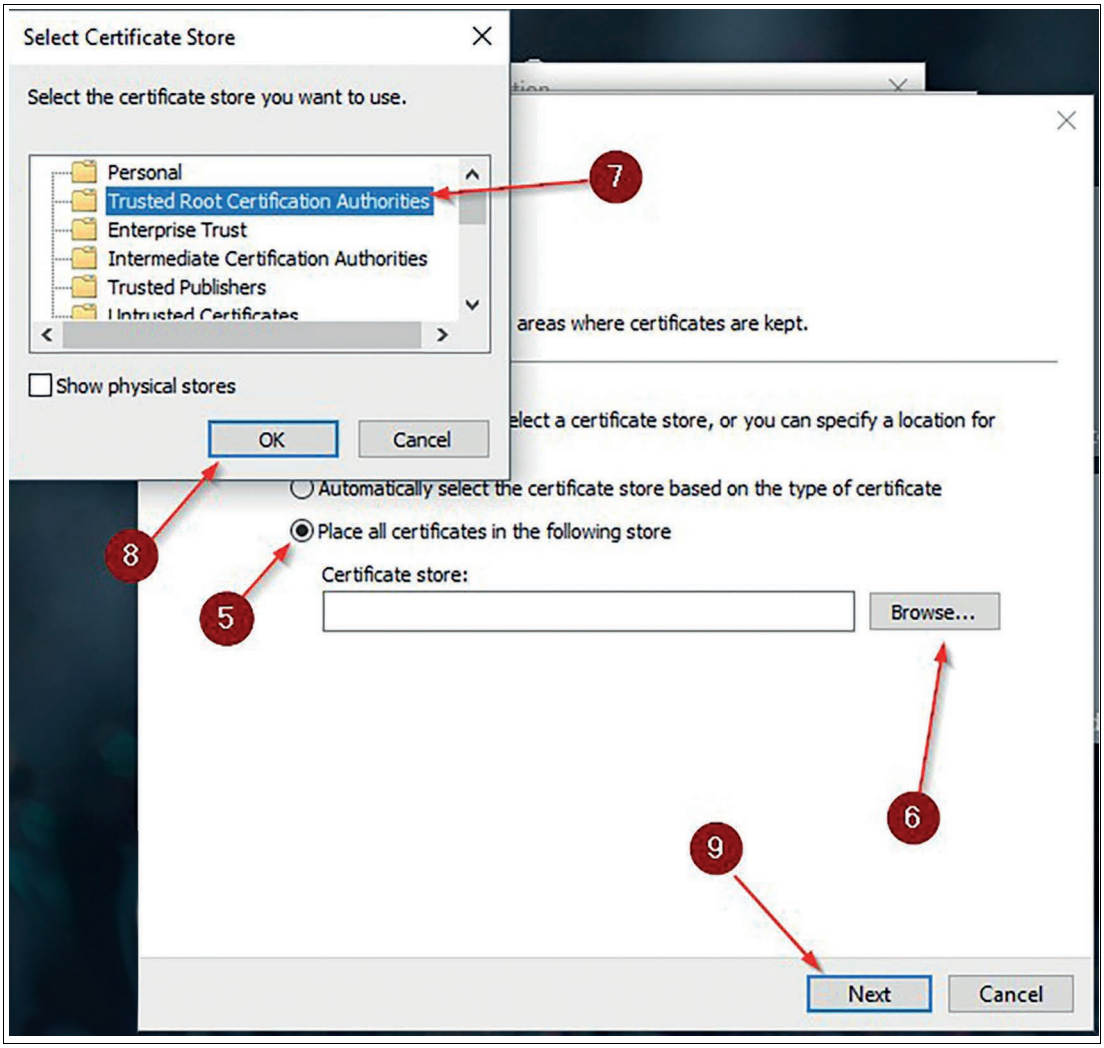


Figure 11.7

9. After clicking “finish” the certificate is imported. No certificate message should appear anymore.

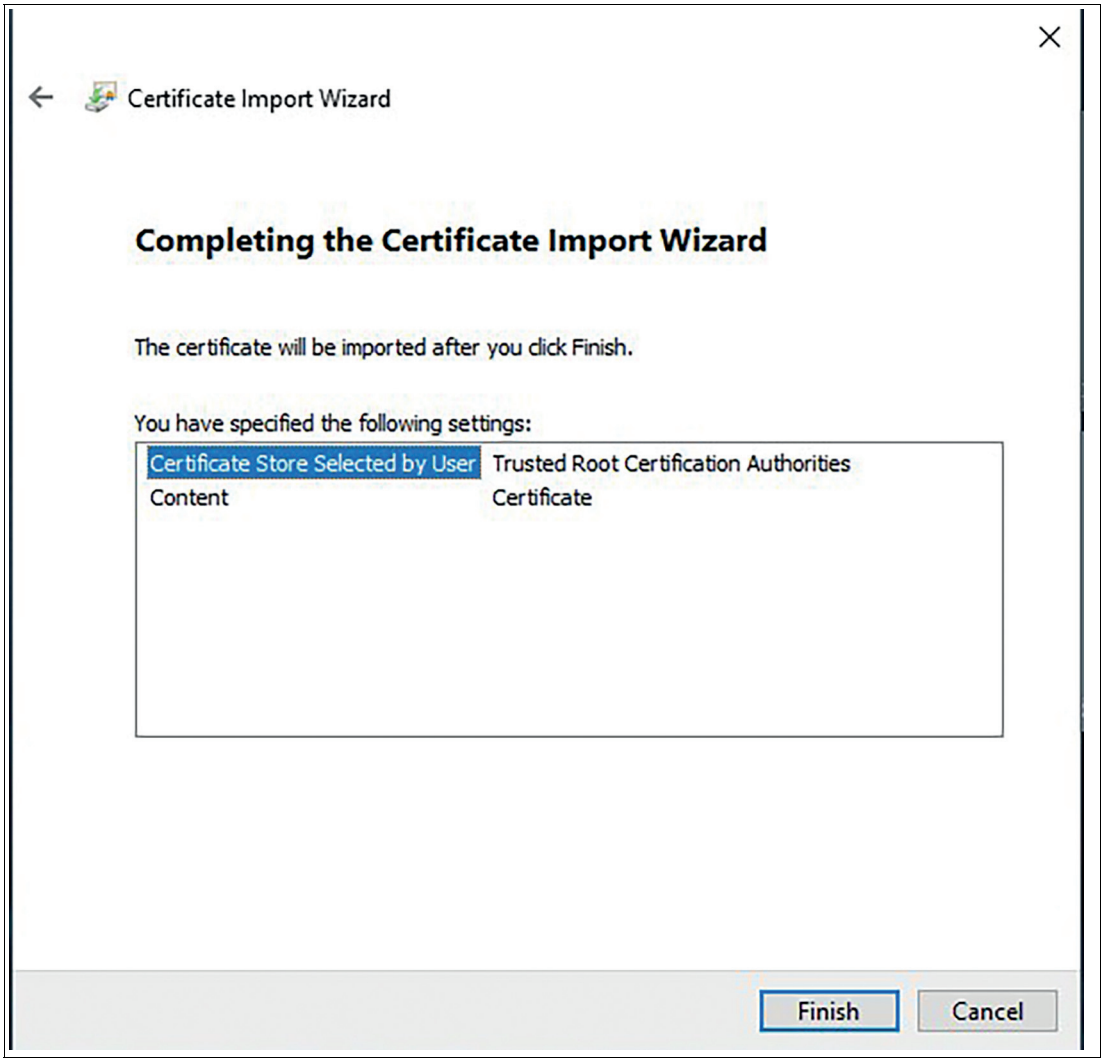


Figure 11.8

How to integrate a domain

1. Login as Administrator and open the System Settings / Security page and change the “Local Windows User” Password.
2. Disable the “Keyboard Filter and block Ctrl+Alt+Del”.
3. Apply the settings of the Security Page.
4. Click on System Settings
5. Navigate to the General Tab
6. Expand the advanced windows settings
7. Follow the path Control Panel > System and Security > System
8. Click “Change Settings”

Note

If you can´t open the “Change Settings”, disable “Remove Properties from Computer icon context menu” in the Local Group Policy Editor. To open the Local Group Policy Editor search for “gpedit.mcs".

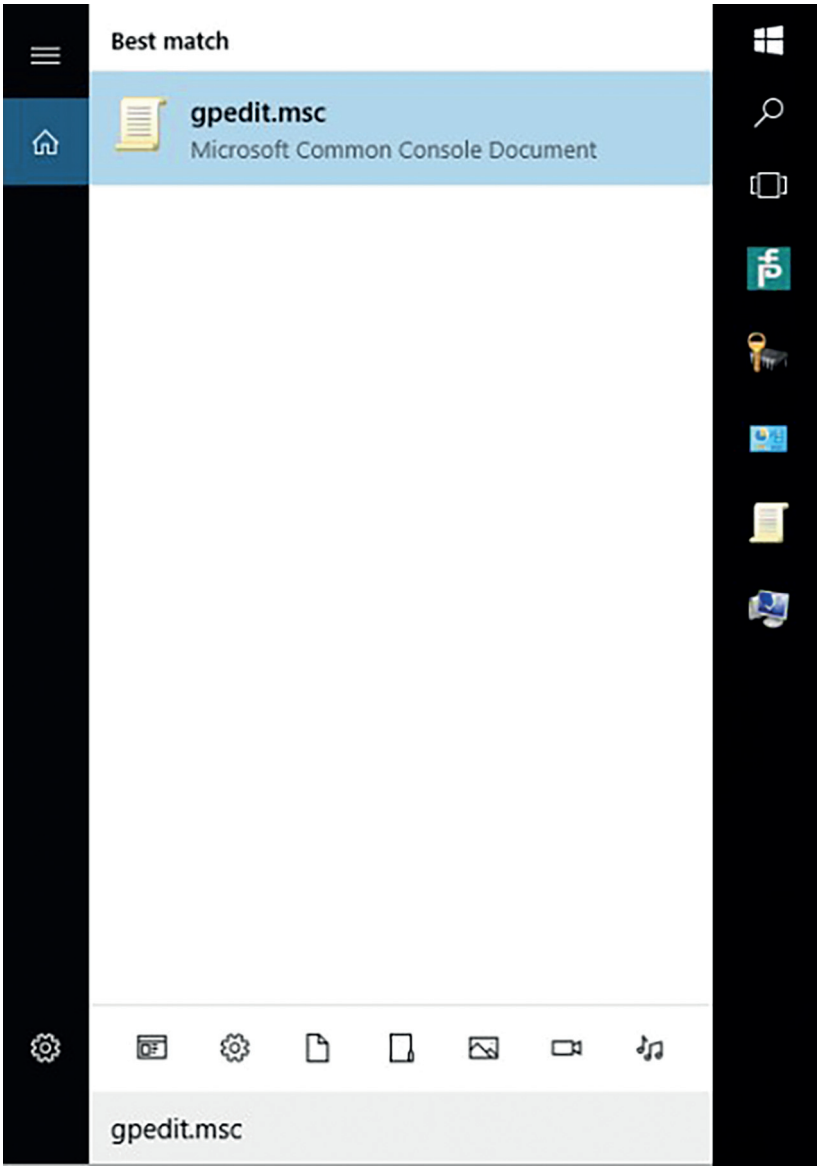


Figure 11.9

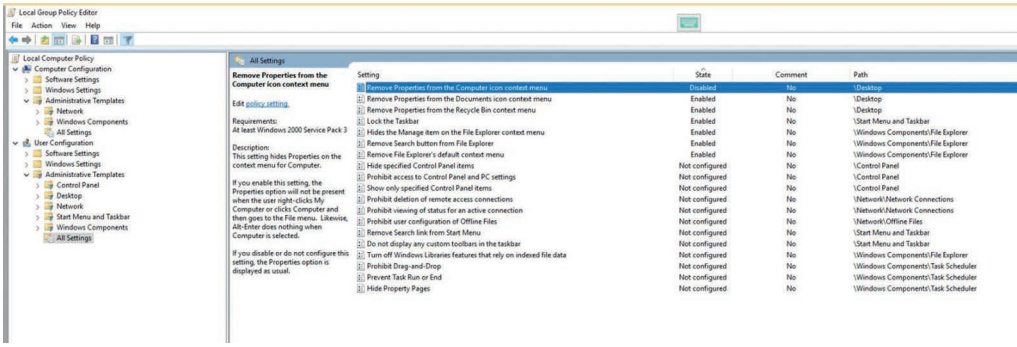


Figure 11.10

9. Use the following path: Local Computer Policy/User Configuration/Administrative Templates/Desktop/Remove Properties from the Computer icon context menu
10. Select Domain and enter the Domain Name. A credential window will open.Enter the credentials of a domain administrator.

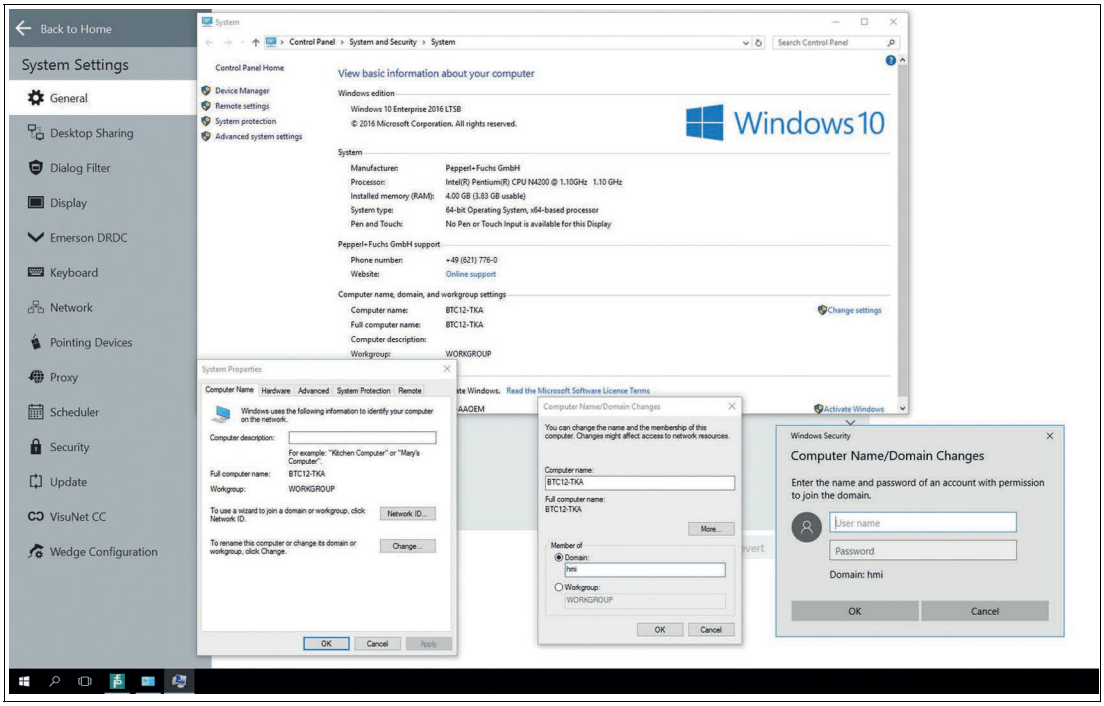


Figure 11.11

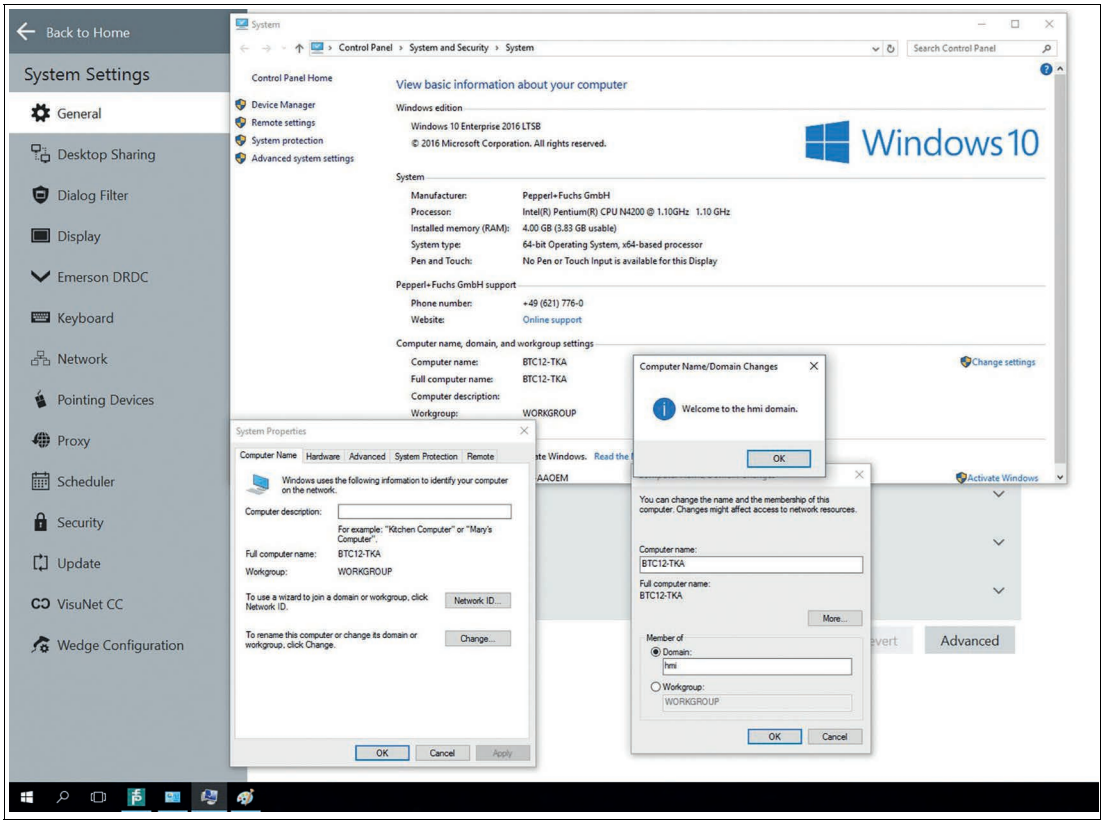


Figure 11.12

11. Reboot the device

2022-02

PEPPERL+FUCHS

12. After rebooting, you have to enter the Credentials for the PFUser. The password is VisuNetRMShell5 . Please note, that you have to use the local account.The user should look like this: .\PFUser
13. Add a domain user to the local administrator group.Therfore open lusrmgr.msc
14. Go to the groups, right click Administrators and press "Add to Group…"

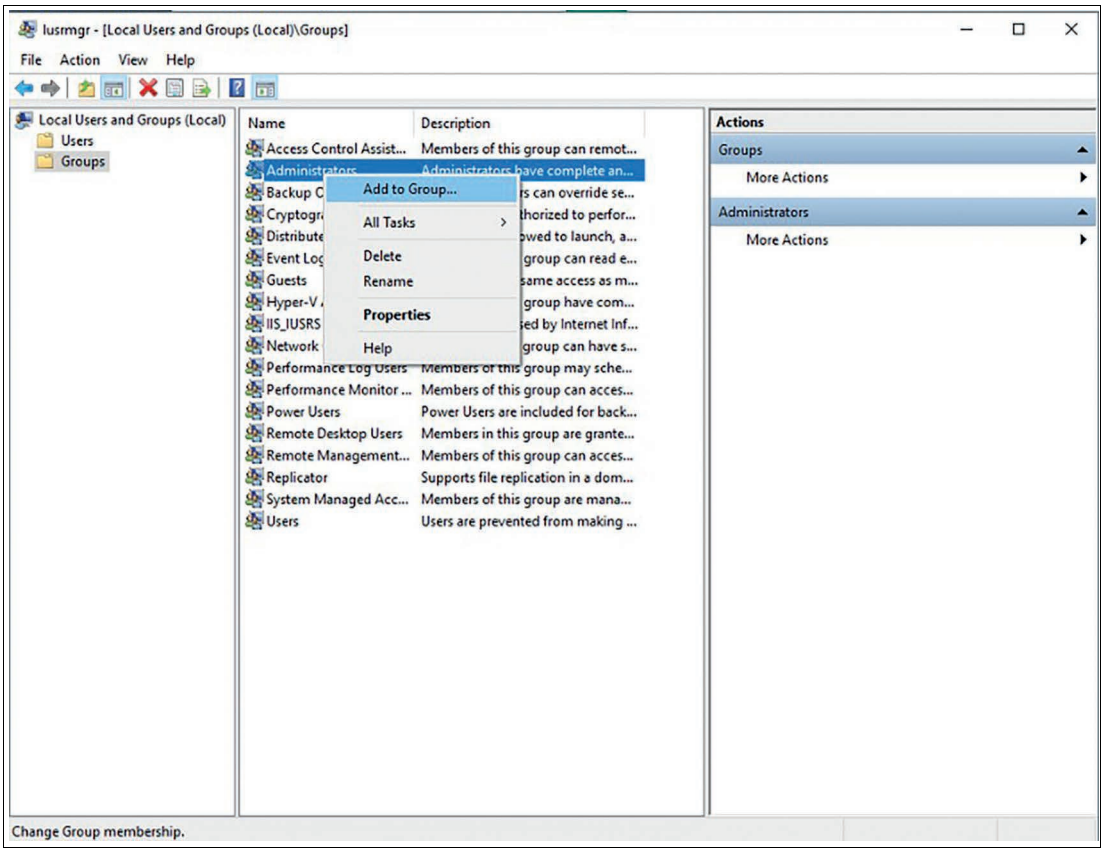


Figure 11.13

15. Enter the username with domain prefix and click “check names” to verify it. Click OK

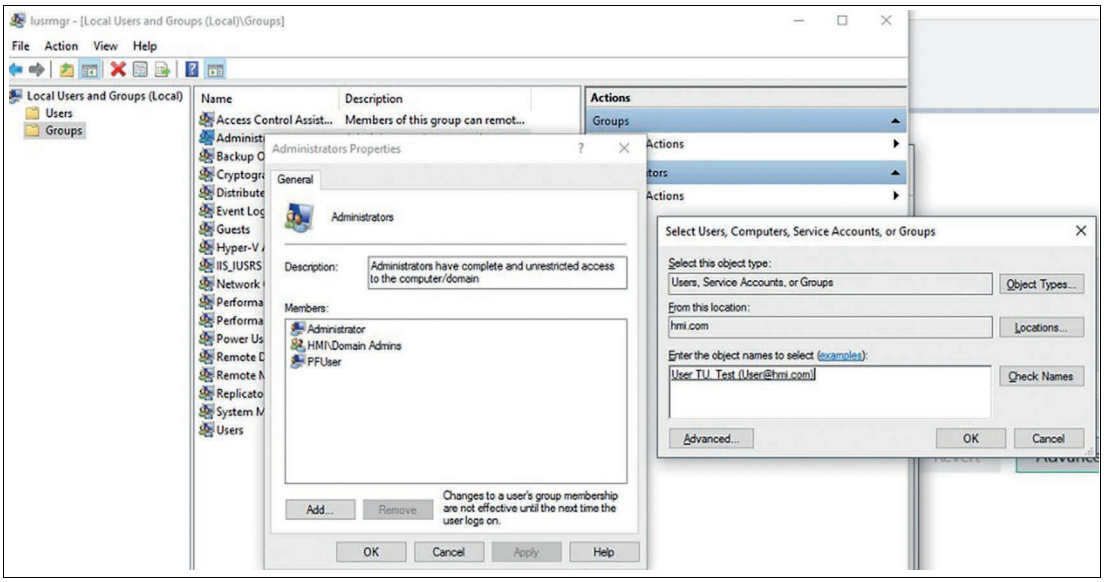


Figure 11.14

16. Now you are able to switch the user. Inside the RM Shell you can activate "ctrl+alt+del" for fast logout or use the taskbar for the regular logout.

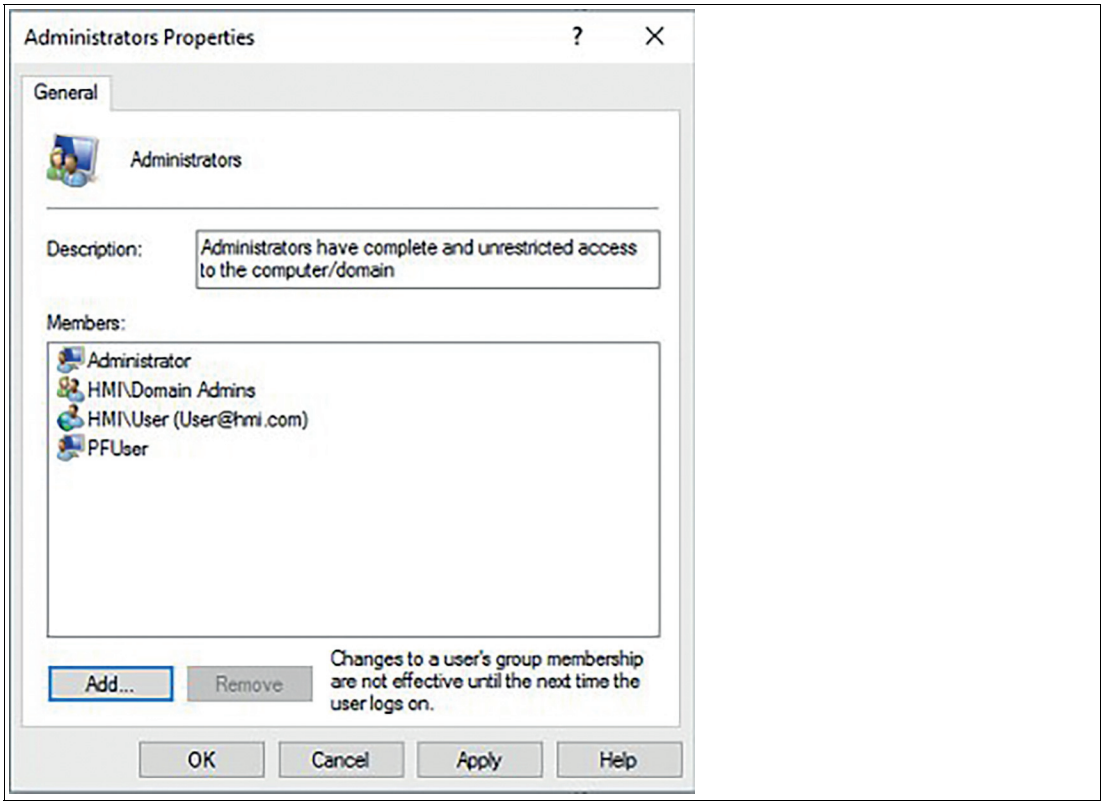


Figure 11.15

Note

Autologin will be disabled per default. We recommend not to change the default settings. If your application requires an autologin, please refer to: https://support.microsoft.com/de-de/help/324737/how-to-turn-on-automatic-logon-in-windows.

11.8 Enable TLS 1.0 (for Raritan DKX2-101 or older Webservers)

1. Open the System Settings in the administrator role.
2. Open the Group Policy Editor "gpedit.msc"

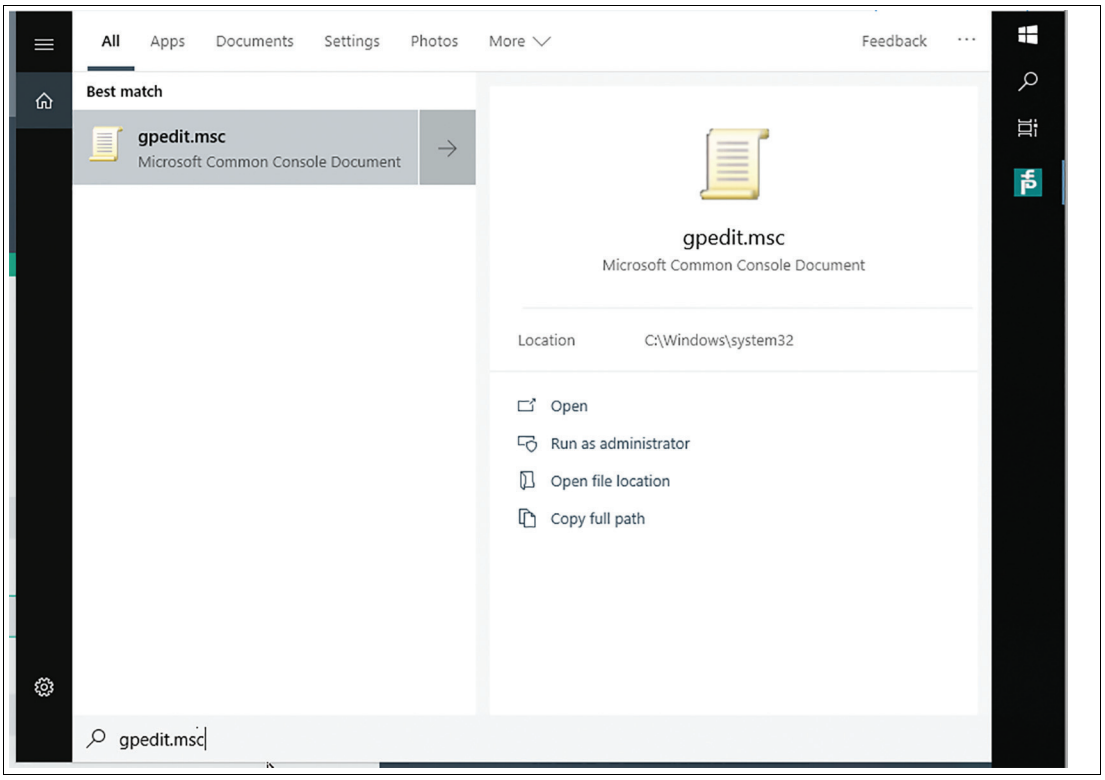


Figure 11.16

3. Navigate to: Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> Turn off encryption support
4. Select "Turn off encryption support" and double-click to open the dialog.

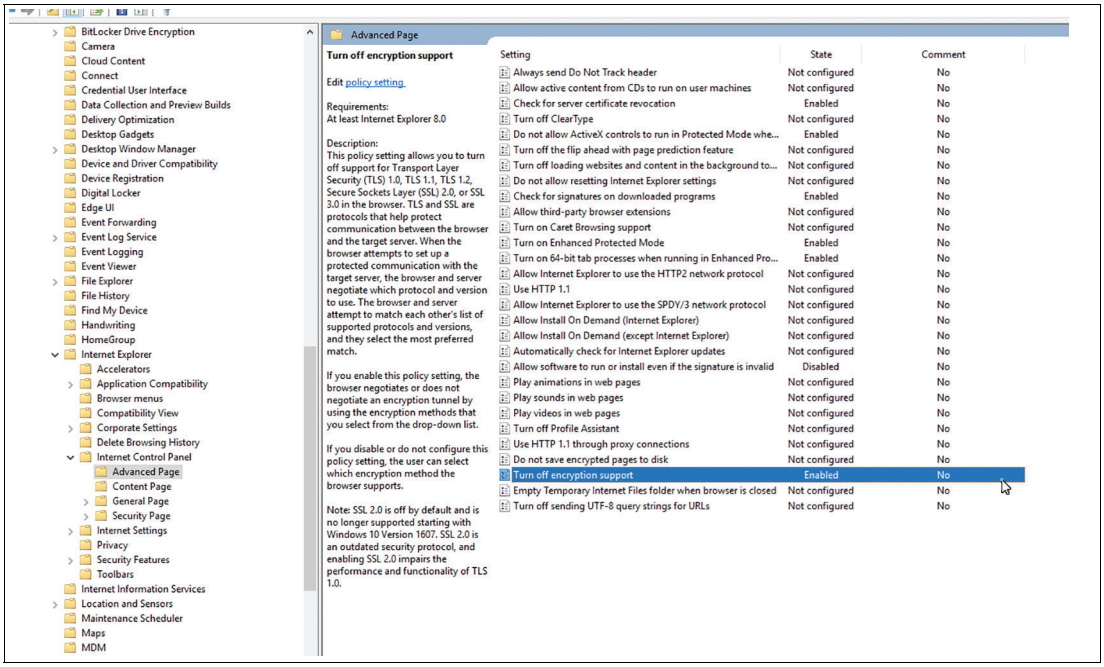


Figure 11.17

5. Select TLS 1.0, TLS 1.1, and TLS 2.0

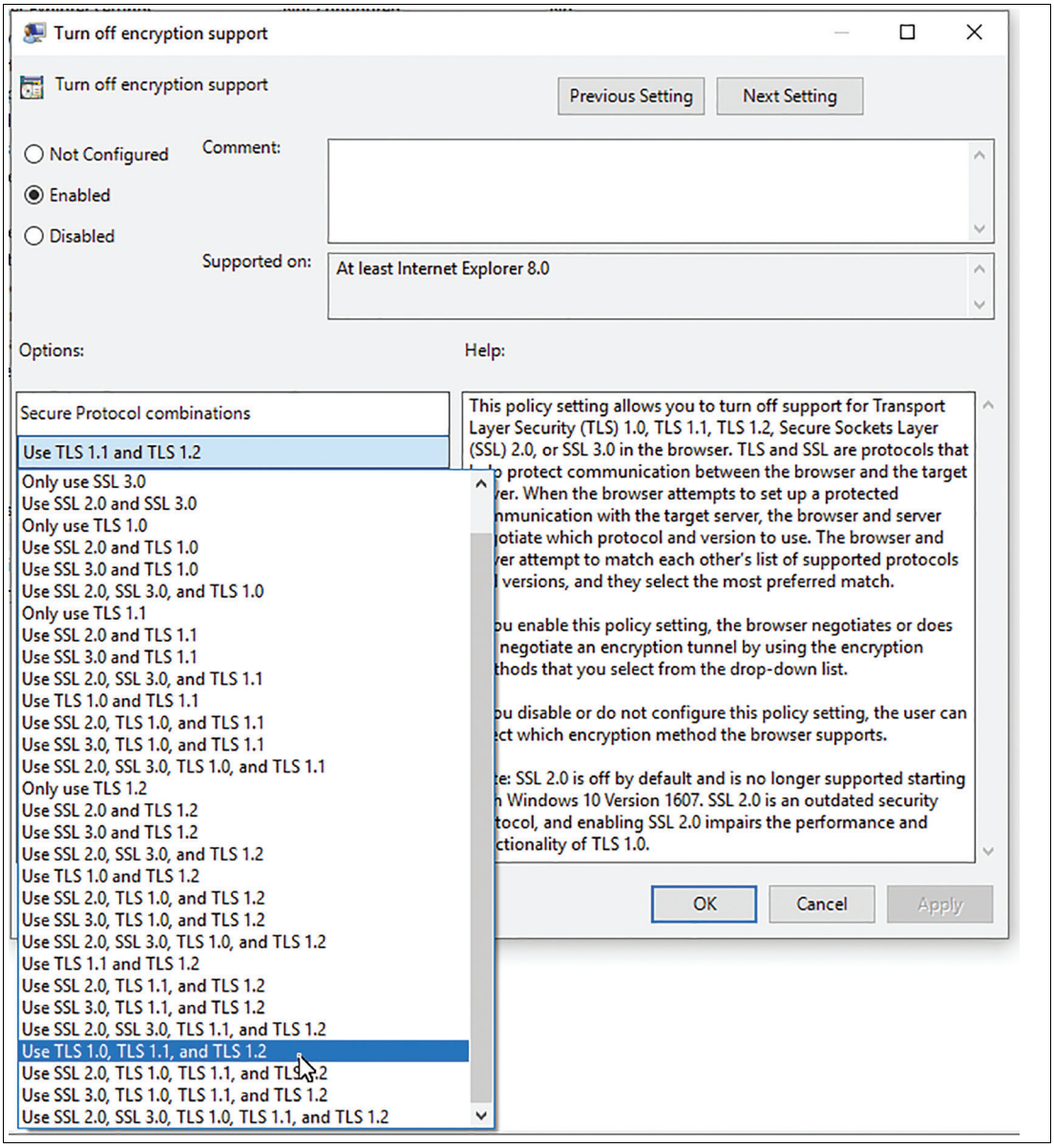


Figure 11.18

6. Close the dialog with Ok.
7. Reboot the Shell.

11.9 VLAN Tagging

Qualified with the following devices:

- BTC12
- BTC14
- VisuNet FLX
- VisuNet GXP (2020 Generation with Apollo Lake Processor)

Note

Install the Driver Update for the following devices BTC12, VisuNet FLX, VisuNet GXP (2020 Generation with Apollo Lake processor) if necessary (Step 4 fails). The individual driver updates are available online within the product pages of the devices.

Procedure

1. Login as Administrator
2. Open System Settings
3. Search inside the Windows® Taskbar for "Windows PowerShell" and open it.

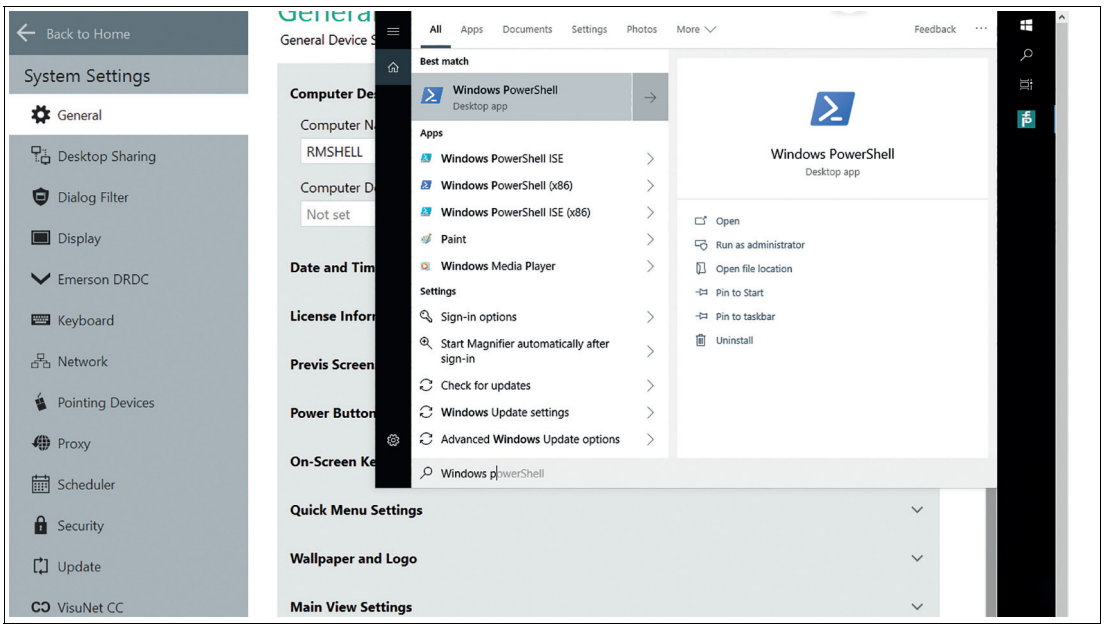


Figure 11.19

4. Load the needed PowerShell Module with: "Import-Module -Name 'C:\Program Files\Intel\Wired Networking\IntelNetCmdlets\IntelNetCmdlets'".
5. If this step fails, install the online available driver package of your device.
6. You can list all available network adapter with: "Get-IntelNetAdapter". Search for the network adapter Name, which should have the VLAN Tag.

Note

Typically the relevant Ethernet adapters are named Ethernet or Ethernet 2.

7. Now you can execute: "Add-IntelNetVLAN -ParentName "<device name>" -VLANID "<vlanid>"". Replace <device name> with the network adapter name of the step before and <vlanid> with your wanted VLan Id.
8. **Remove VLanTag:**
9. Remove-IntelNetVLAN -ParentName "<device name>" -VLANID "<vlanid>"

11.10 NIC Teaming

NIC Teaming via Windows® Implementation:

This option is compatible with the NICs of different manufacturers and for Pepperl+Fuchs devices driver updates are not necessary but has fewer configuration options compared to the Intel CMDlets.

This option is tested for all Pepperl+Fuchs devices based on Windows® 10 IoT 2019 LTSC with multiple network adapters including VisuNet GXP (2020 Generation with Apollo Lake processor).

Procedure

1. Log in as Administrator
2. Open System Settings
3. Search inside the Windows® Taskbar for "Windows PowerShell" and open it.
4. Execute the command "Get-NetAdapter" to get the names of the Network Adapters

   Note

   Typically the relevant Ethernet adapters are named Ethernet or Ethernet 2.

5. Execute "New-NetSwitchTeam -Name "<team name>" -TeamMembers "<network adapter name 1>", "<network adapter name 2>""
6. Replace <team name> with the team name you want to configure and "<network adapter name 1>", "<network adapter name 2>" with the Network Adapter Names, which were shown in step 4.
7. A new Network Adapter should appear, which can be configured.

   Remove Teaming:

   Execute "Remove- NetSwitchTeam -Name "<team name>""

NIC Teaming via Intel CMDlets:

For this option multiple team modes are available but works only for Intel NICs.

This option is tested for the following Pepperl+Fuchs devices: BTC12, BTC14, VisuNet FLX.

Note

Install the Driver Update for the following devices BTC12 and VisuNet FLX. The individual driver updates are available online within the product pages of the devices. For the BTC14 a driver update is not necessary.

Procedure

1. Log in as Administrator
2. Open System Settings
3. Search inside the Windows® Taskbar for "Windows PowerShell" and open it.
4. Load the needed PowerShell Module with: "Import-Module -Name 'C:\Program Files\Intel\Wired Networking\IntelNetCmdlets\IntelNetCmdlets'"
5. You can list all available network adapter with: "Get-IntelNetAdapter". Search for the Network Adapter Names, which should be Team Members.

   Note

   Typically the relevant Ethernet adapters are named Ethernet or Ethernet 2.

6. Execute the following command to create a new team:
7. New-IntelNetTeam -TeamMemberNames "<network adapter name 1>", "<network adapter name 2>" -TeamMode AdapterFaultTolerance -TeamName "<team name>"
8. Replace <network adapter name 1> and <network adapter name 2> with the names of the Network Adapters and replace <team name> with the name of the team you want to create.
9. There are more TeamModes that can be used. Seehttps://www.intel.de/content/www/de/de/support/articles/000032008/ethernet-products.html
10. A new Network Adapter should appear, which can be configured.

Remove Teaming:

Execute "Remove-IntelNetTeam -TeamName "<team name>"

12 Appendix

12.1 Open Network Ports

For communication between Control Center and RM Shell, the TCP port 8023 is used.

For the detection of existing RMs / BTCs (scan) use the UDP/TCP port 3702. https://en.wikipedia.org/wiki/WS-Discovery.

There is no DNS server for the NetBIOS translation. UDP port 137 is required. https://en.wikipedia.org/wiki/NetBIOS_over_TCP/IP

12.2 Shell freezes on RDP log-on screen

1. Navigate to "Touch" in the System Settings.

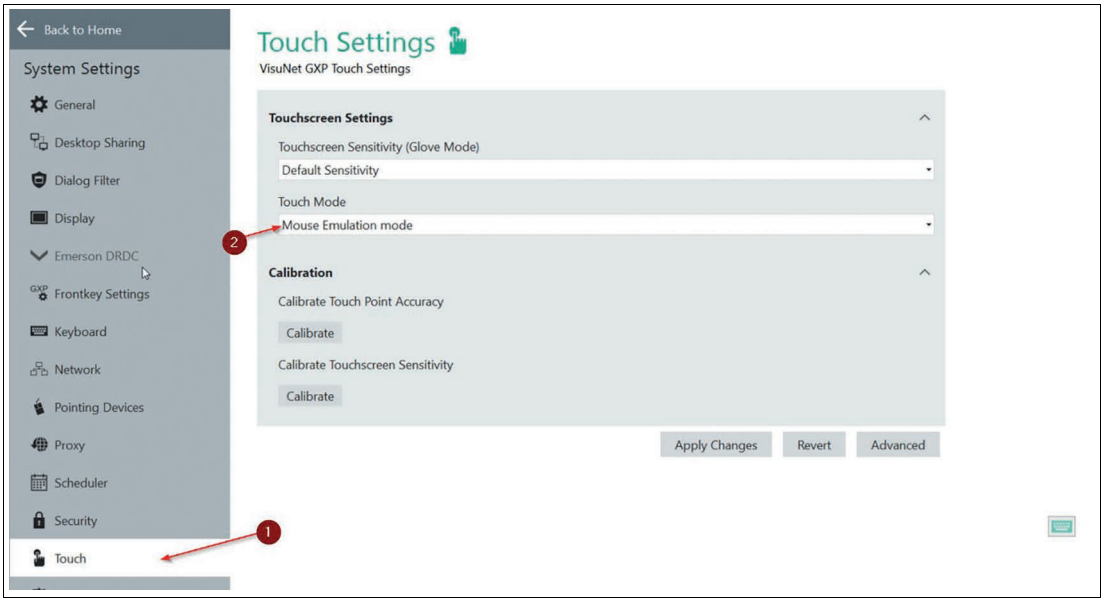


Figure 12.1

2. Select "Mouse Emulation mode" (2) in the System Settings "Touch"-tab (1).

Note

It is recommended to use the DRDC Profile. The no touch functionality when using an RDP-Profile is a windows bug.

12.3 Pepperl+Fuchs SE End User License Agreement (EULA)

IMPORTANT NOTE - READ CAREFULLY

THIS END-USER SOFTWARE LICENSE AGREEMENT IS A LEGALLY BINDING AGREEMENT BETWEEN YOU, AS A DESIGNATED USER OR AS A REPRESENTATIVE IN THE NAME OF A COMPANY OR AN ORGANIZATION, CALLED IN THE FOLLOWING THE “LICENSEE” AND THE PEPPERL+FUCHS SE, MANNHEIM, GERMANY CALLED IN THE FOLLOWING THE “LICENSER”.

READ THE WHOLE AGREEMENT CAREFULLY BEFORE YOU CONTINUE TO USE THE SOFTWARE. BY USING THE SOFTWARE, LICENSEE CONFIRMS HIS ACCEPTANCE AND AGREES TO BE BOUND BY THE TERMS OF THIS AGREEMENT.

IN CASE THE LICENSEE DOES NOT AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT, THE LICENSEE SHALL NOT USE THE SOFTWARE AND SHALL RETURN THE DEVICE AT HIS OWN EXPENSE TO THE LICENSER.

1 - Definitions

Licenser	Pepperl+Fuchs SE, Lilienthalstr. 200, 68307 Mannheim, Germany
Software	Means the Licenser software program(-s) including Microsoft Software, in each case, supplied by Licenser herewith, and the related information called “VisuNet RM Shell 5“ which are delivered by Licenser together with and already installed on one Device. Any updates to such Software which the Licensee is entitled to receive and that has been provided to him by the Licenser shall also mean Software for purposes of this Agreement.
Microsoft Software	Means the MICROSOFT SOFTWARE LICENSE TERMS - WINDOWS 10, which is subject to additional terms and conditions referenced in the About screen of the “VisuNet RM Shell 5”. By using the Software, the Licensee is also bound by the additional terms and conditions of the Microsoft Software.
Device	Means each product of the Licenser incorporating the Software.
License	By granting a License the Licenser grants to the Licensee the right to use the Software under the terms and conditions defined in this EULA.

2 - Subject Matter of the EULA

2.1 The Licenser provides the Software which is subject to the following terms and conditions of use “VisuNet RM Shell 5”.

2.2 A Service Contract for the Software is not available.

3 Grant of License

3.1 Subject to the terms and conditions set forth in this EULA, the Licenser grants the Licensee a personal, non-exclusive and timely not limited License to use the Software according to the following provisions:

3.2 The Licenser grants to the Licensee the right to use the Software on the Device on which it is delivered to the Licensee. The Licensee may only use the Software for that use.

3.3 The Licensee is entitled to make one copy of the Software only for backup purposes, provided that such copy clearly marks all copyright notices and any other proprietary legends regarding the original copy.

3.4 The Licensee shall only after prior written consent of the Licenser be entitled to transfer the right to use the Software to a third party provided the third party accepts to enter into the terms and conditions of this EULA and the Licensee dos not retain any copies of the Software. The transfer of the right to use the Software may only take place together with the Device on which the Software has been installed by the Licenser.

4 - License Restrictions

4.1 The Licensee is in no way entitled to change, alter, enhance the Software or any parts of the Software and may not make any modifications on the Software or create derivative works based upon the Software except with the prior written consent of the Licenser.

4.2 The Licensee is in no way entitled to de-compile, disassemble or otherwise reverse engineer the Software or any parts of the Software, in whole or in parts or attempt to access or derive the source code of the Software or any algorithms, concepts, techniques, methods or processes embodies therein.

4.3 Other than as set forth in Section 3 the Licensee is no way entitled to make or distribute copies of the Software, rent, lease, lend or sublicense the Software, or electronically transfer the Software from the Device to another or over a network.

5 - Infringement of Third Party Rights

5.1 In the event that any material part of the Software becomes subject of a valid third party claim of copyright, patent or other proprietary right infringement, the Licenser shall, at its option, either (i) replace the Software with a compatible, functionally equivalent, non infringing software product; (ii) modify the Software or take some other action so that it is no longer infringing; (iii) procure the right for the Licensee to continue using the Software; or (iv) if, in the sole discretion of the Licenser, none of the foregoing alternatives is reasonably or with reasonable costs and/or efforts available, terminate this License.

5.2 The foregoing states the entire liability of the Licenser with respect to claims for copyright or patent infringement and except as provided in this section Licenser shall have no other liability to Licensee whatsoever for any loss or damage or infringement claims against Licensee by third parties arising out or related to any allegation or determination that Licensee`s use of the Software infringes any proprietary or intellectual property right.

6 - Ownership and Intellectual Property Rights, passing of risk

6.1 The License grants to the Licensee the limited license to use the Software according to the terms of this EULA.

6.2 All title and interest to, and intellectual property rights in the Software and any related documents are and shall remain owned and/or controlled solely and exclusively by the Licenser. The Licenser reserves all rights in the licensed Software not specifically granted to the Licensee in this EULA, including national and international Copyright.

6.3 Passing of the risk between Licenser and Licensee concerning the Software takes place at the time the Device on which the Software is installed is delivered to the Licensee.

7 - Limited Warranty and Disclaimer

7.1 The Licensee expressly acknowledges and agrees that he is using the licensed Software at his own sole risk. The Licenser provides no warranties or other remedies, whether express or implied, for the licensed Software. It is provided “as is” without warranty, term or condition of any kind unless otherwise agreed to in this EULA.

7.2 The Licenser warrants that at the date of passing of risk, that when the Software is installed in the hard- and/or software configuration in which it is delivered to the Licensee, the Software will perform in substantial conformance with the performance described in the related information.

7.3 Except as set forth in the forgoing limited warranty the Licenser disclaims all other warranties whether express, implied or otherwise, including the warranties of merchantability or fitness for a particular purpose. Also, the Licenser does not warrant that the Software is error-free or will operate without interruption.

7.4 No additional oral or written information or advice given by the Licenser, its dealers, distributors, agents or employees shall create a warranty or in any way increase the scope of any warranty provided above.

7.5 Licenser and Licensee agree that there is a defect in the Software if it does not have the above stipulated qualities and properties defined in Sec. 7.2 on passing of risk. Defects in the Software recognized on the Licensee's side can only be accepted when they are reconstructable or proven.

7.6 There is no defect if the Software is used on hardware other than the Device on which the Software has been installed. There is either no defect in the following cases:

- damages resulting from faulty or negligent handling of the Software not caused by the Licenser,
- damages resulting from particular external influences not assumed under this EULA,
- any modifications made by the Licensee or third parties, and any consequences resulting there from,
- incompatibility of the Software with the data processing environment of the Licensee.

7.7 If there is any defect, the Licenser is entitled to choose the option of remedying the defect at its own sole discretion by (a) delivering a substitute for the defect Software or (b) offering a subsequent performance. The warranty period shall be governed by the purchase contract of the Device.

8 - Limitation of Liability

8.1 The maximum aggregate liability of the Licenser or its officers, directors, employees, agents, distributors and resellers under this License for all losses or damages, expenses or injuries either direct, indirect, incidental or otherwise, arising out of the breach of any express or implied warranty, term or condition, breach of contract, tort, statue or any other legal theory arising out of, or related to this EULA or the use the Software shall be limited to 10% of the purchase price for the Device paid by the Licensee.

8.2 IN NO EVENT SHALL LICENSER BE LIABLE TO LICENSEE OR ANY THIRD PARTY FOR (A) LOSS OF PROFITS, LOSS OF REVENUE, (B) INDIRECT, INCIDENTAL OR CONSEQUENTIAL LOSSES EVEN IF ADVISED OF THE POSSIBILITY OF SUCH (C) LOSS OF DATA OR ANY ASSOCIATED EQUIPMENT DOWN TIME.

8.3 The limitation of liability does neither apply when the Licenser is liable for intentional breach of duty or gross negligence regardless of the legal ground nor when a higher liability is asked according to compulsory statutory regulations such as but not limited to provided in the Product Liability Act.

8.4 No action or proceeding relating to this EULA may be commenced by Licensee more than three month after the cause of action arises.

9 - Third Party Software

Portions of the Software are developed in part on the work of software of the third parties which requires notices and/or additional terms and conditions which are located at the About screen of the "VisuNet RM Shell 5". In addition, the Software contains Open Source Software Programs of third parties which are provided in verbatim copies. A list of the contained Open Source Software Programs including the required prominent notices and the respective license terms are also located at the About screen of the "VisuNet RM Shell 5".

10 - Additional features of the Software

In case of acquisition of additional features of the Software, the Licenser will provide to the Licensee a product key that authorizes the use of the additional features on the Device which it is delivered to the Licensee; any other use of the product key, especially for any other devices is not allowed.

11 - Governing Law and Place of Jurisdiction

11.1 The validity, interpretation and legal effect of this EULA shall be governed by, and construed in accordance with, the laws of the Federal Republic of Germany under the exclusion of German conflict law.

11.2 The courts of Landgericht Mannheim, Germany, shall have sole jurisdiction of any controversies regarding this EULA. Any action or other proceeding which involves such a controversy shall be brought in those courts in Mannheim and not elsewhere.

2022-02

12 - Severability and Inconsistencies

12.1 Should any provision of this EULA be determined to be overly broad, ambiguous or otherwise unenforceable, such provision shall be redrafted in order to narrow its scope to the extent necessary to make the provision reasonable and enforceable. If the scope of the provision cannot be narrowed to such an extent that the provision will become enforceable, such provision shall be severed from this EULA.

12.2 In all cases the remainder of the EULA shall continue in full force and effect.

12.3 In case the terms of this EULA are in conflict with the terms of Microsoft Software License terms, the terms of the latter shall prevail with regard to the Microsoft Software.

13 - Alterations

Alterations and changes of as well as amendments to this EULA are only valid when they were made in writing and signed by both parties; this requirement of written form can be waived only in writing.

Your automation, our passion.

Explosion Protection

- Intrinsic Safety Barriers
- Signal Conditioners
- FieldConnex® Fieldbus
- Remote I/O Systems
- Electrical Ex Equipment
- Purge and Pressurization
- Industrial HMI
- Mobile Computing and Communications
- HART Interface Solutions
- Surge Protection
- Wireless Solutions
- Level Measurement

Industrial Sensors

- Proximity Sensors
- Photoelectric Sensors
- Industrial Vision
- Ultrasonic Sensors
- Rotary Encoders
- Positioning Systems
- Inclination and Acceleration Sensors
- Fieldbus Modules
- AS-Interface
- Identification Systems
- Displays and Signal Processing
- Connectivity

Pepperl+Fuchs Quality
Download our latest policy here:

www.pepperl-fuchs.com/quality

PEPPERL+FUCHS

www.pepperl-fuchs.com

Printed in Germany / DOCT-6044G