VisuNet RM Shell 6

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

1 History of the Manual

The following editions of the manual have been released:

Version	Comments
05/2023	First version
07/2023	Addition of chapter "Information about Cyber Security" including the following topics: - Security Context - Commissioning of the device - Operation of the device - Decommissioning of the device - User roles and their tasks to ensure cybersecurity in device operations - User roles and rights Minor corrections Minor corrections
02/2024	Added new Features of VisuNet RM Shell 6.07 - KM Switch 2 Settings - RFID reader Settings Revision of Chapter 11.11 VLAN Tagging

2 Introduction

2.1 Note

This manual revision was released with VisuNet® RM Shell version 6.

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.

Note

For specific device information such as the year of construction, scan the QR code on the device. As an alternative, enter the serial number in the serial number search 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
- Functional safety 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 restricted web browser features, 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 Program Features

Feature	Description	Notes
Operating system	Based on Microsoft® Windows® 10 IoT Enterprise LTSC 2021	
Modern, simplified user interface	Touch-optimized, modern UI, Dark Mode	
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	
Auto-connect	Allows you to configure the RM to automatically connect to host systems after startup	
Smart Task Bar	Provides easy access to relevant functions and enables quick switching between connections	New feature in VisuNet RM Shell 6
Backup connection	In case of a network or host failure, an RM can automatically connect to a backup host system	
Hybrid Management Mode	Distinction between OT and IT administrators. The Shell is accessible for OT administrators while only IT administrators can access the Windows®.	New feature in VisuNet RM Shell 6

Feature	Description	Notes
Centralized management of all RMs	RMs can be managed and configured centrally via VisuNet Control Center.	Optional CC license feature. Find further information at www.pepperl-fuchs.com/hmi
Remote Protocols and Clients		
MS RDP	Latest version of Microsoft® Remote Desktop Protocol	
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 Chromium (same technology as 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	
Antivirus software support	Administrators can install third-party virus protection software. Windows® defender is activated by default	
Dialog filter	Closes application windows that are not whitelisted and blocks user access to the file system	
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.	Check for updates regularly or use our Thin Client Software Update Service to be informed by Pepperl+Fuchs.
Backup Image	Capture your individual device settings of the RM/BTC as a backup image and apply when required back on to the device. Apply your individual device settings of the RM/BTC which were earlier captured as a backup image and overwrite the full Windows® partition.	

Feature	Description	Notes
Additional Security Features		
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
Supports Windows® security update	Windows® security updates can be installed using the Windows® desktop user interface and the integrated update mechanisms	https://www.microsoft.com
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.	
Clean lock	Allows you to temporarily lock the input devices (e.g., touch screen) 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 VisuNet 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	

3.2 Information about Cybersecurity

The devices shipped with RM Shell 6 are secure according to IEC 62443-4-1 for the area of application defined here. For cybersecure operation and protection of the device, the plant operator must implement the measures specified in this section.

3.2.1 Security Context

The RM Shell 6 devices are intended to be used:

1. as Thin Clients that connect to known, trusted, preconfigured remote desktop servers which host the Decentralized Control System (DCS) in an "Automation Network" or "MES" and "ERP" systems that are located in an "Automation" or "Enterprise Network".
2. within the internal "Automation" or "Enterprise network". Both are secured Network, with known, trusted participants which is physically and logically separated from the company network.
3. with a firewall that must be configured in a way, that only specific ports are redirected into other subnets and that an external access from outside those networks is not possible.
4. within non-public environments where access is controlled and where only known persons (operators) have access to the device.

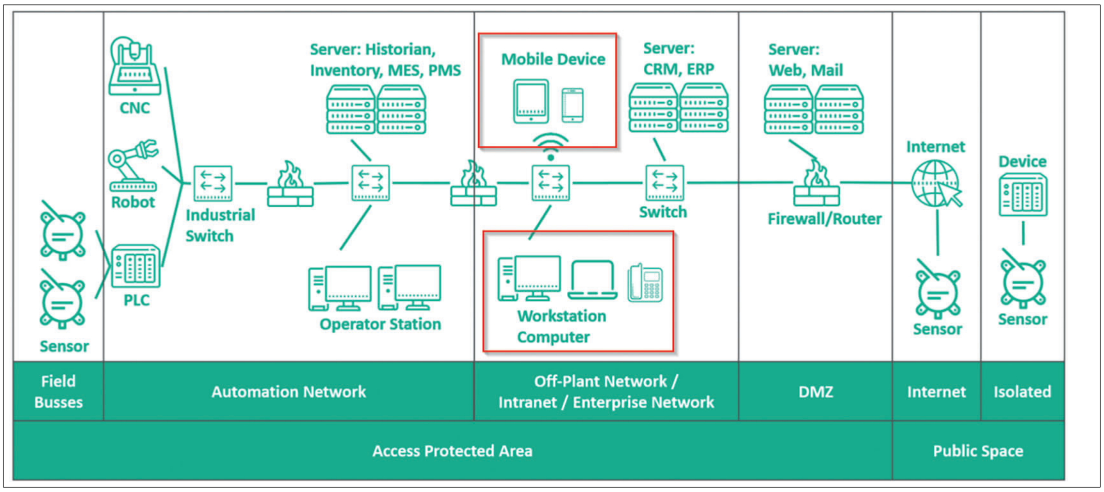


Figure 3.1

A firewall must be configured to forward only defined ports to other subnets.

The device uses the following incoming ports:

Port	Protocol		Description
3702 and 137	-	UDP	VisuNet CC Discovery
8023	TCP	-	VisuNet CC Download/Upload
5900	TCP	-	VisuNet CC Session Shadowing
22314	TCP	-	VisuNet CC Default Secure Tunnel Port
23314	TCP	-	Factory Reset Communication Port

The device must be physically secured against access by unauthorized persons and operated in a lockable control cabinet or room that is only accessible to authorized personnel. Otherwise there is a risk that parts of the device settings can be changed via the display without authentication.

The device contributes to the "defence-in-depth" strategy with the following security functions:

Security function	Addressed threat
Device Protection	- Limit physical access. - Change BIOS password. - Power button (if available) should be physically protected or disable on GXP devices.
Windows protection	- Change Windows users and credentials. - Disable Windows Auto-Login - Join device to domain and manage users via domain.
Factory Reset	- Change Factory Reset password.
Remote connection	- Use encrypted and certificate based remote connections like RDP.
Start of remote connection	- Evaluate the authentication of remote connections. - Control physical access to the device. - Set Smart Screen Saver PIN to mitigate unauthorized access. - Do not leave the Windows OS logged in without observation. - Disable Auto-Login.
Configuration	- Prevent sniffing of touch or keyboard input. - Logout from "Configuration View" when leaving the device. - Logout from "View Logfile" when leaving the device.
Desktop Sharing	- Use Secure Tunnel with custom device dependent certificate.

3.2.2 Commissioning of the device

The following measures must be implemented on the device for commissioning:

Hardening	Run through the first start wizard and set passwords for the preconfigured users and the Factory Reset
Integration with VisuNet CC	Install device dependent certificates
Integration with Domain Network	Disable or remove local pre-configured users

3.2.3 Operation of the device

The following measures must be implemented on the device for operation:

Additional security layers:	Certificate renewal: every 3 years. Password change: every 2 years.
Recommendation for security-related tools	Ensure that Windows defender is enabled or a 3rd party virus scanner is installed
Maintenance	**RM Shell 6:** Check the website regularly for Security Advisories postings and subscribe to the RSS feed:https://www.pepperl-fuchs.com/global/en/29079.htm **Windows 10 LTSC 2021:** For updates of the operating system please check regularly: https://www.microsoft.com Windows security updates can be installed by the Administrator using the Windows desktop and the usual Windows Update functions. **Infrastructure:** Keep your host devices and infrastructure also up-to-date

3.2.4 Decommissioning of the device

The following measures must be implemented for decommissioning the device:

User credentials	Perform a "Factory Reset" or format the internal disc drive using an external live OS
Configuration	Perform a "Factory Reset" or format the internal disc drive using an external live OS
Further operating data	Perform a "Factory Reset" or format the internal disc drive using an external live OS
Log data	Perform a "Factory Reset" or format the internal disc drive using an external live OS

3.2.5 User roles and their tasks to ensure cybersecurity in device operations

User role requirements for cybersecure operations:

Administrator	• Implementation of the measures defined under "The following measures must be implemented on the device for operation". • If necessary: Update the firmware or install security patches. • Assign only necessary rights to a user account.
User	• The user has by default no rights to change the system.

3.2.6 User roles and rights

User roles and rights:

Administrator	• User account management and rights assignment • Switching functions and services on and off • Configuration • Resetting to factory settings • Reading log and device status • Firmware updates
User	• Execute configured connection profiles • View "About" information • Execute "System Tools" • Execute the functions assigned by the administrator

3.3 Factory Reset

Only for the devices with 64 GB of memory, the image is already installed on the local disk. For devices with 32 GB of memory, the image is not stored on the disk.

i

Note

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.	Get in contact with your local sales support if you require a factory reset image. **Caution!** After applying the Pepperl+Fuchs image, the setup of the device must be performed locally! The VisuNet RM Shell first start wizard guides 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.

3.4 Licensing

Ordering Information

When purchasing Pepperl+Fuchs RMs or BTCs, RM Shell 6 is already installed.

License keys are available as digital and paper-based license keys. Digital license keys are available in following countries: Germany, Switzerland, Austria, Italy, Spain, UK, Ireland, France, Netherlands, Belgium, Norway, Denmark, Sweden, Finland, Poland, United Arab Emirates, USA, Brazil and Singapore.

Licenses are sent out via Email in form of a PDF document. Keys are listed in the PDF document.

Following single licenses and license bundles are available:

Shell 6 PRO

Part No.	Model Number	Type
XSP2-037-03R	VISUNET-RM-SHELL6-PRO-DLK	Digital License Key[1]
70162174	VISUNET-RM-SHELL6-PRO	Paper-based License Keys
70162175	VISUNET-RM-SHELL6-PRO-5	
70162176	VISUNET-RM-SHELL6-PRO-10	
70162177	VISUNET-RM-SHELL6-PRO-30	
70162178	VISUNET-RM-SHELL6-PRO-50	

[1] Only available in Germany, Switzerland, Austria, Italy, Spain, UK, Ireland, France, Netherlands, Belgium, Norway, Denmark, Sweden, Finland, Poland, United Arab Emirates, USA, Brazil and Singapore.

Shell 6 CC

Part No.	Model Number	Type
XSP2-037-01R	VISUNET-RM-SHELL6-CC-DLK	Digital License Key[1]
70162159	VISUNET-RM-SHELL6-CC	Paper-based License Keys
70162160	VISUNET-RM-SHELL6-CC-5	
70162161	VISUNET-RM-SHELL6-CC-10	
70162162	VISUNET-RM-SHELL6-CC-30	
70162164	VISUNET-RM-SHELL6-CC-50	

[1] Only available in Germany, Switzerland, Austria, Italy, Spain, UK, Ireland, France, Netherlands, Belgium, Norway, Denmark, Sweden, Finland, Poland, United Arab Emirates, USA, Brazil and Singapore.

Shell 6 DRDC

Part No.	Model Number	Type
XSP2-037-02R	VISUNET-RM-SHELL6-DRDC-DLK	Digital License Key[1]
70162169	VISUNET-RM-SHELL6-DRDC	Paper-based License Keys
70162170	VISUNET-RM-SHELL6-DRDC-5	
70162171	VISUNET-RM-SHELL6-DRDC-10	
70162172	VISUNET-RM-SHELL6-DRDC-30	
70162173	VISUNET-RM-SHELL6-DRDC-50	

[1] Only available in Germany, Switzerland, Austria, Italy, Spain, UK, Ireland, France, Netherlands, Belgium, Norway, Denmark, Sweden, Finland, Poland, United Arab Emirates, USA, Brazil and Singapore.

Note

License Bundles

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

3.5 Default Passwords

Warning!

It is highly recommended to change the default passwords due to security reasons.

Device/Function	User	Password
Factory reset		VisuReset
Raritan KVM over IP Switch DKX4-101	admin	raritan
Shell / Windows User	PFUser	VisuNetRMShell6
Shell / Windows Admin	PFAdmin	VisuNetRMShell6Admin

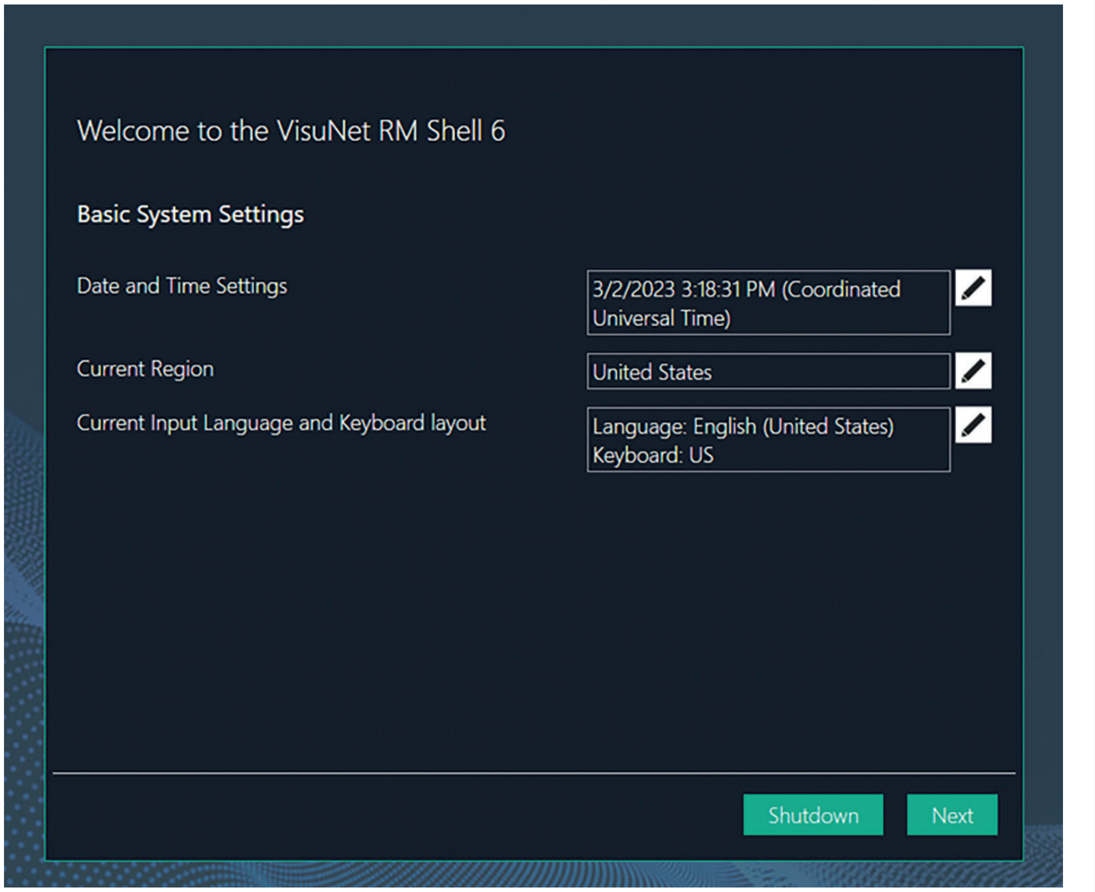
3.6 Installation

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 following window to start using VisuNet RM Shell.



Welcome to the VisuNet RM Shell 6

Basic System Settings

Date and Time Settings: 3/2/2023 3:18:31 PM (Coordinated Universal Time)

Current Region: United States

Current Input Language and Keyboard layout: Language: English (United States) Keyboard: US

Figure 3.2

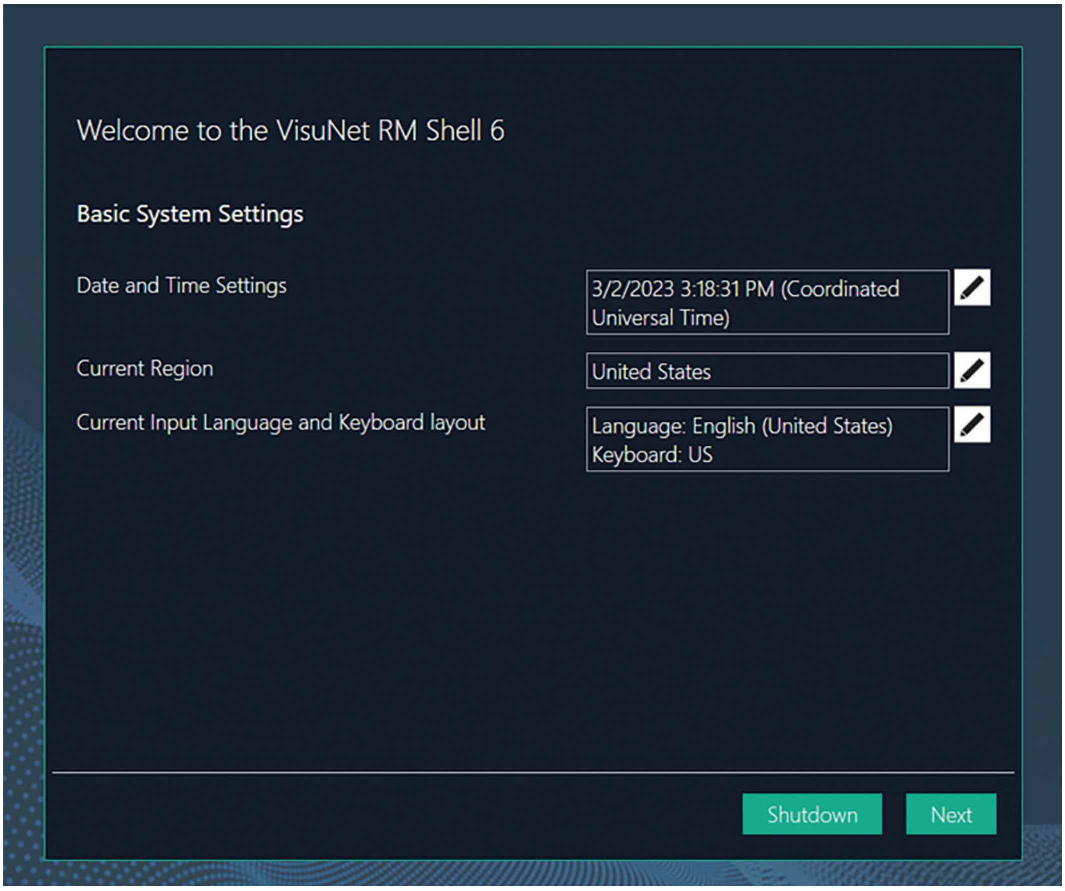
Note

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.**

Set the correct "Region"

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



Welcome to the VisuNet RM Shell 6

Basic System Settings

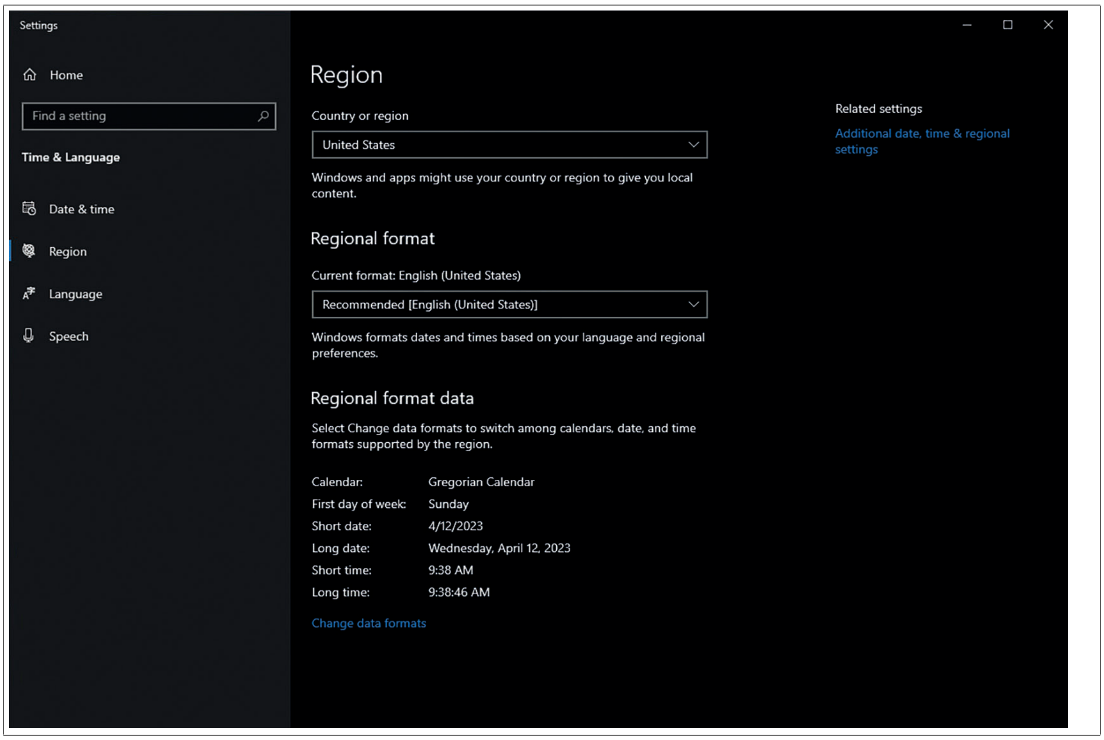
Date and Time Settings: 3/2/2023 3:18:31 PM (Coordinated Universal Time)

Current Region: United States

Current Input Language and Keyboard layout: Language: English (United States) Keyboard: US

Figure 3.3

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



Region

Country or region

United States

Windows and apps might use your country or region to give you local content.

Regional format

Current format: English (United States)

Recommended [English (United States)]

Windows formats dates and times based on your language and regional preferences.

Regional format data

Select Change data formats to switch among calendars, date, and time formats supported by the region.

Calendar:	Gregorian Calendar
First day of week:	Sunday
Short date:	4/12/2023
Long date:	Wednesday, April 12, 2023
Short time:	9:38 AM
Long time:	9:38:46 AM

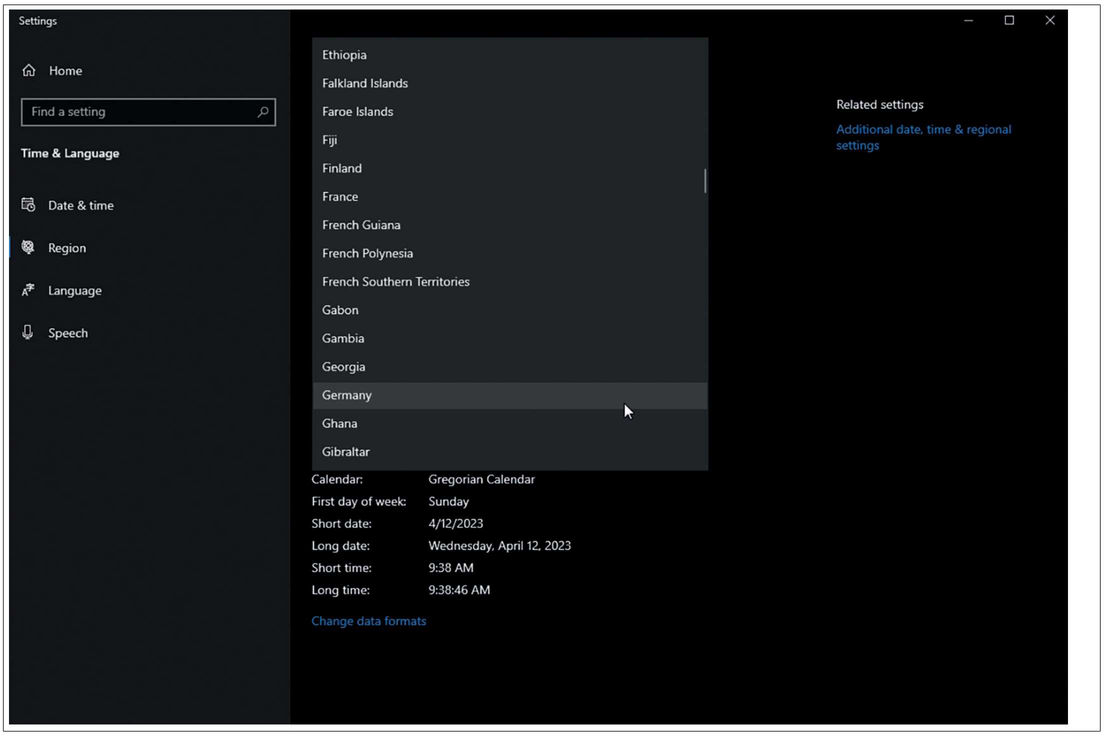
Change data formats

Related settings

Additional date, time & regional settings

Figure 3.4

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



Ethiopia
Falkland Islands
Faroe Islands
Fiji
Finland
France
French Guiana
French Polynesia
French Southern Territories
Gabon
Gambia
Georgia
Germany
Ghana
Gibraltar

Calendar:	Gregorian Calendar
First day of week:	Sunday
Short date:	4/12/2023
Long date:	Wednesday, April 12, 2023
Short time:	9:38 AM
Long time:	9:38:46 AM

Change data formats

Related settings

Additional date, time & regional settings

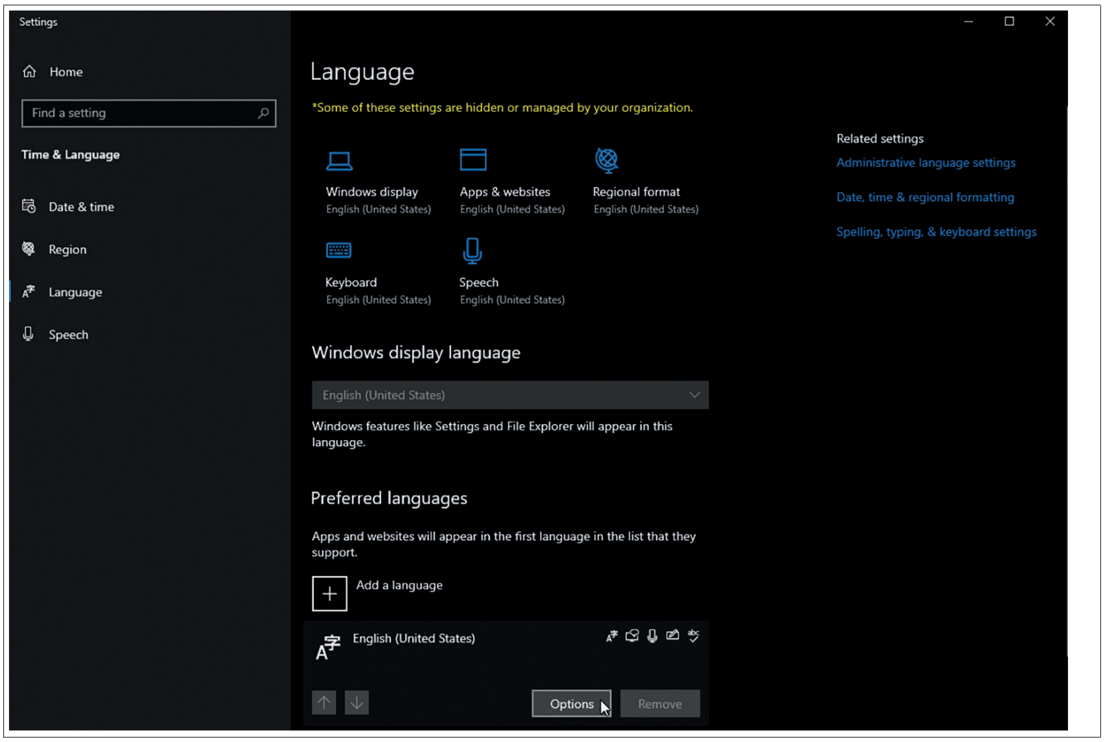
Figure 3.5

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:



Language

*Some of these settings are hidden or managed by your organization.

Windows display
English (United States)

Apps & websites
English (United States)

Regional format
English (United States)

Keyboard
English (United States)

Speech
English (United States)

Windows display language

English (United States)

Windows features like Settings and File Explorer will appear in this language.

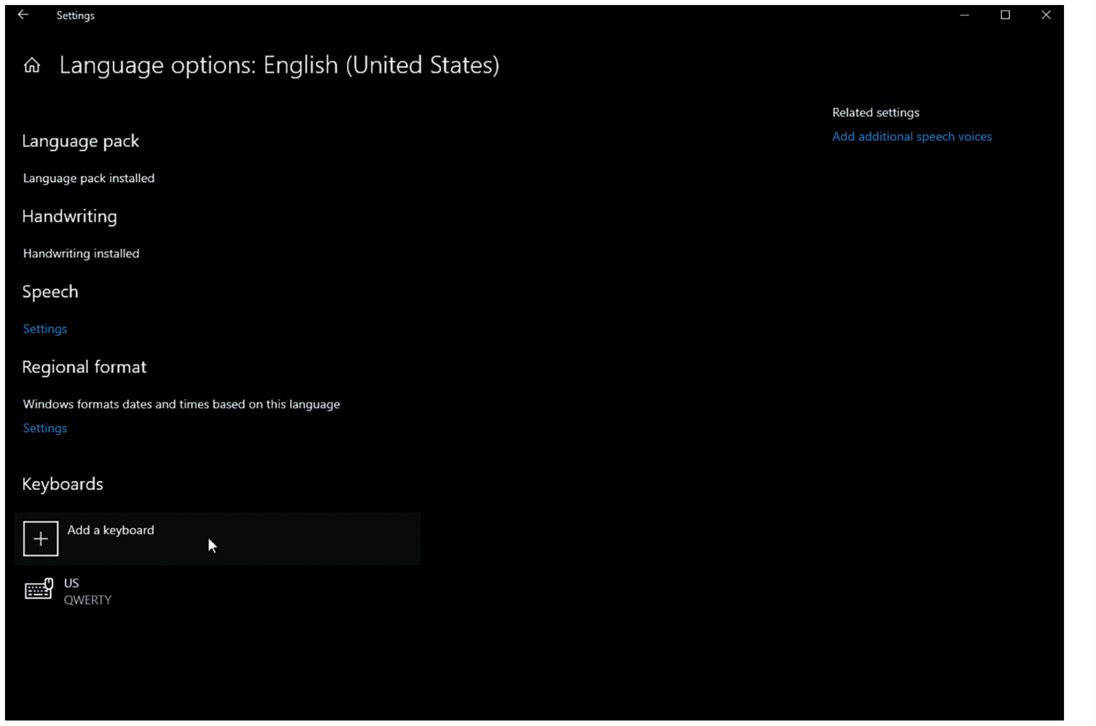
Preferred languages

Apps and websites will appear in the first language in the list that they support.

English (United States)

Figure 3.6

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



Settings

Language options: English (United States)

Related settings
Add additional speech voices

Language pack
Language pack installed

Handwriting
Handwriting installed

Speech
Settings

Regional format
Windows formats dates and times based on this language
Settings

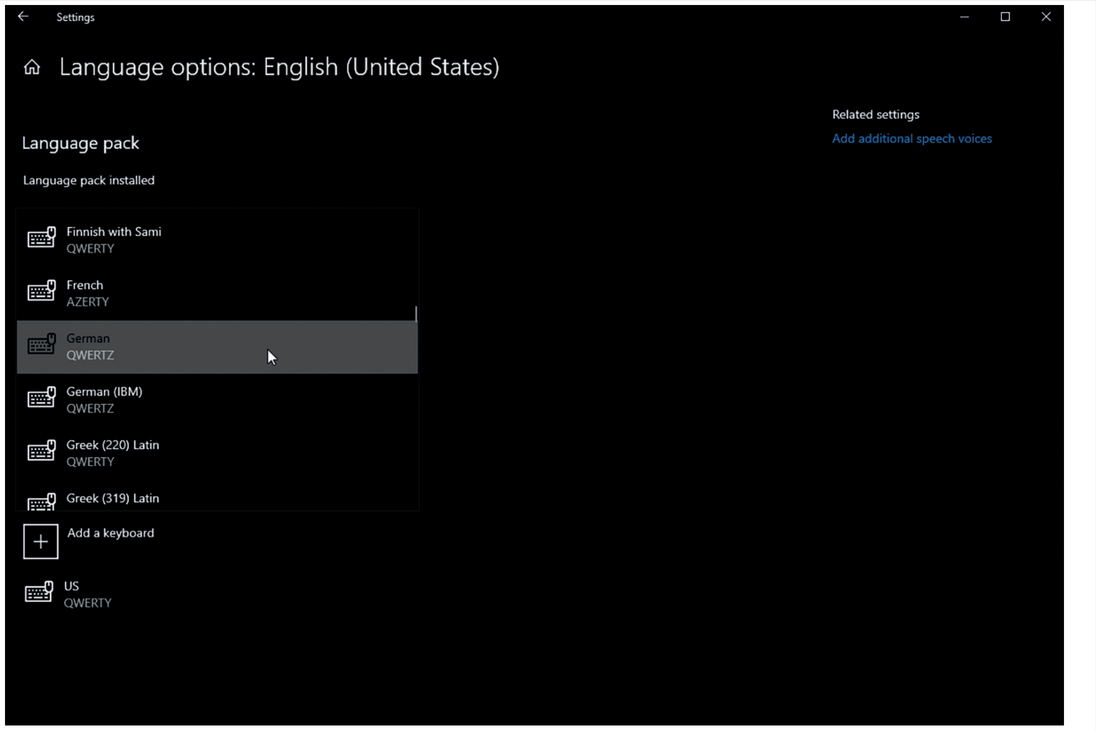
Keyboards

+ Add a keyboard

US
QWERTY

Figure 3.7

3. Select the new "Keyboard" layout:



Settings

Language options: English (United States)

Related settings
Add additional speech voices

Language pack
Language pack installed

Finnish with Sami
QWERTY

French
AZERTY

German
QWERTZ

German (IBM)
QWERTZ

Greek (220) Latin
QWERTY

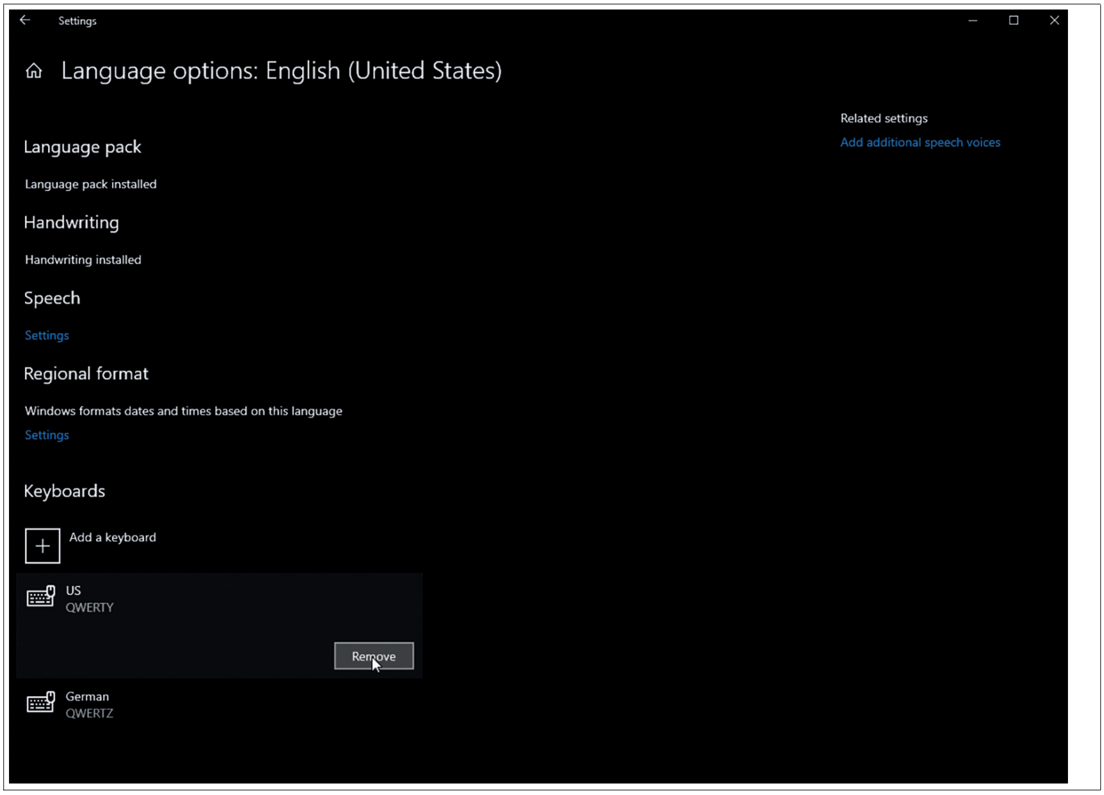
Greek (319) Latin

+ Add a keyboard

US
QWERTY

Figure 3.8

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



Settings

Language options: English (United States)

Language pack

Language pack installed

Handwriting

Handwriting installed

Speech

Settings

Regional format

Windows formats dates and times based on this language

Settings

Keyboards

Add a keyboard

US
QWERTY

Remove

German
QWERTZ

Related settings

Add additional speech voices

Figure 3.9

5. Close the dialog.

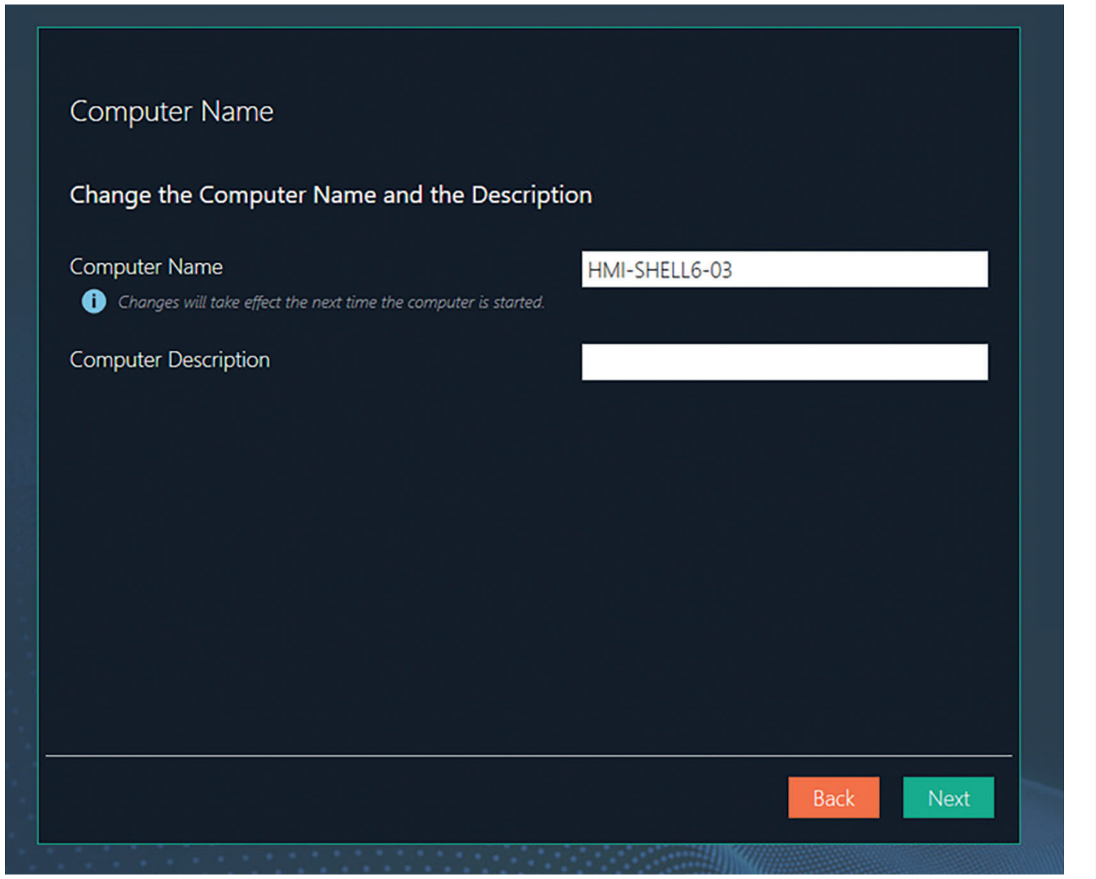
Note

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

"Computer Name"

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

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



Computer Name

Change the Computer Name and the Description

Computer Name: HMI-SHELL6-03

Changes will take effect the next time the computer is started.

Computer Description:

Figure 3.10

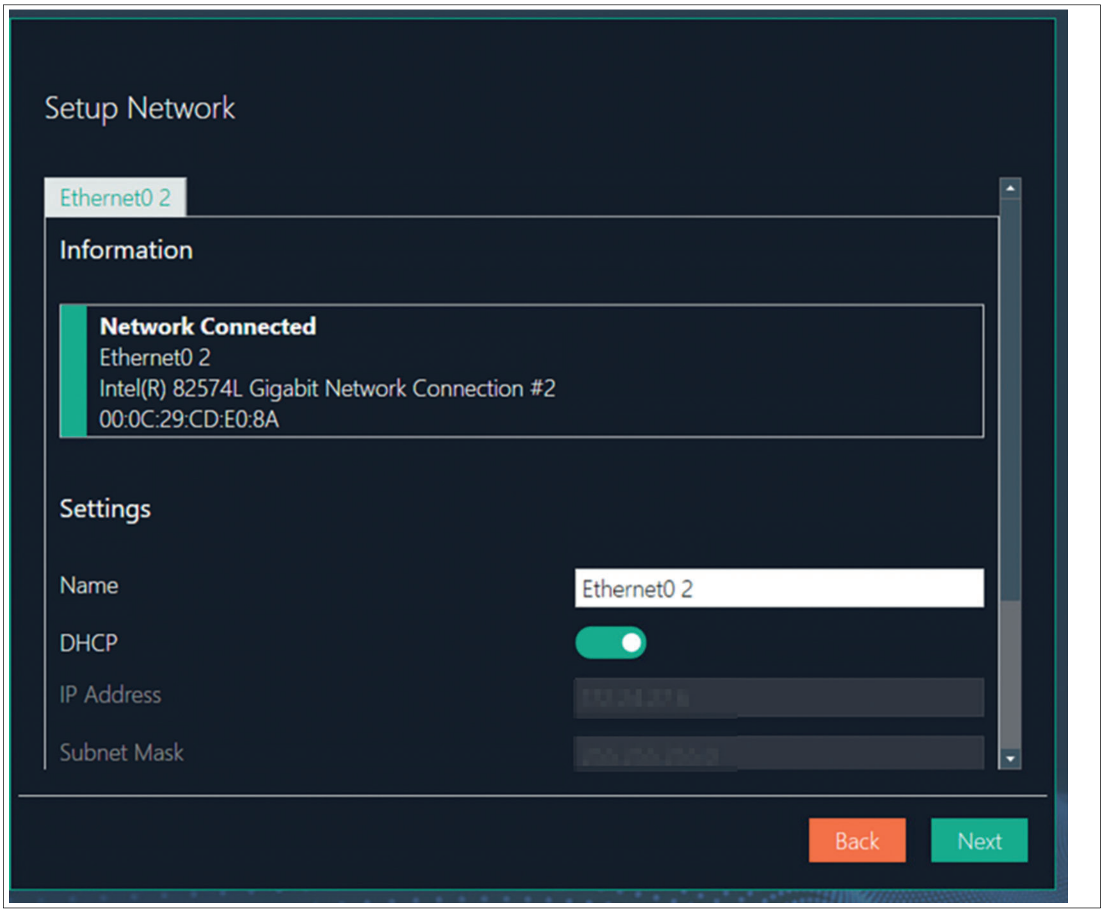
Setup "Network"

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.



Setup Network

Ethernet0 2

Information

Network Connected
Ethernet0 2
Intel(R) 82574L Gigabit Network Connection #2
00:0C:29:CD:E0:8A

Settings

Name: Ethernet0 2

DHCP: on

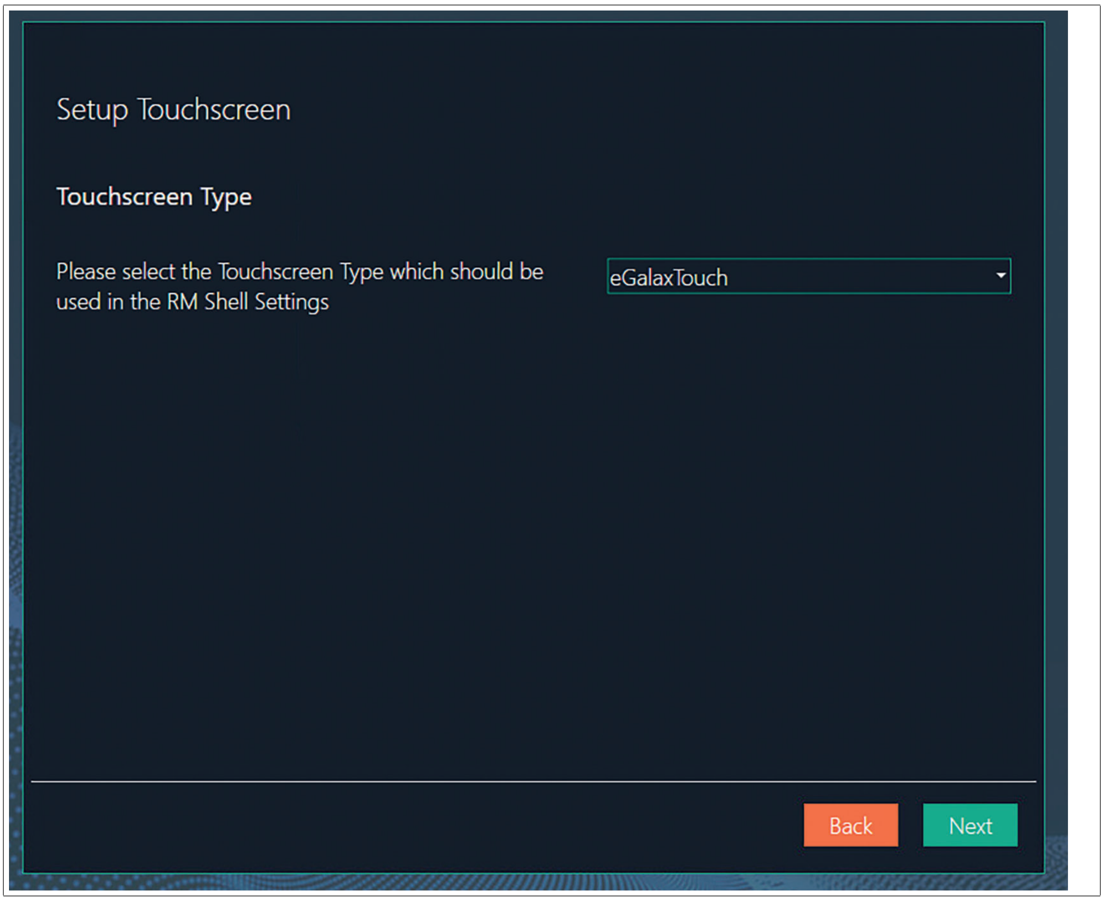
IP Address: [redacted]

Subnet Mask: [redacted]

Figure 3.11

"Setup Touchscreen"

Select the right touch settings, if your RM is equipped with a touch screen option.



Setup Touchscreen

Touchscreen Type

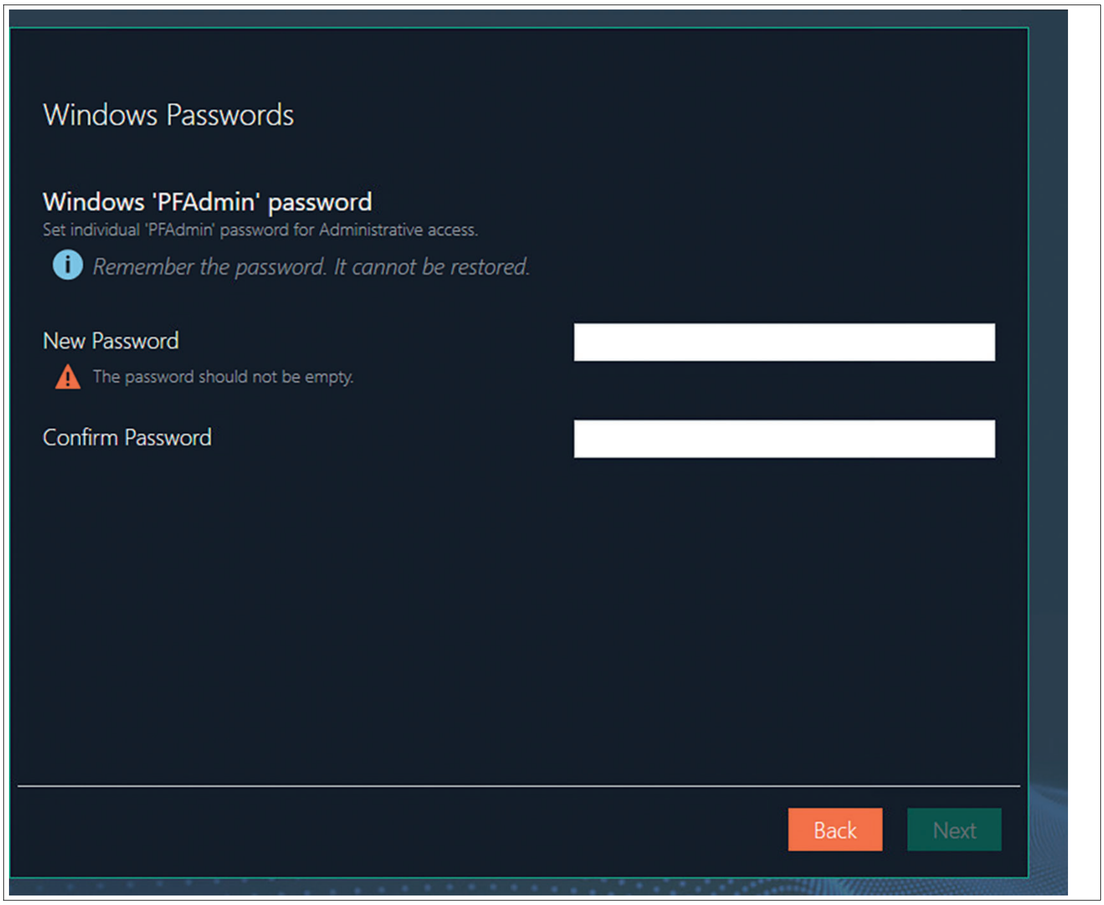
Please select the Touchscreen Type which should be used in the RM Shell Settings: eGalaxTouch

Figure 3.12

Password Settings

There are three different passwords to set.

1. PFAdmin: Default passwords are listed here: see chapter 3.5. The PFAdmin has access to the Windows and RM Shell settings.



Windows Passwords

Windows 'PFAdmin' password

Set individual 'PFAdmin' password for Administrative access.

Remember the password. It cannot be restored.

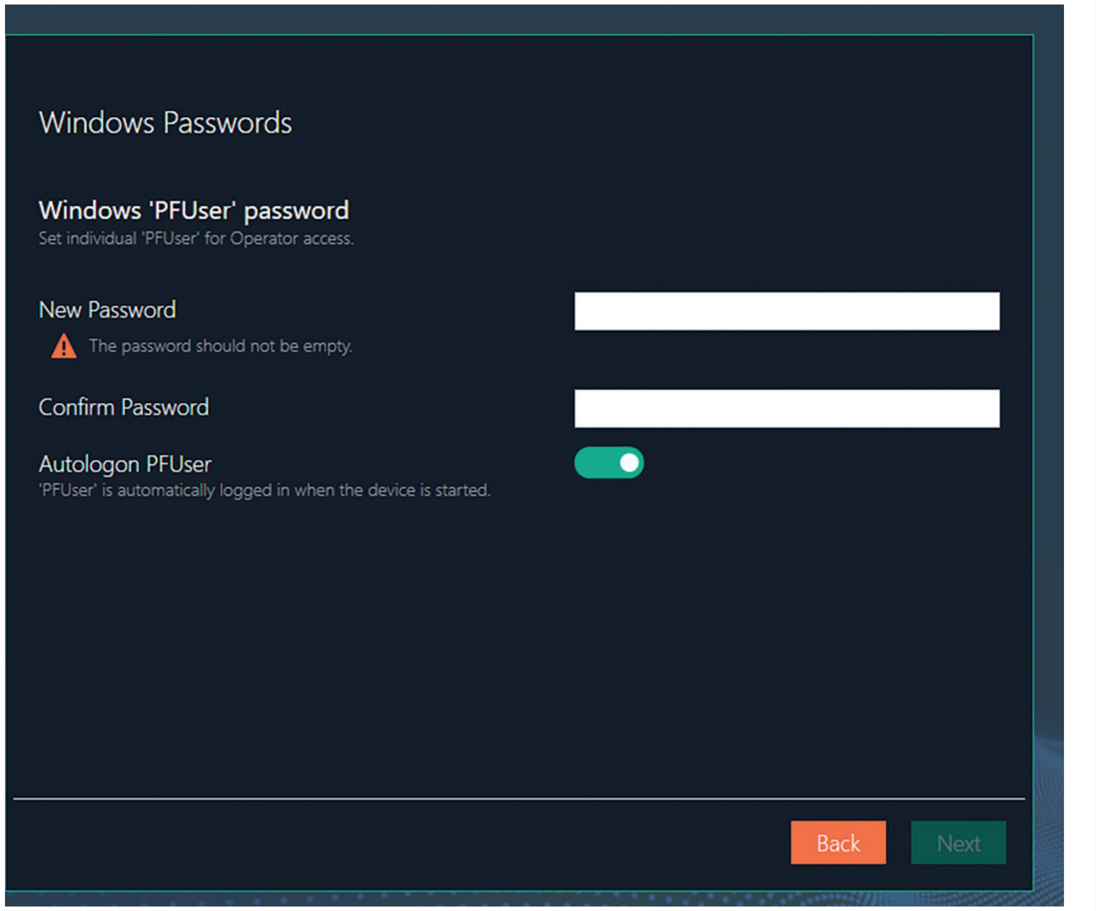
New Password

The password should not be empty.

Confirm Password

Figure 3.13

2. PFUser: Default passwords are listed here: see chapter 3.5. The PFUser is equal to the operator. The PFUser can only access the functionalities configured by the PFAdmin.



Windows Passwords

Windows 'PFUser' password

Set individual 'PFUser' for Operator access.

New Password

The password should not be empty.

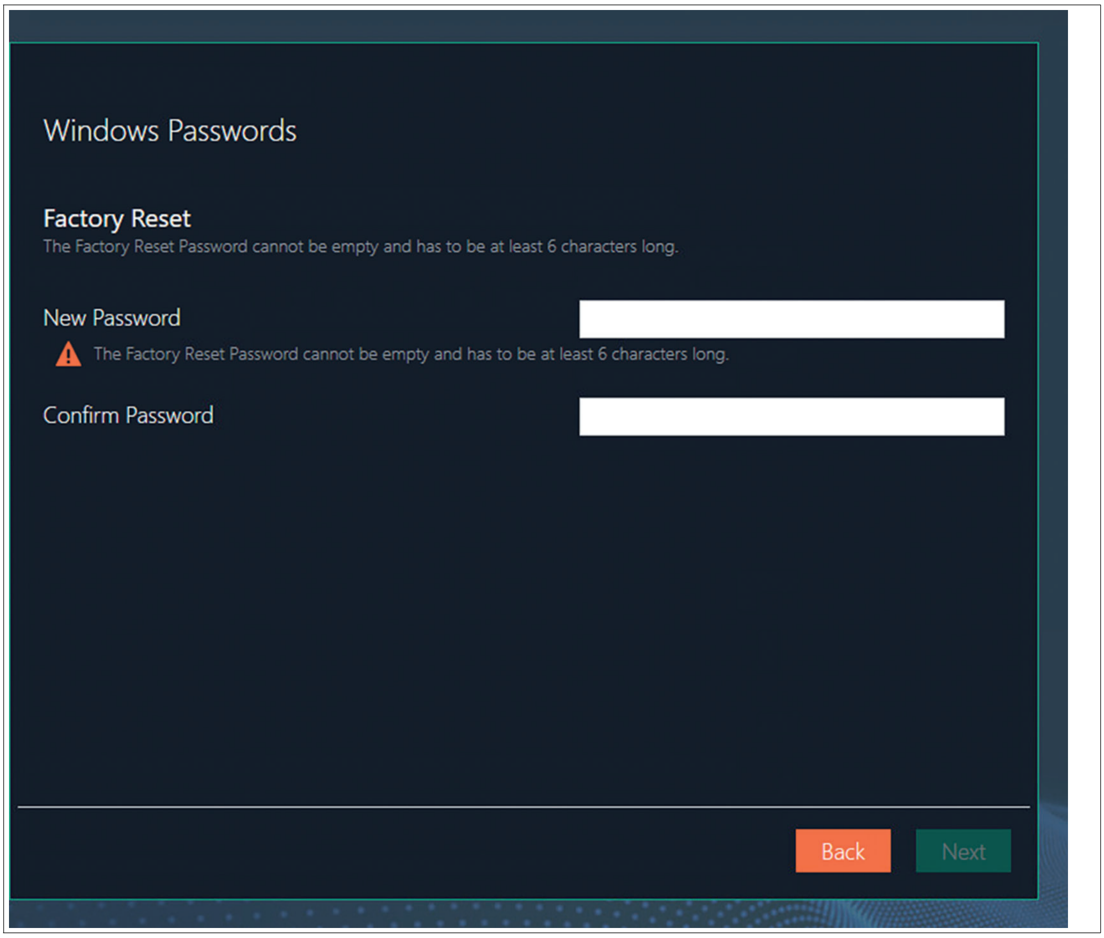
Confirm Password

Autologon PFUser

'PFUser' is automatically logged in when the device is started.

Figure 3.14

3. 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.



Windows Passwords

Factory Reset

The Factory Reset Password cannot be empty and has to be at least 6 characters long.

New Password

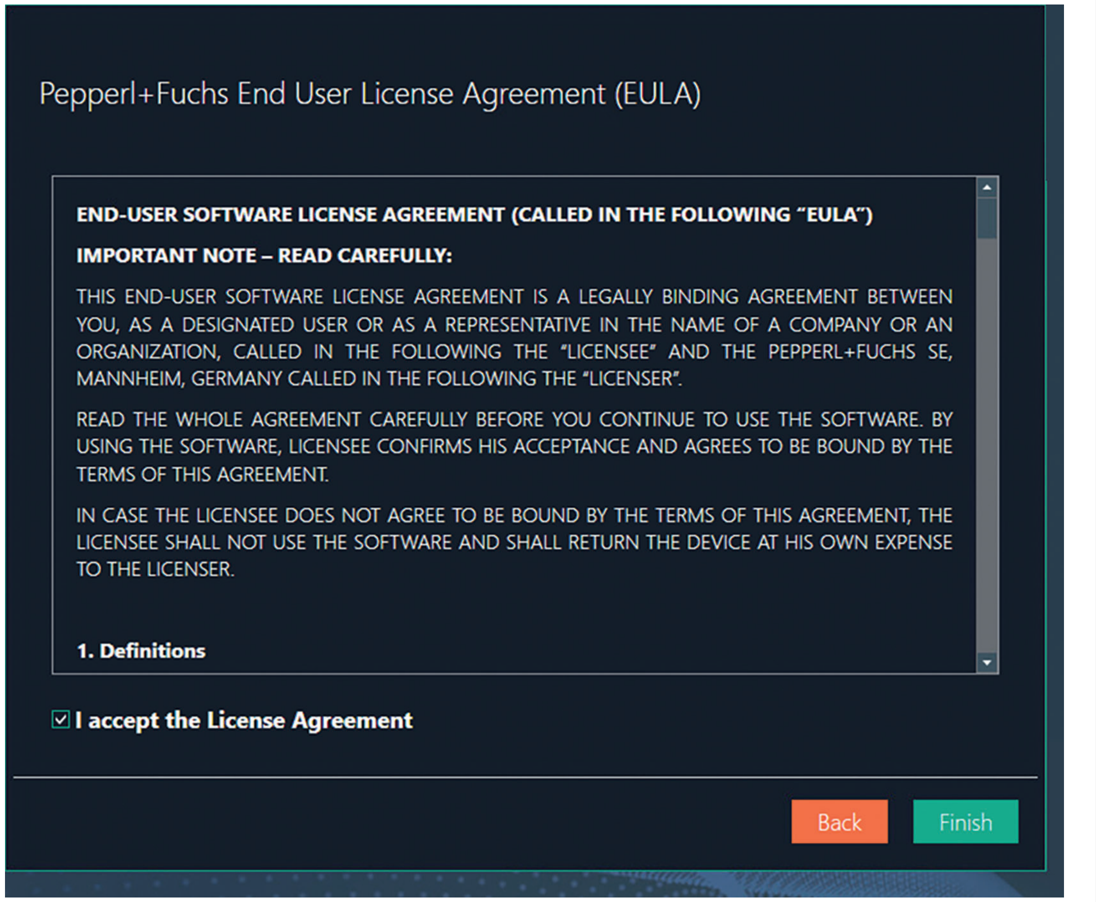
⚠ The Factory Reset Password cannot be empty and has to be at least 6 characters long.

Confirm Password

Figure 3.15

License Agreement

Accept the license agreement to proceed.



Pepperl+Fuchs End User License Agreement (EULA)

END-USER SOFTWARE LICENSE AGREEMENT (CALLED IN THE FOLLOWING "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.

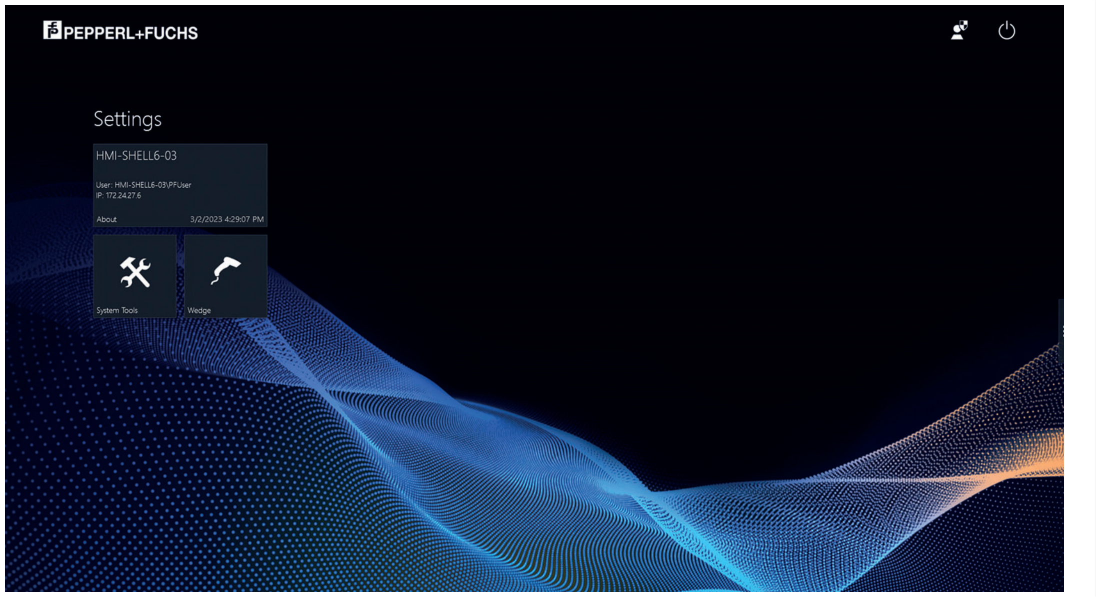
IN CASE THE LICENSEE DOES NOT AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT, THE LICENSEE SHALL NOT USE THE SOFTWARE AND SHALL RETURN THE DEVICE AT HIS OWN EXPENSE TO THE LICENSER.

1. Definitions

☑ **I accept the License Agreement**

Figure 3.16

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.



User: HMI-SHELL6-03\PFUser
IP: 172.24.27.6

Figure 3.17

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 2 user roles that are structured hierarchically. Each user role has different rights.

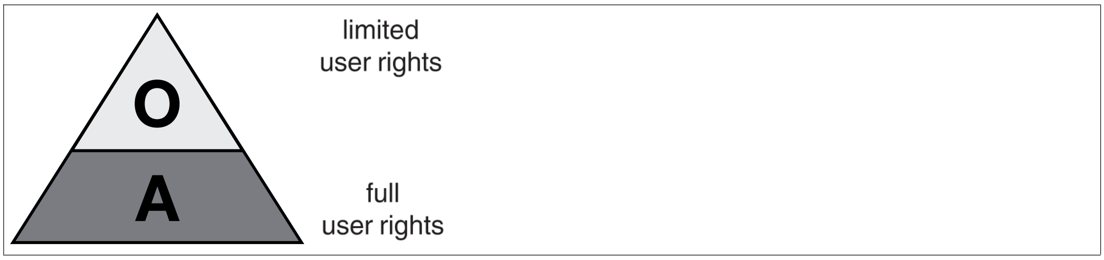


Figure 3.18 Concept of user rights: **O**(perator) and **A**(dministrator)

User Role	Description
Operator (O)	Operators are standard users. They can only execute predefined profiles. Operators have no access to RM settings. The preinstalled Operator is "PFUser".
Administrator (A)	Administrators have rights to change settings within the RM Shell as well as the Windows system settings. In addition, administrators can access Windows environment to install third-party applications and drivers and adjust advanced settings in addtion to VisuNet RM Shell. The preinstalled Administrator is "PFAdmin"

Warning!

Password Protection!

“PFUser”, “PFAdmin” and the Factory Reset have a predefined password (see default passwords). The passwords must be changed for commissioning.

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

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

Note

How to add more administrators, please see chapter 11.2.

User Rights Management

In the operator view, users can only access specific functionalities defined by the Administrators. The preinstalled User is the PFUser. The PFUser only has access to the operator view.

On the other hand, an Administrator can access the configuration view by logging in as PFAdmin. The PFAdmin is the preinstalled Administrator. All users who belong to the Windows Administrators Group are considered "Administrators". In the configuration view, the Administrator can make changes within the RM Shell. This includes adjusting profile settings, app settings, and system settings.

To get to the Windows desktop, you have to login at the Windows login with an administrative account. From the Windows desktop, an Administrator can make changes to system settings. To return to the RM Shell, Administrators need to log out and login in as Users (e.g. PFUser).

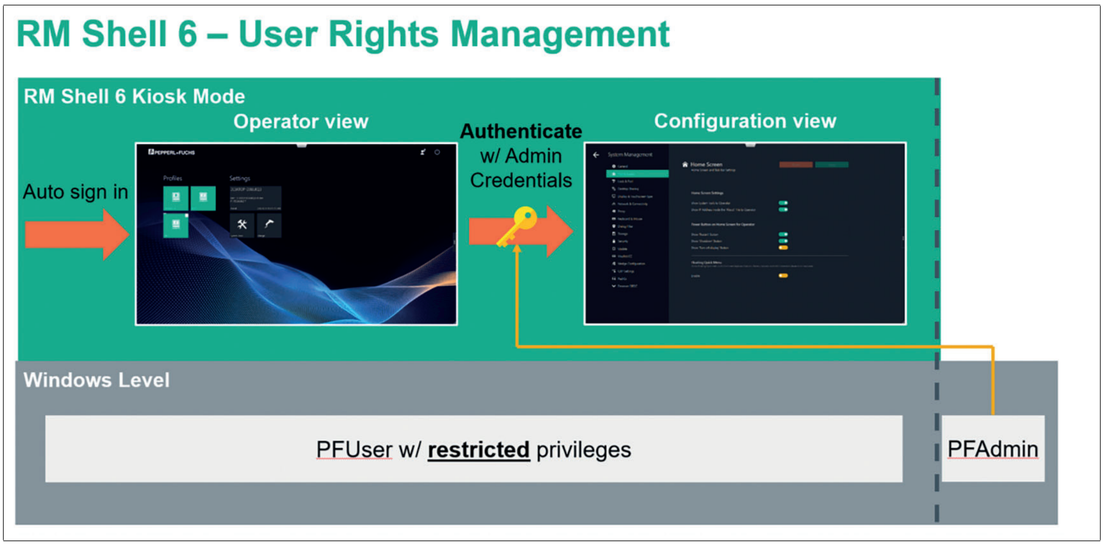


Figure 3.19 The architecture of the RM Shell 6 - Hybrid User Management

In summary, there are two default users on Windows level:

- **PFUser:** Windows user account with restricted rights. Used for operators
- **PFAdmin:** Windows user with elevated priviledges.

4 VisuNet RM Shell 6 User Interface

Home Screen Features (Configuration View, after individual profiles have been created)

The home screen is divided into the following areas:

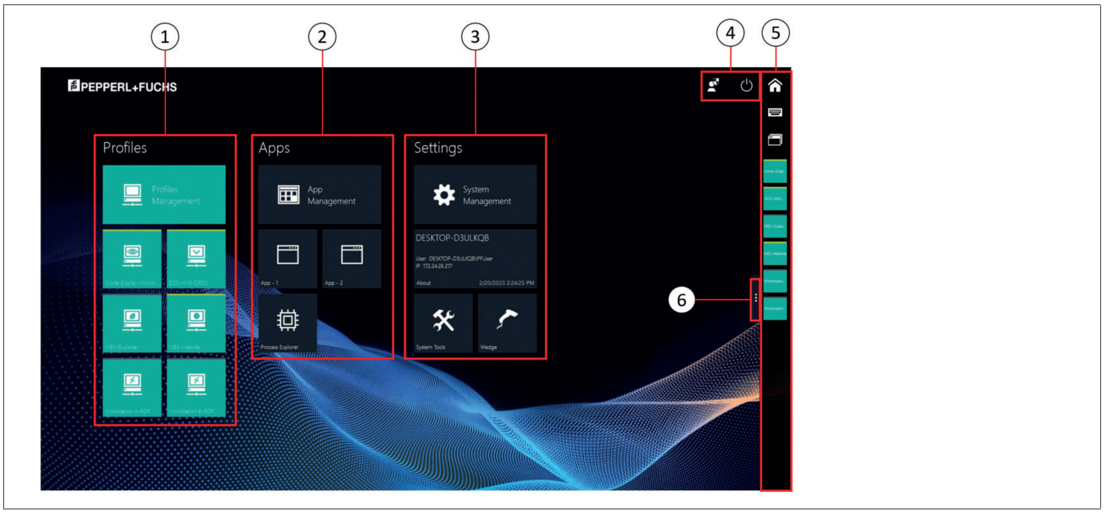


Figure 4.1 VisuNet RM Shell 6 Home Screen

No.	Description
1	Profiles
2	Applications
3	Settings
4	System functions
5	Smart Task Bar
6	Tab for opening and closing the Smart Task Bar

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.
👤	**Enter the Configuration View** The administrator is allowed to enter the Configuration View to make changes within the settings of the RM Shell.
⌨	**On-Screen-Keyboard (OSK)** 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 • Switch Windows User: Switch between the admin and operator user role (PFAdmin and PFUser) The power options can be set by the Administrator user role. The Operator user role is only allowed to run the preconfigured options.
🏠	**Home Screen Icon** Accessable via the Smart Task Bar. Leads back to the Home Screen

Configuration View

This area of the home screen indicates whether the Configuration View is enabled. After successfully logging into the Configuration View, the icon appears red. The timer below indicates the idle time after which the Configuration View is exited automatically. The idle time can be adjusted in System Management.

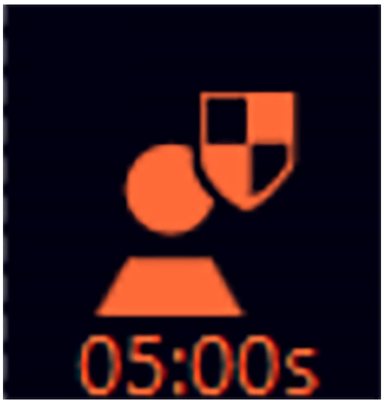


Figure 4.2

User-Role Information

Within the Shell, the operator is always logged in. However, an administrator can unlock the Configuration View. Whether you are in the Configuration View or the Operator View, is indicated by the red icon in the upper right corner. Another inidcator that the Configuration View is active, is the display of the Management Apps (see below). The Profiles Management, App Management and System Management tiles are only visible in the Administrator view.

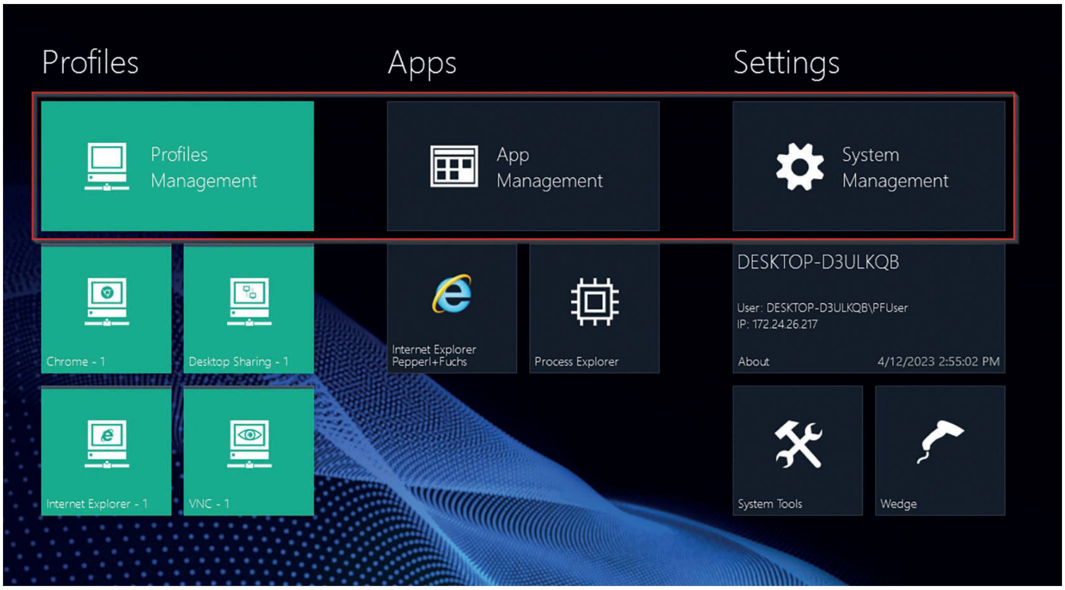
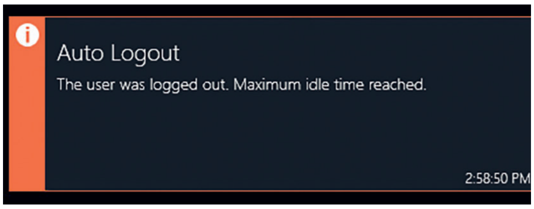


Figure 4.3

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.



Auto Logout

The user was logged out. Maximum idle time reached.

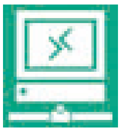
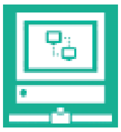
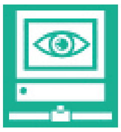
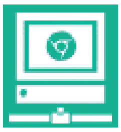
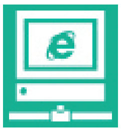
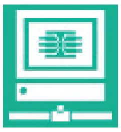
2:58:50 PM

Figure 4.4

Profiles

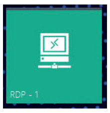
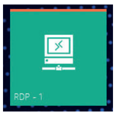
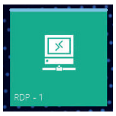
This section shows all profiles that have been created locally. Every profile is represented by a tile that displays the profile type (e.g., "RDP," "VNC"), profile name (e.g., "RDP - 2"), and connection status (e.g., "connected," "disconnected").

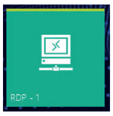
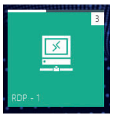
The following symbols indicate the different profile types:

RDP	
Desktop Sharing[1]	
VNC	
Web Browser URL (Chrome)[1]	
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	
Connection failed	An error occurred while trying to establish a connection (orange line).	
Connecting	Profile is connecting to host (blue line).	

Status	Description	
Connected	Profile is connected to a host PC. A green status bar at the top of the profile tile is visible (green line).	
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	

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.

Note

User Access to UWF

Only users logged in as "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.

Note

Enabling and Disabling the UWF

The UWF can only be enabled and disabled in the administrator view. Log in as an PFAdmin before performing following steps.

Enabling and Disabling the UWF

1. Click the "Power" icon at the top-left corner of the VisuNet RM Shell home screen.

2. Click on "Protect Disk and Restart" or to enable UWF or "Unprotect Disk and Restart" to disable UWF.

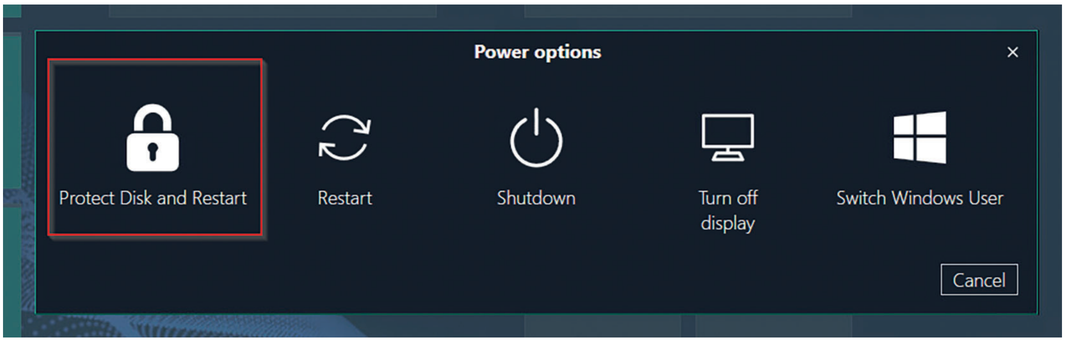


Figure 4.5

3. 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. The status of the UWF can be checked on the About Tile.

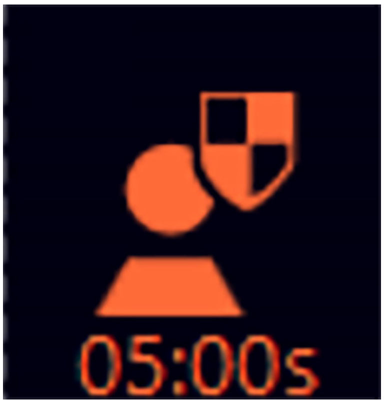
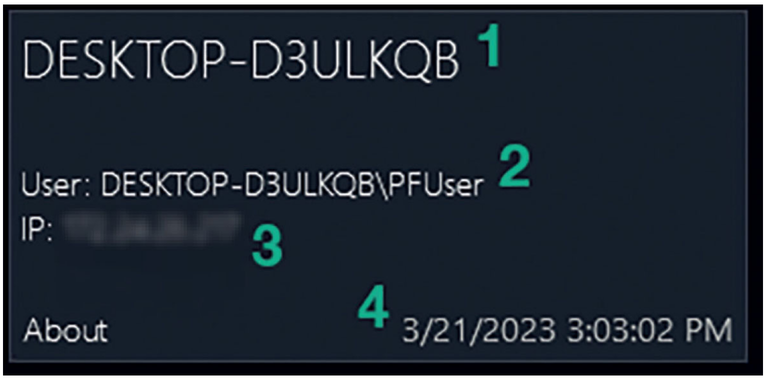


Figure 4.6

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.



DESKTOP-D3ULKQB

User: DESKTOP-D3ULKQB\PFUser

IP: [redacted]

About

3/21/2023 3:03:02 PM

Figure 5.1

No.	Description
1	Computer name of the RM / BTC (see chapter 8.1)
2	Displays currents user name
3	IP address of the RM / BTC (see chapter 8.6)
4	Current date and time (see chapter 8.1)

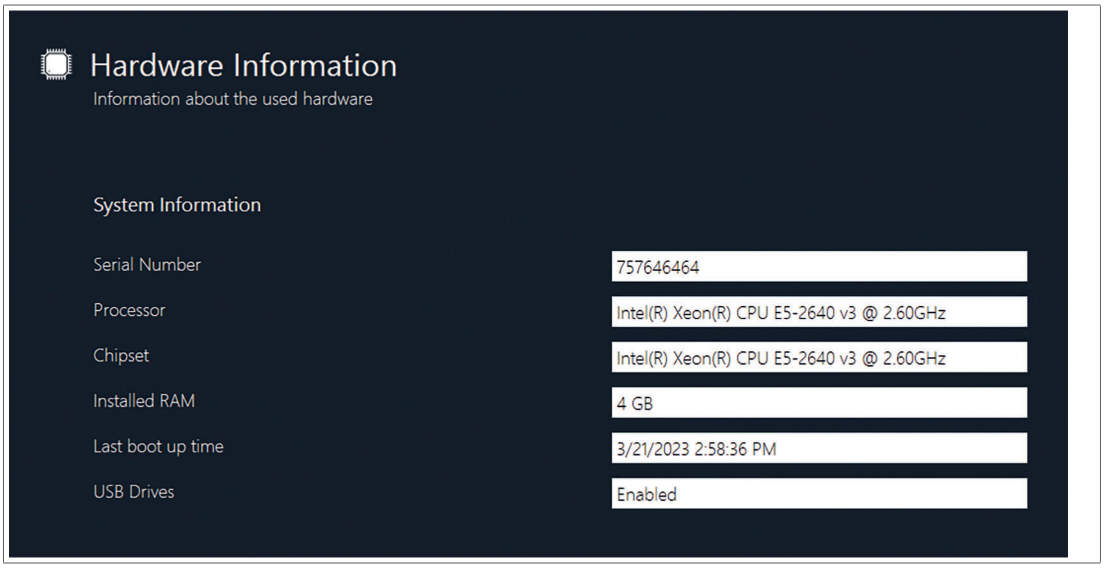
For additional information, click the "About" tile.

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
- When using a DRDC license, DRDC information is listed
- (Submenu for GXP-specific information)
- Hardware, see chapter 5.1
- Licenses, see chapter 5.2
- Software, see chapter 5.3
- 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.



Hardware Information
Information about the used hardware

System Information

Serial Number	757646464
Processor	Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
Chipset	Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
Installed RAM	4 GB
Last boot up time	3/21/2023 2:58:36 PM
USB Drives	Enabled

Figure 5.2

5.2 Licenses and Terms of Use

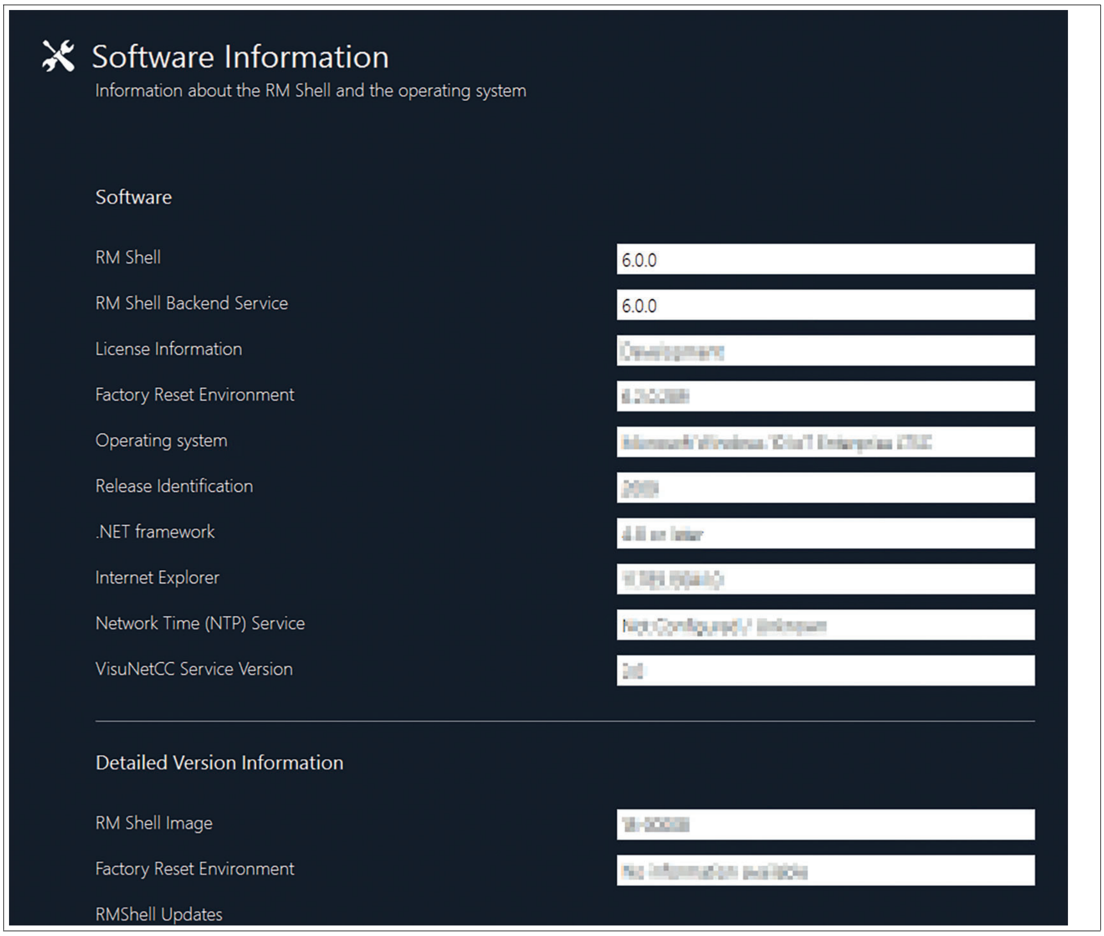
This submenu provides license information for the RM Shell and third-party components.

For more information on the Pepperl+Fuchs End User License Agreement see chapter 12.1.

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.



Software Information

Information about the RM Shell and the operating system

Software

RM Shell	6.0.0
RM Shell Backend Service	6.0.0
License Information	[redacted]
Factory Reset Environment	[redacted]
Operating system	[redacted]
Release Identification	[redacted]
.NET framework	[redacted]
Internet Explorer	[redacted]
Network Time (NTP) Service	[redacted]
VisuNetCC Service Version	[redacted]

Detailed Version Information

RM Shell Image	[redacted]
Factory Reset Environment	[redacted]
RMShell Updates	

Figure 5.3

6 Profiles Management App

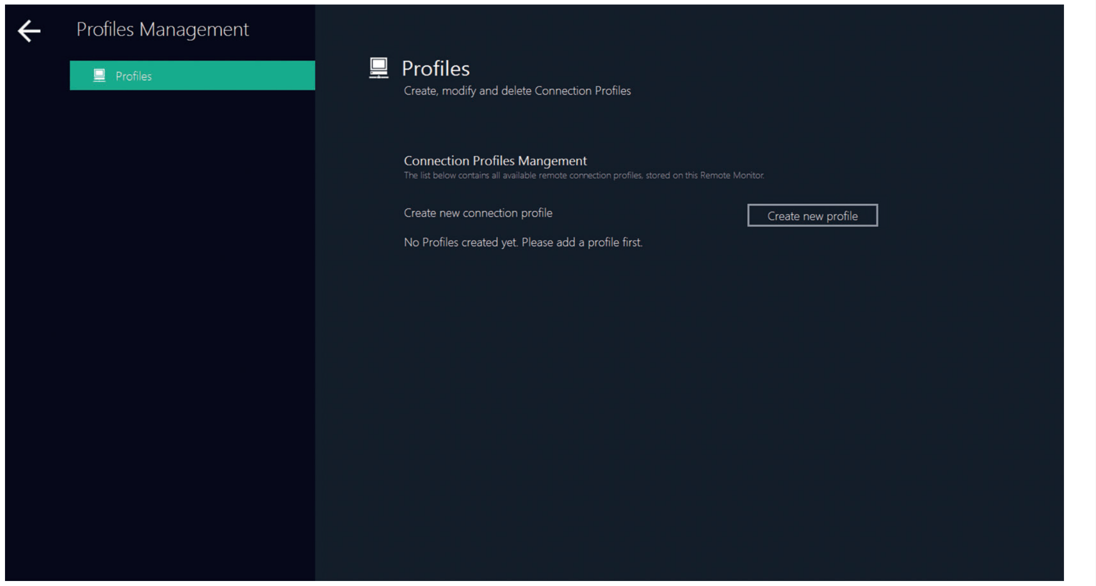
Create and manage remote "Connection Profiles" with the "Profiles Management" app.

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.



Profiles

Create, modify and delete Connection Profiles

Connection Profiles Mangement

The list below contains all available remote connection profiles, stored on this Remote Monitor.

Create new connection profile

No Profiles created yet. Please add a profile first.

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

Opening the Profiles Management App

1. To access the Profiles Management App switch to the configuration mode.
2. To switch to configuration mode authenticate as an administrator with your administrator password (see chapter 4--> Switch to configuration mode).
3. Now the Profiles Management App is displayed.

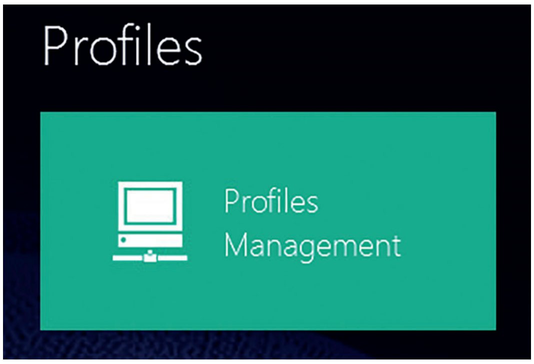
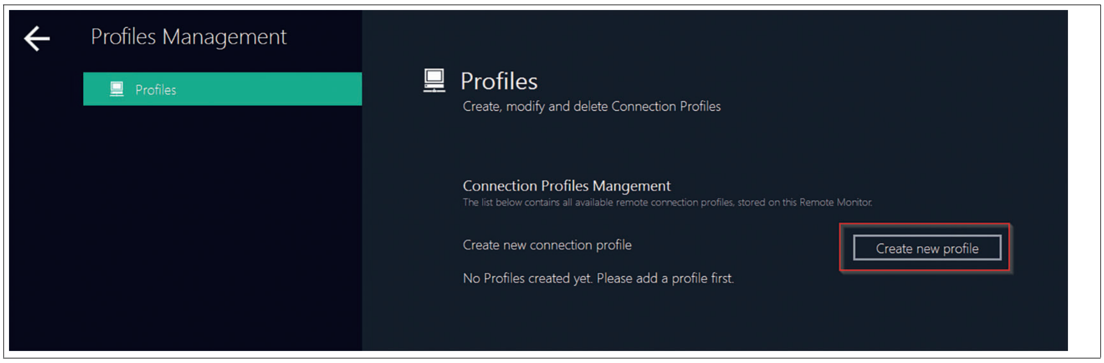


Figure 6.2

Creating a New Connection Profile

1. To create a new connection profile, click **Create new profile**.



Profiles Management

Profiles

Profiles

Create, modify and delete Connection Profiles

Connection Profiles Mangement

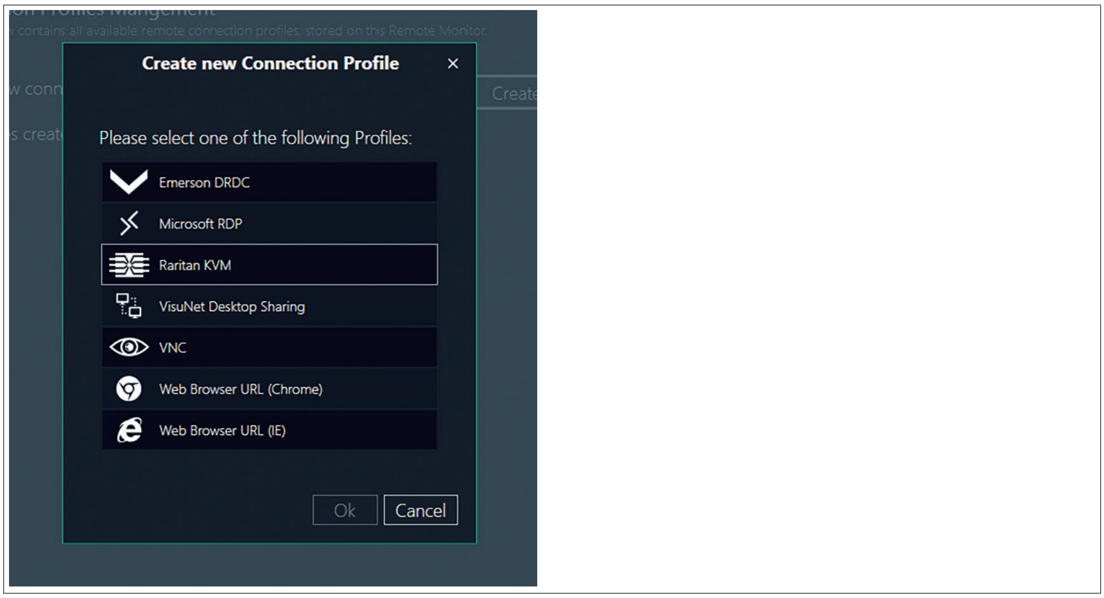
The list below contains all available remote connection profiles, stored on this Remote Monitor.

Create new connection profile — Create new profile

No Profiles created yet. Please add a profile first.

Figure 6.3

2. Select your required connection "Profile" type and click **Ok.**[1]


contains all available remote connection profiles, stored on this Remote Monitor
w conn
s creat
Create

Create new Connection Profile ×

Please select one of the following Profiles:

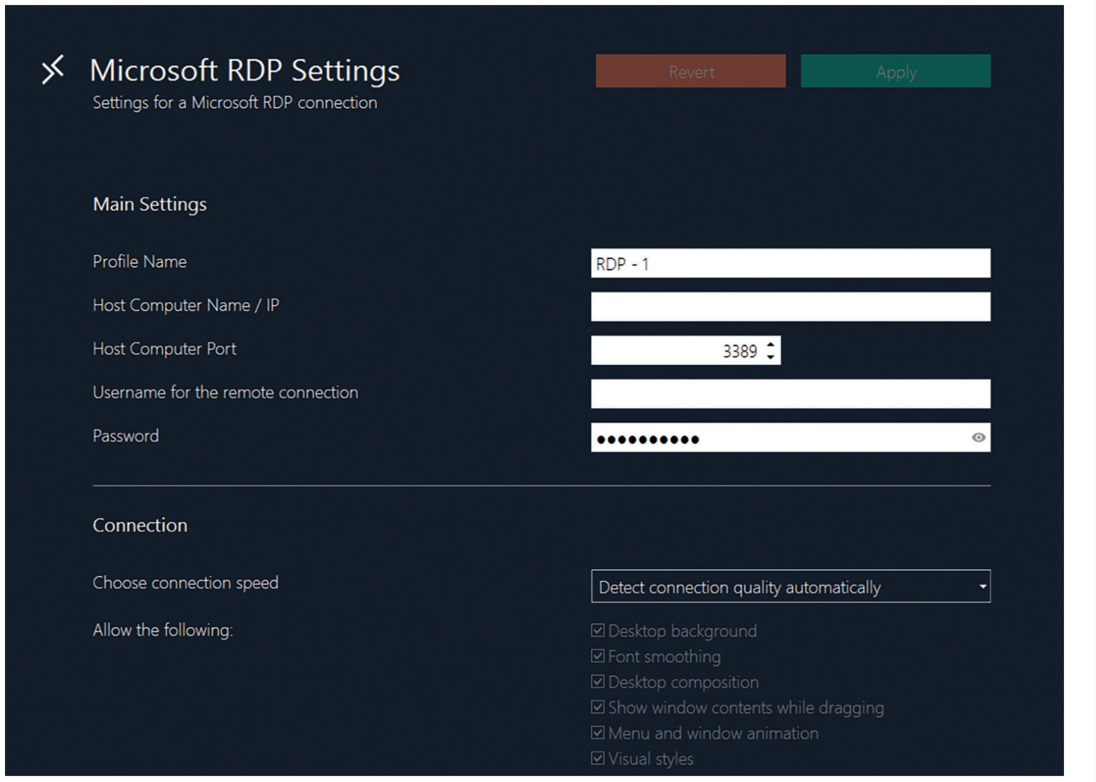
- Emerson DRDC
- Microsoft RDP
- Raritan KVM
- VisuNet Desktop Sharing
- VNC
- Web Browser URL (Chrome)
- Web Browser URL (IE)

Ok Cancel

Figure 6.4

↳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.



Microsoft RDP Settings
Settings for a Microsoft RDP connection

Main Settings

Profile Name: RDP - 1
Host Computer Name / IP:
Host Computer Port: 3389
Username for the remote connection:
Password: ●●●●●●●●●●

Connection

Choose connection speed: Detect connection quality automatically

Allow the following:
☑ Desktop background
☑ Font smoothing
☑ Desktop composition
☑ Show window contents while dragging
☑ Menu and window animation
☑ Visual styles

Editing the Profile Settings

1. Go to **Profiles**.
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.

↳ The changes have been saved.

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 three additional features.

- Auto Connect
- Retry
- Backup Connection

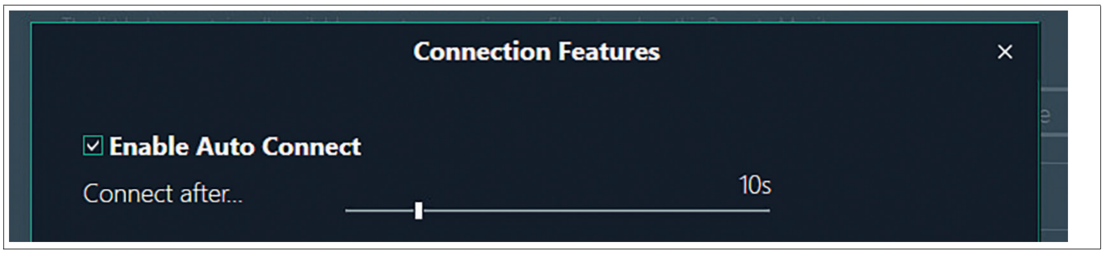
"Auto Connect" Feature

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 **Profiles**.
2. To set up the auto connect for a profile, click ✎ ⏱ 🗑.

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



Connection Features ✕

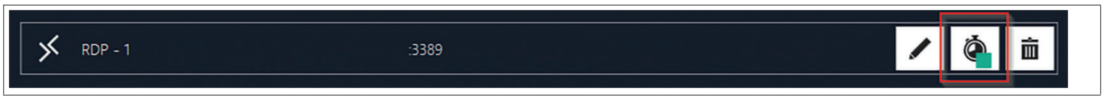
☑ Enable Auto Connect

Connect after... 10s

Figure 6.5 **Auto Connect option:** In this example, VisuNet RM Shell automatically establishes a connection to the RDP profile after 10 seconds

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 enabled auto connect is now activated. The green square shows that connection features are enabled within this connection.



RDP - 1 :3389

Figure 6.6 Profile with preconfigured auto connect (as indicated in the profiles list by the green square).

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.

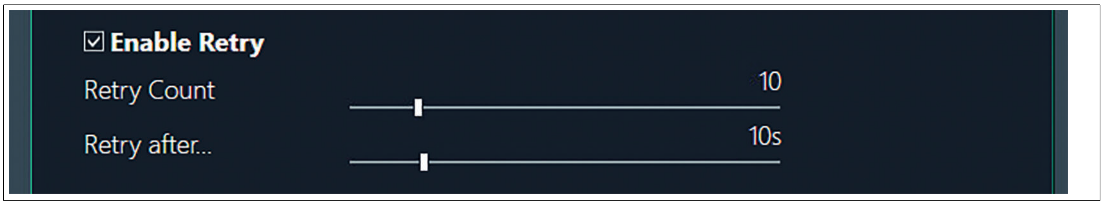
"Retry" Feature

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.



☑ Enable Retry

Retry Count 10

Retry after... 10s

Figure 6.7

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 enabled retry feature is now activated. The green square shows that connection features are enabled within this connection.

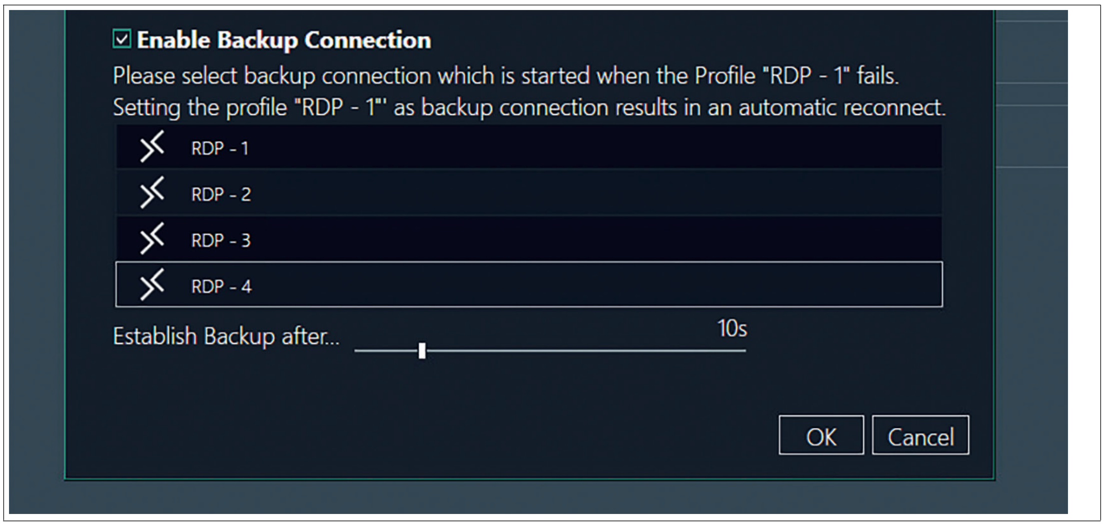
"Backup Connection" Feature

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.



☑ Enable Backup Connection

Please select backup connection which is started when the Profile "RDP - 1" fails.
Setting the profile "RDP - 1"' as backup connection results in an automatic reconnect.

Figure 6.8

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 enabled backup connection is now activated. The green square shows that connection features are enabled within this connection.

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.

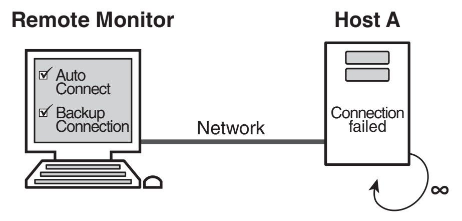
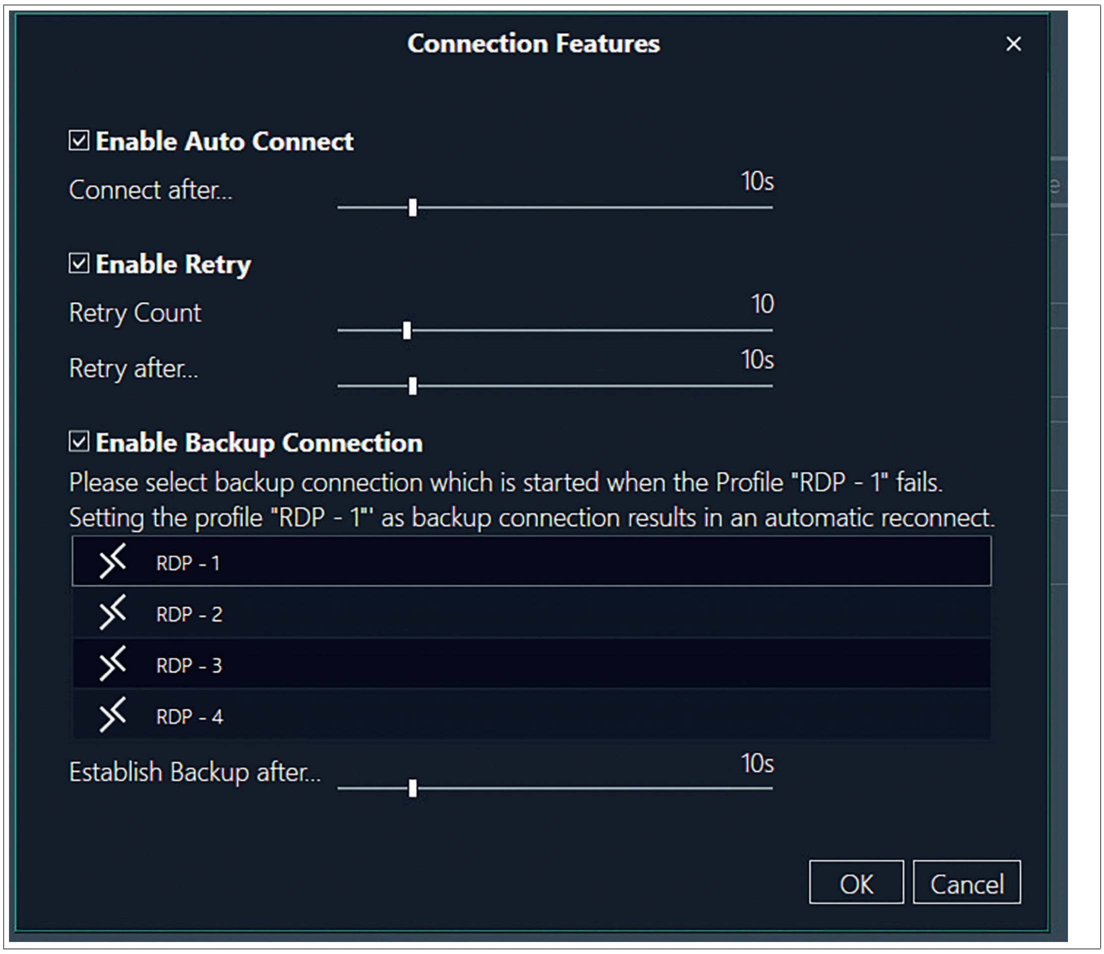


Figure 6.9 Example 1 - Unlimited number of retries to a specific host (with "Backup Connection" feature)

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.



Connection Features ×

☑ Enable Auto Connect

Connect after... 10s

☑ Enable Retry

Retry Count 10

Retry after... 10s

☑ Enable Backup Connection

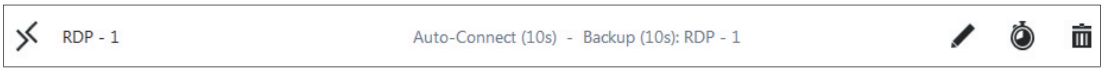
Please select backup connection which is started when the Profile "RDP - 1" fails.
Setting the profile "RDP - 1" as backup connection results in an automatic reconnect.

RDP - 1
RDP - 2
RDP - 3
RDP - 4

Establish Backup after... 10s

Figure 6.10

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."



RDP - 1 Auto-Connect (10s) - Backup (10s): RDP - 1

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.

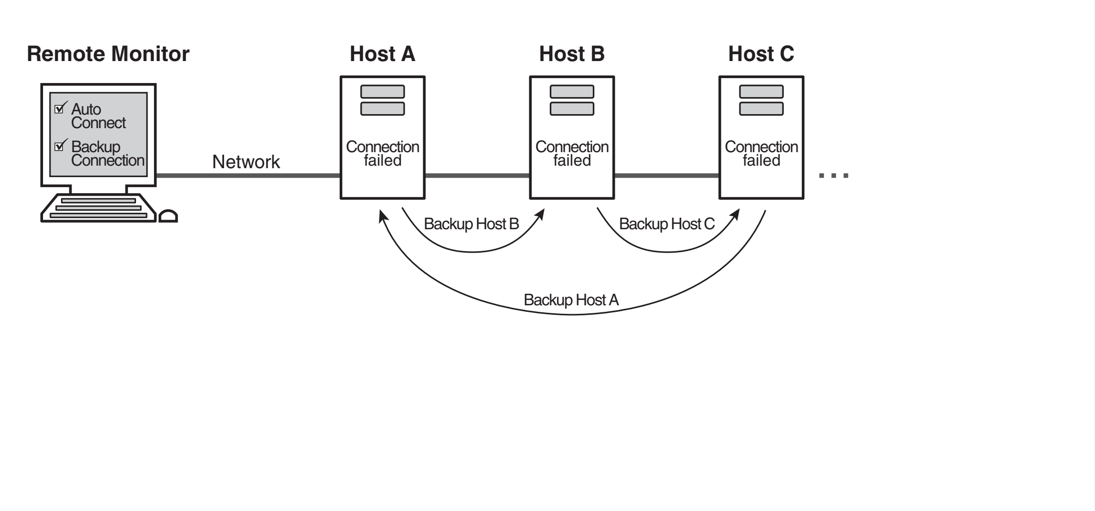
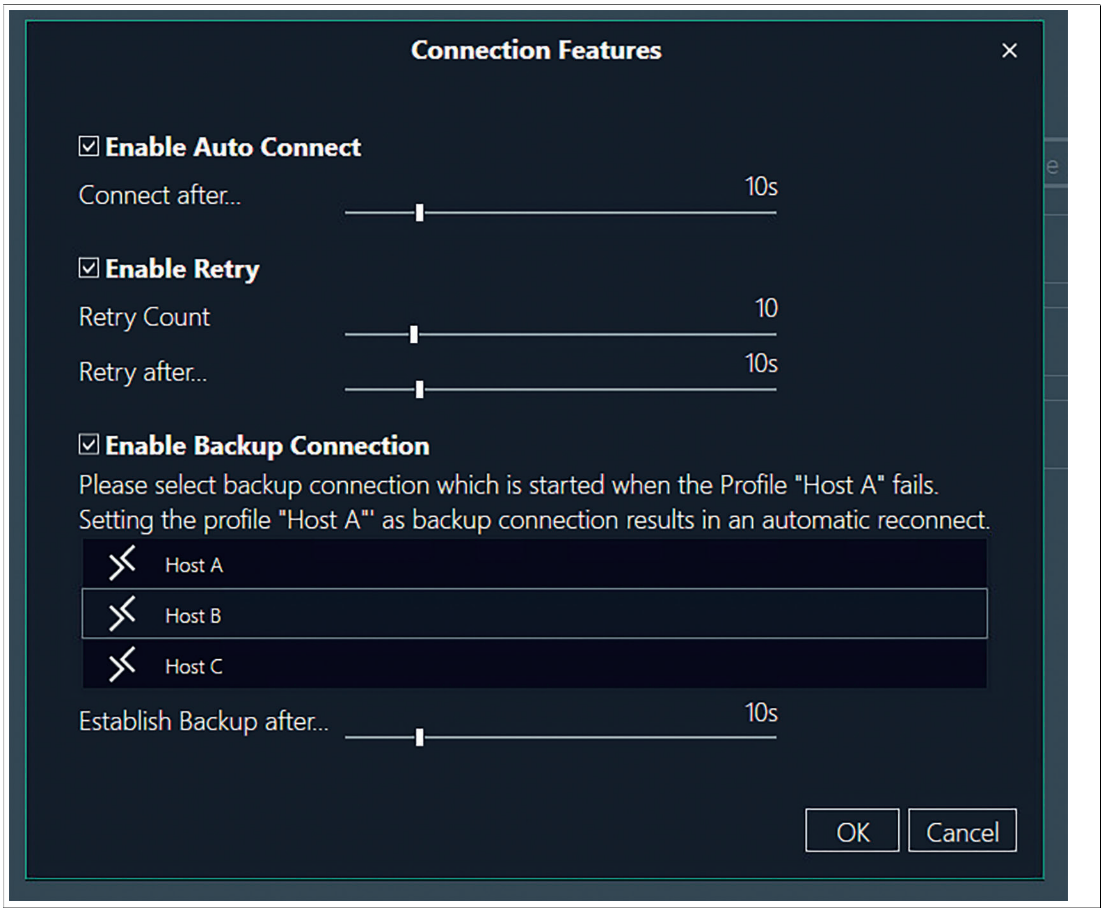


Figure 6.11 Example 2 - unlimited number of connection retries to more than one host (via "Backup Connection" feature)

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").



Connection Features ×

☑ **Enable Auto Connect**

Connect after... 10s

☑ **Enable Retry**

Retry Count 10

Retry after... 10s

☑ **Enable Backup Connection**

Please select backup connection which is started when the Profile "Host A" fails.
Setting the profile "Host A"' as backup connection results in an automatic reconnect.

Host A

Host B

Host C

Establish Backup after... 10s

Figure 6.12

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."

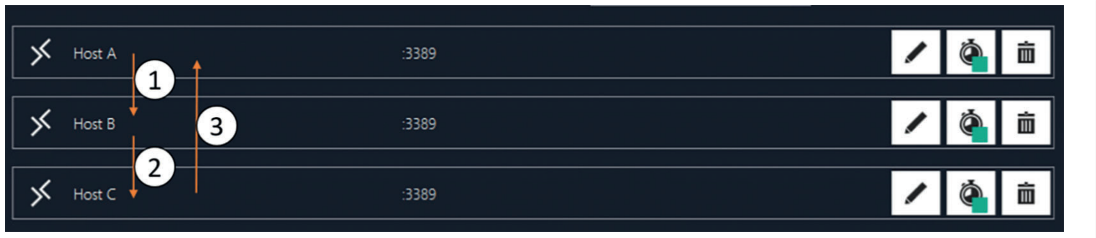


Figure 6.13 Profiles with backup connections

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.

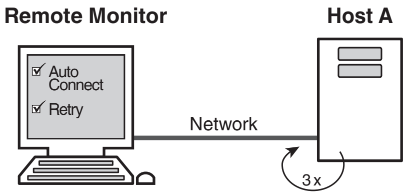
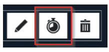
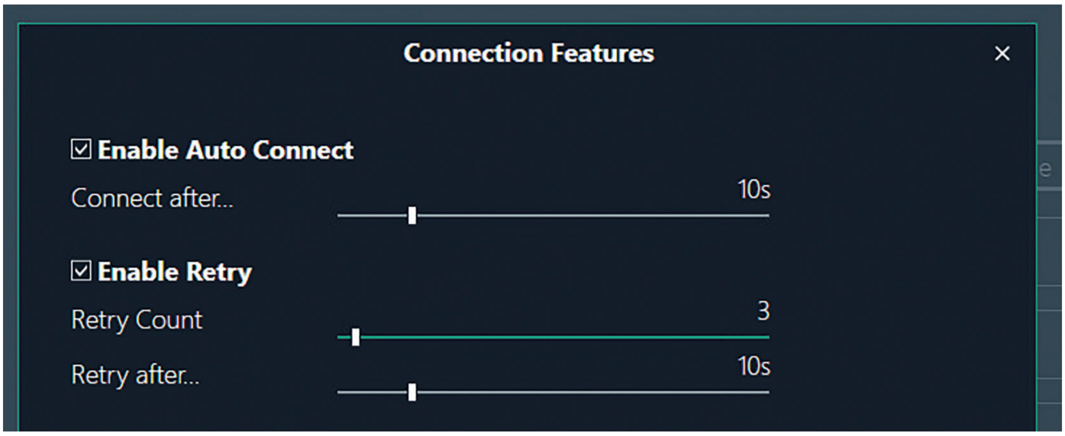


Figure 6.14 Example 3 - Limited number of connection retries to the same host

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.



Connection Features

☑ Enable Auto Connect

Connect after... 10s

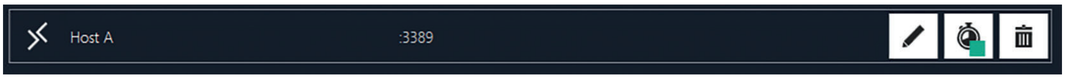
☑ Enable Retry

Retry Count 3

Retry after... 10s

Figure 6.15 Corresponding settings in the VisuNet RM Shell (profile settings - connection features)

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



Host A :3389

Figure 6.16

6.2 RDP Settings

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.
Allow the following	Enable the functions desired. Keep in mind that when choosing "Detect connection quality automatically" as connection speed option, all options are selected.
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
Server Authentification	• 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.
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)

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

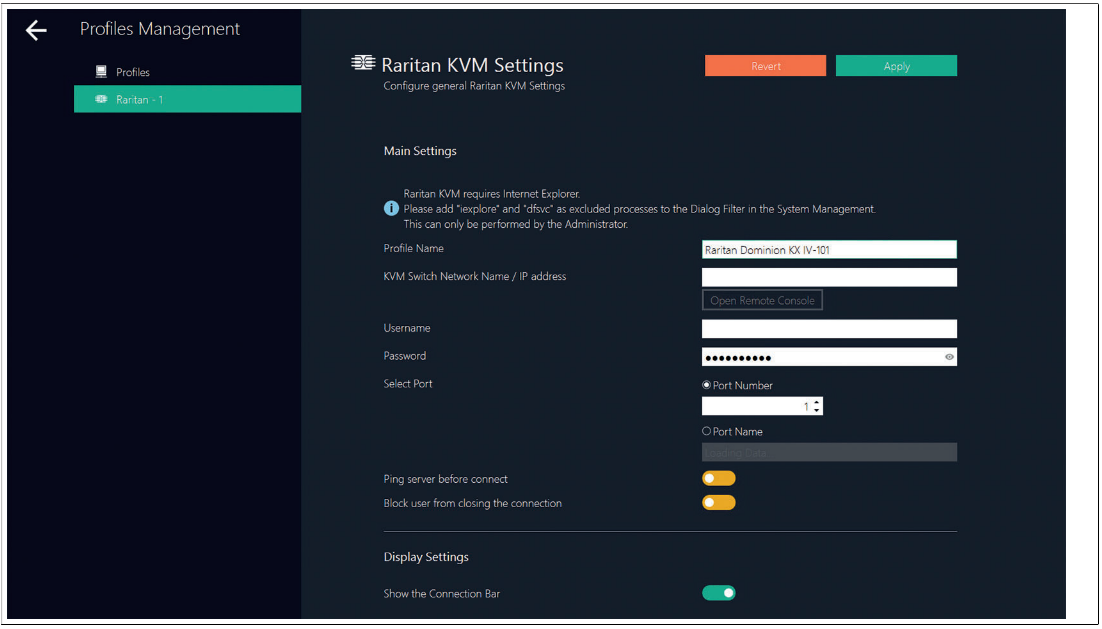
The KVM-over-IP client requires an VisuNet RM Shell PRO License to be unlocked.

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.



Raritan KVM Settings

Configure general Raritan KVM Settings

Main Settings

Raritan KVM requires Internet Explorer.
Please add "iexplore" and "dfsvc" as excluded processes to the Dialog Filter in the System Management.
This can only be performed by the Administrator.

Profile Name: Raritan Dominion KX IV-101

KVM Switch Network Name / IP address:

Username:

Password: ••••••••••

Select Port: ● Port Number 1 ○ Port Name Loading Data...

Ping server before connect

Block user from closing the connection

Display Settings

Show the Connection Bar

Figure 6.17

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.

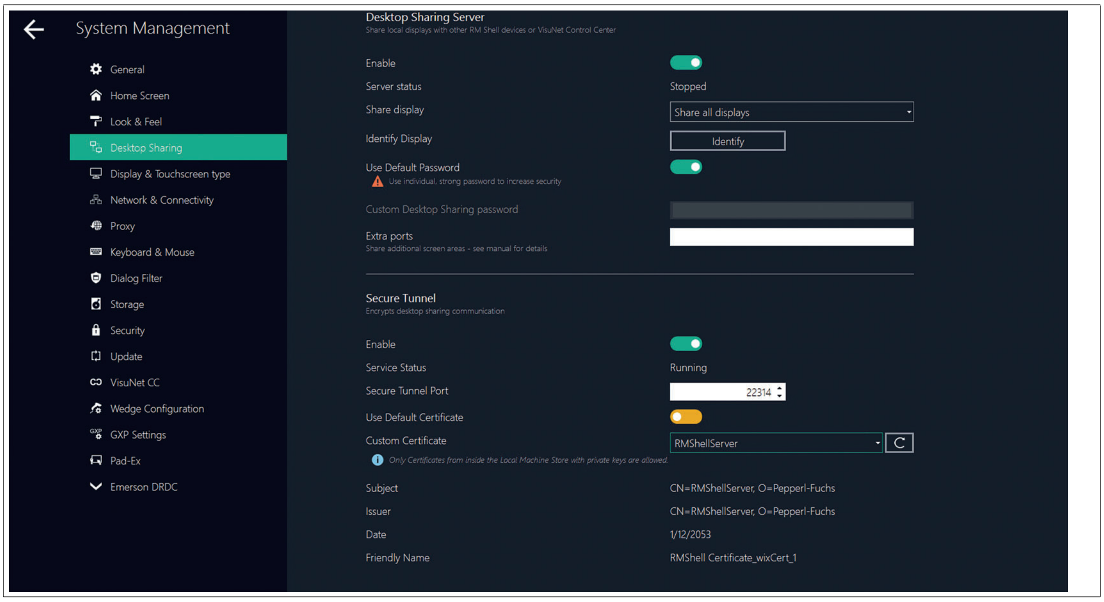
Display Settings

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

Desktop Sharing enables remote access to the local device. With this function you can share your screen with other devices and VisuNet Control Center.



Desktop Sharing Server
Share local displays with other RM Shell devices or VisuNet Control Center

Enable
Server status: Stopped
Share display: Share all displays
Identify Display
Use Default Password
Use individual, strong password to increase security
Custom Desktop Sharing password
Extra ports
Share additional screen areas - see manual for details

Secure Tunnel
Encrypts desktop sharing communication

Enable
Service Status: Running
Secure Tunnel Port: 22314
Use Default Certificate
Custom Certificate: RMShellServer
Only Certificates from inside the Local Machine Store with private keys are allowed.
Subject: CN=RMShellServer, O=Pepperl-Fuchs
Issuer: CN=RMShellServer, O=Pepperl-Fuchs
Date: 1/12/2053
Friendly Name: RMShell Certificate_wixCert_1

Figure 6.18

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.
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

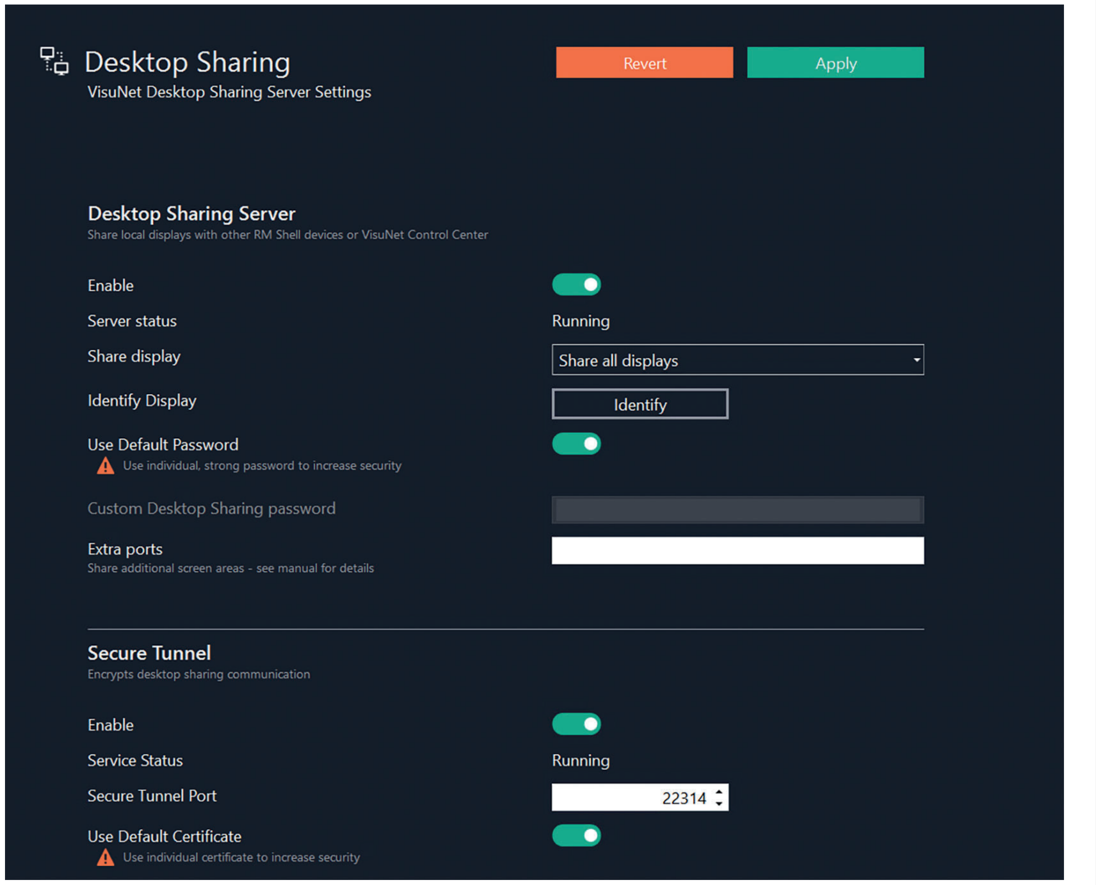
Display Settings

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 to a host, 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. The connection must be established on the client. Secure Tunnel must be enabled on both instances. The Secure Tunnel Service as well as the use of the default certificate will be enabled per default.



Desktop Sharing
VisuNet Desktop Sharing Server Settings

Desktop Sharing Server
Share local displays with other RM Shell devices or VisuNet Control Center

Enable
Server status: Running
Share display: Share all displays
Identify Display: Identify
Use Default Password
Use individual, strong password to increase security
Custom Desktop Sharing password
Extra ports
Share additional screen areas - see manual for details

Secure Tunnel
Encrypts desktop sharing communication

Enable
Service Status: Running
Secure Tunnel Port: 22314
Use Default Certificate
Use individual certificate to increase security

Figure 6.19

Note

Due tue security reasons, we recommend to use an own certificate and to set an own password.

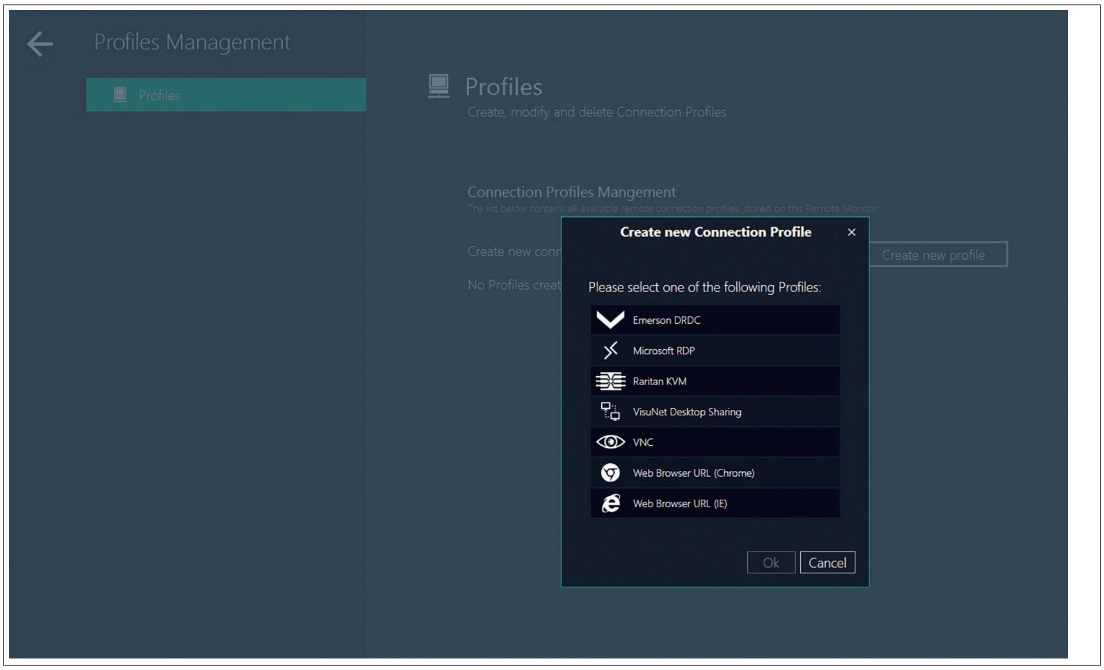
2. To save the changes, click "Apply Changes"

Note

For more information on how to handle Windows certificates, see the Windows website for the relevant documentation: https://learn.microsoft.com/en-us/windows/win32/seccrypto/creating-viewing-and-managing-certificates.

Configuration of Client

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



Profiles Management

Profiles

Profiles

Create, modify and delete Connection Profiles

Connection Profiles Mangement

The list below contains all available remote connection profiles, stored on this Remote Monitor.

Create new conn

No Profiles creat

Create new profile

Create new Connection Profile ×

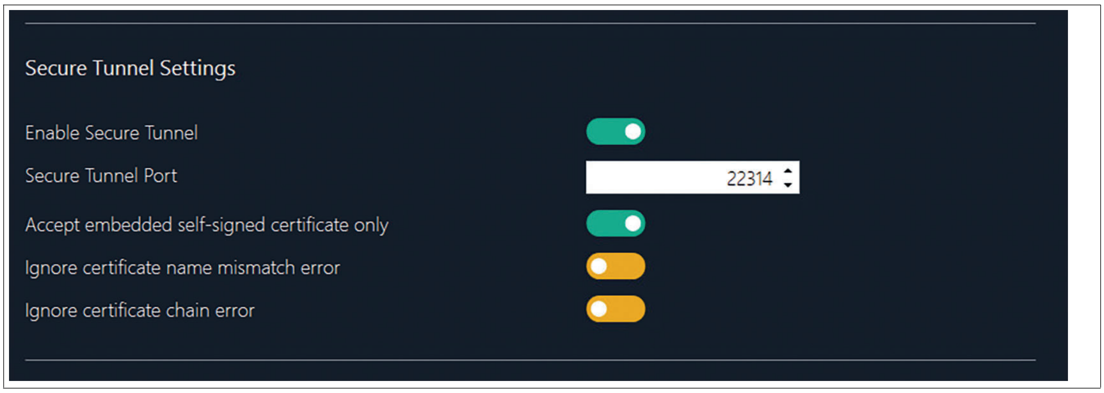
Please select one of the following Profiles:

- Emerson DRDC
- Microsoft RDP
- Raritan KVM
- VisuNet Desktop Sharing
- VNC
- Web Browser URL (Chrome)
- Web Browser URL (IE)

Ok Cancel

Figure 6.20

2. Enable Secure Tunnel.



Secure Tunnel Settings

Enable Secure Tunnel ●

Secure Tunnel Port 22314

Accept embedded self-signed certificate only ●

Ignore certificate name mismatch error ○

Ignore certificate chain error ○

Figure 6.21

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.
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
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.

i

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.

i

Note

When using a Box Thin Client (BTC) with multiple monitors, it is possible to select on which monitor the profile is to be opened or whether it is to be spanned across all monitors.

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 11.7.

Note

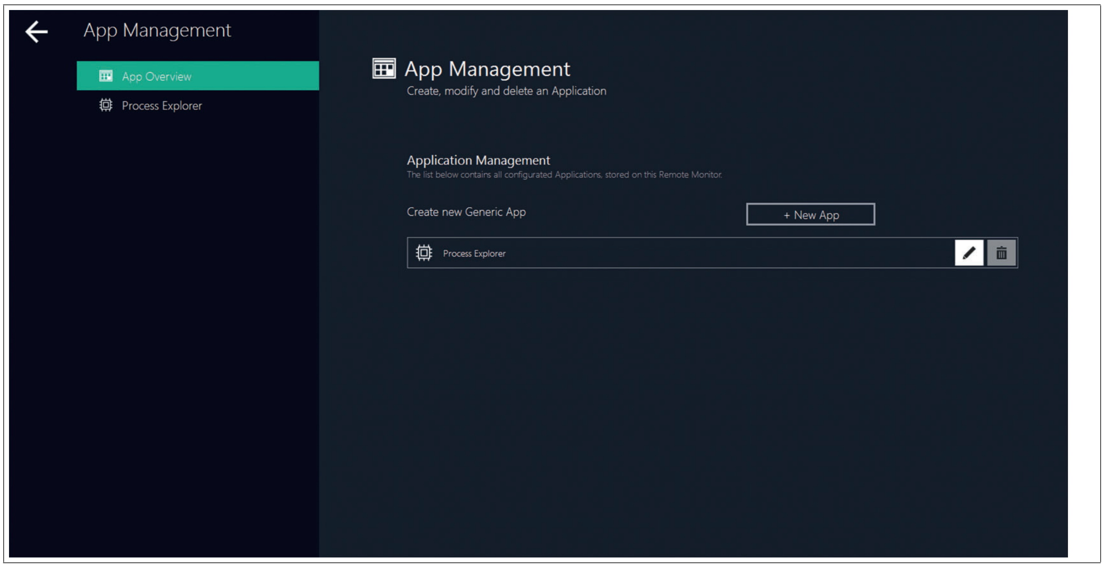
Whitelisting Applications

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 8.10.

Note

Maximum App Size

The maximum size of the installed App should need exceed 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.



Create, modify and delete an Application

Application Management

The list below contains all configurated Applications, stored on this Remote Monitor.

Create new Generic App

Figure 7.1 VisuNet RM Shell 6 App Management

Opening App Management

1. To open app management, unlock the Configuration View. After successfully authenticating as an administrator, the configuration view is displayed. Now click on App Management:

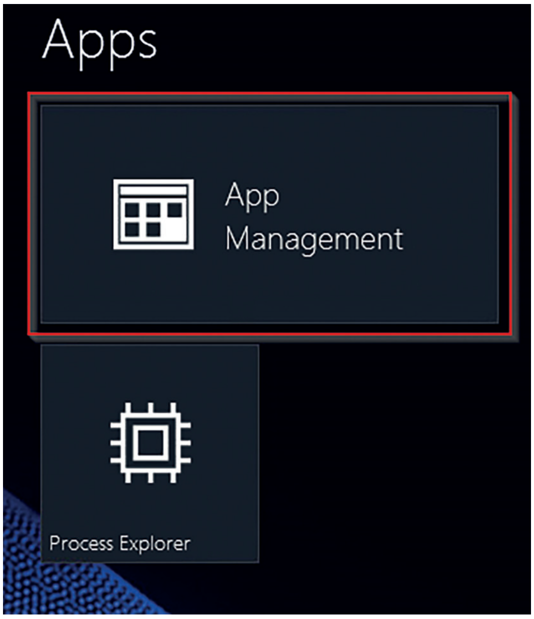
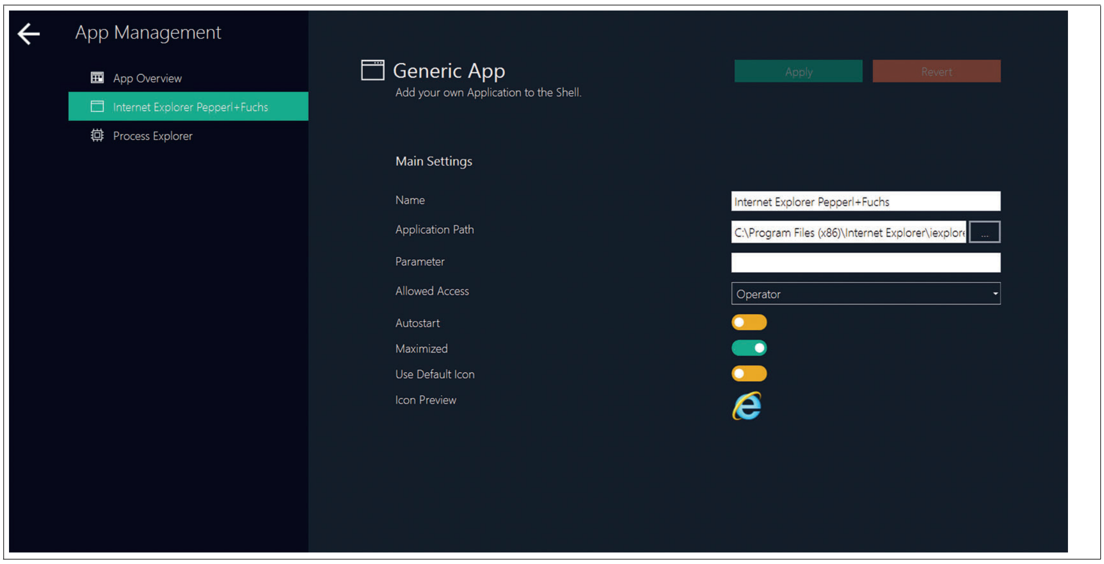


Figure 7.2

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.
   - **Icon Preview:** Shows what the icon would look like.



Generic App
Add your own Application to the Shell.

Main Settings

Name	Internet Explorer Pepperl+Fuchs
Application Path	C:\Program Files (x86)\Internet Explorer\iexplore
Parameter	
Allowed Access	Operator
Autostart	○
Maximized	●
Use Default Icon	○
Icon Preview	

Figure 7.3 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

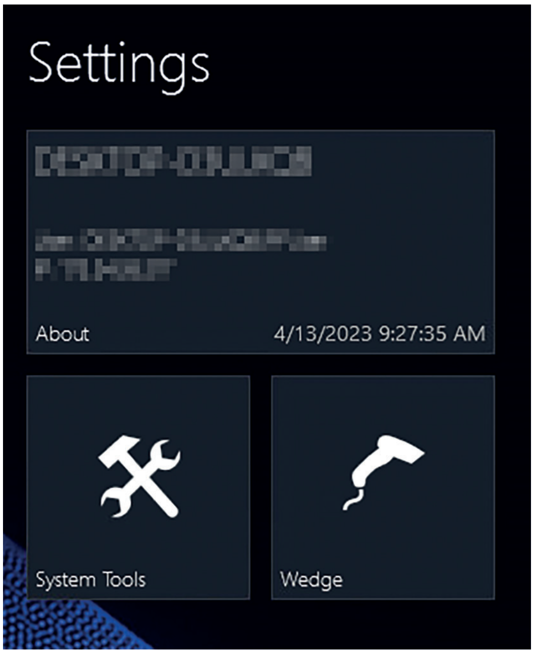
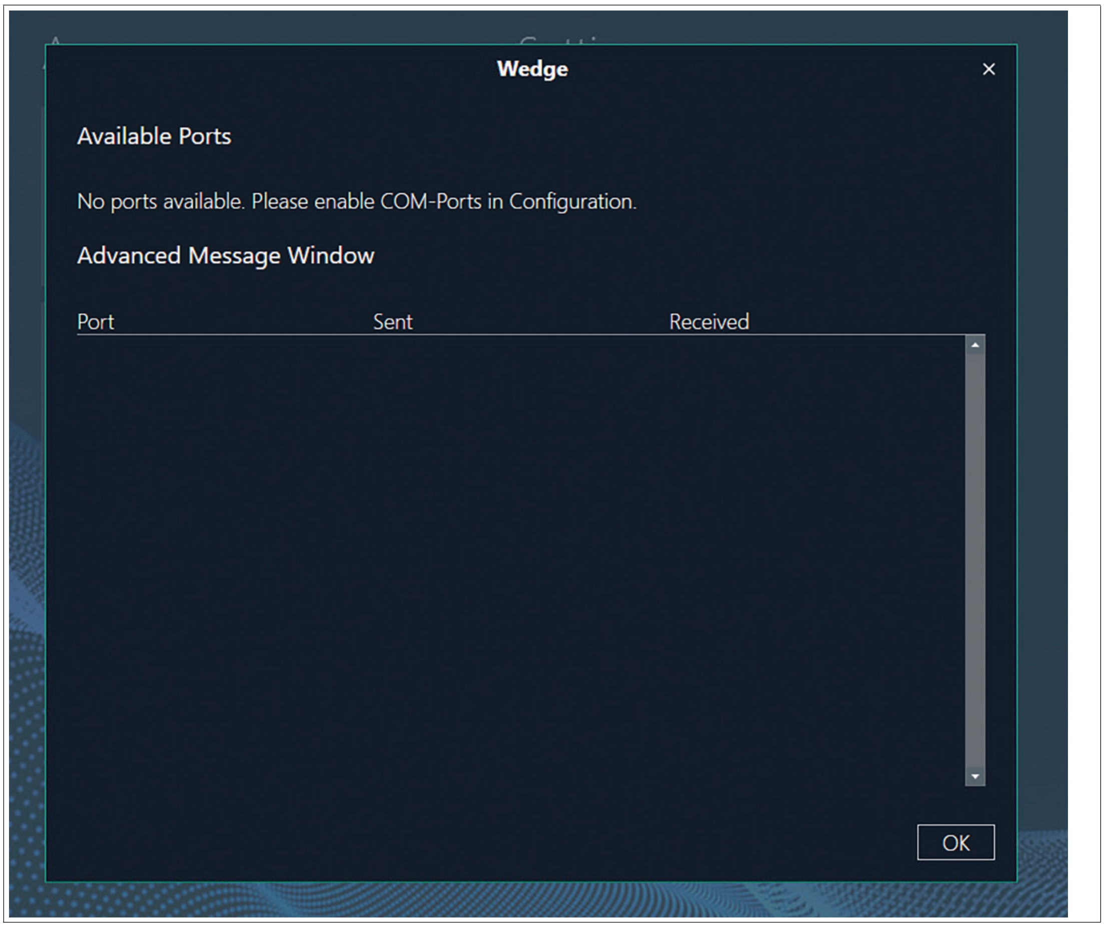


Figure 7.4 VisuNet RM Shell 6 Wedge App

The wedge app is a keyboard emulation program that reads character strings from the serial port and simulates the corresponding keystrokes on the RM. In other words, the Wedge scans serial interfaces (e.g. barcode readers) and converts them into keyboard inputs. 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 8.15.

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 for both user roles (Operator and Administrator).



Available Ports

No ports available. Please enable COM-Ports in Configuration.

Advanced Message Window

Port	Sent	Received

Figure 7.5

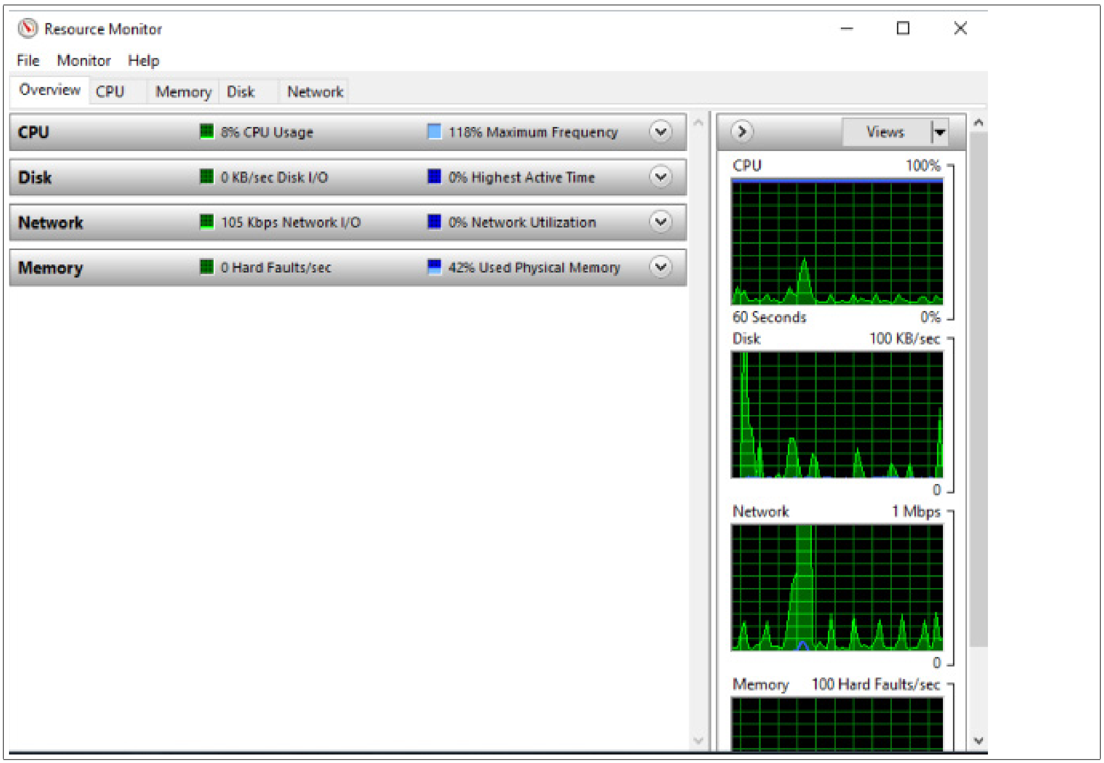
Hide Wedge App from Operator

In VisuNet RM Shell 6 it is also possible to hide the Wedge app from the Operator. To do so, perform following steps:

1. Log in as an Administrator.
2. Go to **System Settings**.
3. Select **Wedge Configuration**.
4. Activate the option **Hide Wedge App from the Operator on Main view**.
5. Apply changes.
6. Wedge App will not be shown in Operator view.

7.2 Process Explorer App

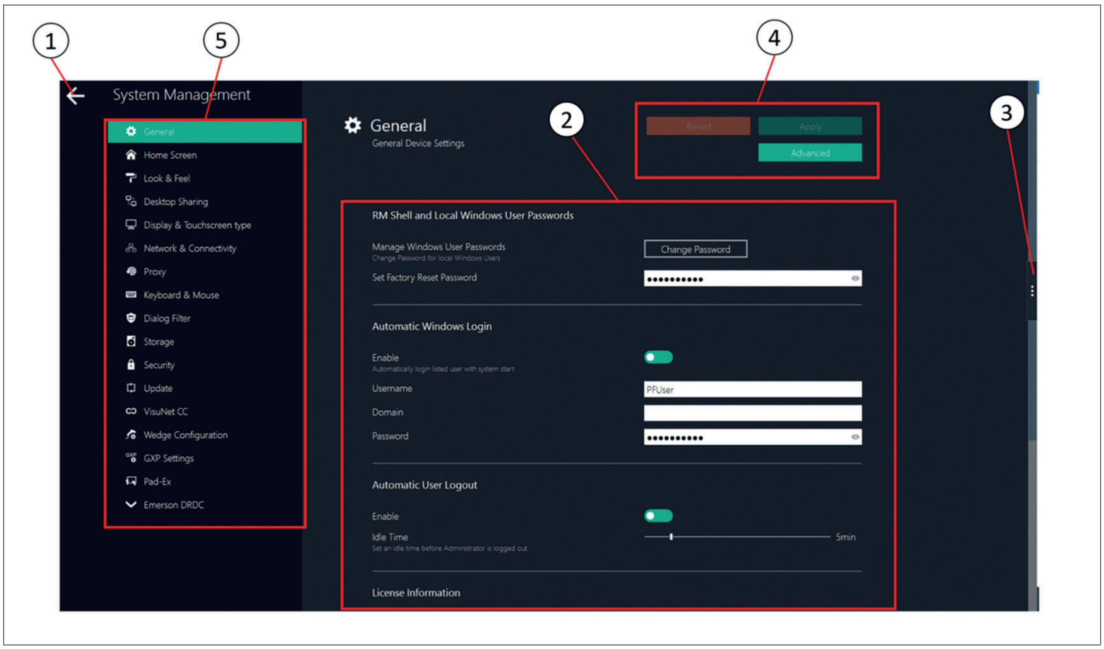
The Process Explorer app allows you to monitor multiple device parameters, including memory, storage usage, and CPU load. This tool can be used to diagnose and test RM Shell. The Administrator user role can determine which users have access to it in the "app management" app, see chapter 7.



CPU	🟩 8% CPU Usage	118% Maximum Frequency
Disk	🟩 0 KB/sec Disk I/O	0% Highest Active Time
Network	🟩 105 Kbps Network I/O	0% Network Utilization
Memory	🟩 0 Hard Faults/sec	42% Used Physical Memory

Figure 7.6 Process explorer window

8 System Settings App



RM Shell and Local Windows User Passwords

Manage Windows User Passwords
Change Password for local Windows Users

Set Factory Reset Password: ••••••••••

Automatic Windows Login

Enable
Automatically login listed user with system start

Username: PFUser

Domain:

Password: ••••••••••

Automatic User Logout

Enable

Idle Time: 5min
Set an idle time before Administrator is logged out

License Information

Figure 8.1 Components of the System Settings App Screen

1	Navigate back to home screen
2	Main Page / content page
3	Smart Task Bar. The bar opens when clicking on the three dots. Allows quick access to home screen, On-Screen-Keyboard, Task Switcher and already established connections.
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 Management App

1. To enter the system settings app, unlock Configuration View. After successfully authenticating as an administrator, the configuration view is displayed. Now click on System Management:

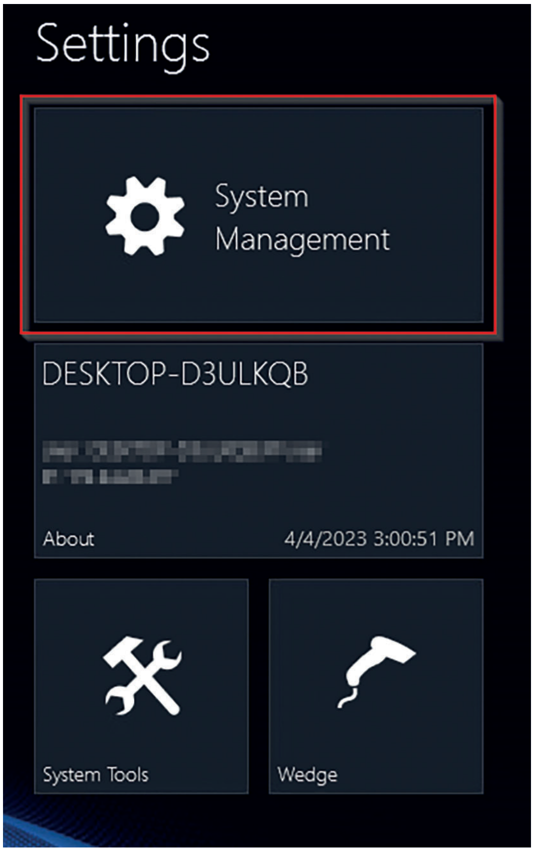


Figure 8.2

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

- **General**
  Specify general settings such as RM Shell and Local Windows User Passwords, Automatic Windows Login/Logout, license information and date and time settings, see chapter 8.1.
- **Home Screen**
  Manage the settings for the home screen and the Smart Task Bar, see chapter 8.2.
- **Look & Feel**
  Manage general Look & Feel settings like Wallpaper and Logo, see chapter 8.3.
- **Desktop Sharing**
  Manage the settings for sharing the screen of an RM, see chapter 8.4.
- **Display & Touchscreen Type**
  Manage display settings such as resolution, color depth, and refresh frequency, see chapter 8.5.
- **Network & Connectivity**
  Manage network settings such as network adapter information and IP address settings, see chapter 8.6.
- **Proxy**
  Enable proxy and manage proxy settings, see chapter 8.7.
- **Keyboard & Mouse**
  Manage keyboard settings such as input language, character repeat, and cursor blink, see chapter 8.8.

- **Dialog Filter**
  Add applications to a whitelist to prevent them from being closed by the dialog filter, see chapter 8.10.
- **Storage**
  Manage Storage Settings and Cleanup, see chapter 8.11.
- **Security**
  Set up VisuNet RM Shell passwords and enable firewalls, see chapter 8.12.
- **Update**
  Enable remote updates or scan for local updates, see chapter 8.13.
- **VisuNet CC**
  Configure VisuNet Control Center, see chapter 8.14.
- **Wedge Configuration**
  Manage wedge configuration settings such as input character delay and remote text input mode. Define assigned functions for HEX codes, see chapter 8.15.
- **GXP Settings**
- **Pad-Ex**
  Manage your Pad-Ex settings as selecting the action for your program key or rotation lock.
- **RFID Reader**
  Set standard or custom RFID reader configurations.
- **Emerson DRDC**
  Configure general Emerson DRDC Settings, see chapter 8.17.

8.1 General Settings

RM Shell and Local Windows User Passwords

Change the passwords for local Windows users (PFAdmin and PFUser). By clicking on **Change Password** a dialogue to change the PFAdmin or PFUser passwords is displayed. To change the password, the old one is required first.

Change and set the password for a factory reset. To reset the device to factory settings, this password is required.

Automatic Windows Login

Enable to automatically login the selected user with system start. Type in the user who should be logged in automatically below. If you want a user from a domain to be logged in automatically, enter the domain below. The user?s password is mandatory for the login to be successful.

Automatic User Logout

Set a timer after which the administrator will be logged out automatically. Logout is executed when the administrator does not perform any registered movement for the set time.

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

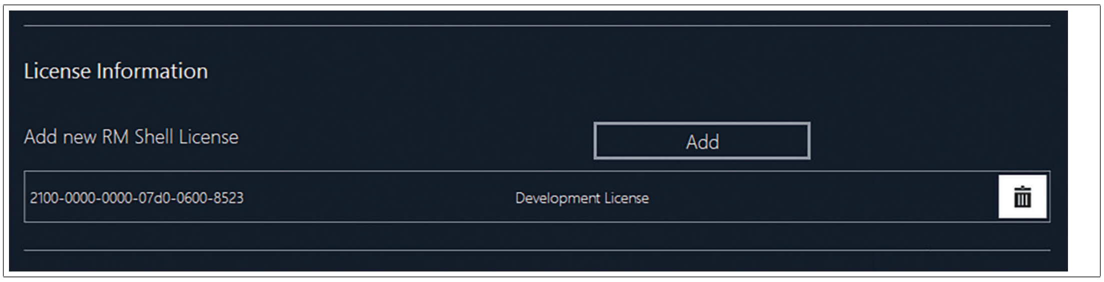
Note

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.

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.



License Information

Add new RM Shell License

2100-0000-0000-07d0-0600-8523 Development License

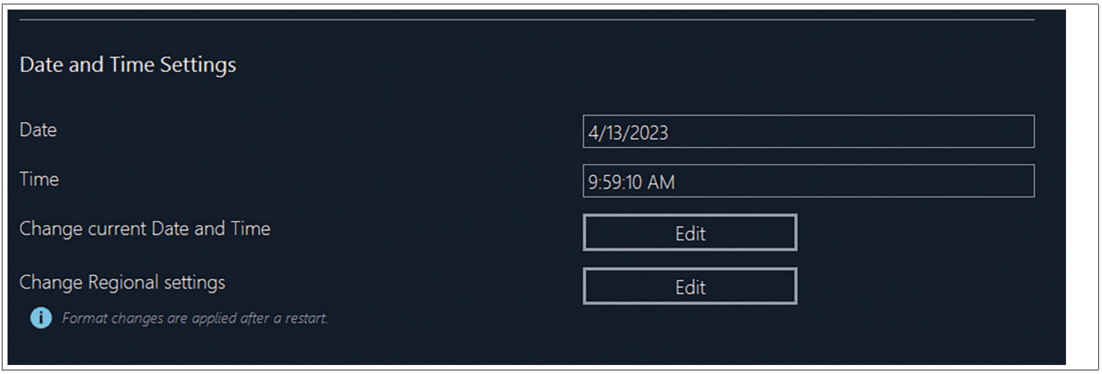
Figure 8.3

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.
Change Date and Time	Click the "Edit" button to configure the date and time. The Windows® "Date and Time" dialog box opens.
Change Regional Settings	Click the "Edit" button to configure regional settings. The Windows® "Region and Language" dialog box opens.



Date and Time Settings

Date: 4/13/2023

Time: 9:59:10 AM

Change current Date and Time: Edit

Change Regional settings: Edit

Format changes are applied after a restart.

Figure 8.4

Caution!

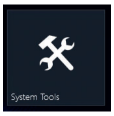
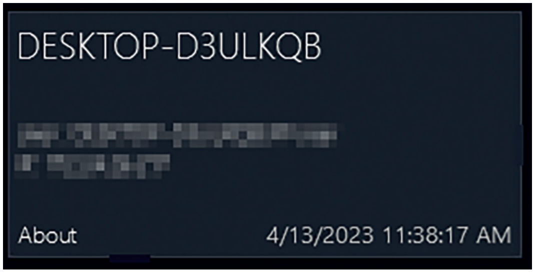
Time Zone, Date and Time

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.

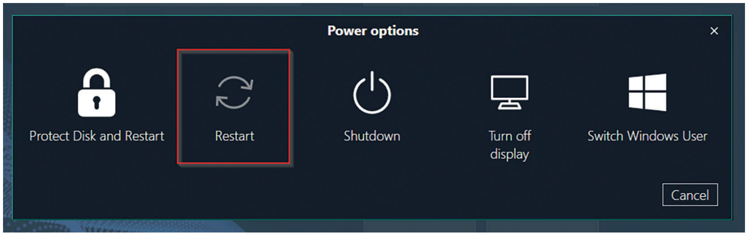
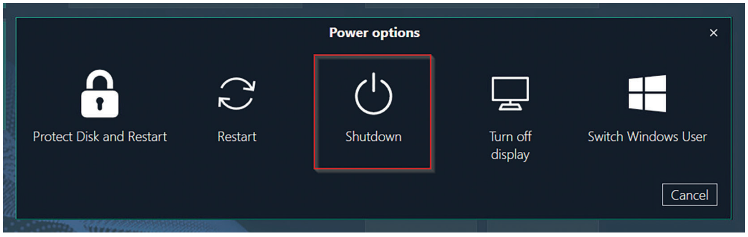
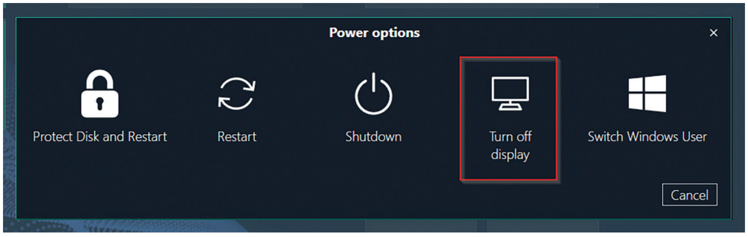
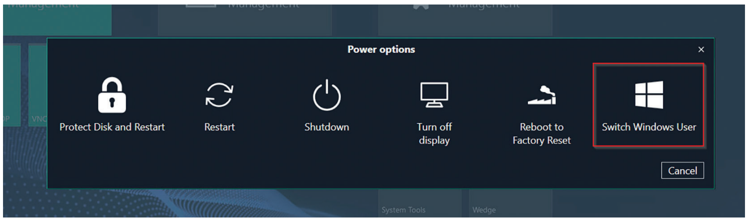
8.2 Home Screen

Customize the layout of the home screen.

Home Screen Settings

Function	Description
Show System Tools to Operator	Show or hide the following tile from the operator: 
Show IP Address inside the "About" Tile to Operator	Show or hide the IP Address text within "About" tile from the operator:  DESKTOP-D3ULKQB About 4/13/2023 11:38:17 AM

Power Button on Home Screen for Operator

Fuction	Description
Show "Restart" Button	Show or hide the restart option within the Power Options from the operator:  Power options × Protect Disk and Restart Restart Shutdown Turn off display Switch Windows User Cancel The operator cannot restart the device when this button is hidden.
Show "Shutdown" Button	Show or hide the shutdown option within the Power Options from the operator:  Power options × Protect Disk and Restart Restart Shutdown Turn off display Switch Windows User Cancel The operator cannot turn off the device when this button is hidden.
Show "Turn off display" Button	Show or hide the display turn off option within the Power Options from the operator:  Power options × Protect Disk and Restart Restart Shutdown Turn off display Switch Windows User Cancel The operator cannot turn off the display manually when this button is hidden.
Show "Switch Windows User" Button	 Power options × Protect Disk and Restart Restart Shutdown Turn off display Reboot to Factory Reset Switch Windows User Cancel Show or hide the Switch Windows User option within the Power Options from the operator: The operator cannot switch the windows user when this button is hidden.

Floating Quick Menu

In this section you can enable or disable the floating quick menu.The floating menu can be located as required by easily moving the menu with your mouse.

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

The Floating Quick Menu pops up in the upper left corner of the screen. Depending on the hardware the RM Shell runs on, the on-screen-keyboard, battery status or WiFi status is shown. In this case, the Floating Quick Menu consists only of the on-screen-keyboard.

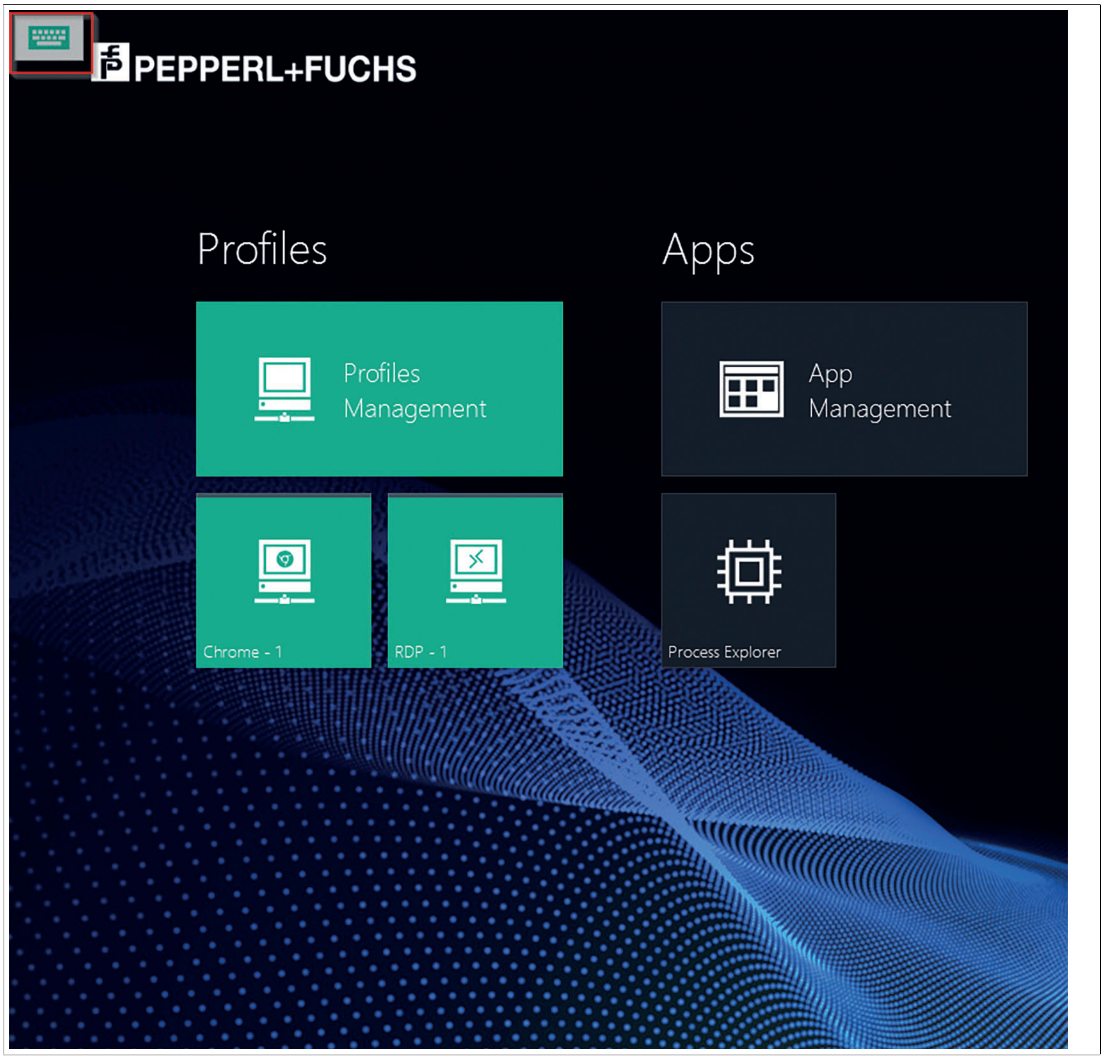
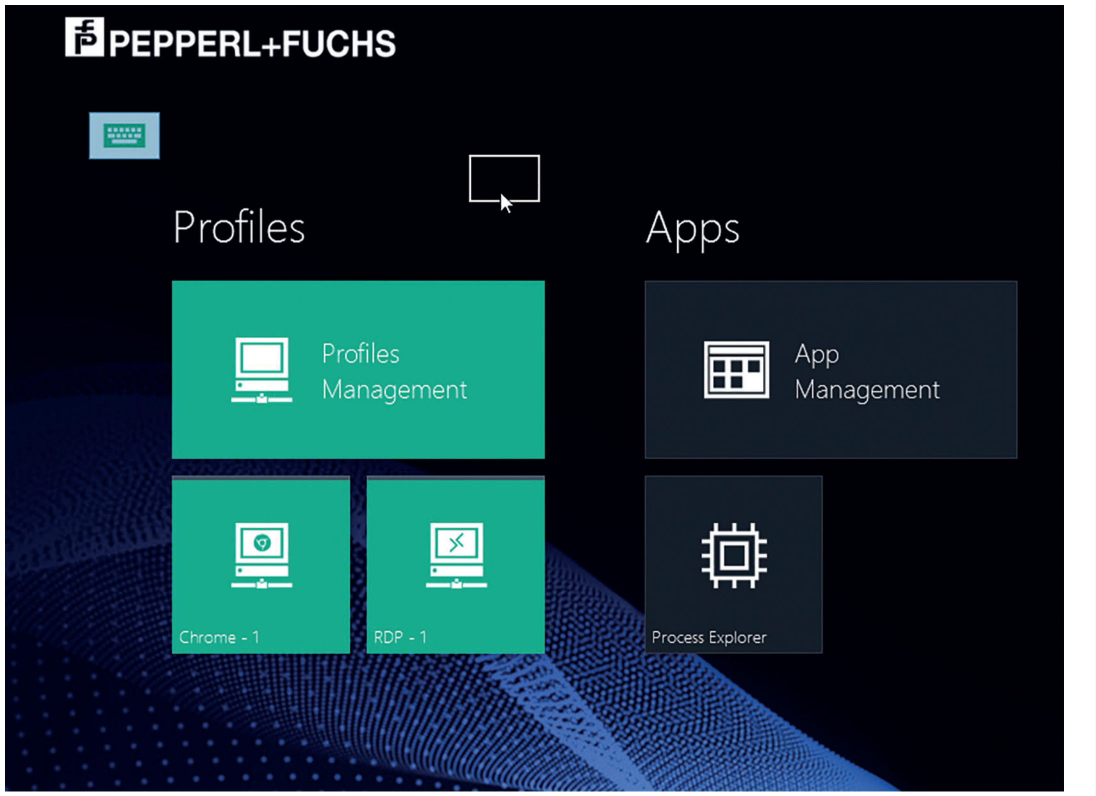


Figure 8.5

The Floating Quick Menu can then be relocated to the desired position. The functionalities can then be activated by clicking directly on the icon.



PEPPERL+FUCHS
Profiles
Apps
Profiles Management
App Management
Chrome - 1
RDP - 1
Process Explorer

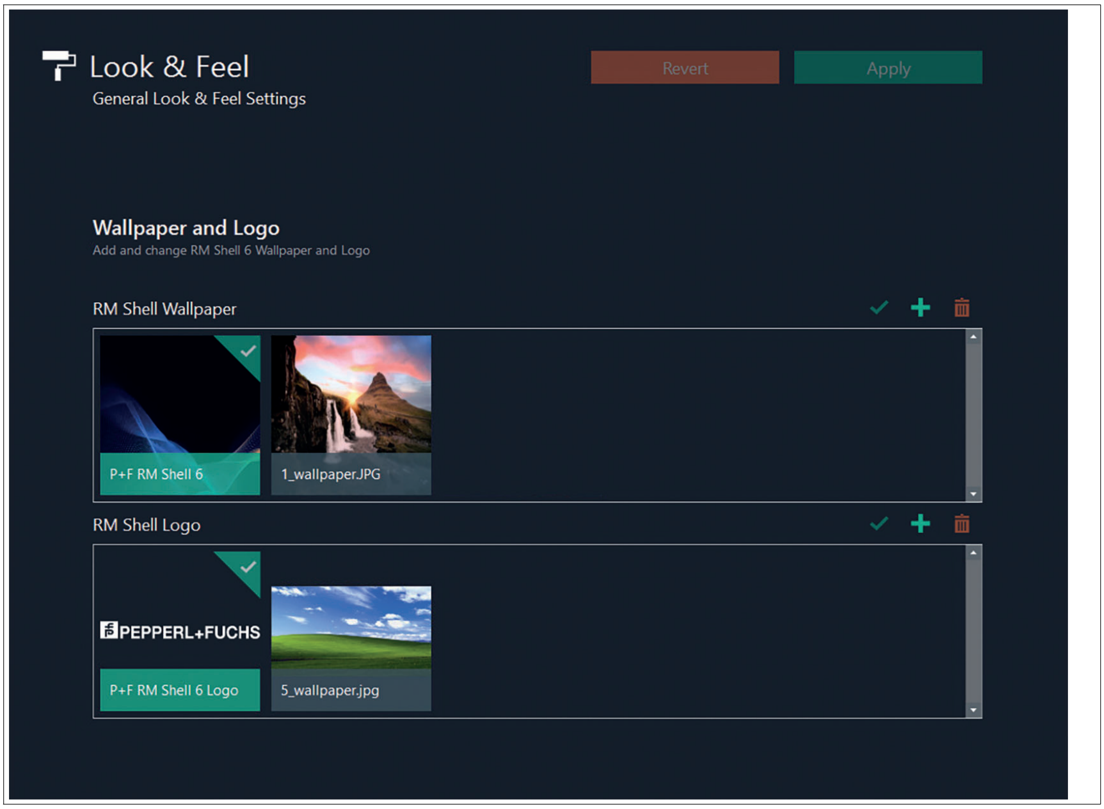
Figure 8.6

8.3 Look and Feel

Change the wallpaper and logo displayed within the RM Shell.

To change the wallpaper, click on the + symbol. Select the desired image from the Windows file explorer. After uploading click on the newly added picture to select it as wallpaper.

Repeat the same process for changing the logo. The logo is displayed in the upper left corner of the screen.



Look & Feel
General Look & Feel Settings

Wallpaper and Logo
Add and change RM Shell 6 Wallpaper and Logo

RM Shell Wallpaper

RM Shell Logo

Figure 8.7

8.4 Desktop Sharing

Desktop Sharing Server

This chapter describes the configuration for sharing local displays with other VisuNet RM Shell devices or VisuNet Control Center.

Function	Description
Enable	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.
Server status	Displays the current status of the Desktop Sharing Server. When enabled, the status is set to "Running". When disabled, the status changes to "Stopped"
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.
Identify Display	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.
Use Default Password (not recommended)	Enable to use the password of the current user to secure Desktop Sharing. It is recommended to use an individual, strong password to increase security

Function	Description
Custom Desktop Sharing Password	Set an individual password for Desktop Sharing (highly recommended)
Extra Ports	By default, the desktop sharing server will capture and broadcast all (or selected) displays on a system as a single feed. Using the extra ports it is possible to either share a second display on an extra network port or capture portions of display(s): Specify the port you wish to use (5901 is the default) and the geometry specification (in pixels) you need. (port: h.resolution x v.resolution + X.offset + Y.offset) 1. For example, to capture the middle display of a 3-monitor setup on port 5901 where all displays are 1920x1080, you would use 5901:1920x1080+1920+0 2. To capture the first and second display on this system, you would use 5901:3840x1080+0+0 3. Note that the canvas is not always the same, depending on monitor layout as it relates to video outputs. Obtaining the desired results from the first above configuration may necessitate changing the X value to either 0 or 3840. 4. Note that the firewall may prevent using the port. So it is necessary to create a custom rule which allows incoming traffic on the desired port 5. Note that the connection is not encrypted. The Secure Tunnel cannot be used for the extra port.

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.

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

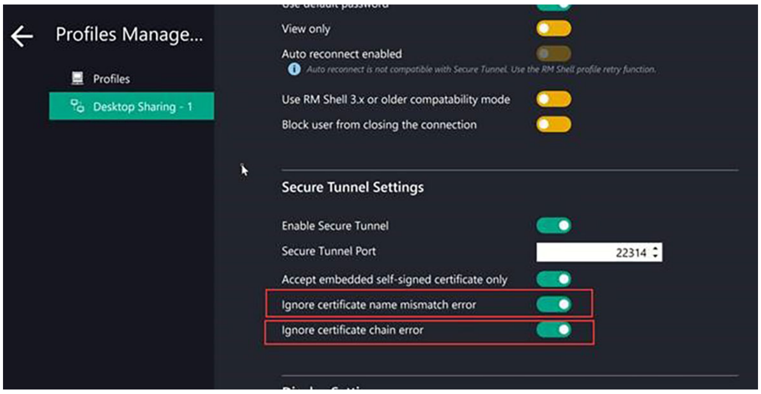
Secure Tunnel

The Secure Tunnel establishes a secure connection between the two devices. Desktop sharing itself is unencrypted. Secure Tunnel enables encrypted connection. This section is for configuring the Secure Tunnel settings.

Function	Description
Enable	Further increase of the security
Service status	Displays the current status of the Secure Tunnel. When enabled, the status is set to "Running". When disabled, the status changes to "Stopped"
Secure Tunnel Port	We recommend using the default setting. If a different port is used, the firewall must be adjusted.
Use Default Certificate (not recommended)	Enable to use the default certificate to secure Desktop Sharing. It is recommended to use an individual certificate to increase security
Custom Certificate	Upload your own trusted root certificate Please note that only certificates from inside the Local Machine Store with private keys are allowed
Certificate Information	When using a custom certificate (recommended) following certification information is displayed: Subject, Issuer, Date, Friendly Name

Desktop Sharing Connection from a VisuNet RM Shell 5 to a Shell 6

1. For a desktop sharing connection from a Shell version prior to 5.7 to a Shell 6 device (with secure tunnel enabled), the following two settings must be set. You can also update your VisuNet RM Shell 5 device to the latest firmware 5.7 (only for Windows® 10 LTSC 2019 systems).



View only

Auto reconnect enabled

Auto reconnect is not compatible with Secure Tunnel. Use the RM Shell profile retry function.

Use RM Shell 3.x or older compatability mode

Block user from closing the connection

Secure Tunnel Settings

Enable Secure Tunnel

Secure Tunnel Port 22314

Accept embedded self-signed certificate only

Ignore certificate name mismatch error

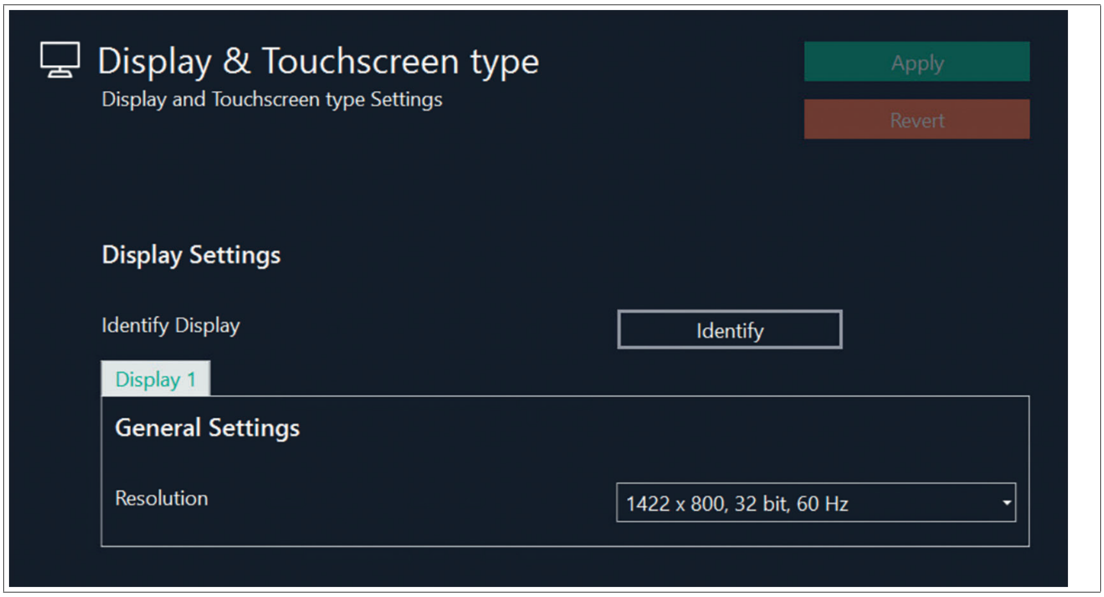
Ignore certificate chain error

Figure 8.8

8.5 Display & Touchscreen Type

8.5.1 Configuring a Single Monitor

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



Resolution: 1422 x 800, 32 bit, 60 Hz

Figure 8.9

Note

We recommend using the default settings.

8.5.2 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.

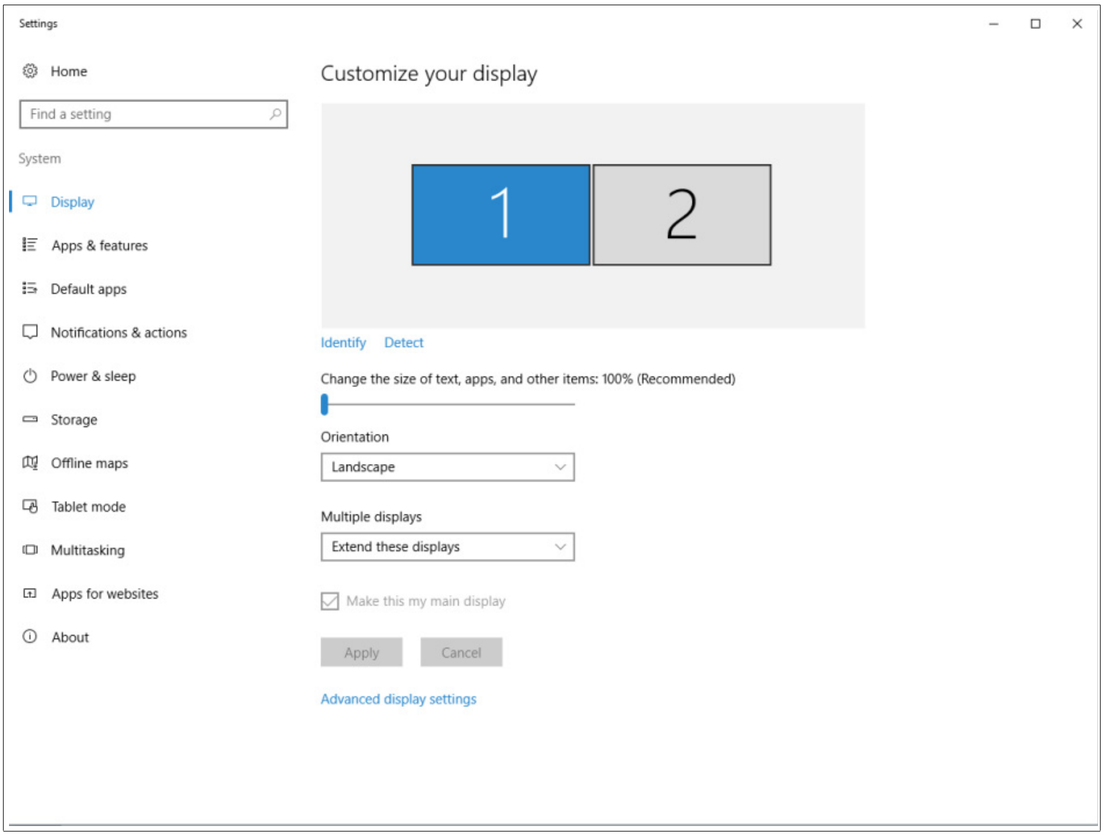
The "Identify" button can be used to check the display numbering of the connected monitors.

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.



Change the size of text, apps, and other items: 100% (Recommended)

Orientation: Landscape

Multiple displays: Extend these displays

☑ Make this my main display

Figure 8.10 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 monitorswith the following requirements are connected: - Identical resolution. - All displays are landscape-oriented. - The displays are arranged in a close-to-2x2-arrangement.

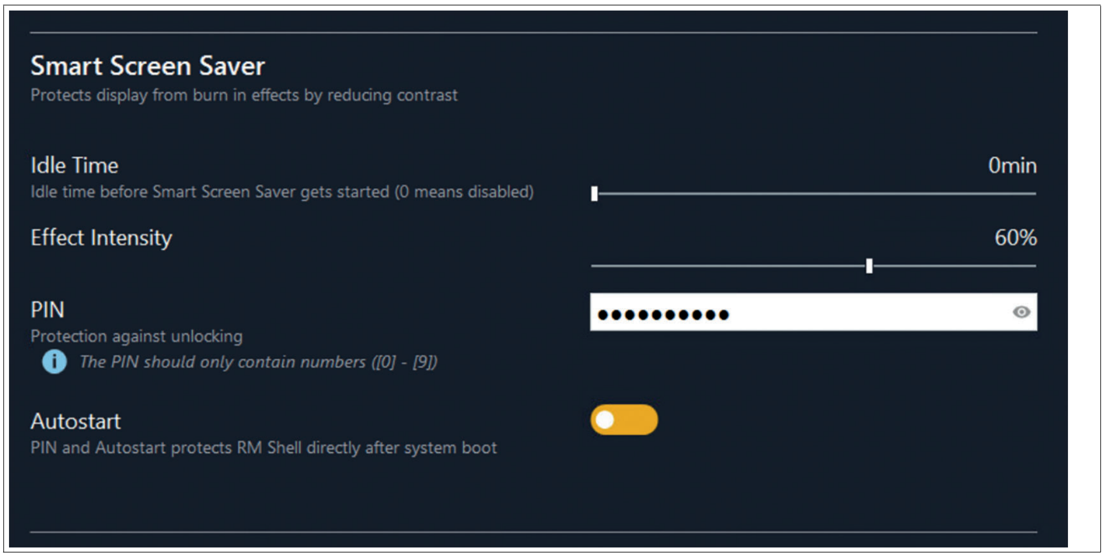
1. Fulfill the requirements listed above
2. The option "Four-Monitor Setup" pops up when the requirements are fulfilled. Click **Align** to set up automatically an accurate 2x2 Quad-Monitor setup.

Smart Screen Saver

In this section, you find the settings for the Smart Screen Saver.

The Smart Screen Saver 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, Smart Screen Saver will start. If the time is set to 0 min, the screensaver is disabled.
Effect Intensity	Configure the intensity of the Smart Screen Saver. 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.
Autostart	After a reboot or a new start of the deviceevery user role has to enter the PIN to unlock the device (PRO license required).



Smart Screen Saver
Protects display from burn in effects by reducing contrast

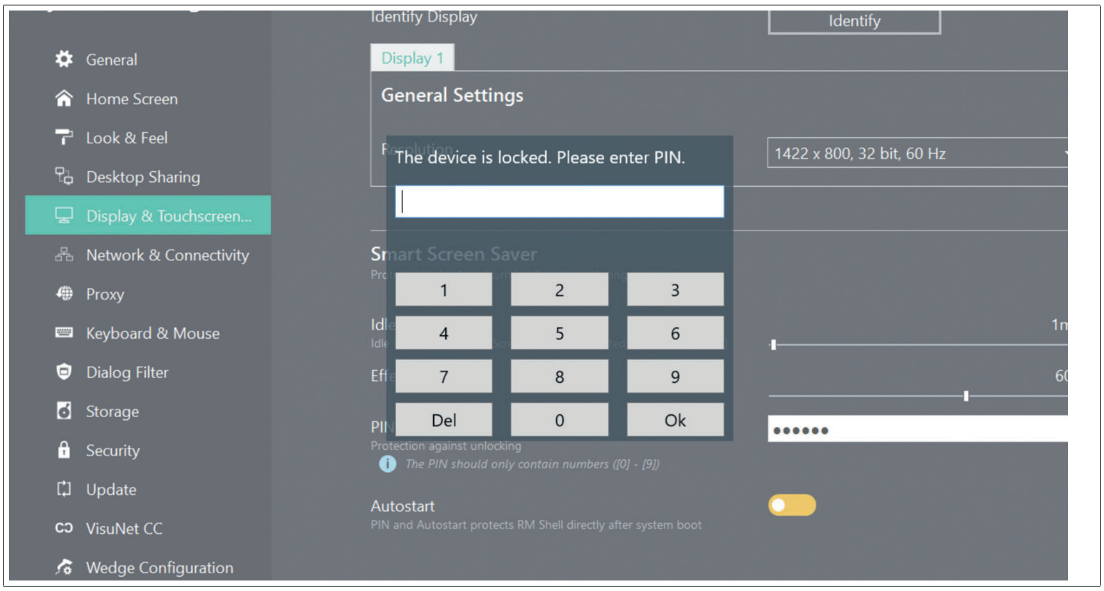
Idle Time
Idle time before Smart Screen Saver gets started (0 means disabled)
0min

Effect Intensity
60%

PIN
Protection against unlocking
The PIN should only contain numbers ([0] - [9])
••••••••••

Autostart
PIN and Autostart protects RM Shell directly after system boot

Figure 8.11 Smart Screen Saver Settings



The device is locked. Please enter PIN.

1422 x 800, 32 bit, 60 Hz

Protection against unlocking

The PIN should only contain numbers ([0] - [9])

PIN and Autostart protects RM Shell directly after system boot

Figure 8.12 Unlock your numeric password with the keypad

Touchscreen

Select the Touchscreen type. This only affects the displayed touchscreen settings within the RM Shell. The Windows drivers remain unchanged.

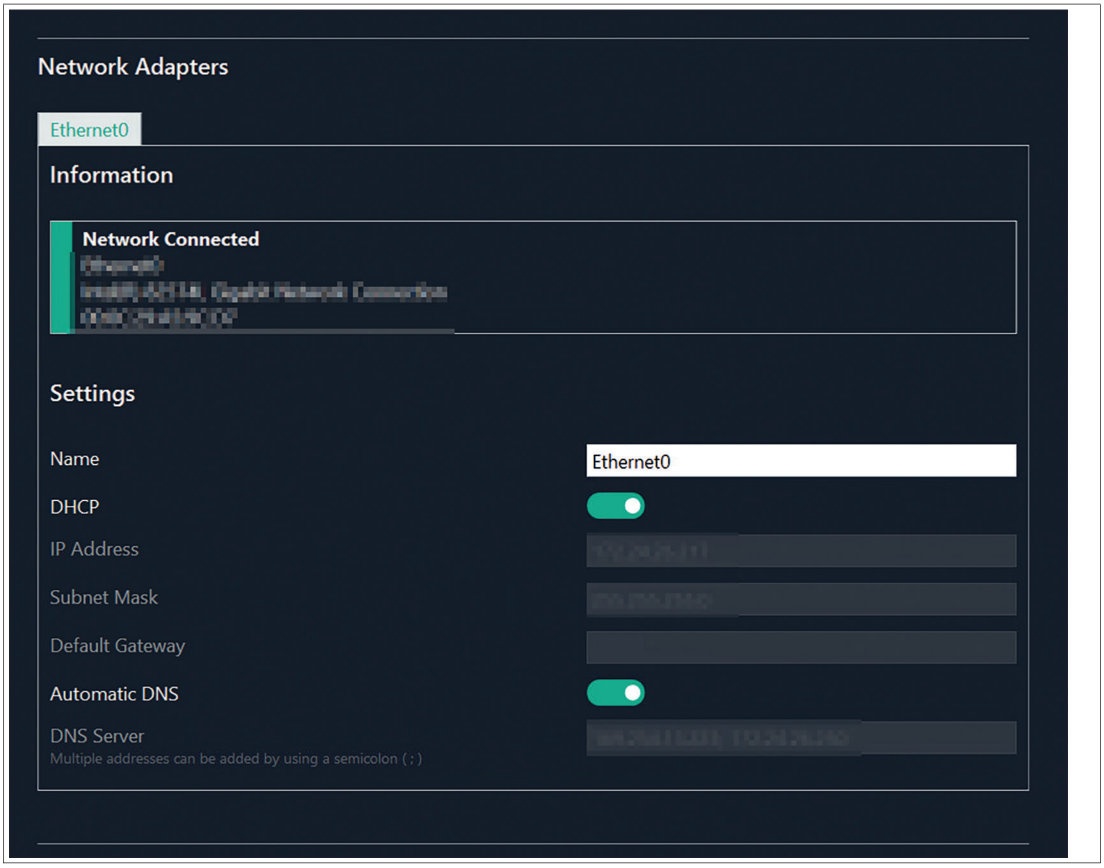
8.6 Network & Connectivity

Computer Information

Function	Description
Computer Name	Rename the computer. The name gets displayed in the "About" tile on the Home Screen. The device name also shows up in the network when connected.
Computer Description	This is an optional feature. Describe the device you are using here. This might be helpful when using several devices to identify RMs and TCs easily.

Network Adapters

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.



Network Adapters

Ethernet0

Information

Network Connected
[redacted]

Settings

Name: Ethernet0

DHCP: ●

IP Address: [redacted]

Subnet Mask: [redacted]

Default Gateway:

Automatic DNS: ●

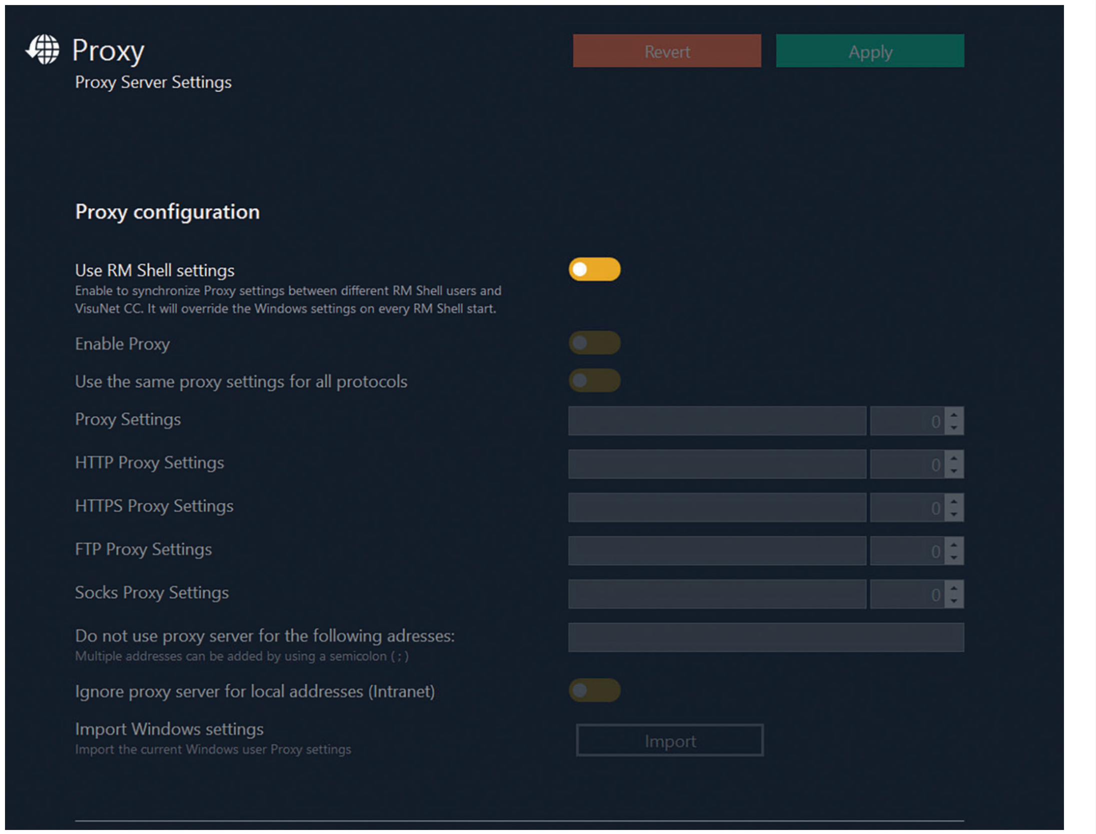
DNS Server: [redacted]
Multiple addresses can be added by using a semicolon (;)

Figure 8.13 Network adapter information and settings

8.7 Proxy

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

Function	
Use RM Shell settings	When enabled, the Proxy settings will override the Windows settings on every RM Shell start. This option synchronizes the Proxy settings between different RM Shell users and VisuNet Control Center
Enable Proxy	Use this option to enable/disable the use of a proxy server
Use the same proxy settings for all protocols	The Proxy configurations done in the next steps will be applied to all protocols listed below (HTTP, HTTPS, FTP, Socks)
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
Import Windows settings	Import the current Windows user Proxy settings to RM Shell



Proxy configuration

Use RM Shell settings
Enable to synchronize Proxy settings between different RM Shell users and VisuNet CC. It will override the Windows settings on every RM Shell start.

Enable Proxy

Use the same proxy settings for all protocols

Proxy Settings 0

HTTP Proxy Settings 0

HTTPS Proxy Settings 0

FTP Proxy Settings 0

Socks Proxy Settings 0

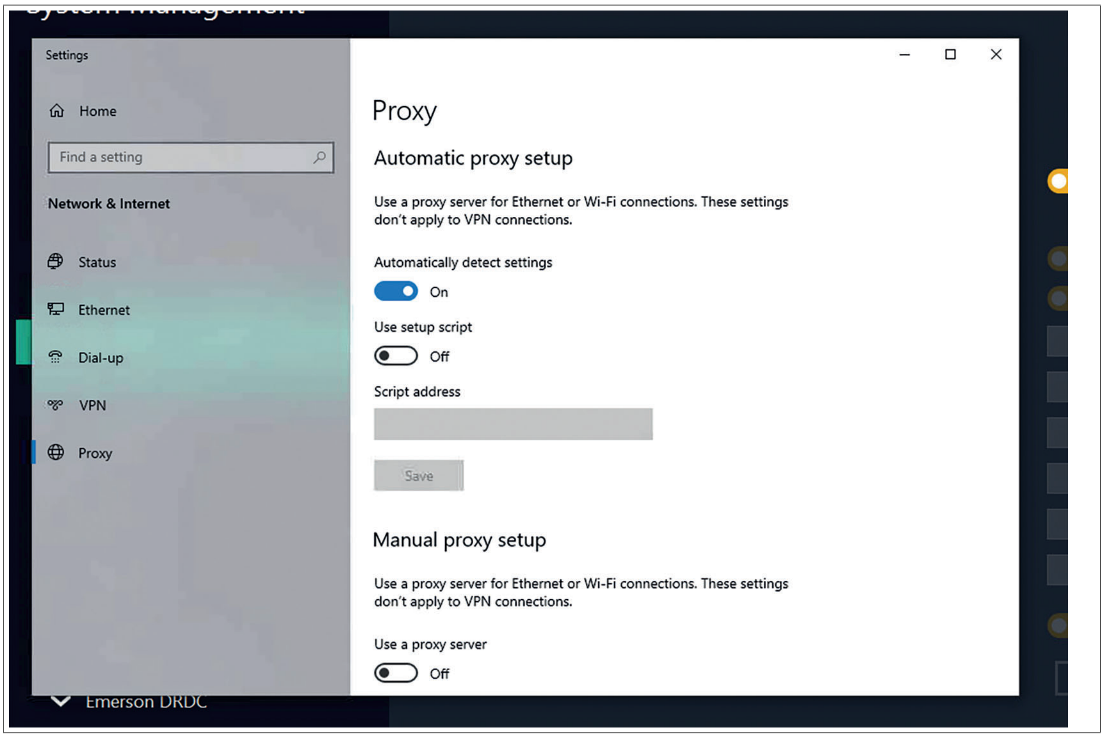
Do not use proxy server for the following adresses:
Multiple addresses can be added by using a semicolon (;)

Ignore proxy server for local addresses (Intranet)

Import Windows settings
Import the current Windows user Proxy settings

Figure 8.14 Proxy Settings

Function	Description
Open Windows control panel	Opens the advanced settings from Windows for Proxy configuration, e.g. Automatic proxy setup and manual proxy setup options
Open Internet Explorer proxy settings	Opens the connections tab within the Internet Explorer Properties for configuring advanced settings



Proxy

Automatic proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatically detect settings: On

Use setup script: Off

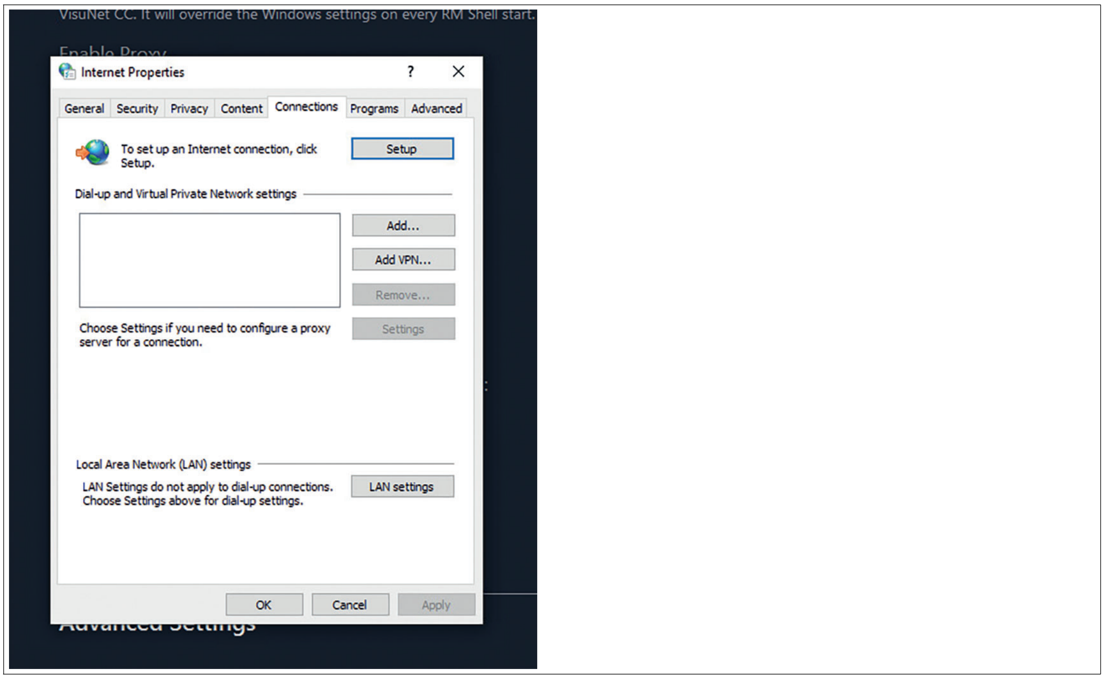
Script address

Manual proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Use a proxy server: Off

Figure 8.15 Advanced Windows Proxy Settings



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

Figure 8.16 Advanced Internet Explorer Proxy Settings

8.8 Keyboard & Mouse

On-Screen Keyboard

The On-Screen Keyboard is a movable keyboard that gets displayed on screen. It can be used to replace or to complement the physical keyboard. The keyboard can be moved via drag & drop to its desired position.

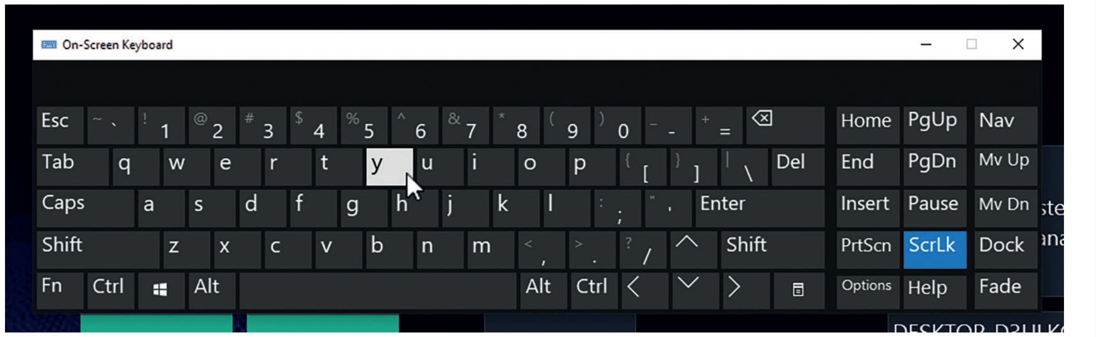

On-Screen Keyboard
Esc ~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ - + = ⌫ Home PgUp Nav
Tab q w e r t y u i o p { [}] | \ Del End PgDn Mv Up
Caps a s d f g h j k l : ; " ' Enter Insert Pause Mv Dn
Shift z x c v b n m < , > . ? / ^ Shift PrtScn ScrLk Dock
Fn Ctrl Alt Alt Ctrl < ˅ > Options Help Fade

Figure 8.17 The On-Screen Keyboard can by operated via the cursor or touchscreen

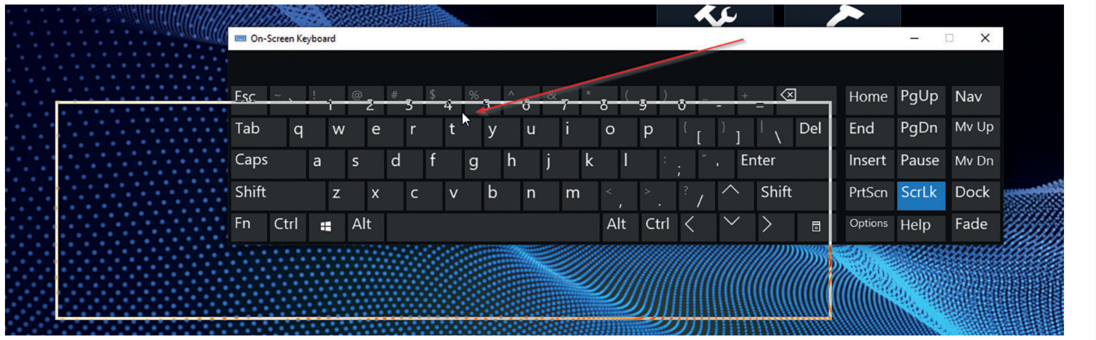

On-Screen Keyboard
Esc Home PgUp Nav
Tab q w e r t y u i o p Del End PgDn Mv Up
Caps a s d f g h j k l Enter Insert Pause Mv Dn
Shift z x c v b n m Shift PrtScn ScrLk Dock
Fn Ctrl Alt Alt Ctrl Options Help Fade

Figure 8.18 The On-Screen Keyboard can be repositioned easily by dragging and dropping

Function	Description
Autostart	Enable to start the On-Screen Keyboard automatically with system start
Select On-Screen Keyboard	Select the preferred On-Screen Keyboard layout: - Movable On-Screen Keyboard (default and recommended) - Tablet Touch Keyboard (recommended for Tablets, e.g. Pepperl+Fuchs' Pad-Ex®), movable option available

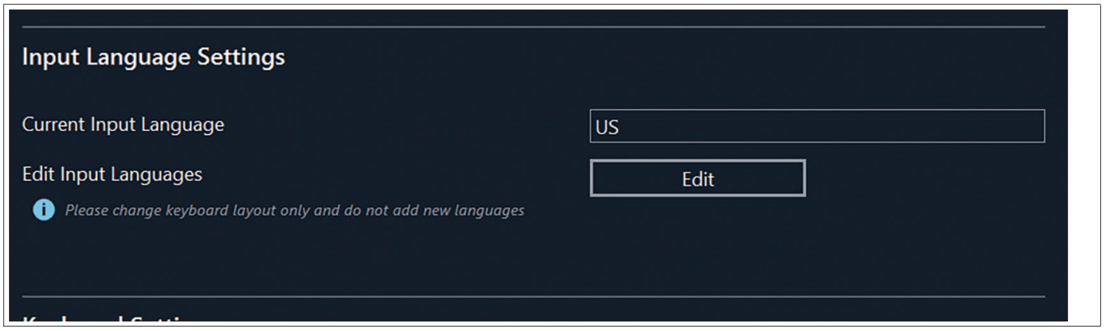
Input Language Settings

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.
Edit Input Languages	To add a specific keyboard layout, click the "Edit" button. A Windows® dialog box opens.

Warning!

Only the layout should be changed here. New language layouts can be added via the Windows desktop.


Input Language Settings

Current Input Language: US

Edit Input Languages

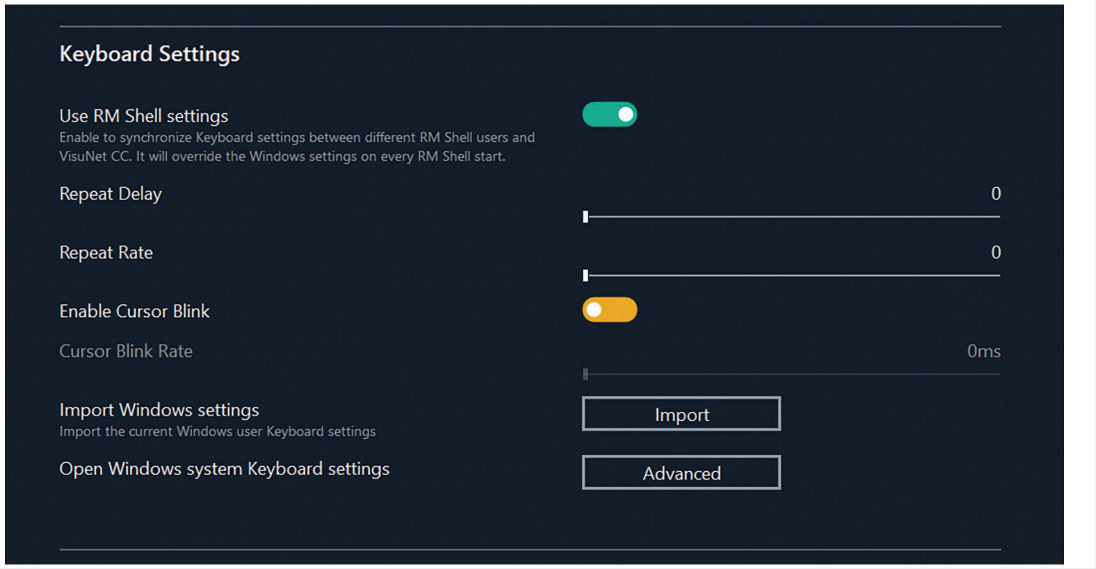
Please change keyboard layout only and do not add new languages

Figure 8.19 Input Language Settings

Keyboard Settings

Function	Description
Use RM Shell settings	When enabled, the keyboard settings will override the Windows settings on every RM Shell start. This option also synchronizes the keyboard settings between different RM Shell users and VisuNet Control Center
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.
Enable Cursor Blink	This function enables the blinking of the cursor. If you turn off cursor blink, the cursor will be constantly visible.

Function	Description
Cursor Blink Rate	Use the slider to adjust the blink rate of the cursor. This option is not available if cursor blink is disabled.
Import Windows settings	Imports the current Windows user's keyboard settings
Open Windows system Keyboard settings	Opens the advanced keyboard settings from Windows



Keyboard Settings

Use RM Shell settings
Enable to synchronize Keyboard settings between different RM Shell users and VisuNet CC. It will override the Windows settings on every RM Shell start.

Repeat Delay 0

Repeat Rate 0

Enable Cursor Blink

Cursor Blink Rate 0ms

Import Windows settings
Import the current Windows user Keyboard settings

Open Windows system Keyboard settings

Figure 8.20

Mouse Settings

Function	Description
Use RM Shell settings	When enabled, the mouse settings will override the Windows settings on every RM Shell start. This option also synchronizes the mouse settings between different RM Shell users and VisuNet Control Center
Mouse Cursor 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.
Invert 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.
Import Windows settings	Imports the current Windows user's mouse settings
Open Windows system Mouse settings	Opens the advanced mouse settings from Windows

Note

The changes become active only after a restart of the system.

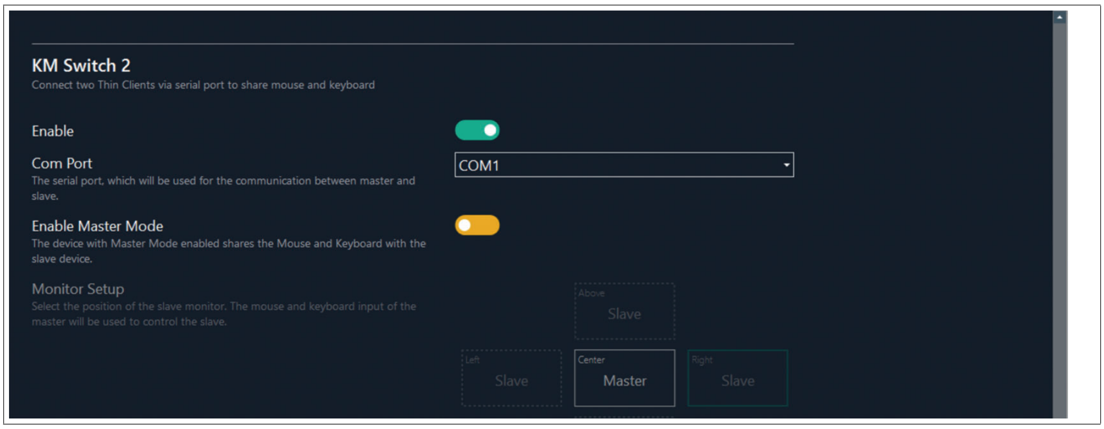
8.9 KM Switch 2

Note

To unlock this feature, an additional PRO license is required.

This feature is relevant for duplex monitor settings and works as well with separate network connections of the two devices.

If two PCs are connected to a COM port, this feature allows you to control both devices with one mouse/keyboard. Use these settings to configure your master and slave options.



KM Switch 2
Connect two Thin Clients via serial port to share mouse and keyboard

Enable

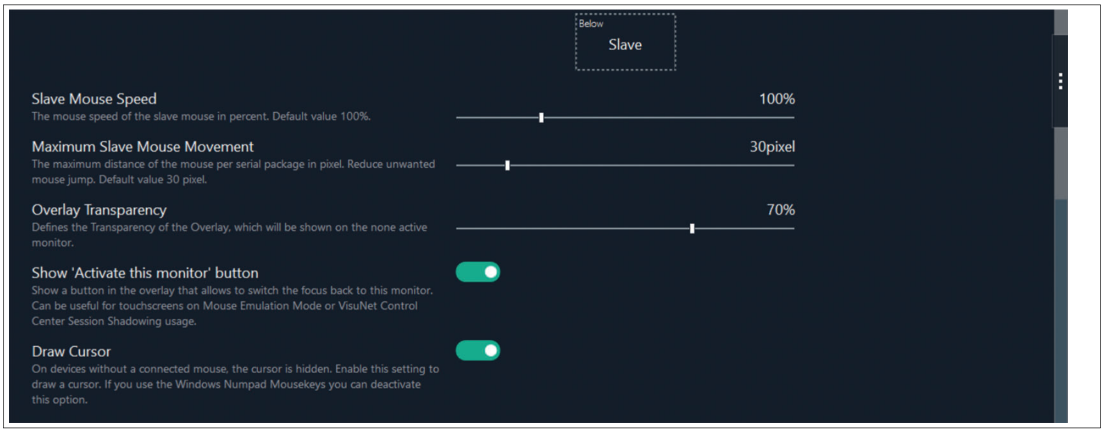
Com Port
The serial port, which will be used for the communication between master and slave.
COM1

Enable Master Mode
The device with Master Mode enabled shares the Mouse and Keyboard with the slave device.

Monitor Setup
Select the position of the slave monitor. The mouse and keyboard input of the master will be used to control the slave.

Figure 8.21

Feature	Description
Enable	PRO license unlocks the KM Switch Feature.
Com Port	Available Com Ports are listed in the drop-down menu. Com Ports are device-dependent.



Slave Mouse Speed
The mouse speed of the slave mouse in percent. Default value 100%.
100%

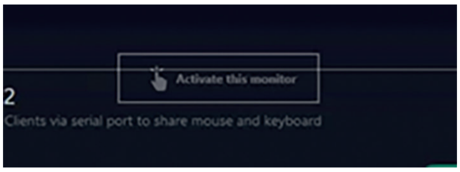
Maximum Slave Mouse Movement
The maximum distance of the mouse per serial package in pixel. Reduce unwanted mouse jump. Default value 30 pixel.
30pixel

Overlay Transparency
Defines the Transparency of the Overlay, which will be shown on the none active monitor.
70%

Show 'Activate this monitor' button
Show a button in the overlay that allows to switch the focus back to this monitor. Can be useful for touchscreens on Mouse Emulation Mode or VisuNet Control Center Session Shadowing usage.

Draw Cursor
On devices without a connected mouse, the cursor is hidden. Enable this setting to draw a cursor. If you use the Windows Numpad Mousekeys you can deactivate this option.

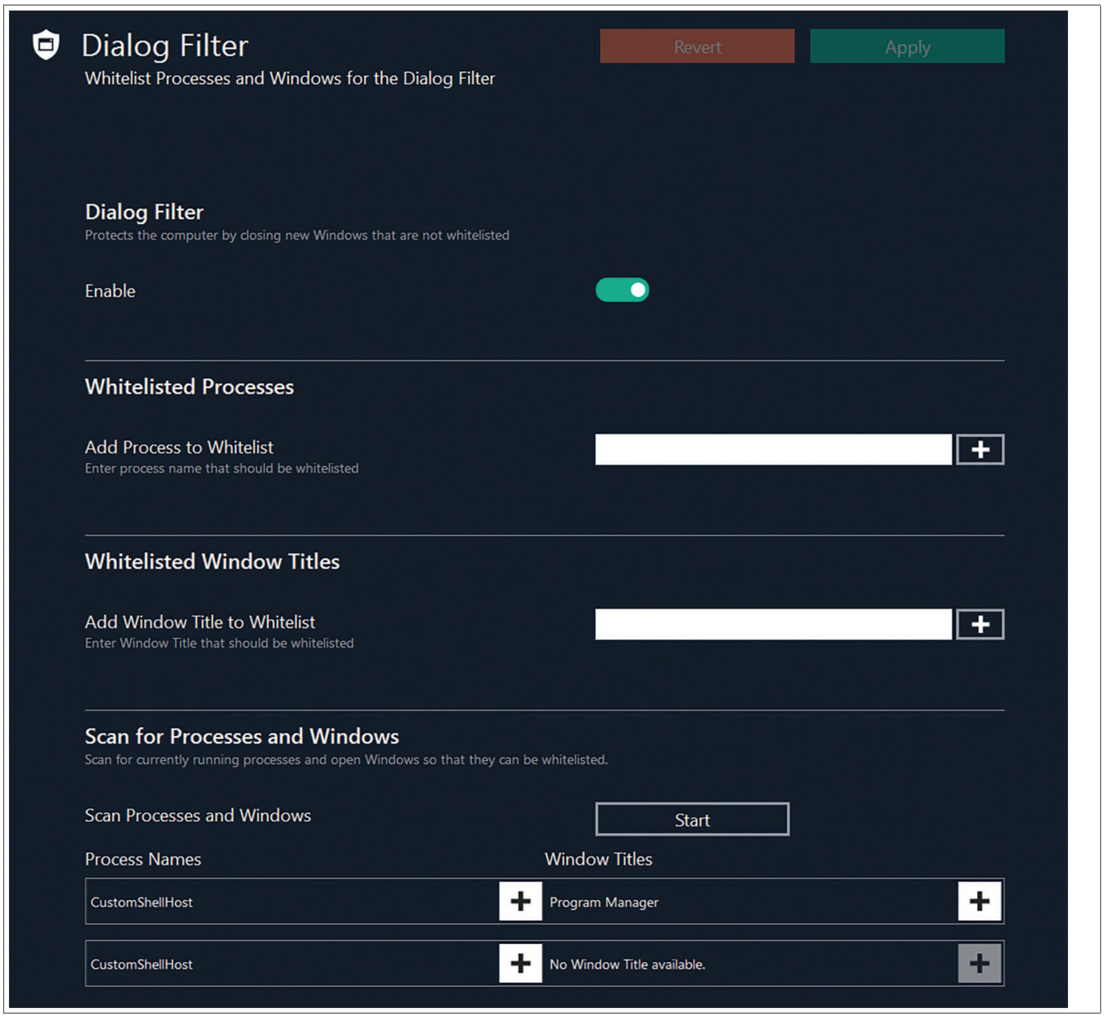
Figure 8.22

Feature	Description
Slave Mouse Speed	Only available on Master screen. Slave device cannot set the mouse speed.
Maximum Slave Mouse Movement	Only available on Master screen. Slave device cannot set the max. mouse movement distance per package.
Overlay Transparency	With this setting you can adjust the transparency of the gray overlay.
Show "Activate this monitor" button	 Clients via serial port to share mouse and keyboard
Draw Cursor	Enable this feature to the mouse draw mechanism of the KM Switch instead of Windows®.

8.10 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. When configuration view is open, the dialog filter is not activated.

Function	Description
Enable	Protects the computer by closing new windows that are not whitelisted
Whitelisted Processes ? Add process to Whitelist	Enter a process name and click the ⊞ button to add a process to the whitelist. Windows that are related to this process will pass the Dialog Filter and will be displayed to the current user. Type in the name of a Windows process to add it to the whitelist. For example, add "explorer."
Whitelisted Window Titles - 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."
Scan for Processes and Windows	Scan for currently running processes and open windows. Those processes will be listed below and can be added to the whitelist by clicking the ⊞ button next to the corresponding process. By clicking **Start**, all Windows which were open within in the last 60 seconds get listed below. 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.



Dialog Filter
Whitelist Processes and Windows for the Dialog Filter

Dialog Filter
Protects the computer by closing new Windows that are not whitelisted

Enable

Whitelisted Processes

Add Process to Whitelist
Enter process name that should be whitelisted

Whitelisted Window Titles

Add Window Title to Whitelist
Enter Window Title that should be whitelisted

Scan for Processes and Windows
Scan for currently running processes and open Windows so that they can be whitelisted.

Scan Processes and Windows

Process Names	Window Titles
CustomShellHost	Program Manager
CustomShellHost	No Window Title available.

Figure 8.23 Dialog Filter Settings

8.11 Storage

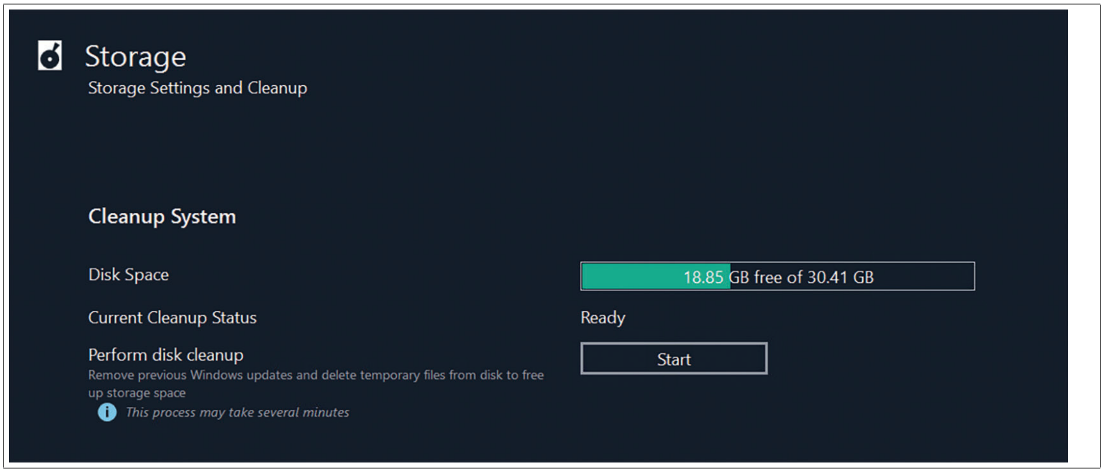
Cleanup System

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. The available disk space is visualized.

Function	Description
Disk Space	Shows the available and occupied disk space
Current Cleanup Status	Shows whether the Cleanup can be performed or not
Perform disk cleanup	By clicking start, previous Windows updates will be removed and temporary files from the disk are deleted to free up storage space This process might take several minutes.

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.



Storage

Storage Settings and Cleanup

Cleanup System

Disk Space: 18.85 GB free of 30.41 GB

Current Cleanup Status: Ready

Perform disk cleanup

Remove previous Windows updates and delete temporary files from disk to free up storage space

This process may take several minutes

Figure 8.24 Storage Settings

8.12 Security

Keyboard Filter

The keyboard filter is enabled per default. If you want to use the Ctrl+Alt and Win-Key, 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
Enable	Activates the Windows defender firewall to protect the system from incoming network access
Open Windows control panel	Click "Open" to open the Windows dialog window for firewall settings.

USB Storage Devices

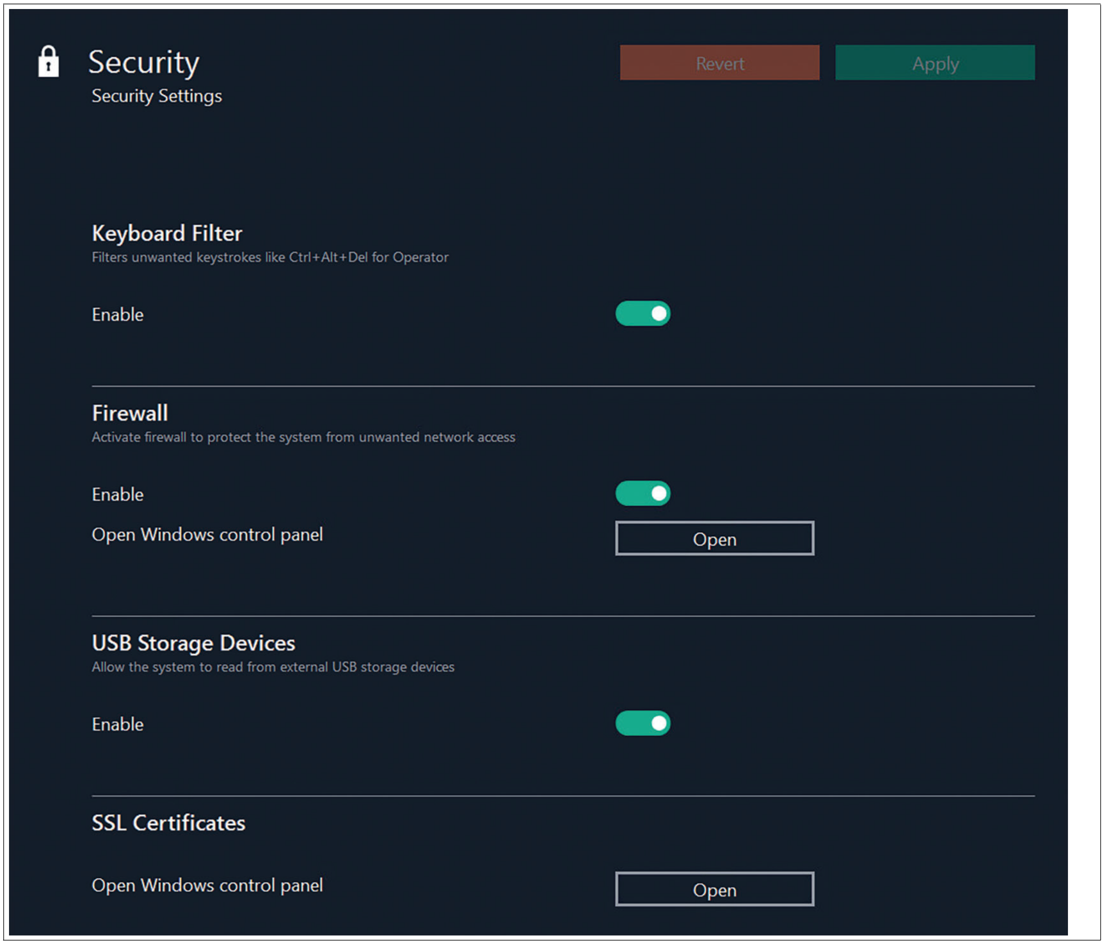
In this section, you can enable or disable external USB storage devices (e.g., pen drives, external hard disks, etc.).

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 **Disable**.

Function	Description
Enable	When enabled, the system is allowed to read data from external USB storage devices

SSL Certificates

In this section, you can edit the Microsoft-specific advanced certificate settings. By clicking **Open**, the advanced Windows settings can be accessed and configured.



Security
Security Settings

Keyboard Filter
Filters unwanted keystrokes like Ctrl+Alt+Del for Operator

Enable

Firewall
Activate firewall to protect the system from unwanted network access

Enable

Open Windows control panel

USB Storage Devices
Allow the system to read from external USB storage devices

Enable

SSL Certificates

Open Windows control panel

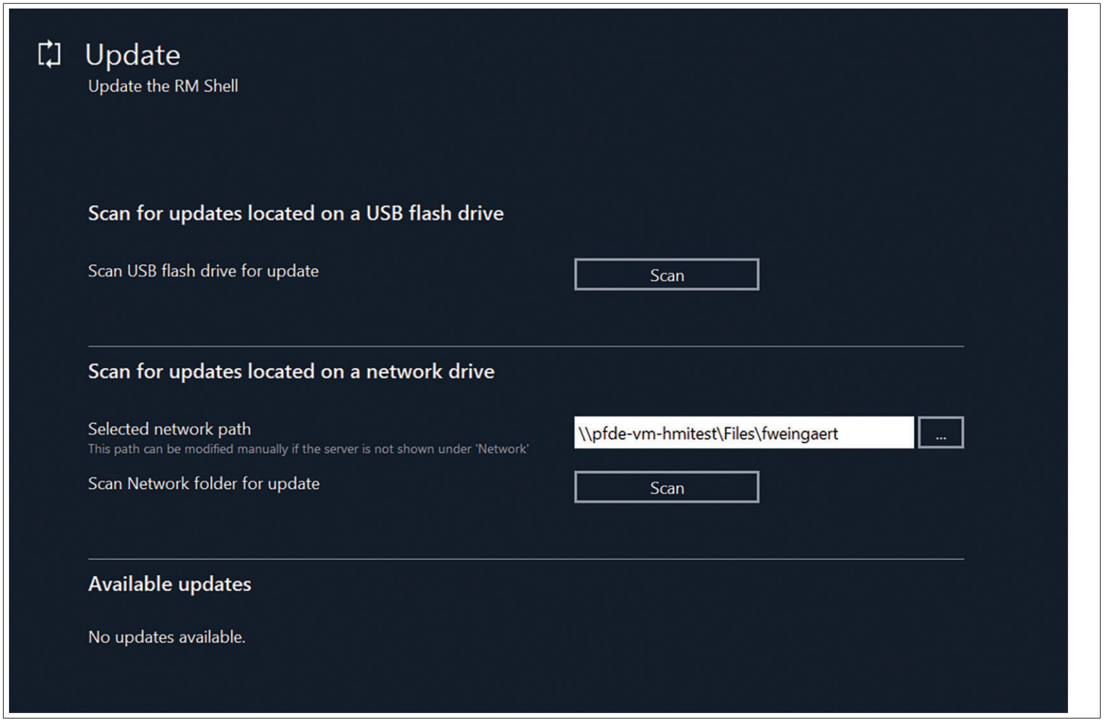
Figure 8.25 Security Settings

8.13 Update

In this section, it is described how you can update the VisuNet RM Shell to the latest version.

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)



Update
Update the RM Shell

Scan for updates located on a USB flash drive

Scan USB flash drive for update

Scan for updates located on a network drive

Selected network path
This path can be modified manually if the server is not shown under 'Network'

\\pfde-vm-hmitest\Files\fweingaert

Scan Network folder for update

Available updates

No updates available.

Figure 8.26

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. Disable "USB storage devices" to enable this updating option.
2. Connect the local device to the RM.
3. In the "Scan for updates located on a USB flash drive" section click **Scan**. The VisuNet RM Shell scans for updates stored on 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.
4. Choose the requested update The "Begin update" dialog box opens.
5. 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 drive

1. Create a share folder to locate the update there. The update is stored on a share that is accessible from the RM. Otherwise a new one must be created.
2. Open the path and scan in the selected folder for the available update.
3. The available update appears in the list.
4. Click **Begin Update** to start the installation.

Updating via VisuNet Control Center

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

8.14 VisuNet CC

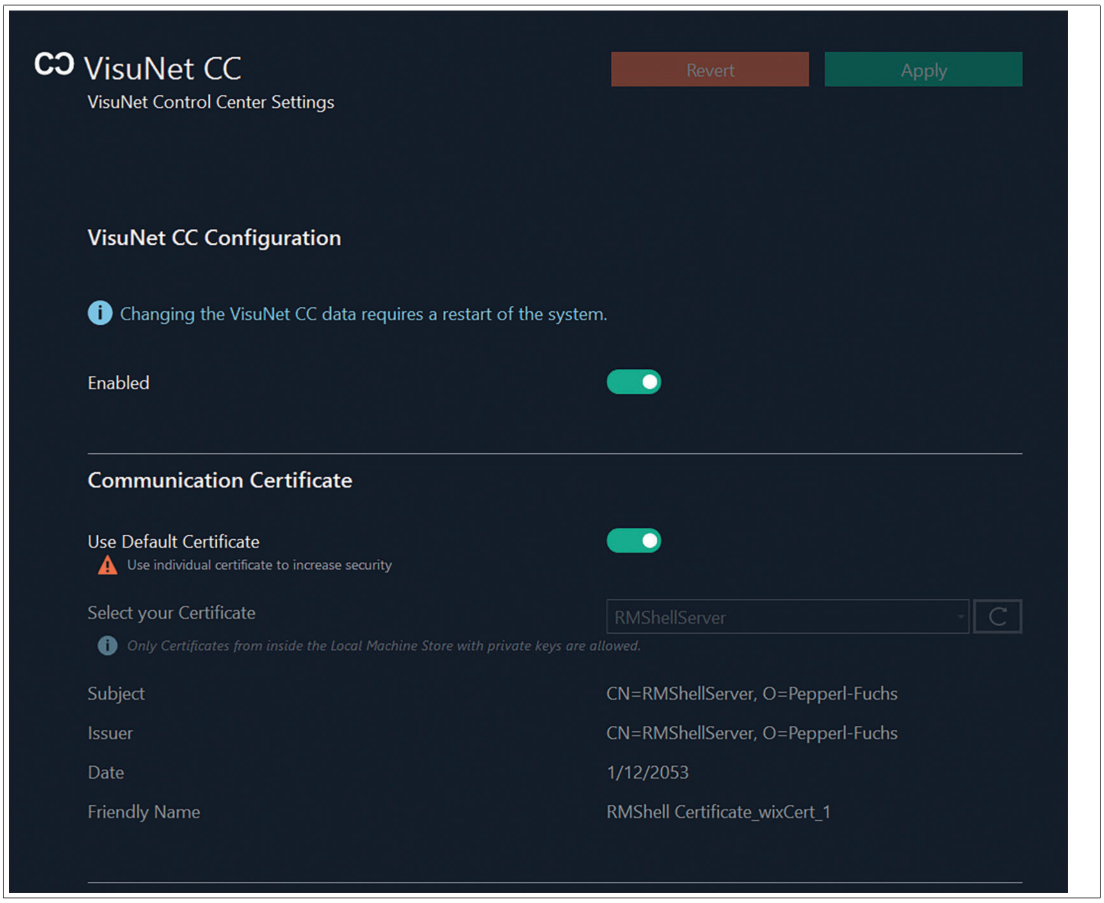
Note

To use VisuNet Control Center an additional licence is required. It is recommended to use your own certificate. Find more information of VisuNet CC online at www.pepperl-fuchs.com.

Note

It is recommended to install your own certificate with private key in the trusted root directory (local machine). This can be done by deselecting the default check mark and then selecting the certificate.

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.



VisuNet CC Configuration

Changing the VisuNet CC data requires a restart of the system.

Enabled

Communication Certificate

Use Default Certificate

Use individual certificate to increase security

Select your Certificate: RMShellServer

Only Certificates from inside the Local Machine Store with private keys are allowed.

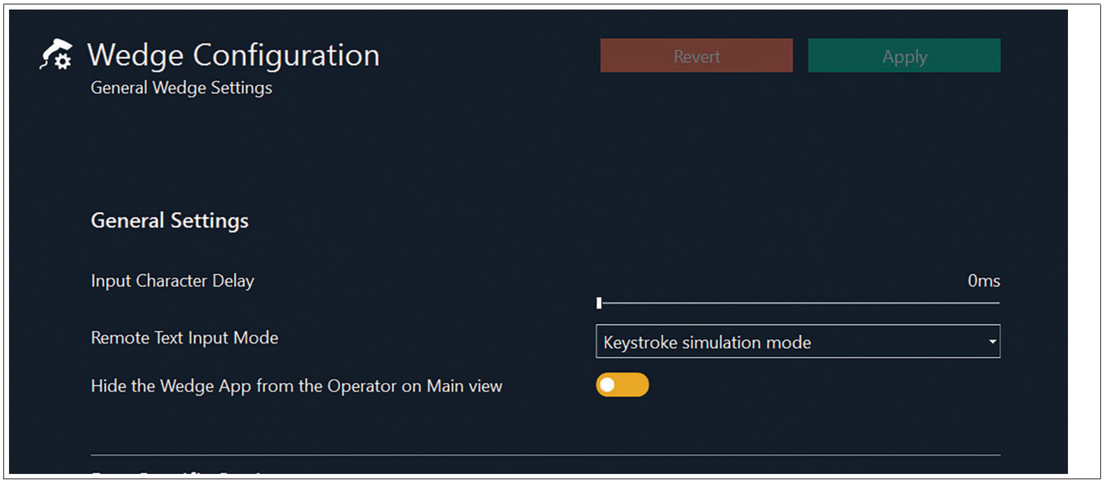
Subject	CN=RMShellServer, O=Pepperl-Fuchs
Issuer	CN=RMShellServer, O=Pepperl-Fuchs
Date	1/12/2053
Friendly Name	RMShell Certificate_wixCert_1

Figure 8.27 VisuNet CC Settings

8.15 Wedge Configuration

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.



Wedge Configuration
General Wedge Settings

General Settings

Input Character Delay 0ms

Remote Text Input Mode: Keystroke simulation mode

Hide the Wedge App from the Operator on Main view

Figure 8.28 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.

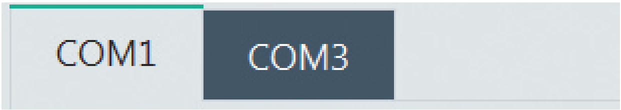


Figure 8.29 COM port selection (in this example COM1 is selected)

Test Connection

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

Testing the COM Port Connection

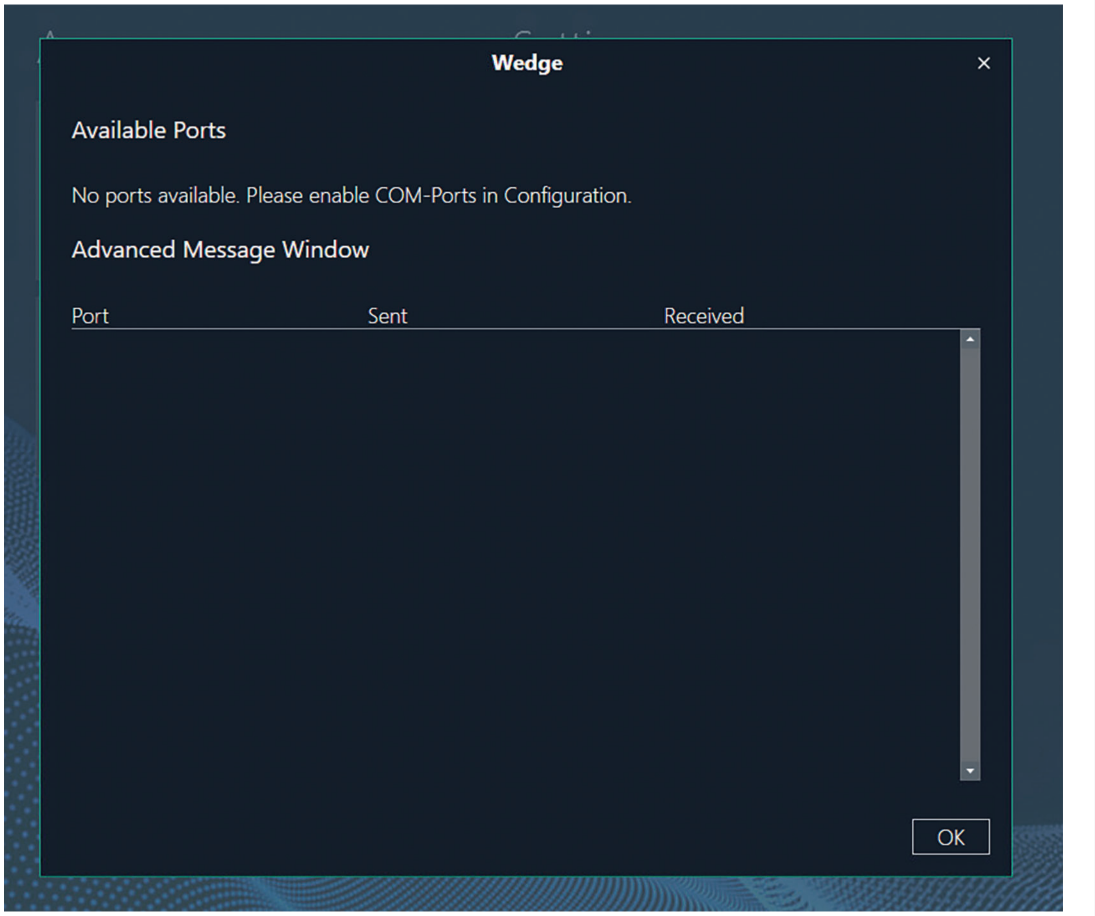
1. Choose the tab of the COM port that you want to test.
2. Click Test Barcode reader.

   ↳ 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.
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.



Wedge

Available Ports

No ports available. Please enable COM-Ports in Configuration.

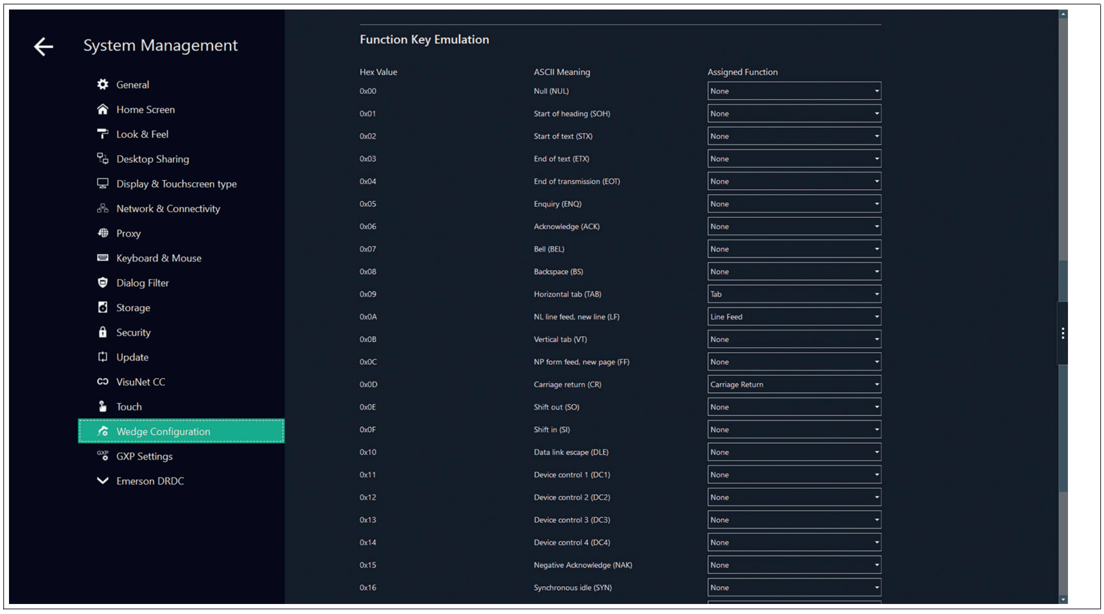
Advanced Message Window

Port	Sent	Received

Figure 8.30

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.



Function Key Emulation

Hex Value	ASCII Meaning	Assigned Function
0x00	Null (NUL)	None
0x01	Start of heading (SOH)	None
0x02	Start of text (STX)	None
0x03	End of text (ETX)	None
0x04	End of transmission (EOT)	None
0x05	Enquiry (ENQ)	None
0x06	Acknowledge (ACK)	None
0x07	Bell (BEL)	None
0x08	Backspace (BS)	None
0x09	Horizontal tab (TAB)	Tab
0x0A	NL line feed, new line (LF)	Line Feed
0x0B	Vertical tab (VT)	None
0x0C	NP form feed, new page (FF)	None
0x0D	Carriage return (CR)	Carriage Return
0x0E	Shift out (SO)	None
0x0F	Shift in (SI)	None
0x10	Data link escape (DLE)	None
0x11	Device control 1 (DC1)	None
0x12	Device control 2 (DC2)	None
0x13	Device control 3 (DC3)	None
0x14	Device control 4 (DC4)	None
0x15	Negative Acknowledge (NAK)	None
0x16	Synchronous idle (SYN)	None

Figure 8.31 Wedge configuration - Function Key Emulation

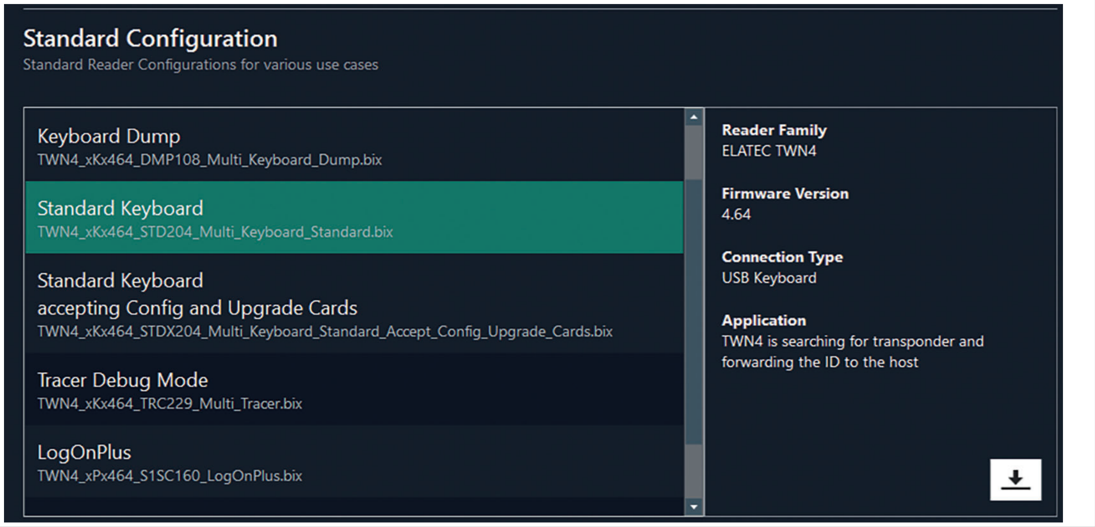
8.16 RFID Reader

Note

This additional configuration setting only appears if an ELATEC RFID reader is connected to the device.

To configure your connected RFID reader, the following options are possible:

1. Standard Configuration



Standard Configuration

Standard Reader Configurations for various use cases

Keyboard Dump
TWN4_xKx464_DMP108_Multi_Keyboard_Dump.bix

Standard Keyboard
TWN4_xKx464_STD204_Multi_Keyboard_Standard.bix

Standard Keyboard
accepting Config and Upgrade Cards
TWN4_xKx464_STDX204_Multi_Keyboard_Standard_Accept_Config_Upgrade_Cards.bix

Tracer Debug Mode
TWN4_xKx464_TRC229_Multi_Tracer.bix

LogOnPlus
TWN4_xPx464_S1SC160_LogOnPlus.bix

Reader Family
ELATEC TWN4

Firmware Version
4.64

Connection Type
USB Keyboard

Application
TWN4 is searching for transponder and forwarding the ID to the host

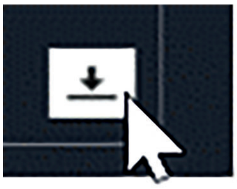
Figure 8.32

1. Select your suitable use case from the list and flash it. Get further information on the preconfigured use cases by clicking them.
   In general, there are three operating types the RFID reader can work in (HID Keyboard, virtual COM Port, Smartcard Reader).

   Note

   LogOn Plus default settings are shown in the VisuNet RM Shell. Select appropriate standard configuration.

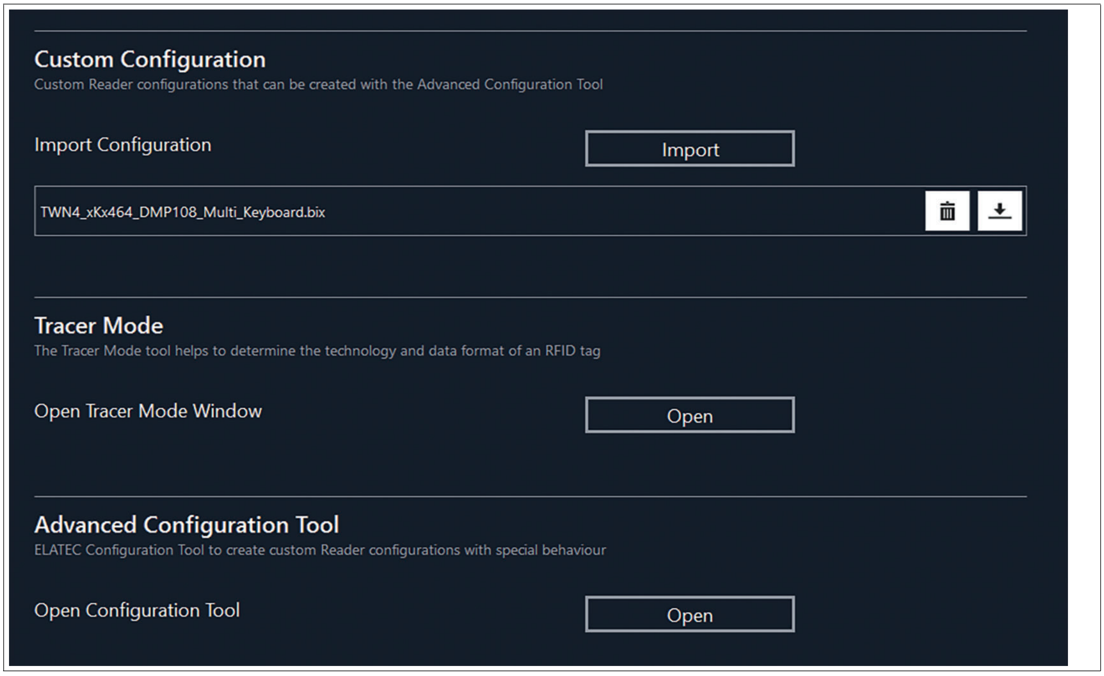
2. Click the flash button to flash the configuration to the Reader.



2. Custom Configuration

If the standard configurations are not suitable for your use-case, you can build your own configuration and import it in the VisuNet RM Shell. Either use the additional "Configuration Tool" below which has integrated configuration tools from ELATEC or redirect directly to the ELATEC website and use the tools on their website.

Please refer to the ELATEC website -> TWN4 Dev-Pack Overview



Custom Configuration
Custom Reader configurations that can be created with the Advanced Configuration Tool

Import Configuration

TWN4_xKx464_DMP108_Multi_Keyboard.bix

Tracer Mode
The Tracer Mode tool helps to determine the technology and data format of an RFID tag

Open Tracer Mode Window

Advanced Configuration Tool
ELATEC Configuration Tool to create custom Reader configurations with special behaviour

Open Configuration Tool

Figure 8.33

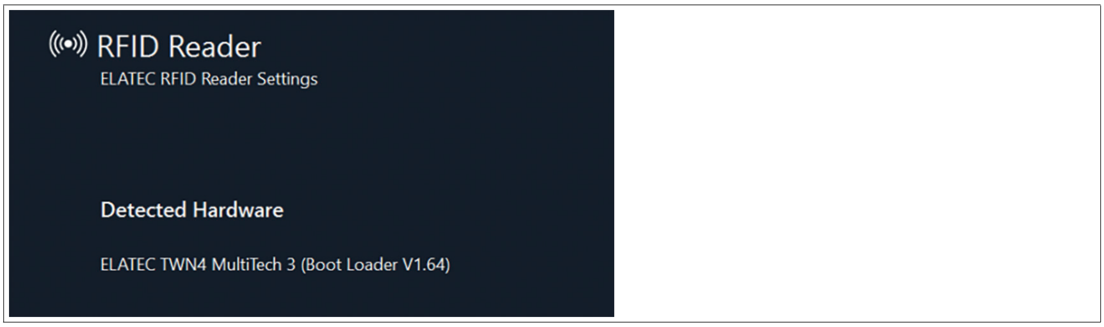
Note

Please find assistance regarding the individual configuration options directly at ELATEC.

Note

When using custom configurations, make sure the configuration is compatible to the detected Hardware. You can find info about compatibility in the ELATEC manual.

Get detailed information on the firmware version within the VisuNet RM Shell.



RFID Reader
ELATEC RFID Reader Settings

Detected Hardware

ELATEC TWN4 MultiTech 3 (Boot Loader V1.64)

Figure 8.34

Tracer Mode

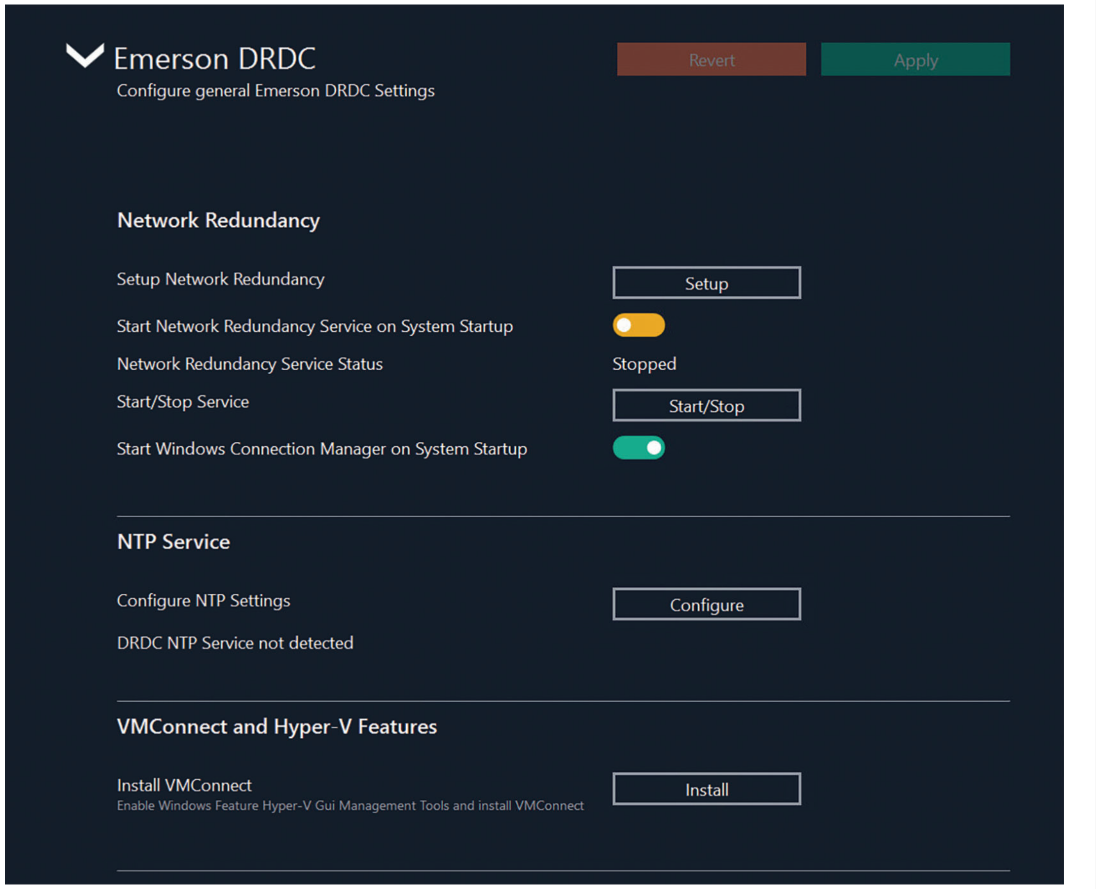
The Tracer Mode helps to determine the transponder technology that an RFID tag uses. Based on this information, custom configurations can be created.

8.17 Emerson DRDC

Note

Emerson DRDC requires a DRDC license.

Configure general Emerson DRDC Settings in this section.



Emerson DRDC

Configure general Emerson DRDC Settings

Network Redundancy

Setup Network Redundancy: Setup

Start Network Redundancy Service on System Startup: off

Network Redundancy Service Status: Stopped

Start/Stop Service: Start/Stop

Start Windows Connection Manager on System Startup: on

NTP Service

Configure NTP Settings: Configure

DRDC NTP Service not detected

VMConnect and Hyper-V Features

Install VMConnect: Install

Enable Windows Feature Hyper-V Gui Management Tools and install VMConnect

Figure 8.35 Emerson DRDC Settings

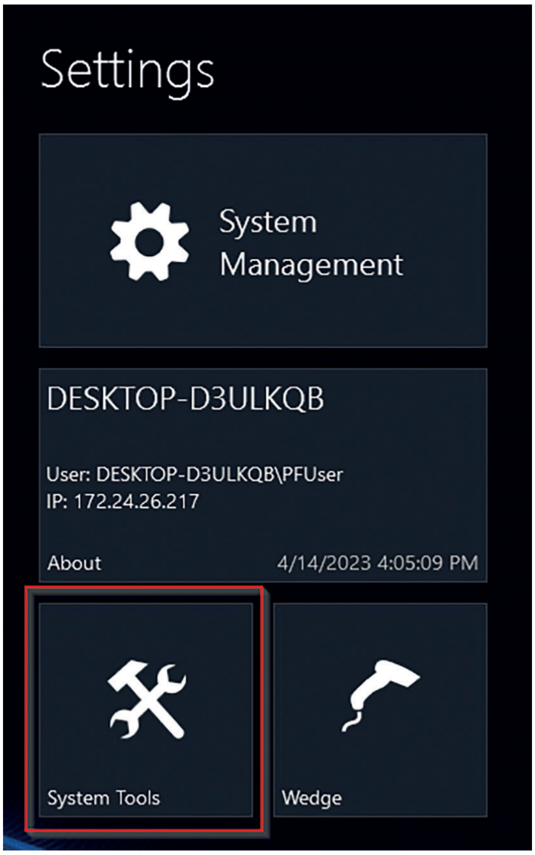
9 System Tools App

Note

It is possible to hide the System Tools App in the Operator mode via General Settings, see chapter 7.

Entering the System Tools App

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

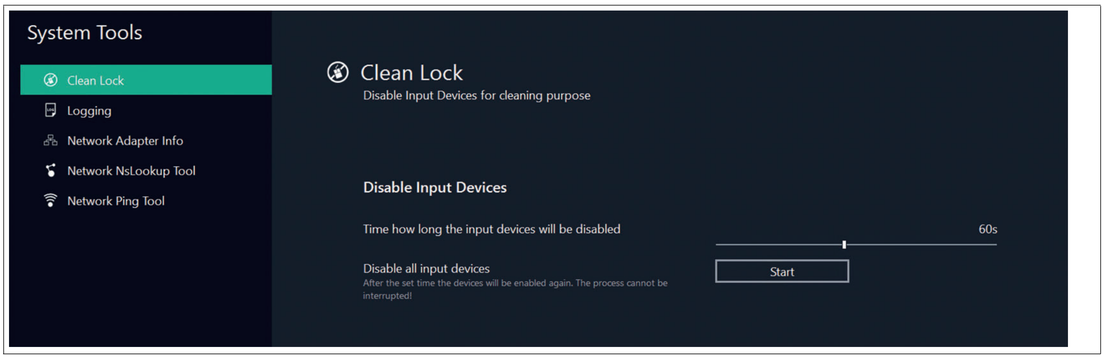


Settings

DESKTOP-D3ULKQB

User: DESKTOP-D3ULKQB\PFUser
IP: 172.24.26.217

About 4/14/2023 4:05:09 PM



Clean Lock
Disable Input Devices for cleaning purpose

Disable Input Devices

Time how long the input devices will be disabled 60s

Disable all input devices
After the set time the devices will be enabled again. The process cannot be interrupted!

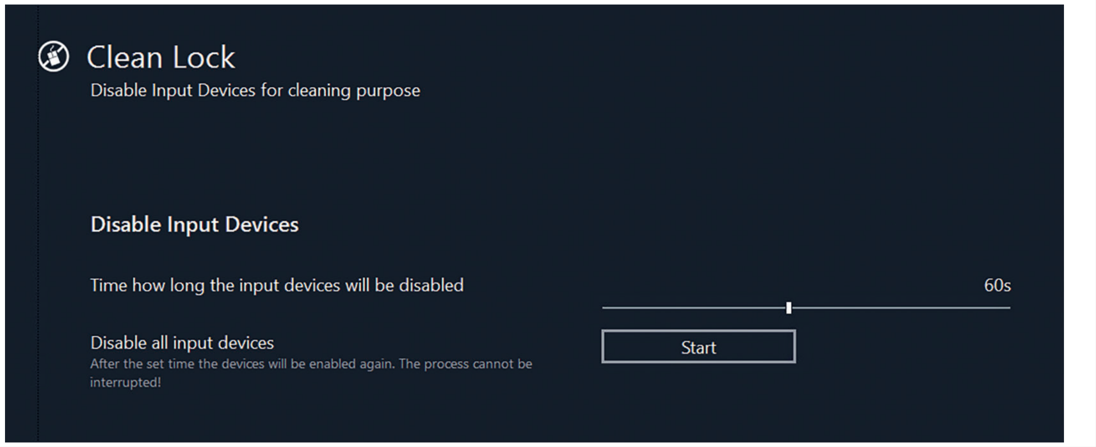
Figure 9.1 Overview

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.



Clean Lock
Disable Input Devices for cleaning purpose

Disable Input Devices

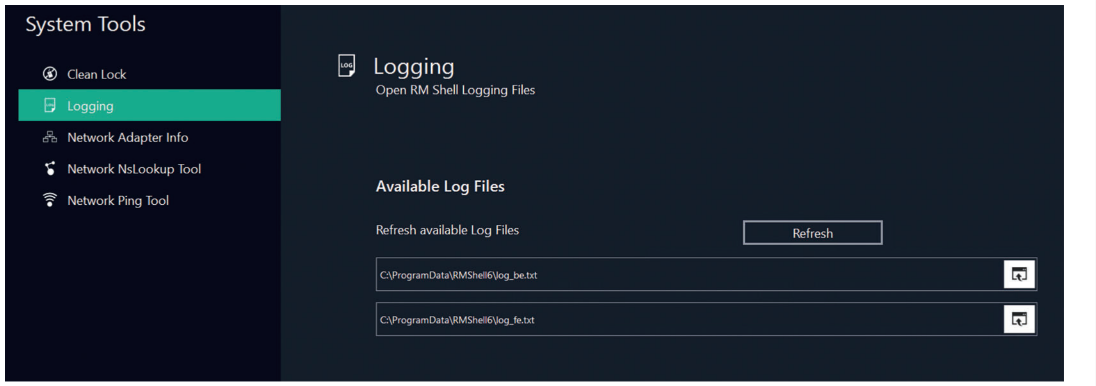
Time how long the input devices will be disabled: 60s

Disable all input devices
After the set time the devices will be enabled again. The process cannot be interrupted!

Figure 9.2 Clean Lock Settings

9.2 Logging

In the logging section of the System Tools, the RM Shell Logging Files can be accessed.



Logging
Open RM Shell Logging Files

Available Log Files

Refresh available Log Files

C:\ProgramData\RMShell6\log_be.txt

C:\ProgramData\RMShell6\log_fe.txt

Figure 9.3

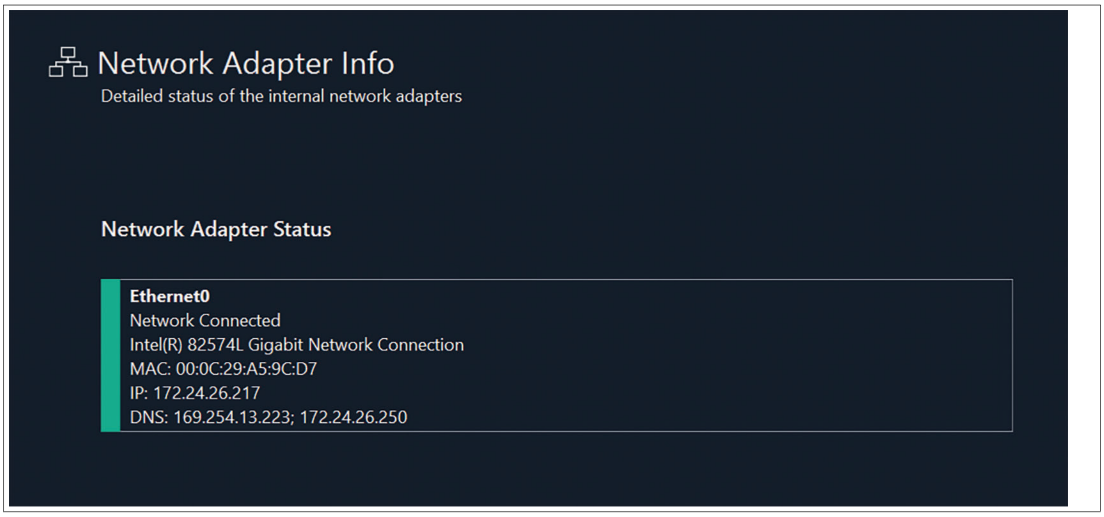
To refresh and update the log files, click on "Refresh". The Logging Files are used to record events or activities that occur within a computer system, application, or program. They present a detailed record of what has happened within the RM Shell. This information can be used for troubleshooting problems or investigating security incidents.

9.3 Network Adapter Info

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.



Network Adapter Info

Detailed status of the internal network adapters

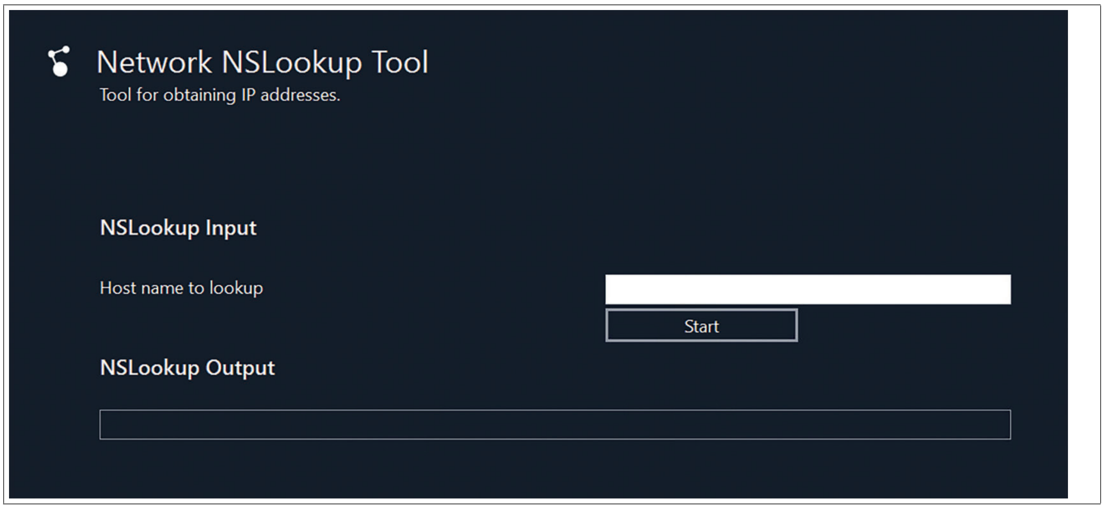
Network Adapter Status

Ethernet0
Network Connected
Intel(R) 82574L Gigabit Network Connection
MAC: 00:0C:29:A5:9C:D7
IP: 172.24.26.217
DNS: 169.254.13.223; 172.24.26.250

Figure 9.4 Network Adapter Info

9.4 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.



Network NSLookup Tool

Tool for obtaining IP addresses.

NSLookup Input

Host name to lookup

NSLookup Output

Figure 9.5 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."

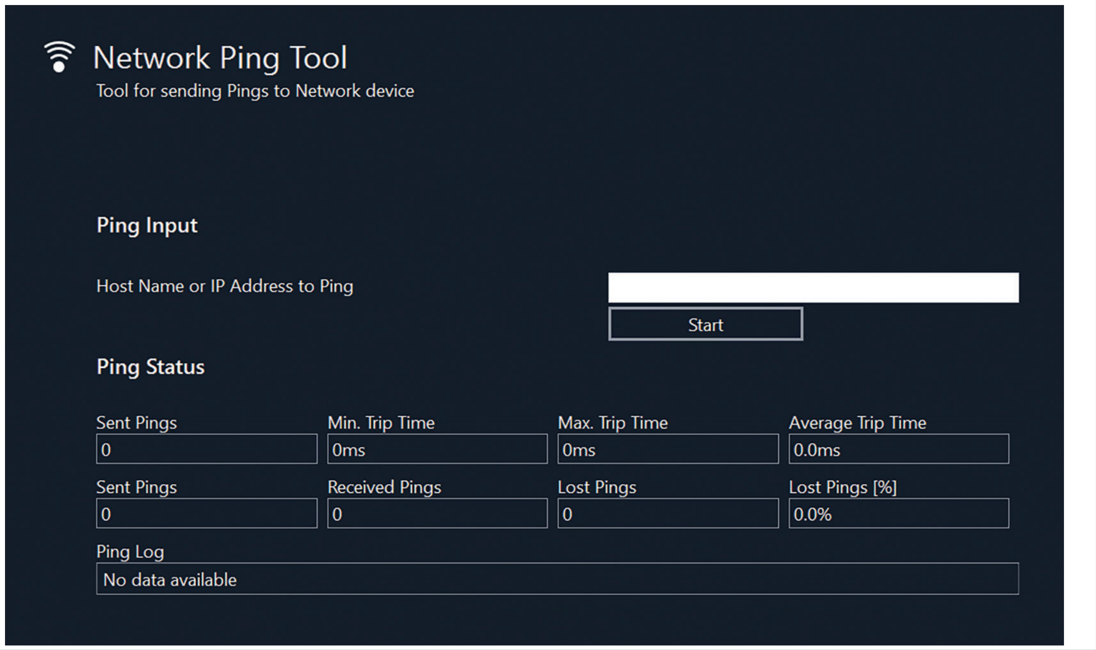
↳ The corresponding IP address is displayed in the "NSLookup Output" field.

9.5 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.



Network Ping Tool
Tool for sending Pings to Network device

Ping Input

Host Name or IP Address to Ping

Ping Status

Sent Pings	Min. Trip Time	Max. Trip Time	Average Trip Time
0	0ms	0ms	0.0ms

Sent Pings	Received Pings	Lost Pings	Lost Pings [%]
0	0	0	0.0%

Ping Log
No data available

Figure 9.6

10 Factory Reset

Note

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". Please keep this information handy for support cases.

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. Log in as an Administrator.
2. On the Home Screen, click on the Power Symbol in the upper right corner.
3. Click on "Reboot to Factory Reset".

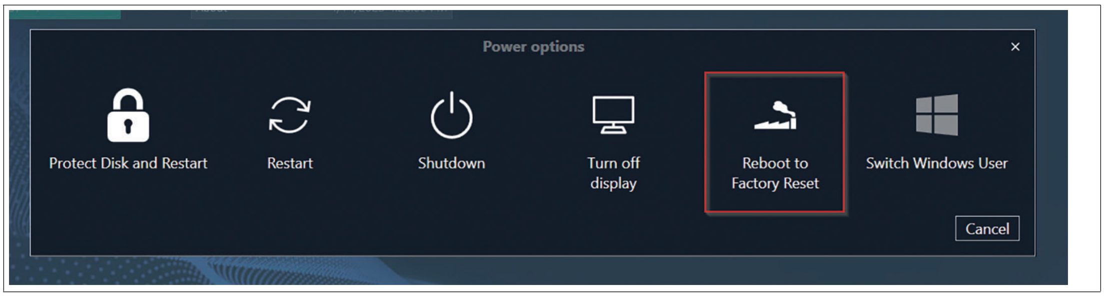
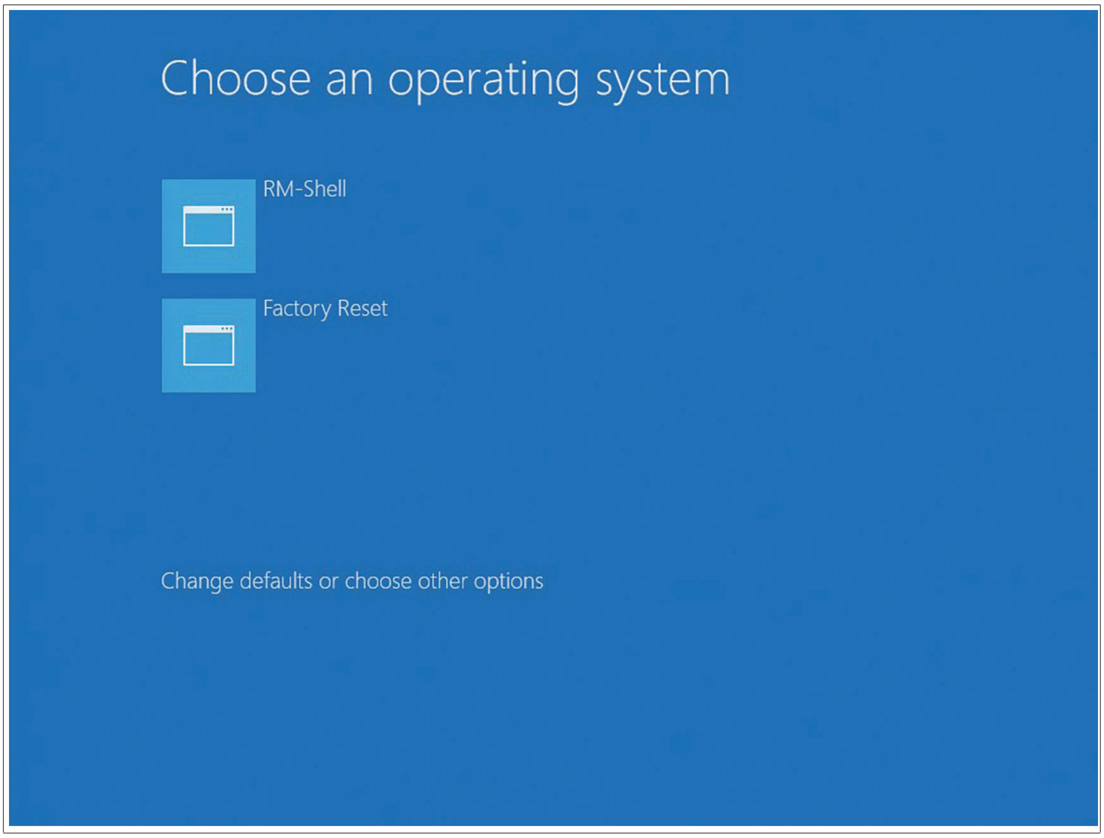


Figure 10.1

4. Click **Yes** to execute the Factory Reset.

Enter the Factory System when the RM Shell is crashed

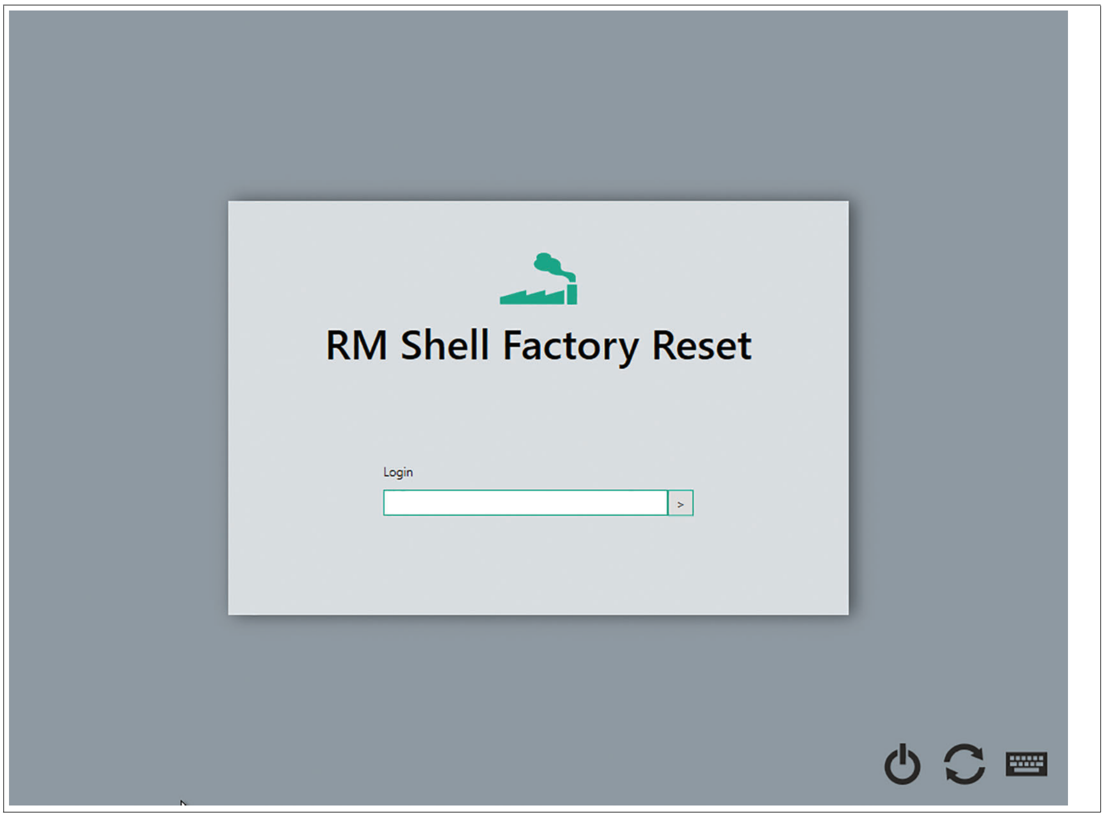
1. Power off the unit completely.
2. Power the unit back on. During the initial boot sequence, repeatedly press the "F9" key.
3. When you see a menu on a blue or black background, stop pressing the "F9" key.



Choose an operating system

Figure 10.2

Login in to the VisuNet RM Shell Factory Reset Management


RM Shell Factory Reset

Login

Figure 10.3

↳ Use the default Login password **VisuReset** to log in to the RM Factory Reset Management tool if you previously did not set a custom Factory Reset Password. You can use the "Recovery Mode" after entering an incorrect password. However, this only allows a reset to an original image provided by P+F.

Note

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

10.1 Introduction

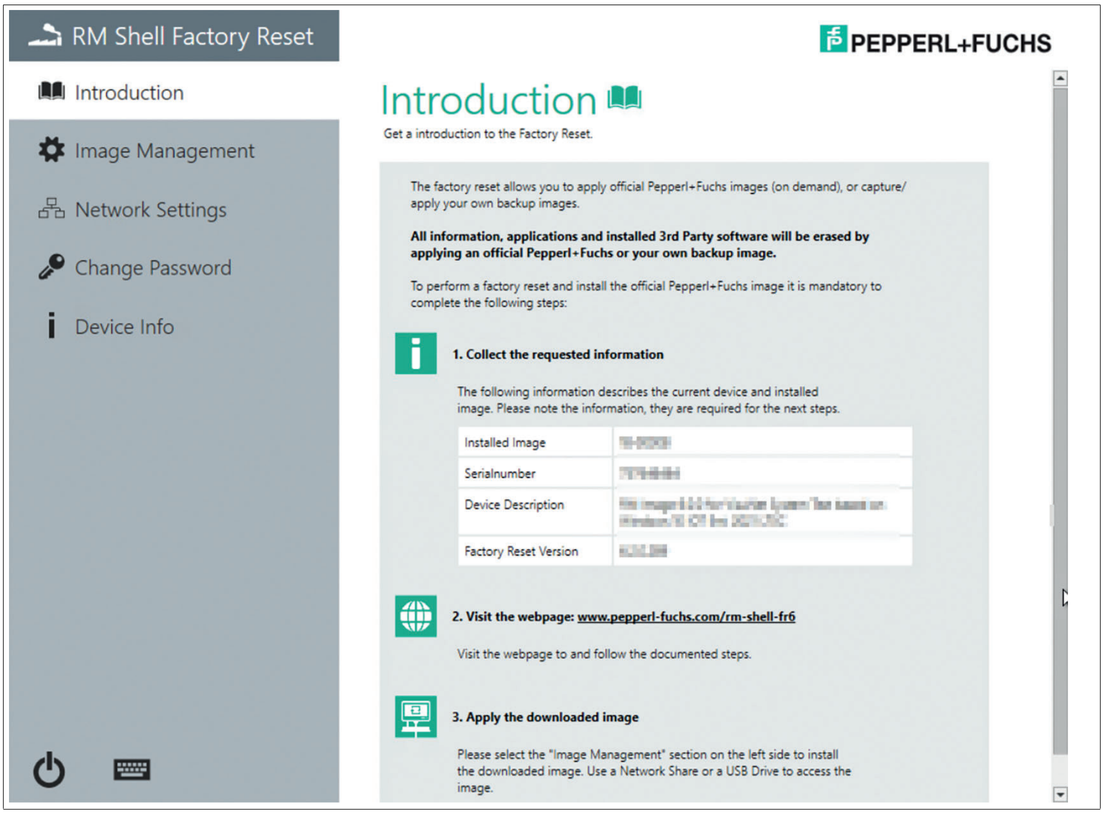
The section gives an overview of the Factory Reset. With the Factory Reset you can capture or apply (backup) images.

Overview

Note

All information, apps and installed 3rd party sortware will be erased by applying an official Pepperl+Fuchs or your own backup image. As described in the introductory section, you have to perform the following steps to complete the factory reset.

1. Collect the requested information. The table shown in the introduction section lists the information required for the next steps. Please note the information.
2. Visit the Pepperl+Fuchs Website (www.pepperl-fuchs.com/rm-shell-fr6) Follow the steps on the website.
3. Apply the downloaded image. The downloaded image can be applied via the "Image Management" section. The image can be accessed via a network share or a USB Drive.



Introduction

Get a introduction to the Factory Reset.

The factory reset allows you to apply official Pepperl+Fuchs images (on demand), or capture/ apply your own backup images.

All information, applications and installed 3rd Party software will be erased by applying an official Pepperl+Fuchs or your own backup image.

To perform a factory reset and install the official Pepperl+Fuchs image it is mandatory to complete the following steps:

1. Collect the requested information

The following information describes the current device and installed image. Please note the information, they are required for the next steps.

Installed Image	[redacted]
Serialnumber	[redacted]
Device Description	[redacted]
Factory Reset Version	[redacted]

2. Visit the webpage: www.pepperl-fuchs.com/rm-shell-fr6

Visit the webpage to and follow the documented steps.

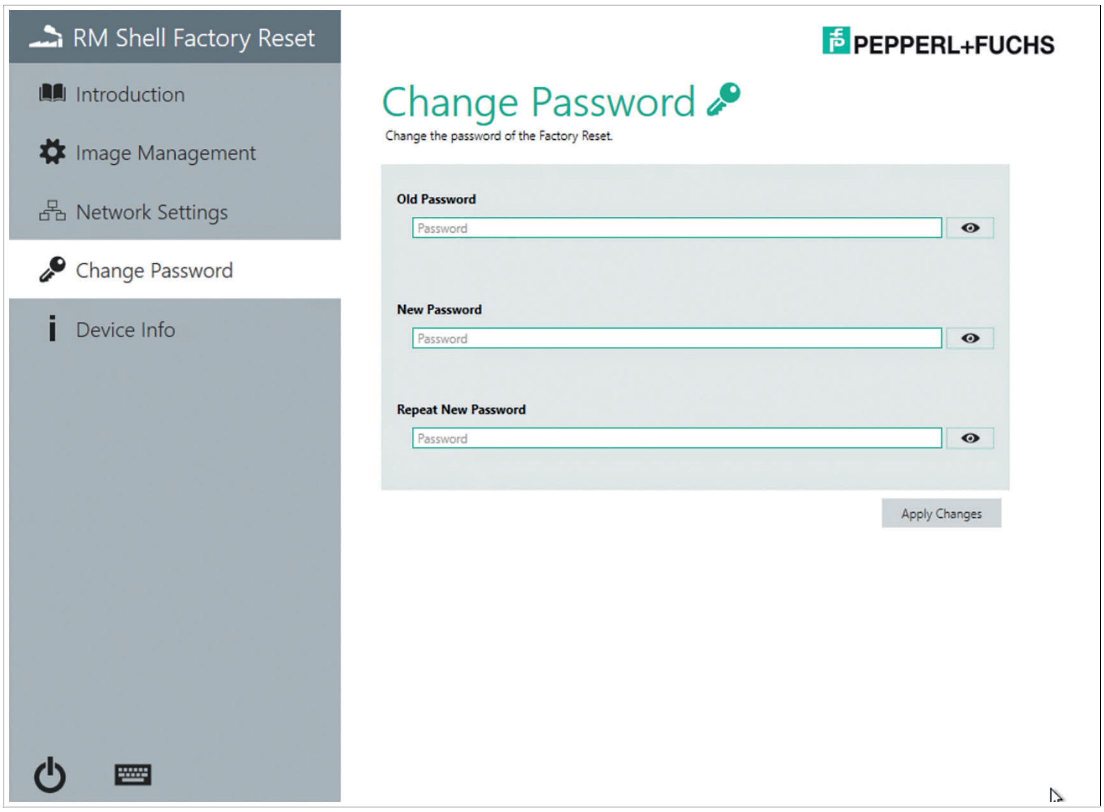
3. Apply the downloaded image

Please select the "Image Management" section on the left side to install the downloaded image. Use a Network Share or a USB Drive to access the image.

Figure 10.4

10.2 Change Password

Change the default login password.



RM Shell Factory Reset

Change Password

Change the password of the Factory Reset.

Old Password: Password

New Password: Password

Repeat New Password: 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.

10.3 Image File Management

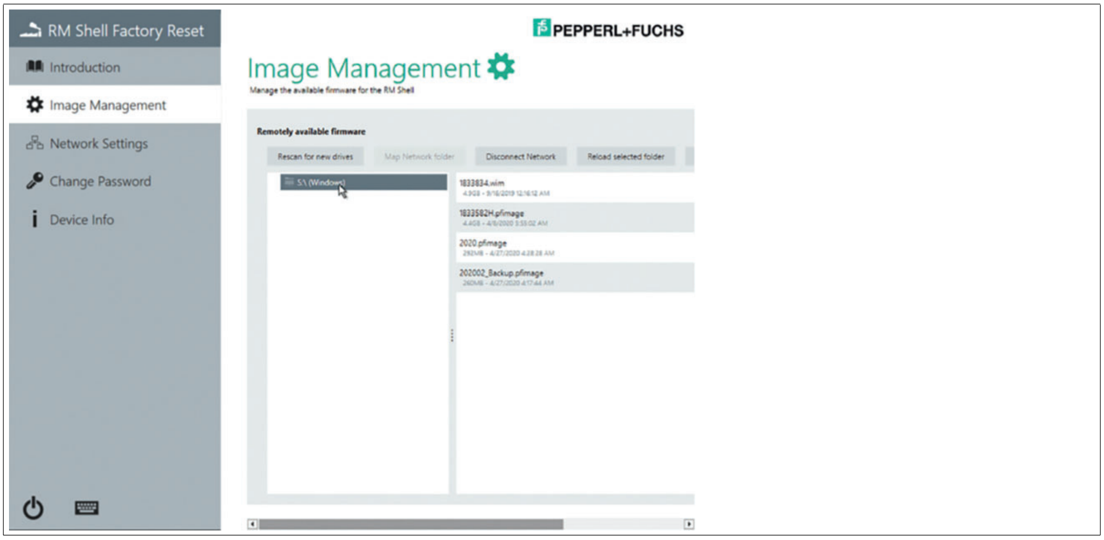


Figure 10.6

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

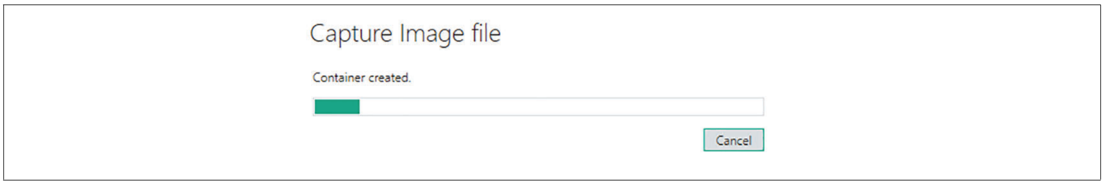
Rescan for new drives	Searches for connected USB flash memory drives. USB flash-drives can directly be used to transfer image files.
Map Network folder	To apply or capture an image file, select the network folder first. The image file is either applied on the RM/BTC from which the network is connected 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. **Caution!** This backup can only be applied to the same device/device with the same serial number. Control Center also provides the option of creating clone images that can also be installed on other systems. **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 Network Share has enough storage. The capture process takes about 30 minutes, depending on the network speed.

Note

Regarding the available image files see chapter 3.3.

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.



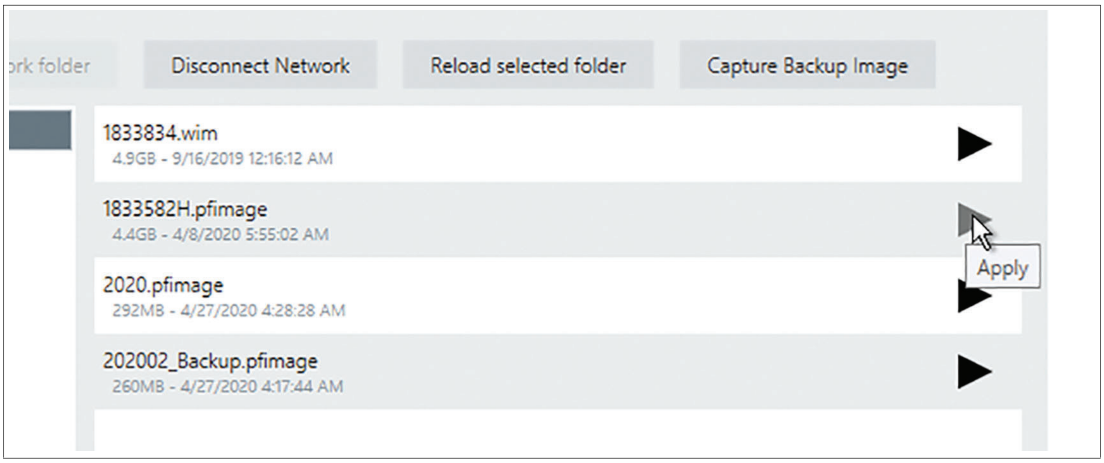
Capture Image file

Container created.

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.



1833834.wim
4.9GB - 9/16/2019 12:16:12 AM

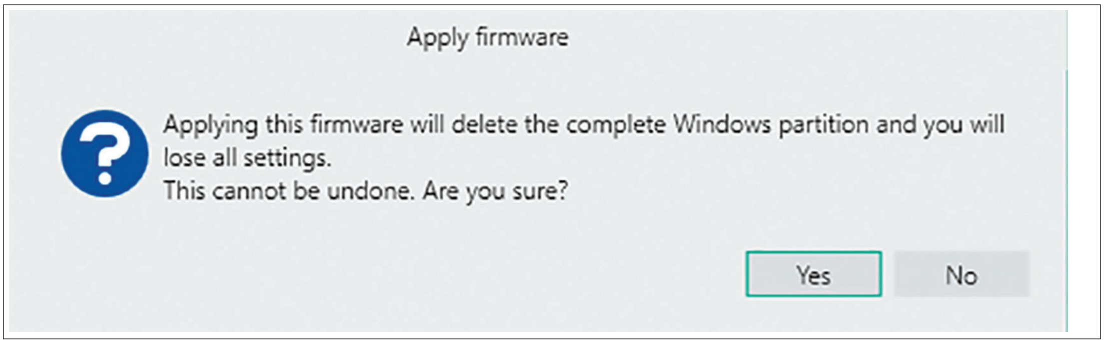
1833582H.pfimage
4.4GB - 4/8/2020 5:55:02 AM

2020.pfimage
292MB - 4/27/2020 4:28:28 AM

202002_Backup.pfimage
260MB - 4/27/2020 4:17:44 AM

Figure 10.8

3. Click Apply to apply the selected firmware.



Apply firmware

Applying this firmware will delete the complete Windows partition and you will lose all settings.
This cannot be undone. Are you sure?

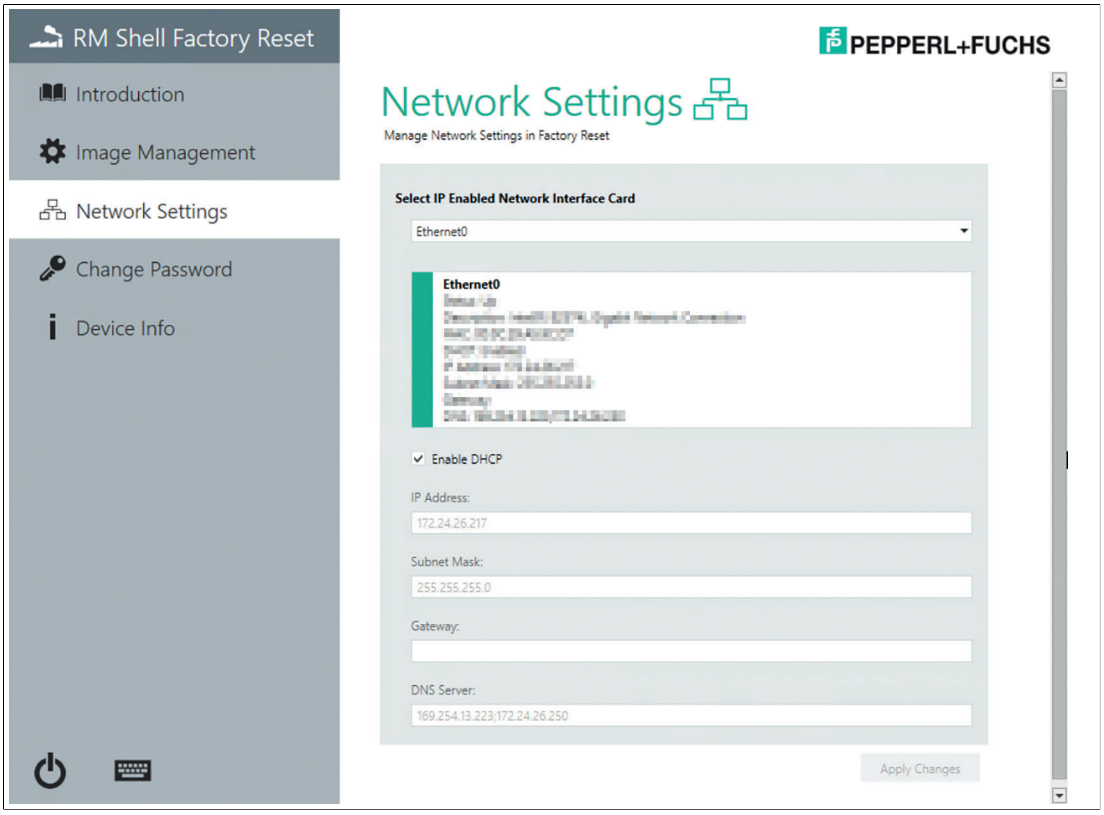
Figure 10.9

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.

10.4 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.



Network Settings

Manage Network Settings in Factory Reset

Select IP Enabled Network Interface Card

Ethernet0

Ethernet0
[redacted]

☑ Enable DHCP

IP Address: 172.24.26.217

Subnet Mask: 255.255.255.0

Gateway:

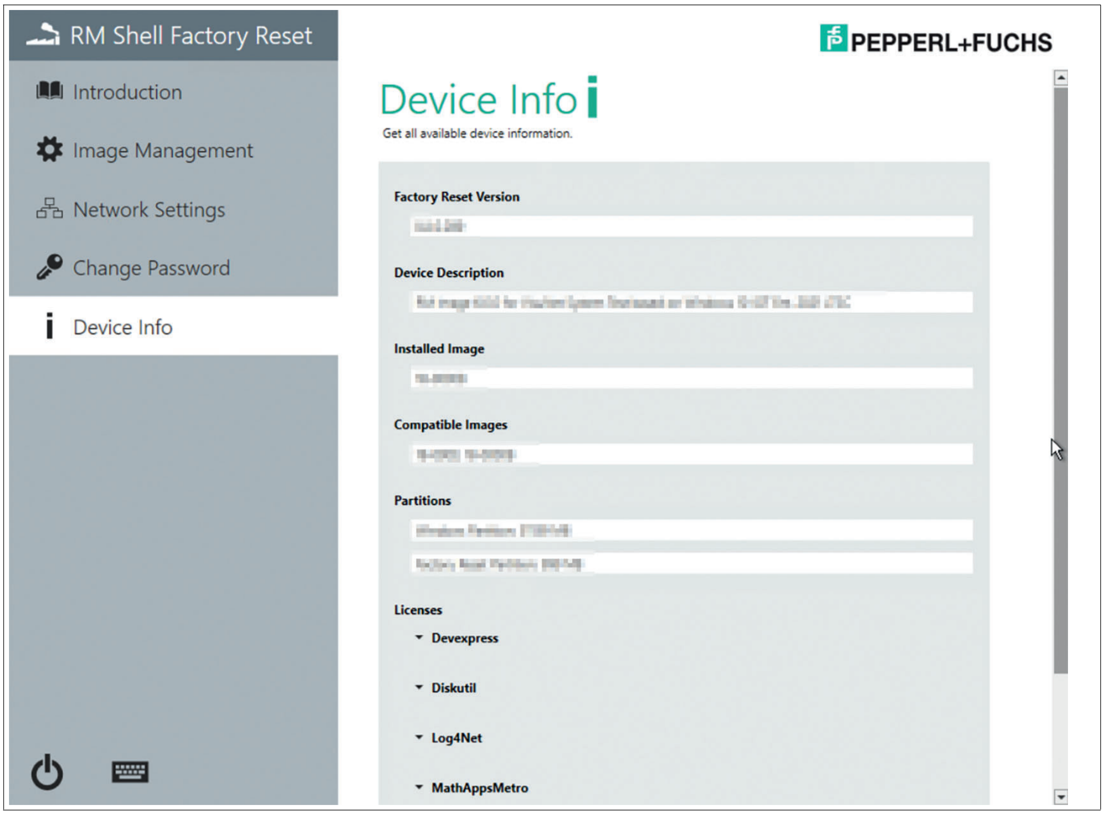
DNS Server: 169.254.13.223;172.24.26.250

Figure 10.10

10.5 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.



Device Info

Get all available device information.

Factory Reset Version

Device Description

Installed Image

Compatible Images

Partitions

Licenses

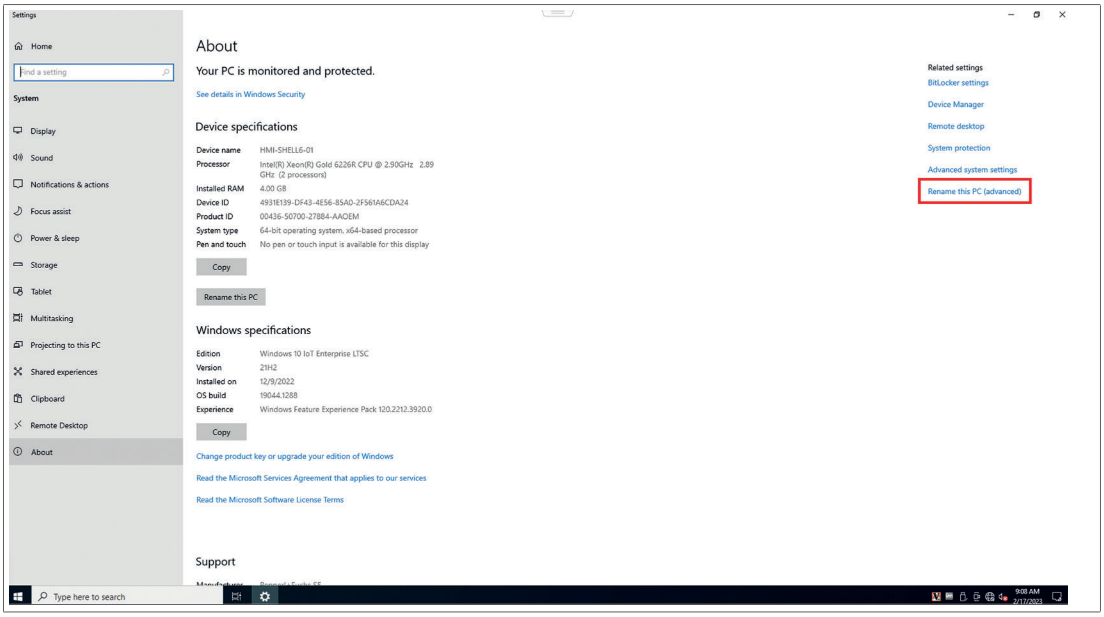
- Devexpress
- Diskutil
- Log4Net
- MathAppsMetro

Figure 10.11

11 How-Tos

11.1 How to join a domain

1. Within the Shell, switch from Operator to Configuration View.
2. In the Configuration View, click on the Power Button -> Switch User.
3. Login as PFAdmin or with an another Administrator Account.
4. Once on Windows desktop, open **Settings** -> **About**.
5. Click **Rename this PC (Advanced)**.



About

Your PC is monitored and protected.

See details in Windows Security

Device specifications

Device name HMI-SHELL6-01
Processor Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz 2.89 GHz (2 processors)
Installed RAM 4.00 GB
Device ID 4931E139-DF43-4E56-85A0-2F561A6CDA24
Product ID 00436-50700-27884-AAOEM
System type 64-bit operating system, x64-based processor
Pen and touch No pen or touch input is available for this display

Windows specifications

Edition Windows 10 IoT Enterprise LTSC
Version 21H2
Installed on 12/9/2022
OS build 19044.1288
Experience Windows Feature Experience Pack 120.2212.3920.0

Change product key or upgrade your edition of Windows

Read the Microsoft Services Agreement that applies to our services

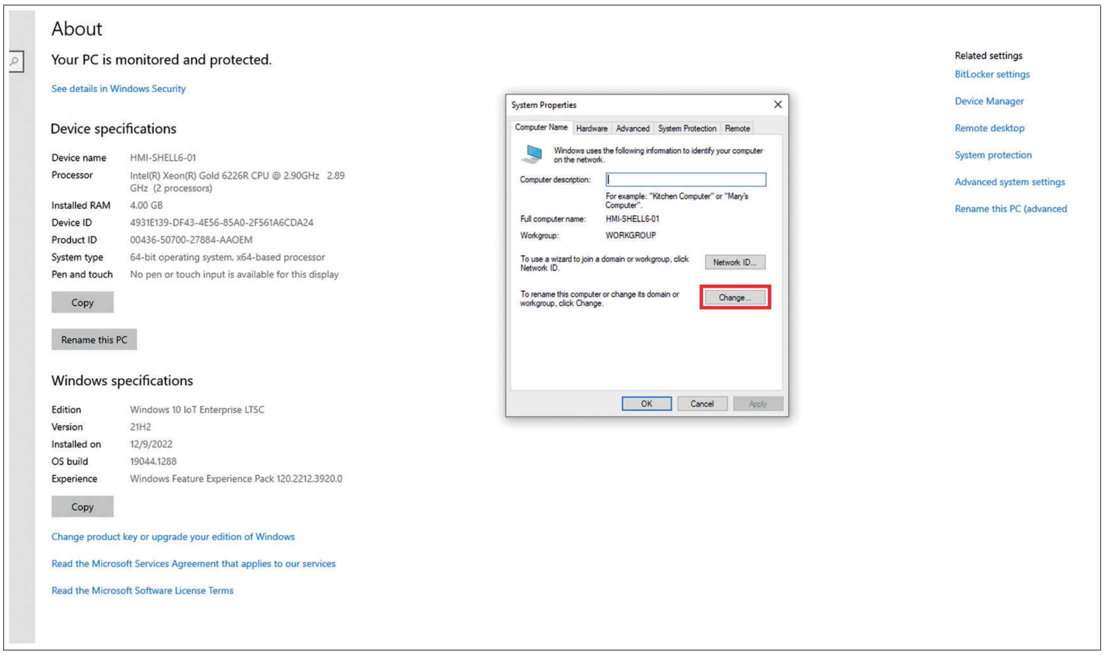
Read the Microsoft Software License Terms

Support

Manufacturer Pepperl+Fuchs SE

Figure 11.1

6. Click **Change**



About

Your PC is monitored and protected.

See details in Windows Security

Device specifications

Device name	HMI-SHELL6-01
Processor	Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz 2.89 GHz (2 processors)
Installed RAM	4.00 GB
Device ID	4931E139-DF43-4E56-85A0-2F561A6CDA24
Product ID	00436-50700-27884-AAOEM
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Windows specifications

Edition	Windows 10 IoT Enterprise LTSC
Version	21H2
Installed on	12/9/2022
OS build	19044.1288
Experience	Windows Feature Experience Pack 120.2212.3920.0

Change product key or upgrade your edition of Windows

Read the Microsoft Services Agreement that applies to our services

Read the Microsoft Software License Terms

System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: HMI-SHELL6-01

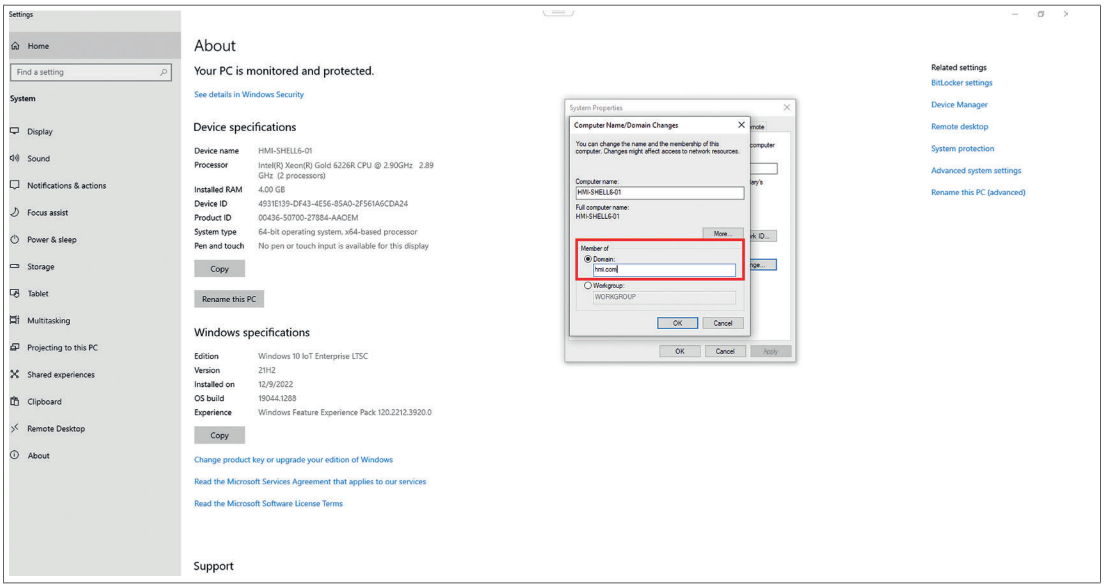
Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Figure 11.2

7. Click **Domain** and enter the domain you would like to join. In this example, the domain is hmi.com



About

Your PC is monitored and protected.

See details in Windows Security

Device specifications

Device name	HMI-SHELL6-01
Processor	Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz 2.89 GHz (2 processors)
Installed RAM	4.00 GB
Device ID	4931E139-DF43-4E56-85A0-2F561A6CDA24
Product ID	00436-50700-27884-AAOEM
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Windows specifications

Edition	Windows 10 IoT Enterprise LTSC
Version	21H2
Installed on	12/9/2022
OS build	19044.1288
Experience	Windows Feature Experience Pack 120.2212.3920.0

Change product key or upgrade your edition of Windows

Read the Microsoft Services Agreement that applies to our services

Read the Microsoft Software License Terms

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: HMI-SHELL6-01

Full computer name: HMI-SHELL6-01

Member of

● Domain: hmi.com

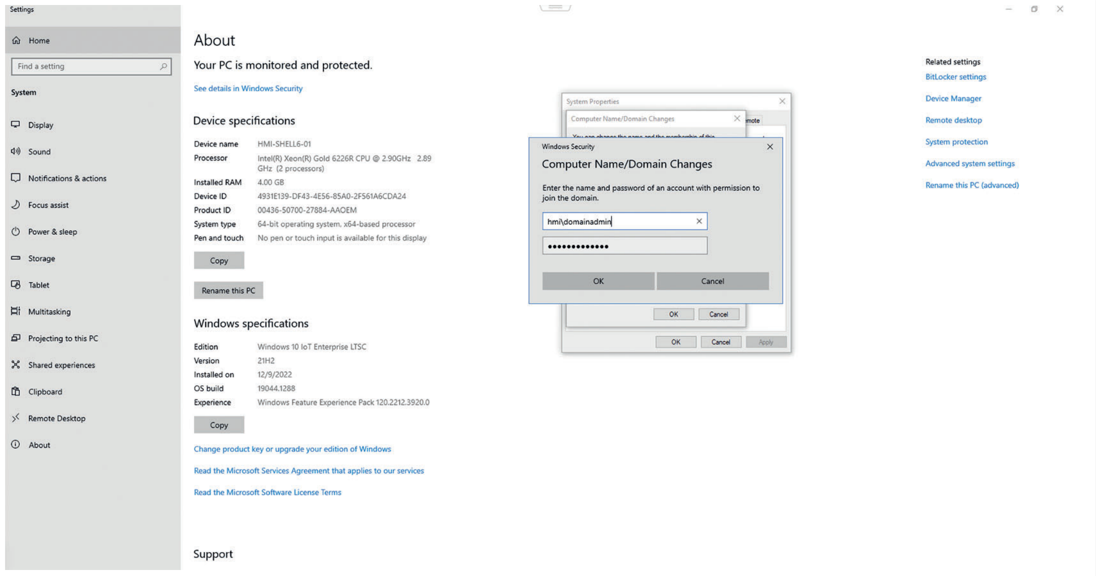
○ Workgroup: WORKGROUP

Figure 11.3

Note

Please note the keyboard settings. Set the keyboard language layout to the corresponding layout on your physical keyboard or use the On-Screen Keyboard. Otherwise they might not match. For example, to enter a backslash on an US keyboard layout with a physical European keyboard, you need to press <.

8. Enter the Computer name.



About

Your PC is monitored and protected.

See details in Windows Security

Device specifications

Device name	HMI-SHELL6-01
Processor	Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz 2.89 GHz (2 processors)
Installed RAM	4.00 GB
Device ID	4931E139-DF43-4E56-85A0-2F561A6CDA24
Product ID	00436-50700-27884-AAOEM
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Windows specifications

Edition	Windows 10 IoT Enterprise LTSC
Version	21H2
Installed on	12/9/2022
OS build	19044.1288
Experience	Windows Feature Experience Pack 120.2212.3920.0

Change product key or upgrade your edition of Windows

Read the Microsoft Services Agreement that applies to our services

Read the Microsoft Software License Terms

Windows Security

Computer Name/Domain Changes

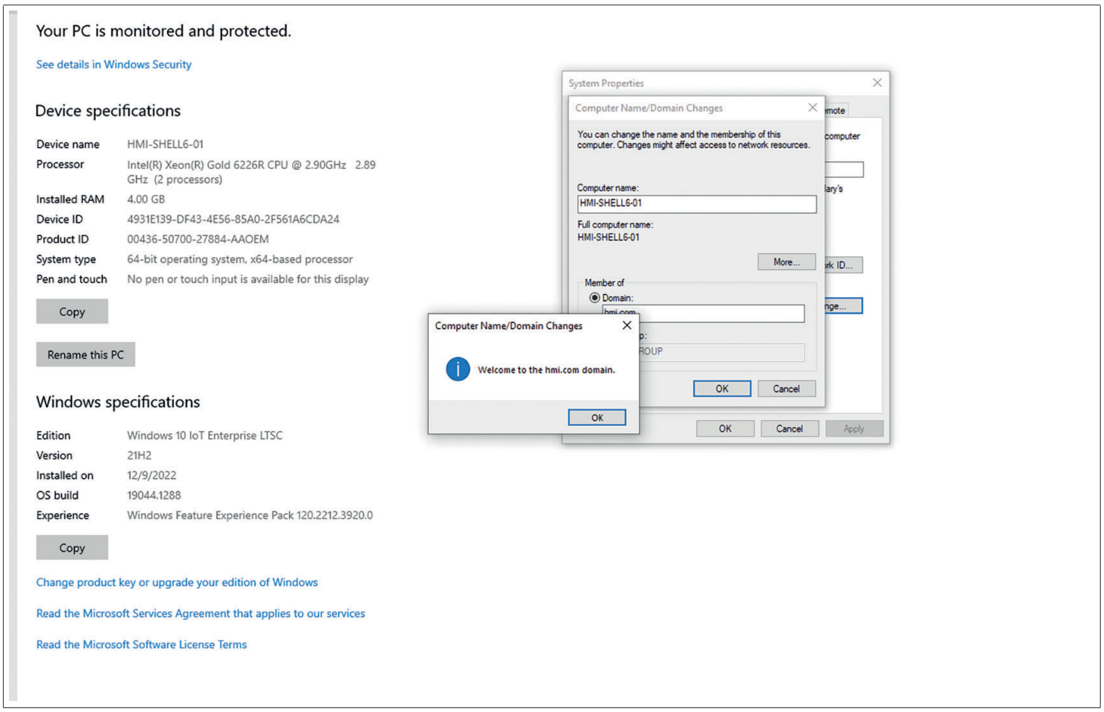
Enter the name and password of an account with permission to join the domain.

hmi\domainadmin

••••••••••••••

Figure 11.4

9. In this example, the domain is now set to hmi.com



Your PC is monitored and protected.

See details in Windows Security

Device specifications

Device name	HMI-SHELL6-01
Processor	Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz 2.89 GHz (2 processors)
Installed RAM	4.00 GB
Device ID	4931E139-DF43-4E56-85A0-2F561A6CDA24
Product ID	00436-50700-27884-AAOEM
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Windows specifications

Edition	Windows 10 IoT Enterprise LTSC
Version	21H2
Installed on	12/9/2022
OS build	19044.1288
Experience	Windows Feature Experience Pack 120.2212.3920.0

Change product key or upgrade your edition of Windows

Read the Microsoft Services Agreement that applies to our services

Read the Microsoft Software License Terms

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
HMI-SHELL6-01

Full computer name:
HMI-SHELL6-01

Member of
● Domain:
hmi.com

Computer Name/Domain Changes

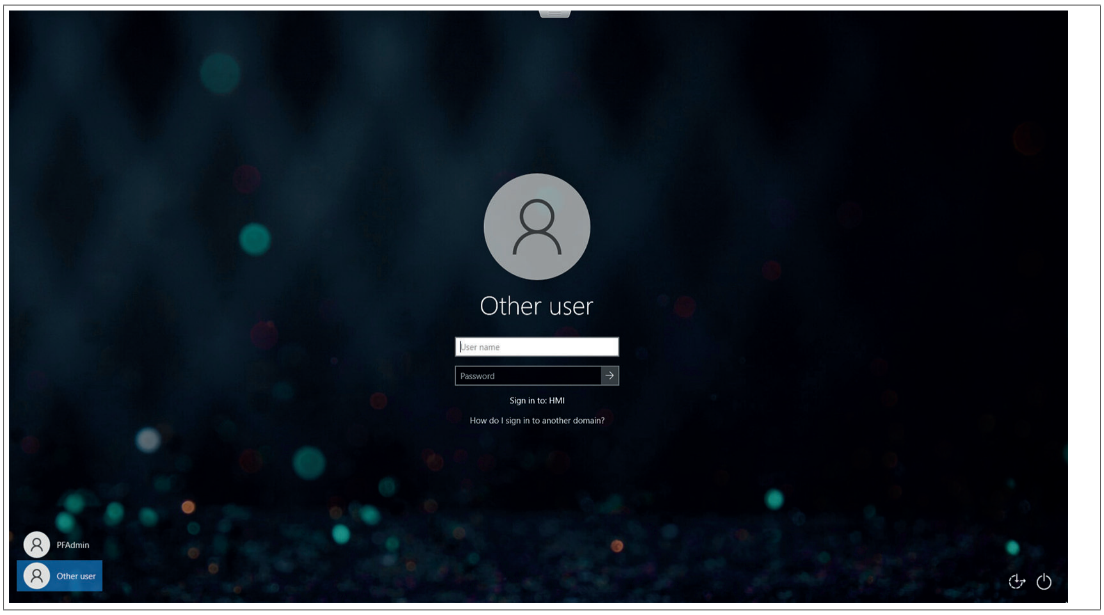
Welcome to the hmi.com domain.

Figure 11.5

10. Close all Windows with **Okay** and restart the system.

11. After restart, select RM Shell.

12. Click on **Other User**.



Other user

User name

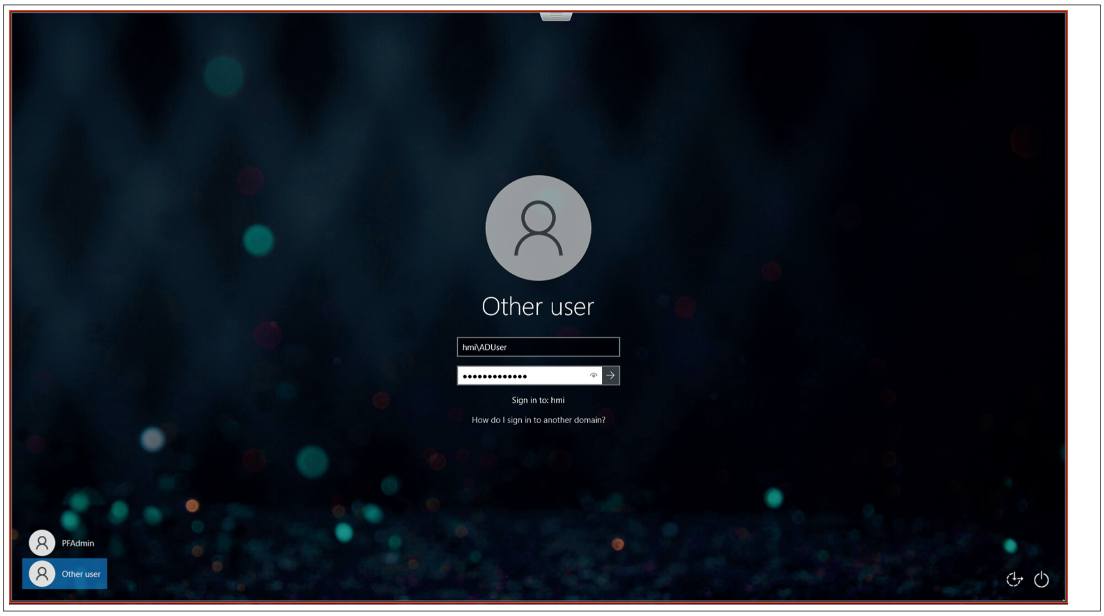
Password

Sign in to: HMI

How do I sign in to another domain?

Figure 11.6

13. Sign in with the domain followed by a backslash and the Username. In this example, this would be **hmi\ADUser.** Enter the password of the corresponding user.



Other user

hmi\ADUser

•••••••••••••

Sign in to: hmi

How do I sign in to another domain?

Figure 11.7

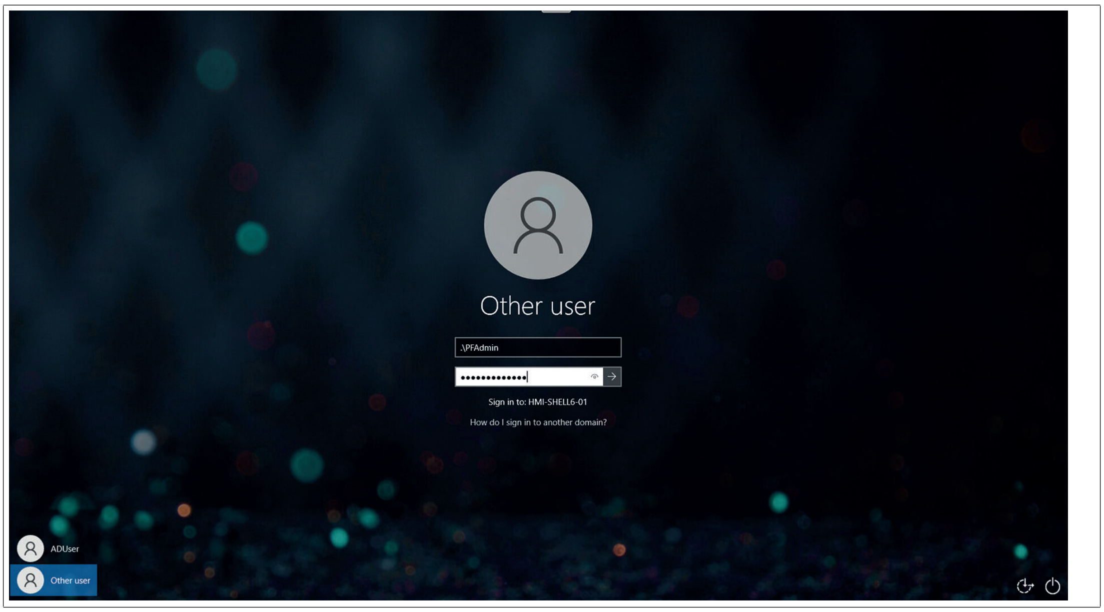
↳You have now joined the domain.

11.2 How to add a Domain Admin to an Administrator Group

With the RM Shell, it is possible to add a domain admin to an admin group. This also includes adding additional administrators in general. This allows the admin to open the configuration view of the RM Shell with a Microsoft Active Directory admin (AD Admin). To add a domain admin perform the following steps:

Procedure

1. Get to the Windows desktop by logging in as PFAdmin.



Other user

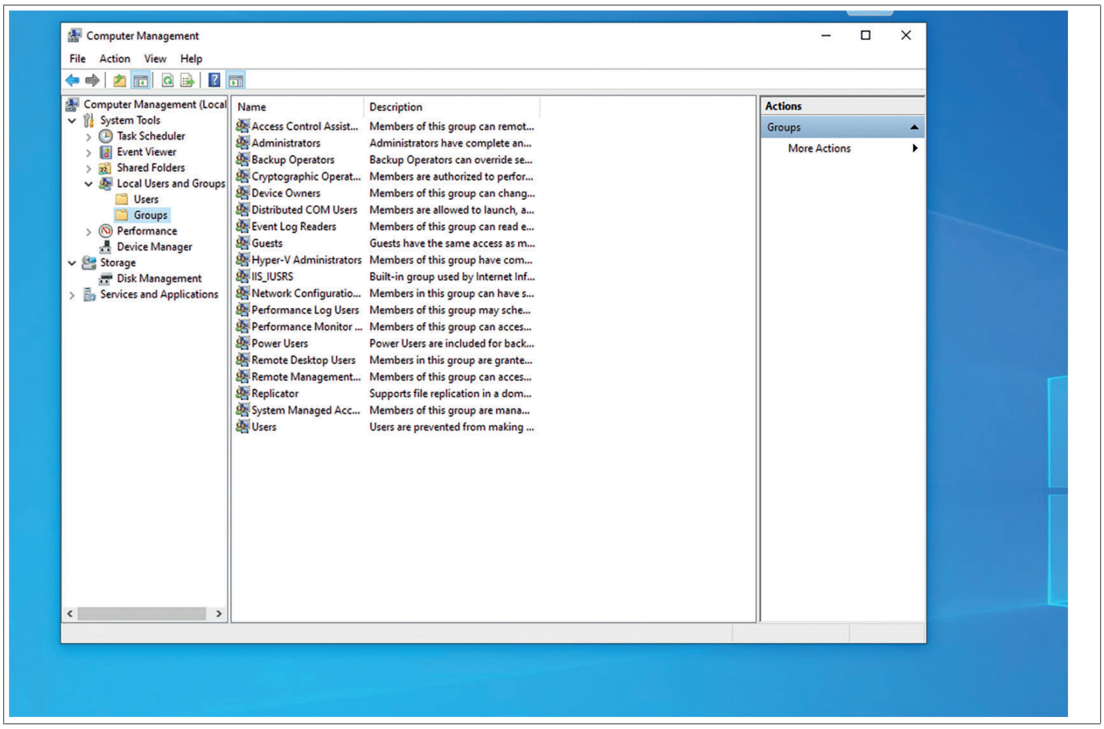
.\PFAdmin

Sign in to: HMI-SHELL6-01

How do I sign in to another domain?

Figure 11.8

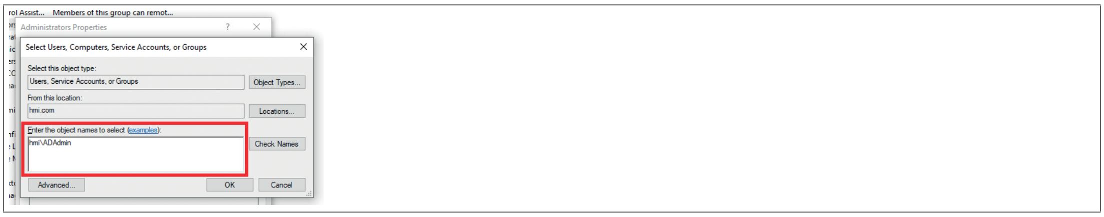
2. Right click on Windows symbol in left bottom corner.
3. Open **Computer Management**.
4. Click **Local Users and Groups** -> **Groups**.



Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Remote Management...	Members of this group can acces...
Replicator	Supports file replication in a dom...
System Managed Acc...	Members of this group are mana...
Users	Users are prevented from making ...

Figure 11.9

5. Open **Administrators**.
6. Enter the domain followed by a backslash and the Admin name (in this case **hmi\ADAdmin)** as the object name.


Administrators Properties
Select Users, Computers, Service Accounts, or Groups
Object Types...
Locations...
Check Names
Advanced...
OK
Cancel

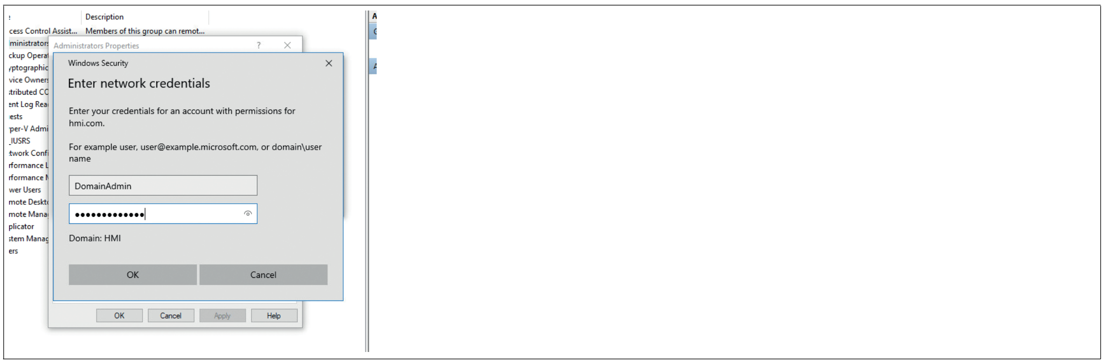
Select this object type: Users, Service Accounts, or Groups

From this location: hmi.com

Enter the object names to select (examples): hmi\ADAdmin

Figure 11.10

7. Click **OK**.
8. Enter the network credentials.



Enter network credentials

Enter your credentials for an account with permissions for hmi.com.

For example user, user@example.microsoft.com, or domain\user name

DomainAdmin

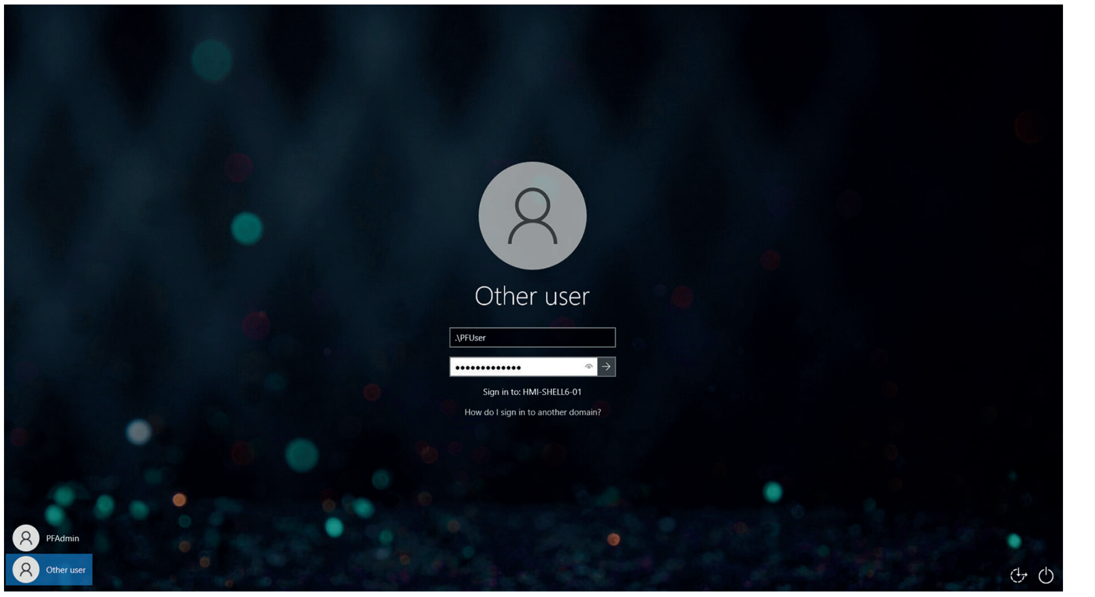
•••••••••••••

Domain: HMI

Figure 11.11

9. Click **OK**.
10. INFO: The newly added administrator gets displayed.
11. Click **OK**.

12. Go back to **PFUser**.



Other user

.\PFUser

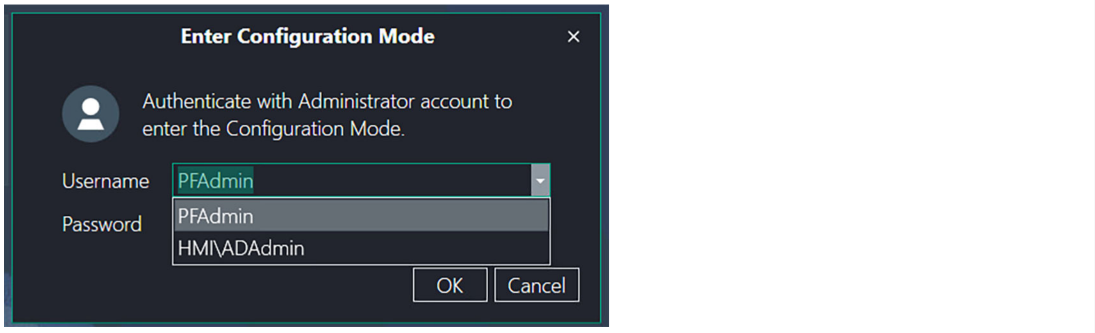
Sign in to: HMI-SHELL6-01

How do I sign in to another domain?

Figure 11.12

13. Sign in with the corresponding credentials (in this example **.\PFUser)**.

↳You have now joined the domain. Users from the domain can now log in to the Shell just as Shell Admins.



Enter Configuration Mode

Authenticate with Administrator account to enter the Configuration Mode.

Username: PFAdmin

Password

PFAdmin
HMI\ADAdmin

Figure 11.13

11.3 Connecting an RM / BTC with a Host PC via RDP

Note

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

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 direct connection, 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:

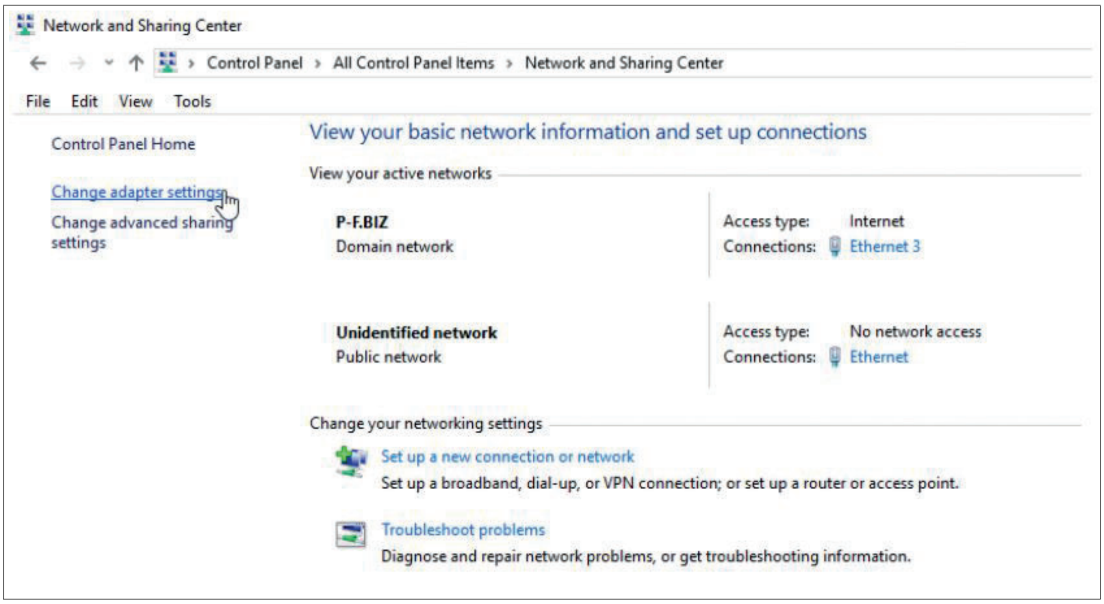
- Step 1: PC Configuration
  - Manual assignment of the IP address
  - Activation of the RDP Server Function
- Step 2: RM / BTC Configuration
  - Manual assignment of the IP address
  - Creation of an RDP profile

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.



Network and Sharing Center

Control Panel > All Control Panel Items > Network and Sharing Center
File Edit View Tools
Control Panel Home
Change adapter settings
Change advanced sharing settings

View your basic network information and set up connections

View your active networks

P-F.BIZ
Domain network

Access type: Internet
Connections: Ethernet 3

Unidentified network
Public network

Access type: No network access
Connections: Ethernet

Change your networking settings

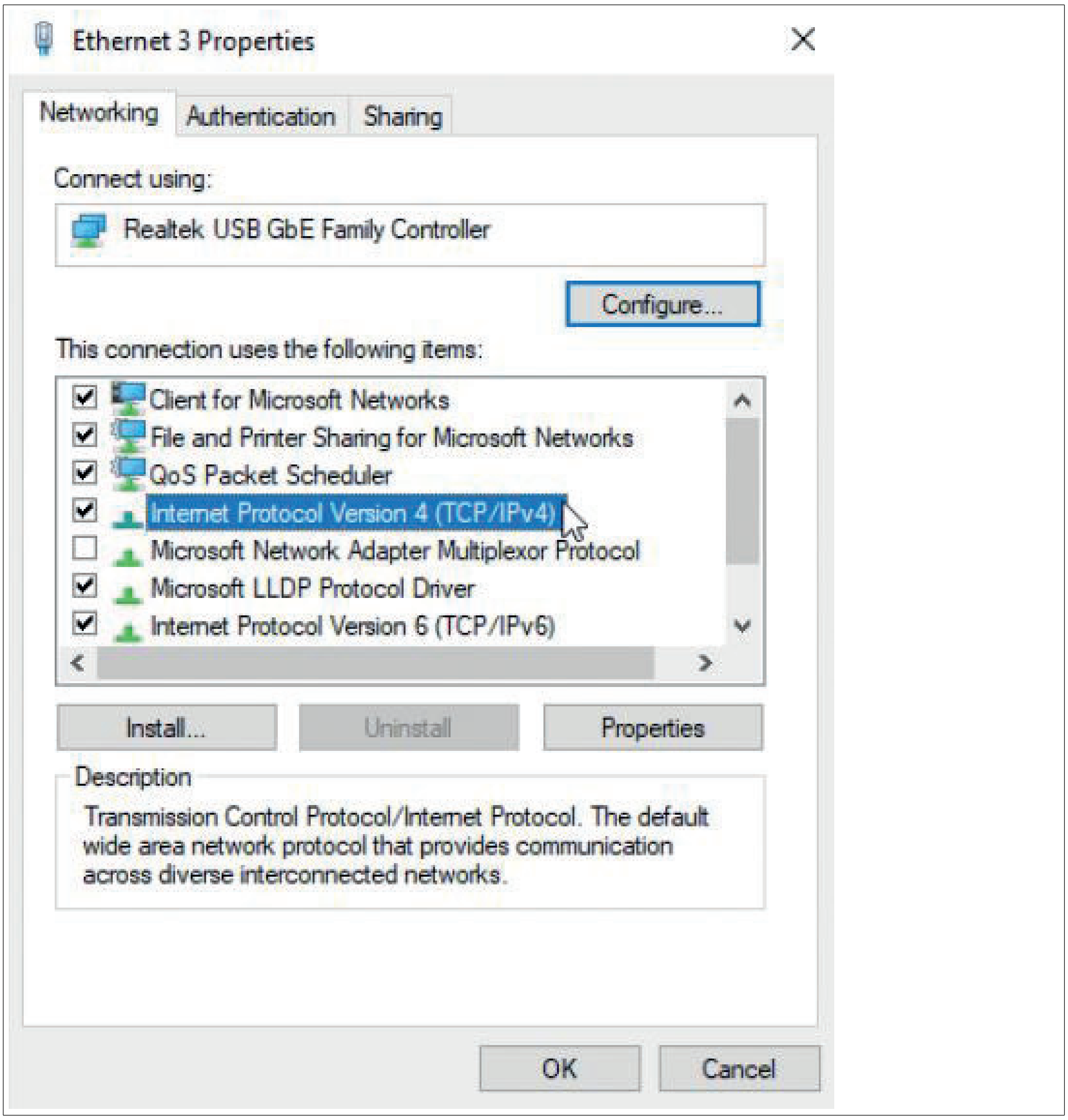
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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".

↳ The "Local Area Connection Properties" window opens.



Ethernet 3 Properties

Connect using:

Realtek USB GbE Family Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

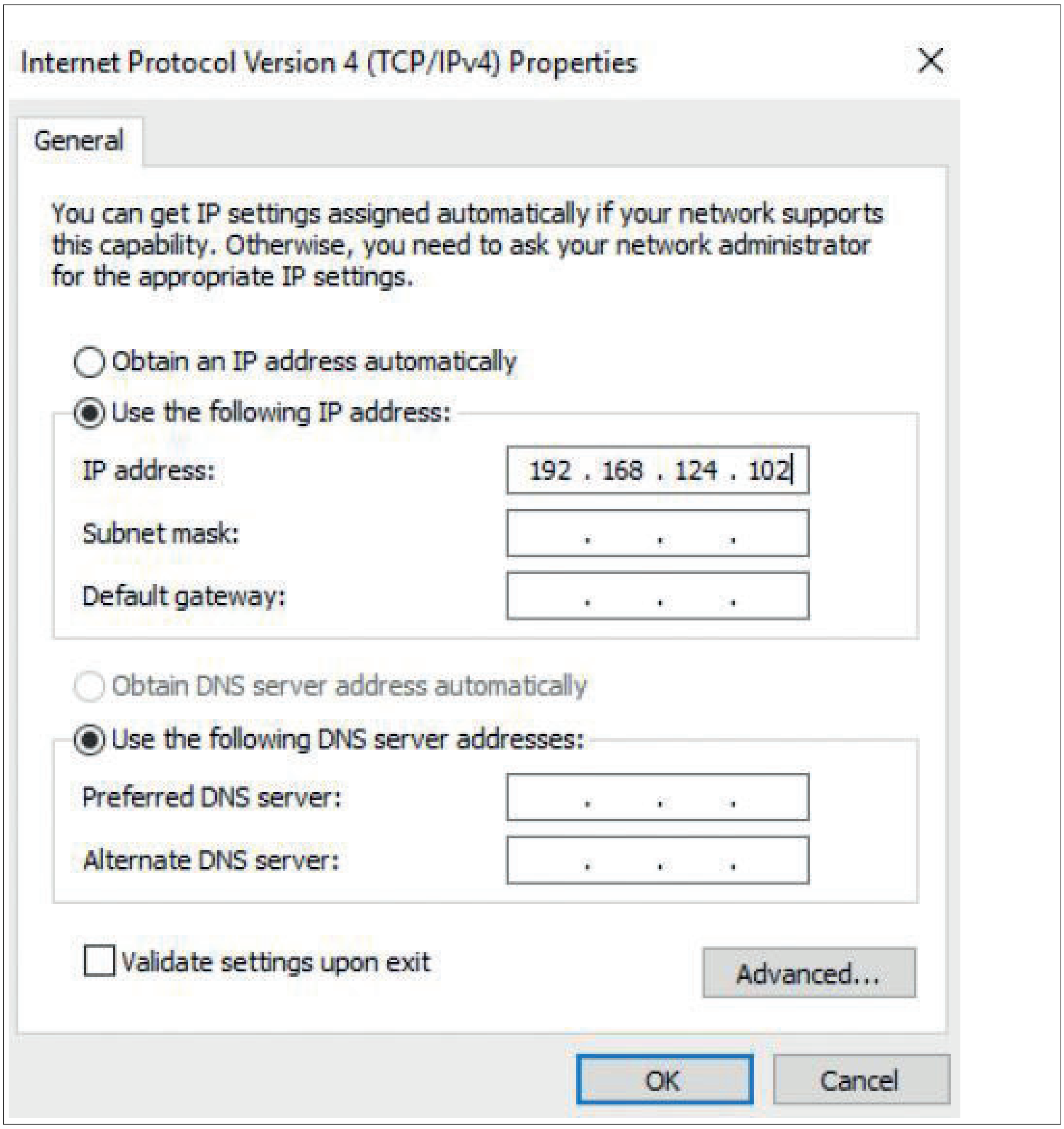
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 124 . 102

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

7. Choose the option "Use the following IP address" and type in a static IP address (e.g., "192.168.124.102").

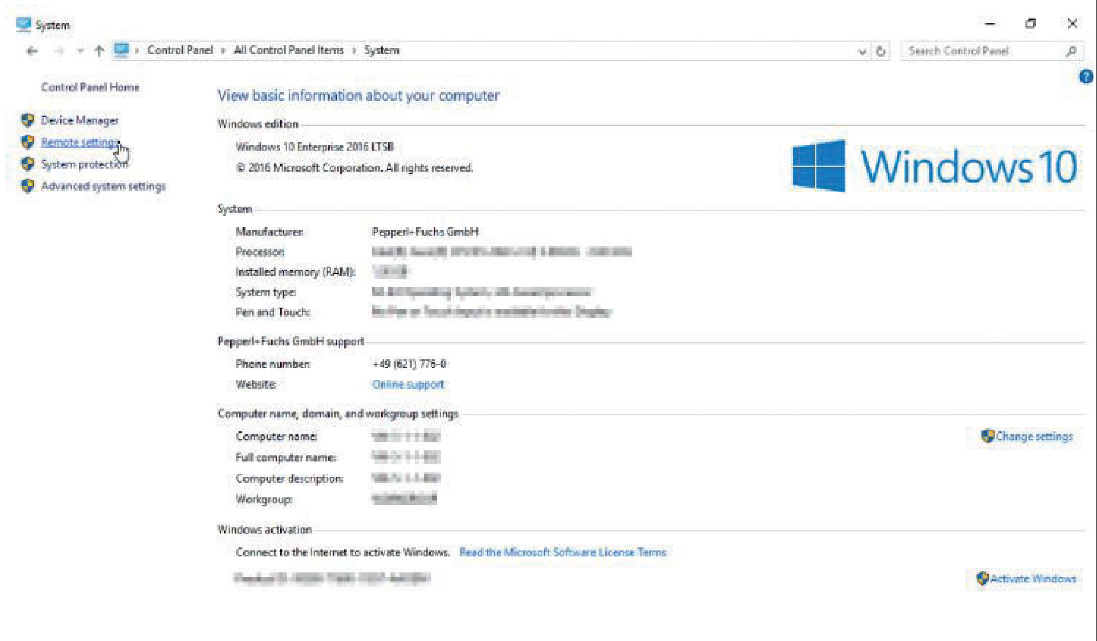
8. To confirm the changes, click "OK."

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.



View basic information about your computer

Windows edition

Windows 10 Enterprise 2016 LTSB
© 2016 Microsoft Corporation. All rights reserved.

System

Manufacturer: Pepperl+Fuchs GmbH
Processor: [redacted]
Installed memory (RAM): [redacted]
System type: [redacted]
Pen and Touch: [redacted]

Pepperl+Fuchs GmbH support

Phone number: +49 (621) 776-0
Website: Online support

Computer name, domain, and workgroup settings

Computer name: [redacted]
Full computer name: [redacted]
Computer description: [redacted]
Workgroup: [redacted]

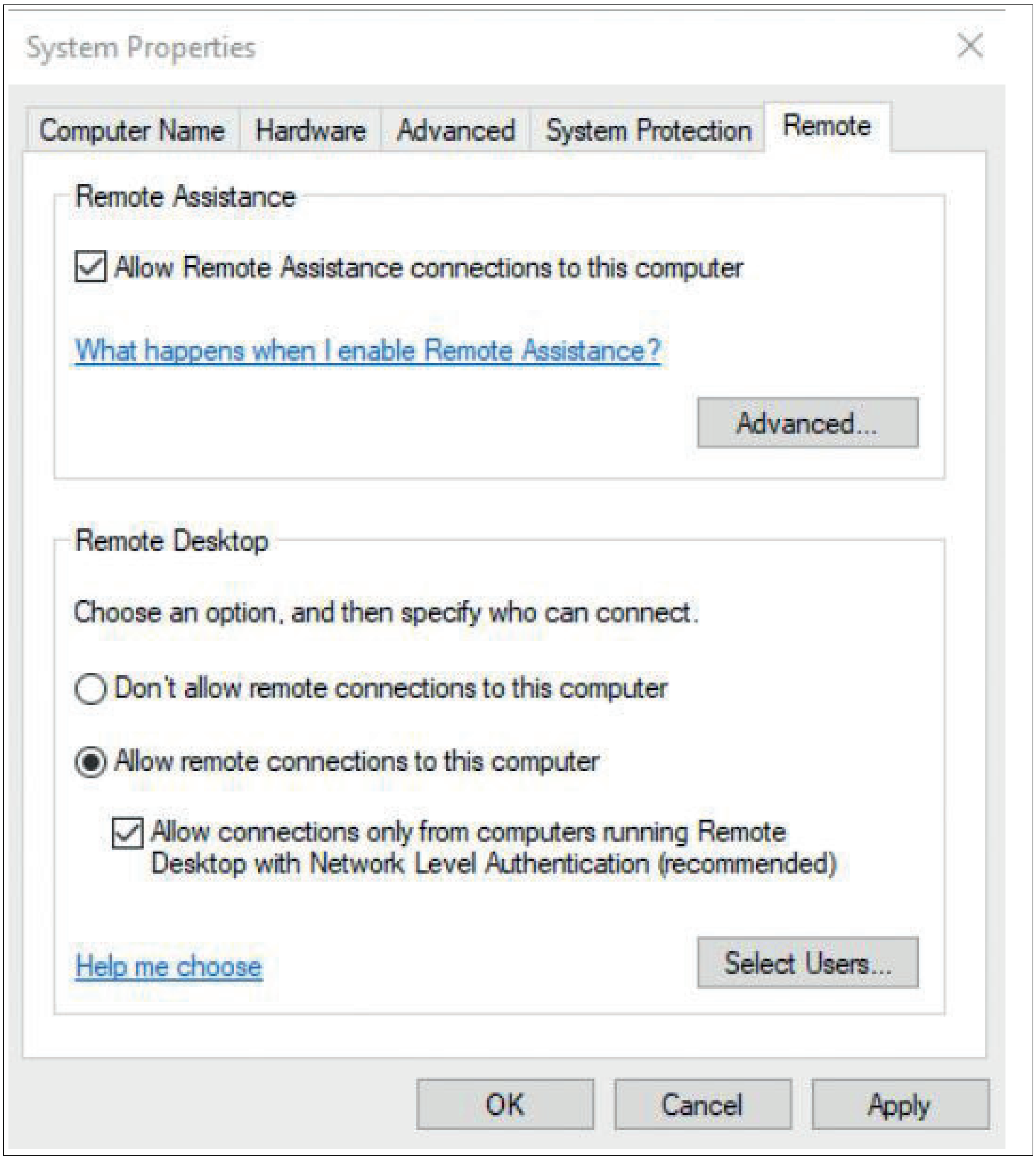
Windows activation

Connect to the Internet to activate Windows. Read the Microsoft Software License Terms

[redacted]

2. Click on "Remote settings."

   ↳ The System properties dialog box opens.



System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Advanced...

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Select Users...

OK | Cancel | Apply

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.

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.

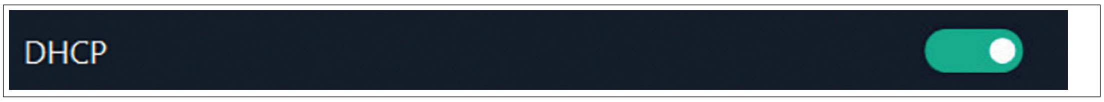


Figure 11.14

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

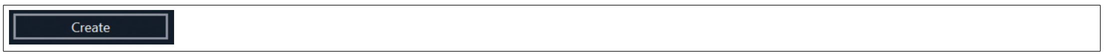
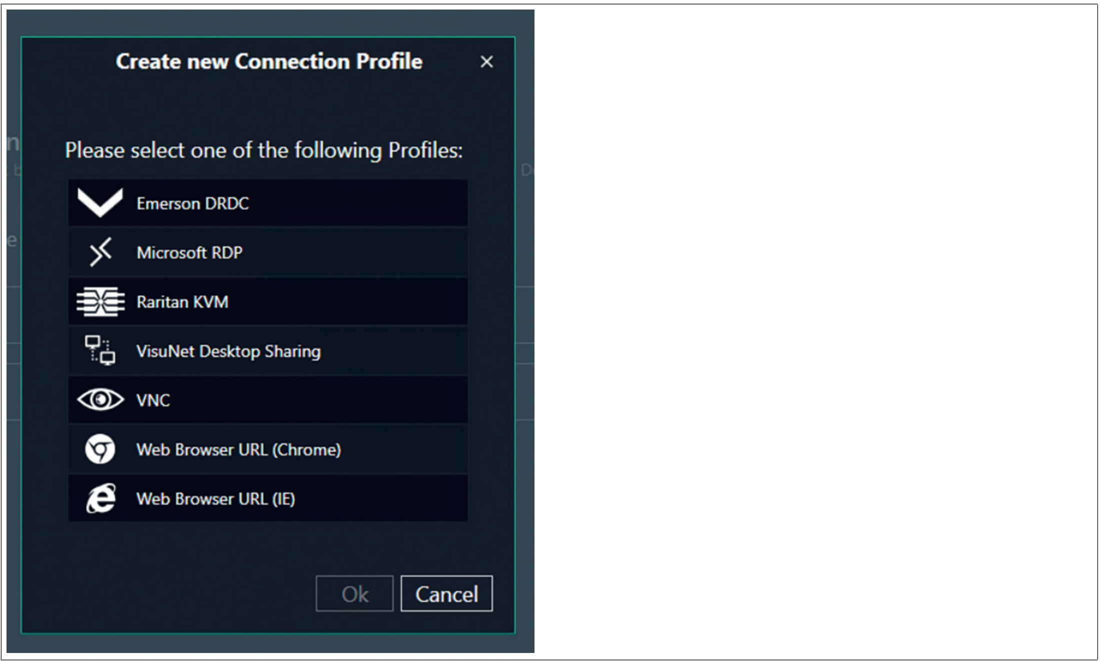


Figure 11.15

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



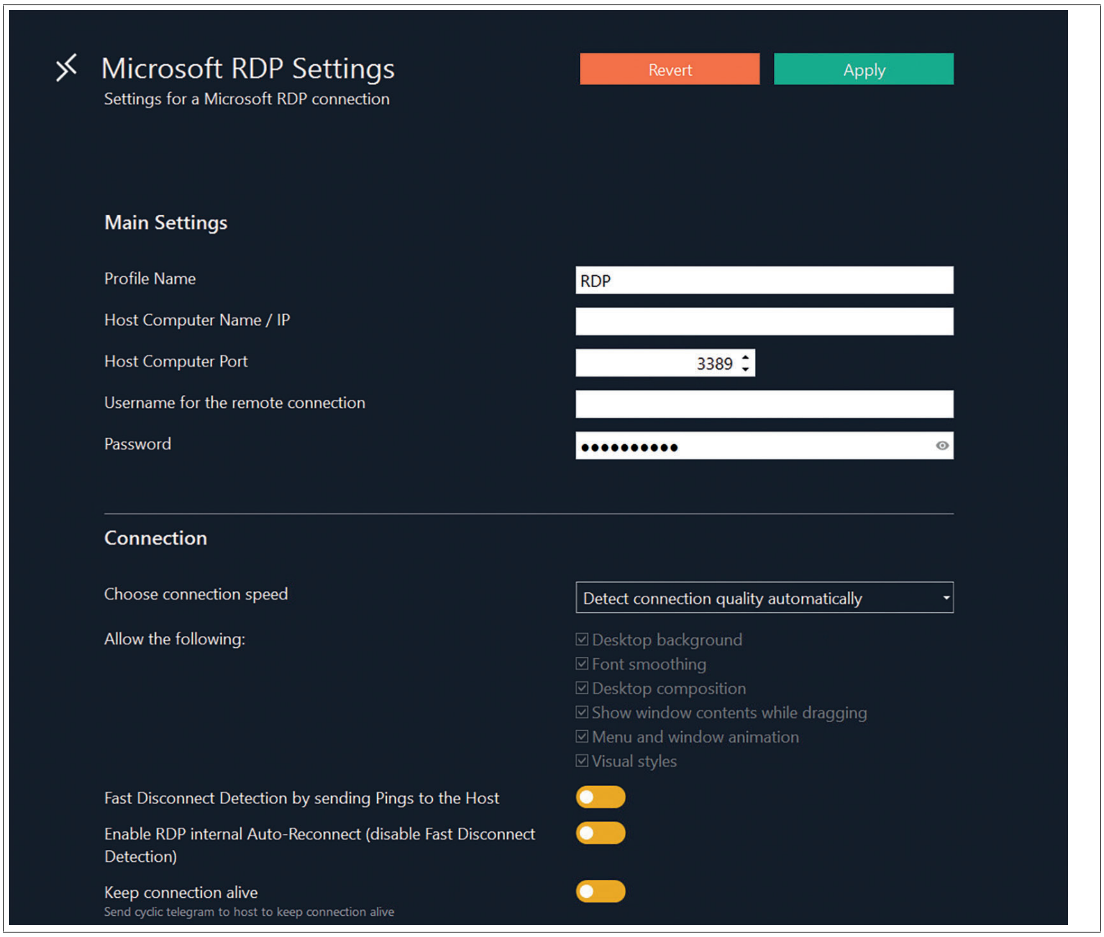
Create new Connection Profile ×

Please select one of the following Profiles:

- Emerson DRDC
- Microsoft RDP
- Raritan KVM
- VisuNet Desktop Sharing
- VNC
- Web Browser URL (Chrome)
- Web Browser URL (IE)

Figure 11.16 The "Create new Connection Profile" dialog box

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



Microsoft RDP Settings

Settings for a Microsoft RDP connection

Main Settings

Profile Name: RDP

Host Computer Name / IP:

Host Computer Port: 3389

Username for the remote connection:

Password: ●●●●●●●●●●

Connection

Choose connection speed: Detect connection quality automatically

Allow the following:

☑ Desktop background
☑ Font smoothing
☑ Desktop composition
☑ Show window contents while dragging
☑ Menu and window animation
☑ Visual styles

Fast Disconnect Detection by sending Pings to the Host

Enable RDP internal Auto-Reconnect (disable Fast Disconnect Detection)

Keep connection alive
Send cyclic telegram to host to keep connection alive

Figure 11.17 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

   ↳ 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.

11.4 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

11.5 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:

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 `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.

11.6 Calibrating a second touchscreen

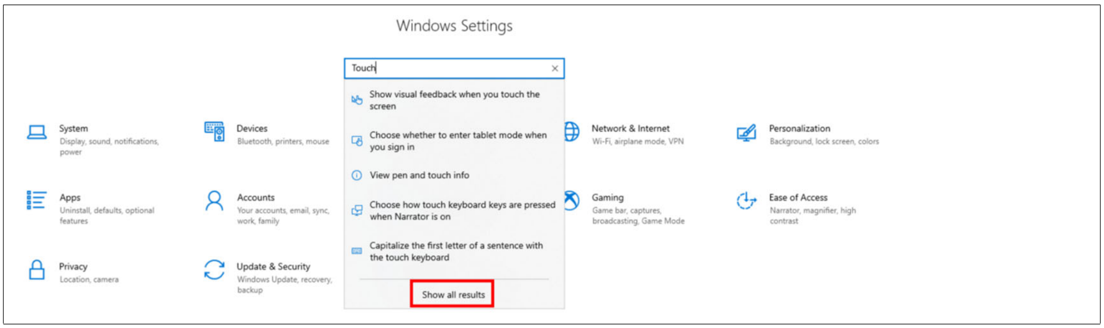
When a DMU is connected with the VisuNet FLX panel, it occurs that when the screen is expanded and not duplicated that the touch event on the main FLX panel occurs on the DMU panel. There are several alternatives to set up a second monitor.

Note

Make sure that you have a keyboard connected to the device.

Setup via system settings

1. Open the system settings and search for touch.



Windows Settings

Touch

- Show visual feedback when you touch the screen
- Choose whether to enter tablet mode when you sign in
- View pen and touch info
- Choose how touch keyboard keys are pressed when Narrator is on
- Capitalize the first letter of a sentence with the touch keyboard

Show all results

System
Display, sound, notifications, power

Devices
Bluetooth, printers, mouse

Network & Internet
Wi-Fi, airplane mode, VPN

Personalization
Background, lock screen, colors

Apps
Uninstall, defaults, optional features

Accounts
Your accounts, email, sync, work, family

Gaming
Game bar, captures, broadcasting, Game Mode

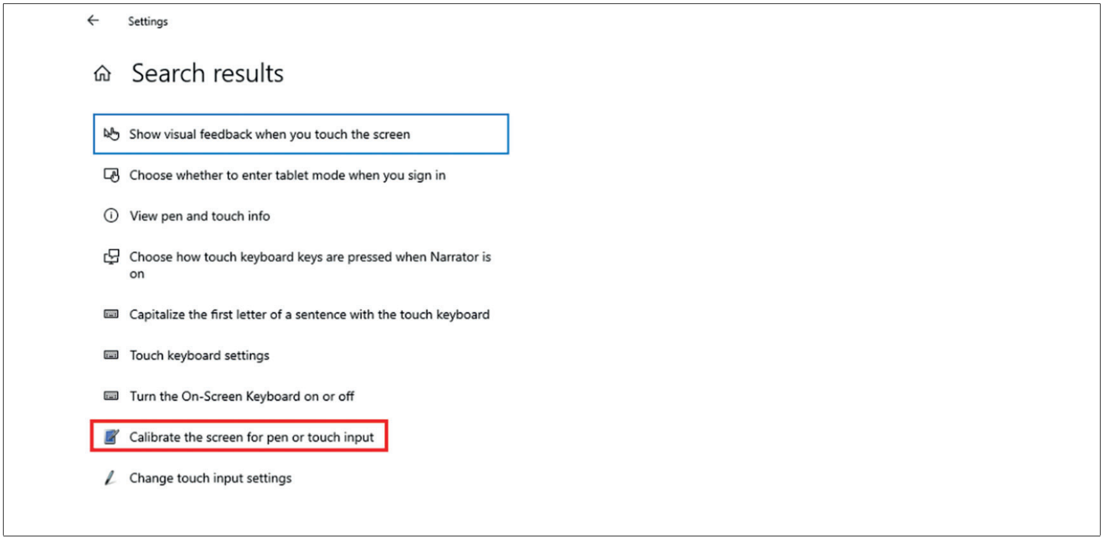
Ease of Access
Narrator, magnifier, high contrast

Privacy
Location, camera

Update & Security
Windows Update, recovery, backup

Figure 11.18

2. Select **Calibrate the screen for pen or touch input**.



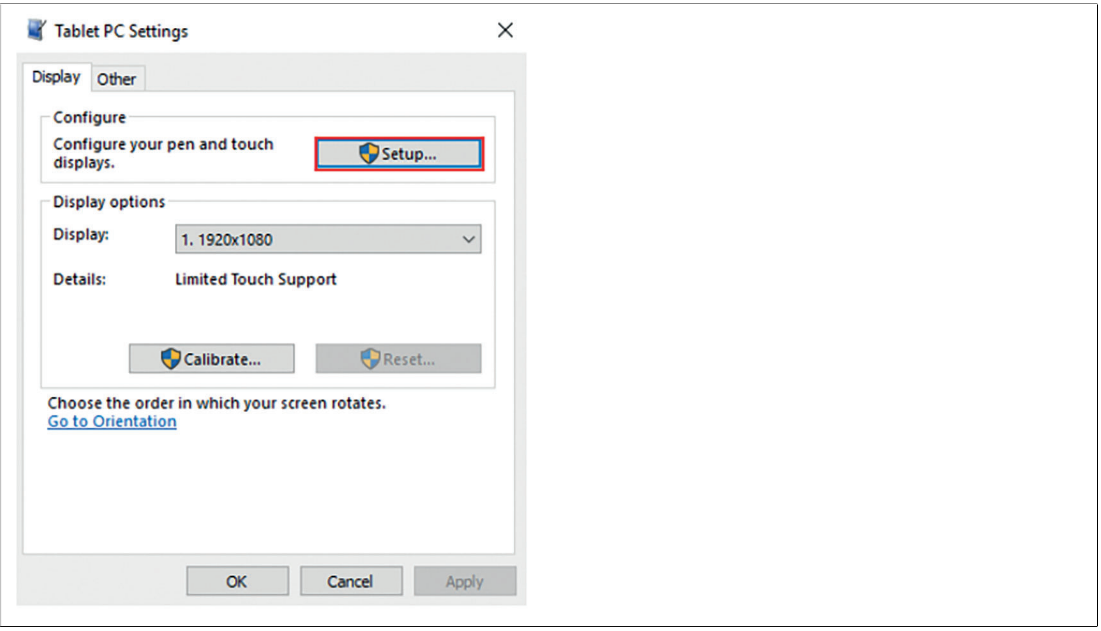
Settings

Search results

- Show visual feedback when you touch the screen
- Choose whether to enter tablet mode when you sign in
- View pen and touch info
- Choose how touch keyboard keys are pressed when Narrator is on
- Capitalize the first letter of a sentence with the touch keyboard
- Touch keyboard settings
- Turn the On-Screen Keyboard on or off
- Calibrate the screen for pen or touch input
- Change touch input settings

Figure 11.19

3. Select **Setup**



Configure your pen and touch displays.

Display: 1. 1920x1080

Details: Limited Touch Support

Choose the order in which your screen rotates.

Figure 11.20

4. Then touch the touchscreen, press the Enter key of the keyboard and touch on the second screen to calibrate the touch.

   ↳ The touchscreen has now been successfully set up.

Alternative way: Configuration via "Control Panel" in Windows

1. Search for "Control Panel" in Windows and open it.

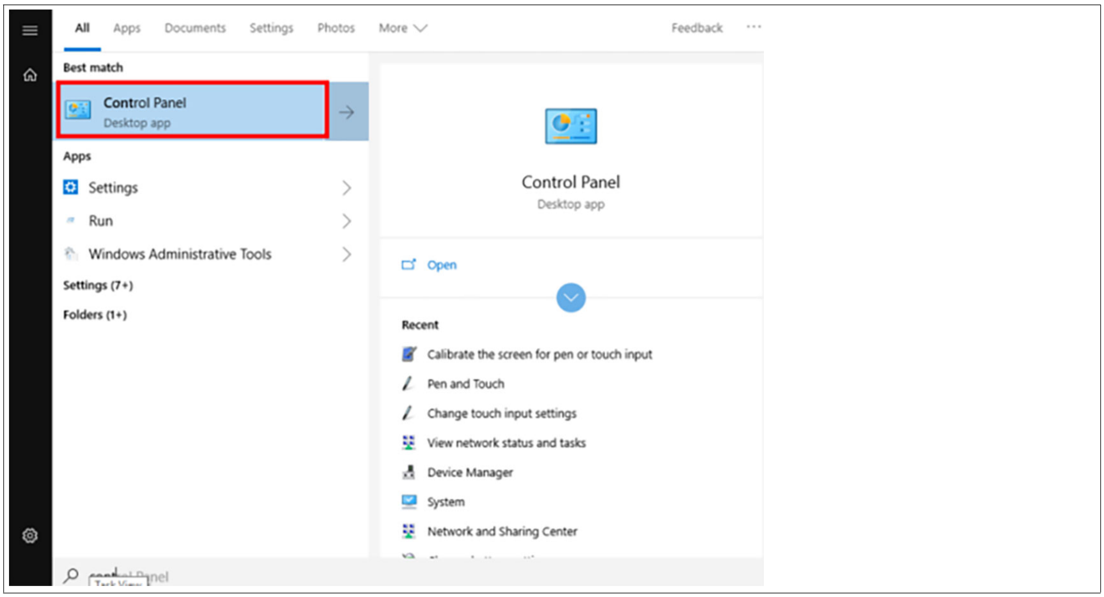


Figure 11.21

2. Click **Hardware and Sound**.

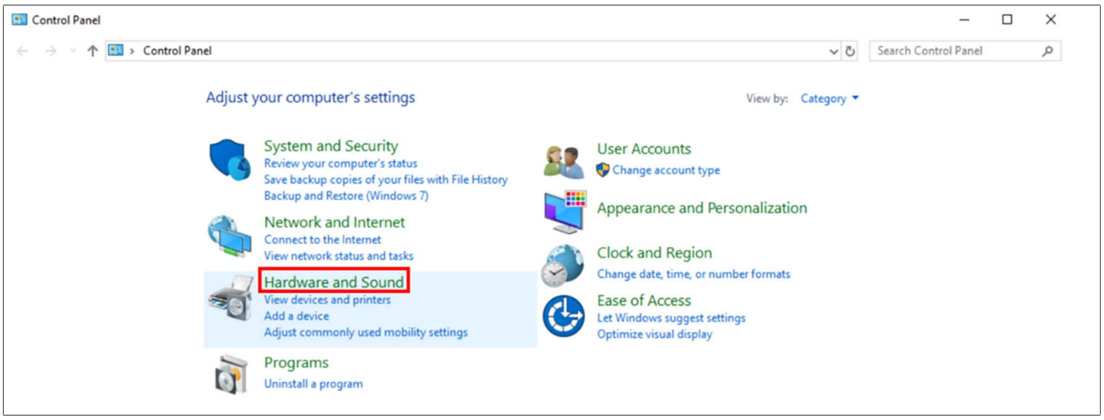

Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
Connect to the Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

Figure 11.22

3. Select **Calibrate the screen for pen or touch input**.

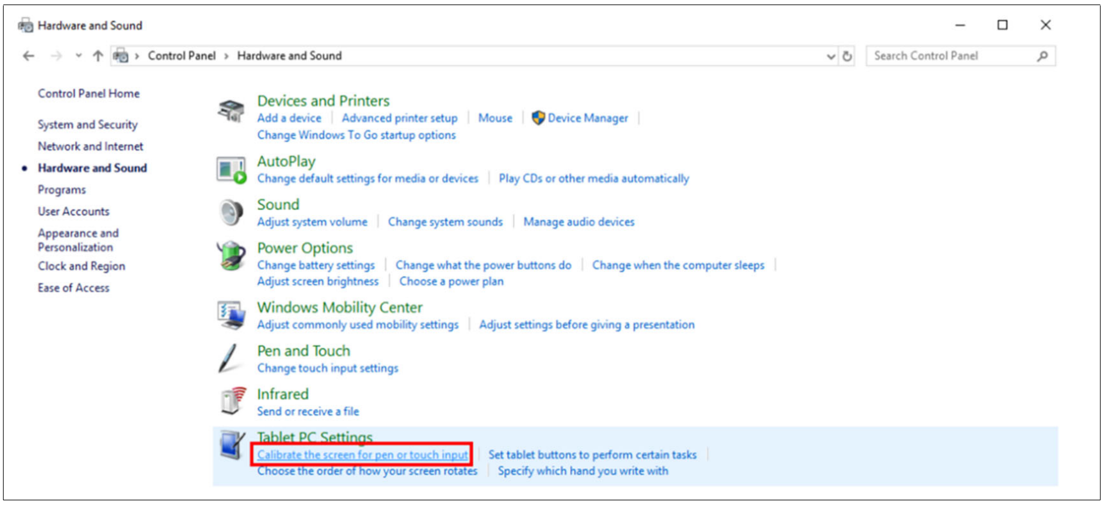
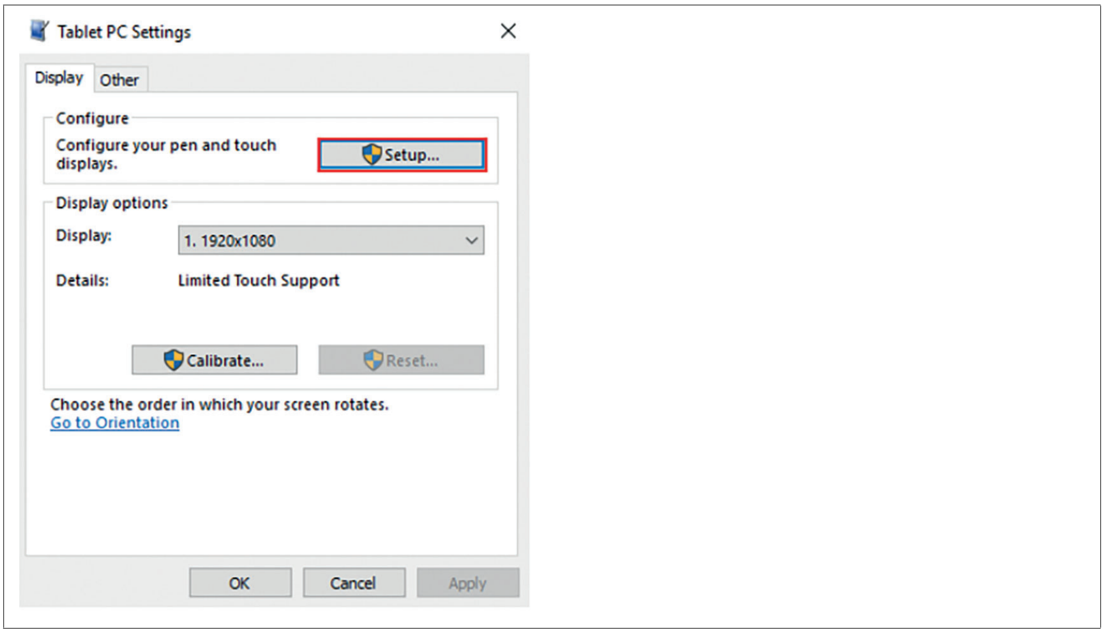

Hardware and Sound
Control Panel › Hardware and Sound
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Devices and Printers
Add a device | Advanced printer setup | Mouse | Device Manager
Change Windows To Go startup options
AutoPlay
Change default settings for media or devices | Play CDs or other media automatically
Sound
Adjust system volume | Change system sounds | Manage audio devices
Power Options
Change battery settings | Change what the power buttons do | Change when the computer sleeps
Adjust screen brightness | Choose a power plan
Windows Mobility Center
Adjust commonly used mobility settings | Adjust settings before giving a presentation
Pen and Touch
Change touch input settings
Infrared
Send or receive a file
Tablet PC Settings
Calibrate the screen for pen or touch input | Set tablet buttons to perform certain tasks
Choose the order of how your screen rotates | Specify which hand you write with

Figure 11.23

4. Select **Setup**.

5. Then touch the touchscreen, press the Enter key of the keyboard and touch on the second screen to calibrate the touch.



Configure your pen and touch displays.

Display: 1. 1920x1080

Details: Limited Touch Support

Choose the order in which your screen rotates.
Go to Orientation

Figure 11.24

↳ The touchscreen has now been successfully set up.

11.7 Installing Trellix (fromerly known as 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 Trellix Endpoing Security, visit McAfee's Knowledge Center to check software and hardware compatibility: https://www.mcafee.com/en-us/consumer-support/help/system-requirement.html.

Requirements

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

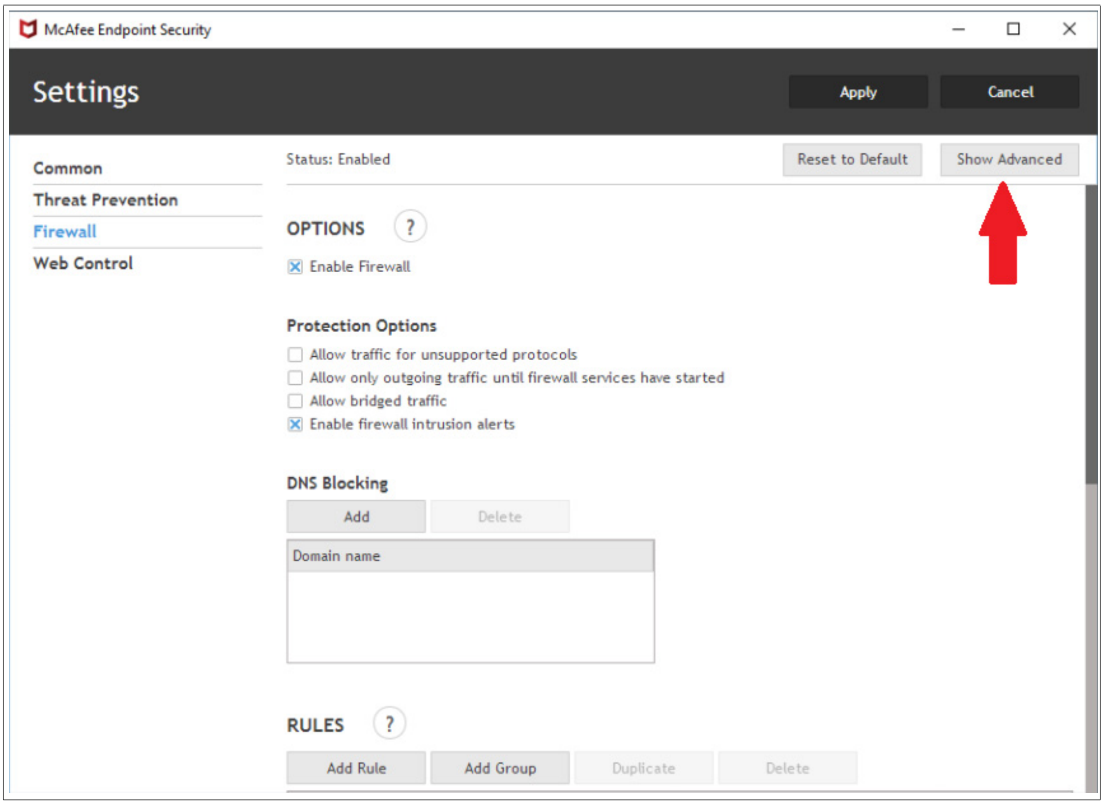
Procedure

1. Download the software on a separate PC and unpack the zip file onto a USB flash drive.
2. Disable the Unified Write Filter on your remote monitor.see chapter 4.1
3. Open the general settings in the administrator role.
4. Open Windows explorer in the start menu.
5. 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.
6. Create a generic app for Trellix (McAfee) Endpoint Security. This will provide a link to the software on the home screen. See chapter 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 Trellix (McAfee) program and click "Show Advanced."



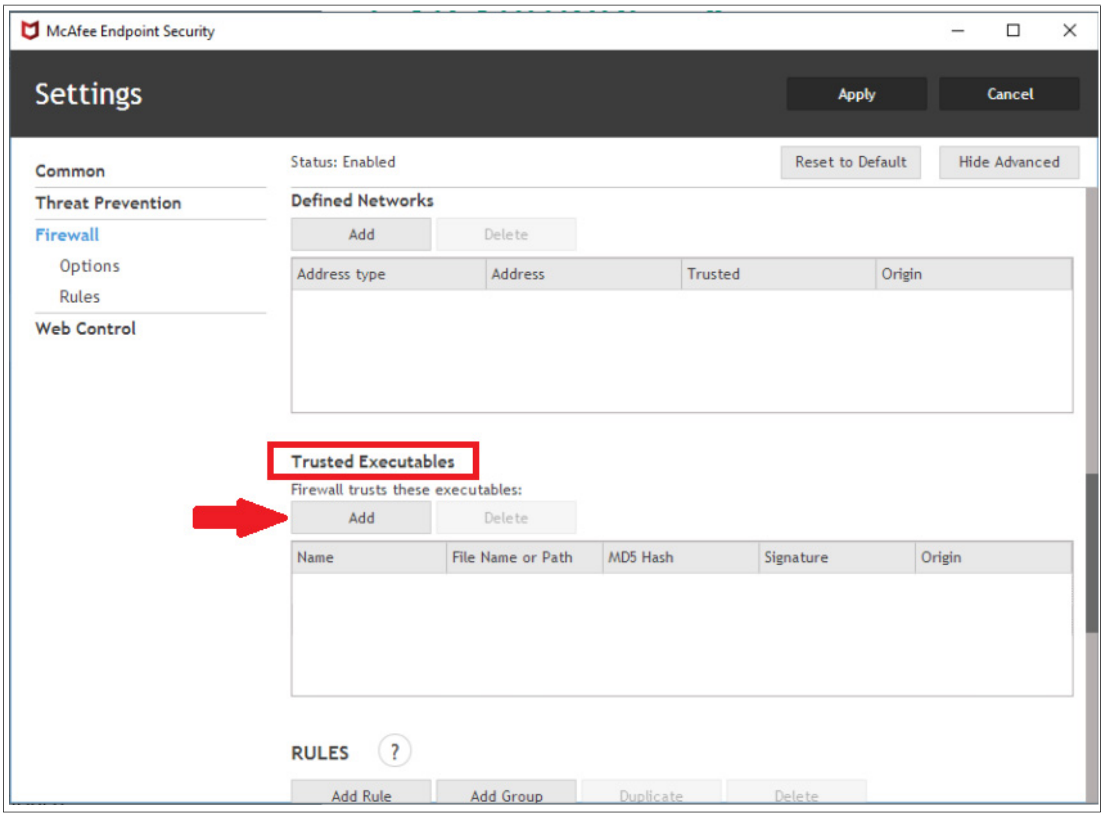
Status: Enabled

☒ Enable Firewall

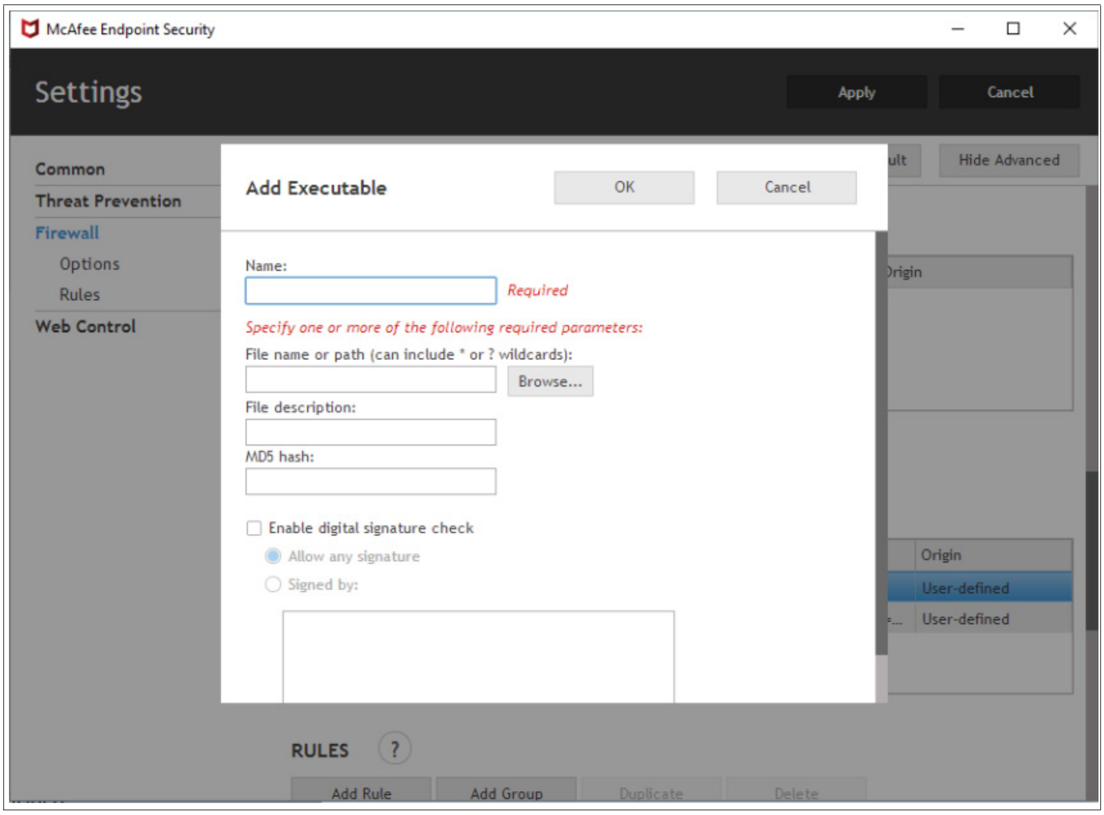
Protection Options

☐ Allow traffic for unsupported protocols
☐ Allow only outgoing traffic until firewall services have started
☐ Allow bridged traffic
☒ Enable firewall intrusion alerts

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."

11.8 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/

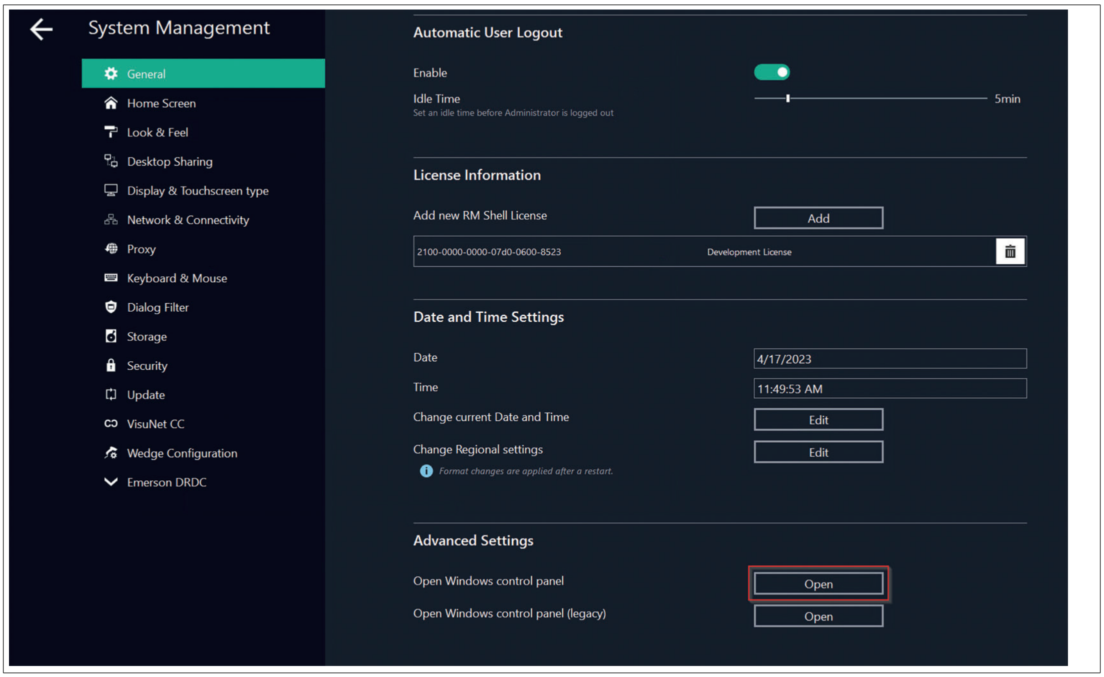
Note

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 Management" app.
3. Click the "Advanced" button at the bottom of the screen.



Automatic User Logout

Enable

Idle Time 5min
Set an idle time before Administrator is logged out

License Information

Add new RM Shell License Add

2100-0000-0000-07d0-0600-8523 Development License

Date and Time Settings

Date 4/17/2023

Time 11:49:53 AM

Change current Date and Time Edit

Change Regional settings Edit

Format changes are applied after a restart.

Advanced Settings

Open Windows control panel Open

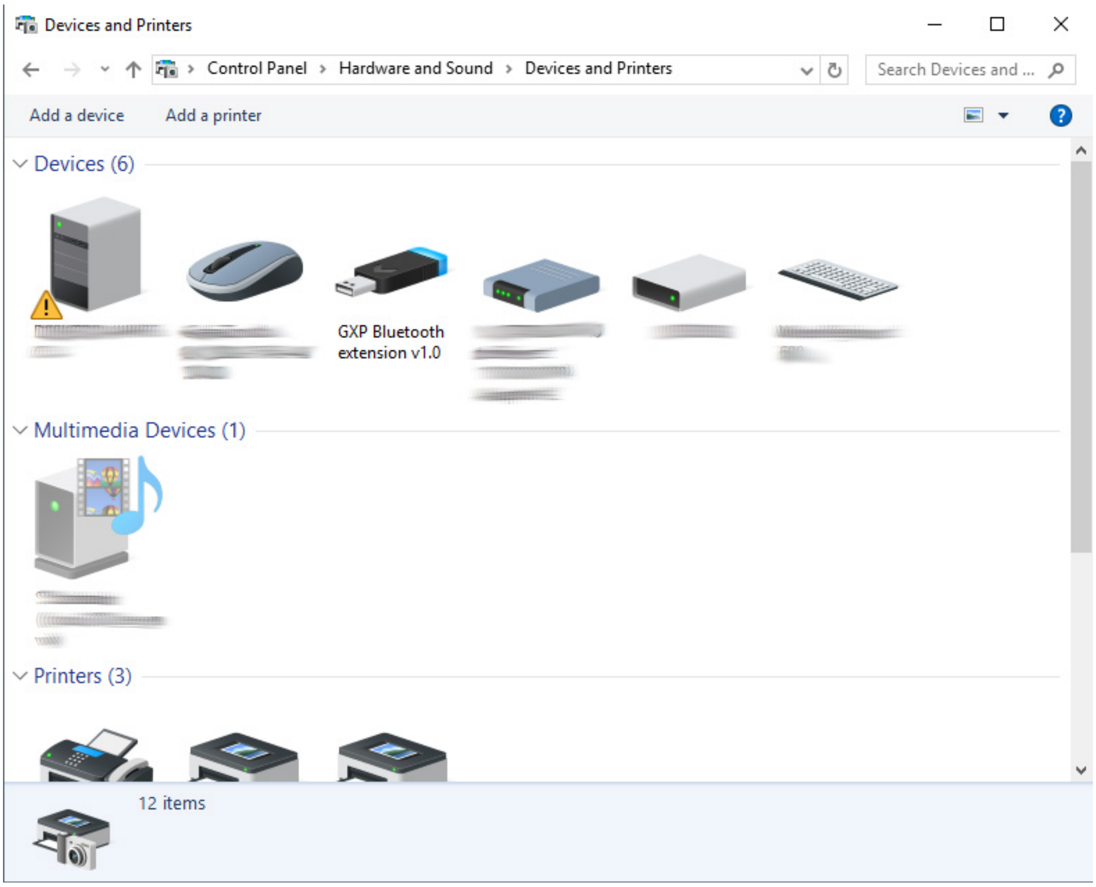
Open Windows control panel (legacy) Open

Figure 11.25

↳ The control panel will open.

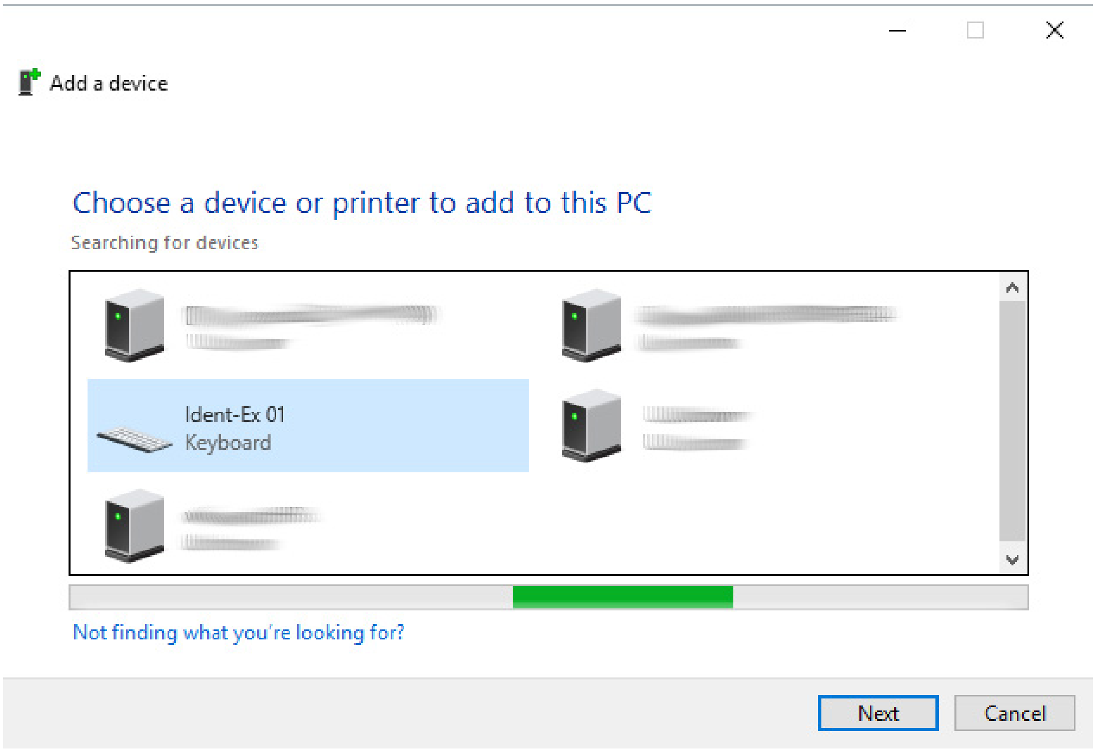
4. Navigate to "Hardware and Sound," then "Devices and Printers."
5. Select "Add a device" in the "Drivers and Printers" window.

2024-03



6. Turn on the Ident-Ex 01. After a few seconds, the Ident-Ex 01 scanner will appear as a keyboard device.

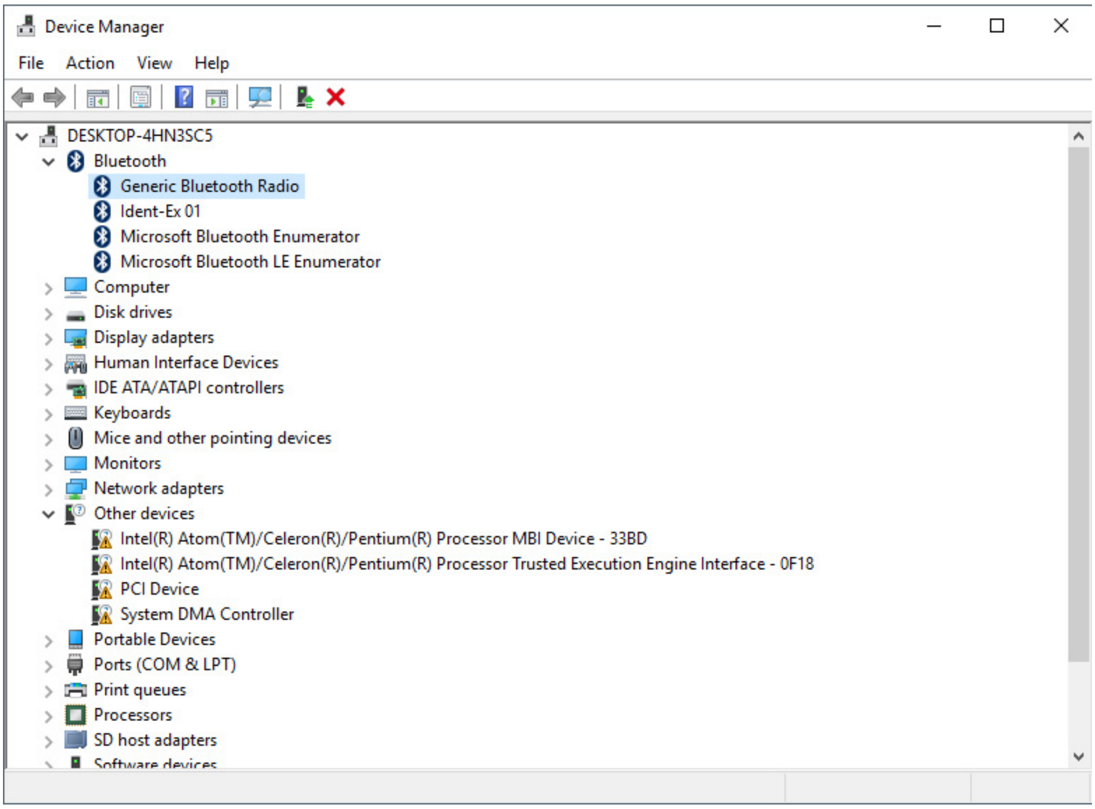
7. Select the device and click "Next."


Add a device
Choose a device or printer to add to this PC
Searching for devices
Ident-Ex 01
Keyboard
Not finding what you're looking for?
Next
Cancel

↳ 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.

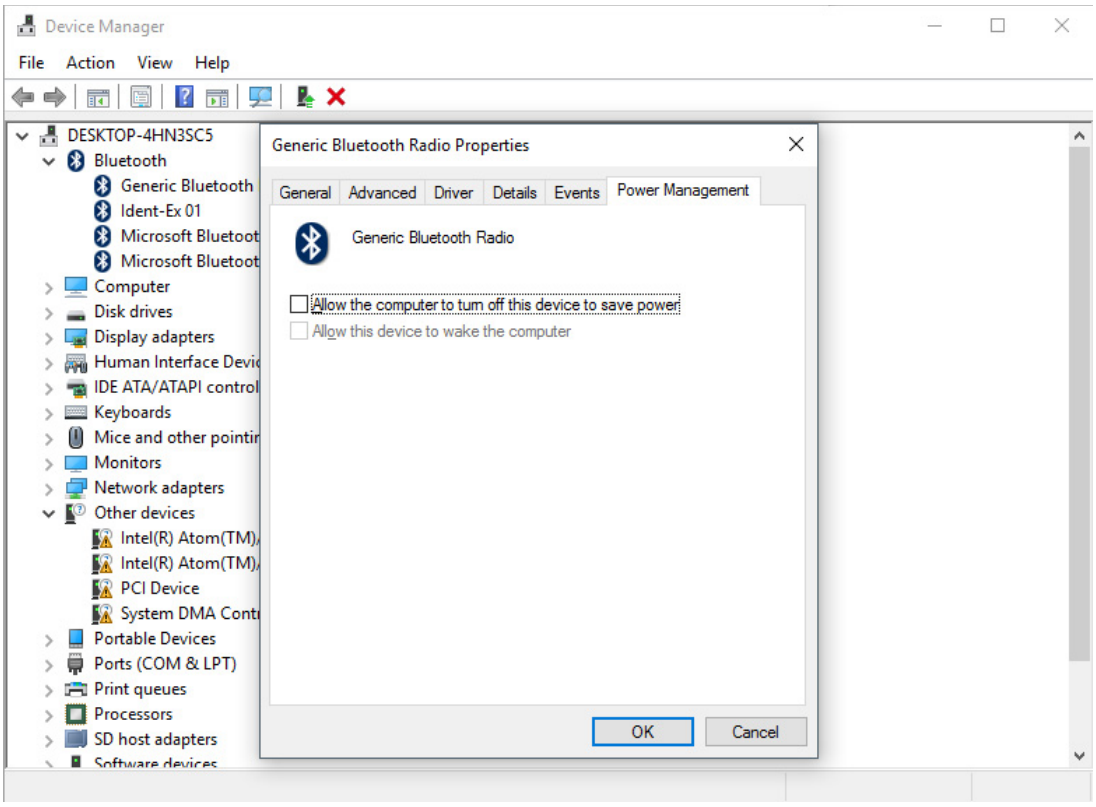
8. Navigate back to the "Hardware and Sound" section of the control panel. Select the "Device Manager" under "Devices and Printers."

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



- DESKTOP-4HN3SC5
  - Bluetooth
    - Generic Bluetooth Radio
    - Ident-Ex 01
    - Microsoft Bluetooth Enumerator
    - Microsoft Bluetooth LE Enumerator
  - Computer
  - Disk drives
  - Display adapters
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
  - Other devices
    - Intel(R) Atom(TM)/Celeron(R)/Pentium(R) Processor MBI Device - 33BD
    - Intel(R) Atom(TM)/Celeron(R)/Pentium(R) Processor Trusted Execution Engine Interface - 0F18
    - PCI Device
    - System DMA Controller
  - Portable Devices
  - Ports (COM & LPT)
  - Print queues
  - Processors
  - SD host adapters
  - Software devices

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



Generic Bluetooth Radio Properties

Generic Bluetooth Radio

□ Allow the computer to turn off this device to save power

□ Allow this device to wake the computer

↳ The device is now ready for operation.

Note

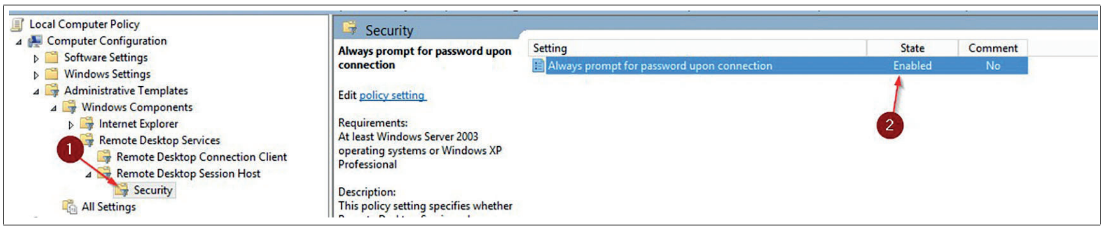
Reestablishing Connection after Reboot

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.

11.9 Importing Host Certificates

Importing certificates for RDP connections

1. Please ensure that the server allows promting for certificate.



Security

Always prompt for password upon connection

Edit policy setting

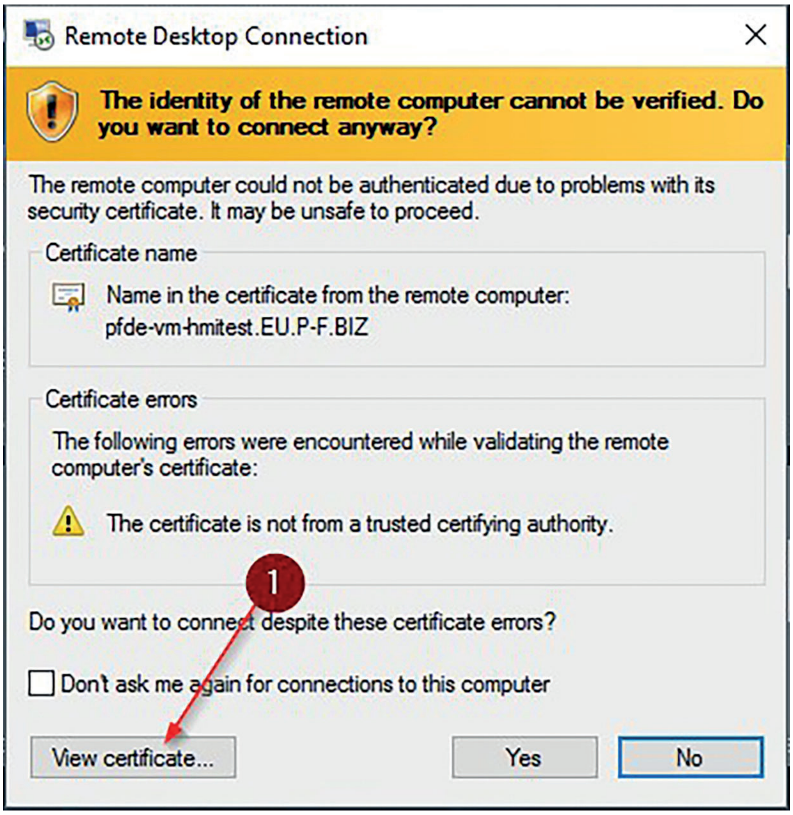
Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

Description:
This policy setting specifies whether

Setting	State	Comment
Always prompt for password upon connection	Enabled	No

Figure 11.26

2. Log into Windows with an Administrator account (PFAdmin).
3. Establish an RDP connection with MSTSC.exe.
4. Certificate warning should appear.
5. Click “View certificate” (1).



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
pfde-vm-hmitest.EU.P-F.BIZ

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

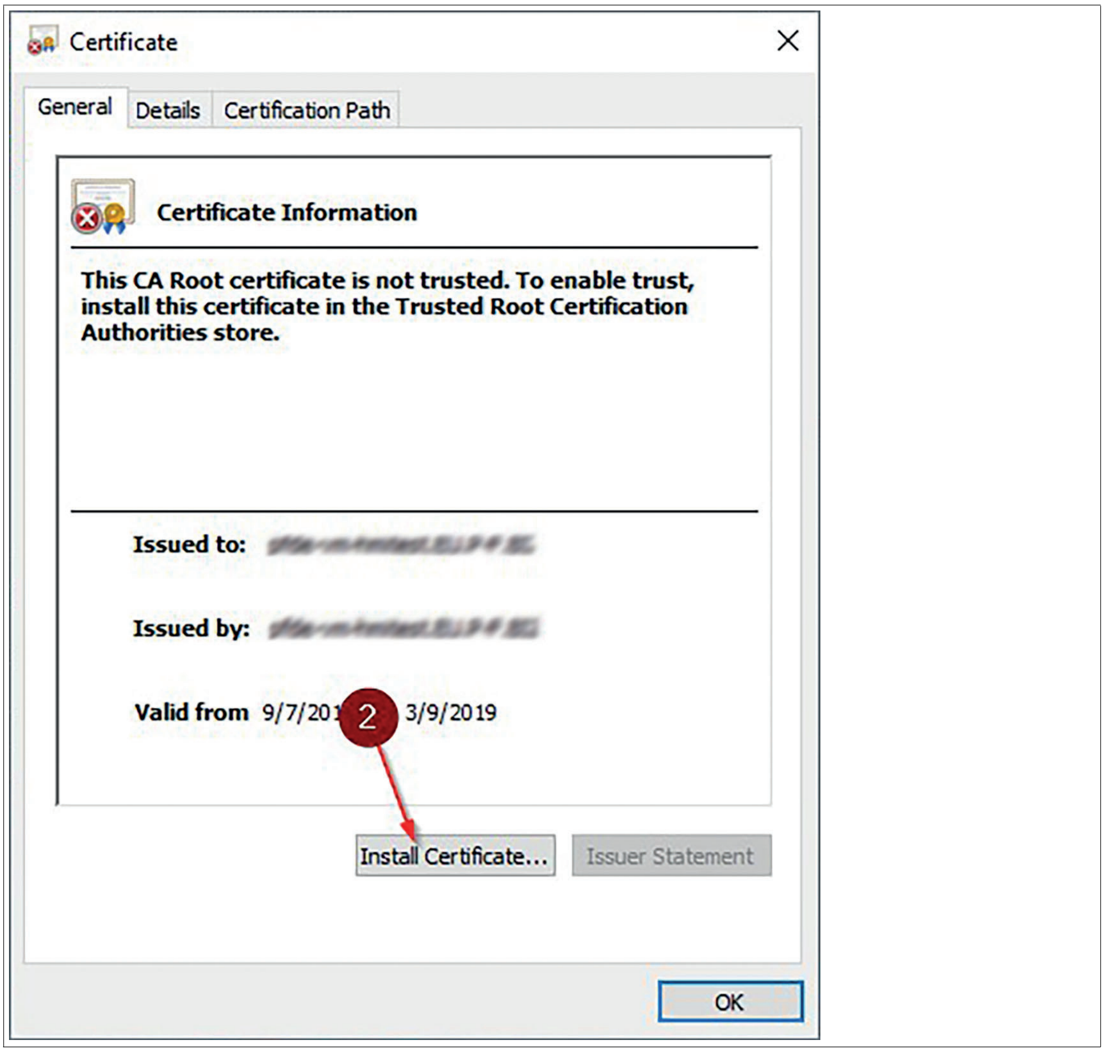
The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

Figure 11.27

6. Click “Install certificate” (2)



Certificate

General | Details | Certification Path

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: [illegible]

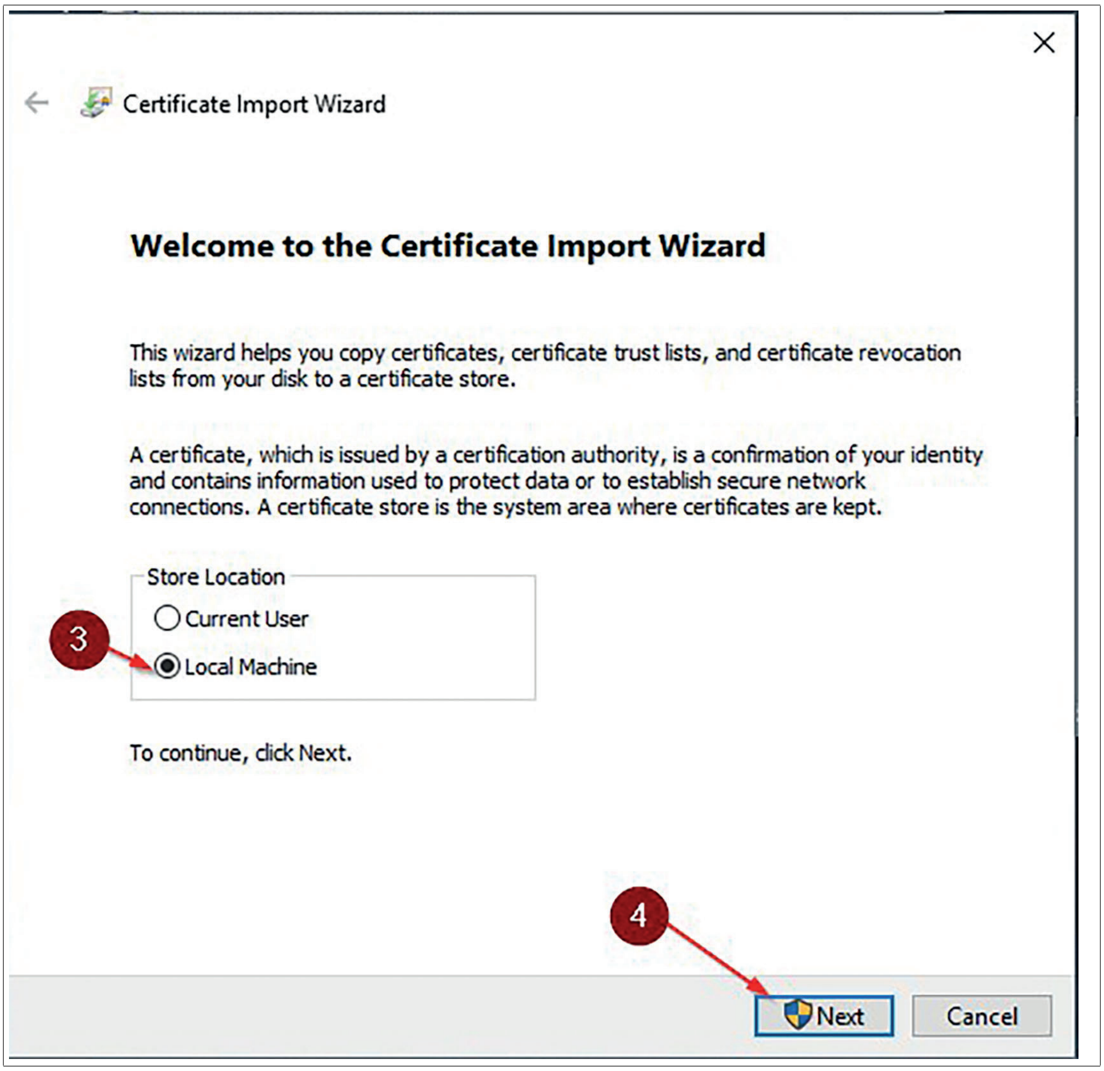
Issued by: [illegible]

Valid from 9/7/201 to 3/9/2019

Figure 11.28

7. Follow the steps of the Certificate import Wizard

8. Select “Local Machine” (3) and click “Next” (4)



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

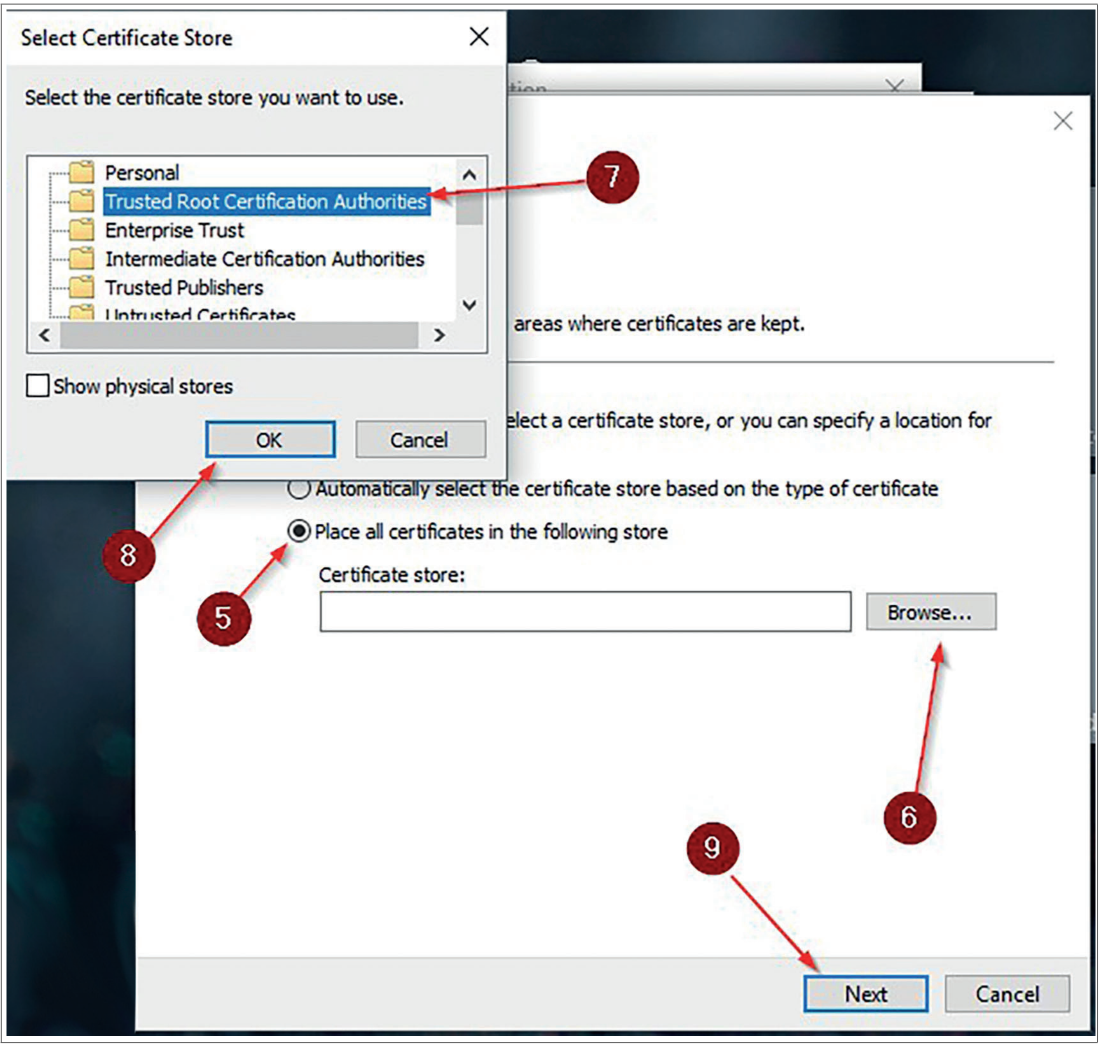
○ Current User

● Local Machine

To continue, click Next.

Figure 11.29

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



Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

areas where certificates are kept.

elect a certificate store, or you can specify a location for

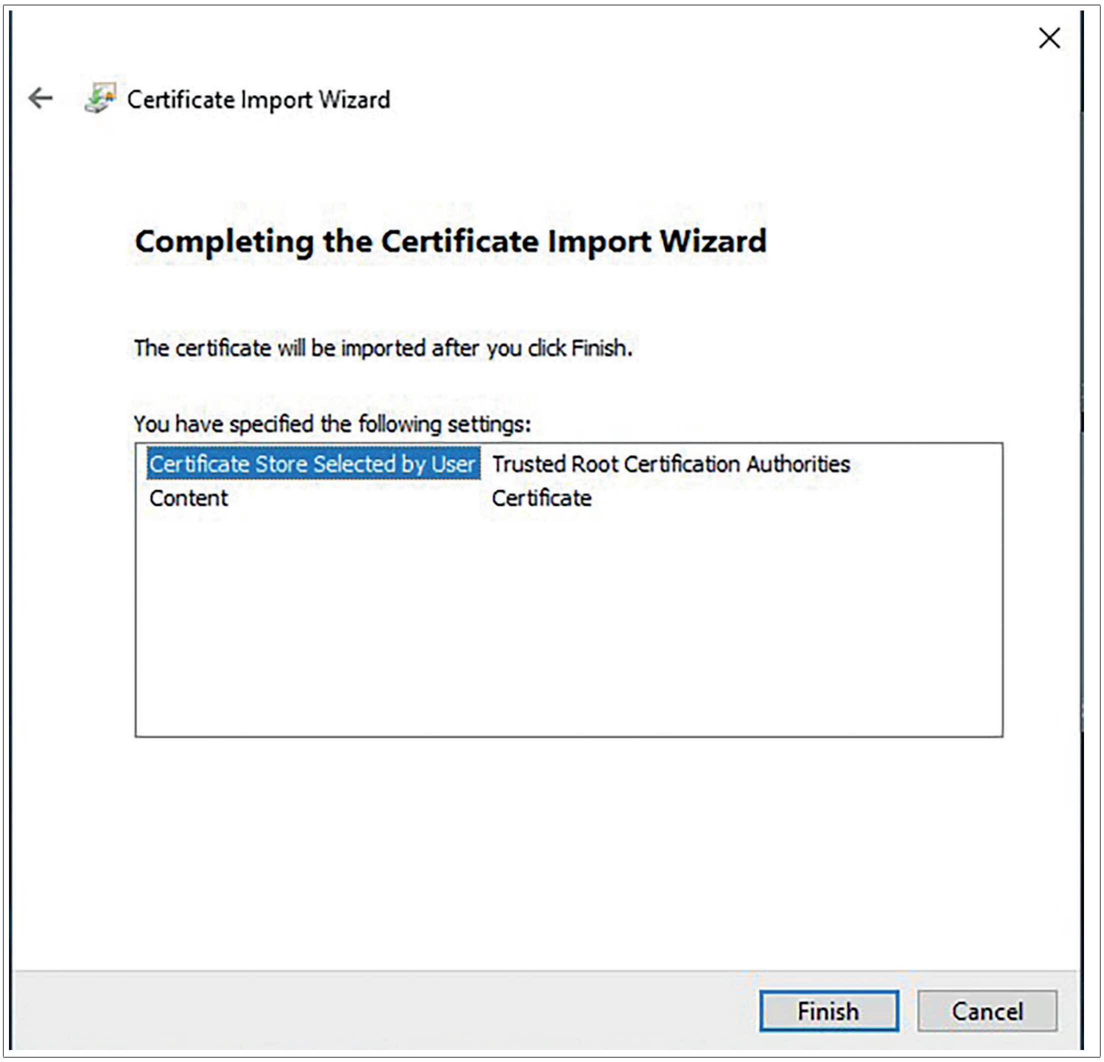
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Figure 11.30

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



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

Figure 11.31

11.10 Enable TLS 1.0 (for older Webservers)

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

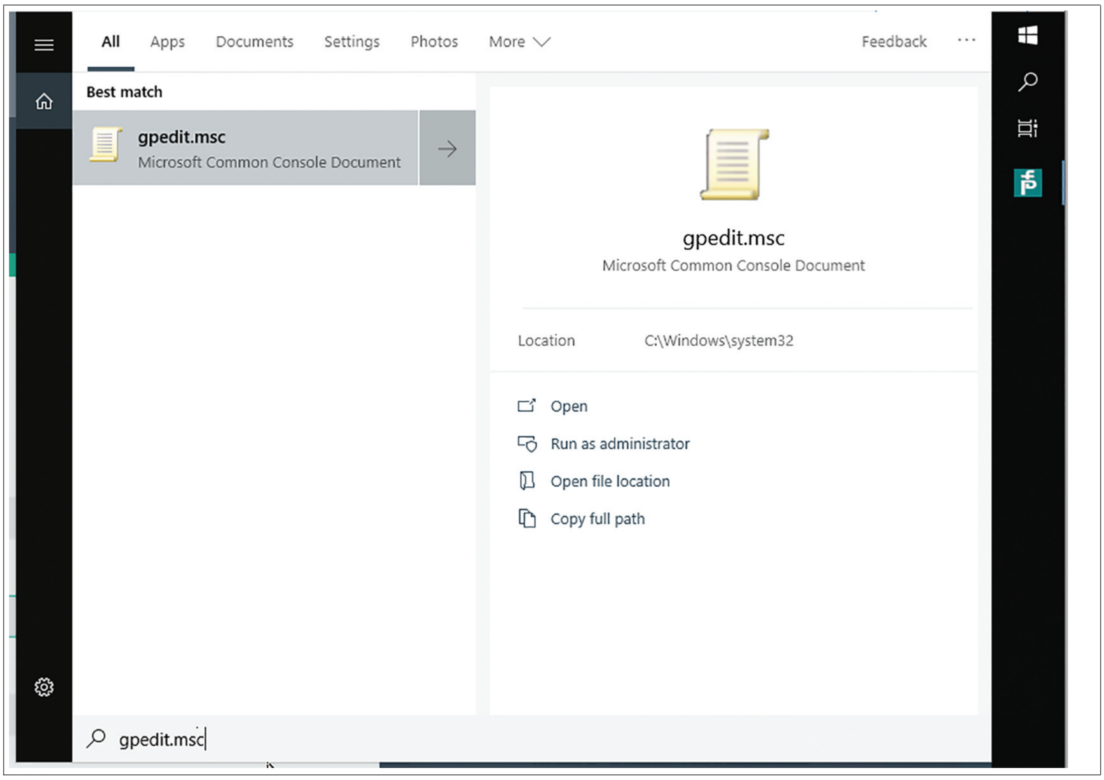
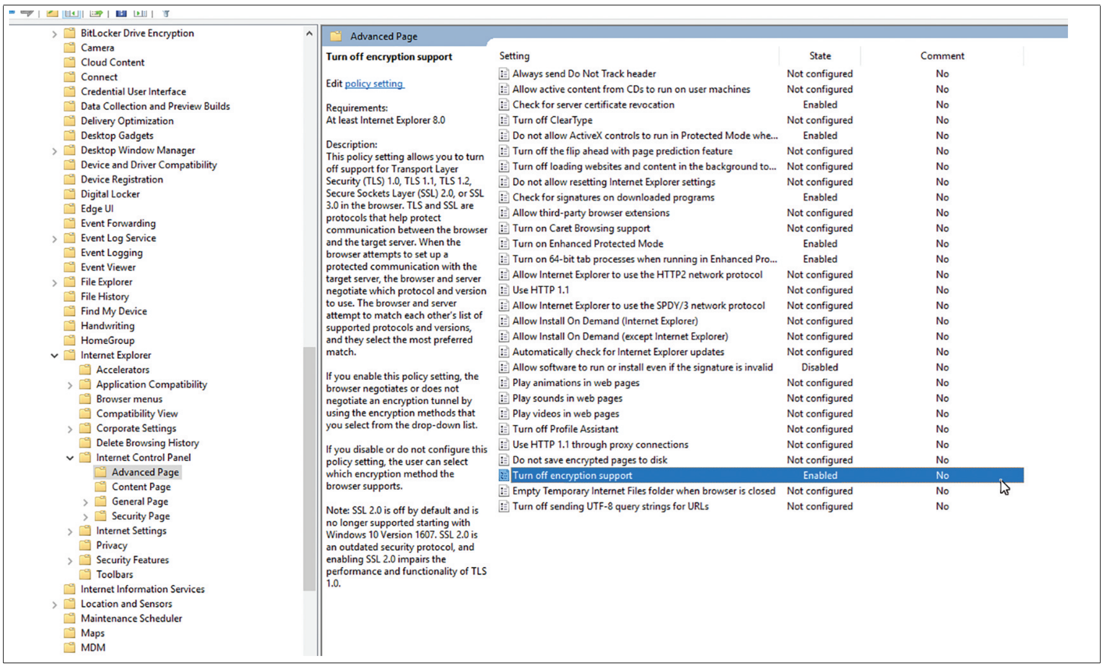


Figure 11.32

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.



Turn off encryption support

Edit policy setting

Requirements:
At least Internet Explorer 8.0

Description:
This policy setting allows you to turn off support for Transport Layer Security (TLS) 1.0, TLS 1.1, TLS 1.2, Secure Sockets Layer (SSL) 2.0, or SSL 3.0 in the browser. TLS and SSL are protocols that help protect communication between the browser and the target server. When the browser attempts to set up a protected communication with the target server, the browser and server negotiate which protocol and version to use. The browser and server attempt to match each other's list of supported protocols and versions, and they select the most preferred match.

If you enable this policy setting, the browser negotiates or does not negotiate an encryption tunnel by using the encryption methods that you select from the drop-down list.

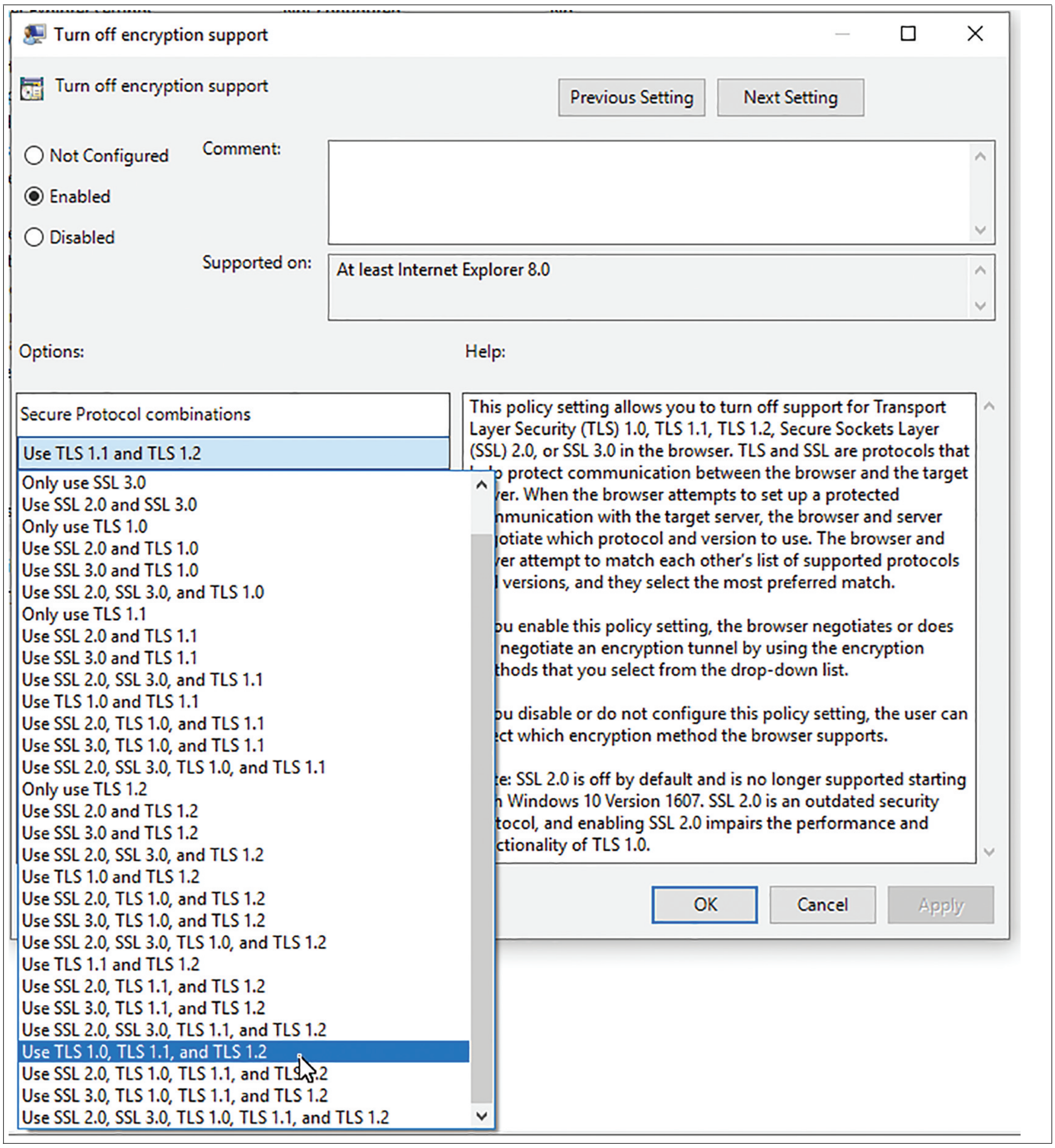
If you disable or do not configure this policy setting, the user can select which encryption method the browser supports.

Note: SSL 2.0 is off by default and is no longer supported starting with Windows 10 Version 1607. SSL 2.0 is an outdated security protocol, and enabling SSL 2.0 impairs the performance and functionality of TLS 1.0.

Setting	State	Comment
Always send Do Not Track header	Not configured	No
Allow active content from CDs to run on user machines	Not configured	No
Check for server certificate revocation	Enabled	No
Turn off ClearType	Not configured	No
Do not allow ActiveX controls to run in Protected Mode whe...	Enabled	No
Turn off the flip ahead with page prediction feature	Not configured	No
Turn off loading websites and content in the background to...	Not configured	No
Do not allow resetting Internet Explorer settings	Not configured	No
Check for signatures on downloaded programs	Enabled	No
Allow third-party browser extensions	Not configured	No
Turn on Caret Browsing support	Not configured	No
Turn on Enhanced Protected Mode	Enabled	No
Turn on 64-bit tab processes when running in Enhanced Pro...	Enabled	No
Allow Internet Explorer to use the HTTP2 network protocol	Not configured	No
Use HTTP 1.1	Not configured	No
Allow Internet Explorer to use the SPDY/3 network protocol	Not configured	No
Allow Install On Demand (Internet Explorer)	Not configured	No
Allow Install On Demand (except Internet Explorer)	Not configured	No
Automatically check for Internet Explorer updates	Not configured	No
Allow software to run or install even if the signature is invalid	Disabled	No
Play animations in web pages	Not configured	No
Play sounds in web pages	Not configured	No
Play videos in web pages	Not configured	No
Turn off Profile Assistant	Not configured	No
Use HTTP 1.1 through proxy connections	Not configured	No
Do not save encrypted pages to disk	Not configured	No
Turn off encryption support	Enabled	No
Empty Temporary Internet Files folder when browser is closed	Not configured	No
Turn off sending UTF-8 query strings for URLs	Not configured	No

Figure 11.33

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



Turn off encryption support

Turn off encryption support

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Internet Explorer 8.0

Options:

Secure Protocol combinations

Use TLS 1.1 and TLS 1.2

- Only use SSL 3.0
- Use SSL 2.0 and SSL 3.0
- Only use TLS 1.0
- Use SSL 2.0 and TLS 1.0
- Use SSL 3.0 and TLS 1.0
- Use SSL 2.0, SSL 3.0, and TLS 1.0
- Only use TLS 1.1
- Use SSL 2.0 and TLS 1.1
- Use SSL 3.0 and TLS 1.1
- Use SSL 2.0, SSL 3.0, and TLS 1.1
- Use TLS 1.0 and TLS 1.1
- Use SSL 2.0, TLS 1.0, and TLS 1.1
- Use SSL 3.0, TLS 1.0, and TLS 1.1
- Use SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1
- Only use TLS 1.2
- Use SSL 2.0 and TLS 1.2
- Use SSL 3.0 and TLS 1.2
- Use SSL 2.0, SSL 3.0, and TLS 1.2
- Use TLS 1.0 and TLS 1.2
- Use SSL 2.0, TLS 1.0, and TLS 1.2
- Use SSL 3.0, TLS 1.0, and TLS 1.2
- Use SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.2
- Use TLS 1.1 and TLS 1.2
- Use SSL 2.0, TLS 1.1, and TLS 1.2
- Use SSL 3.0, TLS 1.1, and TLS 1.2
- Use SSL 2.0, SSL 3.0, TLS 1.1, and TLS 1.2
- Use TLS 1.0, TLS 1.1, and TLS 1.2
- Use SSL 2.0, TLS 1.0, TLS 1.1, and TLS 1.2
- Use SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2
- Use SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2

Help:

This policy setting allows you to turn off support for Transport Layer Security (TLS) 1.0, TLS 1.1, TLS 1.2, Secure Sockets Layer (SSL) 2.0, or SSL 3.0 in the browser. TLS and SSL are protocols that o protect communication between the browser and the target ver. When the browser attempts to set up a protected nmunication with the target server, the browser and server otiate which protocol and version to use. The browser and ver attempt to match each other's list of supported protocols versions, and they select the most preferred match.

ou enable this policy setting, the browser negotiates or does negotiate an encryption tunnel by using the encryption thods that you select from the drop-down list.

ou disable or do not configure this policy setting, the user can ct which encryption method the browser supports.

te: SSL 2.0 is off by default and is no longer supported starting n Windows 10 Version 1607. SSL 2.0 is an outdated security tocol, and enabling SSL 2.0 impairs the performance and ctionality of TLS 1.0.

Figure 11.34

6. Close the dialog with Ok.

7. Reboot the Shell.

11.11 VLAN Tagging

Configuring a VLAN for a network adapter is beneficial for network segmentation, allowing different groups of devices to operate independently on the same physical network. This isolation enhances security by preventing unauthorized access and minimizing the risk of potential security breaches. Additionally, VLAN configuration on a network adapter optimizes resource usage, leading to more efficient data traffic management within the network infrastructure.

The process described below is applicable to the following devices:

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

For VisuNet GXP (2024 Generation with Elkhart Lake Processor) see below.

Procedure

1. Access the Windows desktop by clicking on "Switch User" in the Configuration View and authenticating as PFAdmin in Windows.
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 Name, which should have the VLAN Tag.

   Note

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

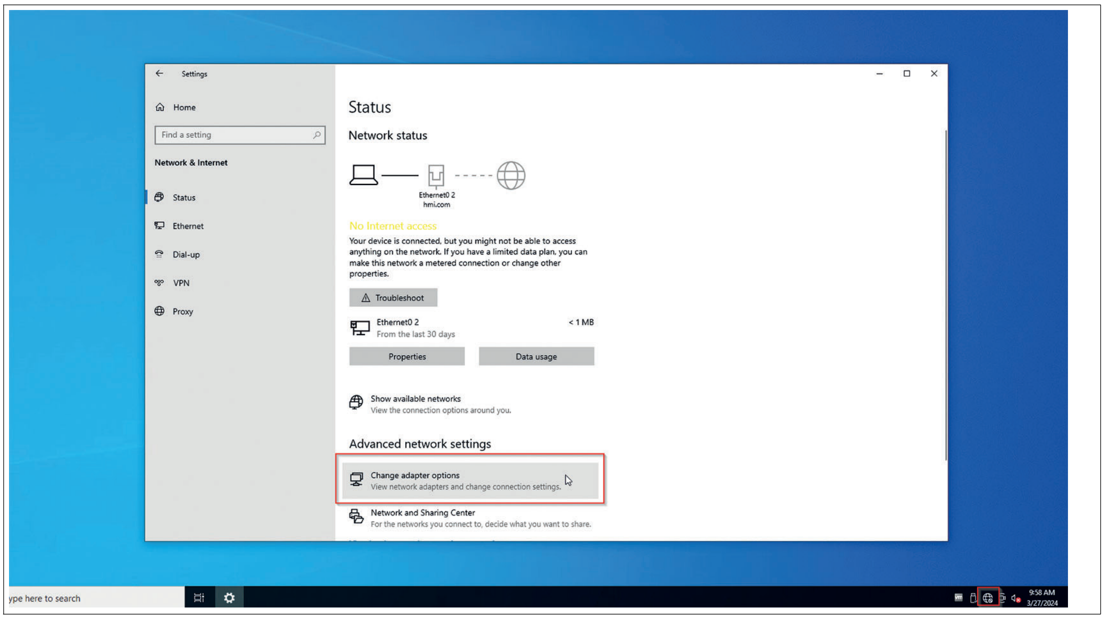
6. Now you can execute: "Add-IntelNetVLAN -ParentName "<device name>" -VLANID "<vlanid>"". Replace <device name> with the network adapter name of the step before and <vlanid> with your wanted VLan Id.

Remove VLanTag

1. `Remove-IntelNetVLAN -ParentName "<device name>" -VLANID "<vlanid>"`

Process for VisuNet GXP (2024 Generation with Elkhart Lake Processor):

1. Log in as PFAdmin -> go to General Settings -> Network & Connectivity -> "Advanced Settings".
2. Go to Settings -> Network and Internet -> Change adapter options.



No Internet access

Your device is connected, but you might not be able to access anything on the network. If you have a limited data plan, you can make this network a metered connection or change other properties.

View the connection options around you.

View network adapters and change connection settings.

For the networks you connect to, decide what you want to share.

Figure 11.35

3. Right-click on the network adapter and select properties.

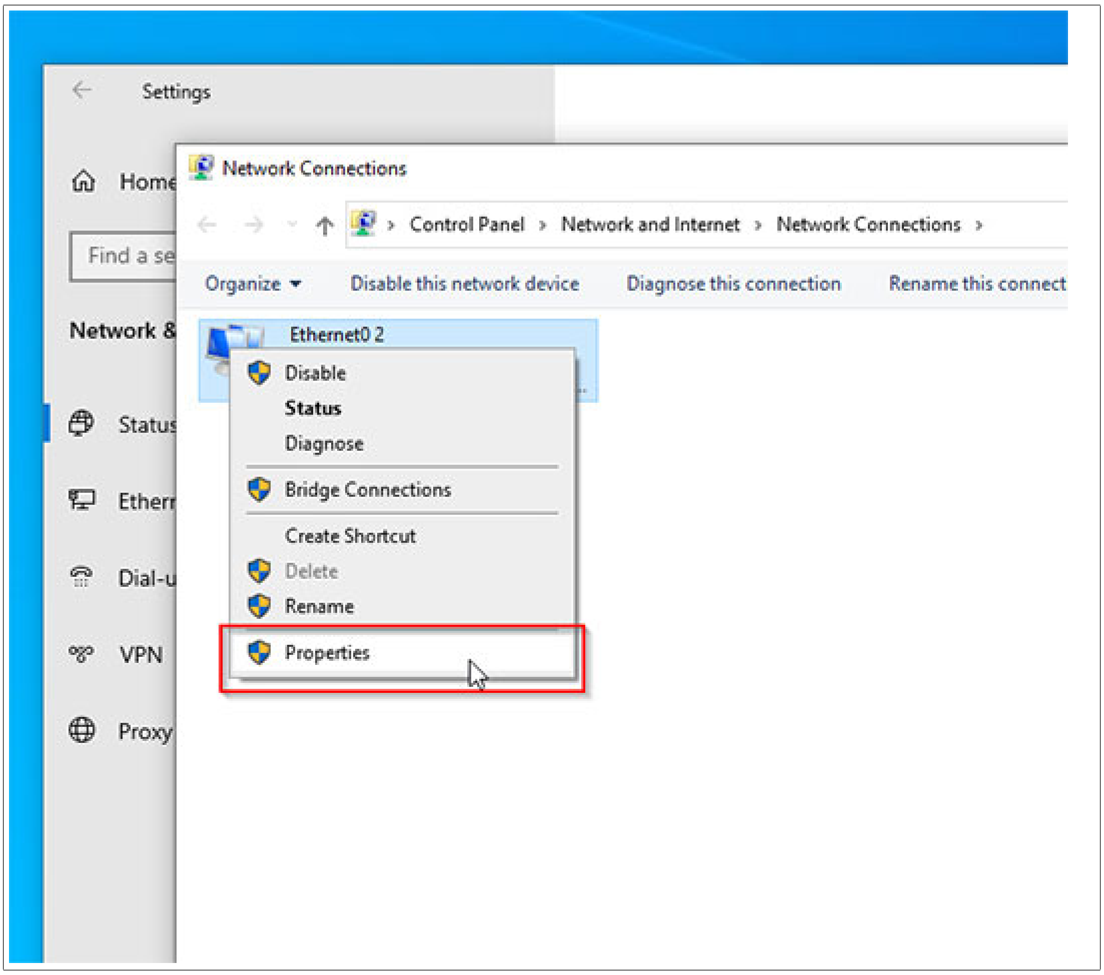
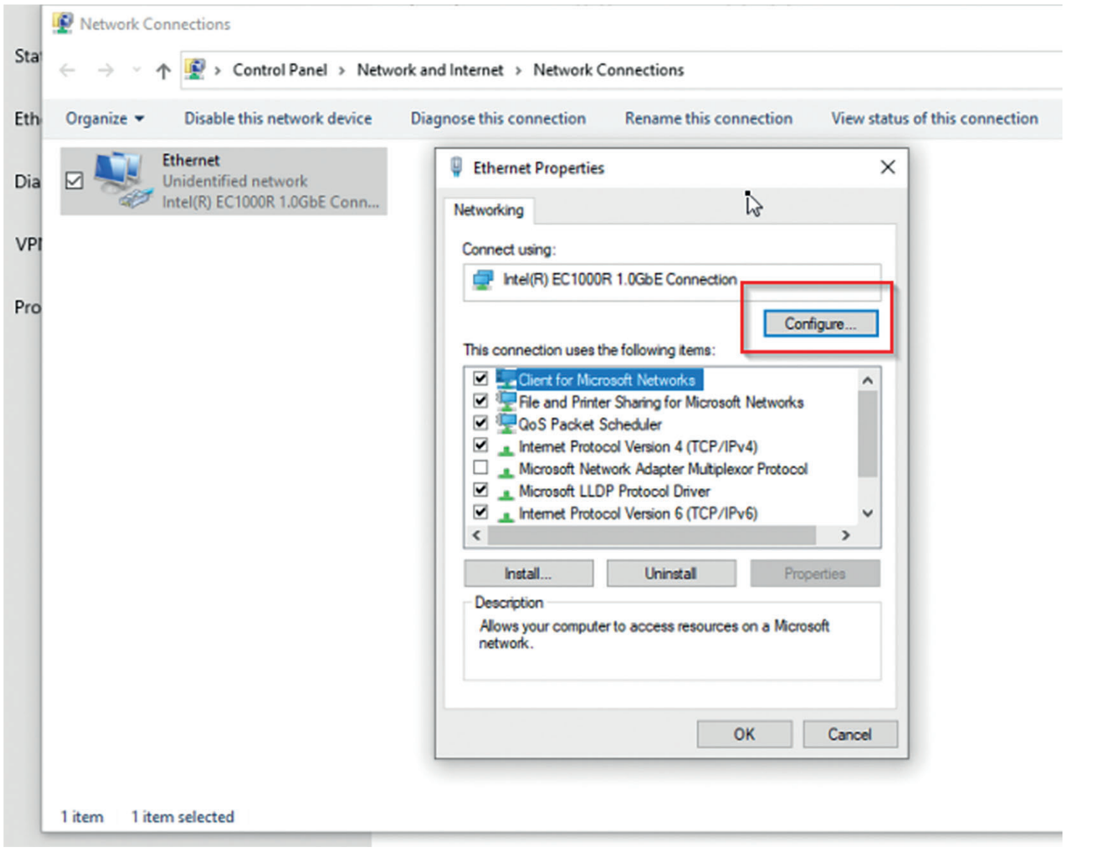


Figure 11.36

4. Click on configure.



Connect using:

Intel(R) EC1000R 1.0GbE Connection

This connection uses the following items:

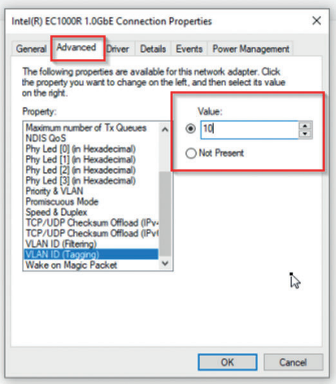
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Allows your computer to access resources on a Microsoft network.

Figure 11.37

5. Open the Advanced Tab, select the "VLAN ID" option and enter your ID.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- Maximum number of Tx Queues
- NDIS QoS
- Phy Led [0] (in Hexadecimal)
- Phy Led [1] (in Hexadecimal)
- Phy Led [2] (in Hexadecimal)
- Phy Led [3] (in Hexadecimal)
- Priority & VLAN
- Promiscuous Mode
- Speed & Duplex
- TCP/UDP Checksum Offload (IPv4
- TCP/UDP Checksum Offload (IPv6
- VLAN ID (Filtering)
- VLAN ID (Tagging)
- Wake on Magic Packet

Value:

● 10

○ Not Present

Figure 11.38

11.12 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 2021 LTSC with multiple network adapters including VisuNet GXP (2020 Generation with Apollo Lake processor and 2024 Generation with Elkhart Lake processor).

Procedure

1. Access the Windows desktop by clicking on "Switch User" in the Configuration View and authenticating as PFAdmin in Windows.
2. Search inside the Windows Taskbar for "Windows PowerShell" and open it.
3. 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.

4. Execute "New-NetSwitchTeam -Name "<team name>" -TeamMembers "<network adapter name 1>", "<network adapter name 2>""
5. 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.
6. 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. See https://www.intel.com/content/www/us/en/support/articles/000032008/ethernet-products.html.
10. A new Network Adapter should appear, which can be configured.

Remove Teaming

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

12 Appendix

12.1 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 6“ 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 6”. 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 6”.

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 6”. 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 6”.

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.

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.

14 - Free and Open-source Software Information

This product contains third party Open Source Software and Free Software distributed under a number of different licenses (hereinafter referred to as "FOSS“). The respective licenses can be downloaded below, and you can obtain comprehensive rights directly from the right holders to the extent specified therein. The FOSS licenses prevail over all other license conditions and contractual agreements with Pepperl+Fuchs with regard to the corresponding FOSS components contained in the product.

At the request of the copyright holders we point out the following: “This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.” This has no effect on any license or warranty agreement between you and Pepperl+Fuchs.

Some of the components are licensed by the copyright holders under a license like the GNU General Public License, Versions 2 and 3, or GNU Lesser General Public License, Versions 2.1 and 3.0 that requires to provide source code of these components. Anyone can obtain the source code for these software components from us on a data carrier (CD-ROM, DVD or USB memory stick). This offer is valid within three years after the most recent distribution of the object code by us. Please send your request to the following email address foss@pepperl-fuchs.com

or via regular mail to the following address:

Pepperl+Fuchs SE
FOSS Compliance
Lilienthalstrasse 200
68307 Mannheim
Germany

Please specify the address to which you wish us to send the source code. Additional product information (e.g. explicit product name, serial number, software version number, etc.) will help us to identify the corresponding source code for you. We may charge a fee to cover the costs of providing the data carrier and shipping it.

If Pepperl+Fuchs has combined or linked certain components with/to components licensed under the GNU LGPL version 2 or later as per the definition of the applicable license and independent from the license of the respective component, the following additional rights apply, if the relevant LGPL license criteria are met:

1. You are entitled to modify the work that uses the Library for your own use, including but not limited to the right to modify the work that uses the Library work to relink modified versions of the LGPL Licensed Module,
2. You may reverse-engineer the work that uses the Library, but only to debug your modifications.

The modification right does not include the right to distribute such modifications and you shall maintain in confidence any information resulting from such reverse-engineering of a combined work.

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

© Pepperl+Fuchs · Subject to modifications