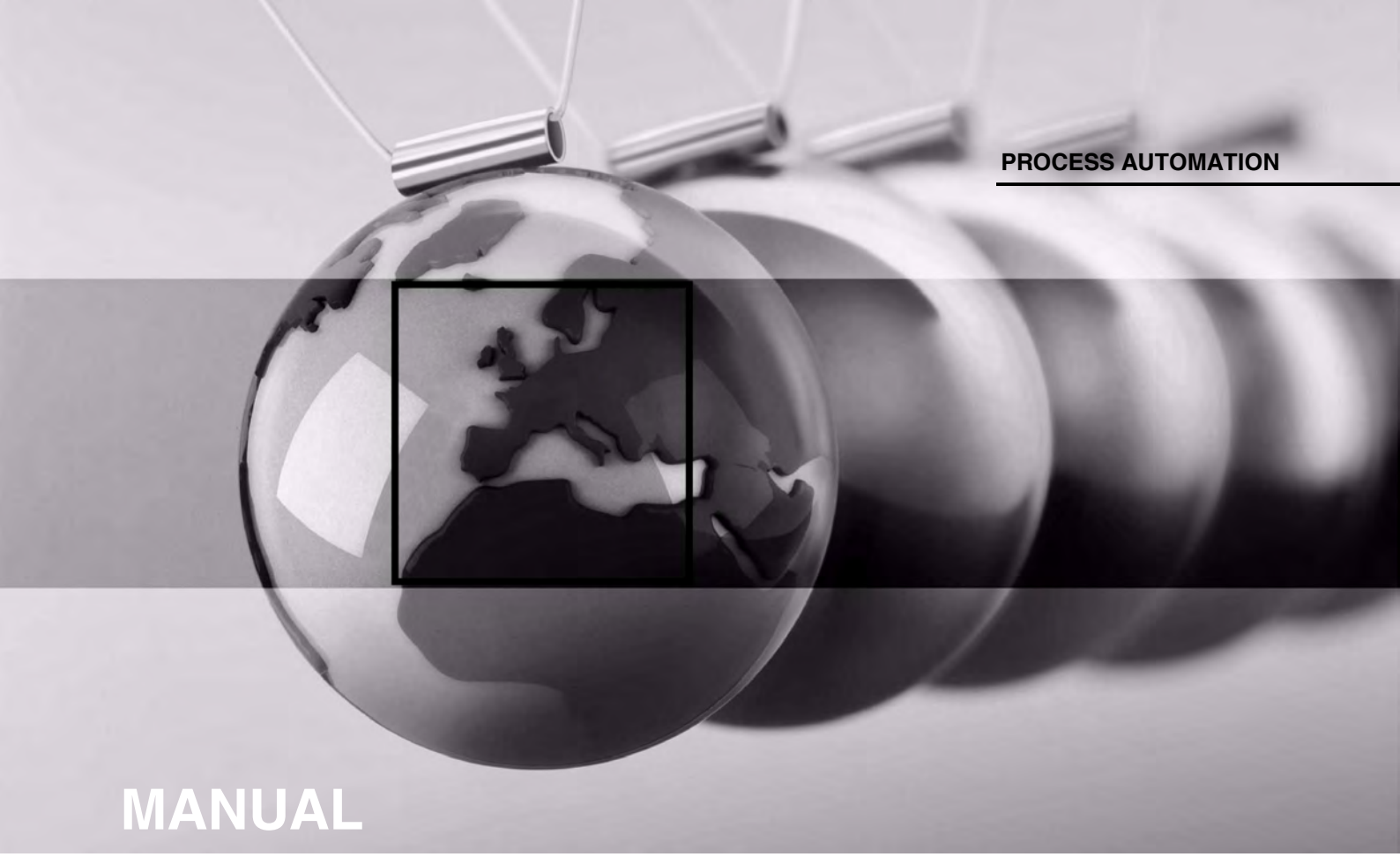


PROCESS AUTOMATION

MANUAL

VisuNet RM Shell 4.2

Version 4.2.0

PEPPERL+FUCHS

PROTECTING YOUR PROCESS

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"

1 VisuNet RM Shell—An Overview

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

With RM Shell, the latest versions of common remote protocol, such as RDP 8.0 or VNC are supported. With these protocols, the RMs can be easily integrated into all major process control systems—whether they are virtualized or conventional, workstation-based setups.

Further, RM Shell has a tailored user interface, which only shows the important system aspects that are relevant for the configuration of the RM. This makes the integration of an RM 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 and touchscreen-optimized design across all protocol editors and a touchscreen-optimized design.

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 the RMs 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 reestablished, backup hosts can be specified in RM Shell to which an RM can automatically connect if a host system fails.

In addition to remote protocols, RM Shell also offers a restricted web browser as an optional feature. This web browser allows fixed addresses to web applications like web-based Manufacturing Execution Systems (MES) to be defined. Operators can only access these pre-defined websites. This helps to further increase the system security and reduce the risk of a malware infiltration from unauthorized websites. The restricted web browser can be enabled via an optional professional license key.

In this manual, the features and functions of RM Shell are described in detail.

2017-08

1.1 First-Start Wizard

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

Configure your basic system settings and click "Next." Accept the terms and conditions on the next window to start using RM Shell.

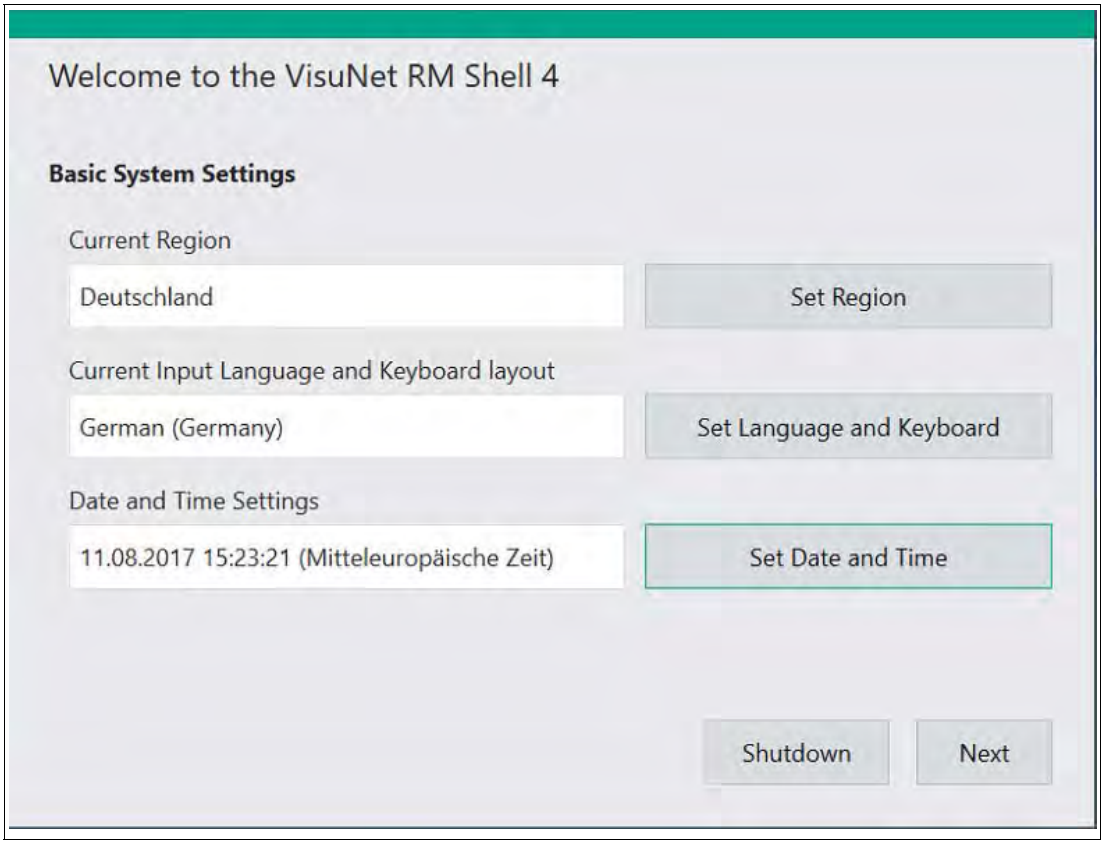


Figure 1.1 First-start wizard

Note!

Correct Information

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

1.2 VisuNet RM Shell User Roles

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

Figure 1.2 Concept of user rights: **O**(perator), **E**(ngineer) and **A**(dministrator)

User Role	Description
Operator (O)	Operators are standard users. They only have access to the profiles. Operators have no access to RM settings.
Engineer (E)	Engineers are responsible for RM setup and integration. They have acces to profiles, system settings, and applications (create, edit, and delete profiles).
Administrator (A)	Administrators have all rights of operators and engineers. In addition, administrators can update the system and enter advanced settings that are not included in the RM Shell itself but in Windows®.

Warning!

Password Protection

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

1.3 Feature List

Feature	RM Shell 4.2.0	Description
Operating system	✔	Based on Microsoft® Windows®
Modern, simplified user interface	✔	Touch-optimized, modern UI
First-start wizard	✔ New feature in version 4.2	An initial setup wizard guides you through the most important steps when configuring an RM for the first time
Process explorer	✔ New feature in version 4.2	Allows you to diagnose an RM and monitor how much RAM, storage, and CPU are being used by local processes.
Remote Protocols & Clients		
MS RDP 8 with RemoteFX	✔	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	✔ Optional PRO license feature	Fast HTML browser that uses Internet Explorer to render websites. Operators can be restricted to visiting only specified websites.
Restricted web browser, based on Chrome engine	✔ Optional PRO license feature	Fast HTML5 browser that uses the Google Chrome rendering engine. Operators can be restricted to visiting only specified websites.
Desktop sharing	✔ Optional PRO license feature	Clone an RM and display its desktop on other RMs (requires RM Shell 4.0.3 or later)
Citrix Receiver 4.8	✔ Optional PRO license feature	Latest version of Citrix Receiver client, compatible with Citrix XenApp & XenDesktop
Raritan KVM Profile	✔ Optional PRO license feature	Client allows you to directly connect to Raritan Dominion KX II-101 V2 KVM-Switch
Security		
Enhanced Write Filter	✔	Prevents local storage of files (e.g., malware, viruses, etc.)
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

2017-08

Feature	RM Shell 4.2.0	Description
Advanced Features		
Auto-connect	✔	Allows you to configure the RM to automatically connect to host systems after startup
Connection loss detection	✔	The RM detects network failures or if a host is unavailable
Backup connection	✔	In case of a network or host failure, an RM can automatically connect to a backup host system
Clean lock	✔	Allows you to temporarily lock the input devices (e.g., touchscreen) when cleaning the device to avoid accidental inputs
Network test tools	✔	A set of network test tools (e.g., ping tool) provide support while commissioning an RM
Task manager	✔	Switch between multiple remote connections and apps that are running on the RM.
Extended desktop support for industrial Box Thin Client BTC01	✔	Remote profile connections can be assigned to different monitors that are connected to the industrial Box Thin Client (BTC01*)
Wireless LAN configuration support	✔	Wireless LAN connections can be managed in RM Shell (requires built-in wireless LAN adapter)
HOSTS file editor	✔	Edit an RM's local network name translation table when no DNS server is available
Centralized management	✔ Optional CC license feature	RMs with RM Shell 4.1 or newer can be managed and configured centrally via VisuNet Control Center.

Ordering Information

Part No.	Model Number
547745	VISUNET-RM-SHELL4-PRO
547751	VISUNET-RM-SHELL4-DRDC
548024	VISUNET-RM-SHELL4-CC

Note!

License Bundles

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

2 VisuNet RM Shell 4.2 User Interface

Home Screen Features

The home screen is divided into 5 basic areas:

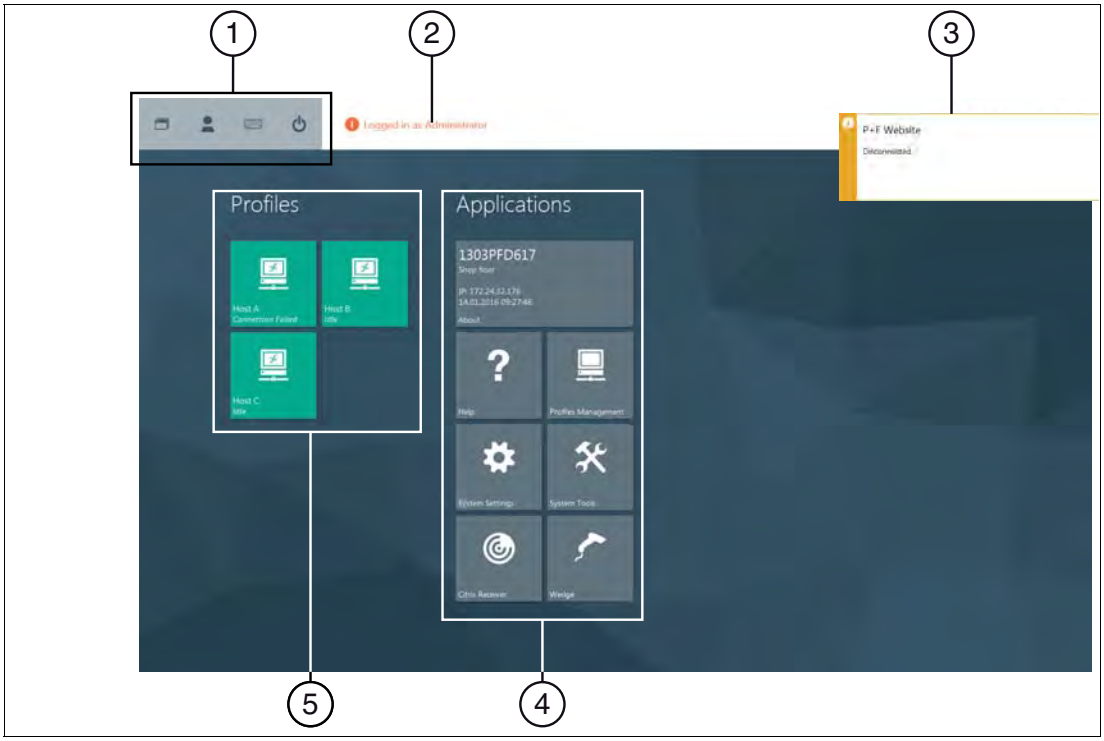


Figure 2.1 RM Shell 4.2 home screen

1	System functions
2	Log-in information
3	Fly-in messages
4	Applications
5	Profiles

1. System Functions

Icon	Description
	RM Shell task manager The RM Shell Task Manager allows you to switch between open connection profiles and applications running on an RM. To open the task manager, click the icon or press the hotkey CTRL+Alt+SCROLL on the keyboard. The task manager shows the currently open remote connections and apps in the form of a window overview. You can change the application by selecting one of the displayed remote connections or apps.
	Switch user role Choose between Operator, Engineer, or Administrator
	Touchscreen keyboard Shows the touchscreen keyboard on the screen.
	Preconfigured power options, such as: ■ Restart ■ Shutdown ■ Power off display The power options can be set up by the Engineer and Administor user roles. The Operator user role is only allowed to run the preconfigured options.

2. Log-In Information

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

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.

4. Applications

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

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

5. Profiles

This section shows all profiles that have been locally created. Every profile has its own profile tile with information on 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	
VisuNet 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	
Disconnected	Profile is not connected to a host	
Connected	Profile is connected to a host PC. A green status bar at the top of the profile tile is visible.	
Connection failed	An error occurred while trying to establish a connection	
Auto connect	If an auto connect is enabled, a defined profile connects automatically to a host. The seconds remaining before the next connection retry are being 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 5.1.	

3 About App

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

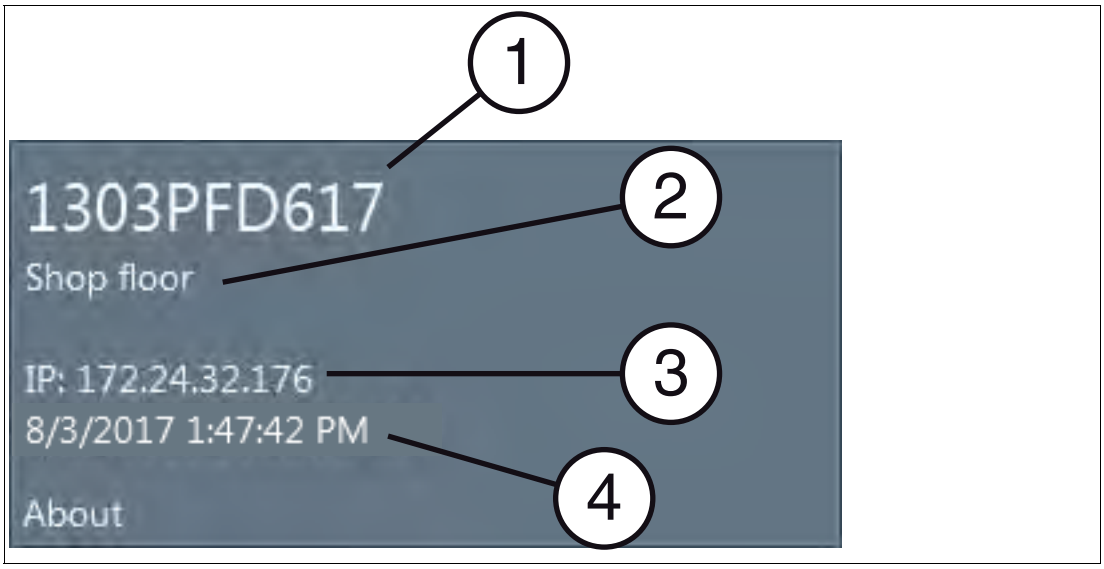


Figure 3.1 The "About" tile on the home screen

1	Computer name of the RM, see chapter 4.1
2	RM description, see chapter 4.1
3	IP address of the RM, see chapter 4.6
4	Current date and time, see chapter 4.1

For additional information, click the "About" tile.

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

- Pepperl+Fuchs GmbH – this submenu provides information on the Pepperl+Fuchs Group
- Hardware, see chapter 3.1
- Licenses, see chapter 3.2
- Software, see chapter 3.3
- (Submenu for GXP-specific information), see chapter 3.3

3.1 Hardware

This submenu provides information on the built-in hardware components (processor, chipset, RAM, boot time) and the serial number of the RM Shell.

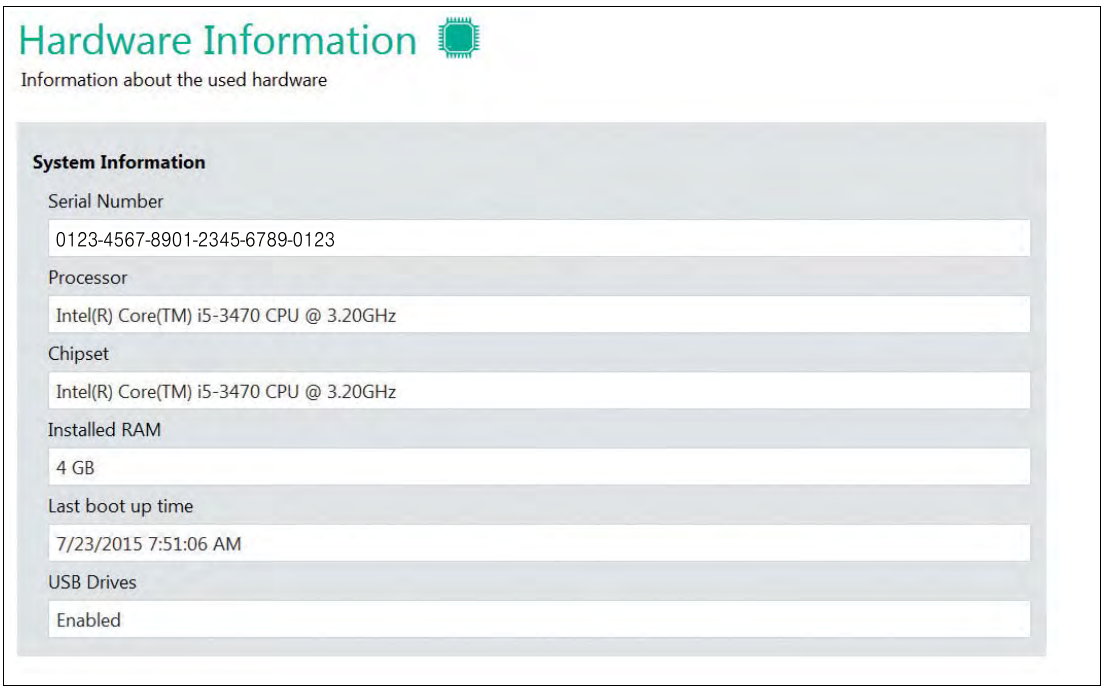


Figure 3.2 Information on the system hardware

3.2 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 GmbH End User License Agreement, see chapter 11.5.

Expanding/Collapsing License Information

1. To expand the license information, use .
2. To collapse the license information, use .

Figure 3.3 License information

3.3 Software

This submenu provides information on the RM Shell version, operating system, system status, and loaded assemblies.

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

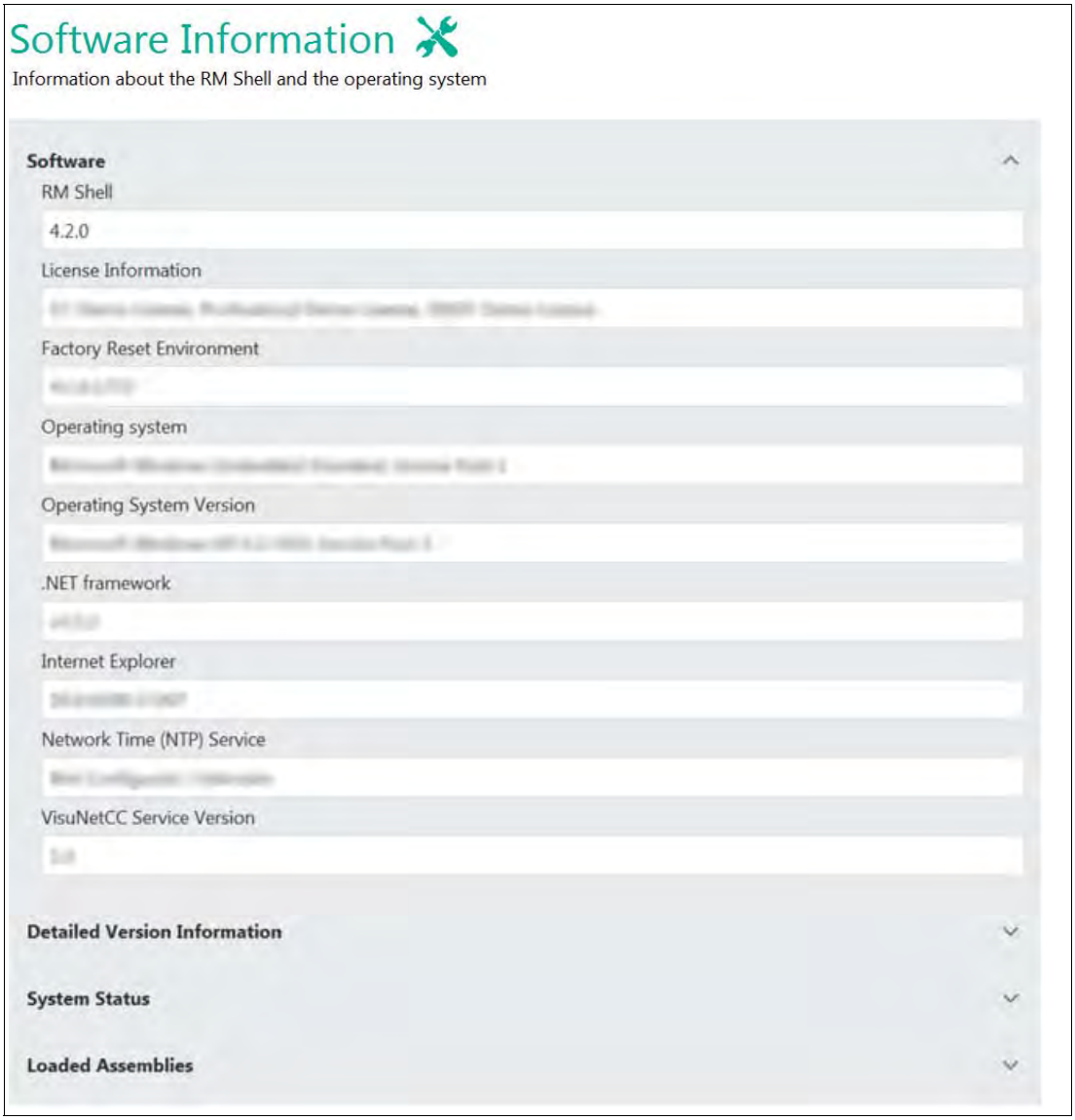


Figure 3.4 Software information

4 System Settings App

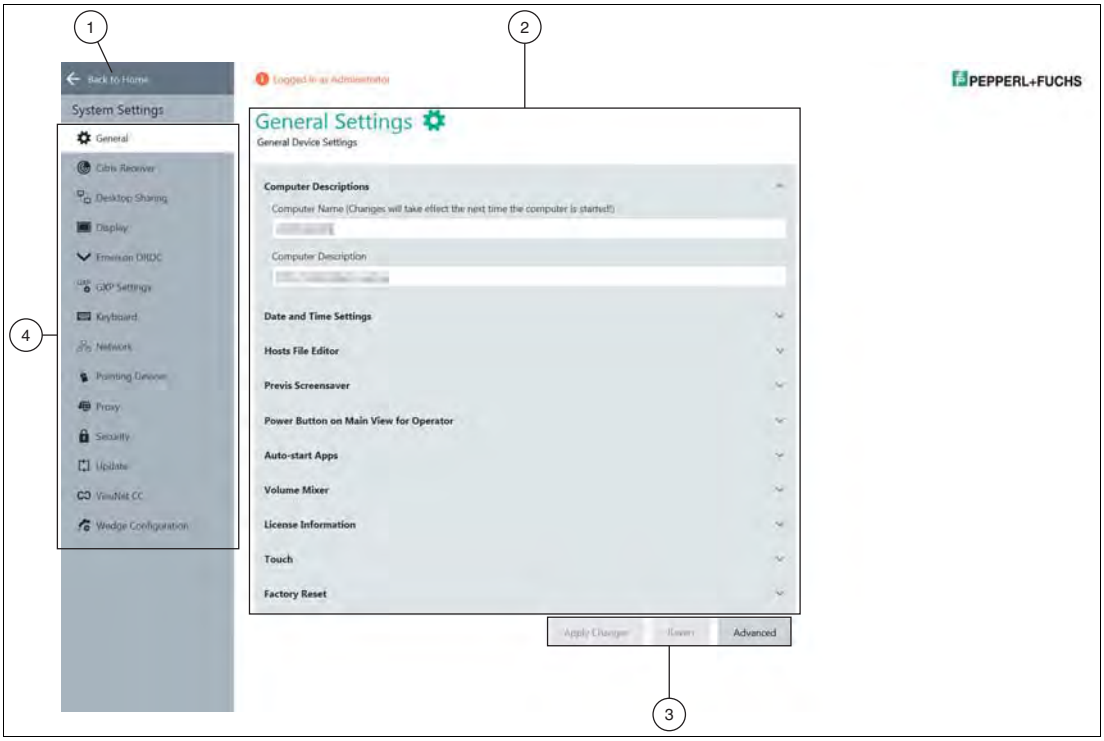


Figure 4.1 Components of the system settings app screen

1	Navigate back to home screen
2	Main Page / content page
3	■ **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 RM Shell but may be of use to Administrators.
4	Navigation bar with all submenus

Note!

Working with Windows®-Specific Advanced Settings

After you change settings via the Windows®-specific Advanced Settings, please reload these settings into the shell by changing the current RM Shell sub-screen once.

Entering System Settings App

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

.

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

- **General**
  Specify general settings such as computer description, system language, date and time, Previs screensaver, power button configuration, and license information. See chapter 4.1.
- **Citrix Receiver**
  Specify Citrix-specific settings. See chapter 4.2.
- **Desktop Sharing**
  Manage the settings for sharing the screen of an RM. See chapter 4.3.
- **Display**
  Manage display settings such as resolution, color depth, and refresh frequency. See chapter 4.4.
- **Keyboard**
  Manage keyboard settings such as input language, character repeat, and cursor blink. See chapter 4.5.
- **Network**
  Manage network settings such as network adapter information and IP address settings. See chapter 4.6.
- **Pointing Device**
  Manage pointing device settings such as sensitivity or button behavior of the pointing device. See chapter 4.7.
- **Proxy**
  Enable proxy and manage proxy settings. See chapter 4.8.
- **Security**
  Set up RM Shell passwords and enable firewalls. See chapter 4.9.
- **Update**
  Enable remote updates or scan for local updates. See chapter 4.10.
- **Wedge Configuration**
  Manage wedge configuration settings such as input character delay and remote text input mode. Define assigned functions for HEX codes. See chapter 4.11.
- **VisuNet CC**
  Configure VisuNet Control Center. See chapter 4.12.
- **Touchscreen**
  Configure GXP touch sensitivity profiles. This submenu is only shown when the RM in use is equipped with this option.

2017-08

4.1 General Settings

Computer Descriptions

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

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

Figure 4.2 General settings - computer descriptions

Date and Time

In this section, you can set up the RM's date and time.

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

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

Figure 4.3 General settings - date and time settings

Caution!

Time Zone, Date, and Time

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

Hosts File

In this section, you can edit the hosts file.

The hosts file is a local text file on an RM that can be used to assign network names (e.g., "server-1") to IP addresses (e.g., "192.168.0.1"). This is usually used when no Dynamic Name Server (DNS) is available in the network that would usually do this name translation.

Figure 4.4 General settings - hosts file

Previs Screensaver

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

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

Function	Description
Idle Time before starting	Configure the time of inactivity. After this time frame, Previs will start. If the time is set to 0 min, the screensaver is disabled.
Effect Intensity	Configure the intensity of the screensaver. Higher values allow better protection against screen burn-in effects.

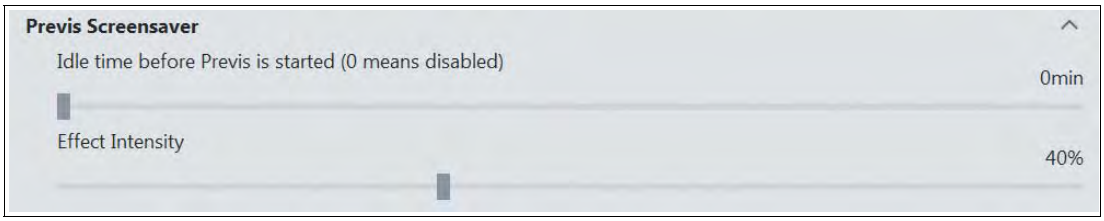


Figure 4.5 General settings - Previs screensaver

Power Button on Main View for Operator

In this section, you can configure the power button behavior, which is located in the system functions on the home screen. See chapter 2.

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

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

Figure 4.6 General settings - power button on home screen for operator

Auto-start Apps

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

Function	Description
On-Screen Keyboard	Causes the on-screen keyboard to start right when the RM starts up.
On-Screen Keyboard Button	Shows a dedicated floating keyboard button that opens the on-screen keyboard.
Citrix Receiver	Causes Citrix Receiver to start when the RM is booted. This enables users in a Citrix XenDesktop/XenApp environment to directly log in.

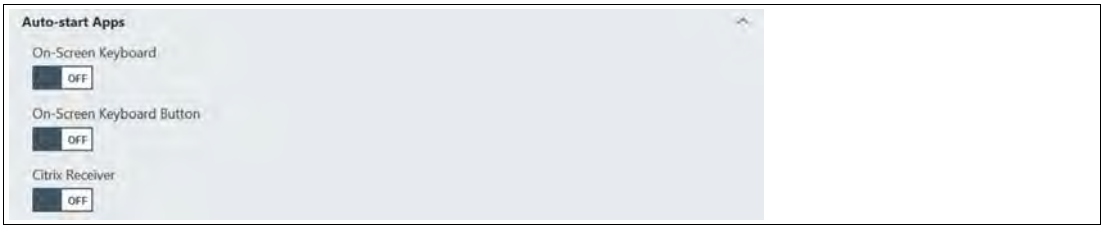


Figure 4.7 General settings - Auto-start apps

Volume Mixer

In this section, you can set the Volume Mixer app to be displayed on the main screen.

Function	Description
Show Volume Mixer App	Enable this option to display the Volume Mixer app on the main screen.

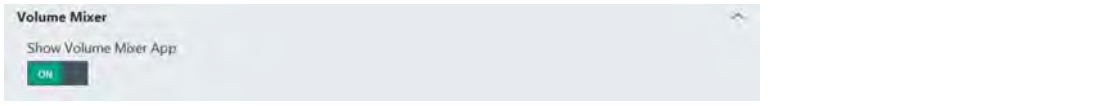


Figure 4.8 General settings - Volume Mixer

When the Volume MIxer is enabled, a new icon appears on the main screen:

Figure 4.9 General settings - Volume Mixer Icon

Note!

The Volume Mixer app is only available on products that have an embedded audio card and an audio interface.

License information

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

Function	Description
Reboot to Factory Reset	If you purchased PRO license keys, enter your license keys to enable additional features of the RM Shell PRO version. Click “Apply.” Changes will take effect after the RM has been rebooted.

Figure 4.10 General settings - license information

Factory Reset

In this section, you can restart the system in factory reset mode. For detailed instructions on performing a factory reset, see chapter 11.2.

Function	Description
License Key	If you purchased PRO license keys, enter the license keys to enable additional features of the RM Shell PRO version. Click “Apply.” Changes will take effect after the RM has been rebooted.

2017-08

4.2 Citrix Receiver

Function	Description
Connection Center	Opens the Citrix-specific window "Citrix Connection Center."
Advanced Preferences	Opens the Citrix-specific window "Advanced Preferences."

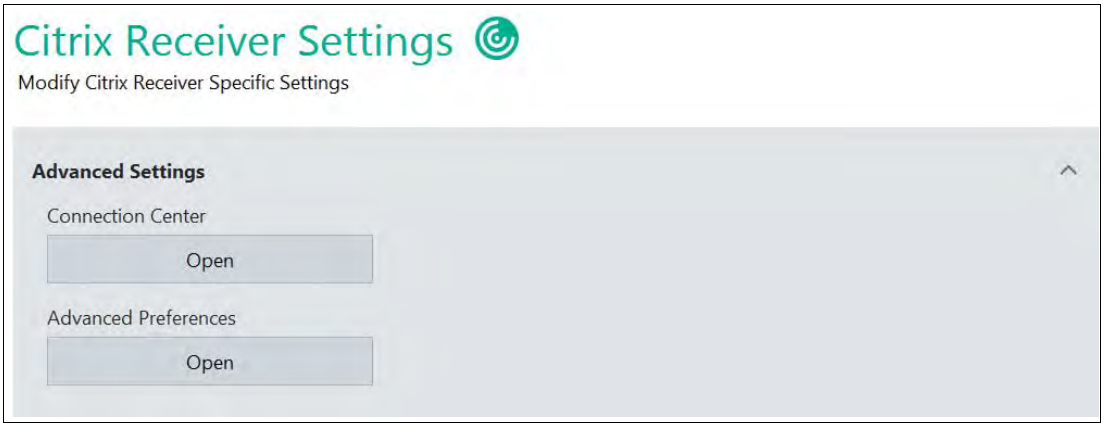


Figure 4.11 Citrix Receiver settings

4.3 Desktop Sharing

Function	Description
VisuNet Dektop Sharing Server Enabled	This function sets up the current RM as a VisuNet RM Master. The function allows other RMs with the corresponding desktop sharing profile to mirror the RM Master's display. For more information, see chapter 5.3.
Share display	Optional setting: If the VisuNet RM Master has multiple external displays (e.g., industrial Box Thin Client BTC01*), you can select which display should be shared with a VisuNet RM Slave.

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 with Control Center.

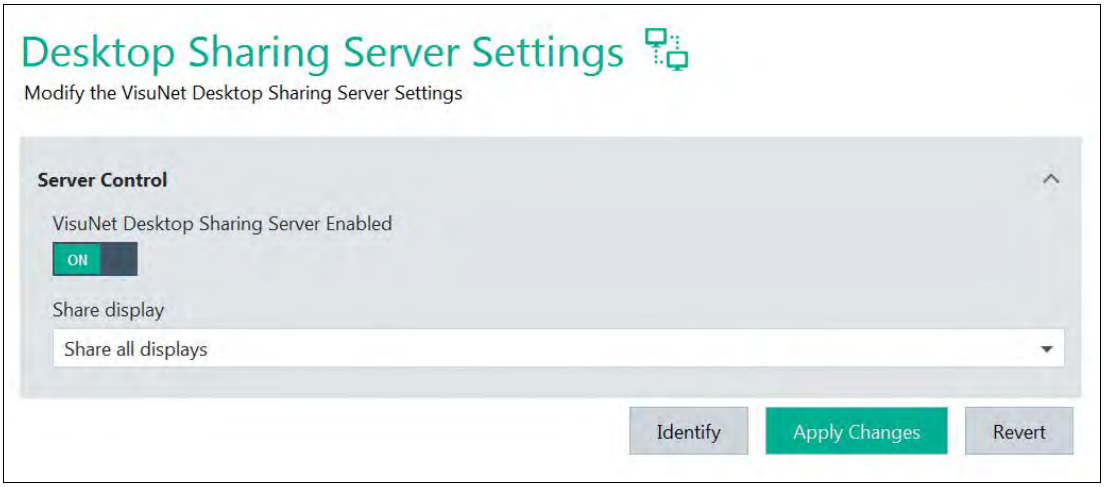
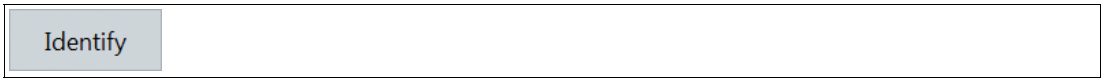


Figure 4.12 Desktop Sharing Server settings

Identify Button

If you are using systems with more than one external display (e.g., extended desktop systems, BTC01*), this button is shown. Use the button to identify the different displays. The number of the respective display is shown on each monitor.



4.4 Display Settings

4.4.1 Configuring a Single Monitor

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

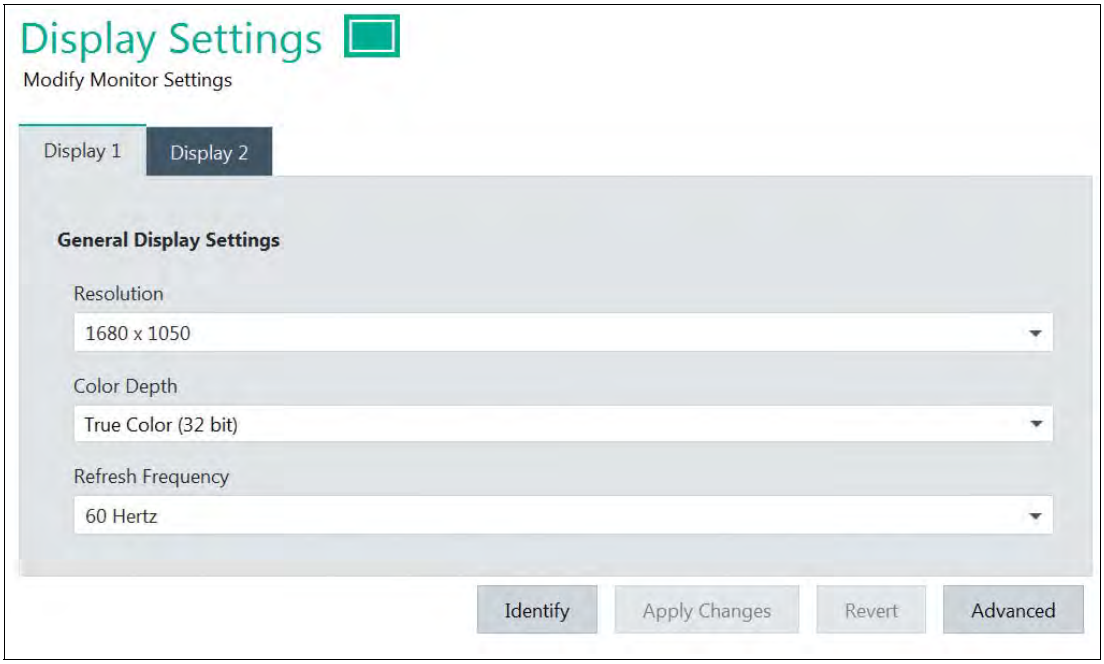


Figure 4.13 Display Settings

Note!

We recommend using the default settings.

Apply/Revert Changes

If you changed settings, the "Apply Changes" button turns green to indicate changes to the current settings.

1. To save the changes, click 

.

   ↳ The changes have been saved.

2. If you want to discard the changes, click 

.

   ↳ The changes have been discarded. The settings have been set back to the last saved version.

Note!

Advanced Settings

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

Identify Button

If you are using systems with more than one external display (e.g., extended desktop systems, BTC01*), this button is shown. Use the button to identify the different displays. The number of the respective display is shown on each monitor.

4.4.2 Configuring Multiple Monitors

When you use a Box Thin Client BTC01* with multiple monitors, each monitor is presented as an individual tab in the display settings view.

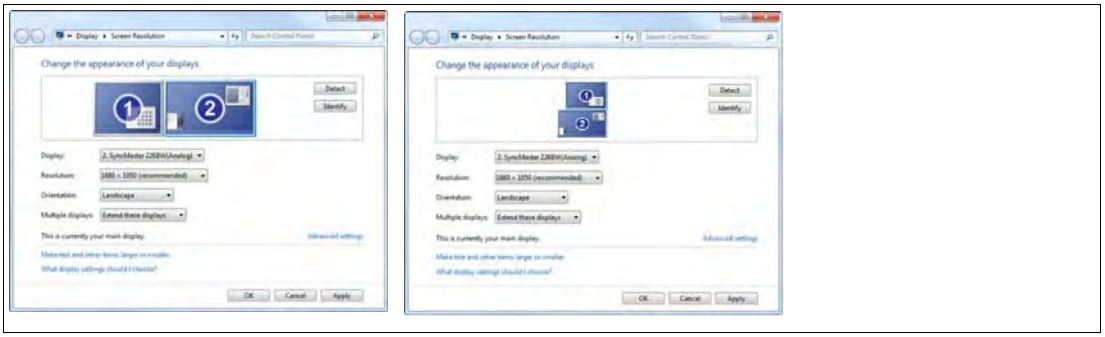
The “Identify” button can be used to check the display numbering of the connected monitors.

To change the orientation/order of the connected monitors, please 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.



4.5 Keyboard Settings

Input Language

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

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

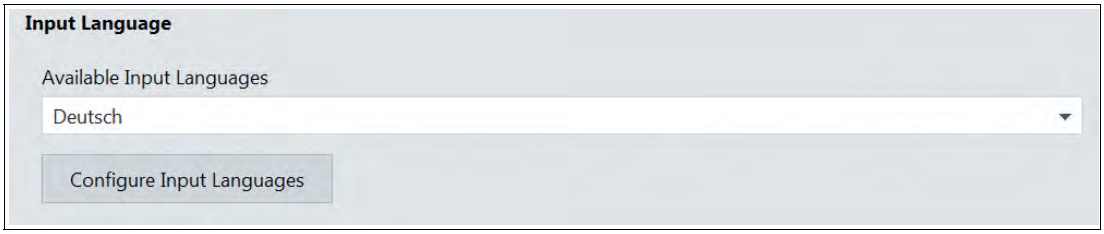


Figure 4.14 Keyboard settings - input language

Character Repeat

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

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

Figure 4.15 Keyboard settings - character repeat

Cursor Blink

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

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

Figure 4.16 Keyboard settings - cursor blink

Apply/Revert Changes

If you changed settings, the "Apply Changes" button turns green to indicate changes to the current settings.

1. To save the changes, click Apply Changes.

   ↳ The changes have been saved.

2. If you want to discard the changes, click Revert.

   ↳ The changes have been discarded. The settings have been set back to the last saved version.

Note!

Advanced Settings

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

4.6 Network

Network Adapter Information

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

Function	Description
Network Adapter Information	All information about the local RM's 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 Protocoll). With DHCP, you can integrate the RM 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. However, you can set up all these parameters manually by disabling the DHCP option.

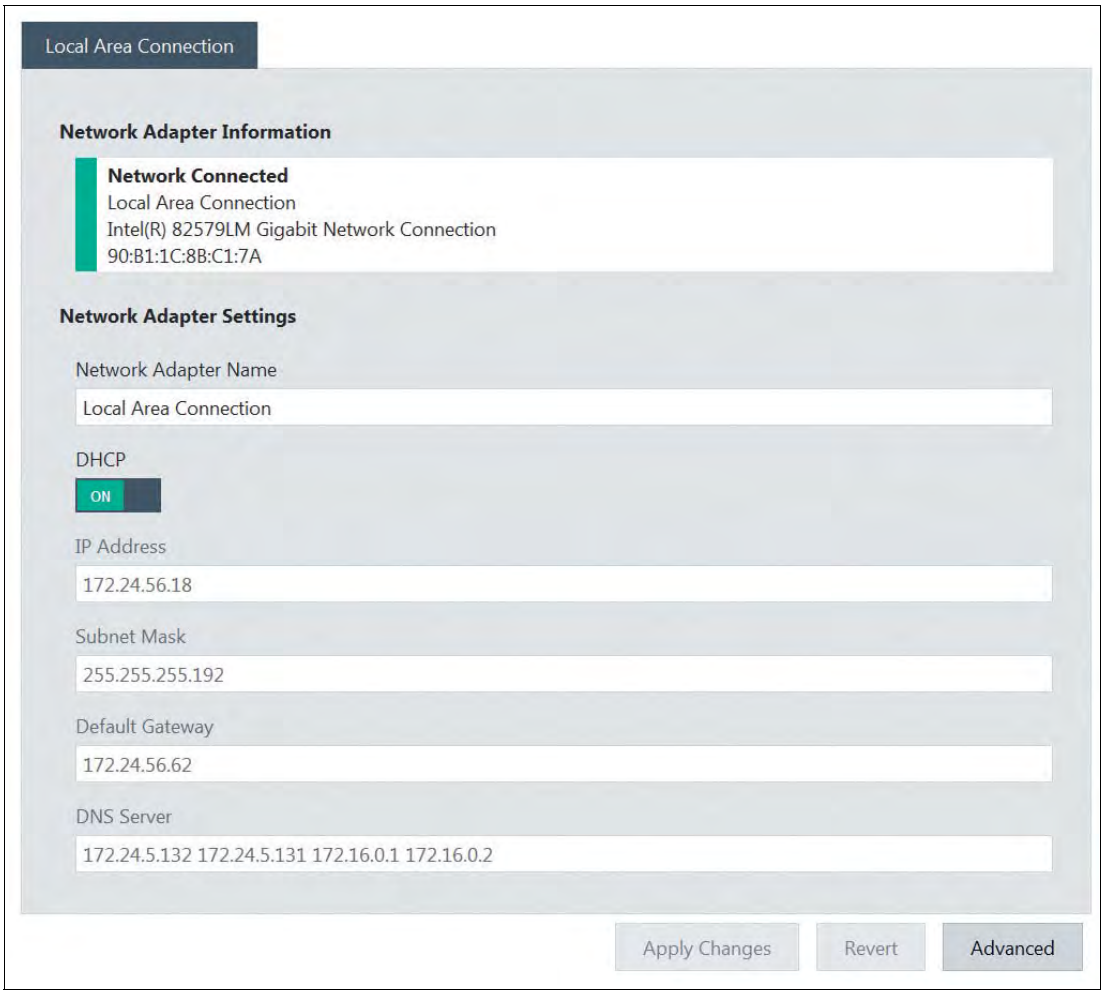


Figure 4.17 Network adapter information and settings

Note!

Open Network Ports

The open network ports that are used in RM Shell are listed in the appendix. See chapter 11.1.

2017-08

PEPPERL+FUCHS

Apply/Revert Changes

If you changed settings, the "Apply Changes" button turns green to indicate changes to the current settings.

1. To save the changes, click Apply Changes.

   ↳ The changes have been saved.

2. If you want to discard the changes, click Revert.

   ↳ The changes have been discarded. The settings have been set back to the last saved version.

Note!

Advanced Settings

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

4.7 Pointing Device Settings

Note!

System Reboot

Changing the mouse settings requires a system reboot.

Pointing Device Sensitivity Settings

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

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

Figure 4.18 Pointing device settings - sensitivity settings

Pointing Device Button Behavior

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

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

Figure 4.19 Pointing device settings - button behavior

Extended Settings

Function	Description
Safe Mode Pointing Device Detection	The safe mode feature increases the initialization reliability of the pointing devices (e.g., touch pad). If you encounter problems with your pointing device, for instance, if it is not working right away after system start, enable this feature. If you do not encounter problems with the pointing device, this setting should be disabled. This setting is turned off by default.

Figure 4.20 Pointing device settings - extended settings

Apply/Revert Changes

If you changed settings, the "Apply Changes" button turns green to indicate changes to the current settings.

1. To save the changes, click Apply Changes.

   ↳ The changes have been saved.

2. If you want to discard the changes, click Revert.

   ↳ The changes have been discarded. The settings have been set back to the last saved version.

Note!

Advanced Settings

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

4.8 Proxy Settings

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

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

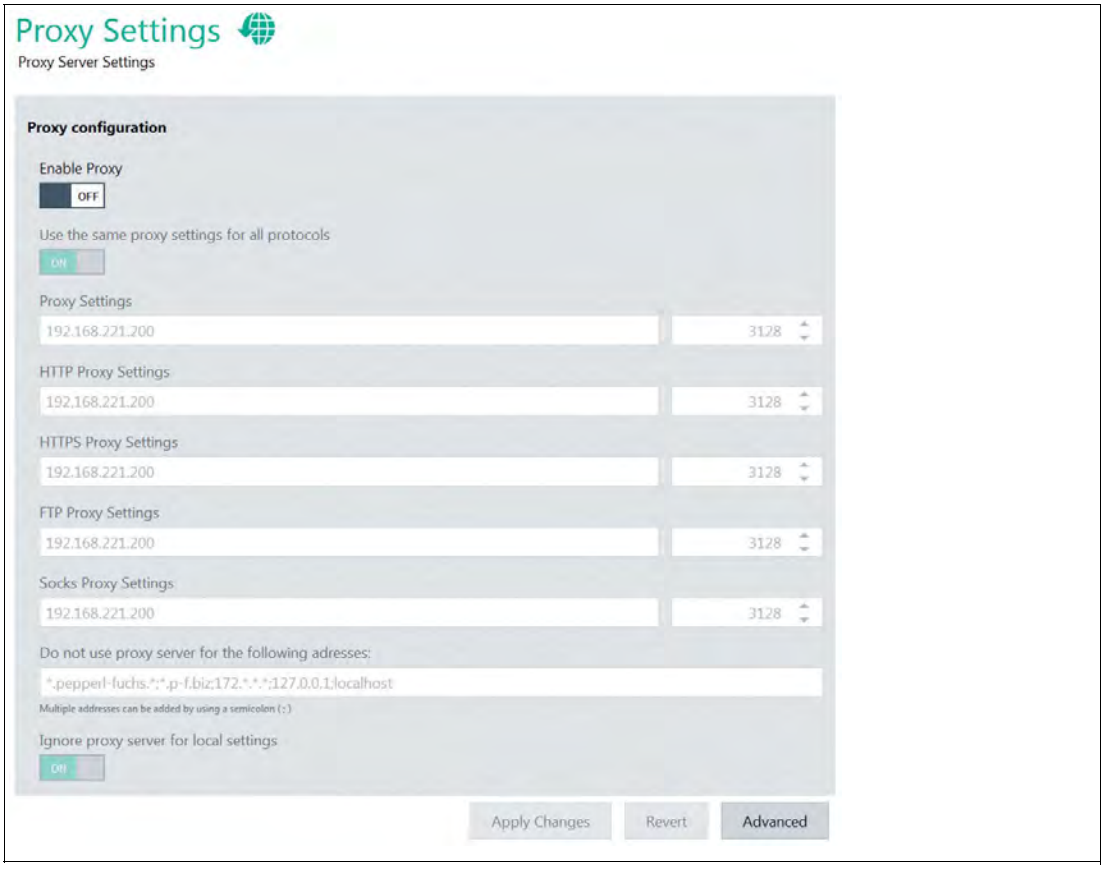


Figure 4.21 Proxy settings

Apply/Revert Changes

If you changed settings, the "Apply Changes" button turns green to indicate changes to the current settings.

1. To save the changes, click 

.

   ↳ The changes have been saved.

2. If you want to discard the changes, click 

.

   ↳ The changes have been discarded. The settings have been set back to the last saved version.

Note!

Advanced Settings

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

4.9 Security

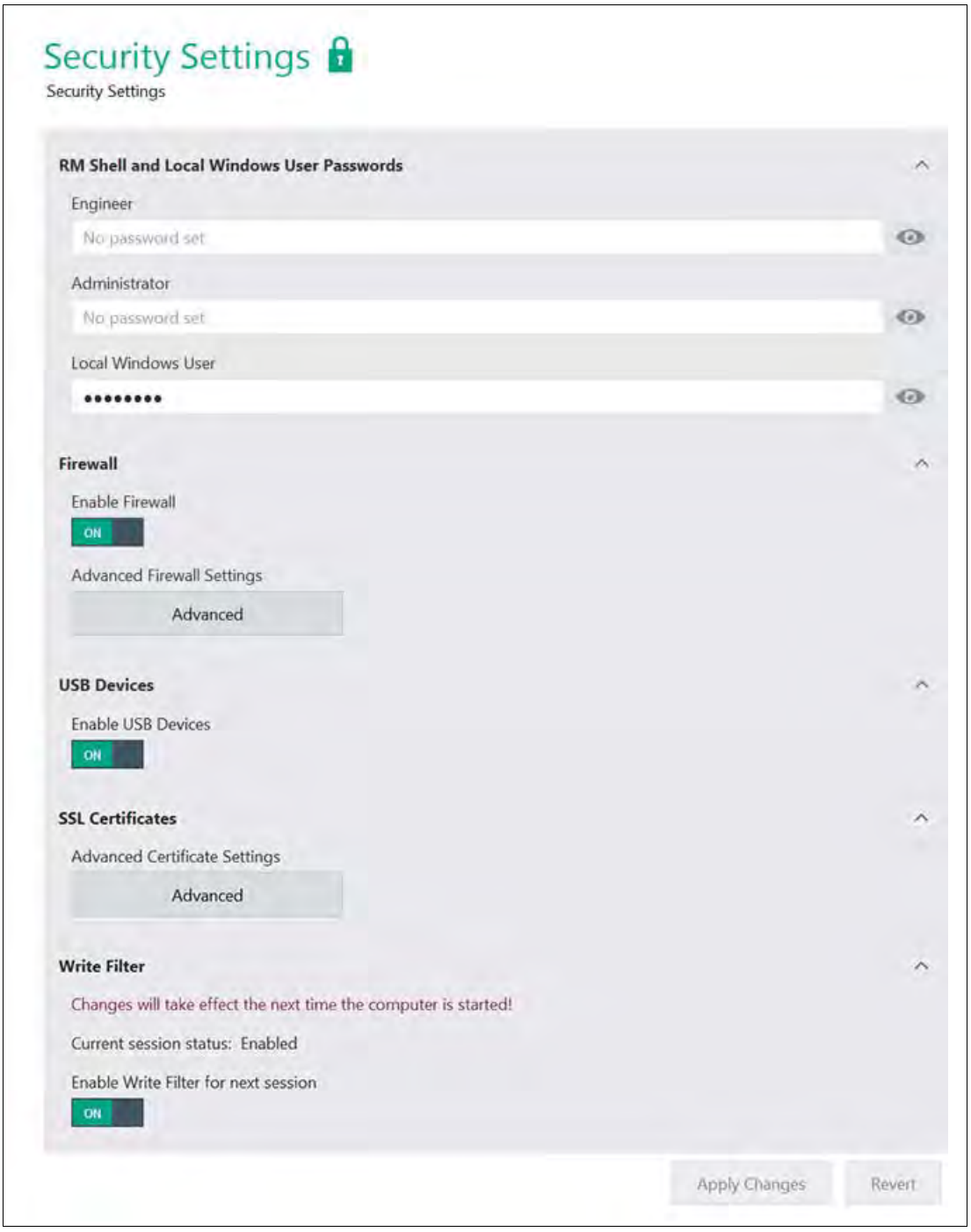


Figure 4.22 Security settings - RM Shell passwords

RM Shell and Local Windows® User Passwords

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

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

Firewall

In this section, you can adjust the firewall settings.

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

Figure 4.23 Security settings - firewall

2017-08

USB Devices

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

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

Figure 4.24 Security settings - USB devices

SSL Certificates

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

Figure 4.25 SSL certificates - edit Microsoft-specific certificate settings

Write Filter

In this section, you can enable or disable the enhanced write filter.

Figure 4.26 Security settings - write filter

Apply/Revert Changes

If you changed settings, the "Apply Changes" button turns green to indicate changes to the current settings.

1. To save the changes, click Apply Changes.
   ↳ The changes have been saved.
2. If you want to discard the changes, click Revert.
   ↳ The changes have been discarded. The settings have been set back to the last saved version.

4.10 Update

In this section, you can update RM Shell to latest version. The update submenu is only available for the Administrator user role.

There are 2 ways to update the VisuNet RM Shell:

- Update via network shared folder
- Update via local device (e.g., USB stick)

Figure 4.27 System settings - update

Updating via Network Shared Folder

You can update RM Shell via the local area network. Both the RM and the PC from which you want to copy the update file to the RM must be connected in the same LAN. The update file is imported by means of a network shared folder, which you can access from the PC.

Creating a network shared folder

In the "Find update" section, click Create.

↳ The network shared folder "update" has been created automatically.

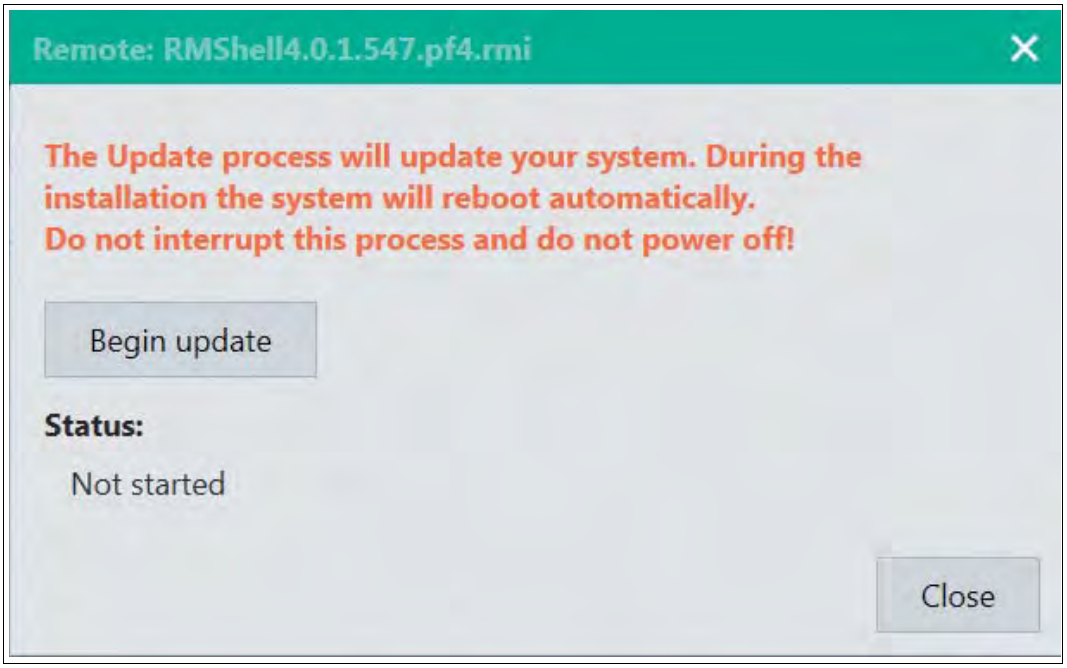
Importing the Update File

1. Copy the latest update file (ending "*.pf4.rmi") from the PC to the RM's shared network folder "update." You can access the shared network folder by entering the RM network name, followed by the "update" folder into the Windows explorer of the PC (e.g., "\\RM12345\update").

   ↳ On the RM, the update file appears in the "Available updates" section. The prefix "Remote" shows that the file is network-shared.

2. Choose the requested update file by clicking .

   ↳ The "Begin update" dialog box opens.



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

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

Updating via Local Device

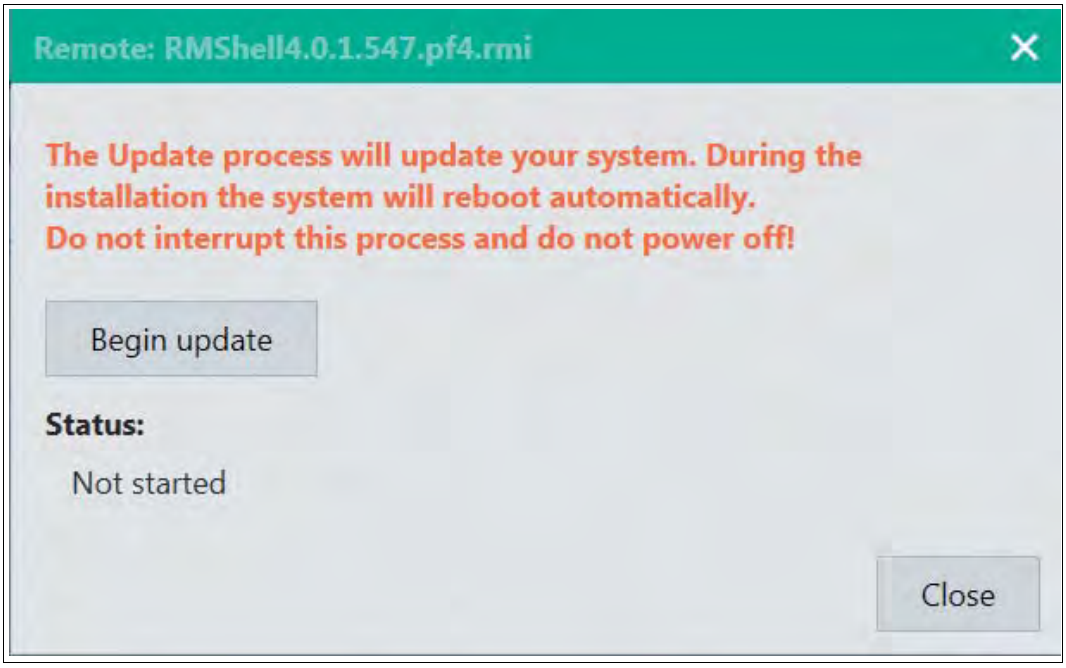
You can update the VisuNet RM Shell by using a local device (USB pen drive) with the current update files.

Updating via local device

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

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

   ↳ The "Begin update" dialog box opens.



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

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

4.11 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 and Citrix connections.

Figure 4.28 S2K Wedge configuration - general settings

Port Specific Settings

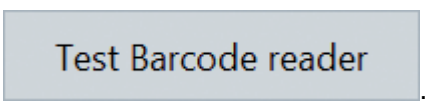
Choose the serial port that the barcode scanner is connected to and configure it by clicking the corresponding tab.

Figure 4.29 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 you want to test.
2. Click 

.

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

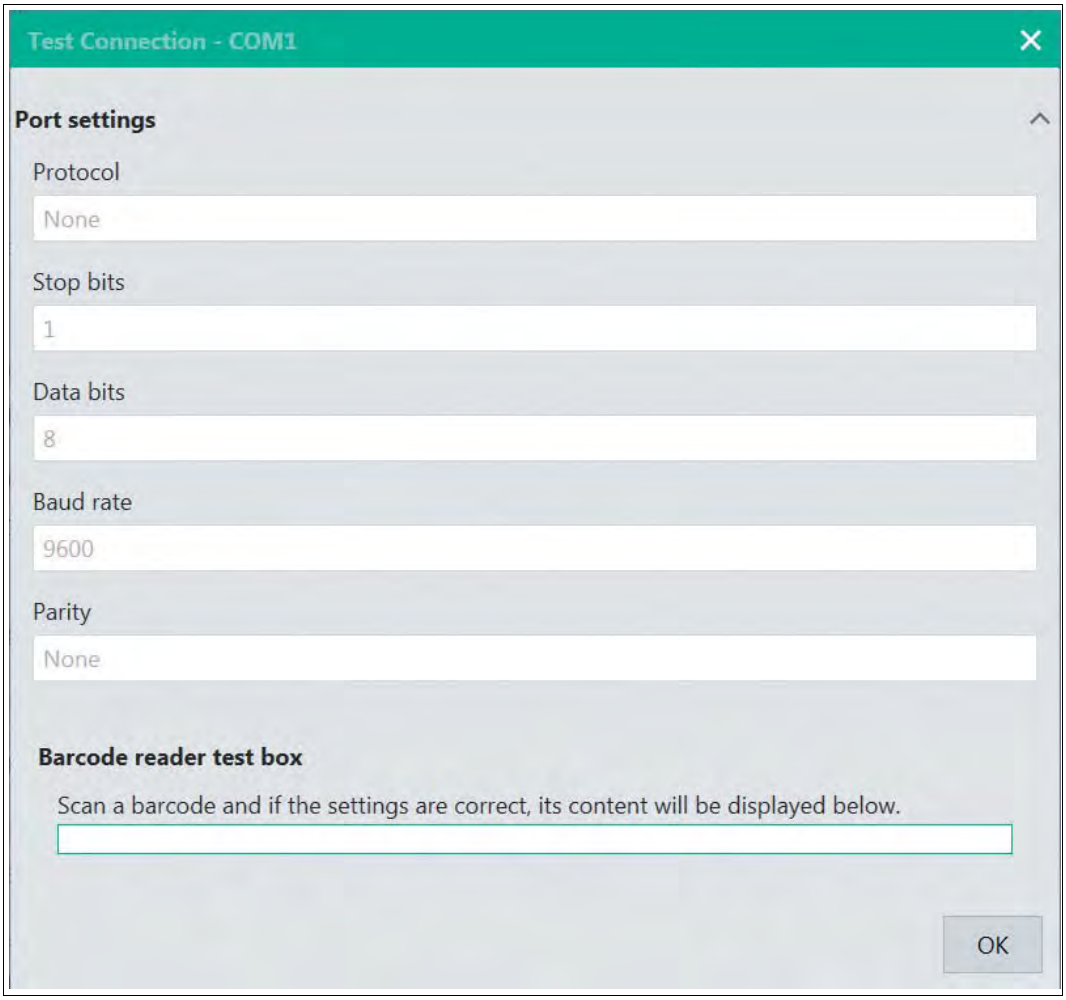


Figure 4.30 Test connection window

3. Use you PSCAN device to scan a barcode.

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

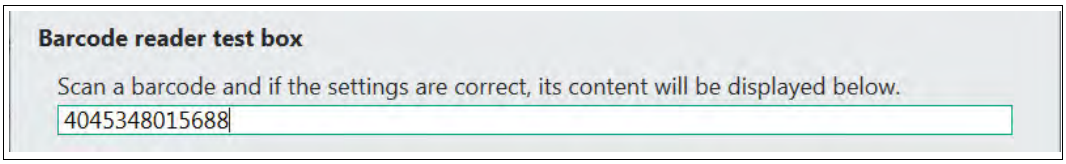


Figure 4.31 Scanner test box

4. To end the test, click 

.

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 or not the parity check bit should be computed, and if so how.
Auto Connect	If enabled, the VisuNet RM Shell automatically opens the serial port and establishes a connection to the barcode scanner, if the RM is (re-)booted.
Visible on Operation screen	If enabled, the serial port is visible as a serial port in the VisuNet Wedge App.

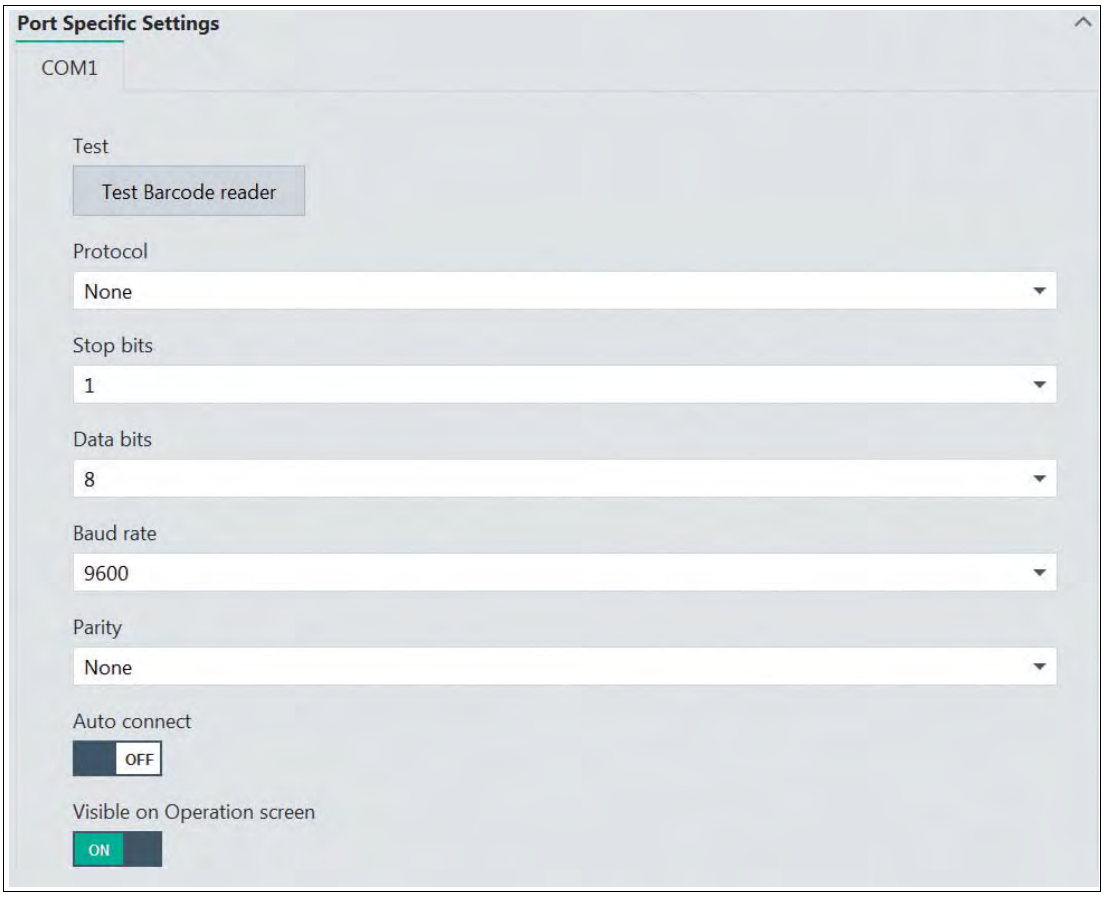


Figure 4.32 Wedge configuration - port specific settings

Function Key Emulation

The character strings from the serial port are transferred into keystrokes according 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 a variety of actions. In the function key emulation section, you can configure different actions for each control character by using the dropdown list.

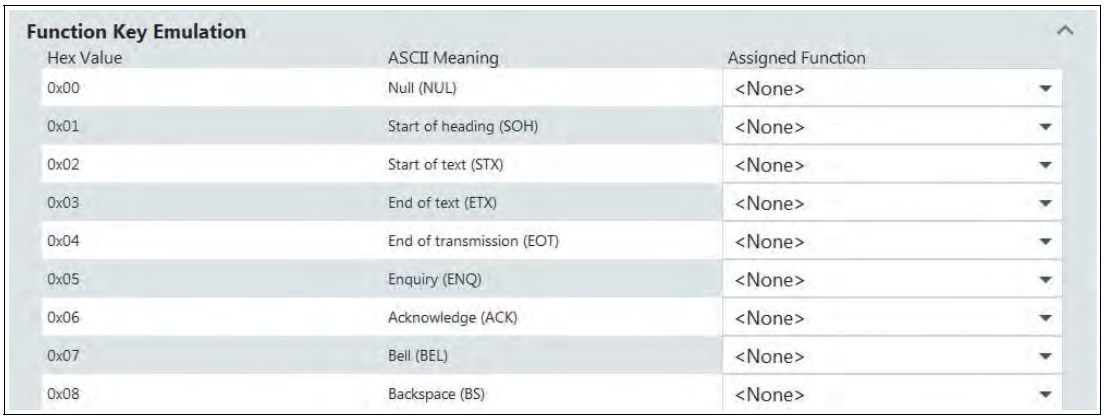


Figure 4.33 Wedge configuration - Function Key Emulation

4.12 VisuNet CC Settings

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.

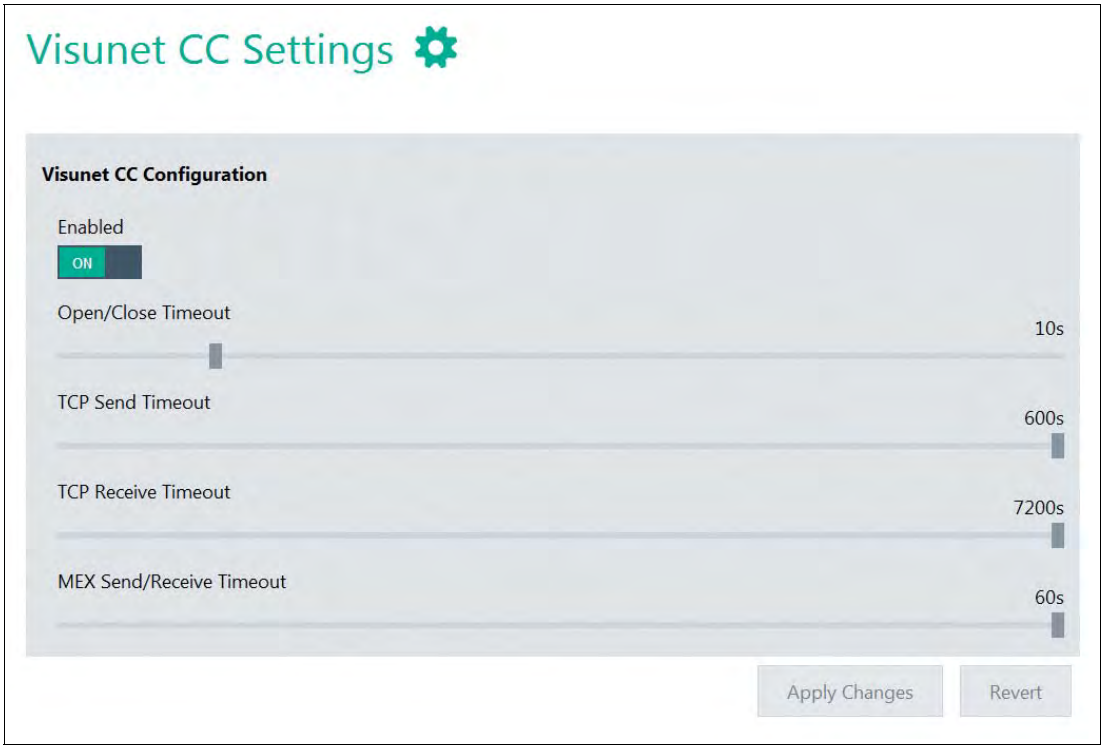


Figure 4.34 VisuNet CC settings

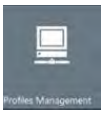
5 Profiles Management App

Create and manage remote connection profiles with the Profiles Management App.

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

Figure 5.1 The profiles management home screen. Initially, the profiles list is empty.

Entering Profiles Management App

To enter the profiles management app, click the appropriate icon on the home screen 

.

Creating a New Connection Profile

1. To create a new connection profile, click + New profile.
2. Select your required connection profile type, and click “Ok.”

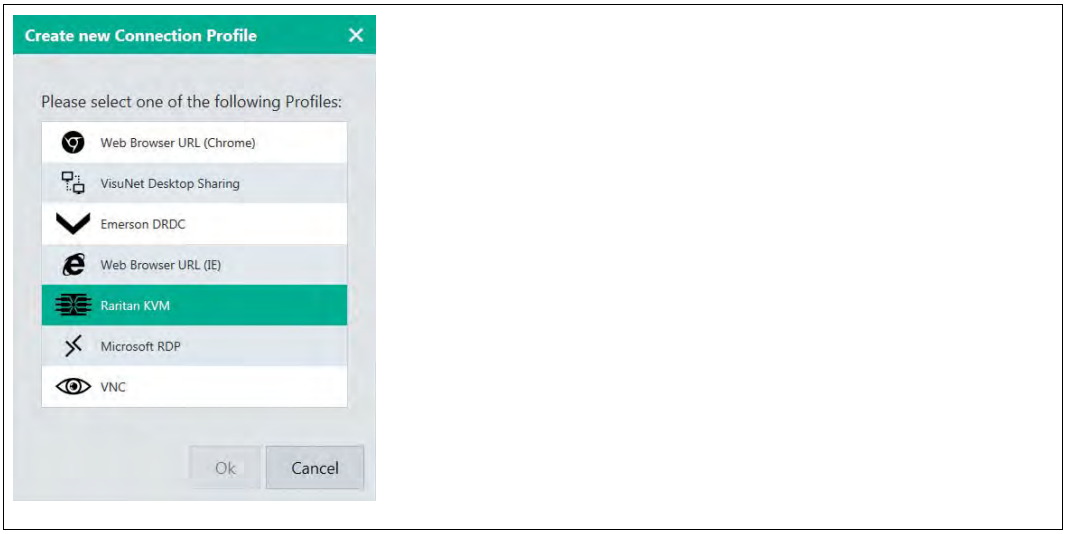


Figure 5.2 The "Create new Connection Profile" dialog box - web browser, Raritan KVM and VisuNet desktop sharing profiles are only available in the pro version.

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

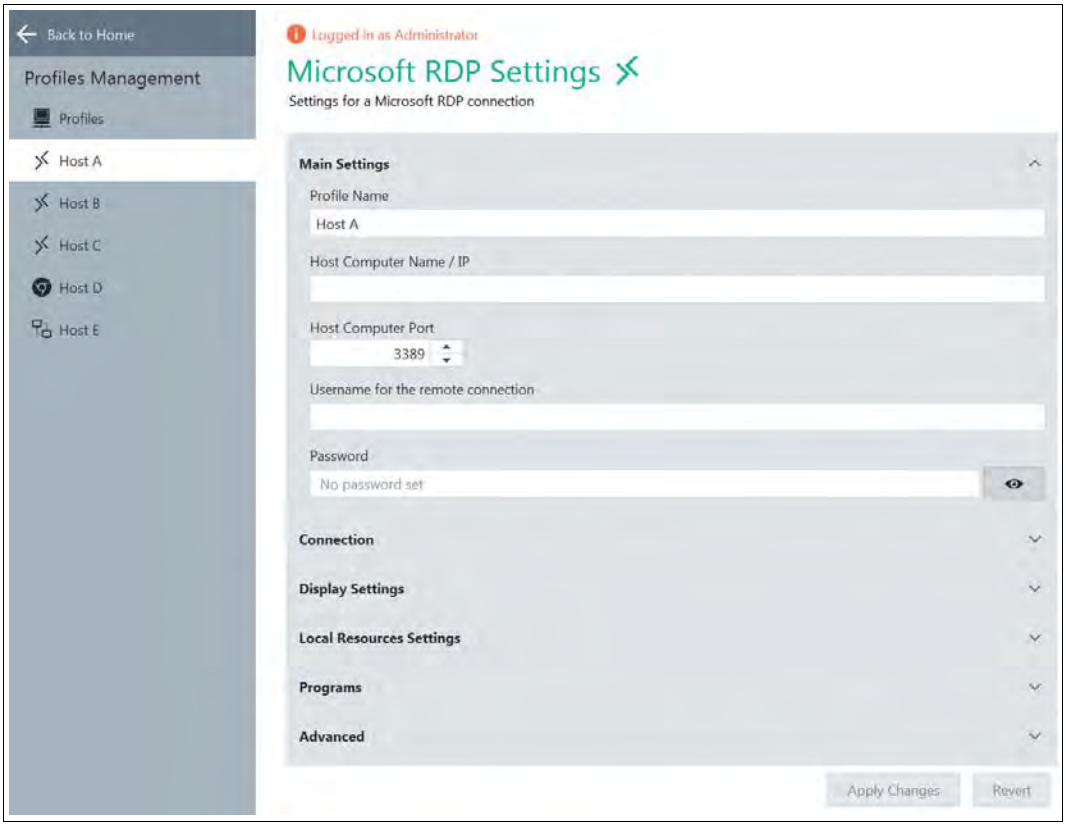


Figure 5.3 Main settings of a Microsoft RDP profile

Editing the Profile Settings

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

   ↳ The changes have been saved.

5.1 Connection Features

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

- Auto Connect
- Retry
- Backup Connection

"Auto Connect" Feature

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

Setting up Auto Connect

1. Go to Profile Settings.

2. To set up the auto connect for a profile, click  .

   ↳ The "Connection Features" dialog box opens.

3. Check the "Enable Auto Connect" box.

Figure 5.4 Auto connect options

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

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

Figure 5.5 Profile with preconfigured auto connect (as shown in the profiles list): in this example, VisuNet RM Shell automatically establishes a connection to the RD - 2 profile after 10 seconds.

Note!

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

"Retry" Feature

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

Setting Up Retry Feature

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

   ↳ The "Connection Features" dialog box opens.

3. Check the "Enable Retry" box.

Figure 5.6 Retry options

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

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

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

"Backup Connection" Feature

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

Setting Up Backup Connection

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

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

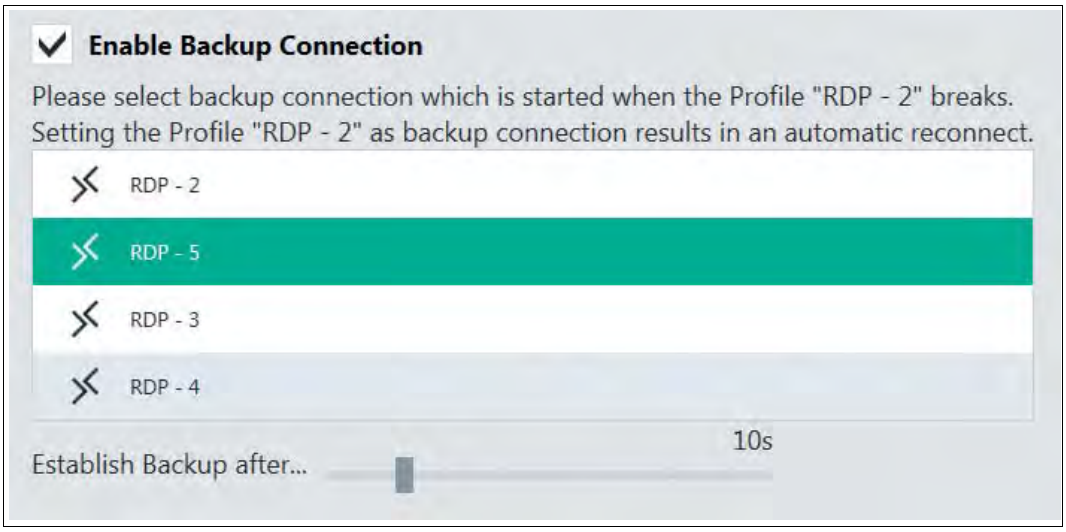


Figure 5.7 Backup connection options

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

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

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

In this example, the RM connects automatically to a predefined host A. If the connection fails, the RM 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 automatically reconnects to the host when it is rebooted.

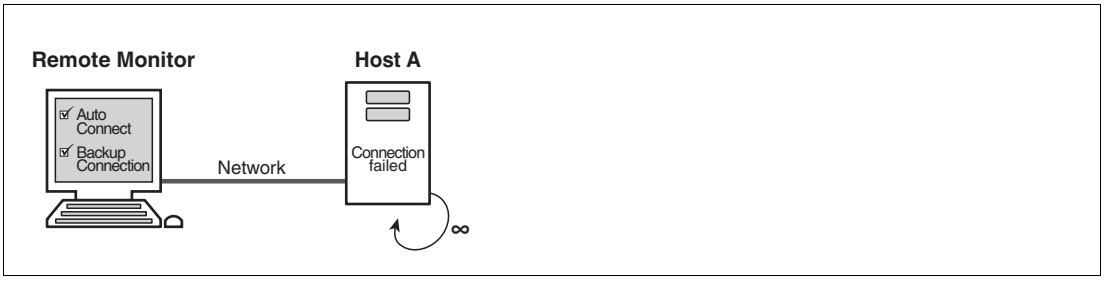
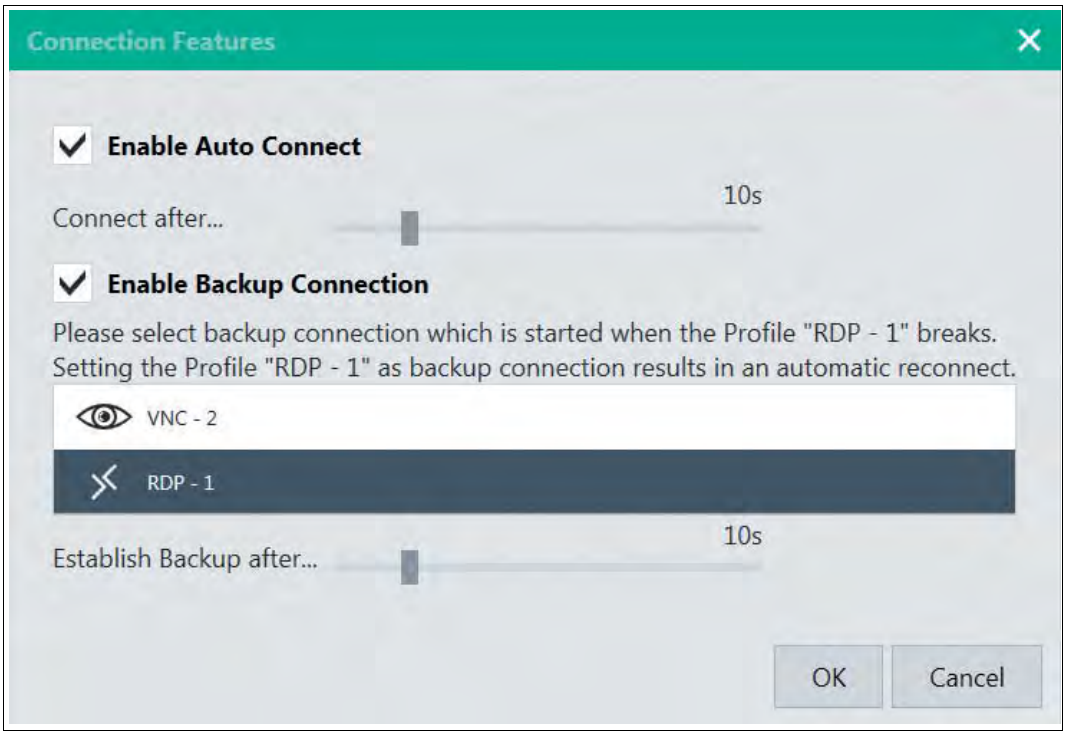


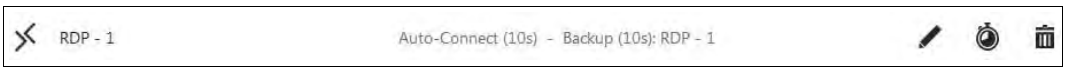
Figure 5.8 Example 1 - Unlimited number of retries to a specific host (with "Backup Connection" feature)

Setting Up a Continuous Connection to a Specific Host

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



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



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

In this example, the RM connects automatically to a predefined host A. If the connection fails, the RM 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 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 to connect to a backup server if the main server fails.

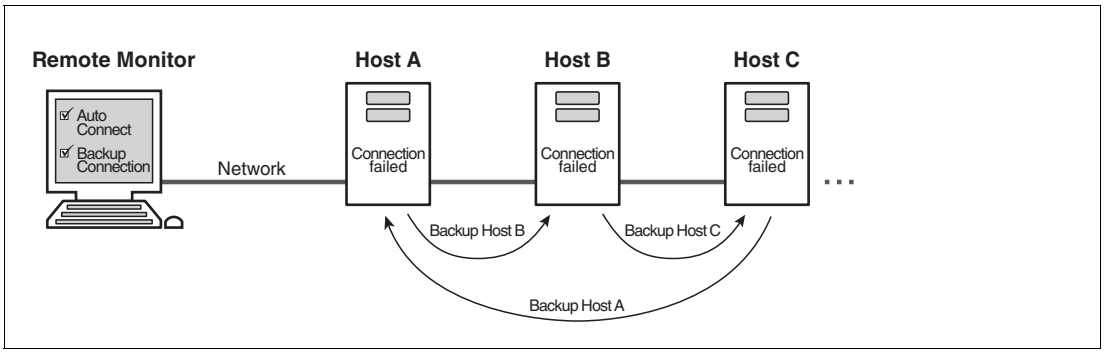
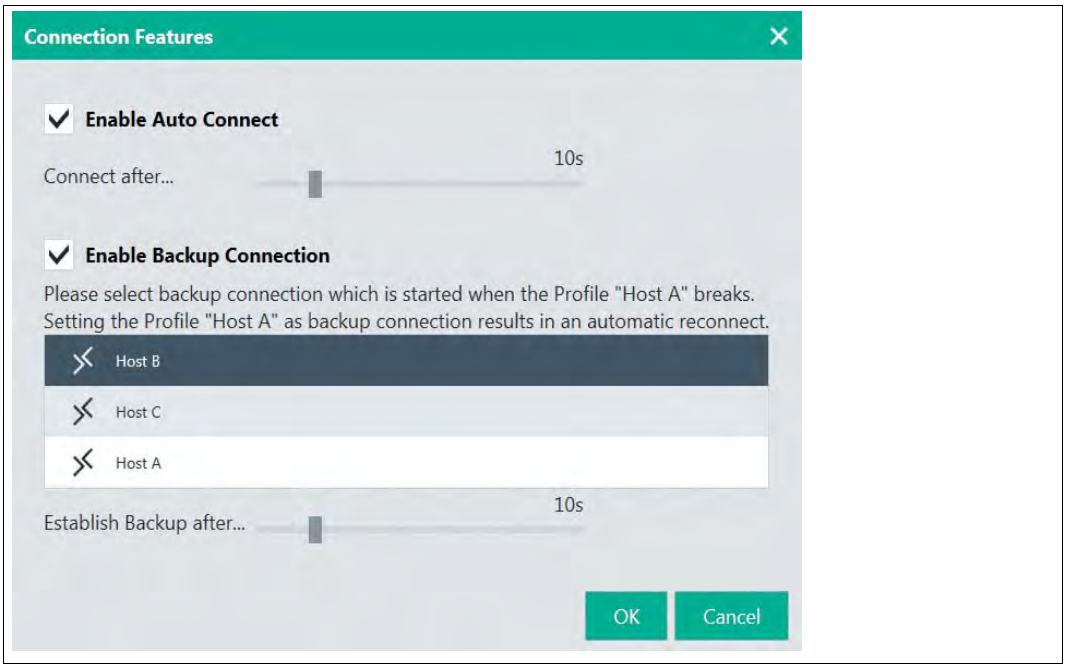


Figure 5.9 Example 2 - unlimited number of connection retries to more than one host (via "Backup Connection" feature)

Setting Up a Continuous Connection to More Than One Host

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



2017-08

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."

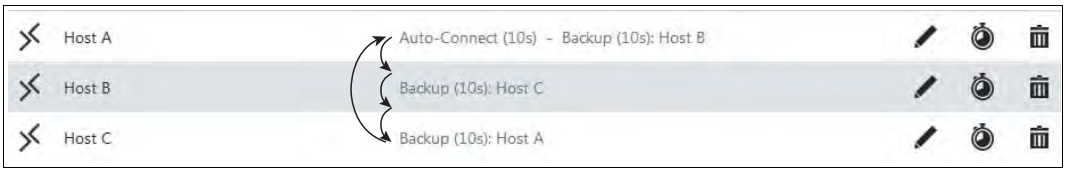


Figure 5.10 Profiles with backup connections

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

In this example, the RM connects automatically to a predefined host A. If the connection fails or gets lost, the RM will try to reconnect to host A 3 times. If the connection cannot be established, the RM 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.

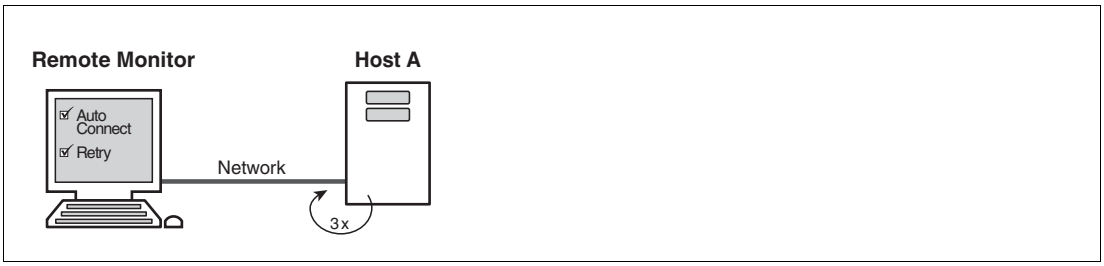


Figure 5.11 Example 3 - Limited number of connection retries to the same host

Setting Up Limited Number of Connection Retries to the Same Host

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

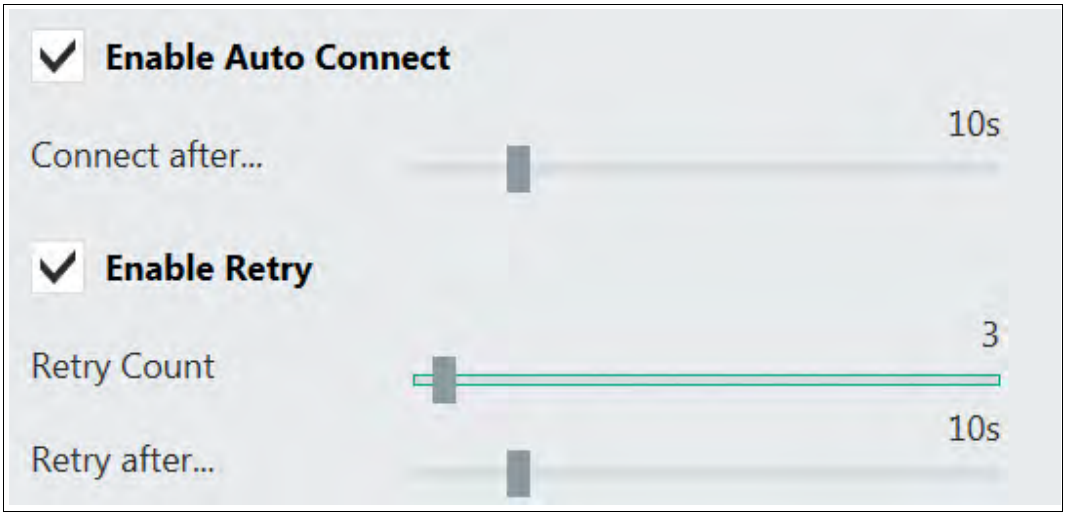
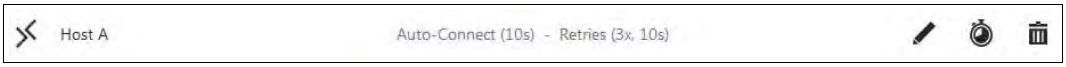


Figure 5.12 Corresponding settings in the VisuNet RM Shell (profile settings - connection features)

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."



5.2 Web Browser Settings (Chrome)

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

Note!

Optional feature, requires PRO license to unlock feature.

General Settings

Option	Description
Connection name	Name of the web connection that is presented on the home screen.
URL that will be navigated to	The URL to which the web profile will be linked.

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 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.
Show the connection on following displays	If you use extended desktop systems or BTC01*, 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.

5.3 VisuNet Desktop Sharing Settings

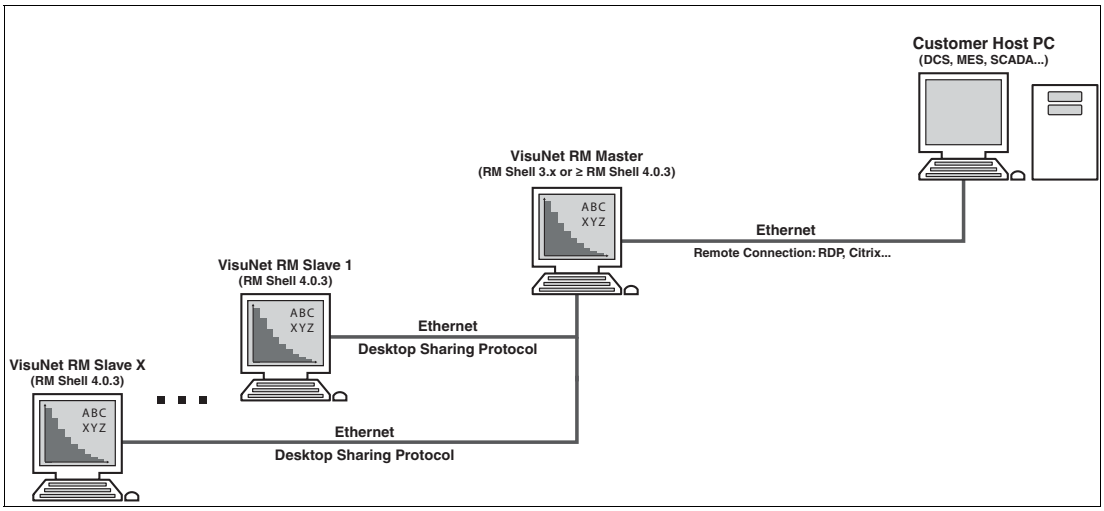


Figure 5.13 Example of a VisuNet desktop sharing infrastructure

Example

The drawing above shows several VisuNet RMs. All RMs are within the same Ethernet. One VisuNet RM is configured as a VisuNet RM Master for desktop sharing. The VisuNet RM Master is connected to the Customer Host PC via a remote connection profile (e.g., RDP profile).

The other VisuNet RMs are set up as "VisuNet RM Slaves." They are connected to the VisuNet RM Master via a desktop sharing profile.

All VisuNet RMs show the same screen, whether they are slave or master—the screen that is provided by the Customer Host PC.

Preferences for the RM Master

What?	How?
Connection profile	To establish a connection to the Customer Host PC, create an appropriate connection profile (e.g., RDP). For more information, see chapter 5.
System settings	To set up the RM as the desktop sharing master, go to system settings > Desktop sharing and activate the function "VisuNet Desktop Sharing Server enabled."

Preferences for the RM Slave

What?	How?
Connection profile	To establish a connection to the RM Master, create a desktop sharing profile. To connect the RM Slave to the Master, use the RM Master's name / IP address ("Host Computer Name / IP"). For more information, see chapter 5.

Note!

Optional feature, requires PRO license to unlock feature.

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.
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 4.2.
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.
Block user from closing the connection	Enable this option to prevent the user from opening a connection window.
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.
Show the connection on following displays	If you use extended desktop systems or BTC01*, 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 is shown on each monitor.

5.4 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.

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.
Block user from closing the connection	Enable this option to prevent the user from opening a connection window.
Show message box when Script errors detected	Enable this option to show error messages.
Allow the right click context menu	Enable this option to allow pointing device right clicks while users are connected to the profile.
Show the connection on following displays	If you use extended desktop systems or BTC01*, 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 is shown on each monitor.

5.5 Raritan KVM Settings

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

Note!

The RM Shell has been tested and qualified with the Raritan Dominion® KX II-101 KVM-o-IP switch that is available as an accessory (DKX2-101-V2; #547998). A separate Quick Installation Guide with the configuration steps for the Raritan Dominion® KX II-101 switch is provided with every DKX2-101-V2 order.

Note!

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

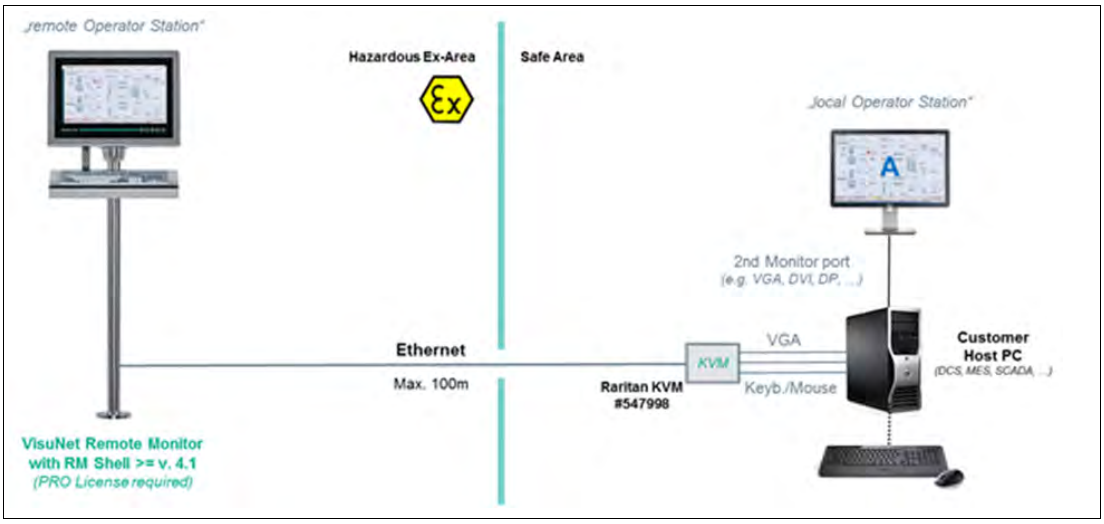


Figure 5.14 Common Setup VisuNet Remote Monitor and Raritan Dominion KVM-o-IP Switch

KVM Profile Settings

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

Note!

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

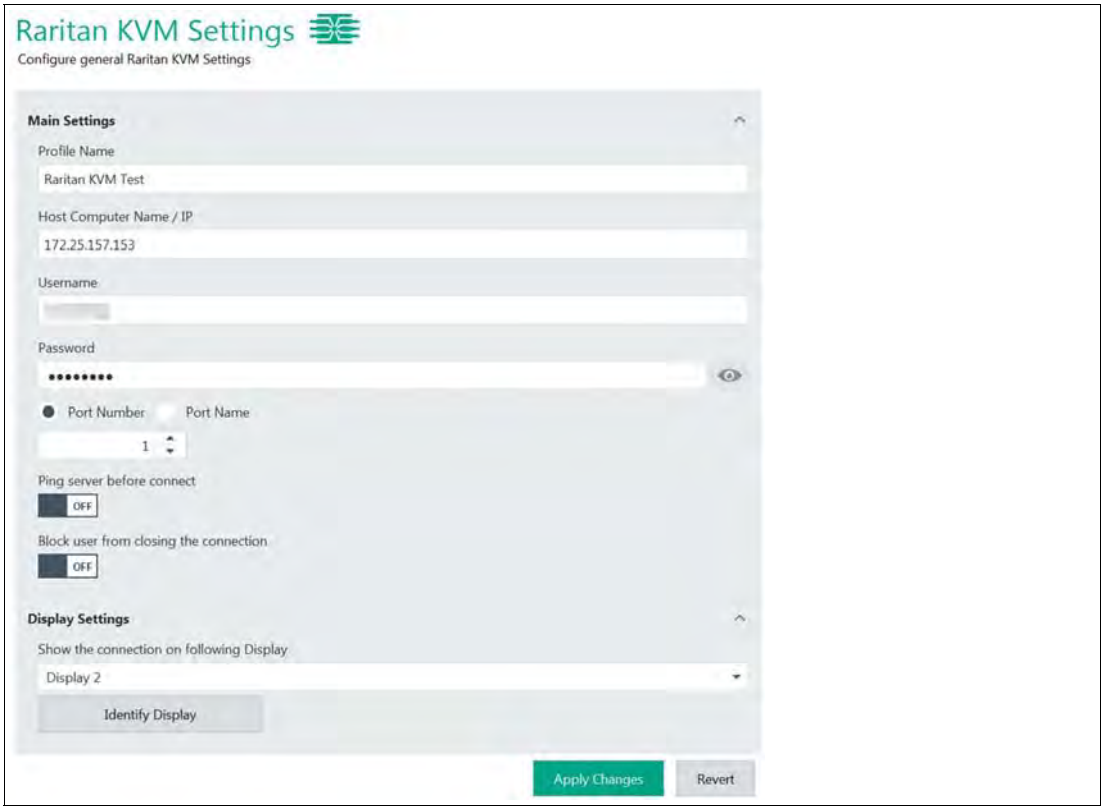


Figure 5.15 Raritan KVM Settings

Option	Description
Profile Name	Name of the KVM connection profile that is presented on the home screen.
Host Computer Name/IP	Network name or IP address of the Raritan KVM switch that you want to connect to. Default IP Address DKX2-101-V2:**192.168.0.192** Ensure that the RM is within the same IP address subnet as the Raritan KVM switch, e.g., 192.168.0.xxx
User Name	User name that is stored on the Raritan KVM switch that you want to connect to. Default User DKX2-101-V2: admin
Password	Password of the user that is stored on the Raritan KVM switch that you want to connect to. Default password DKX2-101-V2: 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. Please note that this function does not stop the user from closing the connection via other client mechanisms, e.g., the Raritan client menu bar.
Show the connection on following display	If you use a Box Thin Client with multiple connected displays, you can select which display the connection should be opened on.

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

5.6 RDP Settings

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

Main Settings

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

Connection

Option	Description
Choose connection speed	Select the connection speed you want from the drop-down list.
Allow the following	There are several visual effects you can activate or deactivate for the host. These options allow you to implement additional visual features. However, it may diminish the performance of the RM.
Fast Disconnect Detection by sending Pings to Host Server	By enabling this option, the RM constantly sends pings to the host. Possible connection failures will be detected much quicker than usual.
Enable Auto-Reconnect of the RDP connection	Enable this option to use the RDP's built-in connection recovery mechanism. This mechanism also tries to reastablish a remote desktop connection when it is disturbed.
Send Keep Alive Telegrams to the RDP server	This function keeps the connection between the RM and the host alive. It does this by sending messages from the RM 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 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 deskop in full size. If you want to set the remote desktop screen size manually, disable the option.
Show the connection on following displays	If you use extended desktop systems or BTC01*, 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.
Remote Color Depth	Select the color depth of the remote desktop connection from the dropdown 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 will be used on the host	Enable the local resources and devices you wish to be available on the host.

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.

Advanced

Option	Description
Authentication	■ No authentication of the server ■ Server authentication is required and must complete successfully for the connection to proceed ■ Attempt authentication of the server. If authentication fails, the user will be 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.

5.7 VNC Settings

The RM Shell 4.2 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 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.

Option	Description
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 reastablish a connection when it is disturbed.
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 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 BTC01*, 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

Option	Description
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 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

Encryption Settings

In this section, you can select the DSM encryption plug-in.

Option	Description
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

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 clipboard. In the default setting, copying content to the RM clipboard is enabled ("Disable clipboard - off")
Enable Ctrl + Alt + Del hotkey	Enable this option to allow users to use the Ctrl + Alt + Del hotkey.
Block user from closing the connection	Enable this option to prevent a connection window from being closed.

6 System Tools App

Entering the System Tools App

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

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

6.1 Clean Lock

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

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

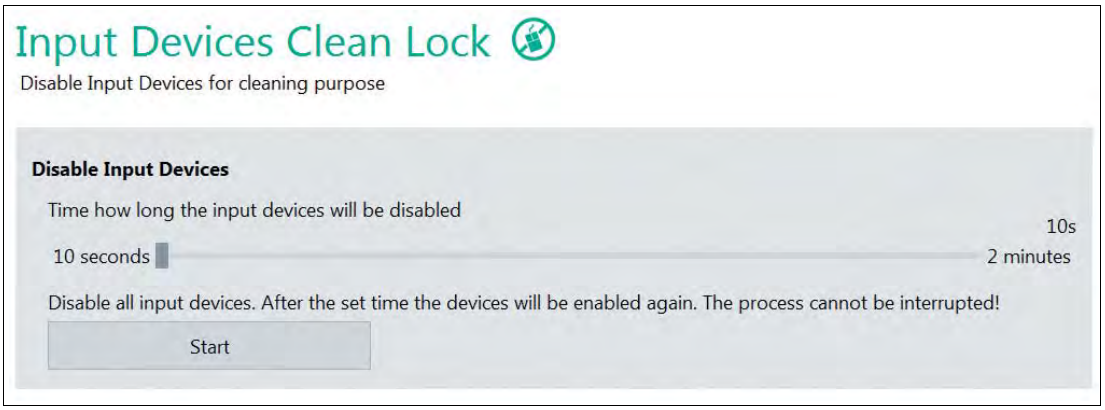


Figure 6.1 System tools - clean lock settings

6.2 Network NSLookup Tool

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

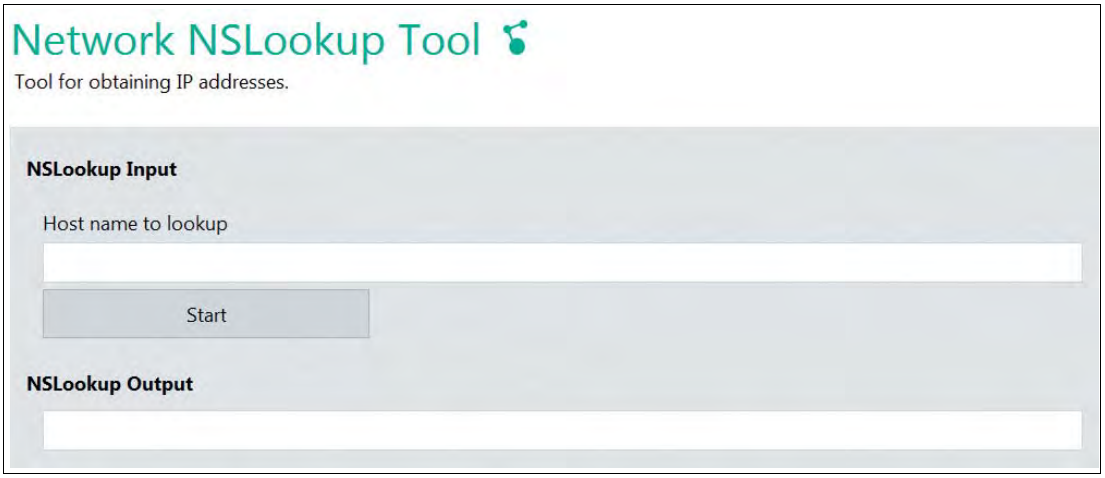


Figure 6.2 Network NSLookup Tool

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.

6.3 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 occured.

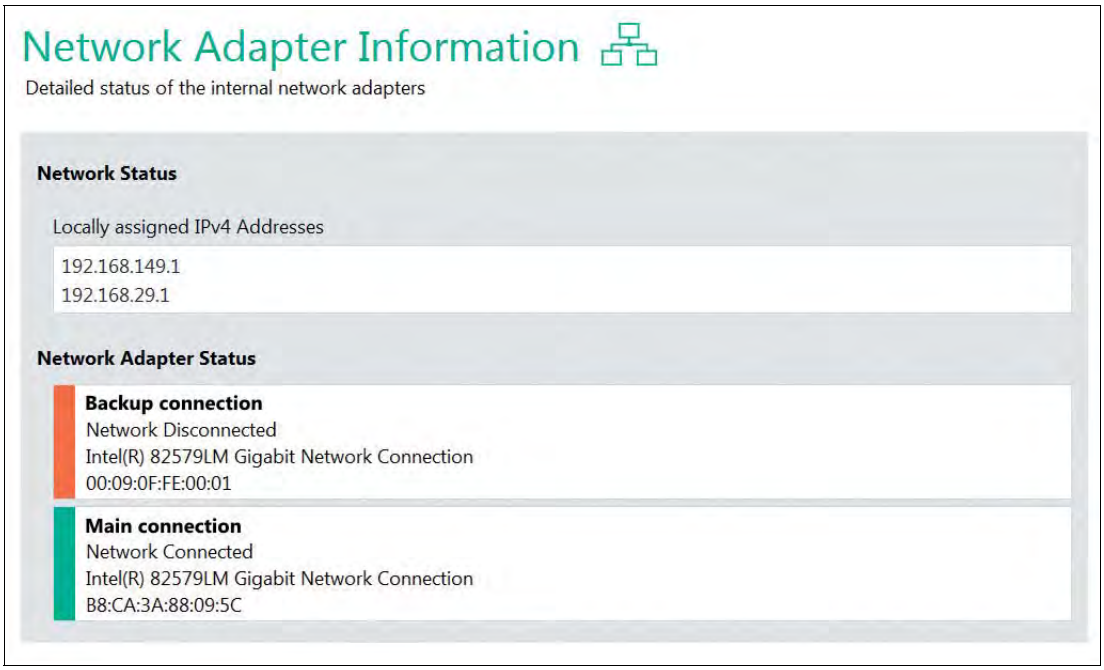


Figure 6.3 System Tools - network adapter information

6.4 Network Ping Tool

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

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

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

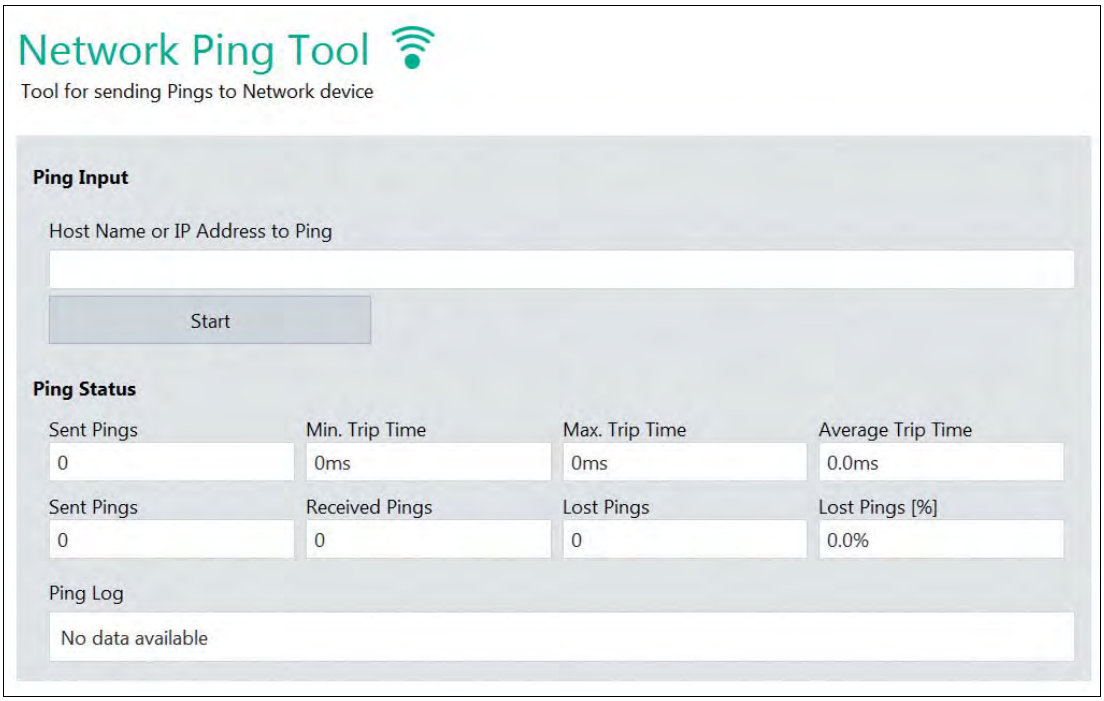


Figure 6.4 System tools - network ping tool

7 Citrix Receiver App

Citrix Receiver is a client software that allows easy access to Citrix XenApp and XenDesktop applications. RM Shell 4.2 integrates the latest Receiver (v 4.8) as a stand-alone app that can be easily configured and allows an RM to automatically connect to a Citrix XenDesktop / XenApp infrastructure after start-up.

Note!

License Information

The Citrix Receiver App is an optional feature that requires a "RM Shell PRO license" key to be unlocked. The PRO license key can be ordered separately (see chapter 1.3).

Setting up a Citrix Receiver Connection

To create a new connection to a XenDesktop/XenApp infrastrucutre, proceed as follows:

1. Open the Citrix app by clicking  on the home screen.

   ↳ The Citrix Receiver log on window opens.

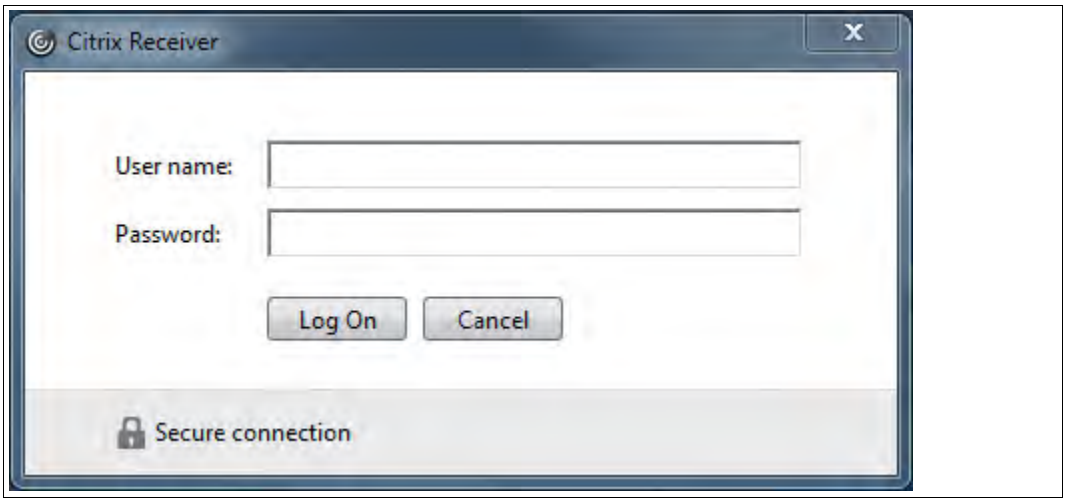


Figure 7.1 Citrix Receiver log on window

2. Type in the user name and password.
3. Click "Log on."

   ↳ The connection will be established.

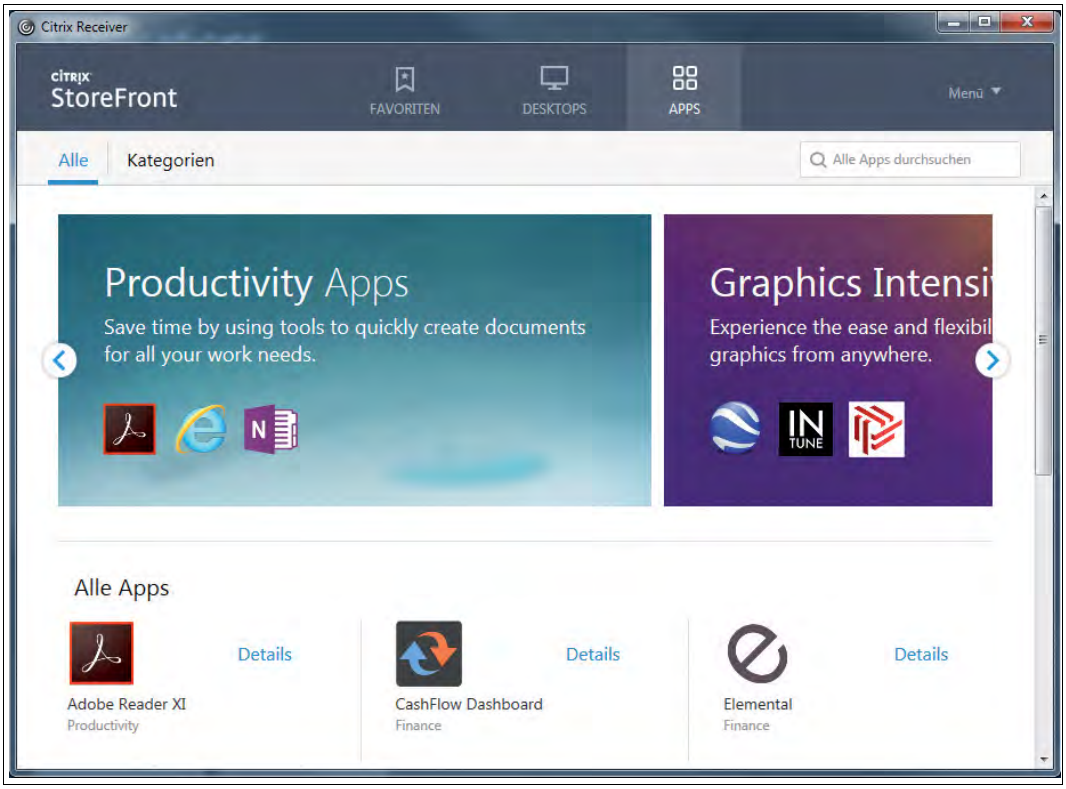


Figure 7.2 Citrix Receiver

Note!

Domain Integration into an Active Directory

RM Shell does not support domain integration into an Active Directory. See chapter 11.4. Active Directory integration can negatively affect the single-sign-on (SSON) behavior of Citrix. If you want to use SSON, contact your local Pepperl+Fuchs representative.

Note!

More Information

For more details and a complete compatibility list of the Citrix Receiver 4.8 client embedded in RM Shell 4.2, please refer to the official Citrix Receiver website: https://docs.citrix.com/en-us/receiver/windows/4-8/system-requirements.html

8 Wedge App

The wedge app is a keyboard emulation program that reads character strings from the serial port and simulates the corresponding keystrokes on the RM. These are then sent to your host PC. The app is specially designed to connect Pepperl+Fuchs barcode scanners (e.g., PSCAN-D). It allows a barcode scanner connected to the serial port to be used as a keyboard input device in a variety of applications. For information on configuring the wedge settings, see chapter 4.11.

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

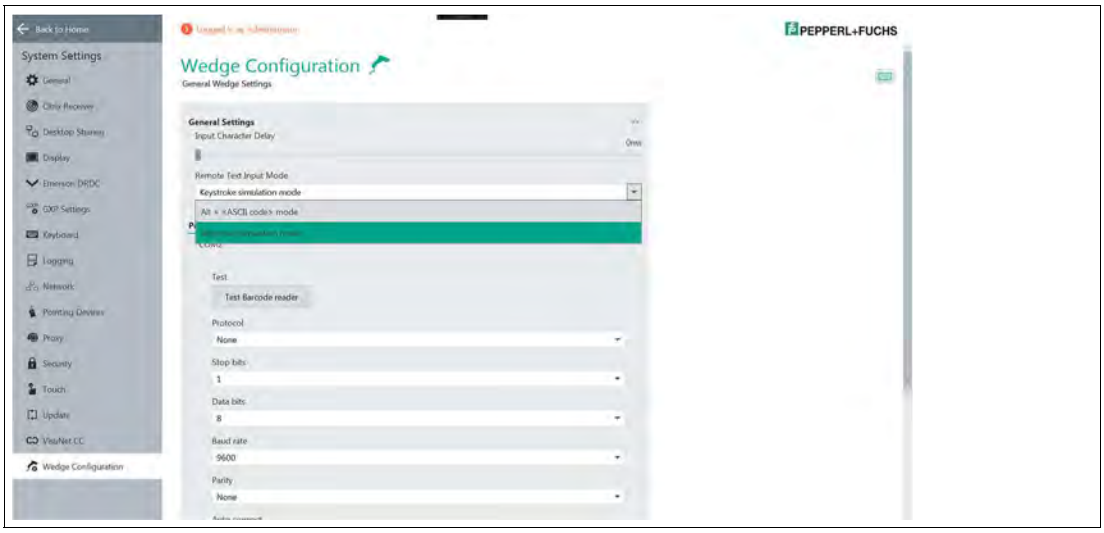


Figure 8.1 VisuNet RM Shell wedge app

In the Wedge Configuration window, use the dropdown list above to specify your preferred remote text input mode. Keystroke simulation is the default setting and simulates a user typing on a keyboard. Should this setting cause problems, you can easily switch to Alt + ASCII-key mode, where scanner-read data is transformed into characters via the Alt code.

9 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. It is only accessible to users who are signed in with the Administrator user role.

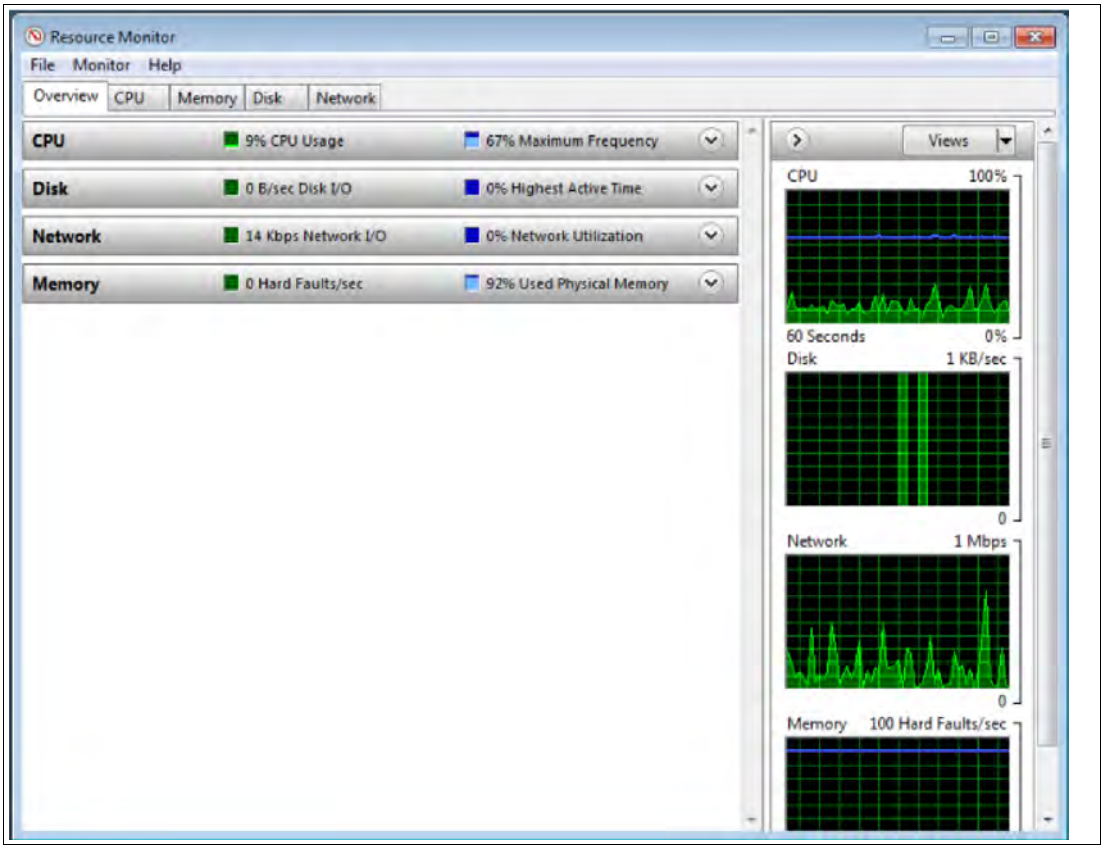


Figure 9.1 Process Explorer window

10 How-Tos

10.1 Connecting an RM with a PC via RDP

Note!

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

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

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

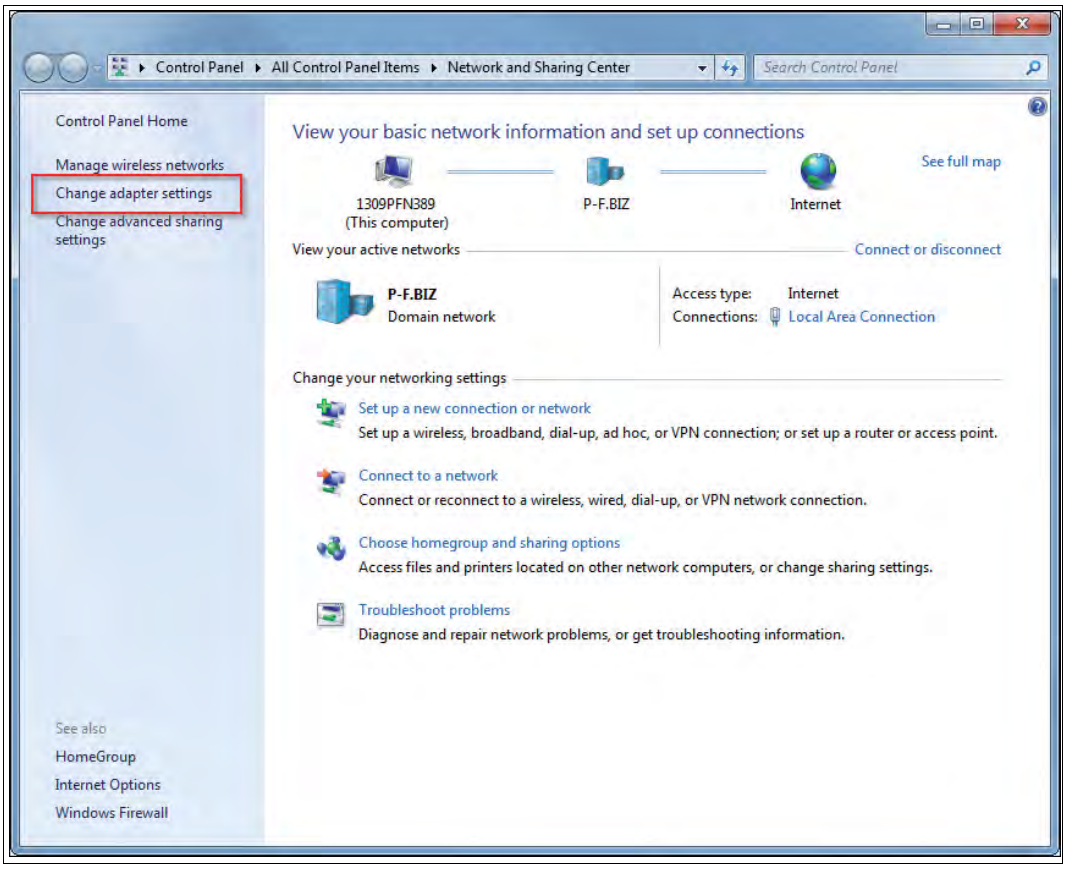
- Step 1: PC Configuration
  - Manual assignment of the IP address
  - Activation of the RDP Server Function
- Step 2: RM Configuration
  - Manual assignment of the IP address
  - Creation of an RDP profile

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".

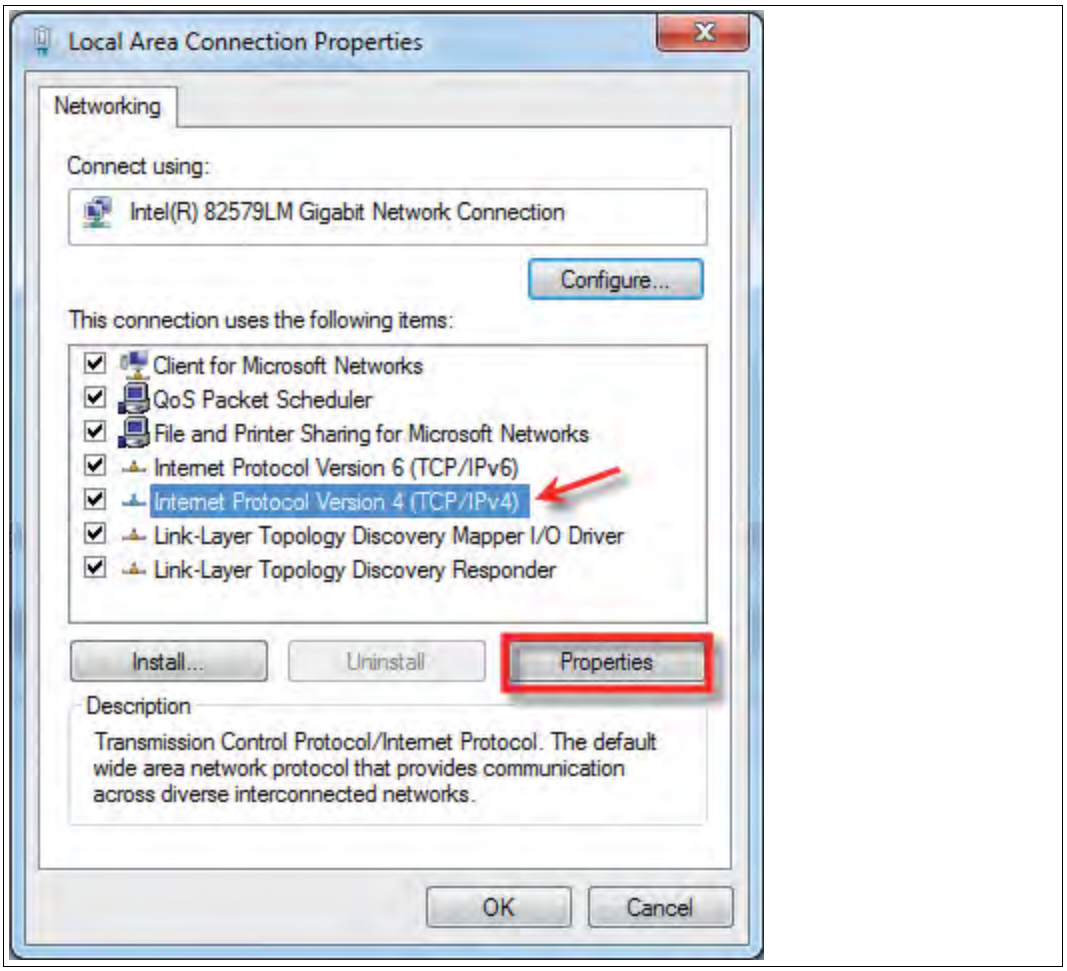
   ↳ The "Network and Sharing Center" window opens.



2017-08

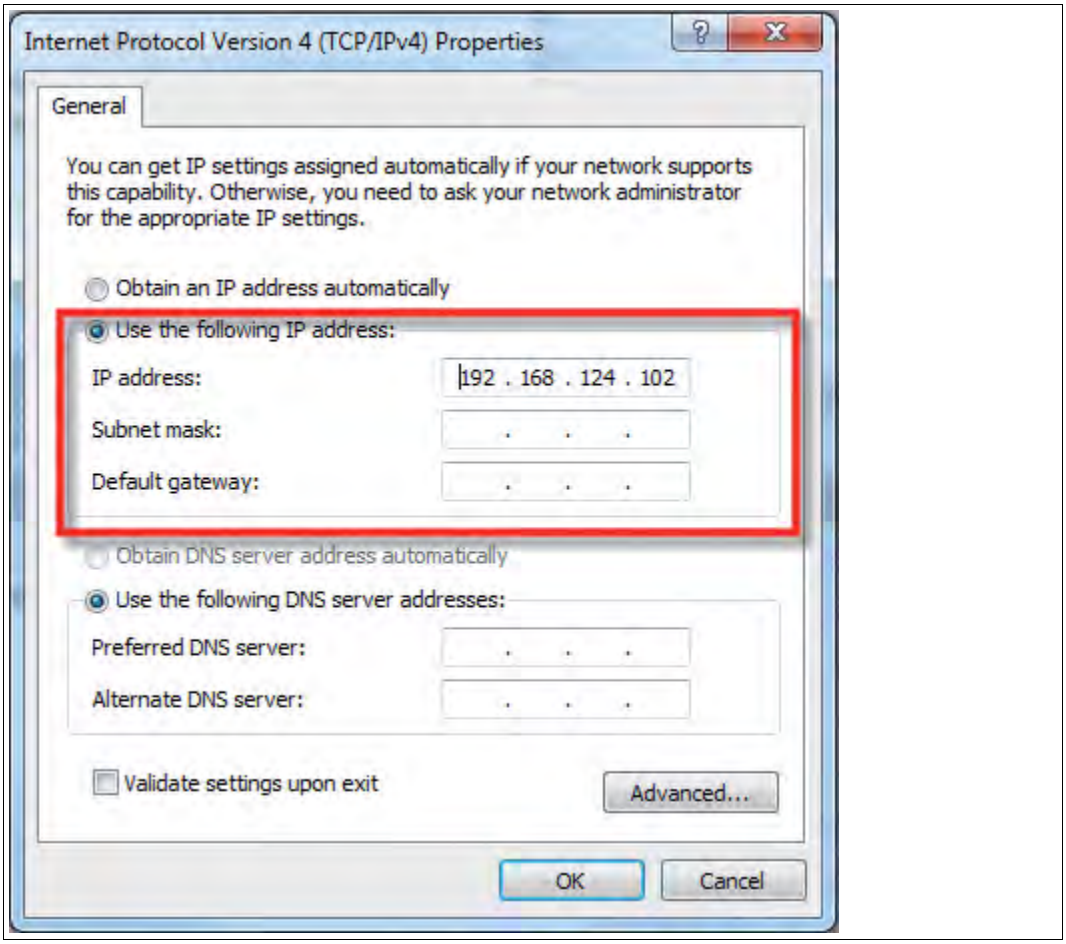
2. From the navigation bar, choose "Change adapter settings."
3. Search for the network connection that shows your physical network port hardware component. The physical network port hardware component is recognizable by its name in the third line (e.g., "Intel(R) 82579LM...")
4. Right-click on the network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

   ↳ The "Local Area Connection Properties" window opens.



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

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

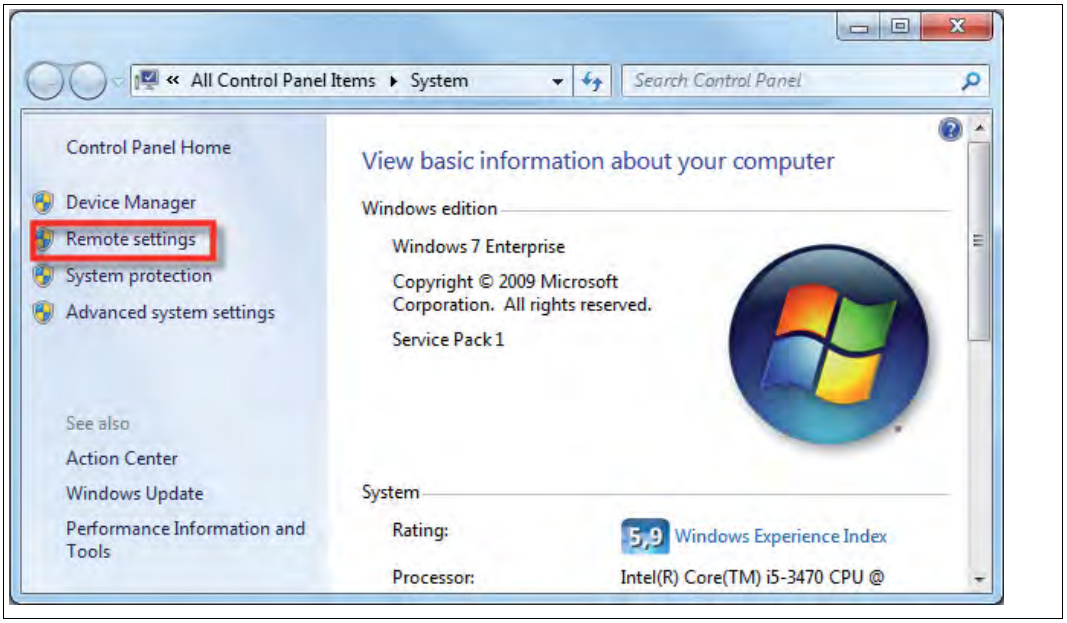


7. Choose the option "Use the following IP address" and type in a static IP address (e.g., "192.168.124.102").
8. To confirm the changes, click "OK."
9. Close the Network and Sharing Center.

Activating the RDP Server Function

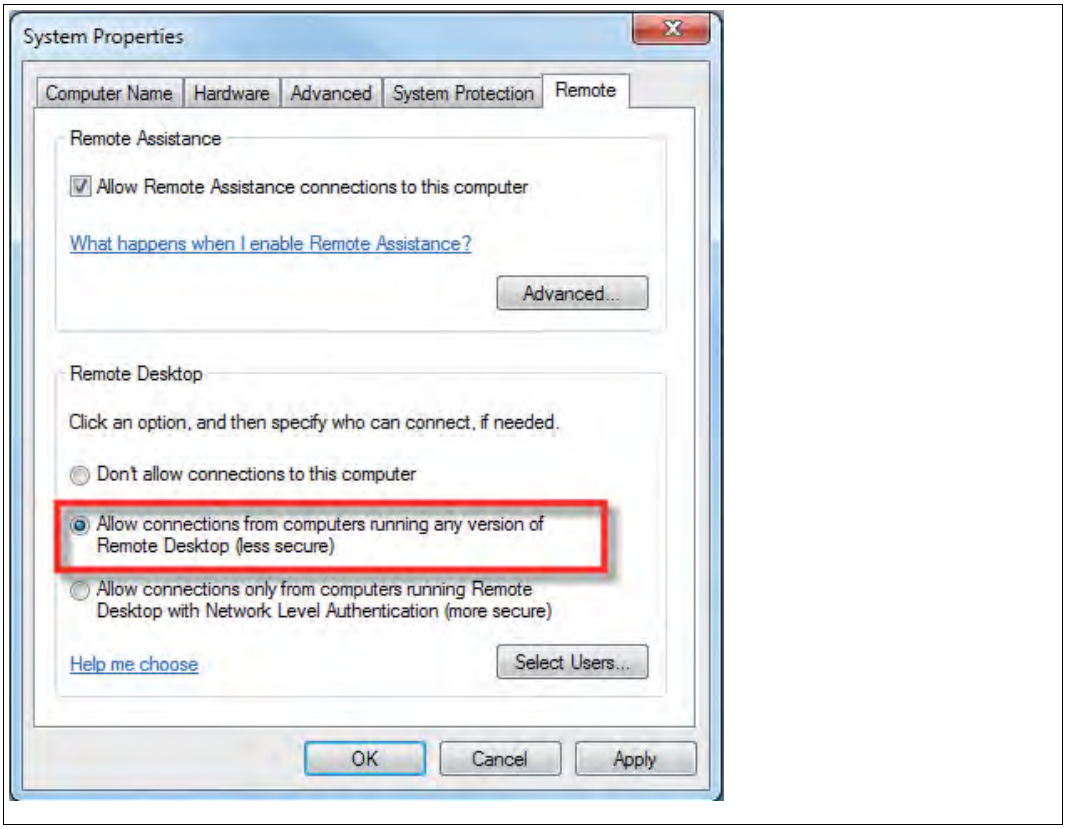
1. Open the start menu, right-click on "Computer" and choose "Properties."

   ↳ The system control panel opens.



2. Click on "Remote settings."

   ↳ The System properties dialog box opens.



3. Choose the option "Allow connections from computers running any version of Remote Desktop (less secure)."
4. Click “OK.”
5. To confirm the changes, close the system control panel.

Step 2: RM Configuration

Assigning IP Address of the RM Manually

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

6. In the IP address field, type an IP address that differs in the last 3 digits from the IP adress 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 RD 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 + New profile.
4. Select "Microsoft RDP," and click "OK."

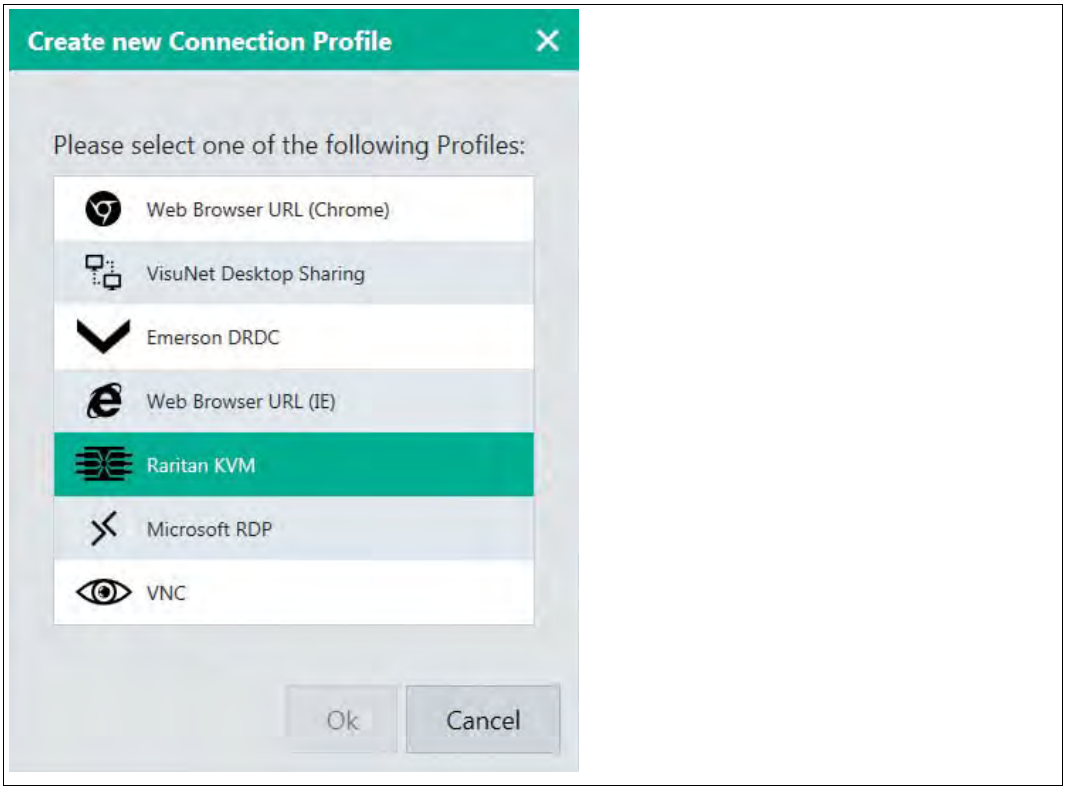


Figure 10.1 The "Create new Connection Profile" dialog box - web browser, Raritan KVM and VisuNet desktop sharing profiles are only available in the pro version.

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

2017-08

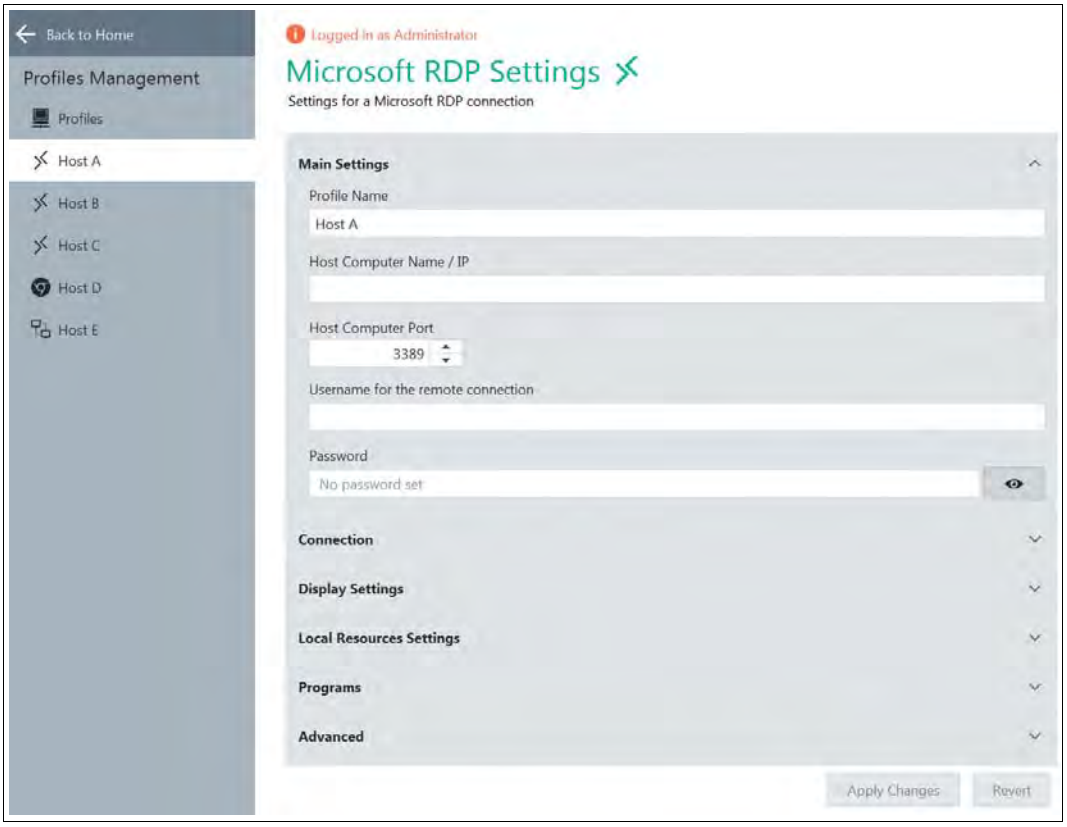


Figure 10.2 Main settings of a Microsoft RDP profile

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

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

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

10.2 Increasing RDP Reactivity and Performance

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

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

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

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

Note!

RDP 8.0 with RemoteFX is enabled by default on all Pepperl+Fuchs devices with RM Shell 4.x (or newer) and does not need to be activated.

10.3 Enabling Auto-Login with RDP

Pepperl+Fuchs devices with RM Shell 4.x (or newer) offer an auto-connect feature that supports the automatic start of a remote connection and the login into a host system.

When trying to use saved credentials in an RDP profile, you might receive this message:

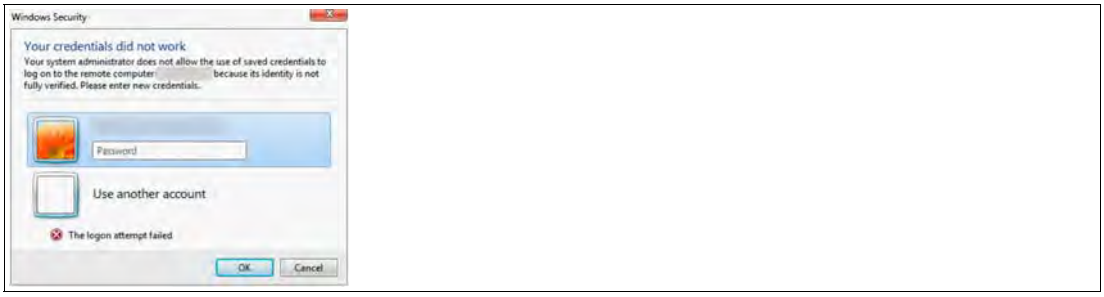


Figure 10.3 Saved credentials not working

To enable the use of saved credentials, you need to perform the following configuration steps on your host system:

Using Saved Credentials

1. Open Group Policy Editor via `cmd -> gpedit.msc`.
2. Navigate to `Local Computer Policy\Computer Configuration\Administrative Templates\System\Credentials Delegation\`
3. Open Setting `Allow Delegating Saved Credentials with NTLM-only Server Authentication`, set it to `Enabled`, click on button `Show ...` and in the `Show Contents` window add the value `TERMSRV/*`. 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.

10.4 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

2017-08

10.5 Configuring a Multi-Monitor (Extended Desktop) Setup with RDP and Box Thin Client BTC01*

When you use a Box Thin Client BTC01* 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

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

11.1 Open Network Ports

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

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

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

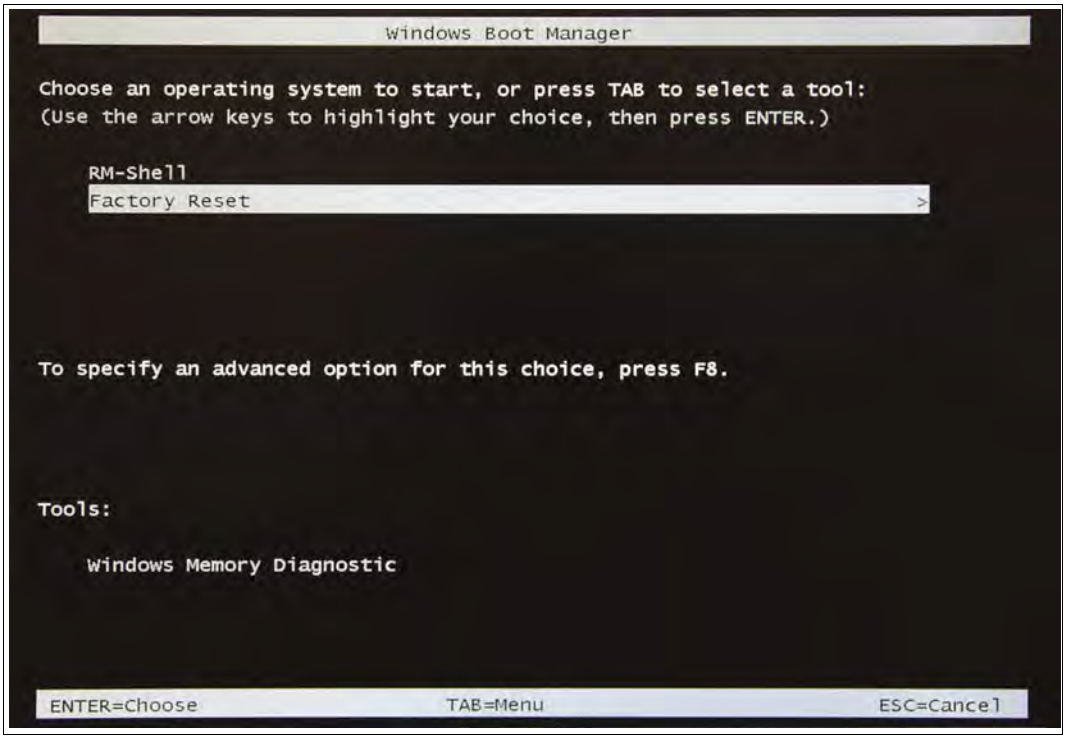
11.2 Factory Reset

Note!

Performing a factory reset requires the use of a keyboard and mouse.

Resetting to Factory Default

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 with white text on a black background repeatedly flashing, stop pressing the "F9" key.

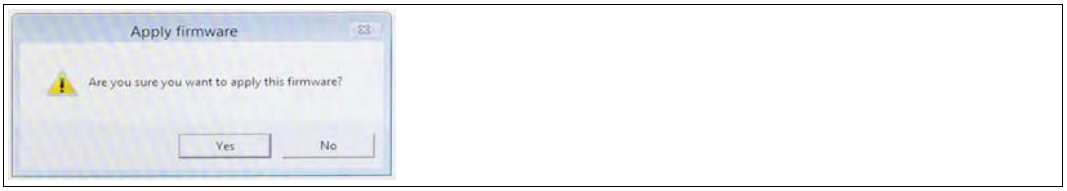


4. Select "Factory Reset."

   ↳ A series of loading pages will display, and you will eventually be presented with the main factory reset window.

5. Under "Available firmware," find the desired firmware version that you want to reset to (there is normally only one firmware version listed). Click the "apply" button next to the desired firmware.

   ↳ You will be presented with the dialog "Apply Firmware."



6. Select "Yes."

   ↳ The factory reset process will begin. You will be presented with a progress bar and an estimate of the time remaining.

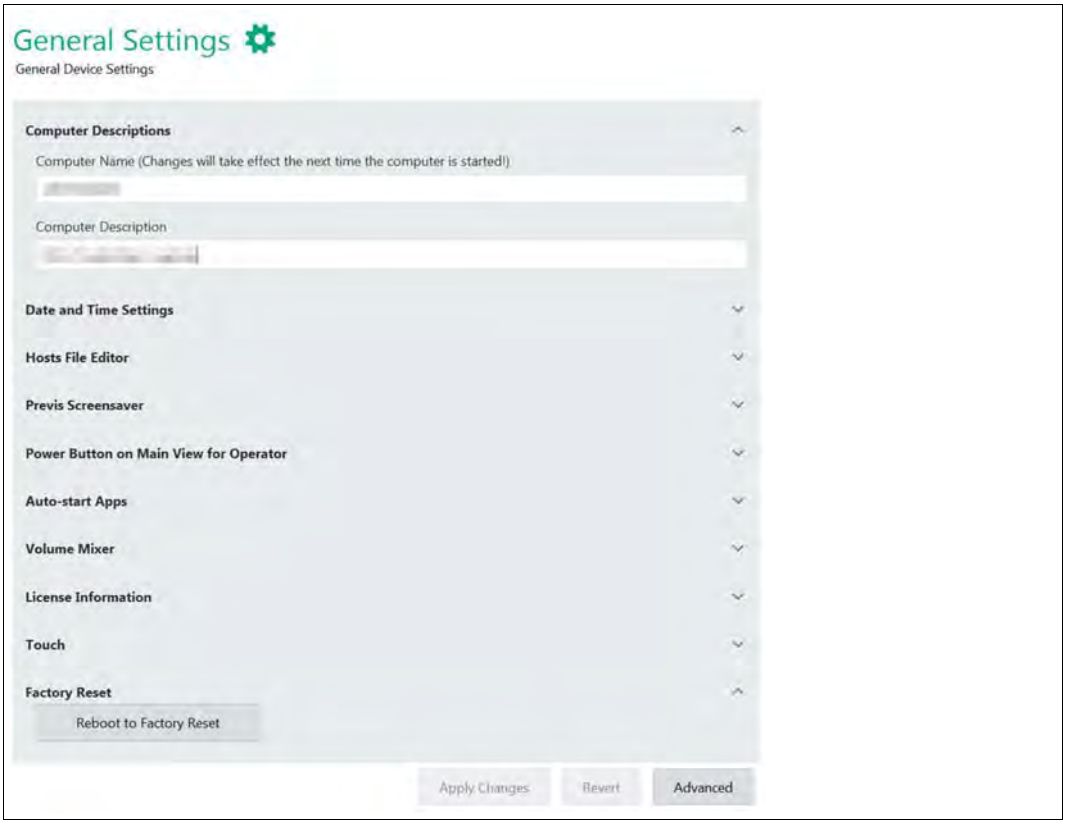
7. If presented with a dialog box with options for "Reboot now" and "Reboot later," ALWAYS select "Reboot later."

   ↳ After all the setup steps are complete, you should be presented with the VisuNet RM Shell main window. The factory reset process is now complete.

11.3 Alternate Factory Reset

Alternate Factory Reset

1. From the main screen, change users to Administrator.
2. Click on System Settings.
3. Navigate to the General tab.
4. Expand the Factory Reset section.
5. Click the Reboot to Factory Reset button.



6. When prompted with "Are you sure you want to reboot to Factory Reset? All open connection profiles will be closed.", click the Yes button, and the RM will reboot to Factory Reset.

7. Continue from step 5 of the factory reset explained above, see chapter 11.2.

11.4 Active Directory Support

We do not support the integration of our RM Shell 4.x-based HMI devices into a Microsoft® Active Directory infrastructure. We advise customers to organize our HMI systems into workgroups.

The main reason for this is that these devices are closed HMI systems and are tested and qualified with the most popular process control systems for compatibility. Integrating RM Shell 4.x-based devices into an Active Directory infrastructure poses the risk that security policies and third-party software can be pushed onto our devices and result in misconfiguration and system incompatibilities. Further, our HMI devices with RM Shell 4.x are optimized for use as terminals that are connected via remote connections such as Microsoft® RDP to host systems and used by multiple users. Operators do not need to log in to our units, except for configuration purposes. Therefore, an individual user and credentials management such as that provided with Active Directory is not required in our common usage scenarios. User authentication is usually implemented on the host machine, which operators connect to via the RDP connection that can be part of an Active Directory.

Pepperl+Fuchs RM Shell 4.x-based devices use a different concept to meet the special demands of the process industry in terms of security, usability, and compatibility with process control systems. The core focus of RM Shell 4.x is to ease the integration of our HMI devices into a process control system—even by users with limited IT knowledge. Therefore, the standard Windows® Shell (Desktop) is replaced by a customized, touch-friendly user interface, called RM Shell 4.x. Although RM Shell 4.x is based on a Windows® Embedded Operating system, it is, in contrast to other thin client systems, a closed system that does not support the installation of third-party applications. Additional security features such as local user roles, USB lock down mechanisms, a firewall, and enhanced write filters further protect the system from infiltration and persistent storage of viruses or other malicious software.

In addition to our thin-client-based HMI technology, Pepperl+Fuchs also offers PC-based products that offer an open Windows® operating system. These products allow full configuration by customers and integration of the devices into an Active Directory.

For more information, contact your local Pepperl+Fuchs representative.

11.5 Pepperl+Fuchs GmbH 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 GMBH, 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 GmbH, 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 4“ 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 EMBEDDED STANDARD 7 which is subject to additional terms and conditions referenced in the About screen of the “VisuNet RM Shell 4”. 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 4”.

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.

2017-08

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 4”. 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 4”.

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.

2017-08

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.

PROCESS AUTOMATION – PROTECTING YOUR PROCESS

Worldwide Headquarters
Pepperl+Fuchs GmbH
68307 Mannheim · Germany
Tel. +49 621 776-0
E-mail: info@de.pepperl-fuchs.com

For the Pepperl+Fuchs representative
closest to you check www.pepperl-fuchs.com/contact

www.pepperl-fuchs.com

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

/ DOCT-4757E
08/2017