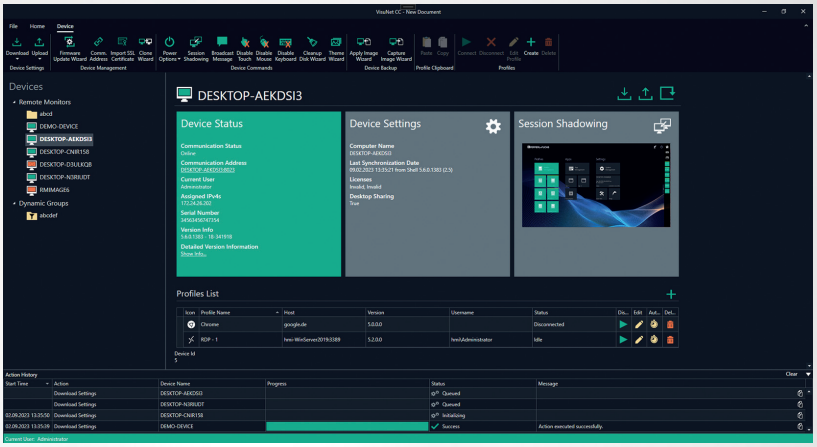
VisuNet Control Center 6

Manual



Your automation, our passion.

PEPPERL+FUCHS

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

Worldwide

Pepperl+Fuchs Group

Lilienthalstr. 200

68307 Mannheim

Germany

Phone: +49 621 776 - 0

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

North American Headquarters

Pepperl+Fuchs Inc.

8093 Darrow Road

Twinsburg, Ohio 44087

+1 330 425-3555

sales@us.pepperl-fuchs.com

United States of America

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

Asia Headquarters

Pepperl+Fuchs Pte. Ltd.

P+F Building

18 Ayer Rajah Crescent

Singapore 139942

Phone: +65 6779-9091

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

https://www.pepperl-fuchs.com

1 History of the Manual 5
2 Introduction 6
2.1 Content of this Document 6
2.2 Target Group, Personnel 6
2.3 Symbols Used 7
3 Security Context 8
4 Product Description 9
4.1 Overview 9
4.2 Program features 10
4.3 Licensing 11
4.4 Installation 12
5 VisuNet CC Setup 13
5.1 Main Structure (User Interface) 14
5.2 Device Structure 17
6 Manage (Home) 18
6.1 Group Management 18
6.2 View 19
6.3 Programm Apperance 19
6.4 Group Actions 19
6.5 User Management 27
6.6 License Manager 29
6.7 Credential Wizard 33
6.8 About 38
7 Manage (Device) 39
7.1 Device Function Tiles 39
7.1.1 Device Status 40
7.1.2 Device Settings (Tile) 42
7.2 Device Settings (Ribbon) 46
7.3 Device Management 47
7.4 Device Commands 54
7.5 Device Backup 62
7.6 Profile Clipboard 74

2025-07

7.7 Profiles 75

8 "How Tos" 76

8.1 Export Data 76

8.2 Transfer configurations from VisuNet RM Shell 5 to VisuNet RM Shell 6 devices 79

8.3 Preparing an RM / BTC for Centralized Management 86

8.4 Connecting to an RM / BTC 87

8.5 Uploading a Configuration to an RM / BTC 88

8.6 Shadowing a Session 89

8.7 Creating a New Local User 90

8.8 Build up secure communication between CC and RM Shell devices 91

9 Troubleshooting 96

2025-07

1 History of the Manual

The following editions of the manual have been released:

Version	Comments
05/2023	First version
01/2024	"License and Credential Manager" added
07/2024	"How to Export Data" added
07/2025	Added Features and Updates of VisuNet RM Shell 6.1

2 Introduction

2.1 Content of this Document

This document contains information that you need in order to use your product throughout the applicable stages of the product life cycle. These can include the following:

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

Note

This document does not substitute the instruction manual.

Note

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

Note

For specific device information such as the year of construction, scan the QR code on the device. As an alternative, enter the serial number in the serial number search at www.pepperl-fuchs.com.

The documentation consists of the following parts:

- Present document
- Instruction manual
- Datasheet

Additionally, the following parts may belong to the documentation, if applicable:

- EU-type examination certificate
- EU declaration of conformity
- Attestation of conformity
- Certificates
- Control drawings
- Functional safety manual
- Additional documents

2.2 Target Group, Personnel

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

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

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

2025-07

2.3 Symbols Used

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

Warning Messages

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

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



Danger!

This symbol indicates an imminent danger.

Non-observance will result in personal injury or death.



Warning!

This symbol indicates a possible fault or danger.

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



Caution!

This symbol indicates a possible fault.

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

Informative Symbols



Note

This symbol brings important information to your attention.



Tip

This symbol brings an useful tip to your attention.



Example

This symbol provides an example of the issue described.



Action

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

3 Security Context

From the security point-of-view, the responsible plant operator requires to take the following measures:

- Limit the access for the workstations with an installation of VisuNet CC.
- Limit the access of the file store which contains the project files and stored data.
- The workstation with an installation of VisuNet CC should be connected to an network which is managed by the IT.
- Ensure only the following Ports are open.
  - For the Intranet which contains the RM Shell devices:
    - VisuNet CC Discovery Port outgoing UDP 3702 and 137
    - VisuNet CC Download/Upload Port outgoing TCP 8023
    - VisuNet CC Session Shadowing Port outgoing TCP 5900
    - VisuNet CC Default Secure Tunnel Port outgoing TCP 22314
    - Factory Reset communication Port outgoing TCP 23314
  - For the Internet:
    - Update Service outgoing Port 443 TCP to the domain www.pepperl-fuchs.com

Note

For detailed information regarding Cybersecurity please refer to the Brief Instructions Cybersecurity VisuNet RM Shell and VisuNet RM Shell manual.

4 Product Description

4.1 Overview

The VisuNet Control Center (VisuNet CC) is a software tool for the centralized management of Pepperl+Fuchs VisuNet Remote Monitors (RMs) and Box Thin Clients (BTCs). The software can be installed on any Windows®-based PC, such as a service Notebook or a virtualized Engineering Workstation. It allows remote setup, management, and maintenance of all RMs and BTCs that are connected to the same network infrastructure. VisuNet CC offers the following valuable functions:

- Remotely set up device configuration (e.g., hostname) of an RM / BTC
- Create and edit remote profiles (e.g., a RDP connection profile) on an RM / BTC
- Clone device settings and profiles from one RM / BTC to another RM / BTC
- Copy one or multiple remote profiles from one RM / BTC to another RM / BTC via copy and paste function keys of the keyboard or via the copy and paste icons in the ribbon
- Monitor operators' screens and support them remotely via session shadowing
- Update system firmware
- Restart and reboot an RM / BTC



Note

VisuNet CC is compatible with all Pepperl+Fuchs devices with pre-installed RM Shell 5 or 6 firmware or newer.



Tip

VisuNet CC provides further information for several functions via tool tips. Please hover with the mouse cursor over a user interface item (e.g. button) to get tool tip information.



Caution!

Time settings

The Time zone, Time and Date Settings of the RM Shell and the VisuNet CC must be identical, otherwise the time is invalid and a synchronization is not possible.

The maximum feasible Date and time difference is 12 h.

4.2 Program features

The VisuNet Control Center allows the user to manage all HMI systems with RM Shell 6 as well as RM Shell 5.0 or newer from a central location. Therefore, the administrators no longer need to enter hazardous areas or other restricted areas like clean rooms to setup or maintain a Remote Monitor or box thin client. Instead, access to the Remote Monitors is granted from a central location, which saves time and costs.

Via the VisuNet Control Center, connection profiles can be created for a Remote Monitor and then transferred to other devices. Firmware updates are realized with a single click. In addition, the user can connect to any Remote Monitor with RM Shell 6 or 5, monitor the device status and the screen content or even take over control remotely. This simplifies support and significantly increases the availability of the devices.



Figure 4.1

- Efficient, centralized remote configuration (e.g. device settings, remote profiles)
- Easy and simplified Maintenance (e.g. security patches and updates)
- Monitoring and remote support (e.g. secured session shadowing via own own public key certificate)
- Optimally aligned to P+F Firmware RM Shell 6 and 5
- Mass configuration and profile copying to multiple devices
- Wizards that guide users simply through the different processes

Caution!

The program must only be used in an enterprise network that is protected against unauthorized usage by operators or malware.

4.3 Licensing

VisuNet Control Center can be downloaded from the Pepperl+Fuchs website. Visit www.pepperl-fuchs.com and use the search term “VISUNET-CONTROL-CENTER.”

To unlock the VisuNet CC management interface on an RM / BTC, an additional license must be entered.

Item number	Type code	Description
#XSP2-037-01R	VISUNET-RM-SHELL6-CC-DLK	Digital license for one VisuNet RM Shell 6 device required to unlock the VisuNet Control Center
#70162159	VISUNET-RM-SHELL6-CC	License for one VisuNet RM Shell 6 device required to unlock the VisuNet Control Center
#70162160	VISUNET-RM-SHELL6-CC-5	5 licenses key to enable VisuNet Control Center
#70162161	VISUNET-RM-SHELL6-CC-10	10 licenses key to enable VisuNet Control Center
#70162162	VISUNET-RM-SHELL6-CC-30	30 licenses key to enable VisuNet Control Center
#70162164	VISUNET-RM-SHELL6-CC-50	50 licenses key to enable VisuNet Control Center
#548284	VISUNET-RM-SHELL5-CC	One license per VisuNet RM Shell 5 device required to unlock the VisuNet CC interface.
#548285	VISUNET-RM-SHELL5-CC 5	5 licenses keys to enable VisuNet Control Center
#548286	VISUNET-RM-SHELL5-CC 10	10 licenses keys to enable VisuNet Control Center
#548287	VISUNET-RM-SHELL5-CC 30	30 licenses keys to enable VisuNet Control Center
#548288	VISUNET-RM-SHELL5-CC 50	50 licenses keys to enable VisuNet Control Center
#548024	VISUNET-RM-SHELL5-CC	One license per VisuNet RM Shell 4 device required to unlock the VisuNet CC interface.

Table 4.1

Features that can be used without a Control Center license

You can use the following features in Control Center even if you do not have a valid license:

- View device status
- View the diagnostic tool and export the diagnostic data
- View and download device settings (License required to upload)
- Export Data from Control Center

4.4 Installation

VisuNet CC can be installed via a standard installer. Follow the installation wizard to perform the installation. The software can be installed on any WIndows Operationg System that supports the Microsoft .NET Framework 4.7.2.

Tip

The firewall on either a service PC or Pepperl+Fuchs RM / BTC will be configured automatically. During the installation the firewall rules will be activated.

For individual firewall settings at your service PC use the following ports:

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

The firewall of the device must allow "pepperl-fuchs.com" as a domain to allow the internal update function to operate.

5 VisuNet CC Setup

- **Project-based approach:**
  VisuNet CC uses a project-based approach.
- **Configuration storage:**
  - Configurations of RMs/BTCs can be stored in a file.
  - This file can be saved locally (e.g., on a hardware drive) or shared across multiple computers running VisuNet CC.
- Local storage of changes:
  - All configuration changes made in VisuNet CC are stored locally.
- Synchronization with RMs/BTCs:
  - To synchronize the local configuration in the project with the configuration on RMs/BTCs, use the "Download" function.
  - This function loads the configuration from an RM/BTC into the local project file.
- Applying changes to RMs/BTCs:
  - To apply changes to an RM/BTC, they must be uploaded.
  - Use the "Upload" function to transfer the configuration to the RM/BTC.
  - This also allows editing configurations while the RM/BTC is offline.
- Project selection on startup:
  - When starting VisuNet CC, a dialog appears.
  - You can choose to:
    - open the last used project,
    - open a project from a file, or
    - create a new project.

The projects needs to be password protected.

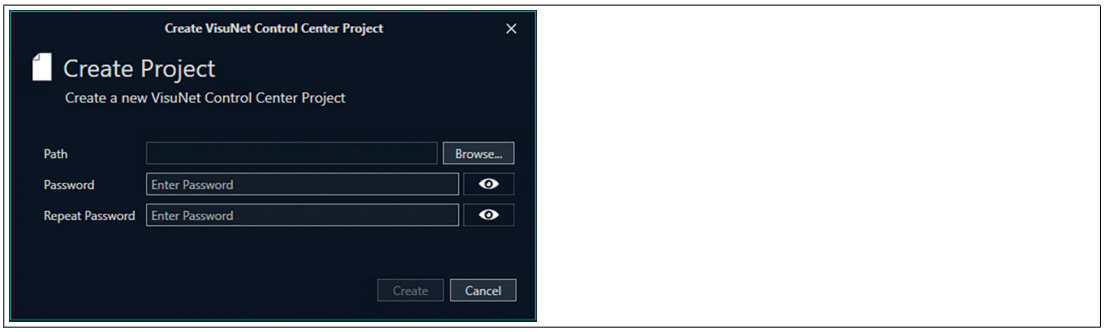


Figure 5.1

VisuNet CC Wizard:

Whenever actions need to be perfomed for multiple devices it is necessary to perform these with the VisuNet CC Wizard.The Wizard guides you with a sequence of dialog boxes through defiend steps and turns complex tasks into easy executable steps.

5.1 Main Structure (User Interface)

To find all your devices in the network, use the “Scan for Remote Monitors” icon.



Figure 5.2

All online devices, Remote Monitors and Box Thin Clients are listed.

Note

If your device is not listed, you can use the “Add Device” function and add a device manually by stating the IP address.

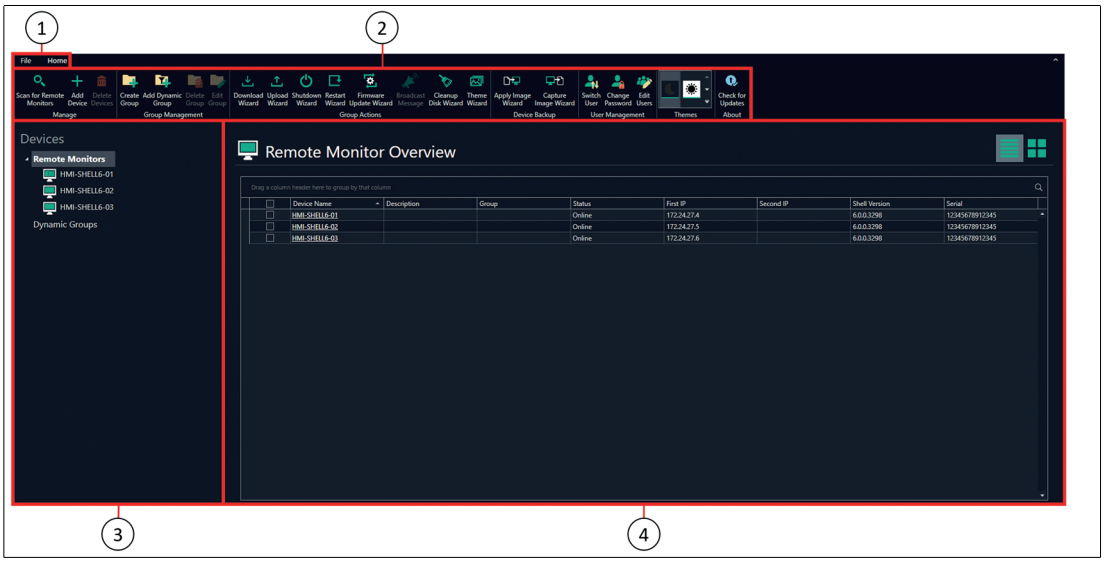


Figure 5.3

VisuNet CC’s user interface is divided into three main sections:

1 **Tabbed toolbars**: In the toolbar the following tabs can be selected:

File: Click the "File" tab in the top-left corner of the VisuNet CC screen to enter the file view.

2 Toolbar

3 Devices

4 Remote Monitor overview

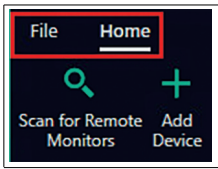


Figure 5.4

2025-07

PEPPERL+FUCHS

VisuNet CC Settings

1 Options:

Select "Options" from the navigation bar to adjust VisuNet CC settings. The following settings can be adjusted:

Function	Description
Open/Close Timeout	Specifies the time VisuNet CC waits for an answer from the RM / BTC during establishing/closing of a connection before a timeout occurs. Increase the timeout, when there are problems establishing a connection to device.
Connection Timeout	Specifies the time VisuNet CC waits for an answer from the RM / BTC when a connection has been established before a timeout occurs.
Refresh Cycle Timeout	Specifies the time intervals in which VisuNet CC automatically polls the connected RM / BTC for new device information. Increase the timeout, if connections are interrupted at short notice from time to time.
Maintenance Access Timeout	Specifies the time the local operator is given to respond to the dialog prompt before the maintenance mode is automatically entered.
Max simultaneous Actions:	Specifies the number of actions performed simultaneously. **Note:** Multiple simultaneous action can cause high network traffic, resulting in high latencies for other devices on the network.

In the log settings you can choose which Control Center events are being loged in the log file and where this will be stored on the local machine.

Home: Click the "Home" tab in the top-left corner of the VisuNet CC screen to enter the home view.

There are two different “Home” ribbon toolbars, depending on if a device is selected or the group view is active

Device: the device ribbon toolbar will only appear when a device is selected
Click the "Device" tab in the top-left corner of the VisuNet CC screen to enter the device view

For detailed information on the icons and their functions, see chapter 5.2.

2 Ribbon toolbar

On the toolbar, all available functions that can be performed in the mode currently in use, are grouped together.
For detailed information on the icons and their functions, .

3 **Navigation menu**

- The navigation menu lists all RMs/BTCs, that have been found during a network scan or have been added manually.
- The navigation menu list shows offline RMs/BTCs, that have been added to the project.
- The navigation menu allows RMs/BTCs to be added to group folders. With this feature, RMs/BTCs can be grouped according to their location.
- The devices can be right-clicked to open a top down menu with quick access.

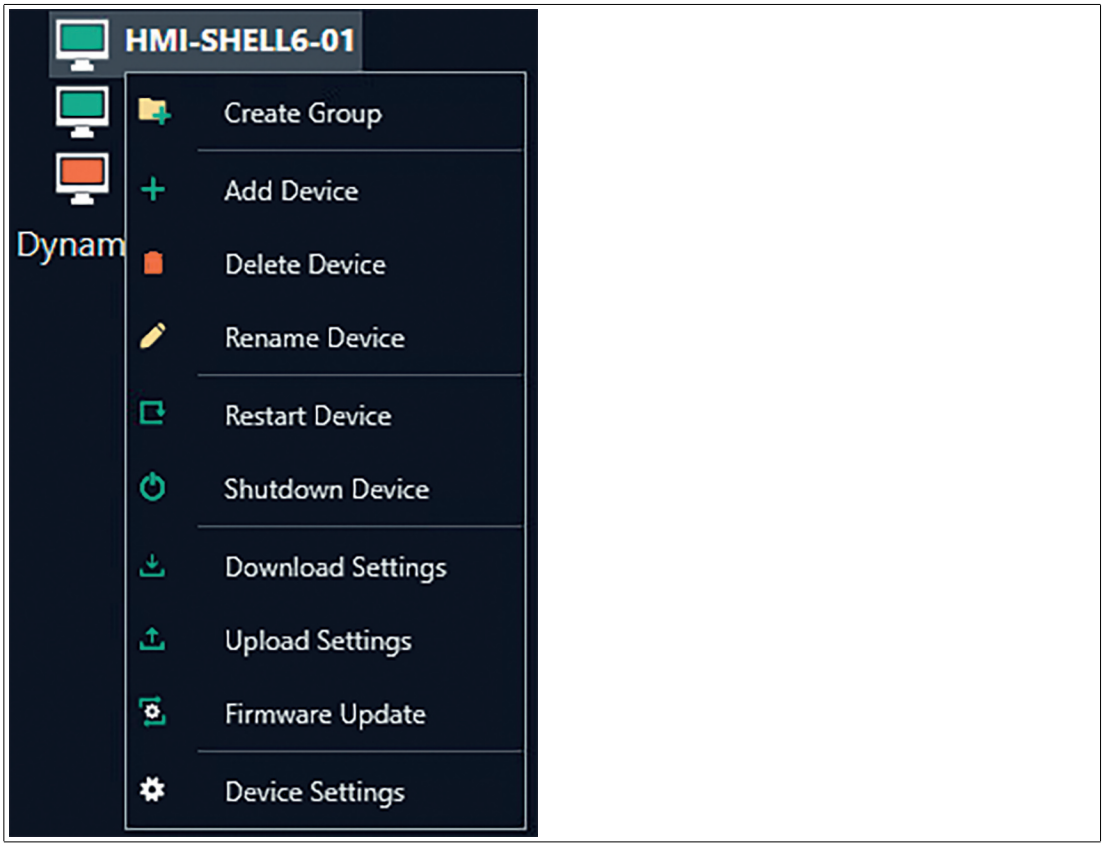


Figure 5.5

4 **Main screen**: In the center of the user interface, the main information is displayed. Based on the mode currently in use, the information for a RM/BTC, a group of RMs/BTCs or a general device overview either as list or tile view is presented.

Click "Remote Monitors" in the navigation menu to view an overview of all devices. "Tile view" is the default mode. This mode displays a live screenshot of each device.

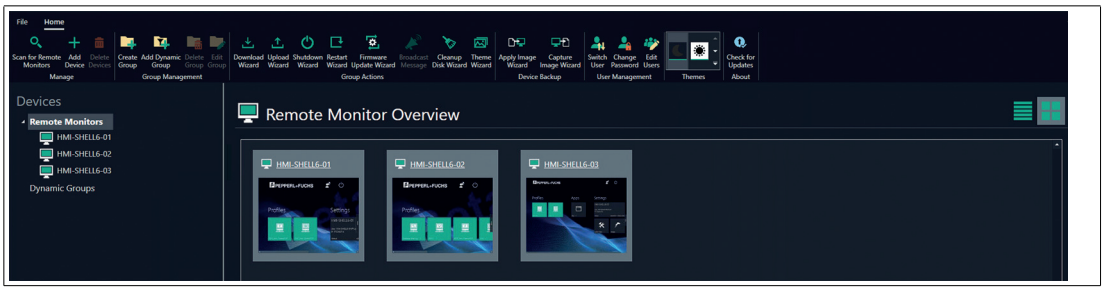


Figure 5.6

Click ☰ in the upper right corner to switch to list view. This mode displays a table of the devices with information about their online status, IP addresses, VisuNet RM Shell version and serial number.

2025-07

PEPPERL+FUCHS

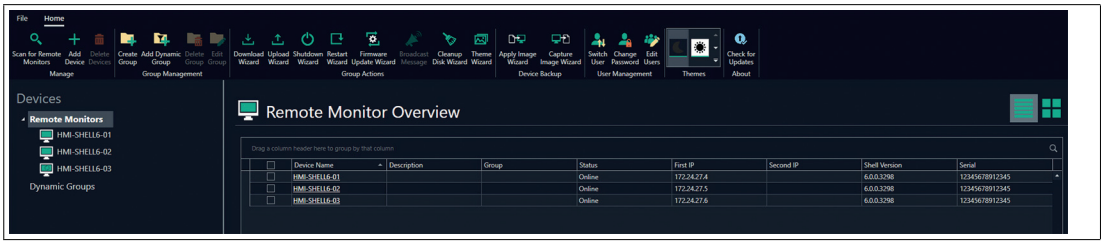


Figure 5.7

The single tiles or devices in the table are selectable by clicking. One or more RMs/BTCs can be selected to perform either single or group actions (ctrl + click to select multiple devices in the tile view).

Now, click on the device to enter the Device View.

5.2 Device Structure

To get further information of the single devices, use the double-click either in the navigation menu or at the list or tile view in the main screen.

This mode allows you to manage individual devices. The settings, information, and functions available in this view are divided into 5 general sections.

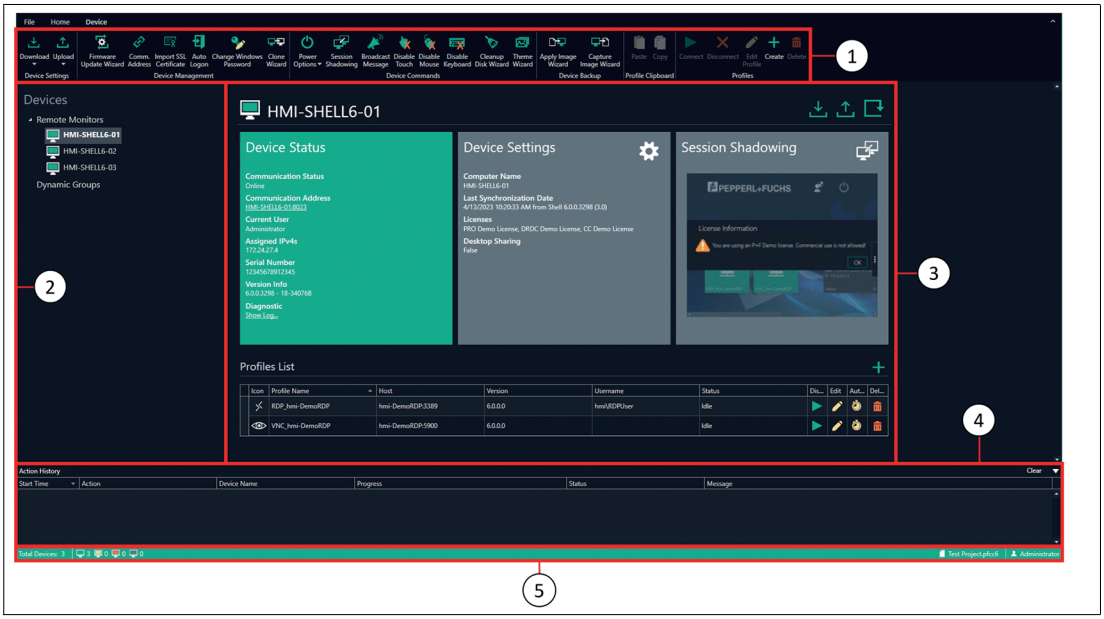


Figure 5.8

1 **Ribbon toolbar**
For further information regarding the control and manage elements .

2 **Navigation menu**

3 **Device function tiles** including the list of profiles.
For further information regarding the control and manage elements refer to the Device Function Tiles Chapter.

4 **Action History list** that contains all executed actions and all actions currently being executed.

5 **Status bar** indicating the device in the project with the number of online, in maintainance, faulty and offline devices. Project Name and currently active user is displayed.

6 Manage (Home)

In this chapter group actions and features are explained. The following actions can be executed when the remote monitor overview and the home tab are activated.

6.1 Group Management

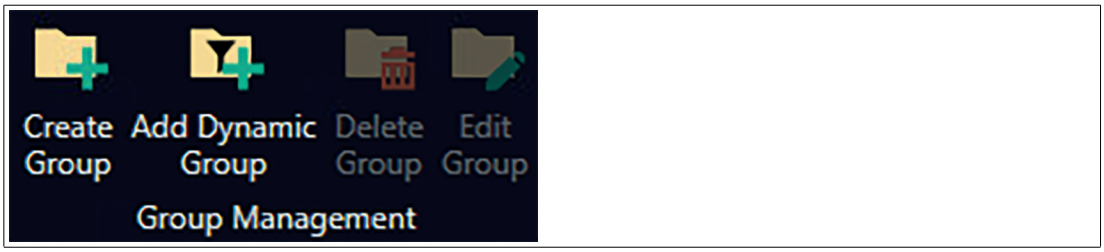


Figure 6.1

The Group Management helps you to organize your remote monitors. The different groups are the basis for the group actions.

Static Groups

An RM / BTC may be assigned to either one or zero groups. These groups are represented by a folder in the navigation menu. To assign a device to a group, click “Remote Monitors” in the navigation menu from list view mode. Click the group cell for the RM / BTC that you would like to assign, and assign it to the group you would like it to be in. Alternatively, click, hold, and drag an RM / BTC into a group folder on the navigation menu. To keep the assignment of an RM / BTC to a group, you must save the project.



Figure 6.2 Static groups

Dynamic Groups

Dynamic groups allow you to filter your list of RMs / BTCs based on their current online status.

To add a dynamic group, click “Add Dynamic Group” on the ribbon tool bar. You must assign it a name, and you can select which online statuses you would like to see when viewing the dynamic group. To keep a dynamic group, you must save the project.

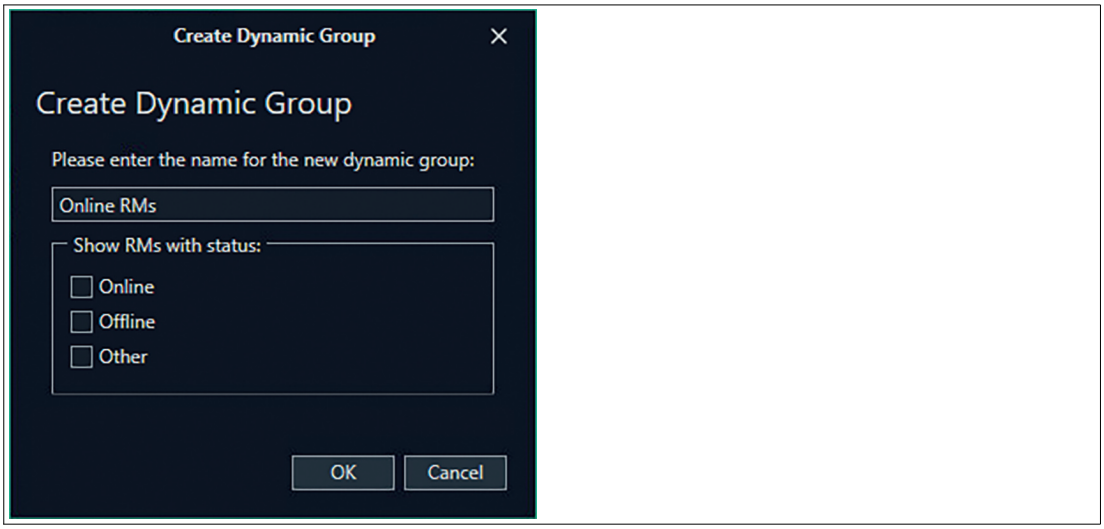


Figure 6.3 Create dynamic group window

6.2 View

Depending on your required actions either chose List View or Tile view. In both views multiple devices can be selected. Double click a device in either view or in the navigation menu to switch from device group view to device detail view.

6.3 Programm Apperance

The Programs appierance can be changed from the default dark theme to a light one.

6.4 Group Actions

Group actions allow you to perform actions on multiple devices with only one time set-up. This allows remote, multi device management which decreases set up times and therefore costs.

All group actions are performed via a wizard, which guides you through the single steps of your action. The wizards support you when down- or uploading multiple device settings, shutting down or restarting multiple devices, update multiple devices with a newer firmware or cleanup the disk of multiple devices. Additionally an RFID Wizard allows simply configuration of connected RFID readers.

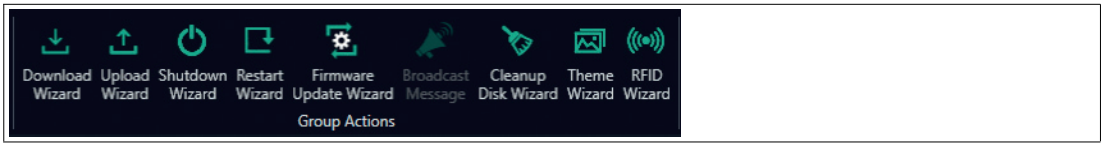


Figure 6.4

Performing a Group Action via Wizard

Perform Group Action via List View

Perform an action for a device group. Select your required devices by using one of the following methods:

1. Switch to "List View" mode.
2. Select one or more RMs / BTCs from your list of devices.



Figure 6.5 Selecting RMs for group actions

3. Switch to “Tile View” mode.

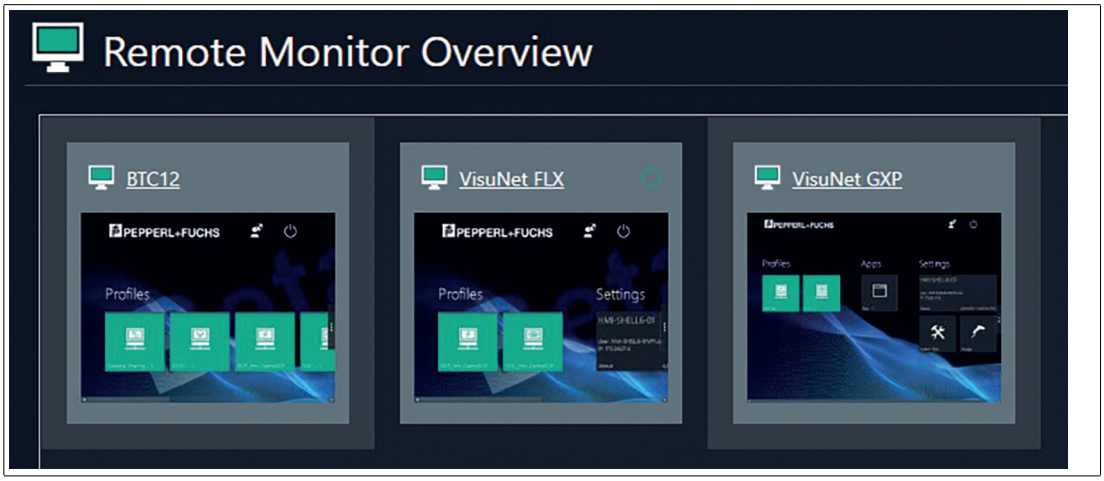


Figure 6.6

4. Select one or more RMs / BTCs by holding down the Ctrl key and click any device you would like to add.
5. Perform the same selection procedure within the static or dynamic groups.

Perform Group Action via Action Icon

1. Click on the icon that performs the desired action. In the following example, this action is a restart of the devices.

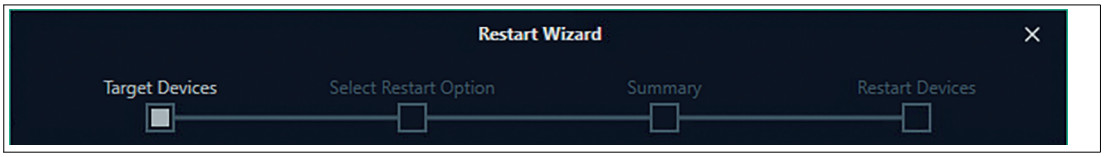


Figure 6.7 Restart Wizard: Target Devices

↳ A window of the wizard appears that guides you through all the actions.

2. Double check if the right devices are selected. Further devices can be added or removed from the selection.

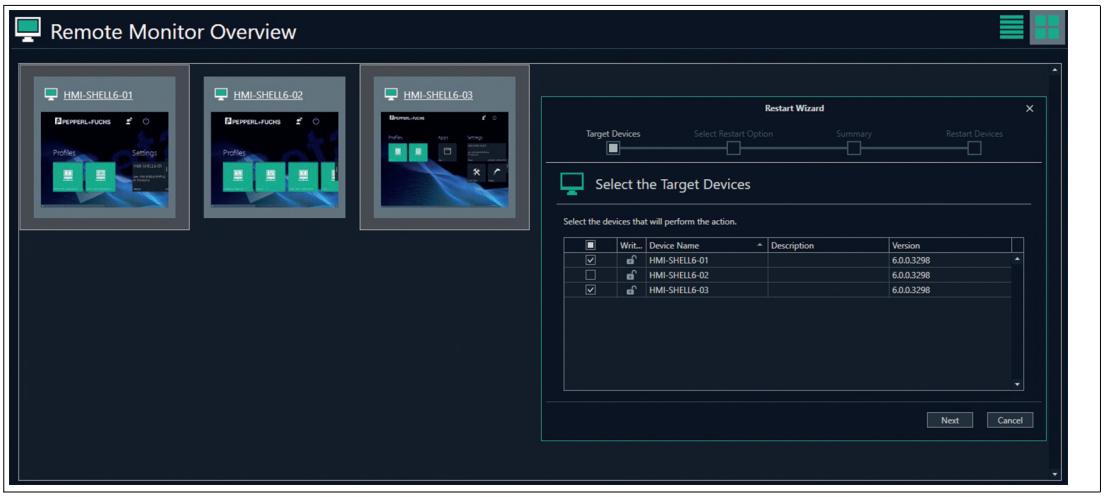


Figure 6.8

3. Click "Next".

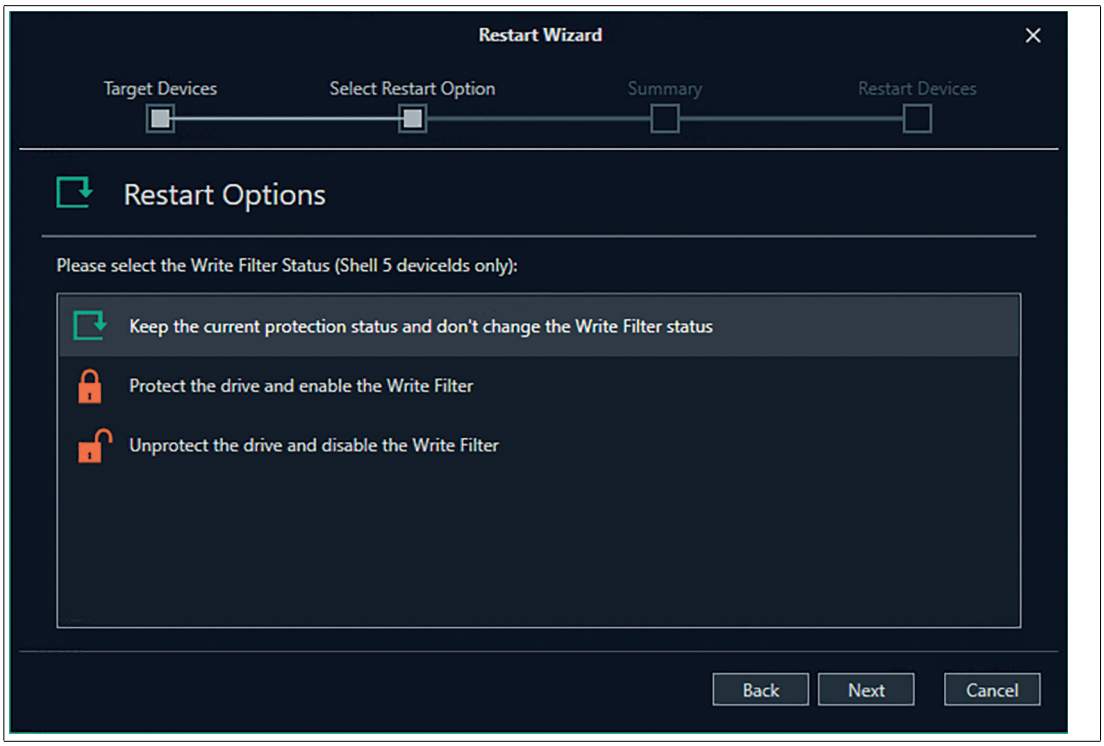


Figure 6.9 Restart Wizard: Select "Restart Options"

4. Select one of the options and click "Next".

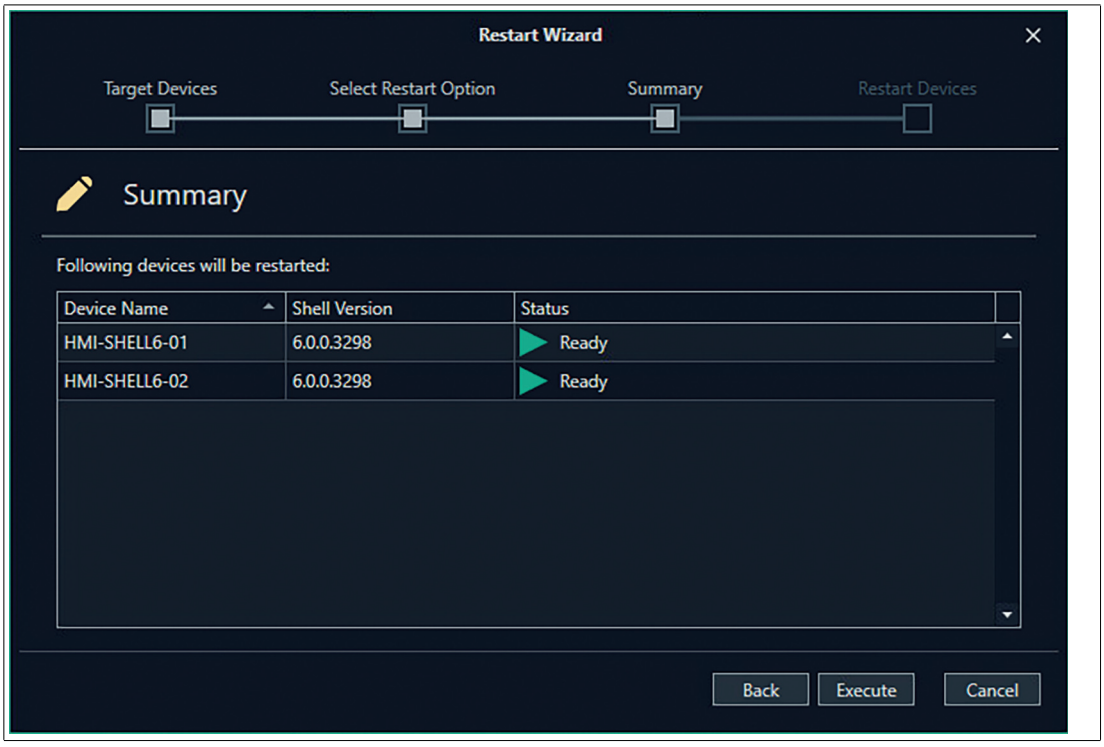


Figure 6.10 Restart Wizard: Summary

↳ In the ongoing steps you always have the option to move backwards and adjust your selection.

5. In the Summary recheck your selections and click "Execute" to proceed further.

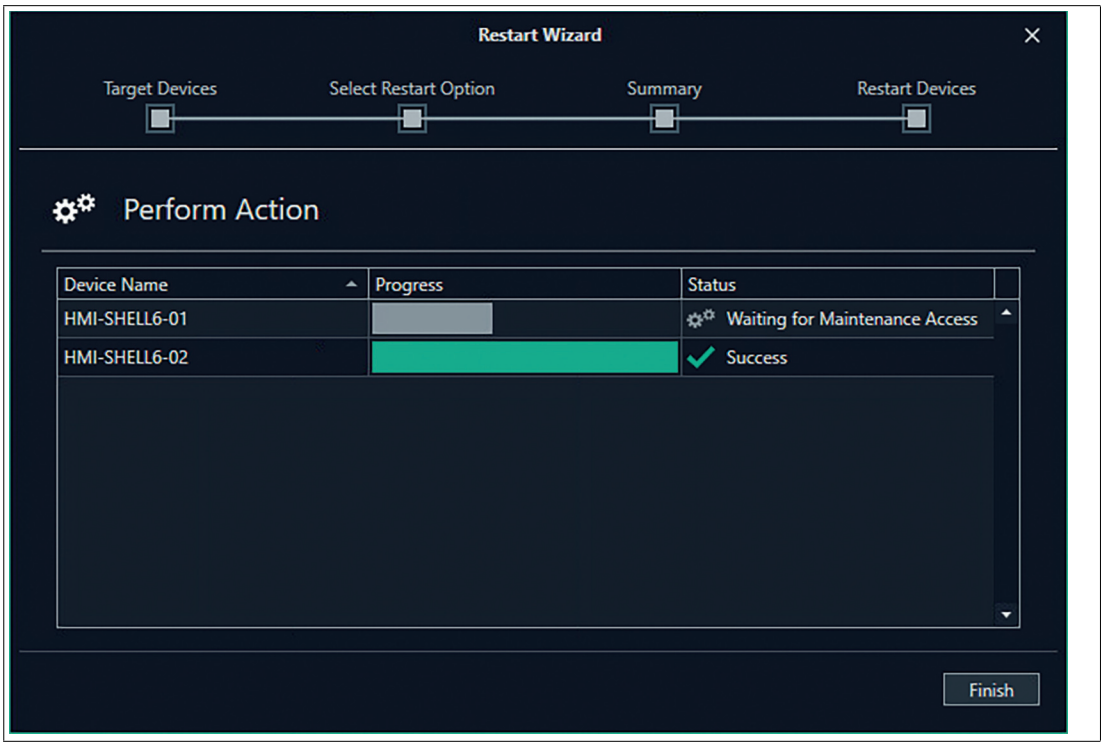


Figure 6.11 Restart Wizard: Restart Devices

↳ The wizard can be finished. The action will performed in the background until the status is set to success. The actions will be added to the action history, here the staus can be checked.

Firmware Update Wizard

The Firmware Update Wizard supports you in updating your latest version of the firmware e.g. VisuNet RM Shell 6.0 to VisuNet RM Shell 6.1.

Note

The Firmware Update Wizard is not the right tool to upgrade VisuNet RM Shell 5 to VisuNet RM Shell 6. Use the Quick Start Guide which is provided when purchasing the Upgrade Kit to get further information.

Updating Firmware

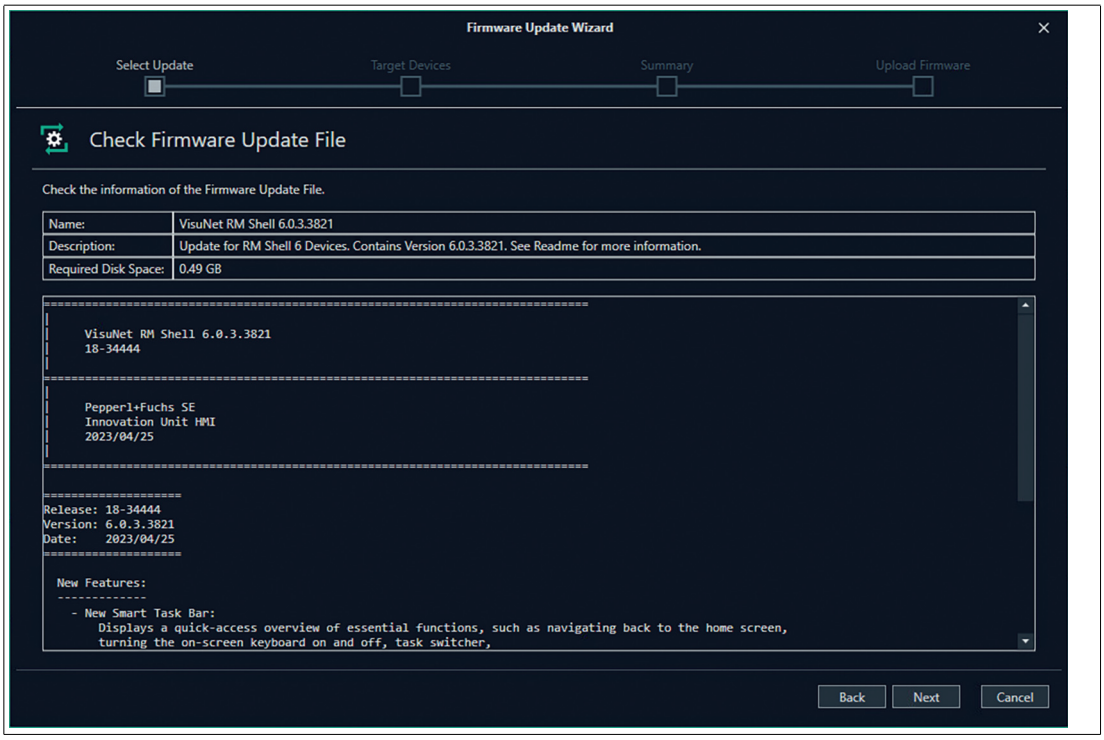


Figure 6.12 Firmware Update Wizard: Select Update

1. Select "Firmware Update File" and click "Open". You can find the latest available update on www.pepperl-fuchs.com and download the Zip file.
2. In step "Target devices", select required devices as described above. Double check if the right devices are selected. Further devices can be added or removed from the selection. By clicking , get detailed information about the selected device regarding communication status, enabled or disabled Write Filter or if your installed versions are compatible and supported. If your status has a red exclamation mark, follow the information provided.

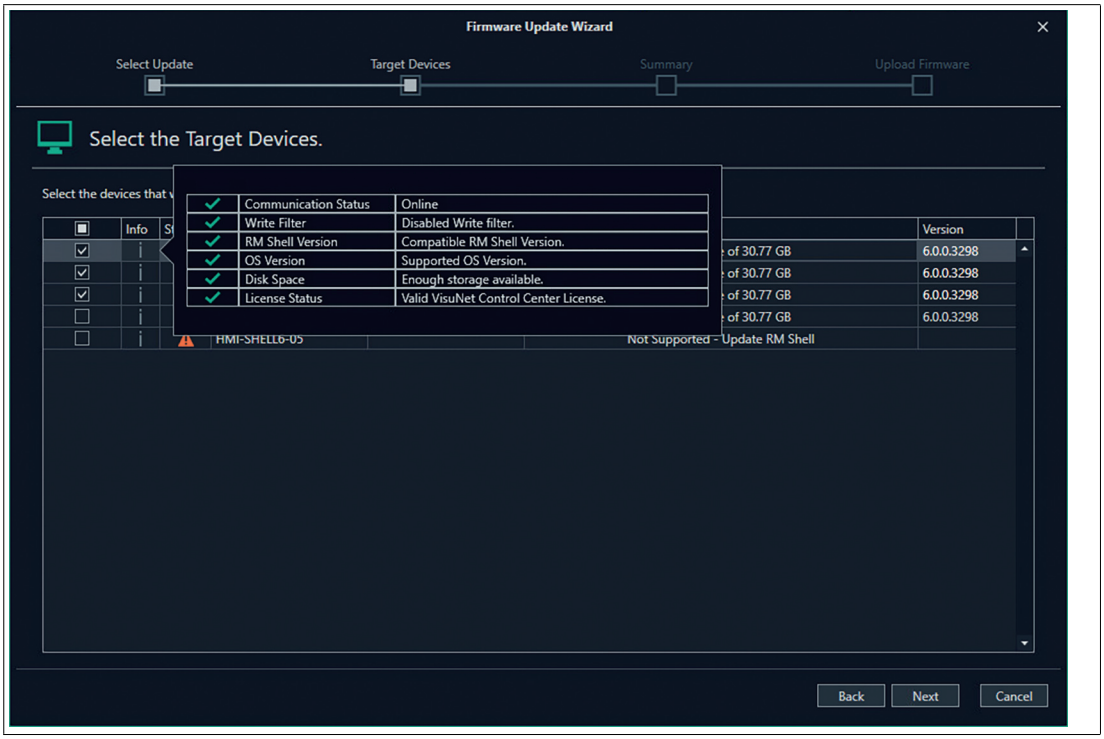


Figure 6.13 Select your target device

Category	Description	Troubleshooting
Communication Status	Offline	Make sure your device is online.
Write Filter	Write Filter is enabled. Please deactivate the write filter.	Please refer to chapter "Device Commands" to disable the Write Filter by restarting the device.
RM Shell Version	Incompatible RM Shell Version.	Refer to the RM Shell and Image version in the Device Status to check on your RM Shell version. Use the correct update, available online.
OS Version	Unsupported OS Version. Please download the relevant update for your OS.	Refer to the Software information in the **About** tile in your RM Shell to check on which Operating System your device is based on.
Disk Space	Not sufficient storage available. Please use the Cleanup Disk Wizard.	Please use the Cleanup Wizard. If the storage after cleaning up the disk is still not sufficient we recommend to update your device with the latest factory reset version >6.0. This will adapt your partition and increase the available storage.
License Status	Checks if a valid VisuNet Control Center License is assigned to the Device.	Assign VisuNet Control Center License

3. Click "Next".
4. In the summary recheck your selections and click "Execute" to proceed further.

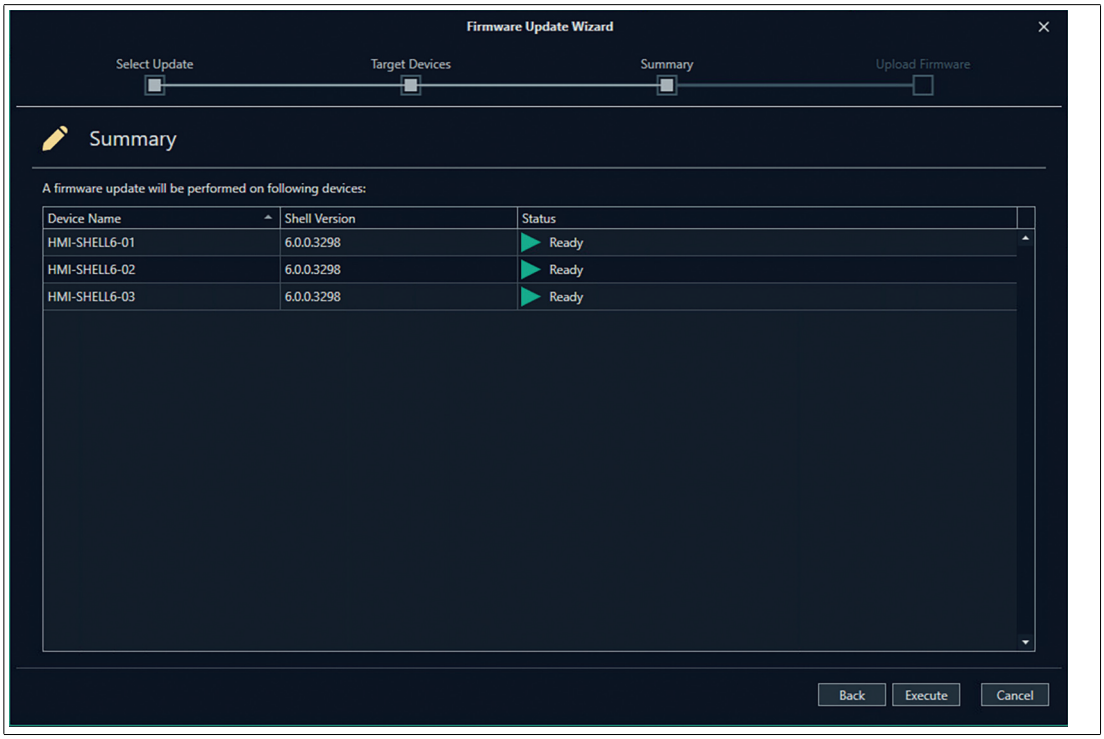


Figure 6.14

↳ When every device Status is set to "Success", the performed action is completed and the wizard can be finished

Broadcast Message

1. With one or more RMs selected, click the "Broadcast Message" icon.

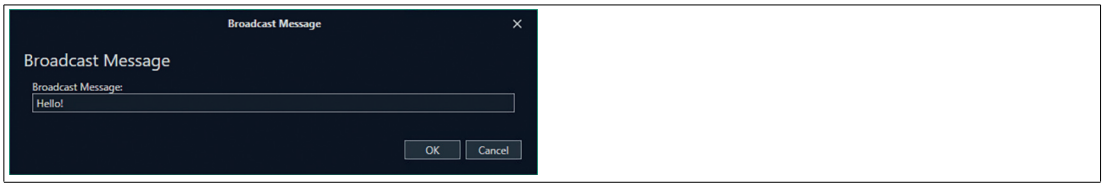


Figure 6.15 Broadcast Message Window

2. Type a message into the space provided. Click "OK".

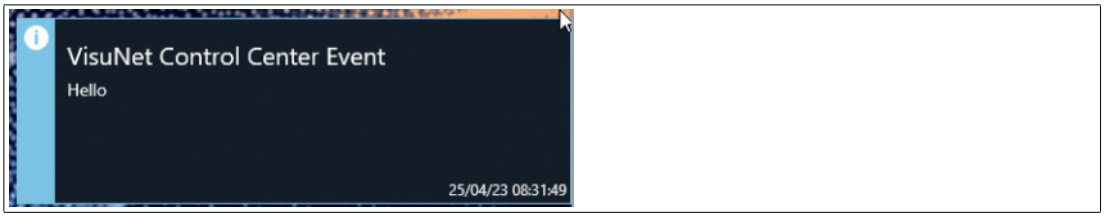


Figure 6.16 Fly-in message on RM Screen

↳ The text that you entered appears in a fly-in message to the users of the selected RMs.

6.5 User Management



Figure 6.17 User Management

VisuNet CC allows a project to be protected from access by unauthorized personnel via a user management system. For each project, an individual user structure can be created that allows you to assign permissions to individual user accounts. Further, a user group mechanism allows user to be added to groups and to assign group-based permissions to the users.

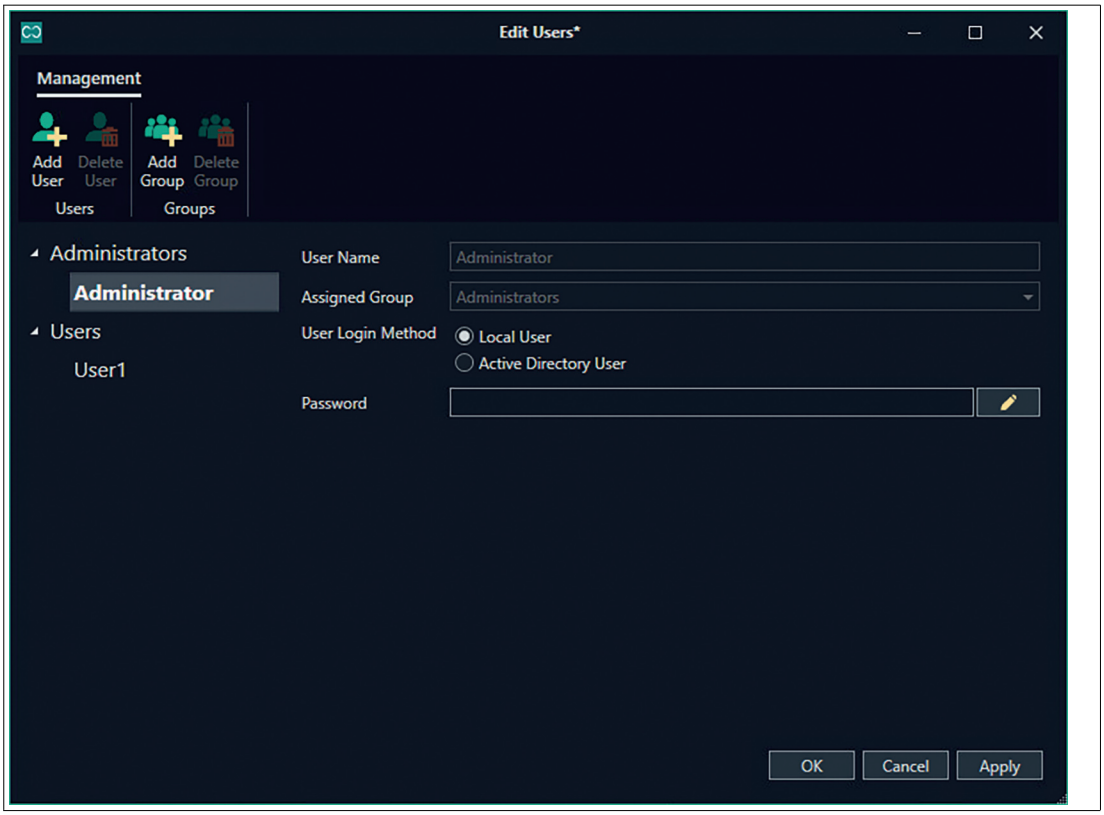


Figure 6.18 Add User Window - Local User

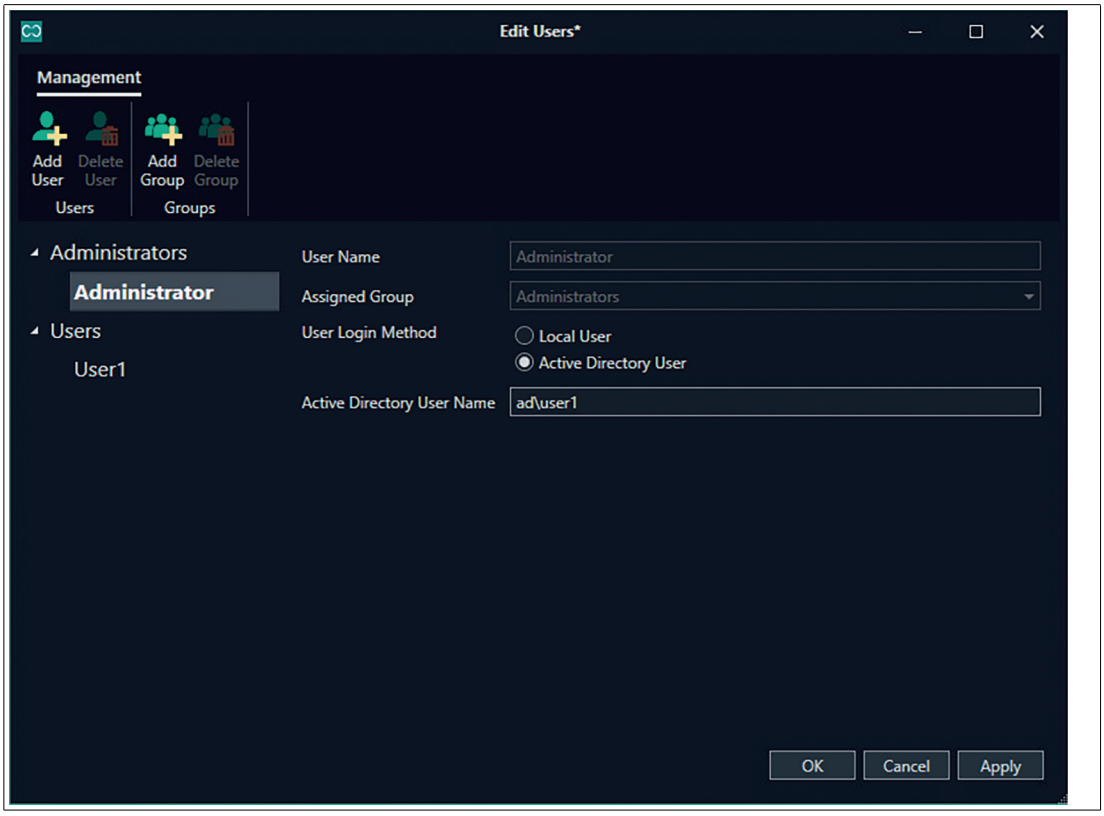


Figure 6.19 Add User Window - Active Directory User

User authentication can be configured by the "Administrator" account to be either a local user or an active directory user.

- **Local user:** Local user accounts are only stored within a Control Center project file and may have a password assigned to them, which they will need to enter to open the project.
- **Active Directory user:** Active directory users have an active directory user name associated with their account. When opening a project, if the logged-in Windows user's account is associated with a Control Center project account, the user will be automatically logged into the project under that name. The local user account may also have a password assigned to it as an alternative means of accessing it.

Per default, every project has an "Administrator" user account, an "Administrator" user group that has every privilege, and a "Users" user group that will act as the default group for newly created users.

Note

If you create a new project, you will automatically be logged in as Adminsitrator.

Note

By default, the Administrator user has no password set. To protect the project from unauthorized access, always set a strong password for the Administrator.

User accounts must be assigned to a single user group, which may have any number of VisuNet CC permissions assigned to it. The following permissions can be set for a user / user group:

Function	Description
Allow upload settings	Allows a user to upload configuration to an RM, import an SSL certificate to an RM, and perform a firmware update on an RM.
Allow Session Shadowing Remote Control	Allows a user to take control of an RM while in session shadowing.
Allow Viewing of Session Shadowing	Allows a user to view an RM via session shadowing.
Allow Editing Profiles	Allows a user to create, delete, and edit connection profiles.
Allow Starting/Stopping Profiles	Allows a user to start and stop the connection of profiles.
Allow Editing User Privileges	Allows a user to access the “Edit Users” screen and add, delete, and modify users and user groups.
Allow Local Commands	Allows a user to enable or disable an RM’s keyboard, mouse, and touchscreen. In addition the user is allowed to reboot, and shut down the devices as well as using the Apply/Capture Wizard.
Allow Editing of Project Structure	Allows a user to scan for RMs, manually add an RM, remove an RM, or assign an RM to a group.
Allow Firmware Update	Allows user to Update single or multiple Devices with the latest Firmware.

Table 6.1

6.6 License Manager

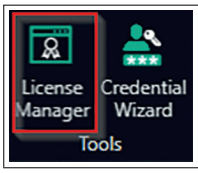


Figure 6.20

Using the License Manager, you can manage your licenses for VisuNet Control Center, DRDC and the pro version of VisuNet RM Shell 6. You can add, remove, and (re)assign licenses to devices.

The License Manager consists of three tabs: The License Vault and two pages for assigning VisuNet RM Shell 5 and 6 licenses.

Note

After pressing "OK" after (re)assigning the licenses, the licenses are only changed in Control Center. If you want to transfer the changes to the devices, please use the upload wizard afterwards.

License Vault

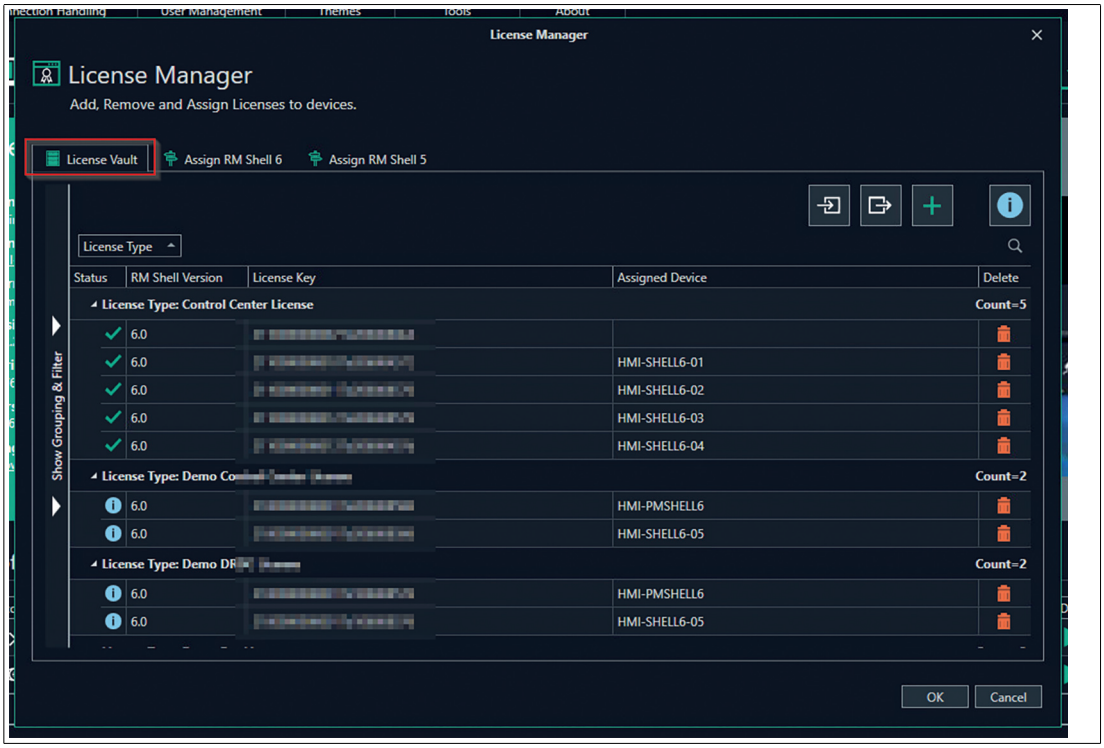


Figure 6.21

All licenses that have already been assigned are listed in the License Vault. You can see the license keys and which devices the licenses are currently assigned to. By default, the licenses are sorted by license type. Drag and drop the desired category to filter by it.

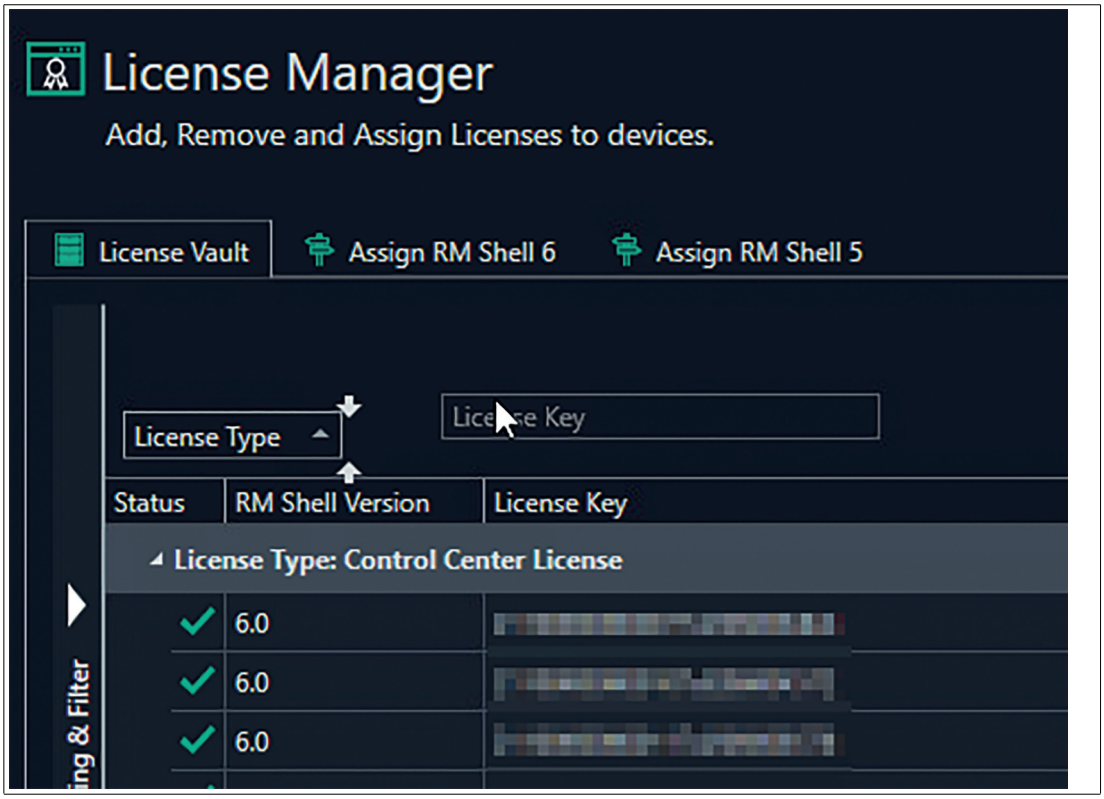


Figure 6.22

2025-07

PEPPERL+FUCHS

Expand the "Grouping & Filter" menu on the left to get an overview of the possible filtering and grouping options. This can be particularly helpful if you have many devices with assigned licenses.

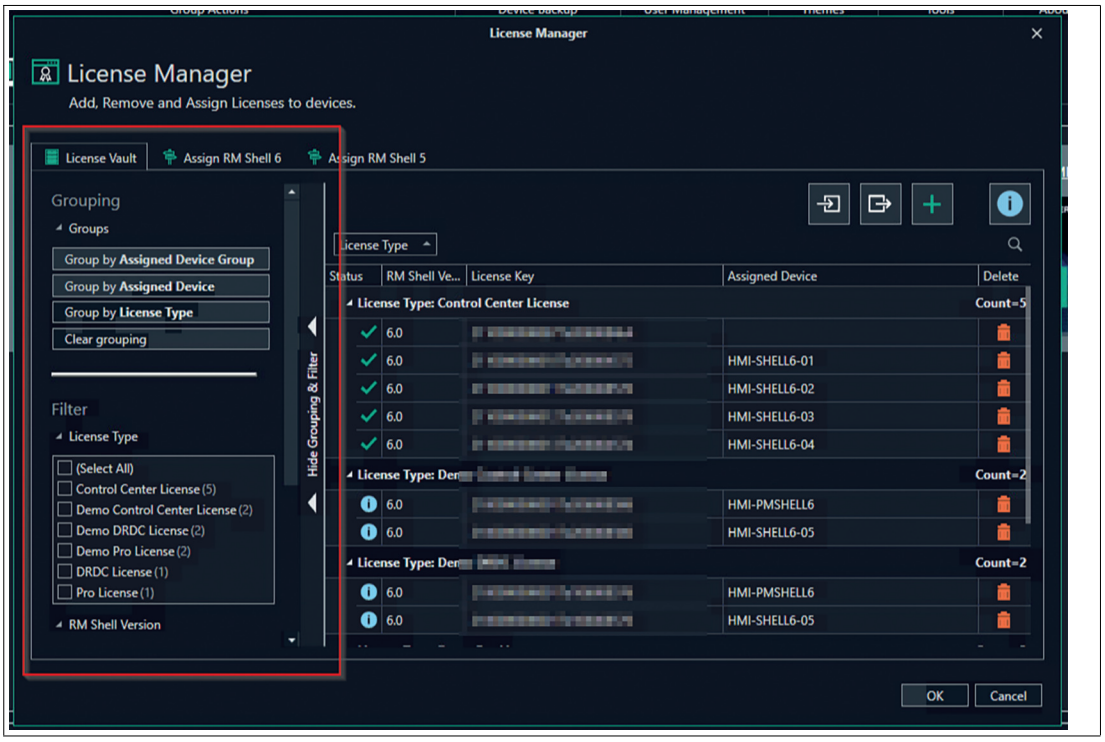


Figure 6.23

Importing, exporting and entering licenses manually:

You can add licenses in the License Vault. You can either import this as a .xml file or enter it manually. If you ordered digital licenses, you will also receive a .xml file via mail that you can import. You can also export your licenses as a .csv file.



Figure 6.24 Import licenses as .xml and .txt files



Figure 6.25 Export licenses as .xml and .txt files



Figure 6.26 Add licenses manually

Assign Licenses to devices

Under the tab "Assign RM Shell 6" and "Assign RM Shell 5" you can assign licenses to devices. On the left side you can see the available licenses and how many of them have already been allocated or not yet allocated. At the bottom left you can see the devices to which you can assign the licenses. To now assign one or more licenses to one or more devices, follow the following steps:

1. Select the license(s) you want to assign
2. Select the device(s) you want to assign it to
3. Click "Assign" in the middle of the page. On the right you can see which licenses are assigned to which device.
4. After assigning, click OK
5. The licenses are now assigned

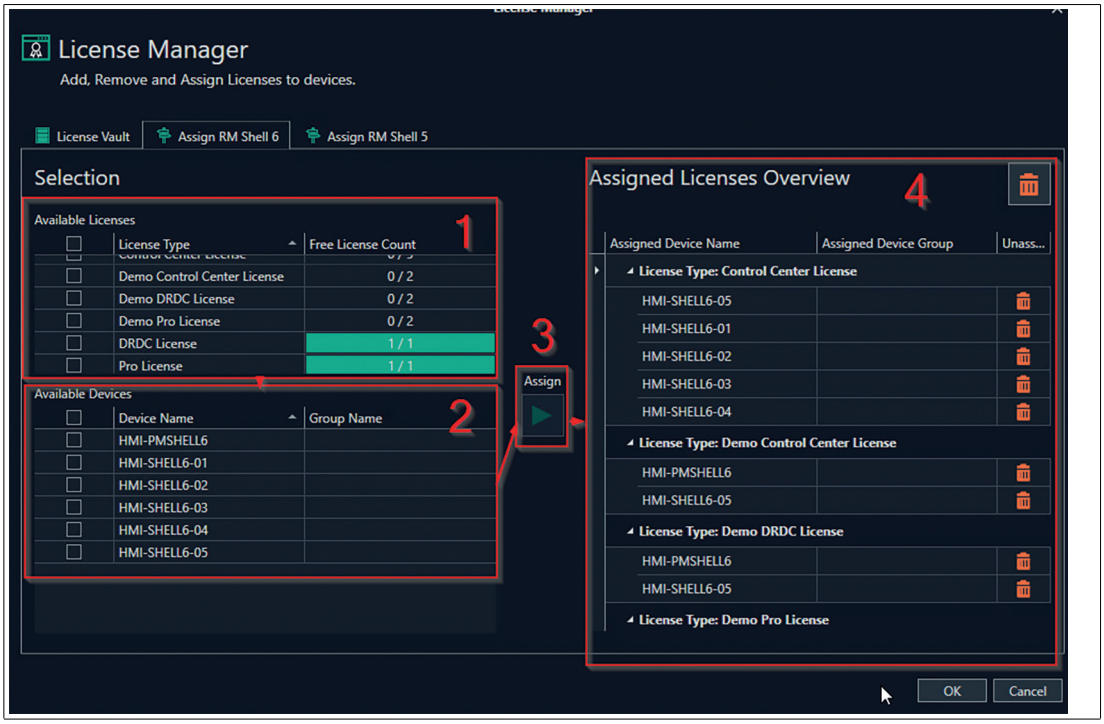


Figure 6.27

Note

Please make sure that you have enough licenses for the selected devices in your License Vault. If you do not have enough licenses to assign to the selected devices, you will see an error message.

You can unassign all licenses on the red trash can in the top right corner. They then return back to the "Available Licenses" section and you can assign them to the desired devices again.

Unassign licenses:

On the right, there is a red trash bin icon:



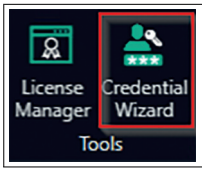
Figure 6.28

If you have unassigned a license, it will reappear under either the "Assign RM Shell 6" or "Assign RM Shell 5" tab, depending on which license type it is. You can reassign the unassigned licenses under the corresponding "Assign" tab.

Delete licenses

Licenses can be deleted in the License Vault only. In the "Assign" tabs, licenses are not deleted but unassigned. Deleting licenses removes the license completely. This means that the license is no longer listed in the vault and is no longer assigned to the device.

6.7 Credential Wizard



The Credential Wizard is a tool that allows you to update, change and manage various credentials for different scenarios for all VisuNet RM Shell 5 and 6 devices in bulk and simultaneously.

There are four different options as to which actions that you can select:

1. Change Device Accounts

This path can be used to change passwords for a device or Windows® account. The password is changed locally on the respective device. With VisuNet RM Shell 6, local Windows® user passwords can be changed (e.g. PFUser or PFAdmin). With VisuNet RM Shell 5, the local user roles can be changed (e.g. Engineer, Operator). In addition, local services such as the Desktop Sharing password, the Smart Screen Saver Pin and the Factory Reset password can be changed.

You can select one or more options that you want to change at the same time.

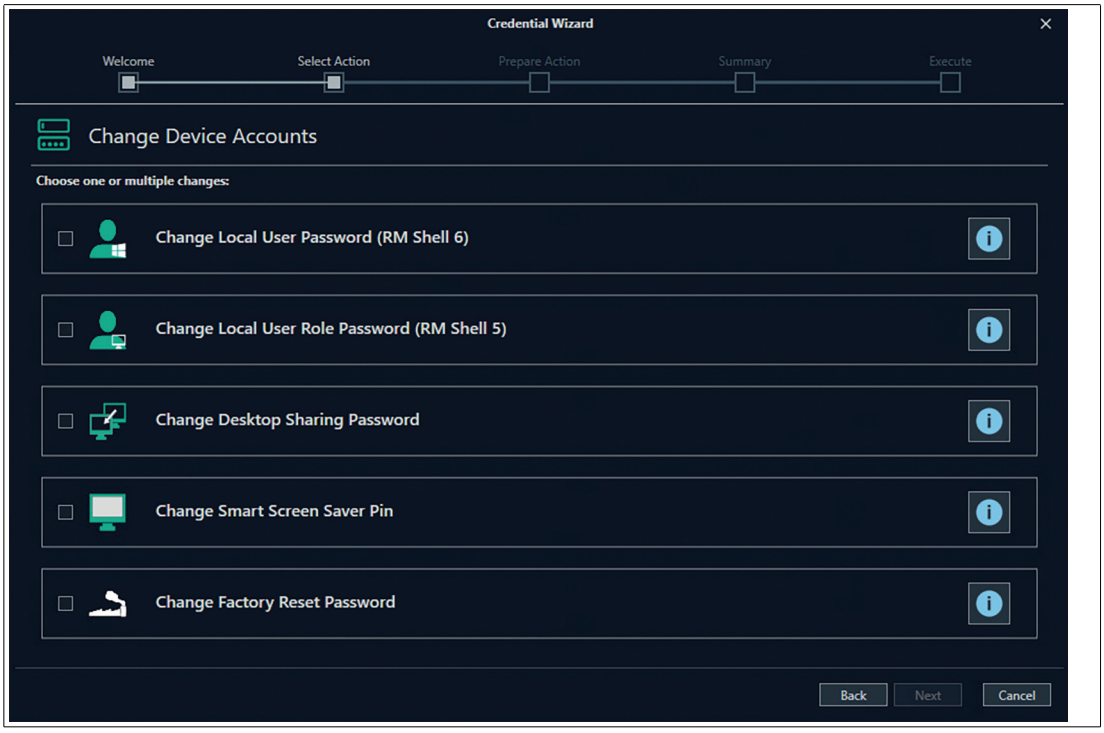


Figure 6.29

The structure of the pages is quite similar for the "Change Device Accounts" path for all sub-pages.

Please note:

- Empty lines with no entered passwords are skipped
- The password policy is set externally for "Change local user password (RM Shell 6)" and "Change local user role password (RM Shell 5)"
- Data can be exported and imported as .csv in Control Center (see graphic)
- The changes are only executed in the "Execute" step

Change Local User Password (RM Shell 6):

Via this path the passwords for the local users (e.g. PFAdmin and PFUser) can be changed. Those passwords are stored locally on the device. The password change will be applied directly to the device after the selected options wizard have been executed via the credential wizard.

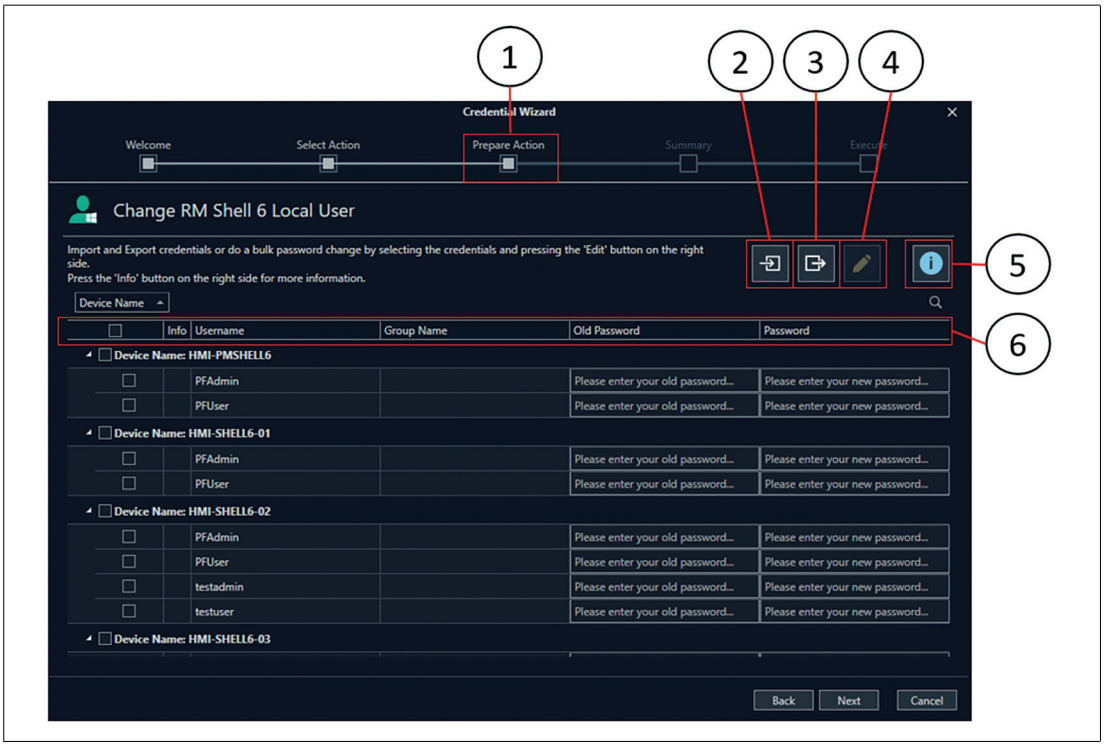


Figure 6.30

1. Navigation im Credential Wizard
2. Import Data as .csv file
3. Export Data as .csv file
4. Enter Data manually
5. Info (e.g. Password Policy)
6. Categories (drag and drop to sort by them)

Change Local User Role Password (RM Shell 5):

Via this path, passwords local user roles ("Engineer" or "Administrator") of VisuNet RM Shell 5 devices can be changed locally on the device itself.

Change Desktop Sharing Password:

Desktop Sharing is a service that - when enabled within the VisuNet RM Shell device - allows Control Center (and other VisuNet RM Shell devices) to access the desktop via Session Shadowing. This means that a user in Control Center is able to remotely gain access to the desktop of an VisuNet RM Shell device. This access from Control Center can be password protected. If you want to change the password, it can be updated via this path.

Change Smart Screen Saver Pin

The Smart Screen Saver (formerly known as Previs) is a screensaver that reduces burn-in effects.

Via this path, this pin can be bulk changed on the required VisuNet RM Shell devices.

Note

The PIN must only contain numbers (0 - 9).

Change Factory Reset Password:

The factory reset password is required to reset a device to the factory state.

Via this path, this password can be bulk changed remotely.

Note

The factory reset password must be at least 6 characters long.

2. Update Profile Credentials

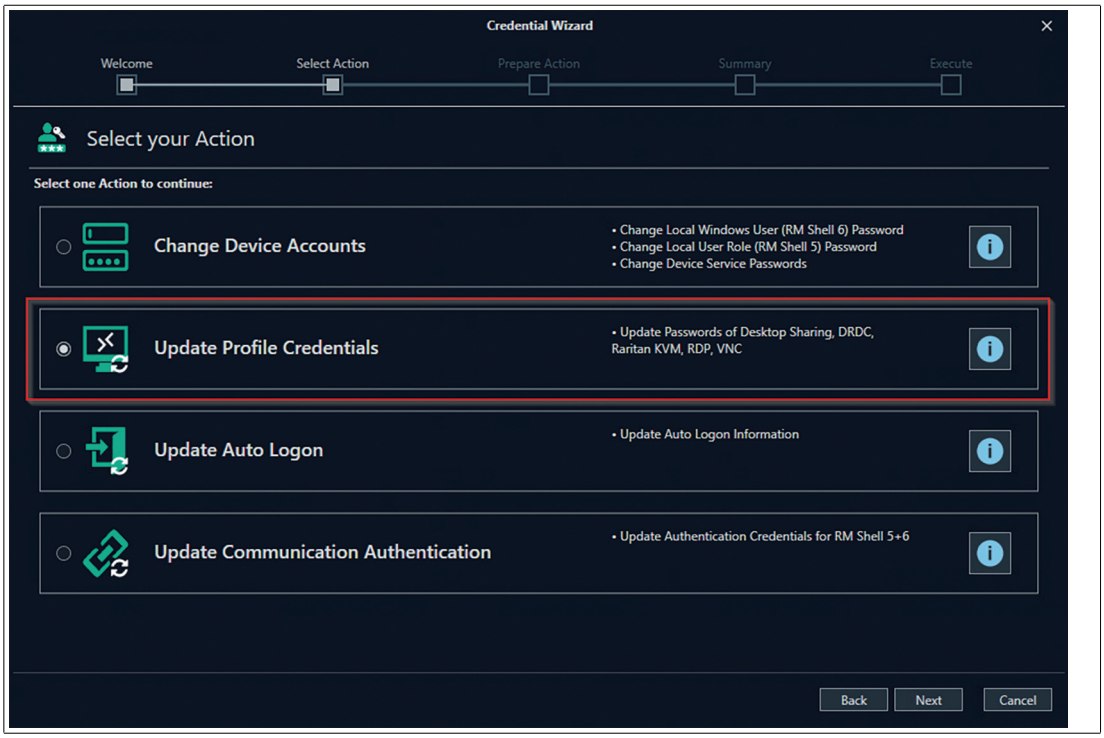


Figure 6.31

When configuring a connection in VisuNet RM Shell, you can set a password that is required to establish the connection. These passwords are saved in the profiles on the local devices. If this password is changed externally (e.g. by the domain), they can be updated in this way.

Note

The password policy is set externally.

3. Update Auto Logon

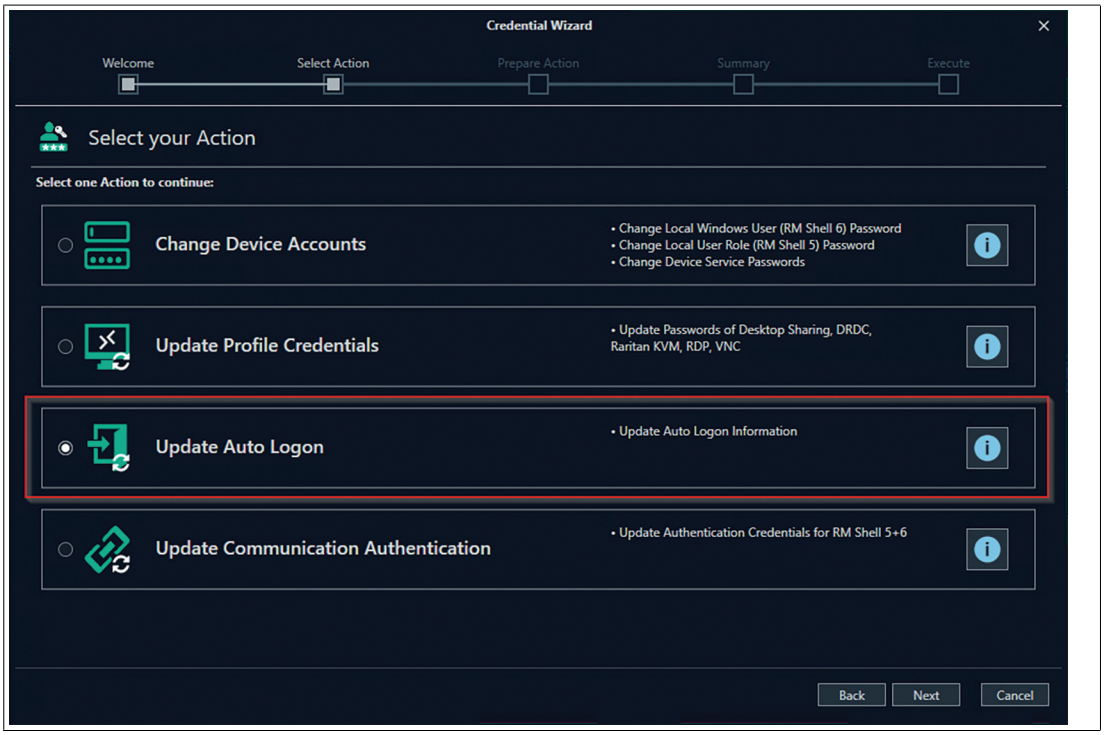


Figure 6.32

In VisuNet RM Shell 6, you can set a user to automatically log in when the system is started. To do this, a user is defined and the password is saved in the RM Shell so that the user can log in automatically when the system starts up.

If this password is changed (e.g. via the domain), it can be updated via this Auto Logon path so that the automatic logon process is retained.

4. Update Communication Authentication

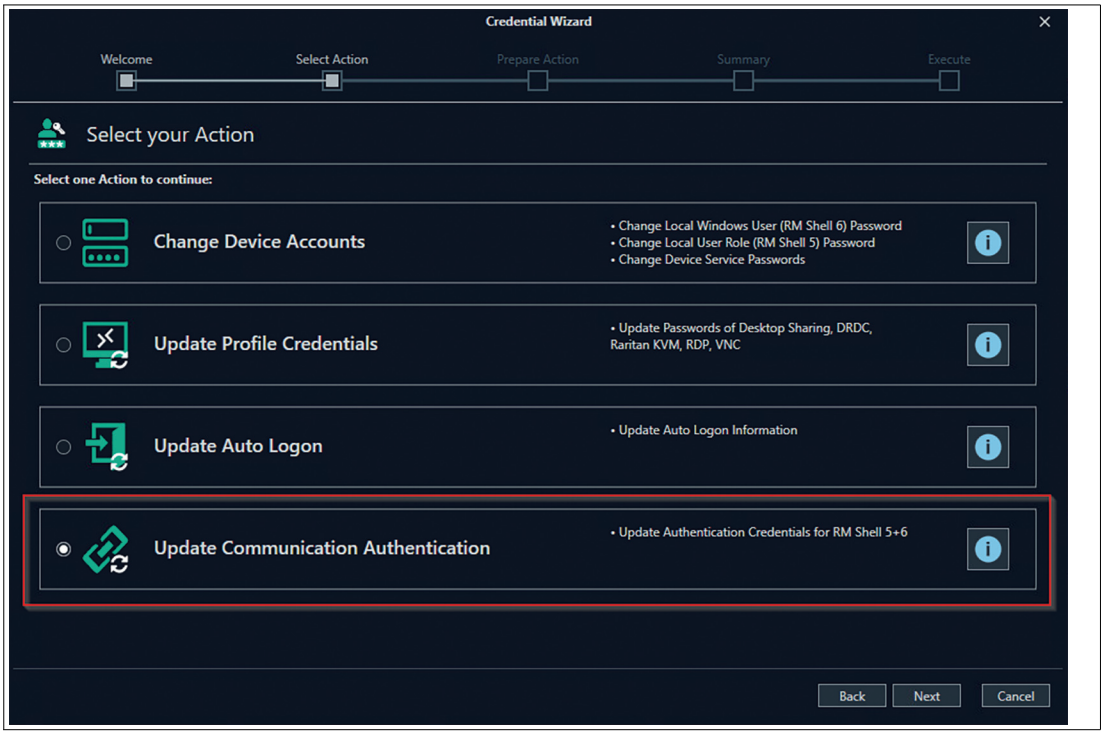


Figure 6.33

When accessing an RM Shell 5 or 6 device via Control Center for the first time, it is required to enter the password of the local administrative account to gain access. If Control Center already knows the VisuNet RM Shell device, but the password of the local administrative account on the VisuNet RM Shell device has changed, the password must also be reentered in Control Center in order to establish communication between Control Center and the VisuNet RM Shell device.

To avoid having to enter these passwords individually, you can use this path.

Here you can enter the passwords of the local administrative accounts of the VisuNet RM Shell 5 and 6 devices in order to be able to access the VisuNet RM Shell devices from Control Center.

6.8 About

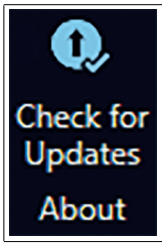


Figure 6.34

With this button you can check if any Updates for VisuNet Control Center are available. To use this function the device needs to have Internet access. Updates can be directly installed to the device.

Otherwise you can update the program by downloading the latest version on the Pepperl+Fuchs website.

7 Manage (Device)

To change to the device view, click the required device in the navigation menu or main screen.

Overview of the Device Structure, see chapter 5.2.

7.1 Device Function Tiles

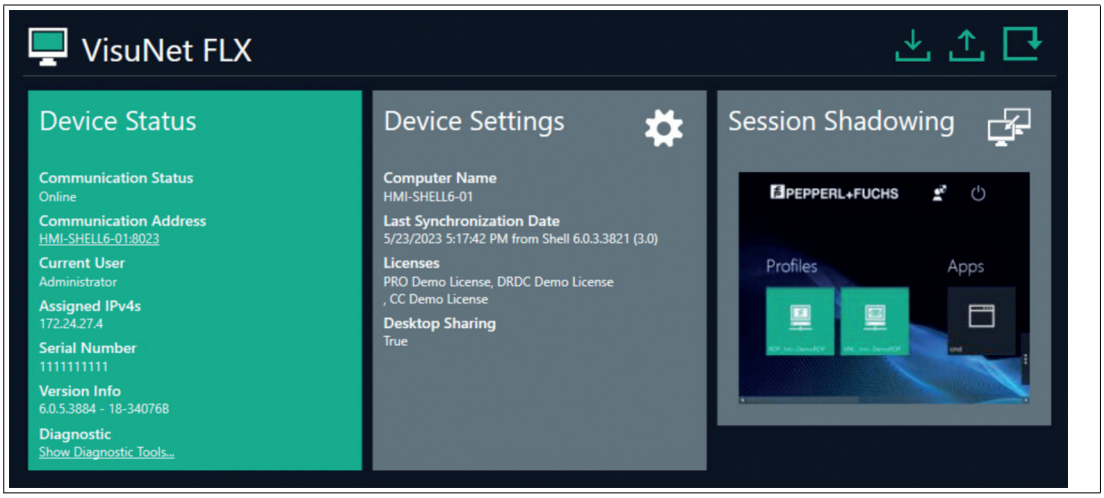


Figure 7.1 Device Function Tiles - Overview

The function tiles provide an overview of the core RM / BTC system information. Three tiles are used to summarize the following information and functions:

- **Device Status:** Read-only information about the RM / BTC. If the connection to the RM / BTC is active, the displayed data is live information that is periodically updated.
- **Device Settings:** The "Device Settings" tile groups all settings of an RM / BTC. Clicking once on the tile opens a separate window that groups all available functions for changing the RM / BTC settings.
- **Session Shadowing:** The "Session Shadowing" tile provides a live preview of the current RM / BTC screen. Clicking once on the tile opens a separate session shadowing window.

Device Settings

Above the tiles, there are also two shortcuts to synchronize the data of the Control Center with the RM / BTC:

- **Upload/Download:** The left arrow in the upper right corner is a shortcut that allows settings and data from the RM / BTC to be downloaded to VisuNet CC when the connection to the RM / BTC is active. The right arrow allows current configuration of VisuNet CC to be uploaded to the RM / BTC when the connection to the RM / BTC is active.

7.1.1 Device Status

The device status tile displays important device information.

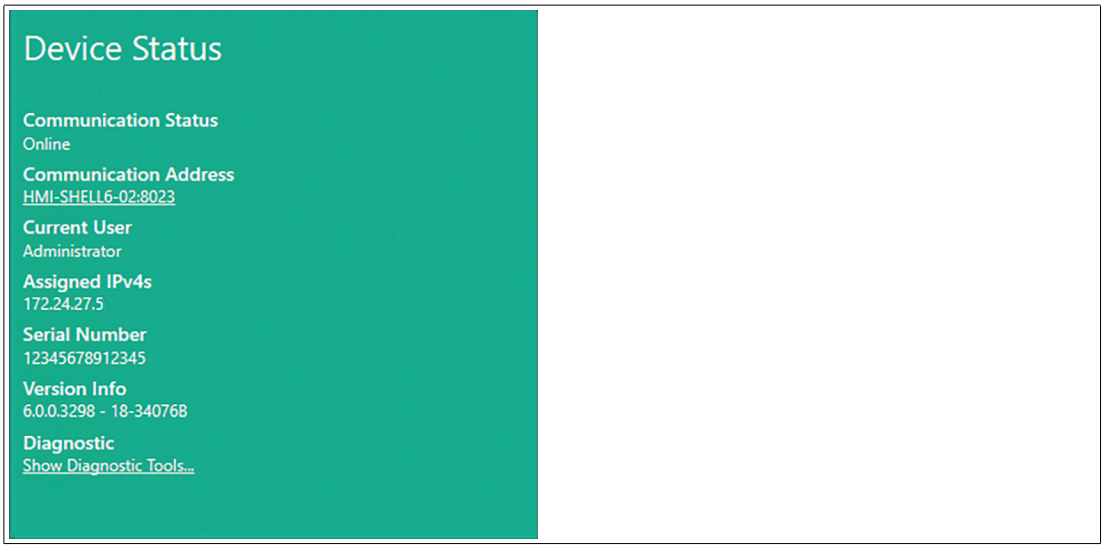


Figure 7.2 The tile color indicates the current status of the device:

- Green: The device is online
- Yellow: The device is in maintainance mode
- Orange: The device is in a fault state
- Grey: The device is offline

Function	Description
Communication Status	• Shows the status of a connection to an RM / BTC. • Shows correction steps, if the connection is disrupted.
Communication Address	The communication address establishes the communication between VisuNet CC and the RM / BTC device and can be the name of the device or the IP address. The computer name is, when enabled, independent from the communication address and will appear in the main device screen as well as the navigation menu and will only be stored in VisuNet CC.
Current User	Shows the current user role that is logged in on the RM / BTC.
Assigned IPv4s	List of the RM's IPv4 address. If the RM has multiple network interface cards and IP addresses, additional IPs will be listed here.
Serial Number	Shows the product serial number of the RM / BTC. The serial number is also on the type plate of the RM / BTC.
RM Shell and Image Version	Shows the version number of the RM Shell and Image on the RM / BTC. The image version is only listed in the latest RM Shell 5.1 version.
Show Diagnostic Tool	The menu shows the system information, update log and image log. For more information see below.

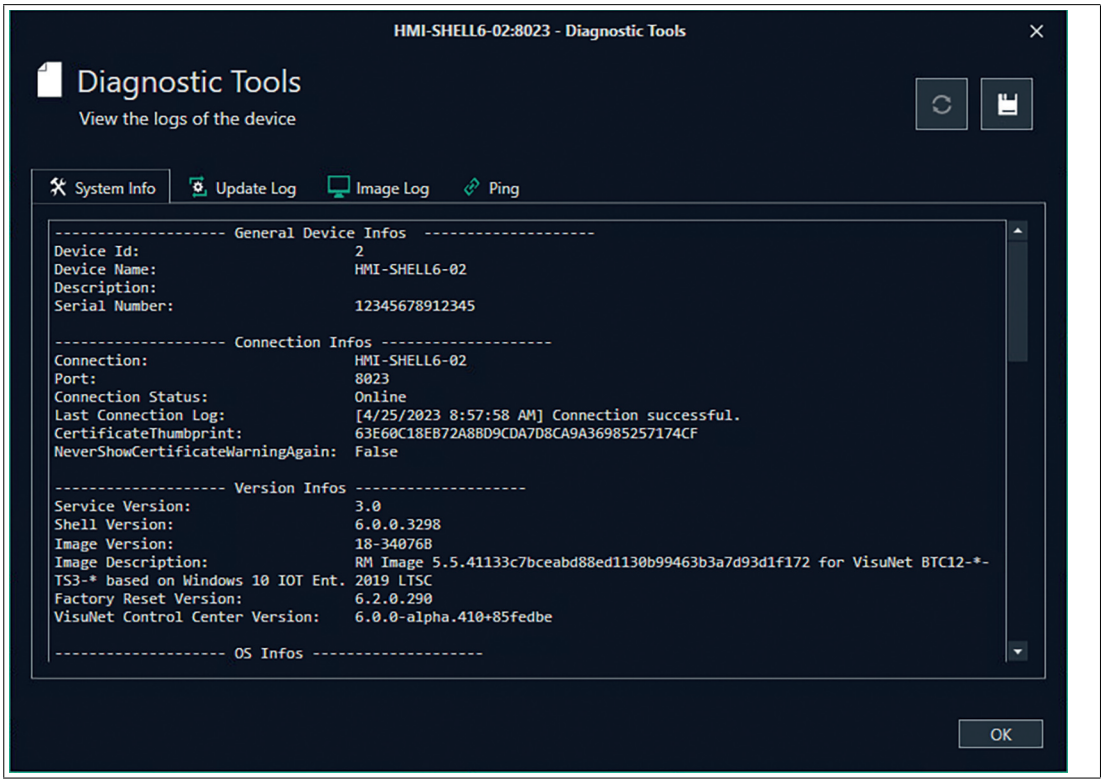


Figure 7.3

The menu shows the system information, update log, image log and VisuNet RM Shell log. This can be saved and exported into a file. Additionaly the device can be pinged manually here.

Note

Info! System info are important information for support log information provides information about errors - error handling can then be performed. The ping tool provides information about whether the device can be contacted on the network. Data can be saved and sent directly to support.

7.1.2 Device Settings (Tile)

Caution!
VisuNet RM Shell 5 devices have different categories and order of options.



Figure 7.4

Function	Description
Computer Name	When changing the Computer Name, the device must be restarted to adapt the settings to the Windows® settings.
Last Synchronization Date	Shows the date and time that the configurations between the VisuNet CC project and the RM were last synchronized via an upload or download.
Licenses	Shows which licenses are currently entered in the VisuNet RM Shell of the RM.
Desktop Sharing	Shows if the "Desktop Sharing" mode of the RM is enabled or disabled. "Desktop Sharing" must be enabled on an RM to use the session shadowing function in VisuNet CC.

When you click the tile, a window opens that groups the RM's / BTC settings. In this window, all relevant settings that can be changed in the VisuNet RM Shell can also be modified.

Note
The RM's / BTC settings must be uploaded onto the RM / BTC in order to be updated.

General

- **RM Shell and Local Windows User Passwords:** Set the password for factory reset.
- **Automatic User Logout:** Enable the automatic logout of the user and specify the idle time before an administrator is logged out.
- **RFID Reader** - choose connected RFID reader, only possible if an RFID Reader is connected to the device.
- **License Information:** Find license information on the actively used licenses. You can also add new licenses by clicking on the button below

2025-07

Home Screen Settings

- **Smart Task Bar Settings:** Enable the Smart Task Bar for quickly switching between tasks, easily accessing the Home Screen, open the On-Screen Keyboard or to open the Task Switcher
- **Home Screen Settings:** Select which functions and information is visible to the operator
- **Power Button on Home Screen for Operator:** Chose the displayed Power Buttons for the Operator. When hiding the corresponding button, the operator is not able to perform the action. The configurable Power Buttons are "Restart", "Shutdown", "Switch Windows User" and "Turn off display"
- **Floating Quick Menu:** Shows Floating Quick Menu with On-Screen Keyboard function, battery indicator and Wifi connection (depending on hardware)

Look & Feel

- **Wallpaper and Logo:** To use this function, an additional PRO license is required.

Desktop Sharing

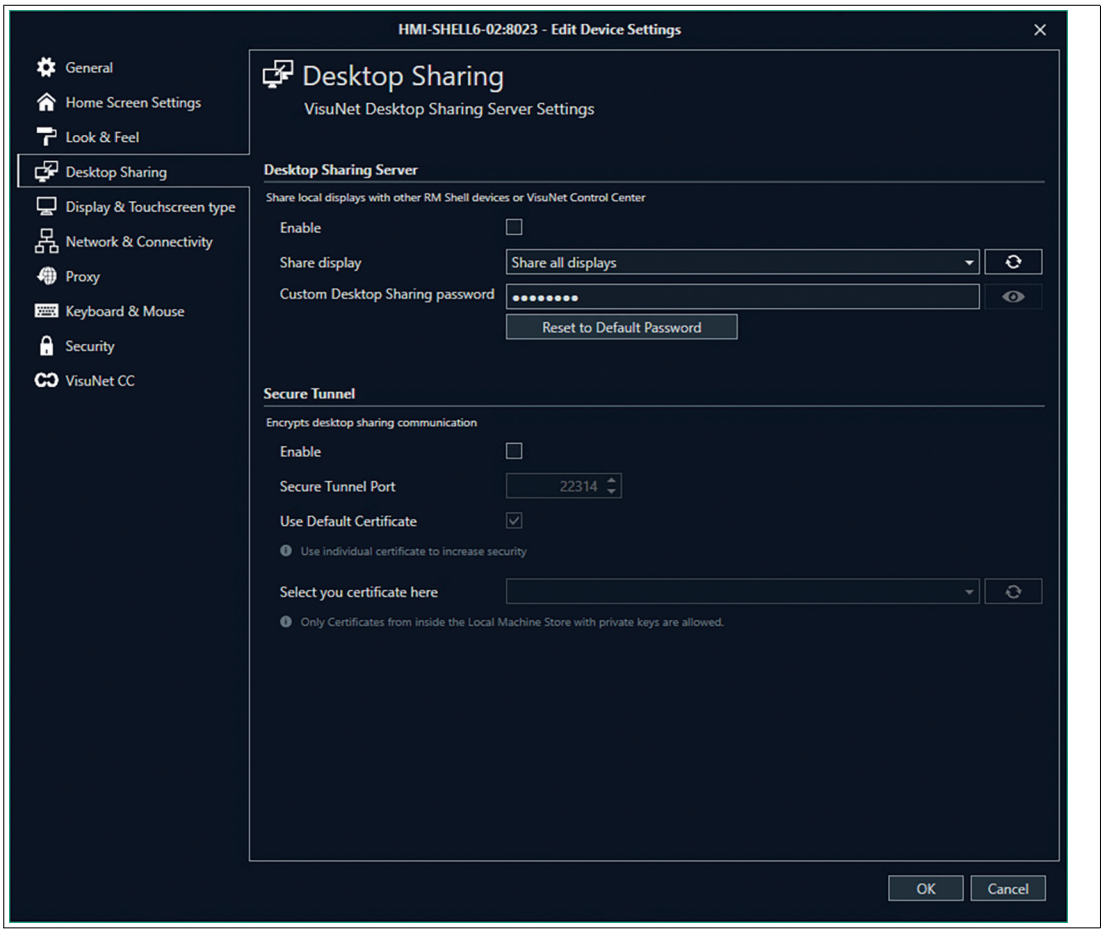


Figure 7.5

The VisuNet Desktop Sharing Server is per default disabled.

When enabling this function, we highly recommend enabling the Secure Tunnel Service as well to ensure high security connections. It is also recommended to use your own certificate. Be aware that only certificates with private keys are allowed.

Further information on how to set up a connection with an own certificate, see in chapter 5.

Display & Touchscreen Type

- **Smart Screen Saver:** The Smart Screen Saver is a screensaver which prevents permanent image retention or image sticking on LC displays while presenting the process picture at the same time. Process pictures stay visible, and you still have direct access to all important process information. The Smart Screen Saver is per default disabled. Set the idle time to activate Previs.
  With the additional PRO license you are able to set a PIN so only authorized personal can unlock the device.

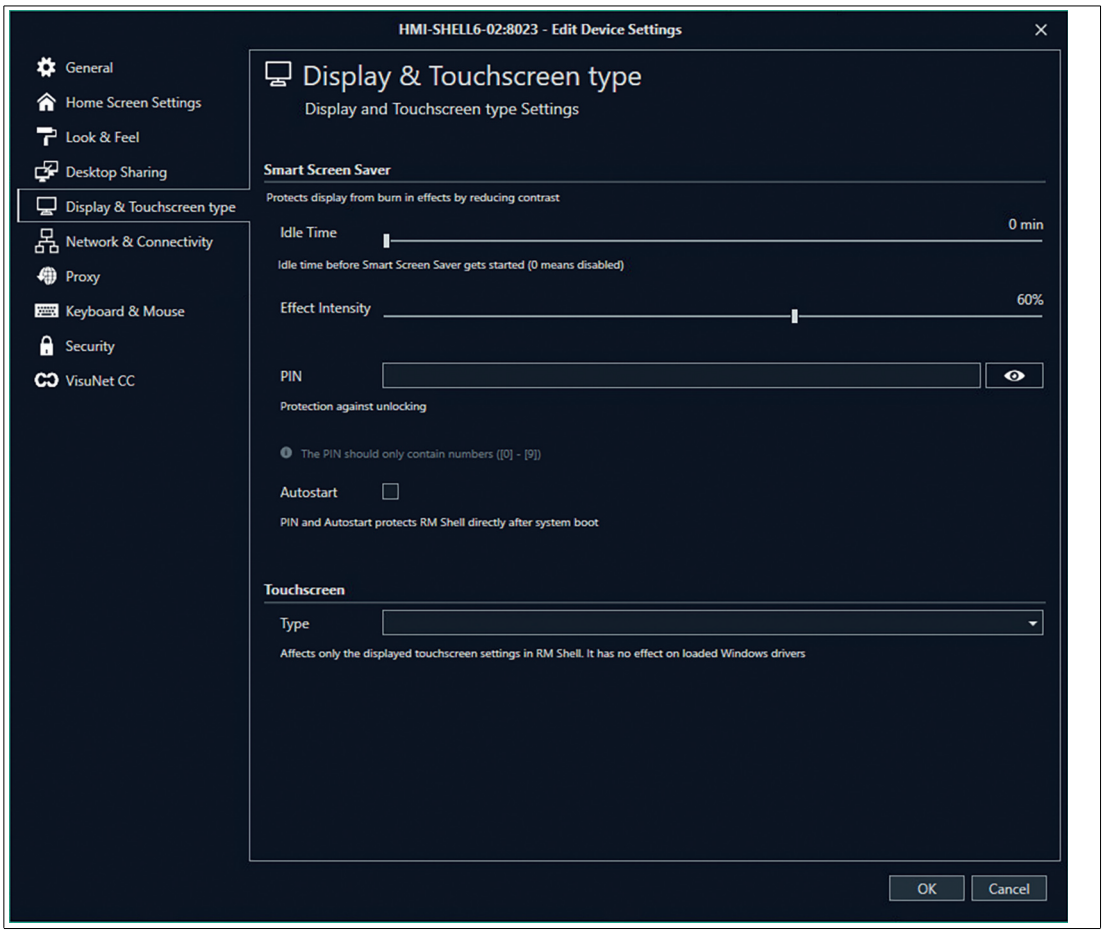


Figure 7.6

- **Touch:** Depending on the installed Image you can choose the implemented touch screen. Touchscreens are per default enabled and can be disabled in this menu

Network & Connectivity

- **Computer Description:** Here the name of the device can be changed. When the device is restarted, the new name is adapted.Remember to upload the new device settings to your Shell device and restart it. If the Communication Address or IP address of the RM / BTC Shell Device and the VisuNet Control Center are not identical, the connection fails.

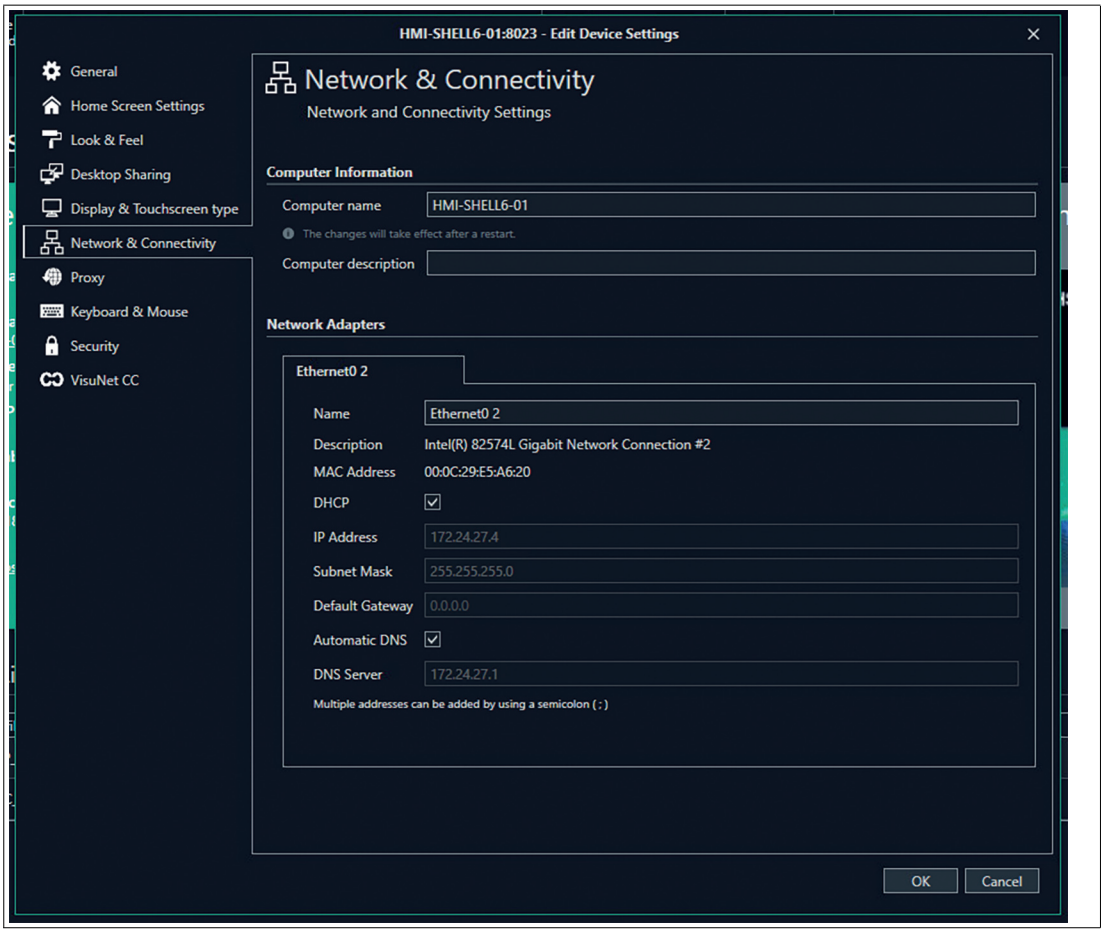


Figure 7.7

Proxy

Proxy settings are identical with the proxy settings of Windows®.

Keyboard & Mouse

Set your required keyboard and mouse settings here.

Security

This menu allows to set the keyboard filter, firewall and USB Storage Devices Security Settings.

VisuNet CC

Note

Communication Certificate: Use your own certificate for communication between VisuNet RM Shell 6 and Control Center 6.

Open / Close, TCP Send / Receive, MEX Send / Receive Timeout

If the speed of your device or Network is low, you might must adjust the time-out settings of the VisuNet CC by extending them to prevent errors and timeouts.

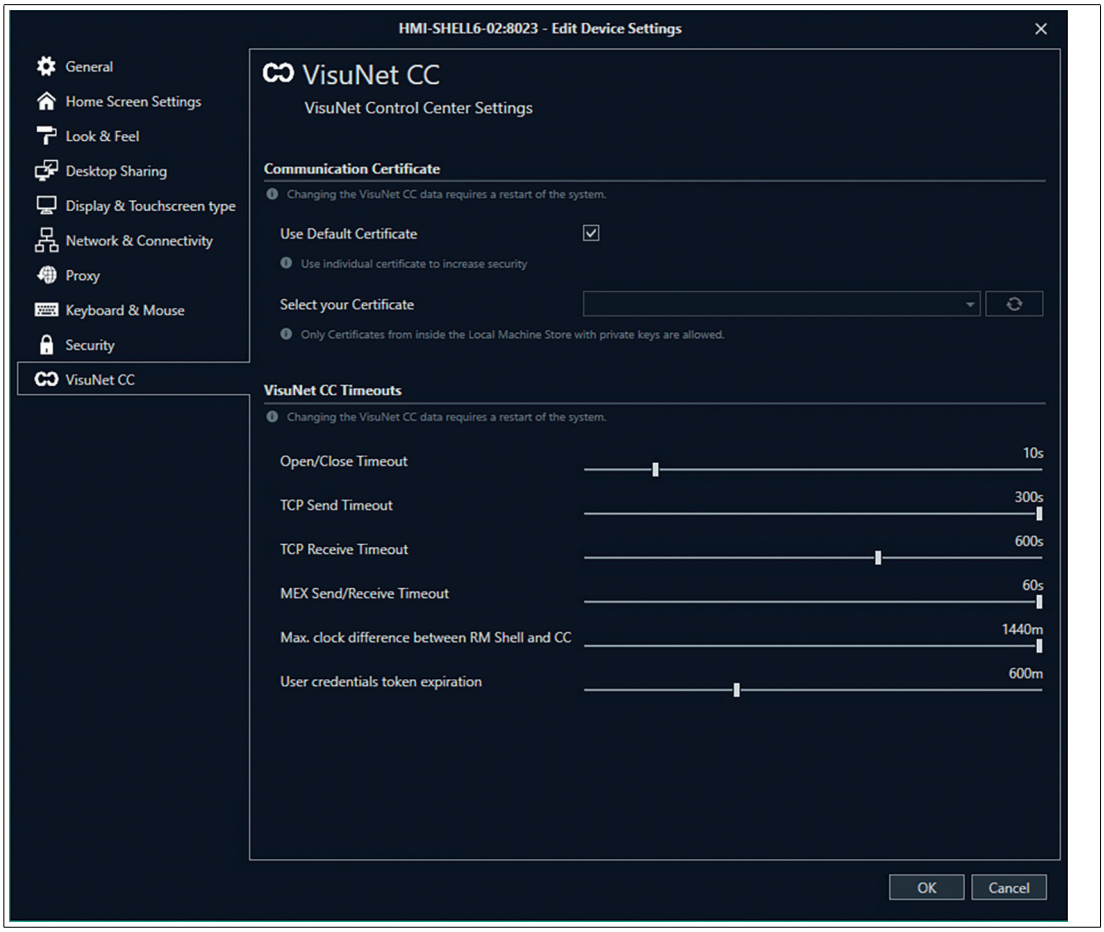


Figure 7.8

7.2 Device Settings (Ribbon)



Figure 7.9

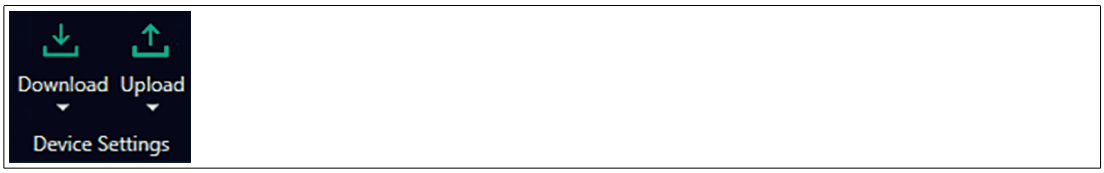


Figure 7.10

Either use direct function for one device or chose the Firmware Wizard to get guided through the process and use the function for multiple devices with the dropdown menu. Depending on which device either the RM / BTC or the VisuNet Control Center you edited your settings you can either download or upload them to synchronize your local data. Please note that the downloaded or uploaded data always overwrites the existing data.

7.3 Device Management



Figure 7.11

Update Firmware

Use the Firmware Update Wizard to get guided through the update process and update an individual or multiple devices.

To get further information on the Wizard, see chapter 6.4.

Communication Address

Decide if your Device Name should be the same as your communication address / IP address. You can name your device any name in VisuNet CC. The device name will not be uploaded to the RM Shell but only be saved locally in your project.

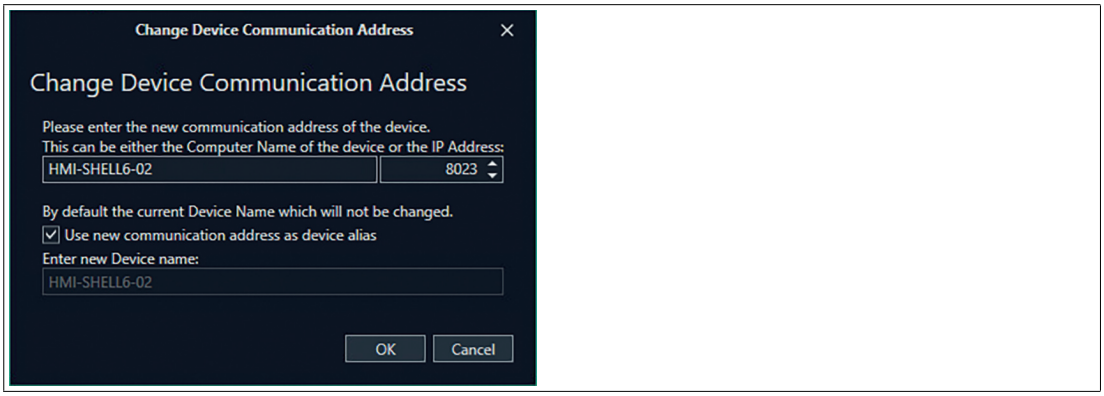


Figure 7.12

The Device Name will appear in the navigation menu as well as in the device main screen.

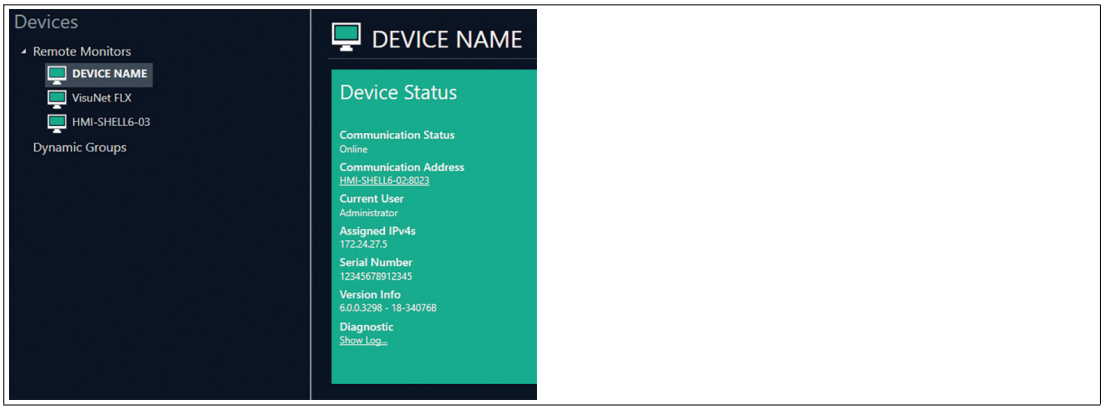


Figure 7.13

Import SSL Certificate

Send an SSL Certificate (e.g. to access an encrypted website) to an RM. Create your own certificate with a private key and import it here. You can choose your Store as well as the location the certificate is stored at.

- Current User (only available for VisuNet RM Shell 5): Cannot be seen or used by other users
- Local Machine: Any user can access and select it

Auto Logon

Since VisuNet RM Shell 6, with auto Logon feature a user can be automaticaly logged into the RM Shell device on startup of the device.

Change Windows Password

Since VisuNet RM Shell 6, you can change the password of a windows user on the device. For the default RM Shell 6 users use Domain ". \".

Clone Wizard

Use the Clone Wizard to clone configurations from one device to multiple other devices. Please note that the cloning and target devices need to be compatible in terms of the Firmware Version. To clone e.g. Profiles from a device with Shell 5 to a target device with Shell 6 an Upgrade needs to be performed in advance.

1. Make sure that all devices are updated to the latest Version and are online.

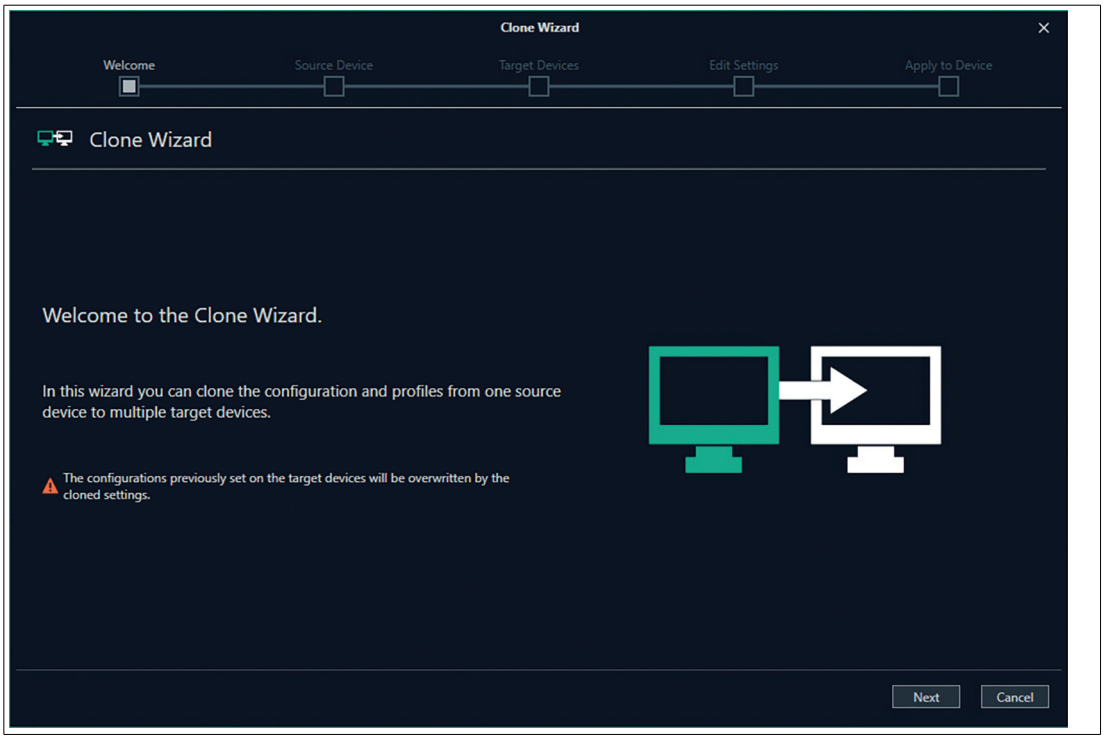


Figure 7.14 Clone Wizard - Welcome

2. Click "Next".

3. Click "Next".

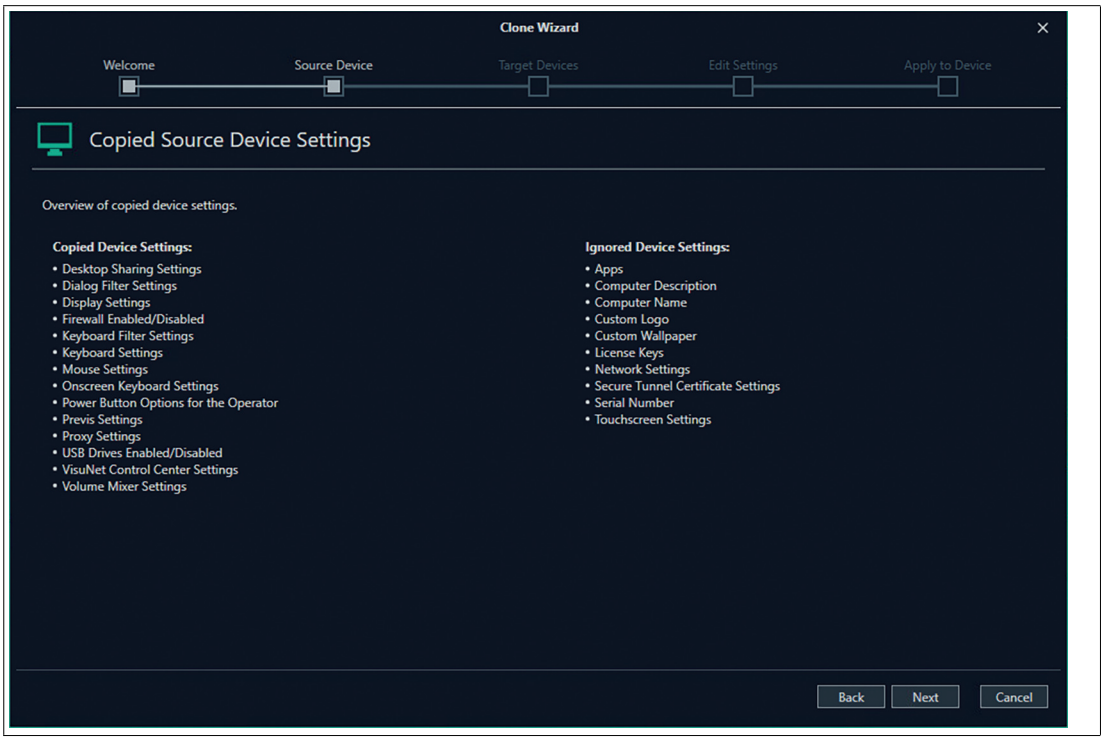


Figure 7.15 Clone Wizard - Source Device - Copied Source Device Settings

4. The Copied Source Device Settings are only an overview. The assignment cannot be adjusted.

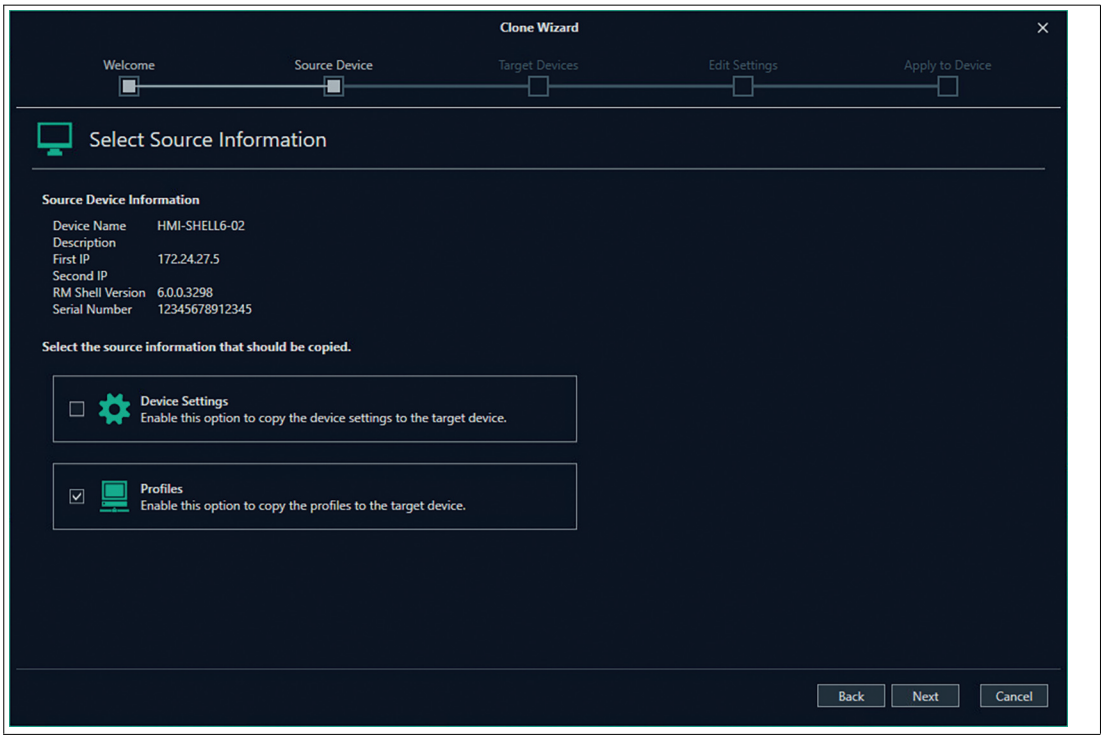


Figure 7.16 Clone Wizard - Source Device - Select Source Information

5. Choose the source of information you like to copy.

6. Both options Device Settings and Profiles are selected by default. Remove the check mark if the source is not to be selected.

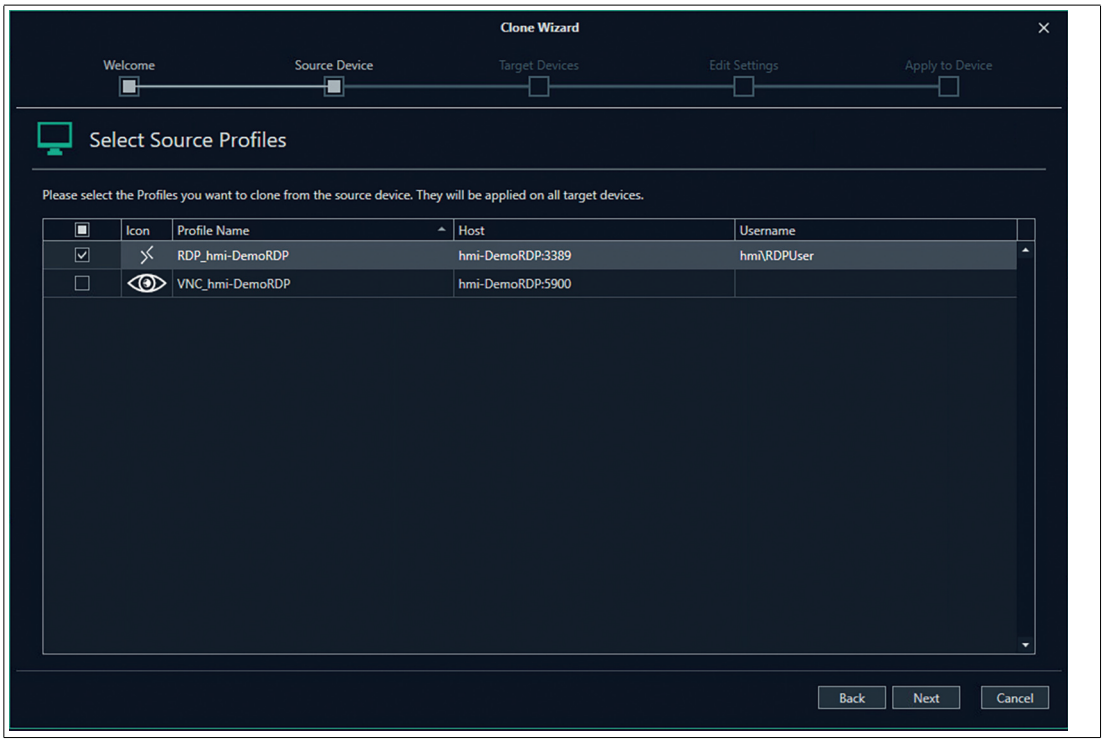


Figure 7.17 Clone Wizard - Source Device - Select Source Profiles

7. Choose the profiles that should be cloned to the target devices.

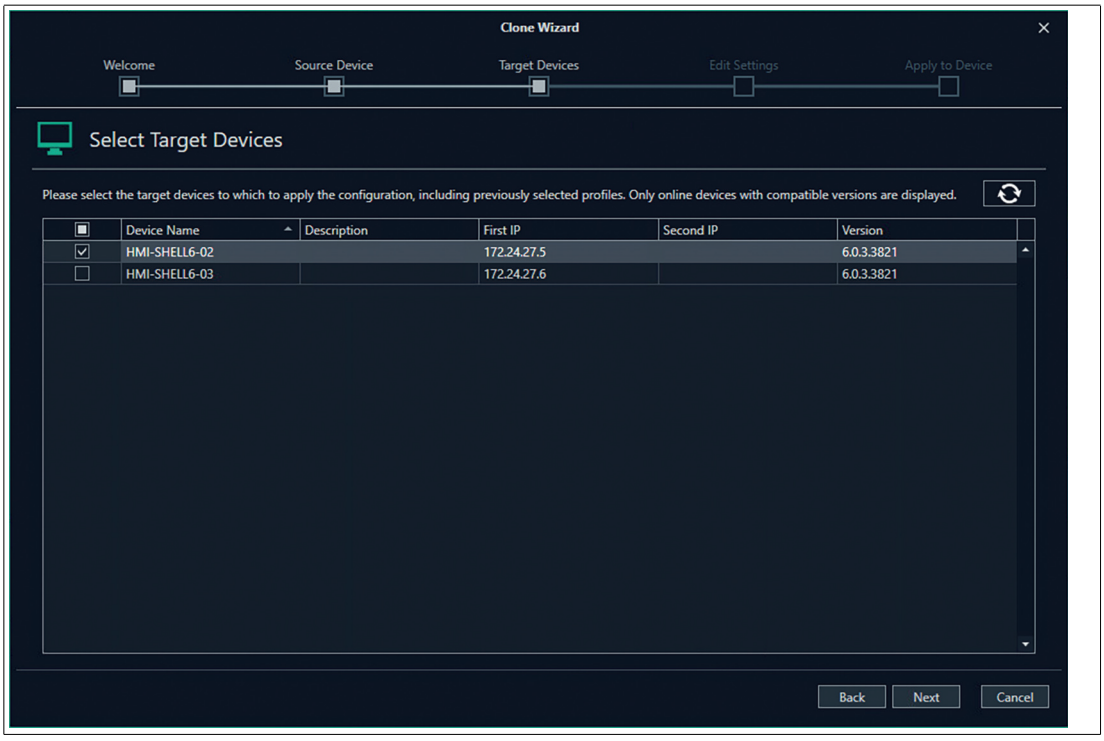


Figure 7.18 Clone Wizard - Target Devices

8. Choose target devices you want to apply the configuration.

9. For RM Shell DRDC and RM Shell PRO licenses are required. Make sure that you only copy the profiles you also have additional licenses for the target devices as well.

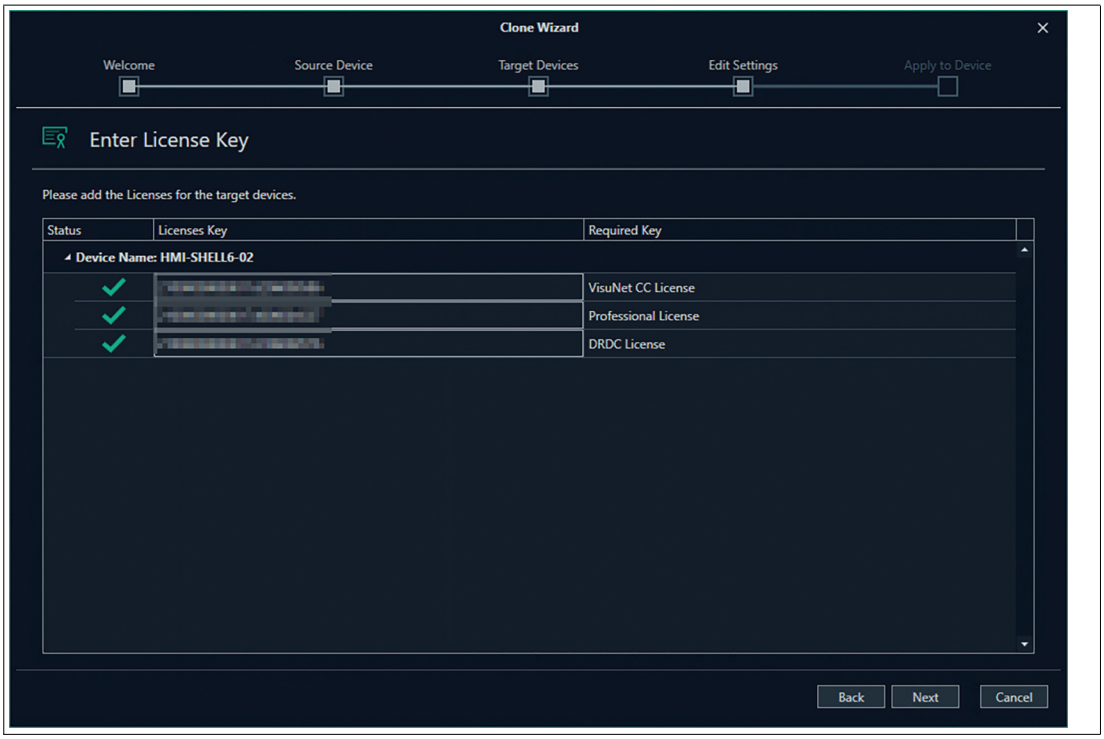


Figure 7.19 Clone Wizard - Edit Settings - Enter License Key

↳ If you add the profiles via VisuNet CC for the first time, you will be asked for the license keys in “Edit Settings”.

↳ If you already have licenses for the target devices the licenses Keys will be transferred and filled in already.

↳ If there is an error within in typed in license number the status will be marked with a red cross. Use the mouse to hover over the Red Cross and get further information what error occurred.

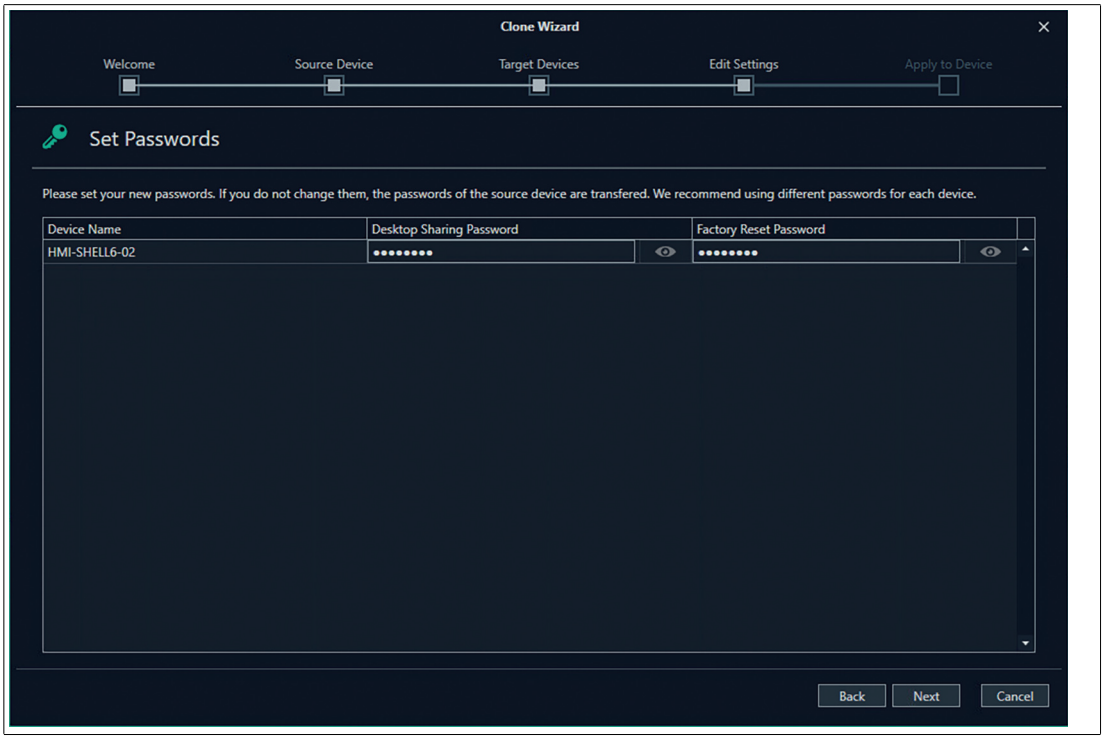


Figure 7.20 Clone Wizard - Edit Settings - Set Passwords

↳ If the source device is provided with passwords for the Administrator, Operator, Desktop Sharing and Factory Reset, the list would be prefilled. If you do not set new passwords the same passwords will be transferred.

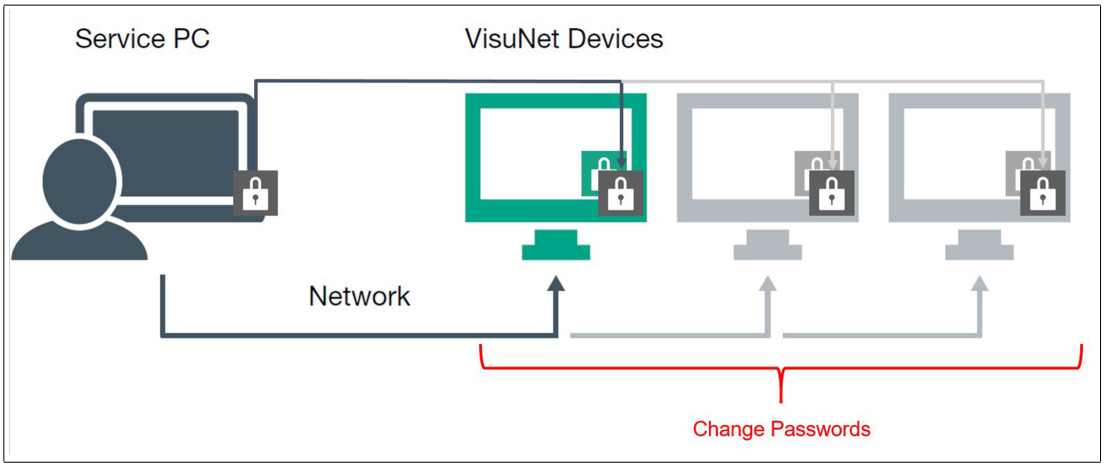


Figure 7.21

↳ We do not recommend to use the same password.

10. Change the profiles of each target device individually.

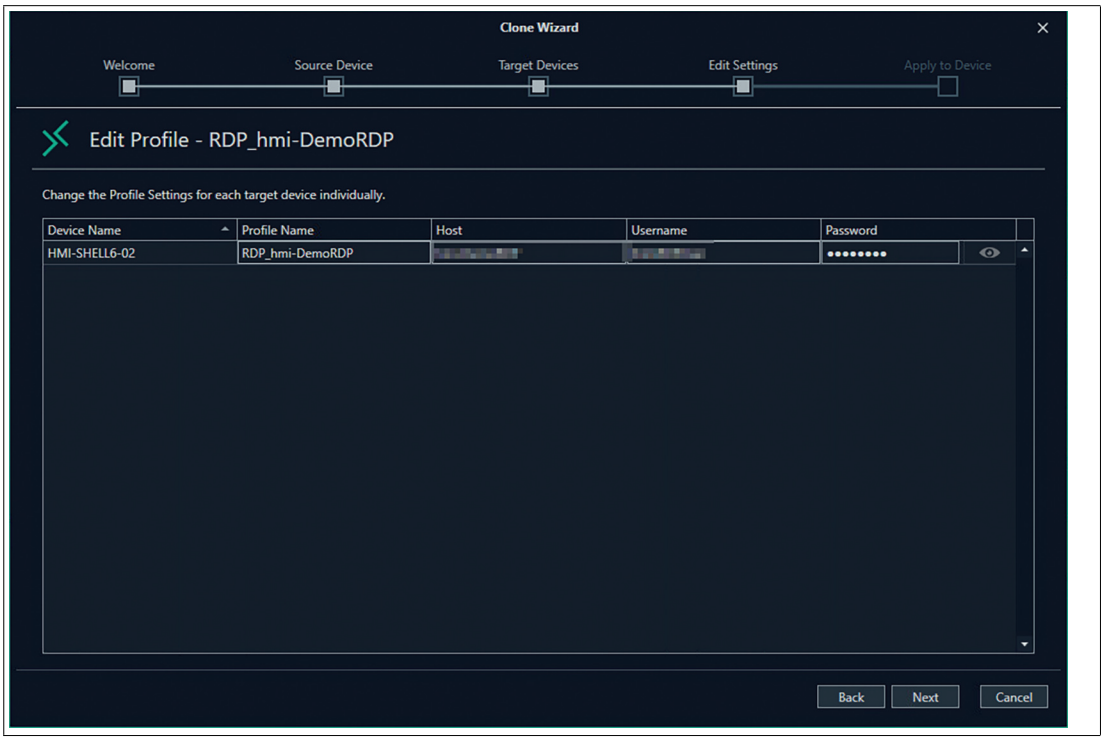


Figure 7.22 Clone Wizard - Edit Settings - Edit Profile - RDP

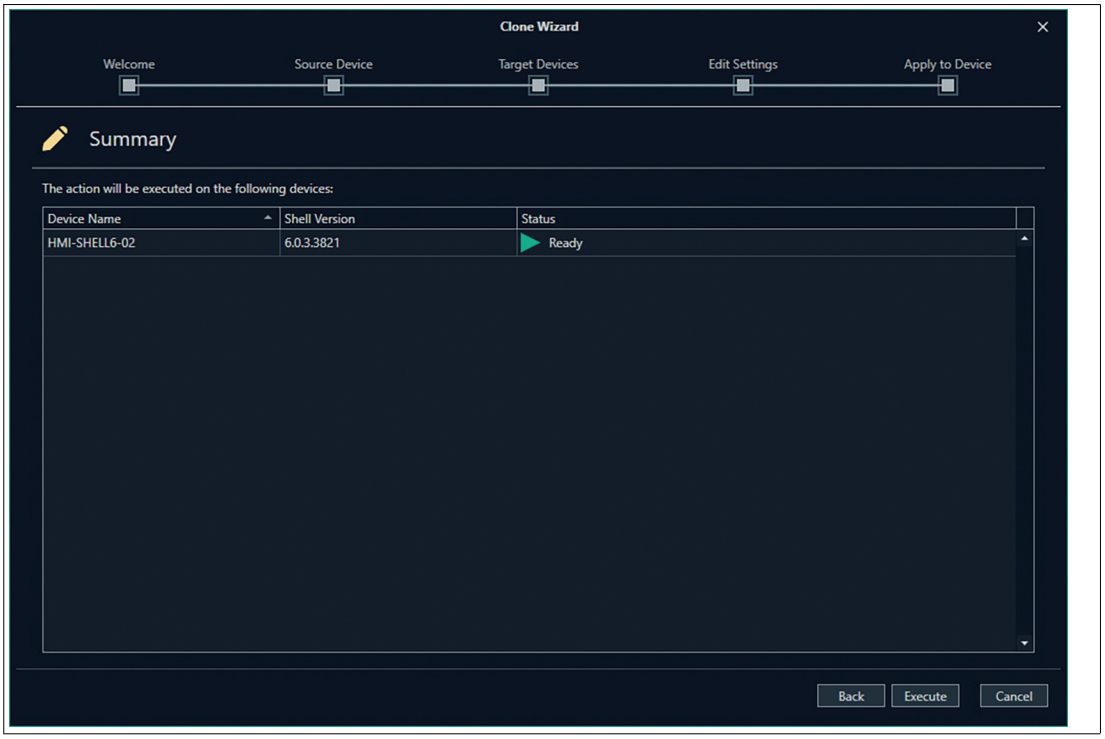


Figure 7.23 Clone Wizard - Apply to Device - Summary

↳ The wizard guides you through all the different profiles of the cloning device.

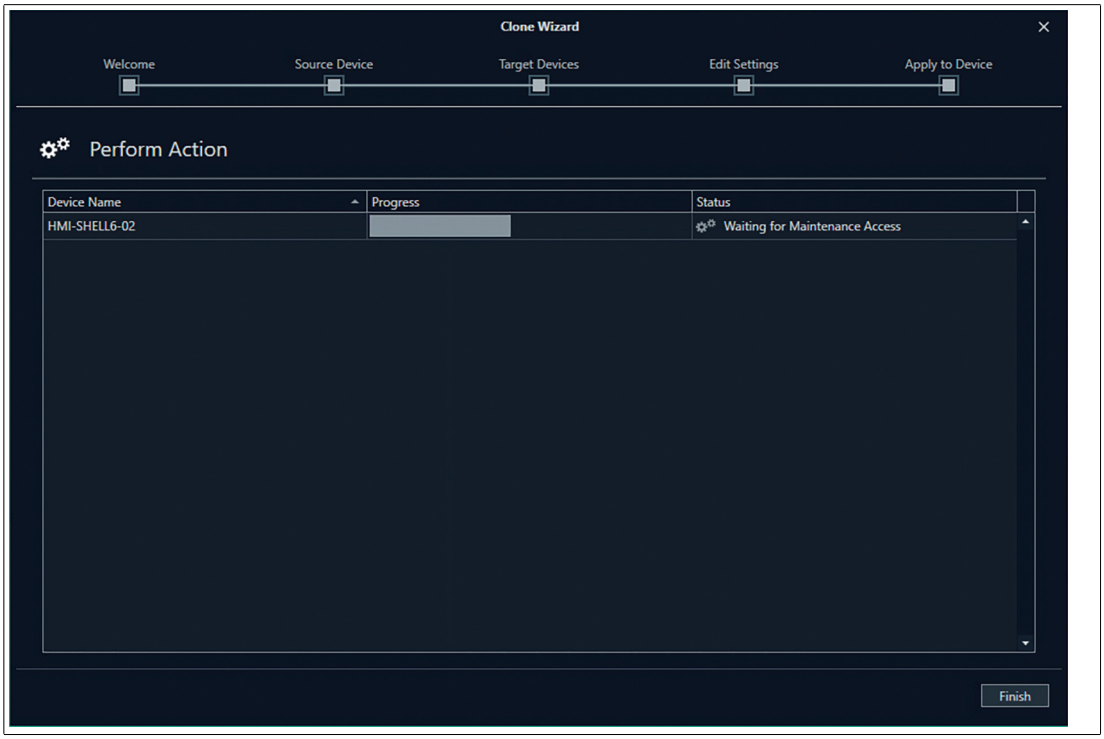


Figure 7.24 Clone Wizard - Apply to Device - Perform Action

11. When the Status changes to "Success", click finish to complete the cloning process.

7.4 Device Commands

Shutdown and Restart Device

1. Choose in the drop-down menu to shutdown/restart one device directly or choose the Firmware Wizard to get guided through the process and Shutdown/restart multiple devices.

Caution!

It is not possible to boot devices via VisuNet CC.

2. Devices have two different restart modes. You can restart with write filter enabled and restart with write filter disabled.

Note

Before the RM/BTC is shut down, the local operator is prompted and asked if the shutdown process should be stopped. When restarting the device, you can choose whether the Write Filter should be protected or not.

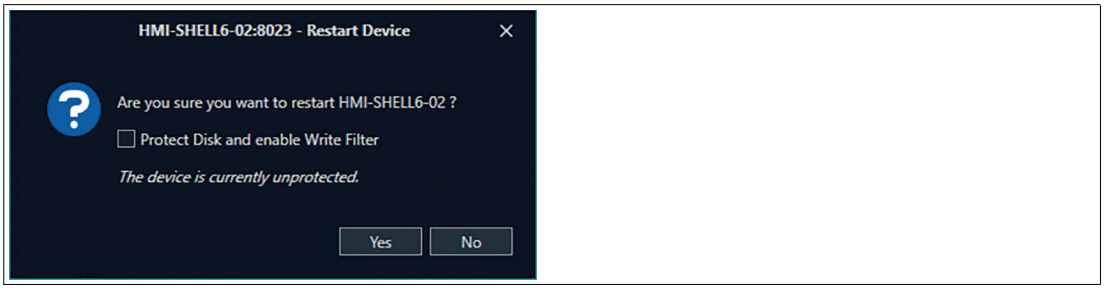


Figure 7.25

In the Device Status you can check whether your device is protected or unprotected.

Besides the control elements of the ribbon bar you can also restart the device using the shortcut on the upper right corner of the main screen in the device structure.



Figure 7.26

Session Shadowing

1. Connect to an RM/BTC by clicking the icon or the minimized live view of the shown RM/BTC screen and share its current screen. The function also allows remote control of an RM/BTC.

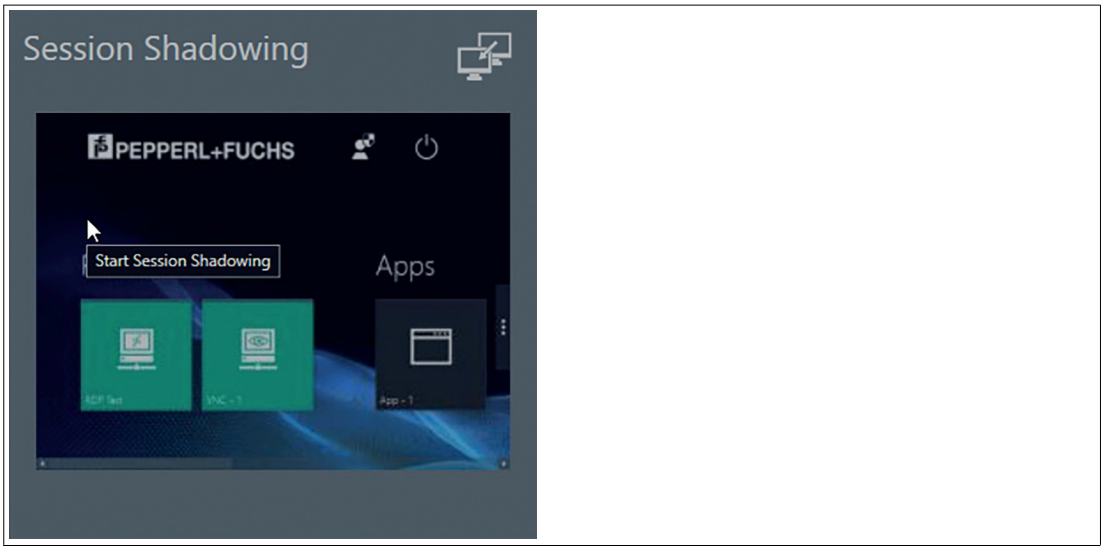


Figure 7.27 Shadowing the Session of an RM user

↳ The session shadowing tile shows a minimized live view of the RMs/BTCs current screen. This allows the VisuNet CC user to get an overview of the RMs/BTCs current status.

2. For a detailed view of the RMs/BTCs screen, click the tile. This opens a new window that allows the user to shadow the RM/BTC or remotely control the system.

↳ The RM/BTC screen is displayed in the session shadowing window. The screen of the RM/BTC is scaled to the current size of the session shadowing window. Using the “Enable Fullscreen” function, the window can be maximized to show the native resolution of the RM/BTC screen in the VisuNet CC window.

3. While shadowing a session, you can click the Task Switcher  in the upper-left corner of the screen to open the RM Shell Task Switcher. This tool allows you to change open protocol connections on the monitored device.

Note

The desktop sharing function must be enabled in the RM Shell to use this feature.

Tip

If you need to take control of the mouse, click the “control” item in the Session Shadowing Mode.

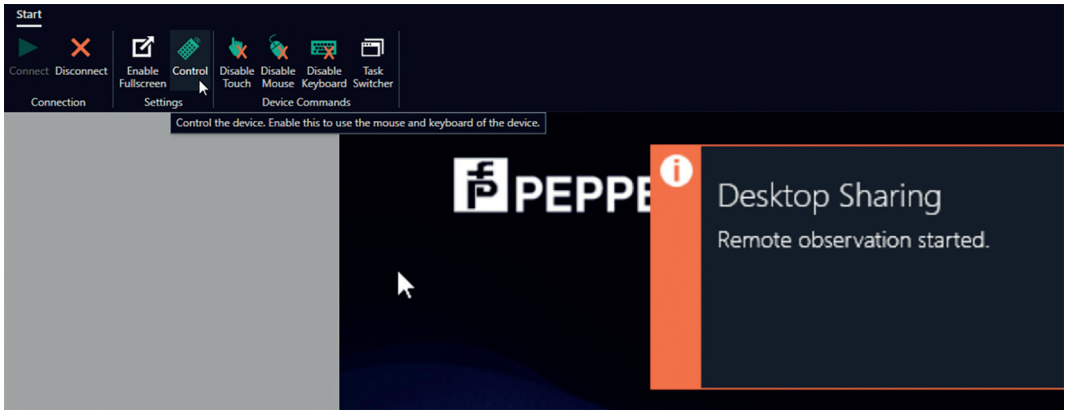


Figure 7.28

Disable Touch

Disable the touchscreen of an RM, e.g., during a washdown.

Note

This device command has an immediate effect on the RM.

Disable Mouse

Disable the mouse of an RM/BTC.

Note

This device command has an immediate effect on the RM/BTC.

If the mouse is disabled on an RM/BTC, the mouse also cannot be used via session shadowing.

Disable Keyboard

Disable the keyboard of an RM.

Note

This device command has an immediate effect on the RM.

If the keyboard is disabled on an RM, the keyboard also cannot be used via session shadowing.

Maintenance Mode

Whenever data is sent from VisuNet CC to an RM/BTC, the RM/BTC asks the local operator if the RM/BTC is allowed to enter maintenance mode. Maintenance mode is a semaphore that establishes an exclusive communication link between VisuNet CC and the RM/BTC. When maintenance mode is active, no local changes can be performed on the RM/BTC – either by a local operator or by another Control Center.

This mode is used to avoid accidental reconfiguration of an RM/BTC, for instance, when a local operator performs a critical task such as entering a recipe. If an RM/BTC is triggered by VisuNet CC to enter maintenance mode, the local operator is prompted and asked for permission. If the operator accepts, VisuNet CC gains exclusive access to the RM/BTC and can upload the data. After the data is uploaded, VisuNet CC automatically leaves maintenance mode and releases the lock.

Note

If no local operator is working on the RM, a time-out triggers the change into maintenance mode automatically.

VisuNet CC allows the administrator to force entering maintenance mode, even when a local operator declines the remote access.

Secure Tunnel Warnings and how to fix them

Warnings	Fix
The certificate chain is broken. Import a trusted root certificate.	Import the root certificate to complete the trust chain. (Find further information in Chapter 5 “How-To”)
The certificate contains another common name as the server name. Check your server settings.	Check if the common name of the certificate matches with the host name of the VisuNet RM Shell device.
The certificate is not available. Check your server settings.	Check in the device settings if the selected certificate has been uploaded to the VisuNet RM Shell device.
You are using the default certificate. Use your own to increase the security.	Refer to “Build up a connection with your own certificate via Session Shadowing to increase the security level” in the How-To-Chapter.
Enable the Secure Tunnel on the device to establish an encrypted connection.	The secure tunnel is available, but not activated. We recommend to activate the secure tunnel for an encrypted connection.

Cleanup Disk Wizard

Use the Cleanup Disk Wizard to clean up the disk of one or multiple devices. Cleaning out your device frees up your drive space and helps it run better by deleting temporary files and reduce the size of the WinSxS folder.

Note

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

It is recommended to increase the max. simultaneous actions so that the Cleanup process of multiple devices can run simultaneously. (For further information see chapter 6.4).

Cleanup Disk Wizard

1. Make sure that all devices are updated to the latest Version and are online. Choose the devices whose disk should be cleaned up.

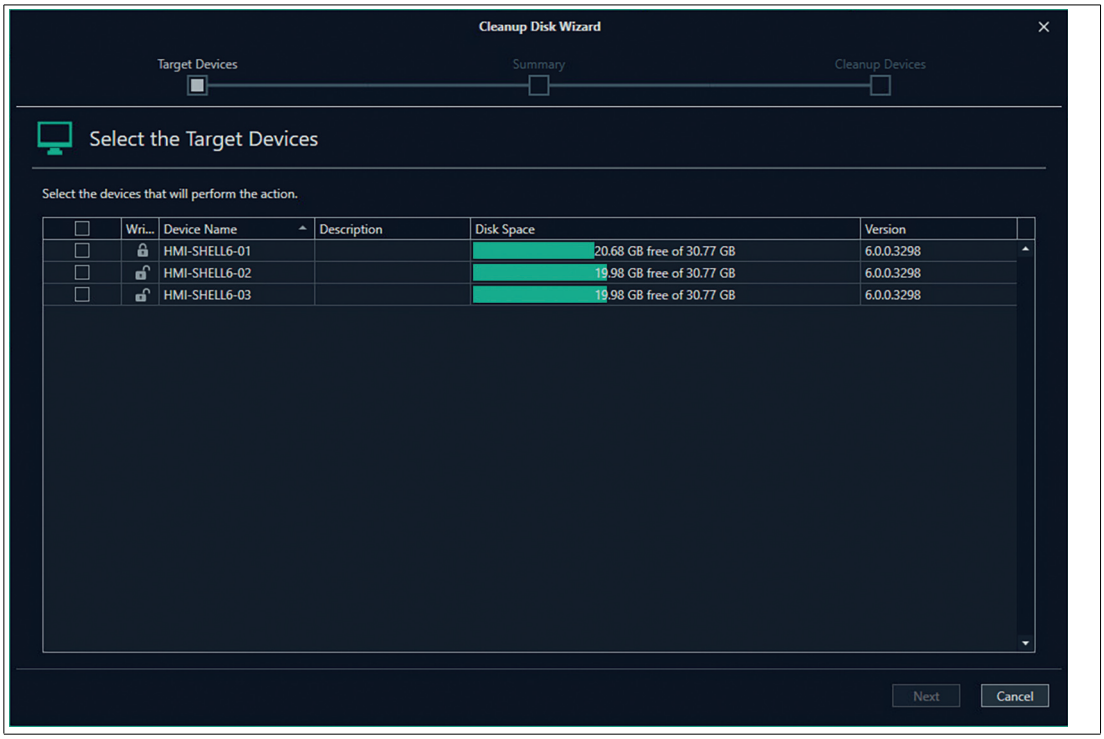


Figure 7.29

From VisuNet RM Shell version 5.5.0 on the available disk space is visualized.

2. Check again the selected devices then click "execute" to perform the Cleanup Process.

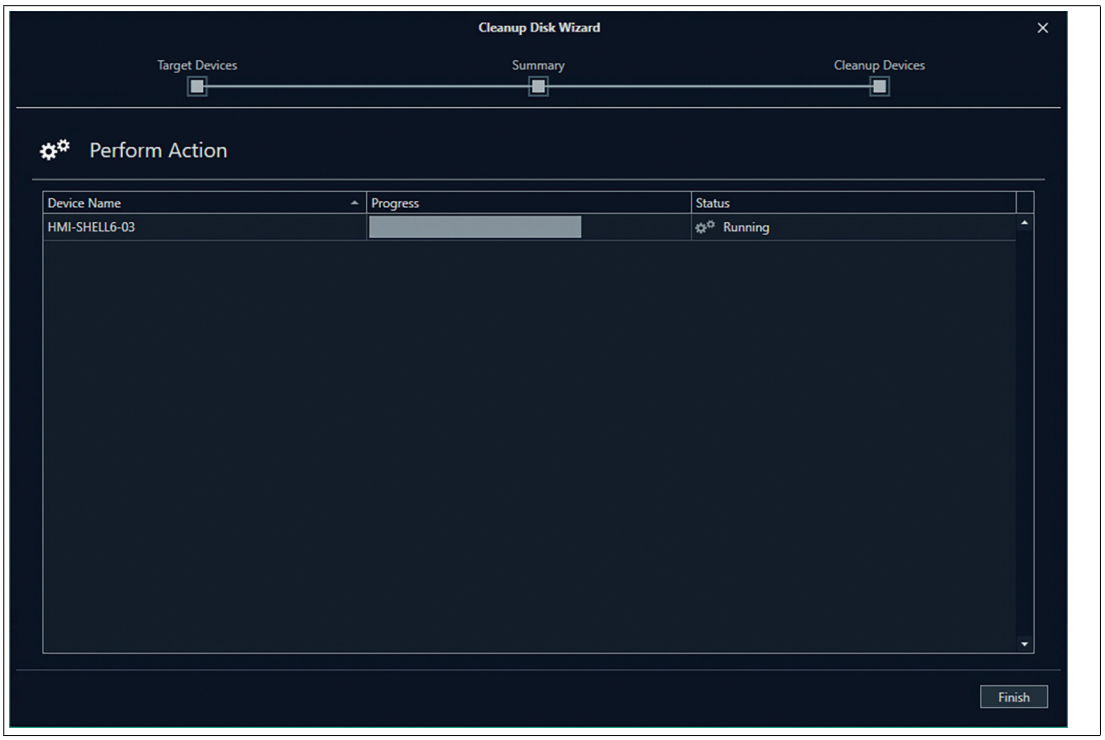


Figure 7.30

3. The Cleanup process might take several hours. During that time the device can be operated but might response slowly.

4. Click "Finish". The Cleanup process runs in the background. You can follow the progress in the Action History list. When every device Status is set to "Success", the performed action is completed. The settings of the simultaneous actions can be reset again.

Note

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

Theme Wizard

1. The Theme Wizard supports you in customizing one or multiple wallpapers and logos of your devices.

Note

This feature requires a PRO license!

Procedure

1. Select your target device(s).

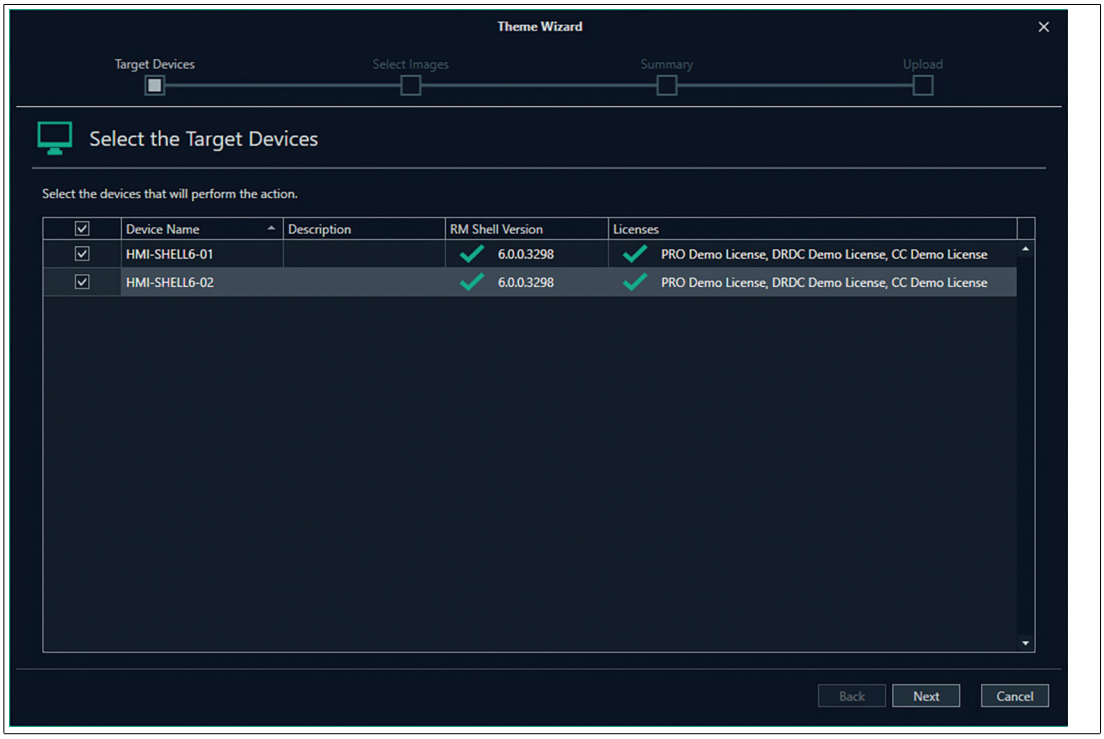


Figure 7.31

2. Use the arrows to preview the aspect ratio and solution for your devices.

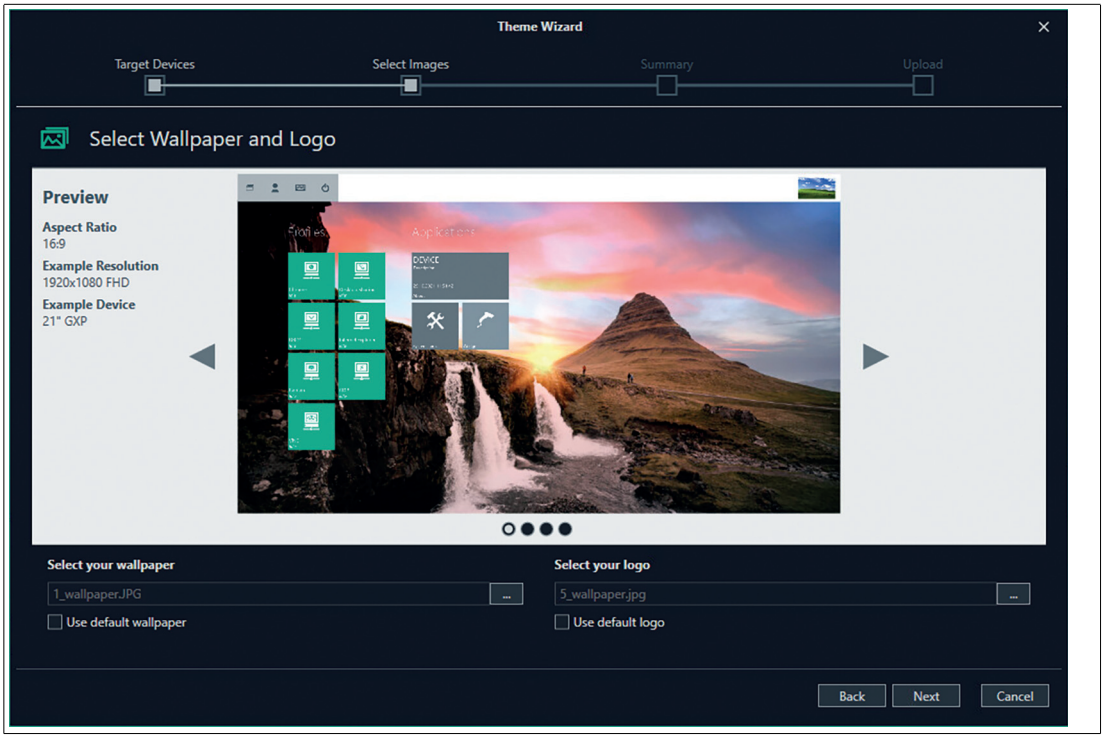


Figure 7.32

2025-07

PEPPERL+FUCHS

3. By clicking "execute", your device(s) is synchronized with the new wallpaper and/or logo.

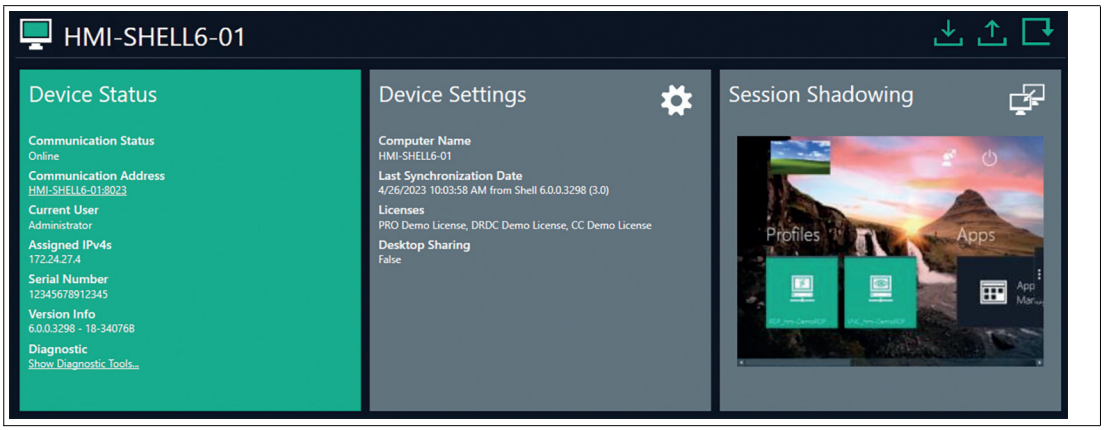


Figure 7.33

RFID Wizard

Choose your required configuration and flash it to your device.

1. Standard Configuration

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

Note

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

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

2. Custom Configuration

1. If the standard configurations are not suitable for your use-case, you can build your own configuration and import it in the VisuNet RM Shell. Either use the additional "Configuration Tool" below which has integrated configuration tools from ELATEC or redirect directly to the ELATEC website and use the tools on their website. Please refer to the ELATEC website -> TWN4 Dev-Pack Overview

7.5 Device Backup

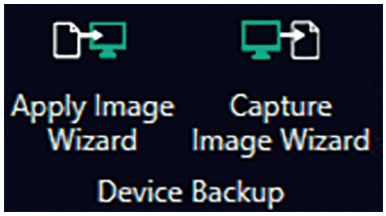


Figure 7.34

Apply Image Wizard

Use the Apply Image wizard to apply multiple images to multiple devices.

Images that can be applied to the RM/BTC:

Image Type	Description	Note
1) Pepperl+Fuchs Factory Reset Image	Available for each specific device. The Pepperl+Fuchs default settings will be applied back to your device. With Factory Reset 6.0 and newer the image won't be stored on the device any more. **Caution!** After applying the Pepperl+Fuchs image the setup of the device needs to be performed locally! The RM Shell first start wizard will guide you through the most important initial configuration steps. Please refer to the First Start Wizard Chapter in the RM Shell Manual for further information.	Get in contact with your local sales support
2) Backup Image	Own captured Backup Image, which can only be applied on the same device with the identical serial number. The backup image can be used to restore a specific state of a device. **Note:** VisuNet CC might not be able to find the device when changes of the computer name or the Network settings have been done after capturing the image.	Has to be captured by the customer in the RM Shell Factory Reset or via VisuNet CC - Device Backup in advance.
3) Clone Image	Own captured Clone Image, which can be applied on devices with the same hardware/same device type e.g. BTC12. Within the clone image all applications as well as 3rd party applications and the whole operating system is cloned. By applying the cloned image a generic Windows image is created, which resets the name and generates a unique ID. **Caution!** The devices on which a clone image is applied to, need to be configured locally. The set up processes can not be performed via VisuNet CC.	Has to be captured by the customer via VisuNet CC - Device Backup in advance.

Follow the steps of the wizard that guides you through the process:

Apply Image Wizard

Note

When applying a Pepperl+Fuchs image or a clone image you need to setup your device locally!

If you want to track the status of the device, VisuNet CC must not be closed during the Apply Image Wizard application.
When closing and restarting VisuNet CC the devices on which the Image is applied to is "offline" and can no longer be detected.

1. Click "Next".

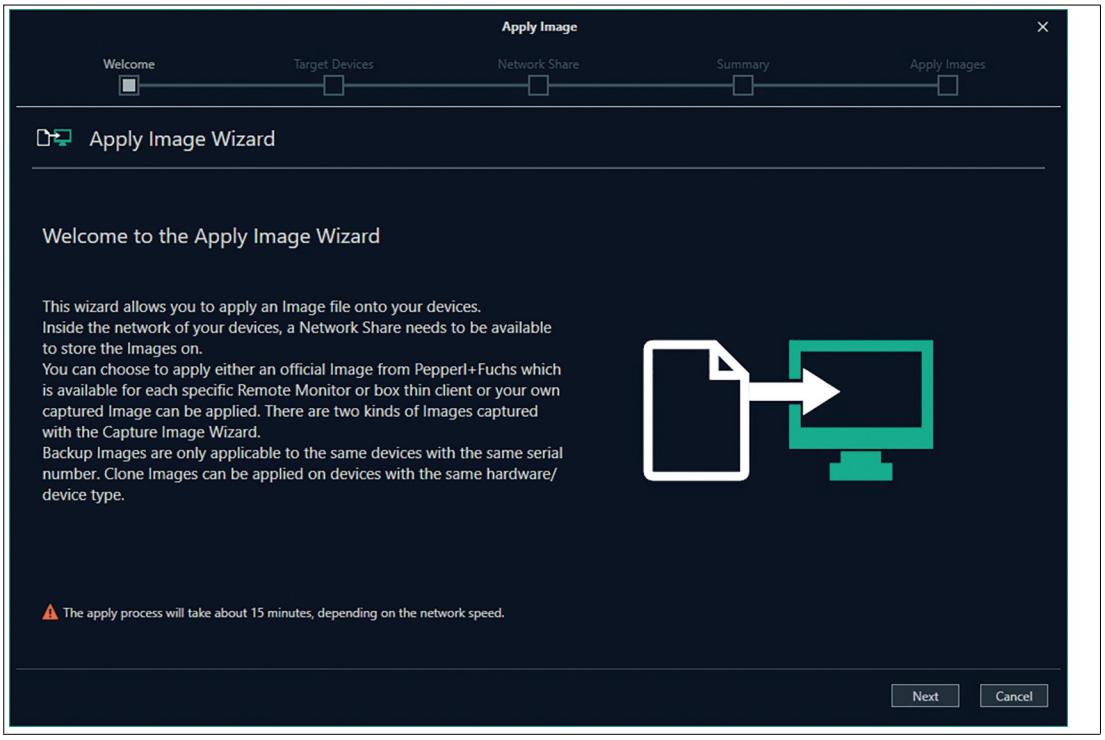


Figure 7.35

2. Click "Next".

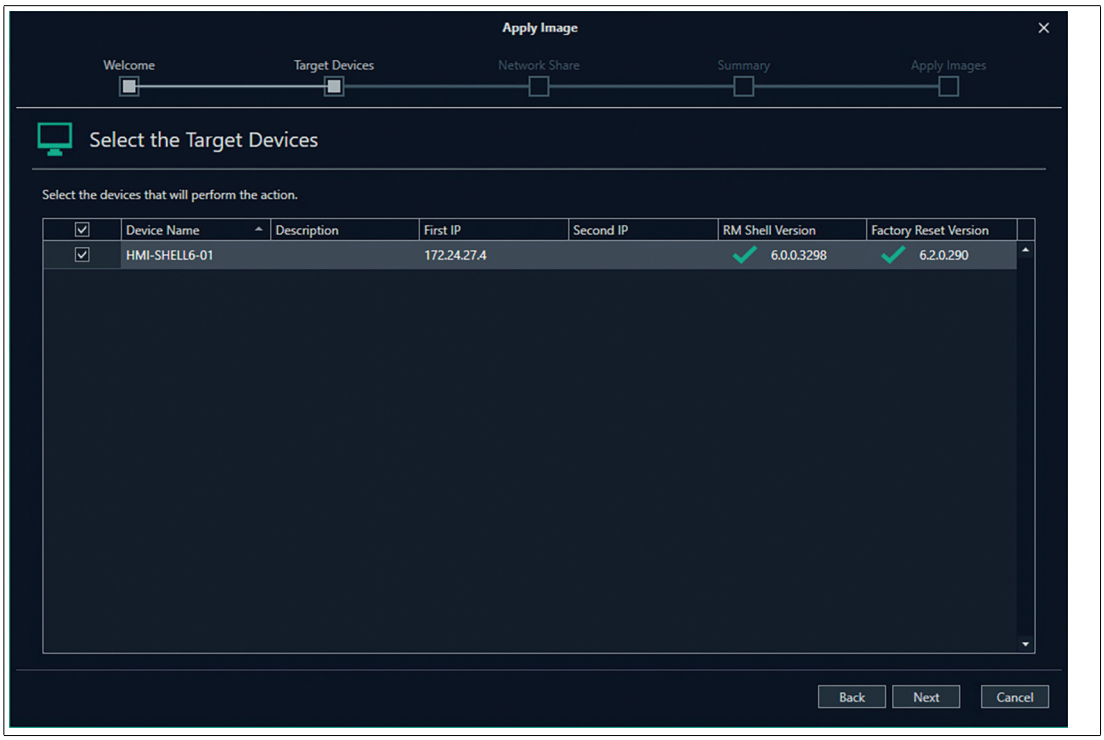


Figure 7.36

3. Select the Network Share which will be used to transfer the image. The Network Share needs to be available in the same network of your devices.

Note

Make sure to select an UNC -path, other paths are not recognized/accepted.

4. Check the connection. If the connection failed, check the server path again. No further procedure is possible. If the connection is successful you can continue the wizard further and click "Next".

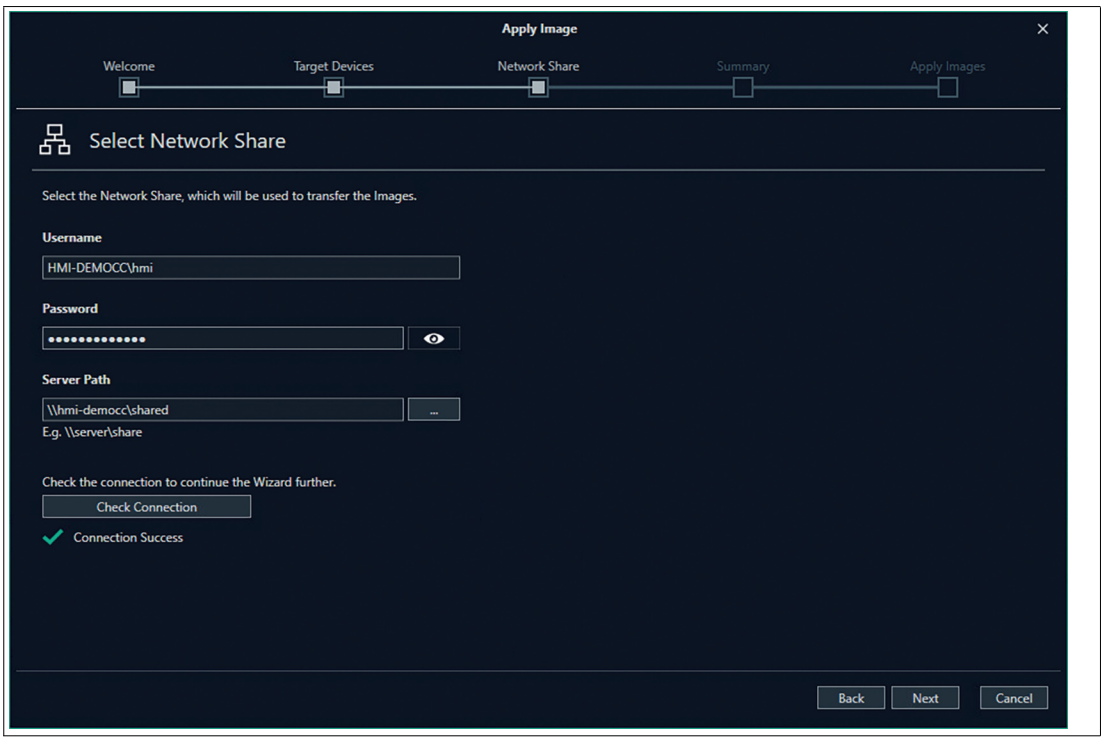


Figure 7.37

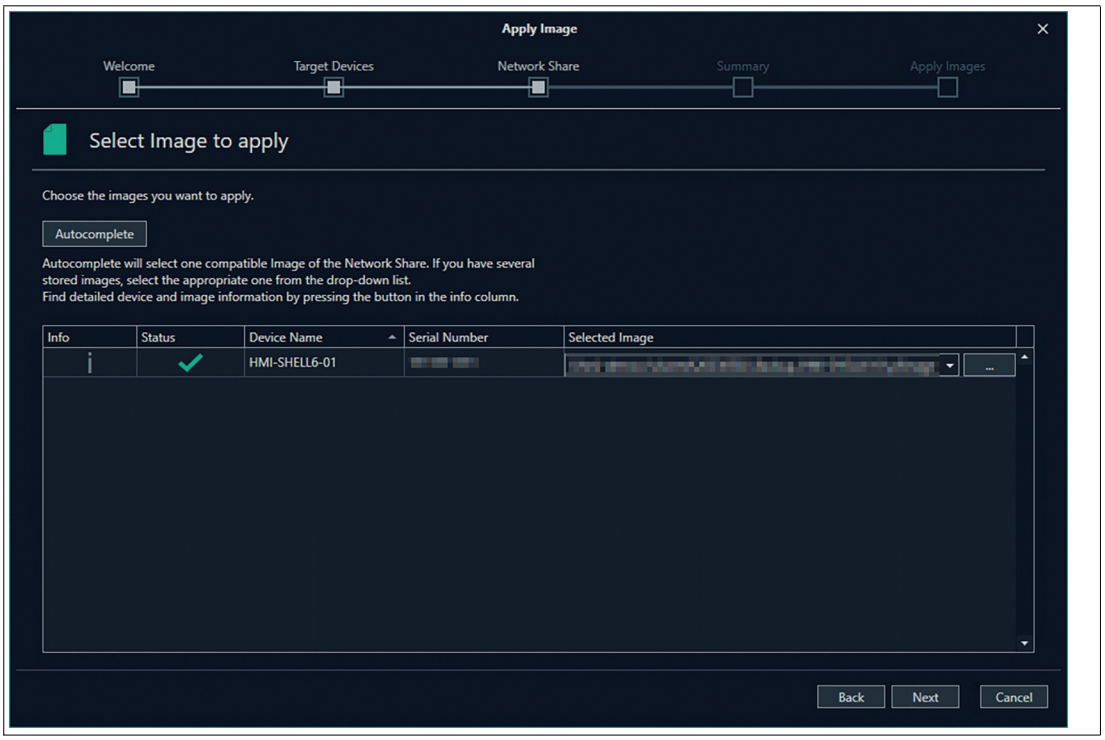


Figure 7.38

5. Use the "Autocomplete" Button to look for all compatible Images within the selected network Share. Use the combo box to select the requested Image if multiple images are stored.

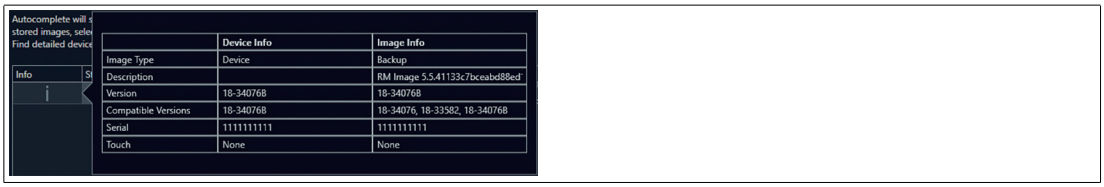


Figure 7.39

6. By clicking  get detailed information about the selected Image and device.
7. After selecting the required image click "Next".
8. Check again the selected settings then click "execute" to perform the apply process.

Note

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

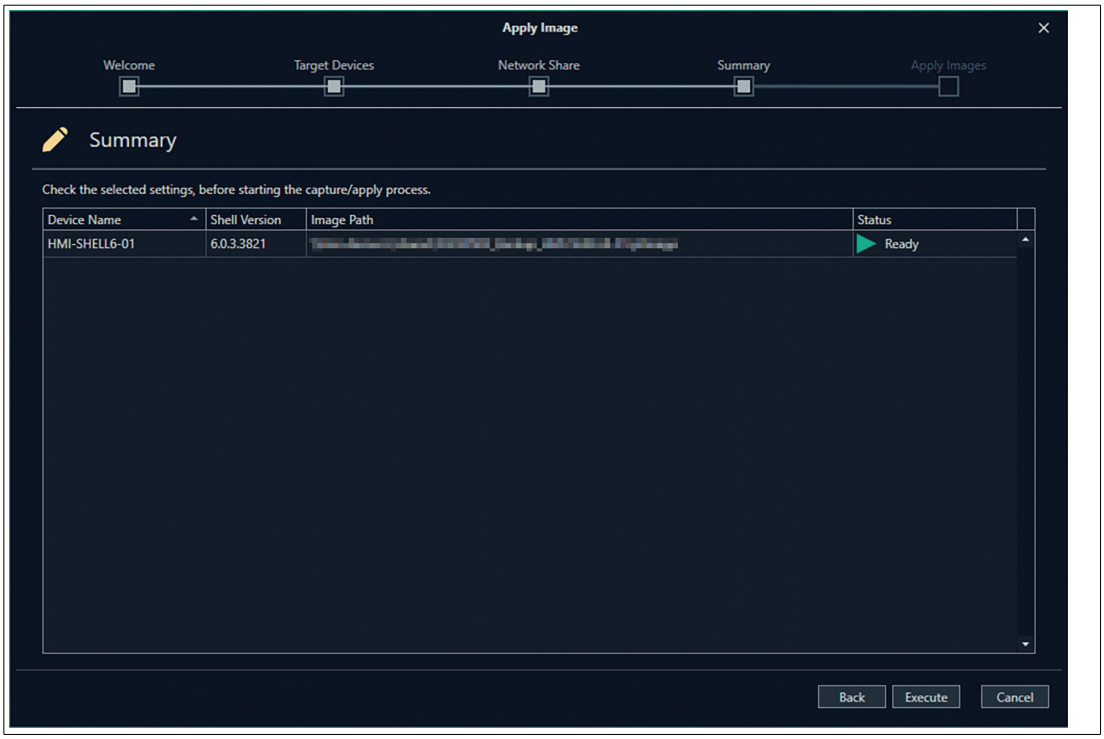


Figure 7.40

9. The apply process will take around 15 minutes. The system will reboot after the image(s) is/are applied.

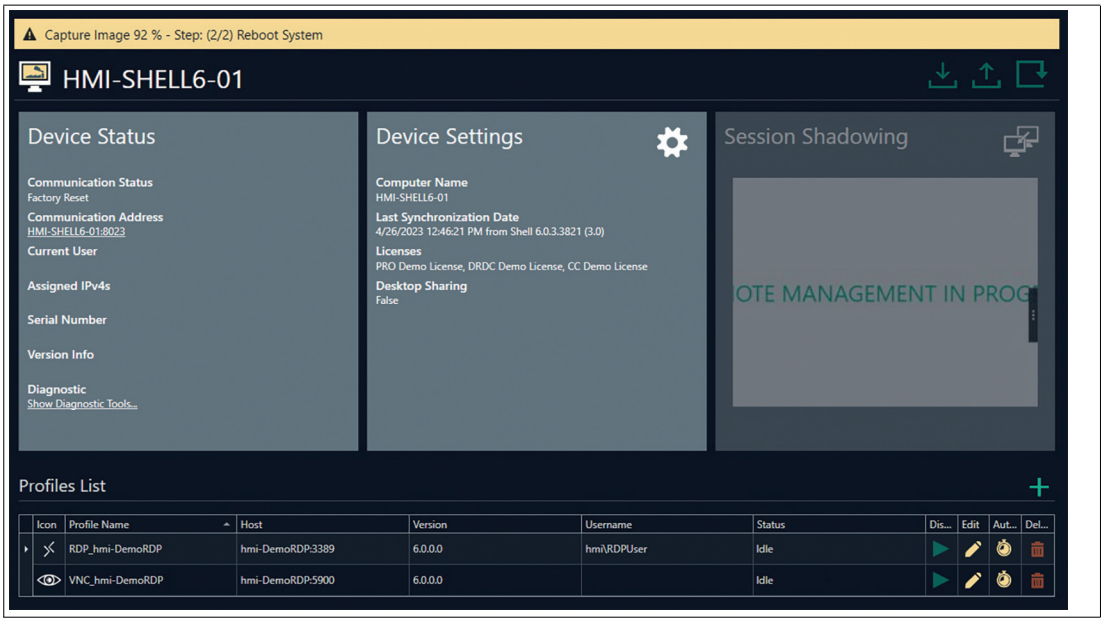


Figure 7.41

Depending on the applied image different further actions are required:

1. Pepperl+Fuchs Factory Reset Image

After the reboot of the device you need to change the following settings **locally.**

- Close the Window "First Start Menu"

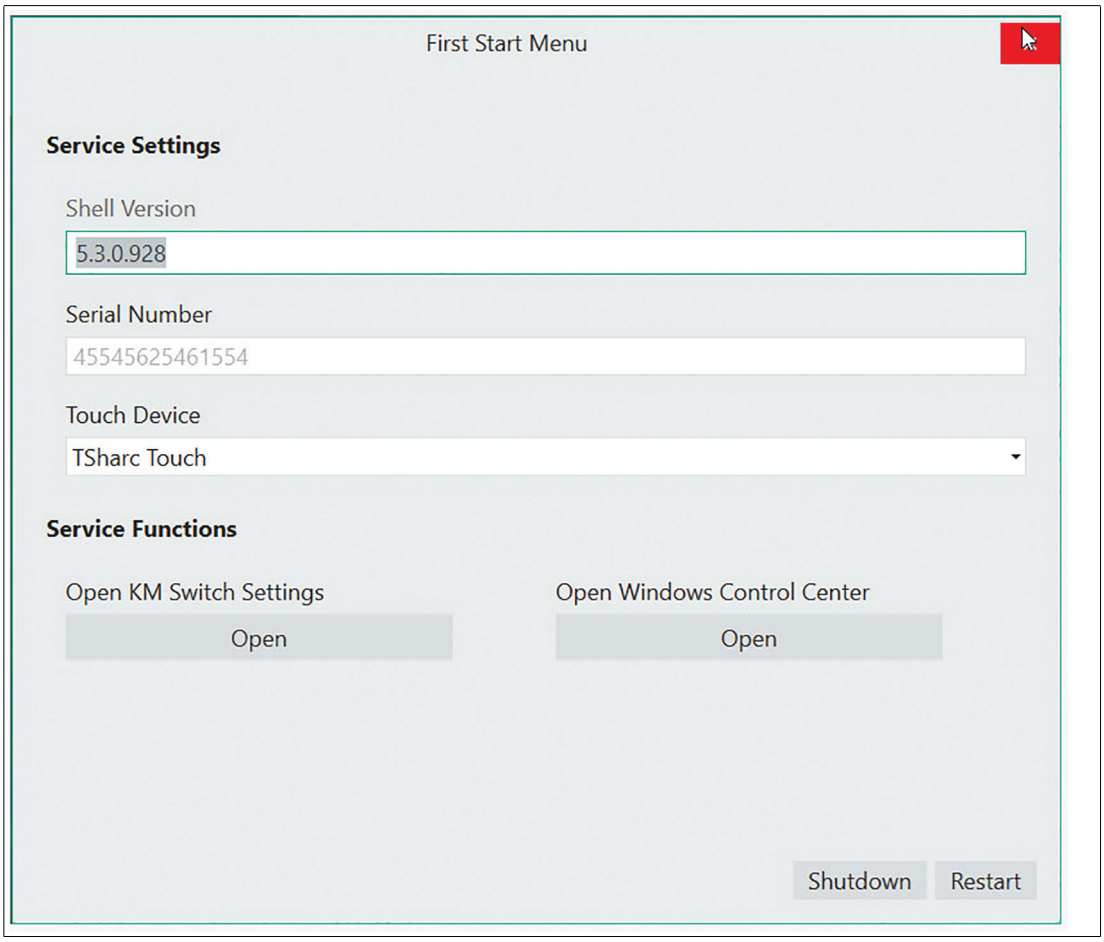


Figure 7.42

- Either follow the RM Shell First Start Wizard steps locally on the device or remotely via VisuNet CC. For further information on the First Start Wizard please refer to the RM Shell manual.
- Enter the System Settings App of the RM Shell (Chapter 7 RM Shell Manual) and set the computer name of your device.
- If your Network requires static IPs, also adjust the IP Settings. If the DHCP is enabled this step is obsolete.
- Reboot your System so that the changes take effect.

2. Backup Image

After the automatic rebooting of the System the device will be found automatically in VisuNet CC. All settings can be adjusted as usual if necessary.

Note! Make sure not to change the Computer Name and the IP address in between the capturing and applying process. VisuNet CC might to be able to find the device and a local setup might be required.

3. Clone Image

After the reboot of the device you need to change the following settings **locally.**

- Close the Window "First Start Menu"

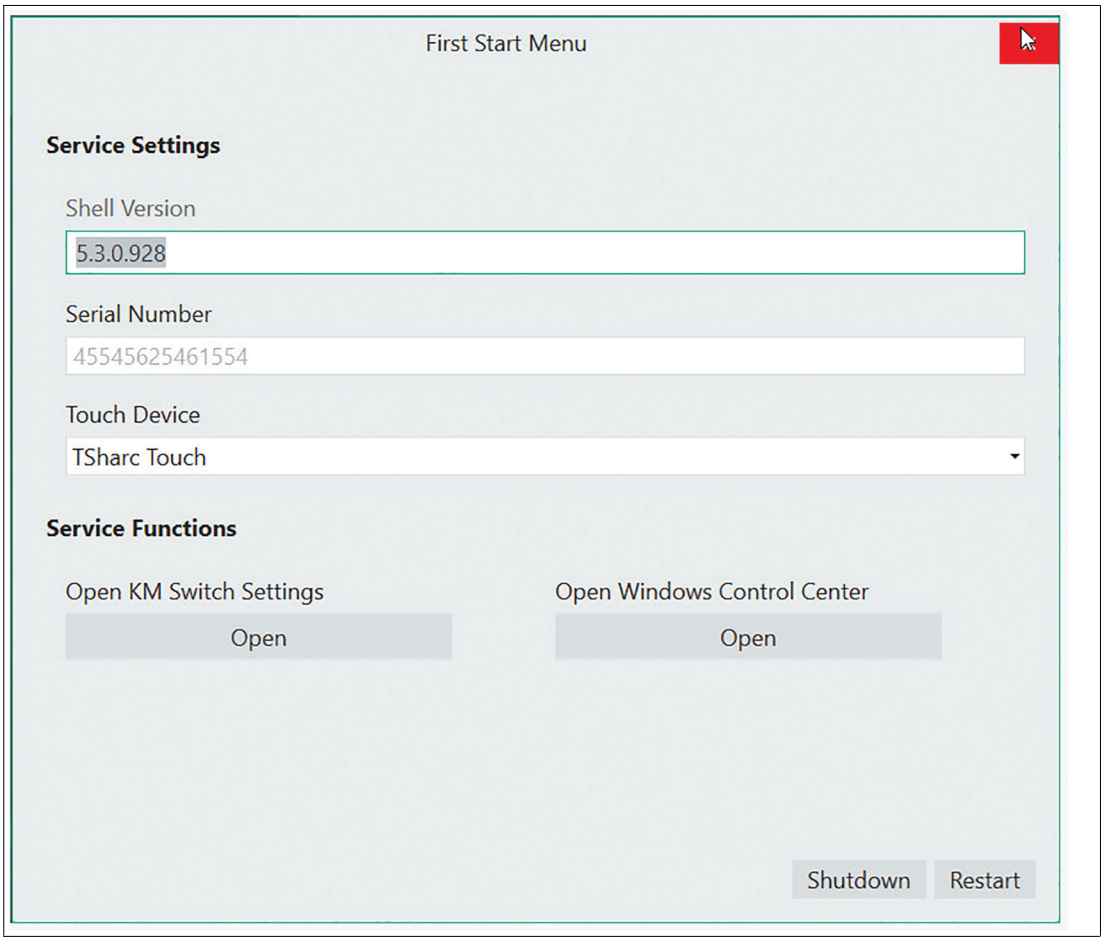


Figure 7.43

- Enter the System Settings App of the RM Shell (Chapter 7 RM Shell Manual) and set the computer name of your device.
- If your Network requires static IPs, also adjust the IP Settings. If the DHCP is enabled this step is obsolete.
- Reboot your System so that the changes take effect.
- Continue the setup process via VisuNet CC. If you already configured your RM Shell device settings in the past und would like to restore these settings follow a). If you would like to configure multiple devices with the same configurations follow b)

a) Set your old computer name and upload the settings (we recommend this option, when your devices haven't been configured).



Figure 7.44

If you set your old Computer Name and the same Network settings as earlier you can upload the device settings via VisuNet CC to the RM Shell and return to the previous setting status of the RM Shell. The settings of Third party software remains identical to the cloned settings. With the Upload wizard the upload can be performed for multiple devices simultaneously.

b) Follow the clone wizard to configure multiple devices with your settings.

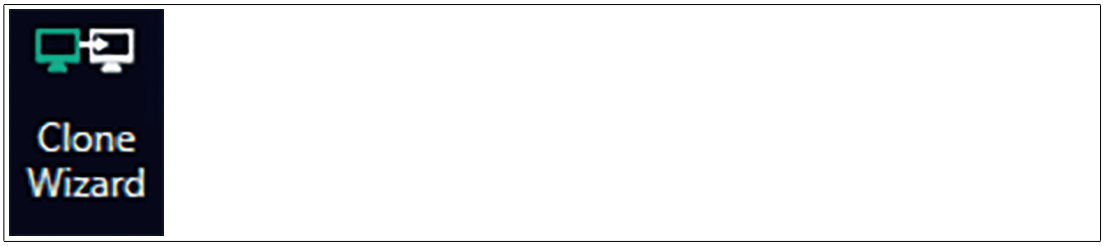


Figure 7.45

Use one device, either set it up or use one device within your network, as a predefined standard and clone the settings to multiple other devices. See chapter 7.3 for further information on the clone wizard.

Note

All devices need individual passwords which are required when executing the Clone Wizard.

The settings of Third party software remains identical to the cloned settings.

Capture Image Wizard

Use the Capture Image wizard to capture multiple images from multiple devices. The complete Windows partition of the selected devices are captured as Image files.
For each Image about 7 GB storage are required in the Network share.

1. Click "Next".

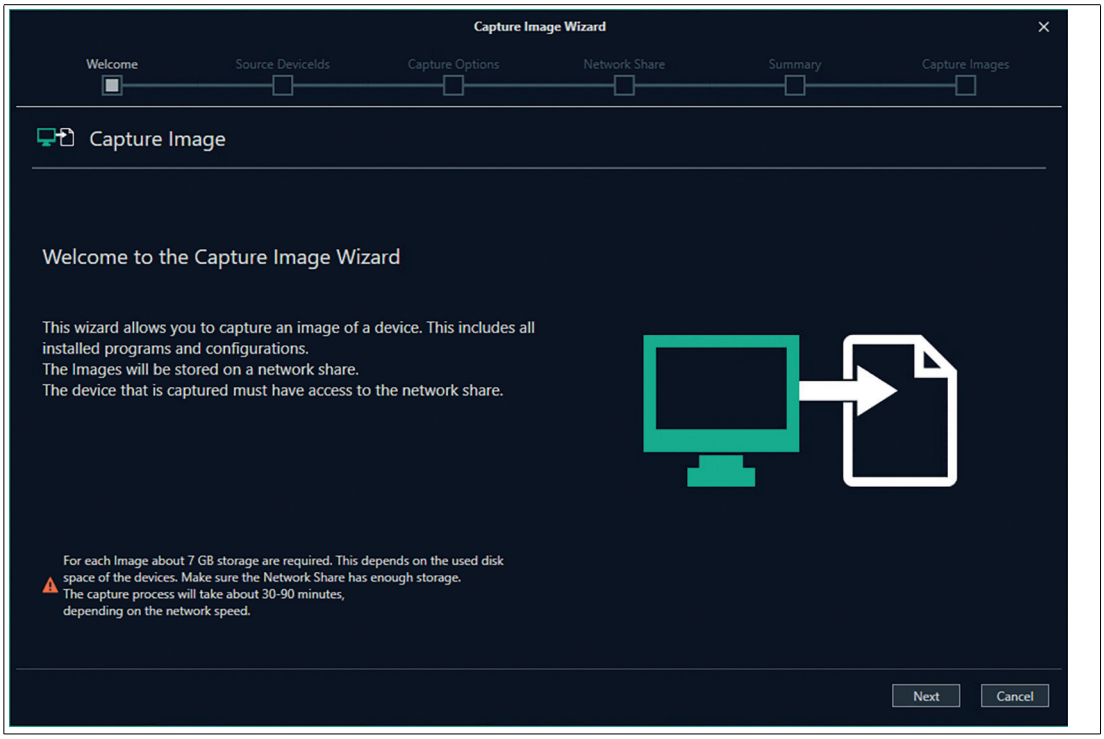


Figure 7.46

2. Click "Next".

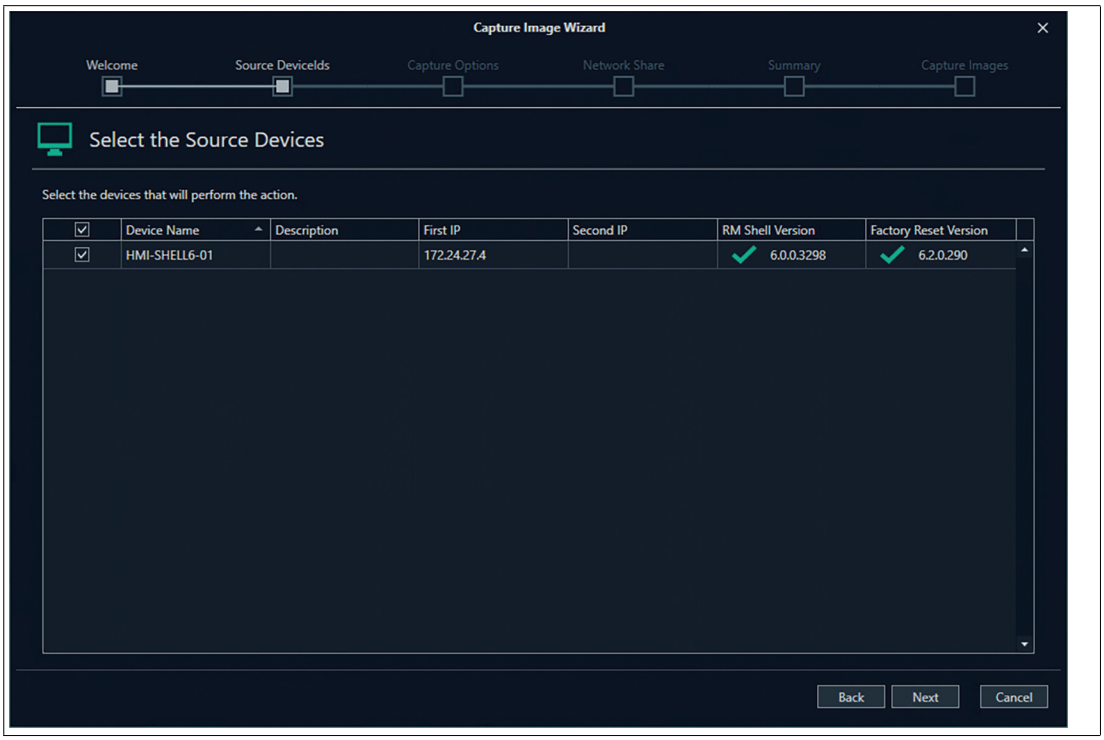


Figure 7.47

3. Select if you would like to either capture a Backup Image or a Clone Image. For further information on the different Images please refer to the table at the beginning of this chapter.

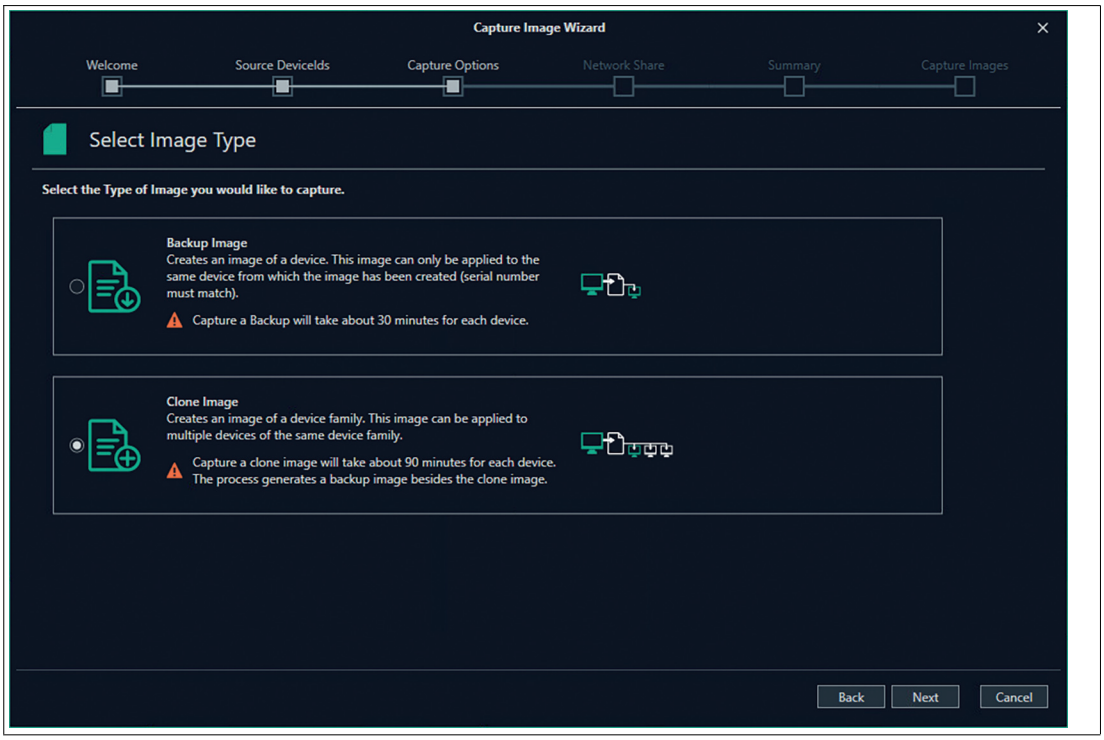


Figure 7.48

4. Select the Network Share which will be used to store the image at.

5. Check the connection. If the connection failed, check the server path again. No further procedure is possible. If the connection is successful you can continue the wizard further and click "Next".

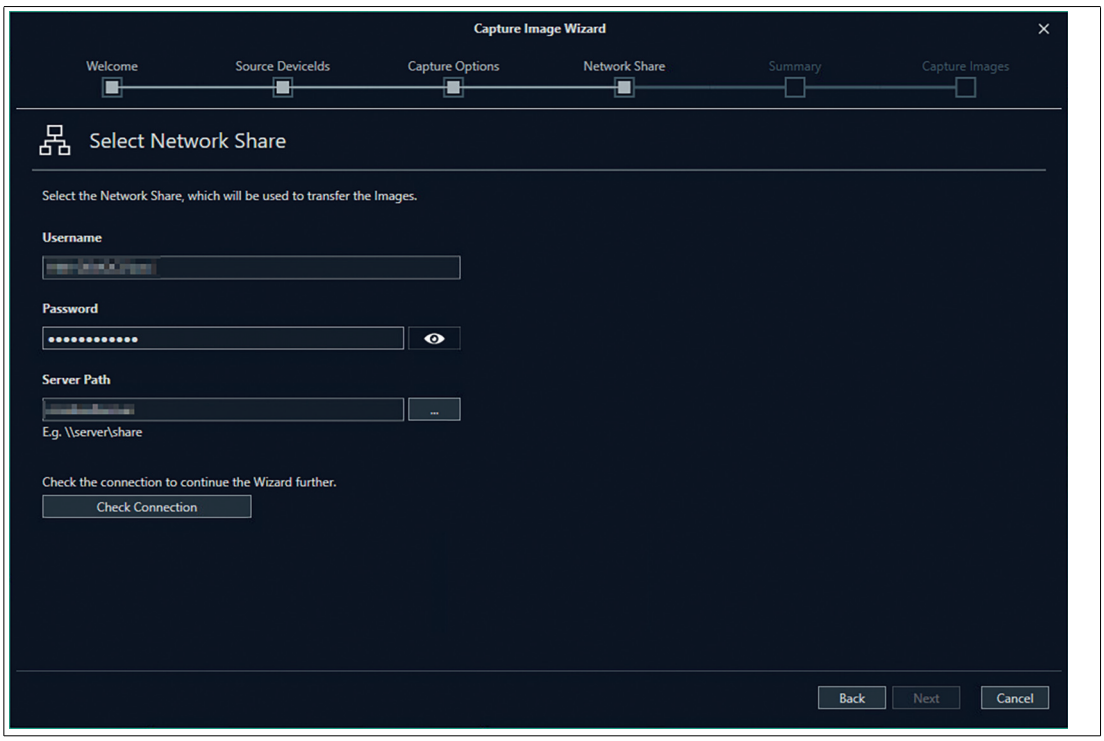


Figure 7.49

6. Choose a name for your Image. Modify the pattern for the name. You can use Variables to unify each image name with properties of the device.

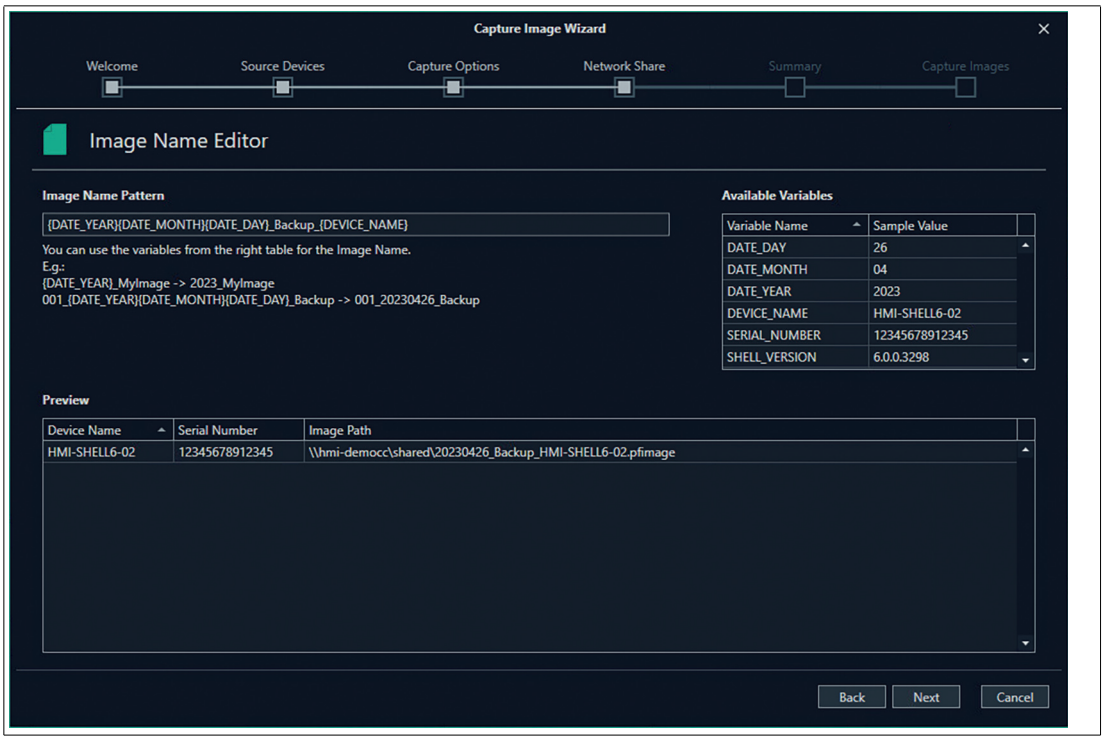


Figure 7.50

2025-07

7. Check again the selected settings then click "Execute" to perform the capture/apply process.

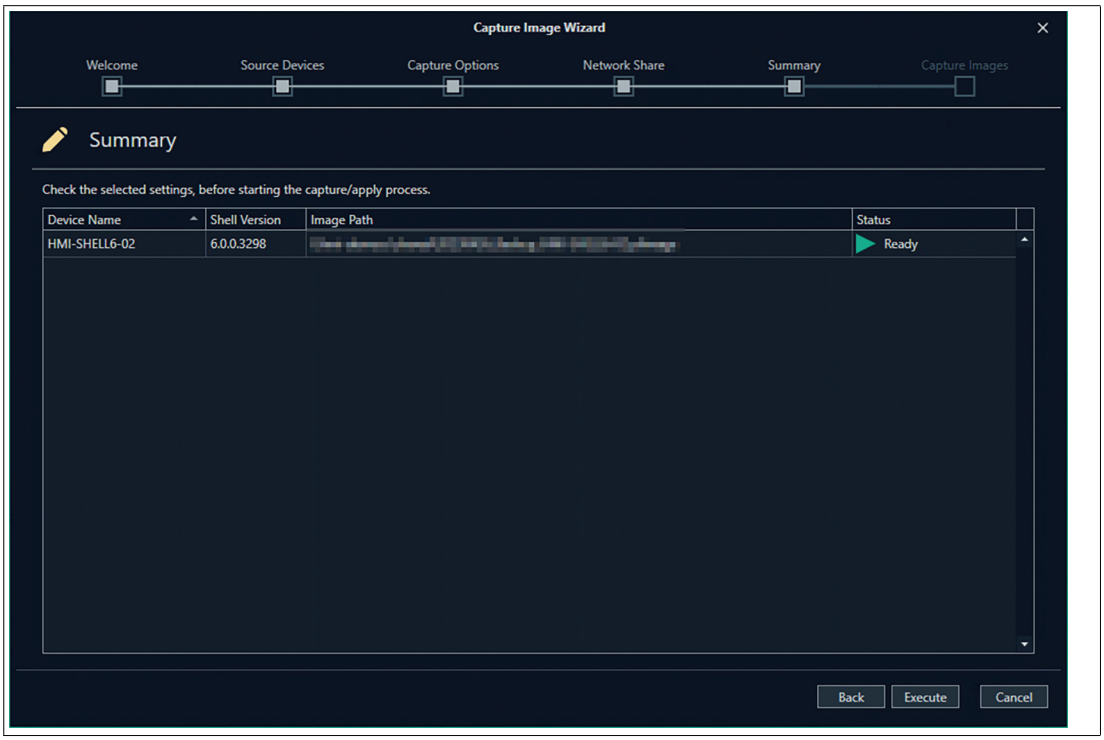


Figure 7.51

8. Capturing a Backup Image will take about 30 Minutes.

Note

During that time the device can not be operated.

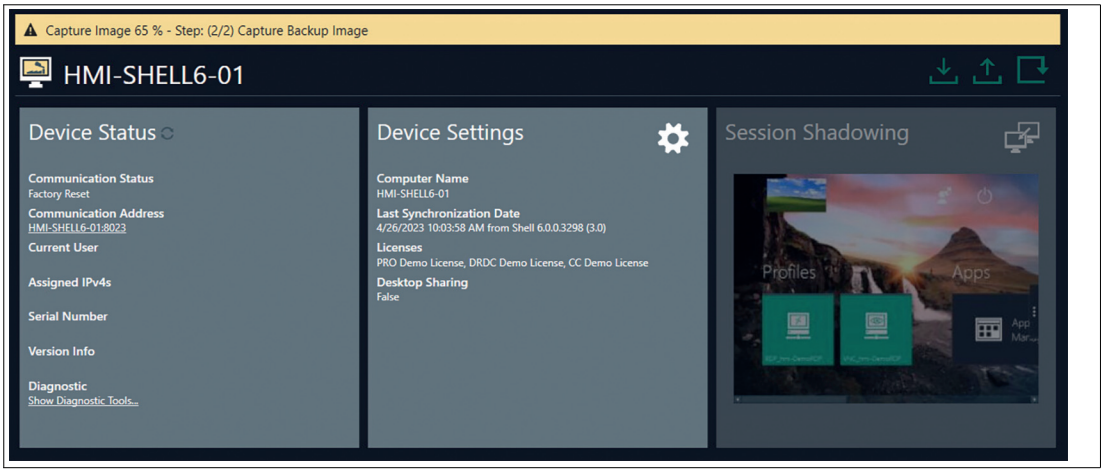


Figure 7.52

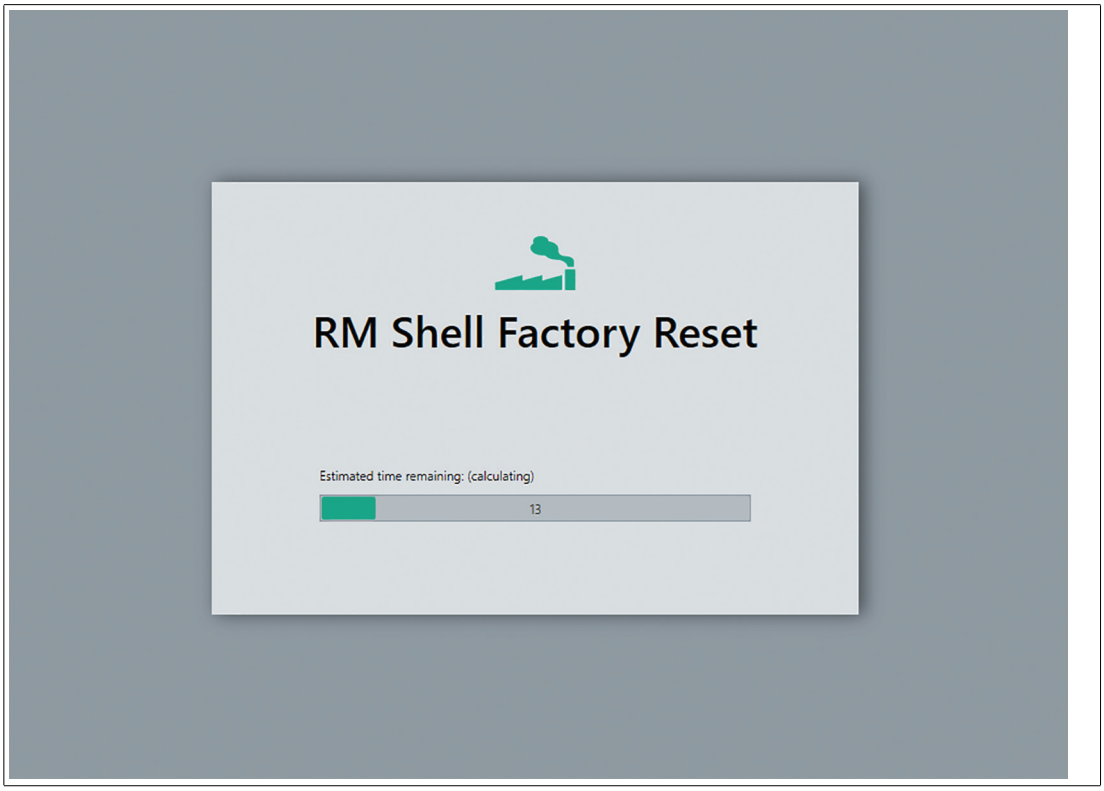


Figure 7.53

7.6 Profile Clipboard



Figure 7.54

One or multiple profiles can be copied between different devices. Select the profile in the profile list out of the device function tiles you would like to copy. Use either the icons or the right click to copy and paste the profiles. Remember to use the “upload” function to synchronize your new profile settings to your RM / BTC devices.

7.7 Profiles

The profiles group on the ribbon tool bar shows all relevant functions for setting up and using a remote profile.

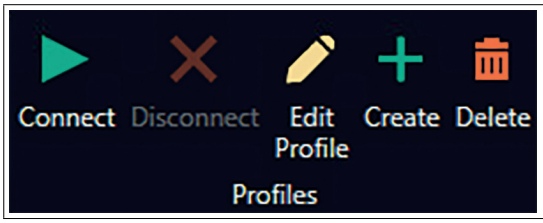


Figure 7.55

Function	Description
Connect	Start the profile selected from the VisuNet CC profile list stored on an RM / BTC. VisuNet CC must be synchronized with the RM / BTC in order for the remote profiles shown on the profiles list to be present on the RM / BTC.
Disconnect	Close the selected active profile connection of an RM / BTC.
Edit Profile	Allows editing core settings of local profiles that are stored in the VisuNet CC project. To change the profile on an RM / BTC after editing, use the "upload" function.
Create	Allows creating a new profile in the Control Center with its core values. To use the profile on an RM / BTC, use the "upload" function.
Delete	Allows a profile on an RM / BTC to be deleted. To delete the profile on an RM / BTC, use the "upload" function.

8 "How Tos"

8.1 Export Data

Data can be exported directly from Control Center as .xlsx, .csv, .pdf and other file formats. This is the collected device data of all connected VisuNet RM Shell devices. Data that can be exported is e.g.:

- Serial Numbers
- Computer Name
- RM Shell Version
- Factory Reset Version
- IP Address
- License Keys
- Last Service Version
- Various device settings
- ...

This list is not complete. Please check in the Export Data wizard which data that you would like to export.

How to open the Export Data Wizard:

1. Go to "File".

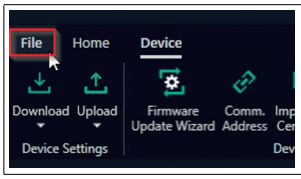


Figure 8.1

2. Click "Export Data".

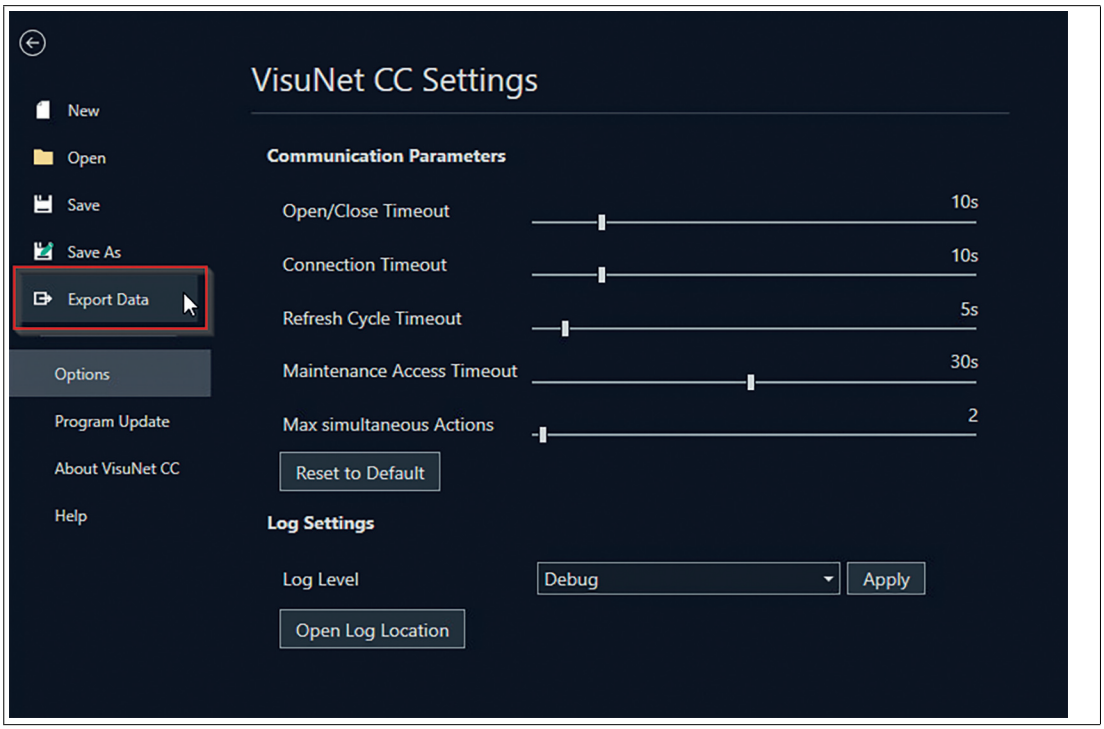


Figure 8.2

3. Select the data (types) you would like to export.

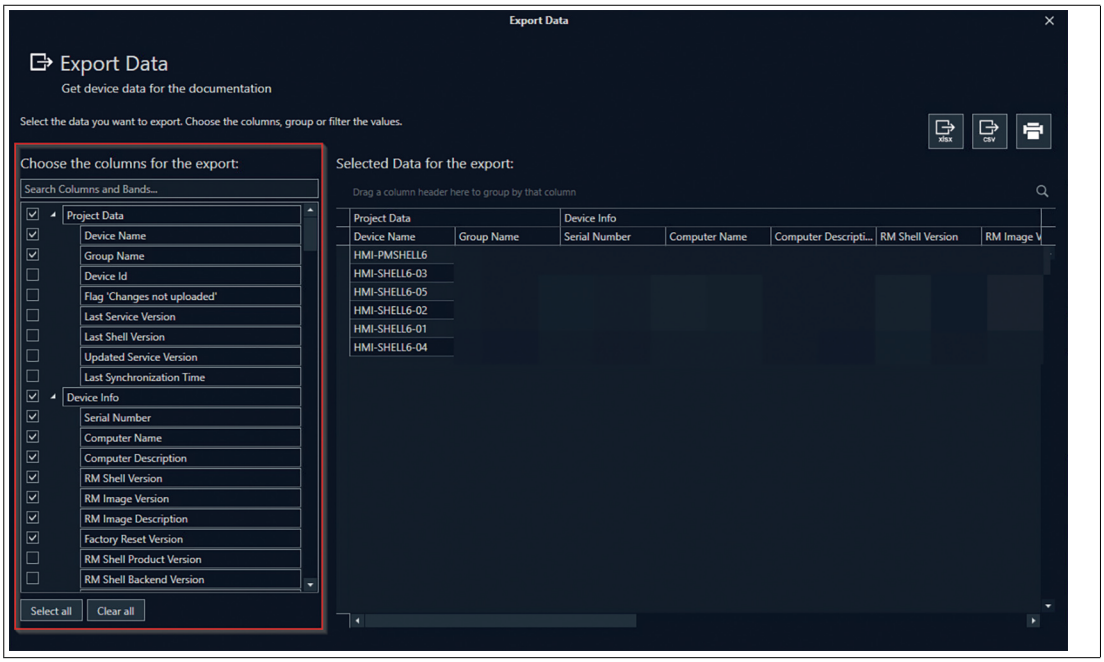


Figure 8.3

4. Select the required file format. You can export .xlsx and .csv directly using the two buttons on the left. You can export .pdf., .html, .docx and other formats under the print view.

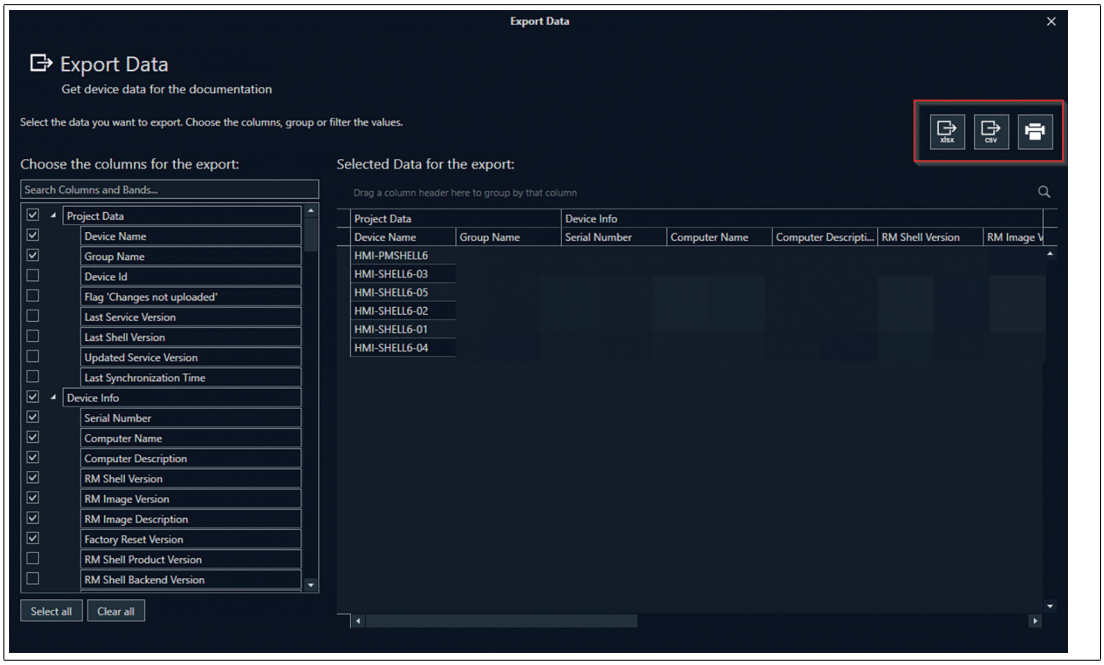


Figure 8.4

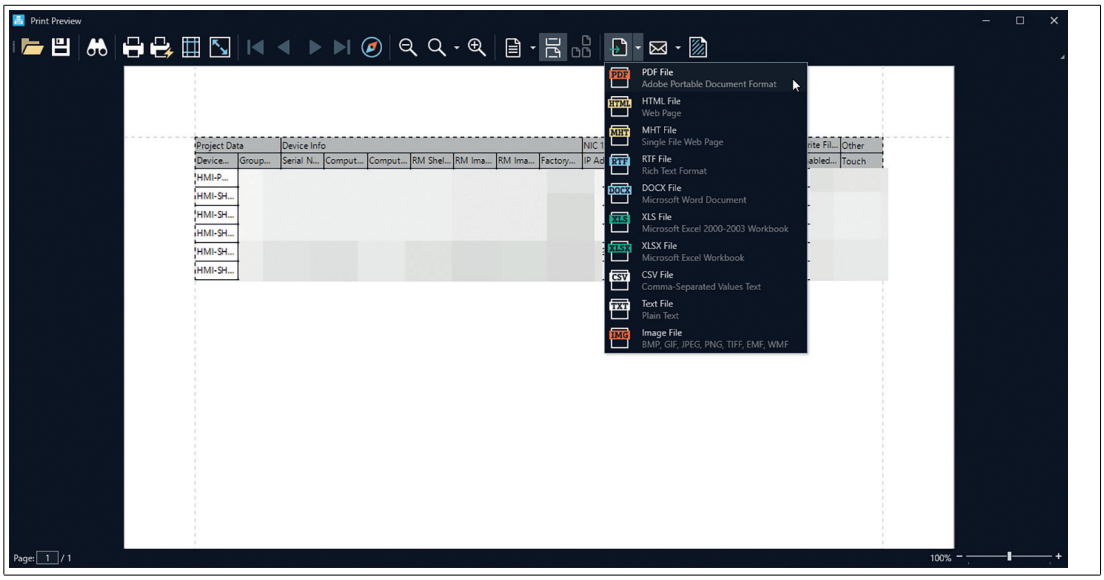


Figure 8.5 Print preview and possible document types to be created.

8.2 Transfer configurations from VisuNet RM Shell 5 to VisuNet RM Shell 6 devices

If you replace a VisuNet device and the firmware is upgraded from VisuNet RM Shell 5 to 6, for example when the TCU is changed, then you can use Control Center to apply the previous configurations from VisuNet RM Shell 5 to VisuNet RM Shell 6.

1. Initial situation: You have an active VisuNet RM Shell 5 device that is about to be upgraded to VisuNet RM Shell 6. This may occur when a TCU with VisuNet RM Shell 5 is replaced with a TCU that runs VisuNet RM Shell 6. All VisuNet RM Shell 5 configurations can be applied to VisuNet RM Shell 6 including active profiles.

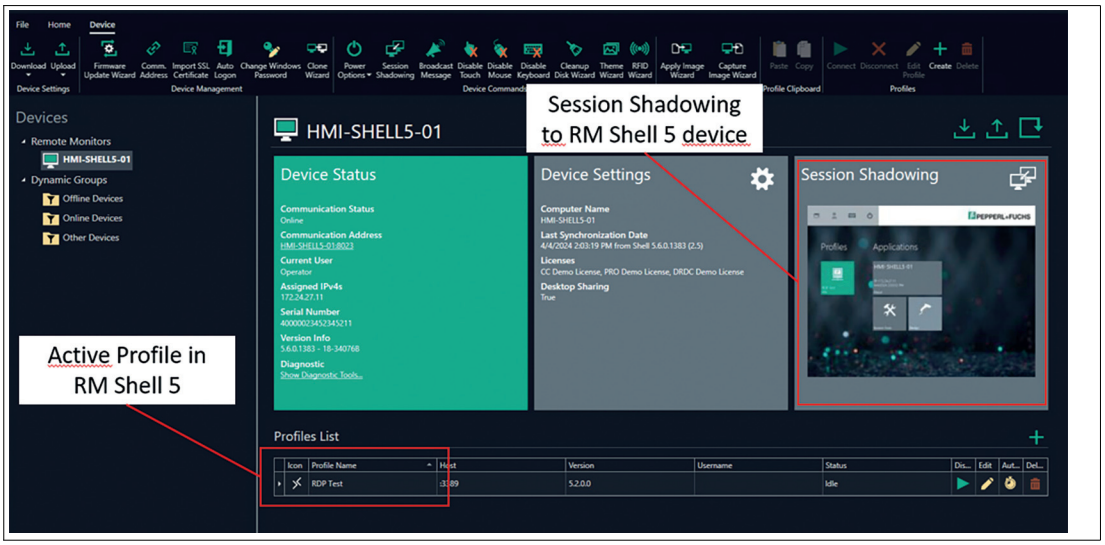


Figure 8.6

2. Before replacing the TCU, download the configurations of the VisuNet RM Shell 5 device one last time.



Figure 8.7

3. After replacing the TCU, you have to name your VisuNet RM Shell 6 device in the First Start Wizard of the VisuNet RM Shell 6.

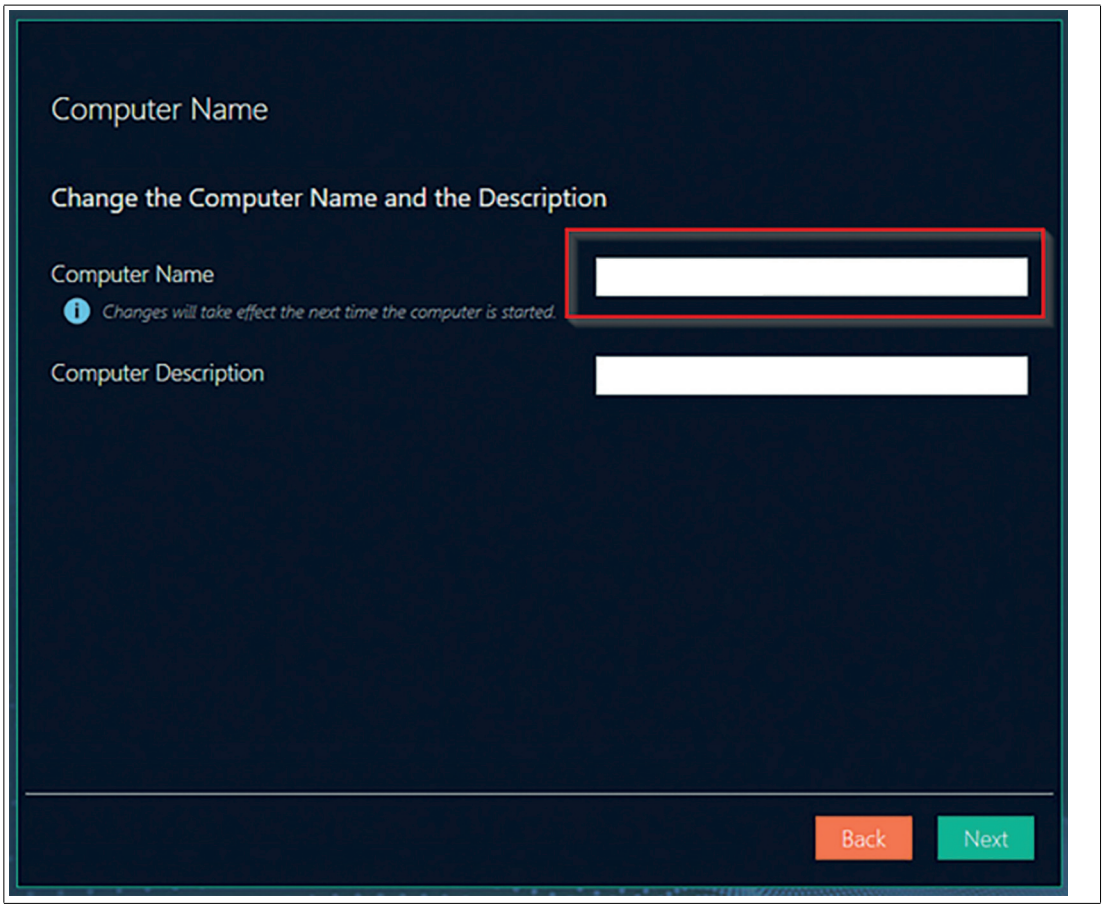


Figure 8.8

4. Update the Communication Address in Control Center. To do this, click on the old name:

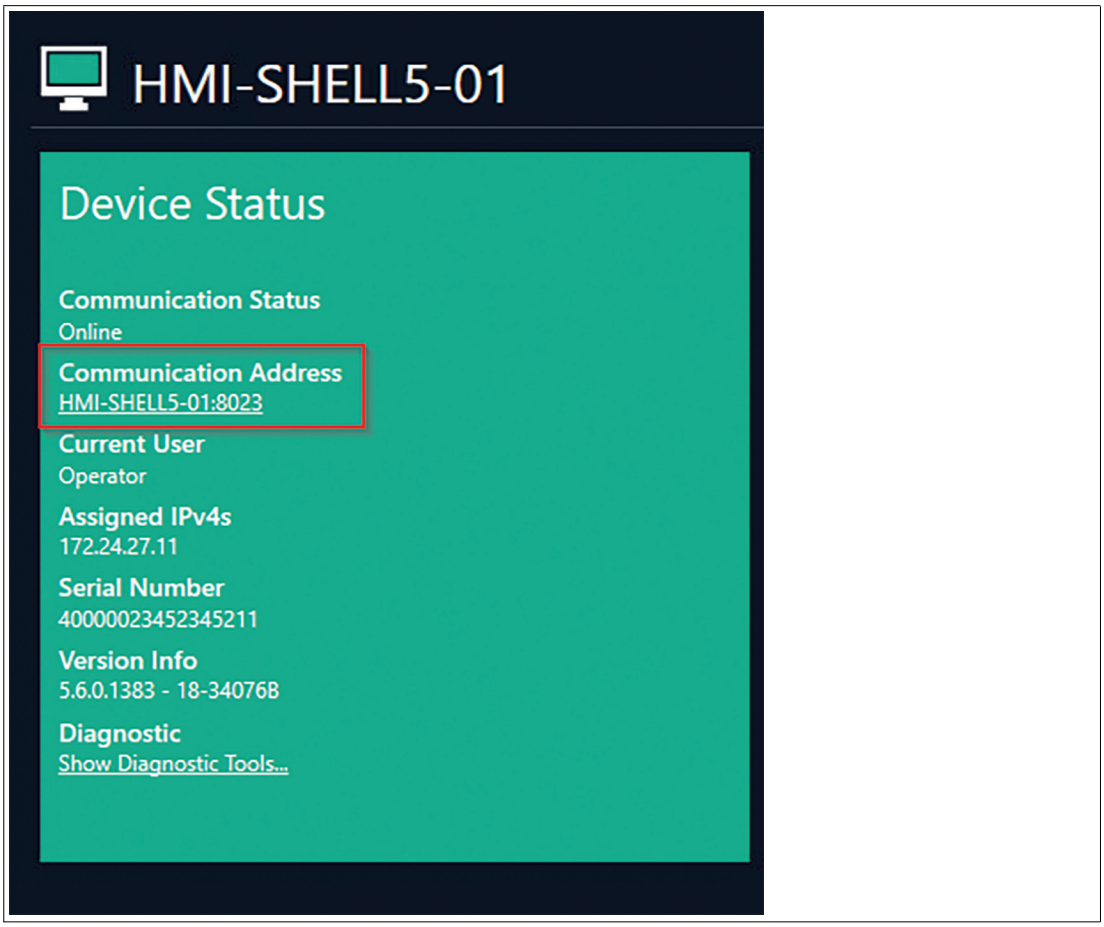


Figure 8.9

5. Enter the new name of the newly configured VisuNet RM Shell 6 device. In this case, the name of the new computer is "HMI-SHELL6-01", which was configured during the First Start Wizard of the VisuNet RM Shell 6.

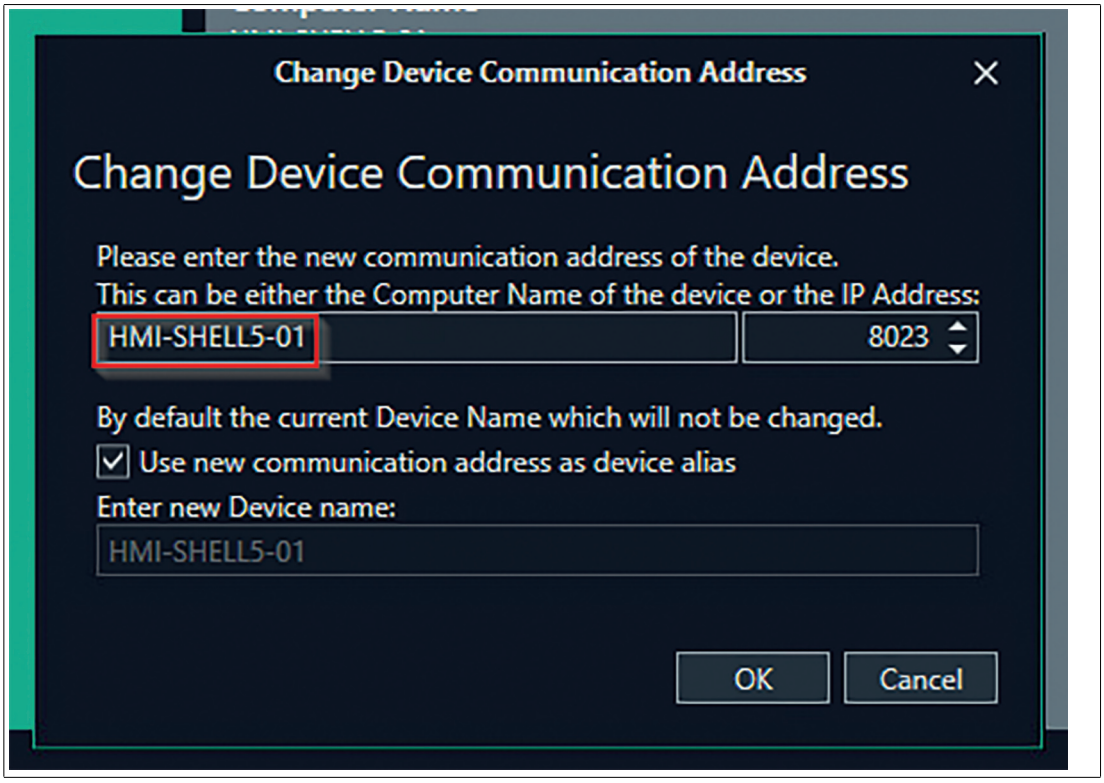


Figure 8.10

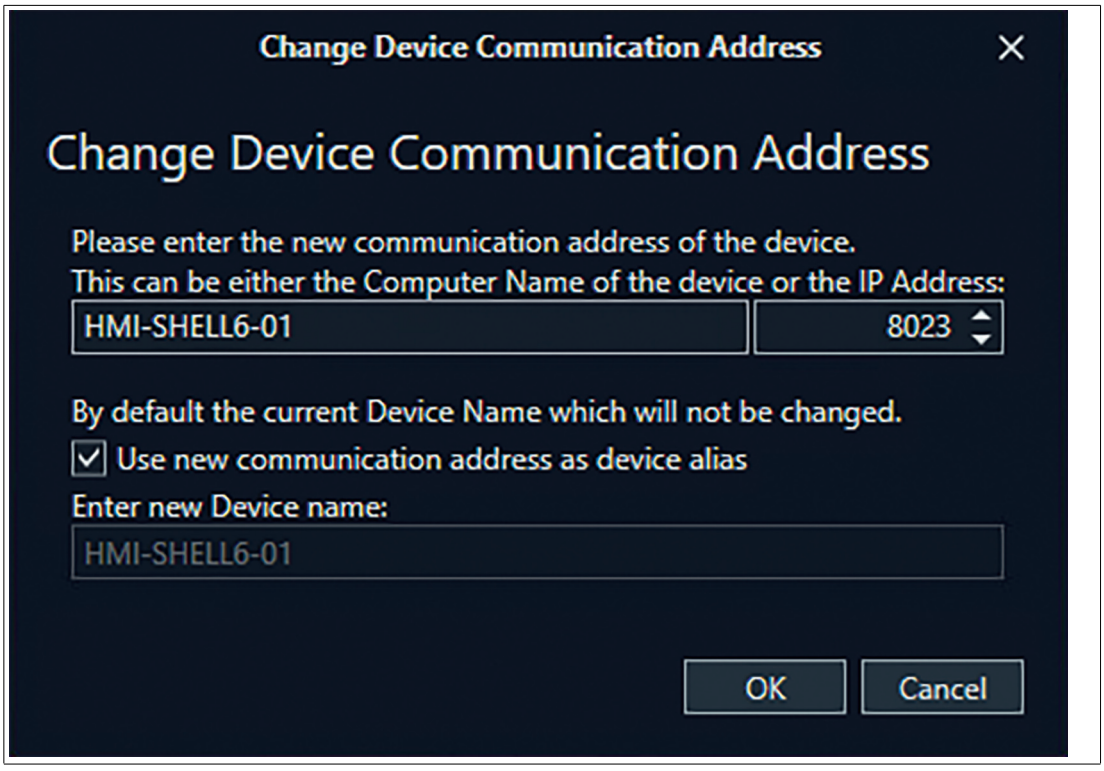


Figure 8.11

6. A certificate note should appear. It is recommended to use your own certificate. Enter the password of the local administrative account to access the device.

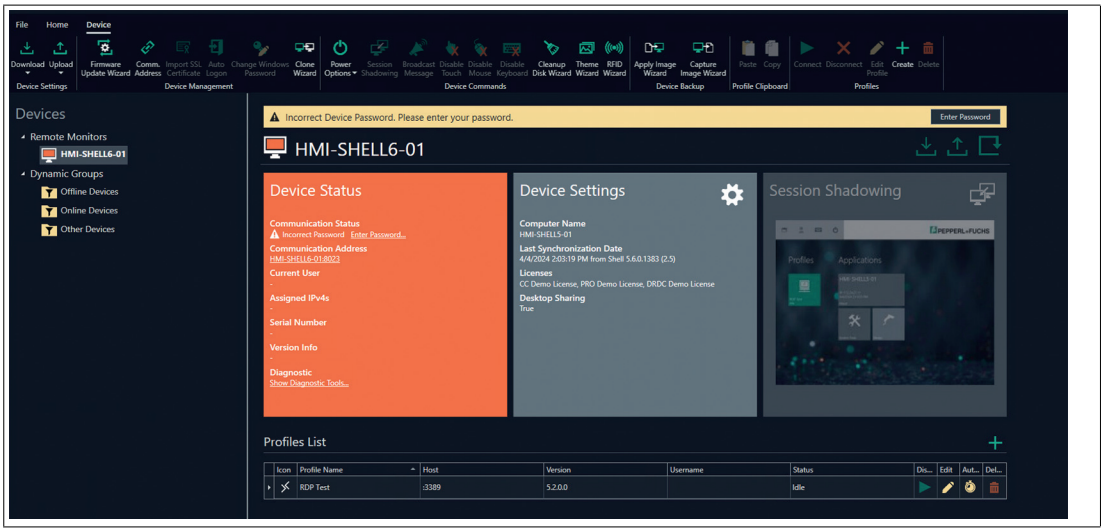


Figure 8.12

7. A message is displayed indicating that the data stored in Control Center originated from an older VisuNet RM Shell version. Click "Convert" to convert the data for use with an VisuNet RM Shell 6 device.

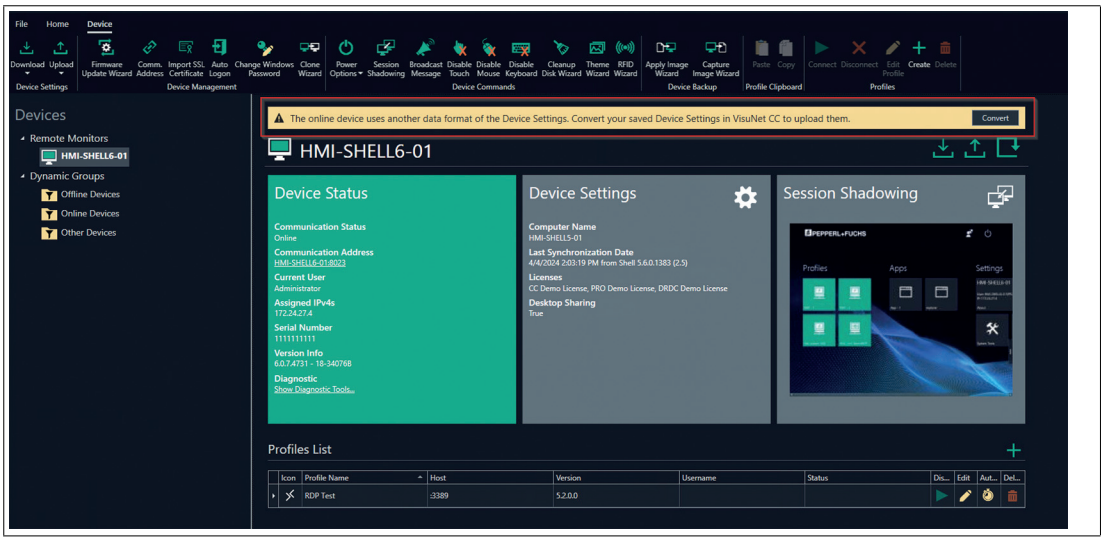


Figure 8.13

8. The "Convert Wizard" opens. Select the target device(s) where a conversion is needed.

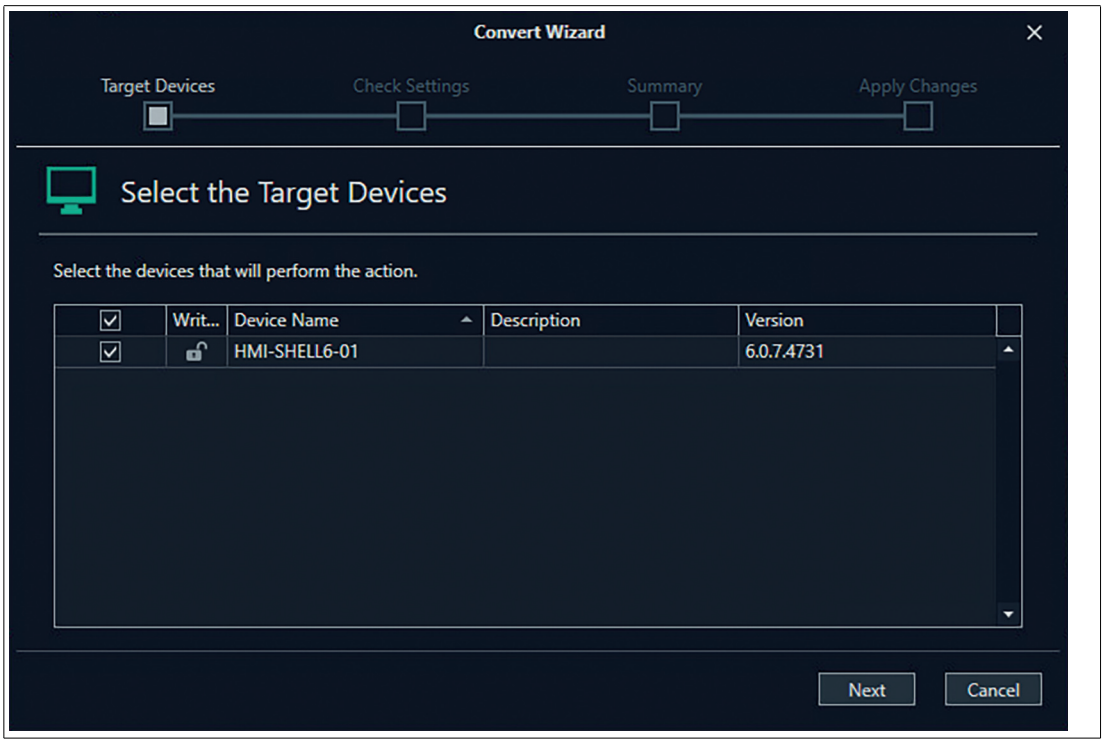


Figure 8.14

9. Make sure to assign the required license keys to the target device. A VisuNet CC license is needed for Control Center to access the VisuNet RM Shell device. You can either enter the license key manually or select a license key from the license manager vault via the drop-down menu.

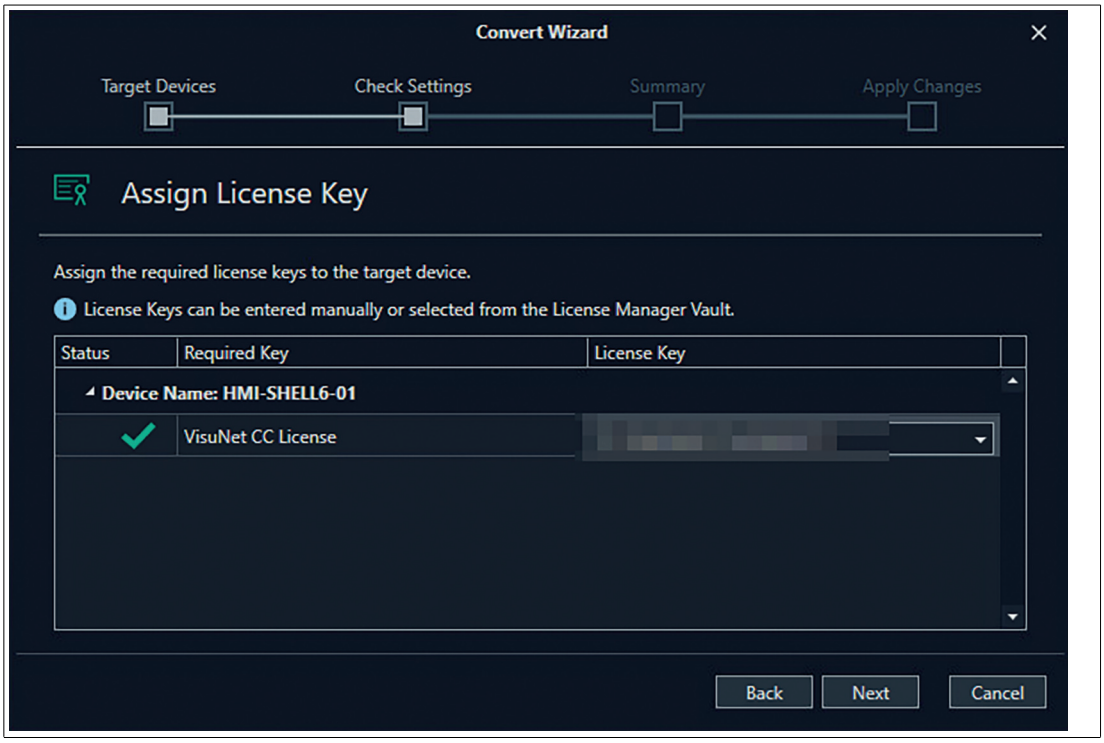


Figure 8.15

2025-07

PEPPERL+FUCHS

10. Deltas between both software versions are shown here.

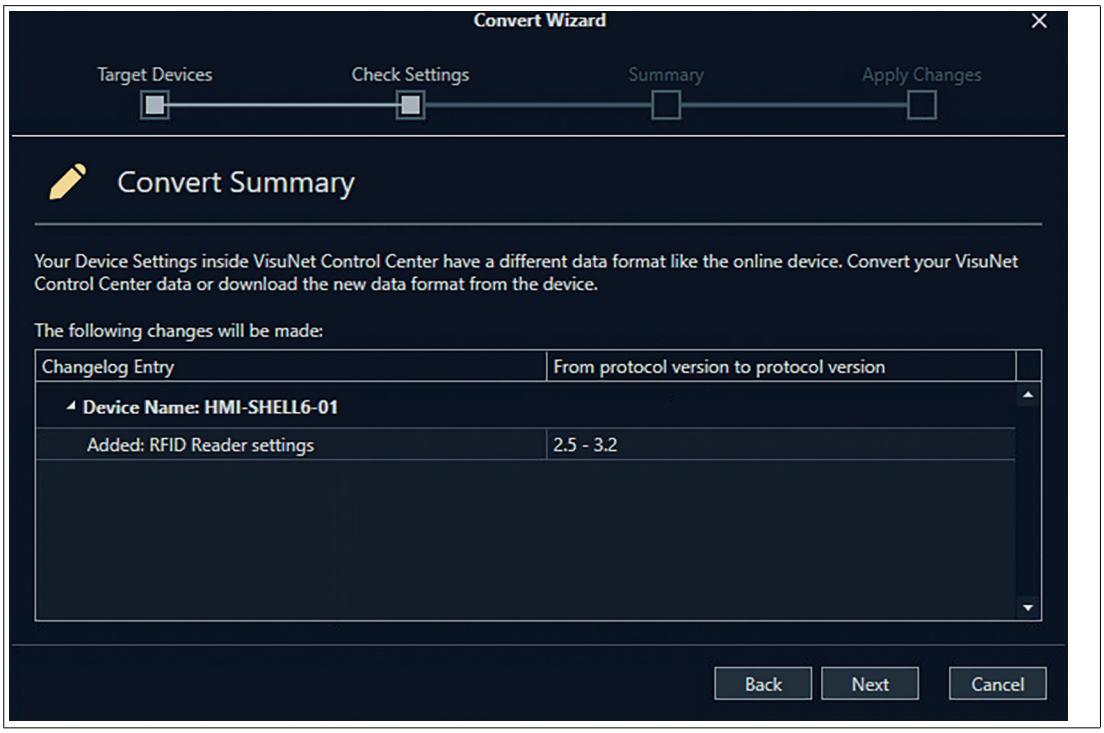


Figure 8.16

11. Execute the conversion.
12. Upload the configurations back to the RM Shell 6 device.



Figure 8.17

13. The configurations of the VisuNet RM Shell 5 device are now transferred to the VisuNet RM Shell 6 device.

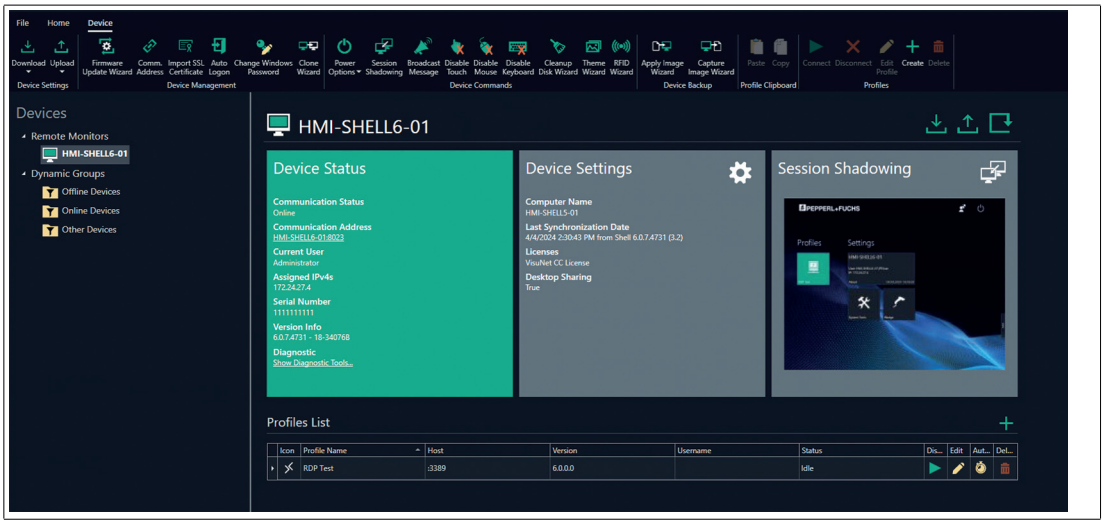


Figure 8.18

8.3 Preparing an RM / BTC for Centralized Management

Goal

Prepare an RM / BTC for centralized management.

Pre-conditions

Ensure, that the following criteria are fulfilled by the RM / BTC:

- Local time zone, date and time of RM / BTC are correct.
- RM / BTC has firmware version RM Shell 5 or newer.
- RM / BTC is connected to the same network as the PC with VisuNet CC.
- RM / BTC IP address and VisuNet CC IP address are in the same IP address range. DHCP is enabled as factory default setting in everey RM / BTC.
- VisuNet CC interface is enabled in the RM Shell (= default setting).
- VisuNet CC license key is entered in RM Shell. The license key can also be entered via VisuNet CC.

When all pre-conditions are fulfilled, the RMs / BTCs can be managed over the network by VisuNet CC.

8.4 Connecting to an RM / BTC

Goal

Add an RM / BTC to a VisuNet CC project.

Adding an RM / BTC

1. Add RM / BTC to the list of available devices.
2. Open search window by clicking "Scan for Remote Monitors".
3. You can either search for Host Names or IP Ranges.
4. All RMs / BTCs that have been found will be added to the list of devices.

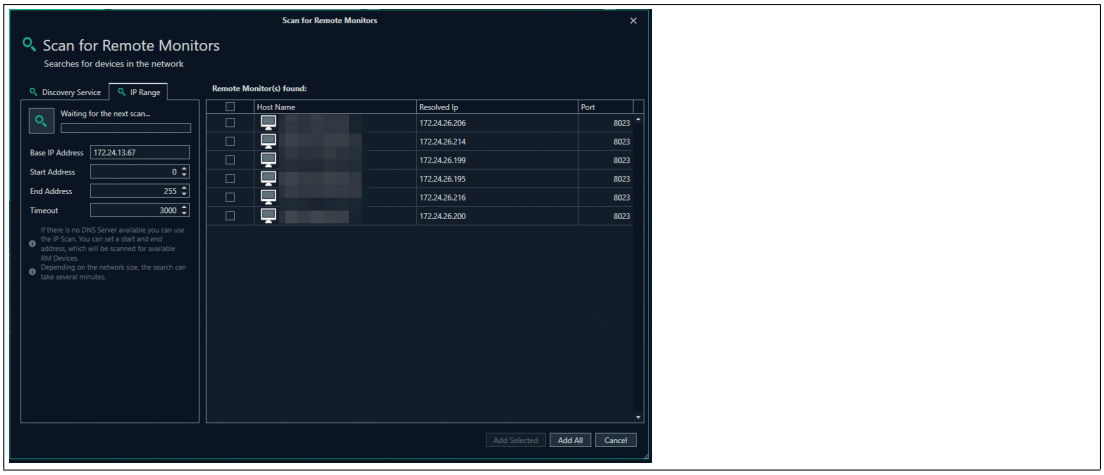


Figure 8.19 Scanning for RMs / BTCs

5. Click on the RM / BTC you want to connect to in device list.
6. To initiate the connection to an RM / BTC, enter the PFAdmin Windows password that has been set during the First Start Wizard of the RM Shell 6.

Caution!

Password security

Use strong passwords for the user roles "engineer" and "administrator" on the RMs / BTCs to ensure a high level of security!

Note

To avoid recurring authentications, the connection password can be stored encrypted in the Control Center project.

↳ After the initial connection, the device settings are automatically downloaded to the VisuNet CC.

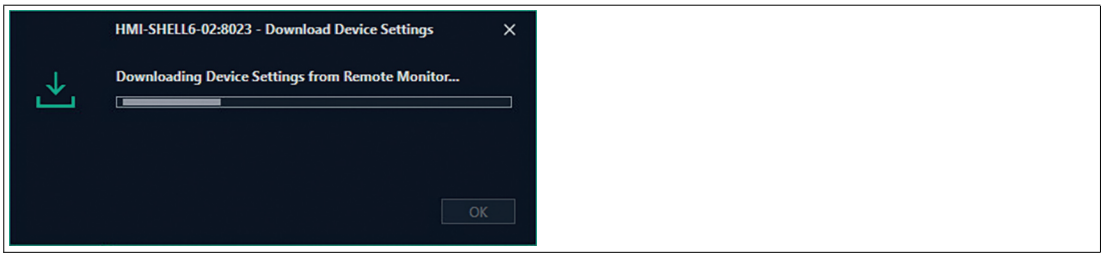


Figure 8.20

8.5 Uploading a Configuration to an RM / BTC

Goal

Updating device information with VisuNet CC

Note

All changes done in VisuNet CC are stored in the local project file. If you want to transfer the changes onto an RM / BTC, you need to upload them to an RM / BTC. Proceed as follows:

Pre-Condition

Connect to an RM / BTC

Update device information

1. When you have changed the device settings, upload them by clicking on the “Upload” button on the ribbon tool bar.
2. Choose in the drop down menu if you would like to upload the data directly from a single device or get guided through the upload Wizard and upload the settings and profiles of multiple devices.

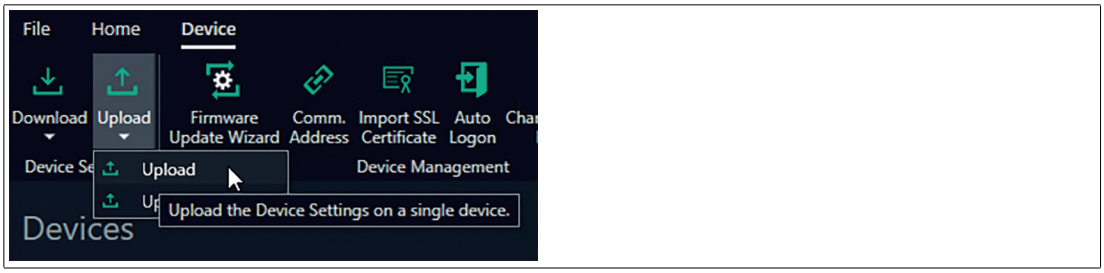


Figure 8.21 Upload the data of a single device

↳ The upload window showing the upload steps is opened.

↳ Before the settings are uploaded to the device, the local operator of the RM / BTC is prompted to give permission for the RM / BTC to enter maintenance mode.

3. Wait until the operator accepts the request, or use the “Force Access” function in the window to switch the RM / BTC into maintenance mode.

↳ As soon as maintenance mode is entered, the data and settings are uploaded onto the device.

↳ If the upload was successful, the RM / BTC will automatically leave maintenance mode, and the operator will be able to use the RM / BTC again.

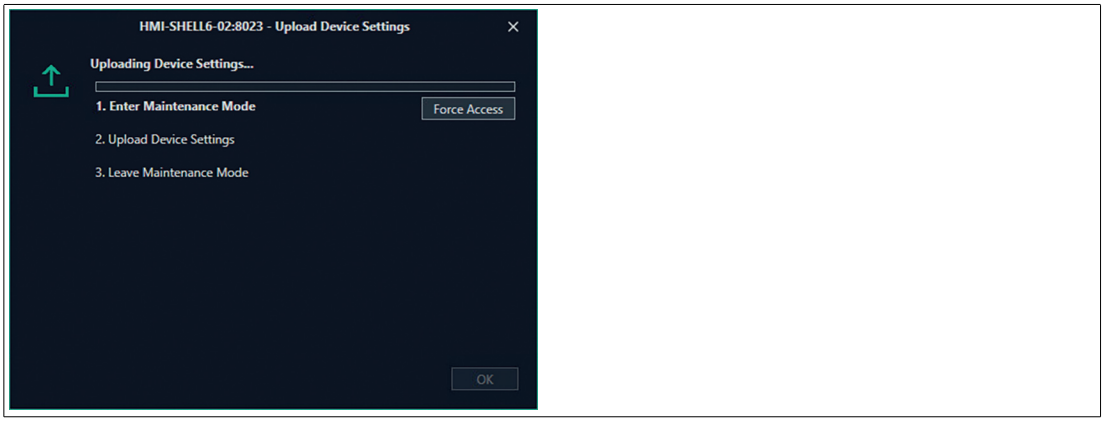


Figure 8.22

2025-07

PEPPERL+FUCHS

Upload data for multiple devices

1. The wizard showing the upload steps is opened and guides you through the process.

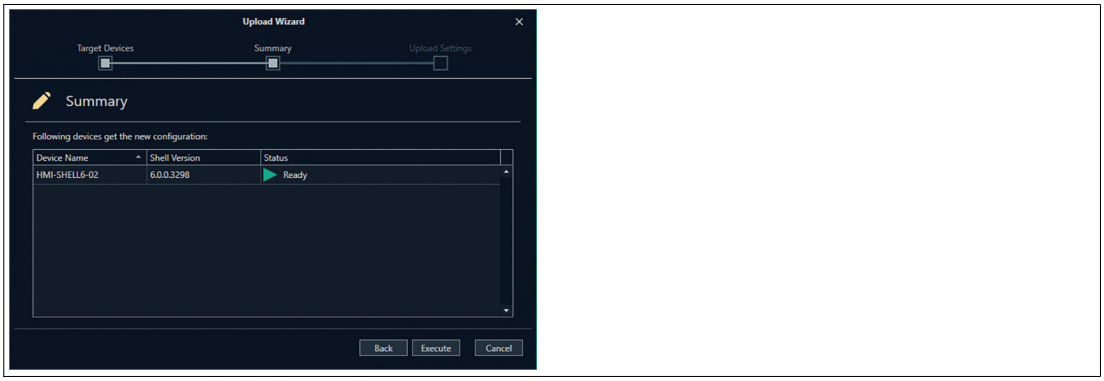


Figure 8.23 Uploading Device Data

8.6 Shadowing a Session

Goal

Connect to an RM / BTC for remote support

Pre-Condition

Connect to an RM / BTC. Enable Session Shadowing via Device Settings.

Remote support

1. Open the session shadowing window by clicking on the session shadowing tile or using the function on the tool bar.
2. In the session shadowing window, you are now able to shadow the session of the RM / BTC that you are connected to.
3. If you want to control the RM / BTC, click “Control” on the ribbon tool bar of the session shadowing window.

   ↳ Before VisuNet CC gains control of the RM / BTC, the local operator is prompted and asked to grant permission. If the local operator does not deny access within the defined amount of time, that can be specified in VisuNet CC under “Start”, VisuNet CC gains access to the RM / BTC.

Note

When controlling the RM / BTC, the local operator can still do local inputs on the Remote Monitor.

Note

Use “force” mode to immediately take over control of the RM / BTC without asking the local RM / BTC operator for permission.

8.7 Creating a New Local User

Pre-Condition

Ensure that you are logged into a project as administrator or another account that allowse editing user privileges.

Creating new user

1. Click the “Edit Users” icon on the ribbon tool bar.

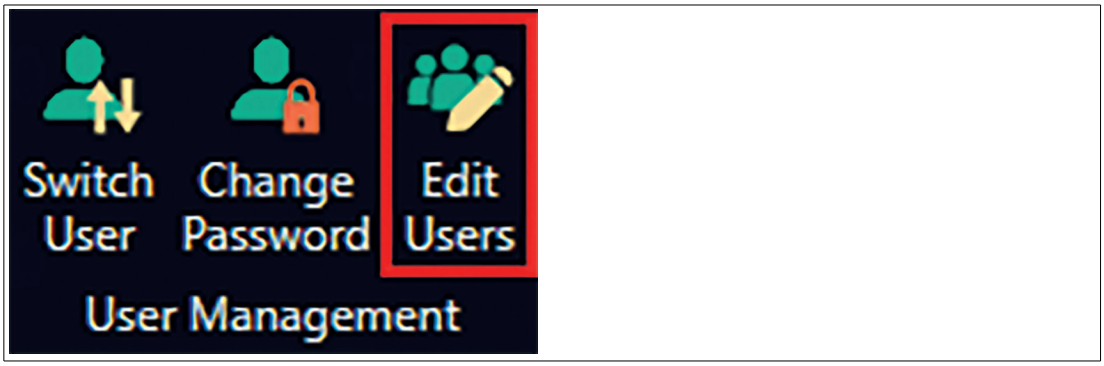


Figure 8.24

2. Click the “Add User” icon on the ribbon tool bar of the “Edit Users” window.
3. Use the displayed form to give the new user a name, assign them to a group, give them a single-sign-on name, and set his password.

4. Click “OK.”

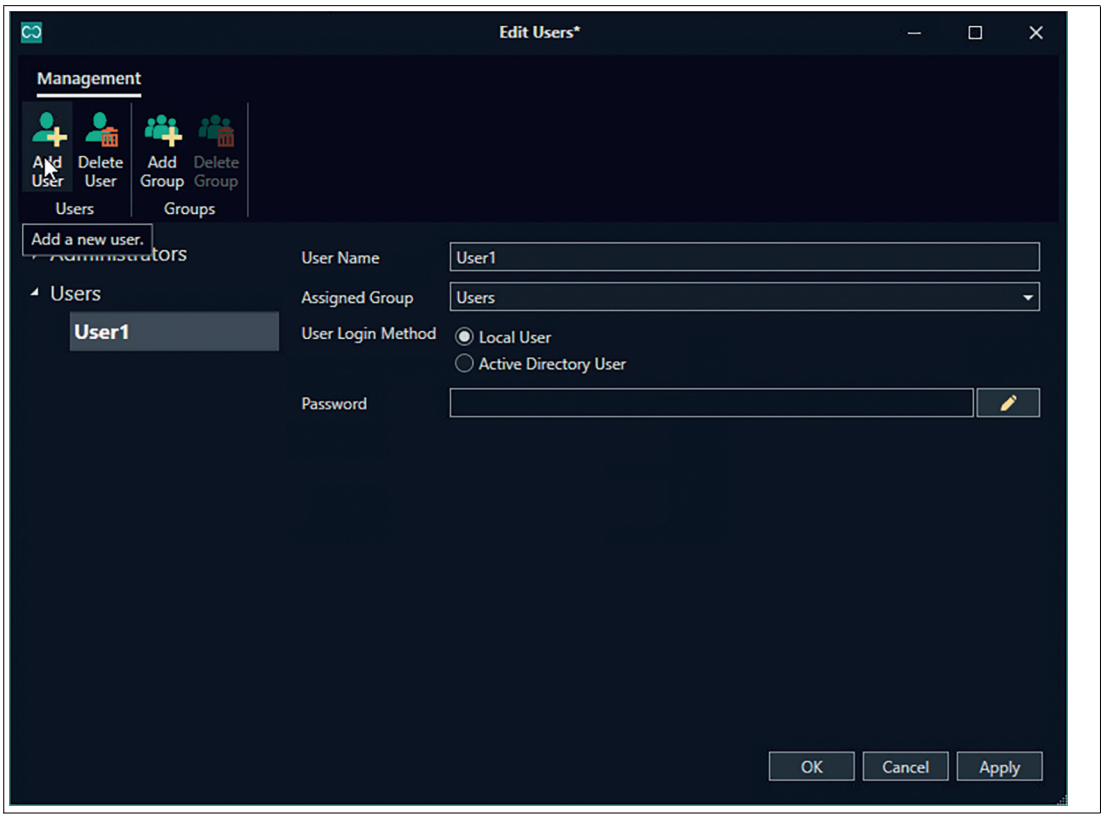


Figure 8.25

5. Save the project file to keep the changes.

8.8 Build up secure communication between CC and RM Shell devices

Pre-condition

An own root CA (public key certificate) as well as and end-user certificate with the import certification passwords need to be provided.

Note

The end-user certificate needs to be based on a private key! The common name of the end-user certificate has to have the same name as the host computer name of the target device.

When first adding a device to the a CC project you are faced with two error messages.



Figure 8.26

To fix the first error, the common Name of the certificate must match with the connection string. Import the certificate to the local device via the "Import SSL Certificate" Ribbon icon.

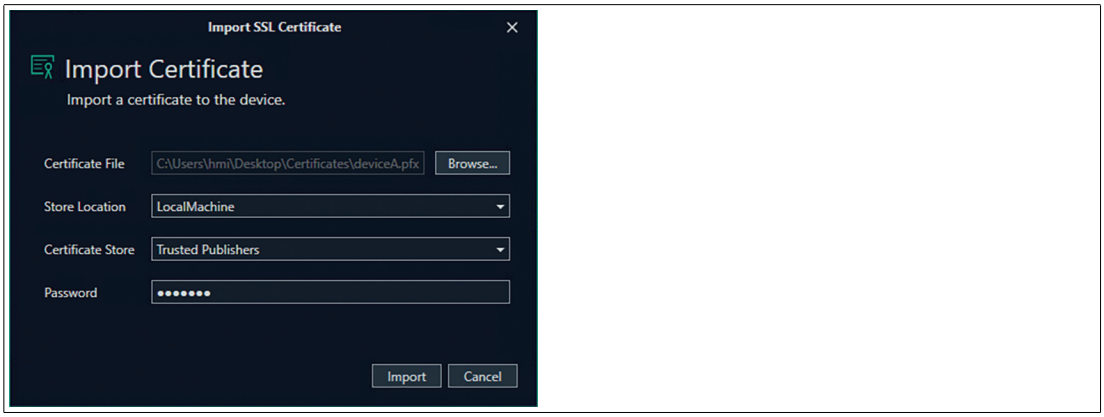


Figure 8.27

Only a certificate with private keys from the local machine store is allowed. (After installing the certificate on the local device).

Select the certificate with the correct common name.

Same can be done with a seperate certificate for the Session shadowing.

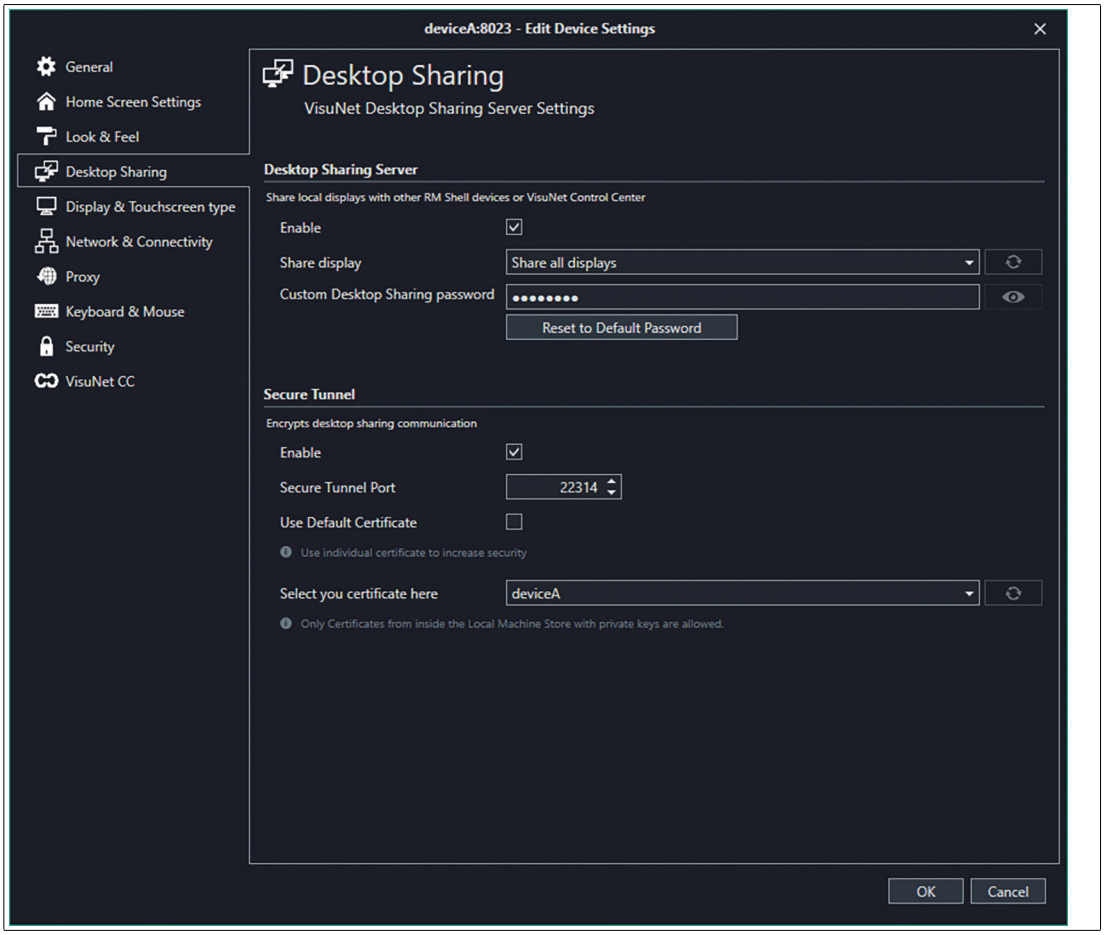


Figure 8.28

To adress the second Error the trusted chain must not be broken. To achive this Install a public certificate (root CA) on your local machine.

Install the public certificate (root CA) on your local machine

1. Open the certificate via right click and open the Certificate Import Wizard when clicking “Install Certificate…”

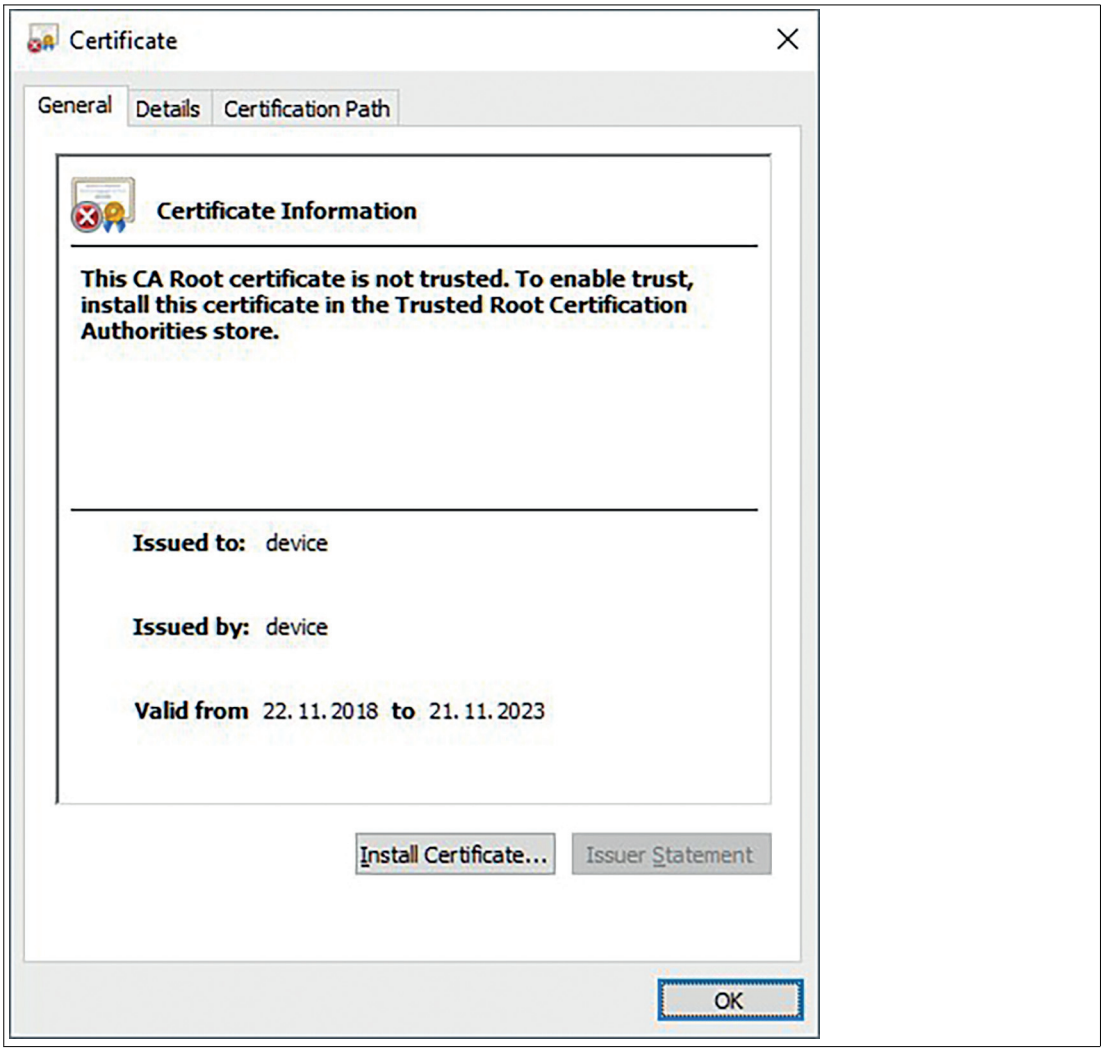


Figure 8.29

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

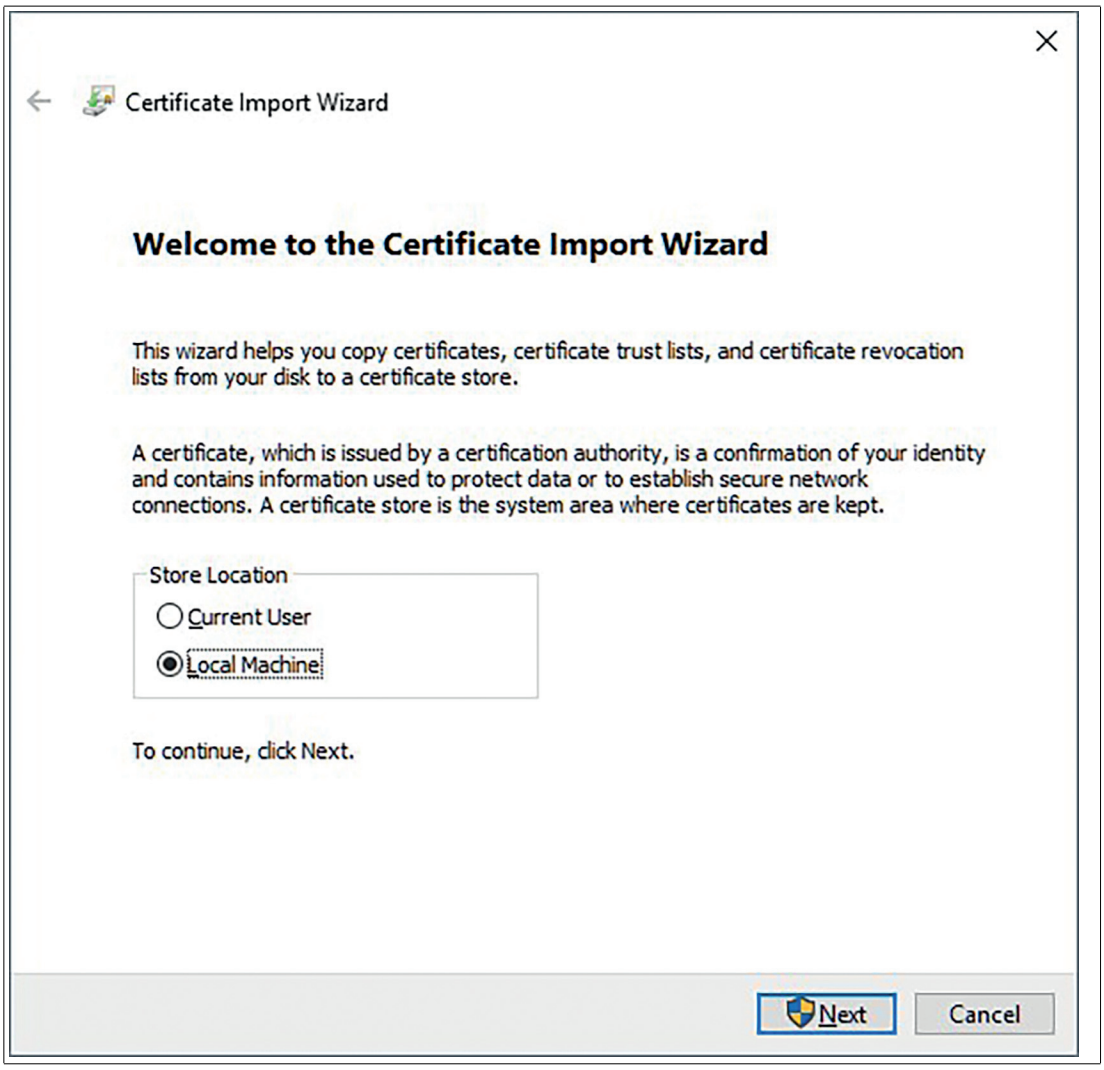


Figure 8.30

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

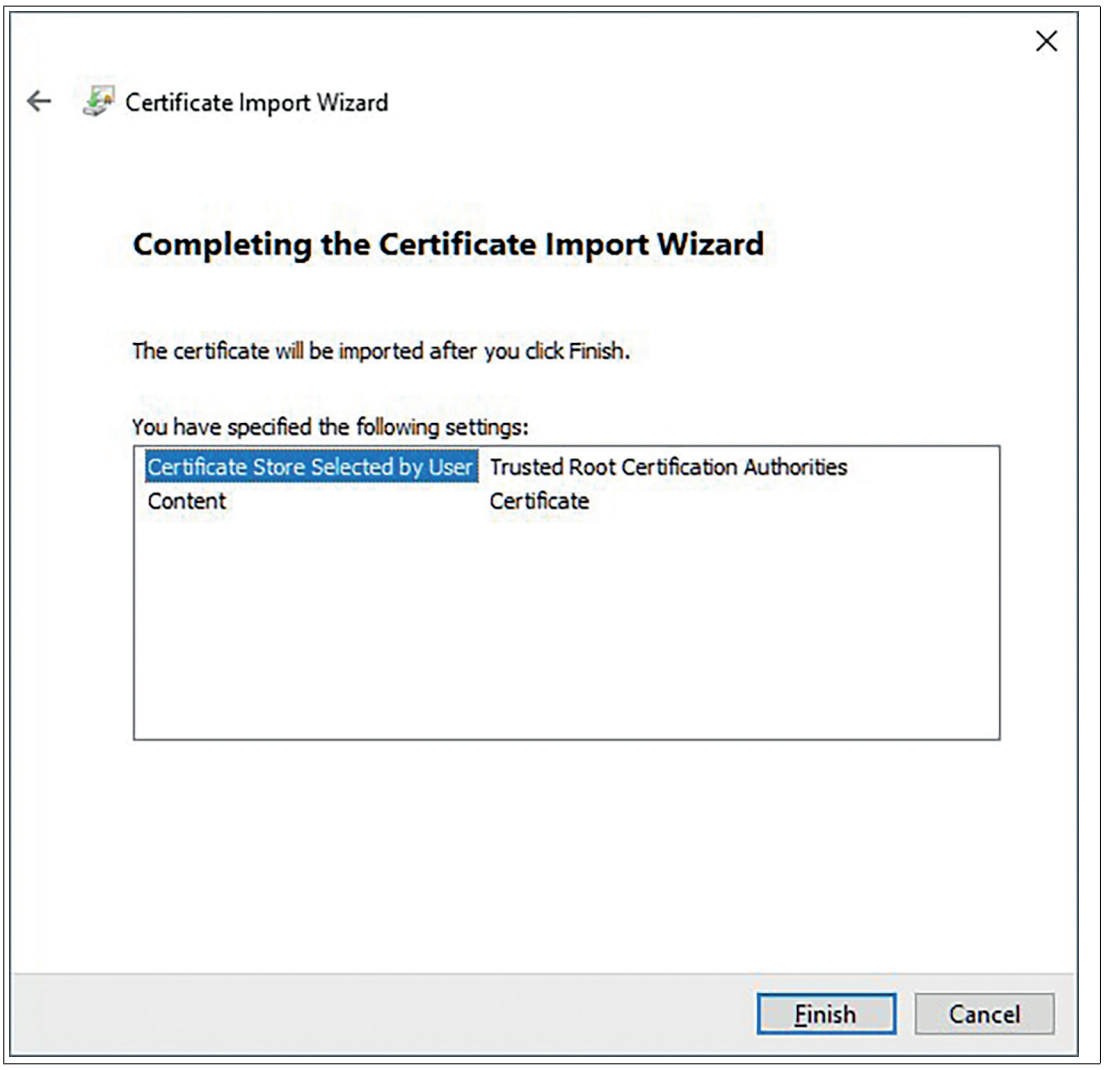


Figure 8.31

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

9 Troubleshooting

Problem	Potential root cause	Possible solution
RM / BTC cannot be found in VisuNet CC, even though I can ping the device.	The communication protocol is not properly routed through the network. One root cause can be that a second network adapter (e.g., WiFi card) is active that is connected to a different network.	Try to turn off or disable all other network adapters (e.g., WiFi card), that might be available in your system so that only the adapter is active that is connected to the RM / BTC network. Use the IP address as communication address.If the RM / BTC is found, check with your local administrator for the network routing settings.
RM / BTC has a status of "Security Error."	The communication protocol uses a certificate-based encryption that requires both communication partners to use the same system time.	Check if the RM / BTC is set up with the correct time zone, date, and system time.[1]
The RM / BTC status is shown as “Incorrect Password.”	One potential root cause for a communication failure can be that an invalid password has been entered for the RM / BTC (or is stored in the VisuNet CC project file). If this error occurred, it is also highlighted in the device status tile under “communication status.”	Try to re-enter the password that is used for the administrator role on the RM / BTC you want to connect to.
I am prompted in VisuNet CC to enter the VisuNet CC license key on the RM / BTC, even though I have already entered it on the RM / BTC.	The VisuNet CC key might not have been synchronized yet with the Control Center and is therefore unknown.	Download the RM / BTC settings via the download function to synchronize VisuNet CC with the RM / BTC. This will also download the VisuNet CC key from an RM / BTC, and remote access should be granted.

1. Reboot the RM / BTC if you change the time zone, date, or system time.

2025-07

Your automation, our passion.

Explosion Protection

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

Industrial Sensors

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

Pepperl+Fuchs Quality
Download our latest policy here:

www.pepperl-fuchs.com/quality

PEPPERL+FUCHS

www.pepperl-fuchs.com

© Pepperl+Fuchs · Subject to modifications

/ DOCT-8725B