Remote HMI Device Manager

For Remote HMI V6 industrial-grade Thin-Client firmware

Manual

Version: 1.00.00

Issue: 11/2020

Table of contents

1 About this documentation

This documentation describes the set-up and operation of the Remote HMI Device Manager, henceforth referred to as "software" for short.

The purpose of the software is to parameterise the Remote HMI firmware and manage the firmware licences. The Remote HMI firmware is henceforth referred to as "firmware" for short.

The firmware with its functions is described in a separate manual, and for remote access to the firmware please also refer to the notes and instructions of the firmware manual.

1.1 Registered trademarks

The products and services referred to in this documentation are registered trademarks and as such the property of their manufacturers.

1.2 Target group

This documentation is intended for administrators and production engineers who are authorised to parametrise HMI systems and set up remote connections.

1.3 Layout features

This documentation uses the following symbols, highlights and notes:

	Notes on system security and how to avoid data loss
	Important information on workflow and its optimisation
Pro	Notes on Pro licence functions

- List

Heading of an instruction

1. First step
   - ➢ Interim result
2. Second step
   - ✓ Result of action

Apply	indicates a button on the user interface
Dashboard	indicates a register, menu or a function of the user interface
[F8]	indicates a key of the keyboard

1.4 Contact details

R. STAHL HMI Systems GmbH

Adolf-Grimme-Allee 8

50829 Köln

Germany

Telephone: +49 221 76806-1200

Facsimile: +49 221 76806-4200

Homepage: r-stahl.com/de

Contact data Support

Telephone: +49 221 76806-5000

E-mail Support.dehm@r-stahl.com

2 Description

The software complements the firmware and is used for central parameterisation and licence management. The software access to the firmware must be granted in the Thin Client firmware under the **System & Proxy** menu item. Once access has been granted, several Thin Clients can be configured and parameterised via templates with the same settings.

Access to the Thin Client is also possible via the **Remote Access** function. This remote access via VNC must be permitted under the **System & Proxy** menu item in the firmware.

The software can be installed on a workstation or on a server. It can be used by multiple users.

The software supports the management of templates and device settings in databases. Each database can be password-protected against unauthorised access.

2.1 Licencing models

A licence key must be activated in order to use the software.

Without a licence key the software works as a demo version limited to one Thin Client with Remote HMI Firmware version 6 or above.

The following licence models are available for the management of multiple Thin Clients:

- Single licence to manage one additional Thin Client
- Package licence to manage 5 Thin Clients
- Package licence to manage 10 Thin Clients
- Package licence to manage 25 Thin Clients

The user activates the licence key in the software and connects it with the PC or server on which the software is installed.

The following firmware licences are available:

- Basic
  Basic licence for establishing remote connections, configuring the firmware and for importing and exporting settings.
  The use of the Device Manager is activated via the device hardware, which also ensures the activation of a Pro package licence.
- Pro
  Licence extension for using and managing applications, using multiple parallel remote connections, importing and exporting settings.
  The additional functions are unblocked by activating the Pro licence.

The Pro package licences of the firmware can only be used together with the Device Manager. It is not possible to activate the package licences in the Thin Client's firmware.

The following Pro licence models of the firmware are available for the Thin Clients:

- Pro single licence
- Pro package licence for 5 Thin Clients
- Pro package licence for 10 Thin Clients
- Pro package licence for 25 Thin Clients

The size of the management licence for the Device Manager must be the same as that of the Pro package licence. This means that in order to use a Pro package licence for 10 Thin Clients, a management licence for 10 Thin Clients must be available in the Device Manager.

2.2 Notes on the firmware

2.2.1 Function

The Remote HMI V6 firmware is a Thin Client software developed for the process industry which is supplied together with R. STAHL SERIES 500 operating devices. It is used to establish and secure remote connections to one or more workstations or application servers. This makes remote access from one operating station to one or more workstations or servers possible.

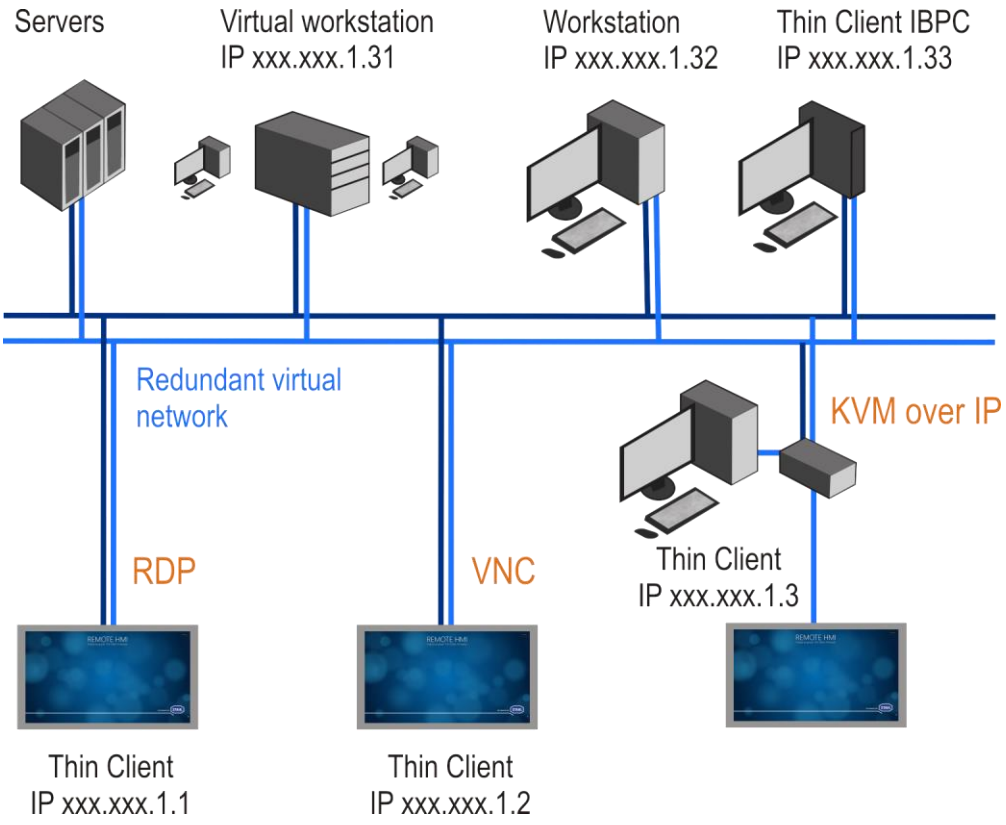
Suitable for device platforms:

- EAGLE series 5X6
- MANTA series 5X7
- MANTA GMP series 5x9
- SHARK series 5X8
- Industrial Box PC
- Tablet series EX80
- Tablet series FT110

The devices are connected to the Ethernet via the Ethernet interface (copper or fibre optic). The number of available Ethernet adapters varies depending on the device platform.

2.2.2 Supported remote protocols

The HMI operating stations and the Industrial Box PCs are integrated as Thin Clients and use the available network resources. Depending on the network architecture and access authority level, a remote connection can be established via the IP address to any Ethernet station. The firmware supports the Remote Desktop Protocol (RDP), Virtual Network Computing (VNC) and Keyboard Video Mouse over Internet Protocol (KVM over IP). The Thin Client can use the firmware to call up applications installed on the connected workstations or installed on virtual servers.



The illustration shows a redundant virtual network. It connects Thin Clients via an RDP, VNC or KVM-over-IP connection with workstations and servers. In such a

network, every Thin Client can access connected systems and call up applications from there.

2.2.2.1 RDP

The Remote Desktop Protocol (RDP) is a protocol for remote access. It can be used to display and control screen content of a remote workstation. RDP is an integral part of all Windows operating systems.

A special session is started on the server for the RDP access, and only the connected client can access this session.

The size of the displayed screen content is determined on the Thin Client's display size. If the screen content is only displayed on one half of the Thin Client it will be scaled accordingly.

A Windows server is required for several RDP connections to access one server. A client access licence is required for each client to access and connect to the Windows server. Licencing depends on the operating system of the server.

Either the computer name or the server IP address can be used for addressing.

If you want the option of redundant connections we recommend you use the DNS naming system.

2.2.2.2 VNC

Virtual Network Computing (VNC) is a platform-independent server system. VNC operates according to the Client-Server model.

The VNC service displays the screen content of a remote PC (server) on a local computer (client) The client sends the keyboard and mouse actions to the remote server. This way, the client can use the resources, applications and programs of the server.

The server's display size determines the size of the displayed screen content. If the server display screen ratio is different to that of the Thin Client, the screen content will be compressed or displayed with black edges.

VNC allows multiple access to the server. The display of the clients is then synchronised.

The VNC service must be installed on the remotely controlled PC (host). The Thin Client accesses the VNC server via a VNC viewer application. The installation and configuration of the VNC system on the server and the client requires administrator access authority. The VNC communication between server and client does not require this level of access authority.

VNC services are available from various providers. Depending on the VNC server, these systems have different functionalities.

For detailed information and a description of the VNC service, please refer to the documentation of the provider.

In order to be able to establish a VNC connection, the VNC server system must be activated on the host. The VNC service acquires the IP address needed for this connection from the settings of the PC's network connection. Depending on the configuration, the IP address is specified manually or allocated by a DHCP server. In the firmware's address book, this IP address is defined as the server IP of the VNC connection.

The way this connection is established depends on the settings of the VNC server and can either be

- a direct connection that is not password-protected
- a connection with VNC password
- a connection with Windows password

2.2.2.3 KVM over IP

KVM over IP provides remote access to keyboard-video-mouse systems (KVM). With these systems, a workstation is connected with keyboard, mouse and screen via an external KVM-over-IP box. The KVM-over-IP box is integrated into the network via an Ethernet interface. Data transmission is via the VNC protocol. A VNC service has been installed to establish the connection. The workstation that is part of the KVM system does not require a network connection or a software installation.

2.2.3 User roles

The access control system of the Remote firmware is based on three user roles. These are tiered in a hierarchy.

User role	Description
Operator (standard user)	The operator can switch between the displays of the connected systems and operate these systems remotely. The operator has access to the basic settings. He or she cannot make any changes to the firmware.
Engineer	The production engineer can set up, parametrise and delete remote connections. With the Pro licence, the engineer can add existing applications in the firmware. He or she cannot access the Windows user interface of the Thin Client. The engineer can adjust the following settings: • Displays • User Interface • Connections • Keyboard Wedge
Admin	The administrator has full access authority to the Windows user interface of the Thin Client. In addition to the options available to the production engineer, the administrator can install third-party applications and drivers on the Thin Client. He or she can configure the network, make system settings via the Remote HMI menu user interface and log into the regular Windows user interface as Admin. The following adjustments in the **Settings** can only be made by the administrator: • Maintenance • System & Proxy • Protection • Access Control • Import & Export • Update

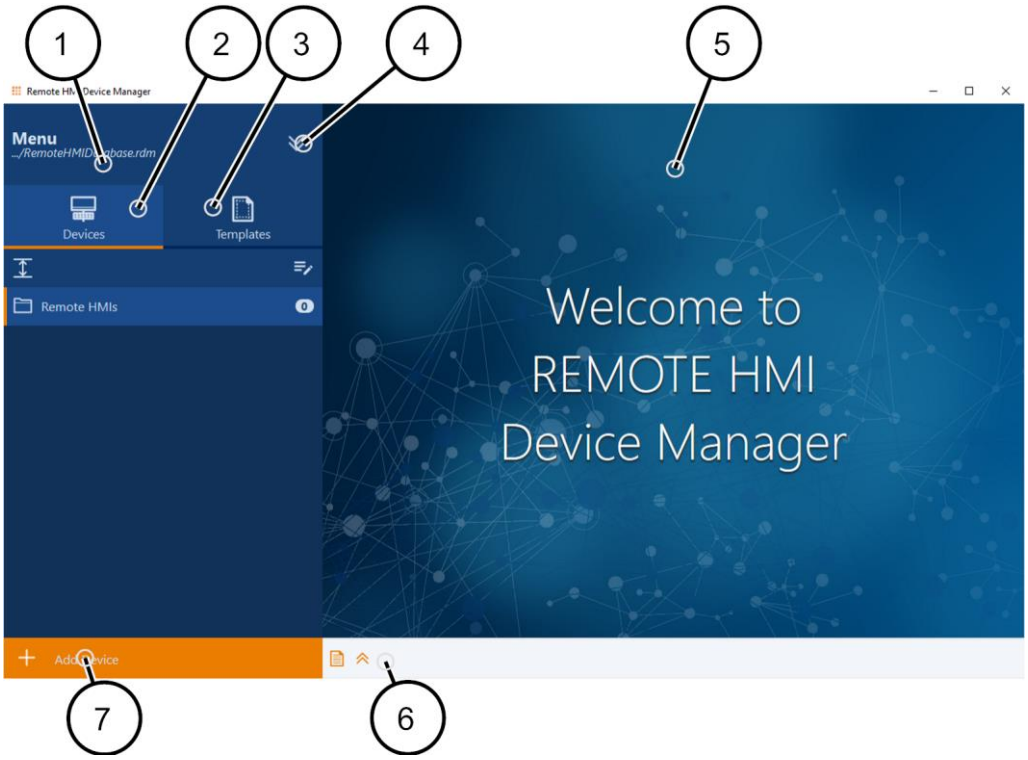
The Admin and Engineer user roles can be password-protected in the "Access Control" menu.

When the firmware is started up for the first time, the user roles are de-activated and the firmware starts with the Admin user role. Password protection is not active.

The Admin and Engineer user roles should only be given to staff familiar with Thin Client administration.

2.3 User interface

The software will start with the following screen.



1 Current database

2 Navigation element, change to main menu

3 Display Devices menu

4 Display Templates menu

5 Work area or preview

6 Call up event log

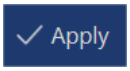
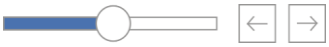
7 Button for adding devices

Navigation elements

	opens menu
	closes menu

Operating elements

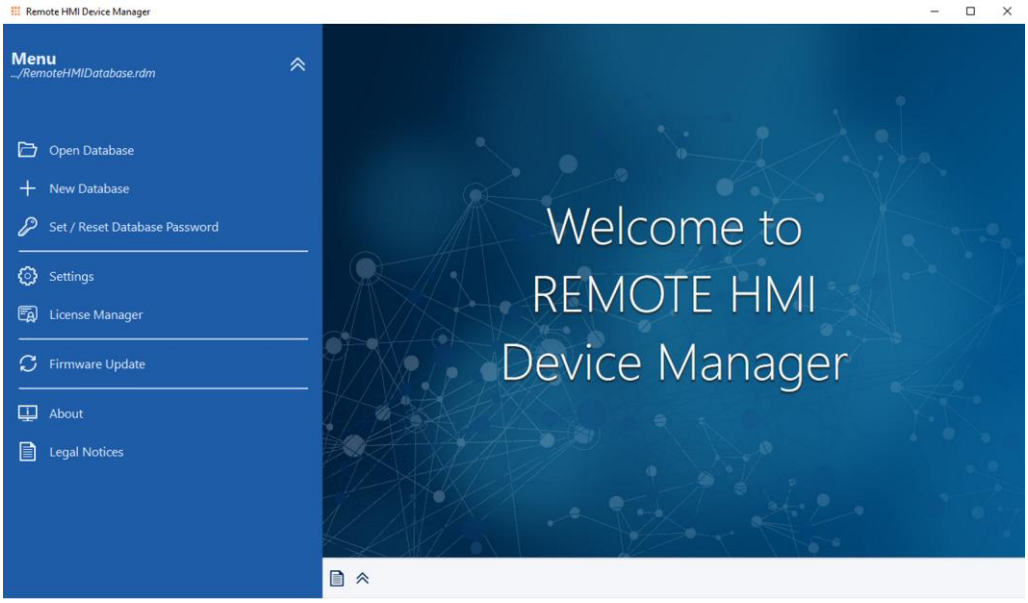
Operating elements vary depending on the menu.

Element	Meaning
	Switch activated
	Switch deactivated
	Button A greyed-out button is unavailable
	Input field
	Scroll bar
	Check box activated
	Check box deactivated

2.4 Menus

2.4.1 Main menu

Use the main menu to set up the software.



The main menu contains the following functions:

Menu entry	Description
Open Database	open existing database
New Database	create new database
Set / Reset Database Password	Set or reset password for the database
Settings	Open settings menu
License Manager	Open licence manager
Firmware Update	Update firmware

Menu entry	Description
About	Information on the Device Manager
Legal Notice	Information on the licence terms of the Device Manager

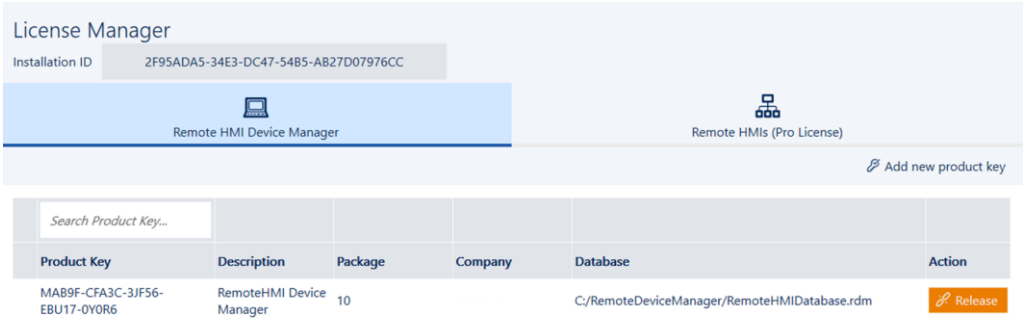
2.4.1.1 Databases

You can save the templates and the firmware configurations of the connected devices in databases. The software saves the data in RDM files (*name.rdm*). You can protect these files with a password.

2.4.1.2 Licence management

The **License Manager** menu contains two registers to manage the licences.

- **Remote HMI Device Manager** contains the number of management licences
- **Remote HMI (Pro License)** contains the number of Pro licences of the firmware



The structure of the lists and the editing options depend on the register.

Remote HMI Device Manager register

The list of package licences is made up of the following columns:

- **Product key** Package licence product key
- **Description** Licence description
- **Package** Number of licences
- **Company** Licence holder
- **Database** Database to which the licence has been allocated
- **Action** Editing options

You can search for product keys in the *Search Product Key* field.

Editing options in the Remote HMI Device Manager register	
Assign	assigns licence to the current database
Release	releases licences for the current database
Add product key	adds a product key

Register Remote HMI (Pro licence)

The list of devices consists of the following columns:

- **Name** Device name in the firmware
- **Type** Device type
- **Folder/Group** Folder of the device menu to which the Thin Client was added

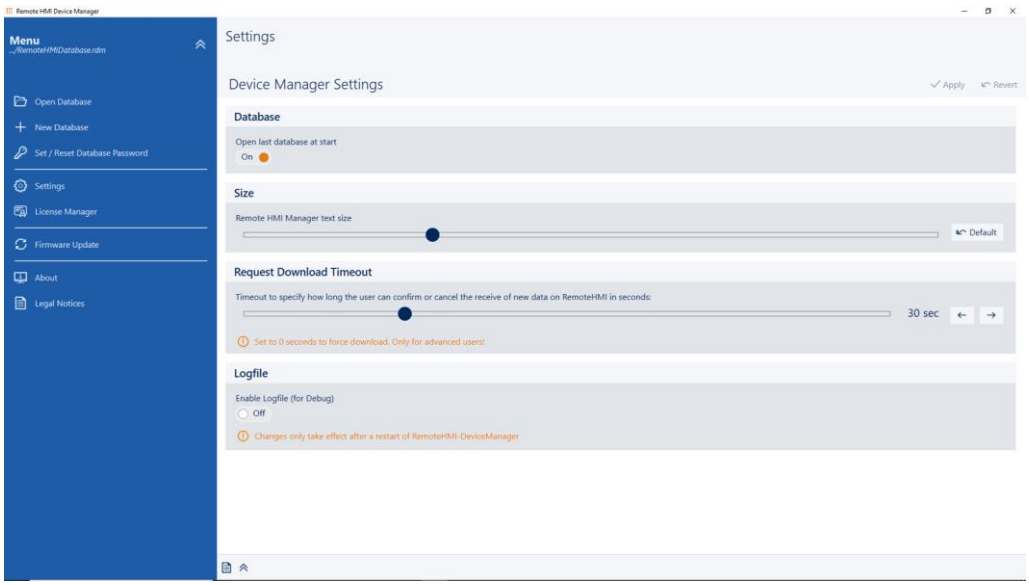
- **Installation ID**
- **Pro License Status** Licence status;
  if an action is carried out, a progress bar will appear in this field
- **Action** Editing option

You can search for device names in the *Search* to search for device names. You can narrow down the search by filtering with the **Type** or **Folder/Group** columns.

Editing in the Remote HMI (Pro Licence) register	
Get License Status	calls up the firmware licence status of the device
Add product key	adds a product key

2.4.1.3 Software-Settings

Use the **Settings** menu to set up the software.

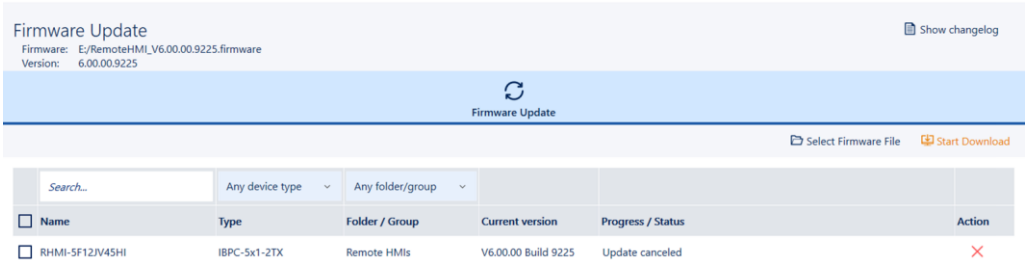


Functions in the Settings menu

Database	specifies how the database reacts during start-up
Size	specifies the text and element size of the user interface
Request Download Timeout	specifies the reaction time (timeout) for the user to confirm or reject the acceptance of the device data. • 0 seconds; confirmation by user not possible (force download) • 1 to 120 seconds
Logfile	activates the debugging log function (logfile)

2.4.1.4 Firmware Updates

Go to the **Firmware Updates** menu for a list of available devices and to initiate a firmware update.



The list consists of the following columns:

- **Name** Thin Client name in the firmware
- **Type** Thin Client type
- **Folder/Group** Folder of the device menu to which the Thin Client was added
- **Current version** Firmware release information
- **Progress / Status** Licence status (none, Pro); if an action has been activated, a progress bar will be shown
- **Action** Editing options

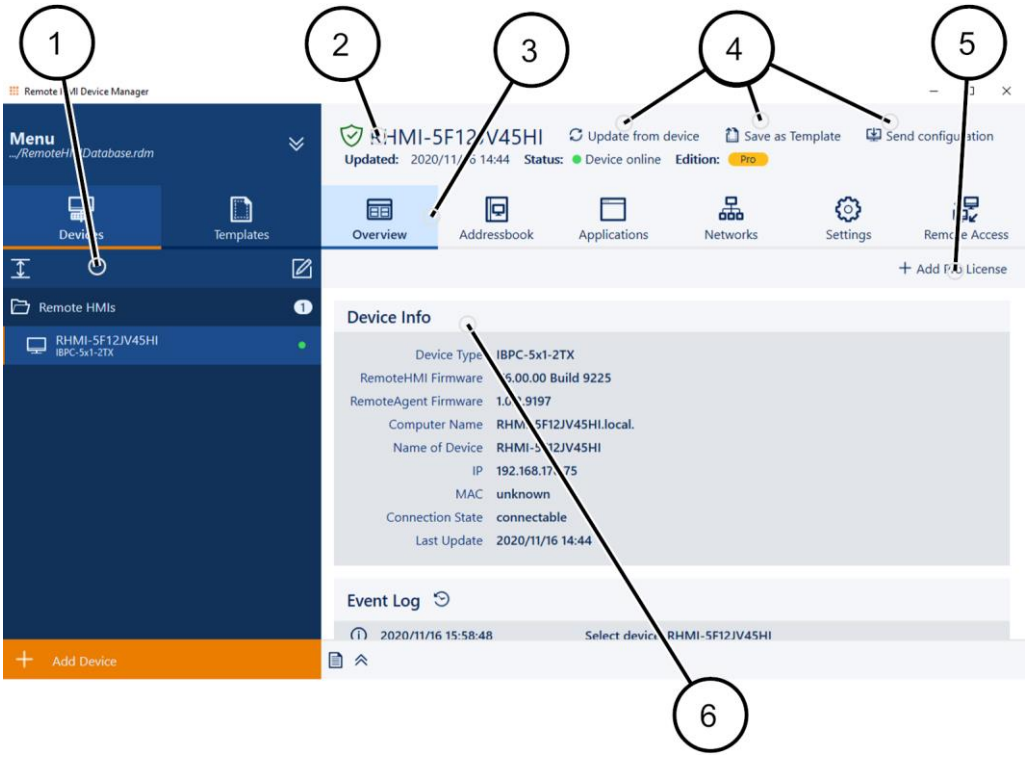
Use the *Search* to search for device names. You can narrow down the search by filtering with the **Type** or **Folder/Group** columns.

Options in the Firmware Updates menu	
Select Firmware File	opens the search window
Start Download	downloads the firmware update to the Thin Client
Show changelog	shows the change log

For an update to be carried out successfully, the UWF filter must be deactivated in the firmware.

2.4.2 Devices menu

Go to the **Devices** menu to add devices to a database and edit them. You can manage address book and applications for each device.



1 Menu functions

2 Device information

3 Register bar

4 Register functions

5 Button for adding a licence

6 Device data, imported from device

Functions in the Devices menu

The devices are listed and managed in folders. The menu contains the following elements:

1 **Edit mode** Open edit mode

2 Number of devices in folder

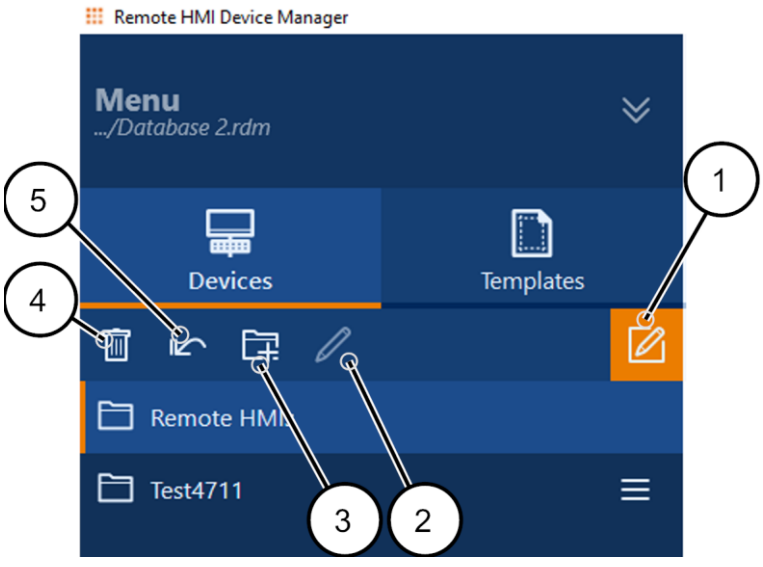
3 Status of connection to device

4 **Add Device** Adding a device

5 Expand or collapse folder

Edit mode

You have the following options in the edit mode:



1 **Edit mode** Open edit mode

2 **Rename selected item**

3 **Add folder** Adding a folder

4 **Revert all** revert all entries

5 **Delete selected item**

Status of connection to device

Symbol	Meaning
	connected
	unavailable, no response to ping request
	available, not connected

Register functions

The software supports the import and transmission of the firmware configuration and the storage of entries in the **Address Book** and **Applications** registers as templates.

You have the following options:

Update from device	Import the settings of the selected Thin Client
Save as Template	Save settings as template
Send configuration	Transmit configuration to Thin Client

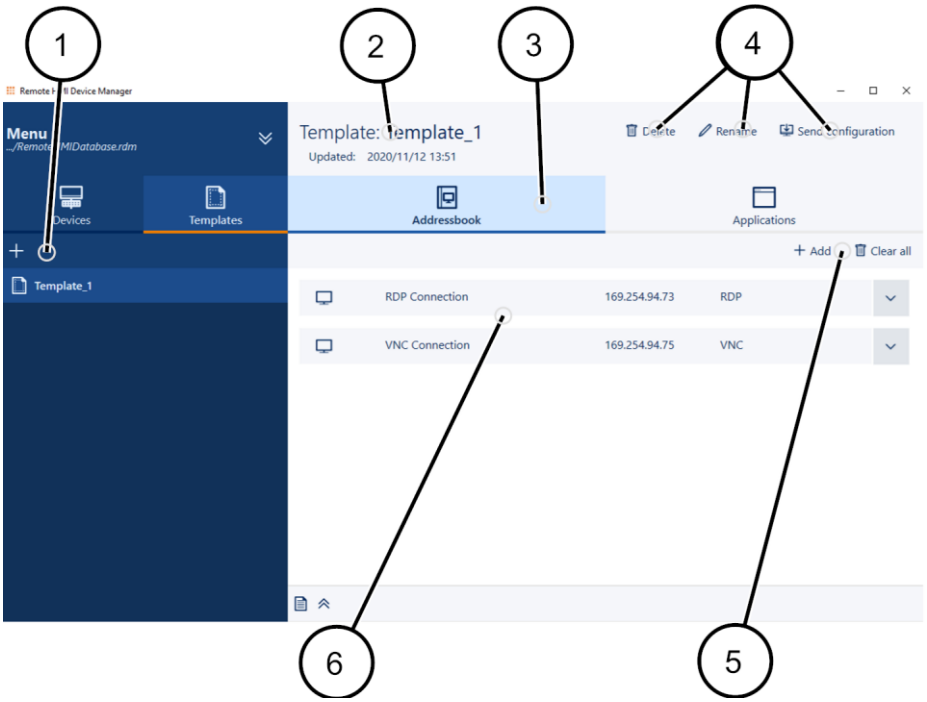
Register

The register bar contains the following functions:

Register	Description
Overview	Overview of system and connection information, display of event log for device
Address Book	Diagnosis and management of remote connections
Applications	Display and management of applications
Networks	Display and set-up of the network adapters only available with remote access
Settings	Menus for display and set-up of system, security and network parameters only available with remote access

2.4.3 Templates menu

Use the **Templates** menu to save address book entries and applications as templates, edit and send them to a device.



1 Menu functions
2 Template information
3 Register bar
4 Register functions
5 Functions for editing the entries
6 Register entries (here: address book entries, i.e. remote connections)

The **Templates** menu consists of two registers.

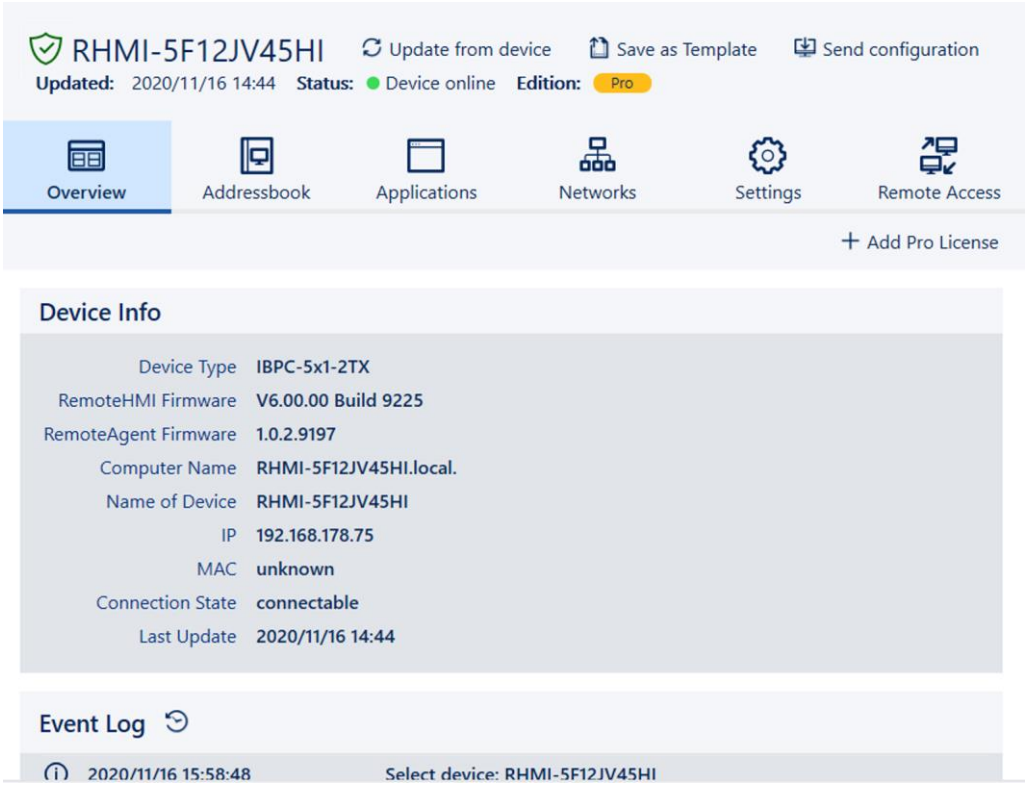
- **Address book** (see Address book)
- **Applications** (see App management)

Functions in the Templates menu	
+ Add New Template	
When a template has been opened, you have the following options:	
Delete	
Rename	
Send configuration	to Thin Client

2.5 Register

2.5.1 Overview

The **Overview** register shows the current device data and the last actions in the event log.

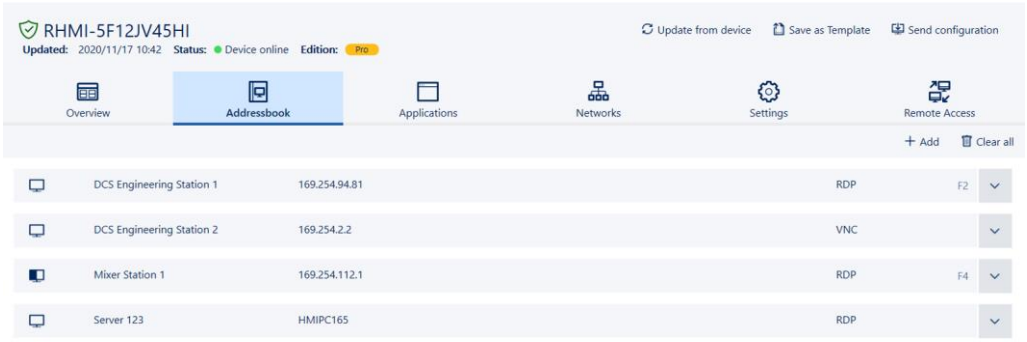


2.5.2 Address book

Use the **Address Book** register to call up or manage configured remote connections or create new remote connections.

2.5.2.1 Address book options

The **Address Book** register lists all configured remote connections.



Register functions

The software supports the import and transmission of the firmware configuration and the storage of entries in the **Address Book** and **Applications** registers as templates.

You have the following options:

Update from device	Import the settings of the selected Thin Client
Save as Template	Save settings as template
Send configuration	Transmit configuration to Thin Client

Navigation elements

⌄	opens an item in the list
⌃	closes an item in the list

Address book functions

The available edit functions or buttons depend on the sub-menu.

+ Add	Add	Adds a new entry.
Clear all	Clear all	Deletes all entries in the list
Edit	Edit	Opens the highlighted entry for editing
Copy	Copy	Copies the highlighted entry and opens the copy for editing
Delete	Delete	Deletes the highlighted entry
Manage	Manage	Navigates back to the list level
Apply	Apply	Applies input
Revert	Revert	Rejects input
↑	Up	Moves the highlighted entry one place up in the list
↓	Down	Moves the highlighted entry one place down in the list
Edit Profile	Edit profile	Opens the dialogue for editing the remote profile

Hotkey for calling up remote connections

You can call up the remote connection via the keyboard if you have specified a hotkey under the **Hotkey** function. Three keys can be specified.

First key	Second key	Third key
[Shift]	[Ctrl]	none
[Ctrl]	[Alt]	[F1] ... [F12]

The Ctrl key must not be selected twice.

2.5.2.2 Notes on the firmware

The menus and operating elements look different in the firmware and in the software. Menu items with identical names have identical functionality.

If a connection in the address book is greyed out, the user's authority level is too low to access it.

Status of the remote connection

Symbol	Meaning
	connected
	not connected
	connection not possible
	default, will be connected automatically during start-up
	connected, parallel remote connection, active in the background (multi-session connections require a Pro licence)

Pro The simultaneous use of multiple remote connections (multi-session connection) requires the Pro licence and must be activated in the **Connections** menu.

If the parallel use of several remote connections has been activated, the connections will be displayed as follows:

2.5.3 App management

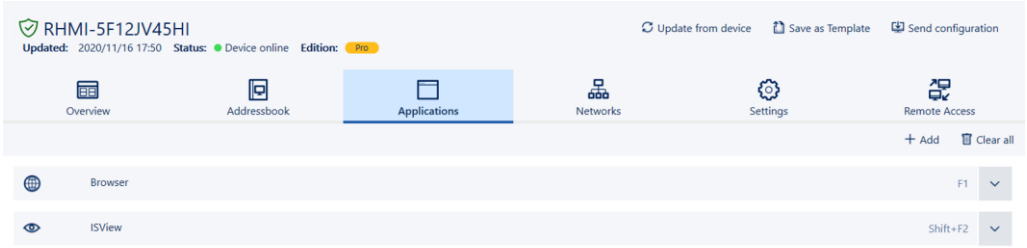
Pro Requires a Pro licence.

Use the **Applications** register to add and manage links to Windows tools and applications, virus protection software or EXE applications such as the Citrix Receiver. You can configure the display and behaviour of an app with various settings, and manage access via the user roles.

Before you can add an app you need to install it on the Thin Client. The Thin Client has to meet the system requirements of the app.

2.5.3.1 Options in the Applications register

The **Applications** register shows the connected Apps.



Register functions

The software supports the import and transmission of the firmware configuration and the storage of entries in the **Address Book** and **Applications** registers as templates.

You have the following options:

Update from device	Import the settings of the selected Thin Client
Save as Template	Save settings as template
Send configuration	Transmit configuration to Thin Client

Navigation elements

⌄	opens an item in the list
⌃	closes an item in the list

Functions in the Applications register

The available edit functions or buttons depend on the sub-menu.

+ Add	Add	Adds a new entry.
Clear all	Clear all	Deletes all entries in the list
Edit	Edit	Opens the highlighted entry for editing
Copy	Copy	Copies the highlighted entry and opens the copy for editing
Delete	Delete	Deletes the highlighted entry
Manage	Manage	Navigates back to the list level
Apply	Apply	Applies input
Revert	Revert	Rejects input
↑	Up	Moves the highlighted entry one place up in the list
↓	Down	Moves the highlighted entry one place down in the list
Terminate	Terminate	only available with remote access Forces the shut-down of an open application with possible loss of data
Select File	Select file	only available with remote access Opens the selection window for executable files

Hotkey for starting applications

An application can be selected via the keyboard if a hotkey has been created under the **Hotkey** menu item. Three keys can be specified.

First key	Second key	Third key
[Shift]	[Ctrl]	none
[Ctrl]	[Alt]	[F1] ... [F12]

The Ctrl key must not be selected twice.

Each hotkey can only be allocated once.

Command line parameters

You can define a command line parameter for each app that allocate application-specific parameters.

Example:
In the browser, the `-k www.stahl.de` parameter entry calls up the website www.stahl.de in the kiosk mode.

Please refer to the description of each application for information on permitted command line parameters.

Application privilege level

Level	Meaning
Run as standard user	Starts the application with standard user authority
Run as administrator user	Starts the application with Administrator authority You can define name and password for the Admin account in the **System & Proxy** menu.
Run elevated	Starts the application with extended Administrator authority You can define name and password for the Admin account in the **System & Proxy** menu.

2.5.3.2 Notes on the firmware

The menus and operating elements look different in the firmware and in the software. Menu items with identical names have identical functionality.

Symbols in the list of apps

You can freely chose the icons representing the apps in the list. In the interest of user-friendliness we recommend you use commonly used symbols.

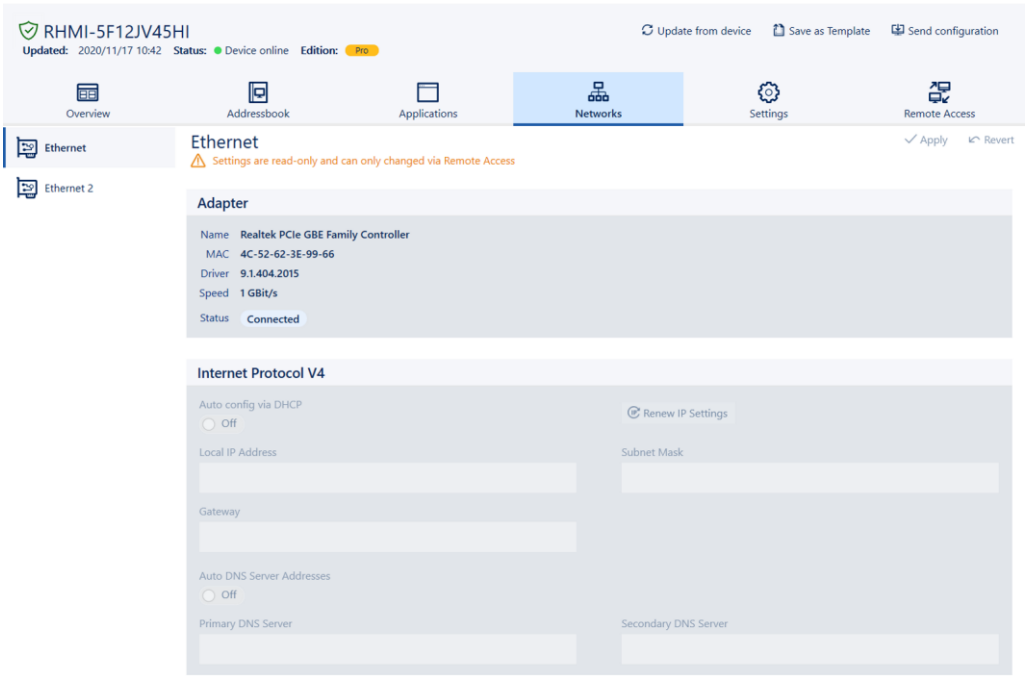
Symbols
 A selection of icons standing for different types of app.
 Engineer, Admin: Defines who is authorised to start the app. If no symbol is shown all user roles are authorised to start the app.
 default, will be connected automatically during start-up

2.5.4 Network

Read only
The settings can only be changed remotely (see Remote access to a device).

Use the **Networks** register to configure the Thin Client for incorporation in the network.

The number and designation of available Ethernet adapters depend on the Thin Client's hardware.



2.5.4.1 Options in the Networks register

Settings on the Windows network level can have an impact on the entire network. Only click on the **Advanced** if you know your way around Windows network settings. If not, ask your network administrator for help.

Buttons in the Networks register

Advanced	Advanced functions	Opens the Windows network settings
Apply	Apply	Applies input
Revert	Revert	Rejects input
Create/Remove Team	Create/remove team	Opens the teaming function dialogue
Renew IP Settings	Renew IP settings	Requests renewed IP configuration from the DHCP server

2.5.4.2 Adapter information

The **Adapter** section lists information on the chosen Ethernet adapter.

Name	Name of the Ethernet adapter
MAC	MAC address of the Ethernet adapter
Driver	Version of the adapter driver
Speed	Speed of the Ethernet connection
Status	Status of Ethernet connection

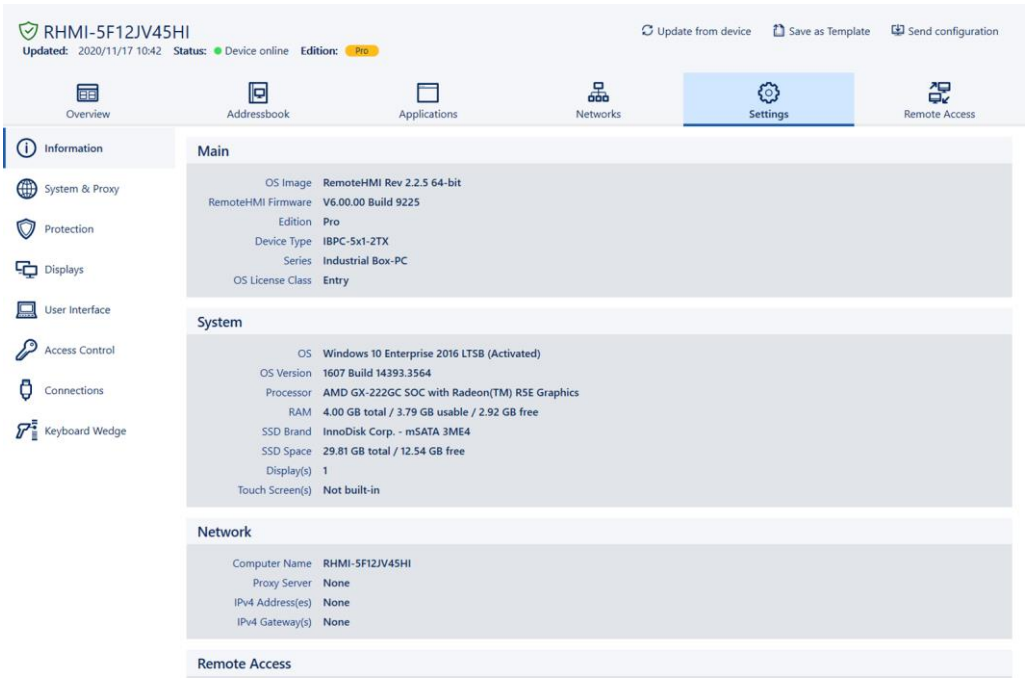
2.5.5 Settings

Read only

The settings can only be changed remotely (see Remote access to a device).

The **Settings** register contains many functions with which the Engineer or Admin can configure the firmware.

2.5.5.1 Options in the Settings register



The **Settings** register contains the following menus:

Menu	Contents	Authorised user
Information	Current system data, settings and configurations The menu contents vary depending on the device platform.	
Maintenance	Functions required for the maintenance of the Thin Client. Allows addition of third-party software and drivers. Activation of Pro licence and Windows LTSB	Admin
System & Proxy	Settings concerning device name (in the network) and proxy server	Engineer / Admin
Protection	Settings concerning system security	Engineer / Admin
Displays	Settings for up to 6 displays	Engineer / Admin
User Interface	Behaviour of RemoteHMI menu	Admin
Access Control	Setting up of protected user roles	Admin
Connections	Settings of connection options	Engineer / Admin
Keyboard Wedge	Setting up the COM interfaces for external scanners or readers	Engineer / Admin
Import & Export	Functions for the export and import of the device configuration	Engineer / Admin

Menu	Contents	Authorised user
Updates	Firmware updates	Admin
Legal Notice	Information on licence terms and conditions for the software used on the Thin Client	

2.5.5.2 Display of system information

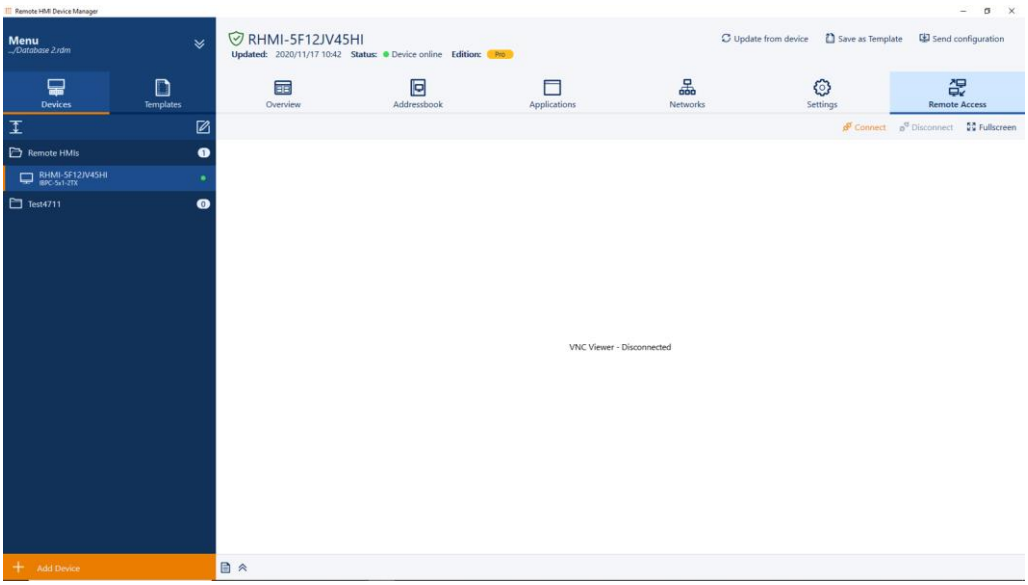
The **Information** menu lists the current system data, settings and configurations. The menu contents vary depending on the device platform.

Menu	Contents
Main	Essential system information, OS image and firmware version
System	Information on hardware and operating system This varies depending on the device type.
Network	Information on computer name and addresses of the proxy server, the device and the gateway
Remote Access	Information on the status of the remote connections
Protection	Up-to-date information on system security
Submodules	List of sub-module versions

2.5.6 Remote Access

The settings in the **Settings** and **Networks** firmware registers can only be changed via remote access.

The remote access must be permitted in the firmware under **System & Proxy** . Depending on the settings a password might be required.



3 Licence management

Opening the main menu

1. Click on ⌄⌄ to open the main menu.

Adding a software licence

1. Open the **License Manager** menu.
2. In the **Remote HMI Device Manager** menu, click on **Add new product key**.
   - ➢ The system will open the activation dialogue.

Adding a firmware licence

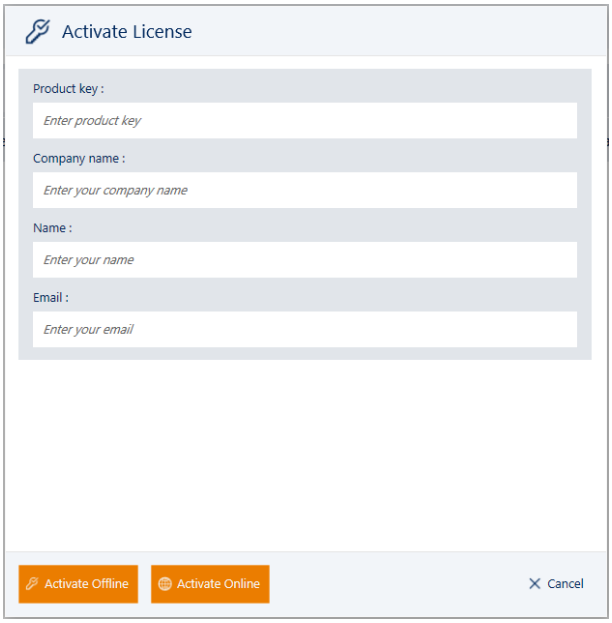
1. Open the **License Manager** menu.
2. In the **Remote HMIs (Pro License)** register, click on **Get License Status**.
   - ➢ The list shows the installation ID and the licence status.
3. In the **Remote HMI Device Manager** register, click on **Add product key**, if you want to activate a Pro licence.
   - ➢ The system will open the activation dialogue.

Adding a firmware licence in the Devices menu

1. Mark the device in the **Devices** menu.
2. Click on **Add Pro License**, if you want to activate a Pro licence.
   - ➢ The system will open the activation dialogue.

Carrying out the activation dialogue

Pro If the PC has internet access, you can activate the Pro Licence online via the software.
If not, you need to request the activation code from remotehmi-licensing.stahl.de .



3. Under **Product key** , enter the licence key you received.
4. Under **Company Name** , enter your company name.
5. Under **Name** , enter the name of the licence holder.
6. Under **Email Address** , enter the e-mail address of the licence holder.
7. Click on **Activate Online** to activate the licence online.
   Click on **Activate Offline** to activate the licence offline.

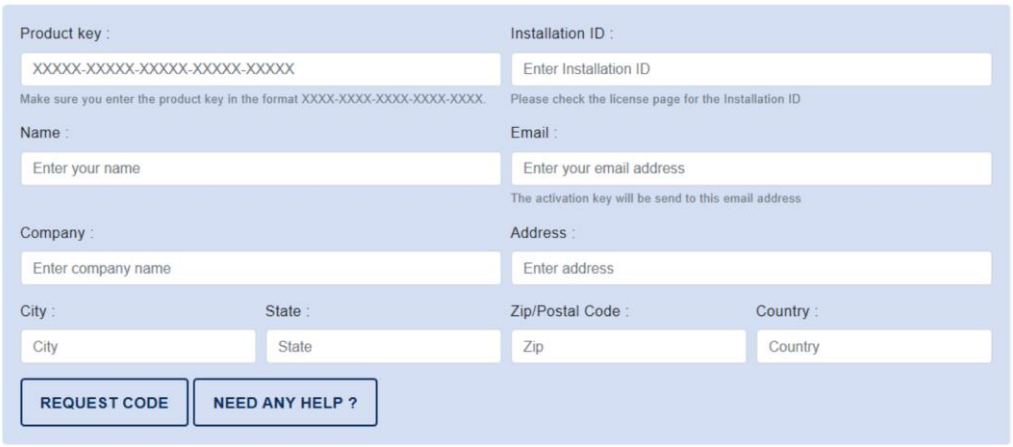
Activating the licence online via internet access

1. Make sure the PC has internet access.
2. Click on **Activate Online**.
   - ➢ The system will start the activation process.
     If the activation has been successful, the system will issue a corresponding message, and the licence key will be shown in the list.

Activating the licence offline

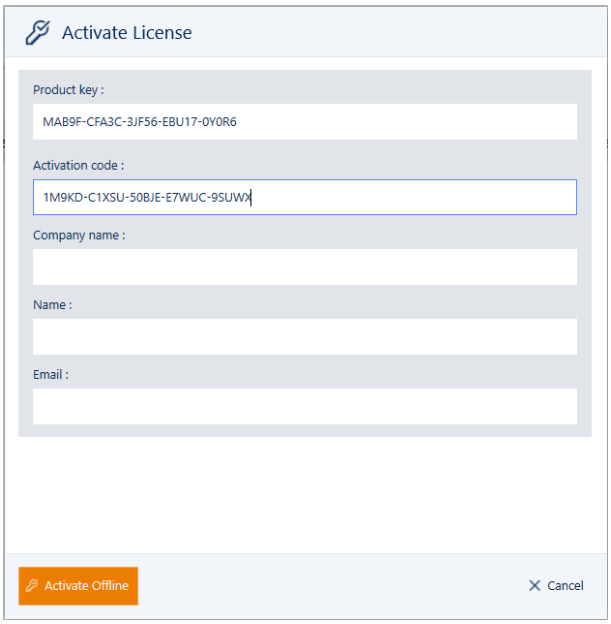
In order to activate the licence you will need the installation ID and the product key (licence key). You will also need a device with internet access.

1. In the browser, go to the following website: remotehmi-licensing.stahl.de.
2. Select "License Activation".
3. Fill in the form and request the activation code.



You will receive an e-mail with the activation code to the e-mail address specified in the form. This may take up to five minutes. If you receive no such e-mail, please check your spam folder.

4. In the **Activate License** window, click on **Activate Offline**.



5. Under **Product key**, enter the product key.
6. Under **Activation Code**, enter the activation code you were given.
7. Under **Company Name**, enter your company name.
8. Under **Name** , enter the name of the licence holder.
9. Under **Email Address** , enter the e-mail address of the licence holder.
10. Click on **Activate Offline**.
    - ➢ The system will start the activation process.
      If the activation has been successful, the system will issue a corresponding message, and the licence key will be shown in the list.

4 Adding and managing devices

Adding a device

1. Open **Devices**.
2. Click on **Add Device** to open the search window.
3. Click on **Start Scan**.
   - ➢ The network will be searched for available devices. The title bar will show the number of available and new devices.
   - ➢ If all devices have already been added, the list of search results will be empty.
4. Select the device you want from the search results.
5. Confirm your selection.
   - ✓ The device will be added to the list.

Open edit mode

1. Open **Devices**.
2. Click on **Edit mode** to open the edit mode.
3. Highlight the entry and click on **Rename selected item** to rename the device or the folder.
4. Highlight the entry and click on **Delete selected item** to delete the device or the folder.
5. Click on **Add folder** to add a folder.
6. Click on **Revert all** to revert all entries.

Adding a folder

1. Open **Devices**.
2. Activate the edit mode.
3. Click on **Add Folder**.
4. Enter a name and confirm the entry.
   - ✓ The folder will be added.

Reading device data (Update from Device)

Reading the device data will overwrite the current software settings.

1. Open **Devices**.
2. Highlight a device.
3. Click on **Device section**.
4. Confirm with **Yes**.
   - ✓ The system will adopt the configuration and issue a message.

Creating a template of a device

1. Open **Devices**.
2. Highlight a device.
3. Click on **Save as Template**.
   - ➢ The **Save as Template** window will pop up.
4. Enter a name and confirm the entry.
   - ✓ The template will be saved.

Sending a configuration to the device

1. Open **Devices**.
2. Highlight a device.

3. Click on **Send configuration**.
   - ➢ The **Download to device** window will pop up.

Use the **Force Download** function to force the download of all changes. It is not possible for the Thin Client user to abort the download.

4. Activate **Force Download** if you want to force the download.
5. Click on **Start download**.
   - ➢ A progress bar shows how the data transfer is progressing.
   - ➢ If you want to abort the transfer, click on **Cancel**.
   - ✓ The system will issue a message.

5 Set-up of remote connections

5.1 Notes on settings options

Automatic logon at the server

The automatic logon at the server can be configured in the settings of the remote connection. For this you need the user ID and the password for the server.

Only users with authority for remote access to the server can log on to the server. Check the user authority at the server or the KVM box.

Display position of the server screen

Different parts of the server screen can be displayed. You can configure the display via **Show on** when creating the remote connection.

The following display options are available:

Symbol	Name	Meaning
	Full display	shows the full screen
	Left display half	Scales the remote screen content and displays it on the left hand side
	Right display half	Scales the remote screen content and displays it on the right hand side
	Upper display half	Scales the remote screen content and displays it at the top half
	Lower display half	Scales the remote screen content and displays it at the bottom half.

Behaviour of firmware when connection is lost

You can configure how the remote connection behaves during a system startup or when it is lost, as follows:

Auto connect on system startup	On	Automatically establishes a connection during system startup, is represented by the ☆ symbol in the address book entry
	Off	During a system startup the dial-up must be started manually
Auto reconnect on connection loss	On	Automatically reconnects after the connection has been lost
	Off	After the connection has been lost, the dial-up must be started automatically

5.2 Set-up of RDP connections

You will need the IP address or the name of the server for the configuration. These are stored in the system properties of the server.

For RDP connections, remote access must be explicitly permitted in the server's system properties. The remote access must be configured for the user.

1. Open the **Address Book** register.
2. Click on **+ Add**.
   - ➢ A new address book entry is created.

3. Click on **Edit**.
4. In **Connection Settings**, via the drop-down field **Type**, select "RDP".
5. Under **Name**, enter the name of the connection.
6. Under **Server Address**, enter the IP address or the name of the server.

To ensure automatic access to the connected server you have to enter the correct logon data. Please note that a domain name may have to be used together with the user name.

7. Under **User Name** and **Password**, enter the logon data of the server.
8. If you want to be able to call up the remote connection via the keyboard, use **Hotkey** to specify a hotkey.
9. Click on **Show on** to select the display option.
10. Specify the minimum user role required for the manual set-up of the connection.

If a user does not have the required authority to set up the connection, this connection is greyed out in the address book.

11. Click on **Apply** to set up the connection.
    - ✓ The connection is shown in the address book.

5.3 Set-up of the VNC connection.

The VNC software must be installed on the Thin Client and the server, requiring Administrator authority on both.

To set up the connection you require the IP address of the VNC server and, depending on the configuration, the VNC password.

If the port number of the VNC server is different from the standard port, the IP address needs to be extended to include the port number, for example: 192.168.1.23:5901

1. Open the **Address Book** register.
2. Click on **+Add**.
    - ➢ A new address book entry is created.
3. Click on **Edit**.
4. In the **Connection Settings**, select "VNC" from the **Type** drop-down field.
5. Under **Name**, enter the name of the connection.
6. Under **Server Address**, enter the IP address of the server.

To ensure automatic access to the connected server you have to enter the correct logon data.

7. Enter the logon data of the server.
8. If you want to be able to call up the remote connection via the keyboard, use **Hotkey** to specify a hotkey.
9. Under **Show on**, select the display option.
10. Specify the minimum user role required for the manual set-up of the connection.

If a user does not have the required authority to set up the connection, this connection is greyed out in the address book.

11. Click on **Apply** to set up the connection.
    - ✓ The connection is shown in the address book.

5.4 Preparation of host for VNC connection

The process varies according to which VNC service is used. For more information, please refer to the documentation provided by the VNC service manufacturer.

This process requires Administrator authority.

1. Make sure that the Thin Client can contact the host. If both are part of the same network, this will be the case.
2. Make sure the VNC service is installed and activated on the host (see Activating VNC server system on the host).
3. If the network connection is protected via a firewall you need to configure this firewall. Permit network communication via the port where the VNC service is ready to receive (5900 as a standard).
4. If the network connection is protected via a router, you need to configure this router. For the transfer of network communication, specify every configured port where the VNC service is ready to receive (5900 as a standard).
5. Check whether the VNC service is working properly and whether it accepts incoming connections.
   ✓ The host is ready.

5.5 Preparation of Thin Client for the VNC connection

The process varies according to which VNC service is used. For more information, please refer to the documentation provided by the VNC service manufacturer.

This process requires Administrator authority.

1. Make sure that the Thin Client can contact the host. If both are part of the same network, this will be the case.
2. If the VNC connection of the Thin Client is protected via a proxy server you have to specify the proxy server in the VNC viewer.
   ✓ The Thin Client is ready

5.6 Test of remote connection

This test can only be conducted via remote access to the Thin Client.

6 Managing remote connections

In order to be able to edit the settings, the connection must be inactive.

Moving connections in the list

1. Open the entry in the **Address Book** register with ⌵.
2. Click on ↑ to move the entry up one place in the list.
3. Click on ↓ to move the entry down one place in the list.
   ✓ The connection is moved in the list.

Editing connection settings

1. Deactivate the connection in the **Address Book** register.
2. Open the entry.
3. Click on **Edit** to edit the settings.
4. Change the settings as required.
5. Click on **Apply** to accept the changes.
   Click on **Revert** to reject the changes.
6. Click on **Manage** to edit the list.
   Click on [⌵] to close the entry and return to the list.

Deleting a connection

1. Deactivate the connection in the **Address Book** register.
2. Open the connection.
3. Click on **Delete** to delete the connection.
4. Confirm the security message.
   ✓ The connection is deleted.

Copying a connection

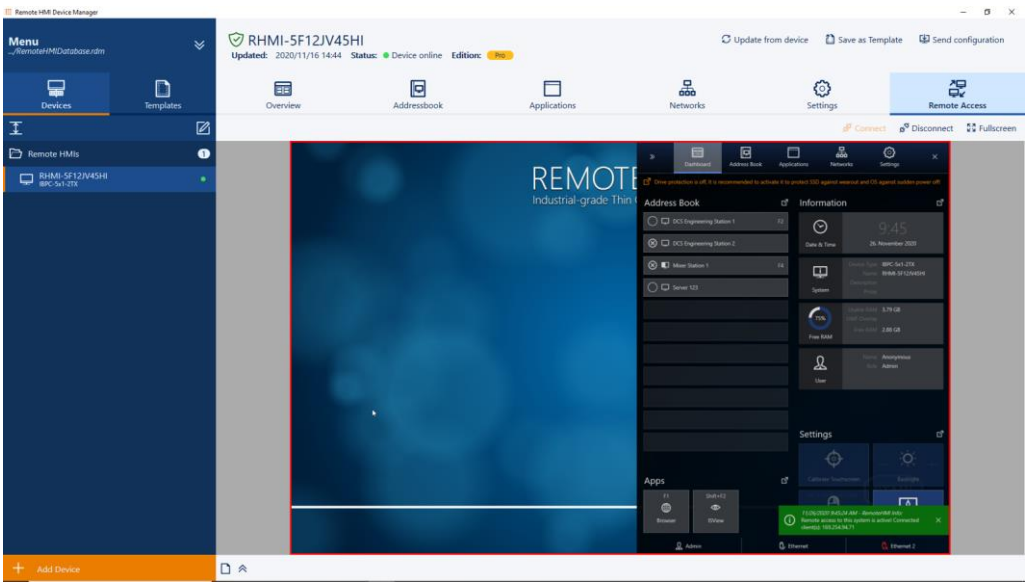
1. Deactivate the connection in the **Address Book**.
2. Open the entry.
3. Click on **Copy** to copy the settings.
   ➢ A new entry is created.
4. Open the entry and edit the settings as required.
5. Click on **Apply** to accept the changes.
   Click on **Revert** to reject the changes.
6. Click on **Manage** to edit the list.
   Click on [⌵] to close the entry and return to the list.

7 Remote access to a device

The remote access must be permitted in the firmware under **System & Proxy** . Depending on the settings a password might be required.

Connecting to the device

1. Under **Devices**, select the device you want to access remotely.
   - ➢ The device configuration will pop up.
2. Select the **Remote Access** register.
3. Click on **Connect** to connect to the Thin Client.
   - ➢ Once the connection has been established, a preview of the screen content of the Thin Client will pop up.



4. Click on **Fullscreen** to switch to full screen mode.

Please also refer to the notes and instructions of the firmware manual.

Disconnecting the remote connection

1. Click on **Disconnect** to actively disconnect the connection.
2. On exiting the **Remote Access** register, the connection will be disconnected.

8 Adding apps

Pro Requires a Pro licence.

Compatibility with third-party software

The firmware is qualified for software that is included in the delivery of the supported HMI devices. R. STAHL HMI Systems GmbH does not accept any liability for the functionality of the software of any other providers. Before installing software of other providers make sure it is compatible.

Checking system requirements and ability to run of the application

1. Make sure that the application is compatible.
2. Check whether the system requirements are met.
3. Check whether the application can be installed on the Thin Client. This is done in the Admin role.
4. Check whether the application works smoothly.
   ✓ If all conditions have been met, the application is compatible and able to run.

Adding an app

1. Open the **Applications**.
2. Click on **+Add**.
   ➢ A new entry is created.
3. Open the entry.
4. Go to **Icon**, select a suitable symbol from the drop-down field.
5. Activate **Autostart** if you want the application to start automatically.
6. Under **Name**, enter the name of the application.
7. If you want to be able to call up the remote connection via the keyboard, use **Hotkey** to specify a hotkey.
8. Enter the file path to the program file on the Thin Client in the **Path** field.
9. If you want to define application-specific parameters, click on **Parameters** to enter a command line parameter. For information on possible parameters please refer to the manual of the application.
10. Under **Application privilege level** to specify how the application should be started.
11. Activate **Close RemoteHMI menu on app start** if you wish to close the firmware when starting the application.

If the application requires Administrator or extended authority, you can store the login data for the Administrator account under **Use predefined admin login credentials**. You then no longer need to enter the login data when starting the app.

12. Activate **Use predefined admin login credentials** if you want to start the application via the login data of the Thin Client. Enter the user name and the password.
13. Click on **Min user role required to start app manually** to define the lowest required user authority level for starting the application.

If the user is not authorised to start the application manually, it will be greyed out in the Applications register.

14. Click on **Apply** to accept the input.

- The application will be displayed on the dashboard and in the Applications register.

15. Click on **Manage** to move the app in the list.
    Click on [⌃] to close the entry and return to the list.
16. Check whether the app opens correctly when clicking on the entry.

9 Managing apps

Moving an application in the list

1. In the **Applications** register, open the entry you want by clicking on ⌵.
2. Click on ↑ to move the entry up one place in the list.
3. Click on ↓ to move the entry down one place in the list.

Changing application settings

1. Open the entry you want in the **Applications** register.
2. Click on **Edit** to edit the settings.
3. Make the required changes.
4. Click on **Apply** to accept the changes.
   Click on **Revert** to reject the changes.
5. Click on **Manage** to edit the list.

Copying an application

1. Check the compatibility and ability to run of the application before creating a link to a new application (see "Adding apps")
2. Open the **Applications** register.
3. Open the entry you want to copy.
4. Click on **Copy** to copy the application's settings.
   ➢ A new entry is created.
5. Click on **Select File** and select the program in Windows Explorer.
6. Open the entry and change its settings as described under Adding apps.
7. Click on **Apply** to apply the changes.
   Click on **Revert** to reject the changes.
8. Click on **Manage** to move the app in the list.
   Click on [⌵] to close the entry and return to the list.

Closing an application

In general, you should shut down applications properly to prevent any data loss. If you cannot shut down an application in the normal way you can force its termination.

1. Open the entry you want in the **Applications** register.
2. Click on **Terminate** to force the termination of the application.
3. Confirm the security message.
   ✓ The application is shut down.

Deleting the link to the application

The **Delete** button only deletes the link to the application and does not de-install the application.

You can only de-install the program in the Windows user interface.

1. Open the entry you want in the **Applications** register.
2. Click on **Delete** to delete the link.
3. Confirm the security message.
   ✓ The link to the app is deleted.

10 Creating and managing templates

Creating templates

1. Open **Templates**.
2. Click on **Add new Template**.
3. Enter a name and confirm the entry.
   ✓ The template will be added.

Editing templates

1. Open **Templates**.
2. Select the template you wish to edit.
   ✓ The template will be opened for editing.

Transferring template to device

1. Open **Templates**.
2. Click on **Send configuration**.
   ➢ The **Send configuration to device** dialogue will pop up.
3. Select the device to which you want to transfer the template.

Use the **Force Download** function to force the download of all changes. It is not possible for the Thin Client user to abort the download.

4. Activate **Force Download** if you want to force the download.
5. Click on **Start transfer**.
   ➢ A progress bar shows how the data transfer is progressing.
   ➢ If you want to abort the transfer, click on **Cancel**.
   ✓ The system will issue a message.

11 Creating and editing databases

You can save the templates and the firmware configurations of the connected devices in databases. The software saves the data in RDM files (*name.rdm*). You can protect these files with a password.

Opening the main menu

1. Click on ⌄⌄ to open the main menu.

Creating a database

1. Click on **New Database** to create a new database.
2. Enter a name.
3. Click on **Browse** to select a folder in which you want to save the database and confirm your selection.
4. Click on **Create database**.
   ✓ The new database will be opened.

Opening a database

1. Click on **Open Database** to open an existing database.
2. Click on "Browse" to select a database and confirm your selection.
3. Click on **Open**.
   ✓ The new database will be opened.

Creating or changing a password

The current database can be password-protected.

1. Click on **Set / Reset Database password**.
2. Enter a password (min. 5 characters long) and confirm.
   ✓ The next time you open the database you will be asked to enter the password.

Deleting a password

1. Click on **Set / Reset Database password**.
2. Click on **Reset Password** to remove an existing password.
   ✓ The database is now no longer password-protected.

12 Software settings

Opening the main menu

1. Click on  to open the main menu.

Specifying and editing settings

1. Activate **Open last database at start** to open the database you last used after a re-start.
2. Click on **Remote HMI Manager text size** to specify the text size.
3. Click on **Request Download Time** to specify the time available to the firmware user to confirm or reject changes.

Only activate **Enable Logfile** when you are looking for a program error.

Accept or reject settings

1. Click on **Apply** to accept the settings.
2. Click on **Revert** to reject the changes.

13 Carrying out a firmware update

Opening the main menu

1. Click on  to open the main menu.

Carrying out a firmware update

Our Support department will provide you with the update file.

1. Click on **Select Firmware File** to select the update file in the Windows Explorer.
2. Click on **Start Download** to download the update to the Thin Client.
   - ➢ A progress bar shows how far the update installation has progressed.

If an interval greater than 0 seconds has been specified under **Request Download Timeout** the Thin Client user can abort the download within this time. The system will issue a message that the download has been aborted.

- ✓ If the update has been finished, the system will issue a message.

14 Useful tips

14.1 Error fixing

No connection possible between Remote HMI Device Manager and Thin Client		
Cause	**How to fix it**	**Who**
Incorrect network configuration	• Check network configuration.	Engineer
Access from Device Manager to Thin Client not permitted	• Allow access in the **System & Proxy** menu.	Engineer

14.2 Configuration of the remote access

These settings can only be made at the Thin Client.

Configuration of remote access to the Thin Client via VNC and RDM

1. Activate **Allow configuration export/import via RemoteHMI Device Manager** to allow the export and import of the Thin Client configuration via the RemoteHMI Device Manager.
2. Activate **Allow remote access via VNC** to allow the VNC remote access to the Thin Client.
3. Enter the password for the remote control.
4. As an option, enter a password for remote access without operating permit.
5. Click on **Advanced VNC Server Config** if you need to change the VNC settings.
6. Click on **Input blocking during remote access** to define access behaviour during a remote connection.
7. Activate **Off** to allow local and remote operation during remote access.
8. Activate **Local** to block local operation of the Thin Client during remote access.
9. Activate **Remote on local activity, inactivity timeout = 3 sec** to block the remote operation via local operation during remote access.
   - ➢ This block is removed if no local operation occurs during a specified idle period. The factory setting for this idle period is 3 seconds. This can be adjusted.
10. To adjust the idle period, click on **Advanced VNC Server Config**.

14.3 Activating VNC server system on the host

The following explains the procedure for the TightVNC server.

In order to be able to establish a VNC connection, the VNC server system must be activated on the host. The VNC service acquires the IP address needed for this connection from the settings of the PC's network connection. Depending on the configuration, the IP address is specified manually or allocated by a DHCP server. In the firmware's address book, this IP address is defined as the server IP of the VNC connection.

The way this connection is established depends on the settings of the VNC server and can either be

- a direct connection that is not password-protected
- a connection with VNC password
- a connection with Windows password

14.3.1 VNC server parameters

The following parameters are necessary to configure the VNC connection. The actual name may vary depending on the VNC server system used.

VNC server address

The VNC server address is the same as the server IP address or the server name.

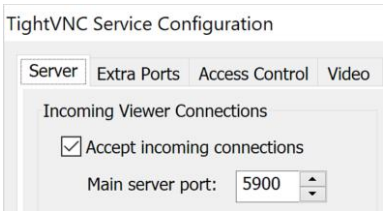
The VNC server systems usually have several ways to find out the address with which the server can be addressed in the network.

In addition to the IP address, port numbers can be allocated in the settings of the VNC server, with which the server can be addressed in the network.

The target address of the Host PC must be located in the network of the Thin Client or must be contactable from the Thin Client.

Ports

Accept connections on port



Defines the server connection port for data transmission (standard port 5900).

If you are using a different port due to network conflicts you need to configure this port. Check the settings of a firewall.

VNC password

VNC server applications authenticate users of a VNC connection via a password. The following password procedures are available:

None	No password is defined. The VNC server on the host allows access to each remote PC (Remote HMI) requesting a VNC connection via its address.
VNC password	Defines one or more passwords (depending on VNC server application) which the VNC server system requests from the Client for authentication purposes.
Windows password	Uses the Windows access authentication. The VNC server system grants the client access to the host if logged on with the valid Windows password.
Single sign on	Uses Windows access authentication and authentication via Windows-based login. The VNC server system grants access to the client if the user has entered a valid Windows login.

Encryption

Most VNC servers use encryption to protect the transmission of image, mouse and keyboard data from unauthorised access.

Always on	Data is always encrypted
Prefer on	Data is always encrypted unless the Thin Client requests no encryption (standard). This setting is necessary if the configuration requests no encryption.

Prefer off	Data is not encrypted unless the Thin Client requests encryption. This setting is necessary if the configuration requests encryption.

Prompt local user to accept connections

Allows the host user to accept or reject a connection request. Since the host is usually used for direct remote access, this setting is not relevant for the Thin Client connection.

Start VNC Server automatically with Windows

Specifies that the VNC server system is automatically activated when Windows is started. If this function is not activated, the remote access must be explicitly started after a system start of the host PC.

14.4 DRDC-Client connection

EMERSON's DeltaV®-Remote-Desktop-Connection-Client (DRDC) allows access to a virtualised operator or engineering workstation within a DeltaV®-virtualisation architecture. This way, applications that run on a distributed control system can be accessed via the Ethernet.

You can add a DRDC connection via an app in the **Applications** register (see Adding apps).

Pro Requires a Pro licence.

14.5 Updating the software

For the software to be updated, the current software version must first be de-installed.

1. De-install the old software version.
2. Double-click on the *...Setup.exe* update file.
3. Follow the instructions of the installation assistant.
   - ➢ A progress bar tracks the progress of the installation. Once the installation has been completed, the system will issue a message.
4. Open the software.
   - ➢ During the start you can either open an existing database or create a new one.