Instruction manual

notion#client

Software
Original version (D)

Copyright and disclaimer

©2021-03 TRsystems GmbH.
All excerpts and reproductions only with prior permission of TRsystems GmbH. All product illustrations and dimensions are principle representations and may differ for individual products. All technical data are subject to change without notice.

TRsystems GmbH is a company of TR-Electronic GmbH.
The products, names, specifications and logos mentioned are for informational purposes only and may be trademarks of their respective owners without specific identification. Intended use: Exclusively for industrial environment! WEEE-Reg. No. DE 11414956

Table of Contents

TABLE OF CONTENTS 3

1. ABOUT THIS GUIDE 6

1.1. Release 6

1.2. Change index 7

2. SAFETY INSTRUCTIONS 8

3. HOME PAGE 10

3.1. Factory reset 11

3.2. Password input 12

3.3. On-Screen Keyboard 13

4. LICENSE VIEW 15

5. PARAMETERIZATION VIEW 16

6. CONNECTION VIEW 17

7. CONNECTION PARAMETERIZATION 20

7.1. Connection parameterization WEB 20

7.1.1 Advanced connection parameterization WEB 22

7.2. Connection parameterization VNC 24

7.2.1 Advanced connection parameterization VNC 28

7.2.2 Accessibility Test 31

7.3. Connection parameterization RDP 32

7.3.1 Advanced connection parameterization RDP 36

7.3.2 Accessibility Test 41

7.4. Connection parameterization RDPApp 43

7.4.1 Connection Configuration RDPApp 43

7.4.2 Advanced Connection Configuration RDPApp 46

7.4.3 Accessibility Test 50

7.4.4 Application Configuration RDPApp 52

7.5. Connection parameterrization Stream 55

7.6. Connection parameterization Multi 58

7.6.1 Advanced connection parameterization Multi 60

7.6.2 Display configuration "Rasterized positioning" 62

7.6.3 Display configuration "Free positioning" 64

8. PARAMETERIZATION VIEW "SYSTEM" 65

8.1. Configure notion#client 66

8.2. Change Date / Time 78

8.3. Font settings....79
8.3.1 Add....80
8.3.2 Choose font file...81
8.3.3 Font info....81
8.4. Configure Remote VNC Access....82
8.4.1 Configure....83
8.5. Configure Web Interface....85
8.6. Configure Remote Shell Access....86
8.7. Screen cleaning....87
9. PARAMETERIZATION VIEW "NETWORK"....88
9.1. Status....91
9.2. Advanced....92
9.3. Configure interface (eth0/eth1)....93
9.3.1 Advanced interface configuration (eth0/eth1)....95
9.4. Configure interface (wlan0)....96
9.4.1 Scanning....98
9.5. Configure interface (vpn0)....99
10. PARAMETERIZATION VIEW "SERVICE"....101
10.1. Export configuration data....102
10.2. Import configuration data....104
10.3. Export log files....105
10.4. Start local update....105
10.5. Advanced....106
10.5.1 Touchscreen Analyse....106
10.5.2 Touchscreen Setup....107
10.5.3 Gesture Analyse....108
11. VIEWER....110
11.1. Web-Viewer....111
11.1.1 Context Menu....114
11.1.2 Certificate Exclusions....115
11.2. VNC-Viewer....117
11.2.1 Daisy chain function....120
11.3. RDP-Viewer....121
11.3.1 Multi-client function....123
11.4. RDPApp-Viewer....124

11.5. Stream-Viewer 125
11.6. Multiple connections 126
11.6.1 Connection switching 128
11.6.2 Display options 129
12. WEB-INTERFACE 130
12.1. Setting the system time and date 132
12.2. Trigger system restart 134
12.3. Performing a system update 135
13. LOCAL SYSTEM UPDATE 138
14. IMPORTANT INFORMATION ABOUT THE UPDATE 140
14.1.1 LIX251_030100, LIX251_030101, LIX251_030102, LIX232_030100, LIX232_030102 140
14.1.2 LIX251_030103 140
14.1.3 LIX251_030200, LIX251_030300, LIX251_030301, LIX251_030302, LIX251_030303, LIX251_030304, LIX232_030200, LIX232_030301, LIX232_030302, LIX232_030303 140
14.1.4 LIX232_030304, LIX251_030305, LIX251_0304xx, LIX232_0304xx and the following versions 140
14.1.5 Table Overview Update 141

1. About this guide

Copyright and disclaimer

This manual, including the illustrations contained therein, is protected by copyright. Third-party applications of this manual that deviate from the which deviate from the copyright regulations are prohibited. The reproduction, translation as well as electronic and photographic archiving and alteration requires the written permission of the manufacturer. Violations obligate to compensation.

1.1. Release

Aim of the instruction		Quality improvement, in line with the company's guiding principles	
Author	**Creation date**	KAO	05.06.2018
Release by		KAO	
		MAS	
Document number		TRS-DOC-001440	

1.2. Change index

On this page of the document, the current version status is noted with the associated date and author. Drawings that may be in the appendix are provided with their own change index.

Version	Change	Reason for change	Date	Author
00			05.06.2018	KAO
01	Images updated and new functions documented	Function extension	12.07.2019	KAO
02	Images updated and new functions documented	Function extension	18.02.2021	KAO
03	none	Internal system-related auditing	26.02.2021	RAB
04	Corrections & additions	Need rework	19.04.2021	KAO
05	Images updated and new functions documented	Function extension	25.05.2021	KAO
06	Corrections and additions: LIX232_030301, LIX251_030301	Function extension	09.07.2021	KAO
07	Corrections and additions: LIX232_030302, LIX231_030302	Function extension	04.08.2021	KAO
09	Correction and additions: LIX232_030401, LIX251_030401	Function extension 9.4 Note: supported WLAN devices	16.03.2022	KAO
10	Corrections and additions: LIX232_031000, LIX251_031000	Function extension	22.02.2024	KAO

Basic

Read these instructions carefully before use and keep them.
Pass the instructions on to the user after assembly and with the product in case of resale.

Target group

These instructions are intended for persons who commission, configure, operate and maintain a product.

Explanation of terms

The table (Table 1) lists terms and briefly explains them for starters.

Term	Explanation
Users	Users are persons who are created in the system.

Table 1 Definition of terms

2. Safety instructions

Classification of the hints

These operating instructions contain information that you must observe for your personal safety and to avoid damage to property. A distinction is made between basic safety instructions and warning instructions.

Safety instructions

The basic safety instructions precede the instructions. The chapter "Safety instructions" warns of basic dangers which can occur in several phases of the product application and which must always be observed by the product user.

Warnings

Warnings are placed within the documents at the specific danger points. They are placed immediately before the action where there is danger.
The warnings are highlighted by a warning triangle and are displayed as follows, depending on the degree of danger:

Warning signs	Significance
⚠ DANGER	DANGER indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	WARNING indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	CAUTION indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	CAUTION indicates a situation which, if not avoided, may result in property damage.

Table 2.1: Type of safety note

Warning structure

The STCE method is a procedure for the systematic design of safety instructions. The acronym STCE stands for the four principles:

- Severity of danger (signal word)
- Type and source of the hazard
- Consequences of disregarding the danger
- Escape (measures to avert the danger)

Example:

⚠WARNING

Danger of cuts due to sharp-edged sheets.
It can lead to cuts.
- ► Wear cut-resistant gloves
- ► If possible, deburr the sharp edges of the sheets.

Misapplication	Nature and source of the hazard
Warning sign	Warning signs according to the following table.
Reasons for misapplication	Describes possible reasons for misapplication.
Possible consequences of misuse	Describes the consequences of non-compliance.
Security measure	Indicates how to avoid the hazard.

Table 2.2: Structure of a safety note

Additional notes

Example ESD area:

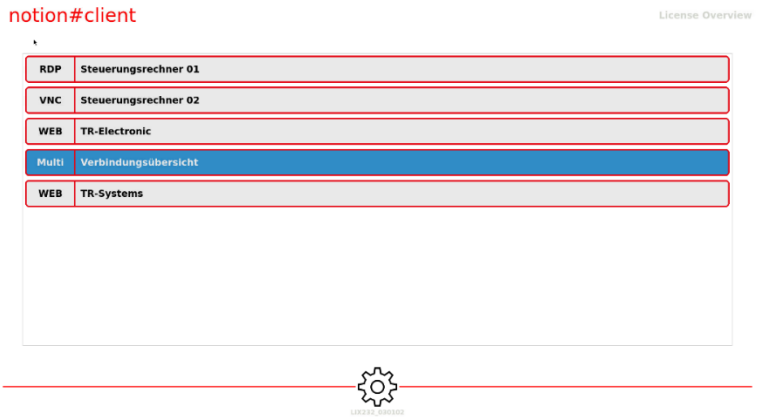
ESD protection measures according to DIN EN 61340-5-1 must be observed.

Example reference / hint:

Refer to chapter X.X. corresponding structure.

3. Home page

The start page displays all configured connections (including the connection type). It also provides access to the configuration of the system and the individual connections as well as to the license overview page.



Homepage

Top right: **„License Overview“:**

Switch to the license view.

Center: **Listing of the existing connection configurations:**

At the beginning of each line the abbreviations of the connection type are given:

- WEB – Web-Viewer
- VNC – VNC-Connection
- RDP – RDP-Connection
- RDPApp – RDPApp-Connection
- Stream – Video-Stream-Connection
- Multi – Multiple connections.

Clicking on one of these connection configurations establishes the connection. The highlighted connection is the one that was used last. It is automatically opened with a delay when the application is started.

The delay can be parameterized (see section 8.1 - Configure notion#client): Setup-Parameter „Start-Timeout"

Below gear wheel: **Change to the parameterization view (see section 5 - Parameterization view)**

If a password has been specified, it will be requested before switching to the parameterization view.

Specification of the password (see section 8.1 - Configure notion#client): Setup parameter "Password" (admin password)

At the bottom: Version number of the software

3.1. Factory reset

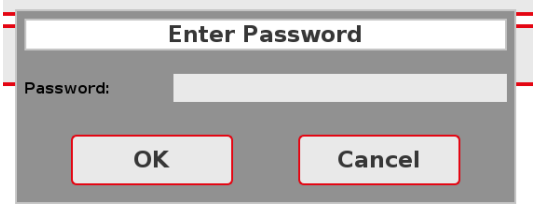
To reset the device to the factory settings, the gear wheel must be clicked for more than 5 seconds. A dialog then appears that requires you to enter an access code. This access code is available on request.

After entering the correct access code, the system restarts and all connections and settings stored on the device are reset to factory settings.

Enter the access code

3.2. Password input

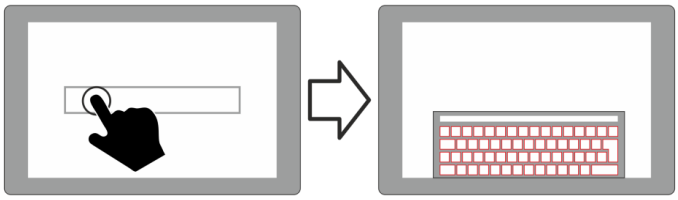
The "Admin password" (see section 8.1) is used to gain access to all subordinate system areas, including those that have been protected with a "Disconnect password"(see sections 7.1, 7.2, 7.3, 7.4, 7.5 and 7.6). The "Disconnect password" is area-dependent and only valid for this defined area. The "Disconnect password" is subordinate to the "Admin password".



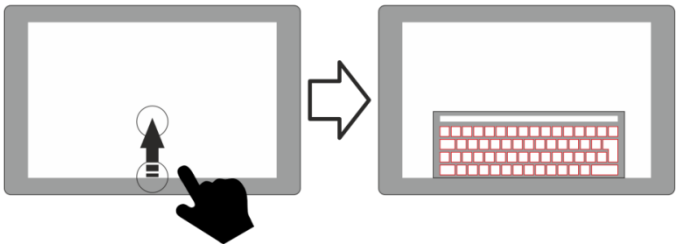
Password prompt when switching to the parameterization view.

3.3. On-Screen Keyboard

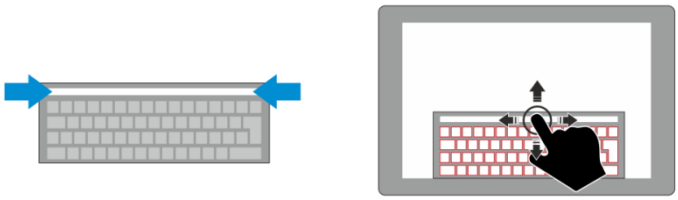
By clicking on the input field, the on-screen keyboard is displayed.



In the viewers, the keyboard is displayed by dragging and releasing it from the bottom edge of the screen to the center of the screen. The distance covered when dragging should be at least 20 % of the screen height. The keyboard appears after the gesture has been successfully executed.



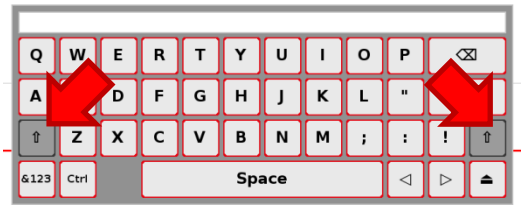
The keyboard can be moved freely on the screen. To do this, touch the drag page (the white field) above the keys with your finger and you can move the keyboard as you wish.



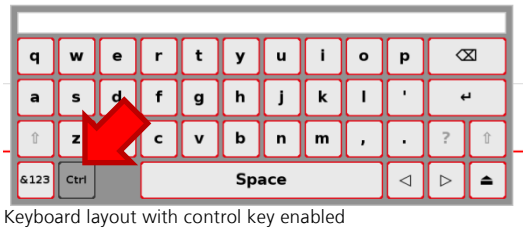
If the "Hide" button is pressed (icon in the lower right corner), the keyboard will be hidden again.

The on-screen keyboard offers different display modes: standard view, with shift key enabled, with control key enabled, and numbers and special characters (1 and 2). These modes are shown below:

Keyboard layout in default view

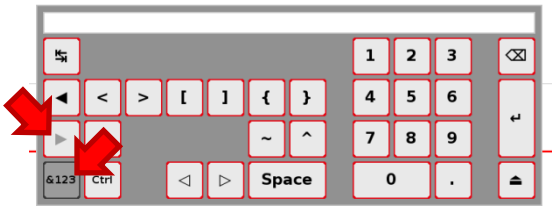


Keyboard layout with shift key enabled



Keyboard layout with control key enabled

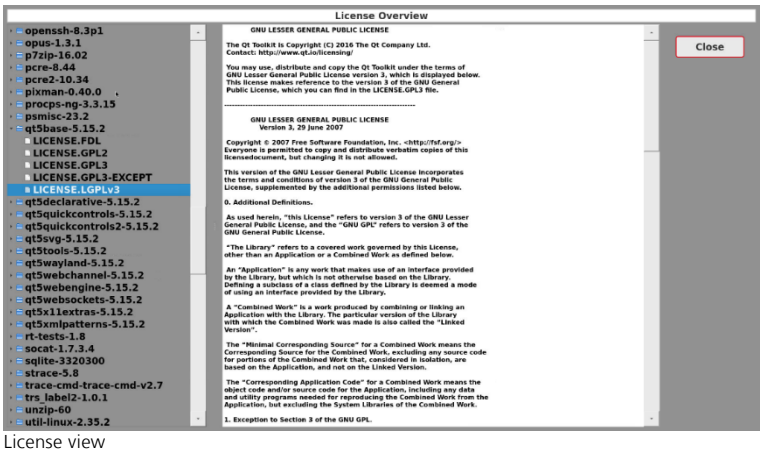
Keyboard layout (numbers and special characters 1)



Keyboard layout (numbers and special characters 2)

4. License view

The license view displays the license texts for the open source packages installed on the system.



License view

Left: Overview of the (open source) packages installed on the system with the license texts they contain. The display is in a tree structure.

Right: Display of the selected license text.

Button at the top right: „Close“

The "Close" button takes you back to the home page (see section 3 - Home page).

5. Parameterization view

The parameterization view is the central entry point for configuring the connections and the system.

Parameterization view

Display
Top center

“Active connection”:

Name of the last active connection.

Button
Top right

“Logout”:

This takes you back to the start page (see section 3 - Home page).

Center button

“Connections”:

Switch to the connection view (see section 6 - Connection view).

Button
Bottom left

“System”:

Change to system parameterization (see section 8 - Parameterization view "System”).

Button
Bottom center

“Network”:

Change to network parameterization (see section 9 - Parameterization view "Network“).

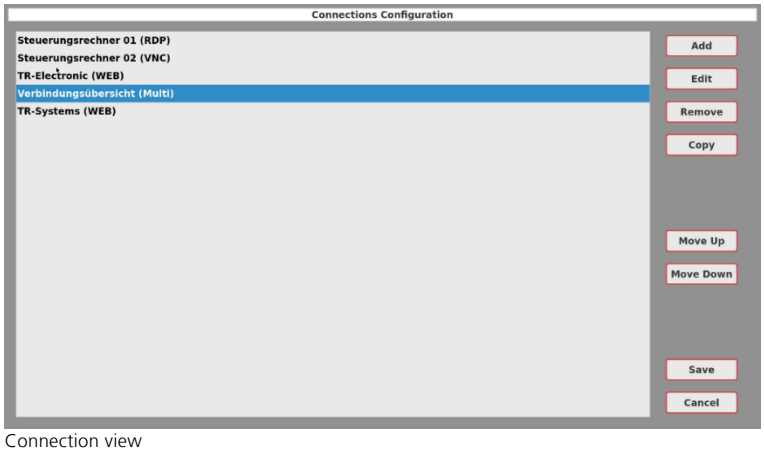
Button
Bottom right

“Service”:

Change to service parameterization (see section 10 - Parameterization view "Service).

6. Connection view

The connection view shows all configured connections and offers the possibility to edit, delete, copy and add new ones. Furthermore, the order of the entries can be changed (see also section 8.1 - Configure notion#client - Gestures (connection switching)).



Connection view

Selection Left: Listing of the existing connection configurations. The connection name is displayed and the connection type in brackets. To be able to edit a connection, it must be selected beforehand.

Buttons Right:

„Add“:

Add a new connection (no selection necessary). A dialog for selecting the type of connection to be created appears (see figure below). Then, depending on the connection type, the connection parameterization WEB / VNC / RDP / RDPApp / Stream / Multi (see section 7.1, 7.2, 7.3, 7.4, 7.5 and 7.6) is displayed.

„Edit“:

Edit the selected connection. Then, depending on the connection type, the connection parameterization WEB / VNC / RDP / RDPApp / Stream / Multi (see section 7.1, 7.2, 7.3, 7.4, 7.5 and 7.6) is displayed.

„Remove“:

Remove the selected connection. A confirmation prompt is displayed (see figure below). If this is confirmed ("Remove"), the connection is deleted.

“Copy”:

The selected connection is to be copied. For this purpose a new connection parameterization WEB / VNC / RDP / RDPApp / Stream / Multi (see section 7.1, 7.2, 7.3, 7.4, 7.5 and 7.6) with the data of the selected connection is displayed and can be edited.

„Move Up“:

The marked connection is moved up by one and thus swaps places with the connection above it. If the marked connection is already at the top, this button is grayed out.

„Move Down“:

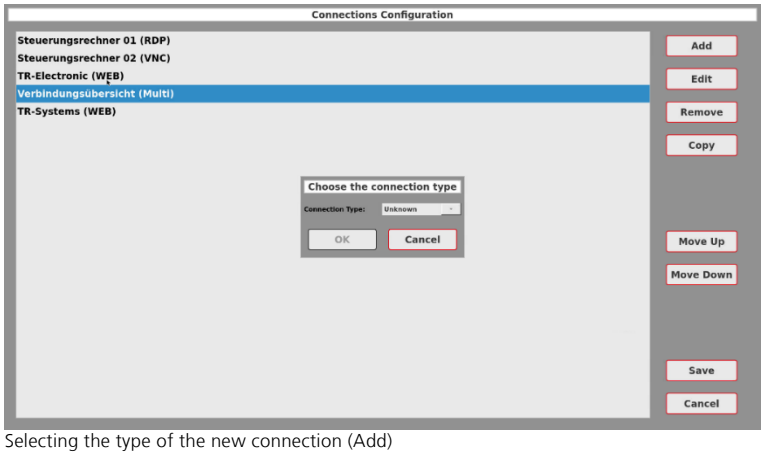
The marked connection is moved down by one and thus swaps places with the connection below it. If the marked connection is already at the bottom, this button is grayed out.

„Save“:

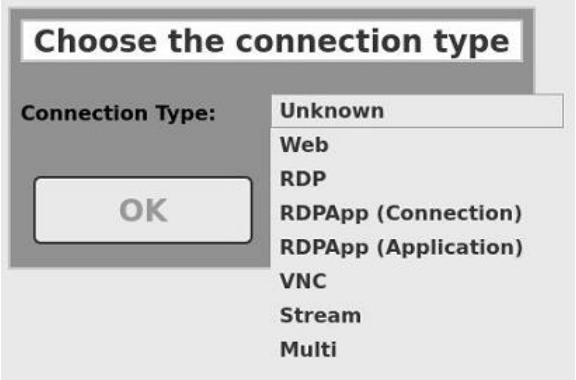
Save the changed settings in the configuration file. This is followed by a return to the previous view (see section 5 - Parameterization view).

„Cancel“:

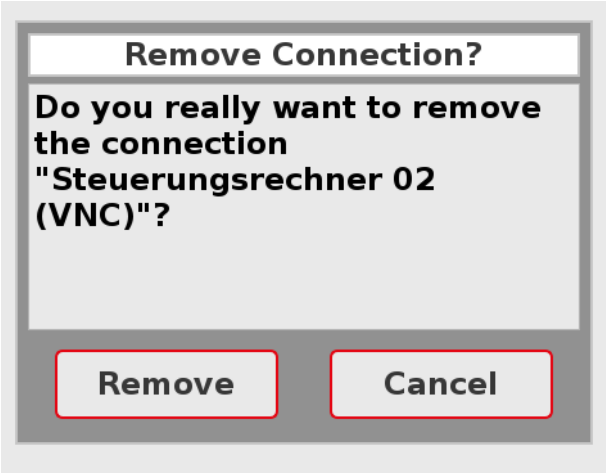
The changes made since the last save are discarded and the previous configuration file is reloaded. This is followed by a change to the previous view (see section 5 - Parameterization view).



Selecting the type of the new connection (Add)



Selection of the type of the new connection (Add, with the selection open).

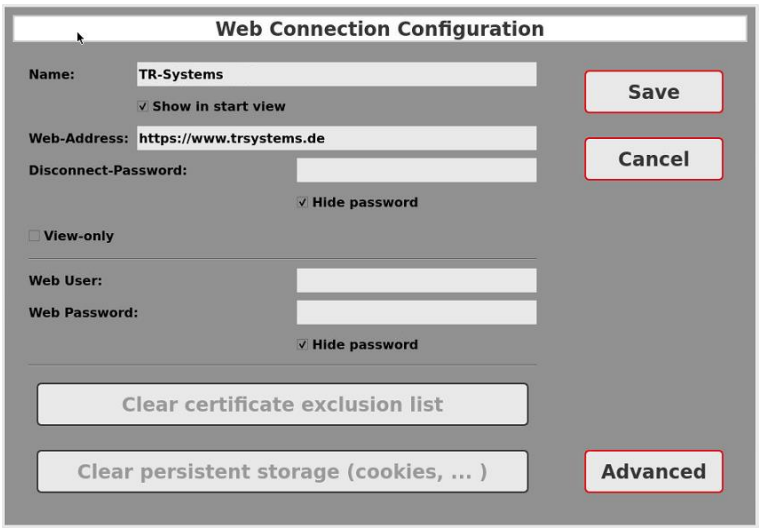


Security prompt before deleting a connection.

7. Connection parameterization

Each connection requires a set of specific parameters to establish a connection and display it in a suitable way. The individual connection parameterizations are presented in the following sections.

7.1. Connection parameterization WEB



Connection parameterization WEB

Input fields

„Name“:

Descriptive name of the connection - displayed in the connection view and on the home page.

“Show in start view”:

This can be used to specify whether this connection should be displayed or hidden in the start view. This is used, for example, if a connection is part of a multiple connection and should not be displayed individually.

„Web-Address“:

URL / address of the web page. A fully qualified identifier is expected here (URL in the form http://www.trsystems.de or https://www.trsystems.de).

„Disconnect-Password“:

Password that must be entered to exit the web viewer and return to the home page. This parameter is optional.

- Passwords are stored encrypted in the configuration file.

Control element

„Hide password“:

This can be used to switch between plain text display and hidden display of the password. This setting is not saved.

Control element **“View-Only”**

Show the web page in view mode - all inputs (keyboard / mouse / touch) are ignored.

Input fields **„Web User“:**

If a website requires authentication when establishing a connection, the required user name can be entered here.

“Web Password”:

The corresponding password for authentication.

Control element **„Hide password“:**

This can be used to switch between plain text display and hidden display of the password. This setting is not saved.

Buttons **„Clear certificate exclusion list“:**

If the certificate of a web connection secured via https is not valid or the certification authority is not known (e.g. self-signed certificates), an exception can be created for this connection. With this button the exception can be remove.

„Clear persistent storage (cookies, ...)“:

When visiting a web page, the web browser creates a cache in which web page elements (such as images) are temporarily stored. If these elements change, the change may not have been detected. By deleting the persistent data, these changes become visible again. In addition, this can also be used to delete cookies stored by the website.

Buttons **„Save“:**

The settings or their changes are saved (but not yet in the configuration file!) and it is switched back to the previous view (see section 6 - Connection view).

„Cancel“:

The settings or their changes are discarded and the program switches back to the previous view (see section 6 - Connection view).

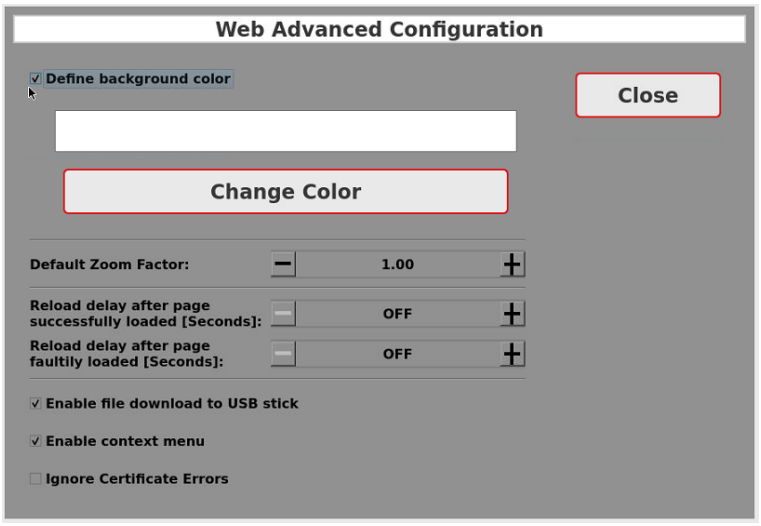
„Advanced“:

Switch to the advanced connection parameterization.

7.1.1 Advanced connection parameterization WEB

In the advanced connection settings, the background color that is displayed when the web page is loaded can be set if required.

In addition, an initial zoom factor can be specified with which the selected web page is to be displayed.



Advanced connection parameterization WEB

Input fields

„Reload delay after page faultily loaded [Seconds].“:

If a web page cannot be loaded, e.g. due to network problems, a value in seconds can be entered here after which a new loading attempt should be started. Values between 0 and 3600 seconds can be entered. The value 0 switches the function off (display "OFF" instead of 0).

„Reload delay after page successfully loaded [Seconds].“:

If a web page is to be reloaded after a certain time, e.g. because of new content, this can be set with this parameter. The value range is between 0 and 3600 seconds, whereby the value 0 switches the function off (display "OFF" instead of 0).

Control element

„Enable file download to USB stick“:

If it should be possible to download files from the website, this option must be activated. The download is done to an inserted USB stick.

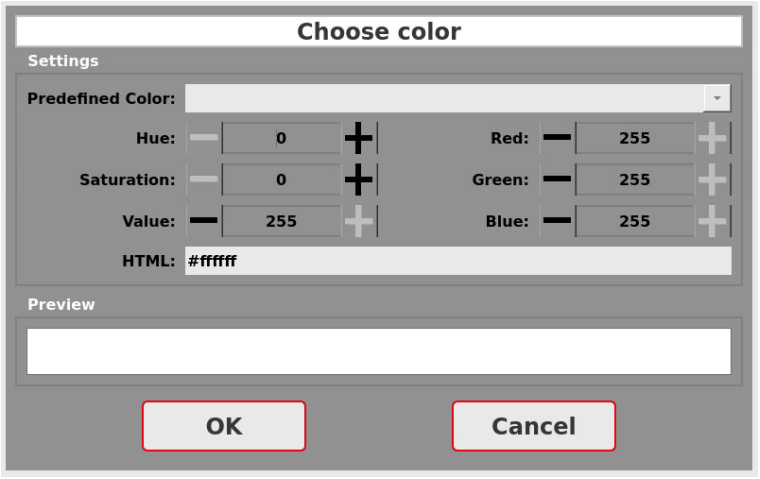
„Enable context menu“:

If this option is activated, a context menu can be displayed by right-clicking or Tap’n’Hold (press and hold the touch until the menu is displayed). The content of the context menu depends on the element on which the click was made.

„Ignore Certificate Errors“:

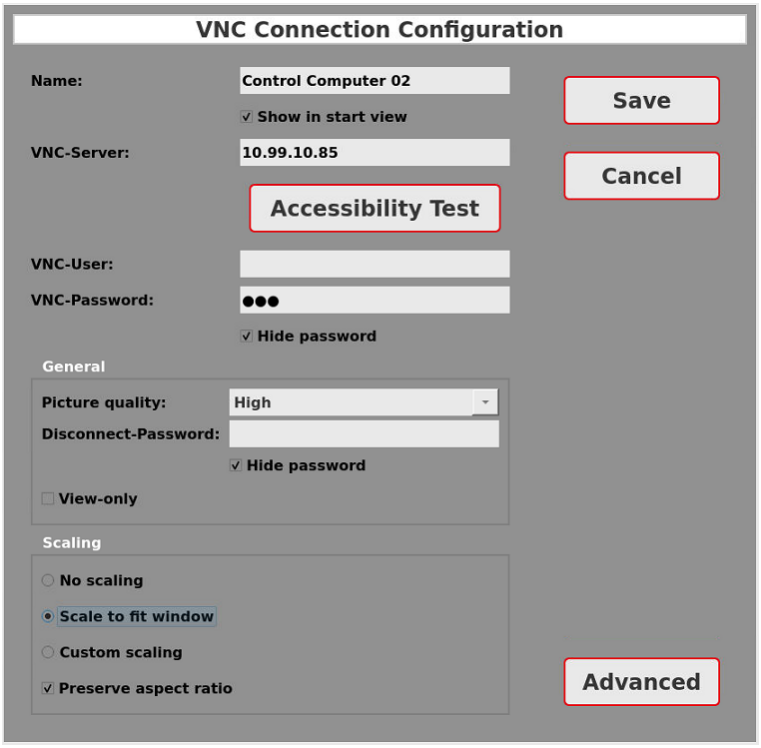
If a web server uses a certificate that has been signed by an unknown certification authority, this certificate can be included in the list of accepted certificates (see 11.1.2 - Certificate Exclusions). However, if it is a self-signed certificate that is regularly recreated on the web server (e.g. after every cold start), the certificate would have to be added to the list each time.

Alternatively, the certificate check can be completely omitted by activating this option. **ATTENTION**: This means that the web server is not validated and the connection is no longer trustworthy!



Color selection dialog

7.2. Connection parameterization VNC



VNC connection configuration

Input fields

„Name“:

Descriptive name of the connection - displayed in the connection view and on the home page.

“Show in start view”:

This can be used to specify whether this connection should be displayed or hidden in the start view. This is used, for example, if a connection is part of a multiple connection and should not be displayed individually.

“VNC-Server”:

IPv4 address or network name of the VNC server. If the default port is not to be used, it can be appended to the IPv4 address or network name using ':' (e.g. 172.18.1.10:5900). When specifying the port number, an abbreviated form can also be used. If the port number is less than 100, the value 5900 is added to the port number.

„VNC-User“:

If a user name is required to log in to the VNC server, it can be specified here. This parameter is optional.

„VNC Password“:

If a password is required to log in to the VNC server, it can be specified here. This parameter is optional.

- Passwords are stored encrypted in the configuration file.

If no user name or password is stored, but this information is required to establish a connection, an input mask is displayed where this information can be entered.

Control element

„Hide password“:

This can be used to switch between plain text display and hidden display of the password. This setting is not saved.

Area

„General“

Selection field

„Picture quality“:

Setting the image quality and thus the required bandwidth of the connection. The following settings are available: High, Good, Medium, Low.

Input fields

„Disconnect-Password“:

Password that must be entered to exit the VNC viewer and return to the start page. This parameter is optional.

- Passwords are stored encrypted in the configuration file.

Controls

„Hide password“:

This can be used to switch between plain text display and hidden display of the password. This setting is not saved.

„View only“:

View in passive mode without transmitting mouse and keyboard events.

Area

Selection points

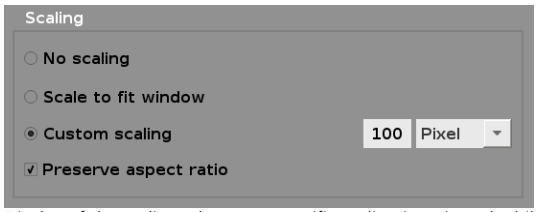
„Scaling“

Selection of the scaling model:

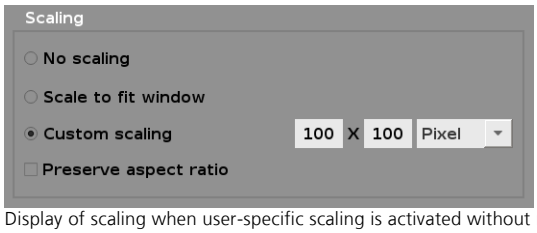
- „No scaling“:
  The received VNC images are displayed in the same resolution as they are transmitted from the server. This may cause the display to show black borders or scroll bars.

- „Scale to fit window“:
  The received VNC images are scaled to fill the entire screen. If additionally, "Keep aspect ratio" is selected, the aspect ratios are kept and black borders (top/bottom or sideways) may occur.

- „Custom scaling“:
  Any scaling in pixels or percent from the original resolution can be selected. If "Preserve aspect ratio" is also selected, the same scaling factor is used for X and Y direction. Otherwise, different scaling factors can be used for X and Y direction.



Display of the scaling when user-specific scaling is activated while maintaining the aspect ratios (Percent / Pixel selection).



Display of scaling when user-specific scaling is activated without maintaining the aspect ratios (Percent / Pixel selection).

Buttons

„Save“:

The settings or their changes are saved (but not yet in the configuration file!) and it is switched back to the previous view (see section 6 - Connection view).

„Cancel“:

The settings or their changes are discarded and the program switches back to the previous view (see section 6 - Connection view).

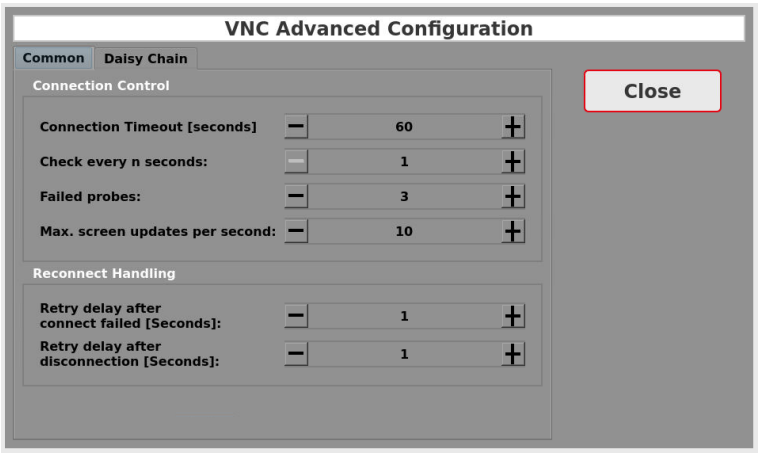
“Accessibility Test”:

Opens a dialog that can be used to check the accessibility of the server computer by means of an ICMP request (echo).

„Advanced“:

Switch to the advanced connection parameterization.

7.2.1 Advanced connection parameterization VNC



Advanced connection parameterization VNC – Common

Area

Input fields

Connection control

"Connection Timeout [seconds]":

Specifies after what period of time the connection setup should be aborted.

„Check every n seconds":

Specifies how often (specified in seconds) to check if the connection to the VNC server is still established.

„Failed probes":

Specifies how many connection errors may occur in succession before a disconnection can be assumed and the user is informed by a corresponding error message.

„Max. screen updates per second":

To prevent overloading of the notion#client or the network when the server is under high load (high rate of change of screen content, e.g. due to videos), the maximum number of screen updates can be limited.

Area

Input fields

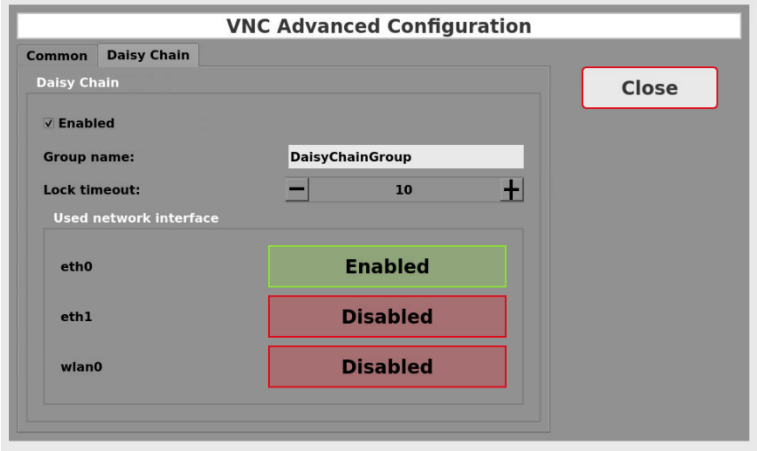
Reconnect Handling

“Retry delay after connect failed [Seconds]”:

Specifies how long to wait after a failed connection attempt until a new connection attempt starts. Values from 0 to 3600 are permissible. With a value of 0 (display OFF), no further attempt is made to establish the connection.

“Retry delay after disconnection [Seconds]”:

Specifies how long to wait after a connection interruption before trying again to re-establish the connection. Values from 0 to 3600 are permissible. With a value of 0 (display OFF), no further attempt is made to establish the connection.

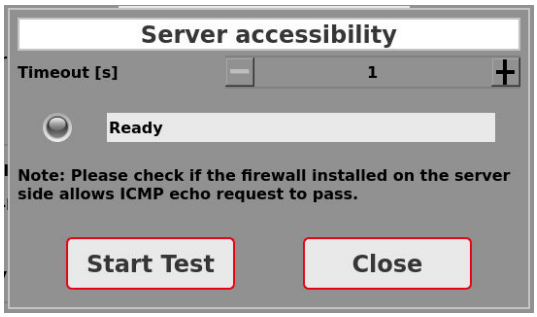


Advanced connection parameterization VNC - Daisy Chain

Advanced connection

Area	**Daisy Chain** This is a method when using multiple VNC clients on a VNC server to lock the input to the other VNC clients while the own VNC client still remains operable (see section 11.2.1 - Daisy chain function).
Control element	**„Enabled“:** Enables the daisy chain on this VNC client. All other VNC clients must then also have daisy chain enabled to use this feature.
Input fields	**„Group name“:** Freely selectable group name, via which VNC clients can be combined into groups. Only VNC clients from the same group react to the mutual input locks! **„Lock timeout“:** Specifies how long the locked VNC clients remain locked after the last action (operation via the touchscreen) until the lock is released again (value in seconds).
Selection field(s)	**„Used network interface“:** Here all active network interfaces are displayed and you can select over which of these interfaces the daisy chain communication should be sent to the other clients.
Button	**„Close“:** It will switch to the previous view (see section 7.2 - Connection parameterization VNC).

7.2.2 Accessibility Test



Server accessibility dialog

Schaltfläche

„Start Test“:

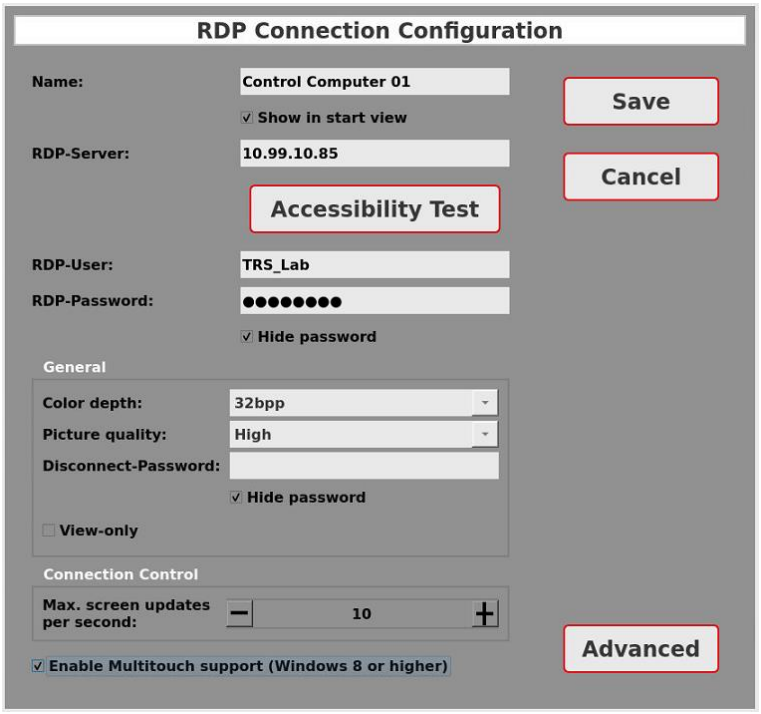
Checks the server accessibility by means of an ICMP request (echo). The maximum waiting time for a response from the server can be made via the timeout setting. The status of the test is displayed as follows:

- Black LED: Ready
- Yellow LED: Running…
- Red LED: Host is not available
- Green LED: Host is available

„Close“:

The Dialog is closed.

7.3. Connection parameterization RDP



RDP connection parameterization

Input fields

„Name“:

Descriptive name of the connection - displayed in the connection view and on the home page.

“Show in start view”:

This can be used to specify whether this connection should be displayed or hidden in the start view. This is used, for example, if a connection is part of a multiple connection and should not be displayed individually.

“RDP-Server”:

IPv4 address or network name of the RDP server. If the default port (port 3398) is not to be used, it can be appended to the IPv4 address or network name using ':' (e.g. 172.18.1.10:3398).

„RDP-User“:

If a user name is required to log in to the RDP server, it can be specified here. This parameter is optional.

„RDP-Password“:

If a password is required to log in to the RDP server, it can be specified here. This parameter is optional.

- Passwords are stored encrypted in the configuration file.

If no user name or password is stored, but this information is required to establish a connection, the RDP server displays an input mask where this information can be entered.

Control element

„Hide password“:

This can be used to switch between plain text display and hidden display of the password. This setting is not saved.

Area

General

Selection fields

„Color depth“:

This can be used to set the color depth and thus the required bandwidth of the connection. The following values are available for selection: 15bpp, 16bpp. 24bpp, 32bpp.

„Picture quality“:

This can be used to set the image quality and thus the required bandwidth of the connection. The following values are available for selection: High, Good, Medium, Low.

Input field

„Disconnect-Password“:

Password that must be entered to exit the RDP viewer and return to the start page. This parameter is optional.

- Passwords are stored encrypted in the configuration file.
- **Note:** the connection can also be terminated via the Windows Start menu. In this case, it is not necessary to enter the password!

Control element

„Hide password“:

This can be used to switch between the plain text display and the hidden display of the password. This setting is not saved.

“View-only”:

View in passive mode without transmitting mouse and keyboard events.

Area

Connection control

Input field

„Max. screen updates per second“:

To prevent overloading of the noton#client or the network when the server is under high load (high rate of change of screen content, e.g. due to videos), the maximum number of screen updates can be limited.

Control element

„Enable Multitouch support (Windows 8 or higher)“:

If the RDP server runs under Windows 8 or higher, multitouch support can be activated. Multi-finger operation is then possible. If multitouch support is activated on older Windows versions, input may be disrupted.

Buttons

„Save“:

The settings or their changes are saved (but not yet in the configuration file!) and it is switched back to the previous view (see section 6 - Connection view).

„Cancel“:

The settings or their changes are discarded and the program switches back to the previous view (see section 6 - Connection view).

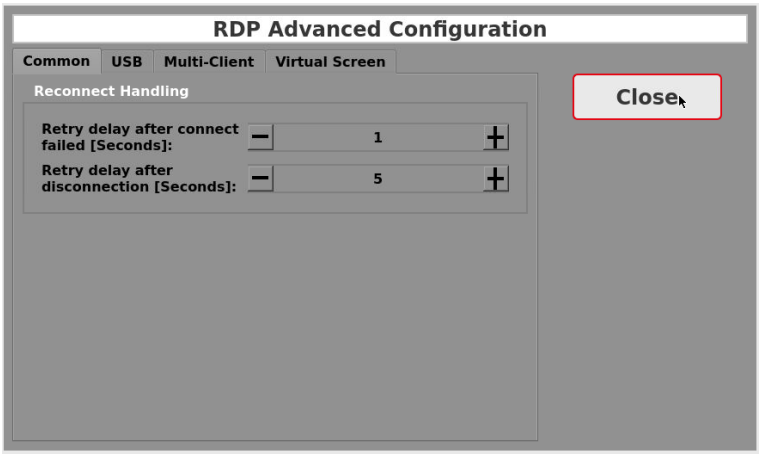
“Accessibility Test”:

Opens a dialog that can be used to check the accessibility of the server computer by means of an ICMP request (echo).

„Advanced“:

Switch to the advanced connection parameterization.

7.3.1 Advanced connection parameterization RDP



RDP Advanced Configuration - Common

Area

Input fields

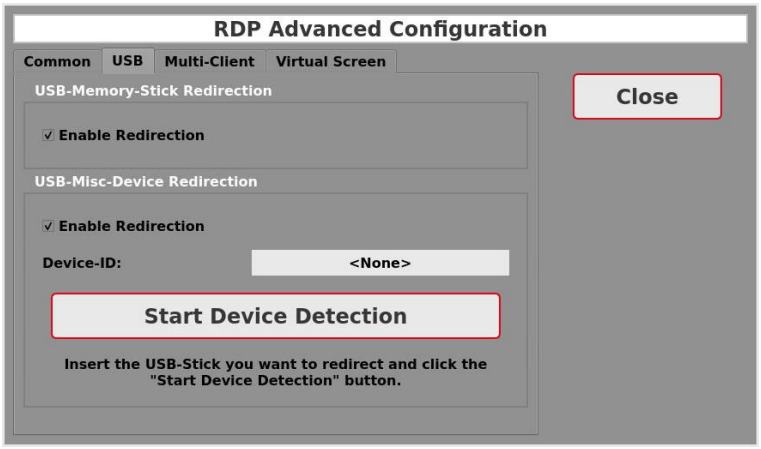
Reconnect Handling

“Retry delay after connect failed [Seconds]”:

Specifies how long to wait after a failed connection attempt until a new connection attempt starts. Values from 0 to 3600 are permissible. With a value of 0 (display OFF), no further attempt is made to establish the connection.

“Retry delay after disconnection [Seconds]”:

Specifies how long to wait after a connection interruption before trying again to re-establish the connection. Values from 0 to 3600 are permissible. With a value of 0 (display OFF), no further attempt is made to establish the connection.



RDP Advanced Configuration - USB

Area USB-Memory-Stick Redirection

Control element **“Enable Redirection”:**

With this function USB memory sticks or USB hard disks plugged into the notion#client can be forwarded to the Windows host and are available there as drives.

Important: The USB sticks must already be plugged in before the connection is established and should remain plugged in for the entire duration of the connection.

Area USB-Misc-Device Redirection

Control element **“Enable Redirection”:**

This function can be used to forward individual USB devices to the Windows host. To do this, the device is plugged in after activating the redirection and then the "Start Device Detection" button is pressed. The detected USB ID (Vendor and Device ID) is then displayed in the "Device ID" field.

Important: If the devices are to be used during the connection, they must be plugged in before the connection is established. If they are not plugged in, however, it does not lead to an error.

Note: This function only works with a limited device circle, which can only be determined by testing.

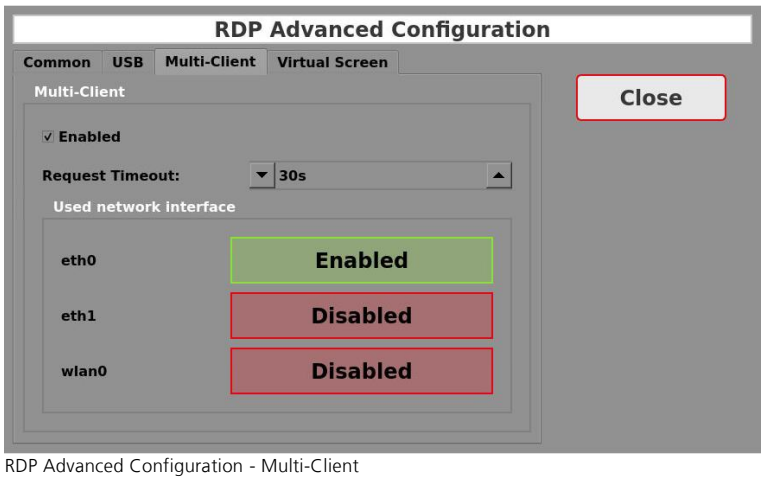
Setting up the Windows host ("Group Policy Editor")

Important: However, this function only works if the Windows host has been configured accordingly. For this, the "Group Policy Editor" gpedit.msc is required (start from the command line as administrator). The following settings must be made.

- Computer Configuration/ Administrative Templates/ Windows Components/ Remote Desktop Services/ Remote Desktop Connection Client/ RemoteFX USB Device Redirection/ All RDP Redirection = Enable
- Computer Configuration/ Administrative Templates/ Windows Components/ Remote Desktop Services/ Remote Desktop Session Host/ Remote Session Environment/ Configure RemoteFX = Enable
- Computer Configuration/ Administrative Templates/ Windows Components/ Remote Desktop Services/ Remote Desktop Session Host/ Connections/ Allow user to connect remotely using Remote DesktopServices = Enable
- Computer Configuration/ Administrative Templates/ Windows Components/ Remote Desktop Services/ Remote Desktop Session Host/ Device and Resource Redirection/ Do not allow supported Plug and Play device redirection = Disable
- gpupdate /force
- Perform reboot of the host

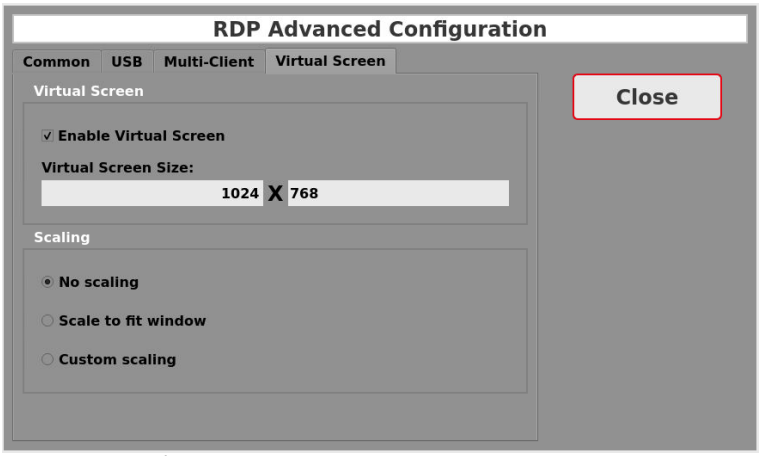
Setting up the Windows host (device driver)

- Appropriate drivers for the USB device are required on the Windows host.



RDP Advanced Configuration - Multi-Client

Area	**Multi-Client** **„Enabled“:**
Input fields	Activates the multi-client function of the RDP viewer (for this, see section 11.3.1 - Multi-client function).
Selection field(s)	**„Request Timeout [Seconds]“:** Specifies after what time period the takeover request is canceled and the connection is forcibly taken over. **„Used network interface“:** All active network interfaces are displayed here and you can select over which of these interfaces the multi-client communication should be sent to the other clients.



RDP Advanced Configuration – Virtual Screen

Area

Virtual Screen

Input fields

„Enable Virtual Screen“:

Enabless the virtual screen and uses the screen resolution specified below instead of using the physical screen resolution or that of the window in the multi-connection view.

„Virtual Screen Size“:

Specifies which screen resolution is to be used for this connection.

Button

„Close“:

Switch to the previous view (see section 7.3 - Connection parameterization RDP).

Area

Selection points

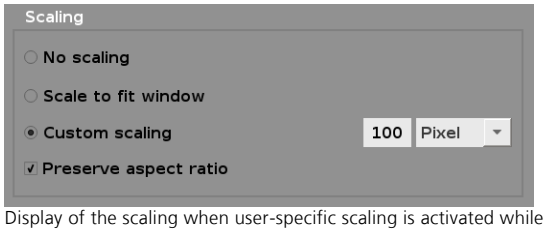
„Scaling“

Selection of the scaling model:

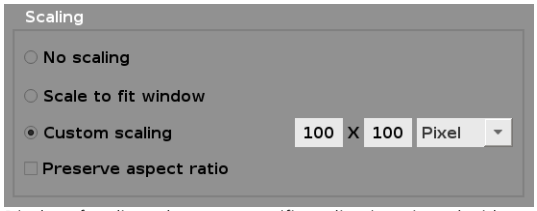
- „No scaling“:
  The received RDP images are displayed in the same resolution as they are transmitted from the server. This may cause the display to show black borders or scroll bars.

- „Scale to fit window“:
  The received RDP images are scaled to fill the entire screen. If additionally, "Keep aspect ratio" is selected, the aspect ratios are kept and black borders (top/bottom or sideways) may occur.

- „Custom scaling“:
  Any scaling in pixels or percent from the original resolution can be selected. If "Preserve aspect ratio" is also selected, the same scaling factor is used for X and Y direction. Otherwise, different scaling factors can be used for X and Y direction.



Display of the scaling when user-specific scaling is activated while maintaining the aspect ratios (Percent / Pixel selection).



Display of scaling when user-specific scaling is activated without maintaining the aspect ratios (Percent / Pixel selection).

7.3.2 Accessibility Test

Server accessibility dialog

Schaltfläche

„Start Test“:

Checks the server accessibility by means of an ICMP request (echo). The maximum waiting time for a response from the server can be made via the timeout setting. The status of the test is displayed as follows:

- Black LED: Ready
- Yellow LED: Running…
- Red LED: Host is not available
- Green LED: Host is available

„Close“:

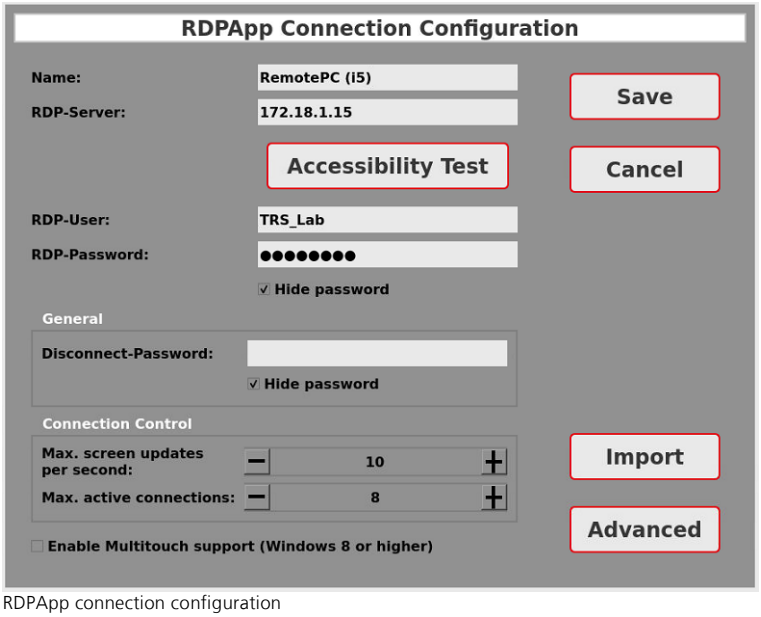
The Dialog is closed.

7.4. Connection parameterization RDPApp

The configuration of an RDPApp connection is divided into two parts: firstly, the connection to the target computer itself must be configured. The second step is to configure the applications that should run on the target computer. Up to 16 applications can run via an RDPApp connection.

7.4.1 Connection Configuration RDPApp

The connection type for the connection configuration is "RDPApp (connection)". This connection is only required internally to configure the applications and is not displayed in the home screen.



RDPApp connection configuration

Input fields

„Name":

Descriptive name of the connection - displayed in the connection view and on the home page.

"RDP-Server":

IPv4 address or network name of the RDP server. If the default port (port 3398) is not to be used, it can be appended to the IPv4 address or network name using ':' (e.g. 172.18.1.10:3398).

„RDP-User":

If a user name is required to log in to the RDP server, it can be specified here. This parameter is optional.

„RDP-Password“:

If a password is required to log in to the RDP server, it can be specified here. This parameter is optional.

- Passwords are stored encrypted in the configuration file.

If no user name or password is stored, but this information is required to establish a connection, the RDP server displays an input mask where this information can be entered.

Control element **„Hide password“:**

This can be used to switch between plain text display and hidden display of the password. This setting is not saved.

Area General

Input field **„Disconnect-Password“:**

Password that must be entered to exit the RDPApp viewer and return to the start page. This parameter is optional.

- Passwords are stored encrypted in the configuration file.
- **Note:** by closing all application the connection is also terminated. In this case it is not necessary to enter the password!

Control element **„Hide password“:**

This can be used to switch between the plain text display and the hidden display of the password. This setting is not saved.

Area Connection control

Input field **„Max. screen updates per second“:**

To prevent overloading of the noton#client or the network when the server is under high load (high rate of change of screen content, e.g. due to videos), the maximum number of screen updates can be limited.

“Max. active connections”:

Specifies the maximum number of applications that may run via this connection. The maximum number here is 16. As a separate virtual monitor is created for each application, this also increases the amount of data to be transferred. You should therefore only select as many active connections as are actually required.

Control element **„Enable Multitouch support (Windows 8 or higher)“:**

If the RDP server runs under Windows 8 or higher, multitouch support can be activated. Multi-finger operation is then possible. If multitouch support is activated on older Windows versions, input may be disrupted.

Schaltflächen

„Save“:

The settings or their changes are saved (but not yet in the configuration file!) and it is switched back to the previous view (see section 6 - Connection view).

„Cancel“:

The settings or their changes are discarded and the program switches back to the previous view (see section 6 - Connection view).

“Accessibility Test”:

Opens a dialog that can be used to check the accessibility of the server computer by means of an ICMP request (echo).

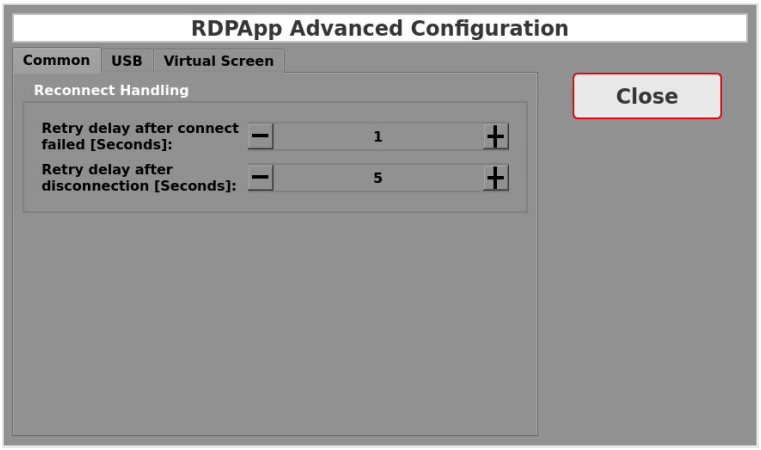
„Import“:

A file-open dialog is used to load an rdp file with the configuration of the RDPApp connection. The configuration file can be created on the RDP host computer with the help of the RemoteApp tool (see also the web page https://github.com/kimmknight/remoteapptool).

„Advanced“:

Switch to the advanced connection parameterization.

7.4.2 Advanced Connection Configuration RDPApp



RDPApp Advanced Configuration - Common

Area

Input fields

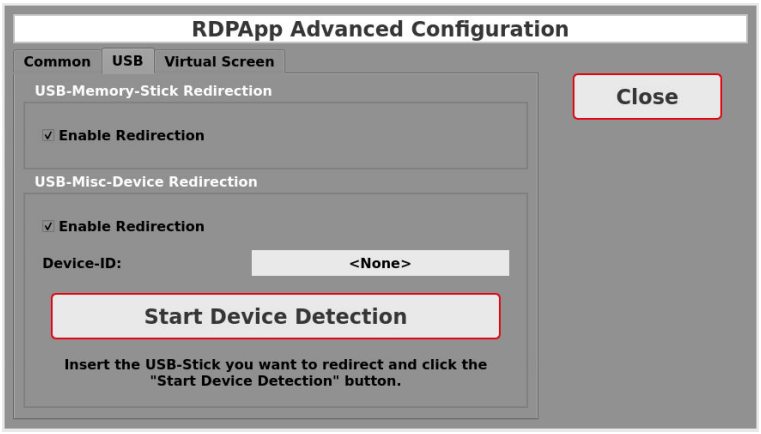
Reconnect Handling

Retry delay after connect failed [Seconds]":

Specifies how long to wait after a failed connection attempt until a new connection attempt starts. Values from 0 to 3600 are permissible. With a value of 0 (display OFF), no further attempt is made to establish the connection.

"Retry delay after disconnection [Seconds]":

Specifies how long to wait after a connection interruption before trying again to re-establish the connection. Values from 0 to 3600 are permissible. With a value of 0 (display OFF), no further attempt is made to establish the connection.



RDPApp Advanced Configuration - USB

Area

Control element

USB-Memory-Stick Redirection

“Enable Redirection”:

With this function USB memory sticks or USB hard disks plugged into the notion#client can be forwarded to the Windows host and are available there as drives.

Important: The USB sticks must already be plugged in before the connection is established and should remain plugged in for the entire duration of the connection.

Area

Control element

USB-Misc-Device Redirection

This function can be used to forward individual USB devices to the Windows host. To do this, the device is plugged in after activating the redirection and then the "Start Device Detection" button is pressed. The detected USB ID (Vendor and Device ID) is then displayed in the "Device ID" field.

Important: If the devices are to be used during the connection, they must be plugged in before the connection is established. If they are not plugged in, however, it does not lead to an error.

Note: This function only works with a limited device circle, which can only be determined by testing.

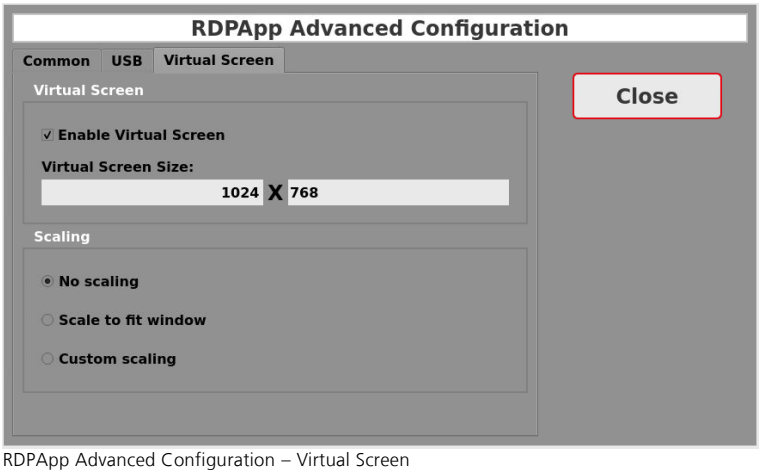
Setting up the Windows host ("Group Policy Editor")

Important: However, this function only works if the Windows host has been configured accordingly. For this, the "Group Policy Editor" gpedit.msc is required (start from the command line as administrator). The following settings must be made.

- Computer Configuration/ Administrative Templates/ Windows Components/ Remote Desktop Services/ Remote Desktop Connection Client/ RemoteFX USB Device Redirection/ All RDP Redirection = Enable
- Computer Configuration/ Administrative Templates/ Windows Components/ Remote Desktop Services/ Remote Desktop Session Host/ Remote Session Environment/ Configure RemoteFX = Enable
- Computer Configuration/ Administrative Templates/ Windows Components/ Remote Desktop Services/ Remote Desktop Session Host/ Connections/ Allow user to connect remotely using Remote DesktopServices = Enable
- Computer Configuration/ Administrative Templates/ Windows Components/ Remote Desktop Services/ Remote Desktop Session Host/ Device and Resource Redirection/ Do not allow supported Plug and Play device redirection = Disable
- gpupdate /force
- Perform reboot of the host

Setting up the Windows host (device driver)

- Appropriate drivers for the USB device are required on the Windows host.



RDPApp Advanced Configuration – Virtual Screen

Area	**Virtual Screen** **„Enable Virtual Screen“:**
Input fields	Enabless the virtual screen and uses the screen resolution specified below instead of using the physical screen resolution or that of the window in the multi-connection view. **„Virtual Screen Size“:** Specifies which screen resolution is to be used for this connection.
Button	**„Close“:** Switch to the previous view (see section 7.4 - Connection parameterization RDPApp).

Area	Selection points

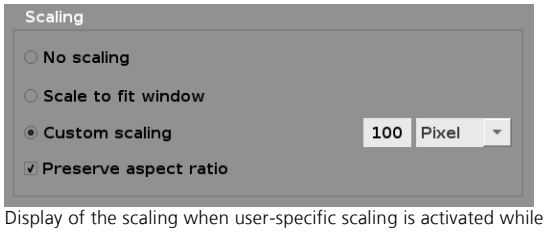
„Scaling“

Selection of the scaling model:

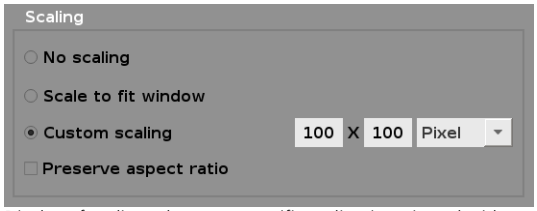
- „No scaling“:
  The received RDP images are displayed in the same resolution as they are transmitted from the server. This may cause the display to show black borders or scroll bars.

- „Scale to fit window“:
  The received RDP images are scaled to fill the entire screen. If additionally, "Keep aspect ratio" is selected, the aspect ratios are kept and black borders (top/bottom or sideways) may occur.

- „Custom scaling“:
  Any scaling in pixels or percent from the original resolution can be selected. If "Preserve aspect ratio" is also selected, the same scaling factor is used for X and Y direction. Otherwise, different scaling factors can be used for X and Y direction.



Display of the scaling when user-specific scaling is activated while maintaining the aspect ratios (Percent / Pixel selection).



Display of scaling when user-specific scaling is activated without maintaining the aspect ratios (Percent / Pixel selection).

7.4.3 Accessibility Test

Server accessibility dialog

Button

„Start Test“:

Checks the server accessibility by means of an ICMP request (echo). The maximum waiting time for a response from the server can be made via the timeout setting. The status of the test is displayed as follows:

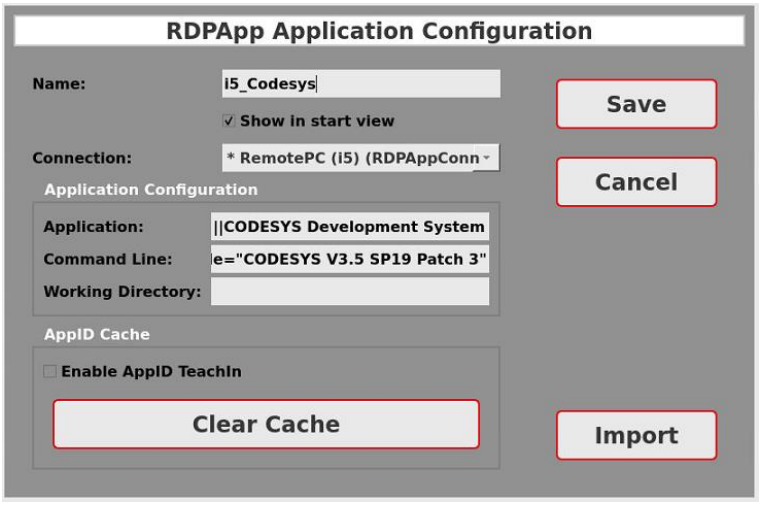
- Black LED: Ready
- Yellow LED: Running…
- Red LED: Host is not available
- Green LED: Host is available

„Close“:

The Dialog is closed.

7.4.4 Application Configuration RDPApp

The connection type for the application configuration is "RDPApp (application)".



RDPApp Application Configuration

Input fields

„Name“:

Descriptive name of the connection - displayed in the connection view and on the home page.

„Show in start view“:

This can be used to specify whether this connection should be displayed or hidden in the start view. This is used, for example, if a connection is part of a multiple connection and should not be displayed individually.

„Connection“:

Selection of the connection to be used for communication with the server. Only connections whose maximum number of connections has not yet been reached are displayed.

Area „Application Configuration“

Input fields

„Application“:

Identifier of the application to be started. The identifier is usually not entered manually, but by importing the rdp file with the configuration of the RDPApp connection.

„Command Line“:

Additional command line parameters with which the application is to be started (optional).

„Working Directory“:

Working directory in which the application is to be started (optional).

Area „AppID Cache“

Application windows are assigned to the application and therefore to the application's display area using so-called AppIDs. This is particularly important in the multiple view, as otherwise windows belonging to the application will appear in the wrong application view. To prevent this, the AppIDs belonging to an application can be collected in a cache.

To set up the AppID cache, first delete the cache and activate the AppID TeachIn. The application is then started in a single view and operated as usual. No connection changes should be made here, as this may result in incorrect AppIDs being recorded. The connection is then disconnected and the AppID TeachIn is deactivated again.

Input field

„Enable AppID TeachIn“:

Activates the AppID TeachIn, with which the AppID cache is filled with the AppIDs belonging to the application.

Control element

„Clear Cache“:

Clear the AppID cache.

Schaltflächen

„Save“:

The settings or their changes are saved (but not yet in the configuration file!) and it is switched back to the previous view (see section 6 - Connection view).

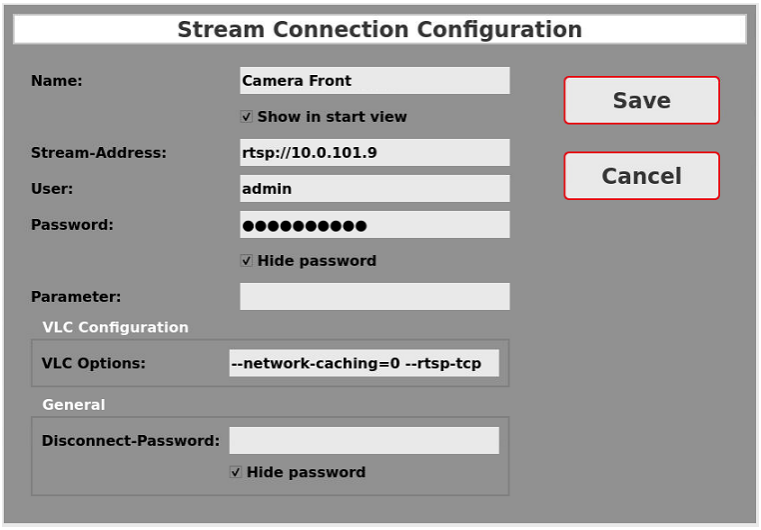
„Cancel“:

The settings or their changes are discarded and the program switches back to the previous view (see section 6 - Connection view).

„Import“:

A file-open dialog is used to load an rdp file with the configuration of the RDPApp connection. The configuration file can be created on the RDP host computer with the help of the RemoteApp tool (see also the web page https://github.com/kimmknight/remoteapptool).

7.5. Connection parameterrization Stream



Stream connection configuration

Input fields

„Name“:

Descriptive name of the connection - displayed in the connection view and on the home page.

“Show in start view”:

This can be used to specify whether this connection should be displayed or hidden in the start view. This is used, for example, if a connection is part of a multiple connection and should not be displayed individually.

„Stream-Address:

Stream URL / source address. A fully qualified identifier is expected here, including the protocol to be used (such as http, rtp, mms, rtsp, or file). A port specification can optionally be appended to the URL with ":".

„User“:

If a user name is required to log in to the stream source, it can be specified here. This parameter is optional.

„Password“:

If a password is required to log in to the stream source, it can be specified here. This parameter is optional.

- Passwords are stored encrypted in the configuration file.

Control element

„Hide password“:

This can be used to switch between plain text display and hidden display of the password. This setting is not saved.

„Parameter“:

If additional settings are required to configure the stream source (see stream source documentation), they can be specified here in the form "param1=value1&param2=value2…&paramN=valueN". They will then be appended to the URL when the connection is established.

Area „VLC Configuration“

Input field **„VLC Options“:**

Options that are passed to the vlc library and are required to configure the connection (e.g. caching and communication protocols).

Area „General“

Input field **„Disconnect-Password“:**

Password that must be entered to exit the stream viewer and return to the start page. This parameter is optional.

- Passwords are stored encrypted in the configuration file.

Control element **„Hide password“:**

This can be used to switch between the plain text display and the hidden display of the password. This setting is not saved.

Buttons

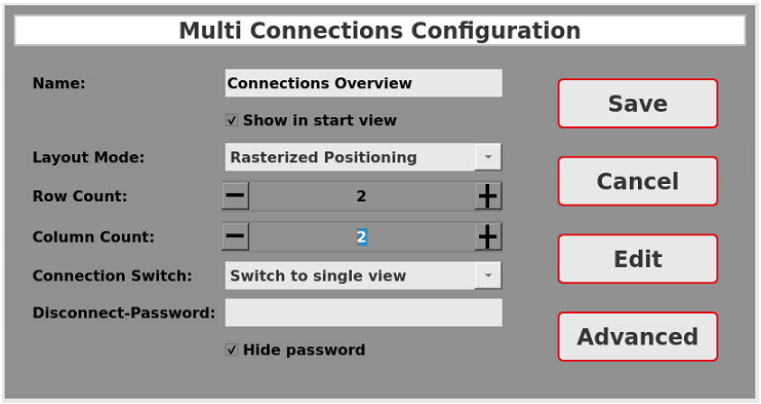
„Save“:

The settings or their changes are saved (but not yet in the configuration file!) and it is switched back to the previous view (see section 6 - Connection view).

„Cancel“:

The settings or their changes are discarded and the program switches back to the previous view (see section 6 - Connection view).

7.6. Connection parameterization Multi



Multiple connection configuration

Input fields

„Name:

Descriptive name of the connection, displayed in the connection view and on the home page.

“Show in start view”:

This can be used to specify whether this connection should be displayed or hidden in the start view. This is used, for example, if a connection is part of a multiple connection and should not be displayed individually.

“Layout Mode”:

The multiple connection view allows two layout modes: the rasterized or the free, pixel-precise positioning of the individual viewers. With free positioning, overlapping of the individual viewers is also possible, whereby the active viewer is always displayed completely.

„Row count”:

Number of rows to be used when positioning the viewers in a grid. If viewers are already configured, the value can only be reduced as far as free rows are available at the edge.

For free positioning, this value is always 1.

„Column count”:

Number of columns to be used when positioning the viewers in a grid. If viewers are already configured, the value can only be reduced as far as free columns are available at the edge.

For free positioning, this value is always 1.

„Connection Switch”:

Specification of how the switching of the active connection responding to inputs is to take place. The following modes are available: Switch to single view, Enable view (Tap'n'Hold) and Enable view (Simple Touch). For details see section 11.6.1 - Connection switching).

Input field

„Disconnect-Password“:

Password that must be entered to be able to exit the multiple connection view and return to the home page. This parameter is optional.

- Passwords are stored encrypted in the configuration file.

Control element

„Hide password“:

This can be used to switch between plain text display and hidden display of the password. This setting is not saved.

Buttons

„Save“:

The settings or their changes are saved (but not yet in the configuration file!) and it is switched back to the previous view (see section 6 - Connection view).

„Cancel“:

The settings or their changes are discarded and the program switches back to the previous view (see section 6 - Connection view).

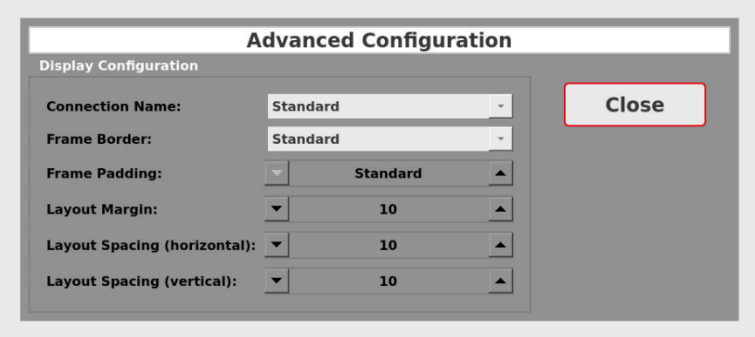
„Edit“:

The display editor will be opened (see section 7.6.2 - Display configuration "Rasterized positioning" or section 7.6.3 - Display configuration "Free positioning").

„Advanced“:

Switch to the advanced connection parameterization (see section 7.6.1 - Advanced connection parameterization Multi).

7.6.1 Advanced connection parameterization Multi



Multi Advanced configuration

Area

Display Configuration

The differences of the representation options are discussed in the section 11.6.2 - Display options.

Input fields

„Connection Name“:

Specifies whether and how the connection name should be displayed when the connection is changed. The following settings are available: Standard, Show, Hide and Overlay (with timeout).

„Frame Border“:

Specifies whether and how a frame is to be placed around the display of the connection contents. The following settings are available: Standard, Without Border, Static Border and State Dependent Border.

„Frame Padding“:

Specifies the distance between frame and connection contents. You can choose between standard and a value in pixels. Specifies the distance between frame and connection contents. You can choose between standard and a value in pixels.

„Layout Margin“:

Specifies the distance between the display edge and the frame or connection content in pixels.

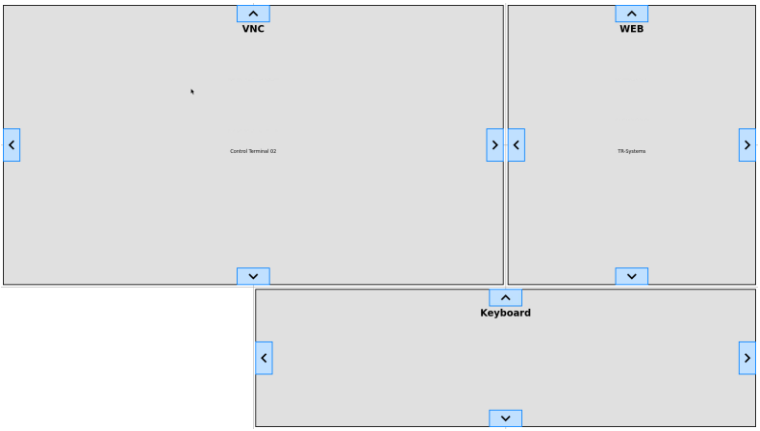
„Layout Spacing (horizontal)“:

Specifies the horizontal distance between the individual frames or connection contents in pixels.

„Layout Spacing (vertical)“:

Specifies the vertical distance between the individual frames or connection contents in pixels.

7.6.2 Display configuration "Rasterized positioning"

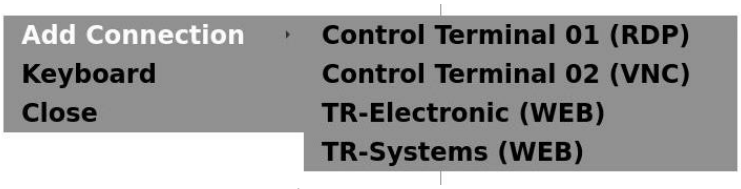


Display editor with 3x3 grid

With the gridded display, views can be arranged in a fixed grid. The grid can be adjusted almost arbitrarily (max. 99 rows or columns). Views can be extended to several rows or columns. Overlapping of views is not possible.

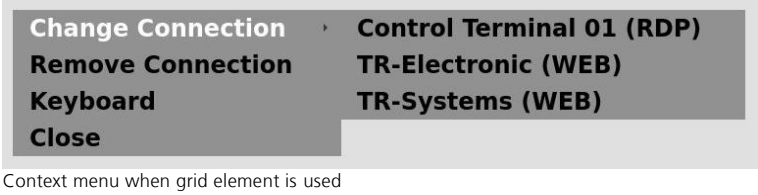
For each view the connection type and the connection name are displayed. In addition, moving elements are available (right, left, top and bottom as bluish elements with arrow), with which the views can be enlarged or reduced.

If desired, a keyboard that is permanently displayed on the screen can be used instead of the fade-in keyboard. This can be embedded in the grid just like a view. Only one keyboard can be embedded.



Context menu when grid element is free

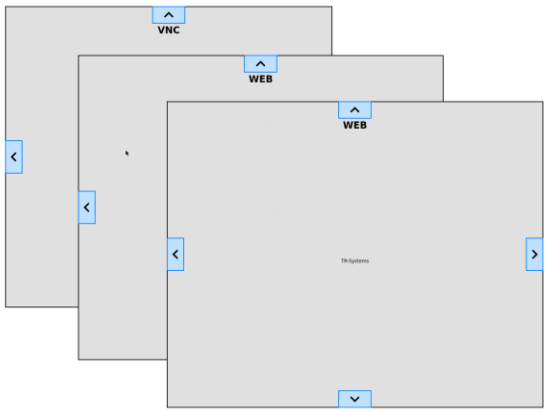
After a right-click or Tap'n'Hold (longer pressing of the Touch until the menu is displayed) on a free grid element, the above context menu is displayed. With the available options a new view or keyboard can be inserted. The menu item "Keyboard" is only available if no keyboard has been inserted yet. The menu item "Close" is used to exit the display editor.



Context menu when grid element is used

After a right-click or Tap'n'Hold (longer pressing of the touch until the menu is displayed) on a used grid element, the above context menu is displayed. Here you can change the connection of the active view or delete the view. The menu item "Keyboard" is only available if no keyboard has been inserted yet. The menu item "Close" is used to exit the view editor.

7.6.3 Display configuration "Free positioning"



Display editor for free positioning

With the freely positionable display, the views can be arranged on the screen with pixel precision. Overlaps are possible here. By clicking on the rear views, they can be brought to the front.

The connection type and connection name are displayed for each view. In addition, moving elements are available (right, left, top and bottom as bluish elements with arrow), with which the views can be enlarged or reduced.

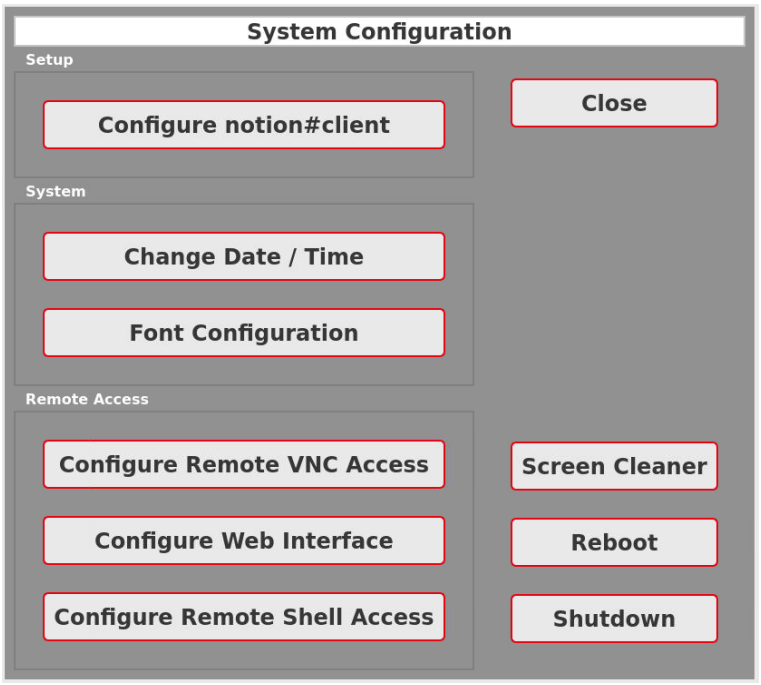
If desired, a keyboard that is permanently displayed on the screen can be used instead of the fade-in keyboard. This can be embedded in the display just like a view. Only one keyboard can be embedded.

The context menus here correspond to those from the "Rasterized positioning" display configuration (see there).

When exporting this connection to a notion#client with a different screen resolution, please note that there is no automatic adjustment to the other resolution. Individual views could therefore lie outside the visible area.

8. Parameterization view "System”

In this parameterization view, both the remote client and the system as such can be configured. For the remote client, for example, the language or the screen rotation can be adjusted. In the "System" section, it is the setting of the system time and the system date as well as the available fonts that can then be used with the WebViewer.



System configuration

Area Setup

Button **„Configure notion#client":**

Configuration of the notion#client (see section 8.1 - Configure notion#client).

Area System

Buttons **„Change Date / Time”:**

Setting the system time or system date (see section 8.2 - Change Date / Time)

„Font Configuration”:

Displays the installed fonts. You can also install additional fonts or uninstall existing fonts (see section 8.3 - Font settings).

Area

Remote access

Buttons

"Configure Remote VNC Access":

Configures remote maintenance access from notion#client via VNC (see section 8.4 - Configure Remote VNC Access).

"Configure Web Interface":

Configures access to the web interface of notion#client (see section 8.5 - Configure Web Interface).

„Configure Remote Shell access":

Configures remote maintenance access from notion#client via SSH (see section 8.6 - Configure Remote Shell Access).

Button

„Close":

Switches back to the parameterization view (see section 5 - Parameterization view).

„Screen Cleaner":

Activates the screen cleaning mode (see section 8.7 - Screen cleaning).

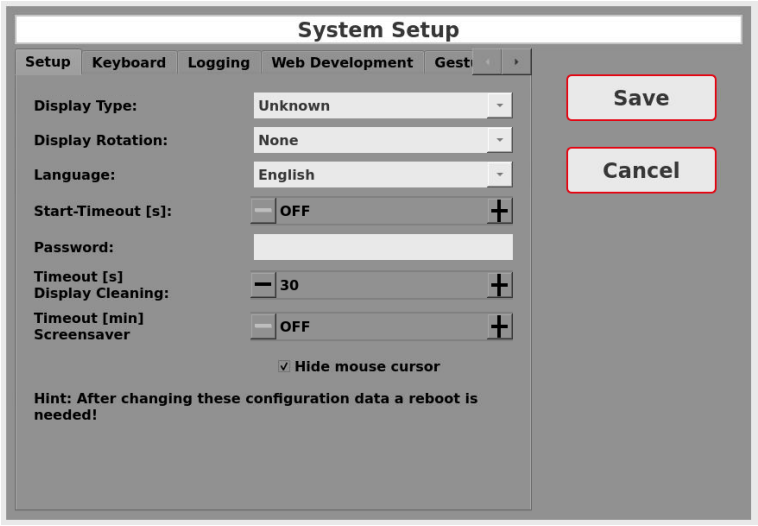
„Reboot":

Performs a restart of the notion#client.

„Shutdown":

Puts the notion#client in a safe state to power off

8.1. Configure notion#client



System setup – Setup

Area

Selection fields

Setup

„Display Type“:

The display of the notion#client is influenced by the selection of the display type. Depending on the available screen size and screen resolution, the elements of the dialogs may be positioned at different locations. A restart of the system is required to activate this setting.

„Display Rotation“:

Depending on the installation position of the device, the display can also be rotated (in 90° steps). When rotating 90° or 270°, the elements of the dialogs may be positioned at other places. A restart of the system is required to activate this setting.

„Language“:

Setting of the display language. A system restart is required to activate this setting. The following language setting is offered: English, German.

Input fields

„Start-Timeout [s]“:

This can be used to specify how long (in seconds) to wait after starting the application until the last active connection is established. A value of -1 (display OFF) results in no automatic connection establishment. To activate this setting, a restart of the system is required.

„Password“:

Password to get from the start page to the parameterization view (also called admin password). If a password is specified, a password query appears when switching to the parameterization view (see section 3.2 - Password input).

„Timeout Display Cleaning“:

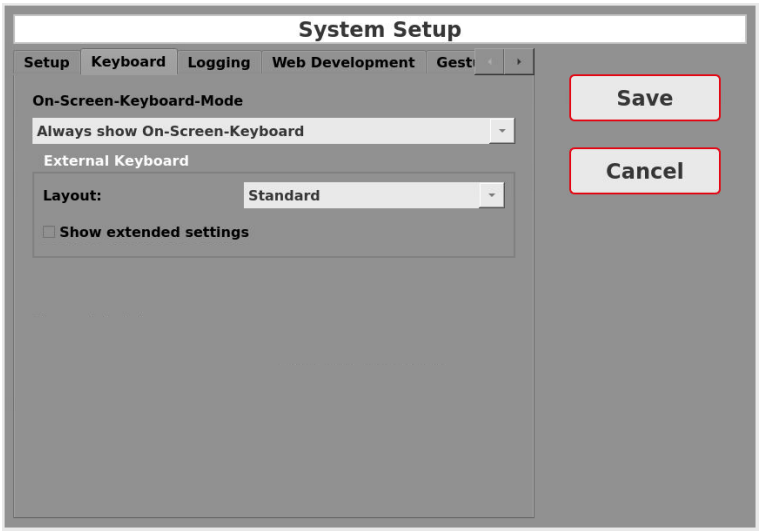
Time period in seconds during which the touch screen is deactivated in the screen cleaning function. A system restart is required to activate this setting.

"Timeout Screensaver":

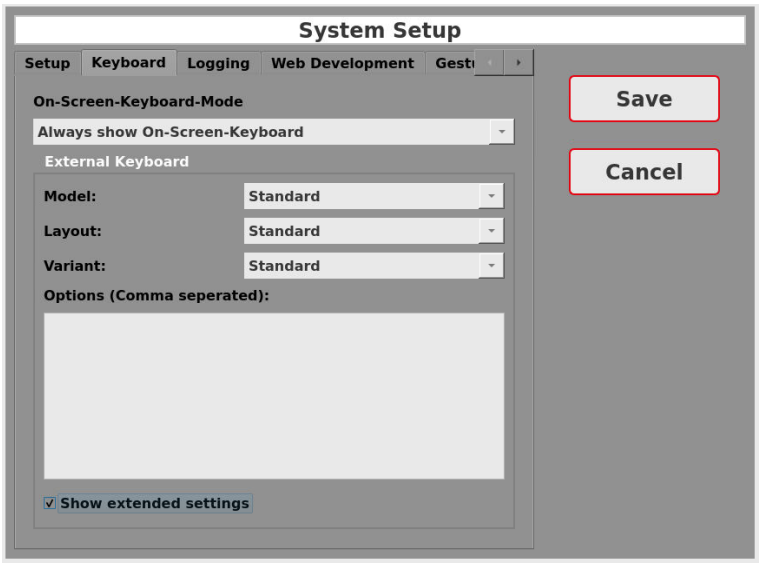
Specifies after what period of time without user activity the screen saver should be activated. The value is given in minutes. The screen saver function can also be switched off completely (time period is set to "OFF").

„Hide mouse cursor“:

Hide mouse pointer when using the touch. If an external mouse is connected, the mouse pointer is displayed regardless of this setting.



System setup - Keyboard



System setup - Keyboard (Advanced settings)

Area

Selection fields

Keyboard / External keyboard (Advanced Settings)

„On-Screen-Keyboard-Mode“:

Selection of when the On-Screen-Keyboard should be displayed. The following modes are available: “Always show On-Screen-Keyboard”, “Always hide On-Screen-Keyboard”, “Only hide On-Screen-Keyboard in Viewer”.

„Model“:

Select your keyboard model here if you do not have a standard PC keyboard.

„Layout“:

Select the country-specific keyboard layout here. If Standard is selected, the country-specific keyboard layout of the set language is used (German or English).

„Variant“:

For some country-specific keyboard layouts, additional variants are available, which can be selected here.

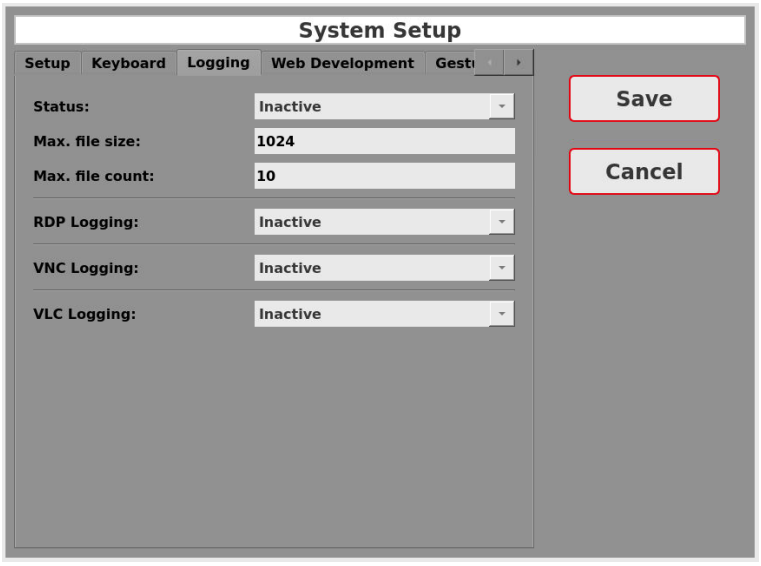
„Show extended settings“:

This allows you to show or hide the extended settings.

Input fields

„Options (comma separated)“:

Some exotic keyboards require even more options. You can find more information e.g. here: https://manpages.debian.org/buster/xkb-data/xkeyboard-config.7.en.html



System Setup - Logging (Advanced Settings)

Area

Logging
This can be used to configure the saving of log messages of the application.

Selection field

„Status“:

The "Status" element can be used to disable / enable logging and set the desired log level.

Input fields

„Max. file size“:

This sets the maximum file size for log file rotation.

„Max. file count“:

This determines how many files are rotated over.

Selection fields

„RDP Logging“

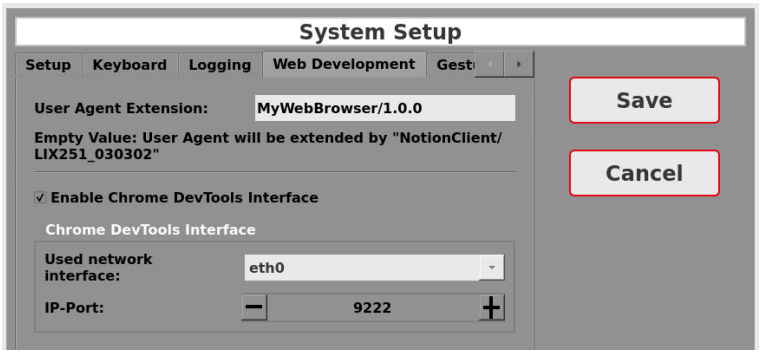
This can be used to separately disable / enable logging of the RDP library. and set the desired log level. There is no log file rotation.

„VNC Logging“:

This allows logging of the VNC library to be separately disabled / enabled. There is no log file rotation.

„VLC Logging“:

This allows logging of the VLC library (Stream View) to be separately disabled / enabled. The log entries are added to the default log file.



System Setup –Web Development

Area

Web Development

The default user agent text of the browser can be extended by a device-specific specification.

Input fields

"User Agent Extension":

Device-specific extension of the user agent text.

"Enable Chrome DevTools Interface":

The Chrome DevToolscan be activated for remote debugging of web applications.

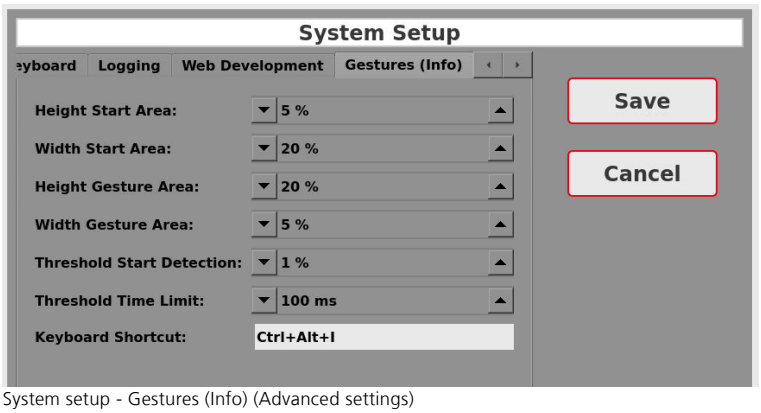
Input fields

„Used network interface":

Specification of the network interface over which debugging is to take place.

„IP-Port":

Specification of the IP port to be used by Chrome DevTools.



System setup - Gestures (Info) (Advanced settings)

Area

Gestures (Info)

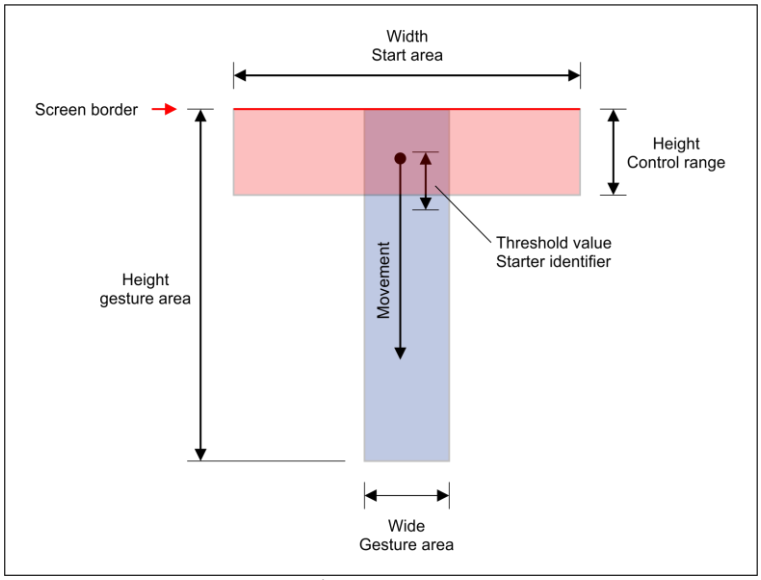
The info gesture is a swipe gesture that starts at the top of the screen and is performed straight down. It is used to show the status display of the viewers. In order to be able to use different touch models optimally, the parameterization of gesture recognition has been introduced.

The gesture start is recognized if the start point of the gesture is within the start area (see sketch). The start area is defined by the height specification (in percent of the screen height) and the width specification (in percent of the screen width). It is centered at the top of the screen.

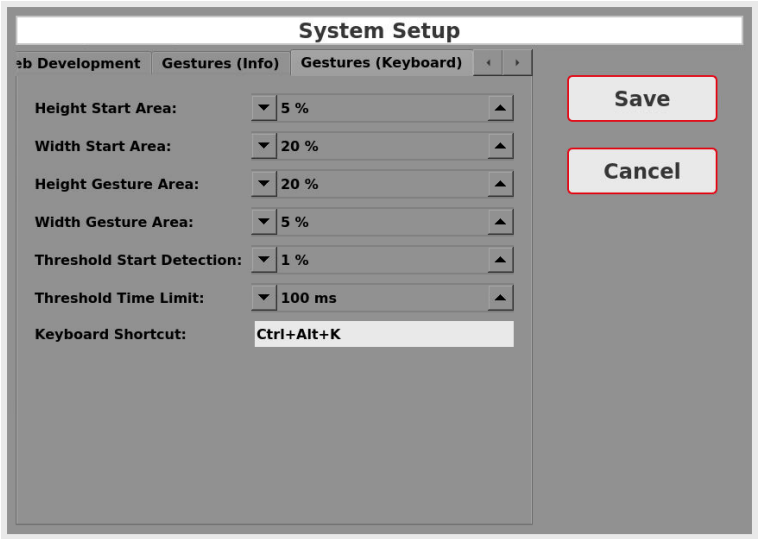
To distinguish to whom the gesture applies (notion#client or the remote system), the gesture speed is evaluated. If the threshold value of the start recognition (in percent of the screen height) is covered within the time limit (i.e. fast movement), the gesture is assigned to the notion#client and the recognition continues. In the other case (i.e. slow or no movement), the information is forwarded to the remote system.

Then, the gesture must be continued in the gesture area. This is defined by the height specification (as a percentage of the screen height) and the width specification (as a percentage of the screen width). If the gesture area is left to the side - the gesture is performed too obliquely - the gesture recognition is aborted. If, on the other hand, the gesture area is exited downwards, the gesture recognition is successfully completed and the status display is shown.

Using the keyboard shortcut, the status display can also be shown via an external keyboard or a VNC remote session.



System setup - Gesture recognition (Info) (Advanced settings)



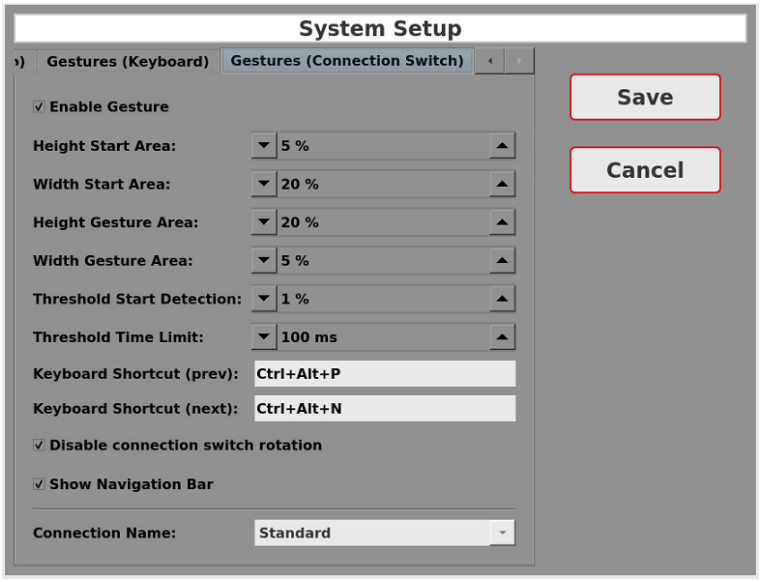
System Setup - Gestures (Keyboard) (Advanced Settings)

Area

Gestures (keyboard)

The keyboard gesture is a swipe gesture that starts at the bottom of the screen and is performed straight up. It is used to fade in the keyboard. In order to be able to use different touch models optimally, the parameterization of gesture recognition has been introduced.

Gesture recognition works in principle as explained before. The difference is only in the direction of movement.



System Setup - Gestures (Connection Switching) (Advanced Settings)

Area

Gestures (connection switching)

The connection switching gestures are two swipe gestures. The first one starts at the right edge of the screen and is performed horizontally to the left. The second, on the other hand, starts at the left edge of the screen and is performed horizontally to the right. These are used to switch between connections in the connection view without having to switch back to the connection view. The switching is done in the order in which the connections are listed in the connection view.

Note: In this mode, the connections that are hidden in favor of another connection are not closed. The connections and the communication remain in order to realize a quick switch between the views without a new, lengthy connection setup. With many active connections there is therefore an increased resource requirement (CPU, memory, network).

Selection field

„Enable gesture“:

This can be used to activate connection switching by means of a swipe gesture.

„Disable connection switch rotation“:

By default, when the last entry in the connection list is reached, swiping rotates back to the first entry in the connection list and vice versa. This option deactivates the rotation and stops it when the first or last entry in the connection list is reached.

„Show Navigation Bar“:

Displays a navigation bar at the bottom of the screen, as you would see on a cell phone, for example.

Each element of the connection list is displayed with a dot. The enlarged dot represents the current connection. The connection status is visualized via the colors:

- Blue: The viewer has not yet been initialized and the connection is not yet active.
- Yellow: The connection is currently being established or terminated.
- Green: The connection is active.
- Red: The connection has been disconnected.

„Connection name“:

Here you can configure whether and how the connection name should be displayed after switching to another connection. The fol61lowing settings are available: Standard, Fade in, Fade out, Overlay (with timeout). With the last setting, a timeout in seconds can also be specified.

Buttons

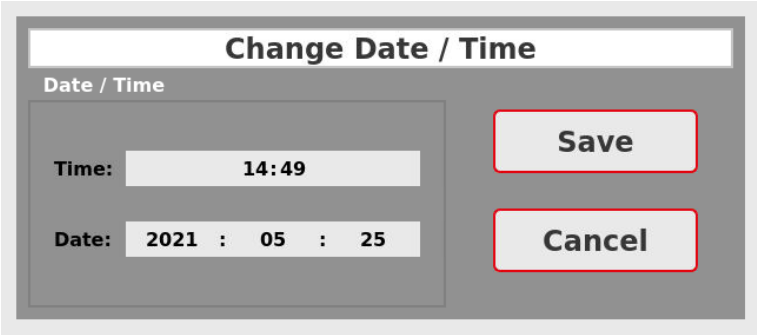
„Save“:

The settings made are saved and you switch to the previous view (see section 8 - Parameterization view "System“).

„Cancel“:

Any settings made will be discarded and you will be returned to the previous view (see section 8 - Parameterization view "System“).

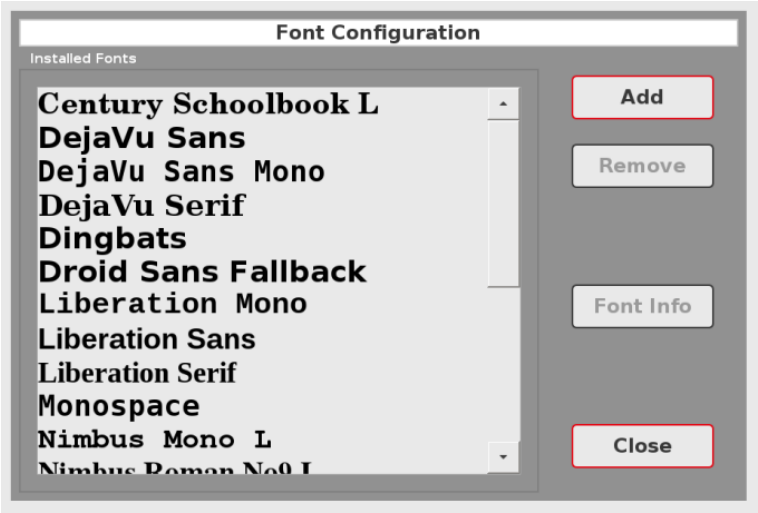
8.2. Change Date / Time



Time / date setting

Area	
Input fields	„Date / Time“ **„Time“:** For setting the current time. **„Date“:** To set the current date.
Buttons	**„Save“:** The values are accepted with the "Save" button. The program then switches to the previous view (see section 8 - Parameterization view "System”). **„Cancel“:** The "Cancel" button cancels any settings you may have made and returns you to the previous view (see section 8 - Parameterization view "System”).

8.3. Font settings



This dialog shows the fonts installed on the system with a font sample.

Buttons

„Add“:

This can be used to install additional fonts (see section 8.3.1 - Add).

„Remove“:

This can be used to remove the selected font. Please note that system fonts cannot be removed. This can be recognized by the fact that the "Remove" button is not activated.

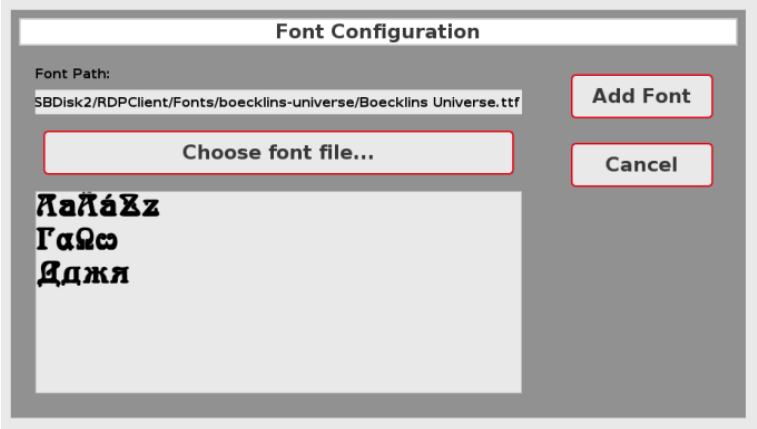
„Font Info“:

A font sample is displayed from the selected font set (see section 8.3.3 - Font info).

„Close“:

Return to the previous view (see section 8 - Parameterization view "System“).

8.3.1 Add



In this dialog another font can be installed from a USB stick. Only True Type Fonts (TTF) are supported. If a font has been selected, a font sample is displayed.

Input field **„Font Path“:**

Path of the selected font.

Button **„Choose font file ...“:**

Selection of the font file (see section 8.3.2 - Choose font file...).

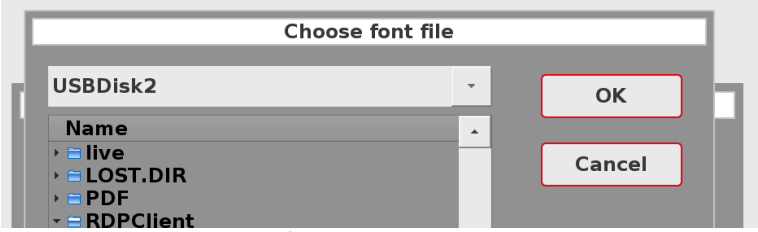
„Add Font“:

Installs the font on the system and returns to the previous view (see section 8.3 - Font settings).

„Cancel“:

Jumps back to the previous view without installing the font (see section 8.3 - Font settings).

8.3.2 Choose font file...

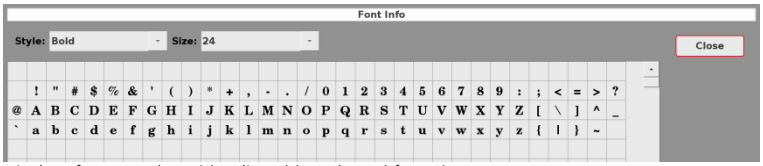


File selection dialog with standard functionality

The desired USB stick can be selected in the upper selection box. They are assigned the name "USBDisk1" to "USBDisk9" depending on the insertion sequence.

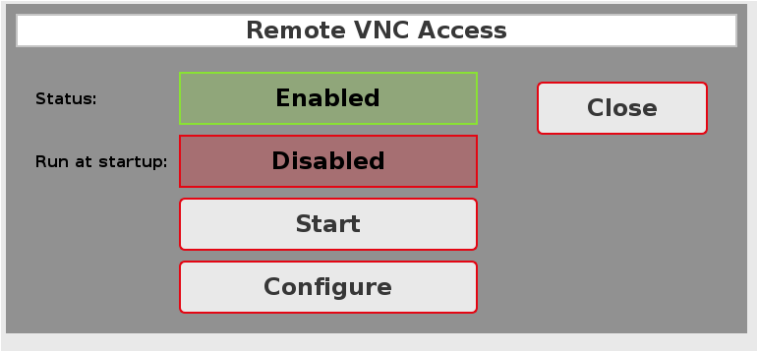
Below that the desired file can be selected. Subdirectories are marked with a small arrow and can be expanded or collapsed.

8.3.3 Font info



Displays font samples with adjustable style and font size.

8.4. Configure Remote VNC Access



With this dialog the VNC remote access can be set up on the notion#client.

Selection fields

„Status":

Enable or disable VNC access

„Run at startup":

Specifies whether VNC access should be restarted automatically after the system reboots.

Buttons

„Start" or „Stop":

Starts / stops the VNC access

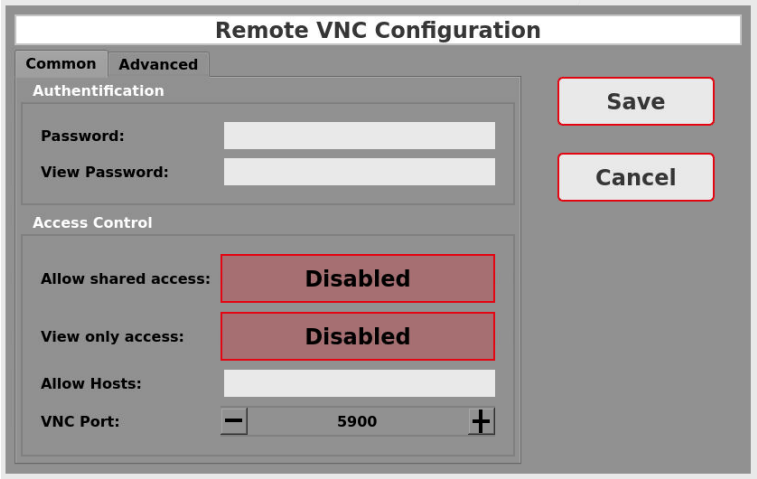
„Configure":

Configuration of the VNC access (see section 8.4.1 - Configure).

„Close":

Switch to the previous view (see section 8 - Parameterization view "System").

8.4.1 Configure



Configure VNC remote access

Area
Input fields

Authentication

„Password“:

Password that must be specified when logging in to the VNC server for full access. This parameter is optional.

„View Password“:

Password that must be specified when logging in to the VNC server for read-only access. This parameter is optional.

Area
Selection fields

Access control

„Allow shared access“:

Allow parallel access from multiple notion#client to the VNC server.

„View only access“:

Allow view-only access to the VNC server.

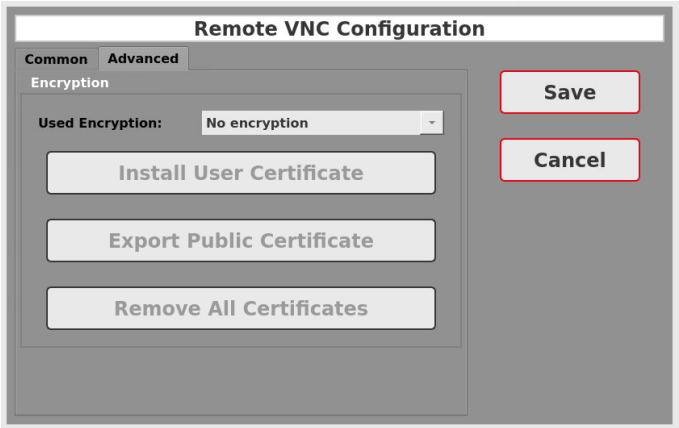
Input field

„Allow Hosts“:

Comma-separated list of hostnames or IP addresses that are allowed to access this VNC server. To allow whole subnets, the format "172.1.17." with trailing dot can be used. This parameter is optional.

„VNC Port“:

IP-Port to be used by the VNC server.



Configure VNC remote access - Advanced

Area	Selection field

Encryption
Connection encryption for libvncclient-based viewers.

Buttons

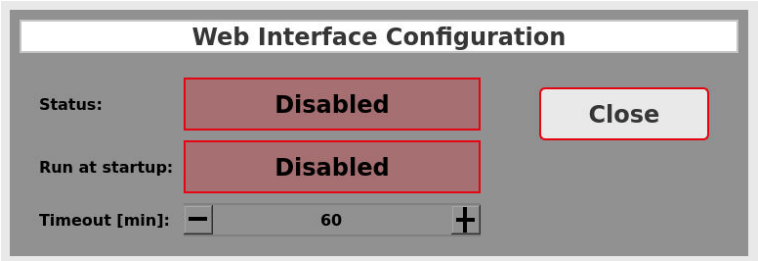
„Save“:

Save the settings and return to the previous view (see section 8.4 - Configure Remote VNC Access).

„Cancel“:

The "Cancel" button cancels any settings you may have made and returns you to the previous view (see section 8.4 - Configure Remote VNC Access).

8.5. Configure Web Interface



Web Interface Configuration

The web interface (see section 12 - Web-Interface) offers the possibility to make various settings and to perform a system update. In the default setting, the web interface is deactivated.

"Status":

Start or stop the web interface. The web interface is automatically stopped by a restart or by the expiration of the timeout.

"Run at startup":

Activate or deactivate the web interface. If this option is active, the web interface is started automatically at every time the system is started. The timeout for automatic shutdown does not apply here.

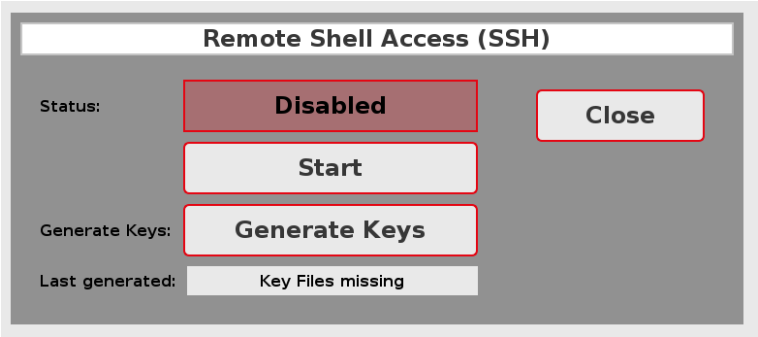
"Timeout [min]":

Time span until automatic shutdown of the web interface (in minutes).
The timeout can also be deactivated (display "OFF").

"Close":

Jumps back to the previous view (see Section 8 - "System" parameterization view).

8.6. Configure Remote Shell Access



This configuration dialog can be used to configure remote console access via SSH. This access can be used for remote error diagnostics if necessary.

Selection field

„Status":

Enable or disable the SSH diagnostic access.

Buttons

„Start" or „Stop":

Starts or stops the SSH access

„Generate Keys":

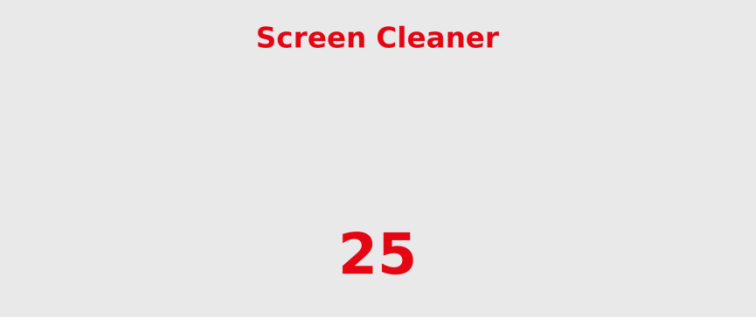
Before the SSH service is started for the first time, individual keys must be created for this notion#client. The field below ("Last generated") shows if and when these keys were created.

„Close":

Jumps back to the previous view (see section 8 - Parameterization view "System").

8.7. Screen cleaning

During an adjustable period of time (see section 8.1 - Configure notion#client) the touch screen is deactivated. A corresponding information page is then displayed with the remaining runtime (see following figure), which is then automatically hidden.



Display when screen cleaning function is active

9. Parameterization view "Network“

In this view, the status of the available network interfaces is displayed. It is also possible to switch to the configuration page of the respective network interfaces.

LED-Status

Display

Dark LED:

- Interface is deactivated
- interface is not available

Yellow LED:

- Interface is activated
- DHCP query running
- DHCP query failed
- No network link detected

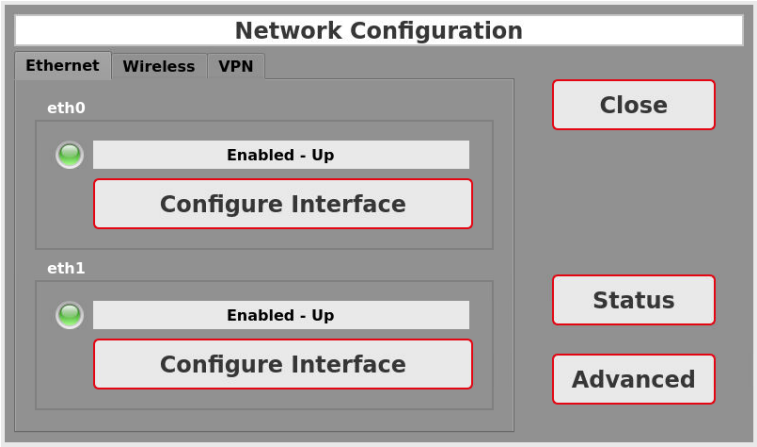
Green LED:

- Interface active

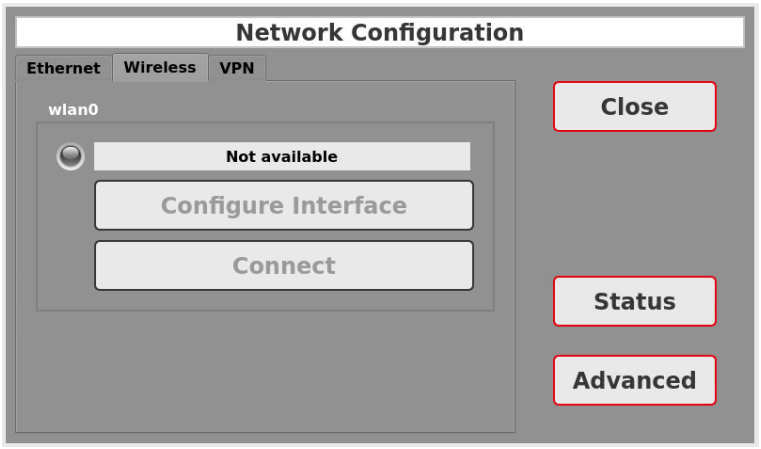
Button

„Configure interface“:

- Ethernet (see section 9.3 - Configure interface (eth0/eth1))
- WLAN (see section 9.4 - Configure interface (wlan0))
- VPN (see section 9.5 - Configure interface (vpn0))



This dialog shows the status of the network connection (Ethernet) by means of LED and status text.



This dialog shows the status of the network connection (Wireless) by means of LED and status text.

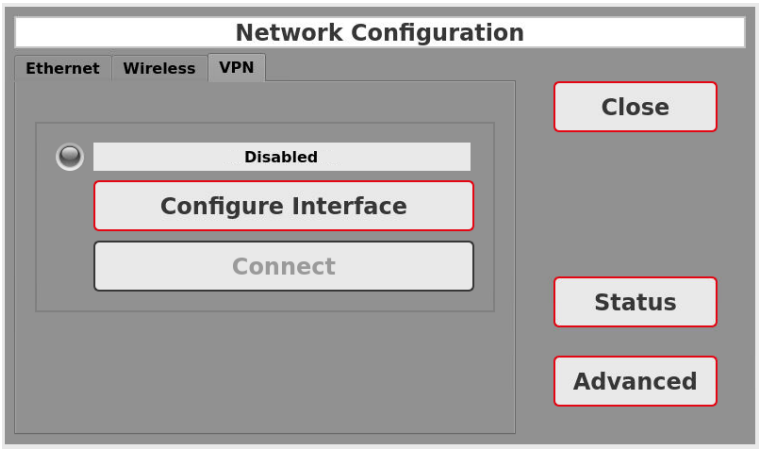
Area

Button

wlan0

“Connect" or "Disconnect:

Starts the connection or disconnection process of a previously configured WLAN connection.



This dialog shows the status of the network connection (VPN) by means of LED and status text.

Area

Button

vpn0

“Connect" or "Disconnect:

Starts the connection or disconnection process of a previously configured VPN connection.

Button

„Status“:

Displays the detailed status of each interface (see section 9.1 - Status).

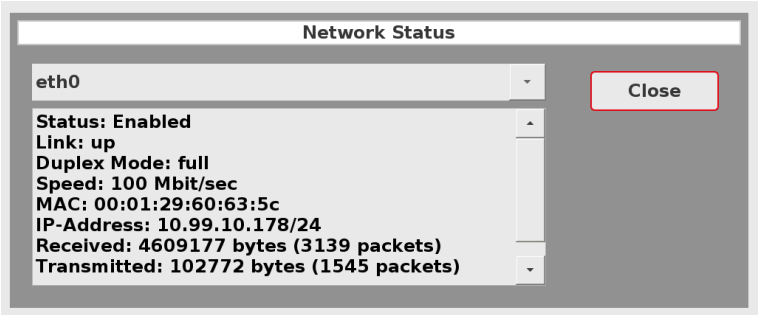
„Advanced“:

Allows you to set general network settings (see section 9.2 - Advanced).

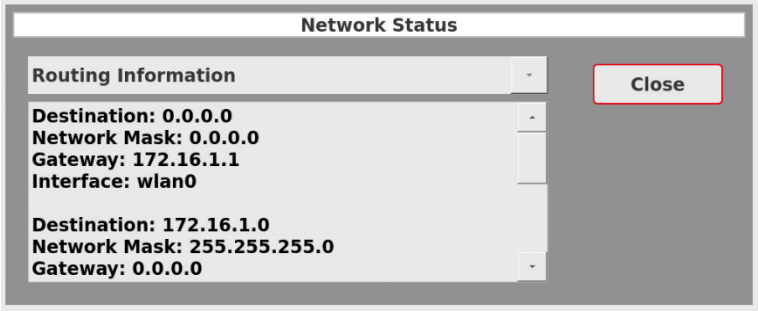
„Close":

Return to the previous view (see section 5 - Parameterization view). If changes have been made to the network configuration, the interfaces are reinitialized with the new settings.

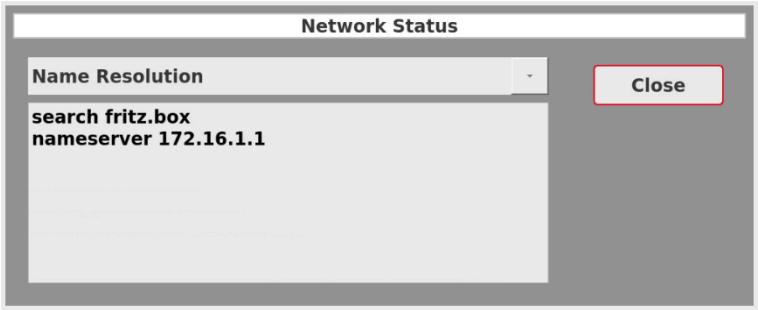
9.1. Status



Displays various information about the selected interface.

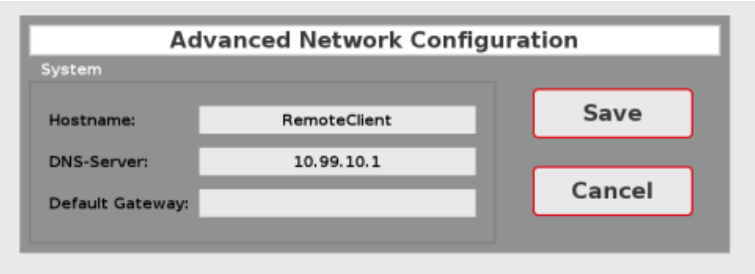


Active Routing Information



Name Resolution Information (DNS)

9.2. Advanced



Advanced network configuration

Area

Input fields

System

„Hostname“:

Host name of the remote client

„DNS-Server“:

Specification of the DNS server (may be overwritten by the DHCP client).

„Default Gateway“:

Default gateway of the remote client (may be overwritten by the DHCP client).

Buttons

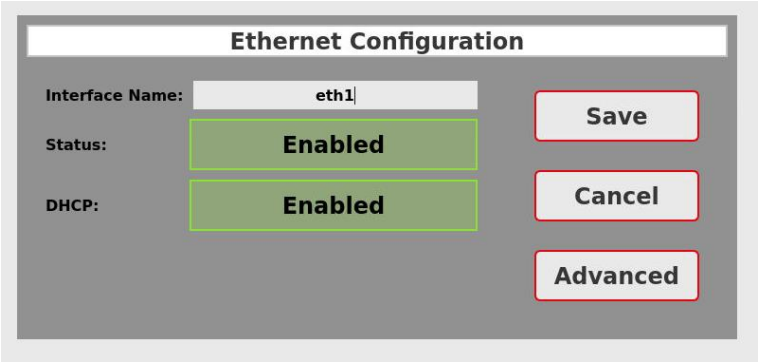
„Save“:

Save the settings and return to the previous view (see section 9 - Parameterization view "Network“).

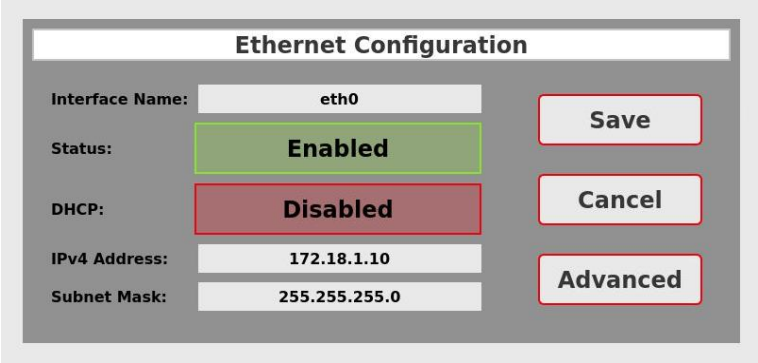
„Cancel“:

Return to the previous view (see section 9 - Parameterization view "Network“) without saving the settings.

9.3. Configure interface (eth0/eth1)



View with DHCP enabled



View with manual IP configuration

Input field

„Interface Name“:

Individual name of the interface used within the remote client to identify the interface.

Selection fields

„Status“:

Activates or deactivates the interface

„DHCP“:

Switches between DHCP and static network configuration.

Input fields

„IPv4 Address“:

Interface address for static network configuration

„Subnet Mask“:

Subnet mask for static network configuration

Buttons

„Save“:

Saves the settings and returns to the previous view (see section 9 - Parameterization view "Network").

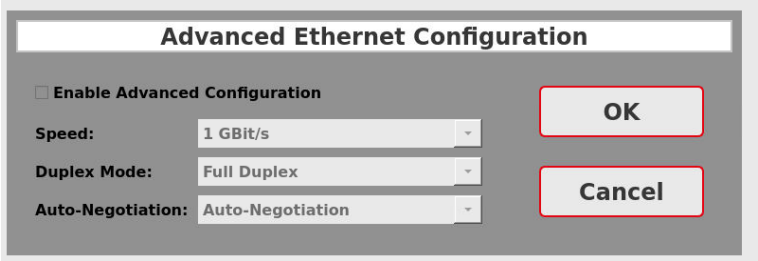
„Cancel“:

Return to the previous view without saving the settings (see section 9 - Parameterization view "Network").

„Advanced“:

The system switches to the advanced interface configuration (see section 9.3.1 - Advanced interface configuration (eth0/eth1)).

9.3.1 Advanced interface configuration (eth0/eth1)



Advanced network configuration

Selection field(s)

„Enable Advanced Configuration“:

Activates the following configuration items and deactivates the automatic interface configuration.

„Speed“:

Sets the speed at which the Ethernet interface should operate. The settings 100 Mbit/s and 1 GBit/s are available.

„Duplex-Mode“:

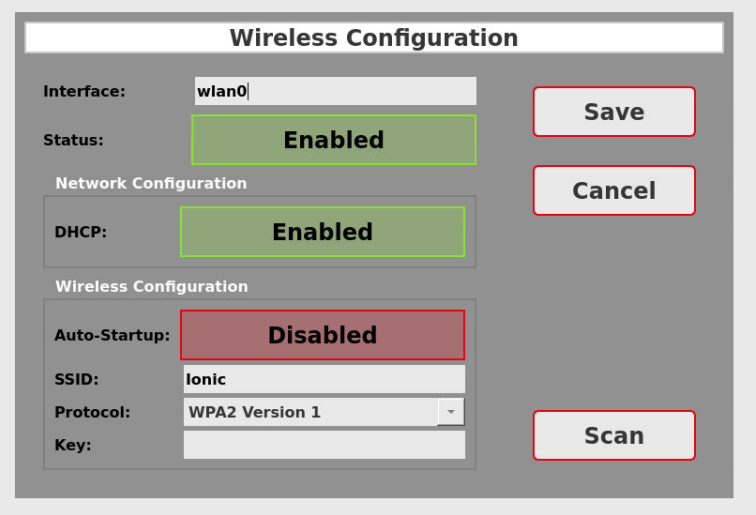
Sets the duplex setting of the Ethernet interface. The following settings are available: Half Duplex and Full Duplex.

„Auto-Negotiation“:

Specifies whether auto-negotiation should be used.

9.4. Configure interface (wlan0)

Note:
Only WLAN sticks from the TRsystems sales program are supported.



Wireless configuration

Input field **„Interface“:**

Individual name of the interface used within the remote client to identify the interface.

Selection field **„Status“:**

Activates or deactivates the interface

Area **Network configuration**

Selection field **„DHCP“:**

Switches between DHCP and static network configuration.

Input fields **„IPv4 Addresse“:**

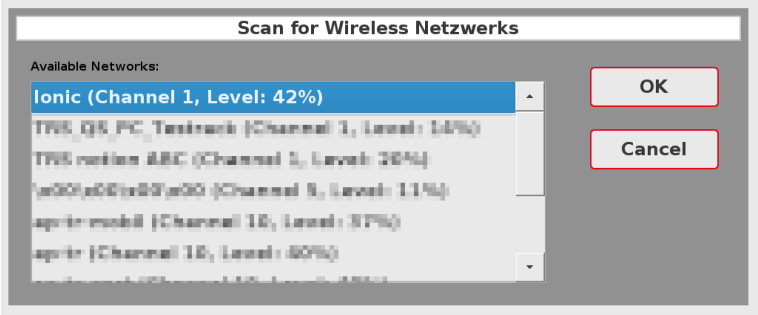
Interface address for static network configuration

„Subnet Mask“:

Subnet mask for static network configuration

Area	**WLAN configuration**
Selection field	**”Auto-Startup”:** Specifies whether the WLAN interface should be activated automatically when the system is started or should be started manually by the user later.
Input field	**„SSID“:** WLAN network name
Selection fields	**„Protocol“:** WLAN protocol (WPA / WPA2)
Input field	**„Key“:** WLAN-Password
Button	**„Save“:** Saves the settings and returns to the previous view (see section 9 - Parameterization view "Network“). **„Cancel“:** Return to the previous view without saving the settings (see section 9 - Parameterization view "Network“). **„Scan“:** Starts a WLAN scan and switches to the display and selection of available networks (see section 9.4.1 - Scanning).

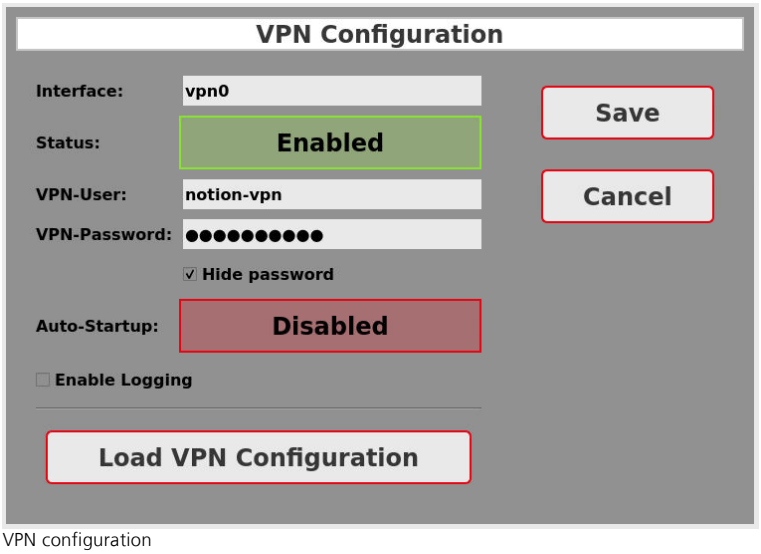
9.4.1 Scanning



Displays all available WLAN networks incl. WLAN channel and reception strength.

The desired network can be selected and accepted with the "OK" button. "Cancel" jumps back to the previous view without selection.

9.5. Configure interface (vpn0)



VPN configuration

Input field **„Interface“:**

Individual name of the interface used within the remote client to identify the interface.

Selection field **„Status“:**

Activates or deactivates the interface

Input fields **„VPN-User“:**

User name for logging in to the VPN server.

„VPN-Password“:

Password for logging in tot he VPN server.

Control element **„Hide password“:**

This can be used to switch between plain text display and hidden display of the password. This setting is not saved.

Selection field **”Auto-Startup“:**

Specifies whether the VPN interface should be activated automatically when the system is started or should be started manually by the user later.

Control element **„Enable Logging“:**

Activates the logging of the OpenVPN client. The log file can be downloaded via the log file export and evaluated for error analysis.

Button

„Save":

Saves the settings and returns to the previous view (see section 9 - Parameterization view "Network").

„Cancel":

Return to the previous view without saving the settings (see section 9 - Parameterization view "Network").

„Load VPN Configuration":

Opens a file selection dialog that can be used to install the VPN configuration file (OpenVPN format).

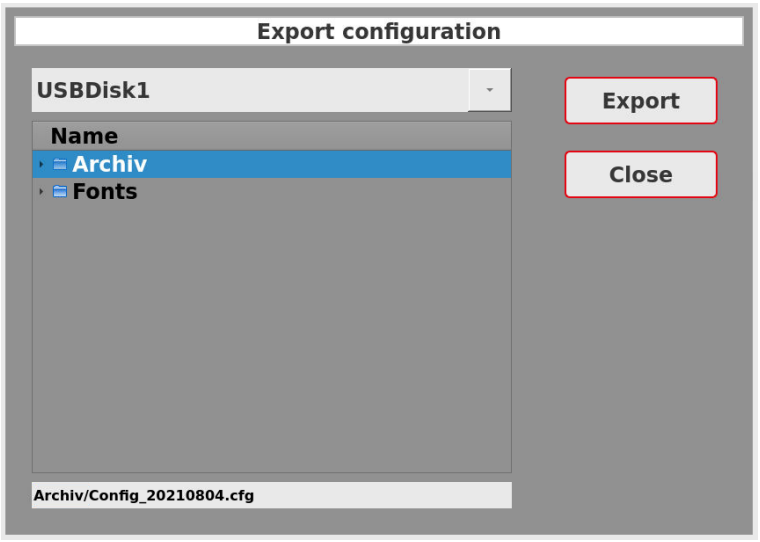
10. Parameterization view "Service“

This dialog offers the possibility to export or import the connection and network configuration. In addition, the log files can be exported. The import / export is done to USB sticks. In addition, the local update mode can be started.

Parameterization view "Service“

10.1. Export configuration data

When exporting the configuration data, it is possible to select which data is to be exported. The following configuration data are available for selection: Network configuration and Connection configuration. One or both of them can be selected. After pressing the "Export configuration" button, a file selection dialog appears.



Export configuration data

The desired USB stick can be selected in the upper selection box. The names "USBDisk1" to "USBDisk9" are assigned depending on the insertion sequence.

Below this, the desired file can be selected. Subdirectories are marked with a small arrow and can be expanded or collapsed. If no file is to be selected, the directory in which the exported configuration is to be stored can be selected here.

Again under it a selected file name can be edited or a new file name is indicated. The path that is displayed here is always relative to the root directory of the selected USB stick.

Buttons

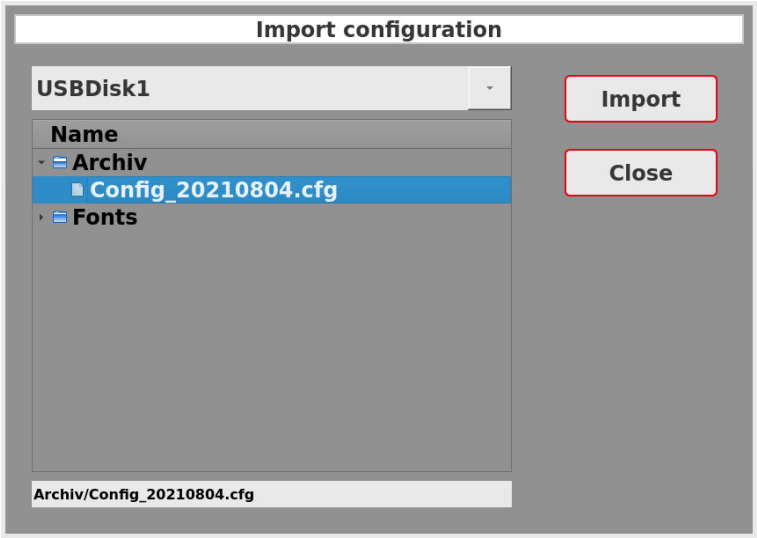
„Export“:

Export the configuration data (format: XML file) to the selected file and return to the previous view (see section 10 - Parameterization view "Service“).

„Close“:

Return to the previous view (see section 10 - Parameterization view "Service“).

10.2. Import configuration data



Import configuration data

The desired USB stick can be selected in the upper selection box. The names "USBDisk1" to "USBDisk9" are assigned depending on the insertion sequence.

Below this, the desired file can be selected. Subdirectories are marked with a small arrow and can be expanded or collapsed.

Buttons

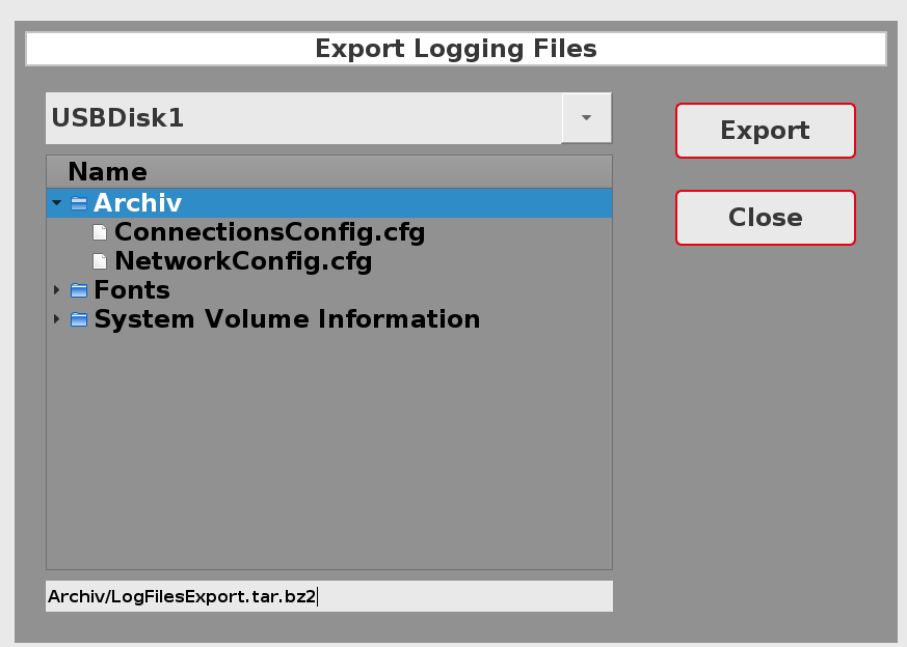
„Import“:

Import the configuration data from the selected file (format: XML file) and return to the previous view (see section 10 - Parameterization view "Service“).

„Close“:

Return to the previous view (see section 10 - Parameterization view "Service“).

10.3. Export log files



Export log files

The desired USB stick can be selected in the upper selection box. The names "USBDisk1" to "USBDisk9" are assigned depending on the insertion sequence.

Below this, the desired file can be selected. Subdirectories are marked with a small arrow and can be expanded or collapsed. If no file is to be selected, the directory in which the exported configuration is to be stored can be selected here.

Again under it a selected file name can be edited or a new file name is indicated. The path that is displayed here is always relative to the root directory of the selected USB stick.

Buttons

„Export":

Export the log files to the selected file (format: bzip2 compressed tar archive) and return to the previous view (see section 10 - Parameterization view "Service").

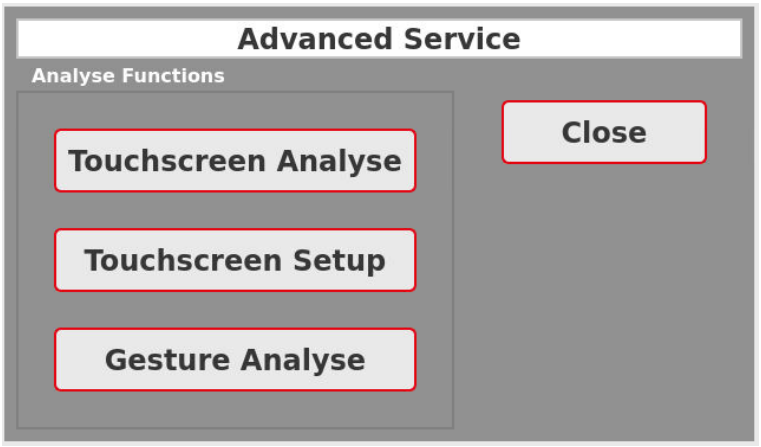
„Close":

Return to the previous view (see section 10 - Parameterization view "Service").

10.4. Start local update

Clicking this button switches to local update mode (see Section 13 -Local system update).

10.5. Advanced



Touchscreen – Setup and Analyse

The extended service area contains tools for analyzing the touchscreen function, fine-tuning the touchscreen and analyzing gesture recognition.

Buttons

„Close“:

Return to the previous view (see section 10 - Parameterization view "Service“).

10.5.1 Touchscreen Analyse

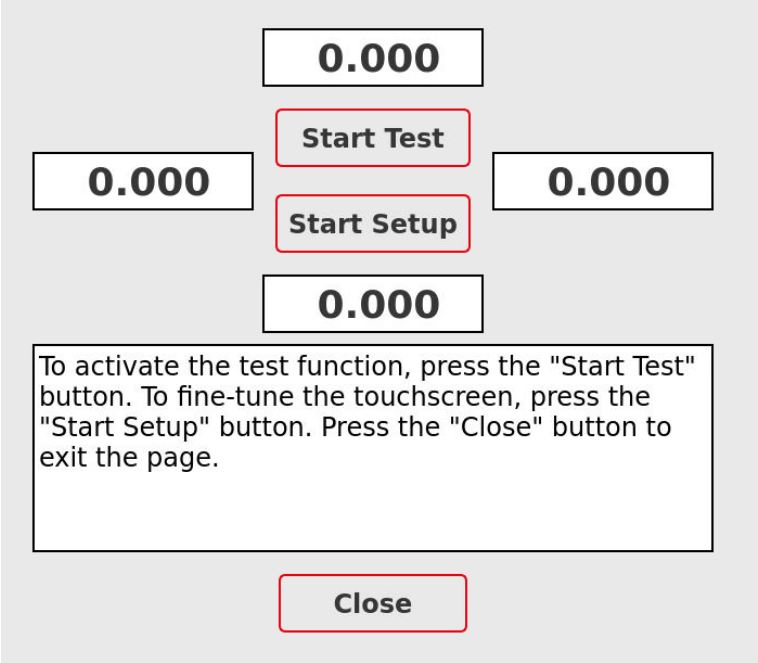
The touchscreen analysis can be used to test which touch and mouse events are received. They are displayed on this page.

Touch events are displayed as follows: Touch start is a green triangle, blue dots represent the position data received and a red cross signals touch end.

Mouse events are displayed as follows: Mouse-Down is a green square, black dots represent the received position data and a red square signals Mouse-Up.

You can leave the page by clicking the "Close" button.

10.5.2 Touchscreen Setup



Fine adjustment of the touchscreen

On this page, the fine adjustment of the touchscreen can be tested ("Start test" button) or set ("Start setup" button). The four number fields show the difference between the actual value and the target value during the test or fine adjustment. In addition, the fields are colored green if the value is within the tolerance and red if the value is outside the tolerance. The text field displays information on performing the test and fine adjustment. The page can be exited using the "Close" button.

Performing the test
The test is started by pressing the "Start Test" button. The text then changes to "Next" and the other buttons are disabled. An arrow is also displayed to indicate the swipe direction. Swipe from outside the display towards the center of the screen with a slow, even movement.

After the swipe movement, the corresponding number field is updated and colored red or green. Press "Next" to move to the next position and another arrow is displayed.

Once all four positions have been processed, the test is complete and the text "Start Test" is displayed again and all buttons are active again. If all number fields are green, the touchscreen is set correctly. If at least one number field is red, the touchscreen should be fine-tuned.

Performing the fine adjustment
The fine adjustment is started by pressing the "Start Setup" button. First, the fine adjustment of the touchscreen is reset to the default values. The procedure is then similar to the test. In contrast to the test, the fine adjustment of the touchscreen is adjusted after each wipe if the corresponding numerical value is outside the tolerance (red coloring). A new wipe is then

required to check the corrected fine adjustment. This process is repeated until the number field is colored green. You can then move to the next position by pressing "Next".

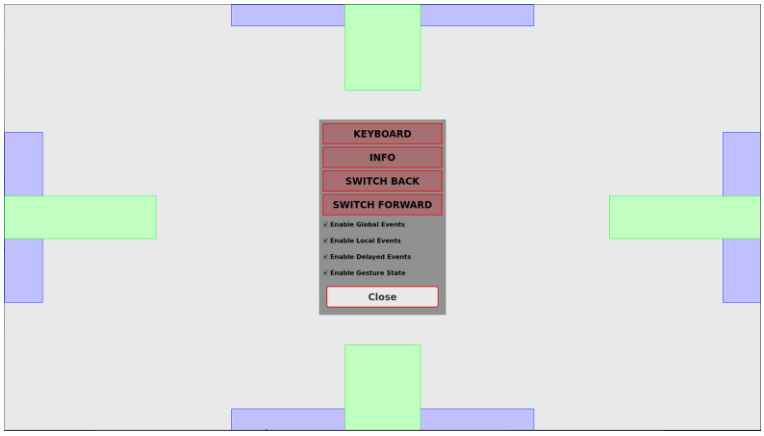
Once all four positions have been edited, the button text changes to "Save". This allows the fine adjustment of the touch to be saved permanently and will be applied automatically the next time the system is started.

If the values are not to be saved, e.g. due to an error during setup, the "Close" button can also be pressed. The default values are then restored and the fine adjustment can be restarted.

If the incorrect fine adjustment makes it impossible to operate the computer, the last saved fine adjustments can be restored by restarting the computer.

10.5.3 Gesture Analyse

With the gesture analysis, a possibility was created to check the gesture parameterization (see 8.1 - Configure notion#client).



View of the gesture analysis

The gesture analysis view is structured as follows: the four gesture areas are located at the edge - the info gesture at the top, the keyboard gesture at the bottom, and the connection switching gestures on the right and left. The blue areas represent the start area and the green areas outline the gesture area. However, the exact position of the gesture area results from the recognized start position of the gesture and is not dynamically displayed here. They are only used here for orientation.

The four buttons "KEYBOARD", "INFO", "SWITCH BACK" and "SWITCH FORWARD" can be used to activate (green) or deactivate (red) the respective gesture recognition. The display can be limited to the activated elements using the four checkboxes.

Global events:
Global events are events that are received and evaluated by the gesture recognition:

- Touch Start: blue triangle
- Touch Move: small blue dot

- Touch End: blue cross

Local events:
Local events are events that have not been filtered out by gesture recognition and are processed by the window or viewer.

- Touch Start: green square
- Touch Move: small green dot
- Touch End: green square with red filling

Delayed events:
Delayed events are events that were initially filtered out by gesture recognition and are forwarded to the window or viewer for processing after gesture recognition has been canceled. They are then also visible there as local events.

- Touch Start: red square
- Touch Move: small red dot
- Touch End: red square

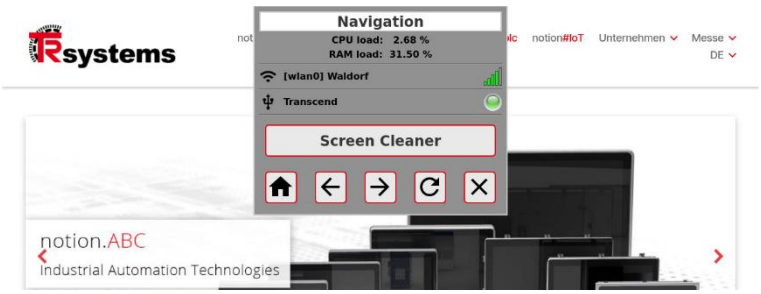
Gesture status:
The gesture status provides an insight into gesture recognition and its status with the associated positions.

- Gesture Start: magenta-colored square with green filling
- Gesture Begin: magenta-colored square
- Gesture Trigger: small magenta-colored circle
- Gesture Finished: magenta cross
- Gesture Canceled: magenta-colored square with red filling
- Gesture Timeout: magenta-colored square with yellow filling

11. Viewer

Depending on the set connection configuration, different viewers are used. Viewers for Web, VNC, RDP, RDPApp and Stream connections are available. A special feature is the viewer for multiple connections, which can display multiple connections (Web, VNC, RDP, RDPApp or Stream connections).

11.1. Web-Viewer

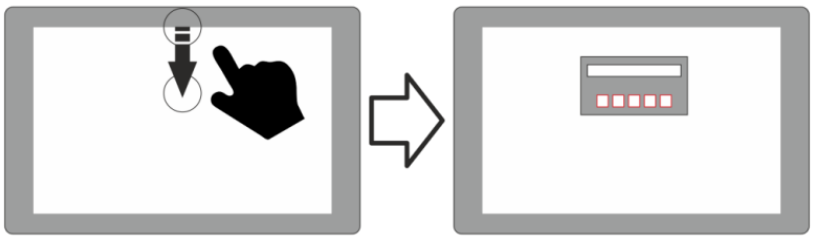


View with the web page loaded and the navigation bar displayed.

The web viewer supports the following operating gestures:

- Scrolling via swipe gestures
- Zoom In/Out via zoom gesture

The navigation bar is displayed by a swipe gesture from the center of the area above the screen downwards into the screen. The distance covered during the swipe should be at least 20% (parametrizable setting) of the screen height. The navigation bar appears after the gesture has been executed successfully.

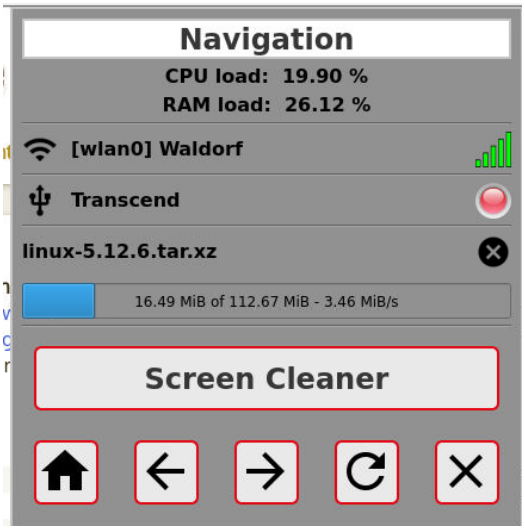


Show navigation bar

The navigation bar is displayed by a swipe gesture from the center of the area above the screen downwards into the screen. The distance covered during the swipe should be at least 20% of the screen height. The navigation bar appears after the gesture has been executed successfully.

The connection status of the WLAN connection (if activated) and the connection quality are displayed in the navigation bar.
The inserted USB memory sticks are also displayed. A red LED indicates active write access to the storage medium. The USB memory stick should not be removed in this state. A green LED signals that there is no active access to the USB memory stick - the USB memory stick will be removed.

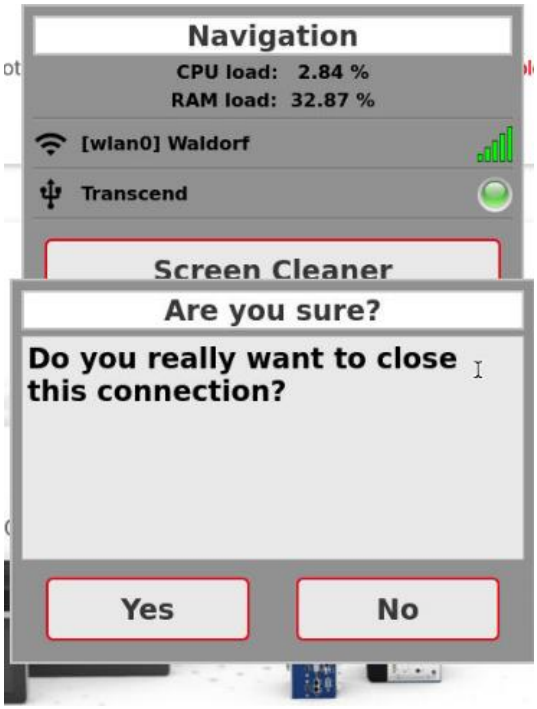
The progress of the download is displayed during active downloads. The download can also be canceled here.



Navigation bar with active download

Besides displaying the current memory and CPU usage, the following actions are possible (from left to right):

- Button to activate the screen cleaning mode
- Loading the start web page
- Go back one page (if possible)
- Go one side ahead (if possible)
- Reload the current page
- Closing the web viewer



Security prompt before closing the web viewer if no "Disconnect password" has been defined.

Alternatively: Enter the "Disconnect password".

11.1.1 Context Menu

The context menu can be displayed by right-clicking or Tap'n'Hold (press and hold the touch until the menu is displayed). However, this requires activation in the connection configuration. It can be hidden by clicking the "Close" entry.

Active context menu

11.1.2 Certificate Exclusions

If a website (only for https connections) uses a certificate that was signed by an unrecognized certificate authority (e.g. self-signed certificates), a message is displayed. There is a certificate error that prevents the website from loading.

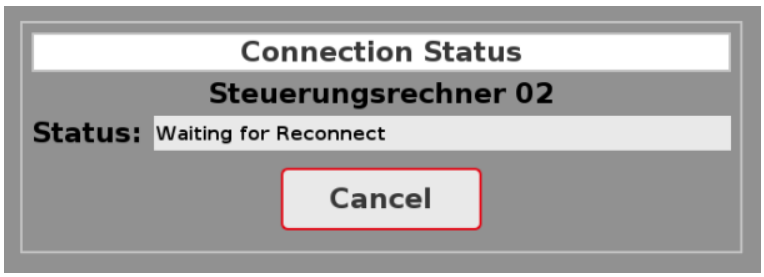
Certificate error message

In the certificate error dialog there is now an option to view the details of the certificate to decide whether to add the certificate to the certificate exclusion list or to terminate the connection.

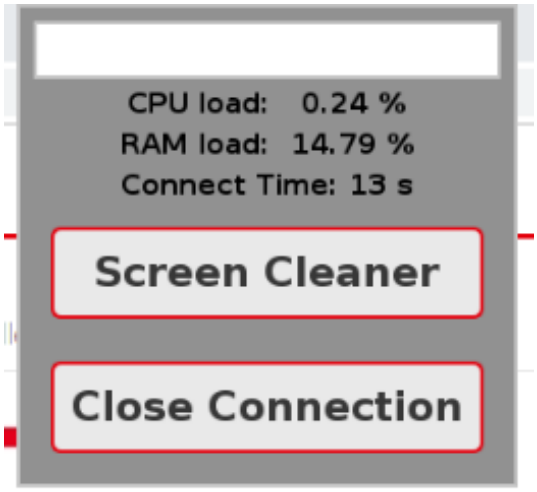
The certificate exclusion list belongs to the active connection and adding a new exclusion does not affect other connections. Any number of exclusions can be added to a connection. Resetting the certificate exclusion list is done on the connection configuration page.

Detail view of the untrusted certificate

11.2. VNC-Viewer



Establishing the connection (status display with connection name)

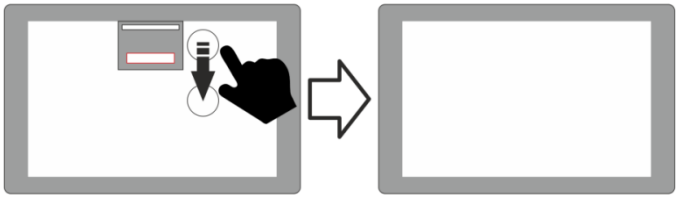


View with established connection and displayed dialog.

Besides displaying the current memory and CPU usage and the connection duration, the following actions are possible:

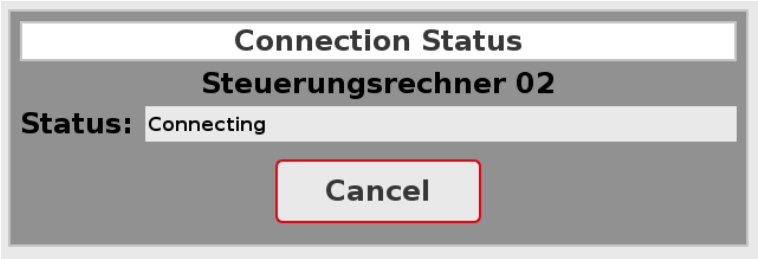
- Button to activate the screen cleaning mode
- Button to disconnect the connection

The dialog is displayed by a swipe gesture from the center of the area above the screen down into the screen. The distance covered when dragging should be at least 20% of the screen height. The dialog appears after the gesture has been successfully executed.

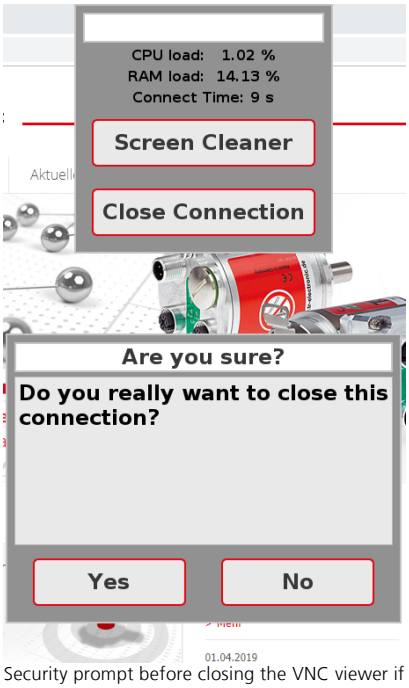


Dialog box

The dialog can be placed anywhere on the screen, just like the keyboard. To do this, touch the drag bar (the white field) with your finger and you can move the dialog as you wish. If you move the dialog out of the screen, it will be hidden.



Status display when disconnected

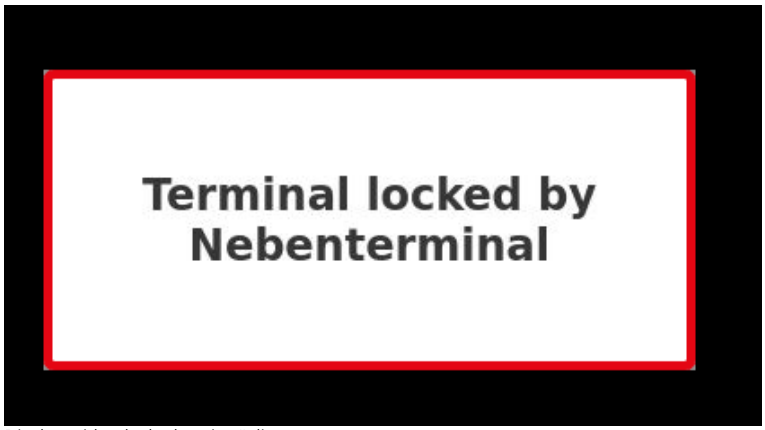


Security prompt before closing the VNC viewer if no "Disconnect password" has been defined.

Alternatively: Enter the "Disconnect password".

11.2.1 Daisy chain function

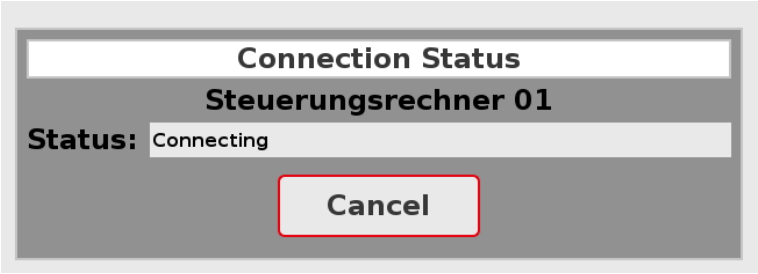
The daisy chain feature, as we provide it for the VNC viewer, is intended to prevent shared operation of the host system by locking all notion#clients that have the daisy chain feature enabled, use the same group name, and are on the same network segment from user input once the first operator starts typing.



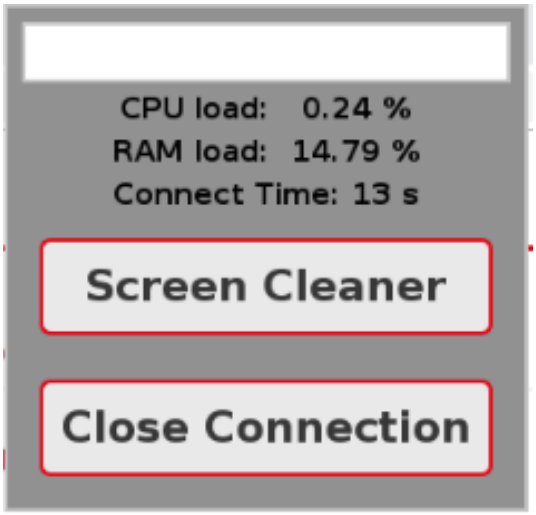
Display with a locked notion#client

The input from the blocked notion#client is blocked according to the set blocking time beyond the input duration. Only after this time period, another operator can start with the inputs. The display also shows the host name of the notion#client that triggered the blocking of the other notion#client.

11.3. RDP-Viewer



Establishing the connection (status display with connection name)

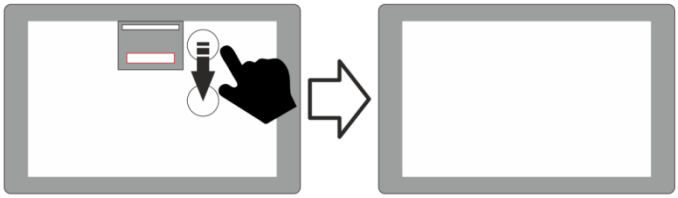


View with established connection and dialog displayed

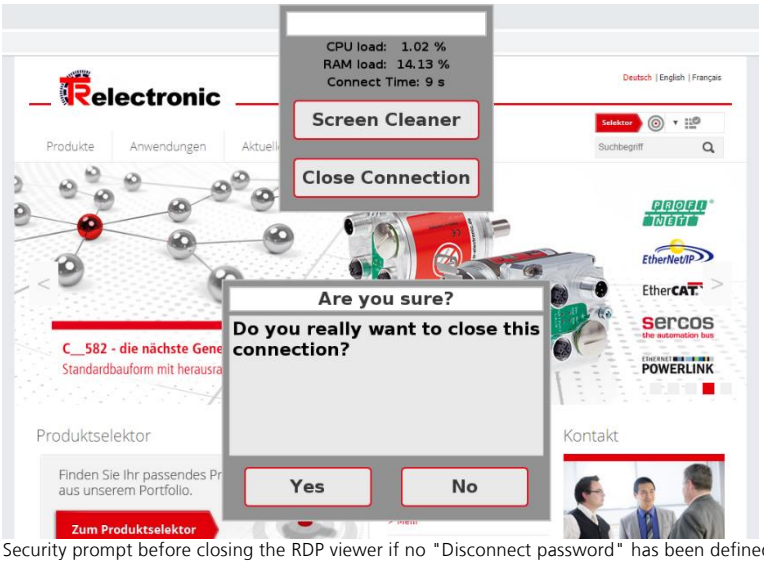
Besides displaying the current memory and CPU usage and the connection duration, the following actions are possible:

- Button to activate the screen cleaning mode
- Button to disconnect the connection

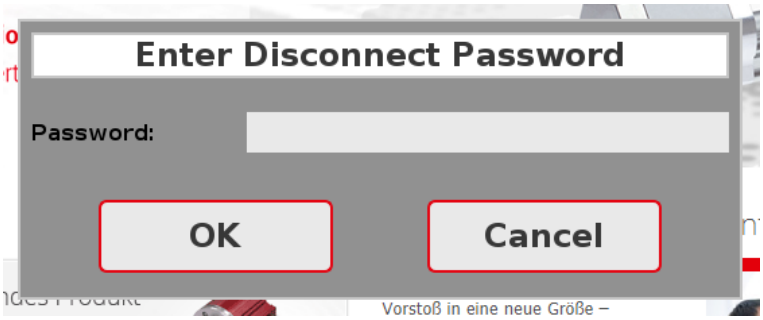
The dialog is displayed by a swipe gesture from the center of the area above the screen down into the screen. The distance covered when dragging should be at least 20% of the screen height. The dialog appears after the gesture has been successfully executed.



The dialog can be placed anywhere on the screen, just like the keyboard. To do this, touch the drag bar (white field) with your finger and you can move the dialog as you wish. If you move the dialog out of the screen, it will be hidden.



Security prompt before closing the RDP viewer if no "Disconnect password" has been defined.



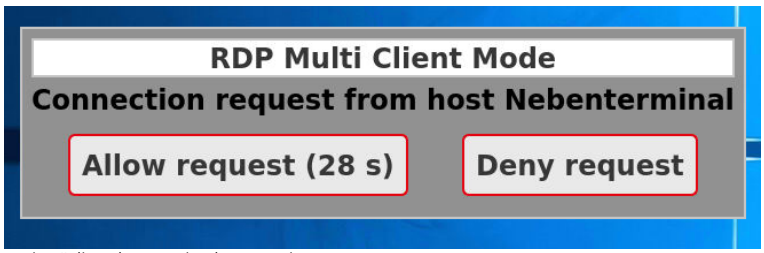
Alternatively: Enter the „Disconnect Password“

11.3.1 Multi-client function

The notion#client provides a function that can be used to access an RDP host computer from multiple notion#clients. Since only direct 1-to-1 connections are possible, a locking mechanism has been implemented so that only one notion#client can actively access the RDP host computer at a time. However, access can be redirected to another notion#client at any time.

notion#client in inactive state

A click on the "Send request" button leads to a check whether another notion#client already has access to the configured RDP host. If this is the case, a dialog is displayed on the other notion#client where the operator has the option to hand over the connection to the requesting notion#client or to reject the request. If there are no operators on the device at the time, the operation is transferred to the requesting notion#client after a configurable period of time (timeout) and the connection is terminated.

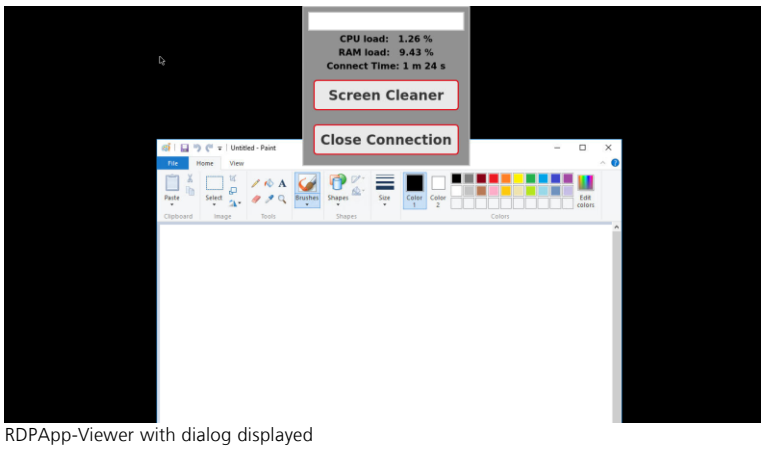


notion#client has received connection request

If the request was rejected, the requestor is informed about it and can start a request again after confirming this message.

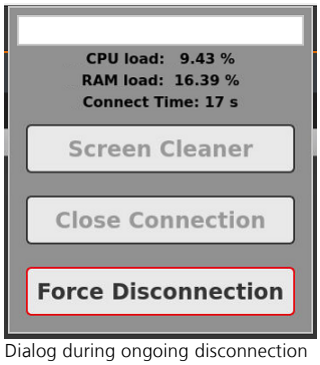
If no other notion#client has access to the RDP host computer, a connection is established immediately. The "Cancel" button takes you back to the connection view.

11.4. RDPApp-Viewer



RDPApp-Viewer with dialog displayed

The RDPApp viewer is based on the RDP-Viewer with the exception of the multi-client function. For a description of the functions, see there (section 11.3 -RDP-Viewer).



Dialog during ongoing disconnection

If an RDP app connection cannot be disconnected even after a longer waiting time (>30s) (black screen background), it is possible to force the disconnection. As this is a disorderly disconnection, it can lead to undesirable behavior the next time a connection is established. In this case, it may be necessary to restart the host system.

11.5. Stream-Viewer

Stream-Viewer with dialog displayed

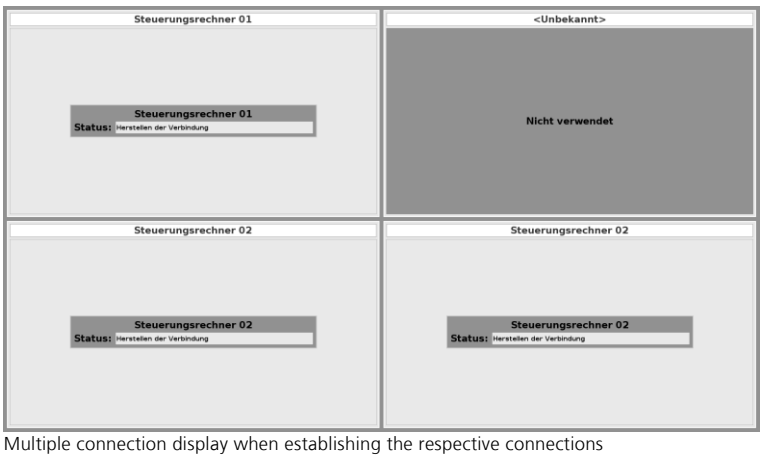
The dialog offers the following functions in addition to displaying the current memory and CPU usage:

- _ button to activate the screen cleaning mode
- _ Button to disconnect

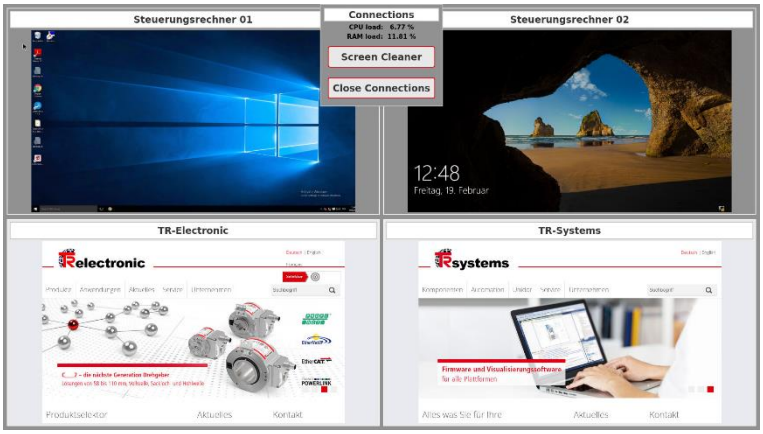
The dialog is displayed by a swipe gesture from the center of the area above the screen downwards into the screen, as described before.

Like the keyboard, it can be placed anywhere on the screen. To do this, you touch the drag bar (white box) with your finger and can use it to move the dialog as desired. If you move the dialog out of the screen, it will be hidden.

11.6. Multiple connections



Multiple connection display when establishing the respective connections

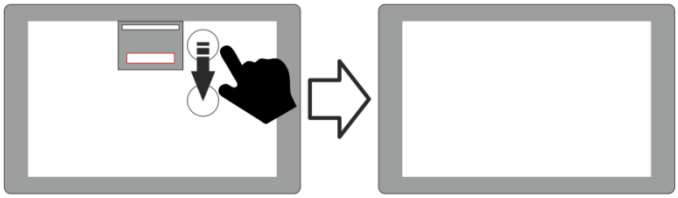


Multiple connection display with established connections and displayed "Connections" dialog.

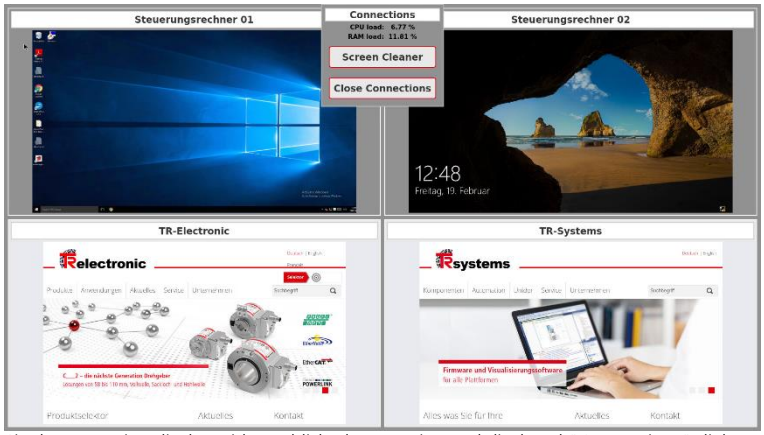
Besides displaying the current memory and CPU usage, the following actions are possible:

- Button to activate the screen cleaning mode
- Button to disconnect the connections

The "Connections" dialog is displayed by a swipe gesture from the center of the area above the screen down into the screen. The distance covered when dragging should be min. 20% of the screen height. The dialog appears after the gesture has been executed successfully.



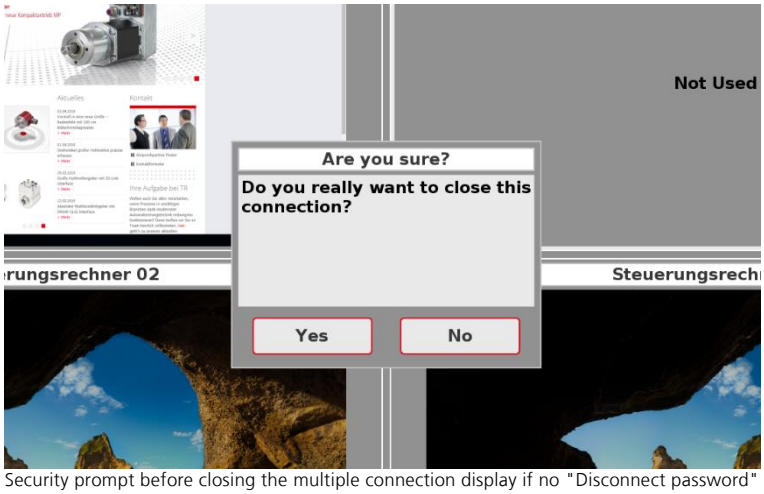
The "Connections" dialog can be placed anywhere on the screen, just like the keyboard. To do this, touch the drag bar (the white field) with your finger and you can move the "Connections" dialog as you wish. If you move the "Connections" dialog out of the screen, it will be hidden.



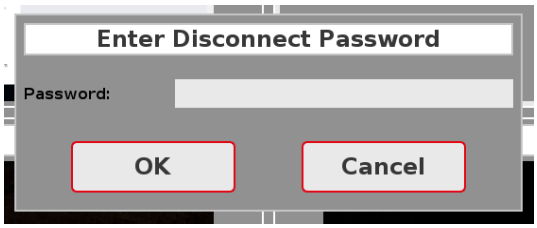
Single connection display with established connection and displayed "Connections" dialog.

Besides displaying the current memory and CPU usage, the following actions are possible:

- Button to activate the screen cleaning mode
- Button to disconnect the connections
- Button to switch to the multiple connection view
- Buttons for web page navigation (only in web viewer mode)



Security prompt before closing the multiple connection display if no "Disconnect password" has been defined.



Alternatively: Enter the "Disconnect password".

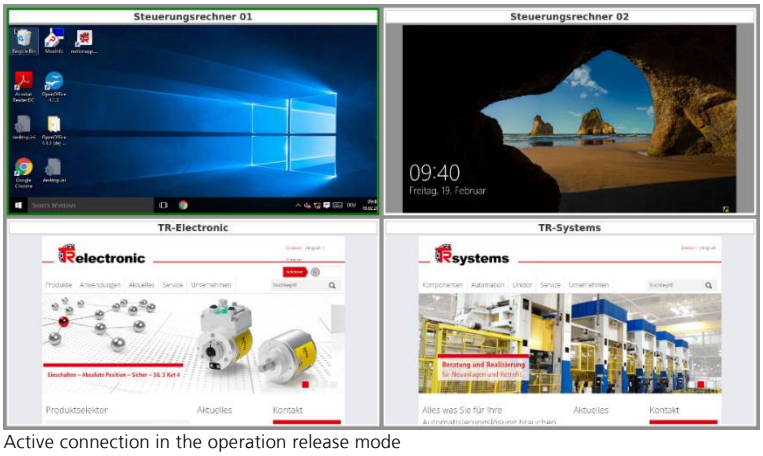
11.6.1 Connection switching

In the multiple connection display, no touch or keyboard inputs are forwarded to the remote terminal by default. This is only possible if the respective connection has been activated. Several variants are available for activation or connection switching

"Switch to single view"
This is the default behavior. To do this, the respective viewer must be pressed with the finger for a few seconds in the split view (tap'n'hold). Afterwards, the viewer switches to the single view.

„Enable view (Tap'n'Hold)“
In this mode, the viewer is activated by pressing it for several seconds (tap'n'hold). There is no switching to the single view. The operation can be done in the split view. The active viewer is displayed with a green frame, the inactive viewers have a white frame.

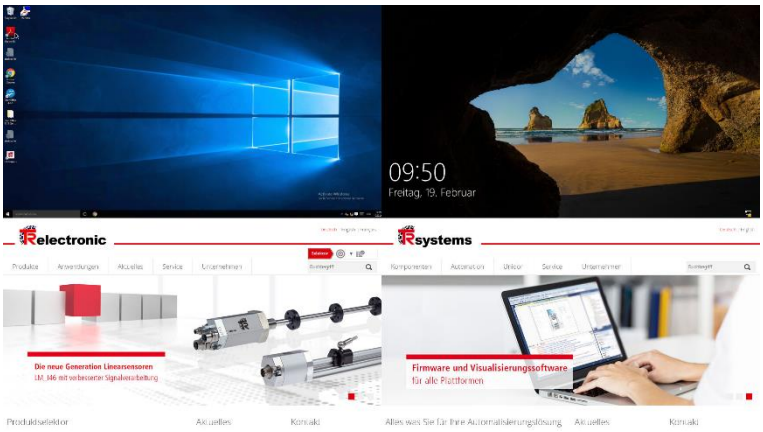
„Enable view (Simple Touch)“
In this mode, the viewer is activated by a simple tap (click). As before, there is no switching to the single view. The display is as described before.



Active connection in the operation release mode

11.6.2 Display options

As already mentioned in section 7.6.1 described, the display of the multiple connection display can be customized.



Modified multiple connection display

In the above example, connection names and frames have been removed and layout spacing has been set to 0.

12. Web-Interface

The web interface offers several configuration options and allows to perform a system update. It is accessible via the first Ethernet interface (eth0) under the URL „http://<IP-Adresse>:8081/config/" accessible.

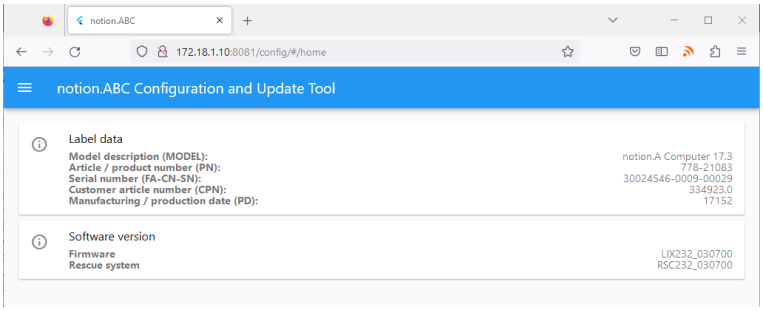
The web interface has beed tested with the following web browsers:

Linux (Debian, 64-Bit):

- Chromium Version 114.0.5735.198 (Official Build) (64-bit)

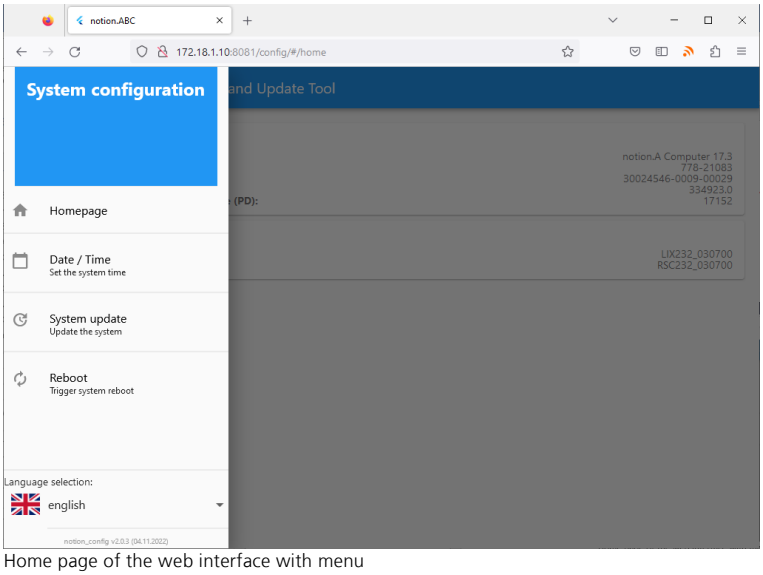
Windows 10 (64-Bit):

- Mozilla Firefox 115.0 (64-Bit)
- Google Chrome Version 114.0.5735.199 (Offizieller Build) (64-Bit)
- Microsoft Edge Version 114.0.1823.67 (Offizielles Build) (64-Bit)



Home page of the web interface

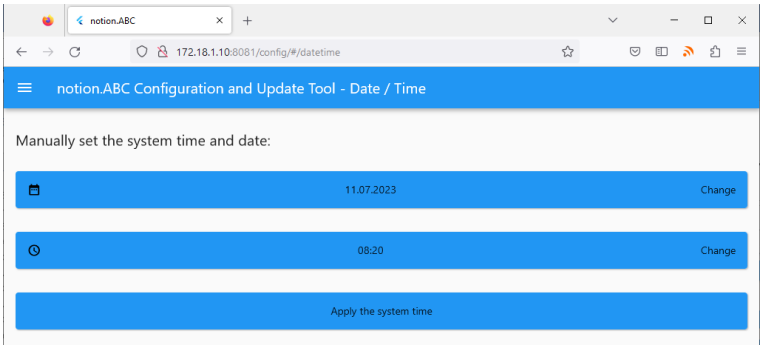
Device information (label data/serial number and the version of the installed software) is displayed on the start page.



Home page of the web interface with menu

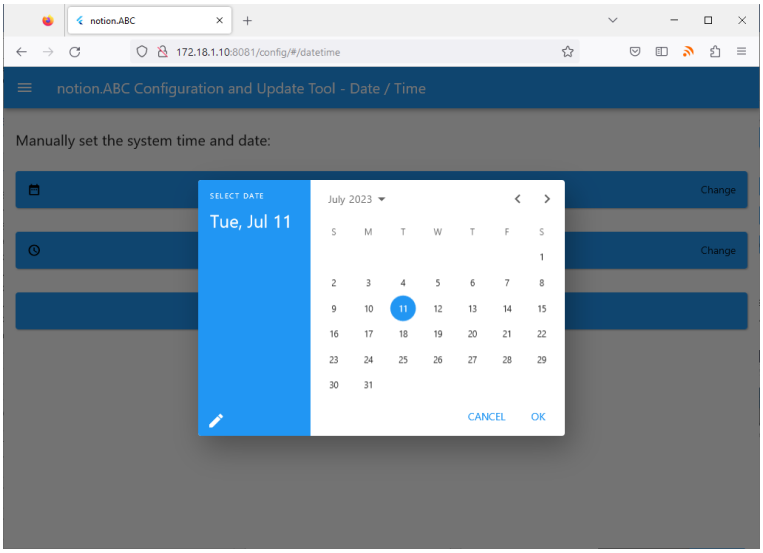
12.1. Setting the system time and date

The menu takes you to the other pages of the web interface.

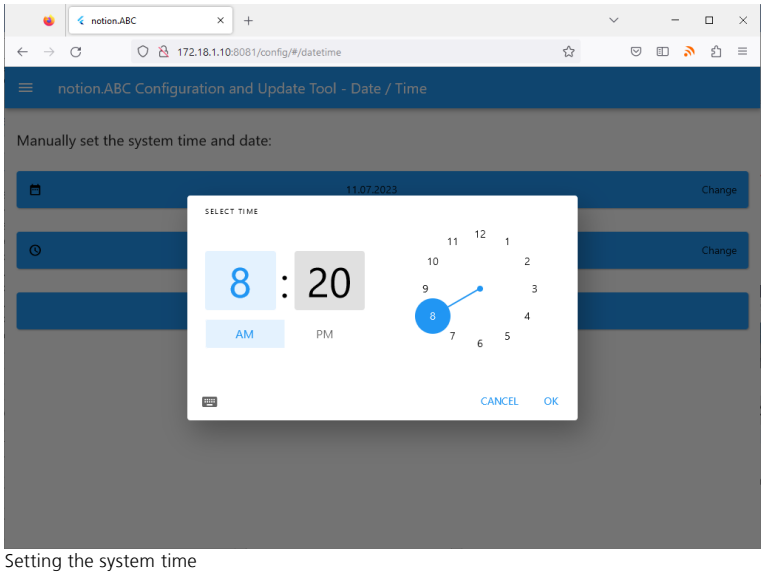


Setting the system time and date

Setting the system time or system date can be done manually or from the system time of the configuration computer.

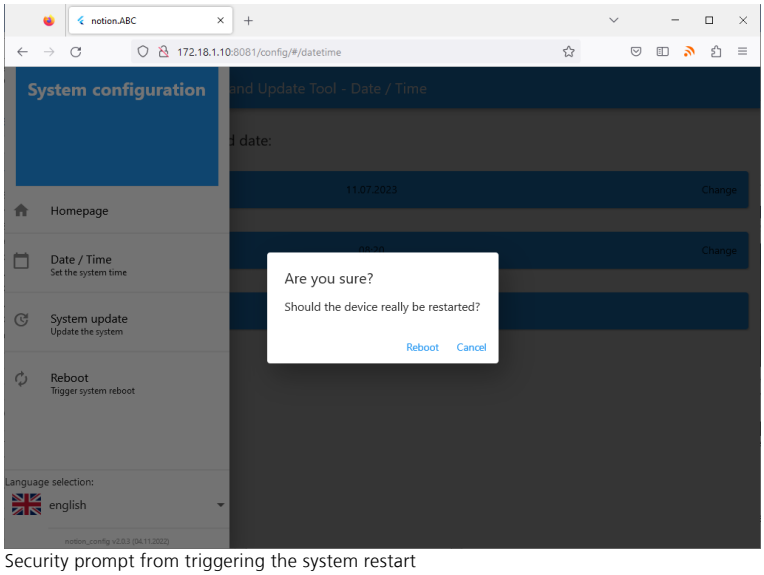


Setting the system date



Setting the system time

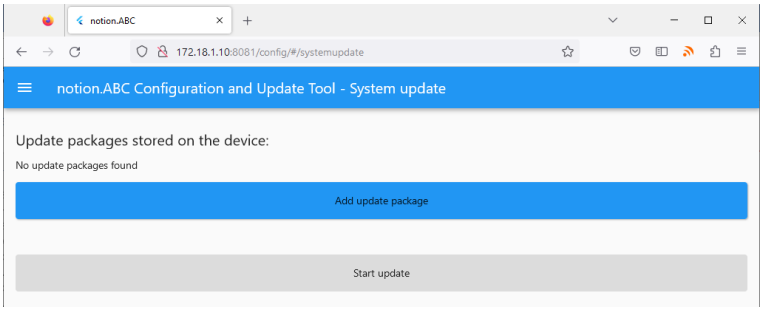
12.2. Trigger system restart



Security prompt from triggering the system restart

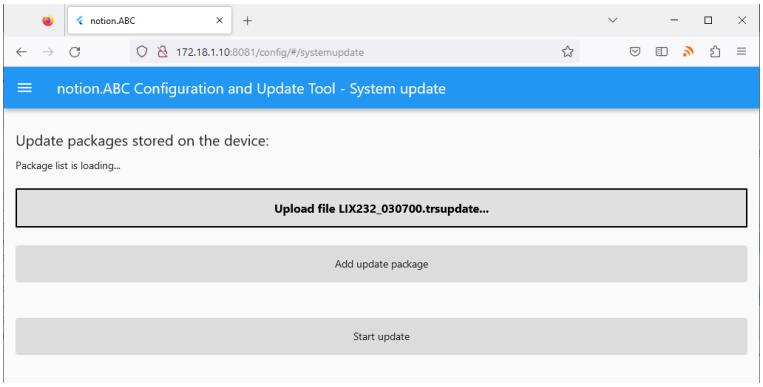
12.3. Performing a system update

To perform the system update, you need the new software as an update package. These have the file extension "trsupdate".



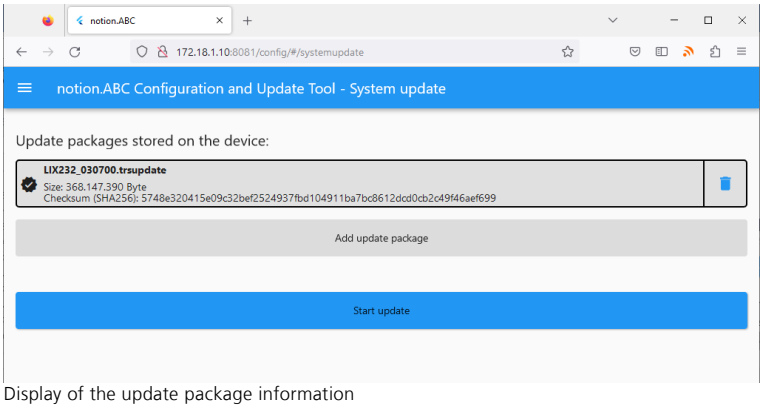
Home page for performing a system update

To load the update package, press the "Add update package" button. A file selection dialog appears, with which the update package can be selected. Afterwards the upload of the package starts.



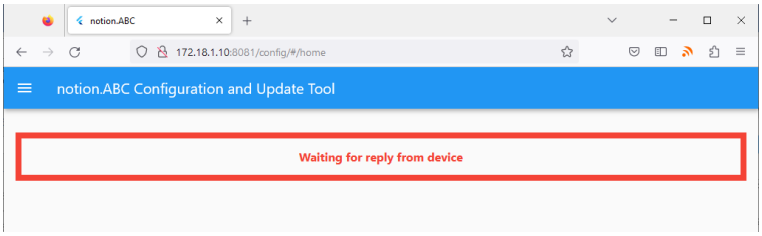
Upload the update package

When the upload is complete, the update package is displayed together with size information and checksum. With "Start Update" the actual update process can be started.



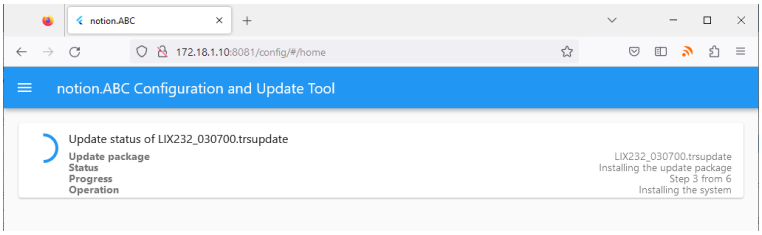
Display of the update package information

For this purpose, the update system is started first. During this, the following display appears:



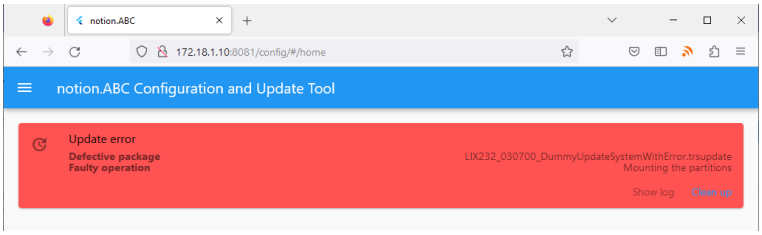
Start of the update system

During the system update, the progress of the update is displayed. You can also follow the update progress on the device's screen. However, you have no possibility to intervene in the update process here.



Display of the update progress

After a successful update - if the web interface is activated - the start page is displayed again. If the update fails, the following display appears.



Error during update

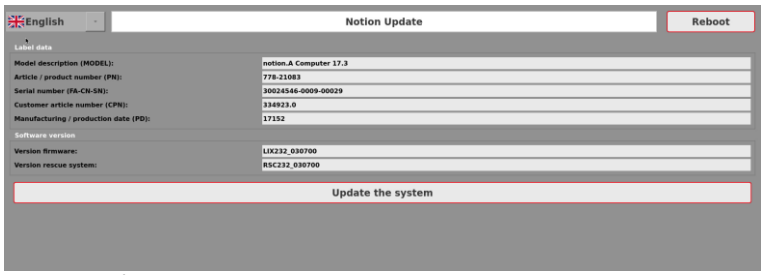
To restart the system update, the "Clean up" button must first be clicked. The start page then appears again. The option "Exit update system" is deactivated in this case and is only available again after a successful update.

If the notion#client is restarted in this state, the system is started in update mode and can only be returned to normal operation after a successful update.

13. Local system update

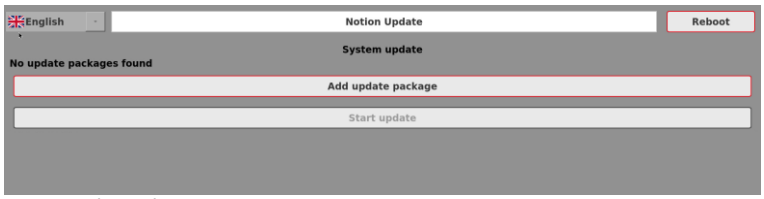
To perform the system update, you need the new software as an update package. These have the file extension "trsupdate". Copy this file on a USB stick.

If the web interface is active, you can follow the update process there. However, you have no possibility to intervene in the update process here.



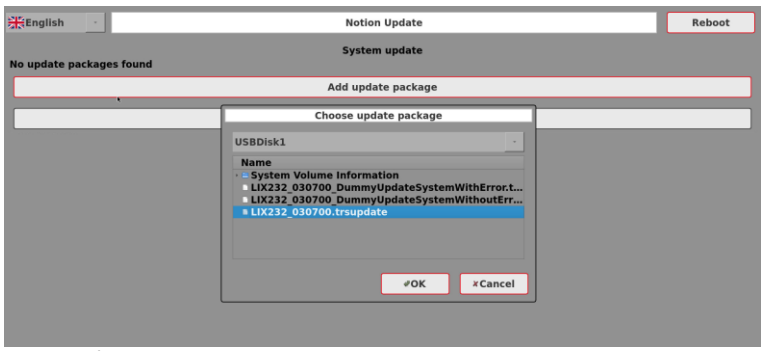
Start display after establishing a connection with the update service.

To start the update process, the "Perform system update" button must be clicked first.



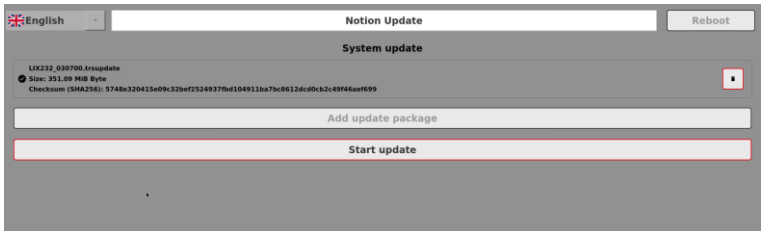
Start page for performing a system update

To load the update package, press the "Add update package" button. A file selection dialog appears, with which the update package can be selected. Afterwards the upload of the package starts.



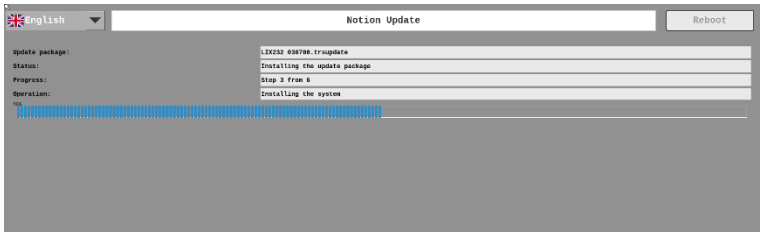
Selection of the update package

When the upload is completed, the update package is displayed together with size information and checksum. With "Start Update" the actual update process can be started.



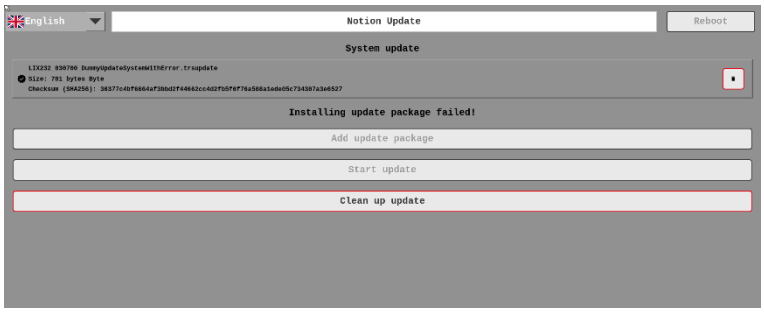
Display of the update package information

During the system update, the progress of the update is displayed.



Display of the update progress

After successful update, the updated system is started. If the update fails, the following display appears.



Error during update

To restart the system update, the "Clean up update" button must first be clicked. The start page then appears again. The "Restart" button is disabled in this case and is only available again after a successful update.

If the notion#client is restarted in this state, the system is started in update mode and can only be returned to normal operation after a successful update.

14. Important information about the update

Starting from the initial version, the following points must be observed when updating to version v3.8.1 (LIX232_031000 or LIX251_031000).

14.1.1 LIX251_030100, LIX251_030101, LIX251_030102, LIX232_030100, LIX232_030102

First an update to the version LIX251_030305 or LIX232_030304 is necessary. For the update you need a Firefox browser and the unsigned version of the update package.

Afterwards the update to version LIX251_031000 or LIX232_031000 can be performed. To do this, the web interface must first be activated. The update can be performed with any browser. The signed update package is required.

14.1.2 LIX251_030103

First an update to the version LIX251_030305 is necessary. The update can be performed with any browser. The unsigned update package is required.

Then the update to version LIX251_031000 can be performed. To do this, the web interface must first be activated. The update can be performed with any browser. The signed update package is required.

14.1.3 LIX251_030200, LIX251_030300, LIX251_030301, LIX251_030302, LIX251_030303, LIX251_030304, LIX232_030200, LIX232_030301, LIX232_030302, LIX232_030303

First an update to the version LIX251_030305 or LIX232_030304 is necessary. The update can be performed with any browser. The signed update package is required.

Afterwards the update to version LIX251_031000 or LIX232_031000 can be performed. To do this, the web interface must first be activated. The update can be performed with any browser. The signed update package is required.

14.1.4 LIX232_030304, LIX251_030305, LIX251_0304xx, LIX232_0304xx and the following versions

Here, the update to version LIX251_031000 or LIX232_031000 can be performed directly without an intermediate update. To do this, the web interface must first be activated. The update can be performed with any browser. The signed update package is required.

14.1.5 Table Overview Update

Version installed	Target Version	1. Update	2. Update
LIX251_030100 LIX251_030101 LIX251_030102	LIX251_031000	LIX251_030305 **unsigned, firefox**	LIX251_031000 **signed, beliebiger browser**
LIX232_030100 LIX232_030102	LIX232_031000	LIX232_030304 **unsigned, firefox**	LIX232_031000 **signed, beliebiger browser**
LIX251_030103	LIX251_031000	LIX251_030305 **unsigned**	LIX251_031000 **signed**

Version installed	Target Version	1. Update	2. Update
LIX251_030200 LIX251_030300 LIX251_030301 LIX251_030302 LIX251_030303 LIX251_030304	LIX251_031000	LIX251_030305 signed	LIX251_031000 signed
LIX232_030200 LIX232_030301 LIX232_030302 LIX232_030303	LIX232_031000	LIX232_030304 signed	LIX232_031000 signed

Version installed	Target Version	1. Update	2. Update
LIX251_030305	LIX251_031000	LIX251_031000	
LIX251_0304xx		signed	
LIX251_0305xx			
LIX251_0306xx			
LIX251_0307xx			
LIX251_0308xx			
LIX251_0309xx			
LIX232_030304	LIX232_031000	LIX232_031000	
LIX232_0304xx		signed	
LIX232_0305xx			
LIX232_0306xx			
LIX232_0307xx			
LIX232_0308xx			
LIX232_0309xx			

TRsystems GmbH
Eglishalde 16
78647 Trossingen

Telefon: +49 (0) 7425 / 228 - 0
Telefax: +49 (0) 7425 / 228 – 34

E-Mail: info@trsystems.de
www.trsystems.de