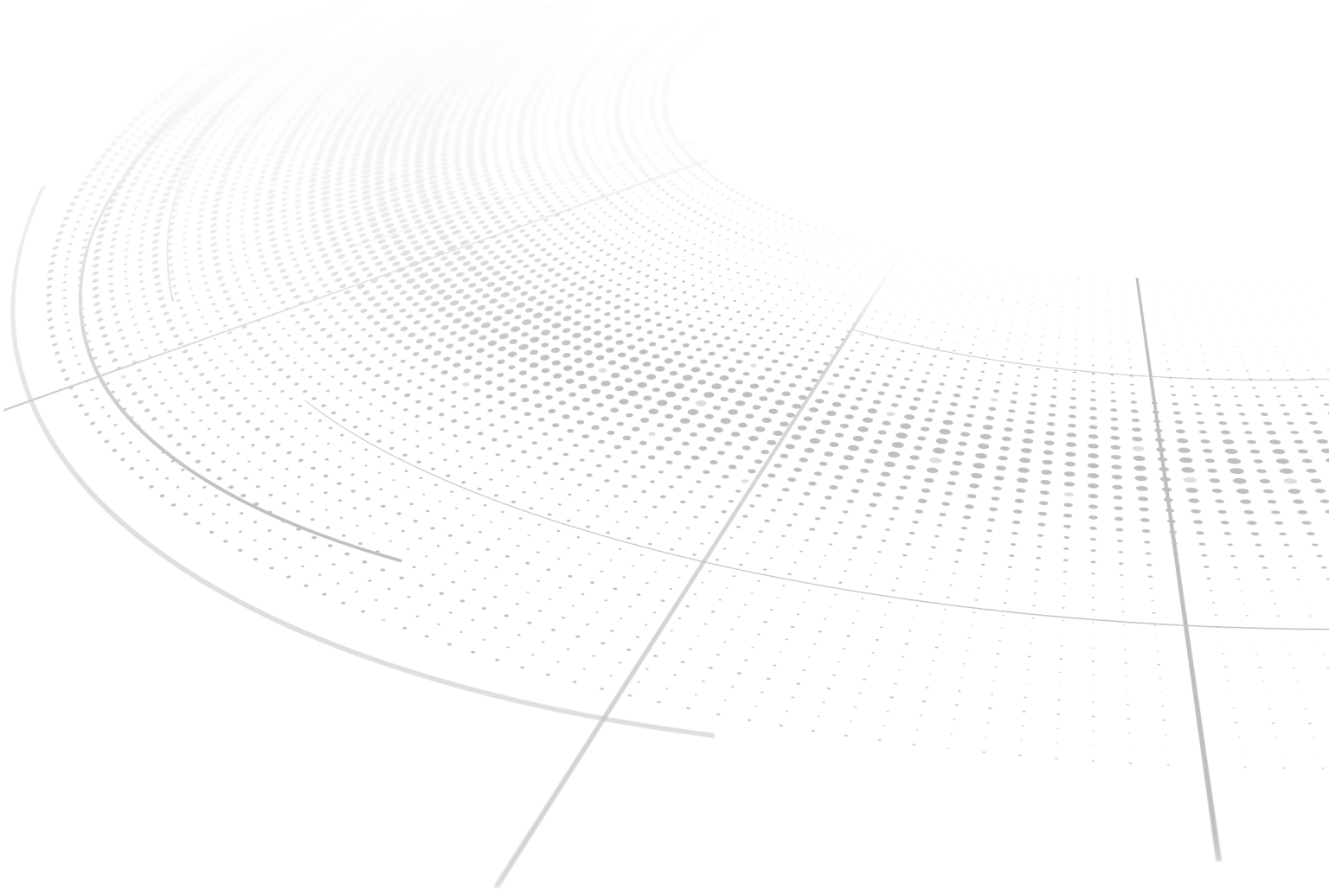
Instruction manual

notion#client



Original Manual | eng
Appliance Type:

Series:

TRsystems GmbH, Eglishalde 16, 78647 Trossingen, Telefon: +49 (0) 7425 / 228 - 0, Telefax: +49 (0) 7425 / 228 – 34, E-Mail: info(at)trsystems.de

Table of Contents

TRsystems GmbH, Eglishalde 16, 78647 Trossingen, Telefon: +49 (0) 7425 / 228 - 0, Telefax: +49 (0) 7425 / 228 – 34, E-Mail: info(at)trsystems.de

TRsystems GmbH, Eglishalde 16, 78647 Trossingen, Telefon: +49 (0) 7425 / 228 - 0, Telefax: +49 (0) 7425 / 228 – 34, E-Mail: info(at)trsystems.de

TRS-DOC_001829-00_20230430

1. About this guide

1.1. Copyright and disclaimer

This manual, including the illustrations contained therein, is protected by copyright. Thirdparty 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.

1.2. Release

Aim of the instruction		Quality improvement, in line with the company's guiding principles	
Author	**Creation date**	KAO	08.07.2025
Document number		TRS-DOC-001440	

1.3. 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
11		Recreation	08.07.2025	KAO

1.4. 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.

1.4.1 Target group

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

1.4.2 Explanation of terms

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

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

Table 1 Definition of terms

2. 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.

2.1. 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.

2.2. 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:

Warnzeichen	Bedeutung
⚠ 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	WARNING indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury
NOTICE	CAUTION indicates a situation which, if not avoided, may result in property damage.
IMPORTANT	IMPORTANT indicates an essential or priority aspect or a course of action.
NOTE	NOTE refers to general information.

Table 2.1: Type of safety note

2.3. Warning structure

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

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

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

2.4. 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.

TRsystems GmbH, Eglishalde 16, 78647 Trossingen, Telefon: +49 (0) 7425 / 228 - 0, Telefax: +49 (0) 7425 / 228 – 34, E-Mail: info(at)trsystems.de

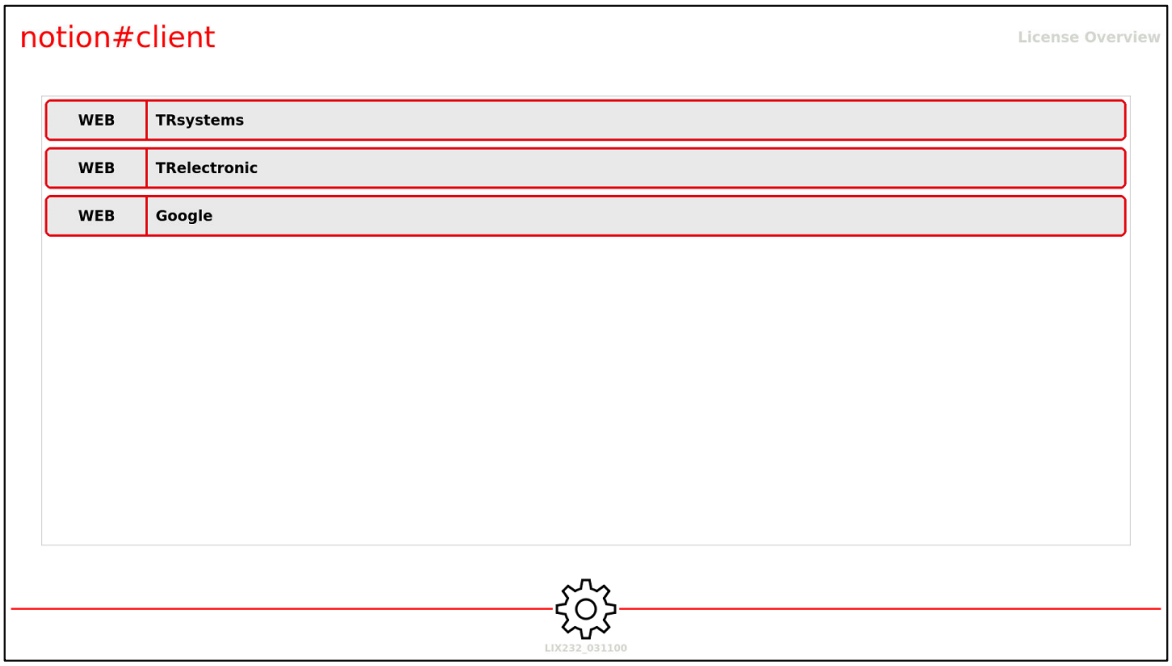
3. Description

The notion#client is a tool for displaying remote connections via VNC, RDP / RDPApp, web and as a video stream. The connections can be shown both individually and as MultiView, in which the screen for the individual connections is divided (variably)

Note: Depending on the screen size set in the system configuration and any rotated screen, the appearance of the screens shown below may vary. However, all the screen elements described are always present.

3.1. Start page

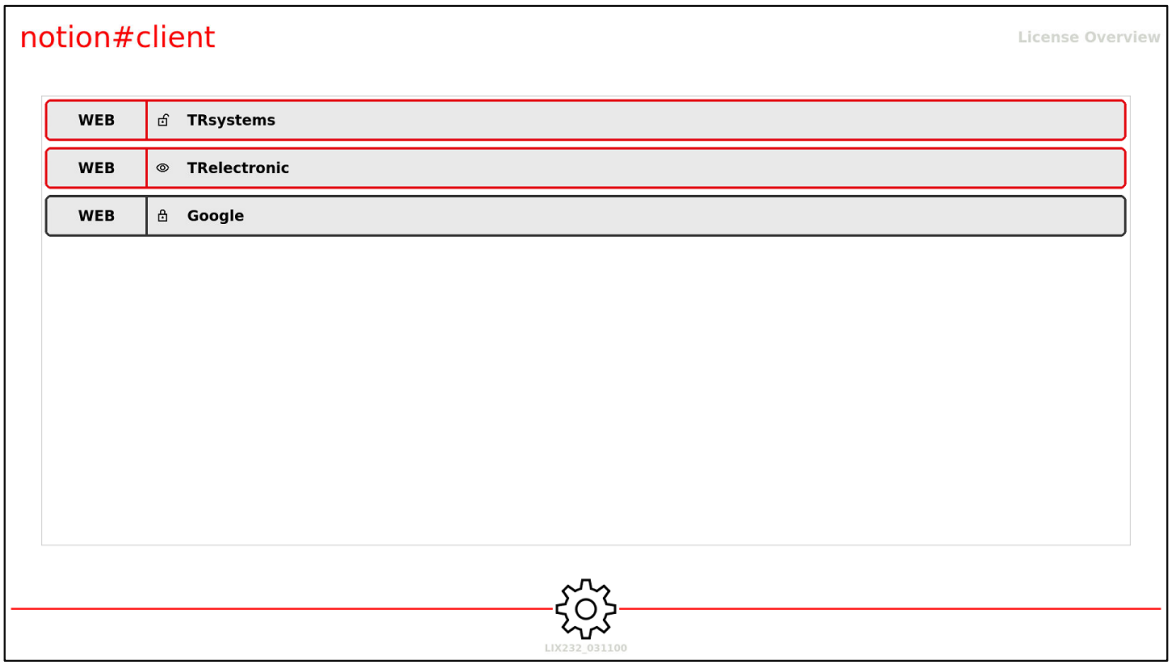
All connections that have been created by the user and released for display on the start page are shown on the start page. In combination with the optional Daisy-Chain-IO-Extension, the connections are shown depending on the logged-in user.



Start page without Daisy-Chain-IO-Extension

The available connections are located in the middle of the start page. Next to the name of the connection is an abbreviation that indicates the type of connection: “VNC” for VNC connections, “RDP” for RDP connections, “RDPApp” for RDPApp connections, “WEB” for web connections, ’Stream’ for video streams and “Multi” for MultiView views (multiple connection views). If one of these connections is clicked, the connection is established and shown in the corresponding viewer.

Note: RDPApp connections are a special subtype of the RDP connection, in which the entire desktop of the remote computer is not shown, but only a single application. This runs on the remote computer, while the display is taken over by the notion#client.



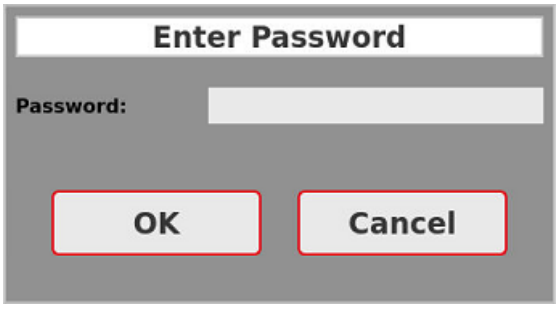
Start page with Daisy-Chain-IO-Extension and logged in user

If the device is equipped with a Daisy-Chain-IO-Extension, the start page looks slightly different. An icon for the access authorization for the user currently logged in is shown in front of the name of the connection. If the user does not have access authorization, the connection is shown as deactivated (darker instead of red frame). The connection cannot be selected

	The user has full access to this connection (view and operation).
	The connection is in view mode. The user cannot operate the connection
	The user has no access to this connection.

The last active connection is highlighted (blue background). Depending on the configuration of the notion#client, the last active connection can be restored automatically when the notion#client is started

Click on the text "License overview" to show the licenses of the software packages used. The gear wheel takes you to the configuration page of the notion#client. If a password has been stored in the configuration, a password prompt is shown here first.

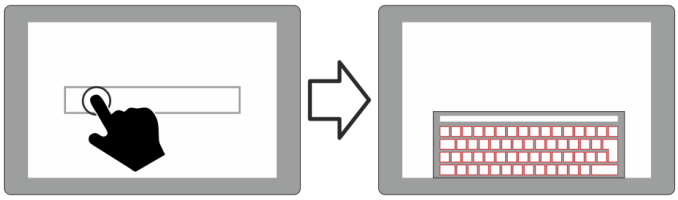


Password prompt when switching to configuration mode

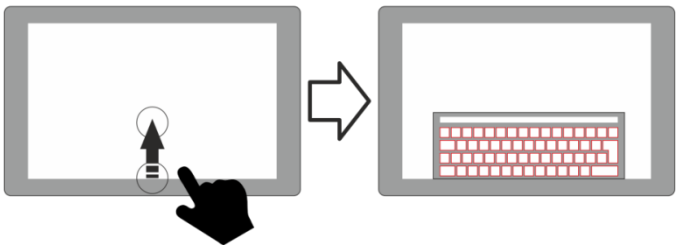
The software version is indicated below the gear wheel.

3.2. On-screen keyboard

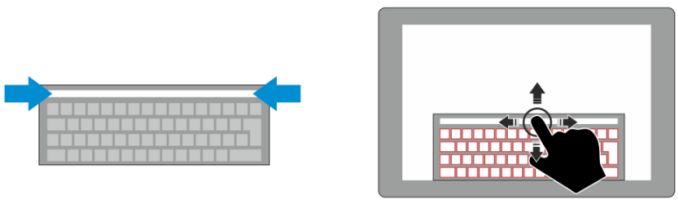
The on-screen keyboard can be activated in two ways. On a configuration page or when a dialog is shown, it can be activated by clicking on the input field



When a viewer is active, a swipe gesture is required. Starting at the bottom of the screen, swipe towards the center of the screen



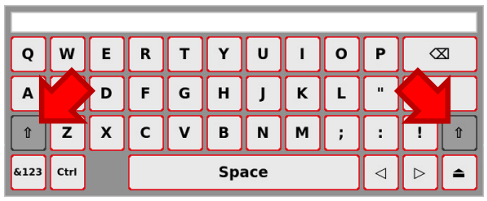
The keyboard can be moved freely on the screen. To do this, touch the drag bar (the white field above the keys) with your finger and move the keyboard as required



If the “Hide” button is pressed (symbol in the bottom right-hand corner), the keyboard is hidden again.

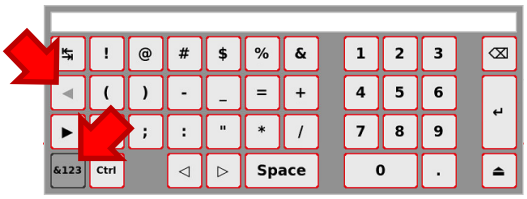
The on-screen keyboard provides several levels. These levels are shown below:

Keyboard in standard view

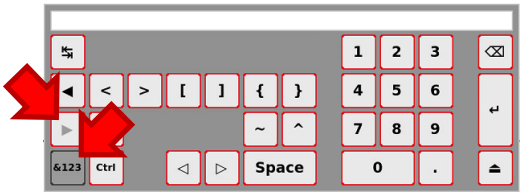


Keyboard with activated shift key

Keyboard with activated control key



Keyboard (numbers and special characters 1)



Keyboard (numbers and special characters 2)

3.3. Reset to factory settings

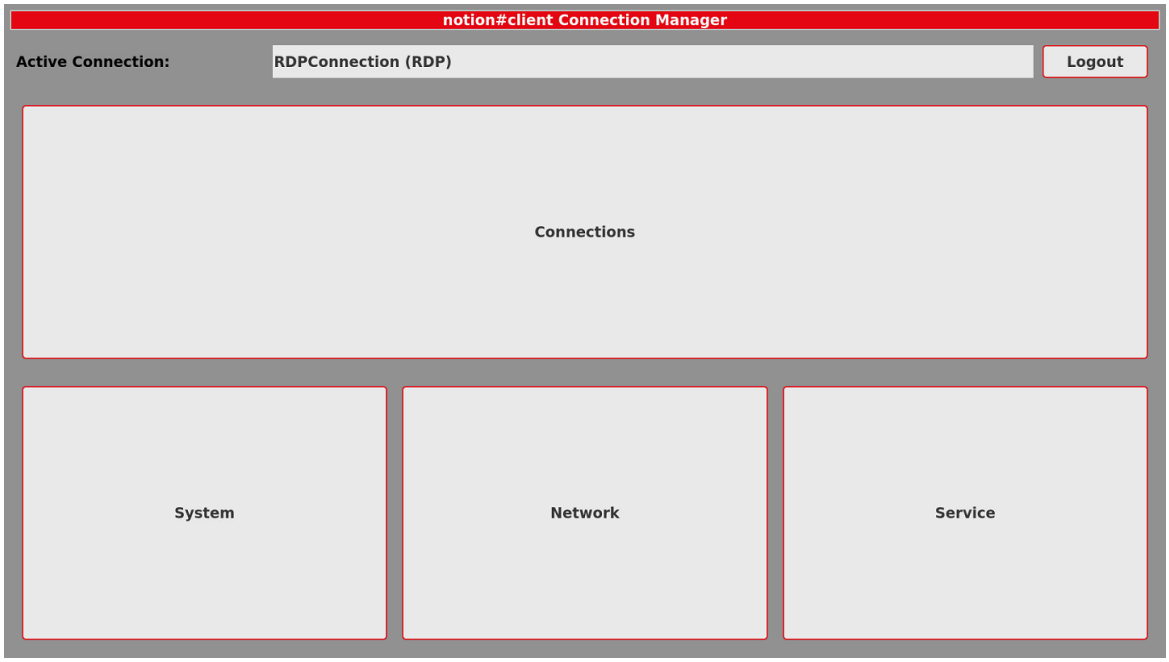
When resetting to factory settings, all user settings and all connections are deleted. The factory settings are restored. To do this, the gear wheel symbol must be pressed for more than 5 seconds. After releasing the button, a dialog will appear asking you to enter an access code

Enter the access code

The 17-digit serial number of the device without hyphens must be entered as the access code. The serial number can be found on the label on the back of the device (“S/N”). If entered correctly, the OK button is enabled. If pressed, the device is reset to the factory settings and restarted

3.4. Configuration page

The configuration page takes you to the various configuration areas: the configuration of the connections and the system configuration.



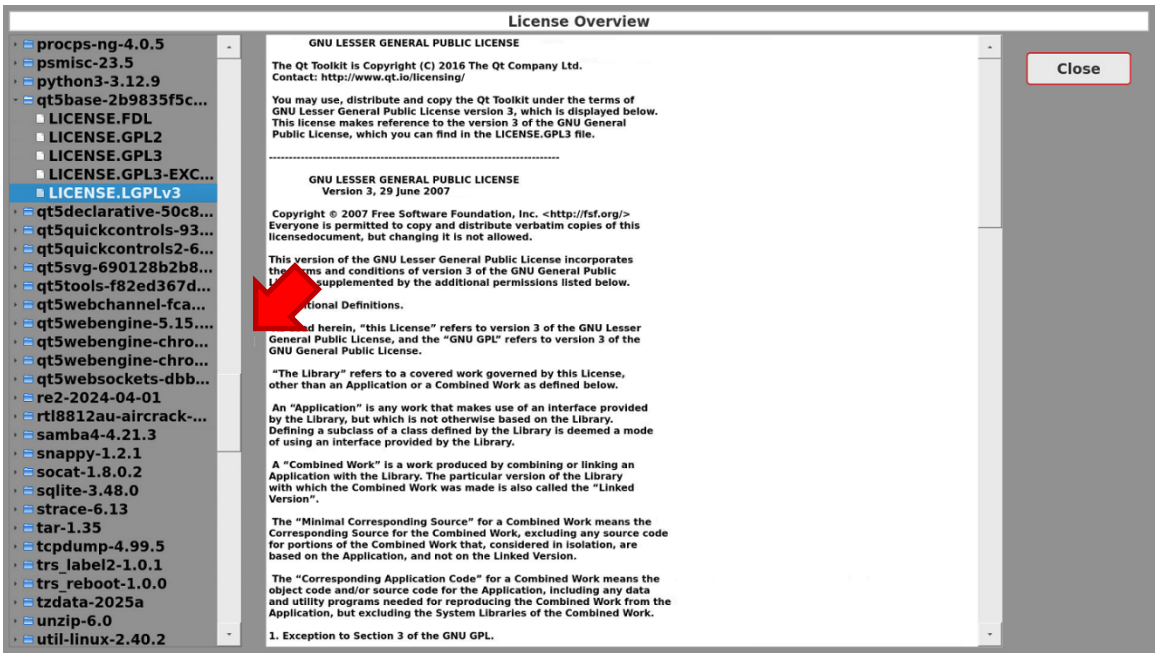
Configuration page

The last selected connection - the active connection - is shown at the top. On the right is the "Logout" button, which can be used to return to the start page. The four configuration areas "Connections", "System", 'Network' and "Service" can be accessed by pressing the respective buttons. In the "Connections" configuration area, the quick selection bar and the users can be configured in addition to the connections (the Daisy-Chain-IO-Extension is required for this).

3.5. License overview

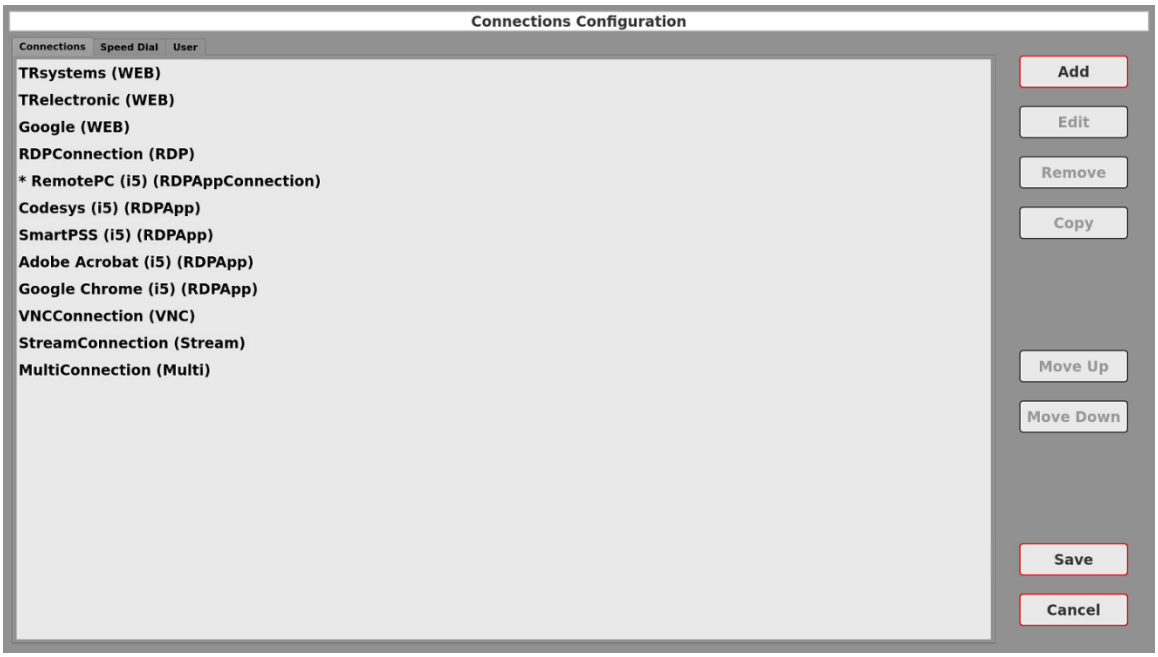
The license texts of the open source packages installed on the system are shown in the license overview. Each package may contain several license texts. They are available for selection on the left-hand side. The text itself is shown in the center of the screen. The license text(s) have been taken unchanged from the source packages and are usually written in English.

The division of the two areas can be varied. To do this, the gray bar (red arrow) can be moved to the right or left as required.



License overview

4. Configure connections

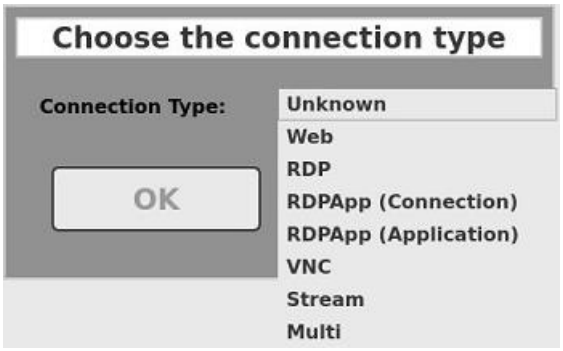


Configure connections

The connection configuration shows all configured connections as they are also displayed in parts on the start page. Connections marked with an asterisk are hidden on the start page. They are used as auxiliary configurations (e.g. in the RDPApp connection configuration) or are embedded in a MultiView view and should not be shown individually. This setting can be made in the respective connection configuration. Connections marked in this way are also not taken into account when using the connection switching gesture and are skipped accordingly during display

On the right-hand side, you will find a series of buttons that are activated or deactivated depending on the selected element. The first four buttons are used to edit the connections. After pressing the "Add" button, a dialog for selecting the connection configuration to be created appears. The respective connection configuration is then shown. The new connection is always added to the end of the list.

Creating a new connection



Create a new connection (selection open)

If an existing connection is selected, it can be changed by clicking on “Edit”. The corresponding connection configuration is shown.

However, if you want to remove the selected connection, click on “Remove”. A confirmation prompt is shown before the connection is removed.

Security prompt when removing a connection

After clicking on “Copy”, the selected connection is used as the base for a new connection configuration and shown. It can then be renamed and customized. This new connection is then also added to the end of the list.

The selected connection can be moved to the desired position using “Move Up” and “Move Down”. A connection that is already at the top or bottom cannot be moved any further in this direction. The respective button is then also disabled.

All changes made are only applied and saved in the configuration file when the connection configuration is exited using the “Save” button. When exiting the connection configuration via the “Cancel” button, all changes made are discarded.

4.1. General configuration elements

4.1.1 Common configuration elements

Each connection configuration has the “Name” input field, which can be used to identify the connection. Although this name does not have to be unique, it is highly recommended.

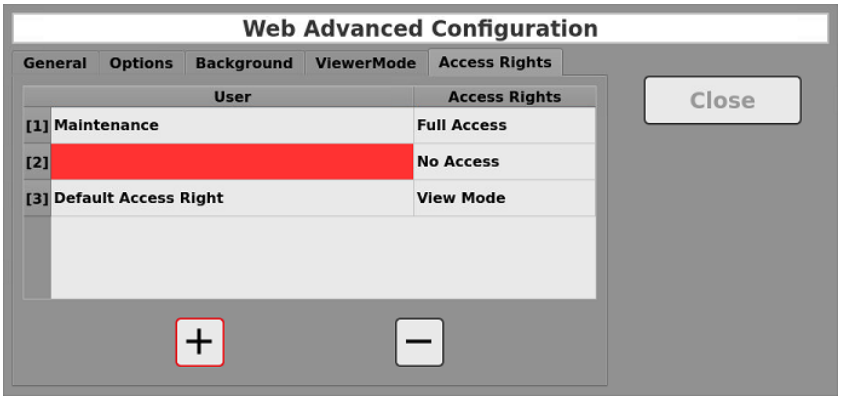
The “Show in start view” checkbox is used to specify whether this connection should be displayed on the start page and taken into account in the connection switching gesture.

The page ID is used when the Daisy-Chain-IO-Extension with IOLink is active. This makes it possible to switch pages externally (e.g. via a PLC). The value 0 indicates that the page ID is not used. Otherwise, this value must be unique. A corresponding check is carried out in the configuration dialog and a page ID that has already been assigned is highlighted in red and the configuration cannot be saved.

If required, the "Advanced" button can be used to switch to the advanced connection configuration in order to set additional connection parameters. The connection configuration can be exited using the "Save" or "Cancel" buttons. The settings made are then accepted or discarded.

4.1.2 User access configuration

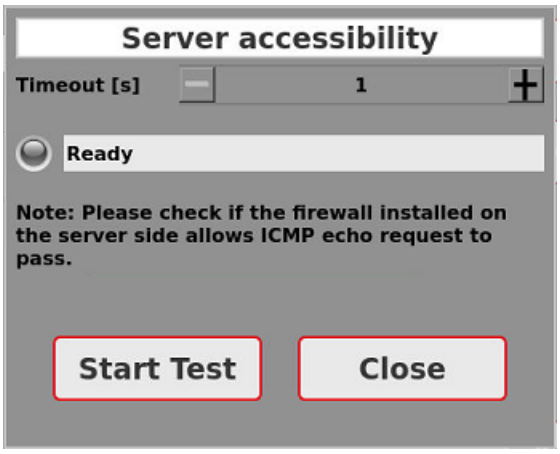
The extended connection configuration includes the user access configuration. This is used if the Daisy-Chain-IO-Extension is installed. Here you can define which user should receive which access right (full access, view mode or no access). The default access right defines which rights users who are not explicitly named in the user configuration should have. Additional users can be added using the "+" button. The "-" button removes the selected user again. Incorrectly configured entries are displayed with a red background and prevent you from exiting the configuration dialog. Users are configured on the overview page of the connection configurations under the "Users" tab.



Configuration of user access rights (with incorrect entry)

4.1.3 Accessibility test

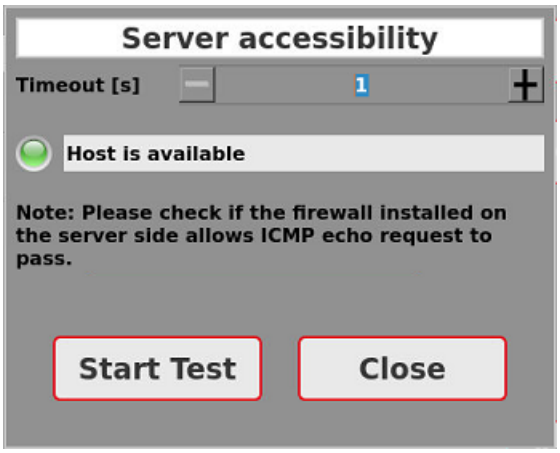
The "Accessibility test" can be used to check whether the specified IPv4 address or network name is accessible or can be resolved. The server computer is pinged for this purpose (sending an ICMP echo request).



Dialog of the accessibility test

The test is started with the "Start Test" button. The "Timeout" parameter specifies the maximum waiting time for a response from the server. The status of the test is shown as follows via the LED and the status field:

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

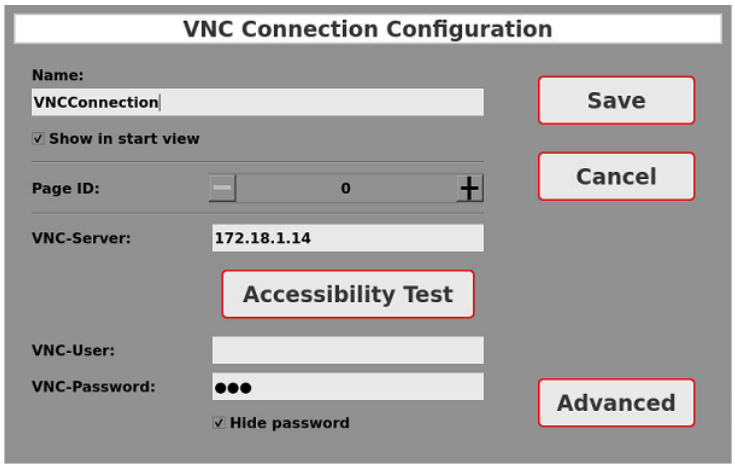


Display of the result of the accessibility test

4.1.4 Storing passwords

Passwords are always stored in encrypted form in the configuration file to make it more difficult to access the password.

4.2. Configuring the VNC connection

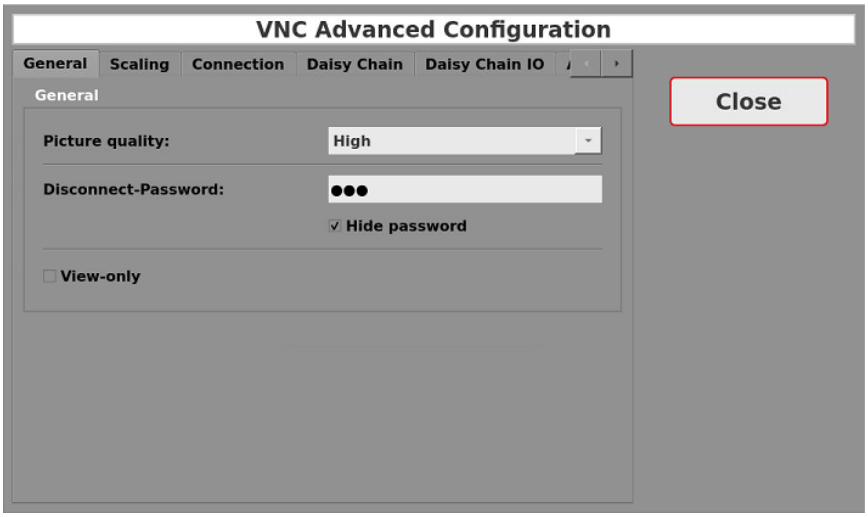


Basic configuration of the VNC connection

The IPv4 address or the network name of the VNC server is entered in the “VNC server” input field. If the VNC standard port (5900) is not to be used, it can be appended to the IPv4 address or network name using “:” (e.g. 172.18.1.10:5900). The port number can also be specified in a short form. If the port number is less than 100, this information is added to the standard port.

Further input fields are the “VNC User” and the “VNC Password”. Depending on the server configuration, they can be entered here. Both input fields are optional. The “Hide password” checkbox can be used to switch between hidden display and plain text display of the password.

If no user name or password is stored for logging on to the server, but it is required by the server, an input dialog is shown where this information can be entered. This information is then stored in the configuration file.

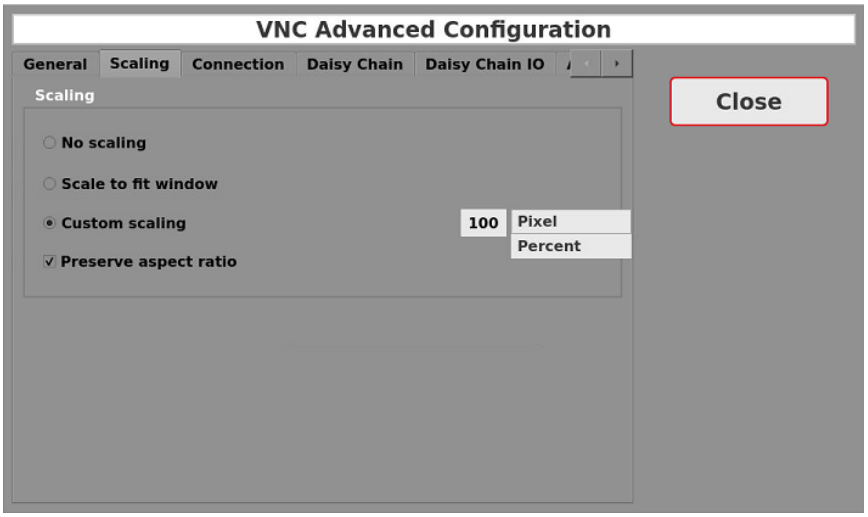


Advanced VNC configuration: General settings

Among other things, the picture quality can be set in the general settings. The following setting options are available: High, Good, Medium and Low. In addition to the picture quality, this parameter also influences the required bandwidth of the connection.

Optionally, a password can be entered that is requested when the connection is to be disconnected. If this field is not empty, a password query dialog is shown. The "Hide password" checkbox can be used to switch between hidden display and plain text display of the password.

If view-only mode is activated, entries via mouse or touchscreen and keyboard are not forwarded to the VNC server



Advanced VNC configuration: Scaling setting

The following options are available when setting the scaling

- No scaling

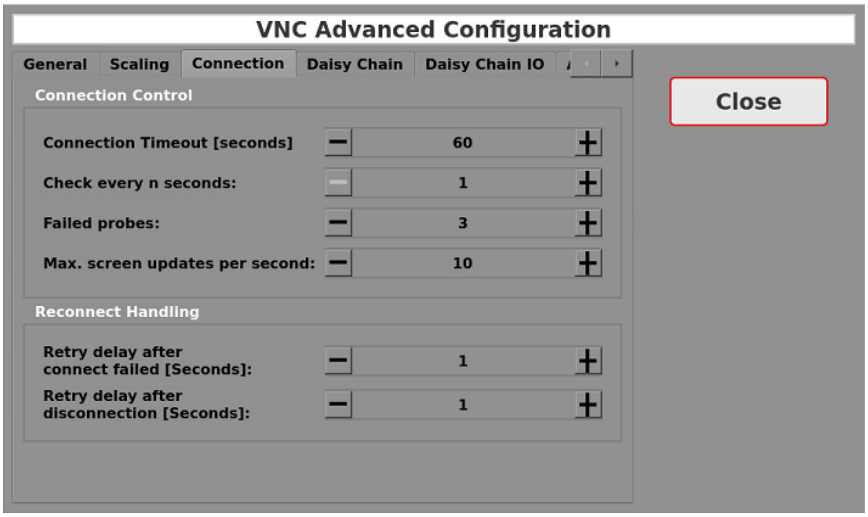
The received VNC images are shown in the same resolution as they are transmitted from the server. This can result in the display showing black borders or scroll bars.

- Scale to fit window

The VNC images received are scaled so that they fill the entire screen. If "Preserve aspect ratio" is also activated, the aspect ratio is preserved and black borders (top/bottom or side) may appear.

- Custom scaling

Any scaling in pixels or as a percentage of the original resolution can be selected. If "Preserve aspect ratio" is also activated, the same scaling factor is used for the X and Y directions. Otherwise, different scaling factors can be specified for the X and Y directions.



Advanced VNC configuration: Setting the connection options

The following options are available for the connection settings

- Connection Timeout [seconds]

Specifies the time period after which the connection setup should be terminated. This is specified in seconds.

- Check every n seconds

Specifies how often the connection to the VNC server should be checked. This is specified in seconds.

- 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

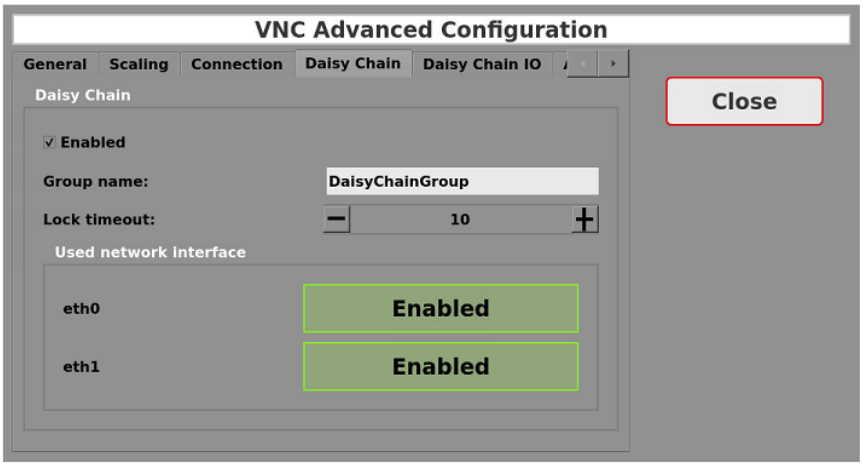
With a high rate of changes to the screen content, it is possible that the notion#client can no longer be operated smoothly or that the screen layout suffers as a result. To prevent this, the maximum number of screen updates can be limited.

- Retry delay after connect failed [seconds]

Specifies how long to wait after a failed connection before starting a new connection. This is specified in seconds and can be between 0 and 3600 seconds. If the value is 0 (display OFF), no further attempt is made to re-establish the connection.

- Retry delay after disconnection [seconds]

Specifies how long to wait after a disconnection before attempting to re-establish the connection. This is specified in seconds and can be between 0 and 3600 seconds. If the value is 0 (display OFF), no further attempt is made to re-establish the connection.



Advanced VNC configuration: Settings of the network-based Daisy Chain

"Daisy chain" is a method for using multiple VNC clients on a VNC server to block input to the other VNC clients while your own VNC client remains operable. However, this function is only available when using notion#clients throughout.

- Enabled

Activates the daisy chain function on this VNC client. All other VNC clients must then also have an activated daisy chain in order to be able to use this function.

- Group name

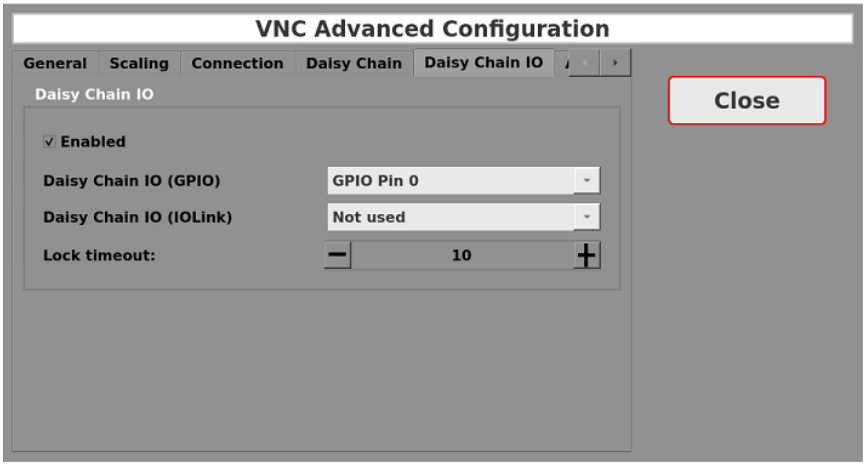
Freely selectable group name that can be used to combine VNC clients into groups. Only VNC clients from the same group react to the mutual input blocks.

- Lock timeout

Specifies how long the locked VNC clients should remain locked after the last action (operation via the touchscreen or keyboard). The blocking time is specified in seconds.

- Used network interface

All active network interfaces are displayed here and you can select which of these interfaces should be used to send Daisy Chain communication to the other clients. The network configuration of the notion#client devices must be designed in such a way that the corresponding devices can also communicate with each other.



Advanced VNC configuration: Daisy Chain IO settings

"Daisy Chain IO" can be used, for example, to signal to a connected PLC that a VNC client is currently being operated. However, it is independent of the "Daisy Chain" option and can also be used individually. The optional Daisy-Chain-IO-Extension is required for this function.

- Enabled

Activates the Daisy Chain IO function on this VNC client.

- Daisy Chain IO (GPIO)

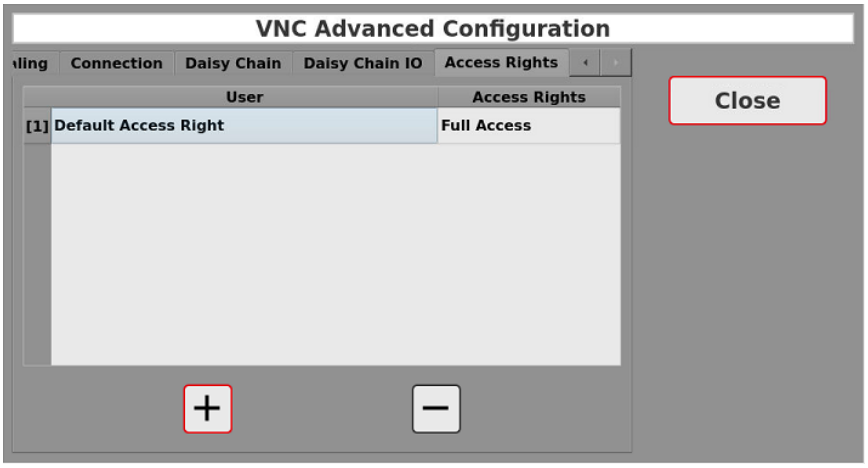
Specifies which GPIO pin is to be used for signaling. The "Not used" setting can be used to switch off signaling via GPIO. Available depending on the equipment of the Daisy-Chain-IO-Extension.

- Daisy Chain IO (IOLink)

Specifies which register bit in the IOLink data area is to be used for signaling. The "Not used" setting can be used to switch off signaling via IOLink. Available depending on the equipment of the Daisy-Chain-IO-Extension.

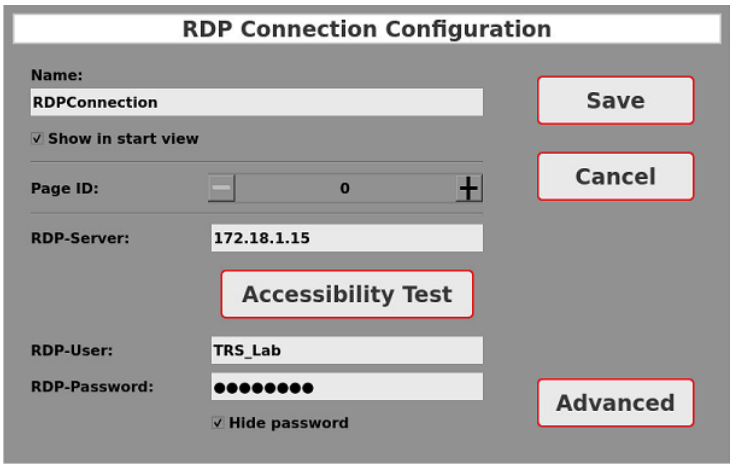
- Lock timeout

Specifies how long the signaling should remain active after the last action (operation via the touchscreen or keyboard). The blocking time is specified in seconds.



Advanced VNC configuration: Setting user access rights

4.3. Configuring the RDP connection

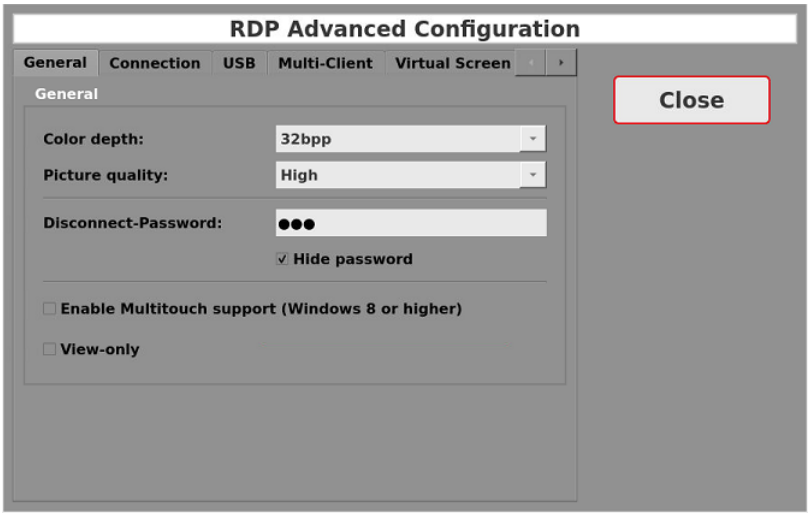


Basic configuration of the RDP connection

The IPv4 address or the network name of the RDP server is entered in the "RDP-Server" input field. If the RDP standard port (3398) is not to be used, it can be appended to the IPv4 address or the network name using ":" (e.g. 172.18.1.10:3398).

Further input fields are the "RDP User" and the "RDP Password". Depending on the server configuration, they can be entered here. Both input fields are optional. The "Hide password" checkbox can be used to switch between hidden display and plain text display of the password.

If no user name or password is stored for logging on to the server, but it is required by the server, an input dialog is displayed where this information can be entered. This information is then stored in the configuration file.



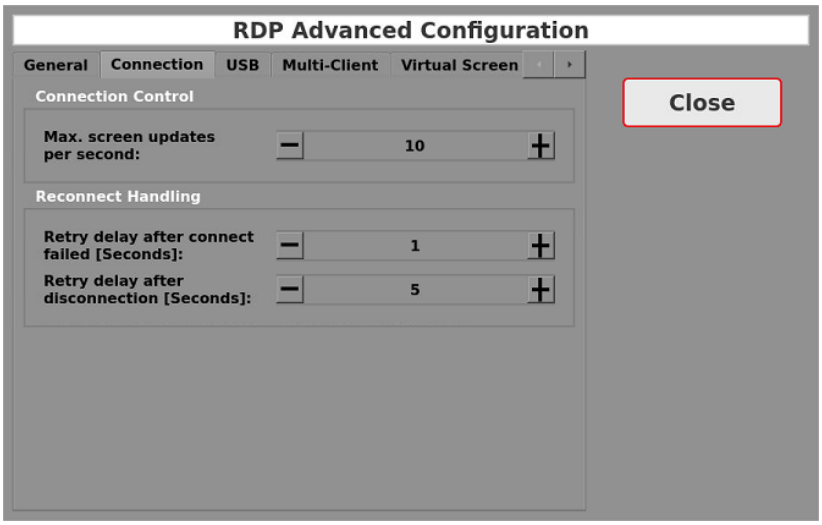
Advanced RDP configuration: General settings

Among other things, the color depth and image quality can be set in the general settings. The setting options 15bpp, 16bpp, 24bpp and 32bpp are available for the color depth. The picture quality can be set with the options High, Good, Medium and Low. In addition to the display, these settings also influence the required bandwidth of the connection.

Optionally, a password can be entered that is requested when the connection is to be disconnected. If this field is not empty, a password query dialog is shown. The "Hide password" checkbox can be used to switch between hidden display and plain text display.

The option "Enable Multitouch support" is available for newer Windows versions. If this option is not active, touch inputs are forwarded as single-touch (1-finger, mouse emulation). If it is activated, however, touch input is forwarded as multi-touch (several fingers) and thus allows multi-finger operation on the connected Windows computer.

If view-only mode is activated, input via mouse or touchscreen and keyboard is not forwarded to the RDP server



Advanced RDP configuration: Setting the connection options

The following options are available in the connection settings

- Max. screen updates per second

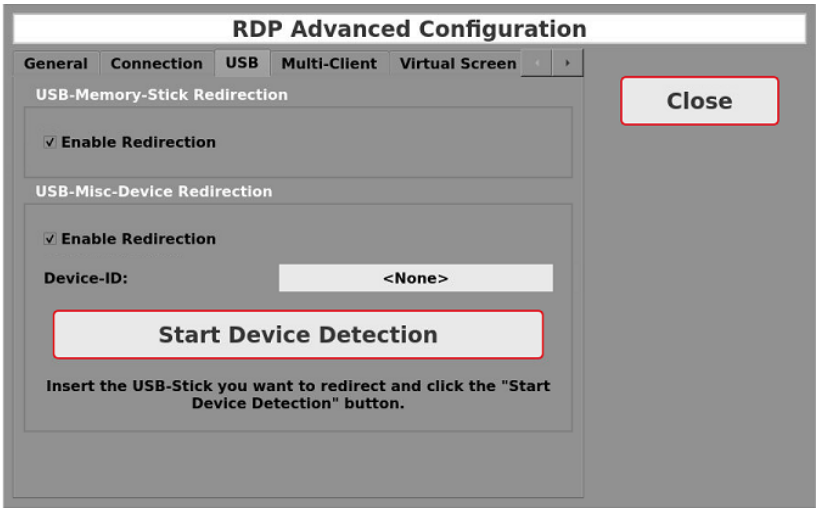
With a high rate of changes to the screen content, it is possible that the notion#client can no longer be operated smoothly or that the screen layout suffers as a result. To prevent this, the maximum number of screen updates can be limited.

- Retry delay after connect failed [Seconds]

Specifies how long to wait after a failed connection before starting a new connection. This is specified in seconds and can be between 0 and 3600 seconds. If the value is 0 (display OFF), no further attempt is made to re-establish the connection.

- Retry delay after disconnection [Seconds]

Specifies how long to wait after a disconnection until another attempt is made to re-establish the connection. This is specified in seconds and can be between 0 and 3600 seconds. If the value is 0 (display OFF), no further attempt is made to re-establish the connection.



Advanced RDP configuration: USB redirection

With the "USB-Memory-Stick Redirection" function, USB memory sticks or USB hard disks that are inserted in the notion#client can be forwarded to the Windows host and are available there as network drives. USB storage media can be inserted or removed as required during the connection and are displayed dynamically.

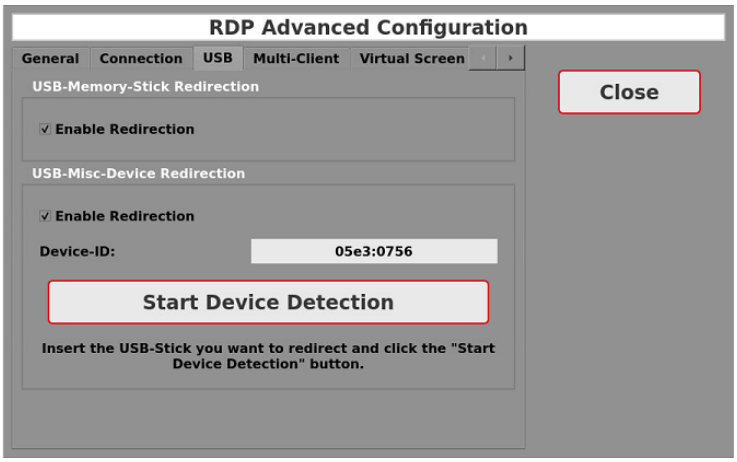
Attention: To avoid data loss, you should check whether the USB storage medium is still being actively used by the notion#client before removing it. The status is shown in the info dialog of the viewer.

With the "USB-Misc-Device Redirection" function, individual USB devices can be redirected to the Windows host. To do this, the device is plugged in after activating redirection and then the "Start device detection" button is pressed. The recognized USB ID (vendor and device ID) is then shown in the "Device ID" field.

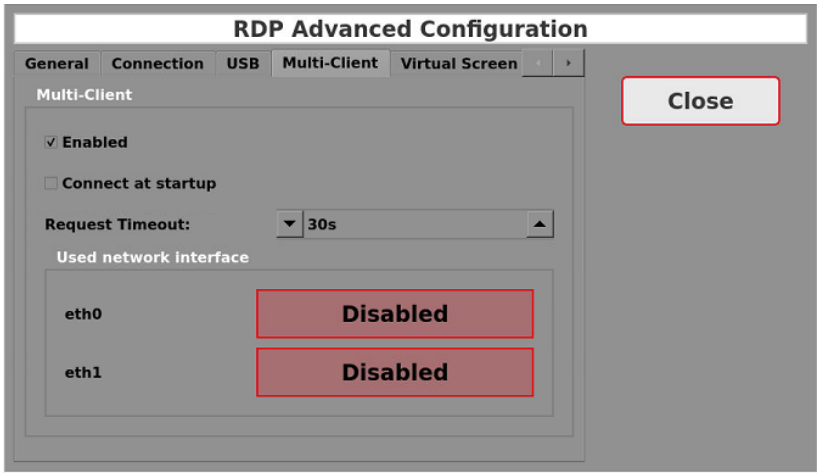
Important: If the devices are to be used during the connection, they must be plugged in before the connection is established. However, if they are not plugged in, this will not result in an error. Suitable drivers are also required for use under Windows. This function is also not available for all USB devices.

To be able to use this function to its full extent, settings must be made on the Windows host. This requires the Group Policy Editor (gpedit.mcs - start as administrator from the command line).

- 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 a reboot of the host



Advanced RDP configuration: USB forwarding (with recognized device ID)



Advanced RDP configuration: Multi-Client settings

The RDP multi-client mode is a function to enable synchronized access to a Windows host for several RDP and RDPApp clients. The clients can be located on the same device or on other notion#client devices connected via the network.

- Enabled

Activates the RDP multi-client function for this RDP client. All other RDP / RDPApp clients must then also activate this function in order to be able to use it.

- Connect at startup

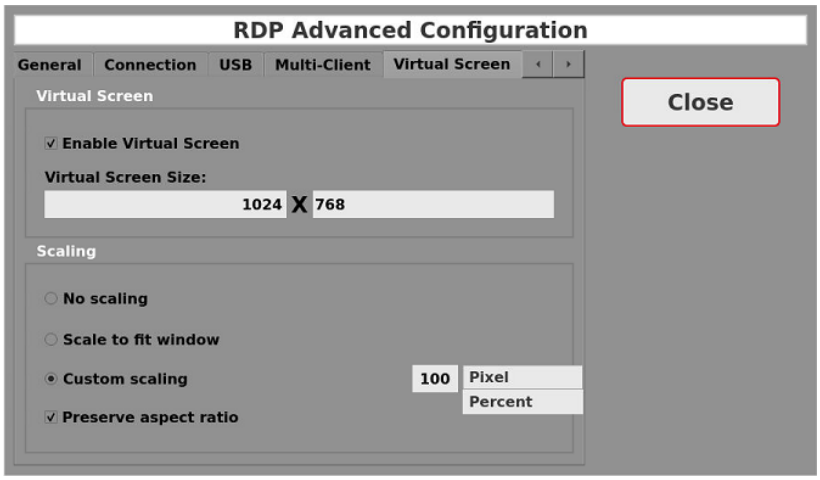
If the connection to the Windows host has not yet been established by any other RDP / RDPApp client, a connection is established immediately instead of the request dialog

- Request Timeout

Specifies the period of time after which the takeover request is canceled and the connection is forcibly taken over. The timeout is specified in seconds.

- Used network interface

All active network interfaces are shown here and you can select which of these interfaces should be used to send the multi-client communication to the other clients. If no network device is selected, the function works purely locally on the device.



Advanced RDP configuration: Virtual screen and scaling

With RDP, the available screen resolution or the resolution of the view with MultiView is used by default. If "Enable Virtual Screen" has been activated, the resolution to be used can be specified. The virtual screen can be scaled to adjust the display.

- No scaling

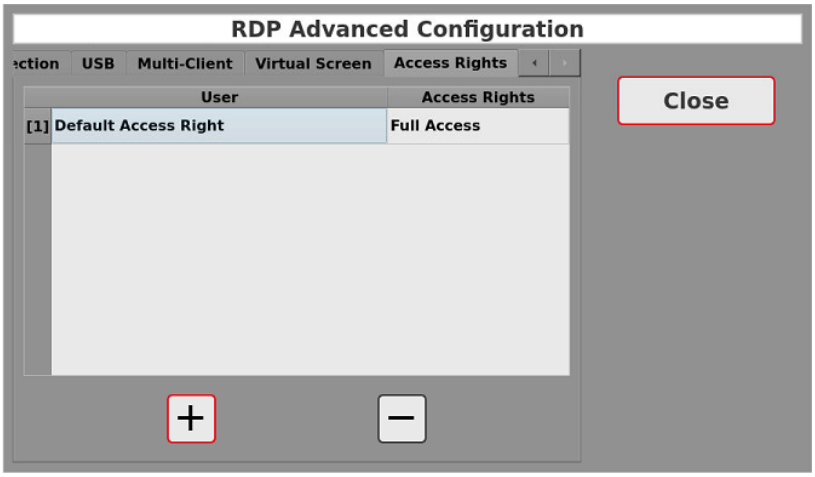
The RDP images received are shown in the specified resolution. This can result in the display showing black borders or scroll bars.

- Scale to fit window

The RDP images received are scaled so that they fill the entire screen. If "Preserve aspect ratio" is also activated, the aspect ratio is preserved and black borders (top/bottom or side) may appear.

- Custom scaling

Any scaling in pixels or as a percentage of the original resolution can be selected. If "Preserve aspect ratio" is also activated, the same scaling factor is used for the X and Y directions. Otherwise, different scaling factors can be specified for the X and Y directions.



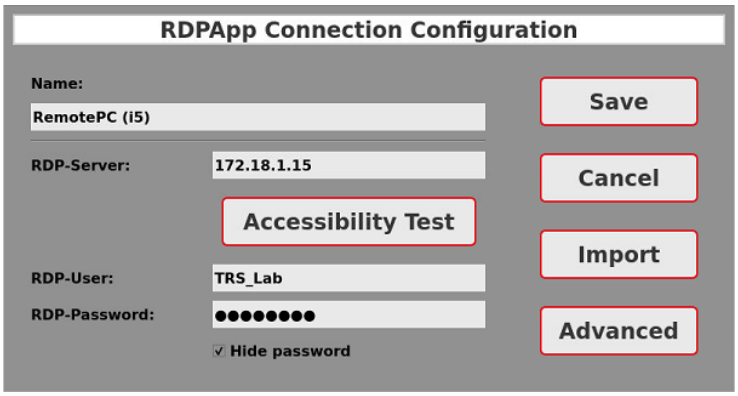
Advanced RDP configuration: Setting user access rights

4.4. Configuring the RDPApp connection

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

4.4.1 Configuring the connection

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

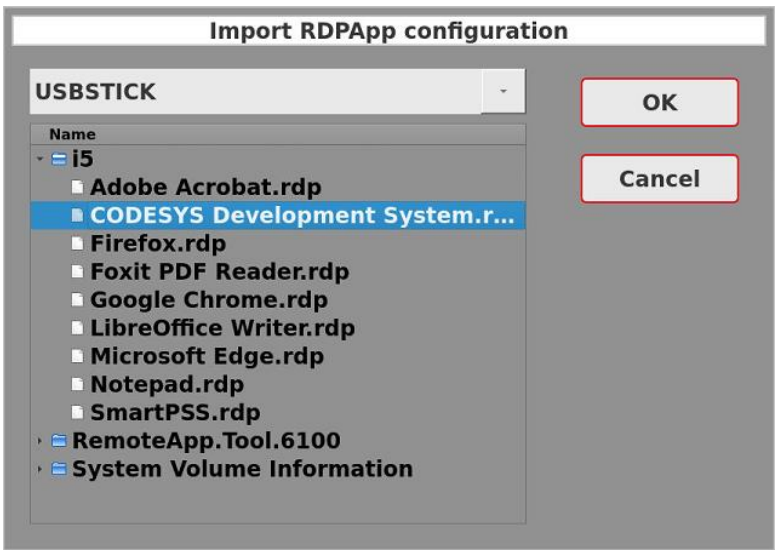


Basic configuration of the RDPApp connection

The IPv4 address or the network name of the RDP server is entered in the "RDP-Server" input field. If the RDP standard port (3398) is not to be used, it can be appended to the IPv4 address or the network name using ":" (e.g. 172.18.1.10:3398).

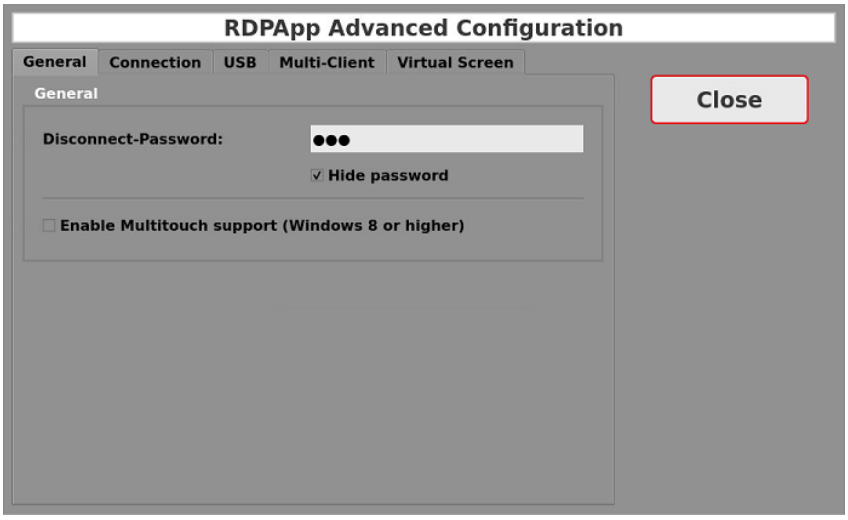
Further input fields are the "RDP-User" and the "RDP-Password". Depending on the server configuration, they can be entered here. Both input fields are optional. The "Hide password" checkbox can be used to switch between hidden display and plain text display of the password.

If no user name or password is stored for logging on to the server, but it is required by the server, an input dialog is shown where this information can be entered. This information is then stored in the configuration file.



Basic configuration RDPApp connection: Import of the configuration file

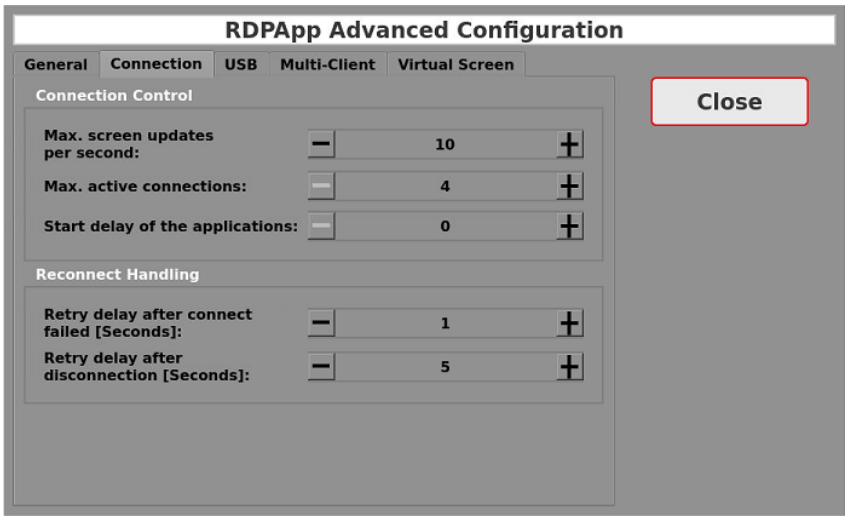
An rdp file with the configuration of the RDPApp connection can be loaded via the "Import" button. This configuration file can be created on the RDP host computer using the RemoteApp-Tool (see the corresponding section).



Advanced RDPApp connection configuration: General settings

Optionally, a password can be entered that is requested when the connection is to be disconnected. If this field is not empty, a password query dialog is shown. The "Hide password" checkbox can be used to switch between hidden display and plain text display.

The option "Enable Multitouch support" is available for newer Windows versions. If this option is not active, touch inputs are forwarded as single-touch (1-finger, mouse emulation). If it is activated, however, touch input is forwarded as multi-touch (several fingers) and thus allows multi-finger operation on the connected Windows computer.



Advanced RDPApp connection configuration: Setting the connection options

The following setting options are available in the connection options settings:

- Max. screen updates per second

With a high rate of changes to the screen content, it can happen that the notion#client can no longer be operated smoothly or that the screen layout suffers. To prevent this, the maximum number of screen updates can be limited.

- Max. active connections

Limits the maximum number of configurable RDPApp applications for this connection. The value can be between 1 and 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.

- Start delay of the applications [Seconds]

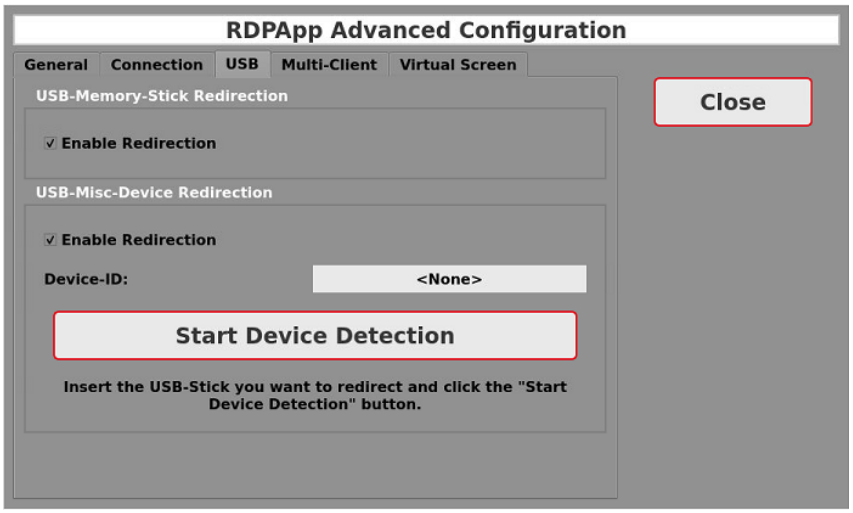
If RDPApp applications do not exit correctly, there may be problems starting the application when reconnecting (see the section Tips and tricks for RDPApp on Windows hosts). If a start script has been installed on the Windows host, a start delay can be configured here to give the script time to run and start the applications afterwards

- Retry delay after connect failed [Seconds]

Specifies how long to wait after a failed connection setup before starting a new connection setup. This is specified in seconds and can be between 0 and 3600 seconds. If the value is 0 (display OFF), no further attempt is made to re-establish the connection.

- Retry delay after disconnection [Seconds]

Specifies how long to wait after a disconnection before attempting to re-establish the connection. This is specified in seconds and can be between 0 and 3600 seconds. If the value is 0 (display OFF), no further attempt is made to re-establish the connection.



Advanced RDP app connection configuration: USB redirection

With the "USB-Memory-Stick Redirection" function, USB memory sticks or USB hard disks that are inserted in the notion#client can be forwarded to the Windows host and are available there as network drives. USB storage media can be inserted or removed as required during the connection and are displayed dynamically.

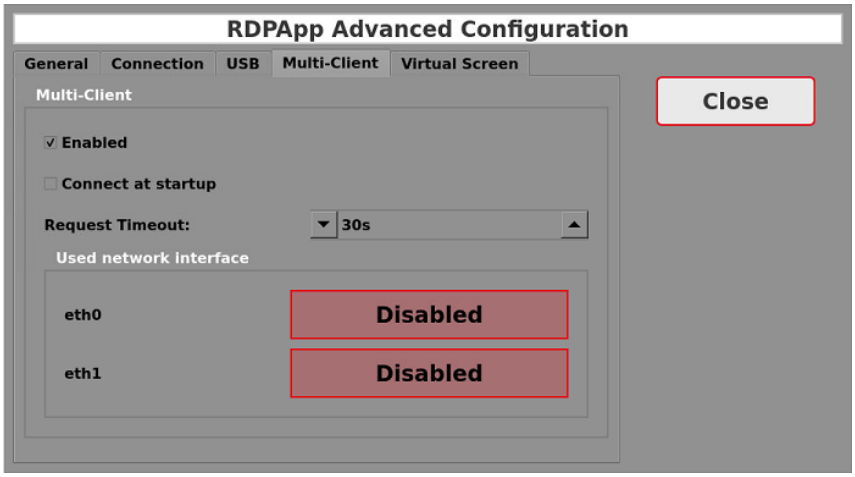
Attention: To avoid data loss, you should check whether the USB storage medium is still being actively used by the notion#client before removing it. The status is shown in the info dialog of the viewer.

With the "USB-Misc-Device Redirection" function, individual USB devices can be redirected to the Windows host. To do this, the device is plugged in after activating redirection and then the "Start device detection" button is pressed. The recognized USB ID (vendor and device ID) is then shown 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. However, if they are not plugged in, this will not result in an error. Suitable drivers are also required for use under Windows. This function is also not available for all USB devices.

To be able to use this function to its full extent, settings must be made on the Windows host. This requires the Group Policy Editor (gpedit.mcs - start as administrator from the command line).

- 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 a reboot of the host



Advanced RDPApp connection configuration: Multi-Client settings

The RDP multi-client mode is a function to enable synchronized access to a Windows host for several RDP and RDPApp clients. The clients can be located on the same device or on other notion#client devices connected via the network.

- Enabled

Activates the RDP multi-client function for this RDPApp client. All other RDP / RDPApp clients must then also activate this function in order to be able to use it.

- Connect at startup

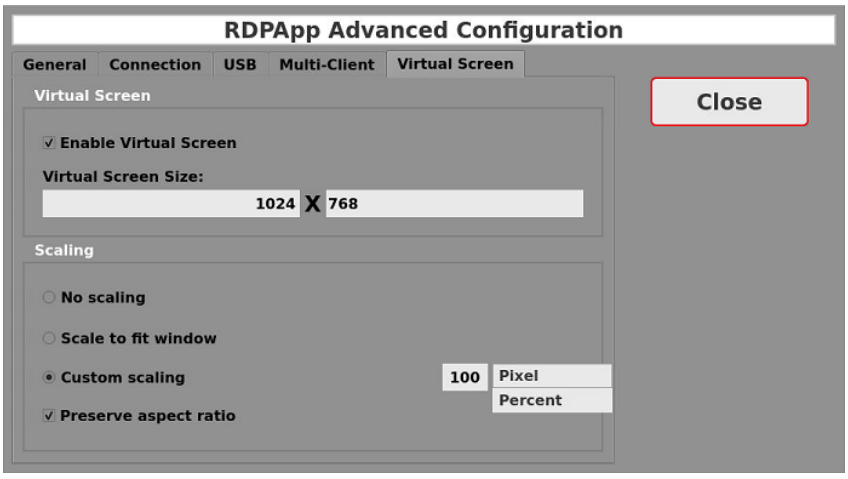
If the connection to the Windows host has not yet been established by any other RDP / RDPApp client, a connection is established immediately instead of the request dialog

- Request Timeout

Specifies the period of time after which the takeover request is canceled and the connection is forcibly taken over. The timeout is specified in seconds.

- Used network interface

All active network interfaces are shown here and you can select which of these interfaces should be used to send the multi-client communication to the other clients. If no network device is selected, the function works purely locally on the device.



Advanced RDPApp connection configuration: virtual screen and scaling

With RDP, the available screen resolution or the resolution of the view with MultiView is used by default. If "Enable Virtual Screen" has been activated, the resolution to be used can be specified. The virtual screen can be scaled to adjust the display.

- No scaling

The RDP images received are shown in the specified resolution. This can result in the display showing black borders or scroll bars.

- Scale to fit window

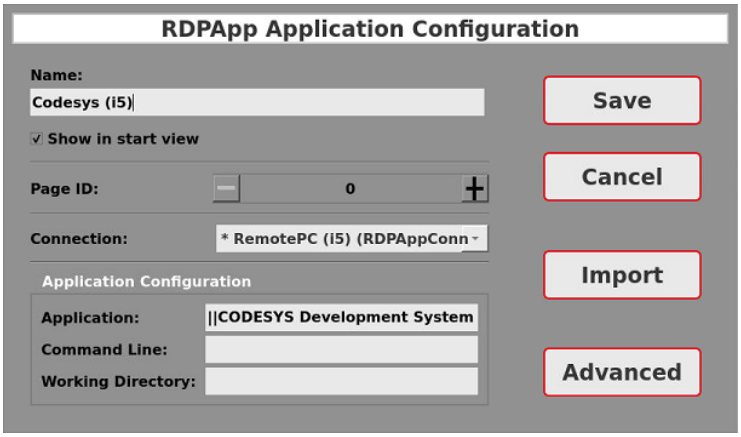
The RDP images received are scaled so that they fill the entire screen. If "Preserve aspect ratio" is also activated, the aspect ratio is preserved and black borders (top/bottom or side) may appear.

- Custom scaling

Any scaling in pixels or as a percentage of the original resolution can be selected. If "Preserve aspect ratio" is also activated, the same scaling factor is used for the X and Y directions. Otherwise, different scaling factors can be specified for the X and Y directions.

4.4.2 Configuring the application

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



Basic configuration of the RDPApp application

The previously configured RDPApp connection to be used for this application is first selected in the "Connection" selection field. Connections that have already reached the maximum number of applications are hidden. If necessary, the maximum number of applications must be adjusted for these connections.

Further settings are:

- Application

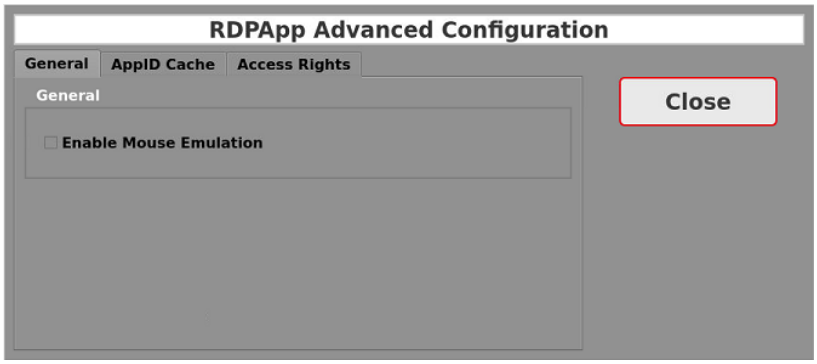
Identifier of the application to be started. The identifier is usually not entered manually, but by importing the rdp file with the configuration of the RDPApp connection.

- Command Line

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

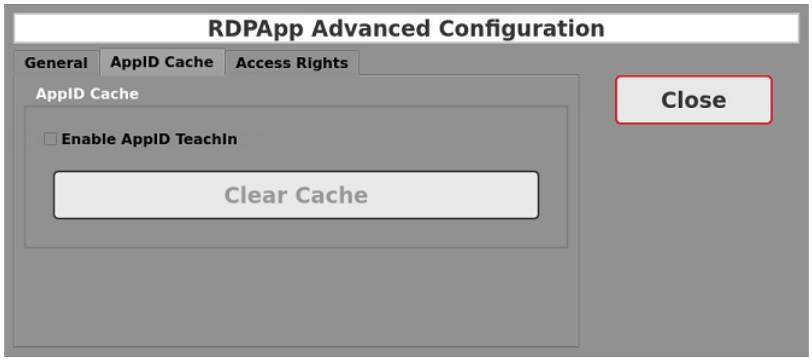
- Working Directory:

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



Advanced RDPApp application configuration: General settings

Only mouse emulation can be activated in the general settings. If multi-touch support is activated in the RDPApp connection configuration, but this causes problems for individual RDPApp applications in the connection, you can switch to mouse emulation (single touch) for the corresponding RDPApp applications. All other RDPApp applications in the connection will then continue to have multi-touch support



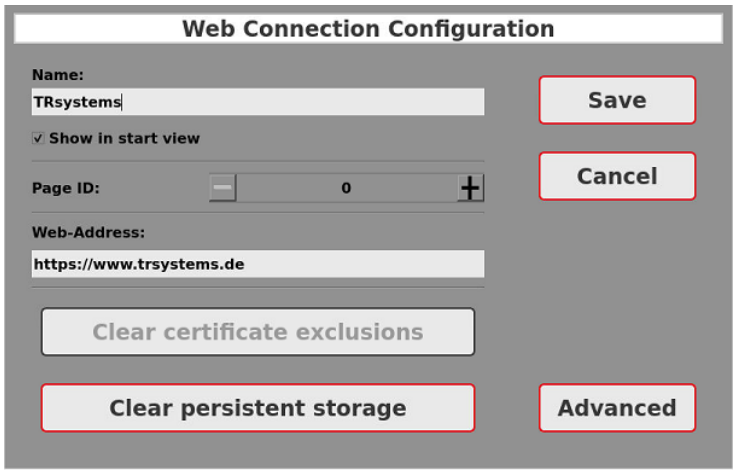
Advanced RDPApp application configuration: AppID Cache

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 MultiView 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, the cache is first deleted and the AppID teach-in is enabled. 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 disabled again.

Advanced RDPApp application configuration: Setting user access rights

4.5. Configuring the Web connection

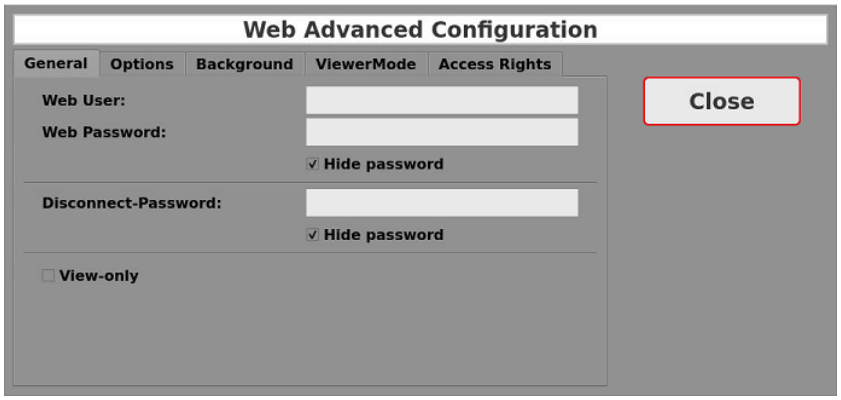


Basic configuration of the web connection

A so-called fully qualified identifier is expected as the web address of the connection (URL in the form http://www.trsystems.de or https://www.trsystems.de)

If the certificate of a connection secured via https is not valid or the certification authority is not one of the generally recognized and trusted certification authorities (e.g. in the case of self-signed certificates), an exception can be created for this connection. In this way, the connection can still be shown. Exceptions created in this way can be deleted again using the "Clear certificate exclusions" button.

When visiting a website, the web browser creates a cache in which website elements (e.g. images) are temporarily stored. If these elements change, this change may not be recognized and the old elements may continue to be shown. Deleting the persistent data makes these changes visible again. This can also be used to delete cookies stored by the website.



Advanced web configuration: General settings

The following settings can be made in the general settings:

- Web User, Web Passwort

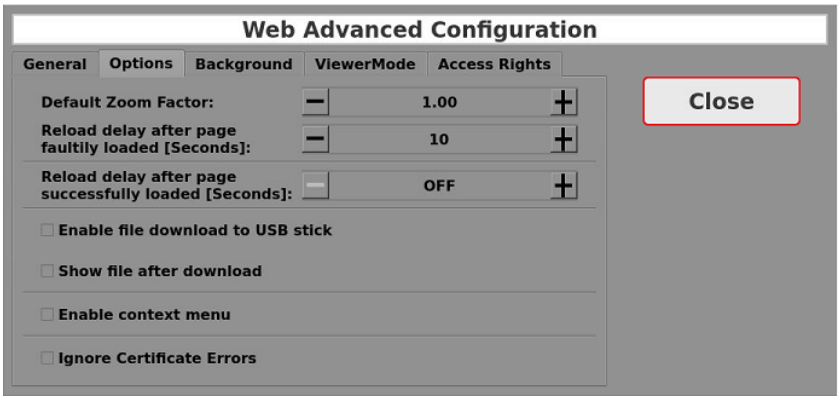
If a website requires authentication when establishing a connection, the necessary user name and password can be entered here. The "Hide password" checkbox can be used to switch between hidden display and plain text display.

- Disconnect-Password

Optionally, a password can be entered that is requested when the connection is to be disconnected. If this field is not empty, a password query dialog is shown. The "Hide password" checkbox can be used to switch between hidden display and plain text display.

- View-only

When view-only mode is activated, inputs via mouse or touchscreen and keyboard are not forwarded to the web browser and the website



Advanced web configuration: Advanced settings

The following settings can be made in the advanced settings:

- Default Zoom Factor

Initial zoom factor with which the website is to be shown

- Reload delay after page faultily loaded

If a website cannot be loaded, e.g. due to network problems, a value in seconds can be entered here after 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

If a website is to be reloaded after a certain time, e.g. due to 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).

- Enable file download to USB stick

If you want to be able to download files from the website, this option must be activated. The download then takes place on an inserted USB stick.

- Show file after download

If a file (such as a PDF document) is to be downloaded temporarily and then displayed immediately, this option must be activated.

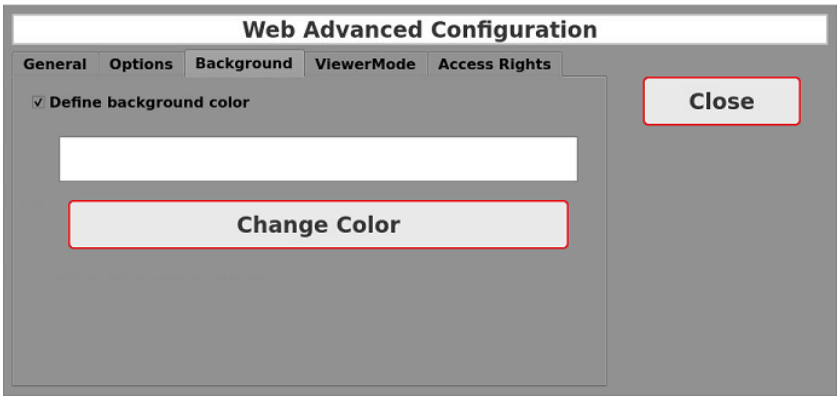
- Enable context menu

If this option is activated, a context menu can be displayed by right-clicking or pressing and holding (tap'n'hold). 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 untrusted certification authority, an exception can be defined for this certificate. However, if it is a self-signed certificate that is regularly recreated on the web server (e.g. after every cold start), an exception would have to be defined for this certificate each time. Alternatively, certificate validation can be dispensed with entirely by activating this option.

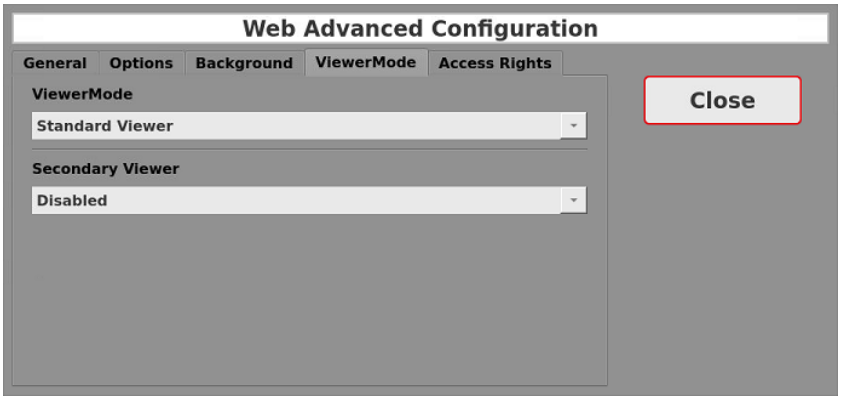
Attention: *This means that the web server is not validated and the connection is no longer trustworthy!*



Advanced web configuration: Background color

If a background color other than the default background color is to be used when the website is loaded, this can be defined here. Both predefined colors can be used and a color can be defined using a color code.

Advanced web configuration: Selecting the background color



Advanced web configuration: Viewer mode

These configuration options can be used to specify how the web viewer should handle websites that request the opening of a new browser tab.

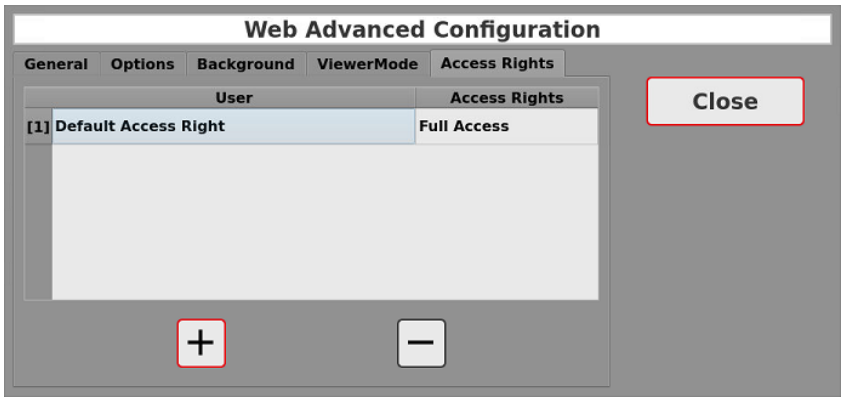
- Viewer Mode

The "Standard viewer" and "Viewer with tabs" options are available. In "Standard viewer" mode, requests to open a new browser tab are simply ignored. The situation is different with the "Viewer with tabs" option. Here, a new tab is created and the corresponding website is shown.

- Secondary Viewer

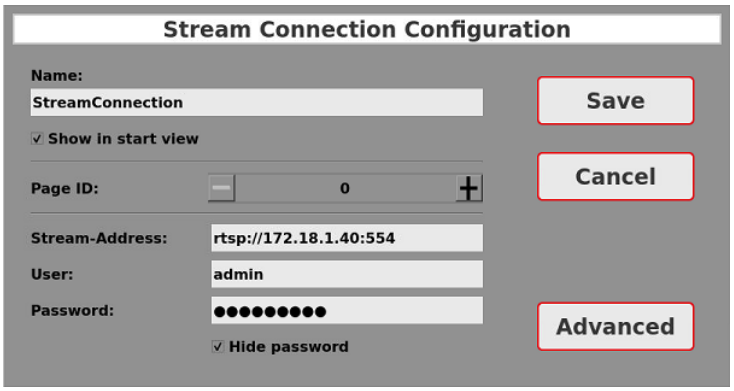
This option can be used to combine two browsers. This makes sense, for example, if a table of contents is to be shown in a MultiView in the main browser and the secondary browser is to show the corresponding website. The secondary browser does not require a URL to be specified in the configuration.

This function is switched off with the "Disabled" option. If the name of another web connection is selected, this function is active.



Advanced web configuration: Setting user access rights

4.6. Configuring the Stream connection



Basic configuration of the stream connection

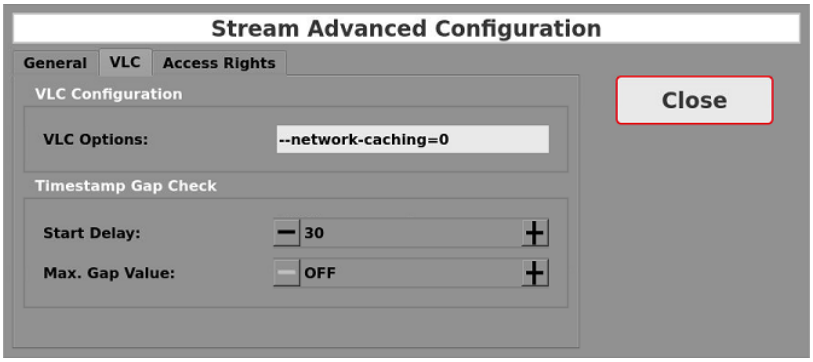
The IPv4 address or the network name of the stream host is entered in the "Stream-Address" input field. If a special port is required, it can be appended to the address as shown above.

Other input fields are the "User" and "Password", which are required to log in to the stream host. Both input fields are optional. The "Hide password" checkbox can be used to switch between hidden display and plain text display of the password.

Advanced stream configuration: General settings

A parameter that is evaluated by the stream host can be entered in the general settings. These are parameters that are appended to the stream address (query part of the URL).

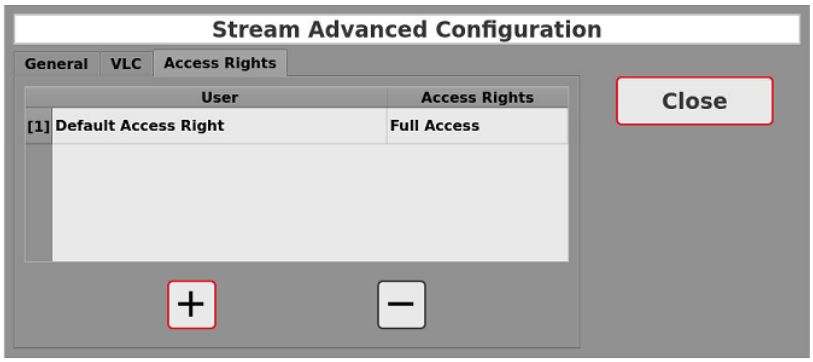
Optionally, a password can be entered that is requested when the connection is to be disconnected. If this field is not empty, a password query dialog is shown. The "Hide password" checkbox can be used to switch between hidden display and plain text display of the password.



Advanced stream configuration: VLC options

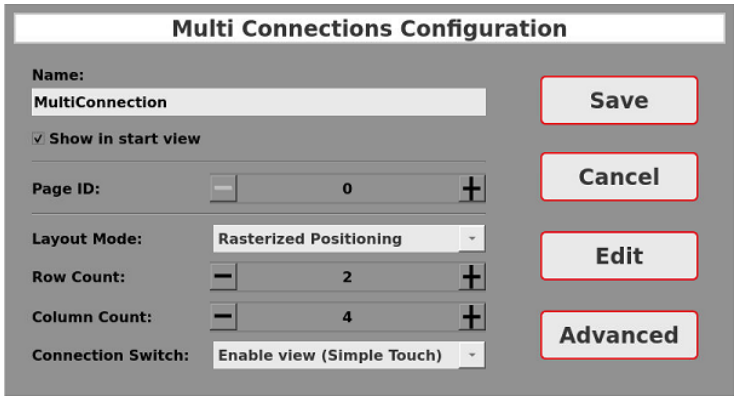
The VLC options can be used to control the behavior of the VLC streaming kernel. For example, the "network-caching" option can be used to specify how many milliseconds should be buffered to ensure a smooth playback. However, this also increases the latency. Another parameter "rtsp-tcp" can be used to switch between TCP and HTTP protocols when transmitting RTSP streams. Further parameters can be found in the VLC documentation if required.

Timestamp Gap Check is used to monitor the timestamp reported by the VLC streaming core. If the gaps are too large, the connection is terminated and reestablished. The start delay (value in seconds) specifies how long the start of monitoring should be delayed after the connection is established. The maximum difference value (value in seconds) specifies how large the gaps may then become.



Advanced stream configuration: Setting user access rights

4.7. Configuring the MultiView connection



Basic configuration of the multiple view connection

The multiple view connection configuration (MultiView) allows several connections to be displayed on one page. They are shown using two layout modes: "Rasterized Positioning" and "Free Positioning". With rasterized positioning, the number of rows and columns can be specified. Up to 99 rows or columns can be set. A connection can then be shown in this grid. It is possible to use several contiguous rows and columns. It is not possible to overlap connections.

With free positioning, the connections can be positioned with pixel accuracy. Overlapping connections are possible. The active connection (with input focus) is always shown in full. The position and size of the connection can also be specified manually via the context menu when editing the multiple view connection screen.

The "Connection Switch" option can be used to specify how the active connection that responds to inputs should be switched. The following modes are available:

- Switch to single view

Press and hold (tap'n'hold) to switch to the single view. You can return to the multiple view via the info dialog that appears (swipe down from the top edge in the middle).

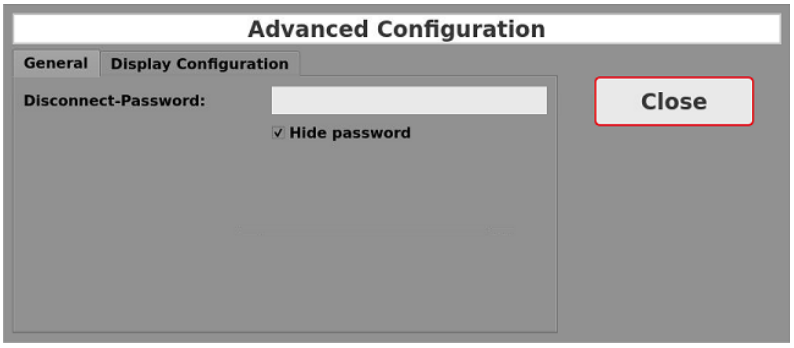
- Enable view (Tap'n'Hold)

After a long press (Tap'n'Hold), the connection receives the focus.

- Enable view (Simple Touch)

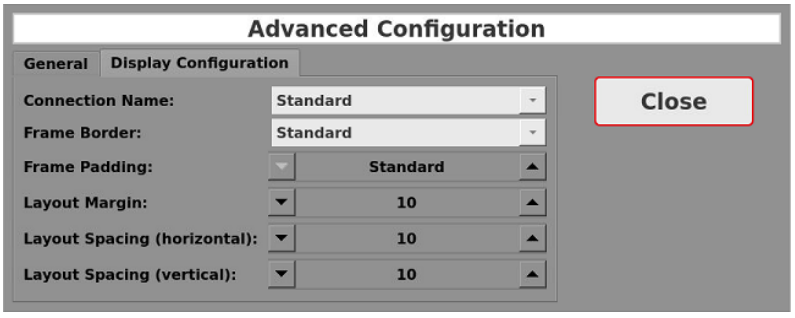
After a single tap, the connection receives the focus.

The "Advanced" button takes you to the advanced configuration of the connection. The positioning of the connections within the configured grid or freely on the screen can be achieved via the "Edit" button.



Advanced multi-connection configuration: General settings

Optionally, a password can be entered that is requested when the connection is to be disconnected. If this field is not empty, a password query dialog is shown. The "Hide password" checkbox can be used to switch between hidden display and plain text display.



Advanced multi-connection configuration: Display settings

The configuration options for the display settings allow you to configure the screen, i.e. how connection names and frames are to be shown. The settings for the layout are only applied if rasterized positioning has been selected.

The following settings are available for displaying the connection name:

- Standard

The default setting corresponds to the "Show" setting

- Show

The connection name is permanently shown at the top of the configured display area of the connection

- Hide

No connection name is shown.

- Overlay (with timeout)

The connection name is shown in the middle of the configured display area of the connection. The display duration can be specified via the separate "Timeout" parameter.

It is also possible to show the display area of the connection with a frame. The following settings are available:

- Standard

The default setting corresponds to the "State Dependent Border" setting.

- Without Border

The display area is shown without a frame.

- Static Border

The display area is shown with a gray frame. The frame spacing can be set using the separate "Frame" parameter. The standard frame spacing is 5 pixels.

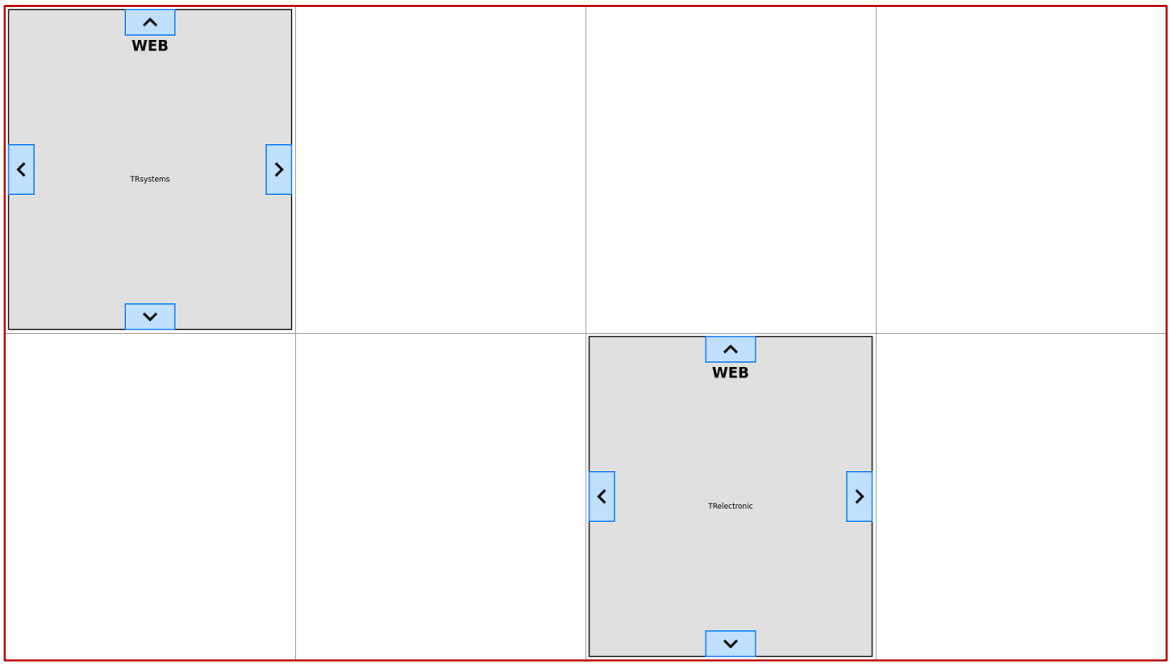
- State Dependent Border

The display area is shown with a colored frame. Depending on the status, the frame is shown in green (display area of the connection has the input focus) or in white. The frame spacing can be set using the separate "Frame" parameter. The standard frame spacing is 5 pixels.

The "Layout Margin" parameter can be used to set the distance of the display areas of the connections to the margin (in pixels) for rasterized positioning. The "Layout Spacing" parameters can be used to set the distance between the display areas of the connections in the horizontal or vertical direction.

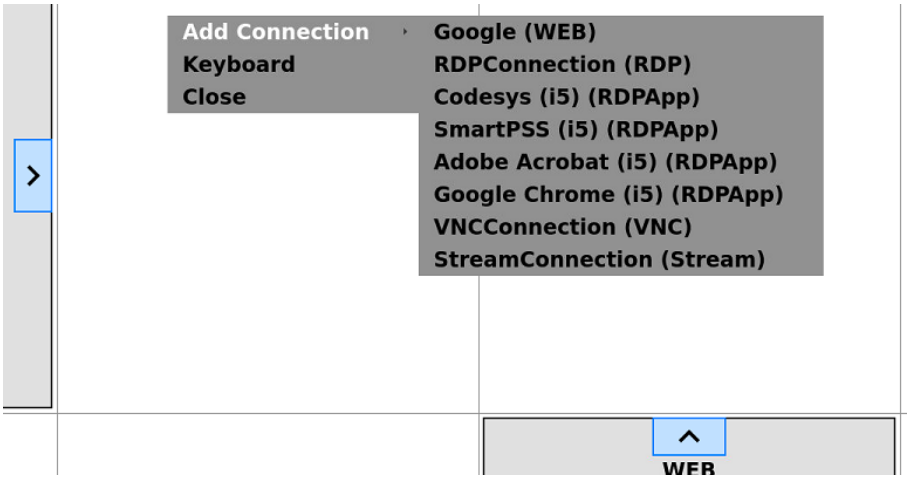
The display editor is used to position the connections. If rasterized positioning is set, the raster is shown with gray auxiliary lines according to the settings. When the connections are shown in the Viewer, these gray lines are not shown. With free positioning, no auxiliary lines are shown. This is a schematic representation; the connection name and frame are not shown. The layout settings are also not taken into account in the display editor.

TRsystems GmbH, Eglishalde 16, 78647 Trossingen, Telefon: +49 (0) 7425 / 228 - 0, Telefax: +49 (0) 7425 / 228 – 34, E-Mail: info(at)trsystems.de



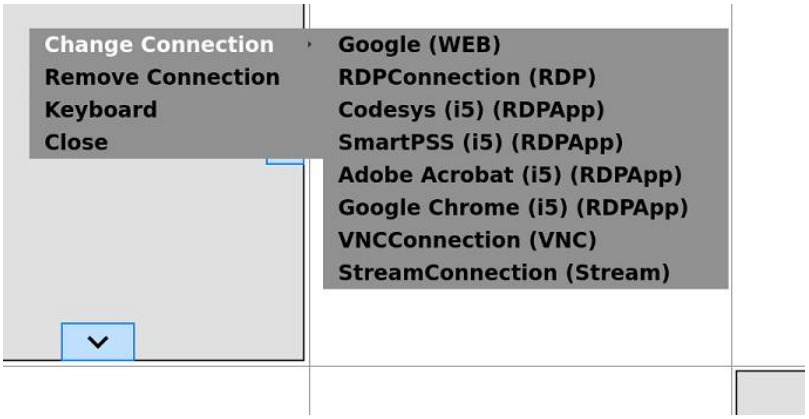
Editing the multiple connection screen

The connections can be positioned on the screen using the blue arrows. With rasterized positioning, the entire area within the grid is automatically used when the auxiliary lines are crossed. If a connection is to be moved, this does not work directly, but can be achieved by enlarging and then reducing the connection in the corresponding directions.



Editing the multiple connection screen: Context menu with empty tile

A new connection can be added by right-clicking with the mouse or by holding down (tap'n'hold) on an empty grid element. A context menu opens. All available connections are shown. Alternatively, a static keyboard can also be added. It serves as a replacement for the dynamic keyboard and, like the connections, can also be positioned in the grid. However, only one keyboard can be used on the multiple connection screen. The “Close” menu item takes you back to the basic configuration.



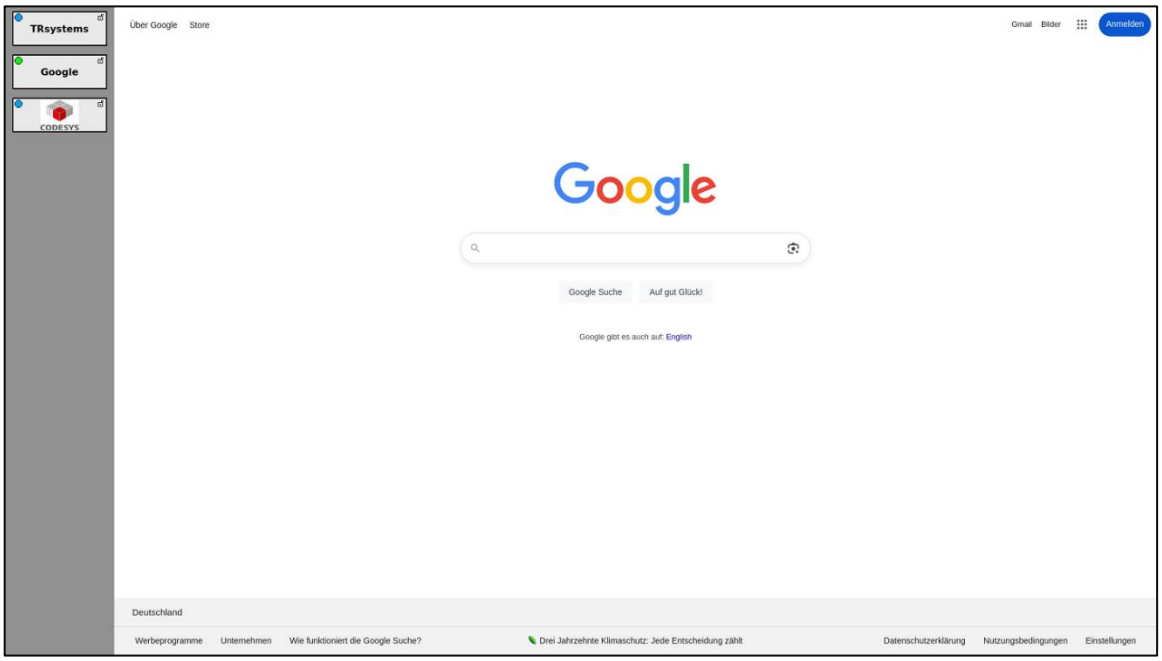
Editing the multi-connection screen: Context menu for tile used

By right-clicking with the mouse or holding down (tap'n'hold) on an existing connection, the connection can be replaced by another connection. A context menu opens for this purpose. All available connections are shown. The existing connection can also be deleted.

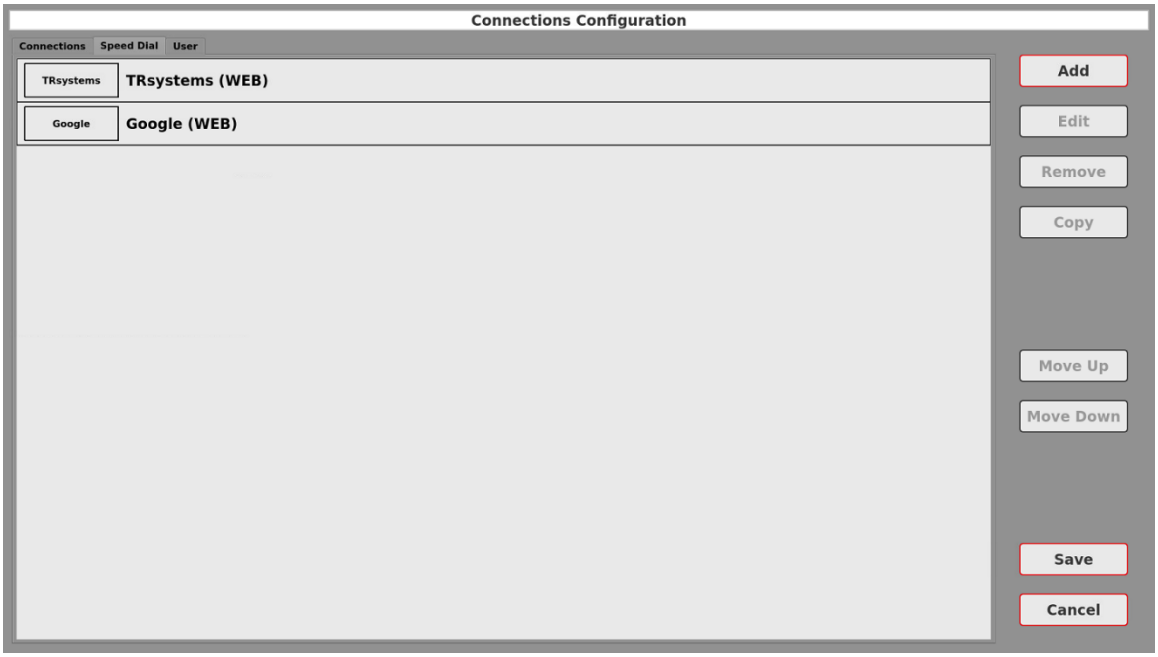
5. Configure the speed dial bar

The speed dial bar allows you to quickly switch between connections at the touch of a button. Unlike the connection switching gesture, the connection is switched directly without displaying any other connections. However, both variants of the connection switch can be activated at the same time.

To be able to use the speed dial bar, it must be activated in the system configuration. There you can also define where the bar should be shown and what dimensions the speed dial buttons should have.

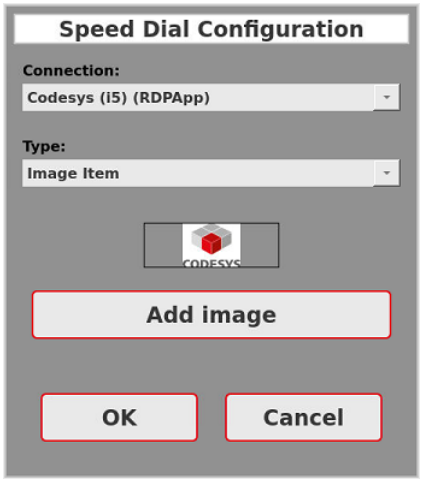


Web viewer with activated speed dial bar



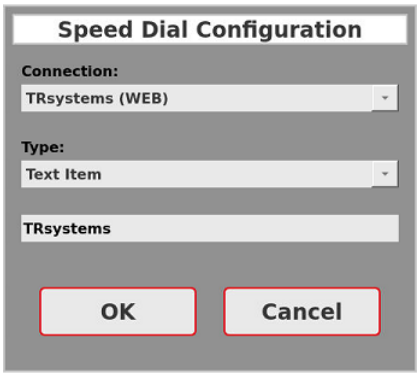
Configure the speed dial bar

The speed dial bar is configured in the same way as the connections. The function of the buttons is identical. There are two speed dial bar element types to choose from: a image item and a text item.



Configuration dialog: Image item

For image items, the type is set to “Image Item”. The connection to be shown can be selected under “Connection”. The common image file types (JPG, PNG, etc.) can be used as the image. The images are scaled to the corresponding size specified in the system configuration. The scaling is carried out taking into account the image aspect ratios.



Configuration dialog: Text item

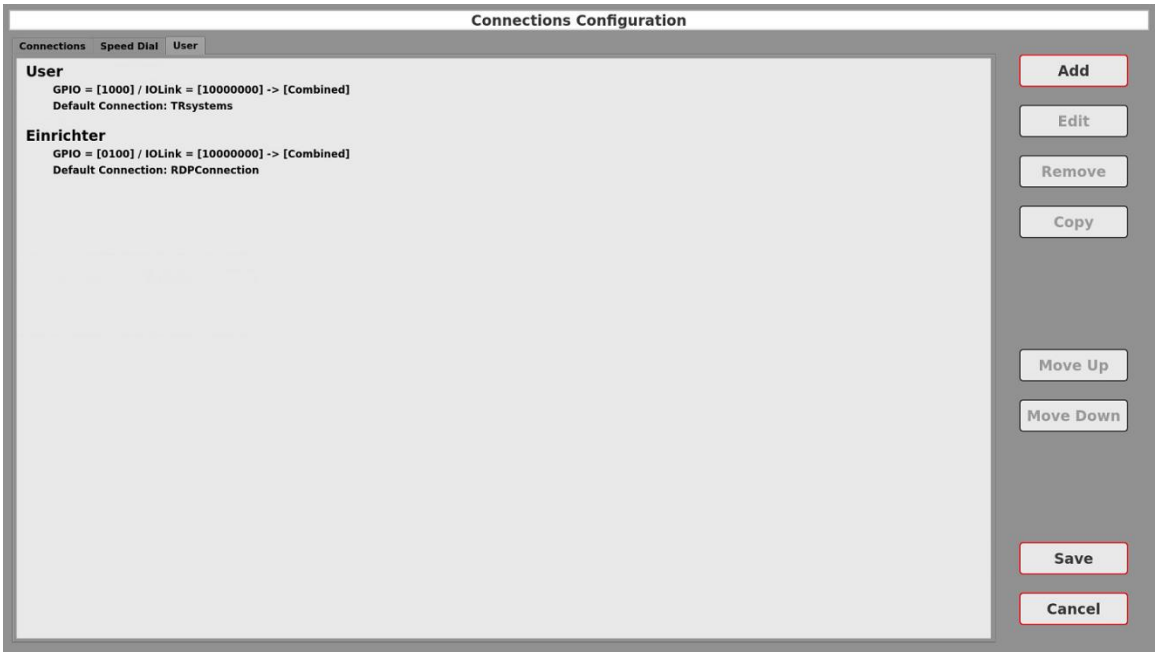
For text items, the type is set to “Text Item”. Under “Connection” you can select the connection to be shown. Any text can be entered. If the text does not fit into a line, it will be wrapped. If it is still too large for the text item, any excess text will be cut off.

Security prompt when deleting a speed dial bar item

6. Configure users

User management is used to restrict access to connections. You can specify whether the connection is fully usable for the current user, only for viewing without interaction or even completely hidden. It is also possible to switch to a standard page when a user changes.

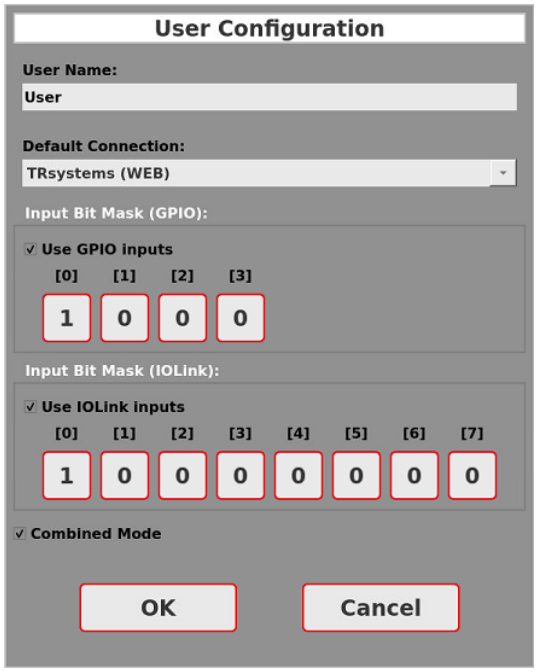
The Daisy-Chain-IO-Extension is required to configure the users.



Configure users

Users are configured in the same way as the connections. The function of the buttons is identical. The users and their configuration are shown in the overview. The order of the user entries is the order in which the bit patterns are later evaluated when evaluating the input signals.

Depending on the equipment variant of the Daisy-Chain-IO-Extension, IOLink inputs and outputs are optionally available in addition to GPIO inputs and outputs. IOLink also provides the PLC with a wide range of additional information (see the chapter on Daisy-Chain-IO).



User configuration dialog

The configuration of the user begins with the entry of a unique name. If the user name is already in use, the user cannot be created. Under "Default Connection", you can optionally select a connection that should be used directly when logging in.

A bit pattern is then entered with which the user can be identified. A number of combinations are available here. GPIO inputs and (if available) IO-Link inputs can be activated independently of each other. They would then be OR-linked. The "Combined Mode" can be used to create an AND link. For each bit, you can specify whether ...

- the input bit must be set (displaying "1"),
- the input bit must be deleted (displaying "0"),
- the state of the input bit should be ignored (displaying "X").

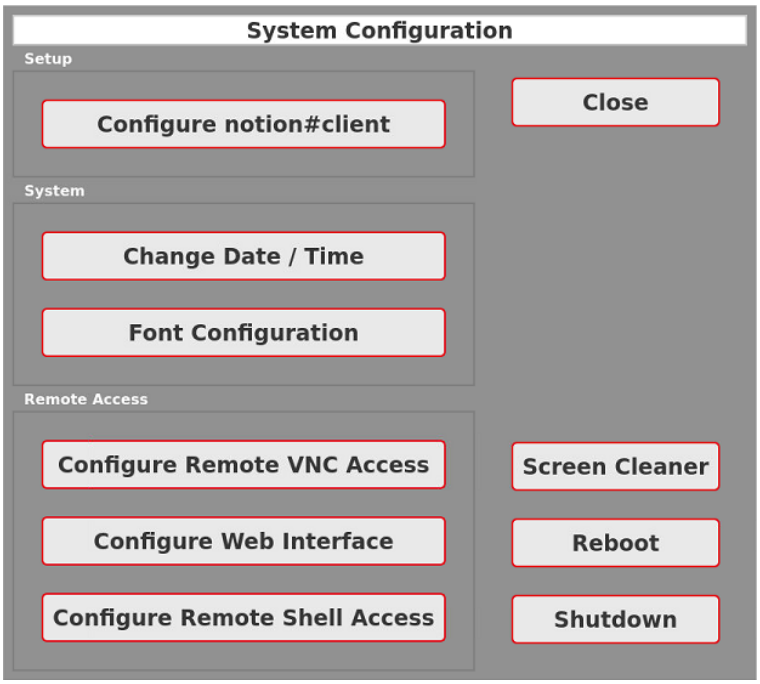
More details on how this works can be found in the chapter on Daisy-Chain-IO.

TRsystems GmbH, Eglishalde 16, 78647 Trossingen, Telefon: +49 (0) 7425 / 228 - 0, Telefax: +49 (0) 7425 / 228 – 34, E-Mail: info(at)trsystems.de

Security prompt when deleting a user

7. System Configuration

The system configuration is the starting point for configuring various aspects of the notion#client.

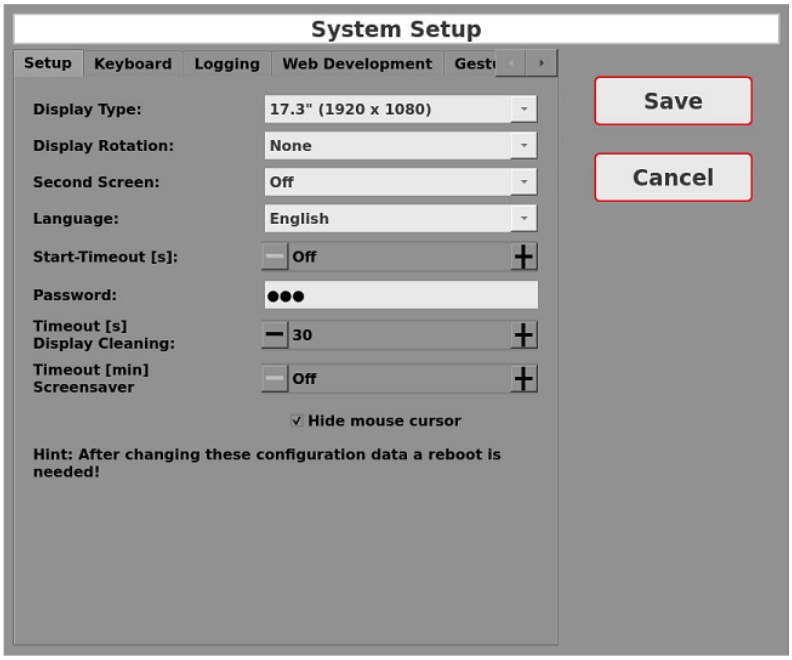


System Configuration

The dialog also offers the option to restart the notion#client (necessary so that various system configuration adjustments can be activated) or to shut it down to switch it off.

7.1. Configuring notion#client

7.1.1 Setup



System Configuration: Setup

The "Display Type" and "Display Rotation" parameters are used to set up the notion#client according to the hardware used and the device installation. Depending on the values set, the layout of the dialogs is also adapted to the circumstances.

The "Second Screen" provides an option to mirror the content of the main screen on a second screen. The prerequisite for this is that the CPU board used supports a second screen and that both screens have an identical resolution. Different resolutions may result in a distorted display.

The "Language" option can be used to switch between German and English texts.

The "Start-Timeout" specifies the delay (in seconds) with which the last selected connection is to be restored after starting the notion#client. This function can be deactivated. The notion#client then shows the start screen and waits for user input.

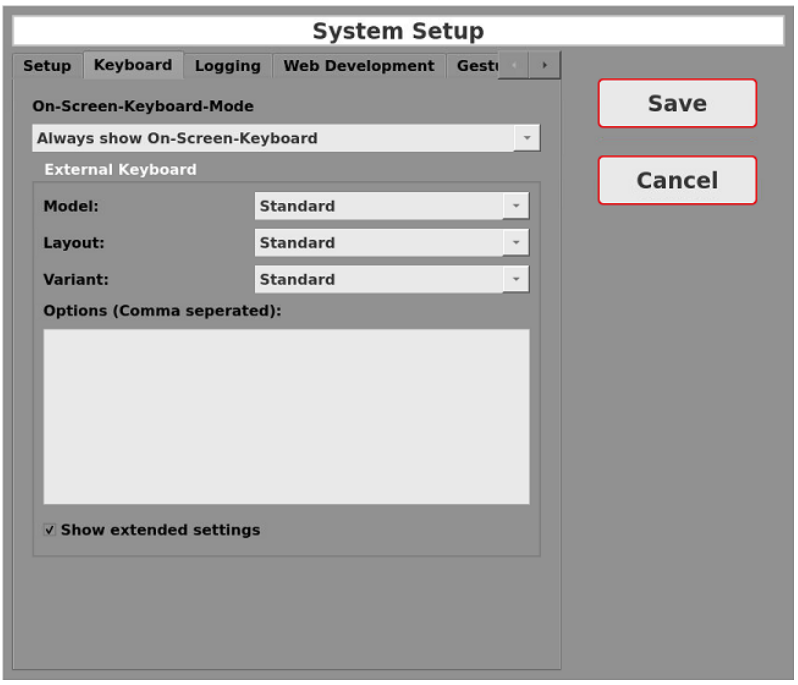
The "Password" option can be used to set a password that must be entered when switching to the configuration view. If this option is set, a password prompt appears on the start page after clicking the gear wheel symbol.

The "Timeout Display Cleaning" can be used to specify the period of time (in seconds) after which the screen cleaning view should be hidden. While the view is active, all inputs (mouse / touchscreen / keyboard) are ignored.
The "Timeout Screensaver" option can be used to specify the period of time (in seconds) after which the screen saver should become active if there is no user activity. Depending on the hardware equipment, either the screen backlighting or the entire screen is switched off. The screen is reactivated when user activity resumes. This function can be deactivated.

To hide the mouse pointer, the "Hide mouse cursor" option can be set. If an external mouse is detected at system startup, this has priority and the mouse cursor is displayed regardless of this option.

Note: Many system configuration settings only become active after a system restart.

7.1.2 Keyboard



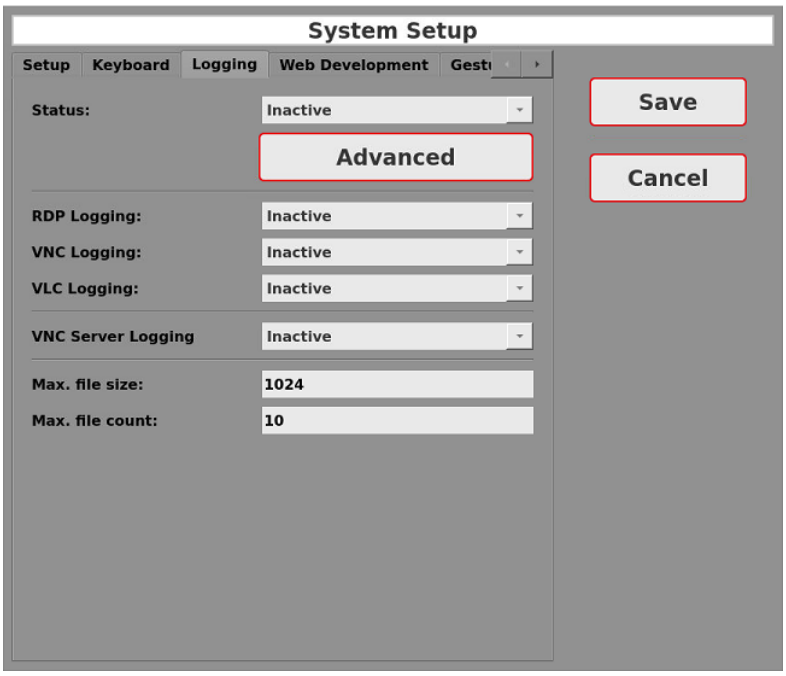
System Configuration: Keyboard

If an external keyboard is to be used instead of the on-screen keyboard, the interaction between the on-screen keyboard and external keyboards can be configured here. The "On-Screen-Keyboard-Mode" parameter offers the following settings for the interaction between the keyboards:

- Always show On-Screen-Keyboard
- Always hide On-Screen-Keyboard
- Only hide On-Screen-Keyboard in viewer

The "Model", 'Layout' and "Variant" parameters can be used to configure the connected external keyboard to work optimally with the notion#client. The "Options" input field also offers further customization options (see https://manpages.debian.org/buster/xkb-data/xkeyboard-config.7.en.html).

7.1.3 Logging



System Configuration: Logging

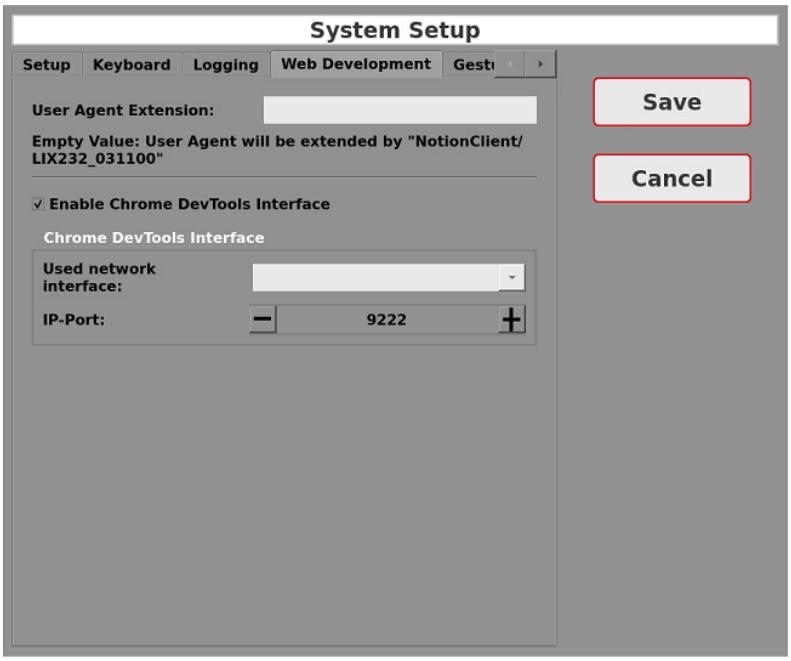
These parameters can be used to control the logging of messages from the application or the components involved. In addition to the filters for which messages are to be logged, the log file rotation can also be set by setting the maximum file size and the maximum number of files.

Note: The logging of messages should only be activated if required. Sometimes a large number of messages are recorded and logged, which may have an impact on the performance of the system and the lifetime of the system storage medium.

TRsystems GmbH, Eglishalde 16, 78647 Trossingen, Telefon: +49 (0) 7425 / 228 - 0, Telefax: +49 (0) 7425 / 228 – 34, E-Mail: info(at)trsystems.de

TRS-DOC_001829-00_20230430

7.1.4 Web Development

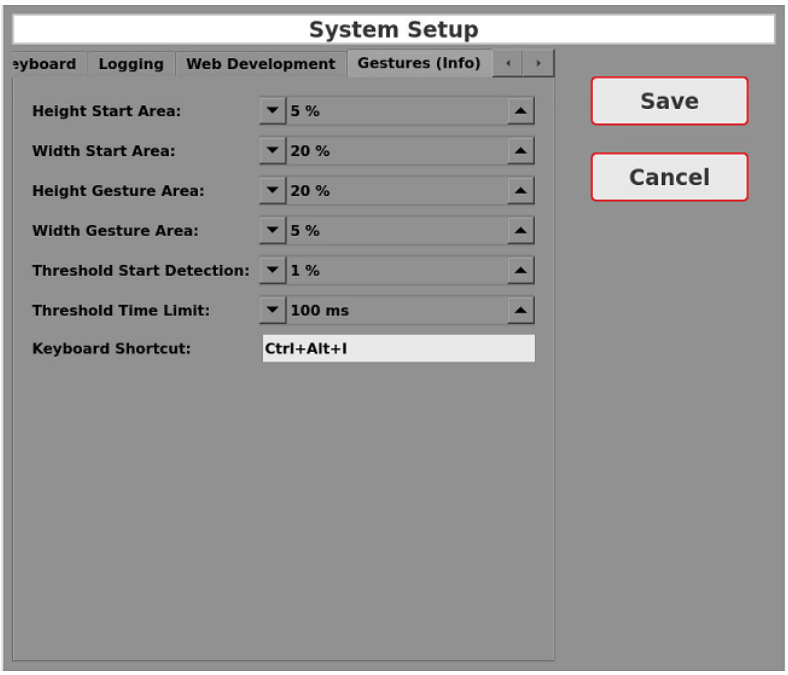


System Configuration: Web Development

This parameter can be used to set the text of the "User Agent" entry in http requests from the web component to a defined value. If no value is entered, the standard text "NotionClient/<VERSION OF APPLICATION>" (e.g. "NotionClient/LIX232_031100") is sent.

For the analysis of web applications, it is possible to activate the "Chrome DevTools Interface" in order to check the behavior of the web application remotely with a Chrome browser (remote debugging). To do this, you can specify which interface should be used for debugging and which port is used for this.

7.1.5 Gestures (Info)



System Configuration: Gestures (Info)

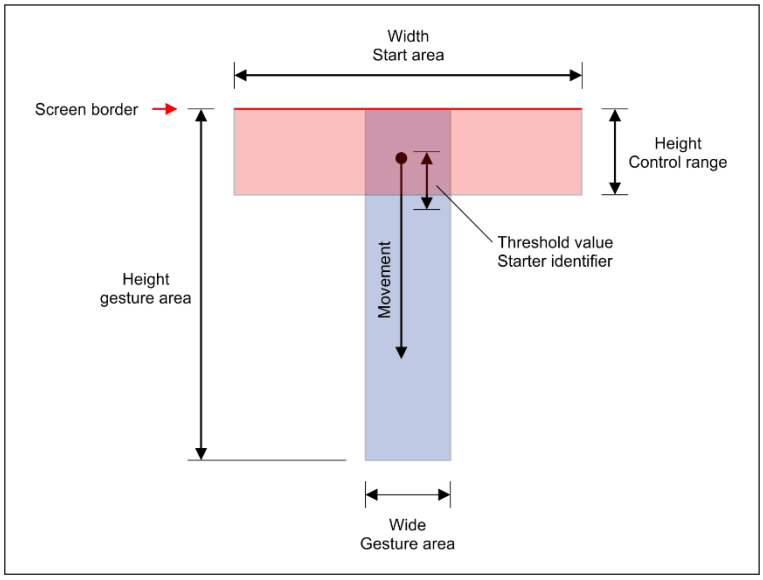
The info gesture is a swipe gesture that starts at the top of the screen and is performed straight down. It is used to show the info view of the viewers. The parameterization of gesture recognition was introduced in order to be able to use different touch models optimally.

The start of the gesture is recognized when the starting point of the gesture is within the start area (see sketch). The start area is defined by the height (as a percentage of the screen height) and the width (as a percentage of the screen width). It is located in the center at the top of the screen.

The gesture speed is evaluated to determine where the gesture applies to (notion#client or the remote system). If the threshold value of the start recognition (as a percentage of the screen height) is reached within the time limit (i.e. fast movement), the gesture is assigned to the notion#client and recognition continues. In the other case (i.e. slow or no movement), the information is forwarded to the remote system.

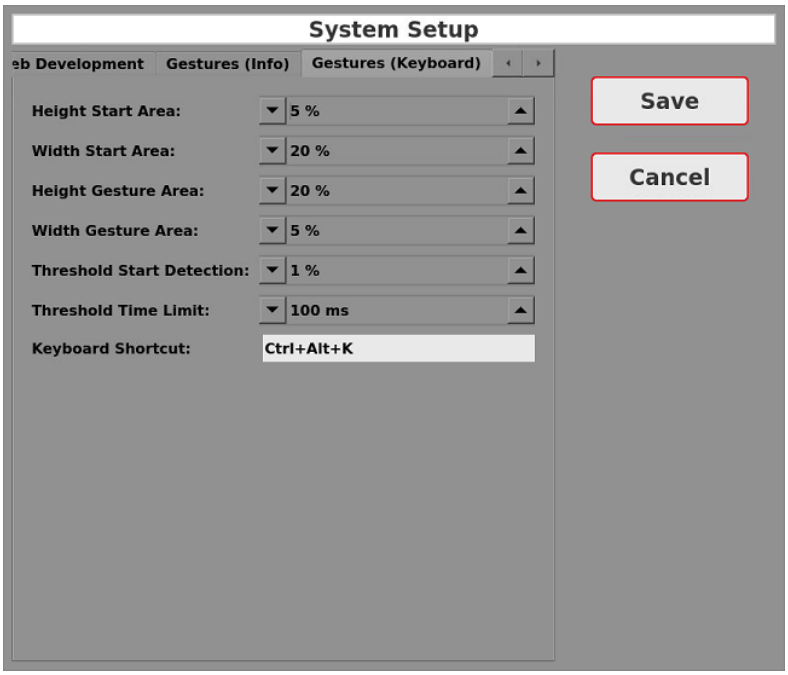
The gesture must then be continued in the gesture area. This is defined by the height specification (as a percentage of the screen height) and the width specification (as a percentage of the screen width). If the gesture area is left to the side - the gesture is executed at too much of an angle - gesture recognition is aborted. If, on the other hand, the gesture area is exited downwards, gesture recognition is successfully completed and the info view is shown.

The shortcut can also be used to show the info view via an external keyboard or a VNC remote session.



System Configuration: Gestures (Info) – Gesture recognition

7.1.6 Gestures (Keyboard)

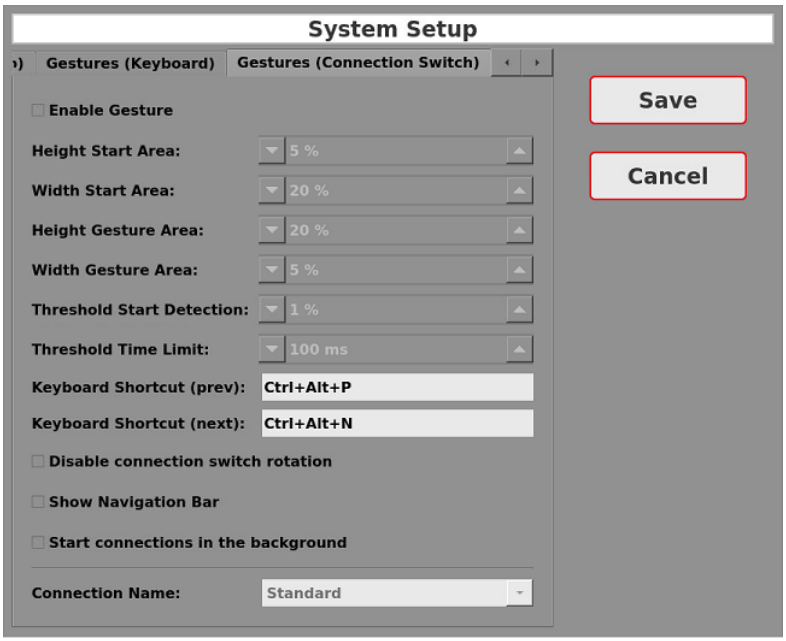


System Configuration: Gestures (Keyboard)

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

In principle, gesture recognition works in the same way as explained above. The only difference is the direction of movement.

7.1.7 Gestures (Connection Switch)



The connection switch gestures are two swipe gestures. The first 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 the connections in the connection view without having to switch back to the connection view. Switching takes place in the order in which the connections are listed in the connection view.

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

The "Enable Gesture" option can be used to activate or deactivate connection switching using a swipe gesture. This option also affects the display of the navigation bar.

Once you have reached the first or last connection of the available connections, the system jumps to the last or first connection. If this rotation through the connections is not desired, this behavior can be switched off with the "Disable connection switch rotation" option.

If required, the navigation bar can be shown or hidden using the "Show Navigation Bar" option.

By default, only the connections that are shown are started. The "Start connections in the background" option can be used to trigger the start of all available connections as soon as the first connection is shown

The following settings are available for displaying the connection name

- Standard

The default setting corresponds to the "Show" setting.

- Show

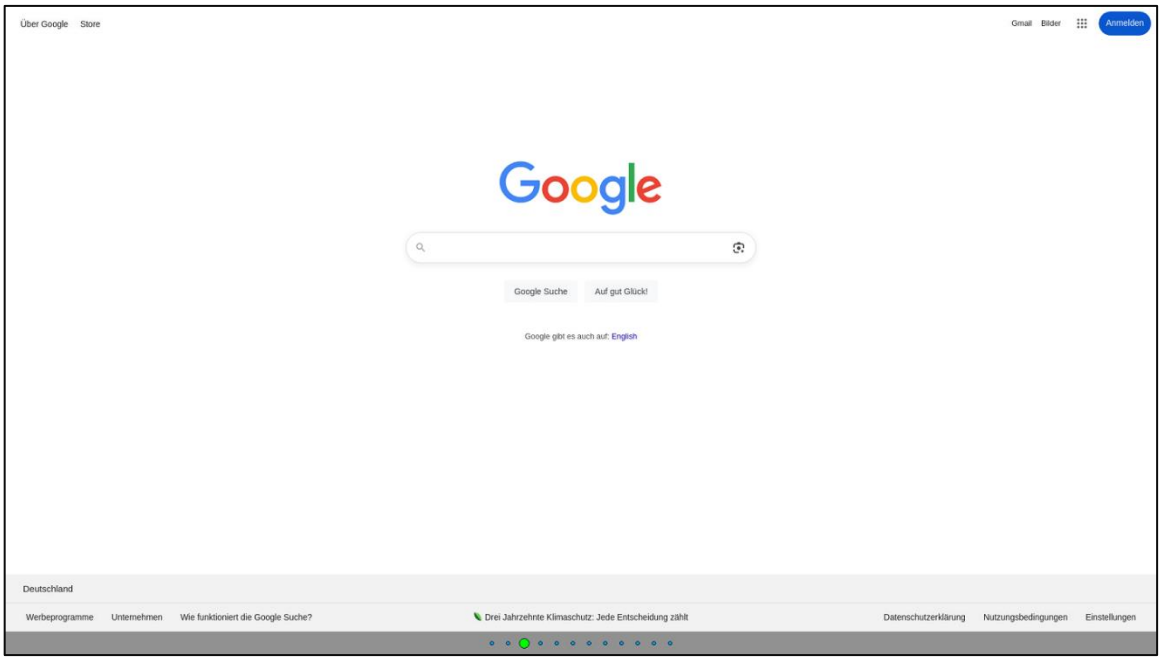
The connection name is permanently shown at the top of the configured display area of the connection

- Hide

The connection name is hidden.

- Overlay (with timeout)

The connection name is shown in the middle of the configured display area of the connection. The display duration can be specified via the separate "Timeout" parameter.

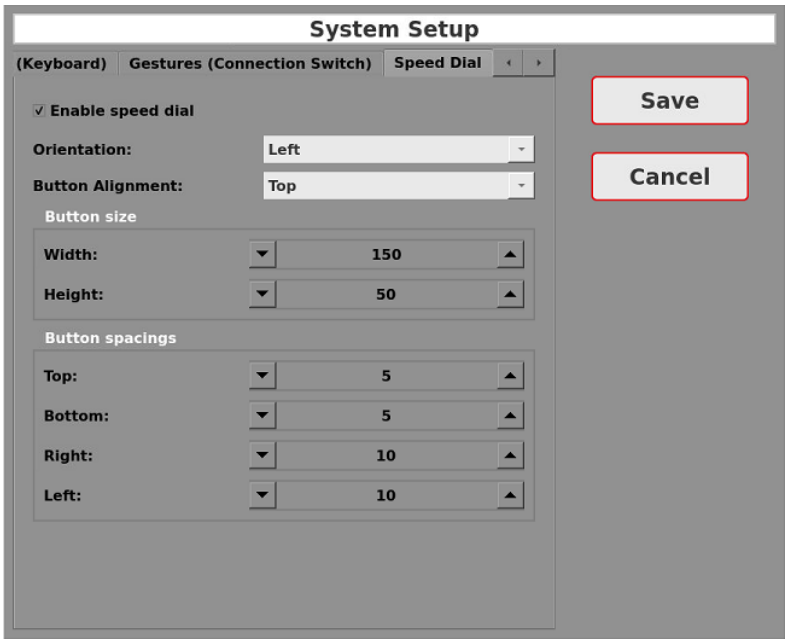


Web Viewer with navigation bar

The navigation bar shows the status of all available connections. The enlarged dot represents the current position within the list. The status of the connection is displayed using a color code:

- Blue: The viewer has not yet been initialized and the connection is not yet active.
- Yellow: The connection is currently being established or terminated.
- Light green: The connection is active.
- Dark green: The connection is on hold (see RDP/RDPApp Multi Client).
- Red: The connection has been disconnected.

7.1.8 Speed dial bar

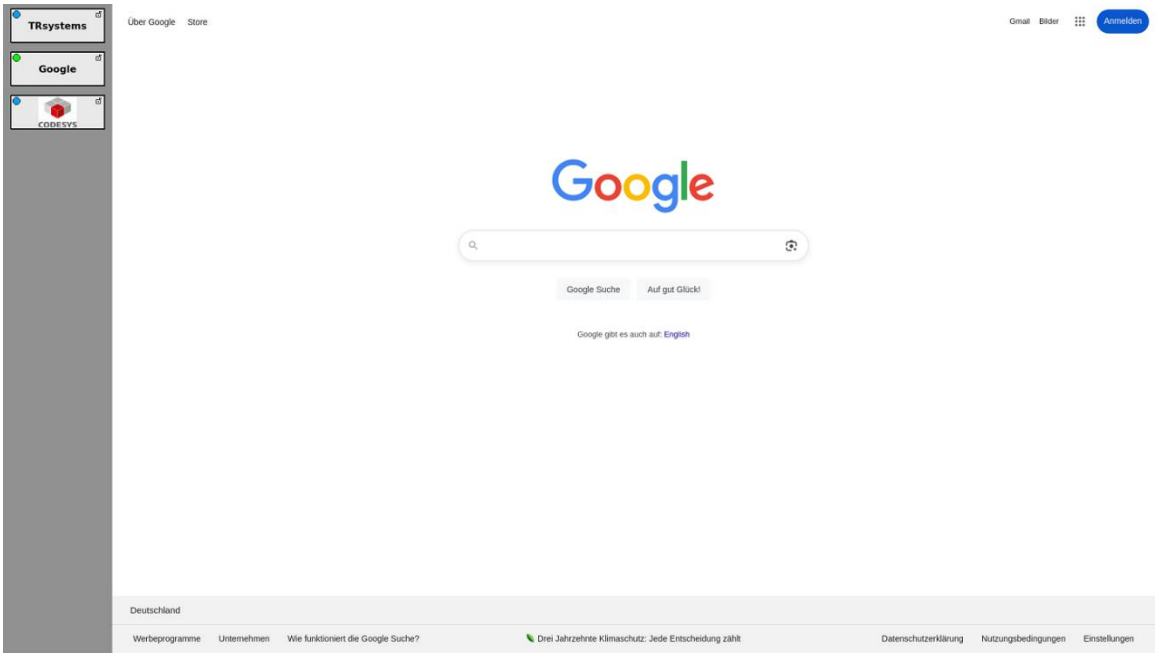


System Configuration: Speed dial bar

The speed dial bar can be activated or deactivated with the "Enable speed dial" option. This setting also affects the configuration of the speed dial bar.

The speed dial bar can be positioned on the left, right, top or bottom edge. The "Orientation" option is used for this purpose. The "Button alignment" option can also be used to specify how the speed dial items should be positioned within the speed dial bar. They can be aligned at the top, bottom or centered if the speed dial bar is positioned on the left or right. If the speed dial bar is positioned at the top or bottom, the speed dial items can be aligned to the left, right or centered.

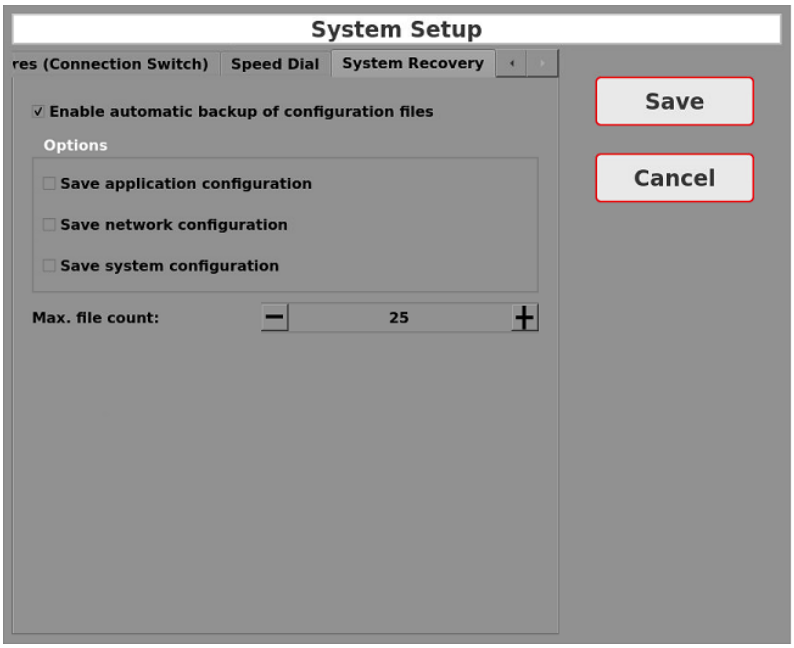
The following options can be used to define the size of the speed dial items and the spacing between them.



Web Viewer with speed dial bar

The speed dial items also provide information on the status of the connection. The color codes used correspond to those used in the navigation bar (see Gestures (Connection Switching)). If the Daisy-Chain-IO-Extension is installed, the access authorization of the active user is also displayed.

7.1.9 System Recovery



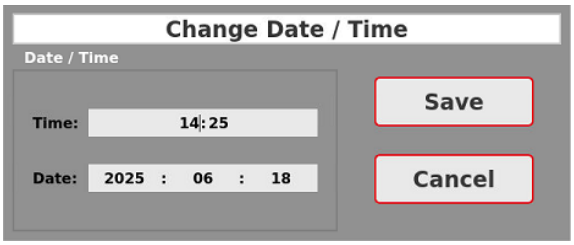
System Configuration: System Recovery

System recovery is primarily an automatic or targeted backup of the configuration data that can be managed in the service area. However, this requires that the "Enable automatic backup of configuration files" option is also activated. This setting also affects the management of backups in the service area. In addition, all required options for backing up the application, network and system configuration must be set.

The "Max. file count" option can be used to specify how many backups should be created. The backup is performed in rotation, so that the oldest backups are removed and the last n backups are retained.

The configuration files are backed up after at least one parameter has been changed and as soon as the configuration level is exited and the start page is accessed again.

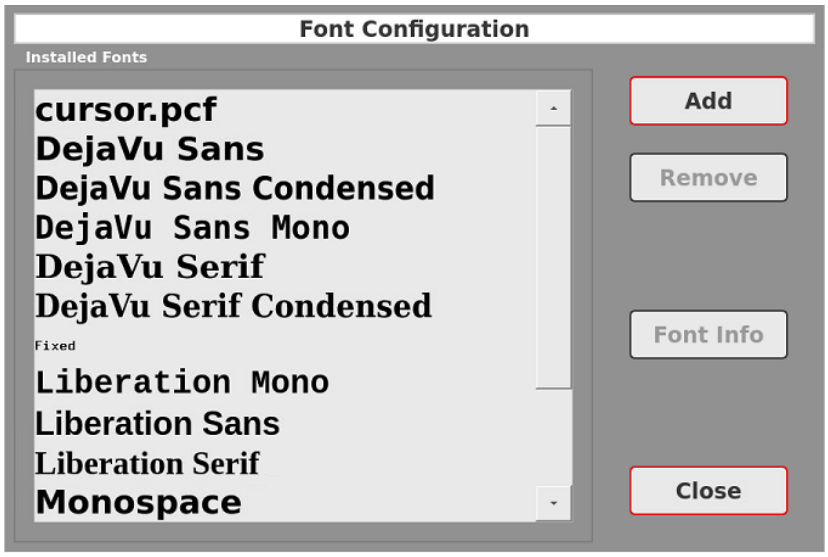
7.2. Change Date / Time



System Configuration: Change Date / Time

The current time and date can be entered via the “Time” and “Date” input fields. Press the Save button to save the entered values.

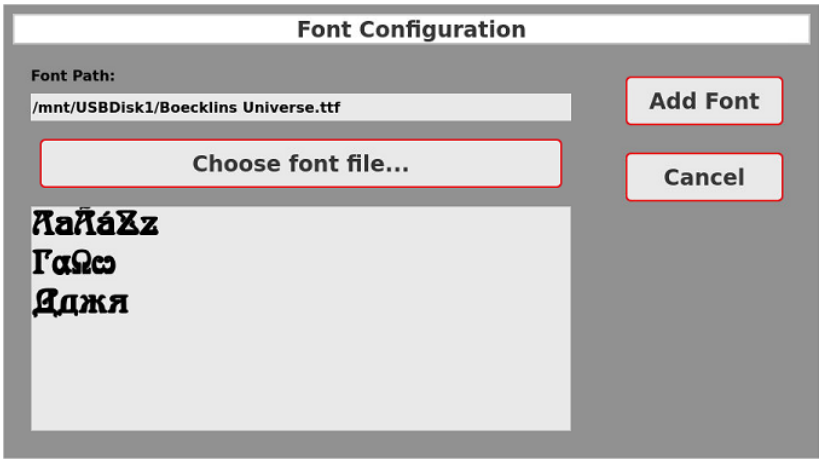
7.3. Font Configuration



System Configuration: Font Configuration

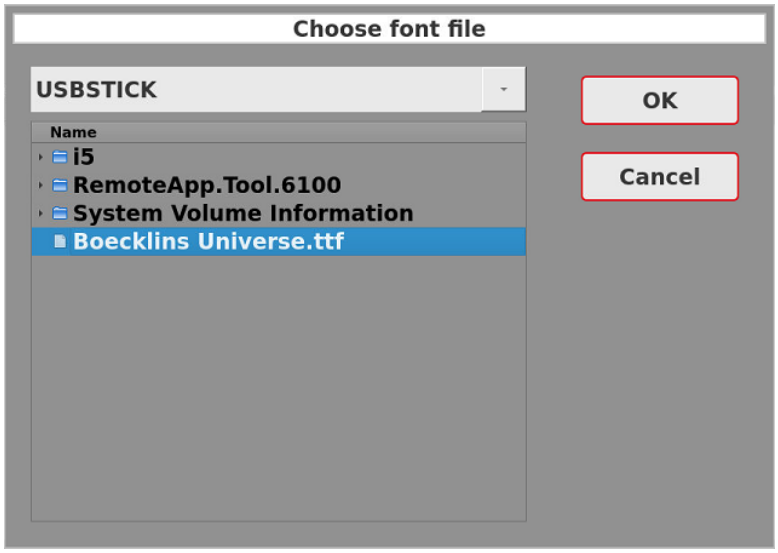
The fonts installed in the system are displayed in this dialog. A distinction must be made here between system fonts and user-installed fonts: only the latter can be uninstalled again. The user-installed fonts are required if a special font is needed on a web page or a web app that is not available in the system fonts or not in the desired quality.

To install a new font, press the "Add" button. User-installed fonts can be deleted again after selection with the "Remove" button. To view the selected font, press the "Font Info" button.

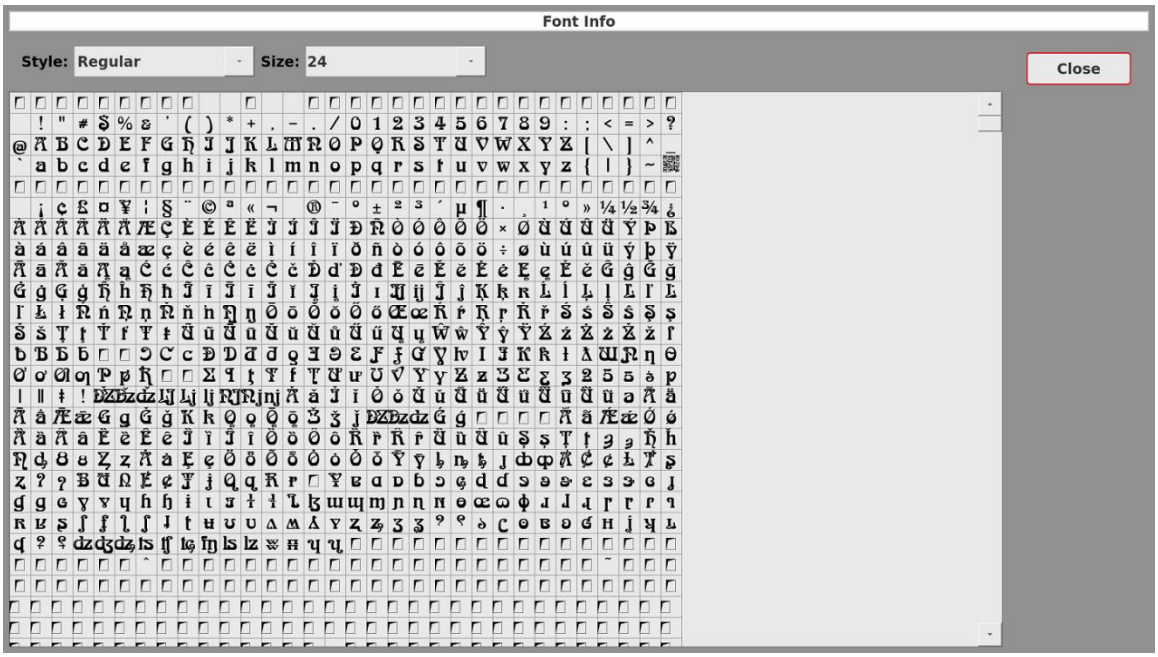


System Configuration: Font Configuration – Add Font

To add a new font, first select the font file, which should be located on an inserted USB stick. After the selection, the path of the file and a small font sample are shown. If the selection is correct, the font can be added.



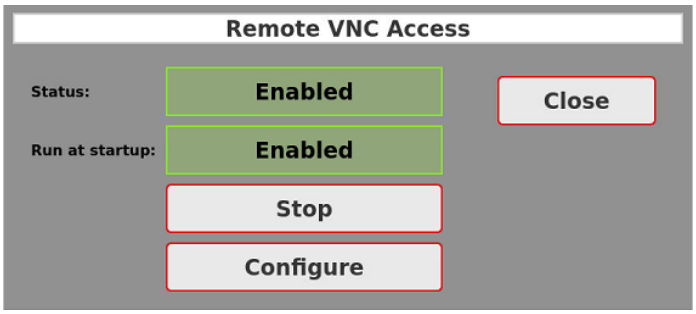
System Configuration: Font Configuration – Add Font



System Configuration: Font Configuration – Font Info

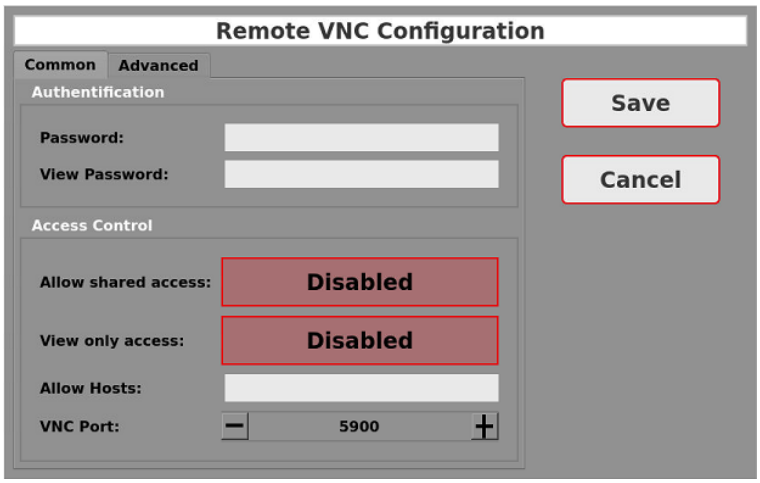
The font info allows you to view all characters of the installed font. The appearance can be adjusted via “Style” and “Size”.

7.4. Configuring Remote VNC Access



System Configuration: Remote VNC Access

The notion#client has a VNC server with which the notion#client can be operated or monitored remotely. The VNC server can be started once or permanently via the configuration dialog.

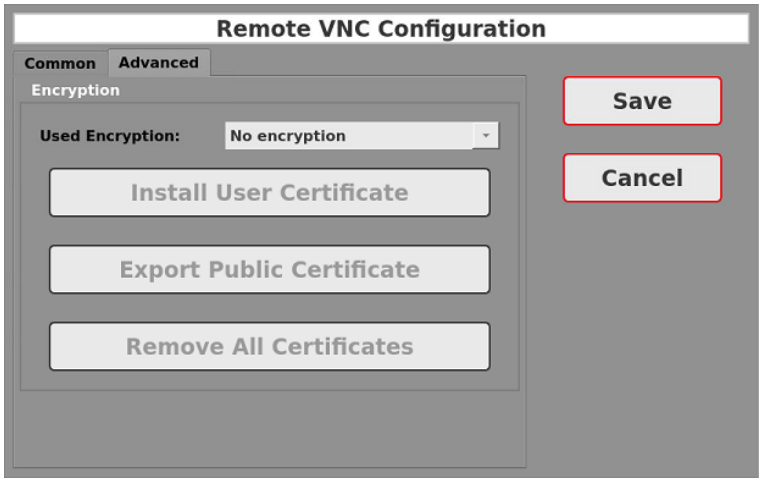


System Configuration: Remote VNC Access - Configuration

Access to the VNC server can be secured with a password and a view-only password. Entering the view-only password takes you to view mode without the possibility of interaction. The “Allow shared access” option is used to control whether one or more connections are permitted. "View only access" is the same as using the view-only password - you are taken to view mode without the option of interaction.

To restrict access to the VNC server, a filter can be specified under “Allow Hosts”. This is a comma-separated list with host names or IP addresses. Subnets can be specified using the notation “172.18.1.”, for example.

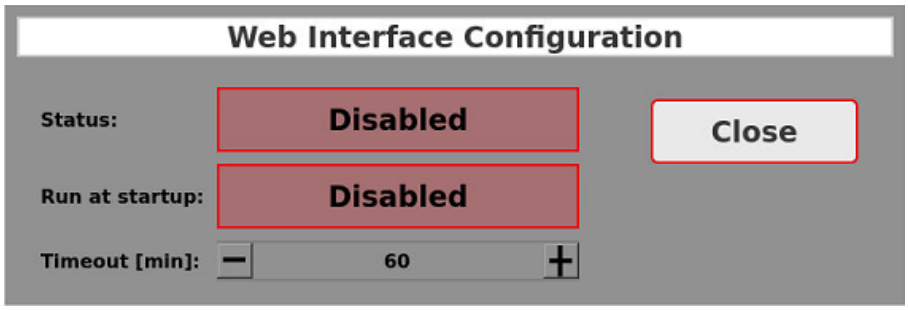
If a VNC port other than the default port is to be used, this can be configured with the “VNC Port” option.



System Configuration: Remote VNC Access - Configuration

Encryption options can be configured in the advanced configuration. However, they only apply in conjunction with libvncclient-based VNC viewers (see the corresponding documentation there).

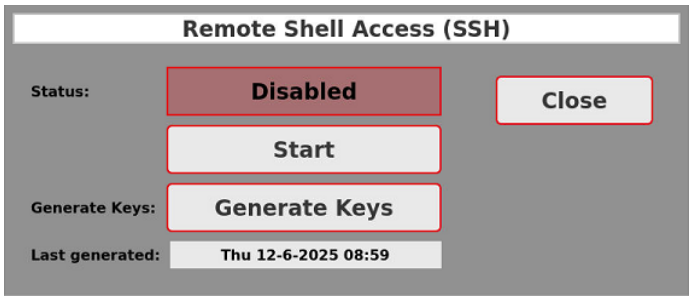
7.5. Configuring the Web Interface



System Configuration: Web Interface Configuration

The web interface can be used to set the system clock, install an update and restart the device. The web interface can be enabled via the "Status" button. The web interface is then disabled again after the time set for "Timeout". The timeout can also be deactivated ("OFF"). If the "Run at startup" button has been enabled, the timeout does not take effect

7.6. Configuring Remote Shell Access



System Configuration: Remote Shell Access (SSH)

The (Linux) console can be accessed for diagnostic purposes. To enable access via SSH, the status must be set to “Enabled”. However, the SSH server requires a set of keys to operate. These can be generated once using the “Generate Keys” button. The SSH server can then be started.

7.7. Screen Cleaner

System Configuration: Screen Cleaner

Screen cleaning can be started in several places: in the system configuration and via the info dialogs of the various viewers. To clean the screen, a window is opened that does not respond to touch, mouse or keyboard inputs. After the configured period of time, the window closes again automatically and the previously visible windows reappear. A timeout counting down is shown in the window.

8. Network Configuration

The various network interfaces are configured in the network configuration if they are available: Ethernet, WLAN and VPN. The status of the network interface is shown in the respective view by LEDs and a text field provides further detailed information. The colors of the LEDs have the following meaning:

- Dark LED

The interface is deactivated or not available.

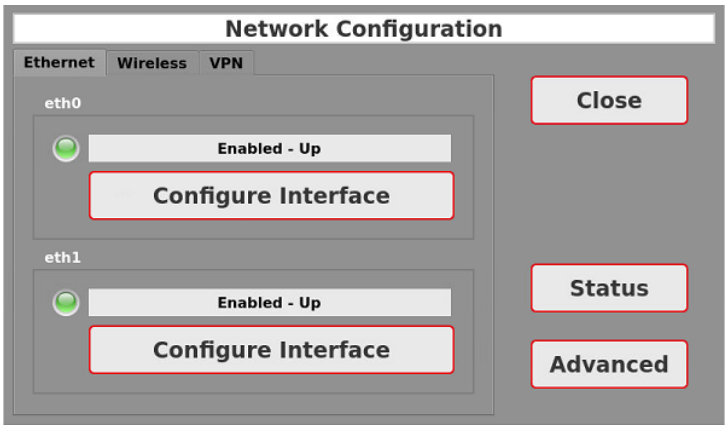
- Yellow LED

The interface is activated, the DHCP request is running, the DHCP request has failed or no network link has been detected.

- Green LED

The interface is active.

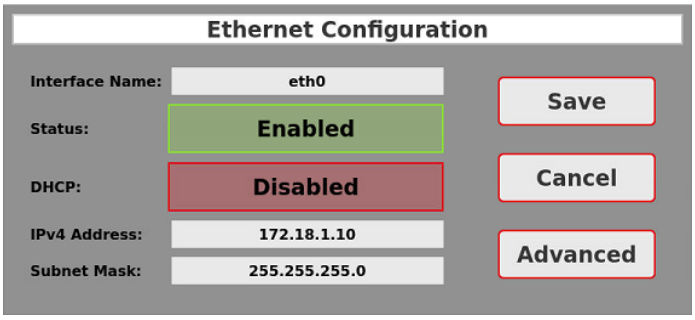
8.1. Ethernet Interface



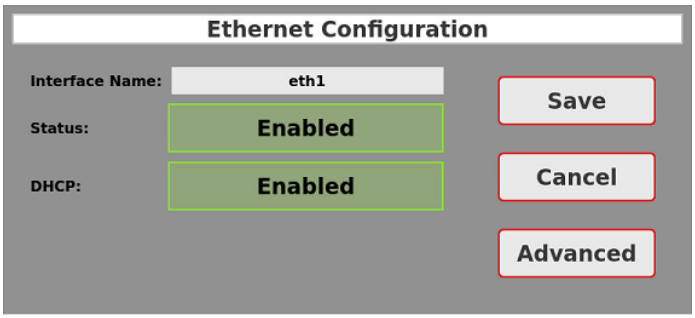
Network Configuration: Ethernet Configuration

Click on "Configure Interface" to open the dialog for configuring the respective interface. There you can enable or disable the interface, set the IPv4 address or enable DHCP.

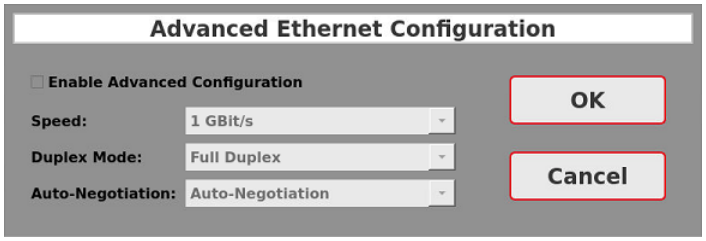
In the extended Ethernet configuration, it is also possible to set additional interface parameters



Network Configuration: Ethernet Configuration (static configuration)

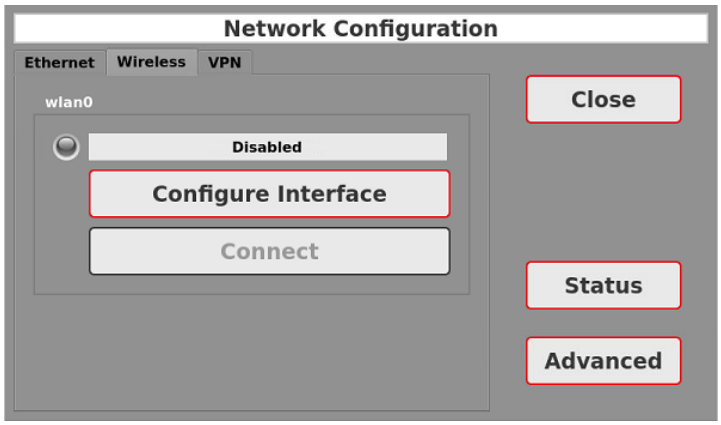


Network Configuration: Ethernet Configuration (DHCP configuration)



Network Configuration: Advanced Ethernet Configuration

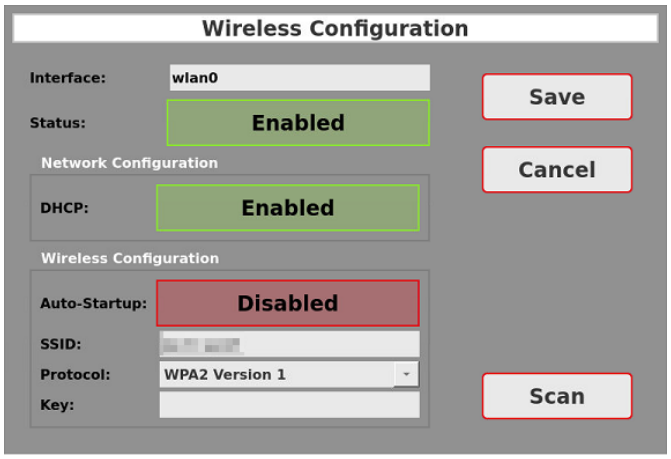
8.2. Configuring WLAN



Network Configuration: WLAN Configuration

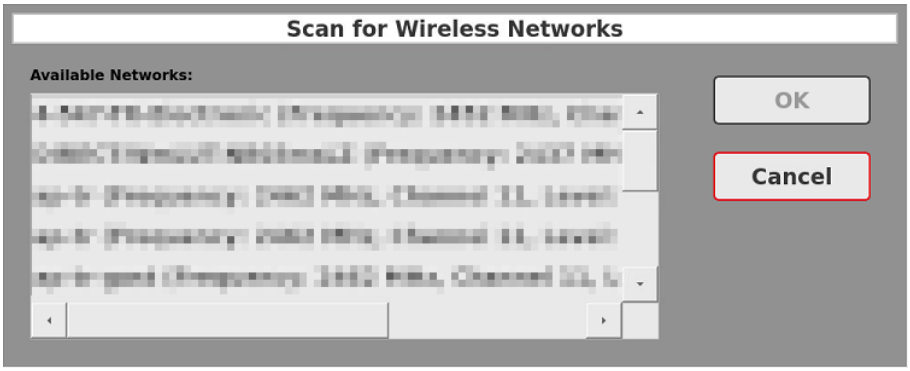
Click on "Configure Interface" to open the dialog for configuring the WLAN interface. Configuration is possible if an inserted and supported WLAN USB stick has been detected.

If the interface has already been configured, the connection can be established manually by clicking on "Connect" and disconnected again by clicking on "Disconnect".



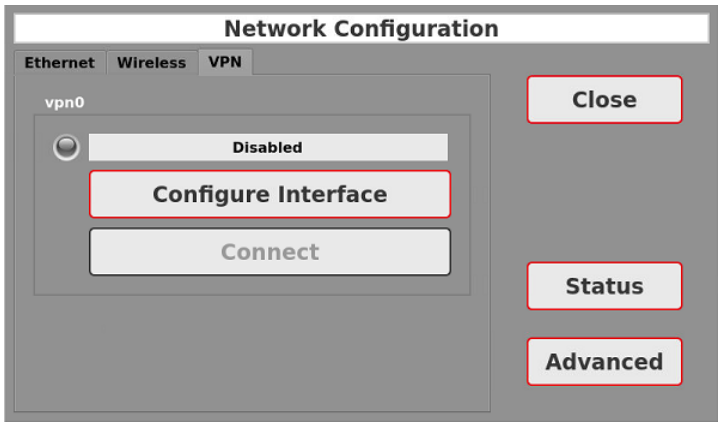
Network Configuraation: WLAN Configuration (Interface Configuration)

The interface can be configured in this dialog. It can be enabled or disabled, the network configuration can be set (static or DHCP) and the WLAN configuration can be entered. To determine the SSID, the network scanner can be started, which displays all available SSIDs for selection.



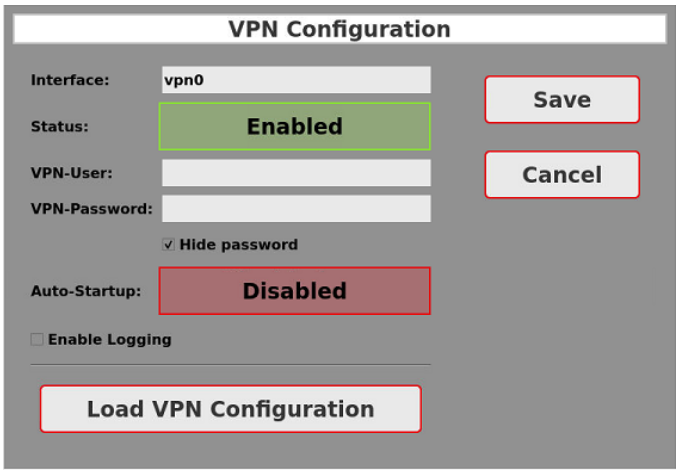
Network Configuration: WLAN Configuration (WLAN Scan)

8.3. Configuring VPN



Network Configuration: VPN Configuration

Click on "Configure Interface" to open the dialog for configuring the VPN interface. Once the interface is configured, the connection can be established manually by clicking on "Connect" and disconnected again by clicking on "Disconnect".

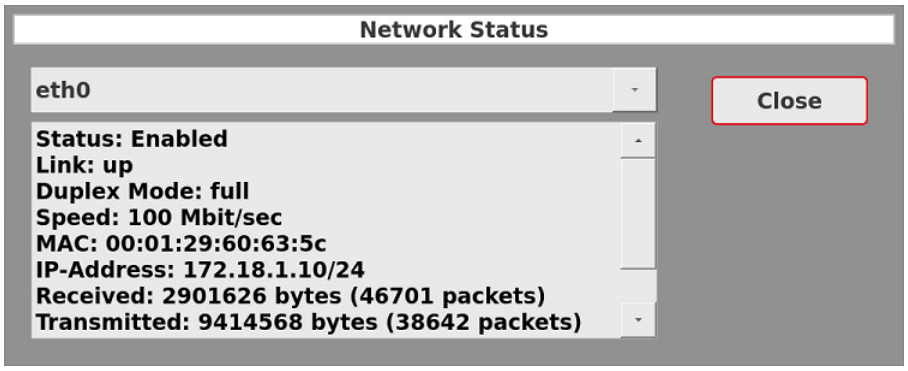


Network Configuration: VPN Configuration (Interface Configuration)

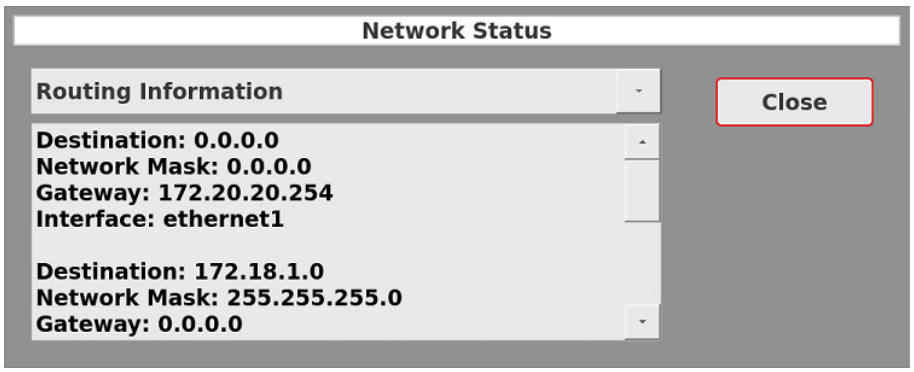
The interface can be configured in this dialog. It can be enabled or disabled and the VPN user and VPN password can be entered. An OpenVPN-compliant configuration file for the connection configuration can be loaded via "Load VPN configuration".

8.4. Network Status

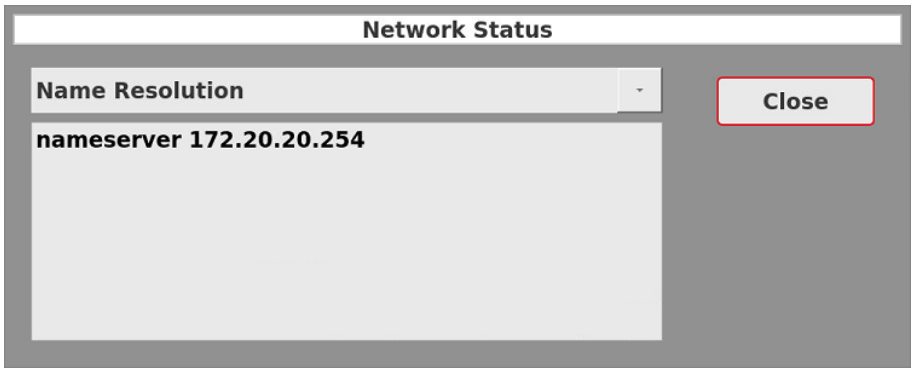
The network status provides detailed information on the individual interfaces and general network information (routing, name resolution).



Network Configuration: Network Status (Information on the interface)

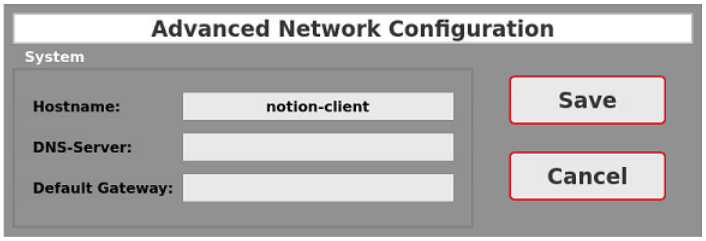


Network Configuration: Network Status (Routing Information)



Network Configuration: Network Status (Name Resolution)

8.5. Advanced Configuration



Network Configuration: Advanced Network Configuration

The advanced network configuration offers the option of setting additional static network parameters if these have not already been determined using DHCP (see Network Status).

9. Service

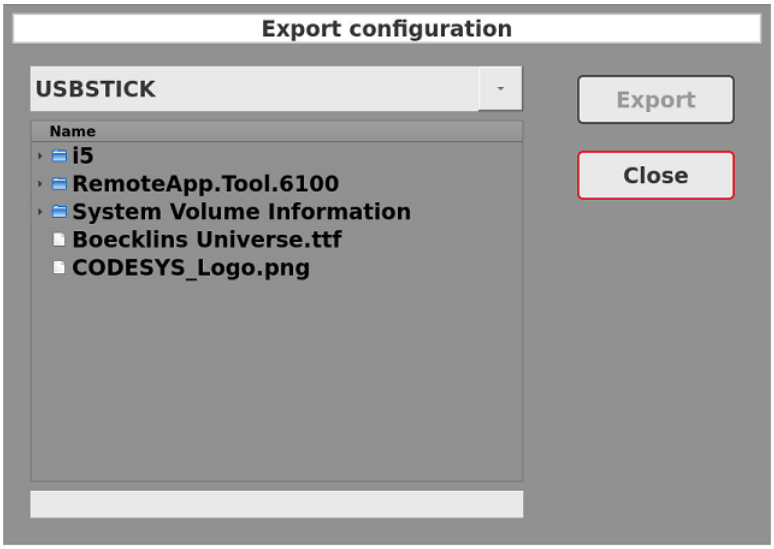
The service area offers a range of functions for system care and maintenance. The configuration can be exported and imported, system logging files can be exported or cleaned up, the local update can be started, configuration data can be backed up and restored, the touchscreen function can be checked and fine-tuned and, if the Daisy-Chain-IO-Extension is installed, its function can be checked in conjunction with the PLC.

9.1. Import / Export

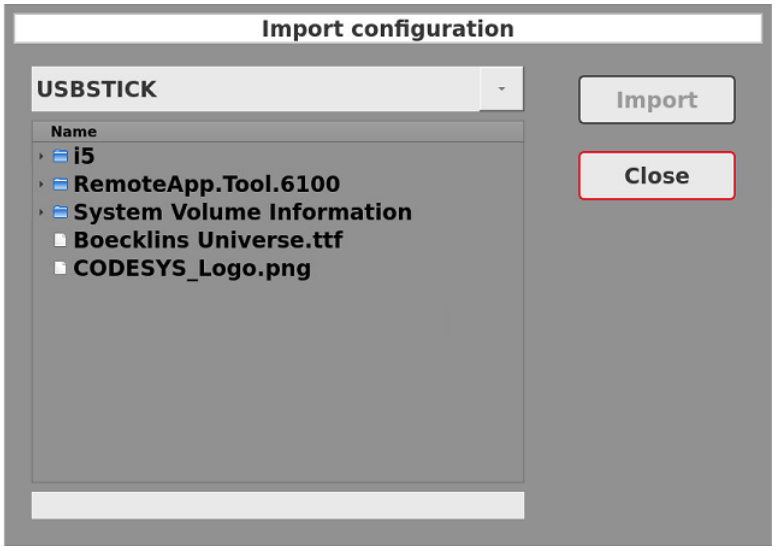
Service: Configuration Import / Export

When exporting the configuration, you must first select which parts of the configuration are to be exported: Application configuration, network configuration or system configuration. Then, after clicking the "Export configuration" button, the export file on the USB stick can be selected or the name of an export file can be entered.

When importing, after clicking on "Import configuration", an import file can be selected on the USB stick, which is then imported in full

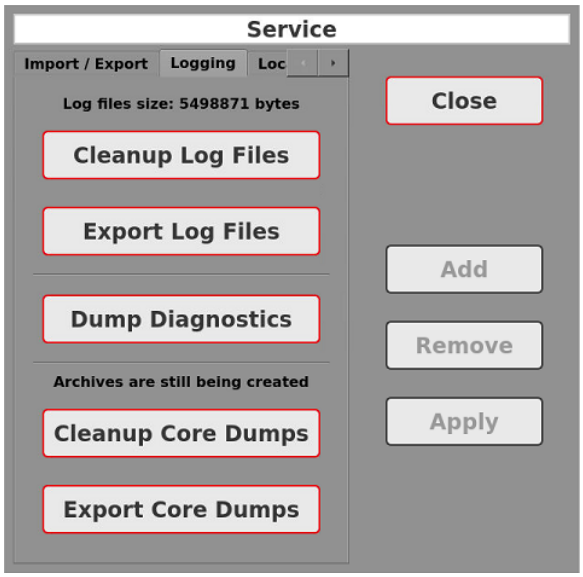


Service: Import / Export – Export Configuration



Service: Import / Export – Import Configuration

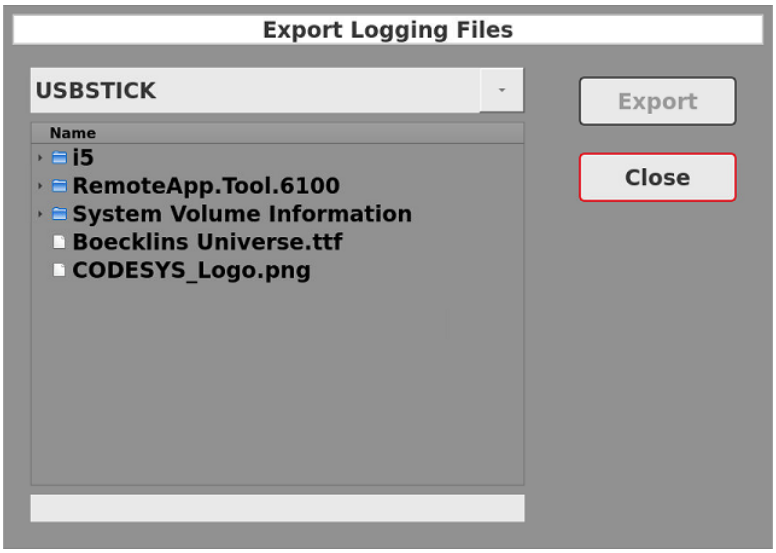
9.2. Logging



Service: Logging

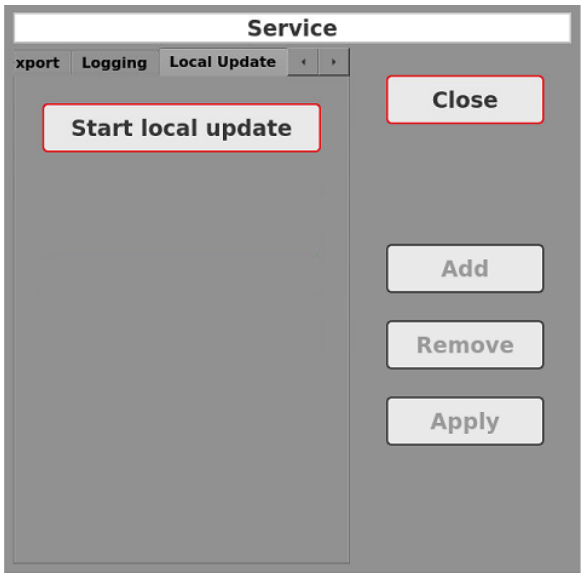
With "Export Log Files", the collected log data can be exported in an archive to a USB stick. "Dump Diagnostics" saves internal diagnostic data in a file in the log directory, which can be exported via the log file export. "Cleanup Log Files" cleans up the entire log directory.

Core dumps are created if the notion#client application is terminated unexpectedly. They are used to analyze the causes. They can be transferred to a USB stick with "Export Core Dumps". All core dumps are deleted with "Cleanup Core Dumps".



Service: Logging – Export Logging Files

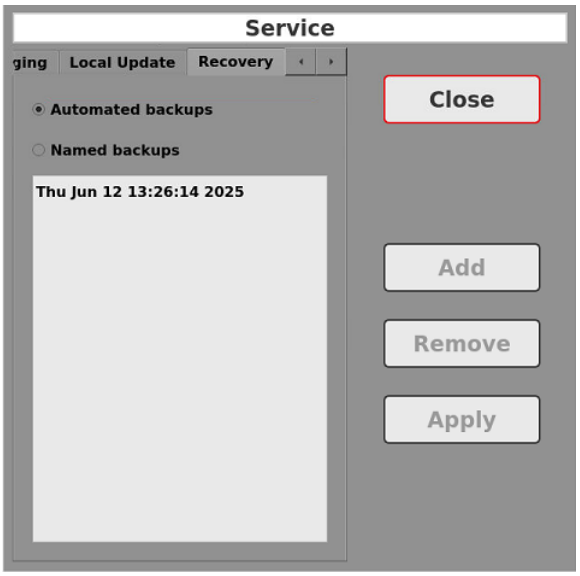
9.3. Local Update



Service: Local Update

Click on “Start local update” to close the notion#client application and switch to the update application. There, an update package can be uploaded via USB and the system update can be started. Further information can be found in the System Update section.

9.4. System Recovery

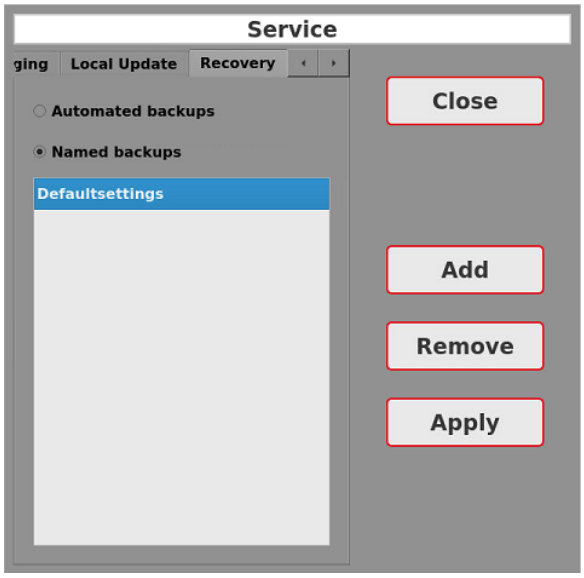


Service: System Recovery

If the "Automated backups" selection is active, a list of the most recent backups of the configuration files is displayed here. Whether and what is backed up depends on the configuration (see System configuration). To restore an older version, it only needs to be selected and can then be reactivated with "Apply".

The second selection "Named backups" is a special case here. As a user, you can back up and restore the configuration files under a specific name at any time. The same data is backed up as with the automatic backup, but there is no limit to the number. Named backups can be overwritten and also deleted.

Service: System Recovery – Named backup



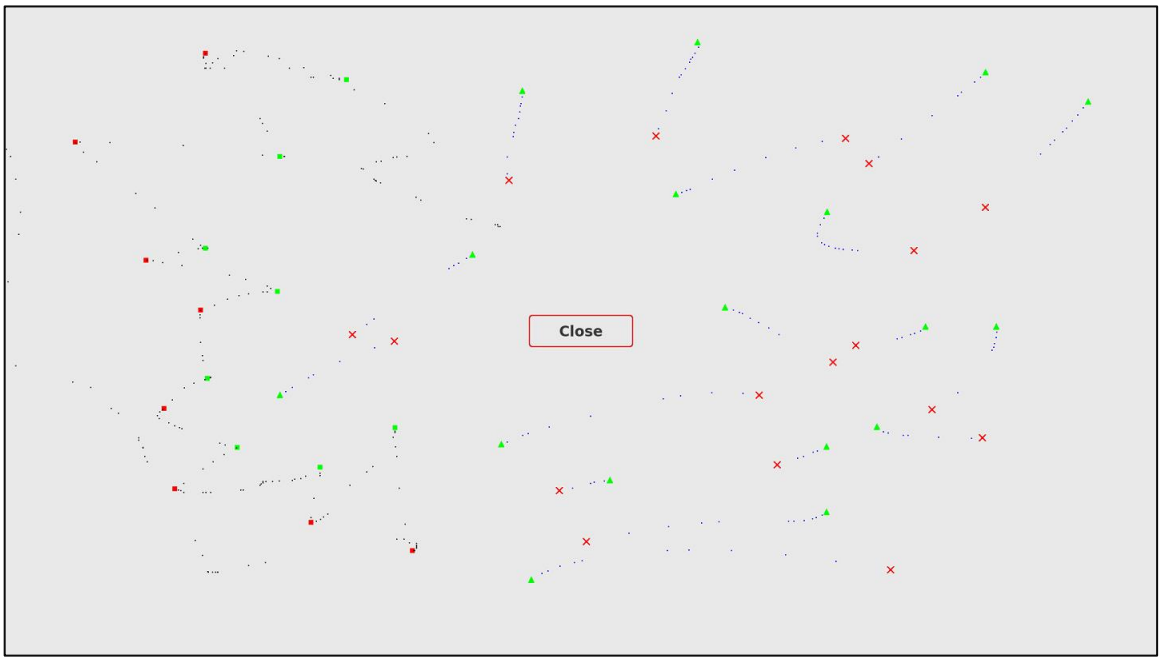
Service: System Recovery – Named backup

9.5. Touchscreen

Service: Touchscreen

Here you will find tools for analyzing the touchscreen function, fine-tuning the touchscreen and analyzing gesture recognition.

9.5.1 Touchscreen Analysis



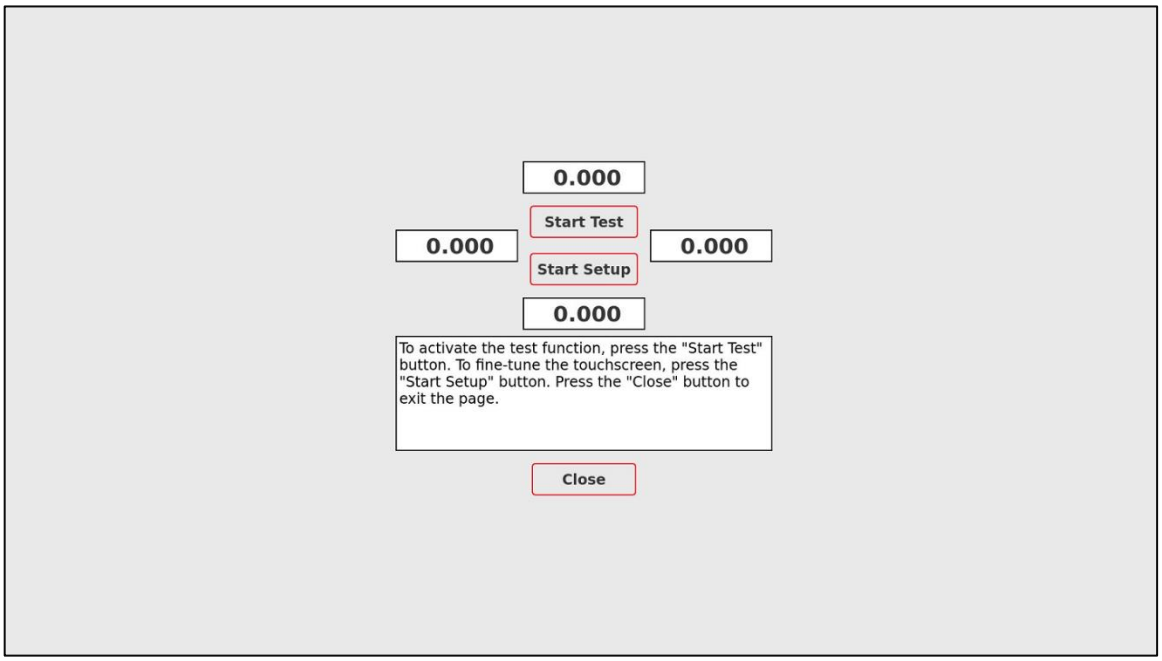
Service: Touchscreen – Touchscreen Analysis

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 received position data 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.

9.5.2 Touchscreen Test / Setup



Service: Touchscreen – Touchscreen Setup

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 again 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 shown to indicate the swipe direction. Swipe from outside the screen 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 shown.

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.

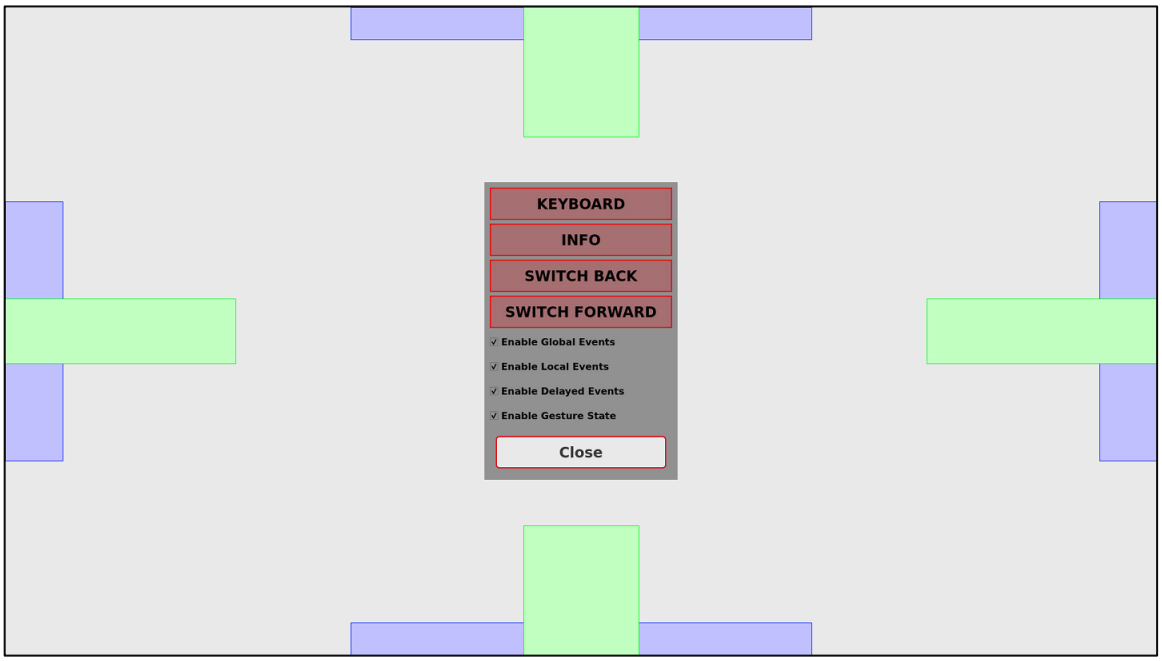
Performing the fine adjustment
Fine adjustment is started by pressing the "Start Setup" button. First, the fine adjustment of the touchscreen is reset to the default values. The procedure is then similar to the test. In contrast to the test, the fine adjustment of the touchscreen is adjusted after each swipe. If the corresponding numerical value is outside the tolerance (red coloring), a new swipe is necessary to further refine the corrected fine adjustment. This process is repeated until the number field is colored green. You can then switch 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

9.5.3 Gesture Analysis



Service: Touchscreen – Gesture Analysis

With the gesture analysis, a possibility has been created to check the gesture parameterization (see system configuration).

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 switch 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 four checkboxes can be used to limit the displayed events to the activated elements.

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 aborted.

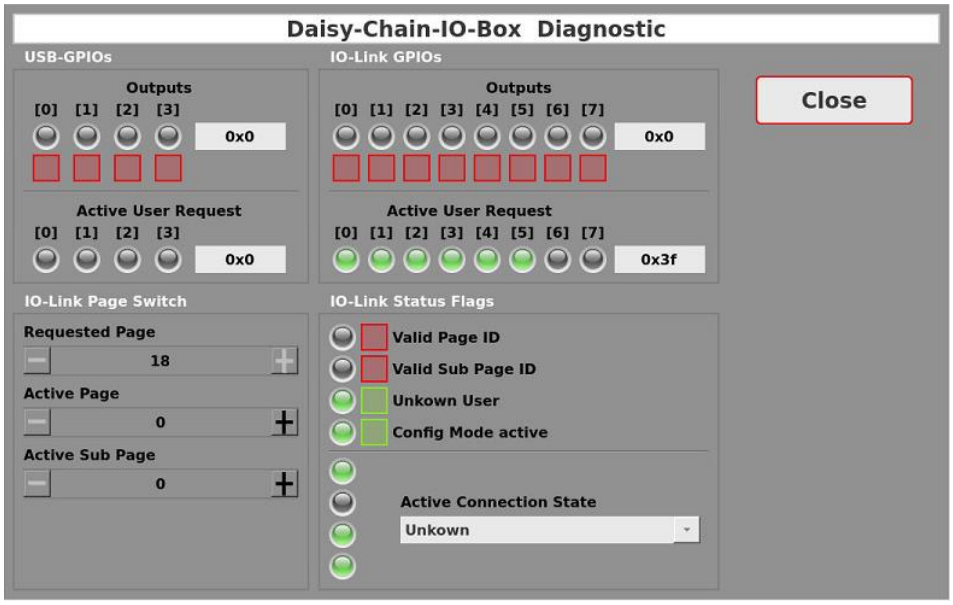
- Touch Start: red square
- Touch Move: small red dot
- Touch End red square

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-colored cross
- Gesture Canceled: magenta-colored square with red filling
- Gesture Timeout: magenta-colored square with yellow filling

9.6. Daisy Chain IO

Setup: Daisy Chain IO



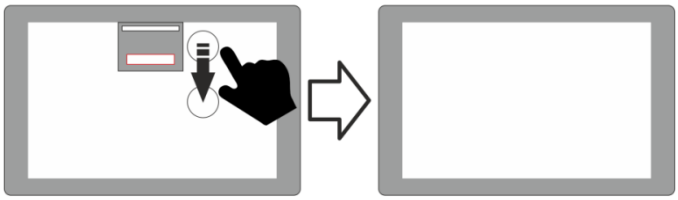
Setup: Daisy Chain IO - Diagnostic

This diagnostic page can be used to test the communication between the notion#client and a PLC via GPIO or IOLink. The Daisy-Chain-IO-Extension (with or without IOLink) is required for this. The various signals are grouped according to their function: USB GPIOs, IOLink GPIOs, IOLink Page Switch and IOLink Status Flags.

When the diagnostics page is shown, the current status as provided by the application is used. Changes to the output signals are only valid as long as the diagnostics page is shown. After leaving the diagnostics page, the previous state is restored.

10. Viewer

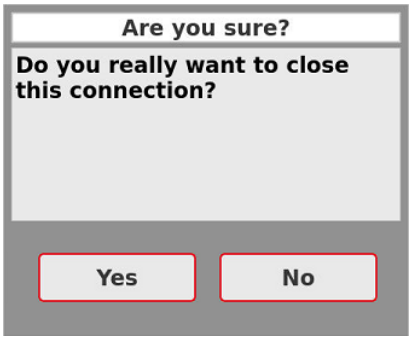
Each viewer has an info dialog. It differs slightly depending on the viewer. The dialog is shown by a swipe gesture from the middle of the area above the screen downwards into the screen. The distance covered when dragging should be at least 20% of the screen height. The dialog appears after the gesture has been successfully performed.



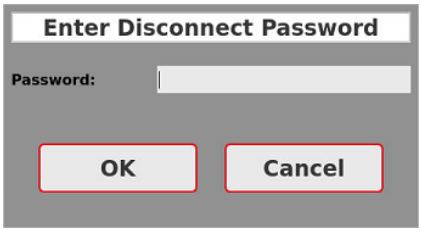
Showing the info dialog

Like the keyboard, the dialog can be positioned anywhere on the screen. To do this, touch the drag bar (the white field) with your finger and move the dialog as required. If you move the dialog out of the screen, it is hidden.

When the connection is disconnected, one of the following dialogs is displayed depending on the configuration (password for disconnection set or not)

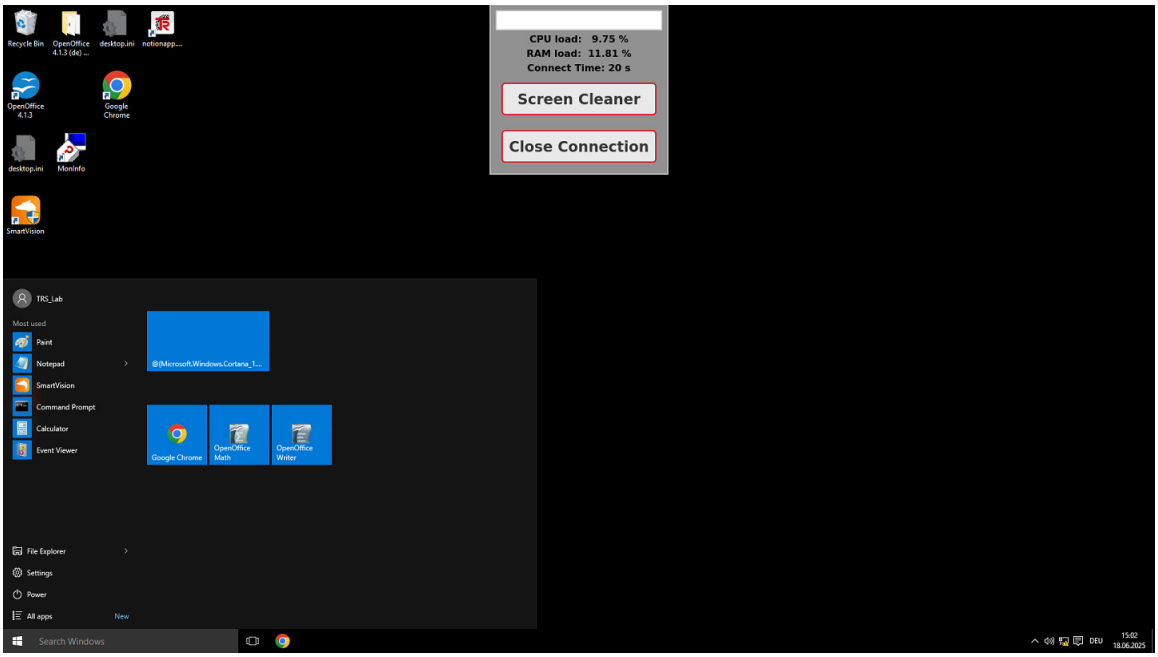


Query when disconnecting without password set



Query when disconnecting with password set

10.1. VNC Viewer

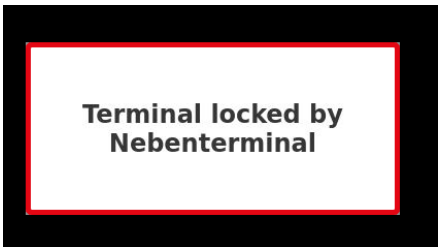


VNC viewer with active info dialog

The info dialog provides information about the current CPU and RAM usage and shows the current connection time. The user has the option of starting screen cleaning or closing the connection and switching back to the start page.

10.1.1 Daisy-Chain

The daisy chain function, as we provide it for the VNC viewer, is intended to prevent shared operation of the host system by blocking all notion#clients for which the daisy chain function has been activated, which use the same group name and are located in the same network segment, from user input as soon as the first operator starts inputting.



Display for a locked notion#client

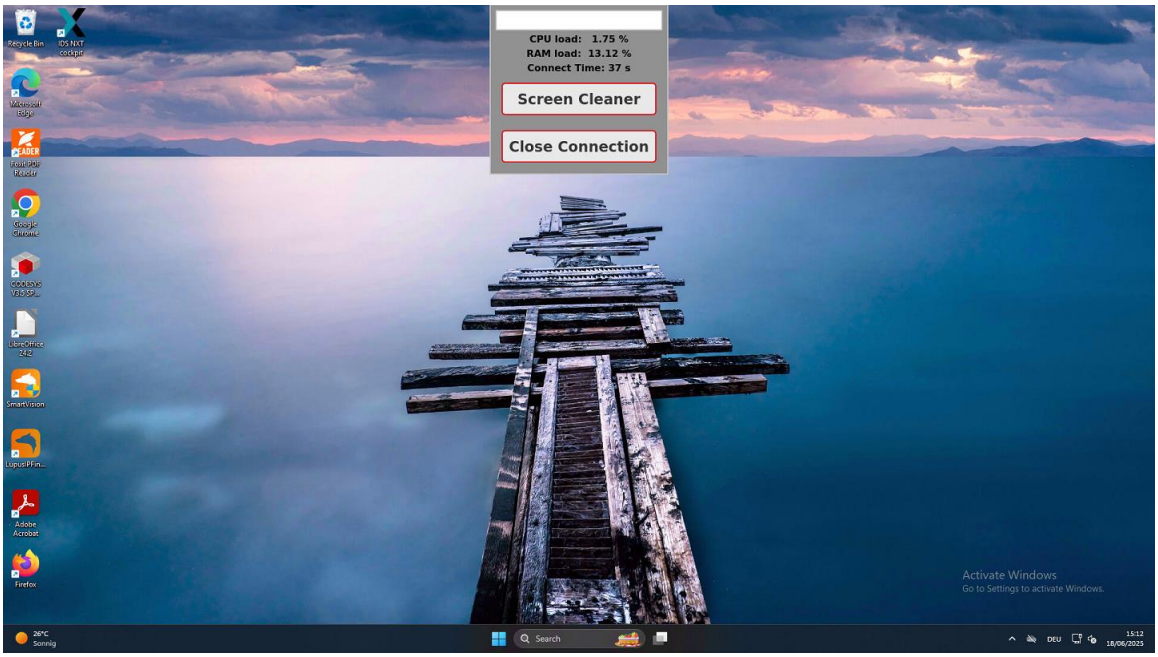
Input from the blocked notion#client is blocked for the duration of the input period in accordance with the set blocking time. Only after this period of time another user can start making inputs. The host name of the notion#client that triggered the blocking of the other notion#client is also shown in the display.

10.1.2 Daisy-Chain-IO

Daisy-Chain-IO extends Daisy-Chain by setting an output in the GPIO or IO-Link area. The time period for which the output should be set can be set for each connection.

Daisy-Chain and Daisy-Chain-IO can be used independently of each other.

10.2. RDP Viewer



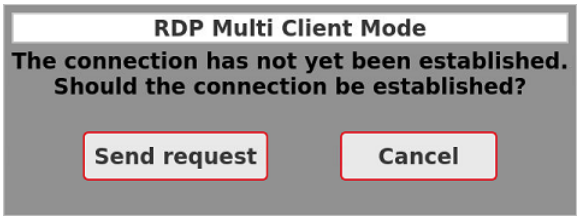
RDP viewer with active info dialog

The info dialog provides information about the current CPU and RAM usage and shows the current connection duration. The user has the option of activating screen cleaning or terminating the connection and switching back to the start page.

10.2.1 Multi-Client

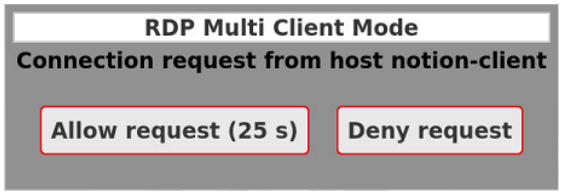
The RDP multi-client function is available for both RDP and RDPApp connections. The prerequisite for this is an activated multi-client function and the use of shared RDP hosts to be accessed. All RDP / RDPApp clients must also be connected and accessible via the network.

If the "Connect at startup" option has not been activated, no connection is initially established and the dialog for requesting a connection is shown instead. If this option is activated, an attempt is made to establish the connection. If another RDP / RDPApp client already has an active connection to the host, the connection request dialog is also shown in this case.



RDP Multi Client: Request to establish a connection

If a RDP / RDPApp client sends a request to establish a connection and no other RDP / RDPApp client has an active connection to the host, the connection is established directly. Otherwise, the request is sent to the active RDP / RDPApp client, which displays the dialog for releasing the connection. If the request is answered positively or not answered within the timeout, the active RDP / RDPApp client terminates its connection and the connection is established with the requesting RDP / RDPApp client. However, if the request is rejected, the requesting RDP / RDPApp client receives a negative response and shows the dialog for rejecting a connection request.

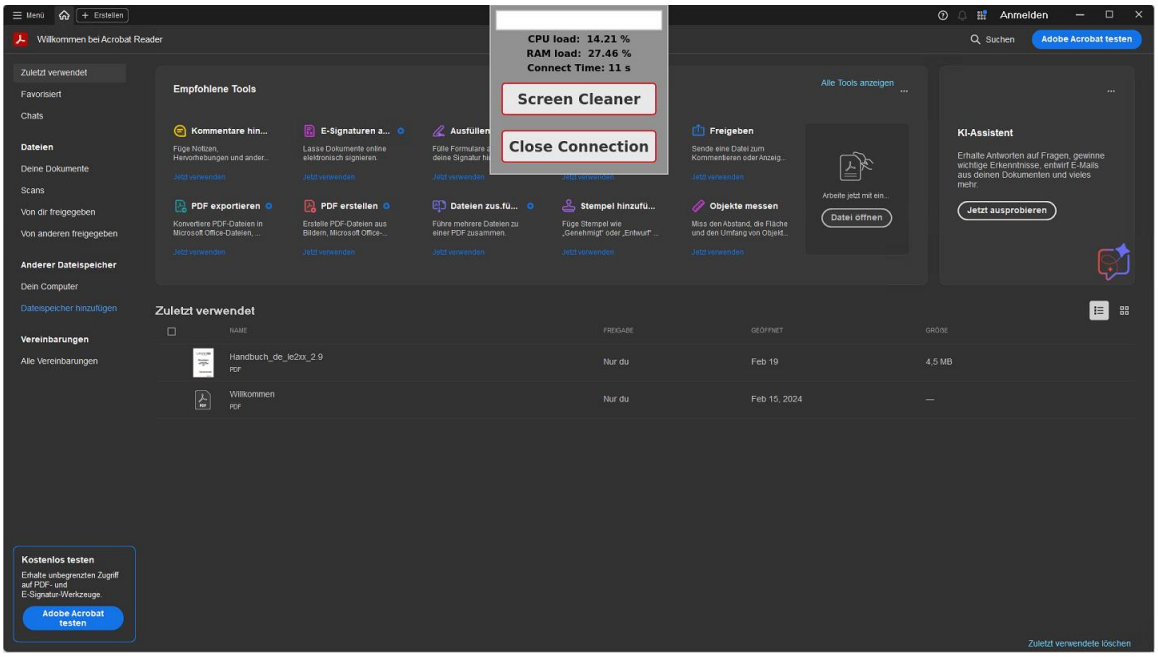


RDP Multi Client: Request to release a connection

RDP Multi Client: Rejection of a connection request

TRsystems GmbH, Eglishalde 16, 78647 Trossingen, Telefon: +49 (0) 7425 / 228 - 0, Telefax: +49 (0) 7425 / 228 – 34, E-Mail: info(at)trsystems.de

10.3. RDPApp Viewer



RDPApp viewer with active info dialog

The info dialog provides information about the current CPU and RAM usage and shows the current connection duration. The user has the option of activating screen cleaning or terminating the connection and switching back to the start page.

RDPApp: Disconnection dialog

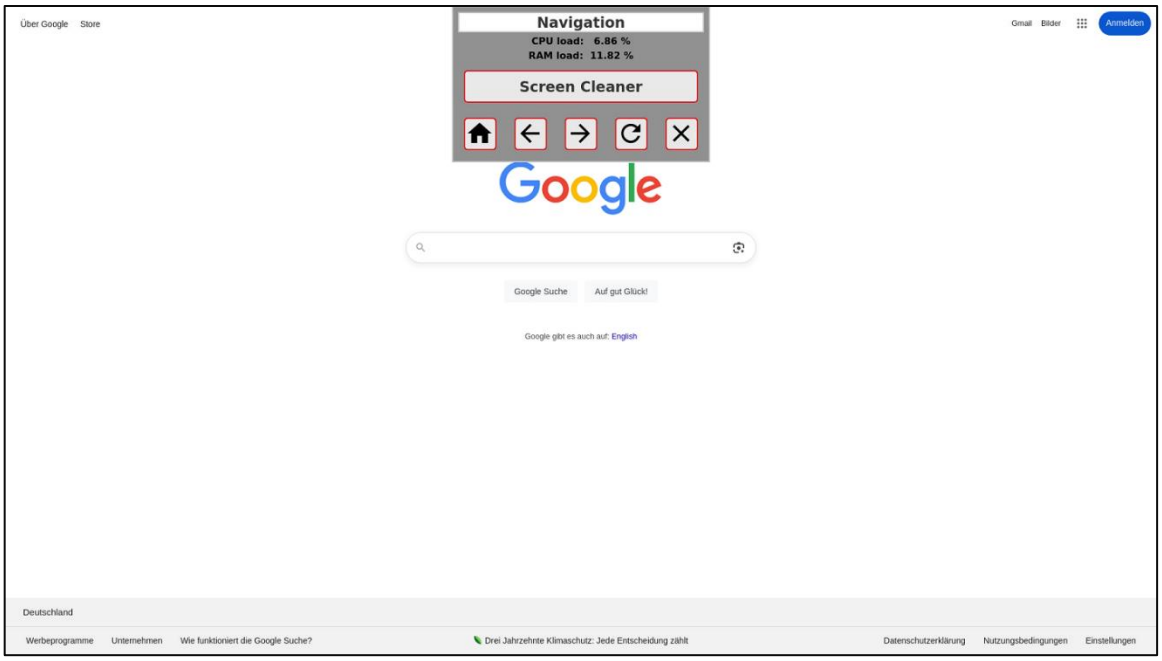
It can sometimes happen that the disconnection is not completed. In this case, the disconnection can be forced by pressing the corresponding button in the info dialog or in the disconnection dialog.

10.3.1 Multi-Client

The RDP multi-client function is available for both RDP and RDPApp connections. The prerequisite for this is an activated multi-client function and the use of shared RDP hosts to be accessed. All RDP / RDPApp clients must also be connected and accessible via the network.

For further details on RDP / RDPApp multi-client, see the RDP Viewer multi-client chapter

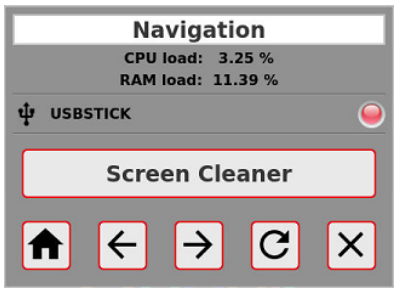
10.4. Web Viewer



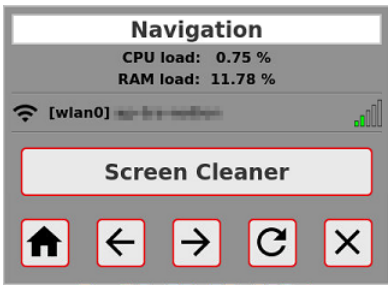
Web viewer with active info dialog

The info dialog provides information about the current CPU and RAM usage. The user has the option of activating screen cleaning, navigating between websites, terminating the connection and switching back to the start page.

For website navigation, functions for jumping to the programmed start page, jumping backwards, jumping forwards and reloading the page are available



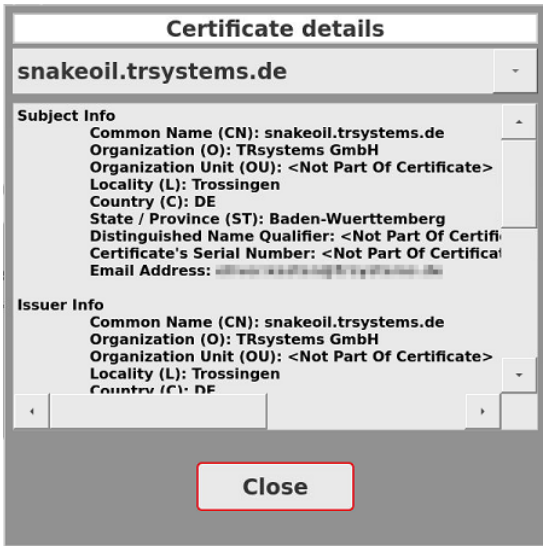
Web viewer: Info dialog with active USB stick



Web viewer: Info dialog with active WLAN connection

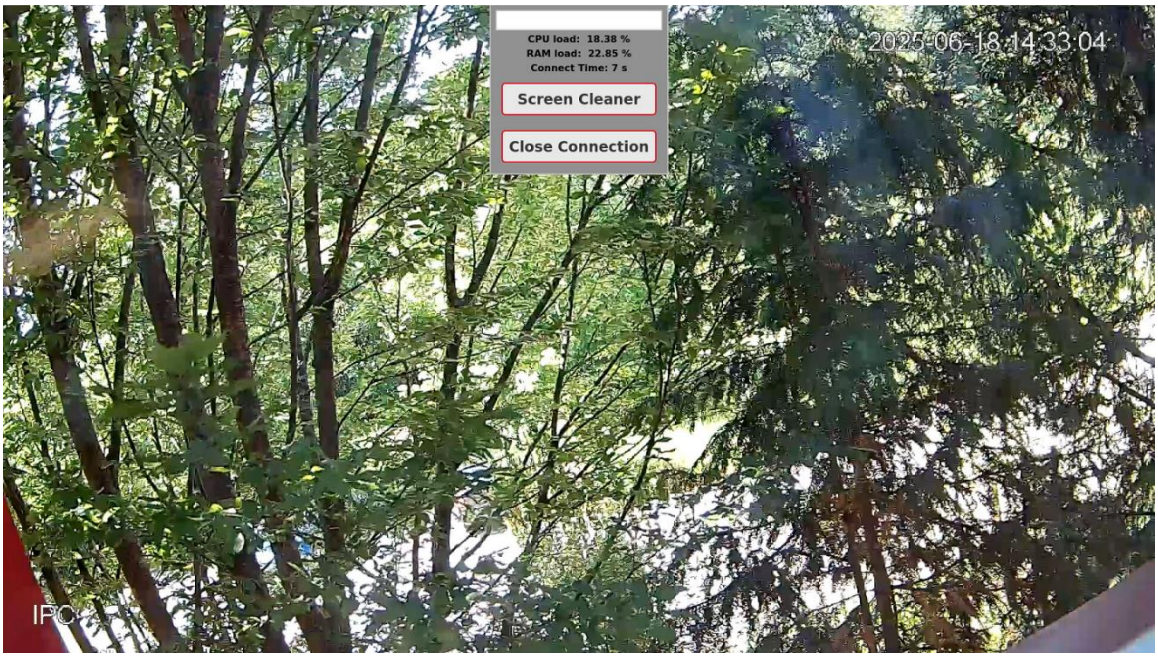
Web viewer: Certificate error when displaying a web page

If the browser reports a certificate error, the user is shown the corresponding message. The user have the choice of adding the certificate as an exception or disconnecting the connection - i.e. canceling the addition of an exception. The certificate details can be shown to help the user make a decision.



Web viewer: Certificate details after certificate error

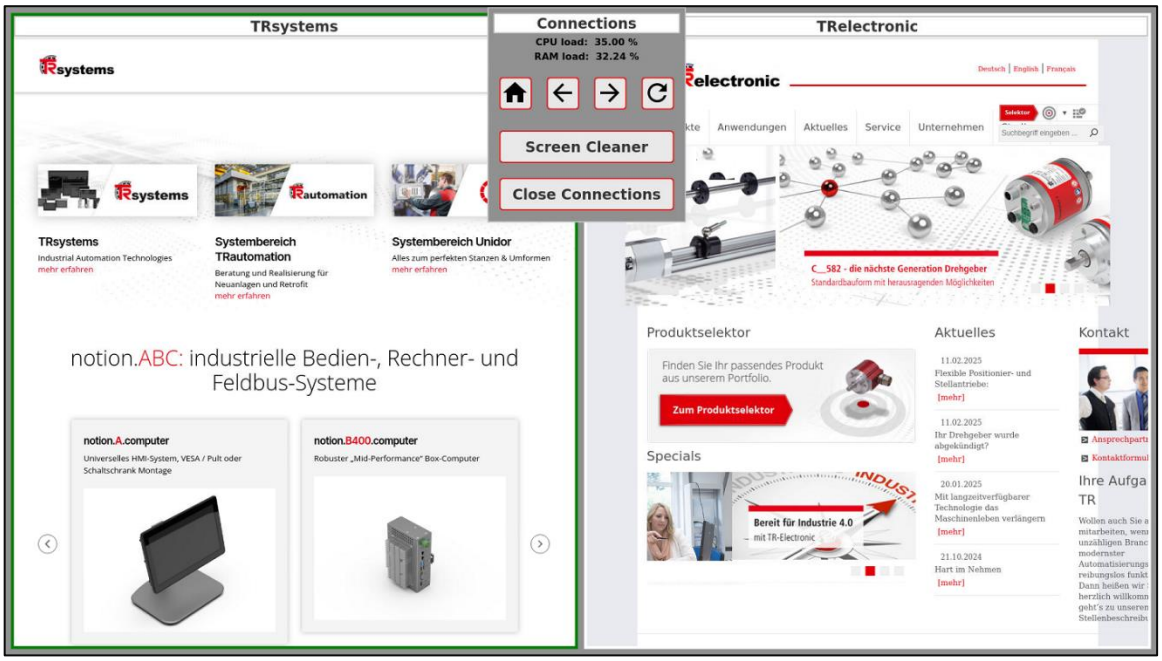
10.5. Stream Viewer



Stream viewer with active info dialog

The info dialog provides information about the current CPU and RAM usage and shows the current connection duration. The user has the option of activating screen cleaning or terminating the connection and returning to the start page.

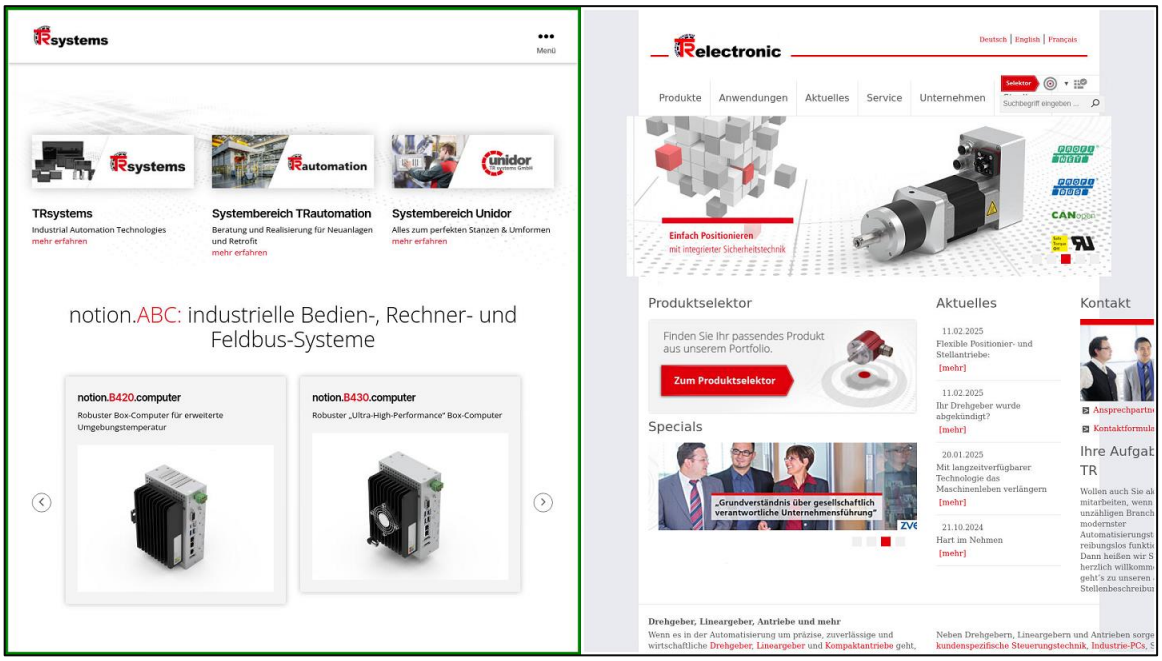
10.6. MultiView – Multiple connection view



MultiView viewer with active info dialog

The info dialog provides information about the current CPU and RAM usage and shows the current connection duration. The user has the option of activating screen cleaning or terminating the connection and returning to the start page.

Other buttons are shown depending on the active window. If the active window is a web viewer, buttons are also displayed that can be used to navigate between web pages: jumping to the programmed start page, jumping backwards, jumping forwards and reloading the page.



MultiView viewer: Representation without spacing

11. Daisy-Chain-IO

The notion#client establishes contact with the outside world via Daisy-Chain-IO. Various status informations are made available via the outputs and actions can be triggered via the inputs. Actions are currently user switching and page switching.

For each connection, you can specify what each user is allowed to do or see (full access, read-only access, no access)

Page switching can be used to specify from outside which connection is currently to be shown. A page ID can be specified for each connection for this purpose.

11.1. I/O via GPIO

Only 4 inputs and 4 outputs are available via GPIO. Parts of the user ID are received via the inputs. The outputs are used by VNC connections to indicate that the VNC client is currently in active use.

Bit Offset	0	1	2	3
	Active User Request 0	Active User Request 1	Active User Request 2	Active User Request 3

GPIO: Inputs

Bit Offset	0	1	2	3
	Daisy Chain IO 0	Daisy Chain IO 1	Daisy Chain IO 2	Daisy Chain IO 3

GPIO: Outputs

11.2. I/O via IOLink

16 inputs and 32 outputs are available via IOLink. Parts of the user ID and the page switch are received via the inputs. The outputs are used by VNC connections to indicate that the VNC client is currently being actively used. Other outputs show the page ID of the active page and, in the case of MultiView connections, also the page ID of the active subpage. Various state flags are also transmitted.

Bit Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

	Active User Request 0	Active User Request 1	Active User Request 2	Active User Request 3	Active User Request 4	Active User Request 5	Active User Request 6	Active User Request 7	Page Switch Request 0	Page Switch Request 1	Page Switch Request 2	Page Switch Request 3	Page Switch Request 4	Page Switch Request 5	Page Switch Request 6	Page Switch Request 7

IOLink: Eingänge

Bit Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	Daisy Chain IO 0	Daisy Chain IO 1	Daisy Chain IO 2	Daisy Chain IO 3	Daisy Chain IO 4	Daisy Chain IO 5	Daisy Chain IO 6	Daisy Chain IO 7	Active Page 0	Active Page 1	Active Page 2	Active Page 3	Active Page 4	Active Page 5	Active Page 6	Active Page 7
Bit Offset	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Active Subpage 0	Active Subpage 1	Active Subpage 2	Active Subpage 3	Active Subpage 4	Active Subpage 5	Active Subpage 6	Active Subpage 7	State Flags Valid Page ID	State Flags Valid Subpage ID	State Flags Unknown User	State Flags Config Mode Active	State Flags Active Connection State 0	State Flags Active Connection State 1	State Flags Active Connection State 2	State Flags Active Connection State 3

IOLink: Ausgänge

The state flags have the following meaning:

- Valid Page ID

The "Active Page" fields have a valid value.

- Valid Subpage ID

The "Active Subpage" fields have a valid value.

- Unkown User

The value of the "Active User Request" field of GPIO and, if available, IOLink does not match any configured user.

- Config Mode Active

The notion#client is currently in configuration mode (initiated by clicking the gear wheel on the start page). No connection is active.

- Active Connection State

Displays the state of the active connection or the state of the connection that currently has the input focus in the MultiView. The following values are available:

  - 0 – Connecting

  Connection is being established.

  - 1 – PasswordRequest

  Host expects a password from the client. If no information has been entered, an input dialog is shown.

  - 2 – UserPasswordRequest

  Host expects a user and a password from the client. If no information has been entered, an input dialog is shown.

  - 3 – Connected

  Connection has been established.

  - 4 – ApplicationStartUpDelayed

  RDPApp: Start of the applications is delayed by the set value.

  - 5 – ApplicationTerminated

  RDPApp: Application has been terminated, the connection still exists.

  - 6 – AwaitDisconnecting

  RDPApp: Wait for all applications to be terminated.

  - 7 – Disconnecting

  Connection will be disconnected.

  - 8 – Disconnected

  Connection is disconnected.

  - 9 – WaitForReconnect

  The connection was terminated, a reconnection attempt is started after the set time.

  - 10 – Error

  The connection is in an error state.

  - 11 – Loading

  Web: The web page is currently loading.

  - 12 – OnHold

  RDP/RDPApp Multi Client: Connection is currently in hold state. Connection is established after request.

  - 13 – Unknown

  Connection is in an unknown state (initialization state).

11.3. User switching

The assignment of input bit patterns to users offers a wide range of possible usage scenarios. The possibilities increase significantly, especially when combining GPIO and IO-Link inputs. In addition to the actual user ID, permissions for user login can also be realized by an external signal or a PLC.

The input bit pattern is evaluated as follows: The input bit pattern has changed. The list of configured users is processed from top to bottom. At the first match between the configured user and the available input signals, the user is identified as the active user and the analysis is ended.

There is a match if the bit patterns are identical. In this case, bits configured with 0 or 1 are taken into account and bits configured with X are ignored. Depending on availability, this evaluation is carried out for GPIO and for IOLink. In combined

mode, both evaluations must report a match in order to be considered a match overall. If the combined mode is not active, it is sufficient if one of the two evaluations reports a match.

Examples:

- Input = 0101 / Configuration = 0101 -> Match
- Input = 0101 / Configuration = 010X -> Match
- Input = 0100 / Configuration = 010X -> Match
- Input = 0111 / Configuration = 010X -> No match
- Input = 0111 / Configuration = 0101 -> No match

If a user has been determined, the “Unknown User” state flag is reset and the determined user is forwarded to the components and viewers involved, which then evaluate this information accordingly. If the user ID is unknown, the “Unknown User” state flag is set and the components and viewers involved are informed that an unknown user is logged in. The components and viewers involved then revert to the default settings.

11.4. Page switching

Page switching works slightly differently, as the page identifier, if set, is always unique. If a change in the input bit pattern is detected, the system checks whether a page/connection has the appropriate page ID. If this is the case, the information is forwarded and ultimately leads to page switching and the display of the corresponding connection.

12. System Update

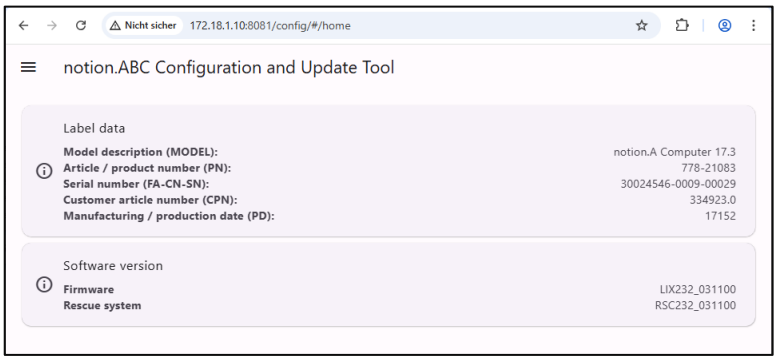
There are two options for installing the system update: installing the update packages via the web interface and the local update using an USB stick.

To update the system via the web interface, it must first be started. For security reasons, the web interface is disabled by default. The web interface is activated via the system configuration. Click on "Configure Web Interface" to access the corresponding dialog. The web interface can be accessed via the following URL: http://<IP address of the notion#client>:8081/config/.

The local update via USB stick can be activated via the service area. In the "Local Update" area, it can be activated using "Start Local Update".

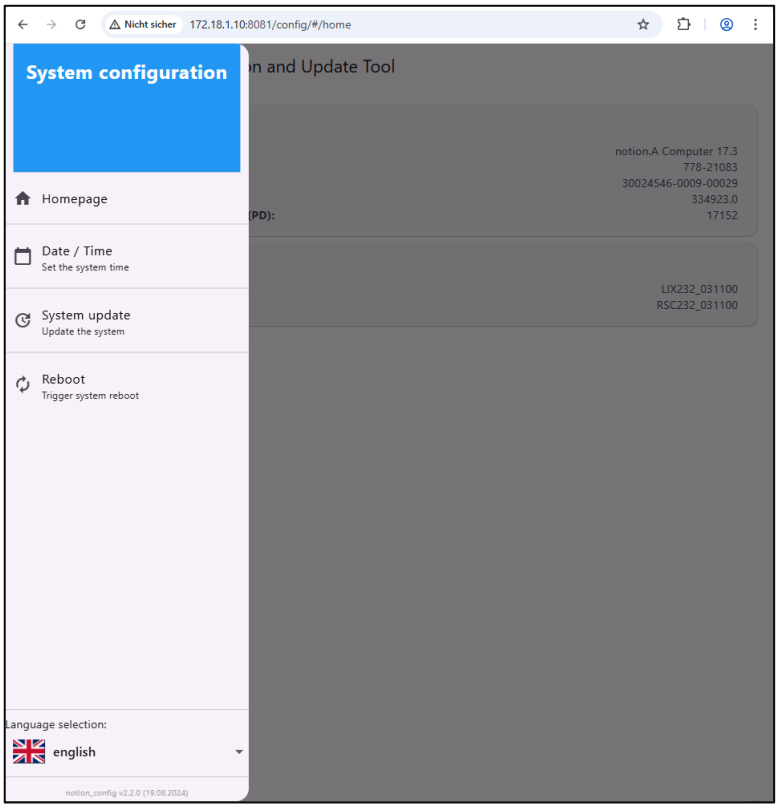
12.1. Remote update via the web interface

A standard browser is required to use the web interface. After establishing the connection to the notion#client, the start page is shown first. The device data, such as the serial number, is shown here. You can also see the version numbers of the installed software.



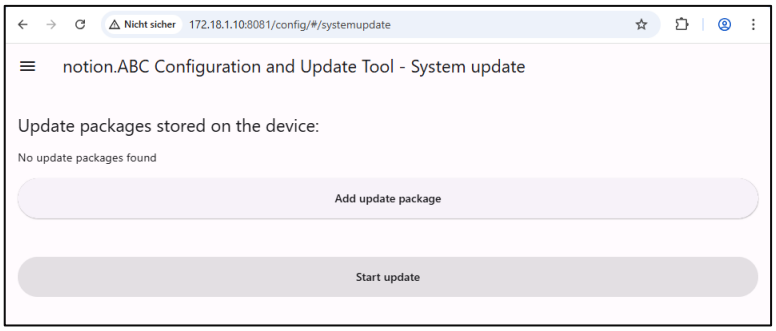
Web Interface: Start page

The “hamburger” button at the top left (three horizontal lines underneath each other) takes you to the menu view. From there, you can set the system time, update and restart the system.



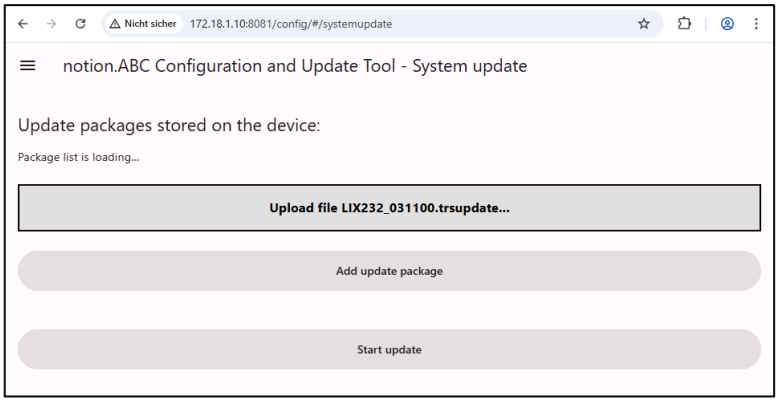
Web Interface: Menu view

If you select the system update in the menu, you will be taken to the system update start page. There you can upload the update package for the update. After clicking on “Add update package”, a file selection dialog opens in which you can select the appropriate package. After confirming, the package is uploaded. This may take a few moments.



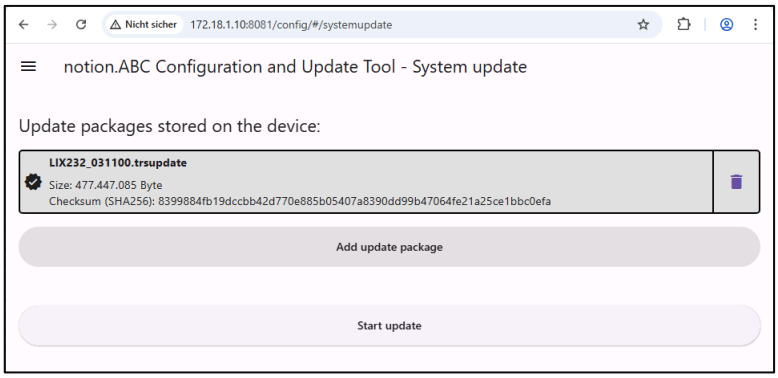
Web Interface: Start page system update

The following view is shown during the upload.



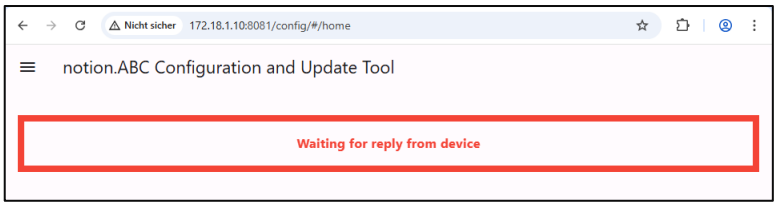
Web Interface: Upload the update package

After uploading the update package, the size of the update package and a SHA256 checksum are displayed. This information can then be checked. To start the system update, click on “Start update”.



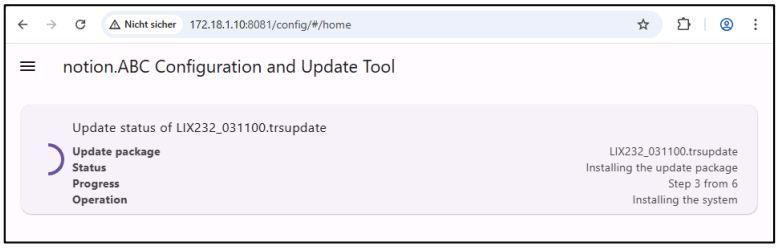
Web Interface: After uploading the update package

To perform the system update, the update system is started first. During the start phase and until a connection to the notion#client can be established again, the following view is displayed.



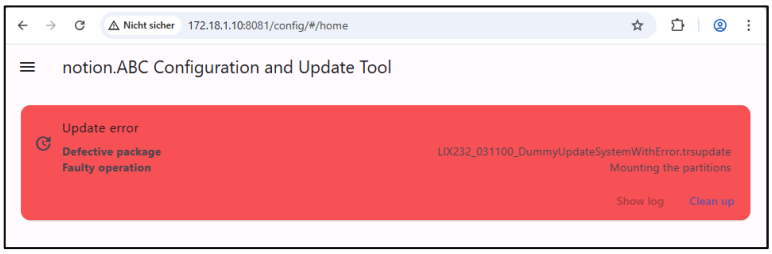
Web Interface: Starting the update system

Status information on the progress of the update is shown during the system update.



Web Interface: Installing the update package

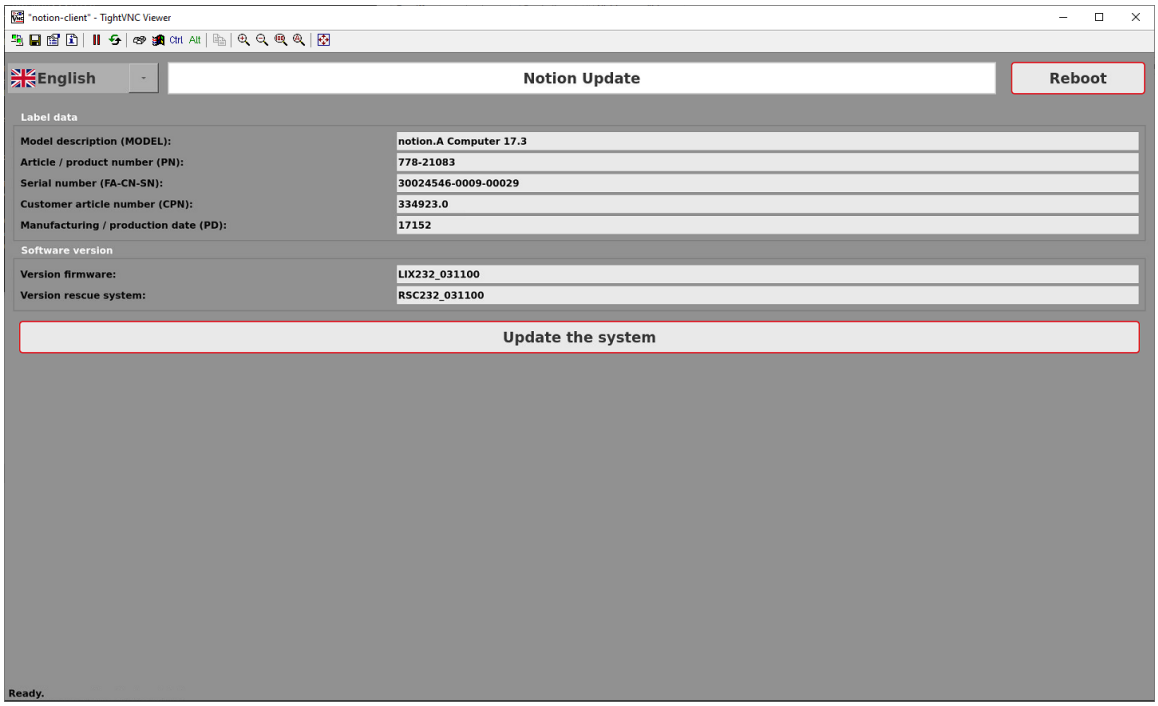
After the update, the system is automatically restarted and the newly installed system is executed. If errors occur during the update, the following view is shown. The faulty update package can be removed there (“Clean up”) and you can restart with a new system update with an error-free version.



Web Interface: Error when installing the update package

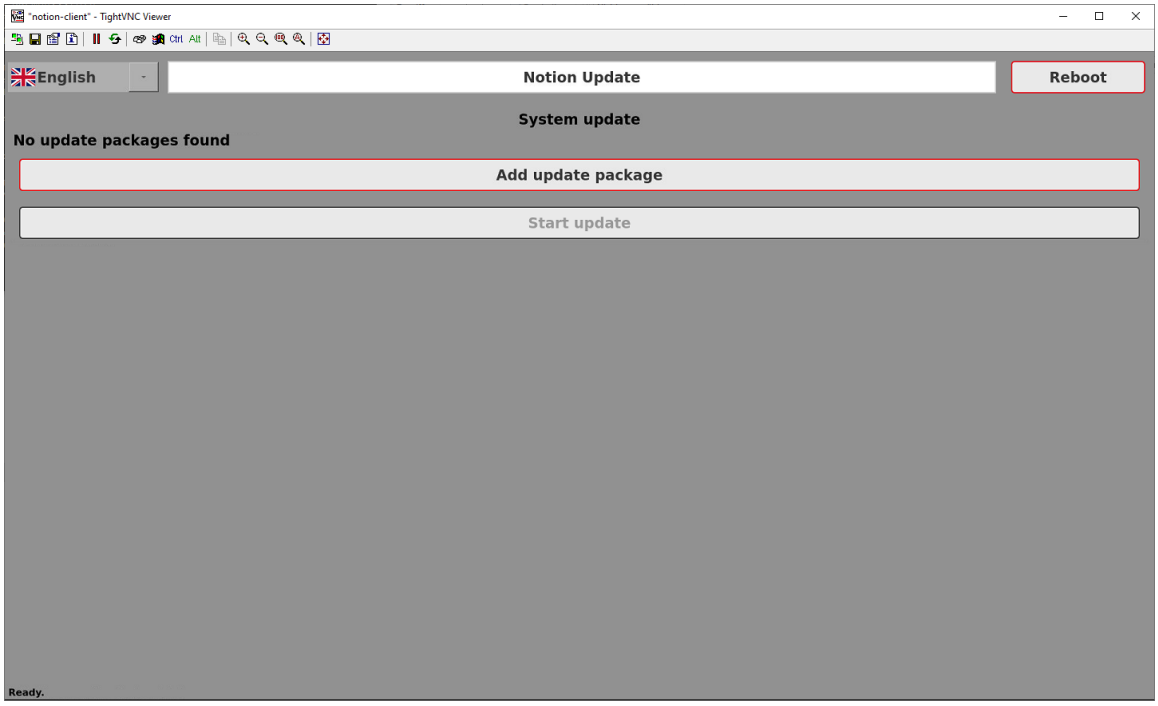
12.2. Local Update

Once the local update has been started, you will see the following view. Similar to the web interface, the device data, such as the serial number, is shown here. You can also see the version numbers of the installed software. Click on "Update the system" to go to the start page of the system update.



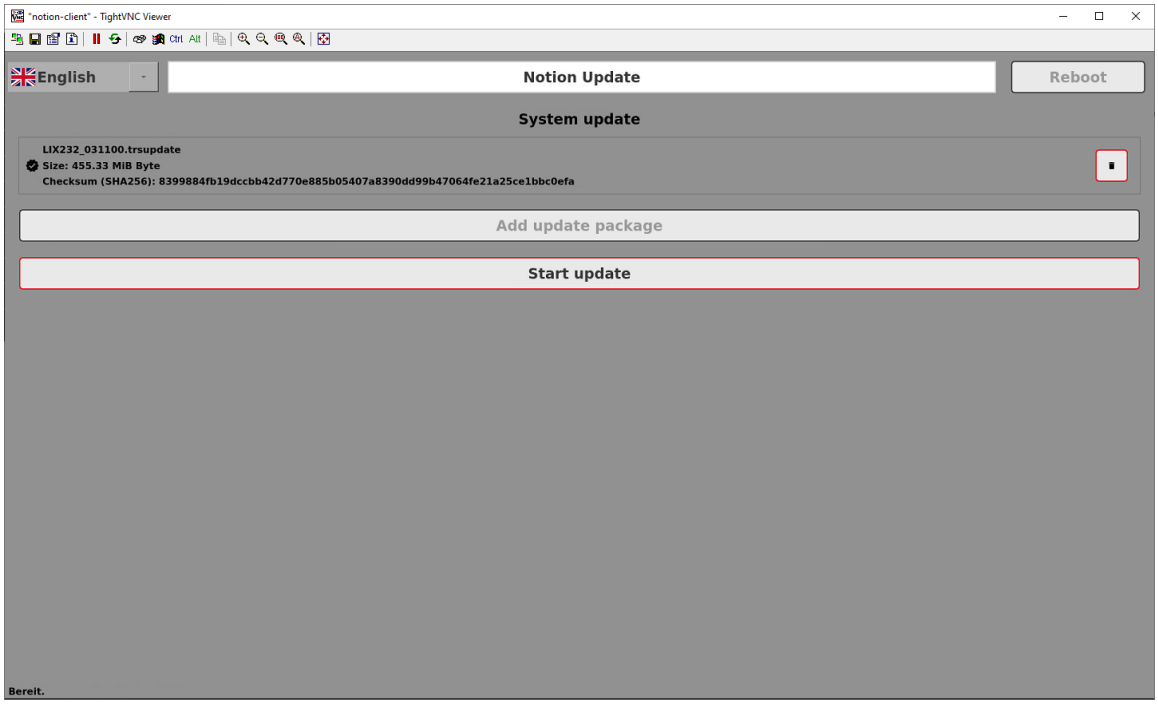
Local Update: Start page

You can then upload the update package for the update. After clicking on "Add update package", a file selection dialog opens in which you can select the appropriate package. After confirming, the package is uploaded. This may take a few moments.



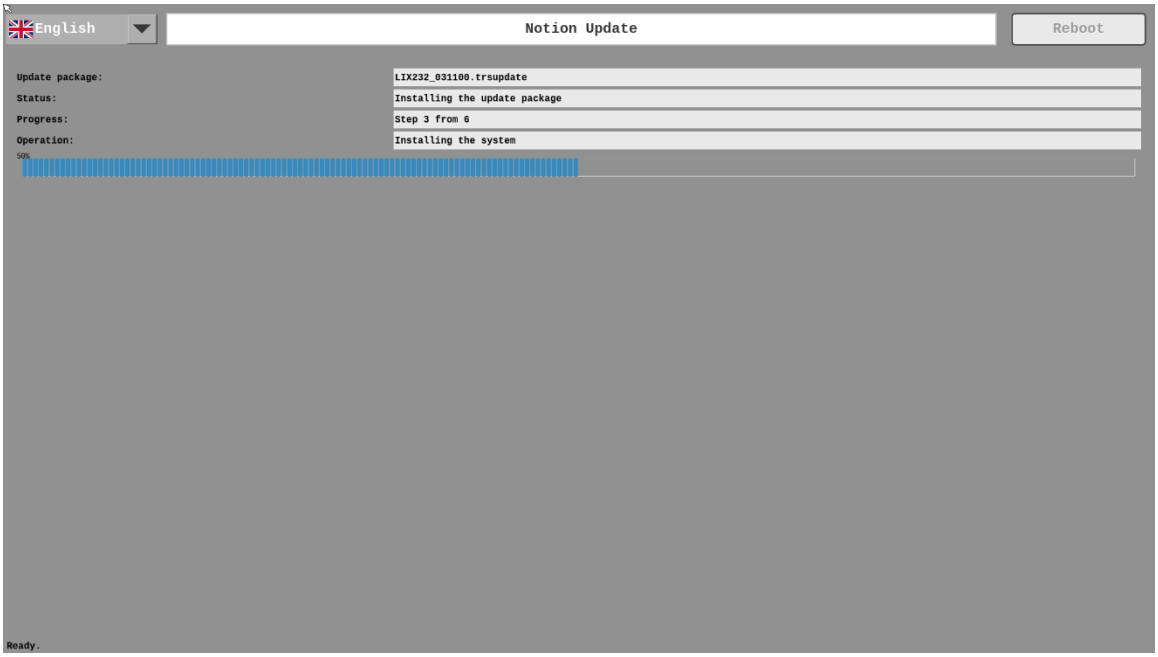
Local update: Start page system update

After uploading the update package, the size of the update package and a SHA256 checksum are displayed. This information can then be checked. To start the system update, click on “Start update”.



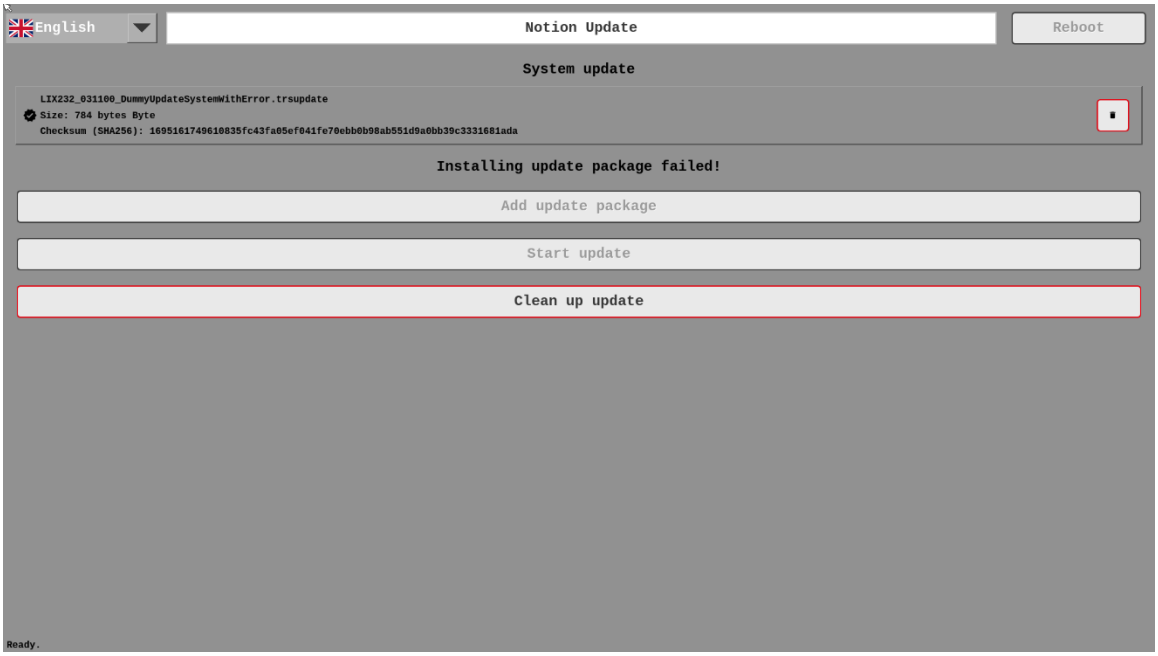
Local update: Upload of the update package

Status information on the progress of the update is shown during the system update.



Local update: Installing the update package

After the update, the system is automatically restarted and the newly installed system is executed. If errors occur during the update, the following view is shown. The faulty update package can be removed there ("Clean up") and you can restart with a new system update with an error-free version.

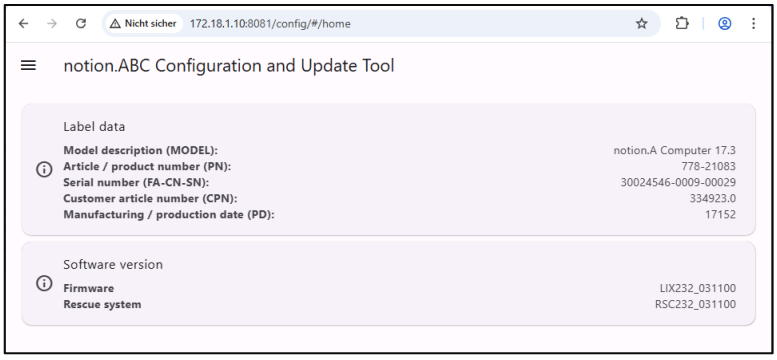


Local update: Error when installing the update package

13. Miscellaneous

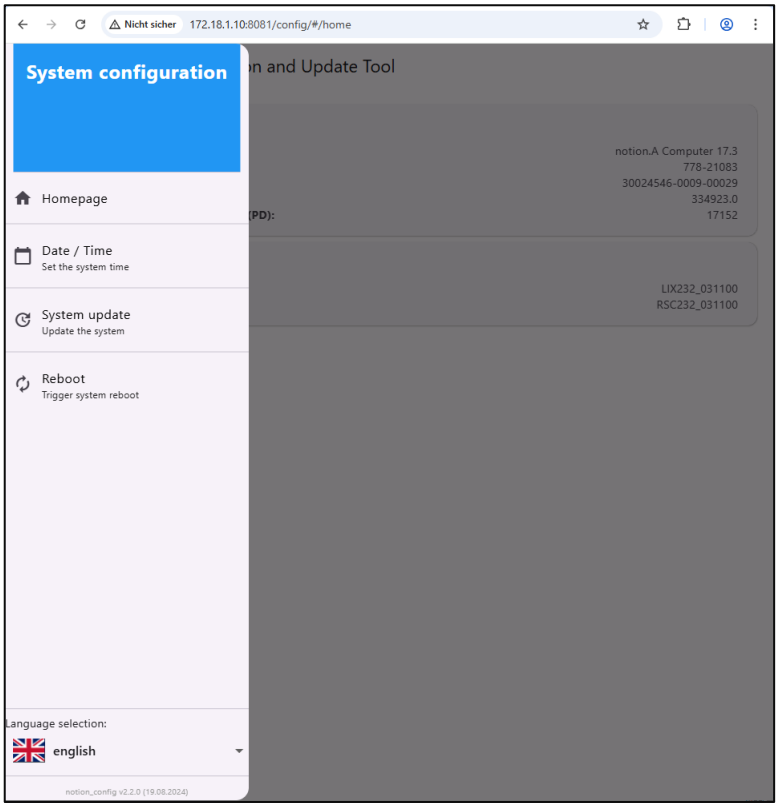
13.1. Setting the system time via the web interface

The system time can also be set via the web interface. To do this, click on the "hamburger" button at the top left of the start page (three horizontal lines below each other).



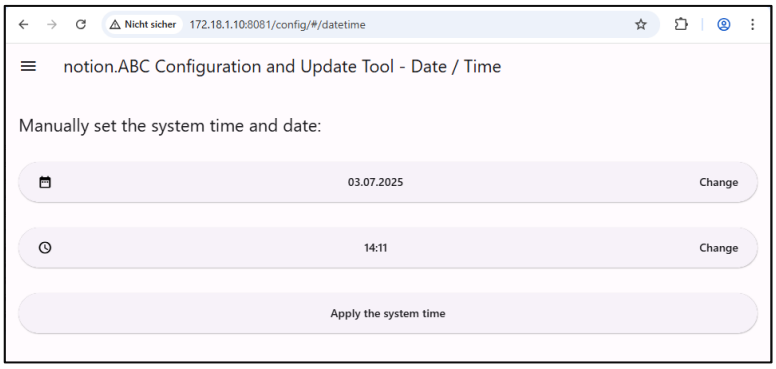
Web Interface: Start page

Use the "Date / Time" entry to set the system time.

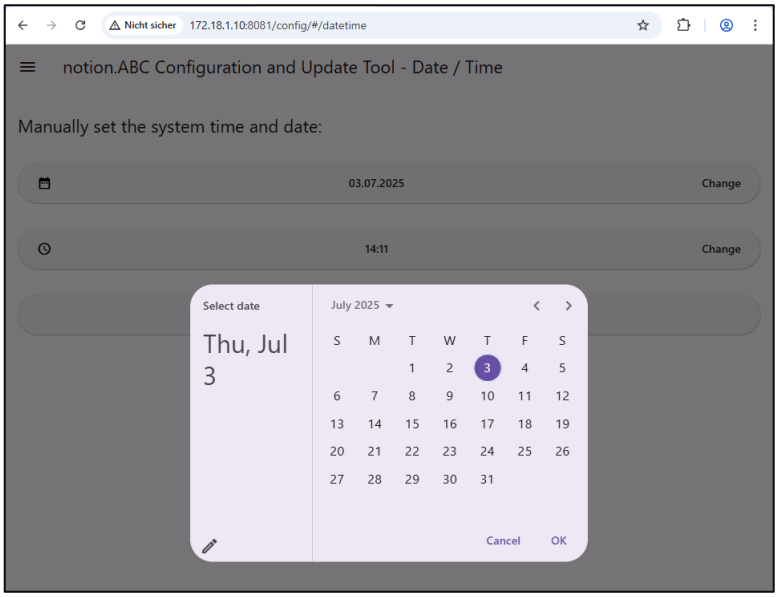


Web Interface: Menu view

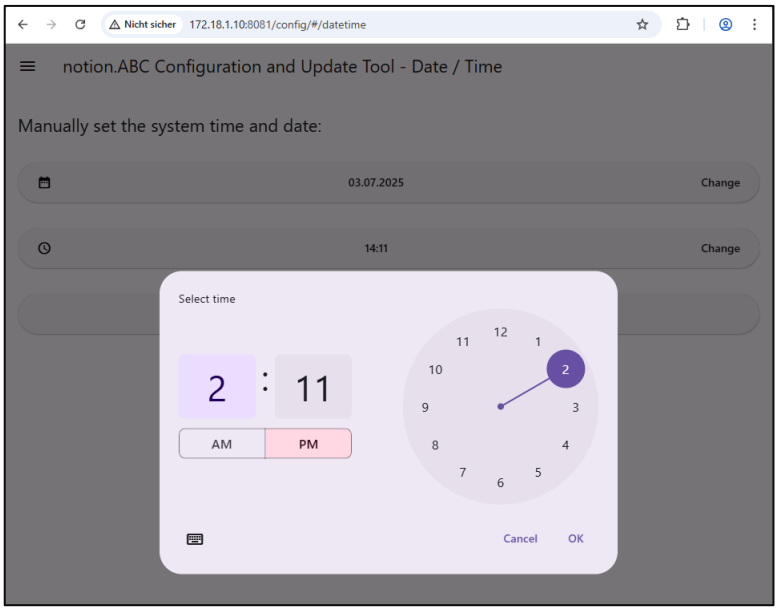
Three setting options are available here: manual setting of date / time and automatic synchronization with the system clock of the computer on which the browser is currently running. To do this, simply click on "Apply the system time" - the system clock values are then transferred.



Web Interface: Setting the system time



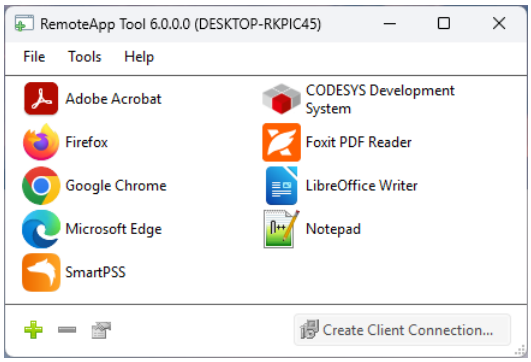
Web Interface: Setting the date



Web Interface: Settings the time

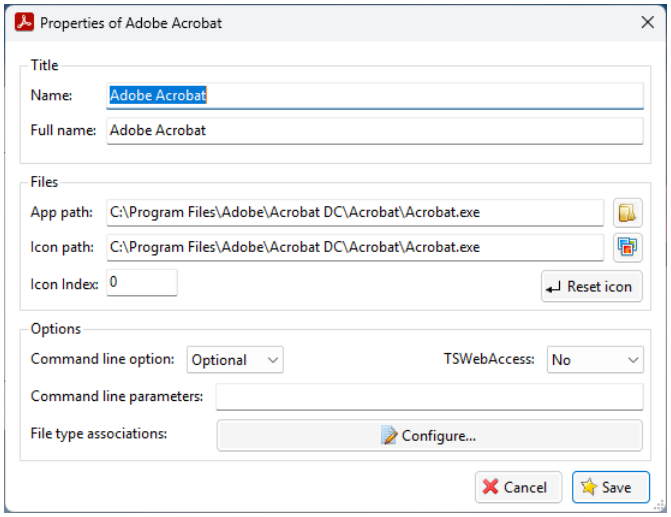
13.2. Creating rdp files on the Windows host

The RemoteApp tool can be used to create rdp files (see the website https://github.com/kimmknight/remoteapptool). This tool can be used to register applications for use as RDPApp applications in Windows. It can also be used to create a client connection (rdp file).



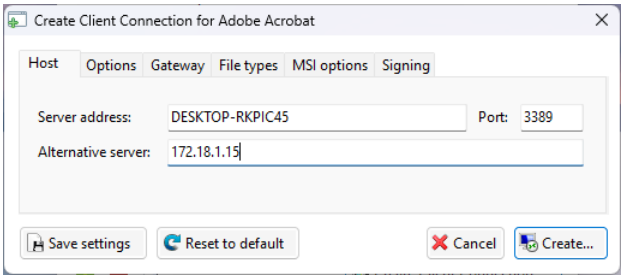
RemoteApp Tool with configured applications

To register an application, select the "New Remote App..." entry under the "File" menu item. A dialog then appears, which must be filled out accordingly. The most important entry here is the application path. The other entries can be adjusted as required.



Dialog for creating or customizing remote apps

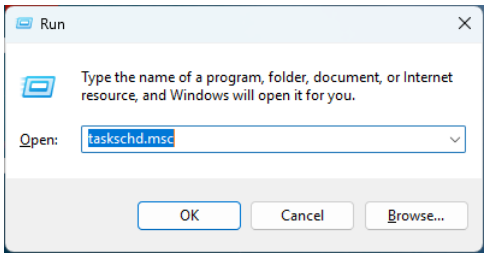
The appropriate rdp file for the application can then be created. Simply select the relevant application and click on “Create Client Connection...”. We recommend replacing the entry under “Alternative server” with the IP address of the Windows host. If the Windows name resolution does not work (reliably), the host can be reached via the IP address. The other options can be adjusted as required.



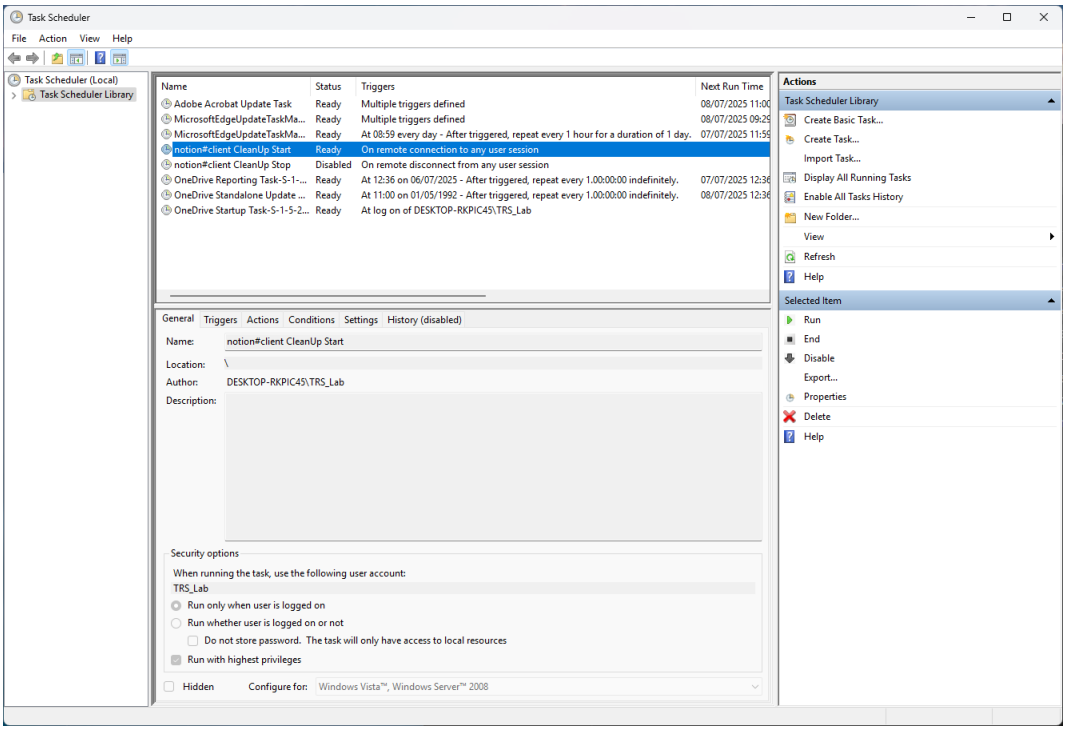
Dialog for creating an rdp file

13.3. Tips and tricks for RDPApp on Windows hosts

With RDPApp applications, it can happen that they do not exit correctly and still run as zombie processes on the host. This can lead to problems when restarting licensed applications. A workaround for such a use case would be the following: Using a PowerShell script, all RDPApp applications are checked after the connection is established to see if there are any running processes of the applications from previous calls, which are then also terminated immediately. The Task Scheduler is used for this purpose.

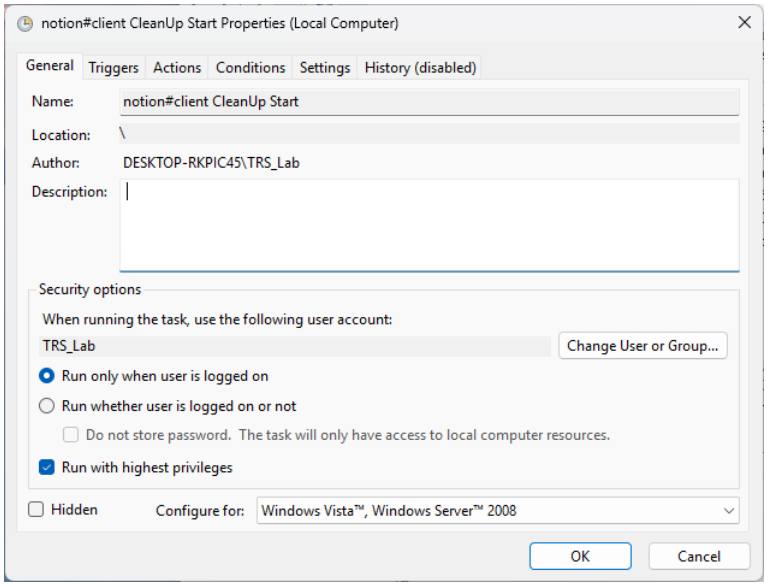


Calling the Task Scheduler (Windows Key + R)

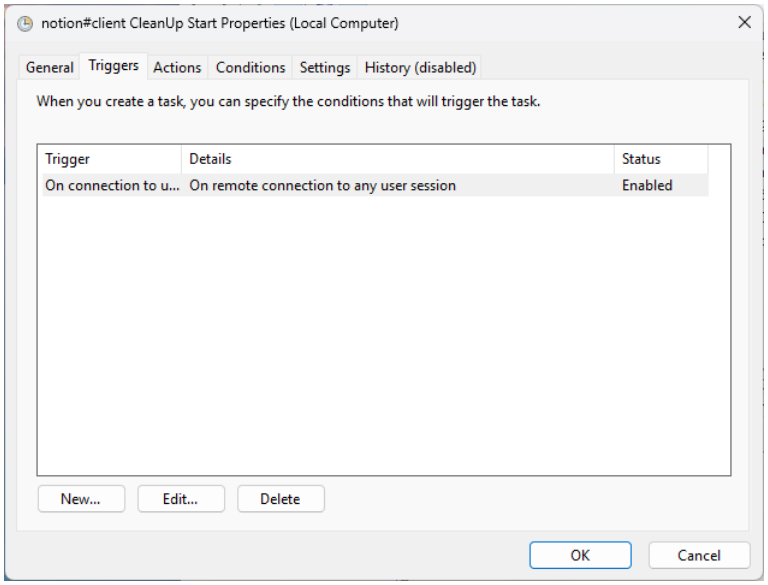


Task Scheduler with registered help script

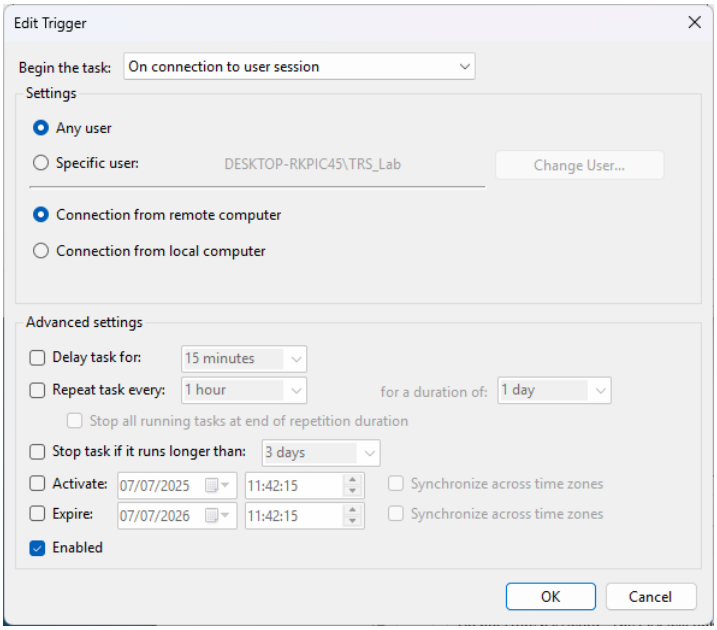
A new task is created to clean up the RDPApp applications (here: "notion#client CleanUp Start"). The task should run under the user account that is also used for the RDPApp applications. A trigger and an action are required for correct execution.



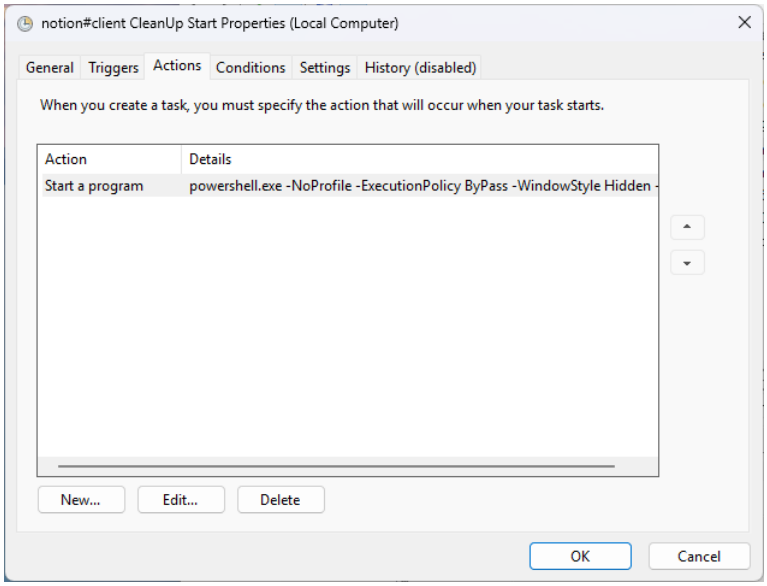
notion#client CleanUp Task Properties



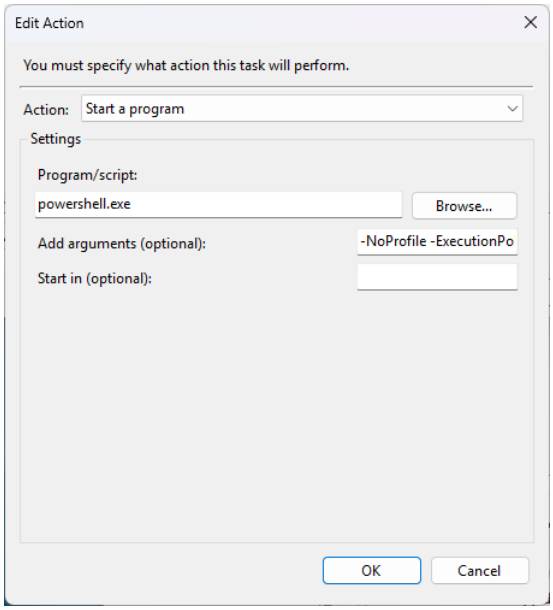
notion#client CleanUp Task Properties



notion#client CleanUp Task Properties



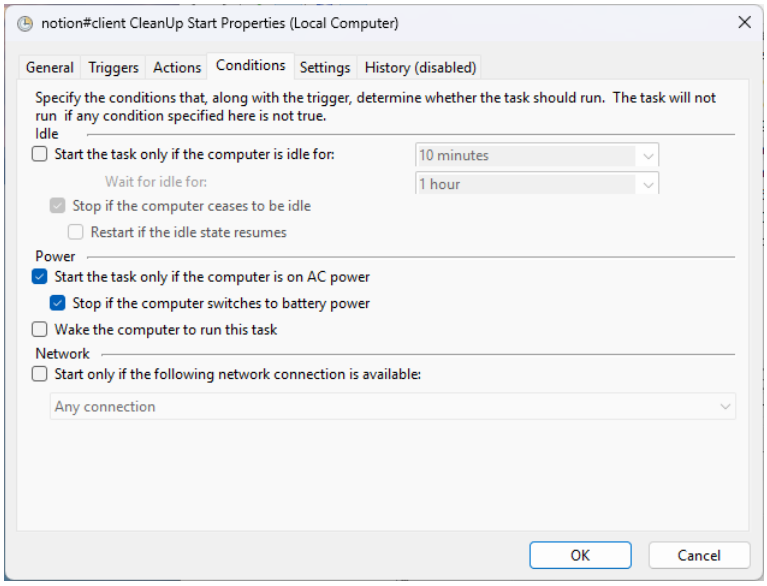
notion#client CleanUp Task Properties



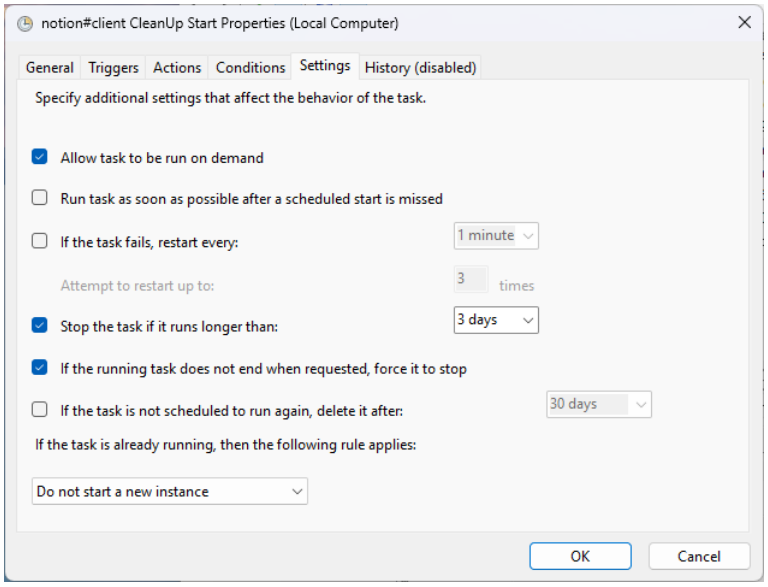
notion#client CleanUp Task Properties

The following text is used as an optional argument (only shown truncated in the image):

```
-NoProfile -ExecutionPolicy ByPass -WindowStyle Hidden -File
       "C:\Skripte\NotionClientCleanUp_Start.ps1"
```



notion#client CleanUp Task Properties



notion#client CleanUp Task Properties

The NotionClientCleanUp_Start.ps1 file contains a section for each registered RDPApp according to the following template. The specified path of the application is identical to the entry in the RDPApp configuration.

```
Add-Content -Path "C:\Skripte\NotionClientCleanUp_Start.log" -Value "Checking Acrobat Reader..."
$proc = Get-Process | Where-Object {$_.Path -like "*C:\Program Files\Adobe\Acrobat
DC\Acrobat\Acrobat.exe*"}
if ($proc) {
        Add-Content -Path "C:\Skripte\NotionClientCleanUp_Start.log" -Value "-> $proc"
        $proc | Stop-Process
}
```

In addition to terminating the RDPApp application for analysis purposes, the template also writes to a log file.