SIEMENS

SIMATIC HMI

Unified Basic Panels Control Panel V19

Operating Manual

11/2023

UBP Image V19.0.0.0

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Ⓟ 11/2023 Subject to change

Table of contents

1 Overview of functions

The table below shows the icons of the Control Panel and provides links to the corresponding function descriptions in the appropriate sections.

Icon	Name	Assigned functions
⌂	-	Open the main window of the Control Panel
▶	Start Runtime	Start project on the HMI device See also "Automatic runtime start (Page 13)"
	System Properties	Panel information (Page 6) Display (Page 7) Screensaver (Page 8) Update OS (Page 9) Reboot (Page 11) Performance (Page 12)
	Runtime Properties	Project information (Page 13) Automatic runtime start (Page 13) Alarm persistency (Page 14) Web client (Page 15) Load project from storage (Page 16)
	Network and Internet	Network settings (Page 19)
🛡	Security	User management (Page 22) Certificates (Page 26) Control panel access (Page 29) UMAC settings (Page 31)
⌨	External Devices and Input	Hardware interfaces (Page 33) Connected devices (Page 34)
🌐	Language, Region and Formats	Date and time (Page 35)
🛠	Service and Commissioning	Transfer (Page 37) Update OS (Page 9) Backup (Page 40) Restore (Page 41) Trace options (Page 43)

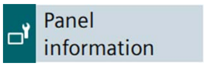
Some settings, such as interface parameters, runtime settings, or settings for user management, can be configured in WinCC and loaded to the HMI device. After loading, you can adjust the settings as needed in the Control Panel of the HMI device.

System Properties

2

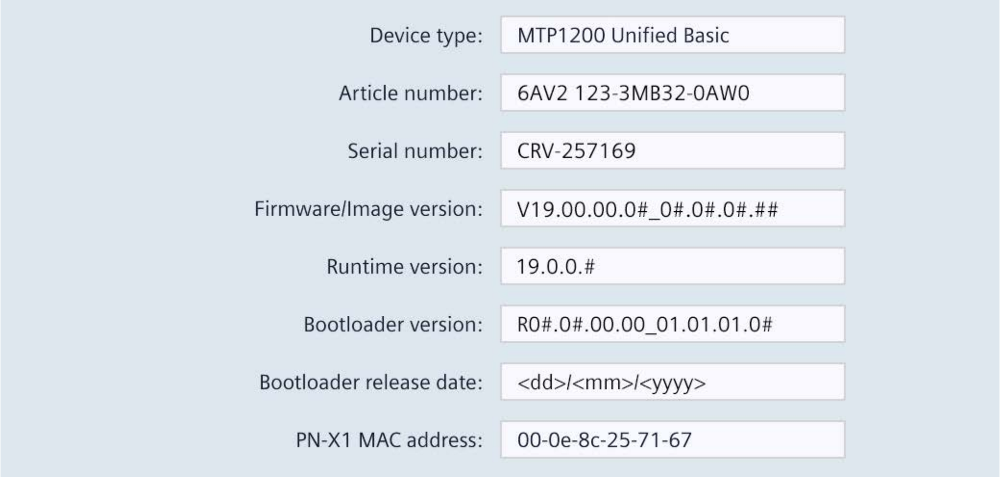
2.1 Panel information

Under "Panel information" you will find information specific to your HMI device, which you will need, for example, if you contact Technical Support.



Properties

The following figure shows an example. Variable display values are shown with the wildcard character "#" or between angle brackets "<>".



Device type:	MTP1200 Unified Basic
Article number:	6AV2 123-3MB32-0AW0
Serial number:	CRV-257169
Firmware/Image version:	V19.00.00.0#_0#.0#.0#.##
Runtime version:	19.0.0.#
Bootloader version:	R0#.0#.00.00_01.01.01.0#
Bootloader release date:	<dd>/<mm>/<yyyy>
PN-X1 MAC address:	00-0e-8c-25-71-67

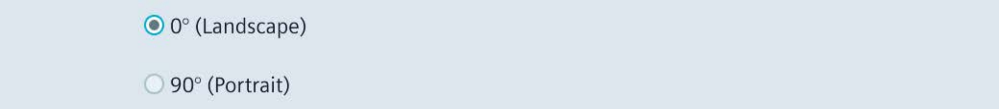
- "Device type": HMI device type designation
- "Article number": Article number of the HMI device
- "Serial number": HMI device serial number
- "Firmware/Image version": Version of the firmware and operating system.
- "Runtime version": Version of the runtime software located on the HMI device
- "Bootloader version": Version of the bootloader
- "Bootloader release date": Bootloader release date
- "PN-X1 MAC address": MAC address of the HMI device interface X1

2.2 Display

Under "Display" you define the display orientation and the display brightness via the intensity of the backlight.

NOTICE
Backlight reduction The brightness of the backlight decreases with increasing service life. To avoid shortening the service life of the backlight unnecessarily, reduce the backlight.

Orientation



● 0° (Landscape)

○ 90° (Portrait)

- "0° (Landscape)" (default setting): Select this option for HMI devices that have been installed and configured in landscape format.
- "90° (Portrait)": Select this option for HMI devices that have been installed and configured in portrait format.

Note

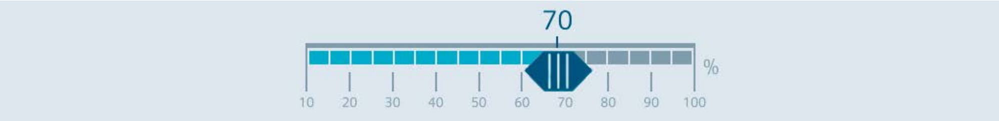
Display orientation and Runtime project

The display orientation in the Control Panel should match the display orientation of the HMI device in the WinCC configuration. Before switching the orientation in the Control Panel, adjust the configuration and reload the project into the HMI device.

The display orientation in the Control Panel should only be switched if no runtime project is running on the HMI device.

The HMI device must restarted if you switch the display orientation in the Control Panel.

Brightness

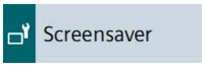


Set the desired display brightness using the slider.
Value range: 10 to 100%. Default setting: 70%

The display brightness can also be set within the value range via the configuration.

2.3 Screensaver

Under "Screensaver" you define the time until the automatic activation of the screensaver and the brightness of the backlight when the screensaver is active.



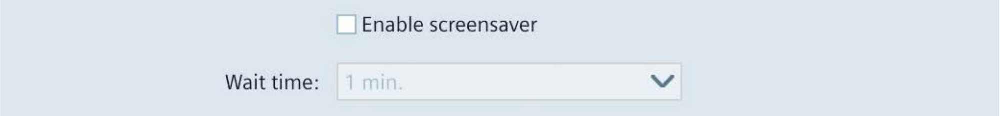
NOTICE

Activating the screensaver

If an image is displayed on the screen for long time, its outline may remain dimly visible on the display.

This effect is reversible when you use a screensaver.

General Settings



□ Enable screensaver

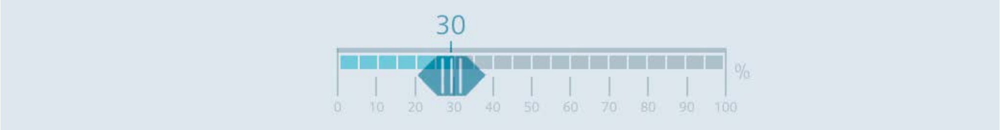
Wait time: 1 min.

- "Enable screensaver": Select this option to activate the screensaver.

  Default setting: "deactivated".
- "Wait time": Time to activate the screensaver, value range 1 to 120 minutes. Default setting is "1 min."

The screensaver is automatically activated if the HMI device is not operated within the specified period of time.

Brightness of screensaver



Use the slider to set the desired display brightness of the screensaver, value range 0 to 100%. Default setting is "30 %".

To deactivate the screensaver, tap the touch screen briefly. For safety reasons, this touch is not evaluated as an operator action. Therefore, no unintentional functions can be triggered.

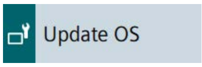
The screen saver is also deactivated when the HMI device is accessed remotely, for example, via the configuration PC.

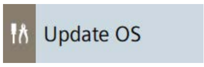
2.4 Update OS

The firmware and operating system version of the HMI device must be compatible with the firmware and operating system version of the installed WinCC software. If this is not the case, then you must update the operating system.

Use "Update OS" to update the operating system of the HMI device. The operating system is contained in several firmware files. The master file has the extension ".fwf". The number of additional files varies; these files have the file name of the master file and a sequential number (".0", ".1", ".2", etc.) as an extension.

The "Update OS" function is available under both "System Properties" and "Service and Commissioning".





NOTICE
Updating the operating system deletes data on the HMI device Project, parameter sets and user administration will be deleted when you update the operating system on the HMI device. Before updating the operating system, backup the data on the HMI device, if necessary. All settings, except the following settings which you changed in the Control Panel before updating the operating system, are retained even after the update of the operating system: • The external interfaces become activated again (default setting), see section "Hardware interfaces (Page 33)". • The time zone is reset to the default setting "(UTC) Coordinated Universal Time", see section "Date and time (Page 35)".

Use an industrial USB flash drive to load the firmware.

Firmware files for the HMI devices can be downloaded from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109746530). Observe the documentation included with the download.

Note

Do not rename firmware files

If you change the name of the firmware files, the operating system can no longer be updated with these firmware files. The firmware files become unusable. Leave the name of the firmware files unchanged.

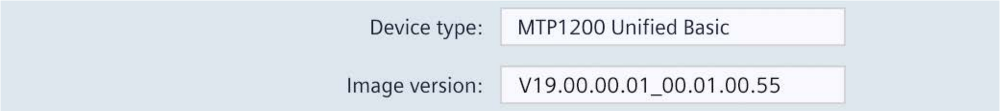
Note

Copy firmware files completely

If you copy the firmware files, be sure to also copy the master file ".fwf" together with all associated firmware files (".0", ".1", ".2", etc.).
If one of the files is missing, the operating system cannot be loaded.

Alternatively to the "Update OS" function in the Control Panel, you can use the "Update OS" function in WinCC.

Panel Information

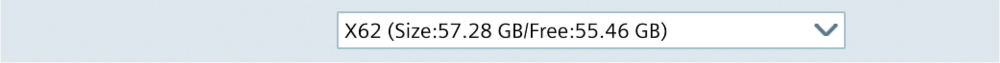


Device type: MTP1200 Unified Basic

Image version: V19.00.00.01_00.01.00.55

- "Device type": HMI device type designation.
- "Image version": Version of the firmware and operating system.

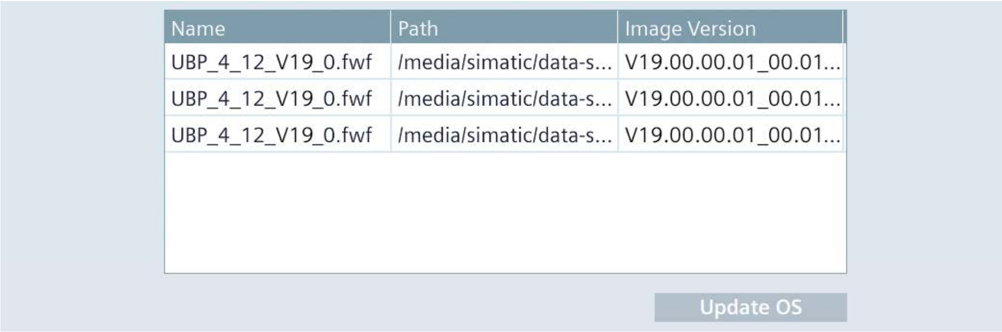
Select storage media for OS update



X62 (Size:57.28 GB/Free:55.46 GB)

Use the selection list to select the storage medium on which the firmware file is located.

Firmware files on external storage



Name	Path	Image Version
UBP_4_12_V19_0.fwf	/media/simatic/data-s...	V19.00.00.01_00.01...
UBP_4_12_V19_0.fwf	/media/simatic/data-s...	V19.00.00.01_00.01...
UBP_4_12_V19_0.fwf	/media/simatic/data-s...	V19.00.00.01_00.01...

- The list shows all firmware files that can be loaded into the HMI device.

  Select the desired firmware master file (.fwf) from the list.
- "Update OS": Button for starting the loading process.

  The HMI device restarts after the "Update OS" button is pressed. The loading process then begins.

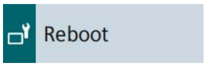
  A dialog with a progress bar is displayed on the HMI device for each firmware file.

  The HMI device is restarted again after the completion of the loading process.

  The main window of the Control Panel is displayed after the restart. The operating system on the HMI device is updated.

2.5 Reboot

You can restart the HMI device manually under "Reboot". The restart can be carried out normally or in maintenance mode.



In the following cases the HMI device is automatically restarted after confirmation:

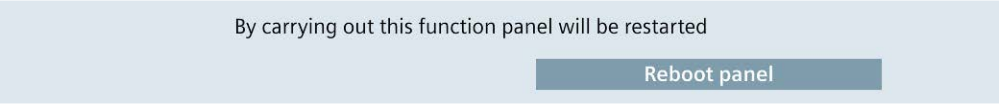
- You have made changes under "Network settings", see section "Network settings (Page 19)".
- You have switched screen orientation under the "Orientation" option, see section "Display (Page 7)".
- You have switched the "Enable alarm persistency" option, see section "Alarm persistency (Page 14)".

A manual restart of the HMI device is required in the following case:

- You have changed the interface parameters under "Media redundancy" in the configuration and loaded the project to the HMI device again.

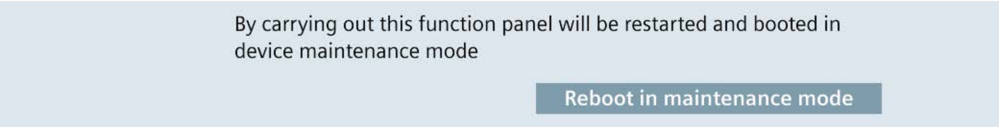
NOTICE
Data loss All volatile data is lost with a restart. Make sure that no project is running on the HMI device and no data is being written to the flash memory.

Reboot panel


By carrying out this function panel will be restarted

"Reboot panel": Button for a simple restart of the HMI device ("soft reboot").

Reboot in maintenance mode


By carrying out this function panel will be restarted and booted in device maintenance mode

"Reboot in maintenance mode": Button for a restart in maintenance mode. The restart in maintenance mode is required to reset the HMI device to factory settings.

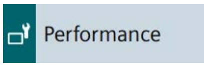
The HMI device restarts after the "Reboot in maintenance mode" button is pressed. The "Maintenance Mode" dialog box is displayed for a period of 10 minutes. In this period you can connect the HMI device to a configuration PC and reset the HMI device to factory settings with the ProSave software.

See also

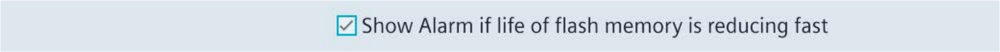
Resetting an HMI device to factory settings via ProSave (Page 50)

2.6 Performance

Under "Performance" you can activate the monitoring of the internal flash memory.

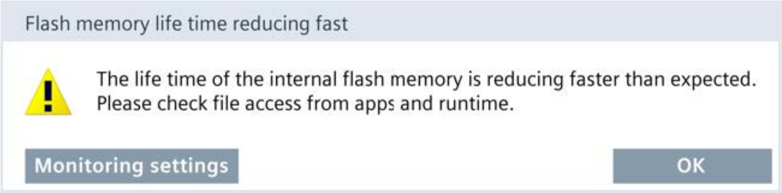


Flash Memory Monitoring Section


☑ Show Alarm if life of flash memory is reducing fast

"Show Alarm if life of flash memory is reducing fast": Option to activate flash memory monitoring. The default setting is "activated".

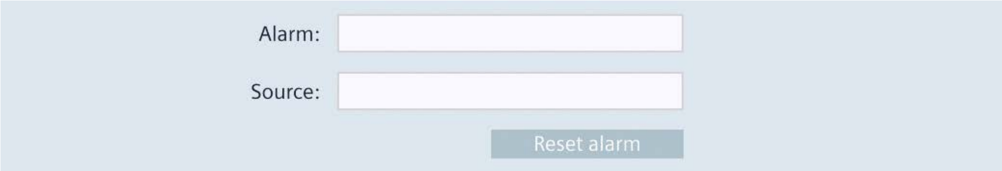
If the option is activated, the state of the flash memory is checked cyclically. If the cyclical check results in a high load on the flash memory, the message "Flash memory life time reducing fast" is displayed regularly.


Flash memory life time reducing fast

The life time of the internal flash memory is reducing faster than expected.
Please check file access from apps and runtime.

- "Monitoring settings": Button for opening the "Performance" settings in the Control Panel. Press the button, note the cause specified under "Source" and contact the corresponding administrator or configuring engineer.
- "OK": Button for acknowledging the alarm.

Last alarm

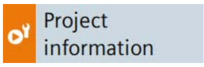


- "Alarm": Display panel with the last alarm that was displayed about the status of the flash memory.
- "Source": Display field with information on the cause of the last alarm. Pass this information on to the administrator or project engineer, who can change the settings in the corresponding app or the configuration of the HMI device so that the "Flash memory life time reducing fast" alarm no longer appears.
- "Reset alarm": Button for deactivating the regularly occurring "Flash memory life time reducing fast" alarm. The button can only be operated by users with the "Control Panel Administrator" authorization. After pressing the button, the "Flash memory life time reducing fast" alarm is only displayed again when the next cyclic check results in a high load on the flash memory.

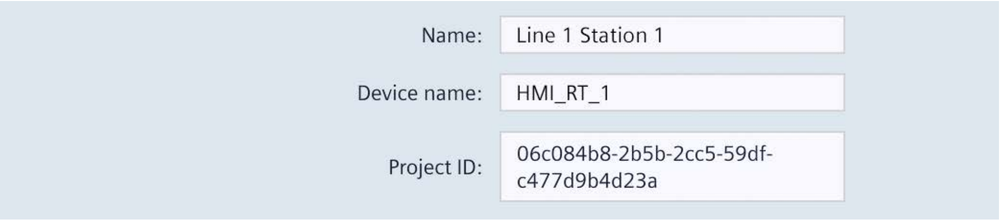
Runtime Properties 3

3.1 Project information

Under "Project information" you can view the project-specific information that uniquely identify the project on the HMI device.



Project information



Name: Line 1 Station 1

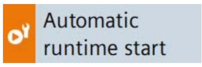
Device name: HMI_RT_1

Project ID: 06c084b8-2b5b-2cc5-59df-c477d9b4d23a

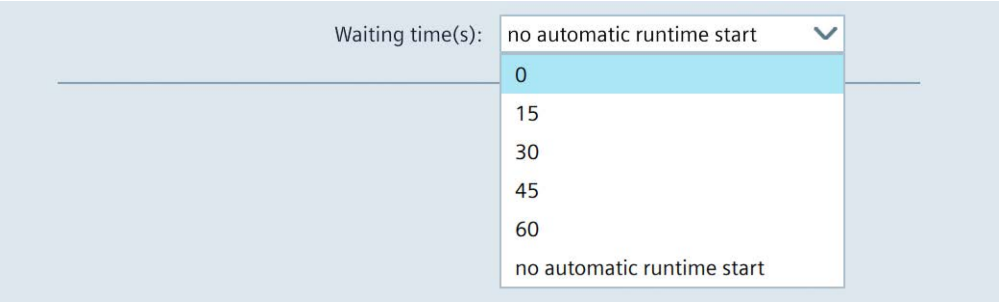
- "Name": Name of the project is equivalent to the name of the project in WinCC (TIA Portal).
- "Device name": Automatically generated name of the runtime project on the HMI device.
- "Project ID": Unique identification of the runtime project is equivalent to the "Runtime ID" of the project in WinCC (TIA Portal).

3.2 Automatic runtime start

Under "Automatic runtime start" you define whether the project on the HMI device starts automatically or not after a defined delay time.



Automatic runtime start



Waiting time(s): no automatic runtime start

"Waiting time(s)": Drop-down list for determining whether the project on the HMI device starts automatically after a specified delay time or not.

Selection options:

- "0": The project is started directly after the operating system.
- "15" to "60": The project starts after a delay time of 15 to 60 seconds. During the delay time, the dialog "Runtime Start" is displayed with a countdown and the following buttons:
  - "Cancel": The dialog is closed, Runtime does not start.
  - "Skip": The delay time is skipped, Runtime is started.
- "no automatic runtime start" (default setting): The project is not started automatically, but via the "Start Runtime" button in the Control Panel.

Starting Runtime

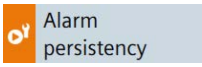
While Runtime starts on the HMI device, the dialog box "Runtime Start" is displayed with an initialization message. The Control Panel cannot be operated while Runtime is starting.

Note

To open the Control Panel from Runtime, configure an operating element to which the "ShowControlPanel" or "StopRuntime" system function is assigned.

3.3 Alarm persistency

You can enable or disable deactivate the retentivity of the alarm buffer under "Alarm persistency". The default setting is "deactivated".

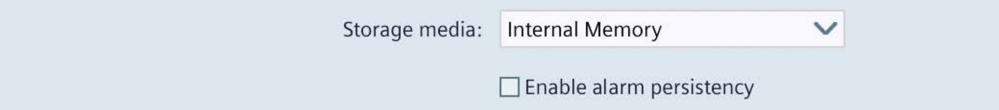


Note

Back up data before deactivating the retentivity

When you deactivate the retentivity of the alarm buffer and still need the data in the alarm buffer, back up this data before deactivating the retentivity in a log.

Alarm persistency configuration



Storage media: Internal Memory

□ Enable alarm persistency

- "Storage media": Selection list for defining the storage medium for the retentive alarm buffer. Selection options:
  - "Internal Memory": Alarms are written to the internal flash memory.
- "Enable alarm persistency": Option to enable or disable the retentivity of the alarm buffer. The default setting is "deactivated".

  When the retentivity of the alarm buffer is activated, the retentive alarm data is backed up every two seconds to the selected storage medium. With a high number of alarms, the storage medium is subject to an equally high number of read and write cycles.

  If the retentivity of the alarm buffer is deactivated, the alarm buffer is emptied and the retentive alarm data is no longer backed up to the selected storage medium. This means the storage medium is used less with a high number of alarms.

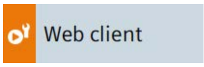
Switching the "Enable alarm persistency" option requires a restart, and the "Enable alarm persistency" dialog is displayed. Restart the system using the "OK" button.

See also

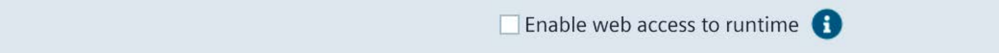
Reboot (Page 11)

3.4 Web client

Under "Web client", you can enable web-based client access to the runtime project. Operator control in runtime via a client is asynchronous, that is, the display content of the server does not change while the client is operating in runtime.



Web client configuration



□ Enable web access to runtime

- "Enable web access to runtime": Option to enable web access to the runtime project.

Web access to the runtime project

When web access is enabled, you can access the runtime project via a browser, see section "Web access to the HMI device (Page 46)".

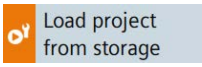
You can find more information on remote access via "Web client" in the TIA Portal Help under: "Visualizing processes (RT Unified) > Using distributed systems > Web client".

3.5 Load project from storage

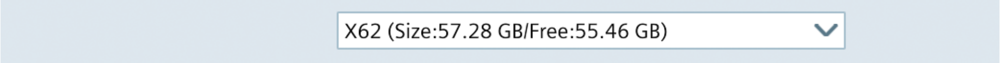
Under "Load project from storage", you can load into the HMI device a project that was backed up on an external storage medium in WinCC (TIA Portal).

You generate the necessary project data in WinCC by configuring the HMI device and then using drag-and-drop to move the folder of the HMI device (e.g. "HMI_1 [<*DeviceType*>]") to an external storage medium (🖴 icon) under "Card Reader/USB memory".

Recommendation: The Runtime and firmware versions of the project should match those of the HMI device.

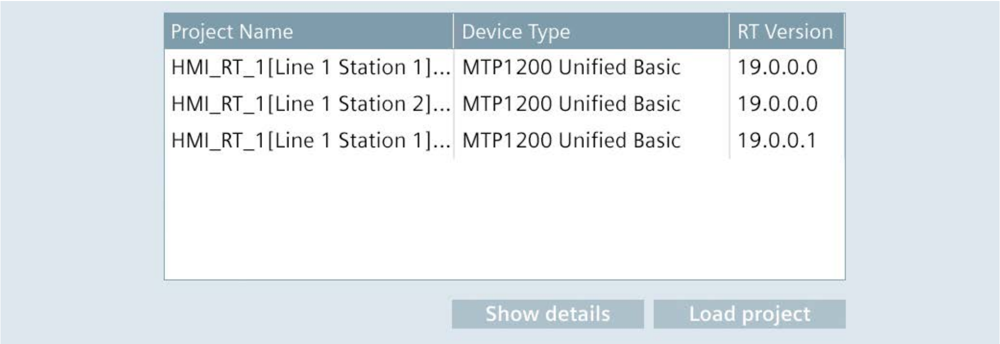


Select storage media for project transfer


X62 (Size:57.28 GB/Free:55.46 GB)

Select the storage medium on which the backed-up project is stored.

Projects on external storage

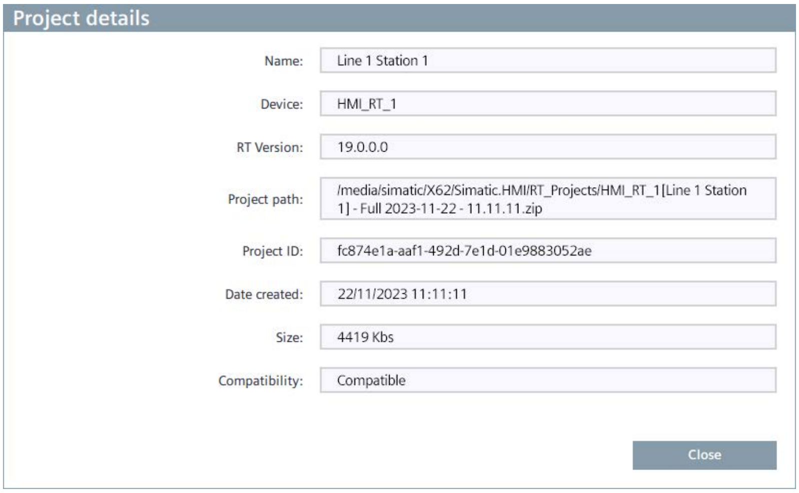


Project Name	Device Type	RT Version
HMI_RT_1[Line 1 Station 1]...	MTP1200 Unified Basic	19.0.0.0
HMI_RT_1[Line 1 Station 2]...	MTP1200 Unified Basic	19.0.0.0
HMI_RT_1[Line 1 Station 1]...	MTP1200 Unified Basic	19.0.0.1

- The list includes all projects that are located on the external storage medium.
- "Show details": Button for displaying additional information on a selected project.
- "Load project": Button for loading the selected project.

Displaying details and checking compatibility

If you have selected a project you can use the "Show details" button to display more information about the selected project and check whether the project can be loaded into the HMI device.



Project details

Name: Line 1 Station 1

Device: HMI_RT_1

RT Version: 19.0.0.0

Project path: /media/simatic/X62/Simatic.HMI/RT_Projects/HMI_RT_1[Line 1 Station 1] - Full 2023-11-22 - 11.11.11.zip

Project ID: fc874e1a-aaf1-492d-7e1d-01e9883052ae

Date created: 22/11/2023 11:11:11

Size: 4419 Kbs

Compatibility: Compatible

- "Name": Name of the project.
- "Device": Name of the HMI device in the project.
- "RT Version": Runtime version of the project.
- "Project path": Path of the project on the external storage medium.
- "Project ID": Unique identification of the runtime project is equivalent to the "Runtime ID" of the project in WinCC (TIA Portal).
- "Date created": Date on which the project in WinCC (TIA Portal) was saved to a storage medium.
- "Size": Size of the project on the storage medium.
- "Compatibility": A message about the compatibility of the project and the HMI device is displayed in this output field. Depending on the degree of compatibility, the message is highlighted in color.

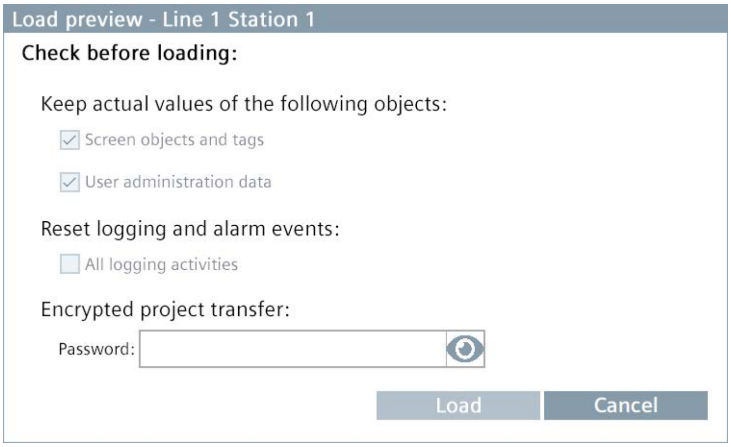
The following messages can be displayed in the "Compatibility" output field:

- The message "Compatible": Project and HMI device are compatible, the project can be loaded without any problem.
- Messages of the "Warning" type highlighted in orange: Firmware and/or runtime version of project and HMI device differ. The versions are compatible, an "Upgrade" or "Downgrade" is optional. The project can be loaded.
- Messages of the "Error" type highlighted in red: The project cannot be loaded for one of the following reasons.
  - Project and device type are incompatible, i.e. the project was created for a different device type. To load the project, replace the device in WinCC.
  - Firmware and/or Runtime version of project and HMI device are incompatible, an "Upgrade" or "Downgrade" is required. To load the project, update the operating system of the HMI device.

  You can find information on updating the operating system at the end of this section and under "See also".

Load project

The "Load preview" dialog is displayed via the "Load project" button.



Load preview - Line 1 Station 1

Check before loading:

Keep actual values of the following objects:

☑ Screen objects and tags

☑ User administration data

Reset logging and alarm events:

□ All logging activities

Encrypted project transfer:

Password:

- Under "Keep actual values of the following objects", you specify whether the process values of the following objects are to be retained:
  - "Screen objects and tags": Option for keeping the process values of screen objects and tags on the HMI device.
  - "User administration data": Option for keeping the user management on the HMI device.

  Under "Reset logging and alarm events", you specify whether data in logs and alarm events are to be deleted:
  - "All logging activities": Option for deleting all logs and alarm events.

  The "Encrypted project transfer" area is displayed when encrypted transfer is enabled for the selected project. In this case, enter the password that was set in WinCC for the encrypted transfer.
- The "Load" button loads the project into the HMI device, taking the selected settings into account.

  After the loading process, you can start the project via the "Start Runtime" function on the HMI device.

Activation of the options that are currently grayed out is envisaged in a later firmware version.

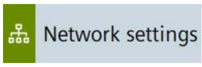
See also

Update OS (Page 9)

Networks and Internet 4

4.1 Network settings

Under "Network settings", you can change settings for the interface X1, which supports PROFINET basic services.



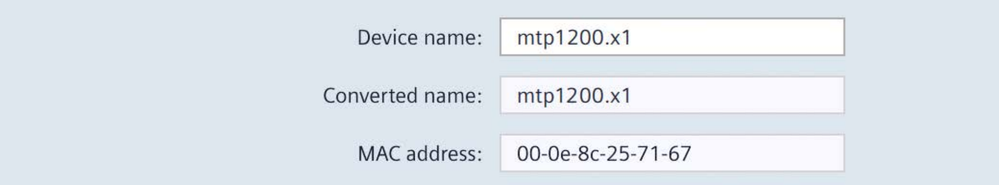
The interface name is displayed above the settings.

The settings under "Network settings" are retained after a restart or update of the operating system.

In the following cases, the settings under "Network settings" are not retained:

- If the HMI device is reset to factory settings, all settings will be reset to their default values.
- When a project with changed network settings is loaded to the HMI device, the values from the project are applied.

PROFINET



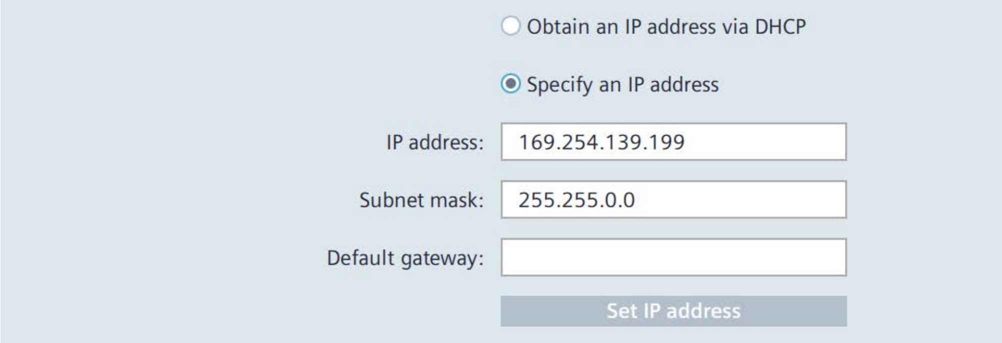
Device name: mtp1200.x1

Converted name: mtp1200.x1

MAC address: 00-0e-8c-25-71-67

- "Device name": PROFINET name of the interface. It may not contain any spaces and must be unique in the local network.
- "Converted name": Display field with the PROFINET name of the interface. It contains the entry under "Device name", automatically converted according to PROFINET naming conventions.
- "MAC address": Display field with the MAC address of the X1 interface of the HMI device.

IP address



○ Obtain an IP address via DHCP

● Specify an IP address

IP address: 169.254.139.199

Subnet mask: 255.255.0.0

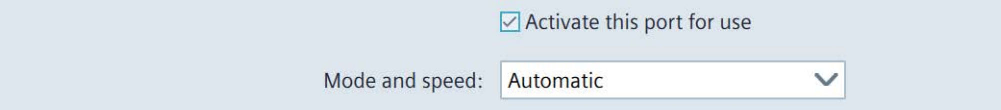
Default gateway:

- "Obtain an IP address via DHCP" (default setting): Option to automatically assign the IP address via the DHCP server.
- "Specify an IP address": Option to manually assign the IP address.
- "IP address": IP address of the X1 interface The IP address must be unique in the local network.
- "Subnet mask": Subnet mask for the IP address of the X1 interface.
- "Default gateway": IP address of the gateway (router) if several different local networks are used.
- "Set IP address": Button for saving the specified IP address parameters.

Note

If you select the option "Specify an IP address via DHCP", this setting is not overwritten when the project is loaded. If you select the option "Specifiy an IP address", you can also configure the network address in the WinCC device configuration and load it to the HMI device together with the project.

Ethernet parameters Port



☑ Activate this port for use

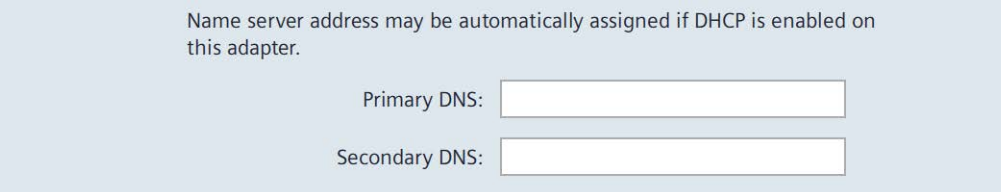
Mode and speed: Automatic

- "Activate this port for use": Option to enable or disable the port. The default setting is "activated".
- "Mode and speed": List for selecting the transmission mode and transmission speed for the interface.

  Selection options:
  - "Automatic" (default setting)
  - "10Mbps / HDX" (10 Mbps, half duplex)
  - "10Mbps / FDX" (10 Mbps, full duplex)
  - "100Mbps / HDX" (100 Mbps, half duplex)
  - "100Mbps / FDX" (100 Mbps, full duplex)

  The preferred default setting is "Automatic".

Name servers



Name server address may be automatically assigned if DHCP is enabled on this adapter.

Primary DNS:

Secondary DNS:

- "Primary DNS": Address of the primary DNS server.
- "Secondary DNS": Address of the secondary DNS server.

If you have activated the "Obtain an IP address via DHCP" option under "IP address", the specifications under "Name servers" are optional.

Security 5

5.1 User management

A convenient user management is available to you under "User management". The user management is configured in WinCC, transferred to the HMI device and managed on the HMI device.

Web access is also available for user management, see "Web access to the HMI device (Page 46)".

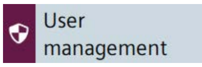
Note

Important information on the configuration and project transfer

- If you do not assign a user a role or a role and no function right in the configuration, the user or the role is not loaded to the device.

  In WinCC, configure all roles required on the HMI device with all function rights required on the HMI device. Assign each role required on the HMI device to at least one user.
- To transfer the user management from WinCC to the HMI device, the option "Keep current user management data in runtime" must be **disabled** in the "Load preview" dialog during project transfer .

You can find detailed information on configuration in the TIA Portal Help under "Visualizing processes (RT Unified) > Configuring users and roles (RT Unified)".



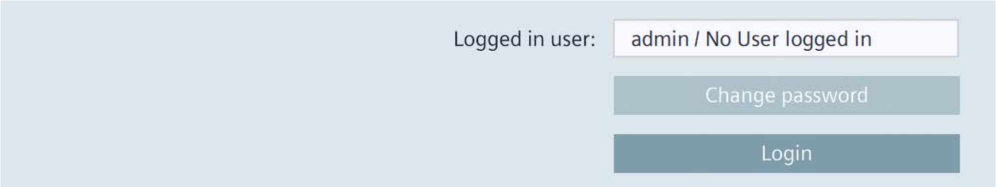
The complete user list is only visible and editable for users who have been assigned the "User management" function right in the configuration.

Users with other function rights see their own entry in the user list and can only use the buttons in the "Current user" area.

When password protection is enabled for the Control Panel, only users with the "Control Panel access" function right can access the Control Panel.

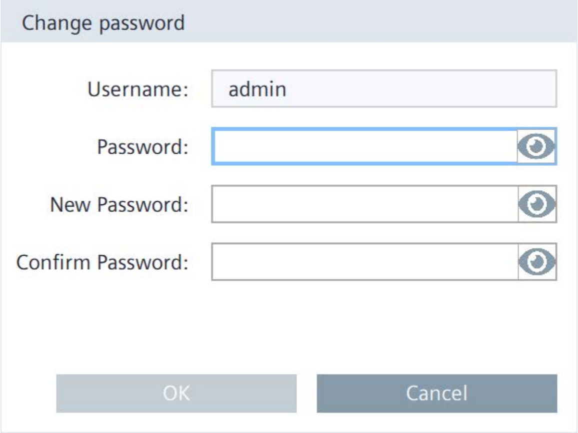
The password guidelines are specified during configuration. The function rights of a user are valid for the Control Panel as well as for the runtime software.

Current user


Logged in user: admin / No User logged in

- "Logged in user": Displays the login name of the user currently logged in. If no user is logged in yet, then "No User logged in" is displayed.

- "Change password": Button to change the password for the user currently logged in. After pressing the button, the "Change password" dialog is displayed.

  Change password

  Username: admin

  Password:

  New Password:

  Confirm Password:

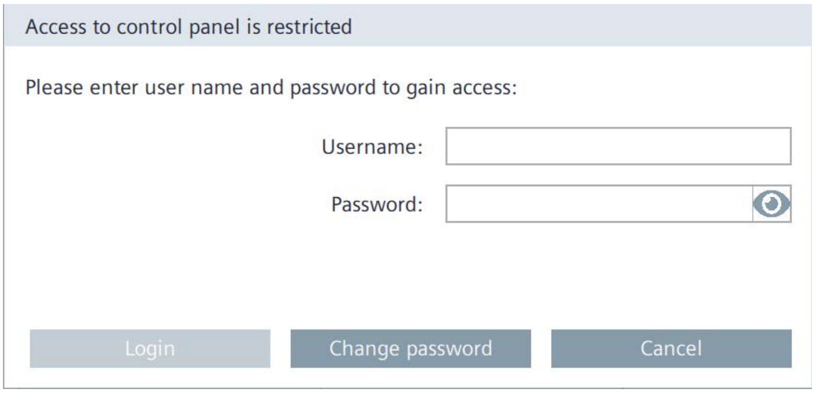
  Enter the previous password once and the new password twice. The following button can be used to make the passwords visible for the display duration of the dialog box:

  👁

- "Change user": Button for changing the current user.

  "Login": Button for logging in a user.

  After pressing the button, the "User Login" dialog is displayed.

  Access to control panel is restricted

  Please enter user name and password to gain access:

  Username:

  Password:

  Enter the desired login name with the associated password and log in using the "Login" button.

Note

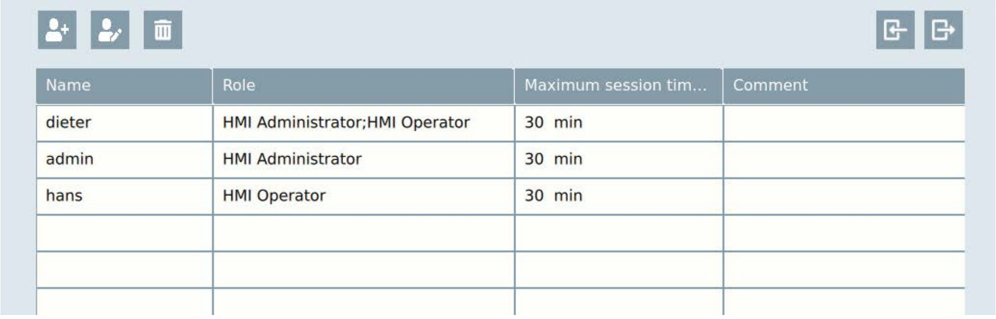
Number of login attempts

The number of attempts for the correct entry of the login credentials can be configured in WinCC under "Runtime settings > Security".

If the login credentials are entered incorrectly one more time, the user involved will be locked. The user must be deleted and recreated, or you must reload the User Management into the HMI device.

Ensure you enter the login credentials correctly.

Users



Name	Role	Maximum session tim...	Comment
dieter	HMI Administrator;HMI Operator	30 min	
admin	HMI Administrator	30 min	
hans	HMI Operator	30 min	

- Above the user list are the following buttons with the following functions for users with the "User management" function right:

👤+	Create a new user.
👤✎	Edit data of the user currently selected in the list.
🗑	Delete the user currently selected in the list.
⇦	Import complete user management from a ".json" file on an external storage medium. [1] Note: Import completely overwrites the user management on the HMI device.
⇨	Export complete user management to a ".json" file on an external storage medium. [1]

[1] For importing and exporting the user management, the "User management" function right is required; the "Import and export users" function right, which can be configured in WinCC, is not required.

- The user list displays the users available on the HMI device with the following user characteristics:
  - "Name": Login name of the user.
  - "Role": Roles assigned to the user.
  - "Maximum session timeout": This value indicates the number of minutes after which the user is automatically logged off if they no longer perform any operator action.

    Value range: 0 to 600 minutes (0 = automatic logout disabled).
  - "Comment": Comment text for the user.

Note

You cannot edit or delete yourself as a user.

To ensure that at least one user with the "User management" function right remains on the HMI device, users cannot edit or delete themselves. A second user with the "User management" function right is required for this purpose.

Note

Maximum session timeout

In the Engineering System, you can configure a maximum session duration for a role as well as for a user. If these values differ, only the smaller of the two values is transferred to the Panel during loading.

Creating or editing users

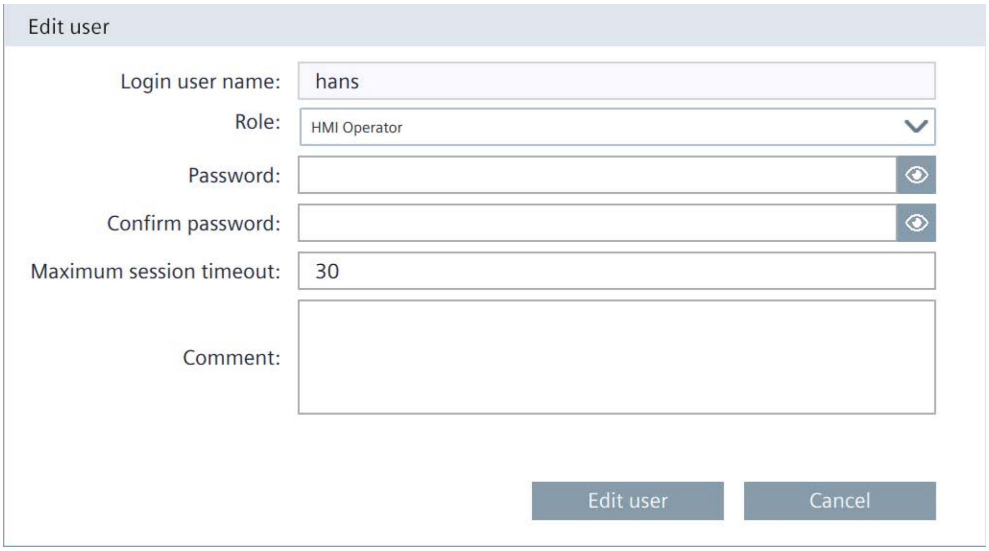
The editing functions are only available for users who have been assigned the "User management" function right in the configuration.

Use the following button to create a new user:

With the following button you edit the data of a user:

After pressing one of the two buttons, the dialog "Add user" or the dialog "Edit user" is displayed. Both dialog boxes are identical in content.

The following figure shows an example of the "Edit user" dialog box.



Edit user

Login user name: hans

Role: HMI Operator

Password:

Confirm password:

Maximum session timeout: 30

Comment:

- "Login user name": Display field with the login name of the user.
- "Role": Drop-down list for assigning the user to one or more roles. The roles are defined in the WinCC project for the HMI device and assigned the corresponding function rights.

The following system-defined roles are always transferred to the HMI device:

Role designation	Authorization in the Control Panel	Authorization in Runtime
HMI Operator	-	Web access, Operate, Monitor
HMI Monitor	-	Web access, Monitor
HMI Monitor Client	-	Web access, monitoring without influencing the processes in the controller
HMI Administrator	User management, Import and export users, Control panel access	Remote access, Monitor, Operate, Web access

The drop-down list also contains the configured roles that were transferred from the WinCC project to the HMI device.

Note

The HMI role "HMI Monitor Client" is superior to all other roles and their function rights. A user to whom the role "HMI Monitor Client" is assigned gets the function rights of only that role. Any superior function rights of other roles that are assigned to the user will be lost.

You can find detailed information on users, roles, and function rights in the TIA Portal Help.

- "Password": Text box for the password of the user. If you do not enter anything, the user's existing password remains unchanged.
- "Confirm password": Text box for confirming the password.
- "Maximum session timeout": This value indicates the number of minutes after which the user is automatically logged off if they no longer perform any operator action.

  Value range: 0 to 600 minutes (0 = automatic logout disabled).
- "Comment": Note on changing the user.
- "Edit user" or "Add user" Button for saving the user.
- "Cancel": Button for discarding the changes.

5.2 Certificates

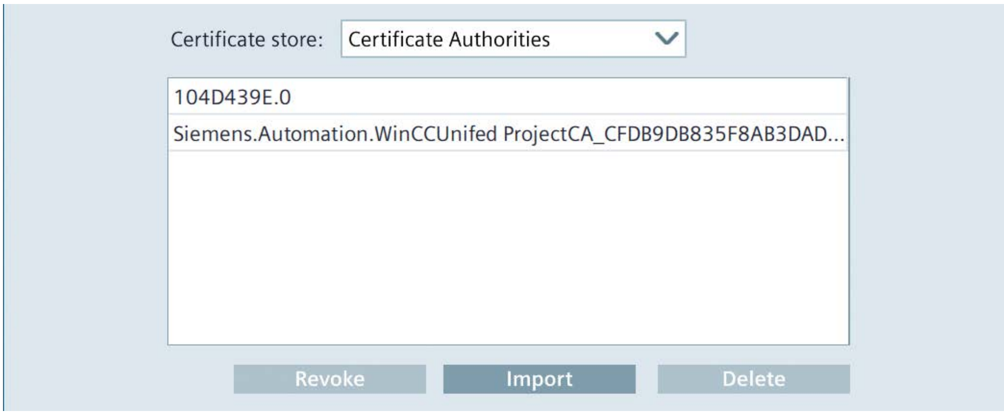
You can use this function to import, display and delete certificates and certificate revocation lists.

Certificates

A digital certificate consists of structured data, which confirms ownership and other properties of a public key.

When handling certificates, note the information on Industrial Security (Page 45).

Certificates on the device



Certificate store: Certificate Authorities

104D439E.0

Siemens.Automation.WinCCUnifed ProjectCA_CFDB9DB835F8AB3DAD...

- "Certificate store": Drop-down list for the following certificate categories:
  - "Certificate Authorities": Trusted root certificate authorities and intermediate certificate authorities.
  - "My Certificates": Application certificates, such as for OPC UA client/server communication.
  - "Other Certificates": Self-signed end entity certificates and trusted end entity certificates.
  - "Certificate Revocation Lists" for certificate revocation lists.
- The certificate list displays the certificates of the selected category.

  If you select an entry in the list, then the "Certificate details" for certificates or the "CRL details" for certificate revocation lists are displayed below the list.
- "Revoke": Button to mark a certificate as not trustworthy. This function is only available in the "Other Certificates" certificate category.

  "Trust": Button to mark a certificate as trustworthy. This function is only available in the "Other Certificates" certificate category.
- "Import": Button for importing one or more certificates from a data storage medium.

Note

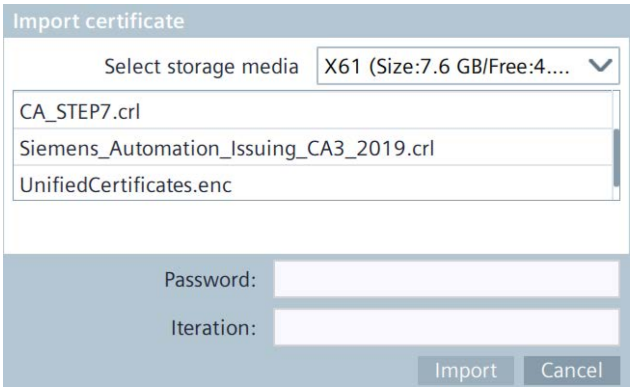
Supported file formats for certificates

The import function supports certificate files of type ".enc", ".der", ".crl" and ".pem".

Files of type ".enc" are exported from the "WinCC Unified Certificate Manager" and contain a collection of keys, certificates and CRLs.

If you want to import an individual cryptographic file, the supported formats for CER and CRL files end in ".pem" and ".der". The individual file should have a CA certificate or a CRL with extension ".der", ".crl" or ".pem".

The "Import certificate" dialog is displayed after the "Import" button has been pressed.



Import certificate

Select storage media: X61 (Size:7.6 GB/Free:4....

CA_STEP7.crl
Siemens_Automation_Issuing_CA3_2019.crl
UnifiedCertificates.enc

Password:

Iteration:

Select the storage medium and certificate file and import the certificate file using the "Import" button.

When you import an encrypted certificate with the ".enc" file extension, enter the following additional data:

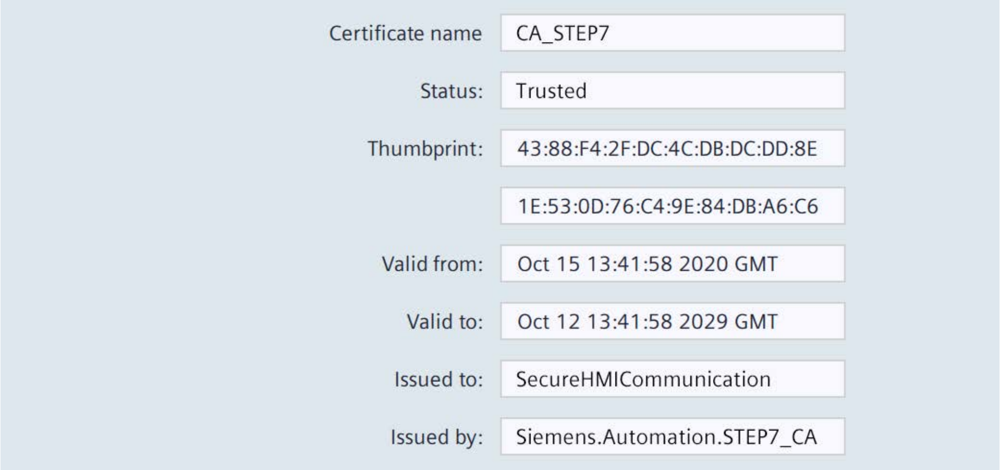
  – "Password": The encryption password that was specified when the certificate was generated.
  – "Iteration": The iteration count that was specified when the certificate was created.

- "Delete": Button to delete the currently selected certificate in the certificate list.

Note

The selected certificate is deleted immediately without prompt.

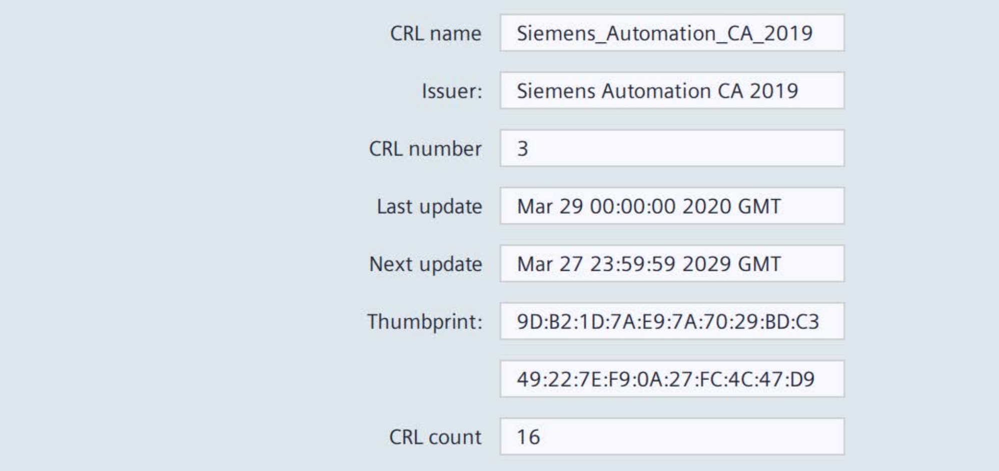
Certificate details



Certificate name: CA_STEP7
Status: Trusted
Thumbprint: 43:88:F4:2F:DC:4C:DB:DC:DD:8E 1E:53:0D:76:C4:9E:84:DB:A6:C6
Valid from: Oct 15 13:41:58 2020 GMT
Valid to: Oct 12 13:41:58 2029 GMT
Issued to: SecureHMICommunication
Issued by: Siemens.Automation.STEP7_CA

- "Certificate name": Name of the certificate.
- "Status": Status of the certificate on the HMI device ("Trusted" or "Revoked"). This display field is only available in the certificate category "Other Certificates".
- "Thumbprint": Character string to prove the authenticity of the certificate.
- "Valid from": Start of the validity of the certificate.
- "Valid to": End of the validity of the certificate.
- "Issued to": Recipient of the certificate.
- "Issued by": Issuer of the certificate.

CRL details

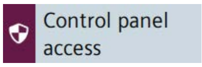


CRL name	Siemens_Automation_CA_2019
Issuer:	Siemens Automation CA 2019
CRL number	3
Last update	Mar 29 00:00:00 2020 GMT
Next update	Mar 27 23:59:59 2029 GMT
Thumbprint:	9D:B2:1D:7A:E9:7A:70:29:BD:C3
	49:22:7E:F9:0A:27:FC:4C:47:D9
CRL count	16

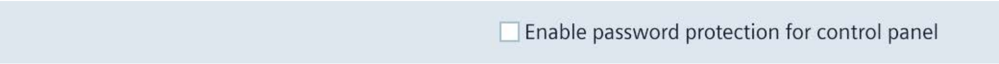
- "CRL name": Designation of the certificate revocation list.
- "Issuer": Issuer of the certificate revocation list.
- "CRL number": Consecutive version number of the certificate revocation list.
- "Last update": Time of creation of this certificate revocation list.
- "Next update": Time of creation of the next certificate revocation list.
- "Thumbprint": Character string to prove the authenticity of the certificate revocation list.
- "CRL count": Number of entries in the certificate revocation list.

5.3 Control panel access

Under "Control panel access" you can protect access with a password on the Control Panel. Only users who have been assigned the "Control Panel access" function right in the configuration can change the password protection.



Control panel access

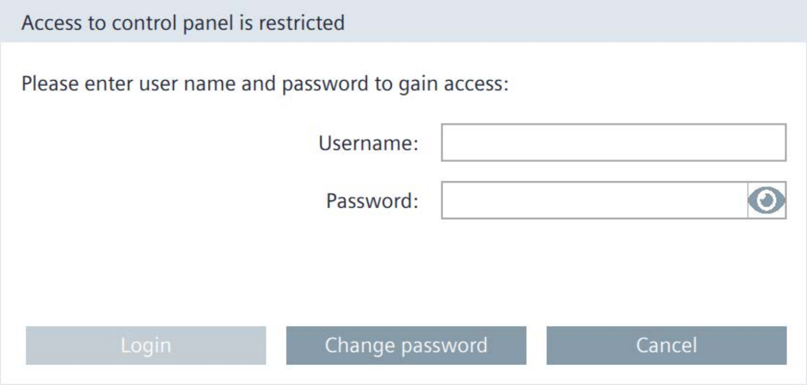


□ Enable password protection for control panel

- "Enable password protection for control panel": Option to enable password protection for the Control Panel.

  The password protection can only be activated or deactivated by users who have been assigned the "Control Panel access" function right in the configuration.

  If you are not yet logged in as a user with the "Control Panel access" function right and enable the option "Enable password protection for control panel", the "Access to control panel is restricted" dialog is displayed.



Access to control panel is restricted

Please enter user name and password to gain access:

Username:

Password:

Log in as a user with the "Control Panel access" function right to activate the password protection for the Control Panel. Use the following button to make the password visible for the display duration of the dialog:

👁

Note

Number of login attempts

The number of attempts for the correct entry of the login credentials can be configured in WinCC under "Runtime settings > Security".

If the login credentials are entered incorrectly one more time, the user involved will be locked. The user must be deleted and recreated, or you must reload the User Management into the HMI device.

Ensure you enter the login credentials correctly.

Note

Password protection of the Control Panel and project transfer

When access to the Control Panel is protected, you must ensure that the user management has been configured correctly in the TIA Portal before transferring a project again. This means:

- A user with "Control Panel access" right has been configured.
- When central user management is being used, all data for accessing the UMC server has been entered correctly.

Recommendation:

- Before loading again, disable the "Enable password protection for control panel" option.
- After loading, verify that the user with the "Control Panel access" right can log in. If this is not the case, correct the configuration of the user management.
- Enable the "Enable password protection for control panel" option again.

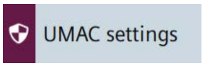
If you are logged in as a user with the "Control Panel access" functional right, the "Access to control panel is restricted" dialog is no longer displayed when accessing the Control Panel.

If you are not logged in or do not have the "Control Panel access" function right, the "Access to control panel is restricted" dialog is displayed when accessing the Control Panel.

Access to the Control Panel can be triggered directly in the Control Panel or via a system function of the Runtime software.

5.4 UMAC settings

Under "UMAC settings", you can see whether local or central user management is used on the HMI device.



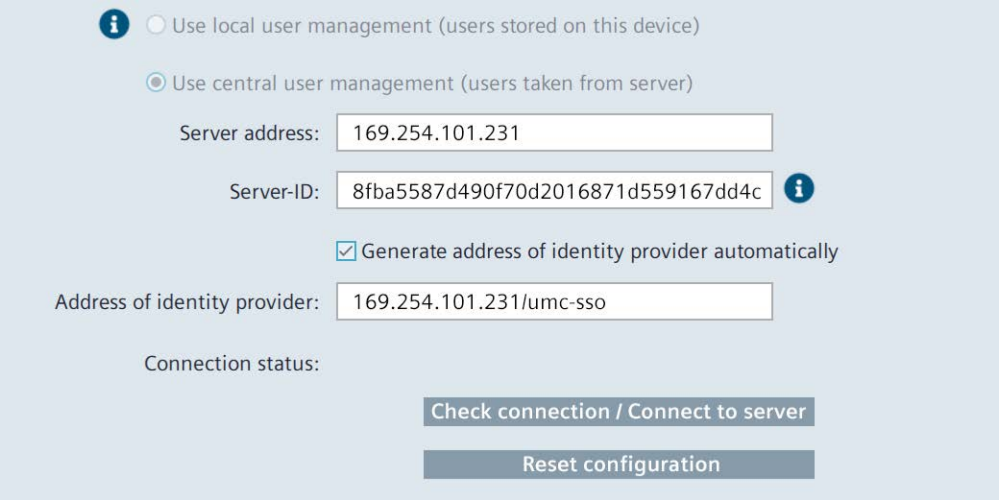
The local or central user management is configured in WinCC and transferred to the HMI with the download.

Note

You can only switch between local and central user management in WinCC.

When loading the central user management, all local users on the HMI device are deleted.

Configuration of user management



○ Use local user management (users stored on this device)

● Use central user management (users taken from server)

Server address: 169.254.101.231

Server-ID: 8fba5587d490f70d2016871d559167dd4c

☑ Generate address of identity provider automatically

Address of identity provider: 169.254.101.231/umc-sso

Connection status:

- "Use local user management (users stored on this device)": Information that local user management is used. The data in this window cannot be edited; the users are managed locally under "Security" > "User management".
- "Use central user management (users taken from server)": Information that central user management is used. The connection settings are configured in WinCC and transferred to the device during loading. The settings on the HMI device can be adjusted, if required.

Meaning of the connection settings for central user management:

- "Server address": IP address or device name of the UMC server.
- "Server-ID": Unique string for identification of the UMC server. You can enter the server ID manually or have it determined automatically during connection setup.
- "Generate address of identitiy provider automatically": Option for automatic generation of the address of the ID provider on the UMC server. The default setting is "enabled". Disable this option if you do not want to use the UMC server but a different server as ID provider. This may be necessary when using a server farm, for example.
- "Address of identity provider": Address of the ID provider either generated automatically via the option "Generate address of identitiy provider automatically" or entered manually, if necessary.
- "Connection status": Connection status to the UMC server, possible values:
  - <empty>: The connection to the UMC server has not been tested yet.
  - "Connected": The connection to the UMC server has been established and tested.
  - "Not connected" - <error message>: There is no connection to the UMC server. The <error message> provides information about the possible cause.
  - "Connection not possible" - <error message>: The connection to the UMC server could not be set up. The <error message> provides information about the possible cause.
- "Check connection": Button to check the connection to the UMC server.
- "Connect to server": Button to set up the connection to the UMC server.
- "Reset configuration": Button to delete the connection settings.

Establishing a connection to the central user management

When all connection settings have been configured correctly and transferred with the project to the HMI device, the HMI device is automatically connected to the central user management. No value is specified under "Connection status" because the connection has not been checked yet. Press the "Check connection" button to check the connection.

When the central user management has not been configured completely or is incorrect, you can adjust the settings on the HMI device. Press the "Connect to Server" button to connect the device to the central user management.

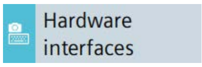
When the connection was set up successfully, the "Connected" information is displayed under "Connection status". The "Connect to server" button turns into "Check connection".

You can find more information in the TIA Portal Help under "Visualizing processes (RT Unified) > Configuring users and roles (RT Unified)".

External Devices and Input 6

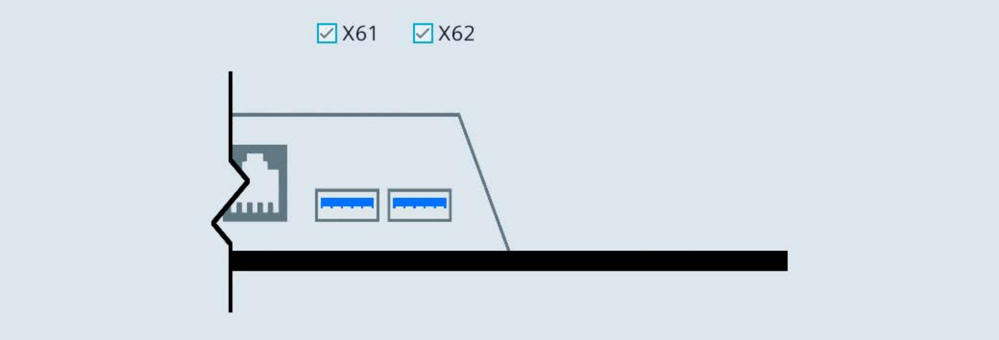
6.1 Hardware interfaces

Under "Hardware interfaces", change the settings for accessing the storage media interfaces.



You can deactivate one or more interfaces to protect the HMI device from unauthorized external access.

Activate USB ports



☑ X61 ☑ X62

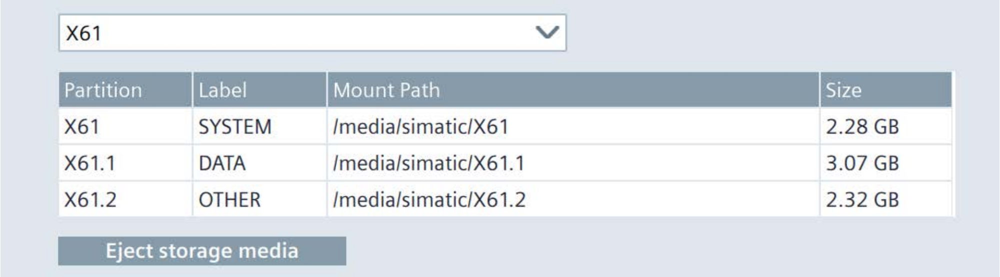
- "X61": Option to activate or deactivate the USB port X61.
- "X62": Option to activate or deactivate the USB port X62.

Default setting for all USB ports is "activated".

6.2 Connected devices

Under "Connected devices" you can show information on the storage media that are connected to the HMI device.

Select storage media



Partition	Label	Mount Path	Size
X61	SYSTEM	/media/simatic/X61	2.28 GB
X61.1	DATA	/media/simatic/X61.1	3.07 GB
X61.2	OTHER	/media/simatic/X61.2	2.32 GB

The drop-down list box shows all the storage media at the interfaces of the HMI device.

Select an entry to display detailed information on a storage medium in the partition list.

- This partition list contains the following information:
  - "Partition": Name of the partition. The first partition carries the designation of the interface to which the storage medium is connected, for example "X61".

    If more partitions are present on the storage medium, they are numbered successively and shown delimited by a period below the first partition, for example, "X61.1".
  - "Label": Designation of the partition that was selected at the time of formatting.
  - "Mount Path": Path via which the HMI device accesses the partition.
  - "Size": Size of the partition.

  The unpartitioned area of a storage medium is not displayed.
- "Eject storage media": Button for securely removing the selected storage medium.

Note

Behavior of the "Eject storage media" function

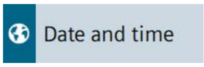
- If data is still being accessed on the storage medium, the storage medium cannot be removed reliably. A corresponding error message is displayed. Confirm the error message with "OK" and execute the function again when the data access has ended.
- After secure removal, the HMI device cannot access the storage medium. For renewed access, the HMI device must be restarted or the storage medium plugged in again. A corresponding warning is displayed. Confirm with "OK" or cancel the action with "Cancel".
- After secure removal, the storage medium is not present in the selection list any more, and all the relevant entries in the partition list are removed.

Language, Region and Formats

7

7.1 Date and time

Under "Date and time", set the date, time, and time zone for the HMI device manually or via a time server on the network.



Date and time

NOTICE

Setting the date and time correctly

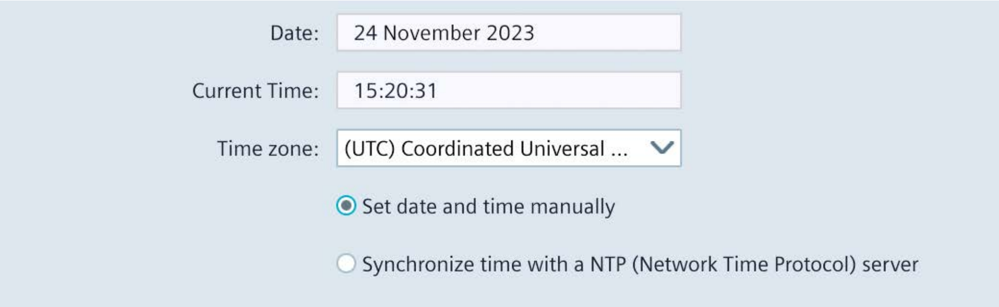
When the date and time are not set correctly, malfunctions may occur in the plant. To prevent malfunctions, set the date and time of the HMI device and all controllers connected to the HMI device to the correct values or use an NTP server for time synchronization. Check the correct settings for date and time after every update of the operating system.

NOTICE

Time synchronization required for time-dependent reactions

A malfunction may occur in the plant if the date and time are not synchronized and time-dependent reactions are triggered in the plant via the HMI device. To avoid malfunctions, use automatic time synchronization via one or more NTP servers.

Date and time



Date: 24 November 2023

Current Time: 15:20:31

Time zone: (UTC) Coordinated Universal ...

● Set date and time manually

○ Synchronize time with a NTP (Network Time Protocol) server

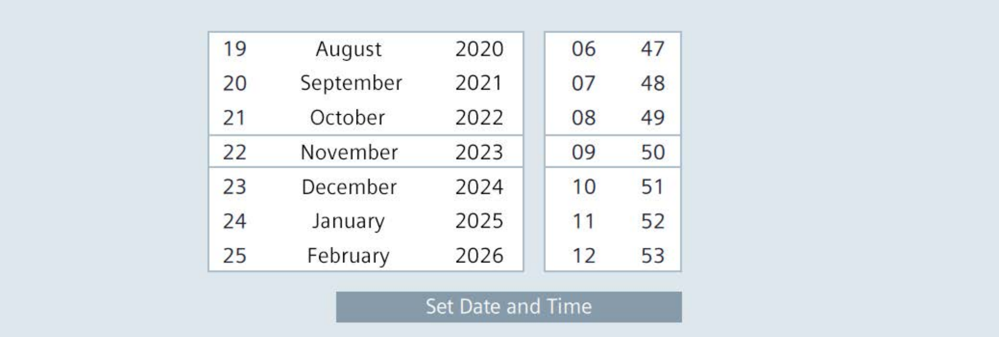
- "Date": Display field with the current date.
- "Current Time": Display field with the current clock time.
- "Time zone": Selection list for the desired time zone.

Note

Automatic daylight saving/standard time switchover

If you select a time zone in which there is a switchover between daylight saving and standard time, the switchover takes place automatically on the relevant date.

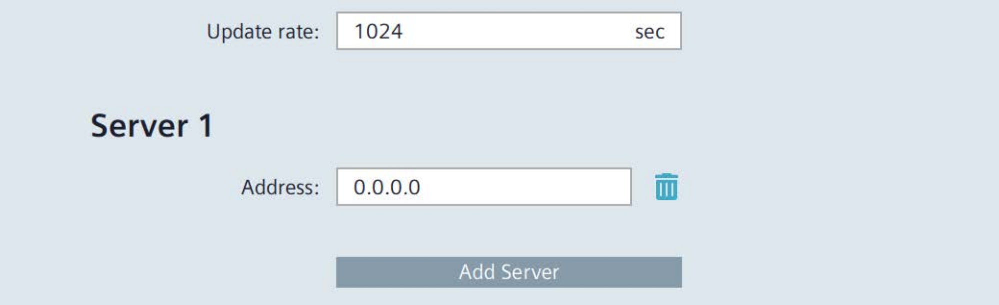
- "Set date and time manually" (default setting): Option for manual time setting on the HMI device. If you select this option, the following list is displayed below the options:



19	August	2020	06	47
20	September	2021	07	48
21	October	2022	08	49
22	November	2023	09	50
23	December	2024	10	51
24	January	2025	11	52
25	February	2026	12	53

  Set the day, month, year and time by scrolling the respective list column so that the desired date and time are displayed in the framed line in the middle of the list. The "Set Date and Time" button is used to save the setting.

- "Synchronize time with a NTP (Network Time Protocol) server": Option for automatic time synchronization via an NTP server. If you select this option, the following parameters for specifying time synchronization via NTP servers are displayed below the options:



Update rate: 1024 sec

Server 1

Address: 0.0.0.0

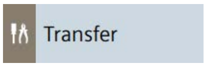
  Enter the desired synchronization interval under "Update rate", value range 10 to 86400 seconds (1 day). After the input, the value is rounded to the nearest power of two based on the internal format.

  Add at least one and a maximum of four NTP servers using the "Add Server" button. Specify the IP address for each NTP server and make sure that the device is set up as an NTP server.

8 Service and Commissioning

8.1 Transfer

Under "Transfer" you define whether and how data is transferred from a configuration PC to the HMI device.



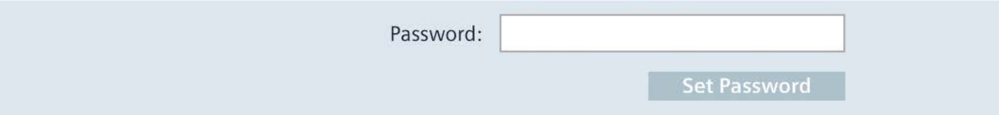
Transfer mode

☑ Enable transfer

- "Enable transfer": Option to enable or disable data transfer to the HMI device. The default setting is "enabled".

  If you disable the transfer, you protect the HMI device against unintended update of the operating system and overwriting the project data.

Encrypted project transfer



- "Password": Password for the encrypted transfer of the project. The password must match the password that was specified in the configuration under the runtime settings of the HMI device.

  To enter the password, tap the entry field.
- "Set Password": Button to save the password for the encrypted project transfer.

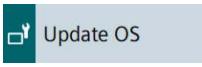
As an alternative, you can transfer the password unencrypted during the initial loading of the project.

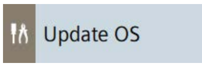
8.2 Update OS

The firmware and operating system version of the HMI device must be compatible with the firmware and operating system version of the installed WinCC software. If this is not the case, then you must update the operating system.

Use "Update OS" to update the operating system of the HMI device. The operating system is contained in several firmware files. The master file has the extension ".fwf". The number of additional files varies; these files have the file name of the master file and a sequential number (".0", ".1", ".2", etc.) as an extension.

The "Update OS" function is available under both "System Properties" and "Service and Commissioning".





NOTICE

Updating the operating system deletes data on the HMI device

Project, parameter sets and user administration will be deleted when you update the operating system on the HMI device.

Before updating the operating system, backup the data on the HMI device, if necessary.

All settings, except the following settings which you changed in the Control Panel before updating the operating system, are retained even after the update of the operating system:

- The external interfaces become activated again (default setting), see section "Hardware interfaces (Page 33)".
- The time zone is reset to the default setting "(UTC) Coordinated Universal Time", see section "Date and time (Page 35)".

Use an industrial USB flash drive to load the firmware.

Firmware files for the HMI devices can be downloaded from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109746530). Observe the documentation included with the download.

Note

Do not rename firmware files

If you change the name of the firmware files, the operating system can no longer be updated with these firmware files. The firmware files become unusable. Leave the name of the firmware files unchanged.

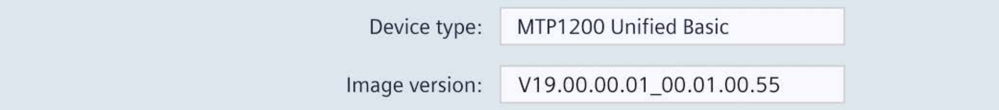
Note

Copy firmware files completely

If you copy the firmware files, be sure to also copy the master file ".fwf" together with all associated firmware files (".0", ".1", ".2", etc.).
If one of the files is missing, the operating system cannot be loaded.

Alternatively to the "Update OS" function in the Control Panel, you can use the "Update OS" function in WinCC.

Panel Information

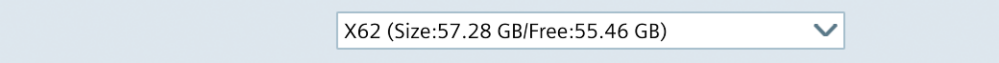


Device type: MTP1200 Unified Basic

Image version: V19.00.00.01_00.01.00.55

- "Device type": HMI device type designation.
- "Image version": Version of the firmware and operating system.

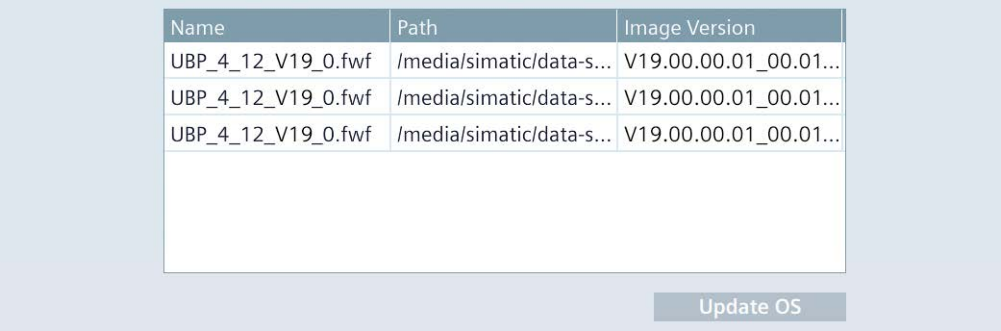
Select storage media for OS update



X62 (Size:57.28 GB/Free:55.46 GB)

Use the selection list to select the storage medium on which the firmware file is located.

Firmware files on external storage



Name	Path	Image Version
UBP_4_12_V19_0.fwf	/media/simatic/data-s...	V19.00.00.01_00.01...
UBP_4_12_V19_0.fwf	/media/simatic/data-s...	V19.00.00.01_00.01...
UBP_4_12_V19_0.fwf	/media/simatic/data-s...	V19.00.00.01_00.01...

- The list shows all firmware files that can be loaded into the HMI device.

  Select the desired firmware master file (.fwf) from the list.
- "Update OS": Button for starting the loading process.

  The HMI device restarts after the "Update OS" button is pressed. The loading process then begins.

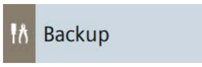
  A dialog with a progress bar is displayed on the HMI device for each firmware file.

  The HMI device is restarted again after the completion of the loading process.

  The main window of the Control Panel is displayed after the restart. The operating system on the HMI device is updated.

8.3 Backup

Under "Backup" you can back up the operating system, applications and data from the flash memory of the HMI device to an external storage medium.

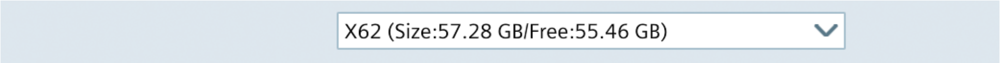


Use an industrial USB flash drive as the storage medium.

Depending on the amount of data on the HMI device, a backup may require up to 20 GB of memory. Make sure that the storage medium has sufficient free space. Recommendation: At least 5 GB of free space on the storage medium.

Do not turn off the HMI device during the backup process.

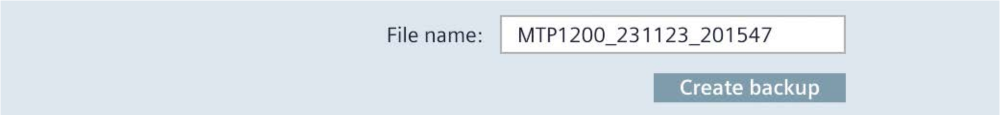
Select storage media



X62 (Size:57.28 GB/Free:55.46 GB)

Select the storage medium on which you want to back up the data.

Complete backup file



File name: MTP1200_231123_201547

- "File name": Name of the backup. Select a name that best identifies the backup.
  A backup includes multiple files. The master file has the extension ".brf". The number of additional files varies; these files have the file name of the master file and a sequential number (".0", ".1", ".2", etc.) as an extension.
- "Create backup": Button to start the backup process.

  After the "Create backup" button has been pressed, the system checks whether a backup with the name specified under "File name" already exists on the storage medium. If yes, then a warning is displayed. Select "OK" to overwrite the backup or "Cancel" to specify a different name for the backup.

  The backup process starts with a restart of the HMI device, followed by the data backup.

  During the data backup, a folder with the name of the backup is created in the root directory of the selected storage medium. The backup files are saved in this folder. A dialog with a progress bar is displayed for each backup file.

  The HMI device is restarted again after the completion of the backup process.

  The main window of the Control Panel is displayed after the restart.

The data of the HMI device are saved on the storage medium.

Note

Do not rename backup files on the data storage medium

If you change the name of the backup files on the data storage medium, these backup files can no longer be loaded into the HMI device using the "Restore" function.

Leave the name of the backup files on the data storage medium unchanged.

Note

Copy backup files completely

If you copy the backup files, be sure to also copy the master file ".brf" together with all associated backup files (".0", ".1", ".2", etc.).

If one of the files is missing, the backup cannot be loaded.

8.4 Restore

Under "Restore", you can restore the backup of an HMI device from a storage medium.

Remote access to the HMI device is not possible during the restore process.

A restore operation deletes the flash memory of the HMI device on confirmation. The data backed up on the storage medium is then transferred.

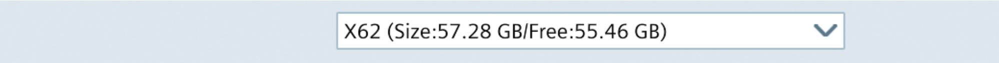
NOTICE

Data loss

All data on the HMI device, including the project and HMI device password, is deleted during a restore operation. License keys are only deleted after a security prompt.

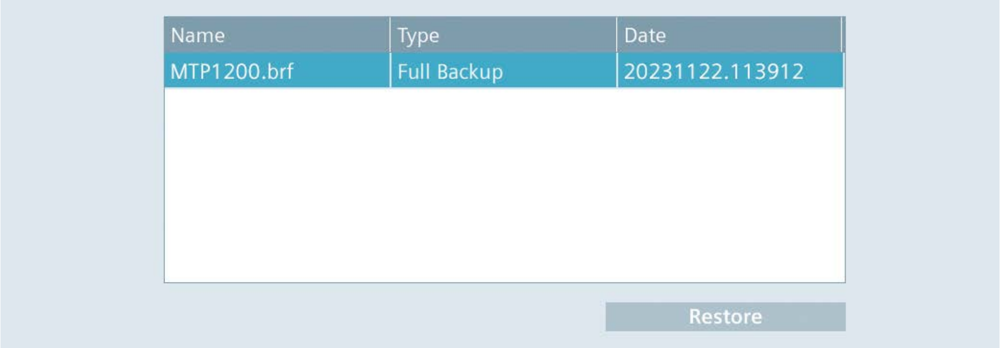
Back up your data before the restore operation, if necessary.

Select storage media


X62 (Size:57.28 GB/Free:55.46 GB)

Select the storage medium on which the backed-up data is stored.

Backup files



Name	Type	Date
MTP1200.brf	Full Backup	20231122.113912

- The list shows all backups that can be loaded to the HMI device.

  Select the desired backup from the list.
- "Restore": Button to start the restore process.

  The HMI device restarts after the "Restore" button is pressed. The restore process then begins.

  Do **not** switch off the HMI device during the restore process and do **not** disconnect the data source from the HMI device.

  During the restore process, a dialog with a progress bar is displayed for each backup file loaded.

  The HMI device is restarted again after the completion of the restore process.

  The main window of the Control Panel is displayed after the restart.

The data from the storage medium is now restored on the HMI device.

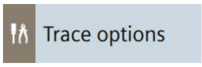
Note

System behavior when the process is interrupted

If the restore process cannot be completed due to a power failure or an interrupted data connection, for example, the HMI device starts in maintenance mode and the factory settings must be restored.

8.5 Trace options

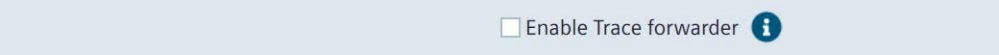
You specify whether or not trace outputs are displayed and backed up on an external storage medium under "Trace options".


Trace options

Note

The settings of the "Trace options", i.e. the settings for "Trace forwarder" and "Trace logger", are retained after restarting the HMI device or updating the operating system.

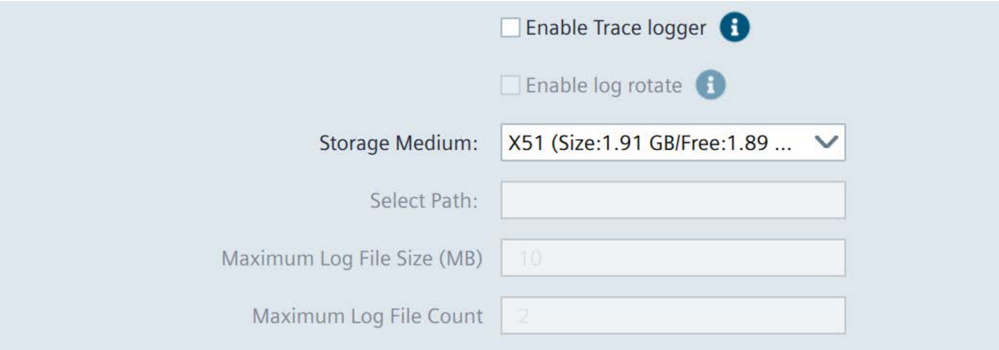
Trace forwarder


□ Enable Trace forwarder

- "Enable Trace forwarder": Option to enable or disable the "tracing" service. The default setting is "deactivated".

  Enable "Tracing" for diagnostics and service purposes, e.g. to display trace outputs from scripts. If you start the HMI device in maintenance mode, the "Tracing" function is automatically enabled. You can find additional information in FAQ Entry 109777593 on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109777593).

Trace logger


□ Enable Trace logger

□ Enable log rotate

Storage Medium: X51 (Size:1.91 GB/Free:1.89 ...

Select Path:

Maximum Log File Size (MB) 10

Maximum Log File Count 2

- "Enable Trace logger": Option to back up "tracing" information on an external storage medium. The default setting is "deactivated".
- "Enable log rotate": Option for activating the "Log rotate" function. The default setting is "deactivated". This option can only be activated in conjunction with "Enable Trace logger".

  If "Log rotate" is activated, then the "tracing" information is successively saved in several files with a specified size ("Maximum Log File Size") on the selected storage medium. If the maximum size of the first log file is reached, then another log file is automatically created, which is written to. When the maximum size of the last log file ("Maximum Log File Count") has been reached, the oldest log file at that time will be deleted and a new log file will be created to back up the further "tracing" information.

- "Storage Medium": Storage medium on which the "tracing" information is to be backed up.
- "Select Path" (optional): Path to location where the "tracing" information is to be backed up. The name of the path must begin with "**/**" and may contain only Latin characters and **none** of the following special characters: **! # $ % & ( ) * + , : ; < = > ? @ [ ] _ { | } ~ ^**

  Log files on the selected storage medium

  The log files with the "tracing" information are always saved in a subdirectory "/TraceLogs" on the selected storage medium.

  If no path is specified, you can find the log files in the "/TraceLogs" directory.

  If a path is specified, you can find the log files here "/<path>/TraceLogs" directory.

  In the figure above, the path "/traces" is given as an example. You can find the relevant log files under "/traces/TraceLogs".

  Names of the log files

  The log files are named, with the date and time, according to the following syntax:
  `TraceLogs-YYYY-MM-DD-T_HH_MM_SS.log`
- "Maximum Log File Size (MB)": Maximum size of a log file in megabytes. Permitted range: 10 MB to 2000 MB. Default setting: 10 MB.
- "Maximum Log File Count": Maximum number of log files that can be created.
  - Minimum value: 2 (default setting).
  - The maximum value results from the size of the free storage space on the selected storage medium.

  If the product of the values specified under "Maximum Log File Size (MB)" and "Maximum Log File Count" exceeds the size of the available storage space on the selected storage medium, then the values are marked as incorrect and must be corrected.

Appendix A

A.1 Industrial Security

Industrial Security

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under (https://www.siemens.com/industrialsecurity).

Disclaimer for third-party software updates

This product includes third-party software. Siemens Aktiengesellschaft only provides a warranty for updates/patches for the third-party software if such updates/patches have been distributed as part of a Siemens software update service contract or officially released by Siemens Aktiengesellschaft. Otherwise, updates/patches are undertaken at your own risk. You can find more information about our Software Update Service offer on the Internet at Software Update Service (https://support.industry.siemens.com/cs/ww/en/view/109759444).

Notes on protecting administrator accounts

A user with administrator privileges has extensive access and manipulation options in the system.

Therefore, ensure there are adequate safeguards for protecting the administrator accounts to prevent unauthorized changes. To do this, use secure passwords and a standard user account for normal operation. Other measures, such as the use of security policies, should be applied as needed.

A.2 Notes on operation

Storage media

Note

Storage media displayed multiple times

The operating system of the HMI device supports multiple mount points. This means that USB storage media may be displayed multiple times in file browser dialogs. This does not affect the functionality of the HMI device.

Note

Directory for storage media in Runtime and in apps

You will find the storage media under "/media" in file browser dialogs of the Runtime software.

Note

Exporting Runtime data

Use a USB storage medium for exporting Runtime data such as the data from a alarm control or trend control.

If several USB storage media are connected to the HMI device, the storage medium at interface X61 is used for the export.

A.3 Web access to the HMI device

As an alternative to direct operation on the device, you can access the following applications of the HMI device via a browser:

- The runtime project
- The user management

The number of supported connections via Web client is 1.

Requirement

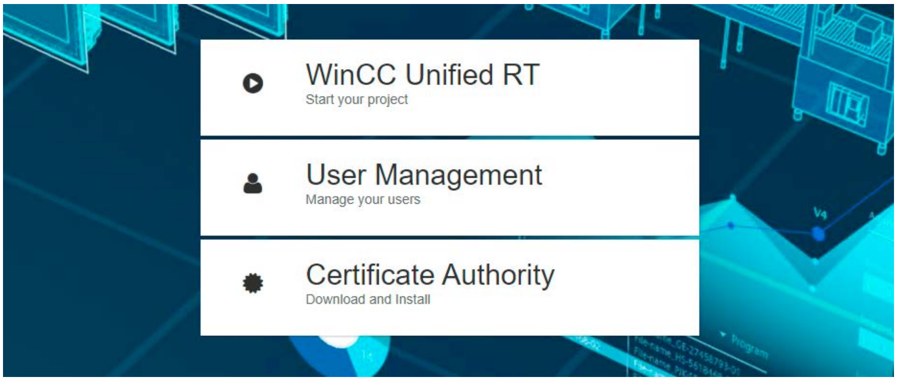
- The device on which the browser is running is connected to the HMI device in the same subnet.
- The browser used supports HTML5 and accepts self-signed certificates.
- The following applies depending on the application you want to access:
  - "WinCC Unified RT": Web access to the runtime project is activated, see section "Web client (Page 15)". The runtime software has been started.
  - "User Management": The settings for the user management were loaded to the HMI device, see sections "User management (Page 22)" and "UMAC settings (Page 31)".

Opening applications via the homepage

The HMI device has a convenient homepage for applications with web access.

To open the homepage, enter the following URL in the browser: **"https://<ip>"**

Use the IP address of the HMI device instead of the placeholder "<ip>".



- "WinCC Unified RT": Button for opening the "Sign in" dialog for runtime.
- "User Management": Button for opening the "Sign in" dialog for the user management.

  You can find detailed information on web-based user management via a browser in the TIA Portal Help under "Visualizing processes (RT Unified) > Configuring users and roles (RT Unified) > Using the user management on the Unified Comfort Panel > Managing local users > Managing local users in runtime".
- "Certificate Authority": Button for downloading the HMI device certificate for a secure connection.

Opening applications without the homepage

Use the following URLs to open the "Sign in" dialog in the respective application without the homepage.

- "WinCC Unified RT": "https://<ip>/device/WebRH", note the uppercase/lowercase spelling.
- "User Management": "https://<ip>/umc"

Use the IP address of the HMI device instead of the placeholder "<ip>". When you use a browser that runs directly on the HMI device, you can also use "localhost" instead of the IP address.

Installing a certificate

The following applies when you open an application with web access for the first time via a browser: To set up a secure connection between browser and application, you must download the certificate of the application and install it in your browser as "trusted".

NOTICE

Use CA certificates generated via the WinCC Unified Certificate Manager

If you use a self-signed certificate from a non-trustworthy source, the data transfer is not protected from attacks.

For web access to the HMI device, use CA-certificates that were generated via the WinCC Unified Certificate Manager. To do so, proceed as follows:

1. Generate a CA certificate with the WinCC Unified Certificate Manager .
2. Copy the CA certificate to a USB flash drive.
3. Import the CA certificate in the Control Panel via "Security">"Certificates" as "Trusted Certificate Authority".
4. Install the certificate in your browser as described in the following sections.

Download certificate

You have the following options to download the certificate:

- Using the "Certificate Authority" button on the homepage.
- By clicking on the icon or the "Not secure" message in the address bar of the browser.

Installing the certificate as "trusted" in the "Web Browser"

Follow the instructions in the browser documentation to import the application certificate and classify it as "trusted".

A secure connection to the website is now established with the trusted certificate.

Note

Certificate is valid for all applications with web access

For a secure connection to the applications with web access, the HMI device certificate must only be downloaded once and classified as "trusted".

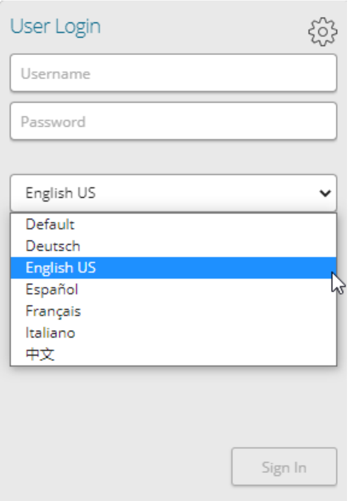
Sign in using the "Sign in" dialog

You use the "Sign in" dialog to sign in to an application with web access.

"Sign in dialog**" for runtime-related applications**

The following figure shows the "Sign in" dialog for the following applications.

- "WinCC Unified RT"
- "User Management"



Procedure:

1. Select the required runtime language.
2. Enter the user name and password.
3. Click "Sign in".

If the selected language is not available in the runtime project, the default language is used.

Notes on web access

After signing in, read the following notes on web access in the various applications:

"WinCC Unified RT"

After successful login, a user session is active. Note the following for user sessions:

- A maximum of one user session is permitted on one HMI device.
- User management is used in a user session when signing in. Changes to the user management of the HMI device have no effect on the session in progress.
- You have the following options to completely close a user session:
  - Configure an operating element with the system function "Log off".
  - Close all instances, that is, all open browser windows.

You can find more information on remote access via "Web client" in the TIA Portal Help under: "Visualizing processes (RT Unified) > Configuring remote access > Web client".

"User Management"

- The user list is only visible and editable for users who have been assigned the "User Management" function right.
- You can find detailed information on web-based access to the user management in the TIA Portal Help under "Visualizing processes (RT Unified) > Configuring users and roles (RT Unified) > Using the user management on the Unified Comfort Panel > Managing local users > Managing local users in runtime".

A.4 Resetting an HMI device to factory settings via ProSave

If the operating system on the HMI device is no longer functional, you must reset the HMI device to factory settings.

NOTICE

Do not switch off the HMI device during data transfer

If you turn off HMI device while the HMI device is being reset to factory settings, the HMI device will not start. You must repeat the procedure.

Do not turn off the HMI device during data transfer.

Procedure

To reset the HMI device to factory settings, follow these steps:

1. If a project is running on the HMI device, close the project.
2. Connect the HMI device to the configuration PC via the X1 interface.
3. In the Control Panel of the HMI device, select "Network and Internet" > "Network settings".
4. Ensure that the "Activate this port for use" option is enabled for the X1 interface under "Ethernet parameters Port".
5. In the Control Panel of the HMI device, select "System Properties" > "Reboot".
6. Press the "Reboot in maintenance mode" button. The HMI device starts. The "Maintenance Mode" dialog box is displayed for a period of 10 minutes. In this period you can connect the HMI device to a configuration PC and reset the HMI device to factory settings with the ProSave software. If the "Maintenance Mode" dialog is not displayed, start the HMI device while pressing the "Maintenance" button, see section "Using the maintenance mode (Page 51)".
7. Open the "ProSave" software on the configuration PC in the WinCC installation directory.

8. Enter the following data in the "General" tab:
   – "Device type": Select the type of your HMI device.
   – "Connection": Select "Ethernet".
   – "Connection parameters": Specify an IP address or computer name for the HMI device. The IP address must be located in the subnet of the configuration PC.
9. Enter the following data in the "OS Update" tab:
   – Under "Opening ...", select the path and file name of the firmware master file (.fwf) containing the desired operating system.
   – Select the option "Reset to factory settings".
   – Under "MAC", enter the MAC address which is shown at the top right of the HMI device display.
   – Use the "Device status" button to display information about the device and the selected firmware.
10. Click "Update OS". A dialog box with the warning that all data on the HMI device will be overwritten is displayed.
11. Confirm the dialog box.

The update of the operating system with "Reset to factory settings" is started. The progress of the update is displayed both in ProSave and on the HMI device. The update operation can take time, depending on the connection selected. The HMI device restarts at the end of the process.

Result

The operating system of the HMI device has been updated to the version of the selected firmware and the HMI device is reset to factory settings.

A.5 Using the maintenance mode

Maintenance mode is used to reset the HMI to the factory settings.

When the operating system starts and the Control Panel is displayed after the HMI device is switched on, you can start the HMI device in maintenance mode by clicking the "Reboot in maintenance mode" button. Follow the description in section "Resetting an HMI device to factory settings via ProSave (Page 50)".

If the HMI starts with the boot splash screen and detects the corrupt operating system, the HMI automatically switches to maintenance mode. The "Maintenance Mode" dialog box is displayed. In this case, follow the procedure from step 6 in section "Resetting an HMI device to factory settings via ProSave (Page 50)".

If the HMI device starts with the boot splash screen and does not detect the corrupt operating system, the HMI device does **not** switch to maintenance mode. The "Maintenance Mode" dialog is **not** displayed. You must reset the HMI device to the factory settings. In this case, start the HMI device while pressing the "Maintenance" button as described in this section.

NOTICE

The operating system must be updated in maintenance mode

If you start the HMI device while pressing the "Maintenance" button, the HMI device is in maintenance mode. In maintenance mode, the "Maintenance Mode" dialog is displayed. The operating system **must** be updated.

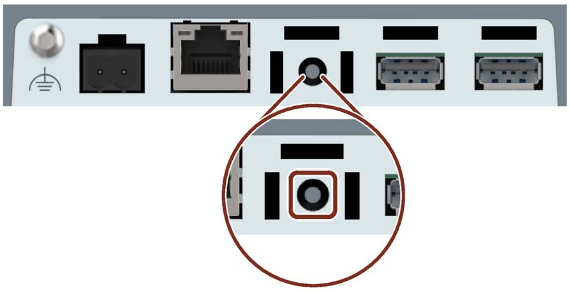
Only start the HMI device while pressing the "Maintenance" button if you are sure that you want to update the operating system.

Procedure

Proceed as follows:

1. Turn off the power supply of the HMI device.
2. Press the "Maintenance" button. Use a blunt, sufficiently sturdy tool made of non-conductive material, diameter approx. 5 mm.

   You can find the "Maintenance" button in the opening between the X1 and X61 interfaces.

   Be sure to hit the button accurately and do not slide the tool off the button.
3. Switch on the power supply of the HMI device and keep the "Maintenance" button pressed until the boot splash screen appears.

The HMI device restarts, the "Maintenance Mode" dialog box is displayed. Connect the HMI device to a configuration PC and reset the HMI device to factory settings using the ProSave software. Follow the procedure from step 6 in the section "Resetting an HMI device to factory settings via ProSave (Page 50)".