SIEMENS

SIMATIC HMI

WinCC Unified
WinCC Unified Runtime

System Manual

Online documentation

11/2023
Online documentation

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

Document order number: Online documentation
Ⓟ 11/2023 Subject to change

Table of contents

SIMATIC Unified PC readme 1

1.1 Security information

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity concept. Siemens' products and solutions only form 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 more information on protective industrial cybersecurity measures for implementation, visit:

https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html)

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends applying product updates as soon as they are available and always using only the latest product versions. 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 at all times, subscribe to the Siemens Industrial Cybersecurity RSS Feed under.

https://new.siemens.com/global/en/products/services/cert.html (https://new.siemens.com/global/en/products/services/cert.html)

Network settings

The following table shows the network ports that are used by WinCC Unified for internal and external communication. These ports must not be used for any other purpose.

The setup configures the firewall to ensure smooth operation.

WinCC Unified		
Name	**Port number**	**Transport protocol**
ILScs Manager	20008	TCP
UMC	20009	TCP

WinCC Unified		
ILPmon Manager	4999	TCP
ILEvent Manager	1235	TCP
ILDist Manager	4777	TCP
ILDataManager	1234 5001	TCP
Node Processes	3103 443 8888	TCP
Graphics Runtime	1339 1345	TCP
License server	1366	TCP
Screen debugger	9222	TCP
Job debugger	9224	TCP
WCCIL Proxy Manager	5678	TCP
Network Discovery (IS)	137	TCP
UMC AttachAgent	4002	TCP
OPC UA Discovery	4840	TCP
RFID	5003	TCP
GraphQL	4000	TCP

Unified Comfort Panel		
Name	Port number	Transport protocol
HmiRuntime	1234	TCP
HmiRuntime	1235	TCP
HmiRuntime	1344	TCP
HmiRuntime	4700	TCP
HmiRuntime	4701	TCP
HmiRuntime	4776	TCP
HmiRuntime	4777	TCP
HmiRuntime	4778	TCP
HmiRuntime	4999	TCP
HmiRuntime	5678	TCP
Snmpd	162	TCP
FwPnManager	34964	UDP

Note

Block HTTP port

For security reasons, it is recommended that Port 80 be disabled on the IIS server.

1. Start "Internet Information Services (IIS) Manager" on the Unified PC.
2. Right-click "Default Web Site".
3. Select "Remove" or "Manage Website > Stop".

See also

www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity)

www.siemens.com/cert (https://www.siemens.com/cert)

1.2 Breaking changes

PI options in ODK

ODK does not support any PI options in V19.

Scrolling behavior for pop-ups

If you move the visible screen section of a process screen in Runtime and a pop-up window is visible there, for example a faceplate container, Runtime behaves as follows:

WinCC Unified V17	The pop-up window is moved together with the screen section.
As of WinCC Unified V18	The pop-up window is not moved with it.
Simulation of an HMI device with installed device version V17 in a WinCC project V18 or higher	The pop-up window is moved together with the screen section.

Operation of objects behind a screen window

If a screen window has an empty area and the screen or faceplate displayed in the screen window has the "transparent" setting as the fill pattern for the background, Runtime behaves as follows:

WinCC Unified V17	Objects that are in the background of the screen window in the empty area of the screen window are visible. The objects cannot be operated by clicking.
As of WinCC Unified V18	The objects can be operated by clicking. Application example: You use a round menu with a button next to it. To prevent the rectangular border surrounding the menu from obscuring the button, make the menu available in a screen window.

Zoom behavior of screen windows on touch devices

Runtime now supports panning and zooming with a two-finger gesture.

WinCC Unified V17	No panning and zooming with two-finger gestures.
As of WinCC Unified V18	Panning and zooming with two-finger gestures is supported. Default: Activated If you want, you can disable this feature by clearing "Format > Allow zoom" property for the screen window.

Exclusion of "Uncertain - initial value" quality code as trigger

WinCC Unified V17	If a tag is used as a trigger for a script and the tag is used in a screen, e.g. by an I/O field, the script is executed twice in quick succession when the screen is loaded: • When reporting the initial value • When reporting the process value
As of WinCC Unified V18	Default setting: QualityCode 0x4C (Quality status: Uncertain, Substatus: Initial value) is ignored as a tag trigger. If a tag is used as a trigger for a script and the variable is used in a screen, e.g. by an I/O field, the script is only executed when the process value is reported as the screen is loaded. To enable the quality code as a trigger, proceed as described below.

To enable QualityCode 0xC4 as a trigger in V18 or higher, do the following:

1. Open a file browser and navigate to the following folder:
   `C:\Program Files\Siemens\Automation\WinCCUnified\bin\_config`
2. Open the following configuration file:
   – For scripts in screens: `IOWA_GfxComponentConfigurationSrv.xml`
   – For scheduled tasks: `IOWA_SchedComponentConfiguration.xml`
3. Delete the line for <Attribute key>:

```
<ComponentConfiguration componentKey="GfxTriggerManager"
name="Trigger Manager">
   <AttributeList>
      <Attribute key="IgnoredTagQualities" value="0x4c"/> <!–
0x4c: “Initial Value” quality >
   </AttributeList>
</ComponentConfiguration>
```

Simulation of Runtime

To use the simulation, you must install WinCC Unified Runtime. If no license is found for Runtime, start the simulation in demo mode.

OPC UA with OpenSSL 3.0

WinCC Unified uses OPC UA OpenSSL 3.0 from V18 Update 3 and higher.

If the OPC UA certificate of an HMI device has been created before V18 Update 3, it becomes incompatible through the device upgrade and has to be recreated. Follow these steps.

IF the HMI device uses a CA-based OPC UA certificate:

1. Upgrade the certificate authority device and the HMI device.
2. Re-create the OPC UA certificate of the HMI device on the certificate authority device with WinCC Unified Certificate Manager.
3. Install the certificate on the HMI device.
   If the communication partner already trusts the root certificate of the certificate authority, it automatically also trusts the newly created OPC UA certificate of the HMI device.

If the HMI device uses a self-signed OPC UA certificate:

1. Delete the certificate from the certificate store before upgrading the HMI device:
   - For Unified PCs:
     The certificate store is located in the folder with the Runtime projects in the subfolder "`certstore`".
     Default: `C:\ProgrammData\SCADAProjects\certstore`
   - For Unified Panel:
     Select "Control Panel > Security > Certificates" and as the "Certificate store" the entry "My Certificates". Select the certificate and delete it.
2. Upgrade the HMI device.
   For Unified PC: The certificate is automatically generated and installed.
3. For Unified Panel: Start Runtime.
   The certificate is automatically generated and installed.
4. Trust the certificate at the communication partner.

1.3 GDPR - General Data Protection Regulations

Siemens takes data privacy principles, such as the privacy by design and default principle, into account when developing its products and services. For this product WinCC Unified Runtime this means the following:

Personal data processed by the Application

This product collects and processes the following personal data:

- User names, i. e. login data, which might directly contain or establish a reference to the family name and/or first name
- Timestamps: date / time of login, logoff and access
- Location data (time zone)
- Computer name

- IP addresses
- Optional: With UMC, the following additional personal data can be added in the tool:
  - Full name
  - Comment

  This data is not needed for the product functionality and should not be stored on the same medium.

If the user links the above-mentioned data with other data, e. g. shift plans, or stores personal data on the same medium, e. g. hard disk, and thus establishes a personal reference, the user must ensure compliance with data protection regulations.

Purposes

The above data is required for the following purposes:

- Access protection and security measures (e. g. Login, IP address)
- Process synchronization and integrity (e. g. time zone information, IP addresses)
- Archiving system for traceability and verification of processes (e. g. access timestamps)
- Alarm system for traceability and availability (for example, e-mail notification)

The storage of data is appropriate and limited to what is necessary, as it is essential to identify the authorized operators and process events.

Data configuration

The customer can configure the data collected via the product as follows:

- Display data in process pictures
- Data output in form of reports, e. g. for printing or display as electronic file
- Data collection and evaluation in form of graphics, e. g. for KPI analysis

Deletion policy

The product does not provide an automatic deletion of the above data.

If necessary, these can be deleted manually if desired. To do this, refer to the product documentation or contact customer support.

Securing of data

The above data will not be stored anonymously or pseudonymized, because the purpose of access and event identification cannot be achieved otherwise.

For WinCC Unified PC-based, the data specified above should be secured by appropriate technical measures:

- Encryption of log data
- Storing the process data in access-protected SQL databases
  The user must ensure the access protection as part of their process configuration.

You can find information on data backup on the WinCC Unified Comfort Panel in the operating instructions for the Comfort Panel.

1.4 Notes on installation

Contents

Important notes on installation.

Previously installed versions of WinCC Unified

The installation of Unified V18 is possible on devices for which the following applies:

- No Unified installed yet, or
- WinCC Unified V17 installed
  The V17 installation must not have been upgraded from V16.

Special characters in the installation path

Special characters in the installation path may lead to objects not being visible when inserted into a screen. To see the object, you have to close the screen and open it again.

Record/play function

When the record/play function is used, the Runtime system settings made in WinCC Unified Configuration Manager during or after installation are not recorded.

Silent installation of Runtime using the record/play function is not supported.

Parallel installation of TIA Portal and Runtime

To operate TIA Portal V19 and WinCC Unified Runtime on the same PC, WinCC Unified Runtime V19 must be installed on the device or an upgrade to this version carried out.

Parallel installation with PCS7

It is not recommended to install WinCC Unified Runtime V19 and PCS7 on the same device. A parallel installation is at the user's own risk.

Parallel installation with WinCC Runtime Professional

It is not recommended to install WinCC Unified Runtime V19 and WinCC Runtime Professional V16, V17 or V18 on the same device. A parallel installation is at the user's own risk.

Parallel installation with WinCC Professional

It is not recommended to install WinCC Unified Runtime V19 and the engineering system for WinCC Professional V17 or V18 on the same device. A parallel installation is at the user's own risk.

Repair installation

Proceed as follows after a repair installation:

1. Start the "WinCC Unified Configuration" application from the desktop.
2. Enable the "Make additional settings" option.
3. Check or correct the configuration of the "Website settings" step.
4. All other settings can be applied with "Keep the existing configuration".

1.5 Notes on use

Contents

Information that could not be included in the online help and important information about product features.

Copying between WinCC Unified and other devices

Copying data via the clipboard or via the library, for example is only supported between Unified devices. Copying data between Unified devices and other devices is not supported.

Secure communication

If you use Inter-Project Engineering (IPE) in your project, i.e. an HMI device is connected to a device proxy PLC, and an error message about inconsistent certificates appears during compiling, you need to correct the certificates of the associated PLC in the original project. Then you have to compile, export and re-import the PLC.

Changing HMI device names or log paths

If you make the following changes in the engineering system for a project that is already loaded in Runtime, the existing log data is lost when you load the device again:

- You rename the HMI device in the project navigation
- You rename a log folder or change the log path in the Runtime settings

The data from the old log is not available in the new log after reloading.

Storage location for databases

If the Runtime project folder is configured as the storage location for a database and you change the location of the project folder, this results in data loss.

To avoid data losses select a different storage location for databases than that of the project folder or do not change the project folder.

For more information, refer to the help "SIMATIC Unified PC Installation" under the keyword "Loading projects".

Access to subnets via TCP/IP Auto

Use the TCP/IP Auto setting on your engineering device (programming device) when you connect the device to a local subnet. (Control Panel > Set PG/PC interface)

The engineering device then allows additional IP addresses from the subnet to be added to its network adapter.

Note

This setting cannot be used if you use a router.

No setting is necessary on the devices belonging to the external network.

For stationary operation, use the TCPI/IP setting.

Fault in the connection between the server and the client

If there is a fault in the connection between the server and client, check the settings of the PG/PC interface. TCP/IP Auto should not be used for the setting "Interface parameter assignment used". Use fixed IP addresses instead.

Changes at a PLC user data type

After a change to a PLC user data type, the PLC must be compiled to make this change known to all Unified devices that use this user data type. If compilation of the PLC does not take place, error messages can occur during the compilation of the HMI devices.

Inter Project Engineering (IPE) in faceplates

Inter Project Engineering is not supported by faceplates. User data types of a device proxy PLC cannot be interconnected with a faceplate.

Collaboration certificates and Runtime version

Runtime Collaboration requires that the Collaboration certificates of 2 Collaboration partners have been created with a Certificate Authority device whose installed Runtime version is equal to or higher than the installed Runtime version of the Collaboration partner with the higher Runtime version.

This is why upgrading Collaboration devices may require re-creation, distribution, and installation of Collaboration certificates.

Example:

- A Unified PC and a Unified Panel with a V17 Runtime are Collaboration partners.
- You upgrade the Panel to V18.
- On a Certificate Authority device with an Runtime version V18 or higher, create new Collaboration certificates for both HMI devices. Distribute and install them on the devices.

Starting Runtime

Runtime cannot be started via WinCC Runtime Start if the "Load preview" dialog is displayed in the engineering system.

Status "Partly running"

If it is not possible to start the simulation or the Unified Runtime, open the Runtime Manager. If the status of the project is displayed as "partly running", check

- whether the user currently logged on in Runtime has sufficient rights. Is the user entered in the following Windows user groups:
  PLCSimUsers
  RTIL Tracing Users
  Siemens TIA Engineer
  SIMATIC HMI
  SIMATIC HMI VIEWER
- whether the computer name is not longer than 15 characters.
- whether "OPC UA" is activated in the Runtime settings and a certificate exists.
- whether "Runtime Collaboration" is enabled in the Runtime settings of a Unified Panel and a certificate is available.

Simulation with S7-PLCSIM

Always start the simulation in WinCC and then S7-PLCSIM.

WinCC Unified Tag Simulator

The WinCC Unified Tag Simulator is not part of WinCC Unified V18 and higher.

Dynamic SVG types

If you manually assign a type version to a dynamic SVG type or rename the type, a delta download is no longer possible.

Encryption with TLS

Always use the most current version of TLS. Disable the older version.

The use of older versions (TLS 1.0 und 1.1) is at your own risk.

Assigning text lists and graphics lists for reports

It is not possible to read in values from texts lists and graphics lists, neither in the add-in nor when generating the report.

Page numbering in audit

Because of a problem with the page numbering, the system functions "ReadElectronicRecord" and "ExportElectronicRecordAsCSV" only deliver the first 1000 electronic data records on the provided filter.

Protecting drives through UWF

If you are using UWF (Unified Write Filter) on a Unified PC, exclude the following folders from UWF:

- Project folder
  Preset project folder: C:\ProgramData\SCADAProjects
- C:\ProgramData\Siemens

In accordance with the UWF implementation of Microsoft, all write accesses are then written directly into these folders, but also into the overlay. If the size of the overlay approaches or exceeds the upper limit, this causes problems when loading projects or in Runtime.

You have the following options:

- Start WinCC Unified Configuration and, in the "Storage location for projects" step, select a folder whose drive is not protected by UWF as the project folder.
- Increase the size of the overlay.
- Change the type of overlay from RAM-based to disk-based.
- Start the Unified PC before reloading a project into the device.
  The overlay is emptied during the restart. This may slow down the restart.

Communication with LOGO! PLC

For the communication with a LOGO! PLC, select “Standard Modbus TCP/IP” in the connection as the communications driver.

Parallel installation of TIA Portal and Runtime

To operate TIA Portal V19 and WinCC Unified Runtime on the same PC, WinCC Unified Runtime V19 must be installed on the device or an upgrade to this version carried out.

"My Controls"

If a device was upgraded to V19 in the engineering system, it is possible that My Controls were not displayed correctly in the "Images" editor. Compiling of the device results in errors.

In that case, click the refresh icon in the "My Controls" palette:

🔄

Working with text list types

Text list types can now be added to the library. You proceed as with adding other types in the library. In the Text List Type editor, select selection mode for the text list. Create the entries with the corresponding values/ranges and the texts. If you have configured several project languages, you can also create multilingual texts.

You can use text list types in the following use cases in the project:

- **Resource list**
  Use text list types on objects that support resource lists as a static value, e.g. symbolic I/O fields.

  Note

  Objects in faceplate types

  For faceplate types, configure an interface property of the "Resource list" type and transfer it to the object. Then transfer the text list type to the faceplate instance at the interface property.

- **Script**
  Use text list types in scripts via the JavaScript object "HMIRuntime.Resources.TextLists". Usages of text list types are shown in the script editor as a reference. You can use text list types in scripts of other types, e.g. faceplate or script module types.
  Example:
  ```
  let entry1 =
  HMIRuntime.Resources.TextLists("@Default.Text_list_type_1_V_0_0_1"
  ).Item(1);
  ```

- **System function**
  You can use text list types in system functions such as `InsertElectronicRecord` and `Lookuptext`.

When you change a text list type, the changes are checked for consistency. If there are consistency errors when the version is released, you can view the error messages under "Info > General" in the Inspector window.

If you release a new version of a text list type, you can update all usages automatically. Types that use the text list type can be automatically set to processing status.

Text list types can be stored in global libraries.

IO field in scripts

The properties "MeasurementUnit" and "MeasurementUnitType" of an IO field are reserved for future versions.

SIMATIC WinCC Unified Station Configurator

SIMATIC WinCC Unified Station Configurator does not support Unified Runtime projects of the type "Simulation".

Renewed loading of the Unified Panel after updating of the CPU configuration

If the configuration of the CPU is changed and loaded into the control unit, the PLC communications certificate of the control unit is updated.

In this case the Unified Panel connected with the CPU also has to be reloaded. After loading, the Panel trusts the PLC certificate.

Configuring automatic logout for central user management

To configure automatic logout on the UMC ring server, it is necessary to empty the cache of the browser in which you open the ring server UI after upgrading the UMC ring server. The ring server is automatically upgraded if the ring server and engineering system are installed on the same PC and you upgrade the engineering system.

Follow these steps:

1. Start a browser and open the web UI of the ring server.
2. Press Shift+F5 or Shift+Ctrl+R.
3. If automatic logout is still not configured correctly after this, follow these steps:
   In Chrome and Edge:
   - Enter `chrome://settings/clearBrowserData` in the address bar.
   - In the "Clear browsing data" window, disable all options except for "Cached images and files".
   - Click "Clear data".

   In Firefox:
   - Enter `about:preferences#privacy` in the address bar.
   - Scroll down to "Cookies and Site Data".
   - Click "Clear Data".
   - Select "Cached Web Content".
   - Click "Clear".

Function rights for My WinCC Unified

In the engineering system, the "Users and roles" editor for the function rights (runtime rights) of My WinCC Unified does not consistently use the correct names and comments in all languages. Below is an overview for the English and German languages:

"Users and roles" editor		Correct	
"Name"	"Comment"	"Name"	"Comment"
"My WinCC Unified - Read and write access to current personalized user settings"	"Read and write access to all user settings"	"My WinCC Unified – read and write access to all user settings"	✓
"My WinCC Unified – Read and write access to device-specific settings"	"Read and write access to device-specific settings"	✓	✓

"Users and roles" editor		Correct	
"My WinCC Unified - Read and write access to current user and device settings"	"Read and write access to current personalized user settings"	"My WinCC Unified - read and write access to user's own settings"	"Read and write access to current user's own settings"
"My WinCC Unified - Read access to user and device settings"	"Read access to user and device settings"	"My WinCC Unified - read device and user settings"	"Read access to current user's own settings and device settings"
"My WinCC Unified – Lese- und Schreibzugriff auf alle Benutzereinstellungen"	"Lese- und Schreibzugriff auf alle Benutzereinstellungen"	✓	✓
"My WinCC Unified – Lese- und Schreibzugriff auf gerätespezifische Einstellungen"	"Lese- und Schreibzugriff auf gerätespezifische Einstellungen"	✓	✓
"My WinCC Unified – Lese- und Schreibzugriff auf aktuelle eigene Benutzereinstellungen"	"Lese- und Schreibzugriff auf aktuelle eigene Benutzereinstellungen"	"My WinCC Unified – Lese- und Schreibzugriff auf die eigenen Benutzereinstellungen"	"Lese- und Schreibzugriff des aktuellen Benutzers auf die eigenen Benutzereinstellungen"
"My WinCC Unified – Lesezugriff auf Benutzer- und Geräteeinstellungen"	"Lesezugriff auf Benutzer- und Geräteeinstellungen"	✓	"Lesezugriff des aktuellen Benutzers auf die eigenen Benutzereinstellungen und die Geräteeinstellungen"

1.6 Notes on the operation of Unified PC

Contents

Information that could not be included in the online help and important information about product features.

Generic logon error due to browser language settings

If a language that is not supported by Unified Runtime is set as the browser language, the "Generic error" occurs during logon.

Follow these steps:

1. Open the browser language settings.
2. Select one of the languages supported by Unified Runtime.
3. Log on in Runtime.

Restoring log segments

The following requirements apply to restoring log segments with SIMATIC Runtime Manager:

- A project that is in the "Running" status is loaded into runtime.
- At least one backup of a tag or alarm log is available for the project.
- If the project was loaded several times, no logs were reset during complete loading in the "Load preview" dialog.

Efficient use of the segment memory

If you work in MS SQL databases with SQL Server 2016 or higher, unused memory may be allocated instead of being used efficiently in the case of few write operations in the respective interval.

TraceViewer

If the user logged on in Runtime belongs to the "RTIL Tracing Users" and "SIMATIC HMI" user groups, all trace messages are visible in the TraceViewer, otherwise only the trace messages from SIMATIC Runtime Manager.

My WinCC Unified

If you do not see the "My WinCC Unified" entry on the Unified Runtime home page, delete the browser data completely (history, form entries, etc.), and reload the page.

After login, My WinCC Unified has the user interface language that you selected in the login dialog. If you have not selected a language, the language that is set for the browser is used.

Kiosk

The following contents could not be taken into consideration before the editorial deadline for the online help "My WinCC Unified":

- The application was renamed from "SIMATIC WinCC Unified Control Center" to "SIMATIC WinCC Unified Station Configurator".
- To install WinCC Unified Station Configurator on a client device proceed as described in the manual "SIMATIC WinCC Unified Station Configurator Installation".
- Installation of WinCC Unified Station Configurator is supported on all client devices with Windows operating system (PCs, notebooks, etc.).
- WinCC Unified Station Configurator does not connect to a Unified PC Runtime web server running a Windows Server operating system.
  To enable such a connection, follow these steps on the Runtime web server:
  - In the Group Policy Management Console (GPMC), open "Windows Defender Firewall with Advanced Security".
  - In the navigation area, navigate to "Inbound Rules".
  - Right-click on "Inbound Rules" and select "New Rule".
  - "Rule type" step: Select the "Port" option.
  - "Protocol and ports" step: Select the "TCP" option and enter "4000" as port under "Specific local ports".
  - "Name" step: Enter the name and description of the rule.
  - Click "Finish".
- WinCC Unified Station Configurator does not support Unified Runtime projects of the type "Simulation".

- For a client device with several monitors, the main screen shows Runtime in kiosk mode. The other monitors show the Windows desktop.
- The following restrictions apply to the import of YAML files with kiosk settings to My WinCC Unified:
  Restrictions for `BreakOutData`:

`Keys`	Mandatory specification. Only ALT+F4 is supported.
`IsEnabled`	• `IsEnabled = true` `SelectedKey` must have a valid value. • `IsEnabled = false` `SelectedKey` must have an empty value.
`SelectedKey`	Only keys that are supported in the `Keys` property are allowed.
`IsPinConfigured`	• `IsPinConfigured = true` `Pin` must have a valid value. • `IsPinConfigured = false` Does not expect a property `Pin` or `Pin` with empty value.

Restrictions for `FolderData`:

`FolderData`	`FolderItems` must have at least 1 item.
`FolderItems`	Per item: • `Path` Mandatory specification • `IsDefault` Mandatory specification Only 1 item can have `IsDefault = true`.

Adding a project offline

Users who add a project in SIMATIC Runtime Manager through the offline transfer and enable the option "Overwrite UMC data with the context of the offline loading", must be members of the Windows user group "umcd_global_admin".

Note that changes to the membership of a Windows user group only take effect with the next Windows login of the user.

1.7 Internet browsers for WinCC Unified PC

Ensure you have the latest operating system and browser version if you want to access Runtime Unified with this device.

WinCC Unified displays the runtime elements in HTML5. The browser used also has to support this standard. Since the browsers interpret HTML5 differently, it is possible that objects are displayed differently depending on the browser and the browser version used. For example, browsers sometimes display fonts differently.

Compatibility tests were performed for the following browsers. The focus of the compatibility tests was on the browsers marked with *:

Operating system	Browser
Microsoft Windows	• Google Chrome* • Microsoft Edge • Mozilla Firefox, Mozilla Firefox ESR
Android	• Google Chrome* • Firefox • Edge
iOS, Mac	• Safari* • Google Chrome • Firefox • Edge

Browser recommendation

In view of the performance and support of the Runtime standard elements, Google Chrome has proven to be the preferred browser. Its memory requirements are slightly higher than those of the other browsers.

Note

Operating system and browser version

For Runtime operation via Android or iOS, always use the latest operating system.

Use the latest browser version.

Note

Performance differences in different versions of individual browsers

The browser versions can differ from each other, which can result in different behavior regarding the memory requirements and speed.

Note

Suitability for continuous operation

Mozilla Firefox has proven to be problematic in continuous operation.

Known browser problems

The following restrictions apply to the following browsers:

Internet browser	Limitation
MS Edge	• If you want to start Runtime in Microsoft Edge and enter the address "https://localhost", the error message "INET_E_RESOURCE_NOT_FOUND" appears. In this case, use the address "https://localhost/WebRH".
Mozilla Firefox	• High memory capacity utilization in continuous operation
Mozilla Firefox ESR	• Support of touch gestures for touch panels as of Firefox ESR V59
Google Chrome	• High memory capacity utilization in uninterrupted duty depending on the version. • On Android: Grid lines with a line width ≤1 are not displayed correctly. This is due to the browser's own line thickness representation. As a solution, it is helpful to use a line width ≥1. • No correct representation of elements that use an SVG graphic as background graphic scaled in the Engineering System.

Restrictions to the various functions can also occur, such as the availability of the before and after buttons in the controls.

Current information on browser problems

You can find up-to-date information on display problems in browsers at the Siemens Online Support under the entry ID 109757952.

1.8 Remote access to a Unified device

Contents

Information that could not be included in the online help and important information about product features.

Synchronize client values with server time

By default, the following controls display values with client time:

- Alarm control
- Trend companion
- Trend control

- f(x) trend control
- Process control

To synchronize the time displayed on the client with the server, proceed as follows:

- iOS devices:
  To prevent an iOS device from synchronizing with time.apple.com, create a profile file and upload it to the device.
  Profile files enable time synchronization within a secure corporate network.
- Android devices:
  Use a third-party app for time synchronization.

Access to a Unified device

Ensure you have the latest operating system and browser version if you want to access Runtime Unified with this device.

WinCC Unified displays the runtime elements in HTML5. The browser used also has to support this standard. Since the browsers interpret HTML5 differently, it is possible that objects are displayed differently depending on the browser and the browser version used.

Compatibility tests were performed for the following browsers. The focus of the compatibility tests was on the browsers marked with *:

Operating system	Browser
Microsoft Windows	• Google Chrome* • Microsoft Edge • Mozilla Firefox, Mozilla Firefox ESR
Android	• Google Chrome* • Firefox • Edge
iOS, Mac	• Safari* • Google Chrome • Firefox • Edge

With respect to the performance and support of the standard Runtime elements, Google Chrome has proven to be the preferred browser. Its memory requirements are slightly higher than those of the other browsers.

Note

Performance differences in different versions of individual browsers

The browser versions can differ from each other, which can result in different behavior regarding the memory requirements and speed.

Note

Suitability for continuous operation

Mozilla Firefox has proven to be problematic in continuous operation.

Unified Collaboration

Unified Collaboration is only permitted between devices with the same device version (starting from V16).

If Unified Collaboration uses local user management and the Collaboration partners are configured in different projects, it is possible to create users with the same name but different function rights. If one of these users logs on to a device in Runtime, the user has the function rights configured for this device as well as the function rights configured for the Collaboration partner. If you use several projects, you should configure the local user management identically in all projects.

SIMATIC Unified PC installation

2

2.1 Software and hardware requirements

Specific requirements for the operating system and software configuration must be met for the installation.

Installation in domains and workgroups

WinCC Unified is generally approved for operation in a domain or workgroup.

However, be aware that domain group policies and restrictions of the domain might hinder the installation. In this case, remove the computer from the domain before installing WinCC Unified and Microsoft SQL Server. Log on to the local machine with administrator rights. Perform the installation. After successful installation, you can restore the WinCC computer to the domain. If the domain group policies and restrictions of the domain do not impede the installation, the computer need not be removed from the domain during the installation.

Be aware that domain group policies and restrictions of the domain might also hinder operation. If you cannot avoid these restrictions, run the WinCC computer in a workgroup.

Consult with the domain administrator if needed.

Operation on a network server

It is not permitted to operate WinCC Unified Runtime on a network server (e.g. domain controller, file server, name service server, router, software firewall, media server, exchange server).

Windows computer name

Before you start the WinCC installation, specify the Windows computer name. Follow the Windows naming rules.

Note

How to proceed after a subsequent change of the computer name is described in the WinCC Unified Runtime installation manual in the section "Changing the computer name or IP address".

The following characters are not permitted for the computer name:

- . , ; : ! ? " ' ^ ` ~ _
- + = / \ | @ * # $ % &
- ( ) [ ] { } < >
- Space

Follow these recommendations when assigning the Windows computer name:

- Only uppercase letters may be used.
- The first character must be a letter.
- The first 12 characters of the computer name must be unique.
- The computer name can have a maximum of 15 characters.

Hardware requirements for the installation

The following table shows the minimum hardware requirements that have to be met for the installation:

Hardware	Requirement
Processor type	Intel Core i3
RAM	4 GB
Free hard disk space	10 GB, 8 GB CF

Software requirements for the installation

Operating system

Software	Configuration	Comments
Windows 10 Pro	Windows 10 Pro Version 1909 (OS Build 18363) Windows 10 Pro Version 2004 (OS Build 19041) Windows 10 Pro Version 2009/20H2 (OS Build 19042) Windows 10 Pro Version 21H1 (OS Build 19043) Windows 10 Pro Version 21H2 (OS Build 19044)	64-bit
Windows 10 Enterprise	Windows 10 Enterprise Version 1909 (OS Build 18363) Windows 10 Enterprise Version 2004 (OS Build 19041) Windows 10 Enterprise Version 2009/20H2 (OS Build 19042) Windows 10 Enterprise Version 21H1 (OS Build 19043) Windows 10 Enterprise Version 21H2 (OS Build 19044)	
Windows 10 IoT Enterprise LTSB	Windows 10 Enterprise 2016 LTSB (OS Build 14393) (Test for IPC) Windows 10 Enterprise 2019 LTSC (OS Build 17763) (Test for IPC) Windows 10 Enterprise 2021 LTSC (OS Build 19044) (Test for IPC)	

Software	Configuration	Comments
Windows 11	Windows 11 Home Version 21H2 (OS Build 22000)	64-bit
Windows 11 Pro	Windows 11 Pro Version 21H2 (OS Build 22000)	
Windows 11 Enterprise	Windows 11 Pro Version 21H2 (OS Build 22000)	
Windows Server 2016 Standard Windows Server 2019 Standard Windows Server 2022 Standard	Full installation	64-bit

Note

Number of supported clients and connections

Desktop operating systems support a maximum of 5 clients. In server operating systems, more than 5 clients can connect to the server.

Windows limits the number of incoming connections on desktop operating systems to 20. This limits the number of possible accesses to runtime.

Compatible browsers

Operating system	Browser
Microsoft Windows	• Google Chrome • Microsoft Edge • Mozilla Firefox, Mozilla Firefox ESR
Android	• Google Chrome • Firefox • Edge
iOS, Mac	• Safari • Google Chrome • Firefox • Edge

More information on the use of browsers is available in the SIMATIC Unified PC Readme in the section "Internet browsers for WinCC Unified PC".

Windows specific software settings for IIS (Internet Information Services)

The following settings for IIS are automatically enabled in Windows during the installation of WinCC Runtime Unified:

- HTTP error
- HTTP Redirection
- Default document
- Static content
- .NET extensibility 3.5
- ASP

- ASP.NET 4.5
- ISAPI extensions
- ISAPI filters
- Dynamic Content Compression
- Static Content Compression
- Request Filtering

Table 2-1 Additional software requirements

Topic	Version / setting	Comment
Web browser	The browser must support HTML 5.	
User rights for installation	Administrator rights	
SIMATIC NET	V18	You need this license to be able to operate Runtime Unified with more than 10 connections.

Previously installed versions of WinCC Unified PC Runtime

The installation of Unified PC Runtime V18 is possible on devices for which the following applies:

- No Unified PC Runtime installed, or
- WinCC Unified PC Runtime V17 installed
  The V17 installation must not have been upgraded from V16.

Ports

When a Windows firewall is used, the installation routine of WinCC Unified Runtime sets up the following ports:

- HTTPS: 443
- Network Discovery (IS): 137
- Totally Integrated Automation administrator: 8888
- UMC AttachAgent: 4002
- OPC UA Discovery: 4840

If your system uses a different firewall solution, make sure the ports are set up accordingly.

You can find a list of the ports used by Unified Runtime in the user help SIMATIC Unified PC readme in the section "Security information".

Note

Disable HTTP port

For security reasons, it is recommended to disable port 80 on the IIS server:

1. On the Unified PC, launch "Internet Information Services (IIS) Manager".
2. Click "Default Web Sites" on the right.
3. Select "Remove" or "Manage Website > Exit".

Note

Blocked ports after operating system update or upgrade

Updating or upgrading the operating system of the Unified PC, e.g. from Windows Server 2016 to Windows Server 2019, may change the firewall settings. As a result, the OPC UA ports may be blocked.

If this happens, start the Siemens "Security Controller" tool and run "Restore settings".

Virtualization

You can install the "SIMATIC WinCC Runtime Unified" software package on a virtual machine. The following virtualization systems were tested:

- VMware vSphere Hypervisor (ESXi) 6.7 (or higher)
- VMware Workstation 12.5.5 and VMware Workstation 15.5.0 (or higher)
- VMware Player 12.5.5 and VMware Player 15.5.0 (or higher)
- Microsoft Hyper-V Server 2019 (or higher)

In a virtualization platform, all approved operating systems can be used as host operating system.

Requirement

The performance data of the virtual computers must meet the minimum requirements of WinCC clients.

Note

- Ensure that terminal and PLC networks are separated on the host system by using separate network adapters (dedicated, physically separated network adapters).
- The same hardware requirements apply to the host operating system as for the respective TIA products.
- The plant operator must ensure that sufficient system resources are available for the host operating systems.
- The hardware certified by the manufacturers is recommended for the use of HyperV server and ESXi.

Supported security programs

The following security programs are compatible with Unified Runtime:

Virus scanner	Symantec Endpoint Protection 14.3
	McAfee Endpoint Security (ENS) 10.6 and 10.7
	Trend Micro Office Scan 14.0
	Windows Defender (as part of the Windows operating system)
	Qihoo 360 "Safe Guard 12.1" + "Virus Scanner"
Whitelisting	McAfee Application Control 8.3.3
Hard disk encryption	Microsoft BitLocker (as part of the Windows operating system)

Principle

Care must be taken to ensure that the use of the antivirus software does not impair the process operation of a plant.

Rules for antivirus software (virus scanning clients)

- Integrated virus scanner firewall
  In WinCC Unified, the local Windows firewall used is configured with SIMATIC Security Control. Do not install or enable the integrated firewall of the antivirus software.
- Manual scan
  You must not perform a manual scan while Runtime is running. Perform disk on regular intervals on all plant PCs, for example, during the maintenance interval.
- Automatic scan
  For automatic scan it is sufficient to scan the incoming data traffic.
- Scheduled scan
  You must not perform a scheduled scan while Runtime is running.
- Pattern update
  The pattern update of the virus scanning clients (the plant PCs which are checked for viruses) performed by the higher-level virus scanning server (the plant PC which centrally manages the virus scanning clients).
- Dialog
  To avoid impairing the process operation, no dialog messages can be displayed on the virus scanning clients.
- Drives
  To prevent overlapping scans on network drives, only the local drives are scanned.

Otherwise apply the default settings.

What is secured?

The incoming data traffic is checked for viruses. The impairment of the process mode is minimized.

Note

If you are using an anti-virus scanner, make sure that the computer has sufficient system resources.

Supported database types

The following database types are supported by SIMATIC WinCC Unified PC:

HMI device	Supported database type
SIMATIC WinCC Unified PC	SQLite
	Microsoft SQL

Microsoft SQL for Unified PC

WinCC Unified PC uses SQLite as the default database type. To use Microsoft SQL, the system provides an installation option with a setup package.

- Logging with SQLite is not possible after the installation of Microsoft SQL.
- Existing SQLite files are retained, but they cannot be accessed in runtime.
- No backup can be created for SQLite.

Microsoft SQL Server 2017 is used as of TIA Portal V17. SQL Management Studio is no longer part of the Microsoft SQL Server installation package and is therefore not included in the Totally Integrated Automation Portal installation. You can install SQL Management Studio separately if needed.

To establish secure SQL Server connections, please observe the notes in the Microsoft documents:

- Server Network Configuration (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/server-network-configuration?view=sql-server-2017)
- Enable encrypted connections to the Database Engine (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017)

See also

Internet browsers for WinCC Unified PC (Page 26)

Changing the computer name or the IP address (Page 47)

Security information (Page 11)

Parallel installation (Page 37)

2.2 Parallel installation

Introduction

It is possible to install WinCC Unified Runtime and WinCC Professional Runtime in parallel on the same device. To avoid conflicts between the Runtimes, you have to change the preset port numbers for WebUX and WebNavigator for WinCC Professional.

Procedure

1. Change the port number of the WebUX web page for HTTPS communication from 443 to 4443. This eliminates the conflict with the Unified Runtime default port number.
2. Change the port number for internal communication between WebUX WebRH(Node Server) and GfxRTS from 1345 to a different number.
3. Change the port number of the WebNavigator web page for HTTPS communication from 443 to 4430. This eliminates the conflict with the Unified Runtime default port number.
4. Create a firewall rule for incoming data traffic to allow TCP traffic with the new WebUX port number 4443.
5. Set firewall rules for incoming data traffic to allow TCP traffic with the new WebNavigator port number 4430.
6. Make sure the firewall rules are securely created.
7. Check that WebUX and WebNavigator websites are accessible with their respective new port numbers.

2.3 Starting installation

Requirement

- You have administrator privileges on your computer.
- All running programs are closed.

Procedure

1. Place the installation medium in the respective drive.
2. Start the Setup.
3. Select the required installation language.
4. Select the required product configuration.
5. Read and accept all the license conditions and safety information.
6. Accept the changes in the security settings.
7. Check the selected installation settings.
8. Start the installation.
9. After selecting the components, make the system settings for operation of Unified Runtime. These are described in the section Configuring Runtime system settings (Page 39).
   You can amend or change the settings at a later time by calling the "WinCC Unified Configuration" tool.
10. Reboot the PC to complete the installation.

Note

Using the Openness SDK

You will find the Openness SDK in the "Support\Openness" folder on the installation medium. Unpack the file "Siemens.Unified.Openness_SDK_<version number>.zip" to your local computer. A WinCC Unified installation is not necessary to use the Openness SDK.

2.4 Configuring Runtime system settings

2.4.1 Configuring the settings during installation

Requirement

- You have completed the component selection in the setup and are now in the step for configuration of the Runtime system settings.

Procedure

Follow the setup instructions and configure the following settings:

- For the website
- For the user management
- Log settings for the storage location of the log databases and the maximum storage limit of the SQL server.
- For reporting
- For loading projects

You navigate between the various steps with "Back" and "Next".

To skip a step or maintain the pre-selected inputs, select the option "Keep the existing configuration" and click "Next".

Result

The installation automatically creates a desktop shortcut for "WinCC Unified Configuration". You can amend or change the settings at a later time by manually starting "WinCC Unified Configuration".

2.4.2 Changing the settings after the installation

With "WinCC Unified Configuration", you amend or change the Runtime system settings made during the installation at a later time.

Requirement

- The program package is installed.

Procedure

1. Start "WinCC Unified Configuration" manually using the desktop shortcut that was created during the installation.
   The same settings are available in "WinCC Unified Configuration" as during the installation.
   - For the website
   - For the user management
   - Log settings for the storage location of the log databases and the maximum storage limit of the SQL server.
   - For reporting
   - For password-protected download
2. If required, change the user interface language of WinCC Unified Configuration. To do so, select the desired language from the list.
3. Follow the setup instructions and configure the required settings.
4. You navigate between the various steps with "Back" and "Next".
   To skip a step or maintain the inputs select during the installation, select the option "Keep the existing configuration" and click "Next".

Result

After you have completed the settings, the system automatically performs the configuration. You will receive an overview of the implemented configuration.

2.4.3 Website settings

In the "Website settings" step you specify:

- How the address of the identity provider and the WinCC Unified Runtime website are being generated.
- Which web server certificate WinCC Unified Runtime uses.
- After a change of the IP address or the computer name of the HMI device: Whether the Runtime system settings are only adapted to the change of the IP address or the computer name or if you are making additional settings.

Note

The options for this are only available if the IP address or the computer name has been changed after you have installed WinCC Unified Runtime on the device or configured it via WinCC Unified Configuration.

Selecting the addressing of the website and of the identity provider

For projects with a local user management, Runtime uses the full computer name (fully qualified domain name) to generate the address of the identity provider and the Unified website.

To use the IP address instead, proceed as follows:

1. Enable the option "Use IP address instead of computer name" under "Addressing the website and identity provider".
2. Select an IP address from the list.

Note

Use this setting only if you cannot access the HMI device from the network using the full computer name.

Selecting the web server certificate

The following options are available for selecting the web server certificate:

- "Install a certificate later"
- "Select an existing certificate"
  Select one of the web server certificates available on the device.
  Requirement: A valid web server certificate is installed on the device (Webserver (IIS)).
- "Create a new certificate"
  The new certificate is self-signed.

Secure communication through trusted certificates

To enable web clients to establish a secure connection to WinCC Unified Runtime, it is recommended to select a certificate issued by a root certificate in this step. Web clients must install this root certificate in the web browser. Create the root certificate and the web server certificate with the WinCC Unified Certificate Manager tool.

NOTICE

Security risk due to self-signed web server certificate

Using a self-signed certificate, e.g. for test purposes, is possible but not recommended for the operation of the system for security reasons.

Web clients must install this certificate in the web browser. The installation of self-signed certificates is not supported by all web browsers. Depending on the web browser, it is possible to define exceptions.

For more detailed information, refer to the operating instructions of the web browser.

Adapting system settings to changed IP address or computer name

See Changing the computer name or the IP address (Page 47).

See also

Handling certificates (Page 51)

2.4.4 User management

In the "User management" step, you configure which user management configuration the HMI device uses and whether users can log in to Runtime via RFID.

Using a configuration from the TIA Portal

In the following cases, select the option "Select local or central user management in TIA Portal":

- Only projects with a local user management are to run on the HMI device.
- Projects with a central user management are to run on the HMI device; Runtime and the UMC server or its agent are installed on different devices.
- Projects with local and central user management are to run on the HMI device, and Runtime and the UMC server or its agent are installed on different devices.

Procedure

1. Select the "Select local or central user management in TIA Portal" option.

Result

When you have completed your settings and the system has implemented the configuration, Runtime uses the user management configuration configured in TIA Portal.

Using a configuration from the system settings

Note

This option can only be selected in the following cases:

- A UMC server or its agent is installed on the HMI device.
- Or the Runtime installation has been started via the TIA Portal engineering DVD.

Select the option "Use central user management with the following configuration" if only projects with a central user management are to run on the HMI device and the UMC server of the central user management or its agent are to be installed on the same device as Runtime.

Procedure

1. Select the "Use central user administration with the following configuration" option.
2. Enter the address of the UMC server.
3. Optional: To enter the identity provider address manually, proceed as follows:
   - Clear the "Identity provider address generated by the UMC server" option.
   - Enter the identity provider address. Use the following notation:
     `"https://<Computer name>/umc-sso"`

Note

Automatic generation of the identity provider address

By default, the identity provider address is automatically generated based on the UMC server address.

Result

When you have entered your settings and the system has terminated the configuration, Runtime uses the UMC server configured here.

Note

Loading a project with local user management

When a project with local user management is loaded in Runtime, the user management connects to the UMC server configured here.

Enable login via RFID

For local web clients, WinCC Unified Runtime supports login with RFID and PM-LOGON.

Requirement

- The option "Select local or central user management in TIA Portal" is enabled.
- You are using local user management.
- PM-LOGON is installed on the HMI device.
  Information on the licensing and installation of PM-LOGON can be found in the PM-Logon user help. For more information click here (https://support.industry.siemens.com/cs/document/109810587/pm-logon-manual?dti=0&lc=en-DE).

Procedure

1. Select the "Enable login with RFID" option.

Result

- The logon via RFID is enabled.
  On the start of a local web client or on connection to Runtime, the web client automatically authenticates itself with the following user data:

A UMC user is already logged in on the HMI device via UMC Desktop Single Sign-on (DSSO)	
Yes	The logged-on user is used.
No	The default user is used.

  The operator can be changed with an RFID card.
- The communication with PM-LOGON uses port 5003.

See also

Changing users in runtime (Page 74)

2.4.5 Archive settings

In this step you configure the log database location and SQL server settings.

You have the following options:

- Select the target folder and the name of the log database.

  Note

  To avoid data loss, select a different location for storing databases than the project folder or do not change the project folder.

  See also section Loading projects (Page 46).

- Select the memory high limit of the SQL server.
  This option is only available if the Microsoft SQL server is installed.

2.4.6 Reporting settings

In this step you configure the settings for generating reports.

Specify the storage location for reports

Under "Storage location for reports" enter the local main storage location for reports. Select a local folder.

The folder is used in Runtime when the "Default" value was configured under "Storage location for reports" in TIA Portal in the Runtime settings of the Unified PC.

The folder serves as:

- Storage location for reports with the target "Local main storage location"
- Root folder for reports with the "File system" target type whose targets were added in the "Reports" control.
  The reports are stored in subfolders of the local main storage location.

Specify storage location for Reporting database

Under "Storage location for the Reporting database", you enter where the Reporting database is stored. Select a local folder.

The Reporting database stores the actions and settings made in Runtime in the "Reports" control.

The folder is used in Runtime when the "Default" value was configured under "Storage location for the Reporting database" in TIA Portal in the Runtime settings of the Unified PC.

Select the application for PDF creation

1. Select whether Excel or LibreOffice is to be used for the PDF creation of the reports.
   The selected application must be installed on the HMI device.
   If you select "Do not configure", no PDF files are created for the reports in Runtime.

   Note

   PDF creation for large reports

   Generating PDFs with Excel is significantly slower than with LibreOffice. To generate large PDF reports, it is therefore recommended that you install LibreOffice.

   Note

   Deviating PDF results possible

   A PDF report created by LibreOffice may differ in content or layout from a PDF report created with Excel. Such deviations are possible if general Excel functions that LibreOffice does not support are used in the report template, for example, special fonts or chart types.

2. When Excel is creating the PDFs: Specify the user name and password of the Windows user under whose name the PDF creation is running.
   During the Runtime installation, an appropriate user account is created.
   Do not use a user that already exists in Windows user management.
   Adhere to Windows policies for user passwords.

   Note

   Checking the security settings of the user management

   Clarify with your administrator whether the security settings of the Windows user management prevent the new user created on your device during the Runtime installation from being permanently available.

   If required, modify the settings or select LibreOffice as the application for PDF creation.

3. When LibreOffice creates the PDFs: Select the LibreOffice installation directory.

2.4.7 Loading projects

In this step, you make the settings for loading projects from the Engineering System.

Configure storage location for local Runtime projects

Default location for storing Runtime projects when loading them into the device (Runtime project folder): `C:\ProgramData\SCADAProjects`

You can configure a different storage location.

Procedure

1. Under "Storage location for local Runtime projects", click "Browse".
2. Select a drive and folder and confirm your entries.
3. (Optional) To move Runtime projects that have already been loaded to the new storage location, enable "Move existing Runtime projects to the new storage location".

Result

When applying the settings, the following occurs:

- The folder is set as the storage location for Runtime projects.
  The following applies:
  - This folder is used when downloading to the device.
  - Only Runtime projects from this folder can be started.
  - SIMATIC Runtime Manager only shows the Runtime projects of this folder.
- The Unified certificate store is moved to the new storage location.

  Note

  The web server certificate is configured in the IIS Manager and therefore cannot be moved.

  The device's certificates are still valid and will be used.
- If the "Move runtime projects" option is enabled: Projects already loaded on the Unified PC will be moved to the new location.

Restrictions when moving projects

The "Move Runtime projects" option is not available in the following cases:

- If one of the projects contains a database (e.g. alarm log or data log)
- If there is already a project in the new location that has the same name as a loaded project.

  Note

  To enable moving, delete the project with the same name manually from the new storage location before selecting "Apply settings" in WinCC Unified Configuration.

To avoid data loss when moving or later during runtime, no project is moved in these cases.

Activate secure download

To protect the projects with a password during download, follow these steps:

- Select the "Activate secure download" option.
- Enter the password and confirm it.

Note

Requirements for the password

- Length: 8 to 120 characters
- Characters: In each case at least one uppercase letter, one lowercase letter, one number and one special character

2.4.8 Changing the computer name or the IP address

Workflow

If the computer name or the IP address of a WinCC Unified HMI device changes after installing WinCC Unified, for example, when adding the computer to a domain, follow these steps:

1. After changing the computer name or IP address on the HMI device, run WinCC Unified Configuration.

   Note

   This step is not necessary if the IP address was changed, but access of the web clients to the website uses the computer name, or vice versa.

2. Renew the certificate configuration of the HMI device.
3. If the HMI device participates in Unified Collaboration, adapt the configuration of the other devices in the engineering system and download the change to the devices.
4. If you use central user management and change the computer name of a Unified PC, you must enter the new computer name on the UMC-S ring server manually in the whitelist. You can add the computer name of your WinCC Unified PC station to the UMC whitelist using the following command:
   umconf-c -w -d https://hostname/WebRH/webssoservice □
5. Restart the HMI device.

The projects loaded onto the HMI device using a user configuration loaded by TIA Portal are subsequently executable without reloading.

Note

Adapt the configuration of the HMI device in the engineering system before reloading the HMI device.

Running WinCC Unified Configuration

Note

The options "Only adapt to new computer names or IP" and "Make additional settings" are only available if the IP address or the computer name was changed.

1. Start WinCC Unified Configuration on the HMI device whose IP address or computer name was changed.
2. To only include the change to the computer name or the IP address in the configuration, follow these steps:
   - In the "Website settings" step, select the option "Only adapt to new computer names or IP".
   - Click "Next".
   - In the "Apply settings" step, click "Accept".
3. To change other settings, follow these steps:
   - In the "Website settings" step, select the "Make additional settings" option.
   - Make the desired settings in the step "Website settings" and in the following steps.
   - In the "Apply settings" step, click "Accept".

The Runtime system settings are automatically adapted to the changed computer name or the IP address.

Renewing the certificate configuration

1. Start WinCC Unified Certificate Manager on the computer that serves as the certification authority.
2. Delete the HMI device whose computer name or IP address has been changed from the Certificate Manager.
3. Add the HMI device again and enter the new computer name or the new IP address.
4. Generate the required certificates for the device.
5. Distribute and install the certificates.

Note

When a Unified PC is used as an HMI device as well as the certificate authority device, you must create, distribute and install the entire configuration of the certificate authority again after changing the name of the computer or its IP address.

When the certificate authority device is not used as an HMI device, there is no need to renew the certificate configuration.

2.5 Starting removal

Introduction

You have two options for removing:

- Removing selected components via the Control Panel
- Removing the product using the installation data medium

Note

Some components are not automatically removed by the uninstall routine of the software package as these are used for other purposes. For example, ALM is used to manage the license keys of several Siemens products.

Removing selected components via the Control Panel

To remove selected software packages, follow these steps:

1. Open the program list via "Start > Settings > Control Panel > Programs > Programs and Features".
2. Start the uninstall in Windows.
3. Select the Setup language.
4. Select the software components that you want to uninstall.
5. Check the selected uninstall settings.
6. Start the uninstall in the Setup.
7. Reboot the PC to complete the uninstall.

Removing a product using the installation medium

To remove all software packages, follow these steps:

1. Start the Setup.
2. Select the Setup language.
3. Select the full installation.
4. Check the uninstall settings.
5. Start the uninstall.
6. Reboot the PC to complete the uninstall.

2.6 Working with license keys

Introduction

To use WinCC Runtime Unified, transfer a license key to the Runtime PC.

When you transfer a license, the associated license key is removed from the storage location.

Note

A license key cannot be copied. The copy protection employed prevents the license keys from being copied.

Data backup

Transfer the license keys from the PC when backing up data on the PC and when creating a backup during device replacement.

You use the Automation License Manager to save license keys for PC-based HMI devices at the storage area of the license key.

NOTICE

Destruction of license keys on PCs

Transfer all license keys to a storage location in the following cases:

- Before you format the hard disk
- Before you compress the hard disk
- Before you restore the hard disk
- Starting an optimization program that moves fixed blocks
- Installing a new operating system

Read the description of Automation License Manager. Observe all warnings and notices.

The location of the license keys is capable of storing multiple licenses when the Automation License Manager is used on PC-based HMI devices. This capability means you can store multiple licenses of the same type at one location. Save all license keys of the HMI device to the same storage location.

Invalid license after time-zone change

The transferred license no longer functions in the following case:

- If you change the time zone on a WinCC PC as follows:
  - From a time based on a complete hour to a time not based on a complete hour.
    Example: You change the time zone from GMT +3:00 to GMT +3:30.

To work around this, transfer the license key from the HMI device with a time zone setting that was set when the license key was transferred to the HMI device.
Example:

You transferred the license key to the HMI device with a time zone setting based on a full hour. Then, also transfer the license key from the HMI device with a time zone setting based on a full hour.

This behavior does not apply to the trial license.

Defective license

A license is defective in the following cases:

- If the license key is no longer accessible at the storage area.
- If the license key disappears during its transfer to the destination drive.

Note

Resetting of the system status to an earlier time causes all licenses to become defective.

You can use the Automation License Manager to repair the defective licenses. Use the "Restore" function or the "Restore Wizard" of the Automation License Manager for this purpose. Contact Customer Support in order to restore the license.

Note

The runtime software can also be operated without errors if the license is missing or defective. The system alerts you with an alarm at brief intervals that you are working in non-licensed mode.

2.7 Handling certificates

Introduction

Communication between web clients (browser) and Runtime (web server) is encrypted. The communication partners authenticate themselves with a certificate. The web server certificate must be known to the web client browser as trusted.

You determine which certificate you are using when installing Runtime on the web server or at a later time in the WinCC Unified Configuration tool.

You have the following options:

- Create your own certification authority and use this certificate.
  Create the root certificate and the web server certificate with the WinCC Unified Certificate Manager tool.
- Use a self-signed certificate.

NOTICE
Security risk due to self-signed web server certificate Using a self-signed certificate, e.g. for test purposes, is possible but not recommended for the operation of the system for security reasons. Web clients must install this certificate in the web browser. The installation of self-signed certificates is not supported by all web browsers. Depending on the web browser, it is possible to define exceptions. For more detailed information, refer to the operating instructions of the web browser.

Using a certificate issued by a certification authority

With the WinCC Unified Certificate Manager, you can easily create your own certification authority, issue certificates with this certification authority and export them to distribute them to the required devices.

Using a self-signed web server certificate

Select the option "Create a new certificate" while installing the Runtime server or later in "WinCC Unified Configuration".

Add the self-signed certificate in each client that calls this server to the list of trusted certificates:

1. Open the desired browser.
2. In the address line, enter the host name or the IP of the Runtime server that was used when creating the certificate.
   You will receive a security warning.
3. Continue loading the web page.
4. Install the certificate in the certificate store "Trusted Root Certification Authorities".
5. If you receive a security warning as to whether you want to trust the certificate, confirm it with "Yes".
6. Load the page again.

Operating Unified PC

3

3.1 Basics

3.1.1 Process screens

Behavior of process screens

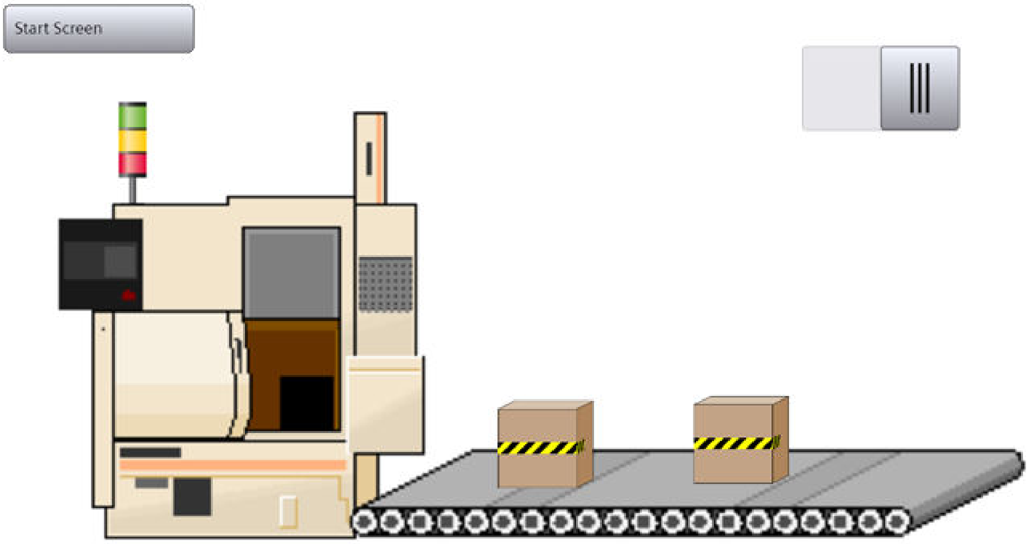
Process screens are static and dynamic representations of the plant, plant units or processes. You use the process screens to operate and monitor the plant or areas within it.

A project on an HMI device consists of multiple process screens. When you start Runtime, the process screen that was defined as the start screen is displayed. You navigate between process screens according to a sequence, navigation or link that was defined by the configuration engineer.

The process screen contains static and dynamic screen objects. Screen objects visualize the current process values from the controller memory and record operator inputs that influence the process. Dynamization is realized through the connection of tags to the screen object during configuration.

Process values and operator inputs are exchanged between the controller and the HMI device by means of tags.

A process screen can be opened and operated by several operating stations simultaneously in Runtime.



Note

Displaying a start screen changed by reloading

A start screen was defined for a project, and the project was started in Runtime. If another start screen is then defined in engineering and the project is loaded into the device again, the last active screen is displayed in Runtime after the connection is established again.

After reloading the project, refresh the screen in Runtime. If your HMI device is a computer, use the F5 key or the browser "Refresh" button to do this.

Screen navigation

Process visualization is generally split between multiple process screens, for example on the basis of functional or technological aspects. Changing between process screens is referred to as screen navigation.

Popup window

With corresponding configuration in the engineering system, clicking on a screen area opens a popup window containing additional information on the screen area.

Example: A screen represents a pump with its valves. When you click on a valve, a popup window opens with detailed information on the valve as well as input fields. You can check the state of the valve in the pop-up window and edit using the input fields.

Predefined styles

The following predefined styles are available for the process screens of the HMI devices:

- Light style
- Dark style
- Expanded style

Note

Compact mode in light and dark style

If the following elements in light or dark style fall below specific dimensions, they are automatically displayed in compact mode:

- Bar
- Slider
- Gauge
- Clock

3.1.2 Tags

Behavior of tags

Tags correspond to defined memory areas to which values are written and/or from which values are read. In runtime, tags are output in trends or tables, for example.

External tags correspond to the process values from the memory of an automation system. They are connected to the tags of a connected PLC.

Internal tags transport values within the HMI device. The internal tag values are only available as long as runtime is running.

Value changes to external tags

Value changes to external tags are triggered as follows in runtime:

- By a PLC
  The PLC changes the value of the connected PLC tags.
  During the next update of the external tags, the new value is written to the HMI process image.
- By operator actions or by a script running on the HMI device
  The value change requested in runtime is not directly applied from the HMI process image.
  Runtime transfers the value to the PLC. The PLC writes the value to the linked PLC tag after successful verification.
  During the next update of the external tags, the new tag value is written to the HMI process picture.

Acquisition mode and acquisition cycle for updating the tags are specified during configuration.

Executing the script of a trigger tag

The script defined for a trigger tag in engineering is executed in Runtime in the following cases:

- During start of Runtime
  The start value of the trigger tag is reported to Runtime.
- When the condition defined for the trigger tag occurs
  For example if the trigger tag changes its state or exceeds a limit value.

Floating point numbers in the web client

Since the web client is implemented via JavaScript, tag values for floating point numbers can only be displayed with a mantissa of up to 54 bits. This leads to rounding of values with a mantissa greater than 54 bit in Runtime.

Note

Values with a mantissa of up to 64 bits are correctly displayed by I/O fields.

Restricted scope of validity "local session"

By default, internal tags apply "system-wide".

As an option, the scope of validity of an internal tag can be limited to "local session". Data related to a session in a multi-user environment is processed independently in each local session.

The use of local session tags is supported in Unified Collaboration and in the web client.

Local session tags permit, for example:

- Individual navigation in screen windows or in different menu structures
- Session-related disabling/enabling of the user
- Session-related position, alignment and rotation of objects in a screen

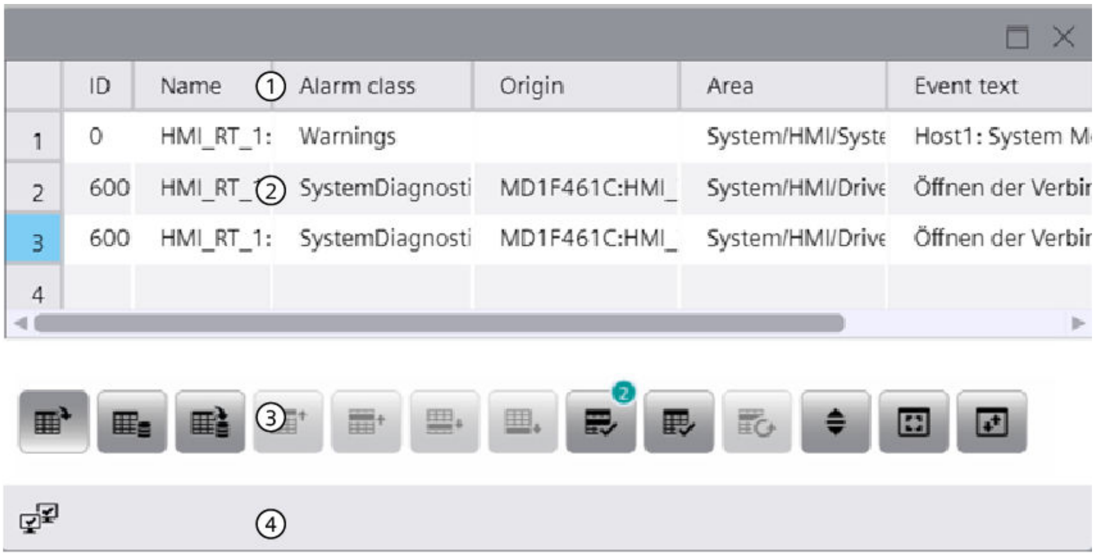
The values of a local session tag are not saved and will be lost at the end of a session.

3.1.3 Alarms

Behavior of alarms in Runtime

Depending on the configuration, PLC alarms and HMI alarms from various areas of the plant are displayed in Runtime.

Depending on the configuration, the alarms are labeled according to importance or type and are represented and displayed differently. For example, a pending alarm can be displayed as follows:



	ID	Name	Alarm class	Origin	Area	Event text
1	0	HMI_RT_1:	Warnings		System/HMI/Syste	Host1: System M
2	600	HMI_RT_	SystemDiagnosti	MD1F461C:HMI_	System/HMI/Drive	Öffnen der Verbir
3	600	HMI_RT_1:	SystemDiagnosti	MD1F461C:HMI_	System/HMI/Drive	Öffnen der Verbir
4						

3.1.4 Logs

Data log

In Runtime, the data logging functions on the server as a log server. On the clients, the data logging functions as a log client. Only the log server accesses the database and compiles and logs the process data. The clients receive log data from the log server.

The log data is visualized in tabular or graphic format on all clients running tag logging in Runtime. The data to be displayed always comes from the log server. All operations on the client are transmitted to the server and the result of the processing is transferred back to the client.

Alarm log

Alarms in the project indicate fault states and operating states of a process. They are generally triggered by the controller. Alarms are displayed on the HMI device in screens. All the data associated with an alarm and configuration data are saved in an alarm log, for example, alarm class, time stamp and alarm text. Each alarm class can be logged separately. Alarms are logged either automatically or by operator intervention.

3.1.5 Contexts

Contexts allow you to view plant units according to a certain viewpoint, e.g. according to a certain customer, product, job or shift.

Principle

Contexts always belong to a plant object. They are indicated as follows:

- User-defined contexts:
  Using a program created with the ODK-API
- System-generated contexts:
  For installed Performance Insight and Calendar option packages: Automatically in Runtime
  Example: When a shift starts in Calendar, an archived context value is created with the shift ID

A log entry is generated each time a context (e.g. "Product") is executed. The logged context saves:

- The context value (e.g. "orange lemonade")
- Start time and end time of the execution time
- The quality code

Contexts in the trend control and alarm control

You can filter the content of these controls so that only data that has been generated in a specific plant unit and for the context you have selected is displayed. To do this, select a plant object, a context and one of its logged context values.

Example

A press house produces juices for various beverage brands. Using contexts, employees can display in runtime which alarms have occurred:

- During the production of a specific product (cloudy apple juice, clear apple juice, pear juice etc.).
- For orders for a specific customer (Schmitt, Schulze, Meier).
- During a specific shift (early shift, late shift, night shift).

Contexts in the "Reports" control.

You have the option of linking the generation of reports to the execution of contexts.

If the templates are configured appropriately, the reports available in the control can also contain information about contexts. When a report was generated as an Excel file and reads both contexts and alarms or tag values, you can then use the Excel filter function to filter the alarms and tags by context.

See also

Display context-dependent alarms of a plant object (Page 112)

Display context data of the plant objects in a trend control (Page 151)

Adding contexts (Page 254)

3.2 Starting and displaying runtime

3.2.1 Internet browsers for WinCC Unified PC

Ensure you have the latest operating system and browser version if you want to access Runtime Unified with this device.

WinCC Unified displays the runtime elements in HTML5. The browser used also has to support this standard. Since the browsers interpret HTML5 differently, it is possible that objects are displayed differently depending on the browser and the browser version used. For example, browsers sometimes display fonts differently.

Compatibility tests were performed for the following browsers. The focus of the compatibility tests was on the browsers marked with *:

Operating system	Browser
Microsoft Windows	• Google Chrome* • Microsoft Edge • Mozilla Firefox, Mozilla Firefox ESR
Android	• Google Chrome* • Firefox • Edge
iOS, Mac	• Safari* • Google Chrome • Firefox • Edge

Browser recommendation

In view of the performance and support of the Runtime standard elements, Google Chrome has proven to be the preferred browser. Its memory requirements are slightly higher than those of the other browsers.

Note

Operating system and browser version

For Runtime operation via Android or iOS, always use the latest operating system.

Use the latest browser version.

Note

Performance differences in different versions of individual browsers

The browser versions can differ from each other, which can result in different behavior regarding the memory requirements and speed.

Note

Suitability for continuous operation

Mozilla Firefox has proven to be problematic in continuous operation.

Known browser problems

The following restrictions apply to the following browsers:

Internet browser	Limitation
MS Edge	• If you want to start Runtime in Microsoft Edge and enter the address "https://localhost", the error message "INET_E_RESOURCE_NOT_FOUND" appears. In this case, use the address "https://localhost/WebRH".
Mozilla Firefox	• High memory capacity utilization in continuous operation
Mozilla Firefox ESR	• Support of touch gestures for touch panels as of Firefox ESR V59
Google Chrome	• High memory capacity utilization in uninterrupted duty depending on the version. • On Android: Grid lines with a line width ≤1 are not displayed correctly. This is due to the browser's own line thickness representation. As a solution, it is helpful to use a line width ≥1. • No correct representation of elements that use an SVG graphic as background graphic scaled in the Engineering System.

Restrictions to the various functions can also occur, such as the availability of the before and after buttons in the controls.

Current information on browser problems

You can find up-to-date information on display problems in browsers at the Siemens Online Support under the entry ID 109757952.

3.2.2 Displaying runtime

Introduction

Use a web browser (web client) to display and operate the Runtime project running on the HMI device. The following options are available to access and display Runtime:

- From the same device (local web client)
  The web browser is installed on the same device as Runtime.
- Remote access from the same network
  The device on which the web browser is installed belongs to the same network as the HMI device.
- Remote access from a foreign network
  The device on which the web browser is installed does not belong to the same network as the HMI device.

Requirement

- The Runtime project is loaded on the HMI device.
- The project runs in runtime.
- The user management configuration of the project is active.
- When using the central user management:
  - At least one user is created in the UMC system.
  - The user created in the UMC system has been imported into the TIA Portal project before the loading.
  - The user has function rights via his/her roles to monitor or monitor and operate the Runtime project.
- When using the local user management:
  - Before the loading, at least one user has been created in TIA Portal.
  - The user has been assigned at least one role. The user has function rights via his/her roles to monitor or monitor and operate the Runtime project.
  - At least one user has the "HMI Administrator" role.

Procedure

1. To view the Unified start page, enter the Unified URL in the browser address bar: "`https://<IP address of the HMI device or its FQDN or device name>`"
   To display the Unified Runtime page directly, append the following string to the URL: "`/WebRH`"
   Step 5 is omitted.
   Example: "`https://141.73.65.245/WebRH`"

   Note

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name in the URL depends on how the web server certificate has been bound to the HMI device. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   The following restrictions apply to entering the URL:

   - FQDN: Only if the HM device belongs to a domain
   - IP address: Not when using dynamic IP addresses
   - Device name: Only when accessing from the same network

   Note

   When using a local web client, you can also enter the "`localhost`" command.

   Example: "`https://localhost/WebRH`"

   Regardless of whether the web server certificate is already installed in the browser, you will first see a security warning. Bypass this warning by clicking "Advanced" and "Continue to <link> (unsecure)".

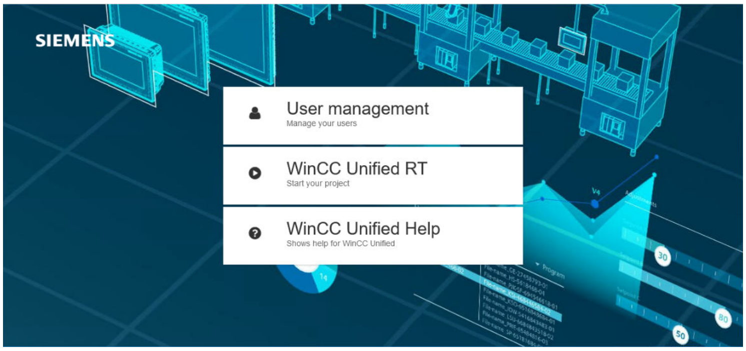
2. Press Enter.

3. If you are accessing the Runtime of the HMI device from this device for the first time and there is no corresponding certificate, install the certificate in the browser. Then reload the page.

4. The start page of Runtime is displayed.

Note

If you experience display problems in the web client, completely delete the browser data (history, form entries, etc.).



If WinCC Unified Online Engineering is installed on the device, the "WinCC Unified Configuration" button also appears.

5. Select "WinCC Unified RT".
   The login page of WinCC Unified Runtime is displayed.

Note

After a complete download of a project, an error (SwacLogin) may occur when opening the WinCC Unified Runtime page.

You can find more information at SwacLogin: Errors after complete download (Page 70).

6. Specify the user name and password of a runtime user.
7. (Optional) Select the language in which runtime is displayed.
8. Confirm your entry.
   The Runtime project that is running is displayed in the web browser.

Note

Displayed runtime language

When using central user management, runtime is displayed in the language you have selected in the "User login" dialog during login.

If this language is not available for the current project or if the language setting was not set in the central user management, the following language is displayed:

- Engineering with TIA Portal: The language for which the lowest number was configured in the runtime settings.
- Engineering with Online Engineering: The language set as default language in the "Languages" tab in the "Languages and Resources" editor.

If you do not select a language in the "User login" dialog, runtime is displayed in the language that is set for the browser.

See also

Changing users in runtime (Page 74)

Activating automatic login (Page 575)

Starting and stopping a project (Page 76)

Installing a certificate when accessing via web client (Unified PC) (Page 64)

Activating user management (Page 581)

User management (Page 42)

3.2.3 Installing a certificate when accessing via web client (Unified PC)

Using root certificates

To enable web browsers to establish a secure connection to WinCC Unified, the root certificate with which the web server certificate of WinCC Runtime was issued must be known in the web browser as a trusted certification authority.

By installing the web server certificate on the PC device, the public root certificate is made available as a download for installation in web browsers on the WinCC Unified home page.

The procedure for installing the root certificate differs depending on your web browser.

Use of self-signed certificates

As an alternative to the root certificate, you can use a self-signed certificate.

NOTICE
Security risk from self-signed certificate A self-signed certificate is not issued by a trusted certification authority. If you use a self-signed certificate from an untrustworthy source, the data transfer is not protected from attacks. Before using self-signed certificates, check the source. Depending on the firewall and network settings, the use of self-signed certificates may be prohibited.

The installation of self-signed certificates is not supported by all web browsers. Depending on the web browser, it is possible to define exceptions.

For more detailed information, refer to the operating instructions of the web browser.

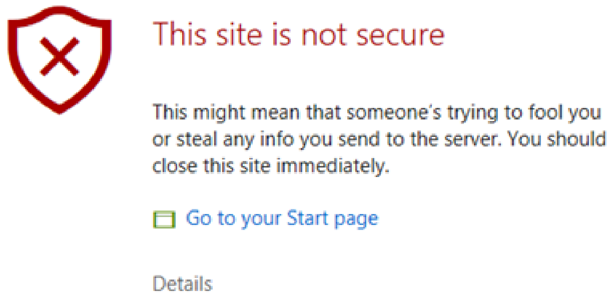
Installing the root certificate for Chrome and Microsoft Edge

Chrome and Microsoft Edge use the Windows system certificate store.

- On devices **with WinCC Unified installation**, whose certificates have been configured with the WinCC Unified Certificate Manager, these web browsers can immediately establish a secure connection to the WinCC Unified web pages because the root certificate has already been installed in the system certificate store.
- On devices **without WinCC Unified Installation** the root certificate must be installed manually.

To install manually, follow these steps (for example, Microsoft Edge):

1. Open the WinCC Unified home page via the URL https://<host name>
   At first, an error message appears:

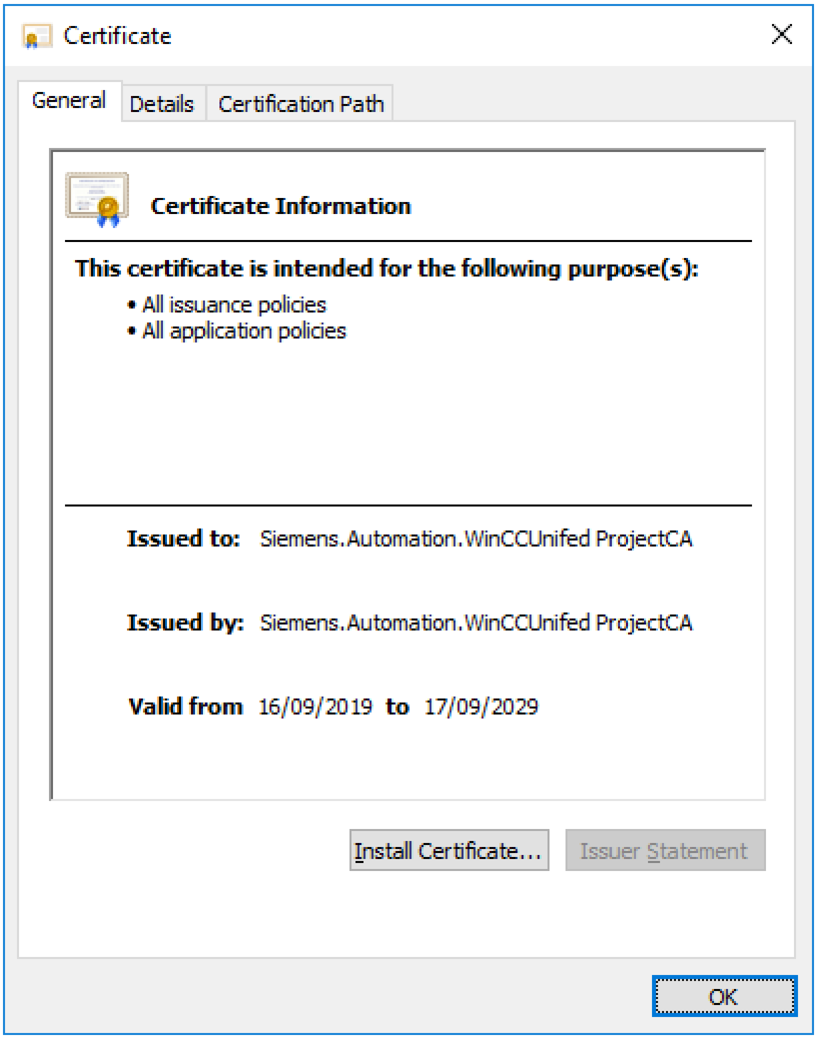


This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

2. Open the field with the error details and confirm that you want to open the web page.
3. On the WinCC Unified home page, select the field "Certificate Authority" and confirm "Open file" in the download dialog.
   The root certificate is downloaded to the default download directory.

4. Open the downloaded file.
   The root certificate is opened with the Windows standard form.



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: Siemens.Automation.WinCCUnifed ProjectCA

Issued by: Siemens.Automation.WinCCUnifed ProjectCA

Valid from 16/09/2019 **to** 17/09/2029

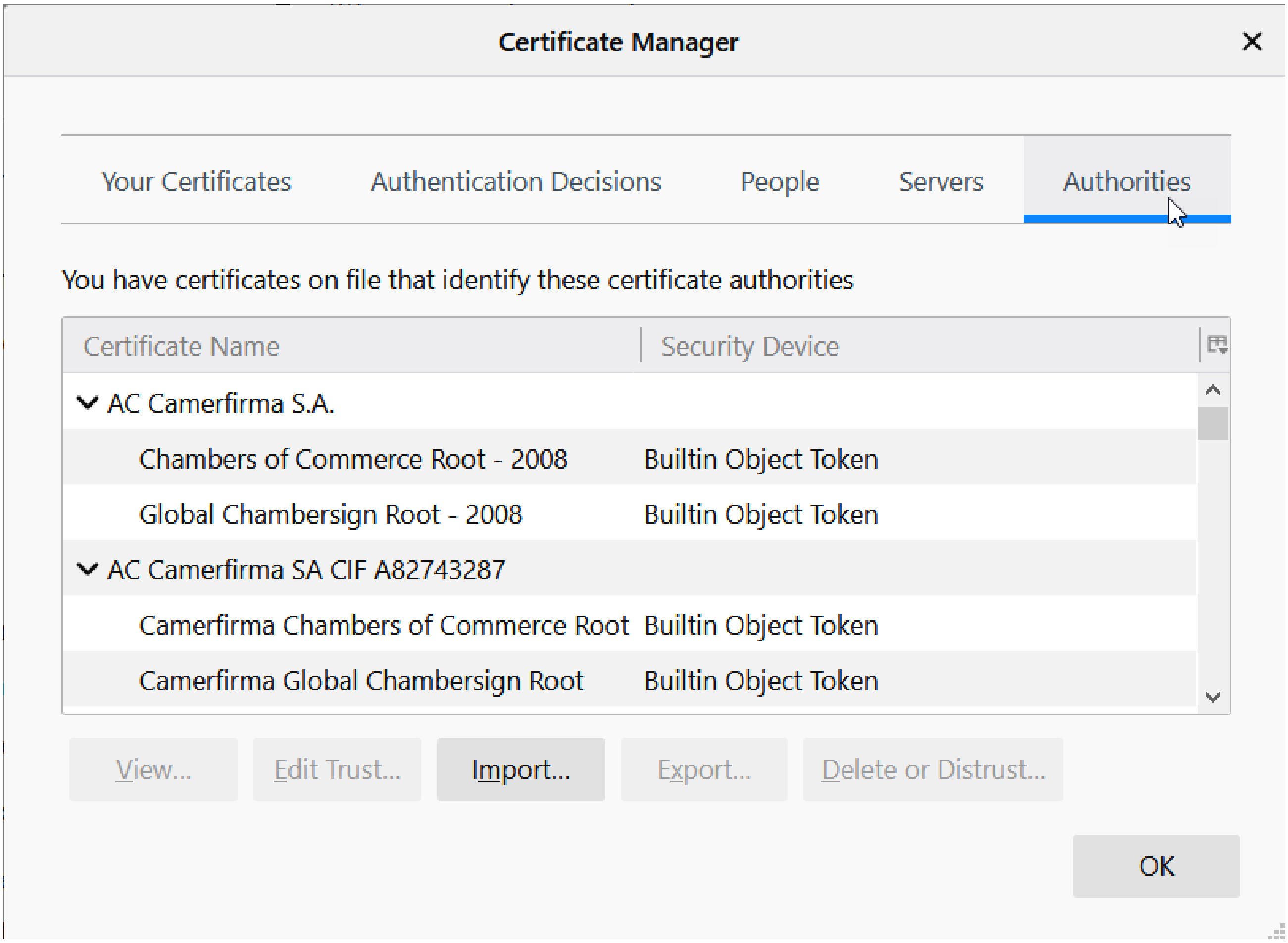
5. To import the root certificate into Windows, select "Install Certificate".
6. In the certificate import wizard, select "Local Machine" as the storage location, "Trusted Root Certification Authority" as the certificate store and start the import process.

Installing the root certificate for Firefox

Firefox uses its own certificate store and must therefore be configured manually on each device once:

1. Open the WinCC Unified home page via the URL https://<host name>
   At first, an error message appears.
2. Open the field "Advanced" and confirm the field "Accept the Risk and Continue".
   An exception is entered for this page in the Firefox certificate management.
3. On the WinCC Unified home page, select the field "Certificate Authority".

4. Save the root certificate. To do this, click "Save file" in the Firefox dialog that follows.
5. Store the certificate in the Firefox certificate store. Proceed as follows:
   – Open the "Settings" page of Firefox.
   – Select "Privacy & Security". There you will find the "Certificates" area further down. Open "Show certificates...".
   – In the "Certificate Management" window, select the "Certification authorities" tab:



You have certificates on file that identify these certificate authorities

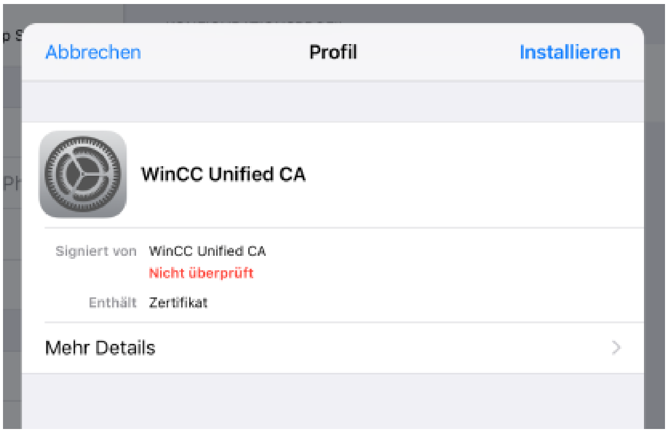
Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

   – Click "Import" and select the root certificate you saved in step 3.
   – In the window that opens, select the option "This certificate can identify websites" and confirm your selection.
     The connection to Runtime is now secure. In the Firefox address bar it is still displayed as unsecure.
   – To show the connection as secure in the address bar, click "Server" and remove the exception created by step 2.

Installing the root certificate on iOS devices

iOS uses its own certificate store and must therefore be configured manually on each device once. An error message also appears when the WinCC Unified home page is opened.

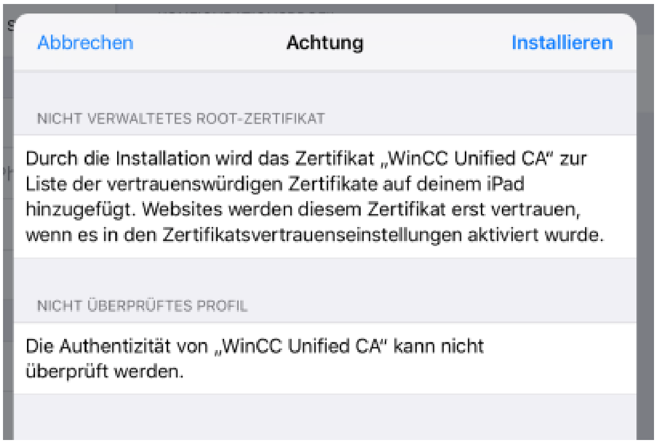
1. Open the field "Advanced" and confirm the field "Accept the Risk and Continue".
2. On the WinCC Unified home page, select the field "Certificate Authority".



WinCC Unified CA

Signiert von WinCC Unified CA
Nicht überprüft
Enthält Zertifikat

3. Select "Install".



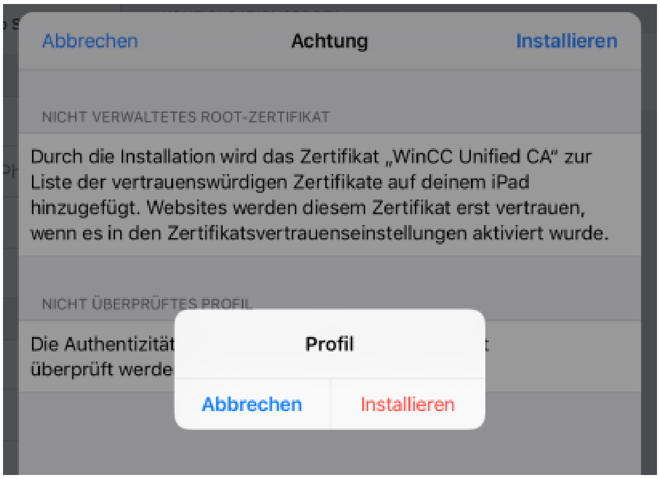
NICHT VERWALTETES ROOT-ZERTIFIKAT

Durch die Installation wird das Zertifikat „WinCC Unified CA“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

NICHT ÜBERPRÜFTES PROFIL

Die Authentizität von „WinCC Unified CA“ kann nicht überprüft werden.

4. Select "Install" again.



Abbrechen Achtung Installieren

NICHT VERWALTETES ROOT-ZERTIFIKAT

Durch die Installation wird das Zertifikat „WinCC Unified CA" zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

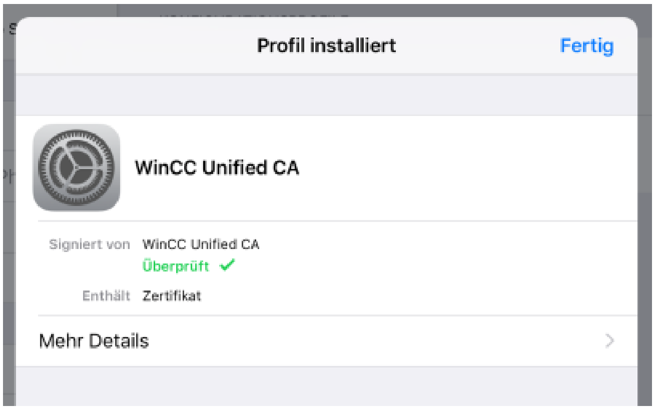
NICHT ÜBERPRÜFTES PROFIL

Die Authentizität
überprüft werde

Profil

Abbrechen Installieren

You see the entry "Trusted".



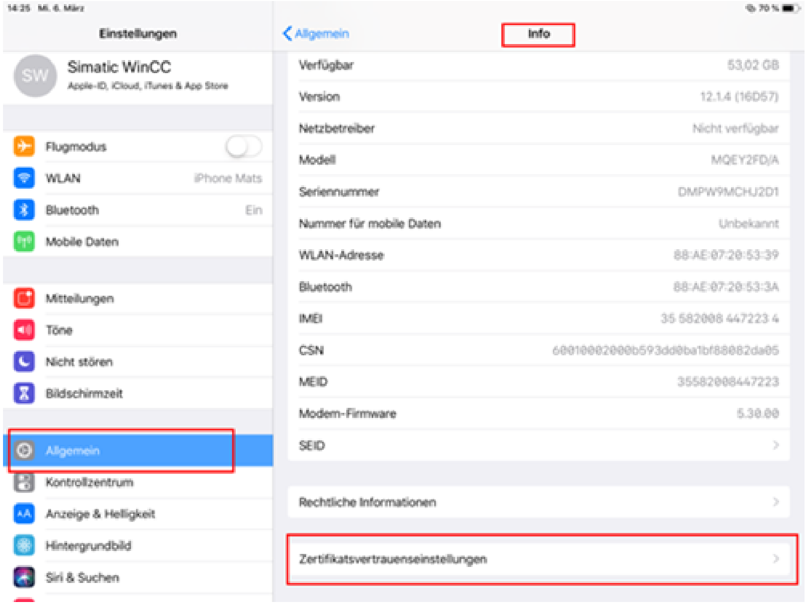
Profil installiert Fertig

WinCC Unified CA

Signiert von WinCC Unified CA
Überprüft ✓
Enthält Zertifikat

Mehr Details >

5. Select "General > Info > Certificate Trust Settings".



Verfügbar 53,02 GB

Version 12.1.4 (16D57)

Netzbetreiber Nicht verfügbar

Modell MQEY2FD/A

Seriennummer DMPW9MCHJ2D1

Nummer für mobile Daten Unbekannt

WLAN-Adresse 88:AE:07:20:53:39

Bluetooth 88:AE:07:20:53:3A

IMEI 35 582008 447223 4

CSN 60010002000b593dd0ba1bf88082da05

MEID 35582008447223

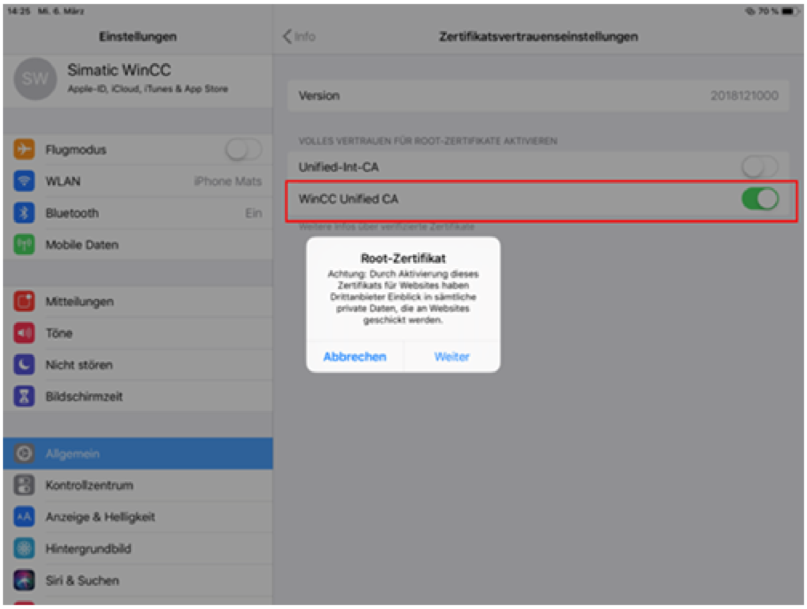
Modem-Firmware 5.30.00

SEID

Rechtliche Informationen

Zertifikatsvertrauenseinstellungen

6. Enable "WinCC Unified CA" and select "Next".



Version 2018121000

VOLLES VERTRAUEN FÜR ROOT-ZERTIFIKATE AKTIVIEREN

Unified-Int-CA ○

WinCC Unified CA ●

Weitere Infos über verifizierte Zertifikate

Root-Zertifikat

Achtung: Durch Aktivierung dieses Zertifikats für Websites haben Drittanbieter Einblick in sämtliche private Daten, die an Websites geschickt werden.

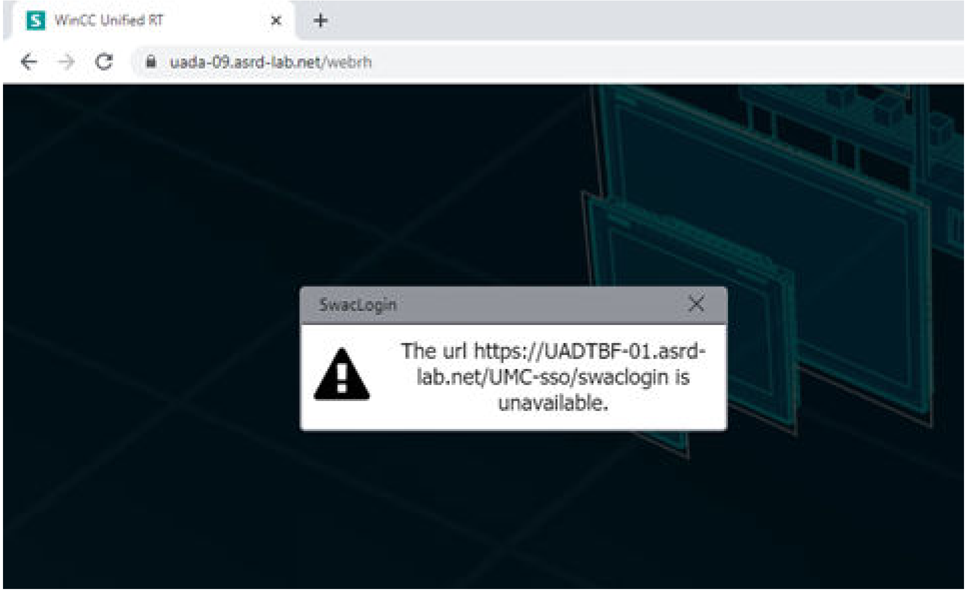
3.2.4 SwacLogin: Errors after complete download

After complete download of a project to a Unified PC, an error can occur when you open the WinCC Unified home page. The error can occur regardless of whether you open the home page locally on the PC or from a different device.

A possible cause of the error is the deletion of the browser cache.

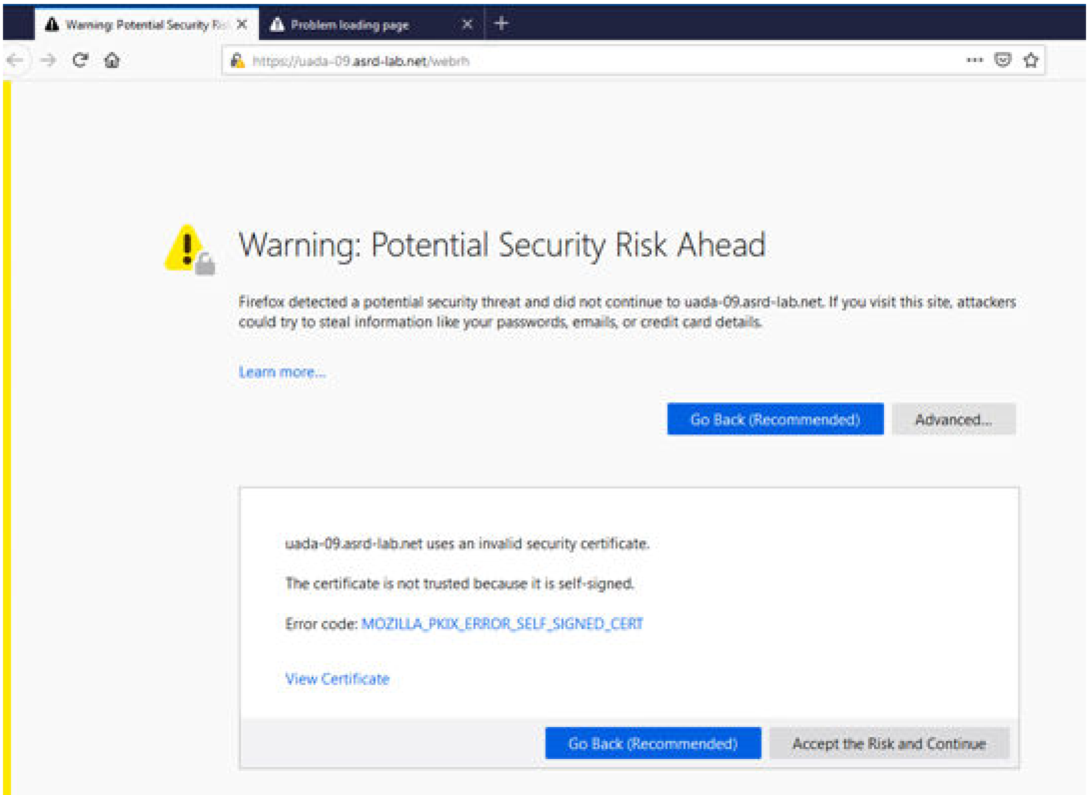
Error description

In "Chrome" and "MS Edge", the error is displayed with the following alarm:



The url https://UADTBF-01.asrd-lab.net/UMC-sso/swaclogin is unavailable.

In "Firefox", the error is displayed with the following alarm:



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to uada-09.asrd-lab.net. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

uada-09.asrd-lab.net uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

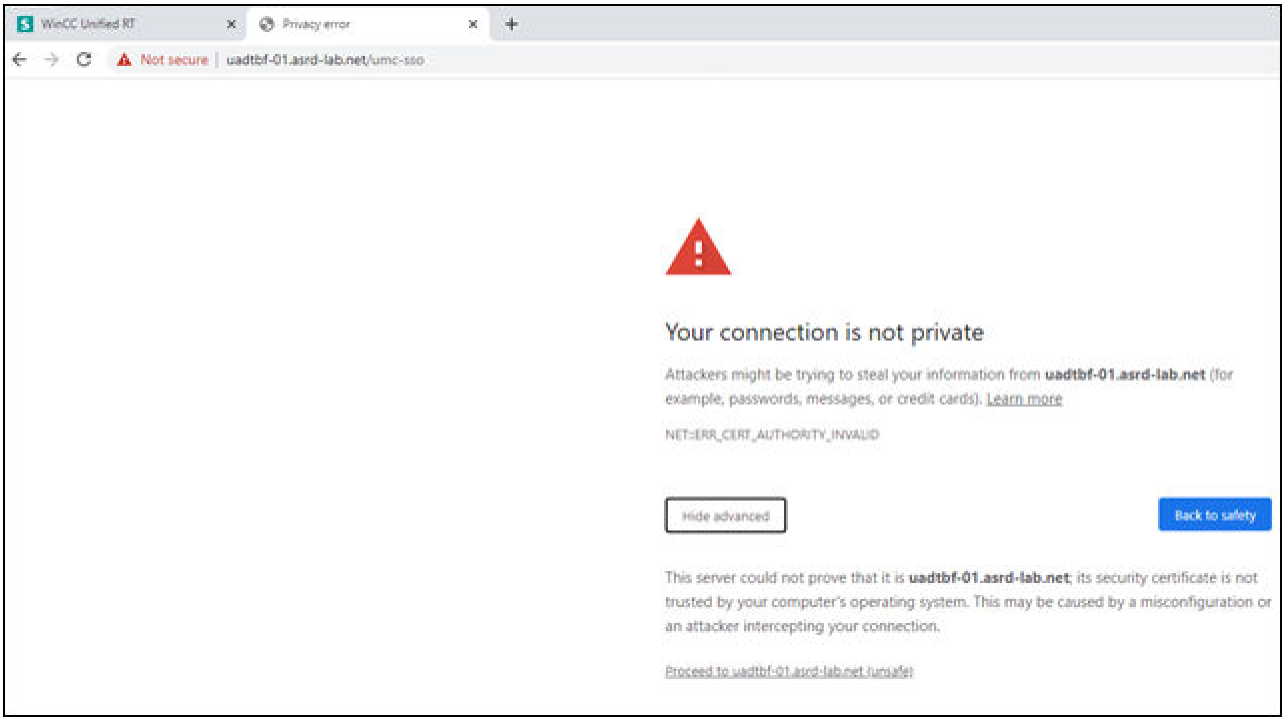
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

After accepting the warning of a potential security risk, the page remains empty in Firefox. Only the background screen is visible.

Remedy the error in "Chrome" and "MS Edge"

To fix the error in "Chrome" and "MS Edge", proceed as follows:

1. Open a new tab.
2. Enter the URL address of the identity provider of the UMC server in the address line of the browser. The URL is the same as the one in the error message without "/swaclogin", for example, "https://uadtbf-01.asrd-lab.net/umc-sso".
3. The page with a warning regarding the secure connection is displayed.



Your connection is not private

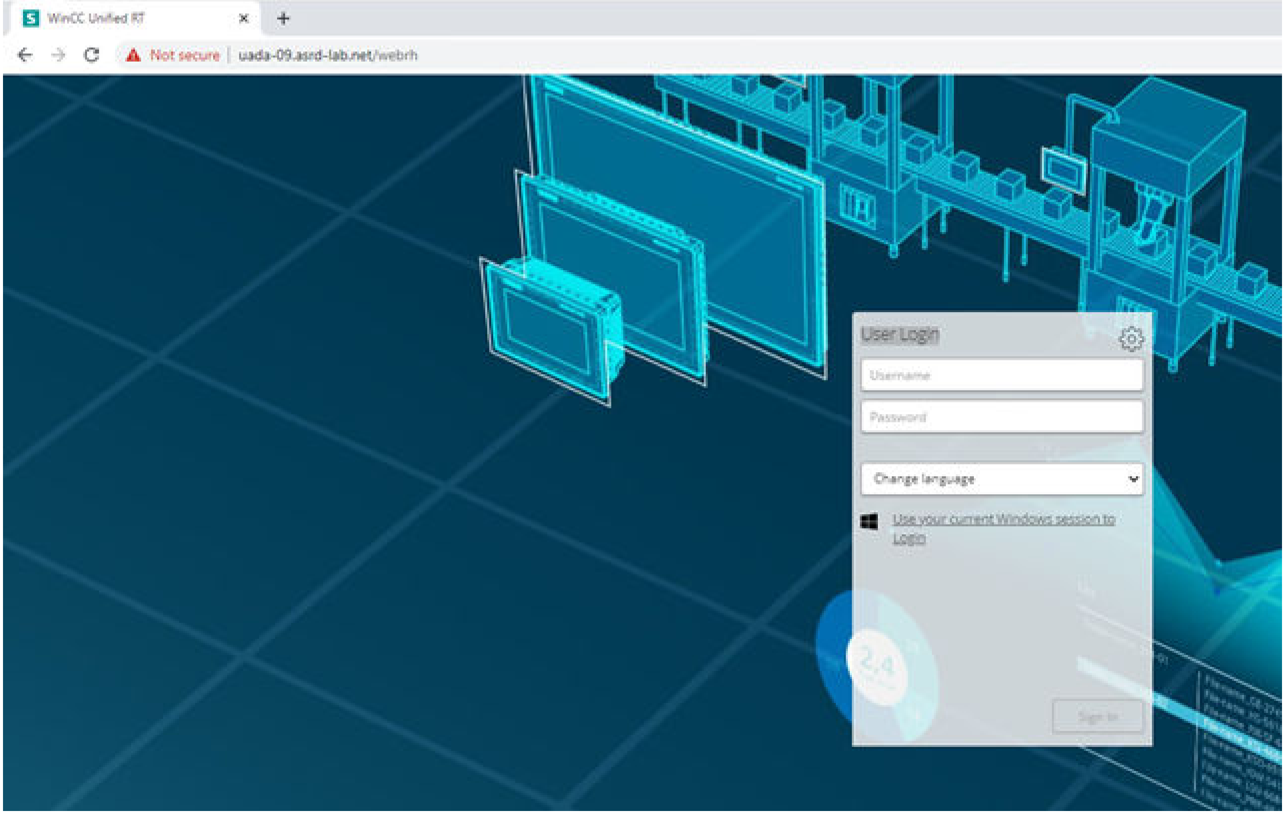
Attackers might be trying to steal your information from **uadtbf-01.asrd-lab.net** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **uadtbf-01.asrd-lab.net**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to uadtbf-01.asrd-lab.net (unsafe)

4. Accept the warning by clicking on "Proceed to uadtbf-01.asrd-lab.net (unsafe)".
5. The home page with the "User login" dialog is displayed.



Remedy the error in "Firefox"

To remedy the error in "Firefox", follow these steps:

1. Open a new tab.
2. Enter the URL address of the identity provider of the UMC server (ring server) in the address line of the browser, for example, "https://uadtbf-01.asrd-lab.net/umc-sso".
3. A blank page opens. Close the page.
4. Refresh the home page with the function key <F5>. The home page with the "User login" dialog is displayed.

See also

Displaying runtime (Page 60)

3.2.5 Logging out user

If you want to end your Runtime session, you have the following options to log out completely:

- Use the "Logout" system function.
- Log out in the user management.
- Close all instances, i.e. open windows, of the browser in use.

Requirement

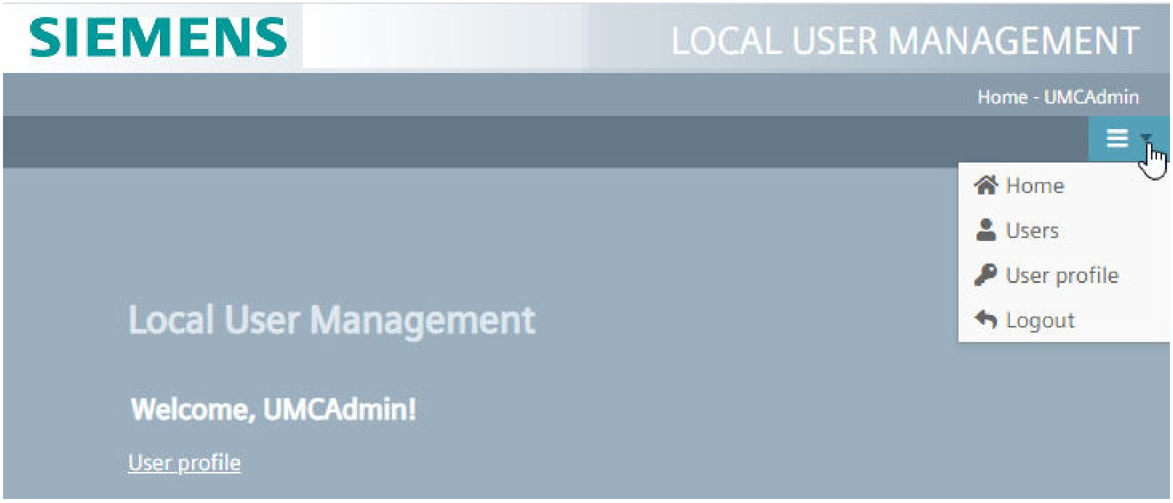
- You are logged in to Runtime.
- When you want to log out in the Runtime project, the system function "Logout" is configured, for example, to the event "Click left mouse button".

Logging out in the Runtime project with the system function "Logout"

- Select the button at which the system function "Logout" is configured.

Logging out in the user management

- Select "Logout" from the menu.
  Your session is ended.



New data downloaded from the TIA Portal is applied during the next login.

3.2.6 Changing users in runtime

Introduction

In Runtime, the users that are created in the engineering system can log on.

Requirement

- The IP address or the fully qualified name (name and domain) of the PC on which Runtime is installed is entered in the browser.
  If Runtime is installed on the same PC as the browser, the "localhost" designation can also be used.
- A user is logged into runtime.
  You log in by selecting "WinCC Runtime RT" or "User management".

Procedure

To log off a user and then log on a different user, proceed as follows:

1. Select "User management" on the start page of Runtime.
2. Expand the menu at the top right.
3. Select "Logout".
4. Log in with a different user.

Change logged-on user via RFID card

For local Web clients, WinCC Unified Runtime supports login with RFID and PM-LOGON.

Requirement

- Runtime uses local user management.
- Logon via RFID is active for the HMI device.
  This setting is made during installation of Runtime or later in WinCC Unified Configuration in the "User management" step.
- PM-LOGON is installed on the HMI device.
- The teach-in of the used RFID card with PM-LOGON is completed.
- An RFID reader supported by PM-LOGON is connected to the HMI device.
- The local web client is opened and connected to Runtime.
- A user is logged into runtime.

Procedure

1. Hold the RFID card in front of the reader or insert the card into the reader.
2. If the entry of a PIN was set in PM-LOGON during the teach-in of the card, enter the PIN.

Result

After successful validation of the credentials stored on the card, the user logged-on in Runtime is changed.

If the card requires PIN entry and an incorrect PIN is entered, the previously logged-on user remains logged on.

Note

There is no system feedback about the user change. If required, process screens can be configured in engineering to display the logged-on user.

Note

Additional information on PM-LOGON

See the PM-LOGON user help for information:

- For licensing and installation of PM-LOGON
- To the card readers supported by PM-LOGON
- To the teach-in of the RFID cards.

You can find the PM-LOGON user help at https://support.industry.siemens.com/cs/document/109810587/pm-logon-manual?dti=0&lc=en-DE (https://support.industry.siemens.com/cs/document/109810587/pm-logon-manual?dti=0&lc=en-DE).

See also

User management (Page 42)

3.2.7 Starting and stopping a project

A project must be running on the HMI device for Runtime to be displayed.

If no project is running, follow these steps:

1. Start the SIMATIC Runtime Manager tool on the HMI device.
2. Use the tool to get an overview of which projects are loaded on the HMI device.
3. Start the desired project.

You can find more information about the functions of the SIMATIC Runtime Manager and its operation, in the "SIMATIC Runtime Manager" user help.

See also

SIMATIC Runtime Manager functions (Page 565)

3.2.8 Switching the Runtime language

Introduction

The project running on the HMI device can be configured in multiple languages. If a corresponding operating element has been configured, you have the option of switching the language set on the HMI device during ongoing operation.

The project always starts with the language set in the previous session.

Requirement

- The desired language for the project is available on the HMI device.
- An operating element is configured, for example, a button that is linked to the language switching function.

Procedure

You can switch between the languages at any time in runtime. Language-specific objects are immediately displayed on the screen in the new language when you switch languages.

Depending on the configuration, you have the following options:

- Use a configured operating element to switch from one language to the next in a list.
- Use a configured operating element to directly set the required language.

3.3 Runtime operation

3.3.1 Overview

Operating variants

The following operating options for Runtime are available:

- Operation with the touch screen
  The device of the web client has a touch-sensitive touchscreen. Use your finger or a suitable touch pen to operate the touch screen.
- Mouse and keyboard operation
  The device of the web client has a mouse and keyboard.

Adhere to the instructions for operating the device in the operating instructions.

Individually configured operation

The configuration engineer has various options available for setting up operation.

Examples of actions whose execution is always determined on a project-specific basis:

- Screen change
- Reporting
- Change the Runtime language

There are no specific operating elements to execute certain functions. The configuration engineer specifies the project-specific execution. The screen change can be triggered, for example, via a button.

Information on project-specific operations can be found in the system documentation.

3.3.2 Operation with the touch screen

3.3.2.1 Overview of operation with the touch screen

Special features when operating using the touch screen

Operation with the touch screen is characterized by the following special features:

- Enable
  To enable the operating element, use your finger or a suitable touch pen to operate the touch screen. To generate a double-click, touch the operating element twice in rapid succession.
- Value input
  You enter numbers and letters on the touch screen with a screen keyboard.

Input using the screen keyboard

The screen keyboard is displayed when you select a screen object that requires input. The screen keyboard is hidden again when input is complete.

Further information on the screen keyboard can be found in the operating instructions of the HMI device.

3.3.2.2 Supported gestures

Definition

Various touch gestures are available for the runtime operation on touch devices. Some touch gestures have different effects in the process screens than in the controls.

Note

No operation with three or more fingers.

Only use one or two fingers when operating with touch gestures.

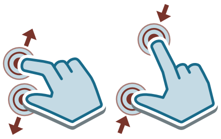
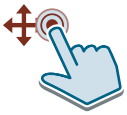
If you use more than two fingers with touch gestures, this can cause incorrect operation.

In the case of multi-touch operation with several fingers, you only operate the respectively configured objects.

Requirement

- Zoom gestures: Zooming was configured in the engineering.
- Move in process screen and screen window with 2-finger gesture: Zooming was configured in the engineering.

Supported touch gestures in process screens

Icon	Gesture	Function
	Tap	To select an object, tap on the corresponding position in the process screen.
	Zoom	To zoom in or zoom out, drag simultaneously with two fingers. For restrictions on the starting point of the gesture, see section Special features of touch operation (Page 82). The fingers form the zoom center. With the exception of pop-up windows opened in the process screen, the entire content of the process screen is zoomed.
	Drag with one finger	After zooming in a process screen, you can move the screen section. To do this, drag with one finger in the desired direction. For restrictions on the starting point of the gesture, see section Special features of touch operation (Page 82). Pop-up windows open in the process screen are not moved with it.

Icon	Gesture	Function
	Drag with two fingers	With the appropriate configuration in the engineering, you can also move the screen section with two fingers, as single gesture or in combination with the zoom gesture.
	Keep pressed	To call the shortcut menu, press for longer than a second on the object or the link. The function corresponds to a right-click.

Supported touch gestures in screen windows

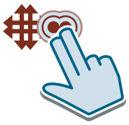
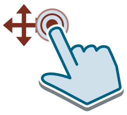
The following gestures in the screen window only affect the screen window, not the process screen:

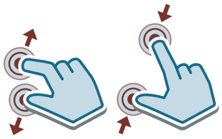
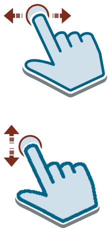
Icon	Gesture	Function
	Drag with one finger	After zooming into a screen window, you can move the screen window section. To do this, drag with one finger in the desired direction. For restrictions on the starting point of the gesture, see section Special features of touch operation (Page 82).
	Drag with two fingers	With the appropriate configuration in the engineering, you can also move the screen window section with two fingers, as a single gesture or in combination with the zoom gesture.
	Zoom	With corresponding configuration in the engineering, you can enlarge or reduce the screen window section independent of the zoom factor of the process screen. Drag simultaneously with two fingers (zooming). If the screen window section is smaller than the content configured for the screen window due to zooming, the fingers serve as zoom center, otherwise the upper left corner of the screen window.

The following gestures work analogously to the gestures supported in the process screen:

- Tap
- Keep pressed

Supported touch gestures in controls

Icon	Gesture	Behavior	Supported WinCC controls
	Tap	- To select a row, tap the row. - With corresponding configuration of the control: To select a cell. - To sort a column, click on the column header. - In trend controls: Zooms in on the trend area along the X/Y axis. Requirement: The "Zoom +/-", "Zoom time axis +/-" or "Zoom value axis +/-" button is pressed.	- Alarm control - Process control - Trend control - f(x) trend control - Ruler window - System diagnostics control - Parameter set control
	Tap with two fingers	Zooms out of the trend control. Requirement: The "Zoom +/-", "Zoom time axis +/-" or "Zoom value axis +/-" button is pressed. Leave a little space between your fingers when tapping.	- Trend control - f(x) trend control
	Drag with two fingers	To scroll vertically or horizontally in the table of the control, drag in the control window with two fingers in the desired direction.	- Alarm control - Process control - Ruler window - System diagnostics control - Parameter set control
	Drag with one finger	- Moves the ruler. - Moves the X axis or Y axis. Requirement: The "Move trend area" or "Move axis area" button is pressed or the control is zoomed in.	- Trend control - f(x) trend control
		To select multiple rows, tap a row and drag your finger up or down. With corresponding configuration of the control: To select multiple cells.	- Alarm control - Process control - Ruler window - System diagnostics control - Parameter set control
		To adapt the column width, tap a column grid line and drag your finger to the right or left.	
	Double tap	To edit a cell value, double-tap the cell. Requirement: - Table view: The "Edit" button is pressed. - Parameter set control: A parameter set is selected.	- Process control - Parameter set control

Icon	Gesture	Behavior	Supported WinCC controls
	Zoom	To zoom in or out in the trend control, drag with two fingers in the control window. Requirement: Trend control is paused and no zoom button is active. Or "Move trend area" is active.	Trend control
	Swiping (horizontally and vertically)	To quickly scroll left or right or up or down within the table of the control, swipe in the corresponding direction.	• Alarm control • Process control • Ruler window • System diagnostics control • Parameter set control

3.3.2.3 Special features of touch operation

Multi-touch operation of process pictures

WinCC Unified supports multi-touch operation in screens.

Simulation of projects with multi-touch functions

WinCC Unified supports the simulation of configured multi-touch functions. Requirement is that your monitor supports multi-touch operation.

Restrictions for touch gestures

Do not start the move 1-finger gesture or 2-finger gesture on the following objects:

- Release button
- Buttons with configured "Release" or "Press" event.
- "Browser" controls
- Custom web controls
- Touch area
- Elements and controls that manage touch gestures themselves (e.g. sliders and trend control)

Releasing locked operator controls by two-hand operation

Unified supports safe operation of controls that can be used to change critical system settings, such as control variables with machine limits. Such operator controls can be configured as locked.

Locked operator controls are displayed dimmed in runtime. To operate them, simultaneously press the release button provided for this purpose.

Releasing the locked operator controls by pressing the release button has a cross-screen effect on all open screens.

In Runtime, locked operator controls can only be accessed with the tab sequence if a release button is pressed at the same time.

Scrolling in lists and controls

You can scroll through lists and controls by dragging.

Special features of the trend control

You enlarge or reduce the view in "Trend control" and "function trend control" objects by pinch-to-zoom with two fingers.

Double tap to switch from the magnified trend control back to the normal view.

The zooming function is limited to the time axis in the "Trend control" object.

If you have enabled the option "Range > Auto-size" during configuration of the value axes in function trend control, the axes are constantly calculated during zooming.

Horizontal scrolling is not supported in the "Trend control" object.

Note

Current view is not persistent

The changes of zoom factor and position changed by scrolling are not saved.

The trend control is reset to the default setting during a screen change.

3.3.3 Zooming and moving in process screens and screen windows

Introduction

Depending on the configuration in the engineering, you have the following options in runtime:

	Zooming with	Move screen section with
Process screen	• Mouse • Keyboard • 2-finger gesture	• Mouse • Keyboard • 1-finger gesture • 2-finger gesture
Screen window		

This section describes how to zoom and move using the mouse and keyboard.

For information on zooming and panning with gestures, see sections Supported gestures (Page 79) and Special features of touch operation (Page 82).

General requirement

- The process screen or the screen window has the focus.
- For zooming: Zooming has been configured in the engineering.
- For moving: The process screen or screen window has been zoomed.

Starting point

Possible starting points for zooming or moving in process screens and screen windows are:

- An empty area
- Objects that cannot be zoomed or moved by themselves
- Buttons for which no "OnUp" or "OnDown" event has been configured by default

Zoom

Using a mouse

Your procedure depends on how zooming in engineering was configured in the runtime settings:

	Zooming with <Ctrl> configured (default)	**Zooming without <Ctrl> configured**
Zoom in	Hold down <Ctrl> and move the mouse wheel upwards.	Move the mouse wheel upwards.
Zoom out	Hold down <Ctrl> and move the mouse wheel downwards.	Move the mouse wheel downwards.

Scroll center is the mouse pointer.

Using a keyboard

- To zoom in, press <Ctrl + Plus>.
- To zoom out, press <Ctrl + Minus>.

Scroll center is the upper left corner.

Result

The entire content of the process screen or screen window is zoomed. Open pop-up windows are not zoomed.

Moving a screen section

Using a mouse

- Move to the left or right: Hold down the left mouse button and move the mouse in the desired direction.
- Move up or down:
  Your procedure depends on how zooming in engineering was configured in the runtime settings:

	Zooming with <Ctrl> configured (default)	Zooming without <Ctrl> configured
Moving up	Move the mouse wheel upwards.	Hold down <Ctrl> and move the mouse wheel upwards.
Moving down	Move the mouse wheel downwards.	Hold down <Ctrl> and move the mouse wheel downwards.

Using a keyboard

Use the following keys:

- Arrow keys: Move left/right and up/down
- Screen keys: Move up/down
- <Home>: Show upper left corner
- <End>: Show lower right corner

Result

The entire content of the process screen or screen window is moved. Open pop-up windows are not moved.

3.3.4 Triggering an action

Introduction

Triggering an action at an operating element can mean the following:

- A command is executed.
  Example: Click a button to trigger a script or to execute a pre-defined function.
- An object is enabled.
  Example: To enter a value in a list, click in a table cell.

Requirement

- You have navigated to the operating element on which you want to trigger the action.
- The operating element has the focus.

Procedure

- Tap the operating element on the touchscreen once or twice in quick succession.

Result

The following results are possible:

- The requested command is executed.
- The cursor flashes in the input area of the operating element.
  When accessing via touch devices: The screen keyboard opens.
- The element is selected and can be moved.

3.3.5 Entering a value

Introduction

Depending on the input format, you enter numerical or alphanumerical values in an input box.

Requirement

- The object is an input field or table field.
- The operating element is enabled.

Entering a value

1. Enter the desired value.
2. To confirm the value, press the <Enter> key or click on a blank area of the screen.
3. To discard the value, press the <Esc> key.

Result

The input is accepted or discarded.

The input box still has the focus.

3.3.6 Moving operator controls

Introduction

There are screen objects with movable operator controls, e.g. a slider.

Requirement

- A movable operating element is selected.

Procedure

1. To move the operating element, move it while holding down the mouse button or use a corresponding touch gesture, e.g. "Drag" for a slider.

Result

The position of the movable operating element and the display in the screen object have changed.

3.3.7 Placing the focus on objects

You have the following options:

- Click on the object.

  Note

  Giving focus to objects with a transparent background

  If an object has a transparent background, click on a visible area of the object.

- Press <Tab> until the object has the focus.

See also

Operating objects with transparent fill (Page 87)

3.3.8 Operating objects with transparent fill

The objects displayed on a screen can have transparent ranges.
Example: Sliders, bars and pointer instruments are enclosed by a transparent rectangle.

Requirement

An event which is triggered by operating actions such as typing or clicking has been configured for the object in the engineering.

Trigger event

To trigger the event, proceed as follows:

- If the object does not have the focus, click a visible part of the object, e.g. its border.
- If the object already has the focus, the event is also triggered by clicking in the transparent area.

3.3.9 Flashing

Flashing in Runtime

You can display the objects flashing in Runtime. Scripts can be used to switch flashing on and off and influence the properties of the flashing.

Configure the flashing behavior of an object property in the engineering system for each color setting of an object that supports flashing.

Note

The flashing in Runtime does not change the color value of the property.

3.4 Controls

3.4.1 Overview of controls

Runtime has operable controls in process pictures.

The following controls are available depending on the configured access rights:

Icon	Control	Brief description
	Screen window	Displays other screens of the object.
	Trend control	Displays graphical representations of tag values from the current process or from a log in the form of trends with values over time from the controller or a log.
	f(x) trend control	Represents the values of a tag as a function of another tag.
	Browser	Displays HTML pages.
	Media Player	Enables video and audio files to be played.
	Alarm control	Shows currently pending alarms or alarm events from the alarm buffer or alarm log.
	Process control	Represents current or logged process data in a table.
	Trend companion	Displays evaluated data and statistics in a table.
	Parameter set control	Shows the parameter sets with which the PLC is set up for production.

Icon	Control	Brief description
	System diagnostics control	Shows the diagnostic status of multiple PLCs via traffic light SVGs.
	GRAPH overview	Displays the current program status for executed steps of the GRAPH sequencer.
	PLC code view	Displays the current program status of user programs.
	ProDiag overview	Provides an overview of the current status of the configured monitoring.

3.4.2 Operating alarms

3.4.2.1 Basics of alarms

Alarm system

Introduction

Alarms show events, operating modes or faults that occur in runtime in the plant.

You can use alarms for diagnostic purposes, for example, when troubleshooting. They will help you to immediately locate the cause of the fault. You can adjust your processes through targeted intervention so that compliant products continue to be produced despite the fault, or the process is stabilized, and the fault only causes a minimal loss of production.

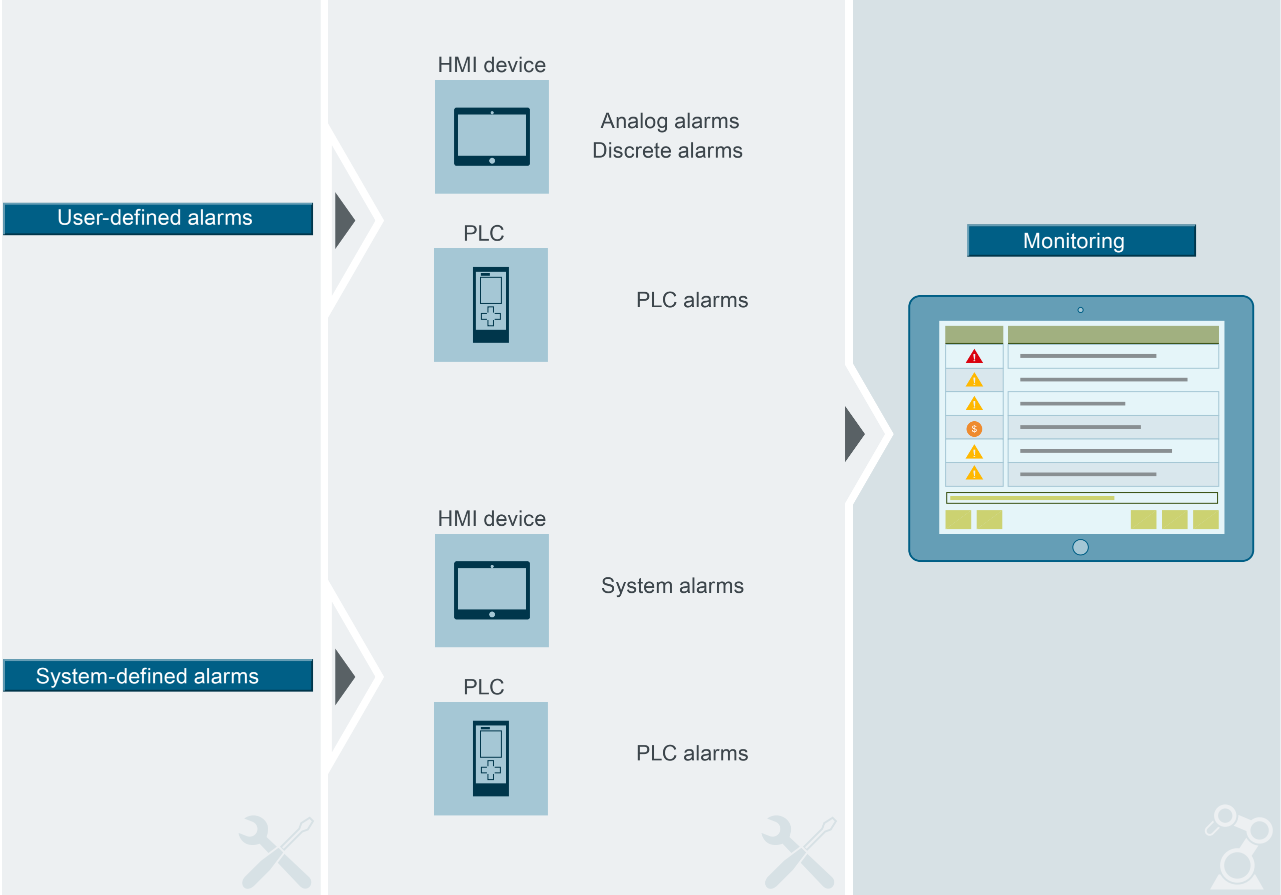
The acquired alarms are displayed on the HMI device in screens. The alarm system logs the alarms from the ongoing process. Targeted access to the alarms combined with supplementary information about individual alarms ensures that faults are localized and cleared quickly. This reduces stoppages or even prevents them altogether.

The alarm system in WinCC Unified Scada

The alarm system distinguishes between the following alarms:

User-defined alarms	Analog alarms	Display limit value violations (value changes) They are used to monitor the plant.
	Discrete alarms	Display status changes They are used to monitor the plant.
	User-defined PLC alarms	Displays the status values of the PLC. They are used to monitor the plant and are configured in STEP 7.

System-defined alarms	System alarms	Are included in the HMI device. They are used to monitor the HMI device.
	System-defined PLC alarms	They consist of system diagnostic alarms and system errors. They are used to monitor the PLC. The types of system-defined PLC alarms depend on the PLC used.



See also

Analog alarms (Page 91)

Discrete alarms (Page 91)

User-defined PLC alarms (Page 91)

System alarms (Page 92)

System-defined PLC alarms (Page 92)

Alarm control overview (Page 100)

Alarms

User-defined alarms

Analog alarms

Description

Analog alarms display limit violations. An analog alarm is triggered when the value of the trigger tag meets the trigger condition defined on the analog alarm.

Depending on the selected trigger condition, the alarm is triggered, for example, when the condition value is higher than, lower than, or the same as the defined value.

Example

When the motor speed reaches a critical range as defined in the engineering, an alarm with matching alarm text is displayed. The alarm text can provide the operator with specific instructions on how to check and remedy the situation.

Discrete alarms

Description

A discrete alarm is triggered when the value of a specific bit of a tag changes. The discrete alarms indicate status changes in a plant and are triggered by a controller.

Example

Imagine that the state of a valve is to be monitored during operation. The state of the valve is "open" or "closed".

A discrete alarm is configured for each state of the valve. If the status of the valve changes, a discrete alarm is output, containing for example the following alarm text: "Valve closed".

User-defined PLC alarms

Example of an alarm

"The temperature in Tank 2 is too high."

Description

A user-defined PLC alarm maps the status values of a PLC, for example, time stamp and process values. It is created by a PLC project engineer in STEP 7.

The PLC alarms configured in STEP 7, are applied into the integrated WinCC operation as soon as a connection is established to the PLC.

Note

Automatic update of new or modified PLC alarms on the HMI device

If PLC alarms are configured in STEP 7 and an HMI connection to a SIMATIC S7-1500 controller (firmware version 2.0 or higher) is established, and the PLC and HMI device are configured accordingly in the engineering, the PLC alarms are sent to the HMI device and updated automatically. You can find more information in the TIA Portal help for WinCC Unified.

Note

WinCC only supports PLC alarms of a SIMATIC S7-1500 controller. In addition, WinCC only supports PLC alarms that are automatically updated by the central alarm management in the PLC.

System-defined alarms

System alarms

Description

A system alarm indicates the status of the system and communication errors between the HMI device and the system. System alarms are output in runtime in the configured alarm control. System alarms are output in the language currently set on your HMI device.

The time format (AM/PM or 24-hour format) is based on the selected language. If no translation of the alarm texts exists in this language, English is used as replacement and the corresponding time format is displayed.

Example of an alarm

"Memory is full!"

System-defined PLC alarms

Note

Device dependency

System-defined PLC alarms are not available for all HMI devices.

Description

System-defined PLC alarms are installed with STEP 7 and are only available if WinCC is operated in the STEP 7 environment.

System-defined PLC alarms are used to monitor states and events of a PLC. System-defined PLC alarms consist of system diagnostic alarms and system errors (RSE)

Note

Automatic update of system diagnostic alarms on the HMI device

When an HMI connection to a SIMATIC S7-1500 controller (firmware version 2.0 or higher) is established, and the PLC and the HMI device were configured accordingly in the engineering, the system diagnostic alarms are sent to the HMI device and updated automatically. You can find more information in the TIA Portal help for WinCC Unified.

Note

Note the following restrictions:

- WinCC only supports system diagnostic alarms of a SIMATIC S7-1500 controller.
- WinCC only supports system diagnostic alarms that are automatically updated by the central alarm management in the PLC.

Example of an alarm

"CPU maintenance required"

Alarm blocks

Overview

In Engineering you configure which columns you can see in runtime and which alarm blocks the columns are evaluating. The following section provides an overview of some important alarm blocks.

Example of alarm blocks output in runtime:

Alarm class	Alarm number	Time of occurrence	State machine	Alarm text	Information	Value	Limit value
Warning	1	08/27/2017 11:09:14 AM	Alarm with single-mode acknowledgment	Maximum speed reached	This alarm is...	50	27

Alarm class

The alarm class controls, for example, the display and the acknowledgment concept of the alarm.

Alarm number

You identify an alarm by its number (ID).

Change the alarm number, if necessary; for example, with a consecutive alarm number to mark alarms that belong together in your project.

Note

The alarm number of a system alarm has a higher priority than the number of a user-defined alarm. Do not use numbers that are used by system alarms for user-defined alarms.

Alarm blocks with time and date

These alarm blocks show the time at which the alarm was active, acknowledged or became inactive, etc.

Note

Time zones

By default, the time stamp in the alarm display is converted into the time zone used by the HMI device.

If the alarm display is configured accordingly, the time stamp can be converted to another time zone in Runtime via the "Time base configuration" button.

State machine

An alarm has the state machine or the acknowledgment concept of the alarm class.

The state machine is the way an alarm is displayed in various states and processed by the system.

See section Acknowledgment model (Page 96).

Alarm state

An alarm always has a specific alarm state in runtime, for example, active or active/ acknowledged. Based on the alarm state, you can understand the process that the alarm went through.

Alarm text

The alarm text (event text) describes the cause of the alarm.

The alarm text can contain output fields for current values. The value is retained at the time at which the alarm status changes.

Priority

Displays the priority of individual alarms.

Note

A priority configured on the alarm has precedence in runtime over the priority configured on the alarm class.

Limit value

Analog alarms display limit violations. Depending on the configuration, WinCC outputs the analog alarm as soon as the trigger tag exceeds or undershoots the configured limit value.

Computer

Operator input alarms have the "Computer" column in the alarm summary. The computer name is displayed for local alarms and the IP address for alarms from the web client.

Users

The user acknowledges the alarm. If an empty user name is passed to an alarm, it does not represent a user name.

For alarms triggered by a variable, no user name is shown in the alarm display.

Duration

Returns the time interval in nanoseconds between triggering of the alarm and its previous status change.

See also

Alarm classes (Page 95)

Alarm classes

Introduction

Many alarms occur in a plant; these are all of different importance. To make it clear to you, which alarms are most important, alarms are assigned to alarm classes.

Assignment of the alarms to alarm classes and configuration of the alarm classes takes place in the engineering system.

Purpose

The alarm class of an alarm defines the following:

- State machine/acknowledgment model
- Appearance in alarm control (e.g. color)
- Priority

  Note

  The priority configured on the alarm has precedence in runtime over the priority configured on the alarm class.

- Logging

Examples of how to use alarm classes

- The alarm class of the alarm "Fan 1 speed in upper tolerance range" is "Warning". The alarm is displayed with a yellow background. The alarm does not require acknowledgment.
- The alarm "Speed of fan 2 has exceeded upper warning range" is assigned to the "Alarm" alarm class. The alarm is displayed with a red background and flashes at high frequency in runtime. The alarm is displayed until you have acknowledged it.

User-defined and predefined alarm classes

The alarms use user-defined or predefined alarm classes:

- Number and configuration of user-defined alarm classes depend on the configuration of the runtime project in the engineering.
- The number and configuration of predefined alarm classes are provided by the system. You can find more information on predefine alarm classes in the TIA Portal help for WinCC Unified as well as in the user help for WinCC Unified Online Engineering.

See also

Acknowledgment model (Page 96)

Logging basics (Page 119)

Acknowledgment model

Introduction

The state machine of an alarm class regulates which statuses the alarms of this alarm class can have. From this it is derived which events can occur for them and whether and how they are acknowledged.

State machines

The following state machines are available for HMI alarm classes:

State machine	Description	Use in predefined alarm classes
Active	Alarm without inactive state without acknowledgment This alarm is only displayed in the views "Show logged alarms" and "Show and update logged alarms".	Information OperatorInputInformation SystemInformation
Active and inactive	Alarm without acknowledgment This alarm becomes active and inactive without having to be acknowledged.	Notification SystemNotification
Active, requires acknowledgment	Alarm without inactive state with acknowledgment This alarm must be acknowledged as soon as the event that triggers the alarm occurs. The alarm is pending until it is acknowledged.	AlarmWithoutClearEvent SystemAlarmWithoutClearEvent SystemWarningWithoutClearEvent
Active and inactive, requires acknowledgment	Alarm with a single acknowledgment This alarm must be acknowledged as soon as the event that triggers the alarm occurs. The alarm is pending until it is acknowledged and inactive.	Alarm Critical OperatorInputRequest SystemAlarm SystemWarning Warning
Active and inactive, requires acknowledgment and reset	Alarm with acknowledgment and confirmation The alarm requires acknowledgment once the event that triggers, the alarm has occurred, or the alarm has been reset. In addition, the alarm requires confirmation when the event that triggers the alarm is no longer pending. The alarm is pending until it is acknowledged and confirmed.	AlarmWithReset CriticalWithReset WarningWithReset

The following state machines are available for HMI alarm classes that are associated with common alarm classes:

- Alarm with a single acknowledgment
- Alarm without acknowledgment

Alarms requiring acknowledgment

Alarms that indicate critical or hazardous states in the process must be acknowledgeable. Every change in the status of an alarm that requires acknowledgment is logged.

Acknowledging the alarm confirms knowledge of the condition that caused the alarm. You acknowledge the alarm using the buttons in the alarm control.

Acknowledgment and confirmation of alarms

- Group acknowledgment of alarms in the alarm control
  With the "Acknowledge visible alarms" button you acknowledge all alarms pending in the alarm control that are visible and require acknowledgment.
- Single acknowledgment of alarms in the alarm control
  With the "Single acknowledgment" button you acknowledge a single alarm that is selected in the alarm control.
- Single acknowledgment of alarms with acknowledgment and confirmation in the alarm control
  With the "Single acknowledgment" button you acknowledge a single alarm with the state machine "Alarm with acknowledgment and confirmation" after it was previously acknowledged via group acknowledgment or single acknowledgment and was inactive.

Note

If the "Show recent" button is active, the most recent alarm is always displayed first and is selected.

Group acknowledgment is only carried out for the visible alarms.

See also

Alarm states (Page 98)

Alarm states

Description

Each alarm has an alarm state. Alarm states are made up from the following events:

- **Active**
  The condition for triggering an alarm is fulfilled. The alarm is displayed, such as "Boiler pressure too high".
- **Inactive**
  The condition for triggering an alarm is no longer fulfilled. The alarm is no longer displayed as the boiler was vented.
- **Acknowledged**
  The operator has acknowledged the alarm.

The alarm state of an alarm at any given time depends on the following factors:

- Which state machine has its alarm class.
  The state machine of an alarm class regulates which events can occur for alarms of this alarm class. From this it is derived which states the alarms can have and whether and how they are acknowledged.
  For an overview of the available state machines, see Acknowledgment model (Page 96).
- Which events occurred for the alarm.

Note

The display texts of the alarm states are different depending on the language and configuration. The texts displayed in Runtime can deviate from the texts shown here.

The active and inactive alarm states can also be displayed in Runtime with Raised and Cleared respectively.

Alarm states are visible to the operator in Runtime through status texts. The status texts can be configured in the Runtime settings.

Alarms without acknowledgment

The following table shows the alarm states for alarms without acknowledgment:

Icon	Alarm state	Status text	Description
⚠	Active	Incoming	The condition of an alarm is fulfilled. The alarm does not need to be acknowledged.
⚠✓	Inactive	Normal	The condition of an alarm is no longer fulfilled. The alarm is no longer pending.

Alarms with acknowledgment

The following table shows the alarm states for alarms with acknowledgment:

Icon	Alarm state	Status text	Description
⚠	Active	Incoming	The condition of an alarm is fulfilled.
⚠✓	Active/inactive	Incoming/Outgoing	The condition of an alarm is no longer fulfilled. The operator has not acknowledged the alarm.
⚠✓	Active/inactive/acknowledged	Normal	The condition of an alarm is no longer fulfilled. The operator has acknowledged the alarm after this time.
⚠✔	Active/acknowledged	Incoming/Acknowledged	The condition of an alarm is fulfilled. The operator has acknowledged the alarm.
⚠✓	Active/acknowledged/inactive	Normal	The condition of an alarm is no longer fulfilled. The operator acknowledged the alarm while the condition was still fulfilled.

Alarms requiring acknowledgment and confirmation

The following table shows the alarm states for alarms requiring acknowledgment and confirmation:

Icon	Alarm state	Status text	Description
⚠	Active	Incoming	The condition of an alarm is fulfilled.
⚠✓	Active/inactive	Incoming/Outgoing	The condition of an alarm is no longer fulfilled. The user has not acknowledged the alarm.
⚠✓	Active/inactive/ acknowledged	Incoming/outgoing/ acknowledged	The condition of an alarm is no longer fulfilled. The user acknowledged the alarm after this time.
⚠✔	Active/acknowledged	Incoming/Acknowledged	The condition of an alarm is fulfilled. The user has acknowledged the alarm.
⚠✓	Active/acknowledged/inactive	Incoming/acknowledged/ outgoing	The condition of an alarm is no longer fulfilled. The user has acknowledged the alarm while the condition was still fulfilled.
⚠✔	Normal	Normal	The condition of an alarm is fulfilled. The user has acknowledged and confirmed the alarm.

Disabled alarms

Operators disable an alarm to, for example, prevent a nuisance alarm from impairing the effectiveness of the system.

- Disabled: The alarm has been deactivated (locked). The alarm transitions to its final state without any further state transitions.
- Not disabled: The alarm is activated (enabled). The alarm is visible again in its last state.

Shelved alarms

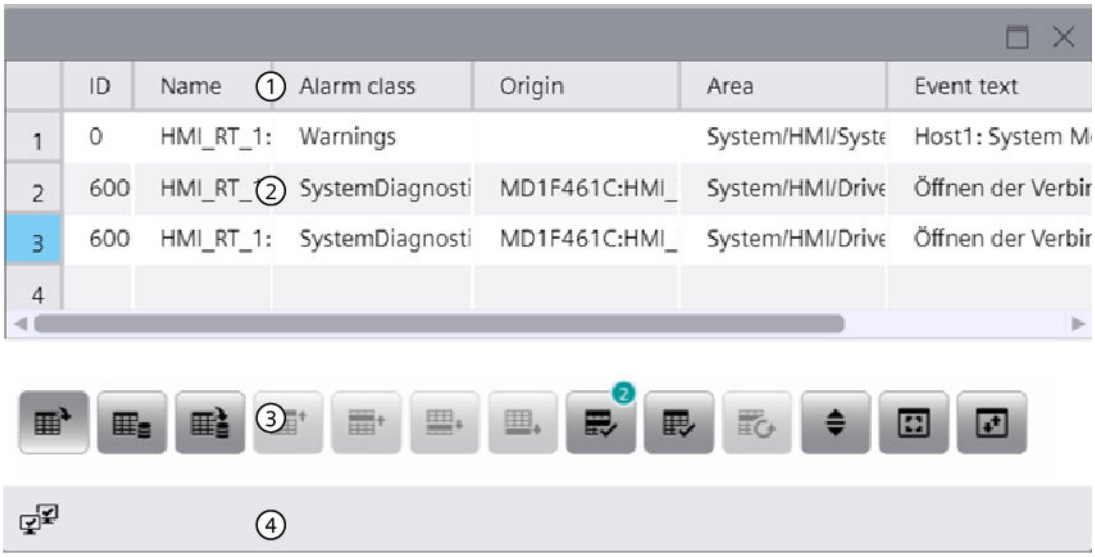
The display of specific alarms is shelved (suppressed) in order, for example, not to overload the operator with information. Manually reset: The alarm was manually reset by the operator. Shelved due to design: The alarm was automatically shelved due to a condition and is automatically hidden in Runtime.

3.4.2.2 Alarm control overview

Introduction

The alarm control displays PLC alarms and HMI alarms that occur during the process in a plant. The alarm control helps prevent faults in the plant or localize and remedy the causes of a fault.

User interface



	ID	Name	Alarm class	Origin	Area	Event text
1	0	HMI_RT_1:	Warnings		System/HMI/Syste	Host1: System M
2	600	HMI_RT_	SystemDiagnosti	MD1F461C:HMI_	System/HMI/Drive	Öffnen der Verbir
3	600	HMI_RT_1:	SystemDiagnosti	MD1F461C:HMI_	System/HMI/Drive	Öffnen der Verbir
4						

① Columns for the output alarm blocks

② Alarm summary

Each alarm is displayed in a separate line.

The alarms that are displayed depend on the view or list selected and whether filters are applied.

③ Toolbar for operating the alarm control

④ Information bar

Note

Selection of alarm blocks, column titles and localization depend on the configuration in engineering.

Note

An alarm appears in the alarm control with the date and time stamp crossed out in the following situations:

- A disabled alarm is enabled again.
- An alarm is reloaded after a power failure. This applies only to chronological alarming.
- The automation system is restarted. This applies only to chronological alarming.

Views and lists

Depending on the configuration of the alarms and the situation in the system, a large number of alarms can occur in runtime.

The alarm control offers various views and alarm lists that filter the alarm summary and thus provide a better overview:

View	Description		
Alarm view	Shows the alarms of the currently selected alarm list. Available alarm lists:		
		Display active alarms	Shows the pending alarms. If the toolbar is configured accordingly, you use the "Display options setup" button to set the alarms that are displayed in this list. Default setting: Displays all alarms that are not suppressed.
		Show logged alarms	Shows the logged alarms. The display is not updated immediately when new incoming alarms occur.
		Show and update logged alarms	Updates the logged alarms and shows them. The display is updated immediately when new incoming alarms occur.
		Display defined alarms	Displays the defined alarms. If the toolbar is configured accordingly, you use the "Display options setup" button to set the alarms that are displayed in this list.
Alarm statistics		Displays statistical calculations of logged alarms.	

You enable a view or list using the corresponding button in the toolbar.

Information bar

The information bar shows the different states related to the alarm servers. The information bar contains the following icons:

Icon	Meaning
	Shows the status to the alarm servers: No faulty connections
	Shows the status to the alarm servers: Faulty connections
	Shows the status to the alarm servers: All connections are faulty

With the corresponding configuration in engineering, the information bar shows the number of alarms that are not acknowledged in runtime. The counter includes all connected servers, but no filters.

When a context is selected, the information bar shows the values of the selected context.

Icons for the alarm state

The column for the alarm state can contain the following icons:

Icon	Meaning
In "Show and update logged alarms" list:	
⚠	Alarm is active
⚠✓	Alarm is inactive
⚠✓	Alarm acknowledged
In the other lists:	
⚠	Alarm is active
⚠✓	Alarm is active/inactive
⚠✔	Alarm is active/acknowledged

Performance data for SIMATIC Unified PC

Number of controller alarms	160000
Number of OPC UA A&C alarms	20000
Number of alarms per second (continuous load)	20
Number of pending alarm events	Unlimited
Number of alarms per 10 seconds (alarm burst)	8000

The maximum number of alarms that can be displayed in Runtime depends on the selected view:

View	Maximum number of alarms that can be displayed.
Display active alarms	No limit
Display defined alarms	
Alarm statistics	
Show logged alarms	1000
Show and update logged alarms	100

See also

Buttons of the alarm control (Page 104)

3.4.2.3 Buttons of the alarm control

You operate the alarm control using the buttons on the toolbar. The buttons that are available depend on the configuration:

Button		Description
	Show active alarms	Show the currently pending alarms. With the ""Active alarms" setup" button, you set which alarms belong to the active alarms.
	Show logged alarms	Shows the logged alarms. The display is not updated immediately when new incoming alarms occur.
	Show and update logged alarms	Updates the logged alarms and shows them. The display is updated immediately when new active alarms occur.
	Alarm statistics - View	Visualizes statistical information of logged alarms, such as frequency and display duration.
	Alarm statistics - Configuration	Setting options for calculating the alarm statistics.
	Show defined alarms	Shows the alarms configured in the system.
	Alarm annunciator	Shows all alarms for which the alarm annunciator was configured. The alarm annunciator is a visual or acoustic signal, such as a horn or warning light, that is displayed in addition to the alarm control in the system.
	First line	Selects the first of the displayed alarms. The visible area of the alarm control is moved, if required. This button can only be operated if the "Alarms - Show recent" button is disabled.
	Previous line	Selects the previous alarm, starting from the currently selected alarm. The visible area of the alarm control is moved, if required. The button can only be operated if the "Alarms - Show recent" button is disabled.
	Next line	Selects the next alarm, starting from the currently selected alarm. The visible area of the alarm control is moved, if required. The button can only be operated if the "Alarms - Show recent" button is disabled.
	Last line	Selects the last of the displayed alarms. The visible area of the alarm control is moved, if required. This button can only be operated if the "Alarms - Show recent" button is disabled.
	Move to next acknowledgeable alarm	Selects the next alarm that requires acknowledgment, starting from the currently selected alarm. The visible area of the alarm control is moved, if required. This button can only be operated if the "Alarms - Show recent" button is disabled.
◀◀	Previous page	Navigates to the previous page.
▶▶	Next page	Navigates to the next page.

Button		Description
1	Single acknowledgment	Acknowledges the selected alarm. If using the multiple selection, the selected alarms which require single acknowledgment are not acknowledged. A counter shows how many alarms are not acknowledged. The counter includes all connected servers, but no filters.
	Acknowledge visible alarms	Acknowledges all pending, visible and acknowledgeable alarms in the alarm control, if they are not individually acknowledgeable.
	Single confirm	Resets the alarm. Relevant for alarms with the state machine "Alarm with acknowledgment and confirmation", which were already acknowledged and inactive.
⇕	Alarms - Show recent	Defines whether it is always the latest alarm that is selected in the alarm control. Button not pressed: The "Alarms - Show recent" button is active: • The most current alarms are always shown first in the alarm control. Alarms that have been filtered out of the alarm control are not displayed. • The visible area of the alarm control moves automatically, if necessary. • You cannot select the alarms individually or sort them by column. Button pressed: The "Alarms - Show recent" button is paused.
ℹ	Info text - configuration	Opens a dialog that shows a help text configured for the selected alarm.
✎	Comment - configuration	Opens a dialog for adding a comment.
🔒	Disable alarm	Disables an alarm.
🔓	Enable alarm	Enables a disabled alarm.
💡	Shelve alarm	Resets an alarm, for example, to prevent a nuisance alarm from impairing the effectiveness of your system.
	Unshelve alarm	Cancels the reset of the respective alarm.
	Copy lines	Copies the selected alarms.
	Time base - configuration	Opens a dialog for setting the time zone for the time information shown in alarms.
	Selection display	Opens a dialog for filtering alarms. Define your own filter criteria or change or remove filters defined in the engineering system.
	Sorting setup	Opens a dialog for setting custom sorting criteria for displayed alarms.

Button		Description
	Display options - configuration	Opens a dialog in which you set which alarms the currently displayed alarm list displays.
	Disabled alarms - Configuration	Opens a dialog for configuring the display options of the disabled alarms.
	Export	Starts the export of alarms to a CSV file.
	Select context	For context-based filtering of alarms. The alarm control only shows alarms that fall within the time period of the selected context entry.

3.4.2.4 Operate alarm control

Note

Displayed alarms

The alarms that you see in the alarm control depend on which alarm view or alarm list you have selected in the toolbar.

Operation using the mouse

Selecting and operating alarms

- Click on an alarm.
- Click a button in the toolbar.

The function of the button is applied to the alarm.

Rearranging columns

You can change the column arrangement configured in the engineering here. See section Rearranging columns at runtime (Page 284).

Sorting alarms by column

You can sort the alarms by column. See section Sorting alarms (Page 113).

Operation using the keyboard

Press <Shift + Enter> until the focus is on the alarm control. Then select the alarm to be edited and operate it using the toolbar.

Use the following buttons for this:

Buttons	Description
<PgUp>	Selects the previous alarm.
<PgDn>	Selects the next alarm.
<Ctrl + Up> or <Home>	If multiple rows were selected, the first row of the selection is selected.
<Ctrl + Down> or <End>	If multiple rows were selected, the last row of the selection is selected.
<Ctrl + Left>	If multiple columns were selected, the first column of the selection is selected.
<Ctrl + Right>	If multiple columns were selected, the last column of the selection is selected.
<Tab>	Selects the next button in the toolbar.
<Shift + Tab>	Selects the previous button in the toolbar.
<Enter>	Executes the currently selected button.
<Shift + Page Up>	Scrolls to the left column-by-column.
<Shift + Page Down>	Scrolls to the right column-by-column.

Alternative operation

- Depending on the configuration, you can also operate the alarm control via the function keys.
- If the alarm control is configured accordingly, all information about the alarm is displayed in a pop-up for a selected alarm. The "Alarms - Show recent" button (Autoscroll) must be disabled for this.

Multiple selection of alarms on Panels via touch gesture

Requirement

Configuration of the alarm control in the engineering system:

- Under "Properties > Miscellaneous > Alarm control > Selection - Mode", the "Multiple" entry is set for "Static value".
- The "Previous line" and "Next line" buttons are configured.

Operator control in Runtime

1. Tap an alarm in the alarm control.
   The alarm is selected.
2. To extend the selection by one or more previous alarms, tap the "Previous line" button until the desired alarms are selected.
3. To extend the selection by one or more subsequent alarms, tap the "Next line" button until the desired alarms are selected.

See also

Supported gestures (Page 79)

3.4.2.5 Filtering alarms

Introduction

You can use filters to control which alarms you see in the alarm view in runtime. To do so, define filter conditions.

The following settings are available in the "Alarm filter" dialog:

Setting	Description
"AND/OR" column	Adds additional criteria to the existing criteria with the Boolean operations AND or OR.
"Criterion" column	Selection list with the available criteria. Criteria correspond to the alarm blocks in the alarm control.
"Operator" column	Selection list with the available relational operators.
"Setup" column	Free text field
"Remove" button	Removes the selected filter criterion.
"Up/down" button	Moves the selected filter criterion.
"Filter" area	Free text area for direct input and editing of filter criteria.

Requirement

The "Selection display" button is configured in the alarm control.

Procedure

The following example describes how to define a filter. In the example, a filter is defined that filters for alarms that contain the alarm text "Motor on" and have a priority less than or equal to 5:

1. Click the "Selection display" button.

   The "Alarm filter" dialog opens.
2. Click in the "Criterion" column and select the "Alarm text" entry.
3. Click in the "Operator" column and select the "Equal to" entry.
4. In the free text field of the "Setup" column, enter the value "Motor on".
5. In the next row in the "And / Or" column, click "Add" and select the AND logic operation.

6. Click in the "Criterion" column and select the "Priority" entry.
7. Click in the "Operator" column and select the entry "Less than or equal to".
8. Enter the value "5" in the free text field of the "Setting" column.
9. Confirm your entries.
10. Close the dialog.

With some alarm blocks, for example, you can define the start and end times or search texts for "Date" and "Time". Your input must be in the format required in the dialog.

Note

In multi-user systems, make sure that contents displayed in the "Alarm filter" dialog on a client have the same names on all servers.

When filtering by time, the start and stop values are not adjusted automatically when the time base of the alarm control is changed.

Example: At the PC location with the time zone "UTC + 1h", the alarm control has the "Local time zone" time base. You should filter by the time 10:00 to 11:00. Change the time base from "Local time zone" to "UTC". If you want to display the same alarms, change the filter to 9:00 to 10:00 hrs.

Result

The filter is applied to all alarm lists in the alarm view.

Time-based filtering

Define the filter period

During time-based filtering of the alarm control, always define two filter conditions linked via "And". For these conditions, use the operators "Greater than", "Greater than or equal to" and "Less than or equal to".

Do not use the "Equal to" operator. When filtering, you specify the filter period down to the millisecond. Internally, the time stamp of alarms is stored precisely down to the nanosecond and the missing information for nanoseconds is supplemented by 0. A search with "Equal to" will therefore only find alarms whose time stamp has the nanosecond value 0.

Examples:

You can use the following filter conditions to filter for alarms that were triggered between 12:00 and 12:01:

- Filter condition 1: "Raise time", "Greater than or equal to", 12:00:00.000
- Filter condition 2: "And", "Raise time", "Less than or equal to", 12:01:00.001

You can use the following filter conditions to filter for alarms that were triggered at 12:00:00.000 hrs:

- Filter condition 1: "Raise time", "Greater than or equal to", 12:00:00.000
- Filter condition 2: "And", "Raise time", "Less than or equal to", 12:00:00.000

Change time base

If the time base of the alarm control is changed, the start value and stop value are not automatically adjusted when you filter by time.
Example: At the location of the PC with the time zone "UTC + 1h", the time base "Local time zone" was selected for the alarm control. If you filter for the time 10:00 to 11:00 and then change the time base to "UTC", you need to change the start value and stop value of the filter to 9:00 and 10:00 to display the same alarms as before.

See also

Display alarms for plant objects (Page 110)

3.4.2.6 Display alarms for plant objects

Introduction

In the case of the corresponding configuration, the alarm control shows the alarms of the plant objects that are configured in the plant hierarchy:

- Automatic display
  When the HMI device is assigned to a plant hierarchy or a plant object, and a plant overview and an alarm control are configured for the screen, the alarm control automatically shows the alarms of the plant object selected in the plant overview.
- Manual display through filters
  If no plant overview is configured in the screen, filter the alarm control to display alarms of a plant object.

The alarm control offers the following options for plant object alarms:

- Display the hierarchy path of the alarm source
- Filter the alarm control by plant objects
- Display alarm log of a plant object
- Context-dependent display of plant object alarms

General requirements

- The plant hierarchy has been created and a device assigned in the engineering system.
- An alarm control with the column "Area" has been configured in the screen of the assigned device.
- Runtime is active.

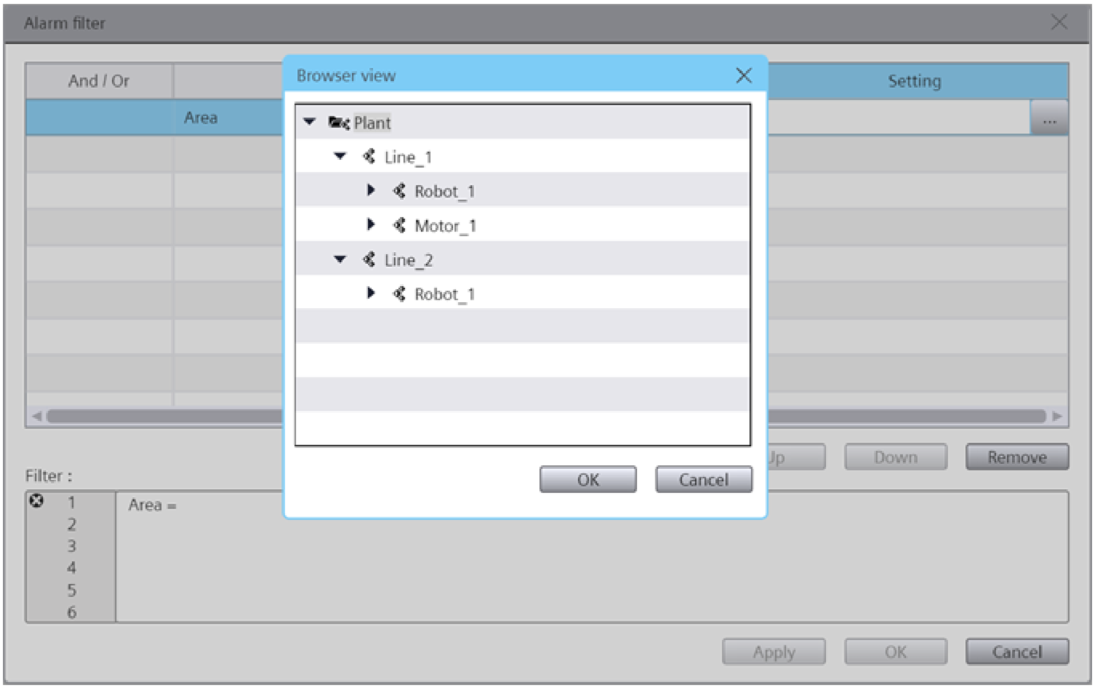
Filter alarm control by plant objects

Additional requirements

- Alarms are available for a plant object from the plant hierarchy.

Procedure

1. In Runtime, click the "Selection display" button in the alarm control.
2. Select "Area" as the criterion in the "Alarm filter" dialog.
3. Click the cell of the "Setting" column
4. Click "...".
   A tree of the plant hierarchy is displayed.
5. Select a plant object and confirm your selection.



6. Under "Operand", select one of the following operators:
   - To display the alarms of the selected plant object, select "Same as".
   - To output the alarms of the lower-level plant objects, select "Begins with".

The alarm control shows its setting according to the alarms of the selected plant object or its lower-level plant objects. The "Area" column shows the complete path of the plant object.

Note

Display of the filter string for filters configured in engineering

The plant view is based on a type/instance architecture. When a filter has been configured in engineering that filters the alarm view by plant objects, you will first see a filter string with information from the type level in the "Filter" field of the "Alarm filter" dialog.

If you select an operand under "Operand" or a plant object under "Setting", the filter string changes to the instance level and adopts the device ID.

Display alarm log for a plant object

Additional requirements

- The alarm log contains entries for a plant object from the plant hierarchy.

Procedure

1. In runtime, click on the "Display logged alarms" button.

The alarm control shows the logged alarms of the plant object.

See also

Filtering alarms (Page 108)

Plant overview (Page 167)

3.4.2.7 Display context-dependent alarms of a plant object

This section describes how to show alarms that occurred on a plant object that you selected for a context that you selected.

Requirement

- An HMI device has been configured.
- An alarm control is configured in the device screen.
- The plant hierarchy has been created and assigned to the HMI device.
- There are alarms for the plant object.
- Contexts and context entries are available for the plant object.
- The "Select context" button is configured in the alarm control.

Procedure

1. In the alarm control, click the "Select context" button.
   The "Alarm context" dialog opens.
2. Click "..." and select the plant object whose data you want to display in the alarm control.
3. Select one of the contexts assigned to the plant object in the "Context" drop-down list.
   A list of the entries logged for the context appears under "Logged context values".
4. Select an entry.
5. Click "OK".

The alarm control shows the alarms of the plant object that fall within the time period of the selected entry. The information bar shows the values of the selected context.

Note

"AND" link with other filters

When a filter is defined for the alarm control, the filter condition and the context conditions are linked via "AND".

When no alarms appear in the alarm control, check your filter settings by clicking "Selection display".

See also

Contexts (Page 57)

3.4.2.8 Sorting alarms

Introduction

You can control the columns according to which the alarm control sorts the alarms in runtime.

Examples for sorting alarms:

- In descending order by date, time, and alarm number. The latest alarm appears at the top.
- By priority
  You must have defined the priority of the alarms in the "HMI alarms" editor and configured the "Priority" alarm block in the alarm control. As a result, in a single-line alarm control, only the top-priority alarm appears in the alarm window. A lower-priority alarm is not displayed, even if it is more recent. The alarms are displayed in chronological order.
- The "Alarm state" alarm block is sorted by the type of state and not by the configured status texts. For an ascending sort order, the following order is used:
  - Active
  - Inactive
  - Acknowledged
  - Disabled
  - Activated
  - Automatic acknowledgment
  - Emergency acknowledgment
  - Active/Inactive

When sorting the alarm control by columns, define the sort order over up to four columns. An arrow and a number are shown on the right in the column header. The arrow indicates the sort order (ascending or descending). The number beside the arrow indicates the sort order of the column headers.

Requirement

- "Allow sorting" is enabled for the respective columns in the configuration of the alarm control.
- The "Show recent" function is paused in the alarm control.

Procedure

To filter alarms in the alarm control by column, follow these steps:

1. Click the column header by which you want to sort the alarms first.
   The number "1" is displayed with an arrow pointing upwards for ascending sort order or an arrow pointing downwards for descending sort order.
2. Optional:
   – To reverse the sort order for this column, click the column header again.
   – To cancel the sorting for this column, click the column header a third time.
3. If you want to sort by several columns, click the column header in the required order.

Alternatively, click the "Sorting setup" button and configure the sorting in the "Sorting" dialog.

3.4.2.9 Disabling individual alarms

Note

No locking and unlocking of PLC alarms

Locking and unlocking of PLC alarms for an S7-1500 PLC is not supported.

Introduction

If you disable an alarm, the alarm is not checked to determine whether the alarm condition applies. The alarm is not logged.

Note

Disabled alarm

Disabled alarms are no longer disabled after a restart of Runtime. Only alarms that are disabled directly in the automation system via data blocks remain disabled (disabled at source).

Requirement

- The "Visibility" and "Allow operator control" settings have been enabled for the following buttons in the engineering:
  - "Disable alarm"
  - "Enable alarm"
- The user is authorized to disable and enable alarms.

  Note

  The "Disable alarms" and "Enable alarms" authorizations must be configured directly one below the other. This is necessary because the authorization level used automatically for the "Enable alarms" authorization is directly below the "Disable alarms" authorization.

- An alarm is displayed on the HMI device.

Disable alarm

1. Select one of the following alarm lists in the alarm control:
   - "Show logged alarms"
   - "Show and update logged alarms"
   - "Show defined alarms"
2. Select the alarm.
3. Click "Disable alarm".

Result

The alarm is removed from the "Show active alarms" alarm list. Its alarm condition is no longer checked.

The alarm is visible in the alarm lists for logged alarms and defined alarms and has the status "Removed".

Enable alarm

To enable a disabled alarm, follow these steps:

1. In the alarm control, select an alarm list for logged alarms or defined alarms.
2. Select the alarm in the alarm list.
3. Click "Enable alarm".

The alarm condition of the alarm is checked again.

3.4.2.10 Shelving alarms

Introduction

You shelve an alarm for a specific period of time, for example, to prevent that a conformity error alarm affects the efficiency of your system.

Shelving can be canceled at any time. To do so, you use the buttons "Shelve alarm" and "Unshelve alarm" in the alarm control in runtime.

Requirement

- The "Visibility" and "Allow operation" settings have been activated for the following buttons in the engineering system:
  - "Shelve alarm"
  - "Unshelve alarm"
  - "Show active alarms"
  - "Display options setup"
- To unshelve: An alarm is displayed on the HMI device.

Procedure

To shelve an alarm, follow these steps:

1. Select one of the following alarm lists in the alarm control:
   - "Show active alarms"
   - "Show logged alarms"
   - "Update and display logged alarms"
   - "Show defined alarms"
2. Select the alarm.
3. Click the "Shelve alarm" button.

Result

The alarm is shelved. Its status remains unchanged.

The shelving creates a log entry. Shelved alarms are still available and logged in the system.

Note

Display of shelved alarms in the alarm list "Show active alarms"

Whether shelved alarms are visible in the alarm list for active alarms depends on the settings in the alarm list.

By default, the alarm list for active alarms does not display any shelved alarms.

Display shelved alarms

To display the currently shelved alarms, follow these steps:

1. In the alarm control, select the "Show active alarms" alarm list.
2. Click the "Display options setup" button.
3. Activate the option for shelved alarms.

Unshelve an alarm

To unshelve an alarm, follow these steps:

1. Display the shelved alarms.
2. Select the alarm in the "Show active alarms" alarm list.
3. Click the "Unshelve alarm" button.
4. If required, hide the shelved alarms from the "Show active alarms" alarm list.

Unshelving is canceled. Canceling the unshelving creates a log entry.

3.4.2.11 Acknowledging

Acknowledging alarms

The number of alarms to be acknowledged is indicated by a counter at the "Single acknowledgment" button or, if the alarm control was configured accordingly in engineering, by the information bar.

Introduction

You can acknowledge alarms in runtime according to your project configuration settings. You acknowledge alarms as follows:

- In the alarm control with the buttons "Single acknowledgment" and "Acknowledge visible alarms", and for alarms with dual-mode acknowledgment also with the button "Single confirm".
- With customized buttons

When an operator authorization is configured for the buttons, the alarms can only be acknowledged by authorized users.

Acknowledgment variants

You acknowledge individual alarms or multiple alarms together in Runtime. The following options are possible:

- Single acknowledgment
  Acknowledgment of an alarm using the "Single acknowledgment" button of the alarm control.
- Group acknowledgment
  Acknowledgment of all pending, visible alarms that require acknowledgment in the alarm control using the "Acknowledge visible alarms" button in the alarm control.
- Dual-mode acknowledgment
  When an alarm requires dual-mode acknowledgment, you must acknowledge both the enabling and disabling of the alarm. Or you acknowledge the alarm and reset it with the "Single confirm" button in the alarm control. The alarm status changes from "Active/Acknowledged" to "Inactive".

Requirement

- The "Visibility" and "Allow operator control" settings have been enabled in the engineering for the following buttons of the alarm control:

✓ 2	Single acknowledgment
✓	Acknowledge visible alarms
↻	Single confirm
⇕	Show recent

- For the single acknowledgment: An alarm that requires acknowledgment is pending.
- For the group acknowledgment: Several alarms that require acknowledgment are pending. The alarms do not require single acknowledgment.

Acknowledge alarms individually

To acknowledge an alarm, follow these steps:

- Read the alarm texts of the pending alarm and perform corrective measures, if necessary.
- Pause "Show recent".
- Select the alarm.
- Click "Single acknowledgment" in the alarm control.

Result

The alarm status is set to "Acknowledged". When the trigger condition for an alarm no longer applies, the alarm status is set to "Inactive" and no longer displayed on the HMI device.

Acknowledging alarms collectively

For group acknowledgment of alarms, follow these steps:

1. Read the alarm texts of the pending alarms and perform corrective actions, if necessary.
2. In the alarm control, click "Acknowledge visible alarms".

Note

The "Acknowledge visible alarms" button acknowledges all visible alarms only if no alarm is selected or highlighted.

If an alarm is selected or highlighted, only the selected or highlighted alarm will be acknowledged after clicking the "Acknowledge visible alarms" button.

Result

All pending alarms with the following properties are acknowledged:

- Requires acknowledgment
- Does not require single acknowledgment
- Visible

When the trigger condition for an alarm no longer applies, the alarm status is set to "Inactive" and no longer displayed on the HMI device.

3.4.2.12 Logging alarms

Logging basics

Introduction

An alarm log documents the alarms that occurred in the monitored process. You can use alarm logging to analyze error states and to document the process. When you analyze the logged alarms, you can extract important business and technical information regarding the operating mode of the plant.

With the appropriate configuration in engineering, logging alarms are created in runtime. If an error or limit violation occurs, for example, an alarm is output in runtime.

The alarm events are saved in a log database and/or printed out. The alarms logged in the database can be output in runtime if required, for example, in an alarm control.

The logged alarms are stored in a circular log that consists of multiple single segments.

With the appropriate configuration of the HMI device and a PLC connected to it, the alarms of the connected PLC are logged as well and made available in all configured languages.

Operating principle

An alarm is only logged if logging has been configured for its alarm class. The alarm logs are automatically created by the system in runtime.

Each alarm event of an alarm that has occurred is logged, for example, the status change from "Active" to "Active, acknowledged".

Note

Alarm classes for pure logging

Alarms of the alarm classes "Information", "OperatorInputInformation" and "SystemInformation" are only used for logging. In runtime, they are only displayed in the alarm lists "Show logged alarms" and "Show and update logged alarms".

Content of the alarm log

The alarm logs are used to store all alarm data, including configuration data. You can read all properties of an alarm from the logs, for example, alarm class, time stamp and alarm texts.

A new log segment with the new configuration data is generated whenever you edit configuration data of an alarm. This function prevents any change from influencing alarms logged previously.

The possible number of logged alarms depends on the database used.

Note

The time stamp of a logged alarm is always specified in standard UTC format (Universal Time Coordinated).

Because the alarm configuration is language-specific, the logs contain a configuration data table for each language configured.

Storage location and storage media

Log data are stored in a database. You can further process the saved data in other programs for analysis purposes, for example.

Backup for log segments

Take backups of your log segments to ensure complete documentation of your process.

Note

Database types for backups

- Microsoft SQL
  Must support the "Microsoft ODBC Driver 17 for SQL Server" driver in Version 17.9.
- SQLite
  Must support the "SQLite3" driver.

Note

Segments from logs for which a backup was created can be restored in runtime. To do so, open SIMATIC Runtime Manager on the HMI device. See also section Restoring and deleting log segments (Page 572).

Display of logged data

You can view the logged data on the HMI device with the buttons "Show logged alarms" and "Show and update logged alarms".

No logging due to overload

When an alarm cannot be written to the log after the configured number of attempts and within the defined time interval, the alarm is lost. The memory state is set to "StorageSystemWriteDataLost" internally. This documents that the number of alarms in the queue exceeds the configured high limit. No more alarms can be written to the log.

The alarm "SystemOverloadAlarm" of the alarm class "ALCL@%SystemInformation" is triggered. It is displayed in the alarm control but not logged.

Possible reasons for the overload:

- There are more alarms in the queue than can be processed.
- The alarms in the queue cannot be processed due to additional error conditions or memory states, for example, because the storage space is used up (memory state "StorageSpaceExceeded").

See also

Alarm classes (Page 95)

Connecting and disconnecting the alarm log backup

Introduction

When you want to access the data of an archived alarm log, connect the log backup to the project. You can configure an automatic connection or connect the alarm log to the project via a script. The logged alarms are displayed in the alarm control.

If you no longer want to access the backup of a log segment, disconnect the log backup from the project.

Requirement

The relevant backup files in "*. ldf" and "*.mdf" format are stored locally.

Display Time Range

Alarms are only displayed if you have configured the time range in the alarm control accordingly.

Example

You have configured the time range so that only the alarms of the past 24 hours are displayed. When you connect to a log backup containing alarms that are older than 24 hours, these alarms are not included in the alarm control.

Automatically connecting to an alarm log

To automatically connect to the alarm log backup, follow these steps:

1. Insert the log backup files in the "RuntimeProjectPath\ProjectName\CommonArchiving" folder.
2. In runtime, the alarm log is automatically connected to the project.

If signing is enabled, signed log backup files that are changed will not be connected automatically. A WinCC system alarm is generated and an entry is added to the Windows event log in the "Application" section.

Connecting to the alarm log using a script

Using the "AlarmLogs" VBS object, you can link the log backup files to the project using a script. The log segments are then copied with the "Restore" VBS method to the "Common Archiving" folder of the Runtime project.

Automatically disconnecting the alarm log

To automatically disconnect the alarm log backup from the project, follow these steps:

1. Go to the folder "RuntimeProjectPath\ProjectName\CommonArchiving".
2. Remove the log backup files from the folder.

Disconnecting from the alarm log using a script

Using the "AlarmLogs" VBS object, you can disconnect the log backup files from the project using a script. The log segments are then removed with the "Remove" VBS method from the "Common Archiving" folder of the Runtime project. For additional information, see the description of the "AlarmLogs" VBS object and the "Remove" VBS method.

Display logged alarms

Introduction

You can display the logged alarms with the buttons "Show logged alarms" and "Show and update logged alarms".

Requirements

- An alarm log is configured.
- All logged data that is to be displayed must be stored locally on the logging server. The SQL server does not allow access to backup files held elsewhere, such as another computer on the network.
- The buttons "Show logged alarms" and "Show and update logged alarms" are configured in the alarm control.

Procedure

1. To display only logged alarms, click the "Show logged alarms" button in the alarm control:

   The alarm control shows the logged alarms. The display is not updated immediately when new incoming alarms occur.
   Each page shows a maximum of 1000 alarms. Use the "Previous page" and "Next page" buttons to change pages.
2. Click the "Show and update logged alarms" button in the alarm control to display logged and current alarms:

   The alarm control shows the logged alarms. The display is updated immediately when new active alarms occur.
   The alarm control shows a maximum of 100 alarms.

Restriction for the alarm list "Show logged alarms"

For log alarms with identical time stamp, it is possible in rare cases that log alarms are skipped when paging forwards and backwards.

To display the skipped alarms, page again, this time in the opposite direction.

Note

In the case of more than 1000 log alarms with identical time stamp, not all skipped alarms can be displayed by scrolling in the opposite direction.

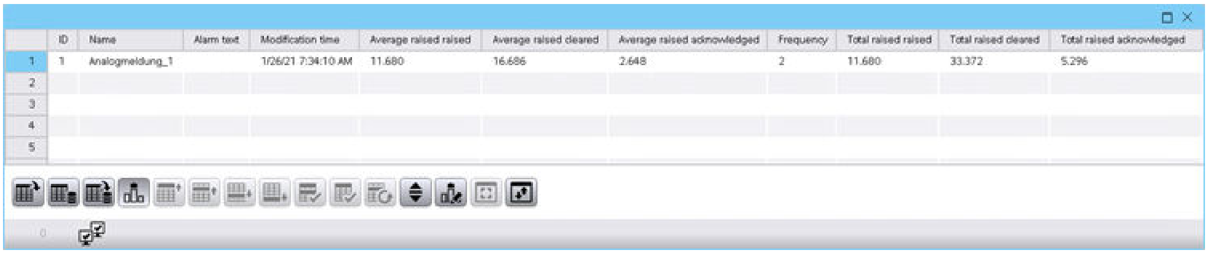
Example

- The alarm log contains several 1000 log alarms. Ten alarms of the log have an identical time stamp. The first five are shown at the end of the current page.
  The alarm control is sorted by time stamp in ascending order.
- Click "Next page".
  You see the next 1000 alarms whose time stamp is higher than the time stamp of the last alarm shown on the previous page.
  The remaining five alarms with identical time stamp are skipped on the page change.
- Click "Previous page".
  You will see all ten alarms with identical time stamp as well as the next 990 alarms with lower time stamp.

3.4.2.13 Displaying alarm statistics

Introduction

The alarm statistics represent statistical calculations of logged alarms.



	ID	Name	Alarm text	Modification time	Average raised raised	Average raised cleared	Average raised acknowledged	Frequency	Total raised raised	Total raised cleared	Total raised acknowledged
1	1	Analogmeldung_1		1/26/21 7:34:10 AM	11.680	16.686	2.648	2	11.680	33.372	5.296
2											
3											
4											
5											

You can use a button in the alarm control to export the alarm statistics to an Excel file.

Note

Filter

A filter set in the alarm control is not effective in the alarm statistics.

Note

Display options

Selected display options via the "Display options - setup" button in the alarm control have no effect in the alarm statistics.

Requirement

- Alarms are logged.
- For the following button of the alarm control, the "Visibility" and "Allow operator control" are enabled in the engineering system:

📊	Alarm statistics - view

Procedure

To display the alarm statistics in Runtime, proceed as follows:

1. Click the "Alarm statistics - view" button in the alarm control.

Result

The alarms to be displayed in the alarm statistics are specified in the engineering system. Depending on the engineering system, the following columns are displayed:

Column	Description
Number	Configured number of the alarm.
Frequency	Frequency of an alarm. The system counts the number of occurrences of an alarm with "active" status in the log. If the alarm number is not found, this alarm number is not included in the statistics.
Sum active active	Total display time of an alarm in seconds. The time period between the alarm states "active" and "active" is calculated.
Sum active inactive	Total display time of an alarm in seconds. The time period between the alarm states "active" and "inactive" is calculated.
Sum active acknowledged	Total display time of an alarm in seconds. The time period between the alarm states "active" and "acknowledged" is calculated.
Average active active	Average display time of an alarm in seconds. The time period between the alarm states "active" and "active" is calculated.
Average active inactive	Average display time of an alarm in seconds. The time period between the alarm states "active" and "inactive" is calculated.
Average active acknowledged	Average display time of an alarm in seconds. The time period between the alarm states "active" and "acknowledged" is calculated.

The calculation of the time of acknowledgment includes the "acknowledged" alarm state. This "acknowledged" alarm state includes the acknowledgment by the controller.

Note

For the calculation, alarms with the status "acknowledged" and "inactive" are only used if a suitable alarm with the status "active" is found in the result set beforehand.

If an alarm from the controller is pending and runtime is disabled and enabled several times, the alarm is entered into the log several times with the state "active". The alarm is also included multiple times in the calculation.

3.4.2.14 Operating alarm statistics

Introduction

Using the alarm statistics setup, you can change the settings for calculating the alarm statistics. The following settings are available:

Setting	Description
Time range start	• Now The current time is displayed as the start time of the calculation. • Fixed The start time of the calculation can be changed as required.
Start time	Start time for the calculation. If the "Now" option is selected under "Time range start", the start time cannot be changed.
Time range base	Unit of time for the calculation. The following settings are available: • Undefined The default time unit "Minute" is used with this setting. • Millisecond • Second • Minute • Hour • Day • Month • Year
Time range factor	The time range factor depends on the "Time range base" setting. For example, if the number 4 is set for the time range factor and "Minutes" is set for the time range base, all alarms that are logged within this period will be evaluated.

Requirement

- Alarms are located in the alarm log.
- For the following button of the alarm control, the "Visibility" and "Allow operator control" are enabled in the engineering:

	Alarm statistics - setup

- The alarm statistics are selected in the alarm control.

Procedure

To display the alarm statistics setup in runtime, follow these steps:

1. Click on the "Alarm statistics - setup" button in the alarm control.
   The configuration opens.
2. Change the settings as required.
3. Click the "OK" button.

Result

The calculation of the alarm statistics is displayed according to the changed settings.

3.4.3 Displaying tags in Runtime

3.4.3.1 Outputting the tag values

Overview

With WinCC you can output tag values in the HMI screen with different screen objects and change them.

- The I/O field is used for the input and output of process values.
- Bars are used for graphic display of the process values in form of a scale.
- Sliders are used for the input and output of process values within a defined range.
- The gauge is used to display the process values in form of an analog gauge.

In runtime you can also output tag values as table or as trend. You can use either process values or logged values as source for the tag values.

- Use a trend for the graphic display of tag values. Trends allows you to display the change in motor temperature, for example.
- Use a table to compare tag values. In the table you can, for example, compare fill levels of supply tanks.

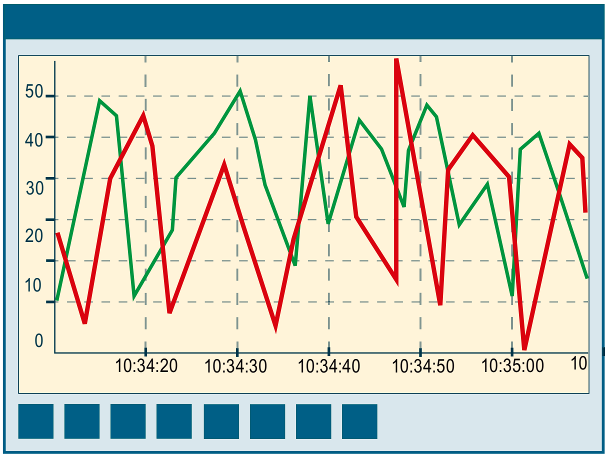
Controls for displaying tag values

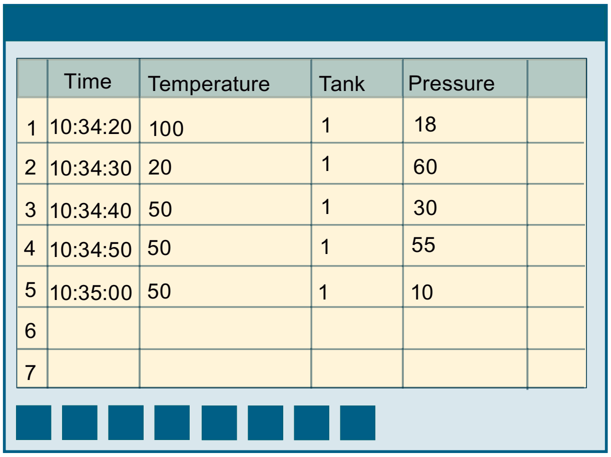
To display tag values as a trend, use the trend control. The versions of trend views are available:

- "Trend control": You display a tag value over time, for example, the change in temperature. You can compare the current values and logged values or monitor the change in current values on the HMI device.
- "Function trend control": You display a tag value against a second tag value, for example, the engine speed against the heat produced.

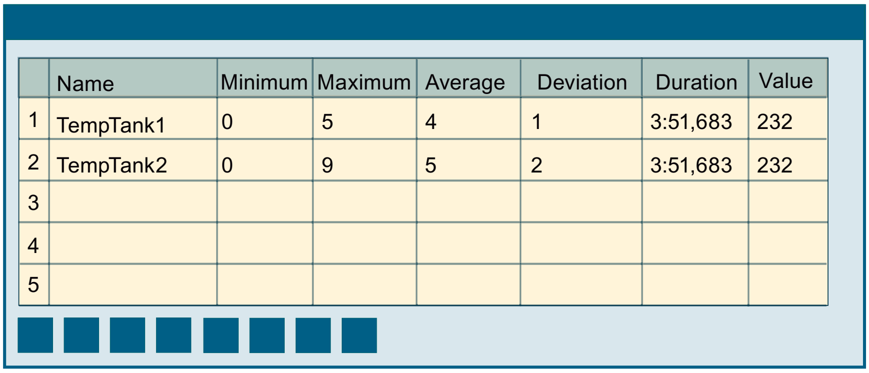
You can use the "Trend companion" to create statistics, for example, from the displayed values. Furthermore, you can use the trend companion as reading assistance for the trend control.

To display tag values in a table, use the process control.





	Time	Temperature	Tank	Pressure	
1	10:34:20	100	1	18	
2	10:34:30	20	1	60	
3	10:34:40	50	1	30	
4	10:34:50	50	1	55	
5	10:35:00	50	1	10	
6					
7					



	Name	Minimum	Maximum	Average	Deviation	Duration	Value
1	TempTank1	0	5	4	1	3:51,683	232
2	TempTank2	0	9	5	2	3:51,683	232
3							
4							
5							

Displayed values

When configuring the trend control, specify which tag values are to be displayed.

- "Online": The trend is continued with current individual values from the PLC.
- "Log": In runtime, the trend control displays the values of a tag from a data log. The trend shows the logged values in a particular window in time. The operator can move the time window in runtime to view the desired information from the log.

3.4.3.2 Operating controls

Starting and Stopping Update

Introduction

You can continue the update of the data contained in the control with the "Start/Stop" buttons.

Some buttons stop the update automatically, e.g. "Define statistics area"

The appearance of the button indicates whether the update is stopped or not:

⏸ The update has been stopped. To continue the update, click on the button.

⏸ The update has been started. To stop the update, click on the button

Creating statistics for Runtime data

Introduction

You can generate an analysis of the process data for the Runtime data in the trend or process control. You can display the evaluated data in the trend companion.

Overview

Use the following buttons to create statistics of runtime data:

⏸ "Start/stop"

⏱ "Select time range"

[〰] "Statistics area"

Requirement

- A trend control or process control is configured.
- A trend companion is configured and connected to the trend or process control.
- Runtime is enabled.

Displaying data in a statistics area window

Requirement:

The "Statistics area window" display mode is enabled in the trend companion.

To display data in the statistics area window of the trend companion, proceed as follows:

1. In the trend control or process control, click "Stop".
   The updated display is stopped, the process data continues being logged.
2. If you wish to evaluate data outside the displayed time range:
   - Click "Select time range".
     The "Time - Selection" dialog opens.
   - Enter the required time range.
     The data for the defined time range is displayed.
3. If you are using a trend control:
   - Click on the "Statistics area".
     In the trend control, two vertical lines are displayed on the right and left margin.
   - To define the statistics area, move the two lines to the desired position.
4. If you are using a process control:
   - Use the mouse to select the rows for the desired time range in the table.
     For different time columns with different time frames, you can select different time ranges for the calculation of statistics.
   - Click on "Statistic area" in the toolbar.

The evaluated data is displayed in the columns that you have configured in the statistics area window.

To continue with the display of Runtime data, click "Start".

Note

For additional statistical analysis of process data and logging of results, you can write the scripts yourself.

Displaying logged values

Introduction

Scroll through the displayed data of a log using the buttons in the toolbar of a trend or process control. If key combinations are configured, you can also use these for scrolling.

The buttons for browsing in logs are available only if data is supplied through logging tags.

The logged values of a tag are displayed within a time range in the trend or process control.

Overview

Use the following buttons to display logged values:

⏮ "First data record"

⏪ "Previous data record"

⏩ "Next data record"

⏭ "Last record"

Requirement

- Time range is configured.

Buttons for Archived Values

To scroll in archived values, proceed as follows:

1. To display the first data record of the time range, click on ⏮.
2. To display the previous data record of the time range, click on ⏪.
3. To display the next data record of the time range, click on ⏩.
4. To display the last data record of the time range, click on ⏭.

Elements of the information line

Elements of the information bar

The information bar of the trend control or process control can contain the following elements:

Icon	Name	Description
🖧	Connection status[1]	No faulty data connections.
🖧		Faulty data connections exist.
🖧		All data connections are faulty.
"Line 1"[2]	Selected line	Shows the number of the selected line.
"Column 2"[2]	Selected column	Shows the number of the selected column.
"23.02.2010"	Date	Shows the system date.
"23:59:59"	Time	Shows the system time.
🕓	Time base	Shows the time base used in the display of times.

Icon	Name	Description
[1]: If you double-click on the "Connection status" icon, the "Status of the data connections" window opens. The following properties of each data connection are listed in the window: • Name • Status • Tag name		
[2]: Only in the process control		

Basics of time range

The time range is the range from which the values at the HMI device are shown. The time range is determined by the start time and the end time. The time range is always in the past. If the end time is later than the current system time, the current system time is used as a temporary end time.

A distinction is made between the following time ranges:

- Static time range
- Dynamic time range

Static time range

The static time range is determined by fixed start and end times. The values are displayed within this time range.

Dynamic time range

The dynamic time range is determined by a period of time beginning with a fixed start time. The end time thus corresponds to the conclusion of the time period.

You set the time period as follows:

- Duration, e.g. 30 minutes
- The number of measurement points multiplied by the update cycle also produces a duration.

Configuring time range

Configure the time range for all controls. Configure the time range in the time column or in the time axis for the process control and the f(t) trend control. For the function trend control, configure the time range directly at the trend.

Exporting values

Requirement

- The "Export" button is configured in the control.

Procedure

1. Optional: For the export of a trend control, check the time format for the time axis configured in the control.
   The time axis of the export file takes on the time format configured in the control.
2. Click "Export" in the control.
3. Enter the name of the target file.
4. For the trend companion and process control: Choose whether all values are exported or just the values selected in the control.
5. Optional: Using "Select format", determine which separator and which character set the target file uses.

Note

Displaying Asian languages correctly in MS Excel

If Runtime is running in an Asian language, select the character set "UTF-8".

3.4.3.3 Trend companion

Trend companion basics

Function

The trend companion displays values or statistics from a control. The content of the trend companion is specified during its configuration.

Overview of the trend companion

The trend companion is connected to one of the following controls:

- Trend control
- Function trend control

In the trend companion, a "display mode" is specified during configuration. The display mode determines which data are shown in the trend companion.

Display mode

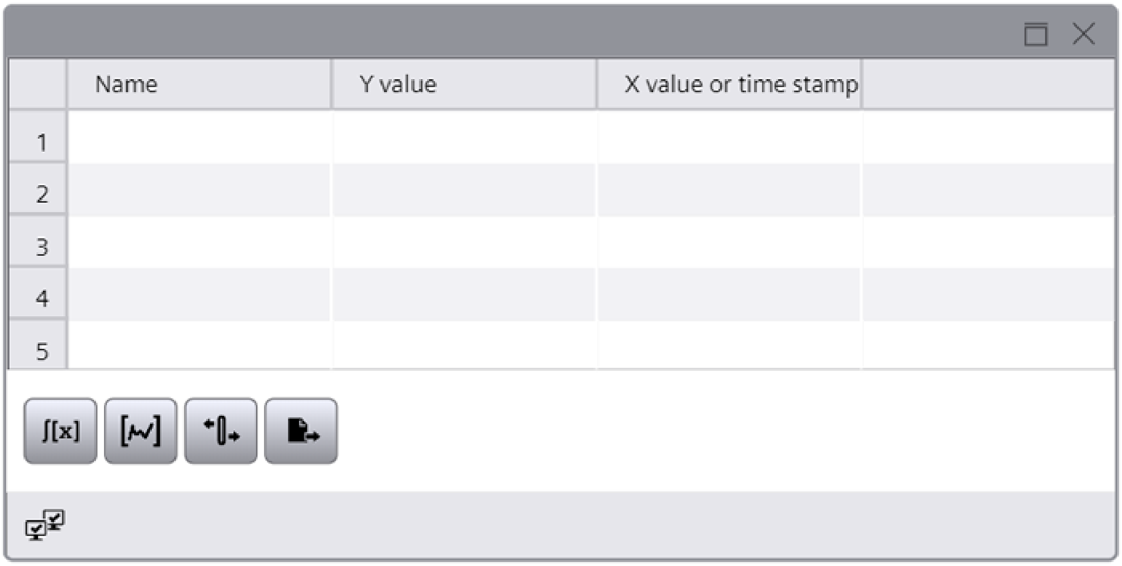
Three different display modes are available in the trend companion.

- Ruler window
  The ruler window shows the coordinate values of the trends on a ruler or values of a selected line in the table.
- Statistics area window
  The statistics area window shows the values of the low limit and high limit of the trends between two rulers or the selected area in the table. You can only connect the statistics area view to the trend control or the process control.
- Statistics window
  The statistics window displays the statistical evaluation of the trends. Among other things, the statistics include:
  - Minimum
  - Maximum
  - Average
  - Standard deviation
  - Integral

All windows can also display additional information on the connected trends or columns, such as time stamps.

Overview of trend companion

With the "Trend companion", you display evaluated data and statistics of a control in a table.



	Name	Y value	X value or time stamp	
1				
2				
3				
4				
5				

Buttons of the trend companion

The toolbar contains buttons for executing specific functions. Depending on the configuration, the following buttons are available for operator input:

Icon	Name	Function
∫[x]	Statistical analysis	Displays the statistical values from a defined "statistics range" of the trend or process controls in the statistics window of the trend companion. Only available with a configured trend companion.
[~]	Statistics area	Specifies the period for calculation of statistics.
←▯→	Ruler window	Displays a ruler that shows the coordinates of the intersection point with a trend in the trend companion. Requirement: The trend companion is configured with "Ruler window" display mode.
🖶	Print	Reserved for future versions.
🗎→	Export	Exports all or selected data to a *.CSV file. Depending on the configuration and authorizations, the following options may be available: • Display export settings and start export • Select file name and directory

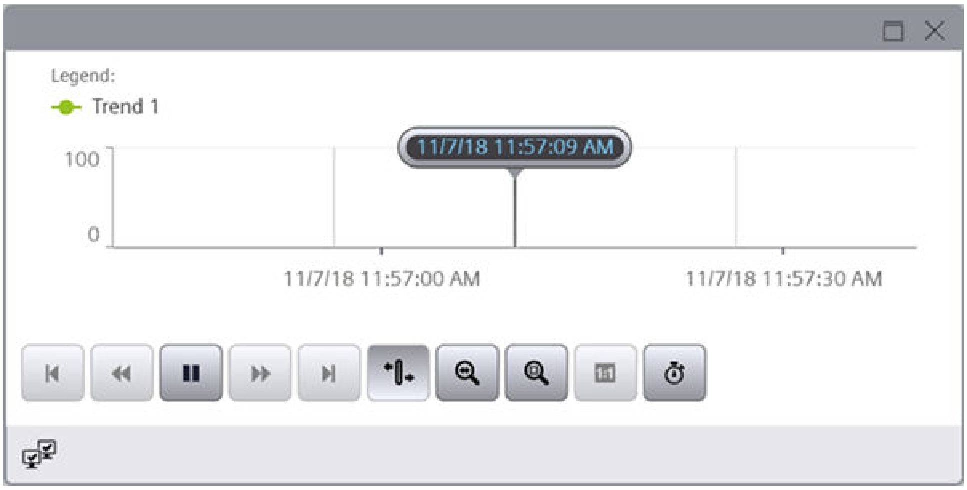
Rearranging columns

You can change the column arrangement configured in the engineering here. See section Rearranging columns at runtime (Page 284).

3.4.3.4 Trend control

Overview of trend control

With the trend control, you show the currently pending process values or logged values as a trend over time. You design the trend display according to your wishes.



Note

Trend display in future time range

The trend area located in the future continues the last drawn value.

Buttons of the trend controls

The toolbar contains buttons for executing specific functions. Depending on the configuration, the following buttons are available for operator input:

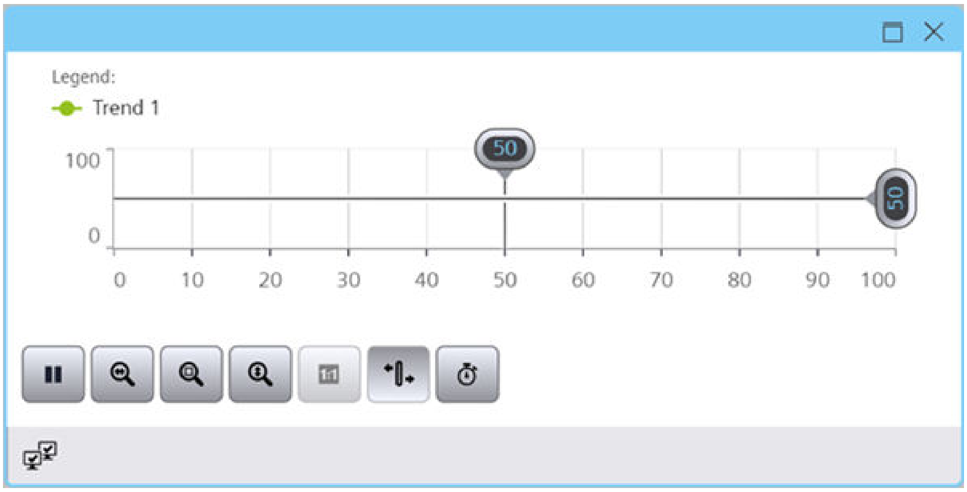
Icon	Name	Function
⏮	First record	Shows the trend direction starting with the first logged value. Requirement: The values come from a process value log.
⏪	Previous record	Shows the trend direction of the previous time range.
⏸	Start/stop	Stops and starts the trend update. Started: The trend is continuously updated. It always shows the latest values. Stopped: New values are buffered and updated as soon as you start the trend update again.
⏩	Next record	Shows the trend direction of the next time range.

Icon	Name	Function
⏭	Last record	Shows the trend direction up to the last logged value. Requirement: The values come from a process value log.
	Previous trend	Displays the previous trend in the foreground.
	Next trend	Displays the next trend in the foreground.
	Ruler	Displays a movable ruler that shows the coordinates of the intersection point with a trend in the trend companion. With stopped trend update, the trend values are also displayed in tooltips. Requirement: The trend companion is configured with "Ruler window" display mode.
	Zoom time axis +/-	Zooms into or out of the time axis in the trend control. Left-click: Zoom in
	Zoom value axis +/-	Zooms in or out of the value axis in the trend control.
	Zoom area	Zooms in on the section of the trend control. You define the section by dragging with the mouse. Use the "Original view" button to return to the original view.
	Zoom +/-	Enlarges or reduces the view in the trend window.
✥	Move trend area	Moves the display in the trend area.
	Move axes area	Moves the display in the axes area.
1:1	Original view	Returns to the original view from the zoomed display.
⏱	Select time range	Opens a dialog in which you configure the time range.
	Select trends	Opens a dialog in which you set the visibility and sorting of trends.
	Select data connection	Opens a dialog in which you select the data source: • Process value log • Tag • Recipe (only function trend control)
	Statistics area	Enables you to define a time range for which statistical values are determined. Vertical lines which you use to set the time range are displayed in the trend window.

Icon	Name	Function
∫[x]	Statistical analysis	Opens a statistics window to display the minimum, maximum, average, and standard deviation for the selected time range and the selected trend.
🖨	Print	Starts printing the trends shown in the trend window.
📈	Export	Opens the dialog for saving the trend data in CSV format. The time axis in the export file takes on the time format configured in the control. If necessary, change the configuration of the time format in the control before the export.
▼◇	Select context	Shows the value range of the resulting data for analysis purposes

Overview of function trend control

With the function trend control, you display active or logged process values as a function of another tag in a trend. You design the trend display according to your wishes.



Note

Trend display in future time range

The trend area located in the future continues the last drawn value.

Button of the function trend control

The toolbar contains buttons for executing specific functions. Depending on the configuration, the following buttons are available for operator input:

Icon	Name	Function
⏸	Start/Stop	Stops and starts the trend update. Started: The trend is continuously updated. It always shows the latest values. Stopped: New values are buffered and updated as soon as you start the trend update again.
🔍	Zoom X axis +/-	Zooms into or out of the time axis in the trend control. Left-click: Zoom in <Shift + Left-click>: Zoom out Use the "Original view" button to return to the original view.
🔍	Zoom area	Zooms in on the section of the trend control. You define the section by dragging with the mouse. Use the "Original view" button to return to the original view.
🔍	Zoom X axis plus minus	Zooms into or out of the time axis in the trend control. Left-click: Zoom in <Shift + Left-click>: Zoom out Use the "Original view" button to return to the original view.
🔍	Zoom Y axis plus minus	Zooms in or out of the value axis in the trend control. Left-click: Zoom in <Shift + Left-click>: Zoom out Use the "Original view" button to return to the original view.
1:1	Original view	Returns to the original view from the zoomed display.
📈	Previous trend	Displays the previous trend in the foreground.
📈	Next trend	Displays the next trend in the foreground.
↔	Ruler	Displays a ruler that shows the coordinates of the intersection point with a trend in the trend companion. Requirement: The trend companion is configured with "Ruler window" display mode.
✥	Move trend area	You can move the trends in the trend window along the X axis and the Y axis using the button. Values from the future trend area apply the last displayed value.
↕	Move axes area	You can move the trends in the trend window along the value axis using the button.
⏱	Select time range	Opens a dialog in which you configure the time range.

Icon	Name	Function
📈	Select trends	Opens a dialog for setting the visibility of trends.
🗂	Select data connection	Opens a dialog in which you select the data source: • Process value log • Tag • Recipe
🖨	Print	Click this button to print the trend shown in the trend window. The print job used during printing is defined in the configuration dialog in the "General" tab.
📈	Export data	This button is used for exporting all or the selected runtime data to a csv file.

Value aggregation

Introduction

If the number of process values or archive values to be displayed for the selected time range in a trend control is larger than the number of pixels available for the trend, they will be aggregated.

Which values are aggregated to a trend value depends on the loading time of the trend control. For this reason, screen changes can result in a change of the trend line.

Avoid aggregation

To avoid that values are aggregated, select a shorter time range or enlarge the width of the trend control.

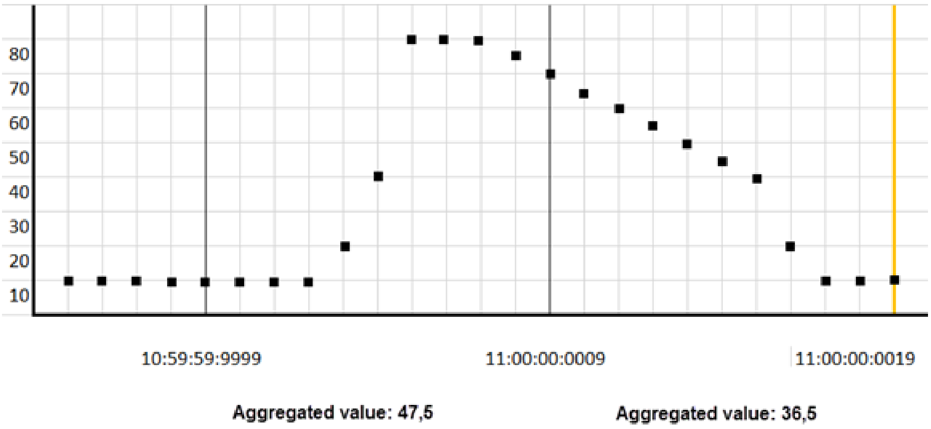
Example

- Pixels available for the trend: 600
- Measuring interval of the tag set as the data source: 10 times per s
- Time range: 10 minutes,

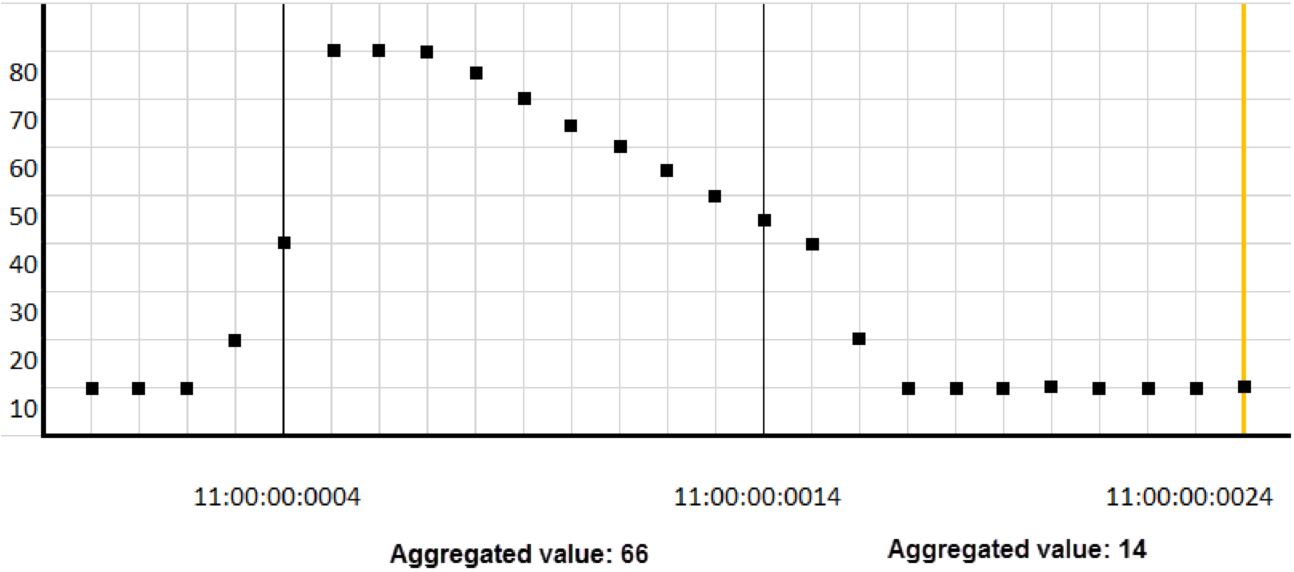
i.e. in the selected time range, 6000 values are measured or logged. When drawing the trend, 10 values are aggregated to each trend value.

The trend displays different values depending on the loading time. The following graphics illustrate how the last two aggregated trend values change when the loading time is 11:00:0019 instead of 11:00:0024.

- Loading time 11:00:0019:



- Loading time 11:00:0024:



Using the trend control

Online configuration of the trend control

Introduction

In Runtime, you configure online and thus change the appearance of the trend control.

During the configuration of the trend control, it is specified whether online configurations are retained or discarded during a screen change or after Runtime is ended.

Overview

Use the following buttons to configure the trend control in Runtime:

▯▯	"Select data connection"	Opens a dialog in which you can set the source from which a configured trend is supplied. Possible sources are the tags or logging tags of an HMI device or plant object and UDTs.
📈	"Select trends"	Opens a dialog in which you set the visibility and sorting of trends.
⏱	"Select time range"	Opens a dialog in which you configure the time range.

In addition, you have the options to add additional trends using drag-and-drop operation.

See also

Select data connection of a trend (Page 147)

Add new trend (Page 142)

Add new trend

Adding new trends is not supported by the f(x) trend control.

Requirement

- A trend control and an IO field are configured in the process screen.
- The IO field has a link to a tag with numeric data type.

Procedure

Drag and drop the IO field onto the trend control.

For trend controls with multiple trend areas, drag the IO field to the desired trend area.

Result

If the tag in the trend area is not already used as the source of a trend, a new trend is added to the trend area and plotted. The trend represents the process values of the tags.

You can change the visibility of the trend via the "Select trends" button or via a script.

Changing the screen and refreshing the page removes the trend from the trend area.

Using the zoom functions in trend windows

Note

Scrolling in a zoomed in trend control

When the trend control is zoomed in, you can scroll using the mouse wheel:

- Move the mouse wheel to scroll up or down.
- Press <Shift> and move the mouse wheel to scroll to the left or right.

Introduction

Key functions can be used for zooming in on, zooming out of and returning to the original view for trends, axes and various zoom areas of the trend window.

Overview

The following zoom functions are available in the trend window:

🔍	Zoom time axis +/-	Zooming in or out of time axis
🔍	Zoom value axis +/-	Zooming in or out of value axis
🔍	Zoom area	Zooming in on a trend control area
🔍	Zoom +/-	Zooming in or out on trend
1:1	Original view	Returning to the original view

Requirement

- The trend control is open
- Buttons with zoom functions are configured
- Runtime is enabled

Zooming in on a trend control area

Via the toolbar

1. Click "Zoom area" in the toolbar.
   The updated display is stopped.
2. Drag with the mouse to draw a box around the area to be zoomed.
   If there are at least two measured values within this area, the area of the trend is zoomed.
3. To return to the original view of the trend, click "Original view".
4. To restart the update, click "Start/Stop".

The default values are used for the axis.

Using the mouse wheel

Requirement: No zoom button was clicked in the toolbar.

1. Pause the update of the trend control.
2. Press <Ctrl> and move the mouse wheel.

Zooming in or out on trends

If you zoom in or out on a trend, the 50% value of the trend is always in the middle of the value axes.

Proceed as follows to zoom in or out on a trend:

1. Click "Zoom +/-".
   The updated display is stopped.
2. To zoom in on a trend, click on the trend with the left mouse button.
3. To zoom out on a trend, hold down the <Shift> key and click on the trend with the left mouse button.
4. To return to the original view of the trend, click "Original view".
5. To restart the update, click "Start/Stop".

The default values are used for the axis.

Note

If you change the value area of a value axis on the "Value Axis" tab in the configuration dialog while zooming, the visible zoom area is set to the new value area.

Zooming in on the time axis or value axis

While zooming with time or value axes, the 50% value of the trend is always in the middle of the axes.

Proceed as follows to zoom the time axis or value axis:

1. To zoom in or out on the time axis, click on "Zoom time axis +/-".
   The updated display is stopped.
2. To zoom in or out on the value axis, click on "Zoom value axis +/-".
   The updated display is stopped.
3. To zoom in on an axis, click on the trend control with the left mouse button.
4. To zoom out on an axis, hold down the <Shift> key and click on the trend control with the left mouse button.
5. To return to the original view of the trend, click "Original view".
6. To restart the update, click "Start/Stop".

The default values are used for the axis.

Zooming using touch gestures

Refer to the section Supported gestures (Page 79).

Sorting trends

If a trend area contains multiple trends, you can select the order of the trends.

You have the following options:

- Specify the top trend
- Specify the order of all trends

Specify the trend order

Requirement

The "Select trend" button is configured in the toolbar.

Procedure

1. Click "Select trend" in the toolbar.
2. Click on a trend.
3. Move the trend to the selected position using the buttons.
4. Repeat these steps for the other trends.

Note

The trend at the top position is displayed in the trend area as the top trend.

Specify the top trend

In the drop-down list of the trend area, select the trend that you want to display as top trend.

Alternatively, use the "Select trend" button in the toolbar and move the desired trend to the top position.

Hiding and showing trends

Requirement

The "Select trend" button is configured in the toolbar.

Procedure

1. Click "Select trend" in the toolbar.
2. Disable the trend option to hide a trend.
3. Enable the trend option to show a trend.

Determining the coordinates of a point

Introduction

The "Ruler" button is used to determine the coordinates of a point on the trend by means of a ruler. You can zoom in on an area of the trend to make coordinate finding easier. If you display the ruler in the trend control, you can move the ruler at any time.

If you click on the trend with the mouse, several trend parameters are shown in the tooltip for the trend control.

Requirement

- A trend control is configured
- A trend companion is configured and connected with the trend control
- The "Ruler window" display mode is activated in the trend companion
- Runtime is activated

Procedure

Proceed as follows to determine the coordinates of a point:

1. Click "Ruler" in the trend control.
   The ruler is shown.
2. Move the ruler to the desired position with the mouse.
3. If you want to zoom in on an area, click on "Zoom area".
   - Move the ruler to the desired position with the mouse.
   - To return to the original view, click "Original view".

Result

In the ruler window of the trend companion, besides the X value/time stamp and the Y value, the data that you have configured in the trend companion is shown in the columns.

In the trend companion, the indices "i" and "u" can be displayed in addition to the values:

- "i.": The displayed value is an interpolated value.
- "u.": The displayed value has an uncertain status:
  - The start value after Runtime activation is unknown
  - A substitute value is used

Note

You can also display the "uncertain" status of a value in the displayed trend curve. You must activate the "Value with uncertain status" option on the "Trends" tab under "Limits".

Alternative procedure

Alternatively, you can also connect the trend companion to the process control. In the "ruler window" display mode, the values of the selected row are displayed in the trend companion.

Select data connection of a trend

You have the option to set in Runtime the source from which a trend is supplied.

Possible sources:

- Tags and logging tags of an HMI device, plant object or PLC
- UDTs

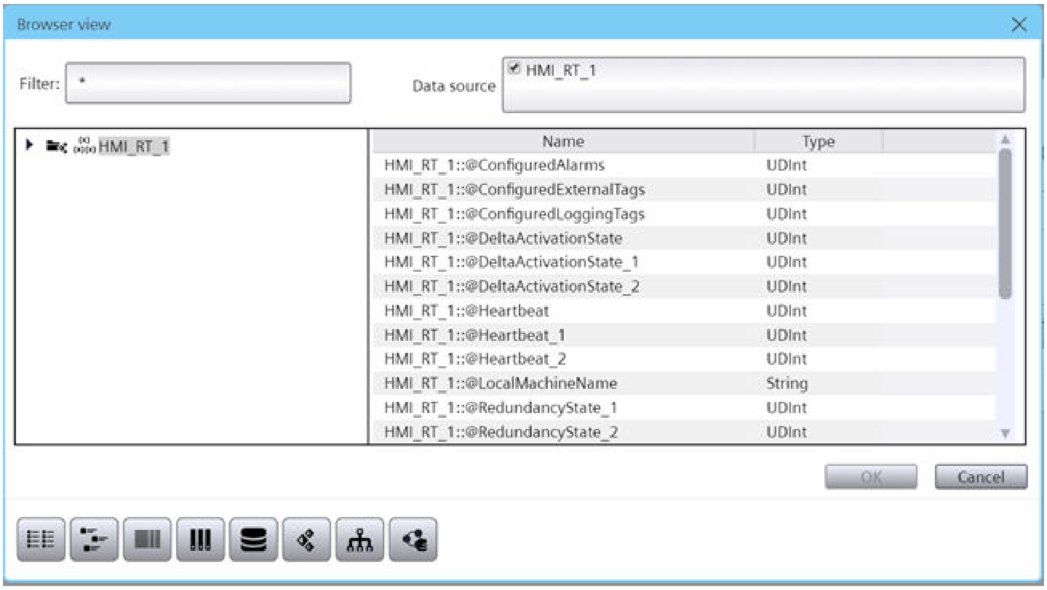
Requirement

- An HMI device has been configured.
- A trend control is configured in the screen of the device.
- To display logging tags: A data log has been configured.
- To display the tags of a plant object: The plant hierarchy has been created and assigned to the HMI device.
- Runtime is active.

Procedure

1. Click on "Select data connection" in the toolbar of the trend control.
   The "Selection of logs/tags" dialog opens.
2. Click "Trend:" and select a trend.

3. Click "Tag".
   The "Browser view" dialog opens in which you specify how the selected trend is supplied with data.



Filter: *

Data source: ☑ HMI_RT_1

HMI_RT_1

Name	Type
HMI_RT_1::@ConfiguredAlarms	UDInt
HMI_RT_1::@ConfiguredExternalTags	UDInt
HMI_RT_1::@ConfiguredLoggingTags	UDInt
HMI_RT_1::@DeltaActivationState	UDInt
HMI_RT_1::@DeltaActivationState_1	UDInt
HMI_RT_1::@DeltaActivationState_2	UDInt
HMI_RT_1::@Heartbeat	UDInt
HMI_RT_1::@Heartbeat_1	UDInt
HMI_RT_1::@Heartbeat_2	UDInt
HMI_RT_1::@LocalMachineName	String
HMI_RT_1::@RedundancyState_1	UDInt
HMI_RT_1::@RedundancyState_2	UDInt

4. (Optional) Define in a filter.
5. Use the toolbar to configure the display in the dialog:

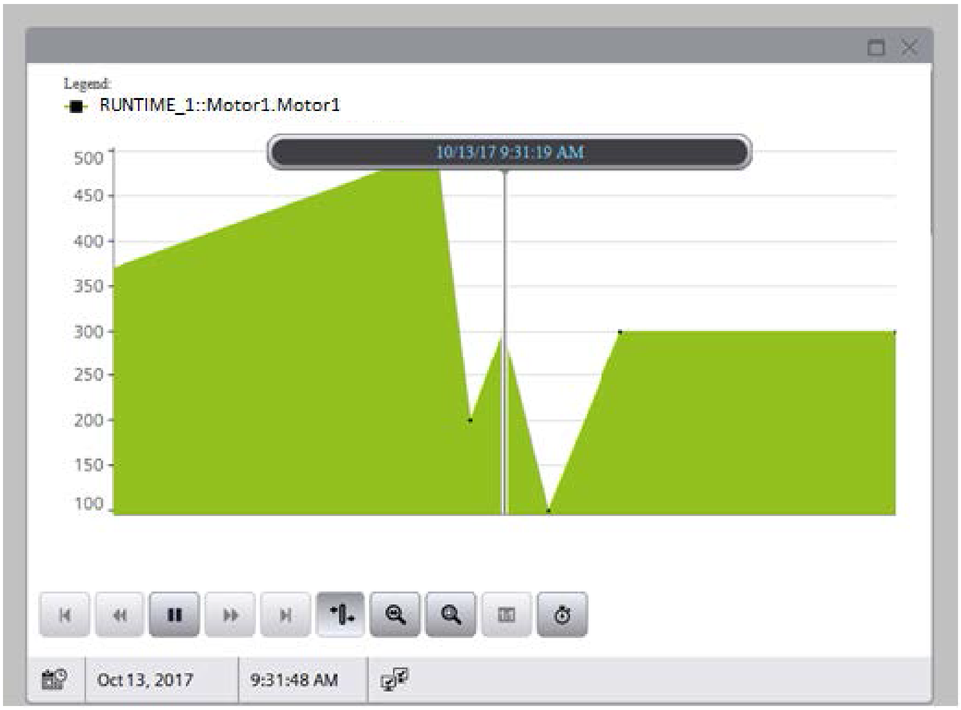
☷	"Small icons"
☰	"List"
▥	"Details"

6. Use the toolbar to configure the contents of the dialog:

	"Online tags"	Shows the device and its tags.
	"Logging tags"	Shows the device and its logging tags.
	"CPM"	Shows the plant hierarchy and the plant object tags.
	"UDT"	Shows the device and its UDTs.
	"CPM logging tags "	Shows the plant hierarchy and the logging tags of the plant objects.

7. In the tree, select the object whose data you want to display in the trend control.
8. Select a tag as the data source.
9. Confirm your entries.

The values of the tags are displayed in the trend control. If the path belongs to a plant object, the path of the plant object is also shown in the trend control.



Changing the time range of a trend

Procedure

To configure the time range, follow these steps:

1. Click "Select time range" in the toolbar of the trend control.
   The "Time selection" dialog opens.
2. Under "Time axes", select the time axis with the time range you want to adjust.
   Under "Trend area", you can see to which trend area the selected time axis belongs.
   If the trends in a trend control are to be displayed with a common time axis, the specified time range applies to all trends.
3. Configure the time range as described below.

Note

The format of date and time depends on the Runtime language used.

Configure time range

1. Select the "Time interval" entry in "Setting".
2. Select date and time of the start time.
3. Set the duration of the time range. To do this, enter a factor and select the time unit.
   Example: "90" as the factor and "Seconds" as the time unit for a duration of one and a half minutes.
4. Confirm your entries.

The time range of the time axis is adjusted:

- If the preset start time has been changed:
  - The trend update is paused.
  - The time axis starts with the selected start time.
- If the preset start time has been retained: The trend update continues. The preset start time is not included in the time axis.
- The duration of the time axis results from the factor and time unit.

Configure start time and end time

1. Select the "Start time and end time" entry in "Setting".
2. Select the date and time of the start time and end time.
3. Confirm your entries.

The time range of the time axis is adjusted:

- If the preset start time and/or end time has been changed:
  - The trend update is paused.
  - The time axis starts with the start time.
- If the preset start time and end time have been retained: The trend update continues. The preset start time and end time are not included in the time axis.
- The duration of the time axis results from the start time and end time.

Configure number of measuring points

1. Select the "Measuring points" entry in "Setting".
2. Select date and time of the start time.
3. Enter the number of desired measuring points under "Measuring points".
4. Confirm your entries.

The time range of the time axis is adjusted:

- If the preset start time has been changed:
  - The trend update is paused.
  - The time axis starts with the start time.
- If the preset start time has been retained: The trend update continues. The preset start time is not included in the time axis.
- The duration of the time axis results from the number of measuring points multiplied by the update cycle.

See also

Basics of time range (Page 132)

Display context data of the plant objects in a trend control

This section describes how to show context-dependent data of a plant object in the trend control.

The evaluation is relevant, for example, in connection with the WinCC Performance Insight in order to analyze the effectiveness or the fault rate of the plant.

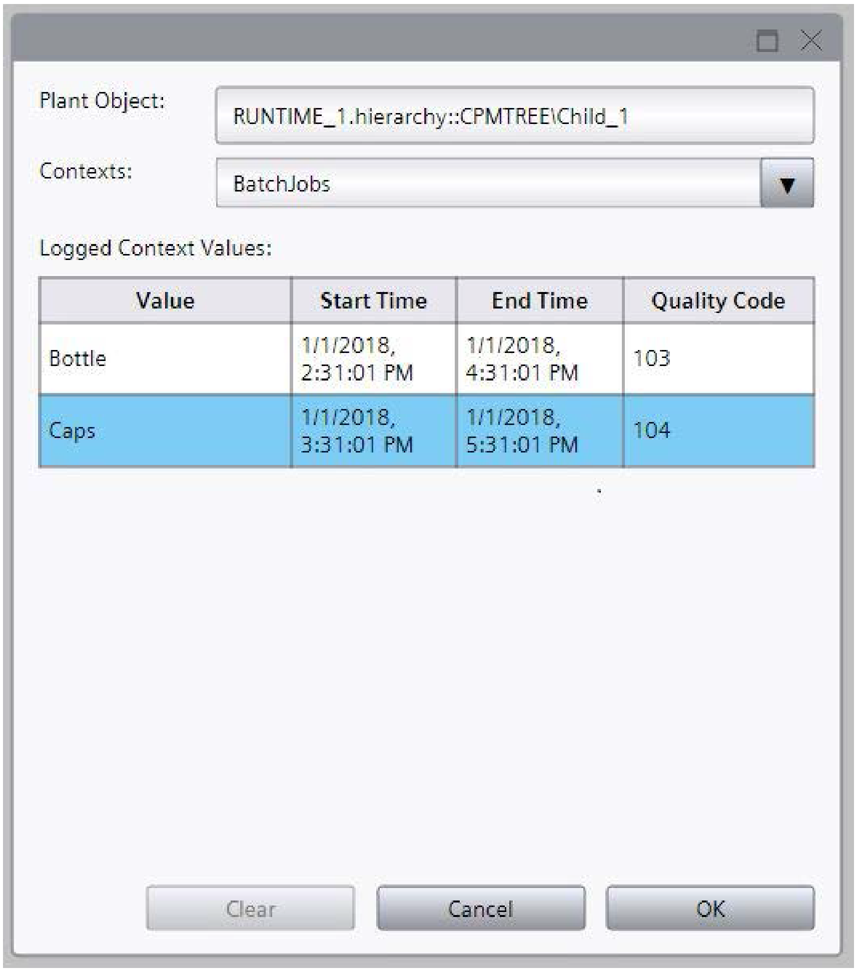
Requirement

- A trend control is configured in the screen of an HMI device.
- The plant hierarchy has been created and assigned to the HMI device.
- The data source of one of the trends in the trend control is a plant object.
- To display the logging tags of the plant object: A data log has been configured.

- Contexts are available for the plant object.
- The "Select context" button is configured for the trend control.

Procedure

1. In the trend control, click "Select context".
2. Select the plant object set as data source.
3. Select one of the contexts assigned to the plant object in the "Context" drop-down list. A list of the entries logged for the context appears under "Logged context values".
4. Select an entry.
5. Click "OK".



Plant Object: RUNTIME_1.hierarchy::CPMTREE\Child_1

Contexts: BatchJobs

Logged Context Values:

Value	Start Time	End Time	Quality Code
Bottle	1/1/2018, 2:31:01 PM	1/1/2018, 4:31:01 PM	103
Caps	1/1/2018, 3:31:01 PM	1/1/2018, 5:31:01 PM	104

Result

The time period of the selected entry is applied to the time axis of the trend area. The trend represents the data that falls within the time period of the selected entry.

Note

Effect on other trend areas

If the plant object selected as data source has multiple interface tags and trends from other trend areas of the trend control display these tags, their time axes are also updated accordingly.

See also

Select data connection of a trend (Page 147)

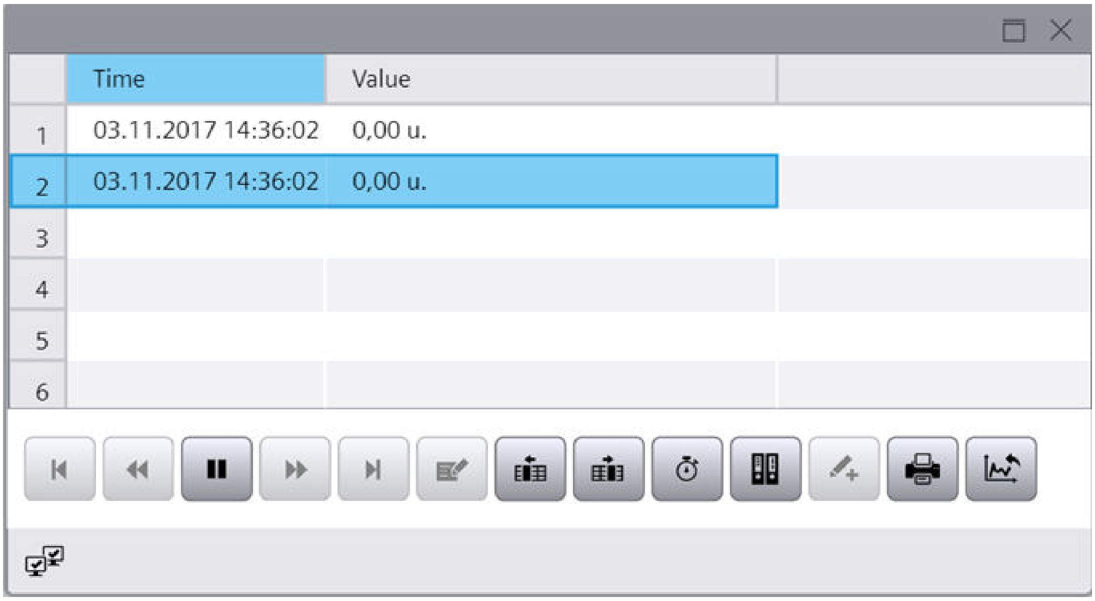
Contexts (Page 57)

3.4.3.5 Process control

Overview of process control

With the process control, you display active or logged process values in a table. You design the display of the table as you wish.

You create statistics from selected data. You also export the data for further use.



	Time	Value	
1	03.11.2017 14:36:02	0,00 u.	
2	03.11.2017 14:36:02	0,00 u.	
3			
4			
5			
6			

Buttons of the process control

The following table shows the buttons that are available in the process control:

Icon	Name	Function	ID
⏮	"First data record"	Displays the history of a tag within a specified time range starting with the first logged value. Requirement: Values come from a process value log.	0
⏪	"Previous data record"	Displays the history of a tag within the previous time interval, based on the currently displayed time interval. Requirement: Values come from a process value log.	1
⏸	"Start/stop"	Stops and starts the column update. The values are buffered and updated as soon as you start the column update again.	2
⏩	"Next data record"	Displays the history of a tag within the next time interval, based on the currently displayed time interval. Requirement: Values come from a process value log.	3
⏭	"Last record"	Displays the history of a tag within a specified time range ending with the last logged value. Requirement: Values come from a process value log.	4
✎	"Edit"	Activates editing of table entries. To edit a value, double-click in the desired table cell. Requirement: Updated display is stopped.	5
←	"Previous column"	Moves the value column in front of the previous value column. The function refers to the value columns that are assigned to a time axis.	6
→	"Next column"	Moves the value column to behind the next value column. The function refers to the value columns that are assigned to a time axis.	7
⏱	"Select time range"	Opens a dialog in which you configure the time range.	8
▥	"Select data connection"	Opens the dialog for selecting the logs and tags of an HMI device, plant object or PLC that serve as data source for this table view.	9
✎+	"Create archive value"	Creates a table entry for a log value. Enter the log value manually. Its time stamp corresponds to the time at which you added the table entry.	10
🗑	"Delete archive value"	Deletes a logged value.	11
➜	"Export"	Exports all or selected data to a *.CSV file. Depending on the configuration and authorizations, the following options may be available: • Display export settings and start export • Select file name and directory	12

Using the process control

Online configuration of the process control

Introduction

In Runtime, you configure online and thus change the layout of the process control. The process control configuration specifies whether online configurations are retained or discarded on a screen change or after Runtime is ended.

Overview

The following buttons make online configuration possible in process control:

"Select data connection"

"Select time range"

Changing the data connection

The following table shows the configuration options for data connection:

Field	Description
Value column	Choose the configured value column for which you want to change the data connection.
Data Source	Define whether the selected value column is supplied with a logging tag or online tag.
Tag name	Select the tag name for the data connection.

Proceed as follows to change the data connection:

1. Click "Select data connection" in the toolbar.
   The "Log/tag selection" dialog is opened.
2. Choose the "Value column" for which you want to change the data connection.
3. Select the "Data supply" and the "Tag name".

Changing a time range

The following table shows the configuration options for the time range:

Field	Description
Time column	Select the configured time column for which you want to define a time range.
Time range	Set the time range: • If you want to define a fixed time interval, select the setting "Start to end time". Enter the date and time for each. • If you want to define a time period, select the setting "Time range". Define the date and time for the start time. The length of the time interval to be displayed is determined by multiplying the "Factor" by the "Unit of time". • If you want to display a certain number of values, select the setting "Number of measuring points". Define the date and time for the start time. Enter the desired number of measuring points in the input field.

To configure the time range, follow these steps:

1. Click "Select time range" in the toolbar of the process control.
   The "Time - Selection" dialog opens.
2. Choose the "Time column" for which you want to adapt the time range.
   If the columns of a process control are to be displayed with a common time axis, the specified time range applies to all columns.
3. Configure the time range.
   The entry format of the date and time depends on the Runtime language used.

Editing a table field

Introduction

You change the values displayed in the process control manually using the "Edit" button.

Overview

The following buttons allow you to edit the table fields:

⏸	"Start/stop"
✎	"Edit"

Requirement

- The process control is configured
- The "Edit" button is configured
- Runtime is activated

Procedure

Proceed as follows to edit a table field in Runtime:

1. Click "Stop" in a process control.
   The updated display is stopped, the process data continues being logged.
2. Click "Edit".
3. Double click on the desired table field of a value column.
4. Enter the new value.
   The changed value is logged.
5. To continue with the display of Runtime data in the process control, click on "Start".

Moving value columns

You can rearrange the value columns assigned to a time axis.

Via the toolbar

1. Click on a column.
2. To move a column to the left, select "Previous column" in the toolbar
   The column is shifted one position to the left.
   If you have selected the first column, it is moved to the end of the value columns.
3. To move a column to the right, select "Next column" in the toolbar.
   The column is shifted one position to the right.
   If you selected the last column, it is moved to the beginning of the value columns.

With the mouse

See section Rearranging columns at runtime (Page 284).

3.4.4 Screen window

Use

The "Screen window" object is used to display other screens of the project in the current screen. To continuously update the content of a screen window, for example, the object must be dynamized. Custom menus and toolbars can add specific buttons to the screen window.

You can also use independent screen windows independently of the screen in question. With appropriate hardware equipment and support by the operating system, you can also control multiple monitors and map processes in a more comprehensive and differentiated manner.

Layout

The settings for the position, geometry, style and color of the object are made during configuration.

In particular, the following properties are changed:

- Zoom factor: Defines the size of the embedded screen.
- Screen section: Defines the section of the embedded screen that is displayed in the screen window. If the embedded screen is larger than the screen window, you configure scroll bars for the screen window.
- Independent screen windows: Specified that the screen windows are displayed independently from the screen in which they were configured.

Note

Cascading screen windows

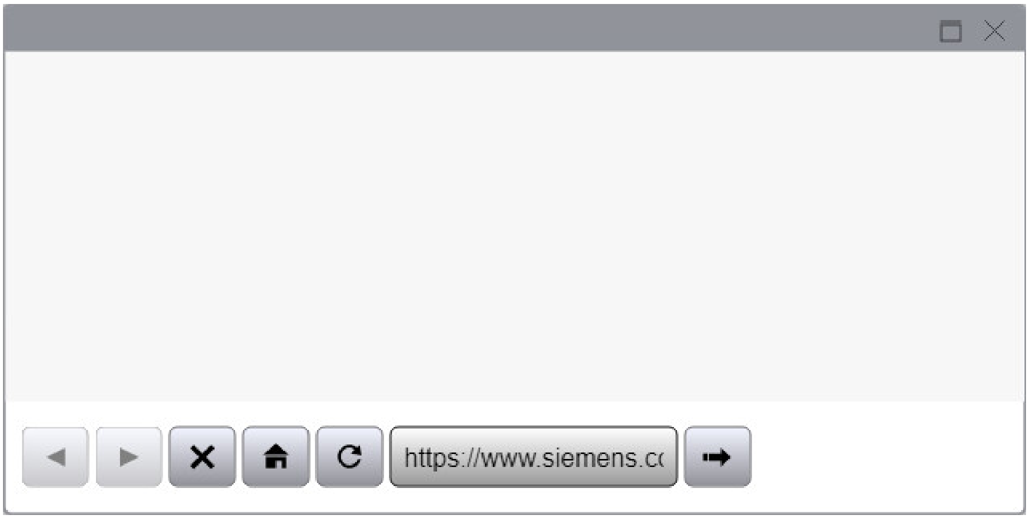
Screen windows can also display screens which, in turn, contain screen windows. Up to 14 cascaded screen windows can be displayed.

3.4.5 Web control

Introduction

The "Browser" control is designed for the visualization of simple HTML pages. It allows creation of centrally stored machine-specific descriptions, which are displayed from different HMI devices.

You have access to the data of the local user management in Runtime via a browser.



Note

Switching the functionality of the web control as a file explorer, in the following ways, for example, is not enabled in WinCC:

- Entry of a folder or drive, e.g. "\" or "C:", or
- Connection to an FTP server, for example, "ftp://"

One reason this function is not implemented is to prevent inadvertent changes to files, their deletion or execution.

When configuring, ensure that the operator can only enter valid Internet addresses, for example, by using symbolic I/O fields. Configure a password-protected input for service purposes.

Note

Page navigation in the web control

Whether you can navigate back and forth between the pages that you have viewed in the web control depends on the browser and browser versions in which Runtime is running. If the browser or browser versions do not support page navigation, the buttons in the web control are disabled.

Displayed content

Remember the following notes when using the control:

- The "Browser" control only shows contents that are supported by the browser in which Runtime is open.
- The control is implemented as IFrame. Pages with X-Frame option settings that prevent the display in an IFrame are not displayed in the control.
- As compared to a standard browser, the "Browser" control has limited functionality:
  - Navigation from the "Browser" control is not supported (top-level navigation).
  - Calls of queries and dialogs (pop-ups and modal dialogs) are only supported if they were activated in the file <Path for the WinCC Unified installation directory>WinCCUnified\WebRH\public\content\custom\CustomSettings.json:
    ```
    {"CustomSettings": {"HmiWebControl" : {"AllowPopups" :
    true,"AllowModals" : true}}}
    ```

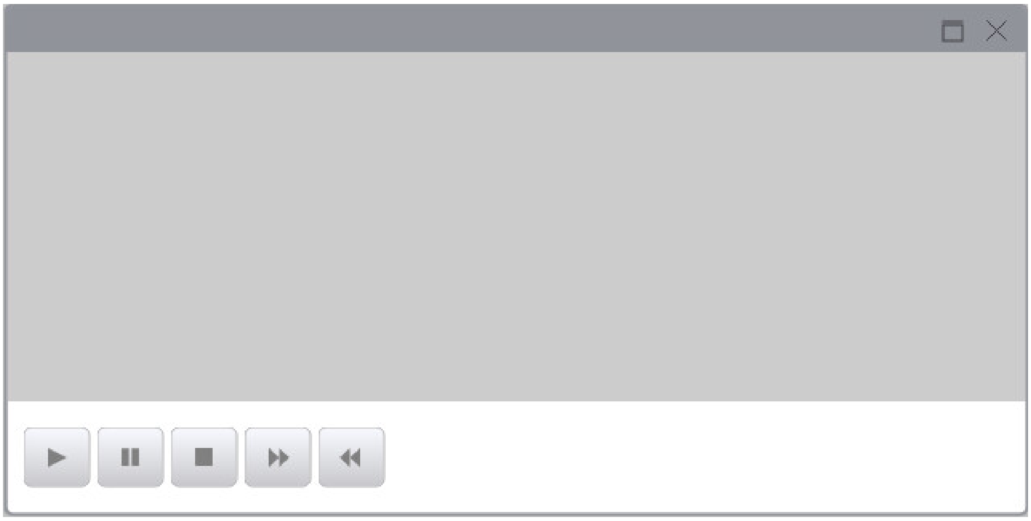
    Note

    Pop-ups and modal dialogs stop the update.
  - Links to embedded files, for example, *.pdf or *.xls, are not supported.
  - Queries and dialogs that are conducted during the access of, for example, protected pages are not supported.

3.4.6 Media player

Use

In Runtime, the media player is used to play multimedia files via an https connection.



Layout

The settings for the position, style and color of the object are made during configuration.

In particular, the following properties are changed:

- Display operator controls: Specifies the buttons in runtime.
- Show tracker: establishes, whether a slider is available for the operation.

Supported file formats

The media player supports all formats that support the HTML5 video tag.

Restrictions

Note

Play restrictions

- The web control security settings do not allow local files to be played.
- Playing multimedia files in the Runtime control system depends on factors such as the installed operating system, the browser used and video and audio codecs installed on the machine.
  Examples:
  - Internet Explorer does not play any video file with an embedded .wav audio file.
  - Most browsers do not support .avi files.
- The browser determines which video formats are supported.
  You can find an overview of the video formats supported by popular browsers here (https://www.w3schools.com/html/html5_video.asp).
  You can find a detailed overview of the browser version used or between browsers here (https://html5test.com/compare/browser/index.html).
- iOS guidelines for the <video autoplay> element are available here (https://webkit.org/blog/6784/new-video-policies-for-ios/).

Note

Requirements for video files

To play video files in the Windows Server 2008 R2 SP1 and 2012 R2, install the Microsoft feature "Desktop Experience". You will find more detailed information on this topic on the Internet in the Microsoft documentation.

Note

Data loss when copying the project

If you copy the project to another PC, keep the following in mind:

Files indicated in the WinCC Media Control are not copied along with the other files if they are dynamically linked and no UNC path is specified. You have to load the files into the project again.

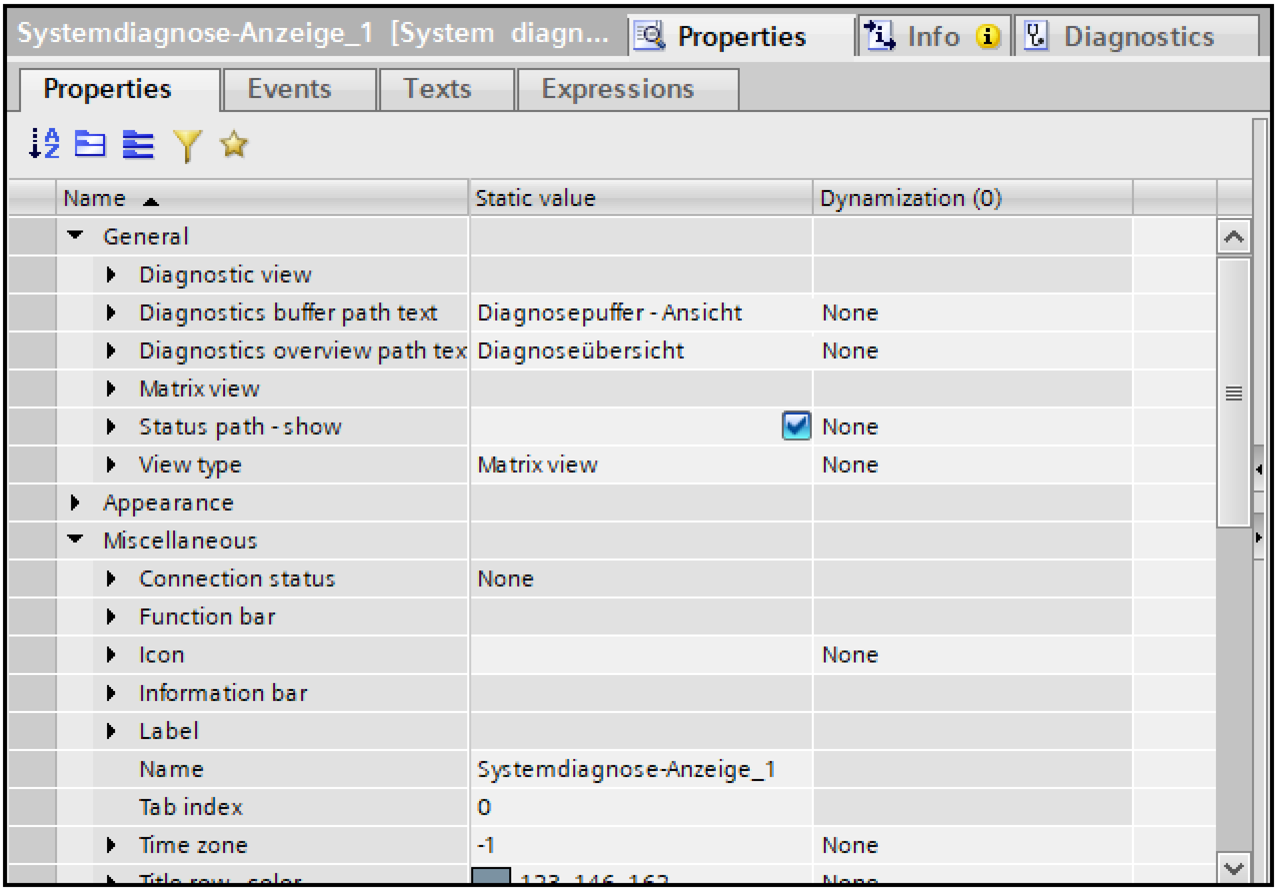
3.4.7 System diagnostics display

Use

You can use the "System diagnostics control" object to display the diagnostic status of several PLCs using traffic light SVGs. The diagnostic status contains the overall status of all relevant PLCs. The merged state is always the worst state of all PLCs.

Defining the properties of the system diagnostics control

You define the properties of the system diagnostics control in the Inspector window under "Properties > Properties".


Systemdiagnose-Anzeige_1 [System diagn...

Name	Static value	Dynamization (0)
General		
Diagnostic view		
Diagnostics buffer path text	Diagnosepuffer - Ansicht	None
Diagnostics overview path tex	Diagnoseübersicht	None
Matrix view		
Status path - show	☑	None
View type	Matrix view	None
Appearance		
Miscellaneous		
Connection status	None	
Function bar		
Icon		None
Information bar		
Label		
Name	Systemdiagnose-Anzeige_1	
Tab index	0	
Time zone	-1	None
Title row - color	123, 146, 162	None

Selecting the view type

You select the view type in the following way:

1. Click "Properties > Properties > General > View type" in the Inspector window.
2. Select between the "Matrix view", "Diagnostic view" and the "Distributed I/O view".

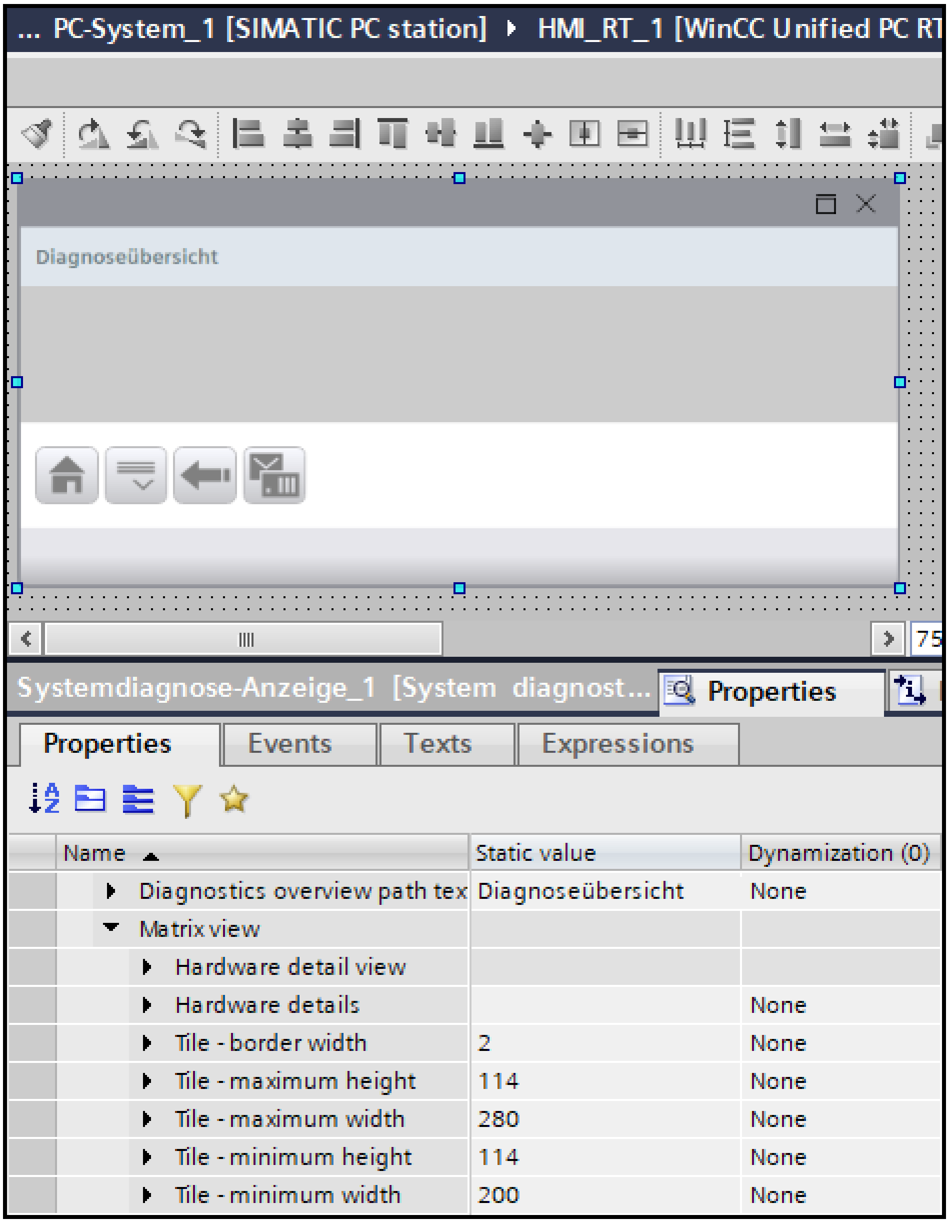
Selection of the matrix view as start view is recommended. From the matrix view, you can switch to the diagnostic view using the corresponding button in the toolbar.

Matrix view

With the matrix view, you have the possibility to check the status of your PLCs and their lower-level hardware components.

All hardware components are displayed as tiles. You can configure the display as well as the content of the tiles:

Make the settings for hardware details and tiles under "Properties > Properties > General > Matrix view".


... PC-System_1 [SIMATIC PC station] ▸ HMI_RT_1 [WinCC Unified PC RT
Diagnoseübersicht
75
Systemdiagnose-Anzeige_1 [System diagnost...
Properties
Properties
Events
Texts
Expressions

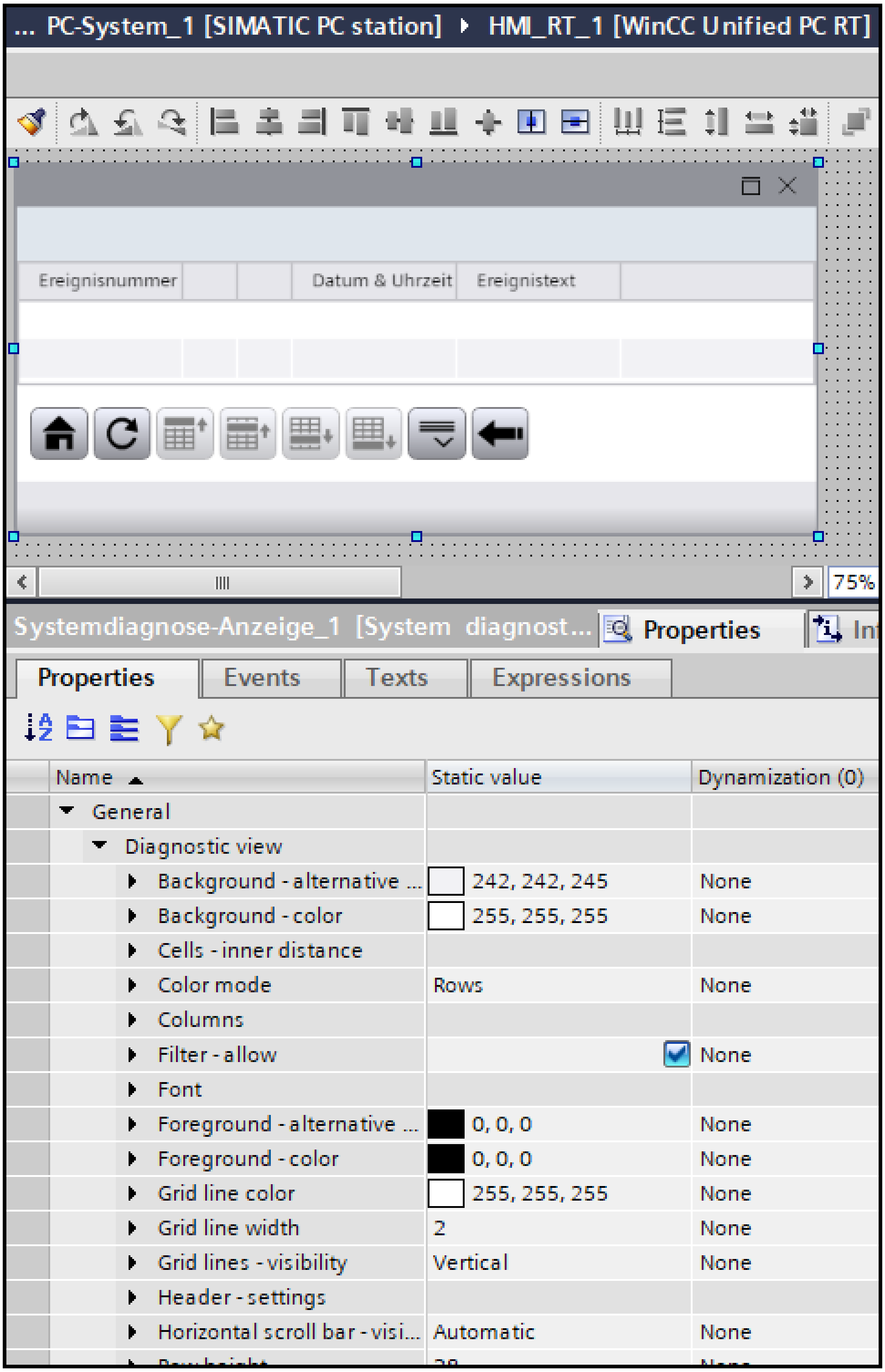
Name	Static value	Dynamization (0)
▸ Diagnostics overview path tex	Diagnoseübersicht	None
▾ Matrix view		
▸ Hardware detail view		
▸ Hardware details		None
▸ Tile - border width	2	None
▸ Tile - maximum height	114	None
▸ Tile - maximum width	280	None
▸ Tile - minimum height	114	None
▸ Tile - minimum width	200	None

Diagnostic view

The diagnostic view shows the diagnostic buffer of the PLC with the diagnostic events of the currently selected PLC.

It is not possible to switch between different PLCs in Runtime. Navigating to the diagnostic view via the selected PLC in the matrix view is recommended.

Under "Properties > Properties > General > Diagnostic view", you make the settings for the rows, header, grid lines, scroll bar, cells and columns.


... PC-System_1 [SIMATIC PC station] ▸ HMI_RT_1 [WinCC Unified PC RT]
Ereignisnummer
Datum & Uhrzeit
Ereignistext
75%
Systemdiagnose-Anzeige_1 [System diagnost...
Properties
In
Properties
Events
Texts
Expressions

Name	Static value	Dynamization (0)
General		
Diagnostic view		
Background - alternative ...	□ 242, 242, 245	None
Background - color	□ 255, 255, 255	None
Cells - inner distance		
Color mode	Rows	None
Columns		
Filter - allow	☑	None
Font		
Foreground - alternative ...	■ 0, 0, 0	None
Foreground - color	■ 0, 0, 0	None
Grid line color	□ 255, 255, 255	None
Grid line width	2	None
Grid lines - visibility	Vertical	None
Header - settings		
Horizontal scroll bar - visi...	Automatic	None
Row height	30	None

Distributed I/O view

The distributed I/O view shows the distributed devices of the Profinet IO system.

The requirement is that only one PLC is configured with a Profinet IO system. Otherwise, Runtime changes back to the matrix view.

Using the "Start page" button, you can switch from the distributed I/O view to the diagnostic overview. From the distributed I/O view, you can also jump to the diagnostic buffer.

If the Profinet IO system is not accessible, the diagnostic overview is displayed.

If you change the device version from 18.00.01.01 to 18.00.01.00, the matrix view is displayed and the distributed I/O view is not visible in the selection field.

Setting up column sorting

To set up the column sorting in the diagnostic view, follow these steps:

1. In the Inspector window, click "Properties > Properties > General > Diagnostic view > Columns > [0] Column".
2. Select the sorting direction and sorting order for the individual columns.

Dynamization of graphic properties with tags or scripts

You can dynamize the following properties containing a graphic with a tag or with a script:

- Graphic
- Icon

Access protection in Runtime

Configure access protection with the property "Operator control - allow" in the Inspector window under "Properties > Properties > Security". A logged-in user having the required authorization can acknowledge and edit the system diagnostics control using the buttons in the system diagnostics control.

Configuring the information bar

The information bar of the system diagnostics control shows the connection status and path.

The connection status is not displayed while the PLC is starting.

To configure the information bar, follow these steps:

1. Configure the general properties of the information bar, such as the font and background color, under "Properties > Properties > Miscellaneous > Information bar".
2. Configure the display of the information bar elements under "Properties > Properties > Miscellaneous > Information bar > Elements".

Toolbar

You can define the buttons of the system diagnostics control in Runtime and their operator authorizations in the Inspector window under "Properties > Properties > Miscellaneous > Toolbar > Elements". Some buttons are enabled by default. To display additional buttons in the object, activate the "Visibility" property in the settings of the corresponding button.

The following buttons are available for the system diagnostics control:

Button		Function
⌂	Home	Shows the home page.
↻	Reload	Updates the view of the diagnostic event.
▦↑	First line	Selects the first of the pending diagnostic events. The visible area of the view is moved.
▦↑	Previous line	Selects the previous diagnostic event, starting from the currently selected diagnostic event. The visible area of the view is moved.
▦↓	Next line	Selects the next diagnostic event, starting from the currently selected diagnostic event. The visible area of the view is moved.
▦↓	Last line	Selects the last of the pending diagnostic events. The visible area of the view is moved.
≡	Share view	Enables/disables the detail view.
←	Previous	Navigates to the previous PLC.
✉	Show diagnostic buffer	Changes from the matrix view to the diagnostic view. The diagnostic view shows the diagnostics buffer of the PLC. This button is only enabled if a PLC or one of its lower-level modules is shown in the matrix view.

Setting the time zone

Under Properties > Properties > Miscellaneous > Time zone, you set the desired time zone by entering a decimal value for the time zone.

- "0" and positive numerical values: The values correspond to the index values of the Microsoft time zones.
- "-1": The local time zone of the device.

Note

In Runtime, you also have the option of setting the time zone via a selection list.

3.4.8 Plant overview

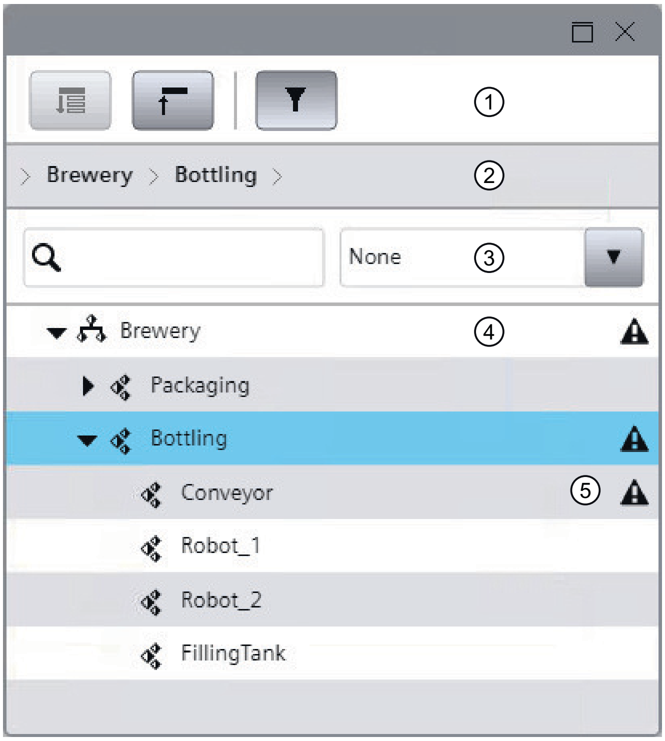
Introduction

The "Plant overview" object shows you the configured plant hierarchy in Runtime. In the plant overview, you can navigate through the system to the plant objects and see the plant at a glance.

With the corresponding configuration of the lower-level plant objects and the assigned HMI device during the engineering, the plant overview also offers you the following options:

- Obtaining an overview of the plant objects for which alarms are available
- Displaying the alarms of a plant object
- Display of configured screens of a plant object.

Overview of the Plant overview



1	Toolbar
2	Menu bar
3	Filter bar
4	Plant tree
5	Alarm icon Alarms are available for the plant object or one of its lower-level plant objects.

The following buttons are available in the toolbar and in the filter bar:

Icon	Name	Function
≣	Expand all	Expands all lower-level plant objects of the plant object selected in the control.
↑	Collapse all	Recursively collapses all lower-level plant objects of the selected plant object.
▼	Expand or collapse the filter bar	Opens or closes the filter bar.
None ▼		Filters the plant overview: • No filter: You see all plant objects • For plant objects for which alarms are available • According to plant objects for which screen windows are configured
🔍	Search field	Filters according to the entered text.

When configuring in the engineering system, you can hide the toolbar and menu bar.

Requirement

- The plant view has been created and assigned to an HMI device.
- The "Plant overview" object is configured in the screen of the assigned HMI device.
- Optional:
  - The "Dynamic" navigation type is configured in the engineering system for the plant overview.
  - A root node is configured in the engineering system for the plant overview.
- Runtime is active.

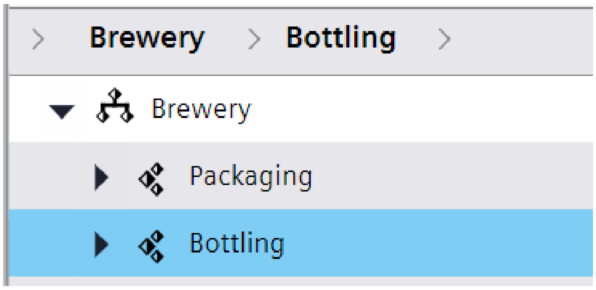
Operation

Expand and collapse plant tree

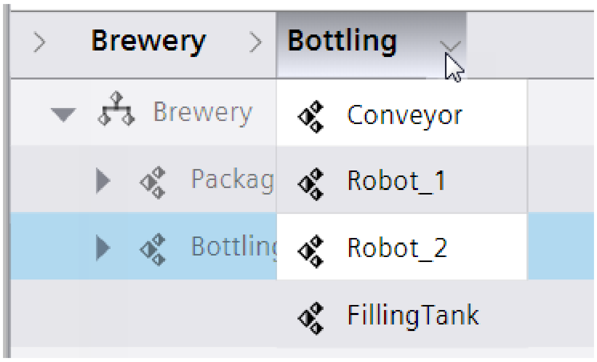
- To show all lower-level plant objects of a plant object, click the "Expand all" button.
  To collapse the plant tree, click "Collapse all".
- To expand only the lower-level objects of the next level, click the button with the triangle next to the plant object.
  To collapse the level again, click again on the button with the triangle.
  Alternatively, you can double-click the plant object to expand or collapse lower-level objects.

Select plant objects

- To select a plant object, click on the plant object in the plant tree.
  The path to the selected plant object appears in the menu bar of the "Plant overview" object:



- To see which lower-level objects a plant object displayed in the menu bar has at the next level, click the arrow in the menu bar next to the plant object.



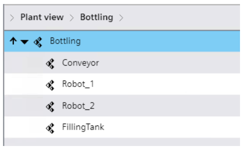
- To go from the menu bar to the overview, click on one of the plant objects shown in the menu bar.

Dynamic navigation

If dynamic navigation is enabled in the engineering system, specify the level from which the plant tree is displayed.

The buttons of the toolbar and the filter bar relate to the displayed area.

- To select a plant object, click on the object in the menu bar or double-click on the object in the plant tree.
  The levels below the selected plant object are available.
- To navigate up one level, click on the up arrow next to the plant object.



Root node

You have the option of defining a root node in the engineering system.

If a root node is configured, the root node and all objects below the root node are available in the plant overview.

See also

Display alarms for plant objects (Page 110)

3.4.9 Plant overview with companion controls

Requirement

- The plant view has been created and assigned to a device.
- The "Plant overview" object is configured in the screen of the assigned device.
- The objects "Alarm control" and "Screen window" are configured in the screen of the assigned device and configured as companion controls of the plant overview.
- Screens are configured at the plant objects.
- Runtime is active.

Display alarms

To display the alarms of a plant object, click on the alarm icon.

The alarm control shows the alarms of the plant object.

Note

The alarm icon only appears when an alarm has occurred at the respective plant object or one of its lower-level objects. The alarm icon disappears again when the alarm is no longer present.

Show a screen of a plant object

To show the screen of a plant object, click on the plant object.

The screen window shows the screen of the assigned HMI device.

If you have not configured any screen window, a screen of the plant object with text box "$POName$" appears.

Note

"$POName$" is an expression with which the name of the plant object is resolved.

3.4.10 Parameter set control

3.4.10.1 Overview of parameter set control

Introduction

Set up the machine for production in Runtime using parameter sets. The elements in a parameter set are defined in engineering by defining its parameter set type.

In Runtime, the parameter sets are displayed in the parameter set control. In the control, you manage the parameter sets and load a parameter set into the PLC to set up a machine for production.

Example

A bakery generates the following parameter set types in the engineering system:

- Bread
- Bread rolls
- Cake

The elements of the parameter set types define the ingredients of these products. For example, the parameter set type "Bread" has the following elements:

- Flour
- Salt
- Syrup
- Yeast
- Water

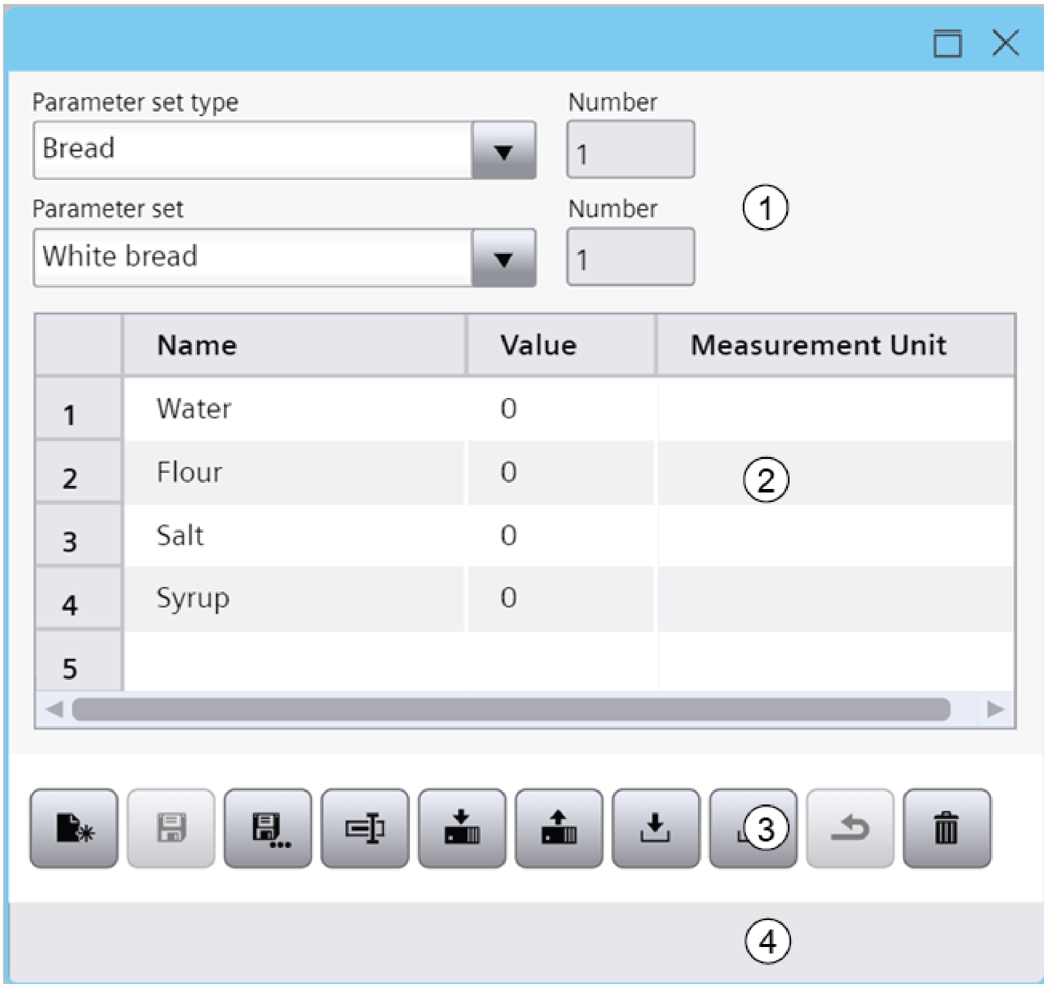
In Runtime, the bakery creates parameter sets for the "bread" parameter set type for the bread types to be produced:

- White bread
- Wholewheat bread
- French bread

The quantities required for this type of bread are entered in the elements.

During production, an operator selects the parameter set to be produced next and writes it to the PLC.

User interface



Parameter set type: Bread

Number: 1

Parameter set: White bread

Number: 1

	Name	Value	Measurement Unit
1	Water	0	
2	Flour	0	
3	Salt	0	
4	Syrup	0	
5			

① Area for selecting the parameter set types and parameter sets

② Parameter table

Displays the values of the selected parameter set or parameter set type. The columns in the table depend on the configuration in engineering.

③ Toolbar

④ Information bar

The elements in the information bar depend on the configuration in engineering.

Note

Fixed parameter set type

The parameter set control in the engineering system can be configured so that you are only offered the parameter sets of a certain parameter set type and cannot select any other parameter set types.

Parameter set control buttons

The toolbar contains buttons for executing specific functions. Depending on the configuration, the following buttons are available for operator input:

	Button	Function
🗋	Create	Creates a new parameter set.
💾	Save	Saves a parameter set.
💾...	Save as	Opens the selection dialog for the storage path of the selected parameter set.
▭I	Rename	Renames the selected parameter set. The new name must be unique.
⬇	Write to PLC	Save the parameter set and writes it to the PLC.
⬆	Read from PLC	Reads a Parameter set type or parameter set from the PLC.
⤓	Import	Imports parameter sets to a TSV file.
⤒	Export	Exports parameter sets to a TSV file.
↩	Cancel	Cancels the process.
🗑	Delete	Deletes the selected parameter set. The table shows the default values at the parameter set type.

Rearranging columns

You can change the column arrangement configured in the engineering here. See section Rearranging columns at runtime (Page 284).

3.4.10.2 Operate parameter set control

Create parameter sets

Requirements

- Parameter set types were configured in the engineering system.
- The parameter set control is configured in the screen of the device that is active in Runtime.

Create a new parameter set

To create a new parameter set, follow these steps:

1. Select a parameter set type in the parameter set control in "Parameter set type".
   The parameter table loads the columns and default values predefined at the parameter set type.
2. Click the "Create" button.

   Note

   Cancel creation

   Another parameter set parameters set type cannot be selected until you have saved the new parameter set or clicked on "Cancel".

3. Optional: Enter the name of the new parameter set in "Parameter set name".
   The name must be unique for the parameter set type.
4. Optional: Enter the ID of the parameters set in "Number".
   The number must be unique for the parameter set type.
5. The find the values of the parameters set by clicking in a table cell and modifying the value predefined by the parameter set type.
6. Confirm.

The parameter set is created and saved.

Create a version of the existing parameter set

To create a new parameter set based on an existing parameter set, follow these steps:

1. Select a parameter set type in the parameter set control in "Parameter set type".
2. Select a parameter set in "Parameter set".
   The parameter set table loads the columns and values defined for the parameter set.
3. Click the "Save as" button.
   The "Save parameter set as" dialog opens.
4. Optional:
   - Overwrite the automatically generated name in "Parameter set name".
     The name must be unique.
   - Overwrite the ID in "Number".

5. Confirm.
   The new parameter set is created.
6. To change the values taken over from the original parameter set, click in a table cell and enter a new value.
7. Click the "Save" button.

The parameter set is created and saved.

Managing parameter sets

Introduction

You manage parameter sets for different productions in a parameter set control in runtime. You have the following options for managing parameter sets:

- Create new parameter sets
- Copy parameter sets
- Change parameter sets
- Delete parameter sets
- Rename parameter sets

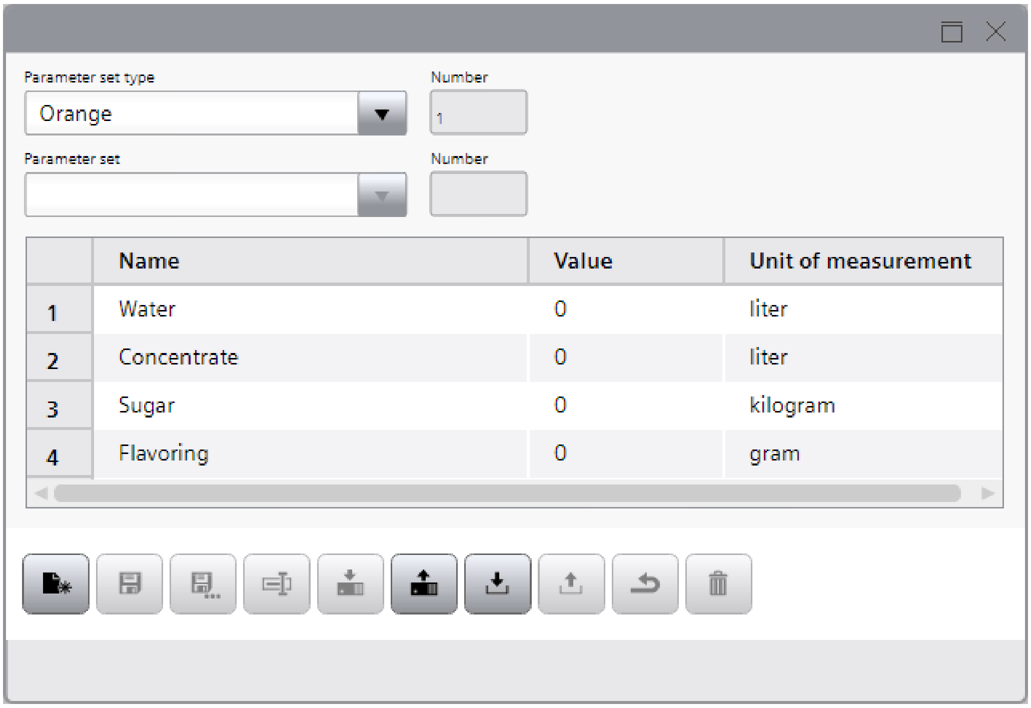
Requirement

- At least one parameter set type with elements has been created.
- A parameter set control has been configured.
- The project is in runtime.

Creating a new parameter set

To create a new parameter set, proceed as follows:

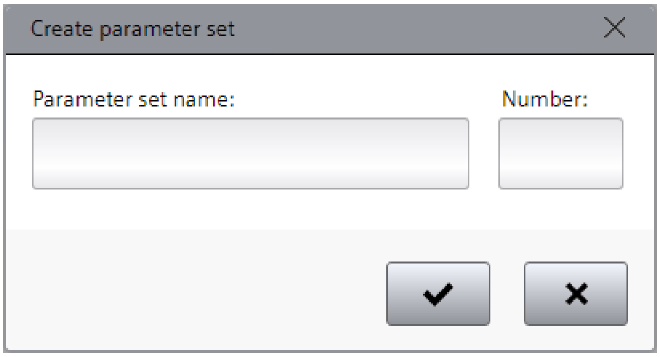
1. In the "Parameter set type" field, select the parameter set type for which you want to create a new parameter set.
   The elements of the selected parameter set type are displayed in the table.



Parameter set type: Orange
Number: 1
Parameter set:
Number:

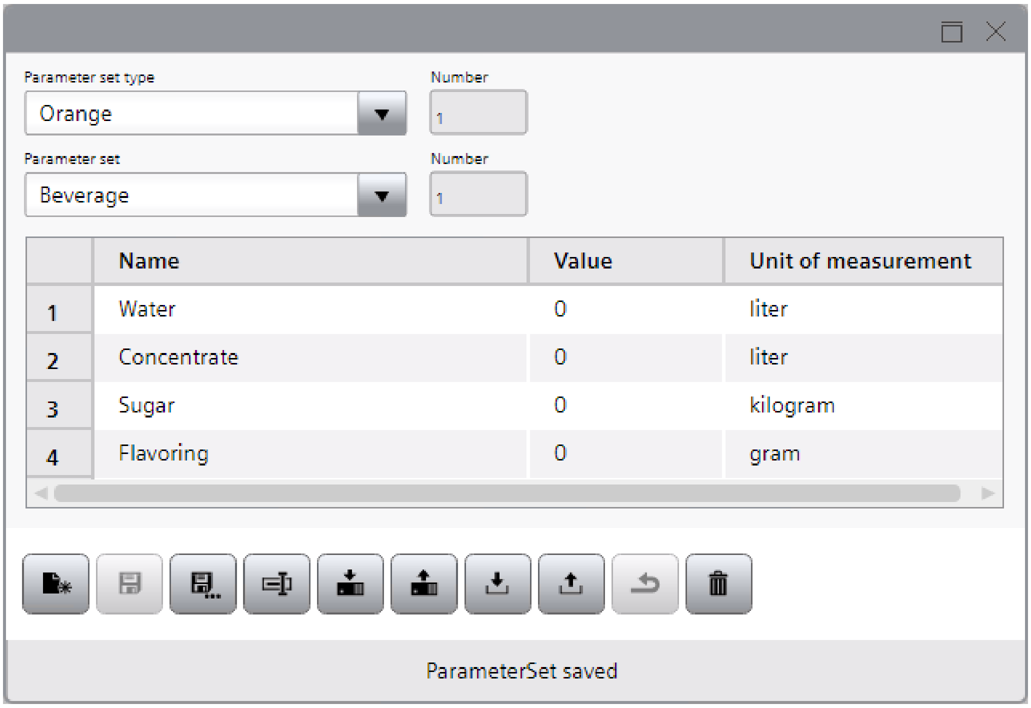
	Name	Value	Unit of measurement
1	Water	0	liter
2	Concentrate	0	liter
3	Sugar	0	kilogram
4	Flavoring	0	gram

2. Click the "Create" button.
   The "Create parameter set" dialog opens.



3. Enter a unique parameter set name under "Parameter set name".
4. Enter a unique parameter set ID under "Number".

5. Confirm the dialog.
   A new parameter set has been created and saved. The parameters of the new parameter set are displayed in the table. The parameters have the same values in the columns "Name" and "Unit of measurement" as the elements of the previously selected parameter set type. The defined start values are applied for the "Value" column. If you have not defined start values, the corresponding default values are used.



Parameter set type: Orange
Number: 1
Parameter set: Beverage
Number: 1

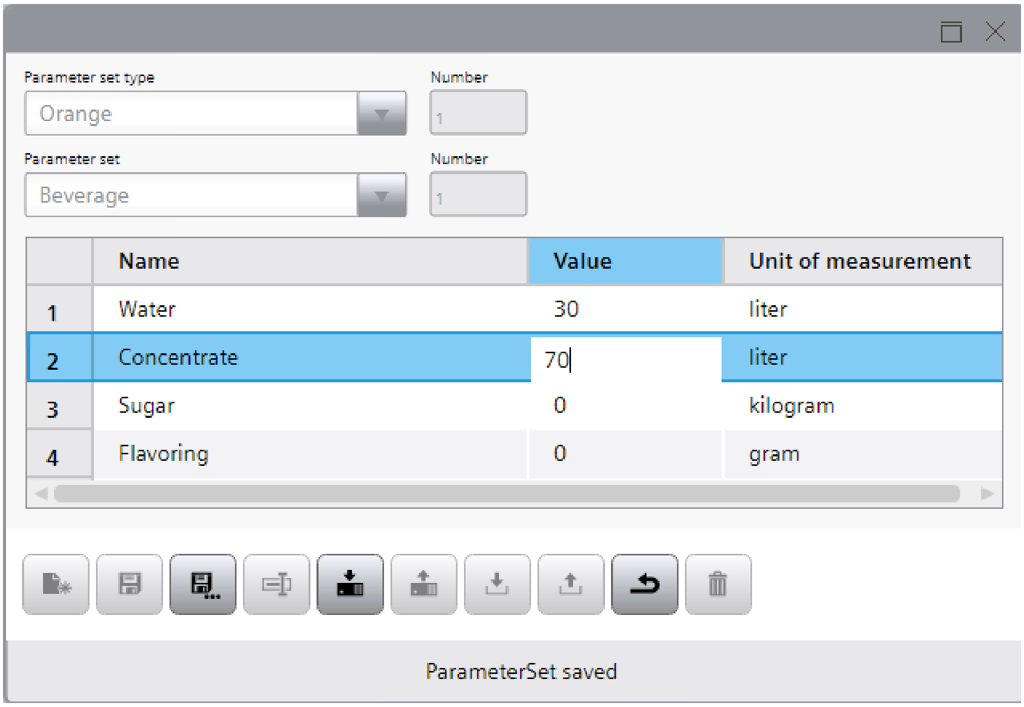
	Name	Value	Unit of measurement
1	Water	0	liter
2	Concentrate	0	liter
3	Sugar	0	kilogram
4	Flavoring	0	gram

ParameterSet saved

Note

If you do not make any entries in the "Create parameter set" dialog and confirm the dialog, a new parameter set is also created and saved. In this case the new parameter set, however, has a unique parameter set name and a unique parameter set ID which were both automatically assigned by the system.

6. Enter values for the parameters in the "Value" column.
   Depending on the configuration, the parameters already contain start values.



Parameter set type: Orange — Number: 1

Parameter set: Beverage — Number: 1

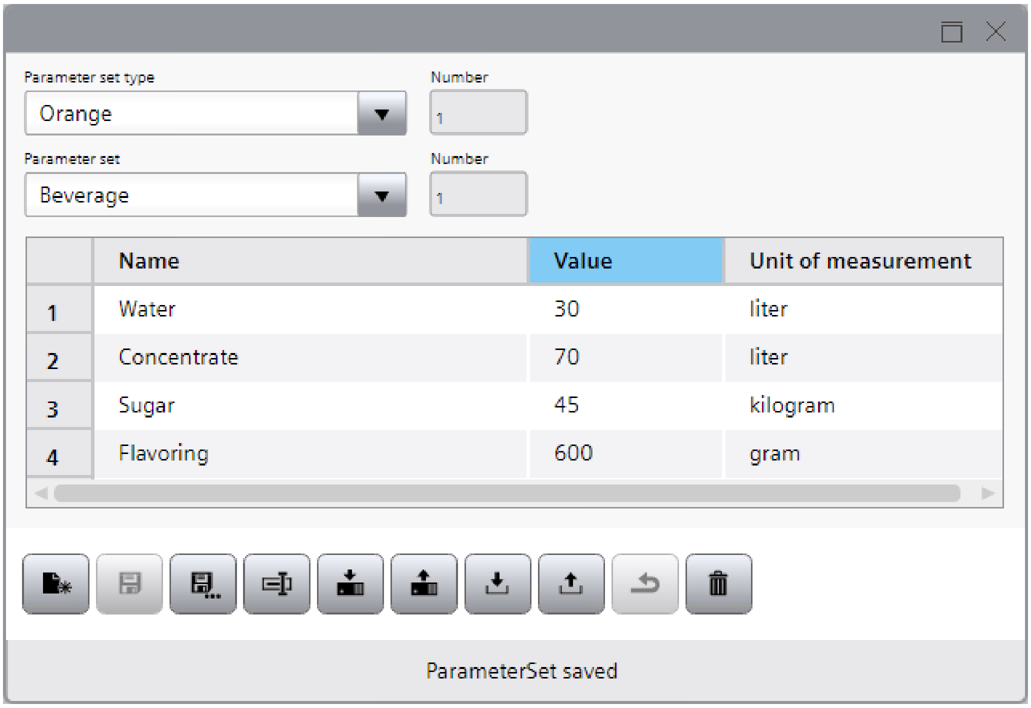
	Name	Value	Unit of measurement
1	Water	30	liter
2	Concentrate	70	liter
3	Sugar	0	kilogram
4	Flavoring	0	gram

ParameterSet saved

Note

The character ' is not permitted in the value of a parameter set.

7. Click the "Save" button.



Parameter set type: Orange

Number: 1

Parameter set: Beverage

Number: 1

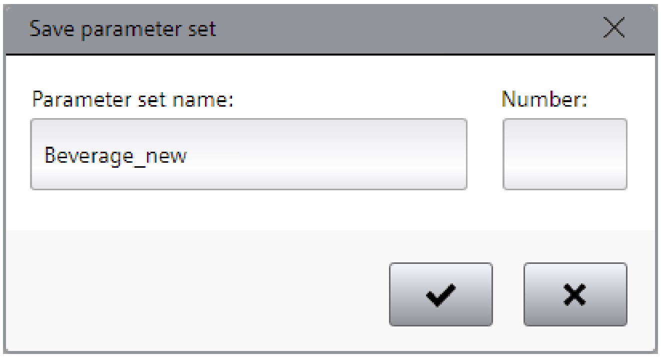
	Name	Value	Unit of measurement
1	Water	30	liter
2	Concentrate	70	liter
3	Sugar	45	kilogram
4	Flavoring	600	gram

ParameterSet saved

Copying a parameter set

To copy a parameter set, proceed as follows:

1. In the "Parameter set type" field, select the parameter set type in which you want to copy an existing parameter set.
   The elements of the selected parameter set type are displayed in the table.
2. In the "Parameter set" field, select the parameter set you want to copy.
   The parameters of the selected parameter set are displayed in the table.
3. Click the "Save as" button.
   The "Save parameter set" dialog opens. A unique parameter set name is pre-assigned to the "Parameter set name" field.



Save parameter set

Parameter set name: Beverage_new

Number:

4. Enter a different unique parameter set name under "Parameter set name" as required.

5. Enter a unique parameter set ID under "Number" as required.
6. Confirm the dialog.

Note

If you do not enter a parameter set ID under "Number" in the "Save parameter set" dialog and confirm the dialog, a unique parameter set ID is automatically assigned to the new parameter set.

Changing the parameter set

To change a parameter set, proceed as follows:

1. In the "Parameter set type" field, select the parameter set type in which you want to change an existing parameter set.
   The elements of the selected parameter set type are displayed in the table.
2. In the "Parameter set" field, select the parameter set you want to change.
   The parameters of the selected parameter set are displayed in the table.
3. Edit the values of the parameters in the "Value" column.
4. Click the "Save" button.

Deleting a parameter set

To delete a parameter set, proceed as follows:

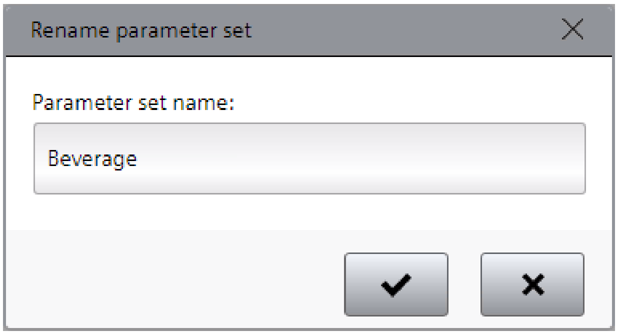
1. In the "Parameter set type" field select the parameter set type in which you want to delete an existing parameter set.
   The elements of the selected parameter set type are displayed in the table.
2. In the "Parameter set" field, select the parameter set you want to delete.
   The parameters of the selected parameter set are displayed in the table.
3. Click "Delete".

Renaming a parameter set

To rename a parameter set, proceed as follows:

1. In the "Parameter set type" field, select the parameter set type in which you want to rename an existing parameter set.
   The elements of the selected parameter set type are displayed in the table.
2. In the "Parameter set" field, select the parameter set you want to rename.
   The parameters of the selected parameter set are displayed in the table.

3. Click the "Rename" button.
   The "Rename parameter set" dialog opens.



4. Enter a different unique name for the parameter set under "Parameter set name".
5. Confirm the dialog.

Exporting and importing parameter sets

Introduction

In a parameter set control in runtime you export parameter sets from the parameter set memory to a "*.tsv" file to be able to edit them a text editor. In a parameter set control in runtime you furthermore import parameter sets from a "*.tsv" file into the parameter set memory. A "*.tsv" file is a text file that uses the tabulator as a list separator.

Note

To export and import the parameter sets, you can also use the system functions in the function list or in the scripts:

- With the system function "ExportParameterSets" or "ExportParameterSets", the parameter sets are exported from the parameter set memory to a "*.tsv" file.
- With the system function "ImportParameterSets" or "ImportParameterSets", the parameter records are imported from a "*.tsv" file into the parameter set memory.

If the parameter `OutputStatus` is set to `True`, a status message is output in an alarm control configured in the screen.

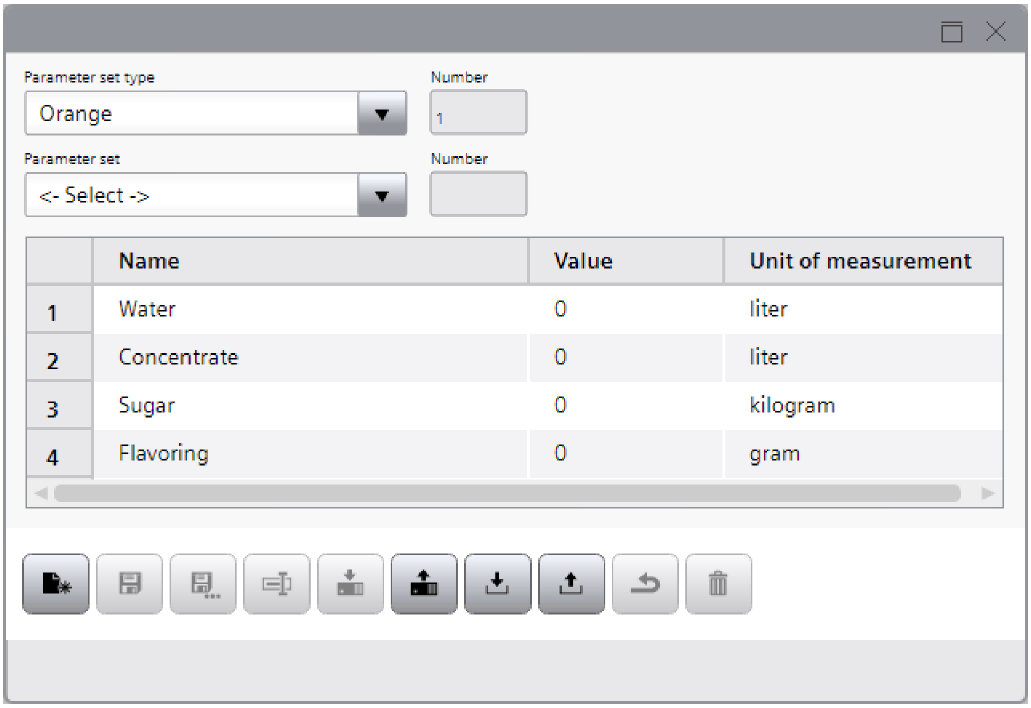
Requirement

- At least one parameter set type with elements has been created.
- A parameter set control has been configured.
- The project is in runtime.

Exporting parameter sets of a parameter set type

Follow these steps to export the parameter sets of a parameter set type:

1. In the "Parameter set type" field, select the parameter set type whose parameter sets you want to export.

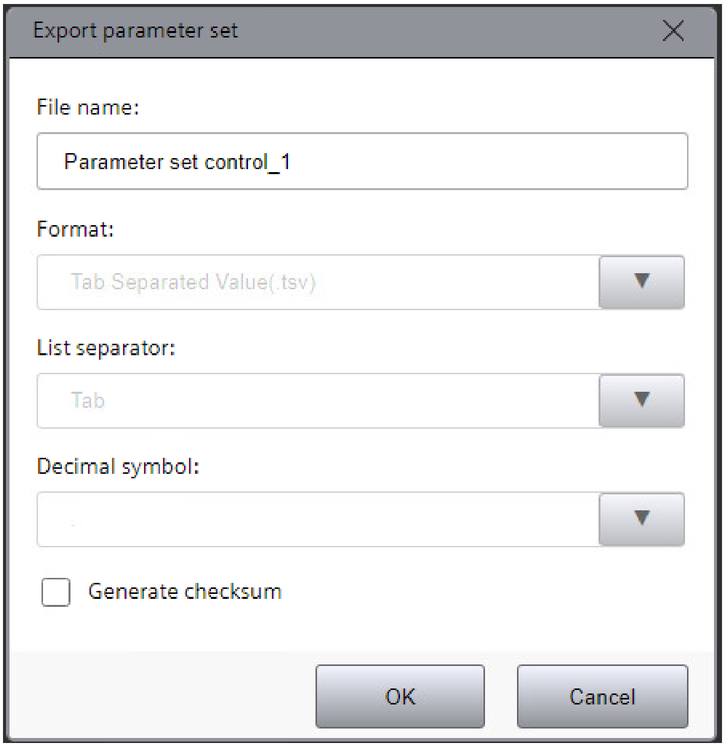


Parameter set type: Orange — Number: 1

Parameter set: <- Select -> — Number:

	Name	Value	Unit of measurement
1	Water	0	liter
2	Concentrate	0	liter
3	Sugar	0	kilogram
4	Flavoring	0	gram

2. Click the "Export" button.
   The "Export parameter set" dialog box opens. The name of the parameter set control is pre-assigned in the "File name" field.



Export parameter set

File name: Parameter set control_1

Format: Tab Separated Value(.tsv)

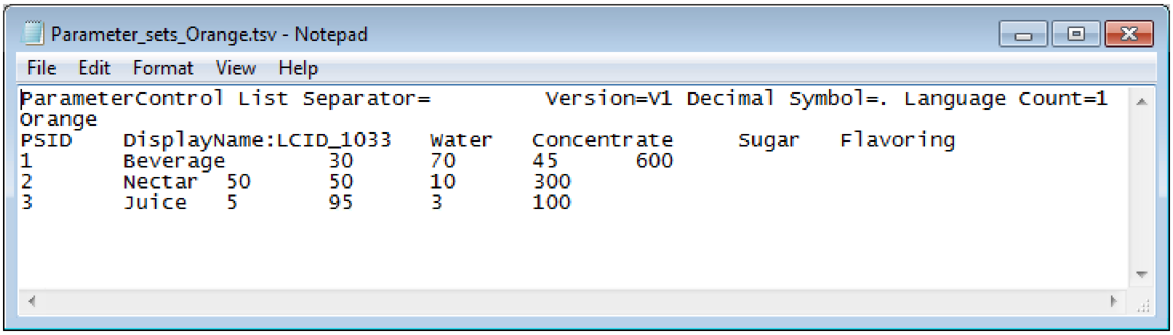
List separator: Tab

Decimal symbol: .

□ Generate checksum

3. If appropriate, change the name of the file to which you want to export the parameter sets under "File name".

4. Enable "Generate checksum" to export the parameter data set with a checksum.
   Parameter data sets with a checksum cannot be imported if they have been manipulated in the meantime.
5. Confirm the dialog.
   The parameter sets are exported to a ".tsv" file.
   This file is stored according to the download settings.
   The file has the following structure:
   - The first line contains the file header. The file header consists of identifier, delimiter, version of the exported file, decimal symbol and information on the number of languages in which the name of the parameter sets is stored.
     The line must not be changed. Otherwise, it is not possible to import parameter sets.
   - The second line contains the name of the parameter set type.
   - The third row contains the headers for parameter sets. LCID of the language and the names of the parameter set type items are listed.
     The header for parameter sets must not be changed.
   - From the fourth line on the parameter sets are listed.


Parameter_sets_Orange.tsv - Notepad
File Edit Format View Help

```
ParameterControl List Separator=         Version=V1 Decimal Symbol=. Language Count=1
Orange
PSID    DisplayName:LCID_1033   Water   Concentrate     Sugar   Flavoring
1       Beverage        30      70      45      600
2       Nectar  50      50      10      300
3       Juice   5       95      3       100
```

Edit exported file

1. You can customize the file to meet your needs:
   - Change the values of existing parameters.
   - Add parameter sets.

   To be able to import the parameter sets after editing, note the following information:

   Note
   - The parameters must be valid for the defined data type.
   - The parameters must be within the limits defined in the parameter set type item.
   - ID and name of the individual parameter sets must be unique.
2. Save the changes.

Importing parameter sets into a parameter set type

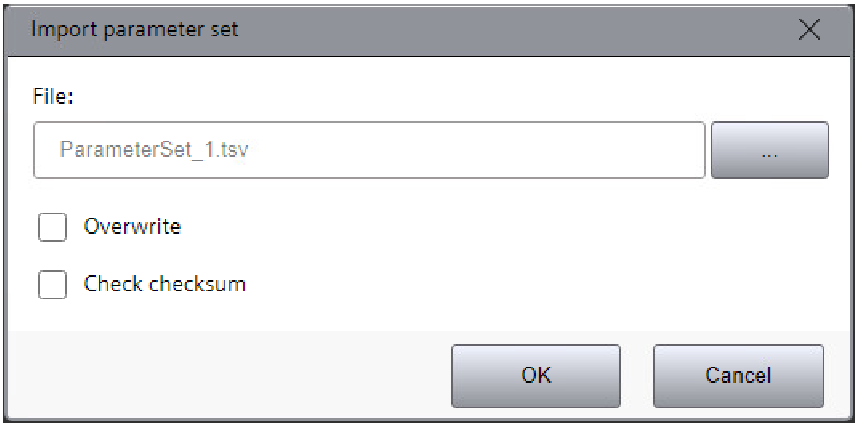
To be able to import parameter sets, note the following requirements:

Note

- The import file must have the same file header and the same header for parameter sets as the export file. Otherwise, it is not possible to import parameter sets.
- There is no parameter set with the same display name in any of the configured languages.
- The numerical values in the import file are within the permitted value range of the corresponding configured data type.

To import parameter sets into a parameter set type, follow these steps:

1. In the "Parameter set type" field, select the parameter set type into which you want to import the parameter sets.
2. Click the ⭳ "Import" button.
   The "Import parameter set" dialog box opens.



Import parameter set

File: ParameterSet_1.tsv

3. Select the file from which you want to import the parameter sets.
4. To overwrite parameter sets in the parameter set control that have the same ID as the imported parameter sets, activate the "Overwrite" option.

   Note

   If you deactivate overwriting and if a parameter set with the same ID or the same parameter set name exists in the parameter set control, the import of parameter sets is not possible.

   Any added parameter sets whose IDs and parameter set names deviate from the existing parameter sets are imported regardless of the "Overwrite" option.
5. Enable "Check checksum" when importing a parameter data set exported with the "Generate checksum" option.
6. Confirm the dialog.
   The parameter sets are imported to the parameter set type.

Transferring parameter sets

Introduction

You have assigned an external HMI tag of the data type HMI or PLC user data type to a parameter set type. In a parameter set control in runtime you transfer the values of parameter sets to the PLC via the HMI tag. The parameter set values are used to set up machines for different productions.

In a parameter set control in runtime you furthermore read active parameter sets from the PLC into the parameter set control via the HMI tag. The read parameter set values are stored in the parameter set memory. By reading from the PLC, you call up currently used values from production machines for later use.

Note

You can also use system functions in the function list or in scripts to transfer parameter sets between HMI device and PLC:

- With the system function "ReadAndSaveParameterSet" or "ReadAndSaveParameterSet", a parameter set is read from the PLC and saved in the parameter set memory.
- With the system function "LoadAndWriteParameterSet" or "LoadAndWriteParameterSet", a parameter set is loaded from the parameter set memory and written to the PLC.

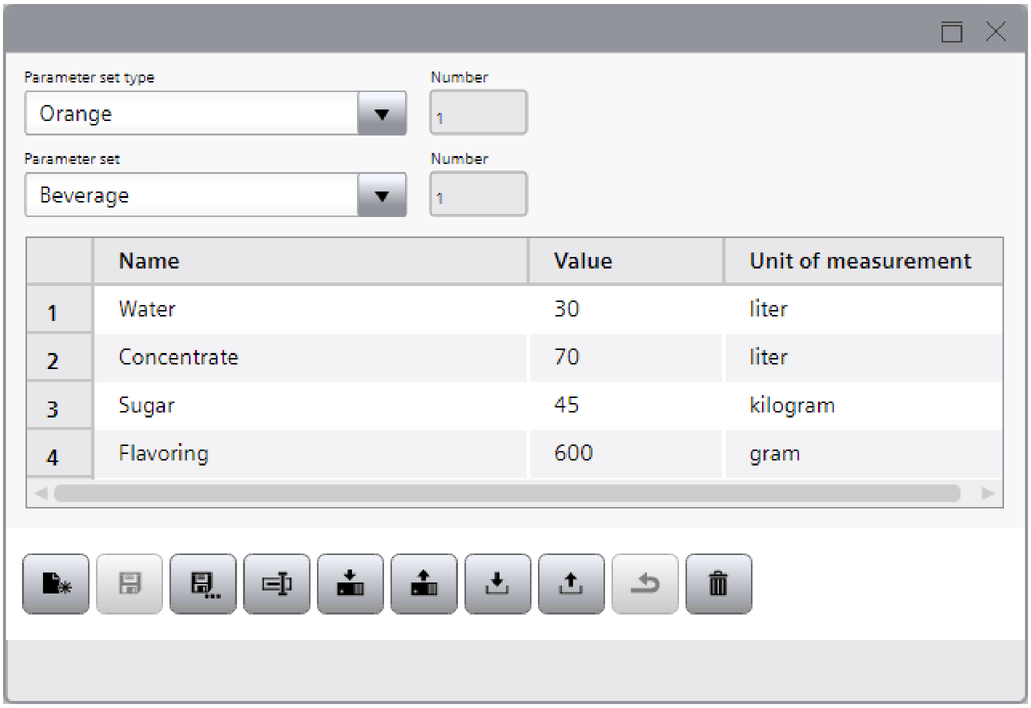
Requirement

- A parameter set type with elements has been created.
- An external HMI tag of the data type HMI or PLC user data type is assigned to the parameter set type.
- A parameter set control has been configured.
- The project is in runtime.
- At least one parameter set has been created in the parameter set type.

Transferring a parameter set to the PLC

To transfer a parameter set to the PLC, follow these steps:

1. In the "Parameter set type" field, select the parameter set type.
2. In the "Parameter set" field, select the parameter set whose values you want to transfer to the PLC.



Parameter set type: Orange
Number: 1
Parameter set: Beverage
Number: 1

	Name	Value	Unit of measurement
1	Water	30	liter
2	Concentrate	70	liter
3	Sugar	45	kilogram
4	Flavoring	600	gram

3. Click the "Write to PLC" button.

Reading a parameter set from PLC

To read a parameter set from the PLC, follow these steps:

1. In the "Parameter set type" field, select the parameter set type.
2. In the "Parameter set" field, select the parameter set whose values you want to read from the PLC.

   Note

   If do you not select a parameter set in the in the "Parameter set" field, a new parameter set is created in the parameter set control while reading from the PLC.

3. Click the "Read from PLC" button.

Note

A parameter set cannot be read from the PLC if minimum and/or maximum values are defined for a parameter set type item and the value in the parameter set to be transferred is outside this range. An alarm is triggered.

Result

- You have transferred the values of parameter sets between the HMI device and PLC.
- If parameter set data was not saved in Runtime, this data is saved by writing to the PLC in Runtime.

Updating the UDTs

Parameter set types are linked to UDTs. If the UDT of a parameter set type is replaced or edited in the engineering system, the derived parameter sets are updated accordingly in Runtime after the next compilation and loading:

- Replacement of the UDT
  The parameter sets created in Runtime are retained. They adopt the elements and default values of the new UDT.
- Assignment of another UDT version
  The parameter sets created in Runtime are retained. New elements are assigned default values, deleted elements are removed.

3.4.11 Reports

3.4.11.1 Basics

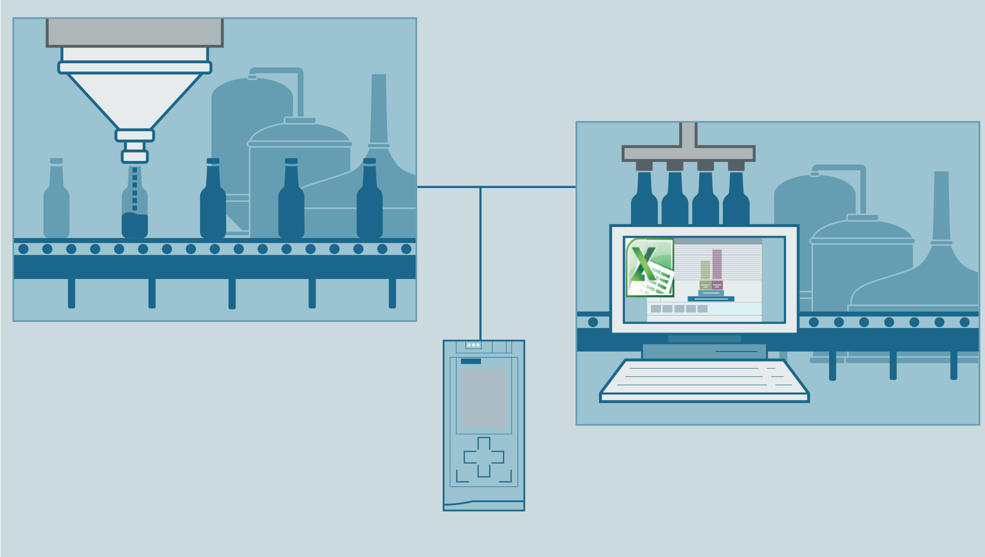
Reporting in Runtime

Introduction

You can use WinCC Unified Reporting to generate production reports in tabular form in runtime for the following project data:

- Logging tags and tags
- Logging alarms
- Contexts:
  - User-defined contexts:
    These contexts are created and executed by a program created with the ODK API.
  - System-generated contexts
    When the Performance Insight and Calendar option packages are installed, these contexts are executed by the system during Runtime.
- Audit Trail of the Runtime device
- If Plant Intelligence options are installed, you can use the WinCC Unified Local Reporting option to generate production logs for additional project data.
  You can find more information in the Help for the respective Plant Intelligence option.

The production reports can be generated as XLSX file or PDF file and sent automatically as an email to a specified group of recipients. For example, you can generate an XLSX report that outputs all alarms occurring in a production line. You then distribute or archive the report for analysis purposes.



Functional scope

In the "Reports" control in runtime, you configure report jobs that use the report templates defined in the Excel add-in. To do so, Reporting offers the following functions in Runtime:

- Maintenance of the global email settings (contact data and SMTP server configuration)
- Maintenance of job parameters, especially import and export of report templates
- Creating new report jobs and managing existing report jobs
- Overview of the generated reports
- Download or deletion of the reports

Basics of Reporting

Report templates

A *report template* is an Excel file (.xslx) that was created with the WinCC Unified Excel add-in. The report template has access to the data of the data source with which the add-in is connected.

For each report template, you define which segments are contained in the reports using the template and which data source items are evaluated by the segments.

After you have imported report templates into the "Reports" control in Runtime, you can select them for configuring report jobs.

Data sources

The *data source* is the source from which you select data source items when you configure the report template.

The following connection modes and data sources are available:

- Connection mode: Online
  The data source is the project that is running on the Runtime server to which the add-in is connected.
- Connection mode: Offline
  Data source is a configuration file. You generate the configuration file by exporting the data source items of the project to a file in the "Reports" control in Runtime. You can use this file to create additional report templates without connecting to a runtime server.

Options and data source items

Options control the types of data source items to which the report template has access.

Data source items are the specific objects whose data is read from the Runtime project during report generation.

The following options and types of data source items are available in Reporting, depending on the installed software:

Software	Option	Types of data source items
WinCC Unified basic installation	Alarms	Logging alarms Alarm statistics for logging alarms
WinCC Unified basic installation	Logging tag	Logging tags
WinCC Unified basic installation	Tag	Tags
WinCC Unified basic installation	User-defined column	User-defined texts or Excel formulas
WinCC Unified basic installation	Context	User-defined contexts[1]
WinCC Unified basic installation	Audit	Audit
Performance Insight option package	Performance Insight	Local KPIs and operands of the PI option Performance Insight: • KPIs • Logged KPIs • Operands (counters and numerical operands) • Machine states • Downtime analysis • System-generated contexts
Line Coordination option package	Line Coordination	Jobs
Calendar option package	Context	System-generated contexts

[1] Only for Unified PC

Report jobs and job parameters

A *report job* is a job for generating reports in Runtime. A new report is generated each time the report job is performed.

The *job parameters* of the report order determine the details of its execution, such as which trigger it has, which report template it uses and the format of the report.

Report jobs are executed automatically when their trigger event occurs or manually by the user.

Reports

A *report* (production report) is an XLSX file or PDF file that is generated when a report job is executed in Runtime. The data source items from the Runtime project defined in the report template are read during generation, and their data are imported into a table in the report.

Using general Excel functions

In addition to the specific add-in functions, you also have access to the standard Excel functions in a report template. These include:

- Layout functions
- Functions for graphical preparation or analysis of the data imported from Runtime, such as charts, pivot tables and formulas

See also Tips on design and layout (Page 282).

Version compatibility

Introduction

When loading a Runtime project for which the "Reports" control has been configured, the general rules for version compatibility of WinCC Unified apply.

The rules described here also apply for the interaction between add-in, data source, report template and runtime version of the project in which reports are generated.

Compatibility between add-in and data source

The add-in can use the following data sources:

Add-in	Online data source	Offline data source
V16	Runtime project V16	Configuration file generated with a Runtime project V16
V17	Runtime project V16 or V17	Configuration file generated with a Runtime project V16 or V17

Compatibility between add-in and report template

The following report templates can be opened and edited in the add-in:

Add-in	Report template
V16	Created with a V16 add-in
V17	• Created with a V17 add-in • Created with a V16 add-in If the add-in is connected to a V17 data source when you open the report template, you will be prompted to migrate the report template to V17. If the add-in is connected to a V16 data source when the report template is opened, no migration is necessary.

Note

Migration of report templates

The migration of the report template is not reversible. A report template migrated from V16 to V17 can no longer be opened in a V16 add-in.

If migration is not desired, connect the add-in to a V16 data source before opening the report template.

Note

Scope of functions of report templates

The functions available in the configuration of the report template in the add-in depend on the version of the data source used by the add-in.

Compatibility between report template and runtime project

In a runtime project, reports can be generated using the following report templates:

Report template	Version of the runtime project
V16	V16 and V17
V17	V17

3.4.11.2 Requirements and restrictions

The following requirements and restrictions apply to configuring report jobs and generating reports on Unified PCs, both in runtime and during simulation.

Enable Reporting

The reporting functionality must be enabled for the Runtime project that is running or being simulated on the HMI device.

You activate the reporting functionality of a Runtime project before loading it into the device in TIA Portal: "Runtime settings" of the HMI device > "Reporting" > "Enable Reporting" option

Note

Devices with a device version lower than V18

Reporting is always enabled for HMI devices with a device version lower than V18.

3.4.11.3 Workflow for working with reports in Runtime

Introduction

The following workflow describes which works are required in the "Reports" control so that production reports are generated in Runtime.

The reports can be stored as file in the file system and sent as an attachment to an e-mail. Alternatively, an e-mail without attachment can also be sent about the generation of the report. In this way, employees from management and production are promptly informed about the production situation, regardless of their location.

You can send the e-mail using a secure SMTP server (authentication with user name and password or via certificate) or an unsecured SMTP server, for example, an internal company mail server.

Requirement

- Requirements in TIA Portal:
  - The necessary project data were configured for the HMI device for which reports are to be created.
  - The "Reports" control was placed on an HMI screen of the device.
  - The "Enable Reporting" option was enabled in the Runtime settings of the device.
  - (Optional) The storage locations for reports and the Reporting database were configured in the Runtime settings of the device.
- The HMI device has been compiled, loaded into Runtime and its Runtime project has the status "Running".
- The HMI device has access to report templates.
- Unified PC: If one of the report templates used in Runtime evaluates contexts, contexts must have been configured for the currently running Runtime project and executed in Runtime.
- For cross-project and cross-Runtime use of report templates: The data sources used in the report template can also be found on the HMI device. Make sure that the names and plant hierarchy are consistent.

Procedure

1. To send reports by e-mail, configure the global e-mail settings:
   - When one of the servers requires a certificate for sending e-mails, upload the certificate.
   - Create contacts for the e-mail receivers and e-mail senders.
   - Create the required SMTP server configurations.
2. Configure job parameters for report templates, triggers and targets.
   These job parameters will then be available to you for selection when configuring the report jobs.
3. Configure report jobs.
   Reports are generated in Runtime when the report jobs are executed.
4. (Optional) Perform report orders manually.
5. In the control, get an overview of which reports have been generated.
6. Download the reports, if necessary.
7. (Optional) To reuse the configuration of the "Reports" control, such as on a device in another network, transfer the existing configuration from the control from one device to the control of the other device.

Configuring job parameters

First, you configure which job parameters are available for selection during the configuration of the report jobs. You configure the following job parameters:

- The available report templates
  The report template defines which data the report outputs. Import and/or delete templates, if required.
- The available triggers
  The trigger defines when a report job is executed. Add triggers, edit triggers or delete them.
- The available targets
  Targets define whether reports are made available to users in the file system or via e-mails. Add targets, edit triggers, or delete them.

You set further job parameters while configuring a report job in the "Report jobs" tab.

Configuring a report job

You configure the following for each report job:

- Name of the report job
- Used report template

- Name of the reports generated by this template

Note

Texts through dynamic placeholders

Placeholders are available to you when defining the report name. The placeholders are evaluated and replaced by text during execution of the report.

See also Dynamic placeholder (Page 220).

- Targets of the generated report
  To send e-mails, select a target of the type "E-mail".
- Per target: The target format of the generated report
  Possible formats: .XLSX and .PDF
- Trigger
- Comment
- Activate

See also

Setting global email settings (Page 199)

Configuring job parameters (Page 201)

Configuring report jobs (Page 208)

Running a report job manually (Page 216)

Downloading reports (Page 216)

Transferring the control configuration (Page 218)

Configuring report templates in the add-in (Page 223)

3.4.11.4 The user interface of the "Reports" control

Note

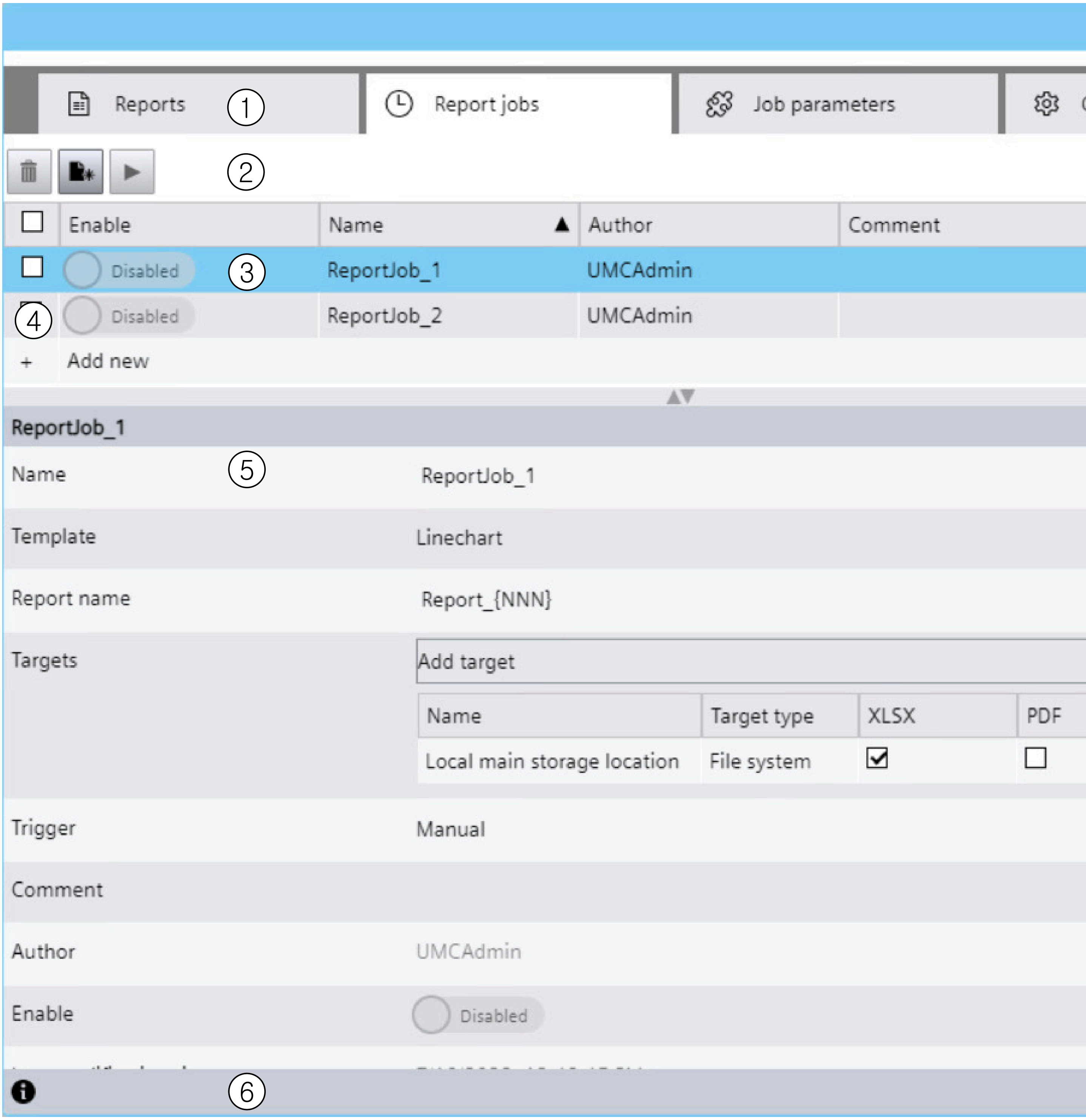
Automatic data transfer

Changes in the "Reports" control are saved automatically.

Layout

You create and manage report jobs in the "Reports" control. You also have access to the reports generated by the report jobs.

The control has the following structure:



☐	Enable	Name ▲	Author	Comment
☐	Disabled	ReportJob_1	UMCAdmin	
☐	Disabled	ReportJob_2	UMCAdmin	

ReportJob_1

Name	ReportJob_1
Template	Linechart
Report name	Report_{NNN}
Targets	Add target
Trigger	Manual
Comment	
Author	UMCAdmin
Enable	Disabled

Name	Target type	XLSX	PDF
Local main storage location	File system	☑	☐

1 Tab for the configuration and management of reports, report jobs, job parameters and global settings

2 Toolbar

The buttons you see depend on the tab.

3 Work area
On the "Reports", "Report jobs" and "Job parameters" tabs: List of elements available on the tab
On the "Global settings" tab: The settings

4 Options for selecting the elements
You can select elements individually or all at once.

5 Detail area
Shows the properties of the selected element.

6 Information bar

Tab

"Reports" tab

Here you can see which reports have been generated. You can download or delete reports via the toolbar.

The "Status" column shows Information:

- On the status of the generated report files (XLSX and PDF)
- On the status of the targets (File system and E-mail)

Overview of the status icons:

Status	Description
✓	Execution has been successfully completed.
⚠	An error occurred during execution.
◔	Execution is in progress.

A click on an icon opens a detailed status message.

"Report jobs" tab

Here you create new report jobs, manage existing report jobs or start a report job manually.

"Job parameters" tab

Here you manage the parameters with which you configure the report jobs in the "Report jobs" tab.

"Global settings" tab

Here you make the following settings:

- For sending e-mails
- For transfer of the control configuration
- For creating an offline configuration file
- For configuring paging

Toolbar

The following buttons are available in the toolbars of the tab:

Icon	Button	
🗑	Delete	Deletes the elements whose option is enabled in the work area.
🗎✱	• Add new • Import	• Creates a new element. • "Job parameters > Templates" tab: To import a report template into Runtime
▶	Run	In the "Report jobs" tab. Manually creates a report for the report job whose option is enabled in the work area.
🗎→	Export	• In the "Job parameters > Templates" tab: To export report templates • In the "Reports" tab: To download reports to the client

Information bar

The button in the information bar displays general information sent by the reporting service, for example, on whether a report job has been executed.

3.4.11.5 Setting global email settings

If configured accordingly, an e-mail is sent automatically after a report job is executed. The e-mail can include the report as an attachment.

Maintenance of the basic settings for sending e-mails is carried out in the "Global settings" tab:

- If necessary: The certificates that the e-mail sender uses to authenticate itself at the SMTP servers.
- The contact information of the e-mail senders and e-mail receivers.
- The configuration of the SMTP server via which the e-mails are sent.

Upload certificates

Store the certificates of the SMTP servers that require authentication via certificate.

Requirement

- You have access to the storage location of a valid certificate file.

Procedure

1. In the "Reports" control, click on the "Global settings > Certificates" tab.
2. Click "Add new" in the toolbar.
   Alternative: In the work area, click "Add new".
3. In the dialog that opens, select the certificate file.
4. Confirm your input.
5. Optional: Select the uploaded certificate in the work area and enter a comment on the certificate in the detail area.

Result

The certificates uploaded here are available in the "Contacts" tab.

Maintaining contacts

Store the data of the e-mail senders and email recipients.

Procedure

To create a new contact, follow these steps:

1. In the "Reports" control, click on the "Global settings > Contacts" tab.
2. Click "Add new".
3. Enter the name of the contact.
4. Enter the e-mail address of the contact.
5. To use the contact as a sender for an SMTP server that requires authentication with a certificate, select the appropriate certificate under "Certificate".
6. To use the contact as a sender for an SMTP server that requires authentication with a user name and password, enter the password.
   The e-mail address is used as the user name.
7. (Optional) Enter a comment relating to the contact.

Result

The contacts configured here are available:

- As the e-mail sender in the SMTP server configuration.
- As an e-mail recipient when configuring "target" job parameters with the target type e-mail

Maintenance of the SMTP server configuration

Store the data of the SMTP servers via which the e-mails are sent.

Requirement

Contacts that are suitable as senders have been entered in the "Global Settings > Contacts" tab.

Procedure

To create a new SMTP server configuration, follow these steps:

1. In the "Reports" control, click on the "Global settings > SMTP" tab.
2. Click "Add new".
3. Specify the following:

Field	Description
"Name"	Enter the name of the SMTP server configuration.
"Address"	Enter the URL of the SMTP server. Servers without authentication (e.g. company-internal mail servers) and with authentication are permitted. Example: URL of a company mail server: `mail.<Company name>.com`
"Port"	Enter the port number of the SMTP server. Default setting: 25
"Sender"	In the list, select the contact that is used as the sender for this SMTP server configuration. All contacts maintained under "Contacts" are offered to you for selection. Select a sender that meets the respective requirements of the server.
"Comment"	(Optional) Enter a comment relating to the SMTP server configuration.

Result

The servers configured here are available when configuring the "Target" job parameters with the target type email.

3.4.11.6 Configuring job parameters

Job parameters define the details of a report job.

You configure the following parameters on the "Job parameters" tab:

- Templates
- Trigger
  Define trigger when a report job is executed.
- Targets
  Targets define how a report is made available to users. The following target types are available:
  - "E-mail"
    An e-mail is sent after a report job is executed. The report generated by the report job can be included with the e-mail as an attachment.
  - "File system"
    The reports generated by the report job are stored in the file system.

The parameters configured here are available to you for selection when configuring the report jobs in the "Report jobs" tab.

You define the remaining job parameters while configuring a report job in the "Report jobs" tab.

See also

Importing and exporting report templates (Page 202)

Deleting templates (Page 203)

Configure trigger (Page 203)

Add target with target type "E-mail" (Page 206)

Importing and exporting report templates

Requirement

- The "Reports" control is placed on a screen of the project.
- The "Job parameters > Templates" tab is visible in the control.
- Import: You have access to the storage location of the report template.
- Export: Report templates have been imported into the control.

Importing report template

1. Click "Add new" in the toolbar.
   Alternative: In the work area, click "Add new".
2. In the dialog that opens, select the file of a report template.

3. Confirm your input.

Note

No validation

The template is not validated during import.

4. Optional: In the work area, select the imported report template in the work area and enter a comment describing the template in the detail area.

Exporting report templates

1. In the work area, select the options next to the report templates you want to export.
2. Click "Export" in the toolbar.

The report templates are downloaded to the download folder or a user-defined directory according to the device settings.

Deleting templates

Requirement

- The "Reports" control is placed on a screen of the project.
- The "Job parameters > Templates" tab is visible in the control.
- Templates have been imported into the control.

Procedure

1. In the work area, select the options next to the templates you want to delete.
2. Click "Delete" in the toolbar.

Deleting used templates

The "In use" column shows whether the template is used by a report job.

If you delete a template that is used by a report job, the report job is marked as inconsistent and no longer executed.

Configure trigger

Introduction

In the "Job Parameters > Triggers" tab you configure which automatic triggers are available for selection when configuring report jobs.

Report jobs with automatic triggers are executed if the report jobs on the "Report jobs" tab are set to active and their trigger event occurs. Users can also start the execution manually.

Requirement

- The "Reports" control is placed on a screen of the project.
- The "Job parameters > Trigger" tab is visible in the control.
- To use the trigger type "Context trigger": Contexts are available in the project.

Add trigger

1. In the work area of the tab, click "Add new".
   A new trigger is created and displayed in the detail area.
2. Assign a unique name to the trigger.
3. Select the trigger mode:

Trigger type	Triggering the trigger
"Tag trigger"	Automatically when the configured value condition occurs at the tag defined in the trigger.
"Serial trigger"	Automatically within the user-defined interval when the time defined by the series has been reached.
"Context trigger"	Automatically when the selected context is started or stopped. Optional: By using a condition, you can also limit the triggering of the trigger to specific context values.

4. Depending on the selected trigger type, set the settings for the new trigger as described below.
5. Optional: Enter a comment for the trigger.

Settings for tag trigger

1. Click "Select tag".
2. Click "Load".
3. Select the required tag and click "OK".
4. Set the condition and the condition value.
   Example:

Set tag	<tag name>
Condition	>
Condition value	100

The trigger will be initiated when the tag receives a value greater than 100.

Settings for serial triggers

1. Select the serial pattern.
   The series pattern defines the occurrence and time at which the trigger is initiated.
   Example: Weekly > Every 2 weeks > Fridays
2. Select the series area.
   The series range defines the period in which the trigger is initiated.

"Start"	Specify the start date
"Time"	Specify the time at which the trigger is initiated.
"End on"	Specify the end date. The trigger will be executed for the last time on this day.
"End after"	Determine the number of dates after which the series ends.
"No end date"	The series runs indefinitely.

Settings for context triggers

1. Click "Select context".
2. In the "Context selection" dialog, click "Select plant object".
3. In the "Browser view" dialog, select a plant object and confirm your input.
   In the "Context selection" dialog you can see all contexts that have been defined for the selected plant object.
4. Select a context and confirm your input.
5. Under "Context status", select when the trigger will be triggered:

"Started"	When starting the context.
"Stopped"	When stopping the context.

6. Optional: To bind the execution of the report order to certain context values, you define a condition:

"Condition"	Select an operator.
"Value"	Select a context value.

Example:

Plant object	"MyPlant.hierarchy::PlantView/Bottling"
Context	"Product"
Context state	"Started"
Condition	=
Value	"Orange lemonade"

Report jobs with this trigger are always executed when the context "Product" defined on the plant object "Bottling" is started with the value "Orange lemonade".

Delete trigger

Select the option of the desired trigger in the work area of the "Job Parameters > Triggers" tab and click "Delete" in the toolbar.

Edit trigger

1. Enable the option of the desired trigger in the work area of the tab.
2. In the detail area, edit the settings of the trigger.

Note

No change of the trigger type

The trigger type can only be set when adding the trigger.

Add target with target type "E-mail"

Requirement

- The "Reports" control is placed on a screen of the project.
- The receivers of the e-mails are maintained as contacts in the "Global settings > Contacts" tab.
- An SMTP server, with which the e-mail is to be sent, has been configured in the "Global settings > SMTP" tab.

Procedure

1. In the "Reports" control, click on the "Job parameters > Targets" tab.
2. In the work area of the tab, click "Add new".
3. Select "E-mail" as target type.
   A new target is created and displayed in the detail area.
4. Assign a unique name to the target.
5. Select an SMTP server configuration.
6. Add the desired receivers and CC receivers:
   – To do so, select a contact from the list "Add receiver" or "Add CC receiver".
   – Add the contact by clicking "+".
7. Enter the e-mail subject.
   To integrate the report name into the subject line, use the placeholder {ReportName}.
8. Enter the e-mail text.
   To integrate the report name into the email text, use the placeholder {ReportName}.
9. (Optional) Enter a comment.

Result

The target is available for selection when configuring report jobs.

An e-mail is sent after a report job is executed with this target. The e-mail can include the report as attachment.

See also

Dynamic placeholder (Page 220)

Add a target with "File system" target type (Unified PC)

This section describes how to add a target with the "File system" target type on a Unified PC in Runtime.

Introduction

A reporting job with a target of the "File system" target type saves reports to a file system.

When configuring the report jobs, you can choose from pre-configured and user-defined targets of this target type.

Preconfigured targets

The following targets with "File system" target type are pre-configured:

Local project storage location	The reports are stored in the following folder: `<Project folder of the Runtime project>\Reports`
Local main storage location	The reports are stored in the local main storage location for reports. The local main storage location is configured in TIA Portal in the Runtime settings of the HMI device. If this setting has not been set in TIA Portal, the reports are stored in the folder configured during the installation of Runtime or later in the "WinCC Unified Configuration" tool:

You can select these targets in the "Report jobs" tab. You cannot edit or delete these targets in the "Job parameters > Targets" tab.

User-defined targets

In the "Reports" control, you can create user-defined targets of the "File system" target type. These user-defined targets are always subfolders of the local main storage location.

Requirement

- The "Reports" control is placed on a process picture.

Procedure

To add user-defined targets of the "File system" target type, follow these steps:

1. In the "Reports" control, click on the "Job parameters > Targets" tab.
2. In the work area of the tab, click "Add new".
3. Select "File system" as target type.
   A new target is created and displayed in the detail area.
   Under "Destination path", you can see the path to the local main storage location for reports.
4. Assign a unique name to the target.

5. Under "Subfolder", enter the path to the subfolder in which the report is to be saved.
   Use the following notation: <folder name> or <folder name>\<folder name>\...

   Note

   Relative path information

   The path specification is relative to the local main storage location for reports.

6. (Optional) Enter a comment.

Result

The target is available for selection when configuring report jobs.

When a report job with this target is being executed, the generated report is stored in the subfolder of the local main storage location defined as the target. If the folder entered under "Target path" does not exist, it is created by the system.

Note

Change of the local main storage location for reports

When the local main storage location for reports changes, the targets are automatically adapted. New reports are stored relative to the new local main storage location. The old folders are not deleted.

See also

Reporting settings (Page 44)

3.4.11.7 Configuring report jobs

Creating a report job

Introduction

A *report job* is a job for generating reports in Runtime. The configuration of a report job controls the details of the generation.

Requirement

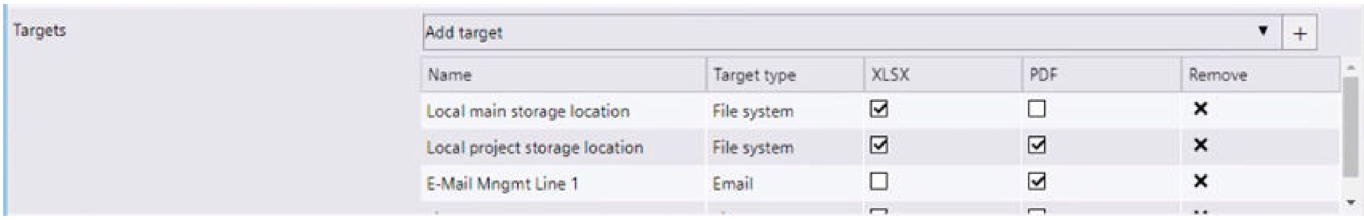
- The "Reports" control is configured on a screen of the project.
- The following job parameters were configured in the control:
  - At least one template has been imported.
  - To automatically execute a report job: Triggers are configured in the "Job parameters > Trigger" tab.

- For sending an email after execution of the report job:
  - Email contacts were configured in the global settings.
  - An SMTP server was configured in the global settings.
  - A target of the target type "E-mail" was configured in the "Job parameters > Targets" tab.
- For a report job with the target format PDF:
  - Microsoft Office Excel or LibreOffice is installed on the runtime server.
  - Depending on whether Excel or LibreOffice is installed, the information required for PDF creation was provided during the Runtime installation or in the "WinCC Unified Configuration" tool.

Procedure

1. Select the "Report jobs" tab in the "Reports" control.
2. Select "Add new" in the work area or click "Add new" in the toolbar.
3. In the detail area, enter a name for the report job.
4. Select a report template.
5. Configure the report name. See section Configuring report names (Page 211).
   The configuration is applied to all reports generated by the report job.

6. Under "Targets", you determine how the reports are to be made available to users. Follow these steps:
   - Click "Add target".
     You see the targets configured in the tab "Job parameters > Targets".
   - Select a target.
   - Add the target by clicking "+".
     The target is added to the table to define the target formats.



Name	Target type	XLSX	PDF	Remove
Local main storage location	File system	☑	□	✕
Local project storage location	File system	☑	☑	✕
E-Mail Mngmt Line 1	Email	□	☑	✕

   - Determine the formats in which the reports generated by the report job are provided for the target. In the table, activate the options of the desired formats for each target.

     Note

     Sending emails without a report

     If you deactivate both options for targets with "E-mail" target type, an email without attachment is sent after the report job has been executed.

     Note

     PDF as target type

     Generating PDFs with Excel is significantly slower than with LibreOffice. To generate large PDF reports, it is therefore recommended that you install LibreOffice.

     A PDF report created by LibreOffice can deviate in content or layout from a PDF report generated with Excel, for example, if the report template uses common Excel features that LibreOffice does not support, such as special fonts or chart types.

   - To remove a target from the report job, click the "Remove" button in the table.

7. Under "Trigger", select which event triggers the execution of the report job:
   - If the report job is only to be executed manually, select "Manual".
   - If the report job is to be executed automatically, select one of the other triggers configured under "Trigger".

     Note

     You can also execute the report job manually.

8. (Optional) Enter a comment for the report job.
9. Specify whether the automatic execution of the report job is active or paused. To do this, set the slider "Enabled" or "Disabled".

   Note

   You can still execute disabled report jobs manually.

Result

The report job is saved automatically.

When its trigger occurs, the report job is executed. A report is generated and made available as configured under "Targets".

See also

Execution of report jobs (Page 215)

Configure trigger (Page 203)

Add a target with "File system" target type (Unified PC) (Page 207)

Add target with target type "E-mail" (Page 206)

Tips on design and layout (Page 282)

Managing report jobs

Requirement

- The "Reports" control is configured on a screen of the project.
- Report jobs have been configured in the control.

Procedure

1. Select the "Report jobs" tab in the "Reports" control.
2. To edit a report job, proceed as follows:
   - Select the report job in the work area.
   - In the detail area, edit the settings of the report job.
     You have the same options as when creating a report job.
3. To delete report jobs, proceed as follows:
   - In the work area, enable the options next to the report job.
   - Click "Delete" in the toolbar.

Configuring report names

Note

Make sure that the generated report name does not violate the policy of the operating system regarding the maximum length of file names.

Introduction

The default name of reports is `Report_{NNN}`.

To use different report names, enter one or more placeholders at the report job. The placeholders are combined to form the report name during execution of the report.

Placeholder types

Placeholders have one of the following types:

Placeholder type	Description	
Text	For user-defined fixed texts	
Counter	On automatic numbering	Dynamic placeholders The placeholders are broken down into values during execution of the report.
Date format	For outputting the generation time	
Tag	To output the process value of an online tag	

Unique report names

If the report name uses counter or date format placeholders, the report job generates unique report names.

Requirement

- The "Reports" control contains a screen of the runtime project that is running.

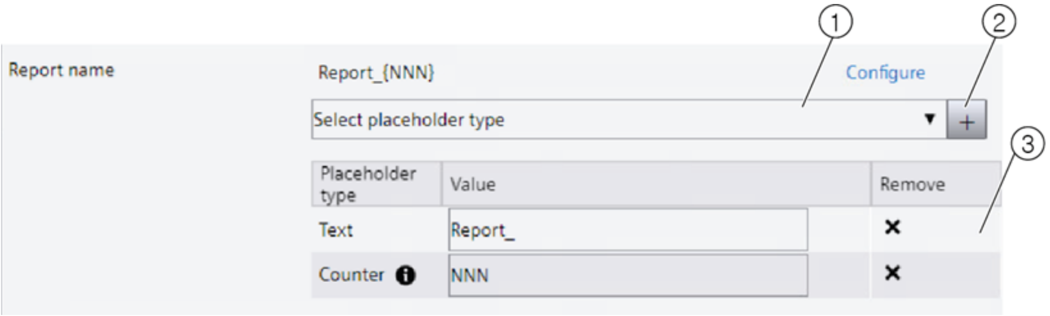
Procedure

You can enter the placeholders manually in the "Report name" field or you can have the software help you configure the report name.

To have the software help configure the report name, follow these steps:

1. Select the "Report jobs" tab in the "Reports" control.
2. Select a report job in the work area.
   You can see the settings for the report job in the detail area.

3. Next to "Report name", click "Configure".
   You see the following operator controls:



Report name	Report_{NNN}		Configure
	Select placeholder type ▼		+
	Placeholder type	Value	Remove
	Text	Report_	✕
	Counter ℹ	NNN	✕

① List for selection of the placeholder type
② Button for adding a placeholder of the selected type
③ Table for configuring or removing the placeholder

Note

For the default report name, the "Report name" has the value `Report_{NNN}` and the table shows the placeholders "`Report_`" and "`NNN`".

To swap the order of placeholders or to add a placeholder in the center, delete the placeholders and then add them in the desired order.

4. Optional: To delete the default placeholders, click "x" in the placeholder table.
5. Select the desired type under "Select placeholder type".

Note

A report name can contain only one counter.

6. Click "+".
   An empty placeholder of the corresponding type is added at the end of the table.
7. Enter the placeholder under "Value" in the placeholder table.

Placeholder type	Description	Example
"Text"	Enter the text.	`Report_`
"Date format"	Enter a date placeholder.	A list of permitted placeholders and examples can be found in section Dynamic placeholder (Page 220).
"Counter"	Enter a counter placeholder.	
"Tag"	Enter the full name of an online tag.	`RT1_Brewery::BatchNo`

Note

Enter the dynamic placeholders without any markup characters.

Alternatively, you can select an online tag via the user interface. Follow these steps:

– Click the "..." button on the tag placeholder.

– In the "Tag selection" dialog, click the "Search" button.
  You can see all the tags of the Runtime project that is running.

Note

Scrolling and filtering

Use the page navigation buttons to scroll forward or backward.

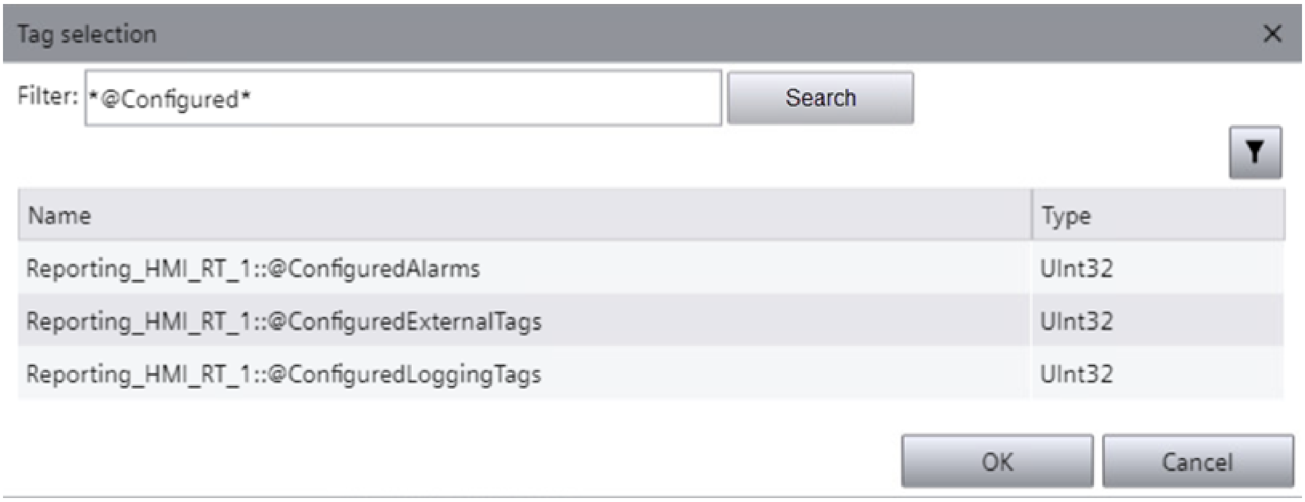
To filter the displayed tags, enter a filter string in "Filter" and click "Search".

You use the wildcard "*" to filter by partial strings.

For example:

- *T* returns all tags with a "T" in their name.
- *T returns all tags that end in "T".
- T* returns all tags that start with "T".

When filtering for structures, the separators must be part of the filter string.



Filter: *@Configured*

Name	Type
Reporting_HMI_RT_1::@ConfiguredAlarms	UInt32
Reporting_HMI_RT_1::@ConfiguredExternalTags	UInt32
Reporting_HMI_RT_1::@ConfiguredLoggingTags	UInt32

– Click the desired tag.

– Confirm with "OK".

In the "Report name" field, the placeholder you added is appended to the end of the report name.

Alternative procedure

To enter the placeholders manually, proceed as follows:

1. Select the "Report jobs" tab in the "Reports" control.
2. Select a report job in the work area.
   You can see the settings for the report job in the detail area.
3. Enter the desired combination of fixed texts and dynamic placeholders manually in the "Report name" field.
   Use markup characters for the dynamic placeholders. See section Dynamic placeholder (Page 220).

Example:

"Report name" value	Generated report name
`Report_{yyyymmdd}_{HHMMss}_{@PC1_Brewery::BatchNo}`	`Report_20190101_170001_BatchNo_87002314`

Result

When generating a report, the dynamic placeholders are resolved and all placeholders are merged to form the report name.

If a process value contains a character that is not permitted in file names, it is replaced by an underscore.

If there is an error resolving the name, e.g. because the tag is not found in runtime, the tag placeholder in the name is replaced by `ERR`. The process is logged in the generation status of the report.

Execution of report jobs

Automatic and manual execution

Automatic execution

Report jobs that have a tag trigger, serial trigger or context trigger and are set to active on the "Report jobs" tab are automatically executed when their trigger occurs.

Manual execution

Report jobs with a trigger of the "Manual" type must always be executed manually.

In addition, you can at any time manually execute report jobs that have a tag trigger, serial trigger or context trigger.

System response to errors

- Error adding the report job to the queue
  The execution of the report job is discarded. A system alarm documents the error.
- Error executing the job
  In the "Reports" control, "Reports" tab, the status icon indicates the error. A click on the icon opens a detailed status message.
  A system alarm documents the error.

See also

Running a report job manually (Page 216)

Configure trigger (Page 203)

3.4.11.8 Running a report job manually

You can execute report jobs manually at any time, regardless of their trigger type. This also applies to report jobs that were disabled in the "Report Jobs" tab and whose automatic execution is therefore paused.

Requirement

Report jobs have been configured in the "Reports" control.

Procedure

1. Select the "Report jobs" tab in the "Reports" control.
2. In the work area, enable the option next to the report job that you want to execute manually.
3. Click "Execute" in the toolbar.

Result

The report is generated. You can download it in the "Reports" tab.

3.4.11.9 Downloading reports

You can download the reports stored by the report job in the file system to your device.

Depending on which file formats have been set in the report job, you can download the report as an XLSX file and as a PDF file.

Requirement

- Report jobs with the target type "File system" have been configured and executed in the "Reports" control.

Procedure

1. Select the "Reports" tab in the "Reports" control.
2. In the work area, select the option in the left column for each report that you want to download.
3. Enable the desired target formats in the "Files" column.

   Note

   Generation status

   You are only offered successfully generated formats.

   In the "Status" column you can check whether the generation for a format has failed. For a detailed status message click on the icon of a target format.
4. Click "Export" in the toolbar.

Result

The reports are downloaded into the download directory of the browser.

You can edit, distribute, or log the reports.

See also

Installation of the Reporting add-in (Page 224)

3.4.11.10 Exporting an offline configuration file

An offline configuration file is required to configure reporting templates in the Reporting Excel add-in without an online connection to the Runtime server.

Requirement

- The "Reports" control is placed on a screen of the project.
- The Runtime project has data that can serve as data source elements in the reporting template, such as alarms and logging tags.

Procedure

1. In the "Reports" control, click on the "Global settings > Configuration" tab.
2. Enter the name of the offline configuration file under "Offline-configuration".
3. Click "Export offline configuration".

Result

A JSON file with the data source elements of the Runtime project is created. The file is downloaded to the download folder or a user-defined directory according to the device settings.

You can select the configuration file in the Reporting Excel add-in as data source for an offline connection.

3.4.11.11 Transferring the control configuration

You have the option of reusing the settings in the "Reports" control, for example, on a device in another network. To do this, export the existing configuration on the one device from the control to a ZIP file. Then import the file into a "Reports" control on the other device.

Scope

The transfer covers the following data:

- Global settings, without passwords and certificates
- Job parameters, including the report templates available in the control
- Report jobs

Reports are not transferred.

Requirement

- The "Reports" control is placed on a screen in the project running in Runtime.
- Export: Settings have been made, e.g. contacts maintained, report templates imported, and report jobs created in the "Reports" control.
- Import: You have access to the ZIP file generated by the export on the device on which Runtime is installed.

Export configuration

1. In the "Reports" control, select the "Global settings > Configuration" tab.
2. Enter the name of the export file under "Export/import configuration > Export".
3. Click "Export configuration".

The configuration is exported to a ZIP file and downloaded to the default download directory of the device.

Import configuration

1. In the "Reports" control, select the "Global settings > Configuration" tab.
2. Click "Select import file" under "Export/import configuration".
3. Select the ZIP file in File Explorer and confirm your selection.
4. Runtime checks whether the control already contains configurations:
   – No: The configuration is imported.
   – Yes:
     Select "OK" to import the configuration. The existing configuration is overwritten.
     Select "Cancel" to cancel the import.

3.4.11.12 Configuring enable paging

To set how many entries the lists in the work area of the "Reports" control display per page, follow these steps:

1. In the "Reports" control, click on the "Global settings > Configuration" tab.
2. Under "List Settings", select the number of entries.

If a list has more entries, these are split over several pages. Use the buttons below the list to switch pages.

Note

The setting is lost through a screen change.

3.4.11.13 Inconsistencies and error diagnostics

Note

Inconsistent report jobs are not executed.

The templates available in the "Reports" control are not validated.

Display of inconsistencies and errors

Errors and inconsistencies are displayed as follows:

In the control	If job parameters are affected. Examples: • No template is set for a report job. • A tag that triggers a report job is deleted in the engineering system. The project is reloaded into the device.
In the "Error log" worksheet of the report	Errors or inconsistencies affecting the content of the report. Example: The report evaluates data from a tag that is no longer available in runtime.
As system alarm	For errors and inconsistencies that do not affect job parameters or the contents of the report. Example: The ExecuteReport system function transfers a report job that does not exist.

Job parameters

The following values lead to errors and inconsistencies:

Parameter	Invalid values	Default setting
"Name"	Zero, empty or already assigned name	"New report job"
"Template"	Zero, empty or "None". Name of a template that is not imported	"None"
"Target name"	Zero or empty	"NewReportJob[NN]"

3.4.11.14 Dynamic placeholder

Introduction

Dynamic placeholders are evaluated when the report job is executed and replaced with text in runtime.

The following job parameters can contain placeholders:

- Report name
- Targets with the target type "E-mail": Subject and text of the email

Dynamic placeholders for report names

Use dynamic placeholders for counters and/or dates to generate unique report names:

Counter placeholder	Description	Example		Area
		Configuration	Result	
{N}	Automatic numbering	Rep_{N}	Rep_1	0...9
{NN}		Rep_{NN}	Rep_01	00...99
{NNN}		Rep_{NNN}	Rep_001	000...999

Date placeholder	Description	Example		Area
		Configuration	Result	
{yy}	Current year	Rep_{yy}	Rep_18	Valid year with 2 digits
{yyyy}		Rep_{yyyy}	Rep_2018	Valid year with 4 digits
{m}	Current month	Rep_{m}	Rep_1	Valid month, no prefixed 0 for months in single-digit range
{mm}		Rep_{mm}	Rep_01	Valid month, prefixed 0 for months in single-digit range
{mmm}		Rep_{mm}	Rep_Jan	Month abbreviation with 3 characters
{mmmm}		Rep_{mmmm}	Rep_January	Month with full name

Date placeholder	Description	Example		Area
		Configuration	Result	
{d}	Current day of the month	Rep_{d}	Rep_1	Valid day, no prefixed 0 for days in single-digit range
{dd}		Rep_{dd}	Rep_01	Valid day, prefixed 0 for days in single-digit range
{ddd}		Rep_{ddd}	Rep_Mon	Day abbreviation with 3 characters
{dddd}		Rep_{dddd}	Rep_Monday	Day with full name
{h}	Current hour	Rep_{h}	Rep_1	Current hour (12-hour clock), no prefixed 0 for single-digit values
{hh}		Rep_{hh}	Rep_01	Current hour (12-hour clock), prefixed by 0 for single-digit values
{H}		Rep_{H}	Rep_13	Current hour (24-hour clock), no prefixed 0 for single-digit values
{HH}		Rep_{HH}	Rep_13	Current hour (24-hour clock), prefixed by 0 for single-digit values
{M}	Current minute	Rep_{M}	Rep_6	Valid minute, no prefixed 0 for single-digit values
{MM}		Rep_{MM}	Rep_06	Valid minute, prefixed by 0 for single-digit values
{s}	Current second	Rep_{s}	Rep_41	Valid second, no prefixed 0 for single-digit values
{ss}		Rep_{ss}	Rep_41	Valid second, prefixed by 0 for single-digit values

Use a dynamic placeholder for tags to integrate process values in the report name:

Tag placeholder	Description	Example		Area
		Configuration	Result	
{@<Full Tag name>}	Process value of an online tag	Rep_{@PC1_LineA::MyTag1}	Rep_On	Process value of the online tags If the value contains a character that is not permitted in file names, it is replaced by an underscore. If there is an error resolving the name, e.g. because the tag is not found in runtime, the tag placeholder in the name is replaced by `ERR`. The process is logged in the generation status of the report.

Examples:

Definition with placeholder	Generated report name
LineA_{yyyymmdd}_{HHMMss}	LineA_20190101_170001
LineA_{yymmmd}_{hhMMss}	LineA_19Jan1_050001
LineA_{NNN}	LineA_014
LineA_{yyyymmdd}_{HHMMss}_BatchNo_{@PC1_Brewery::BatchNo}	LineA_20190101_170001_BatchNo_87002314

Placeholder for email subject and email text

To integrate the report name into the subject line or the email text, use the following dynamic placeholder {ReportName}.

Markup

Use the following markup characters for dynamic placeholders:

- Placeholders for counter and date: `{}`
- Placeholders for tags: `{@}`

Note

There is no markup in the placeholder table for defining the report name. See also section Configuring report names (Page 211).

3.4.11.15 System alarm reporting

System alarm reporting

The following is the list of the most important system alarms.

ID	Alarm text	Effect/causes	Solution
538640385	Initialization of the reporting service failed	Initialization of the reporting service fails.	Contact Siemens customer service.
538640386	Report Data Provider cannot be started	The data provider for reports could not be started.	Contact Siemens customer service.
538640387	The report cannot be started for the job [name].	The Report Creator for report jobs cannot be started.	Check the report job settings. If you use the "ExecuteReport" system function, check the name of the report job and the parameters passed when calling the function.
538640388	An error occurred during communication with the database server	The reporting database cannot be found or access is not possible for other reasons.	Check whether the reporting database is available at the storage location configured in the Runtime settings in engineering. Examples: • Does the folder specified as storage location in the Runtime settings exist? • Has the folder been specified in the correct notation? • On a panel: Is the SD card plugged in?

ID	Alarm text	Effect/causes	Solution
538640389	The creation of the report job [name] failed	The Report Creator is missing information about the report job. A possible reason for this are problems with processing the report template.	Check the report job settings and the report template.
538640390	Report failed	Report Creator reports an error while generating the report.	Check the detailed error message for the report: Control "Reports" > "Reports" tab > "Status" column.

3.4.11.16 Configuring report templates in the add-in

Requirements

General requirements and restrictions

The following requirements and restrictions apply to the configuration of report templates.

Installing the Excel add-in

The installation of the Reporting add-in on a computer requires that the operating system and the local MS Excel installation are regularly updated.

If there are problems with the installation, check the version of the local MS Excel installation. Lengthy maintenance intervals between the operating system and Excel can cause problems during installation of the add-in.

Update the operating system and the Excel version if necessary.

To install the add-in with a local Excel installation, MS Excel with build 16.0.6769 or higher is required.

Note

Note the Microsoft upgrade restrictions

If you have an Excel installation that cannot be upgraded to Build 16.0.6769 or higher (for example, because Excel was installed using a single Office license), purchase a current Office version or use Online Office.

IIS settings for standalone installation of the Excel Add-In

To install the Excel Add-In on a PC without Unified Runtime, the same IIS (Internet Information Services) settings must be active in Windows that are required to install WinCC Unified Runtime on a PC.

You can find additional information in the "SIMATIC Unified PC Installation" user help section on the software and hardware requirements.

Enable Reporting

The Runtime project that is the data source of a report template must have reporting functionality enabled.

You activate the reporting functionality of a Runtime project before loading it into the device in TIA Portal: "Runtime settings" of the HMI device > "Reporting" > "Enable Reporting" option

Note

Devices with a device version lower than V18

Reporting is always enabled for HMI devices with a device version lower than V18.

Unified Comfort Panel

Contexts are not supported for Unified Comfort Panel. This option is not available in a report template with a Unified Comfort Panel as data source.

See also

Version compatibility (Page 192)

Installation of the Reporting add-in

Note

Regular updates of operating system and MS Excel

The installation of the Reporting add-in on a computer requires that the operating system and the local MS Excel installation are regularly updated.

If there are problems with the installation, check the version of the local MS Excel installation. Lengthy maintenance intervals between the operating system and Excel can cause problems during installation of the add-in.

Update the operating system and the Excel version if necessary.

To install the add-in with a local Excel installation, MS Excel with build 16.0.6769 or higher is required.

Note

Note the Microsoft upgrade restrictions

If you have an Excel installation that cannot be upgraded to Build 16.0.6769 or higher (for example, because Excel was installed using a single Office license), purchase a current Office version or use Online Office.

Procedure

1. Install the Excel manifest on the computer.
2. Set up read access to the installation path of the Excel manifest.
3. Add the add-in to Excel.

See also

Installing the Excel manifest (Page 225)

Setting up read access to the Excel manifest (Page 225)

Adding the Reporting add-in in Excel (Page 226)

Installing the Excel manifest

Procedure

1. In the installation package of WinCC Unified on "DVD_2", double-click the file "Support\Reporting\SIMATIC_WinCC_Unified_Reporting_<Version number>.exe".
2. Select the target directory to which the underlying ZIP file is extracted and confirm your input. The ZIP file is extracted and setup starts automatically.

   Note

   Start setup manually

   To start the setup manually after the file was extracted, select the option "Extract the setup files without being installed".

   Start the setup later by running the "Setup.exe" file as administrator in the target directory.
3. Follow the setup instructions.
4. In the "Configuration" step, select the option for the Excel add-in.
5. Click "Next" and follow the setup instructions.

See also

Installation of the Reporting add-in (Page 224)

Setting up read access to the Excel manifest

Requirement

The Excel manifest is installed.

Procedure

Give the users that create templates with the Excel add-in read access to the installation path of the Excel manifest: <target directory>\WinCCUnifiedReporting\Excelmanifest

Note

This step is also necessary if the user belongs to a group in the user management with general read permission.

See also

Installing the Excel manifest (Page 225)

Installation of the Reporting add-in (Page 224)

Adding the Reporting add-in in Excel

Requirement

- The Excel manifest is installed on the PC.
- Read access to the installation path of the Excel manifest is set up.
- The following software is available on the computer:
  - Local Excel
    MS Excel (Build 16.0.6769 or higher)

    Note

    Regular updates of operating system and MS Excel

    The installation of the Reporting add-in on a computer requires that the operating system and the local MS Excel installation are regularly updated.

    If there are problems with the installation, check the version of the local MS Excel installation. Lengthy maintenance intervals between the operating system and Excel can cause problems during installation of the add-in.

    Update the operating system and the Excel version if necessary.

    Note

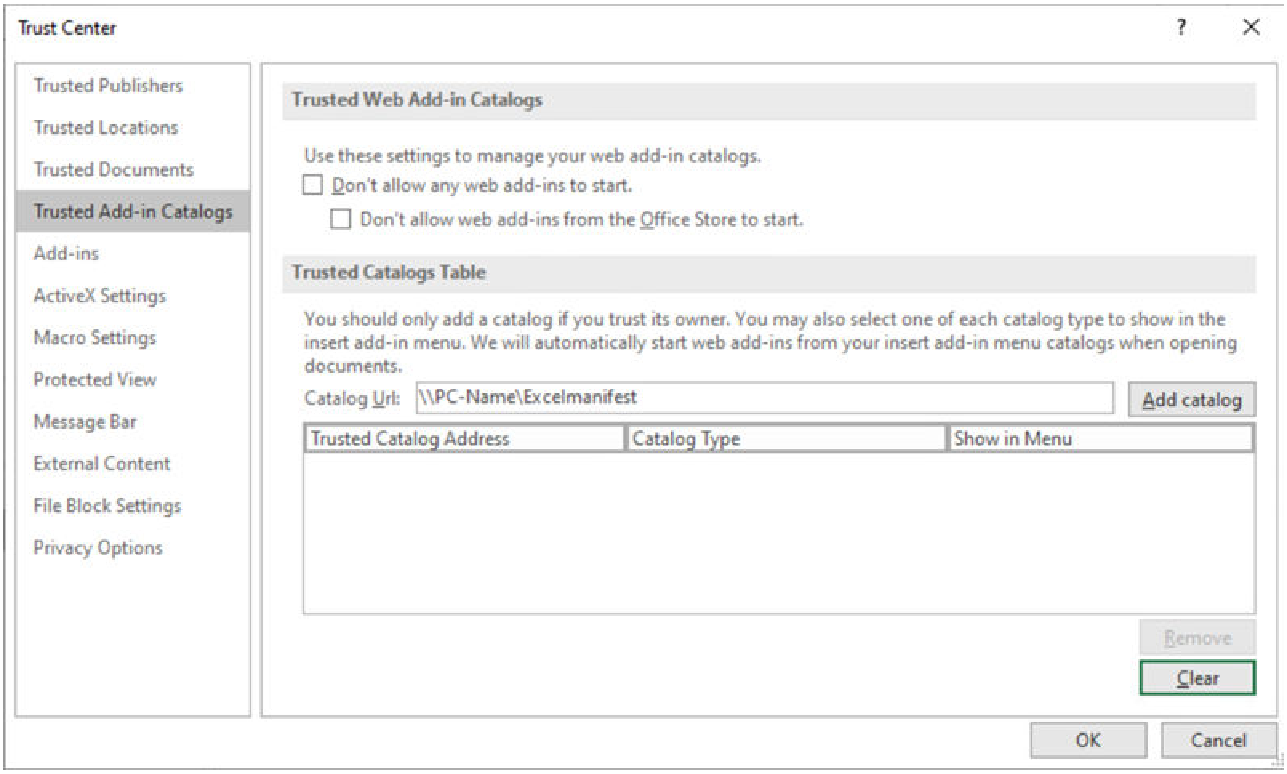
    Note the Microsoft upgrade restrictions

    If you have an Excel installation that cannot be upgraded to Build 16.0.6769 or higher (for example, because Excel was installed using a single Office license), purchase a current Office version or use Online Office.

  - Or Office online

Procedure

1. Open Microsoft Excel.
2. Open the "Trust Center" under "File" > "Options".
3. Click "Trust Center Settings".
4. Click "Catalogs of trusted add-ins".
5. Add the catalog using the URL "\\<Computer name>\Excelmanifest".



Trusted Web Add-in Catalogs

Use these settings to manage your web add-in catalogs.

□ Don't allow any web add-ins to start.

□ Don't allow web add-ins from the Office Store to start.

Trusted Catalogs Table

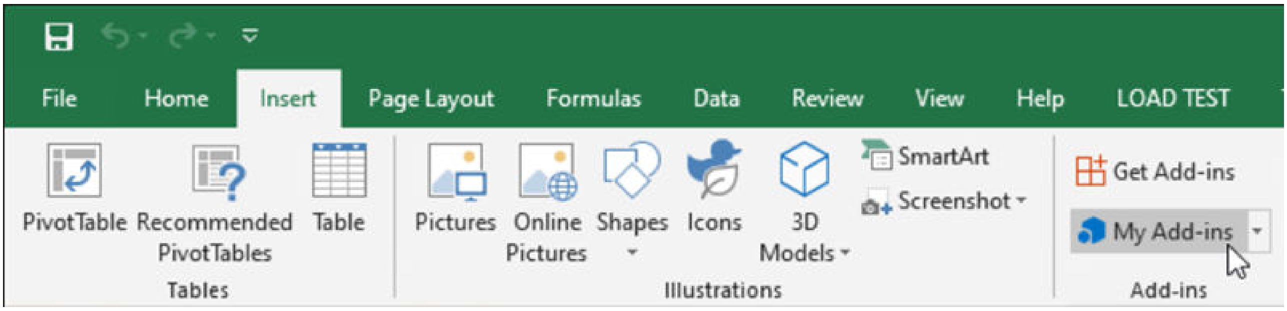
You should only add a catalog if you trust its owner. You may also select one of each catalog type to show in the insert add-in menu. We will automatically start web add-ins from your insert add-in menu catalogs when opening documents.

Catalog Url: \\PC-Name\Excelmanifest

Trusted Catalog Address	Catalog Type	Show in Menu

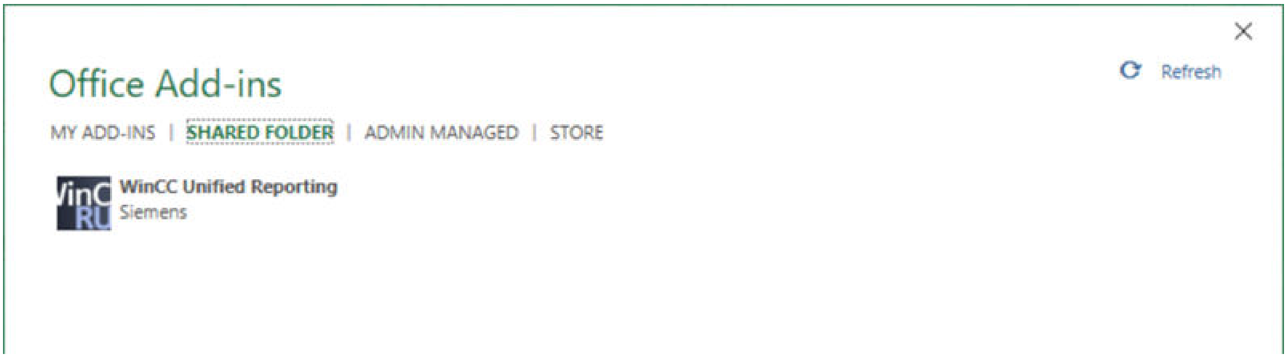
6. Make sure that the check mark in the "Show in Menu" column is set.
7. End and restart Excel.

8. In the "Insert" menu, click "My Add-ins".



In the "Office Add-ins" dialog box, the Siemens add-in is displayed under "Shared folders".

9. Select the add-in and click "Add".



See also

Installing the Excel manifest (Page 225)

Setting up read access to the Excel manifest (Page 225)

Installation of the Reporting add-in (Page 224)

Configuring Internet Explorer and Edge

The Reporting Excel add-in uses the certificate that was selected during installation of WinCC Unified Runtime or later in "WinCC Unified Configuration".

Some browsers do not recognize self-signed certificates as trusted. If you use a self-signed certificate for WinCC Unified Runtime, you must add the certificate to the list of trusted certificates in Internet Explorer or Edge on the device on which the Excel add-in is installed.

You can find detailed information on handling certificates here.

Trusting self-signed certificates

The following section describes the procedure for adding a self-signed certificate to the list of trusted certificates, using Internet Explorer as an example:

1. Start Internet Explorer.
2. In the address line, enter the host name entered when creating the certificate.
   You will receive a security warning.
3. Click "Continue to this website (not recommended)".
4. Click "View Certificates".
5. Click "Install Certificate".
6. Click "Place all certificates in the following store" and "Browse".
7. Click "Trusted Root Certification Authorities" followed by "OK".

   Note

   Do not use the preset options for automatic selection of the certificate store.

8. Exit the dialog.
9. If you receive a security warning as to whether you want to trust the certificate, confirm it with "Yes".
10. Load the page again.

Login

A login dialog opens in the Excel add-in in the following cases:

- After start of Excel and the add-in
- When using an online connection: When the connection to the Runtime server must be re-established.
  Examples:
  - Runtime has been reloaded.
  - The security token has expired due to a timeout.

Requirement

- The add-in is installed.
- When using an online connection:
  - A Runtime server is accessible.
  - A Runtime project is running on the server for which reporting is enabled.

Procedure

In order to use an online connection, log onto a Runtime server:

1. Under "Server", enter the device name or FQDN (Fully qualified domain name) or the IP address of the server on which the project is running that is to serve as the data source for the report template:
   - If the device name/FQDN is used to address the Runtime web page, use Device Name/FQDN.
   - If IP address is used for addressing, enter the IP address.

   Note

   If Runtime is installed on the same computer as the add-in, it is not allowed to enter the string "localhost" under "Server" to register the add-in.

2. Enter the user name and password of a user that is registered on the server in the Runtime user management.
3. Click "Login".

In order to use an offline connection, click "Go offline".

Result

Online connection

The add-in is connected to the Runtime server and the options available there are loaded.

You can now create report templates.

Offline connection

Before you create report templates, set up the offline connection.

See also

Installation of the Reporting add-in (Page 224)

Setting up an offline connection (Page 233)

General requirements and restrictions (Page 223)

Setting up a data source

Using an online connection

When an online connection is present, the add-in establishes a connection to a Runtime server. The project running on the server serves as data source for the add-in.

The connection settings allow you to:

- Change the connected Runtime server to another Runtime server
- When a report template that was created with a different Runtime server than the currently connected server is reused: check the options available on the server and delete the options that were not loaded

Setting up an online connection

Requirements

- A Runtime server is accessible.
- A Runtime project is running on the server.

Procedure

1. In the "Data sources" group on the "WinCC Unified" tab, click on "Connections".
2. Click "Online" under "Connections" in the add-in.
3. Under "Server", enter the server name.
   Use the same spelling as when the Runtime server certificate was created.

   Note

   If Runtime is installed on the same computer as the add-in, use of the name "localhost" is not permitted.
4. Click "Load".

Result

- A server node is created.
- The add-in is connected to the Runtime server and its options are loaded.
  Data source items of these options can be added to report templates. Their data can be read in from Runtime to Excel.

  Note

  To check which options were loaded, click on the server node.

  Options that are being used in the currently open report template but are not available on the connected server have a red icon. You can remove the option:
- If no connection can be established or an incorrect server name has been entered, the add-in will display a corresponding error message.

See also

Removing options (Page 232)

Removing options

Introduction

If you reuse report templates across servers, e.g. in order to adapt an existing template for another project, it may be necessary to remove unavailable options from the connection settings.

The procedure for this is presented using the Performance Insight option as an example.

Requirement

- The add-in was connected to a server on which the Performance Insight (PI) option is installed.
- A report template that uses KPIs was created with the add-in.
- The add-in was then connected to a server without the Performance Insight option installed for the purpose of adapting the template to the project running there.

Removing an option

1. In the "Data sources" group on the "WinCC Unified" tab, click on "Connections".
2. Under "Connections", click on "Online".
3. Select the server node.
   You see the loaded options under the server node:

🟩	Available options The following applies to data source items of these options: • They can be added to the report template. • Their data can be read in from Runtime to Excel in the add-in.
🟥	Unavailable options In the example: Performance Insight The following applies to data source items of these options: • They cannot be added to the report template. • If the report template already has a data source element of this option, its data cannot be read in from Runtime to Excel.

4. Select the "Performance Insight" option under the server node.
5. Click the "Delete" button next to the option.
6. Confirm your input.

Result

The option is removed from the connection settings.

Next, remove all data source items of this option from the report template.

Reloading an option

When the add-in is connected to a Runtime server, all options available on the server are loaded.

To reload an option that was deleted in the connection settings but is available on the server, select the server node and click "Load".

Using an offline connection

With the offline connection, the add-in uses a configuration file as data source.

The connection settings allow you to:

- Change the configuration file used
- When reusing a report template with a configuration based on a Runtime server different to that of the currently selected configuration file: Check the available options and delete the options that were not loaded.

Setting up an offline connection

Requirement

An offline configuration file was created in the "Reports" control in Runtime. The configuration file is available on the device.

Procedure

1. In the "Data sources" group on the "WinCC Unified" tab, click on "Connections".
2. Under "Connections", click on "Offline".
3. Click "Open offline configuration".
4. Select the desired file in the window that opens and confirm your entries.
5. Click "Load".
6. Select the desired options.
7. Confirm your entries.

Result

- A server node is created. The node bears the name of the server on which the configuration file is based.
- The configuration file, together with its options, is loaded into the add-in. The data of the configuration file is available for configuring the report template.

Note

To check which options were loaded, click on the server node.

Options that are being used in the currently open report template but are not available in the configuration file have a red icon. You can remove the option:

See also

Removing options (Page 234)

Exporting an offline configuration file (Page 217)

Removing options

Introduction

If you reuse report templates across servers, e.g. in order to adapt an existing template for another project, it may be necessary to remove unavailable options from the connection settings.

The procedure for this is presented using the Performance Insight option as an example.

Requirement

- The add-in was changed over to an offline connection whose configuration file does not include Performance Insight.
- A report template was opened in the add-in whose configuration is based on a connection to a Runtime server on which Performance Insight is installed.

Removing an option

1. In the "Data sources" group on the "WinCC Unified" tab, click on "Connections".
2. Under "Connections", click on "Offline".
3. Select the server node.
   You see the loaded options under the server node:

🟩	Available options The following applies to data source items of these options: • They can be added to report templates. • Their data can be read in from the configuration file to Excel.
🟥	Unavailable options In the example: Performance Insight The following applies to data source items of these options: • They cannot be added to the report template. • If the report template already has a data source element of this option, its data cannot be read in from the configuration file to Excel.

4. Select the "Performance Insight" option under the server node.
5. Click the "Delete" button next to the option.
6. Confirm your input.

Result

The option is removed from the connection settings.

Next, remove all data source items of this option from the report template.

Reloading an option

When a configuration file is loaded, all options available in the file are loaded.

To reload an option that was deleted in the connection settings but is available in the configuration file, select the server node and click "Load".

Configuring report templates

Requirement

An online connection or offline connection has been established.

Procedure

To create a new report template, proceed as follows:

1. Open a new Excel file.
2. Add a segment.
   You can choose between time series segments and single value segments.
3. Add data source items to the segment.
   The exact procedure depends on the type of the data source item.
4. Optional: If you do not want a data source item to use the default configuration, determine its configuration.
   You have the following options:
   - Select an existing configuration.
   - Create a new configuration and select it.
   - Define a local configuration.
5. Optional: To define additional segments, repeat steps 2 to 4.
6. Optional: When using an online connection, test the template by reading the runtime data of selected segments or all segments.

See also

Setting up a data source (Page 230)

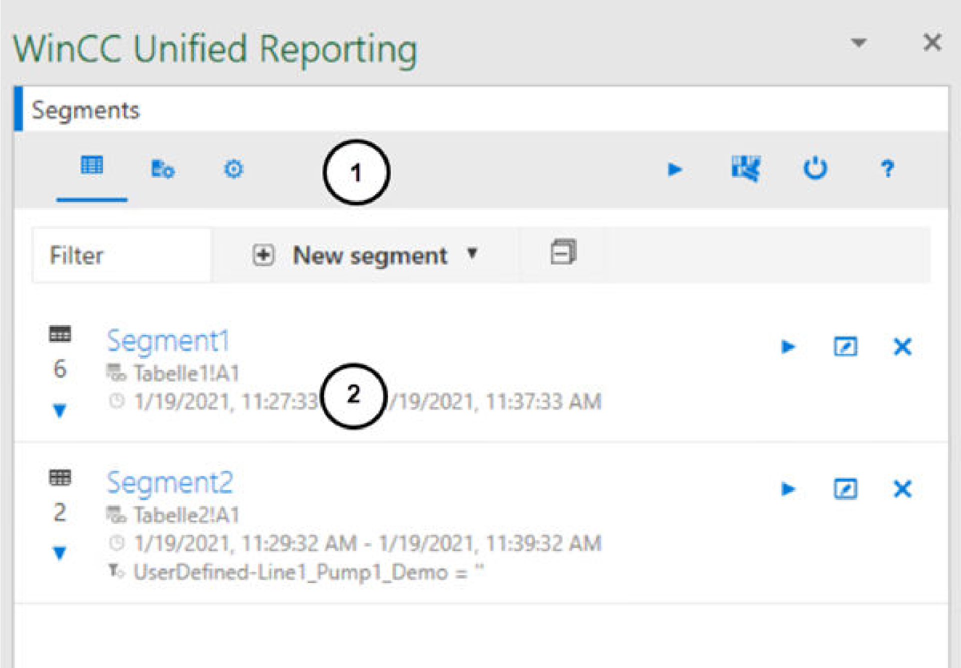
User interface of the add-in

Requirement

- The "WinCC Unified" tab is visible in Excel.

Structure

If you click on "Segments" in the "Configuration" group, you see the following interface:



Segment1
Tabelle1!A1
1/19/2021, 11:27:33 … /19/2021, 11:37:33 AM
6

Segment2
Tabelle2!A1
1/19/2021, 11:29:32 AM - 1/19/2021, 11:39:32 AM
UserDefined-Line1_Pump1_Demo = ''
2

① Toolbar
② Work area

Toolbar buttons:

Button	Tooltip	Description
▦	"Segment configuration"	Loads the interface to add and edit segments in the work area.
	"Data source item configuration"	Loads the interface for adding and editing the configuration of a data source item in the work area.
⚙	"Basic settings"	Loads the interface for setting the language settings in the work area.
▶	"Update all"	Reads the Runtime data of the connected data source into the data tables of the segments.
	"Delete Runtime data"	Removes all Runtime data from the report template.

Button	Tooltip	Description
⏻	Logoff	Logs out the user currently logged in to the add-in.
?	Help	Opens the user help for the add-in.

See also

The segment user interface (Page 241)

Working with segments

Basic information on segments

Definition

A report template consists of any number of segments. Each *segment* is a container to which you can add any number of data source items. The segment reads the data from its data source items.

There are time series segments and single value segments.

Note

Hierarchical segments of PI options

Hierarchical segments are also available with PI Options installed. For more information on this, refer to the PI Options help.

Time series segments

A *time series segment* documents the data of its data source items in a defined time period.

It has a legend table and a data table.

Data source items

Time series segments can have the following data source items:

- Logging alarms
- Alarm statistics
- Logging tags
- User-defined columns
- Contexts
- Audit

Note

Data source items of the PI options

If PI options are installed, additional data source items can be added. For more information on this, refer to the PI Options help.

Legend table

The table header row provides general information about the segment and its data source items.

You decide which type of information is provided when you create or edit the segment.

Data table

The data table outputs the data of the data source items. It documents how the data source items have changed in the defined time period.

The data table of a time series segment has the following columns:

Columns		Description
Time stamp column		Always output Always output as the first column
Per data source item	Standard column	The standard column provides the standard property of the data source item. This property depends on the type of data source item. For a data source item of the Tag type, e.g. the tag value
	Optional columns	Provide more information about the data source item. What information this is depends on the type of the data source item. For a data source item of the Tag type, e.g. the quality code of the tag value You change the default settings for visibility, column title and order of these columns in the configuration of the data source item.

In the default setting, the data source items in the data table have the order in which they were added to the segment.

Note

When the standard columns and optional columns provide numerical values, you can have the actual values replaced with texts or graphics from a text list or graphic list when importing the Runtime data.

Single value segments

A *single value segment* documents exactly one value for its data source items.

Data source items

Single value segments can have the following data source items:

- Logging tags
- Tags

Note

Data source items of the PI options

If PI options are installed, additional data source items can be added. For more information on this, refer to the PI Options help.

Data table

The data table of a single value segment has the following columns per data source item:

Columns	Description
Standard column	The standard column provides the standard property of the data source item. For tags and logging tags: the tag value
Optional columns	Provide more information about the data source item. For tags and logging tags: • Time stamp • Data source item • Quality code of the tag value You change the default settings for the visibility of these columns in the configuration of the data source item.

The data table of a single value segment shows the data source items in the order in which they were added to the segment.

Note

When the standard columns and optional columns provide numerical values, you can have the actual values replaced with texts or graphics from a text list or graphic list when importing the Runtime data.

Single row segments do not have a table header row. However, in the configurations of their data source items, you can determine whether a caption is inserted for the displayed columns and the position at which this occurs.

See also

Standard column (Page 239)

Standard column

Introduction

For each data source item of a segment, a standard column is added in the data table of the segment.

Content of the standard column

The standard column provides the standard property of the data source item and depends on the type of the data source item:

Data source item type	Default column title	Value
Logging alarm	"Alarm ID"	Alarm IDs of the displayed alarms
Alarm statistics	"Alarm statistics [ID]"	Alarm IDs of the alarms displayed in the alarm statistics
Tag or logging tag	"<Name of the tags or logging tags>"	Value of the tag or logging tag
Context	"<Name of the context object>"	Context name
Audit	"Audit [<object name>]"	The name of the object monitored by the Audit Trail
User-defined column	Name entered when creating the data source item	As set in the configuration of the data source item: • A fixed string. Or • A dynamically calculated string

Changing the column title

You can replace the default column title with a localizable display name. See Setting a display name for standard column (Page 276).

Replacing numerical values

If the standard column provides numeric values, you have the option to have the actual values replaced with texts or graphics from a text list or graphic list when the Runtime data is read in. See Assigning text lists and graphic lists (Page 274).

User-defined columns are excluded from this.

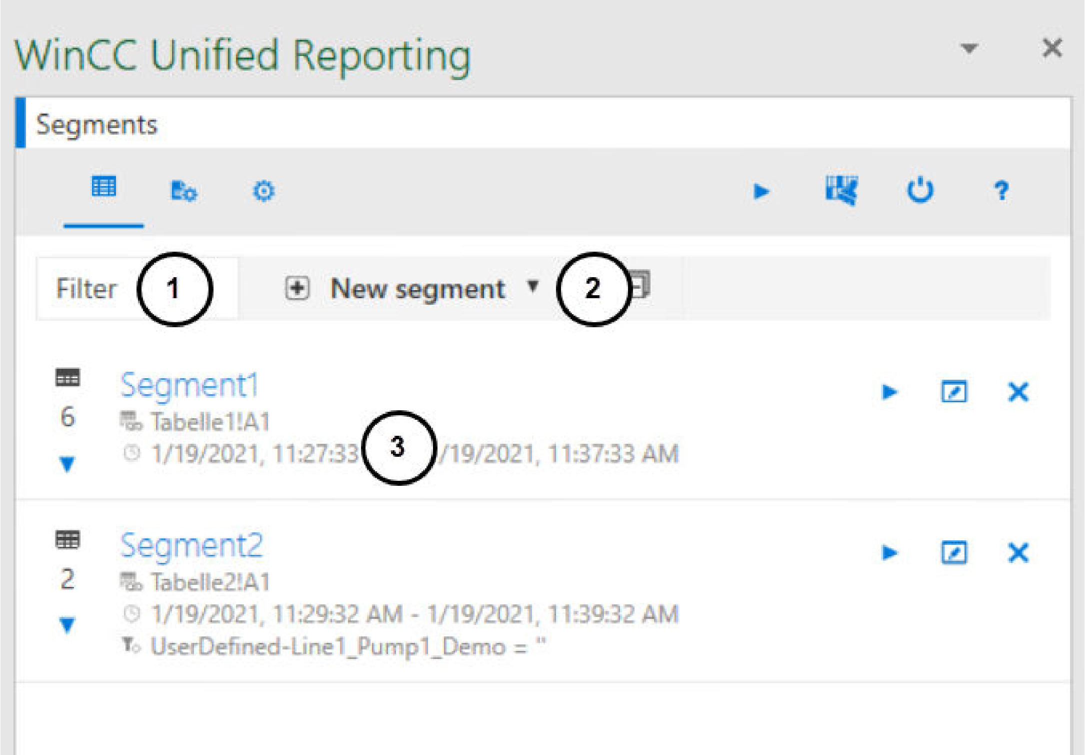
See also

Basic information on segments (Page 237)

The segment user interface

Structure

The interface for creating and editing segments has the following structure:



WinCC Unified Reporting

Segments

Filter

New segment

Segment1
6
Tabelle1!A1
1/19/2021, 11:27:33 … /19/2021, 11:37:33 AM

Segment2
2
Tabelle2!A1
1/19/2021, 11:29:32 AM - 1/19/2021, 11:39:32 AM
UserDefined-Line1_Pump1_Demo = ''

① Filter
Filters the list of segments by name.

② Button for creating a segment

③ List of segments
Each segment has buttons for reading in, editing and deleting the segment.
The following configuration is displayed for each segment:

- Segment name
- Number of data source items
- Insertion location of the segment in the Excel file
- Time span
- If context filters have been configured: The filter string

A click on the segment opens the area with the data source items.

Create segments

Requirement

- The "WinCC Unified" tab is visible in Excel.
- The data source is set up.
- To filter the time interval of the time series segment depending on the context: There are contexts in the project that run on the connected Runtime server or are the basis of the configuration file.

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Click "New segment".
3. Select "New time series segment" or "New single value segment".
4. Enter a segment name.

Note

Note the Excel restrictions for naming tables (for example, do not use blanks).

Change the segment name only via the add-in, not via the Excel property "Table name".

Do not change the name of the worksheet after creating the segment. The add-in addresses the segment by the segment name and the worksheet name.

5. For a time series segment, make the following settings in addition:
   - Under "File location" you determine where the segment will be inserted in the file. Enter the name of the worksheet and the cell.
     Alternatively, click "Select a cell" and use the cell currently selected in the Excel file:

     🔗

   - Under "Start" and "End", you determine the time period for which values are read into the segment.

📅	"Absolute date/ time"	Select a date and a time. The information is absolute to the current date.
🕒	"Relative date/ time"	Select a reference time and a time interval. The information is relative to the current date. See also Formats for relative time information (Page 246).
🔗	"Date/Time of the cell"	Applies the value of the cell currently highlighted in the Excel file. Make sure that the cell supplies a valid time.
🏷	"Date/Time of the tag"	Applies the value of the set tag. Make sure that the tag supplies a valid time. Possible data types: • DateTime • String • Integer

– (Optional) Under "Properties of the legend table", you configure the contents to be displayed in the table header row of the segment:

"Name" "Start" "End" "State"	General information on the segment
"Context filter"	If the segment time was limited by a context filter: The filter string is output. See step 6.
"Audit status"	If the segment has an audit data source item, the field shows the overall status of the audit data: • Green field: No manipulations of the Audit Trail were found in the queried time range. • Red field: Manipulations of the Audit Trail were found in the queried time range. Single or multiple entries have been deleted, added or changed.
"Header"	The table header row includes a list of the segment's data source items showing general information about these data source items. The information displayed for the data source items depends on their type. Example of contexts: Display name of the context, context provider, hierarchy path, short name of the context, full name of the context, option

Use the check boxes to remove information from or add information to the legend table. To change the sorting in the table header row, move the mouse pointer to a row and shift it using the arrow buttons or drag-and-drop.

6. (Optional) You can filter the time interval of the time series segment depending on the context. You can define up to two filter conditions.
   Proceed as follows:
   - Under "Context filter", click "+" or "Add new condition row".
     The condition line is added.
   - Click on "+" in the condition line.
   - Under "Select context", select the root of the common plant model.
     In the next row, you see the top level of the common plant model.
   - Navigate through the common plant model to plant objects with contexts.
     Plant objects and contexts can be recognized by the following icons:

🖧	Plant object
📊	Context

   - Select a context.
   - Select an operator.
   - Enter a value.
   - (Optional) Use "+" or "Add new condition row" to create a second condition and select whether the two conditions are to be linked with a logical AND or OR.
7. (Optional) Under "Autofit", configure whether the column width and row height of the data table is automatically adapted to the text read from Runtime.
8. Confirm your entries with "OK".

Result

The segment is created and added to the list of segments:

Next, add data source items to the segment. Your procedure depends on the type of the new data source item.

See also

Tips on design and layout (Page 282)

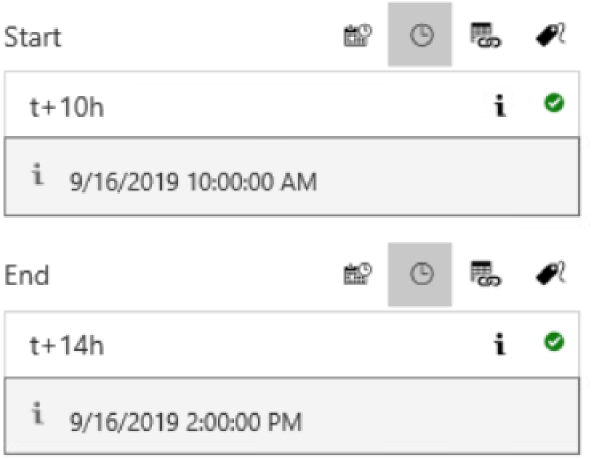
Adding data source items (Page 248)

Working with configurations (Page 260)

Formats for relative time information

Definition of a relative time information

The relative times are entered using a reference time and a time interval.



Start

t+10h

9/16/2019 10:00:00 AM

End

t+14h

9/16/2019 2:00:00 PM

Reference time

Use one of the following characters for the reference time:

- "*" - Now
- "t" (today) - Today at midnight
- "y" (yesterday) - Yesterday at midnight
- "1-31" - Specific day of the current month

Time interval

- "y" (year): +1y = plus 1 year
- "mo" (month): +1mo = plus 1 month
- "w" (week): +1w = plus 1 week
- "d" (day): +1d = plus 1 day
- "h" (hour): +1h = plus 1 hour
- "m" (minute): +1m = plus 1 minute
- "s" (second): +1s = plus 1 second
- "ms" (milliseconds): +250ms = plus 250 milliseconds

Examples

- *-1y: One year ago today
- t+8h: Today at 8:00 am
- y+8h: Yesterday at 8:00 am
- 1+8h: The first day of the current month at 8:00 am
- *-1d: One day ago
- *-2h-30m-30s: 2 hours, 30 minutes and 30 seconds ago

See also

Create segments (Page 242)

Edit segments

Requirement

- The "WinCC Unified" tab is visible in Excel.
- A segment is available.

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Click "Edit" next to a segment in the list of segments.
3. Edit the segment.
   You can make the same settings as when creating the segment.

Delete segments

Requirement

- The "WinCC Unified" tab is visible in Excel.
- A segment is available.

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Click "Delete" next to a segment in the list of segments.
3. Confirm your entries with "OK".

Adding data source items

Adding log alarms

Requirement

- There are logging alarms in the project that runs on the connected Runtime server or is the basis of the configuration file.
- The "Alarm" option is enabled in the connection settings.
- The "WinCC Unified" tab is visible in Excel.
- A time series segment is available.

Adding logging alarms

1. Click on "Segments" in the "Configuration" group.
   The list with the segments already created is loaded into the add-in.
2. Select a segment.
   The segment is extended by the area for the data source items.
3. Click "+".
4. Select the "Alarms" option.
5. Select the "Alarm" entry under "Select alarms".
6. Under "Select alarms", select the entry "Alarm [ID]".

   Note

   Change selection criteria

   After you have added alarms, you can change the selection criteria and add more data source items to the segment.

   For example: Output tags and alarms in the same segment.

7. To cancel your selection, select the entry "Alarm [ID]" under "Selected data source items" and click "Delete".
8. Confirm with "OK".

Result

- The data source item for logging alarms is added to the add-in below the segment.
- The configuration of the data source item controls which data is added when importing the runtime data into the data table.

Note

With the default setting, the data source item uses the default configuration. It shows all logging alarms of the project.

To display data that deviates from the default configuration, select one of the following options:

- Select a different matching configuration.
- Create your own configuration.
- Edit a configuration.
- Overwrite a configuration locally.

See also

Creating or editing configurations for log alarms (Page 260)

Select configuration (Page 271)

Working with configurations (Page 260)

Adding alarm statistics

Introduction

To output statistical calculations for logging alarms in a report, add alarm statistics to a report template. The following calculations are available:

- Frequency of an alarm
- Average display time per state machine
- Total display time per state machine
- Maximum display time per state machine
- Minimum display time per state machine

The alarm statistics add columns with statistical calculations and columns with general alarm properties of the recorded alarms to the reports.

You can find more information about calculations in alarm statistics in the help for the alarm control.

Requirement

- The "Alarm" option is enabled in the connection settings.
- The "WinCC Unified" tab is visible in Excel.
- A time series segment is available.

Procedure

1. Click on "Segments" in the "Configuration" group.
   The list with the segments already created is loaded.
2. Select a time series segment.
   The segment is extended by the area for the data source items.

3. Click "+".
4. Select the "Alarm" option.
5. Under "Select alarms", select the entry "Alarm statistic [ID]".
6. Under "Select alarm statistic" select the entry "Alarm statistic [ID]".

   Note

   Change selection criteria

   After adding the alarm statistics, you can change the selection criteria and add more data source items.

7. (Optional) To cancel your selection, select the entry "Alarm statistic [ID]" under "Selected data source items" and click "Delete".
8. Confirm with "OK".

Result

The added data source item for alarm statistics is displayed below the segment and inserted into the data table.

First, the data table shows the contents configured in the default configuration for alarm statistics. To output other contents, select or create a configuration.

Add logging tags

Requirement

- The project on which the connected Runtime server runs or the basis of the configuration file has logging tags.
- The "Logging tag" option was selected while setting up of the connection.
- The "WinCC Unified" tab is visible in Excel.
- A single value segment or time series segment is available.

Procedure

1. Click on "Segments" in the "Configuration" group.
   The list of segments is loaded.
2. Select a segment.
   The segment is extended by the area for the data source items.
3. Click "+".
4. Select the "Logging tag" option.

5. Optional: To reduce the load time, filter which tags are loaded to the selection under "Add filter".
   The preset filters "*" return all logging tags of the project.
   - "Tag name": Enter the name of the tag whose logging tags you want to add.
   - "Logging tag name": Enter the name of the logging tags you want to add.

   Note that the entry is case-sensitive.

   Note

   Filter by partial string

   You use the wildcard "*" to filter by partial strings.

   For example:
   - *T* returns all tags with a "T" in their name.
   - *T returns all tags that end in "T".
   - T* returns all tags that start with "T".

   When filtering for structures, the separators must be part of the filter string.

   For example: The following filters return the logging tags for all tags of the device "HMI_RT_1":
   - Filter for tag: "HMI_RT_1::*"
   - Filter for logging tag: "*"

6. Click "Load".
   The logging tags of the project are filtered and provided under "Select tags".
7. Optional: Further reduce the number of tags that are offered for selection by clicking next to "Select logging tags" and entering another filter string.
   The list of tags you are being offered is filtered while you type.
8. Select one or more tags under "Select logging tags".
   The tags are added to the "Selected data source items" list.

   Note

   Change selection criteria

   After you have added a tag, you can select a different option or a different filter and add additional data source items.

   For example: Output KPIs and logging tags in the same segment.

9. To remove one or more data source items from "Selected data source items", select them and click "Delete".
10. Confirm with "OK".
    The added logging tags are shown below the segment and added to the Excel table.
11. If you have added the logging tag to a single value segment:
    - In the Excel worksheet, select the cell in which the logging tag is to be inserted.
    - Click the "Select a cell" button on the data source item of the logging tag.
      Alternatively, enter the name of the worksheet and the cell.

See also

Create or edit configurations for logging tags (Page 262)

Working with configurations (Page 260)

Adding tags

Requirement

- The project on which the connected Runtime server runs or the basis of the configuration file has tags.
- The "Tag" option was enabled when the connection was set up.
- The "WinCC Unified" tab is visible in Excel.
- A single value segment is available.

Procedure

1. Click on "Segments" in the "Configuration" group.
   The list of segments is loaded.
2. Select the single value segment.
   The segment is extended by the area for the data source items.
3. Click "+".
4. Select the "Tag" option.
5. Optional: To reduce the load time, filter which tags are loaded to the selection under "Add filter".
   Under "Tag name", enter a filter, e.g. the name of the tag. Note that the entry is case-sensitive.
   The default filter "*" returns all tags of the project.

Note

Filter by partial string

You use the wildcard "*" to filter by partial strings.

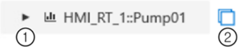
For example:

- *T* returns all tags with a "T" in their name.
- *T returns all tags that end in "T".
- T* returns all tags that start with "T".

When filtering for structures, the separators must be part of the filter string.

For example: The filter "HMI_RT_1::*" returns all tags of the device "HMI_RT_1".

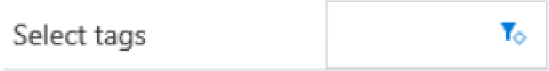
6. Click "Load".
   The tags of the project are filtered and provided under "Select tags".
   You can recognize structs and arrays in the list by the following items:

   ① Button to display the members of the struct or array

   ② "Select all included data source items"
   Button that adds all members with a simple data type to the list of selected data source items

7. Optional: Further reduce the number of tags that are offered for selection by clicking next to "Select tags" and entering another filter string.

   The list of tags you are being offered is filtered while you type.

8. Select which tags will be added to the segment. You have the following options:

Target	Procedure	Result
Show the members of a struct or array.	Click the button with the arrow next to the struct or array.	A second "Select tags" list is added, in which you can see all the members of the struct or array. You can add to the segment any members that have a simple data type, e.g. bool, float or string.
Add all members of a struct or array.	Next to the struct or array, click "Select all included data source items".	All members with a simple data type are added to the "Selected data source items" list and marked as selected under "Select tags":
Select tags with simple data type.	Under "Select tag", click the required tags.	The tags are added to the "Selected data source items" list and marked as selected under "Select tags": HMI_RT_1::@ServerMachineName

Note

Automatic filtering when displaying the members or selection of all members

If you click the button to display the members of a struct or array or activate the option to select their members, the struct or array is set as a filter:

- The list under "Select tags" only shows the struct or array.
- A second "Select tags" list is added below this, in which you can see all members of the struct or array.

To see all available tags again, delete the filters.

Note

Change selection criteria

After you have added a tag, you can select a different option or a different filter and add additional data source items.

9. To remove tags from the segment, click on the tags in "Selected data source items" and click "Delete".
10. Confirm with "OK".

The added tags are added to the segment.

When the report template is updated in the add-in and when the report is generated in runtime, the tag values are inserted into the data table.

See also

Creating or editing configurations for tags: (Page 265)

Working with configurations (Page 260)

Adding contexts

Introduction

To display in a report which contexts are to run during a certain time period, add only contexts to a segment in the report template.

To display which process data has been accumulated during the runtimes of a context, add the context and other data source items, such as logging tags or logging alarms, to the segment.

Requirement

- There are contexts in the project that run on the connected Runtime server or are the basis of the configuration file.
- The "Context" option is enabled in the connection settings.
- The "WinCC Unified" tab is visible in Excel.
- A time series segment is available.

Adding a context to a segment

1. Click on "Segments" in the "Configuration" group.
   The list with the segments already created is loaded.
2. Select a segment.
   The segment is extended by the area for the data source items.
3. Click "+".
4. Select the "Context" option.

5. Select a context:
   - Under "Select a context definition", select the root of the plant model.
     In the next row, you see the top level of the common plant model.
   - Navigate through the common plant model to plant objects with contexts.
     Plant objects and contexts can be recognized by the following icons:

🖧	Plant object
📊	Context

   - Select the desired contexts.
     All selected contexts are included in the "Selected data source items" list

Note

Change selection criteria

After you have added a context, you can select a different option and add additional data source items.

For example: Context and logging tags in the same segment.

6. To remove one or more data source items from "Selected data source items", select them and click "Delete".
7. Confirm with "OK".

Result

The selected contexts are displayed below the segment and inserted into the data table.

If you do not want a context to use the default configuration, select its configuration next.

Content of the data table after executing the segment

In segments to which only contexts or contexts and user-defined columns have been added:

- A line is inserted for each context whose runtime falls within the time period of the segment.
- "Time stamp" column: The time at which the context was started

In segments that combine contexts with logging tags or logging alarms:

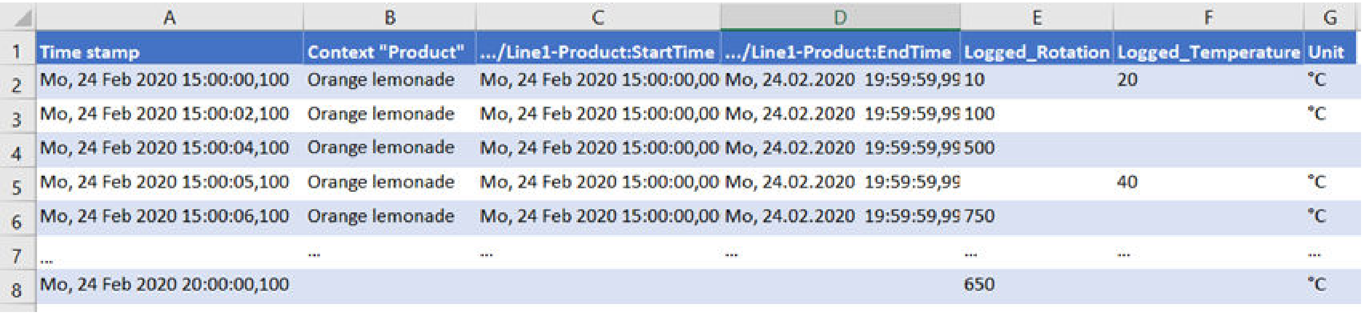
- All logged values with the same time stamp are displayed per row.
- "Time stamp" column: The logging event
- "Start time" column: The time at which the context was started
- "Context " <Context name>"" column: The value passed to the context at start
- If no context was started at the time of logging, the context cells remain empty.

Example

The following data source items were added to a segment:

- The "Product" context
  Runtime of the context: 15:00:00 to 19:59:59 hours
  The context was started with the "Orange lemonade" value.
- The "Logged_Rotation" logging tag
  Logging cycle: 2s
- The "Logged_Temperature" logging tag
  Logging cycle: 5s
- The user-defined "Unit" column
  It contains the unit for "Logged temperatures".

Content of the data table after execution of the segment:



	A	B	C	D	E	F	G
1	Time stamp	Context "Product"	.../Line1-Product:StartTime	.../Line1-Product:EndTime	Logged_Rotation	Logged_Temperature	Unit
2	Mo, 24 Feb 2020 15:00:00,100	Orange lemonade	Mo, 24 Feb 2020 15:00:00,00	Mo, 24.02.2020 19:59:59,99	10	20	°C
3	Mo, 24 Feb 2020 15:00:02,100	Orange lemonade	Mo, 24 Feb 2020 15:00:00,00	Mo, 24.02.2020 19:59:59,99	100		°C
4	Mo, 24 Feb 2020 15:00:04,100	Orange lemonade	Mo, 24 Feb 2020 15:00:00,00	Mo, 24.02.2020 19:59:59,99	500		
5	Mo, 24 Feb 2020 15:00:05,100	Orange lemonade	Mo, 24 Feb 2020 15:00:00,00	Mo, 24.02.2020 19:59:59,99		40	°C
6	Mo, 24 Feb 2020 15:00:06,100	Orange lemonade	Mo, 24 Feb 2020 15:00:00,00	Mo, 24.02.2020 19:59:59,99	750		°C
7	...	...	...	...	...	...	...
8	Mo, 24 Feb 2020 20:00:00,100				650		°C

Lines 2 to 6 Values were logged for "Logged_Rotation" and "Logged_Temperature", while the "Product" context ran with the "Orange lemonade" value.

Line 8 A value was logged for "Logged_Rotation" while no context was running.

See also

Contexts (Page 57)

Adding user-defined columns

Introduction

User-defined columns supplement the data of the other data source items of a time series segment with additional information:

- With a fixed string
  The string appears in each cell of the column.
  Example: Display measurement unit of the tag values in report
- With a formula
  The formula is calculated during generation for each cell in the dynamic column.
  Example: The sum of the tag values output in the report.

The configuration of the user-defined column controls which string or formula it uses.

Requirement

- The "User-defined column" option was enabled when the connection was set up.
- The "WinCC Unified" tab is visible in Excel.
- A time series segment is available.

Procedure

1. Click on "Segments" in the "Configuration" group.
   The list of segments is loaded.
2. Select a segment.
   The segment is extended by the area for the data source items.
3. Click "+".
4. Select the option "User-defined column".
5. Enter the name of the column under "name".
6. Click "Select" or press <ENTER>.
   The column is included in the list "Selected data source items".

   Note

   Change selection criteria

   After you have added a column, you can select a different option or a different filter and add additional data source items.
7. Select a configuration for the user-defined column.
8. To remove one or more data source items from "Selected data source items", select them and click "Delete".
9. Confirm with "OK".

The added columns are displayed below the segment and inserted into the data table.

See also

Creating and editing configurations for user-defined columns (Page 266)

Select configuration (Page 271)

Working with configurations (Page 260)

Add Audit

Introduction

To output the Runtime device Audit Trail in a report, add an Audit data source item to a report template.

You can find more information about the Audit option in WinCC Unified in the Totally Integrated Automation Portal help.

Requirement

- The Audit option was activated in the engineering for the Runtime device.
- The "Audit" option is activated in the connection settings of the Excel add-in.
- The "WinCC Unified" tab is visible in Microsoft Excel.
- A time series segment is available.

Procedure

1. Click on "Segments" in the "Configuration" group.
   The list with the segments already created is loaded.
2. Select a time series segment.
   The segment is extended by the area for the data source items.
3. Click "+".
4. Select the "Audit" option.
5. Select the Audit Trail.
6. (Optional) To undo your selection, select the Audit Trail under "Selected data source items" and click "Delete".
7. Confirm with "OK".

Result

The audit data source item is displayed below the segment.

When an Audit Trail is configured for the data source, the Audit data is added to the report when the Runtime data is read into Microsoft Excel and when it is generated in Runtime:

- In the legend table: Identifier of the overall status of the Audit Trail for the queried time range in the "Audit Status" field

Value	Description
Green	No manipulations of the Audit Trail were found in the queried time range.
Red	Manipulations of the Audit Trail were found in the queried time range. Single or multiple entries have been deleted, added or changed.

Requirement: The "Audit status" option is activated on the segment under "Header properties".

Note

Overall status for check mode "None"

If the check mode "None" is set in the configuration of the audit data sources item, the "Audit status" field is always green.

- In the data table of the segment: Identifier of manipulations

Type of manipulation	Identifier in the data table
Value of entries changed	Directly at the entries
Entries added	
Entries deleted	The manipulated time range receives a start and end entry.

First, the data table shows the contents configured in the standard configuration for Audit. To output other contents, select or create a configuration.

Delete data source elements

Requirement

- The "WinCC Unified" tab is visible in Excel.
- A segment with a data source element is available.

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Expand a segment by clicking on it.
   The area for adding and editing data source elements appears.
3. Move the mouse pointer over a data source element and click "Delete".

Working with configurations

Basics of configuration

The *configuration* of a data source item defines the values of a data source element that are displayed in a segment or how they are calculated and displayed.

There are specific configuration settings for each data-source-item type.

Data source items used in time series segments use a different configuration than data source items used in single-value segments.

You have the following options:

- Use standard configuration.
  There is a standard configuration for all types of data source items. Once added, data source items use the default configuration of their type.
  You can edit the standard configurations.
- Use user-defined configuration.
  You can create any number of user-defined configurations for all types of data source items.
  You can select one of the user-defined configurations on the data source item.
- Overwrite a configuration locally.
  You can overwrite the configuration selected at the data source item locally.

Creating or editing configurations for log alarms

Requirement

- The "WinCC Unified" tab is visible in Excel.

Creating a configuration

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click "New Configuration > Logging alarm configuration".
4. Enter the name of the configuration under "Configuration name".
5. (Optional) Enter texts or graphics from a text list or graphic list in the standard column instead of the alarm IDs.
   See Assigning text lists and graphic lists (Page 274).
6. (Optional) Change the default settings of the optional columns. The optional columns are used to display the alarm properties.
   See Configuring optional columns (Page 272).

7. (Optional) Filter the logging alarms to be displayed. You define a filter query for this purpose. The filter query can consist of up to two conditions.
   Proceed as follows:
   - Under "Filter", click "+" or "Add new condition row".
   - Select an alarm property, an operator, and enter a value.
   - Optional: Use "+" or "Add new condition row" to create additional conditions. Select whether the conditions are to be linked with a logical AND or OR.
8. Enable the option "Use system colors" so that the alarms are highlighted with the same colors as in the alarm control.
9. Confirm your entries with "OK".

Note

To not use the default column title for the standard column, set a display name in the local configuration of the data source item. See Setting a display name for standard column (Page 276).

Editing a configuration

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click a configuration for logging alarms.
4. Edit the configuration settings. You have the same options as when creating the configuration.
5. Confirm your entries with "OK".

The changes are applied the next time you read in the Runtime data.

Creating or editing configurations for an alarm statistics

Requirement

- The "WinCC Unified" tab is visible in Excel.

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click "New Configuration > Alarm statistics configuration".

4. Enter the name of the configuration under "Configuration name".
5. (Optional) Enter texts or graphics from a text list or graphic list in the standard column instead of the alarm IDs.
   See Assigning text lists and graphic lists (Page 274).
6. (Optional) Change the default settings of the optional columns. The optional columns are used to display the statistical calculations and alarm properties.
   See Configuring optional columns (Page 272).
7. (Optional) Filter the contents to displayed in the alarm statistics. You define a filter query for this purpose. The filter query can consist of up to two conditions.
   Proceed as follows:
   – Under "Filter", click "+" or "Add new condition row".
   – Select an alarm property, an operator, and enter a value.
   – Optional: Use "+" or "Add new condition row" to create additional conditions. Select whether the conditions are to be linked with a logical AND or OR.
8. Enable the option "Use system colors" so that the alarms are highlighted with the same colors as in the alarm control.
9. Confirm your entries with "OK".

Note

To not use the default column title for the standard column, set a display name in the local configuration of the data source item.

See Setting a display name for standard column (Page 276).

Editing a configuration

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click a configuration for alarm statistics.
4. Edit the configuration settings. You have the same options as when creating the configuration.
5. Confirm your entries with "OK".

The changes are applied the next time you read in the Runtime data.

Create or edit configurations for logging tags

Requirement

- The "WinCC Unified" tab is visible in Excel.

Creating a configuration

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click "New Configuration".
4. To create a configuration for logging tags in a time series segment, select the entry "Logging tag configuration".
   To create a configuration for logging tags in a single value segment, select the entry "Single value configuration logging tag".
5. Enter the name of the configuration under "Configuration name".
6. Under "Calculation mode", select the data to be written if no current value is available.
7. (Optional) If the configuration is for logging tags with the numeric data type, you can output texts or graphics from a text list or graphic list in the standard column instead of the tag value. See Assigning text lists and graphic lists (Page 274).
8. Set the other settings as described below.
9. Confirm your entries with "OK".

Note

To not use the default column title for the standard column, set a display name in the local configuration of the data source item. See Setting a display name for standard column (Page 276).

Editing a configuration

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click a configuration for logging tags.
4. Edit the configuration settings.
5. Confirm your entries with "OK".

The changes are applied the next time you read in the Runtime data.

Additional settings for time series segments

In time series segments, the following additional settings are available for logging tags:

Setting	Description
"Interval"	Only for the "Stepped" and "Interpolated" calculation modes.
"Columns" > "Quality Code"	(Optional) Change the default settings of the optional "Quality Code" column. See Configuring optional columns (Page 272).

Additional settings for single value segments

In single value segments, the following additional settings are available for logging tags:

Setting	Description
"Time stamp"	Determine the date and time for which the value is read. Proceed as described below.
"Show captions"	Define whether a header is displayed in the columns for the time stamp, the data source item and the quality code.
"Show time stamp"	Determine whether and where this information is displayed in the table. The information is always in relation to the value cell.
"Show data source item"	
"Show quality code"	

To set the "Time stamp", select one of the following options:

📅	Absolute time information	Select a date and a time. The information is absolute.
🕒	Relative time information	Select a reference time and a time interval. The information is relative to the current date.
🔗	Read time information from cell	Applies the value of the cell currently highlighted in the Excel file. Make sure that the cell supplies a valid time.
🏷	Read time information from tag	Applies the value of the set tag. Make sure that the tag supplies a valid time. Possible data types: • DateTime • String • Integer

See also

Calculation modes for data source elements (Page 281)

Creating or editing configurations for tags:

Requirements

- The "WinCC Unified" tab is visible in Excel.

Creating a configuration

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click "New Configuration> Tag single value configuration".
4. Enter the name of the configuration under "Name".
5. (Optional) If the configuration is for tags with the numeric data type, you can output texts or graphics from a text list or graphic list in the standard column instead of the tag value. See Assigning text lists and graphic lists (Page 274).
6. Set the other settings as described below.
7. Confirm your entries with "OK".

Note

To not use the default column title for the standard column, set a display name in the local configuration of the data source item. See Setting a display name for standard column (Page 276).

Editing a configuration

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration".
3. Click a configuration for tags.
4. Edit the configuration settings.
5. Confirm your entries with "OK".

The changes are applied the next time you read in the Runtime data.

Settings for single value segments

In single value segments, the following settings are available for tags:

Setting	Description
"Show captions"	Select whether a header is displayed in the columns for the time stamp, the data source item and the quality code.
"Show time stamp"	Select whether the time stamp is output with the value.
"Show data source item"	Select whether the data source element is also output.
"Show quality code"	Select whether the quality code is output with the value.

Creating or editing configurations for contexts

Requirement

- The "WinCC Unified" tab is visible in Excel.

Core statement

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click "New Configuration".
4. Select the entry "Configuration context".
5. Enter the name of the configuration under "Configuration name".
6. (Optional) Change the default settings of the optional columns. The optional columns are used to display important contextual information.
   See Configuring optional columns (Page 272).
7. Confirm your entries with "OK".

Note

To not use the default column title for the standard column, set a display name in the local configuration of the data source item. See Setting a display name for standard column (Page 276).

Editing a configuration

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click a configuration for contexts.
4. Edit the configuration settings.
5. Confirm your entries with "OK".

The changes are applied the next time you read in the Runtime data.

Creating and editing configurations for user-defined columns

Requirement

- The "WinCC Unified" tab is visible in Excel.

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click "New Configuration > User-defined column configuration".
4. Enter the name of the configuration under "Configuration name".
5. Under "Formula", select one of the following options:
   - Enter a fixed string.
     The string is transferred into each cell of the column.
   - Enter an Excel formula.
     The formula is copied into each cell of the user-defined column and adapted to the respective row.
     To prevent a part of the formula from being adjusted, place the character "$" in front of it.
     Example

Formula in configuration		=B2+C2	=B$2+C2
Adapting the formula in the report	in line 2	=B2+C2	=B2+C2
	in line 3	=B3+C3	=B2+C3
	in line 4	=B4+C4	=B2+C4

Note

No validity check

The formula is not tested for correctness during either input or dynamic adaptation.

6. Confirm your entries with "OK".

Adding or editing configurations for audit

Introduction

Check mode

The check mode of the configuration of an audit data source item determines

- Whether an integrity check is performed when the Runtime data is read, and what is checked.
  You can output the overall result of the check in the table header row in the "Audit status" field.
- Which audit data records are provided in the data table.

Possible check modes:

"None"	Provides the data for all audit data records that fall within the requested time range. No integrity check is carried out. Default setting
"Check only"	Checks all audit data records that fall within the requested time range without providing their data. It is tested whether data records have been manipulated, deleted or added.
"Check entries"	Checks the audit data records. Provides the data that falls within the queried time range and that was not deleted from the Audit Trail or added later. It is checked whether data records have been manipulated.
"Check all"	Checks all audit data records. Provides the data that falls within the queried time range. It is tested whether data records were manipulated, deleted from the audit trail or subsequently added.

Filter type

An audit data record consists of two entries:

- An entry for the user expectation
- An entry for the system response.

User expectation and system response may differ. In addition, there are situations in which only one of the two data records is created.

The filter type controls which data records and which entries are included in the report.

Possible filter types:

Filter type	User expectation equals system response	User expectation does not equal system response	Data record entry for user expectation or system response is missing
"Show all data in detail"	Both data record entries are inserted.		The existing data record entry is inserted.
"Show data and conformity errors"	The data record entry with the user expectation is inserted.	Both data record entries are inserted.	
"Show only data with conformity errors"	No data record entry inserted.		

Requirement

- The "WinCC Unified" tab is visible in Excel.

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click "New Configuration > Audit configuration".
4. Enter the name of the configuration under "Name".

5. Select a check mode:
6. Specify a filter type.
   Preset value: "Show data and conformity errors"
7. (Optional) Change the default settings of the optional columns. The optional columns are used to display the audit attributes.
   You can find more information on configuring the optional columns in the WinCC Unified object model > Creating production logs > Configuring optional columns.
8. (Optional) To further filter the inserted content, define a filter query.
   The filter query can consist of up to two conditions. Proceed as follows:
   – Under "Filter", click "+" or "Add new condition row".
   – Select an Audit attribute, an operator and enter the value of the attribute.
   – Optional: Use "+" or "Add new condition row" to create additional conditions. Select whether the conditions are to be linked with a logical AND or OR.
9. Confirm your entries with "OK".

Note

To not use the default column title for the standard column, set a display name in the local configuration of the data source item. You can find more information on setting the display name in the WinCC Unified object model > Creating production logs > Setting the display name for the standard column.

Editing a configuration

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration":
3. Click a configuration for Audit.
4. Edit the configuration settings. You have the same options as when creating the configuration.
5. Confirm your entries with "OK".

The changes are applied the next time you read in the Runtime data.

Examples of the configuration of the filter type

The following table contains examples of data records that were generated in Runtime through changes to tags monitored by Audit:

Data record ID	Tag name	Modified by	Old value	New value	Description
1A	Motor1_Speed	User1	0	10	An operator changes the speed of a motor in an I/O field of an HMI screen. User expectation and system response are identical.
1B	Motor1_Speed	System	0	10	
2A	ValvePercentile	User1	0	100	An operator opens a valve using a slider on an HMI screen. The valve has a physical blockage and cannot be opened. Therefore, no data record entry for the system response is generated.
3A	ValvePercentile	User1	0	99	A physical block has been removed and the operator repeats the entry. The valve reacts, but cannot be fully opened. User expectation and system response differ.
3B	ValvePercentile	System	0	49	
4B	Motor2_Speed	System	0	20	An operator changed the speed of another motor. The resulting data record was manipulated, and the user expectation entry was deleted. There is only one entry for the system response.

The following table shows which data record entries are inserted into the data table depending on the filter type selected when generating the report:

Data record ID	Tag name	Modified by	Old value	New value
Filter type "Show all data in detail"				
1A	Motor1_Speed	User1	0	10
1B	Motor1_Speed	System	0	10
2A	ValvePercentile	User1	0	100
3A	ValvePercentile	User1	0	99
3B	ValvePercentile	System	0	49
4B	Motor2_Speed	System	0	20
Filter type "Show data and conformity errors"				
1A	Motor1_Speed	User1	0	10
2A	ValvePercentile	User1	0	100
3A	ValvePercentile	User1	0	99
3B	ValvePercentile	System	0	49
4B	Motor2_Speed	System	0	20
Filter type "Show only data with conformity errors"				
2A	ValvePercentile	User1	0	100
3A	ValvePercentile	User1	0	99
3B	ValvePercentile	System	0	49
4B	Motor2_Speed	System	0	20

See also

Configuring optional columns (Page 272)

Setting a display name for standard column (Page 276)

Select configuration

Requirement

- The "WinCC Unified" tab is visible in Excel.
- A segment with a data source item is available.
- There is a user-defined configuration for the type of the data source item.

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Select the segment.
   The segment is extended by the area for the data source items.
3. Select the desired configuration from a data source item in the drop-down list.
4. Click "OK".

Result

The changes are applied the next time you read in the runtime data.

Overwrite a configuration locally

A local configuration overwrites the configuration selected at the data source item. It applies only to the data source item for which it was entered.

Requirement

- The "WinCC Unified" tab is visible in Excel.
- A segment with a data source item is available.

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Select the segment.
   The segment is expanded to include the plant complex for the data source items.
3. Move the mouse over a data source item and click "Edit".
   You create a local configuration that first adopts the values of the original configuration.
4. Enter a name for the local configuration.

5. (Optional) Set a display name. See Setting a display name for standard column (Page 276).
6. Make the remaining settings as required.
   You can make the same settings as in the default and custom configurations.
7. Confirm your entries with "OK".

Result

The changes are applied the next time you read in the Runtime data.

Delete configuration

Requirement

A configuration is available.

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Click "Data source item configuration".
3. Move the mouse to a configuration.

   Note

   Default configurations cannot be deleted

   You can edit default configurations but not delete them.

4. Click "Delete".

Result

- The configuration is deleted.
- Data source items with this configuration obtain a local configuration with the same settings.

Configuring optional columns

Introduction

In time series segments, data source items of the following types have optional columns:

- Logging tag
- Logging alarm
- Alarm statistics
- Audit
- Context

The optional columns of a data source item depend on its type. The configuration of the data source items controls whether and how the data table shows these columns.

This section describes how to configure the optional columns.

Requirements

The data source item configuration is open. The configuration must apply to a time series segment.

Showing and hiding columns

1. To show an optional column in the data table, enable the option for the desired column in the "Columns" area.
2. To hide a column, disable its option.

Changing the column title

The data table uses as default column titles the identifiers you see in the "Columns" area. To change the default column titles, do the following.

1. In the "Columns" area, move the mouse pointer to an optional column.
2. Click the button with the pin.
3. Assign a unique column title.

Note

Localization

The column title is stored in the Runtime language currently set in the basic settings of the add-in.

To localize the column title, change the Runtime language and repeat your entry in the new language.

Changing the column sequence

To change the order of the optional columns in the data table, proceed as described in Changing the column sequence (Page 277).

Assigning text list or graphic list

The values of numeric columns can be replaced by texts or graphics when the Runtime data is read in.

To assign a suitable text list or graphic list to the property, proceed as described in Assigning text lists and graphic lists (Page 274).

Assigning text lists and graphic lists

Introduction

If standard columns and optional columns of data source items output numerical values, you can assign text lists and graphic lists to these columns. When the Runtime data is read in, the cell values of these columns are replaced by texts or graphics from the assigned lists.

This function improves the readability of the report and helps to draw the reader's attention to important information.

Note

Restrictions

- Tags/logging tags
  Assign a text list or graphic list to the standard column of data source items with a Tag or Logging tag type only if the tag or logging tag has a numeric data type.
  You can assign a text list or graphic list to the optional "Quality Code" column regardless of the data type of the tag.
- User-defined columns
  It is not possible to assign a text list or graphic list for data source items with the User-defined column type.
- Context and audit
  Usually, the names of context objects and audit objects displayed in the standard column do not contain purely numerical values. It is not recommended to assign a text list or graphic list.

Example

Add two data source items with the same logging tag to a time series segment.

For the first data source item, use the default configuration. This causes the report to output the tag value in the standard column.

For the second data source item, select a configuration in which a graphic list is assigned to the standard column. The graphic list contains representational graphics staggered by value range. As a result, the report outputs a graphic in the standard column.

After reading in the Runtime data, the standard column of the second data source item makes readers of the report aware of limit violations. Readers can get the exact tag value from the standard column of the first data source item.

Requirements

- A segment with a data source item was created in the add-in.
- Suitable text lists or graphic lists have been configured in engineering for the connected data source.

Assigning text lists and graphic lists to the standard column

1. Click on "Segments" in the "Configuration" group.
2. Select the segment.
   The data source items of the segment are displayed.
3. Move the mouse over a data source item and click "Edit".
   The local configuration of the data source item opens.
4. Select a suitable list under "Assign text/graphic list".
5. To preview the selected list and its graphics or texts, click the "i" button.
   To hide the preview, click the "i" button again.

Assigning optional columns to text lists and graphic lists

1. Click on "Segments" in the "Configuration" group.
2. Select one of the following options:
   To make the assignment apply to a specific data source item, follow these steps:
   - Select the segment.
     The data source items of the segment are displayed.
   - Move the mouse over the data source item and click "Edit".
     The local configuration of the data source item opens.

   To make the assignment apply to multiple data source items of the same type, follow these steps:
   - Click "Data source item configuration": ⚙
     You can see all default and custom configurations.
   - Click on the desired configuration.
     The configuration opens.
3. In the "Columns" area, click the following button next to the desired optional column:
   ⚙

   An interface for assigning a text list or graphic list is loaded into the add-in.
4. Select the desired graphic list or text list from the drop-down list.
5. To preview the selected list and its graphics or texts, click the "i" button.
   To hide the preview, click the "i" button again.

   Note

   If you are connected offline to the data source, no preview of graphic lists is available.
6. Confirm your entries.

Result

When the Runtime data is read in, the assigned lists are searched for an entry that matches the actual cell value:

- If a matching entry is found, the corresponding text or graphic is inserted into the data table.
- If no matching entry is found, the actual cell value is inserted.

Note

The assignment of graphic lists slows down the import of the Runtime data into the Excel add-in.

See also

Standard column (Page 239)

Basic information on segments (Page 237)

Setting a display name for standard column

Introduction

You can assign a display name for the standard column of a data source item. When a display name is set, it is used in the data table instead of the default column title and is listed in the table header row.

Display names make reports clearer, for example, when data source items for contexts or tags have very long names.

You set the display name in the local configuration of the data source item.

Requirement

- The "WinCC Unified" tab is visible in Excel.
- There is a segment with a matching data source item.

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Expand a segment by clicking on it.
   The area for adding and editing data source elements appears.
3. Move the mouse pointer to the data source item and click "Edit".
   The local configuration of the data source item opens.

4. Enter the desired column title in "Display name".
   The column title must be unique within the segment.

   Note

   Localization

   The column title is stored in the Runtime language currently set in the basic settings of the add-in.

   To localize the column title, change the Runtime language and repeat your entry in the new language.

5. Confirm your entry with "OK".

Result

- The data table uses the display name as the column title for the standard column of the data source item.
- As long as the following conditions are met, the "Display name" column is inserted into the table header row:
  - Display of the header row in table header row is enabled.
    Make this setting at the segment.
  - A display name is set for at least one data source item of the segment.

  The column lists the display names of all data source items. If no display name is set for a data source item, its cell remains empty.

Note

- If you assign a different configuration to the data source item, the display name is retained.
- To return to the display of the default column title after assigning a display name, enter the name of the data source item under "Display name".

See also

Standard column (Page 239)

Overwrite a configuration locally (Page 271)

Changing the column sequence

Introduction

For a time series segment, you can change the default column order of the data table.

You have the following options:

- Specify the order which the data source items have in the data table.
- For each data source item: Set the order of its optional columns.

Note

The time stamp column always appears first.

Requirement

- The "WinCC Unified" tab is visible in Excel.
- A time series segment has been created.

Change the order of data source items

Procedure

1. Click on "Segments" in the "Configuration" group.
2. Click the time series segment in the list of time series segments.
   The data source items of the segment are displayed.
3. Left-click a data source item and move it up or down using drag-and-drop operation.

Result

The order of data source items in the segment interface is changed.

The next time the Runtime data is read in, the data table outputs the data source items in this order.

Changing the order of optional columns

Procedure

1. Select one of the following options:
   To change the column order of a particular data source item, follow these steps:
   - Select the segment.
     The data source items of the segment are displayed.
   - Move the mouse over the data source item and click "Edit".
     The local configuration of the data source item opens.

   To change the column order for all data source items that use the same configuration, follow these steps:
   - Click "Data source item configuration":

     You can see all default and custom configurations.
   - Click on the desired configuration.
     The configuration opens.
2. Move the mouse pointer to a column under "Columns".
   The columns you see depend on the type of data source item.
3. Move the column up or down using the arrow buttons or drag-and-drop.

Result

The order of the optional columns in the configuration is changed.

The next time the Runtime data is read in, the data table outputs the optional columns in the changed order.

See also

Basic information on segments (Page 237)

Configuring optional columns (Page 272)

Reading Runtime data in Excel

Note

Reading in Runtime data in Excel is used for testing. It is not intended for mass retrieval of data, as is the case when report jobs are executed in Runtime.

Requirement

An online connection is established.

Reading in all segments

1. Select "WinCC Unified > Segments".
2. Click "Update all":

   ▶

Reading in individual segments

1. Select "WinCC Unified > Segments".
2. Next to a segment in the list of segments click, "Update":

   ▶

Result

The segment or segments are run. The Runtime data of your data source items are read into Excel.

Note

Controlling the column width and row height

When the automatic adjustment of the column width and row height is disabled in the segment properties, the text read in may be truncated or the formula results are replaced with "#" characters.

Check the column widths and row heights and adjust them manually, if required, or select automatic adjustment. Manual adaptations only apply in the Excel add-in. They are not included in the generated reports.

Note

Removing Runtime data from report template

Remove the Runtime data from the report template before you save the report template and make it available for uploading to Runtime.

To do this, click the "Delete Runtime data" button in the toolbar of the Excel add-in.

Diagnostics during the data query

Successful execution of the data query is documented by the add-in with a status message in the table.

If an error occurs during the data query, a general error message is displayed under status. In addition, detailed error messages are displayed in the "ErrorLog" worksheet.

Calculation modes for data source elements

If there is no current value for a data source item for a requested point in time, the following calculation modes are available.

Calculation modes for tags

The following calculation modes are available for tags of a time series segment:

Calculation mode	Description
Raw	The actual value available for the specified period. If no data are available, no value is output.
Stepped	If no data are available, the last value is used. With this mode you can also use values with an invalid quality code.
Interpolate	The values are interpolated linearly for the specified time period. With this mode you can only use values with a valid quality code.

The following calculation modes are available for tags of a single value segment:

Calculation mode	Description
Interpolate	The values are interpolated linearly for the specified time period. With this mode you can only use values with a valid quality code.
Left	If no data is available, the last value before the specified period is used.
Right	If no data is available, the last value after the specified period is used.

See also

Create or edit configurations for logging tags (Page 262)

Making general settings

Adapting the work area

Undocking and moving the add-in

To enlarge your working area, you can undock the Excel add-in:

1. Open the drop-down list in the header of the add-in.
2. Click "Move".
3. Move the mouse pointer to the desired location and click the left mouse button.
4. To move the add-in again, keep the left mouse button pressed in the header of the add-in and move the mouse.
5. To dock the add-in again, double-click in the header of the add-in.

Adapting the size of the add-in

1. Open the drop-down list in the header of the add-in.
2. Click "Resize".
3. Move the mouse pointer to the left to make the add-in wider or to the right to make it narrower.
4. Left-click when you have reached the desired size.

Changing the language

Changing the add-in language

The Excel add-in automatically uses the same user interface language as Excel. If you are using a language for Excel that is not included in the Unified options, English is used as the default language.

You can select the language for the contents of the report independently of the interface. To select another language, the language must be configured in Runtime.

Selecting the language for the report

1. Select "WinCC Unified > Segments".
2. Click "Basic settings":

   ⚙
3. Under "Runtime language", select the language of the report content.
4. Under "Query language" you select which language data queries have that require user input, e.g. filter definitions.

Zooming in the add-in

Procedure

To zoom in or out of the display in the add-in, press <CTRL> and move the mouse wheel.

Undo and redo

The Excel functions "Undo" and "Redo" are not available in the add-in.

Tips on design and layout

This section includes tips on the visual design of reports. The apply for:

- Report templates
- Reports that were generated as XLSX file

Note

Deviating PDF results

A PDF report created by LibreOffice can deviate in content or layout from a PDF report generated with Excel, for example, if the report template uses common Excel features that LibreOffice does not support, such as special fonts or chart types.

Arranging segments

Always place the segments of a report template side by side or each in their own worksheet.

Because the data tables of the segments grow dynamically, tables can overlap when segments are placed one below the other. In the add-in, this causes an error of the OfficeExtension.Error class when reading in the Runtime data.

Changing the column sequence

See section Changing the column sequence (Page 277).

Adapt column width and row height

For each segment of a report template, check whether the column widths and row heights of your data table are wide or high enough for the values to be read. If this is not the case, texts in the generated report are truncated or the formula results are replaced with "#" characters.

To do this, select one of the following options:

- In the properties of the segments, select the options for automatic adjustment of the column width and row height.
- Click "Update all" ▶ in the report template.
  Values are imported to Excel from the data source. Check the column widths and row heights and adjust them manually, if required.

  Note

  The manual adaptations apply only in the Excel add-in. They are not included in the generated reports.

Replacing numerical values

If columns of a data source item output numeric values, you can assign text lists and graphic lists to the columns. When the Runtime data is read in, the cell values of these columns are replaced by texts or graphics from the assigned lists. This improves the readability of the report and helps to draw the reader's attention to important information.

Example: Visualizing limit violations of tags with graphics

See section Assigning text lists and graphic lists (Page 274).

Preparing imported Runtime data

Adjust the cell formatting of the Runtime data, for example, font, color, alignment, or number format. The rows inserted when reading the Runtime data adopt the formatting.

Add diagrams, pivot tables or formulas that graphically visualize, structure or evaluate the data imported from Runtime.

Note

If you have read Runtime data into the report template for better data preparation, remove it before saving the report template and making it available for upload to Runtime.

To do this, click the "Delete Runtime data" button in the toolbar of the Excel add-in.

Set up page

Use "File > Print > Set up page" to define details for printing the report, for example:

- Alignment of the report (portrait format or landscape format)
- Scaling, for example, to print all columns on one page
- Inserting a user-defined header or footer

The print settings set in the report template are applied in Runtime when a report job is executed for PDF generation.

Renaming worksheets and segments

When you add a segment to a report template in the add-in, a table is created in Excel. The add-in addresses the table by the name of the worksheet and segment.

Do not rename worksheets after adding segments.

Do not change the table name of a segment using the Excel property "Table name". Edit the segment in the add-in and rename it there.

3.4.12 Rearranging columns at runtime

Introduction

You can rearrange the table columns in the following table-based controls:

- Alarm control
- Trend companion
- Process control
- Parameter set control
- System diagnostics control

Requirement

Configuration of the control in the engineering requires rearrangement of the columns.

Procedure

To move a column, drag-and-drop its column header onto the column header of another column.

Note

The time column cannot be moved.

Result

The moved column is inserted at the position that the cursor had when the drag-and-drop movement ended.

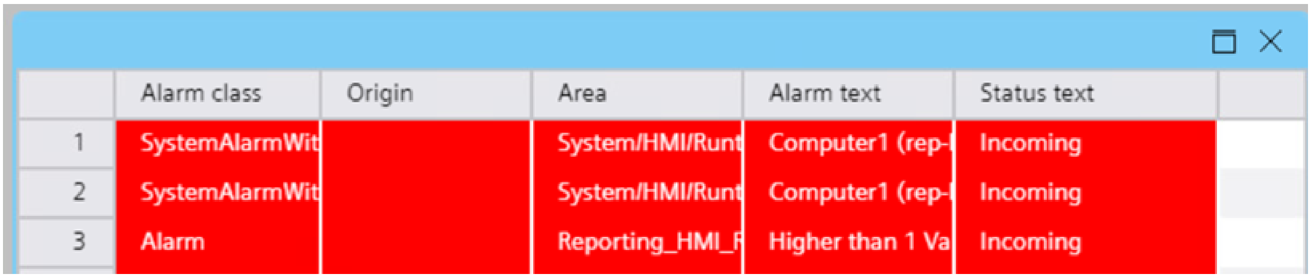
The new arrangement only applies to the current client. If you change the page or refresh the browser window, the arrangement is lost.

Note

If you move a column next to the hidden column and then unhide it, it is always shown to the right of the moved column when it is unhidden.

Example 1: Inserting columns to the left or the right

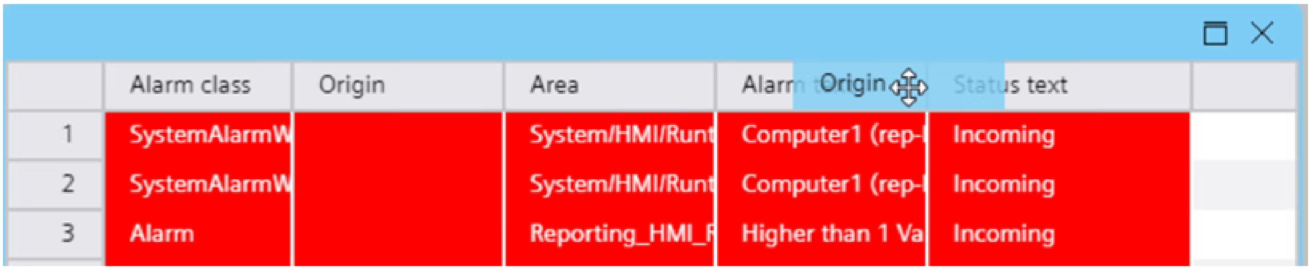
The procedure is illustrated based on the example of an alarm control. In the initial situation, the table of the alarm control has the following column arrangement:



	Alarm class	Origin	Area	Alarm text	Status text
1	SystemAlarmWit		System/HMI/Runt	Computer1 (rep-	Incoming
2	SystemAlarmWit		System/HMI/Runt	Computer1 (rep-	Incoming
3	Alarm		Reporting_HMI_F	Higher than 1 Va	Incoming

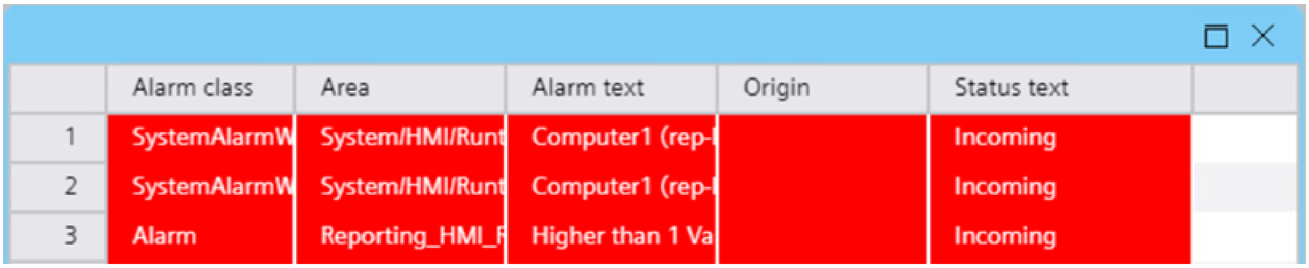
To insert the "Origin" column to the right of the "Alarm text" column, proceed as follows:

1. Use drag-and-drop to move the column header of "Origin" to the right half of the column header of the "Alarm text" column.



	Alarm class	Origin	Area	Alarm Origin	Status text	
1	SystemAlarmW		System/HMI/Runt	Computer1 (rep-I	Incoming	
2	SystemAlarmW		System/HMI/Runt	Computer1 (rep-I	Incoming	
3	Alarm		Reporting_HMI_F	Higher than 1 Va	Incoming	

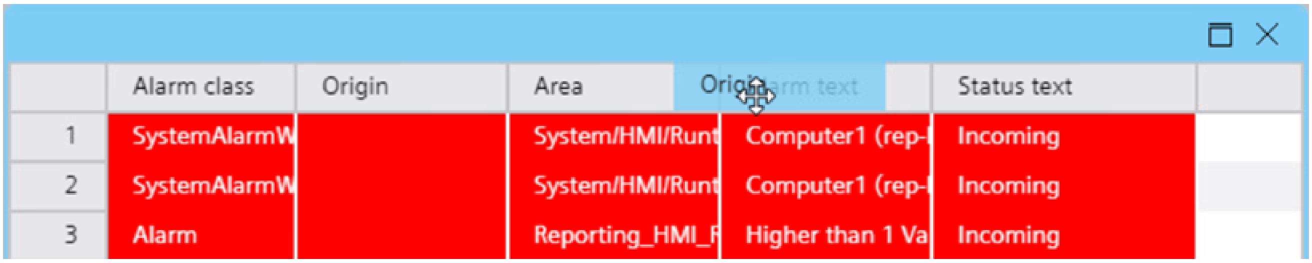
2. The "Origin" column is inserted to the right of the "Alarm text" column.



	Alarm class	Area	Alarm text	Origin	Status text	
1	SystemAlarmW	System/HMI/Runt	Computer1 (rep-I		Incoming	
2	SystemAlarmW	System/HMI/Runt	Computer1 (rep-I		Incoming	
3	Alarm	Reporting_HMI_F	Higher than 1 Va		Incoming	

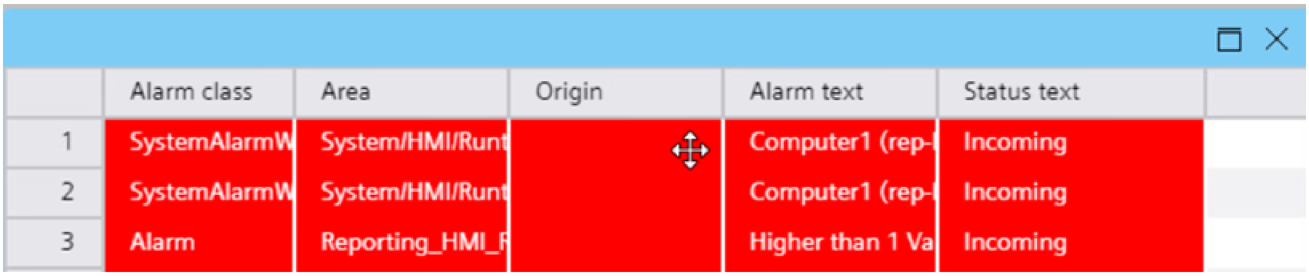
To insert the "Origin" column to the left of the "Alarm text" column, proceed as follows:

1. Use drag-and-drop to move the column header of "Origin" to the left half of the column header of the "Alarm text" column.



	Alarm class	Origin	Area	Origin rm text	Status text	
1	SystemAlarmW		System/HMI/Runt	Computer1 (rep-I	Incoming	
2	SystemAlarmW		System/HMI/Runt	Computer1 (rep-I	Incoming	
3	Alarm		Reporting_HMI_F	Higher than 1 Va	Incoming	

2. The "Origin" column is inserted to the left of the "Alarm text" column.



	Alarm class	Area	Origin	Alarm text	Status text	
1	SystemAlarmW	System/HMI/Runt		Computer1 (rep-I	Incoming	
2	SystemAlarmW	System/HMI/Runt		Computer1 (rep-I	Incoming	
3	Alarm	Reporting_HMI_F		Higher than 1 Va	Incoming	

Example 2: Reordering of columns in combination with hidden columns

The example illustrates the rearrangement of columns in combination with hidden columns.

- The alarm view has the same column order as in Example 1.
- The alarm view has been configured in the engineering system in such a way that the display of the "Origin" column is controlled dynamically in runtime by setting a tag.

To reorder the columns in combination with hidden columns, proceed as follows:

1. Hide the "Origin" column by setting the tag.
2. Insert the "Status text" column to the left of the "Area" column.
3. Unhide the "Origin" column by setting the tag.

The columns have the order "Alarm class", "Status text", "Origin", "Area", "Alarm text".

3.4.13 Process diagnostics

3.4.13.1 Basics of supervision with ProDiag

Introduction

The TIA Portal functionality, ProDiag (Process Diagnostics), is used to monitor and determine errors that occur in your plant or machine. You can use ProDiag to show the type of error, the cause of the error and the location of the error on the HMI device.

Use

You can use ProDiag functions to monitor your plant and to visualize it on an HMI device. The main objective of ProDiag is the reduction of downtime and loss of production after an error occurs, and the avoidance of errors using timely warnings. Diagnostic and display objects provide specific information for the operator for troubleshooting and show the processes on an HMI device on site.

Principle

In STEP 7, you create operand supervisions and configure the settings according to your requirements. When an error occurs, a supervision alarm is generated based on the criteria you have configured. The configured supervision instances are stored in the preset ProDiag function block. You can use the automatically generated ProDiag FBs or create and configure your own ProDiag FBs according to technological aspects.

Advantages

ProDiag enables you to configure supervisions and monitor your plant without changing the user program code.

You perform plant diagnostics on your HMI device. The data is automatically synchronized in order to keep the display on your HMI device always up-to-date.

3.4.13.2 Requirements and licensing

Introduction

You configure the ProDiag supervisions in TIA Portal with STEP 7 and create the screen objects for monitoring and diagnostics with WinCC. You need a license to use the ProDiag functionality and the corresponding screen objects.

Software requirements

You need the following products to configure ProDiag supervisions and visualization on the HMI device:

- TIA Portal STEP 7 Professional
- WinCC Unified

Hardware requirements

ProDiag functionality is available for CPUs of the S7-1500 series with firmware version 2.0 or higher.

The objects for the supervision and diagnostics of plants are available for the following HMI devices:

- WinCC Unified

Note

Objects for supervision and diagnostics of plants can be used under the "Full access" and "Read access" protection levels configured in the CPU.

ProDiag objects under the "HMI access" and "No access" protection levels cannot be used.

Licensing of ProDiag supervisions

The number of ProDiag monitors that you configure with STEP 7 is licensed. You do not need a license for the first 25 supervisions, licenses must be used for additional supervisions.

Number of supervisions	<= 25	<= 250	<= 500	<= 750	<= 1000	> 1000 *)
Number of licenses	None	1	2	3	4	5

*) If it is clear from the beginning that > 1000 supervisions are required in the project, a license to use supervisions can be ordered without limitation.

Licensing of ProjDiag objects

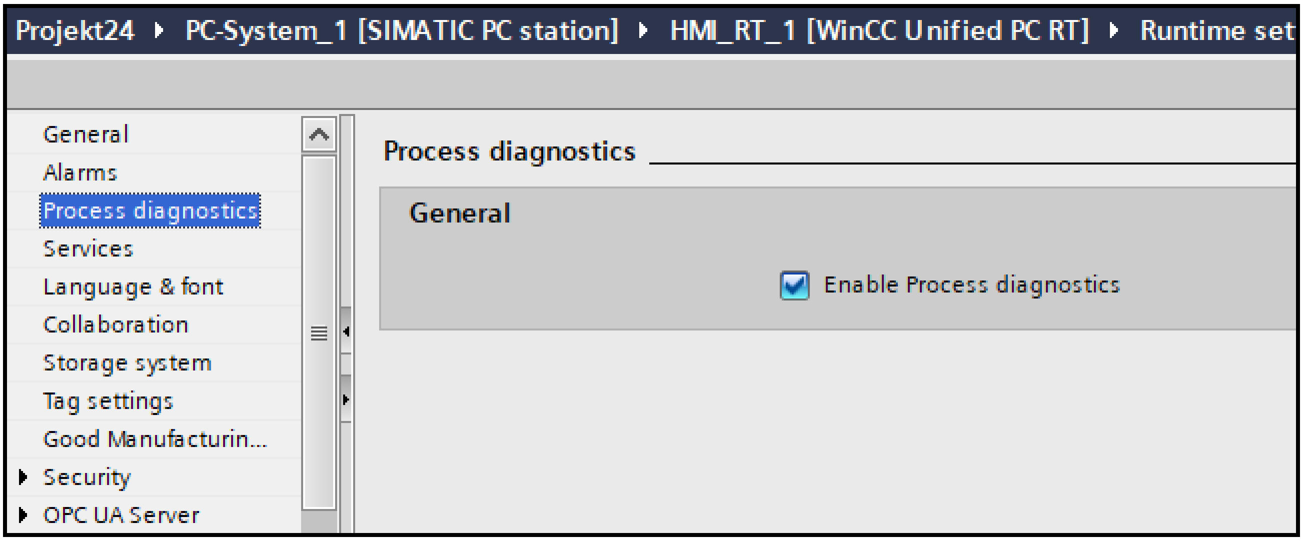
To use the objects for the diagnostics and supervision in conjunction with the ProDiag supervision in your program, you need a WinCC Unified ProDiag license.

Enable process diagnostics

To activate process diagnostics on an HMI device, follow these steps:

1. Open the "Runtime settings" of the HMI device in the project tree.
2. Under Process diagnostics, select the "Enable process diagnostics" option.

The display of process diagnostic alarms is enabled in runtime.



☑ Enable Process diagnostics

3.4.13.3 Objects for the supervision and diagnostics of plants

Introduction

WinCC offers the following objects for displaying the current monitoring status and for fault diagnostics in the program code:

- GRAPH overview
- PLC code view
- ProDiag overview
- Criteria analysis control

GRAPH overview

The "GRAPH overview" object is used to display the current program status for executed steps of the GRAPH sequencer.

PLC code view

The "PLC code view" object is used to display the current program status of user programs that have been programmed in the LAD, FBD or GRAPH graphic programming languages.

ProDiag overview

The "ProDiag overview" object provides an overview of the current status of the supervisions in the context of a ProDiag Overview supervision block.

Criteria analysis control

The "Criteria analysis control" object is used to display the faulty operands in the user program that were determined for a selected alarm by criteria analysis.

3.4.13.4 GRAPH overview

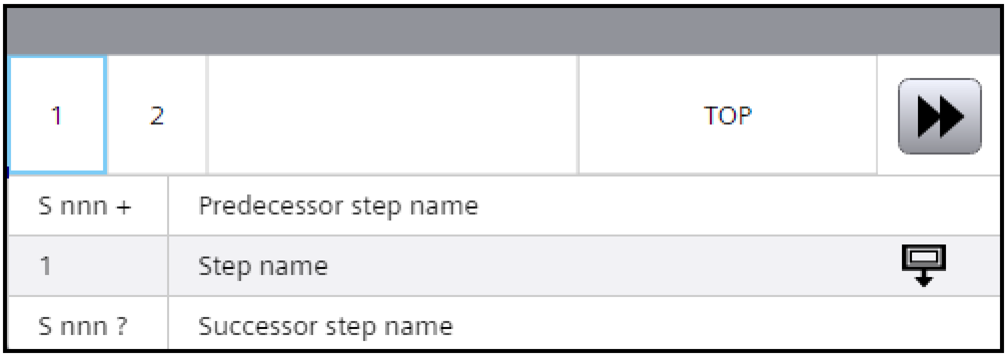
Use

The "GRAPH Overview" object is used to display the current program status for executed steps of the GRAPH sequencer. Errors during execution of a program are displayed directly at the corresponding step.

The following information is displayed in the "GRAPH Overview" object:

- Name and status of the function block
- Status of initial and simultaneous steps
- Number and name of the first step currently executed step
- Operating mode for running the GRAPH sequencer

WinCC supports the display of step names for the GRAPH blocks in multiple languages starting from Version 6.0. The step names will then be displayed in the selected Runtime language following a language changeover in Runtime. If the selected language is not available, the names are displayed in the default language (English).



Note

To view the program status of an GRAPH instance data block in the "GRAPH overview" object, set the block's instance-specific properties to "Visible in HMI" and "Accessible from HMI".

Layout

In the Inspector window, you can change the settings for the position, geometry, style, and color of the object. You can adapt the following properties in particular:

- "Process > Tag": Assign the tag.
- "Function bar": Specifies the buttons of the GRAPH overview.

Operating mode

There are four modes of operation available to you for running the GRAPH sequence:

- AUTO (default setting) - Automatically switches to the next step when the transition is fulfilled.
- TAP - Automatically switches to the next step when the transition is fulfilled and there is an edge change from "0" to "1" at the T_PUSH parameter.
- TOP - Automatically switches to the next step when the transition is fulfilled or there is an edge change from "0" to "1" at the T_PUSH parameter.
- MAN - The next step is not automatically enabled when the transition is fulfilled. You can select and deselect the steps manually.

Note

You set the operating mode by modifying the interface parameters of the GRAPH block in your control program.

In WinCC Unified Runtime, you can customize the name for the operating mode that is displayed in the GRAPH overview.

Configuring a compact view

You can also configure a compact GRAPH overview without function bar buttons and operating mode display.

To display a compact GRAPH overview in single-line compatibility mode, drag the control to the desired size.

Symbols

The symbols displayed in the GRAPH overview are pre-defined:

Symbol		Function
⚠	Error	Indicates that an error has occurred during the execution of a step.
	Initial step	Indicates that the currently executing step is the first step in the GRAPH step sequence.
	Simultaneous step	Shows that there are other simultaneous steps in the GRAPH step sequence in addition to the current one.

Function bar

You can define the buttons of the GRAPH overview in runtime along with their operator authorizations in the Inspector window under "Properties > Properties > Miscellaneous > Function bar > Elements". By default, only the "Next Step" button is available. To display additional buttons in the object, activate the "Visibility" property in the settings of the corresponding button.

The following buttons are available for the GRAPH overview:

Button		Function
⏩	Next Step	Jumps to the next step in parallel step. When you get to the last step, you can jump back to the first step.
△	Jump to Alarm Control	Opens the configured alarm control with the error message in WinCC Unified. The button is intended to be populated with appropriate system functions/scripts.
	Jump To PLC code view	Opens the configured PLC code view. The button is intended to be populated with appropriate system functions/scripts. Ideally, use the "OpenGRAPHViewerFromOverview" system function.
TIA	Jump to TIA Portal	Several script functions are available for opening the TIA Portal.

3.4.13.5 Configuring a GRAPH overview

Introduction

You can use the GRAPH overview to view the current program status for the executed steps of a GRAPH sequencer.

Requirement

- A PLC including a GRAPH instance data block has been created.
- GRAPH instance data block contains at least one tag which is visible in HMI and accessible from HMI.

Note

The process tag you are using for the GRAPH overview must be visible in HMI and accessible from HMI.

To identify the tags of the GRAPH data block as visible and accessible for HMI, open the GRAPH function block, select the block in the work area, and select "Edit > Internal parameters visible/accessible from HMI" in the menu bar. Then compile the program blocks.

- An HMI device has been created.
- You have created a screen.
- The Inspector window is open.

Procedure

1. Drag-and-drop the GRAPH overview from the toolbox view into the configured screen.
2. In the Inspector window, click "Properties > Properties > Miscellaneous".
3. Open the selection button under "PLC Source > Tag".
   The "Add new object" dialog opens.
4. Select the corresponding PLC in the "Program blocks" folder.
5. Select the corresponding PLC tag of the GRAPH instance data block.

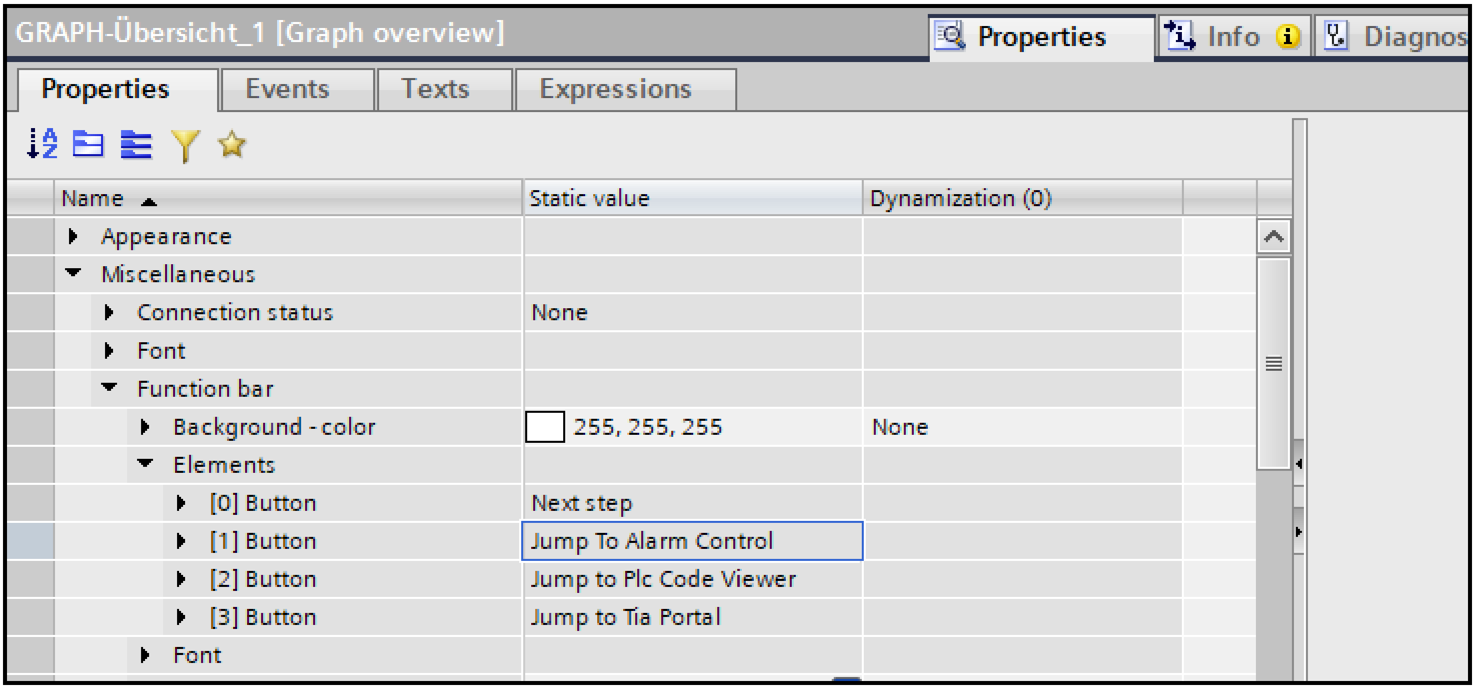
Note

If no connection was configured between the HMI device and the selected PLC, a connection is set up automatically.

In addition, an HMI tag is created which is connected to the PLC tag.

6. To display the GRAPH overview in compatibility mode without function bar buttons and operating mode display, drag the object to the desired size, whereby multiple basic views are possible.

7. Under "Properties > Properties > Miscellaneous > Function bar > Elements", specify the buttons to be displayed in the object.



Name	Static value	Dynamization (0)
Appearance		
Miscellaneous		
Connection status	None	
Font		
Function bar		
Background - color	□ 255, 255, 255	None
Elements		
[0] Button	Next step	
[1] Button	Jump To Alarm Control	
[2] Button	Jump to Plc Code Viewer	
[3] Button	Jump to Tia Portal	
Font		

8. Under "Properties > Events", you can assign system functions or scripts to the buttons in the GRAPH overview in order, for example, to jump to the alarm control or the PLC code view in Runtime and to open the TIA Portal.

Result

The GRAPH overview is inserted in the screen. The current status of the GRAPH step sequence is displayed in Runtime.

See also

GRAPH overview (Page 290)

3.4.13.6 PLC code view

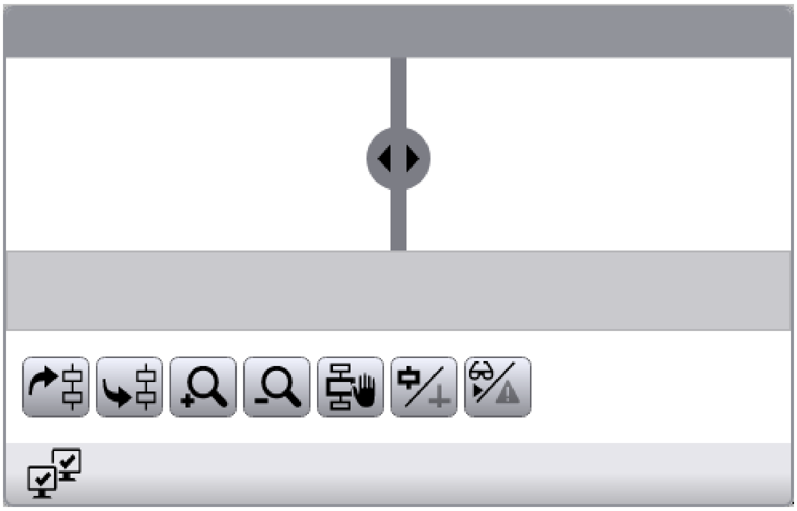
Use

The "PLC code view" object is used to display the current program status of user programs that have been programmed in the LAD, FBD or GRAPH graphic programming languages.

A variety of information about the user program is displayed in the PLC code view:

- Information area
- Symbol line

- Detail view
- Transition/Interlock view



Layout

In the Inspector window, you can change the settings for the position, geometry, style, and color of the object. You can adapt the following properties in particular:

- "Function bar": Specifies the buttons of the PLC code view control.
- "Symbol line": Shows information about the first or the selected icon.

Information area

In the information area of the PLC code view, you are shown:

- In the left area, the GRAPH sequence.
- In the right area, the details, e.g. for the step or for the transition. In the ProDiag view, the networks to the supervised operands are displayed in this area.

Buttons of the function bar

You can define the buttons of the PLC code view control in runtime along with their operator authorizations in the Inspector window under "Properties > Properties > Miscellaneous > Function bar > Elements". Some buttons are enabled by default. To display additional buttons in the object, activate the "Visibility" property in the settings of the corresponding button.

The following buttons are available for the PLC code view:

Button		Function
	Previous	Navigates to the previous sequence / previous network.
	Continue	Navigates to the next sequence / next network.
	Zoom in	Enlarges the information area.
	Zoom out	Reduces the information area.
	Toggle GRAPH mode	Switches between manual and automatic step selection for the active step.
	Toggle detail view	1. GRAPH view: Switches between the transition and interlock networks. 2. ProDiag view: Switches between network and the whole block.
	Toggle criteria analysis	Switches between the network view including criteria analysis and the standard network display without criteria analysis.

3.4.13.7 Configuring the PLC code view

Introduction

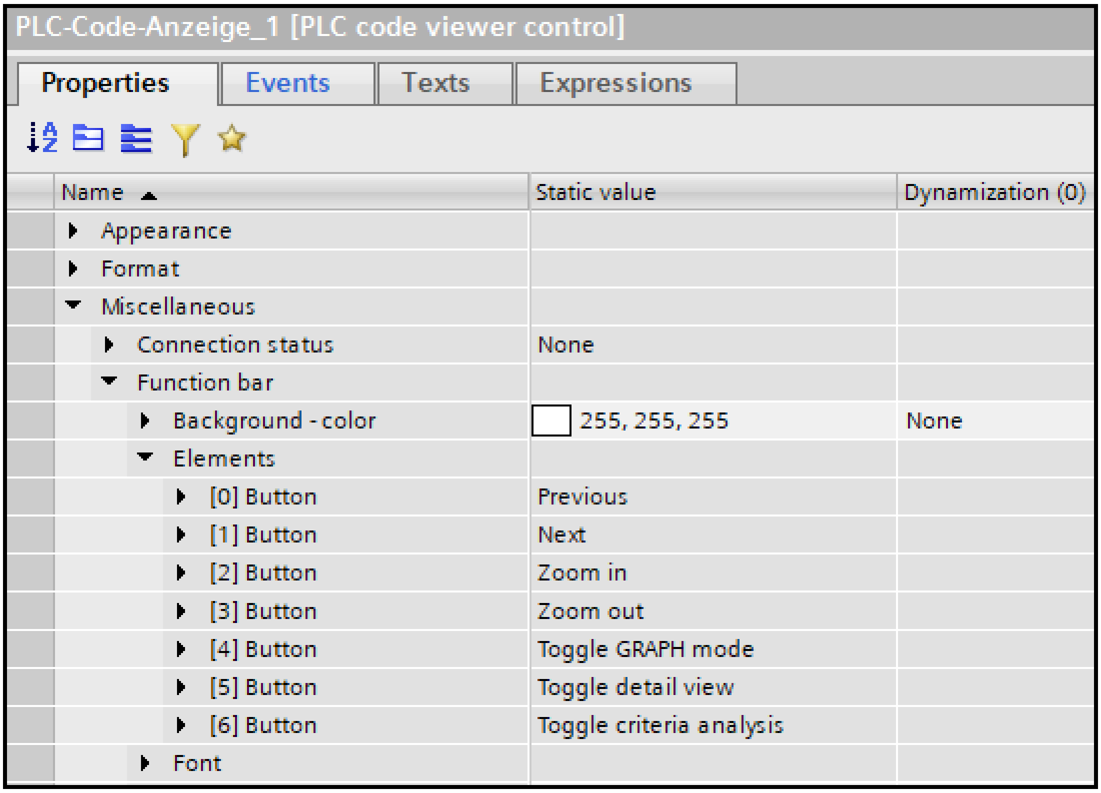
To display the PLC program networks in the graphic programming languages LAD, FBD and GRAPH in Runtime, insert a PLC code viewer control into your project.

Requirement

- At least one PLC has been created.
- An HMI device has been created.
- An HMI connection has been established between the controller and HMI device.
- The process diagnosis is activated on the HMI device.
- You have created a screen.

Procedure

1. Drag-and-drop the PLC code view control from the toolbox view.
2. In the Inspector window, click "Properties > Properties > Function bar".
3. Select the buttons that you require in Runtime, for example: Back, Next, Zoom in.



Name	Static value	Dynamization (0)
Appearance		
Format		
Miscellaneous		
Connection status	None	
Function bar		
Background - color	255, 255, 255	None
Elements		
[0] Button	Previous	
[1] Button	Next	
[2] Button	Zoom in	
[3] Button	Zoom out	
[4] Button	Toggle GRAPH mode	
[5] Button	Toggle detail view	
[6] Button	Toggle criteria analysis	
Font		

Result

The PLC code view is inserted in the screen. In Runtime, PLC user programs can be displayed that are programmed in the graphic programming languages LAD and FBD as well as GRAPH.

You can populate the PLC code viewer using system functions, e.g. jump from the GRAPH overview or from the alarm, or you can select the corresponding parameters directly.

See also

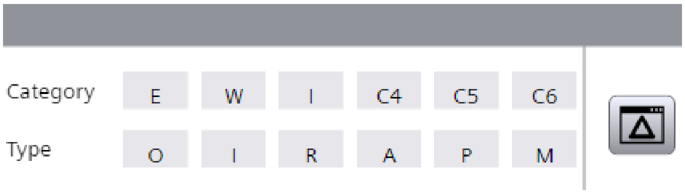
PLC code view (Page 294)

3.4.13.8 ProDiag overview

Use

The "ProDiag overview" object provides an overview of the current status of the configured monitoring in Runtime.

When an error occurs, the type of error and the error category are determined in the ProDiag overview. You can navigate directly to the alarm control to find the error and you can jump from the corresponding alarm to the PLC code viewer control. You can display the affected program code in the PLC code viewer control.



The "ProDiag overview" object is available for WinCC Unified.

Layout

In the Inspector window, you customize the position, geometry, style, color and font types of the object. You can adapt the following properties in particular:

- Displayed buttons
- Names and colors for categories
- Names and colors for monitoring types

Monitoring types and categories

You can display a maximum of 8 categories and 6 monitoring types in the "ProDiag overview" object. The following pre-defined categories and monitoring types are available:

Designation	Categories
E (Error)	Error
W (Warning)	Warning
I (Info)	Information
C4 ... C8	Additional categories

Rename the categories C4 to C8, which are created by default, according to your requirements.

Designation	Monitoring type
O (Operand)	Operand error
I (Interlock)	Interlock error
R (Reaction)	Reaction error
A (Action)	Action error
P (Position)	Position error
M (Message error)	Alarm

You can change display symbols of the supervision types and categories at any time in the Inspector window under "Miscellaneous".

Symbols

The icons displayed in the ProDiag overview are fixed.

Icon	Name	Function
⚠	Error	Indicates that an error has occurred.

"Jump to Alarm Control" button

The "Jump to Alarm Control" button in the ProDiag overview is activated by default.

Button	Name	Function
△	Jump to Alarm Control	Opens the configured alarm control with the error message after system functions or scripts have been assigned to the button.

Deactivated display

If there is a faulty connection to the controller during runtime, the object "ProDiag overview" is displayed grayed-out (unavailable). This deactivated display can be due to the following:

- The controller is deactivated
- The configured ProDiag program block was removed from the control program
- The controller is in Stop mode

As soon as the cause of the error is removed and the connection reestablished, the ProDiag overview shows the current online status of the monitoring during runtime.

3.4.13.9 Configuring the ProDiag overview

Introduction

The ProDiag overview is used to monitor your machine or system at runtime and determination of diagnostic information in the event of a fault occurring.

Once you have set the status tag in the object and the connection to a ProDiag FB has been established, the status of the "State" status tag of the corresponding PLC data type is queried. In Runtime, the states of the monitored operands are represented as symbols in the ProDiag overview, similar to a traffic light colors.

In WinCC, you configure the display and the representation of categories and supervision types that are displayed in the "ProDiag overview" object independent of the supervision settings in STEP 7.

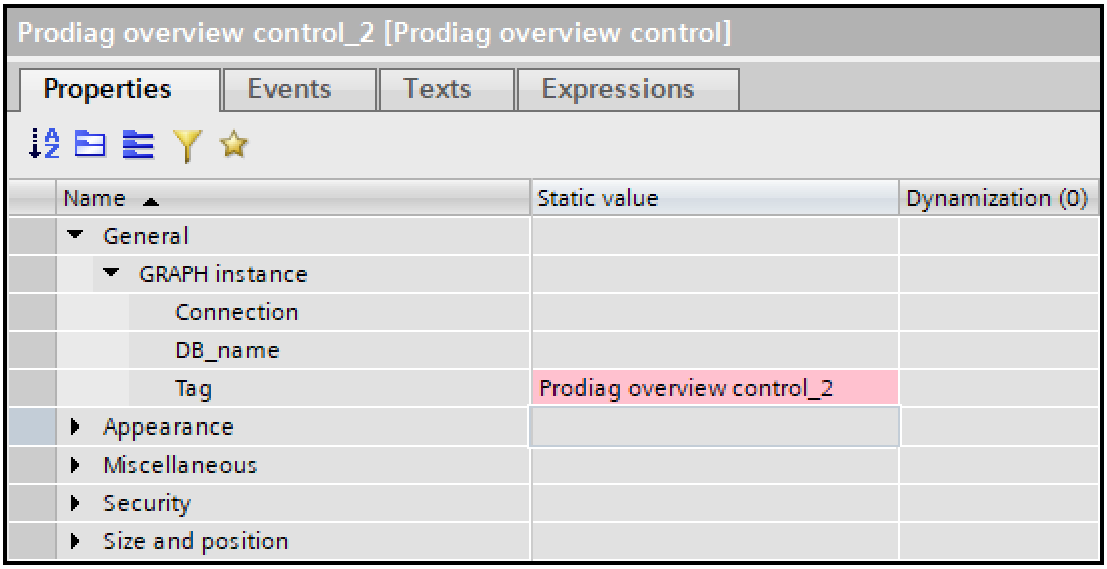
Requirements

- At least one S7-1500 controller has been created.
- At least one supervision instance has been configured.

- A ProDiag FB and ProDiag DB are available.
- A PC station or an HMI device that supports the ProDiag functionality has been created.
- An HMI connection has been established between the controller and HMI device.
- An screen is created and the Inspector window is open.

Procedure

1. Drag-and-drop the ProDiag overview from the toolbox view.
2. In the Inspector window, select "Properties > Properties > General".
3. Open the selection button under the "Tag" property.
4. Select the status tag of ProDiag FB.
   Alternatively, you can add the corresponding status tags from the detail view using drag-and-drop.



Name	Static value	Dynamization (0)
General		
GRAPH instance		
Connection		
DB_name		
Tag	Prodiag overview control_2	
Appearance		
Miscellaneous		
Security		
Size and position		

5. Under "Properties > Properties > Miscellaneous > P Diag Categories", define the names and colors for the supervision categories.
6. Under "Properties > Properties > Miscellaneous > P Diag Supervision types", define the names and colors for the supervision types.
7. Under "Properties > Events", you can configure a system function for the "Alarm view - Button tapped" event to jump from the ProDiag overview to the alarm view in Runtime.

Result

The ProDiag overview is inserted in the screen. The current states of the supervised events are displayed in Runtime.

See also

ProDiag overview (Page 297)

3.4.13.10 Initial value acquisition and criteria analysis

Overview of initial value acquisition and criteria analysis

Introduction

In the TIA Portal you have the option of testing the execution of your user program on the HMI device. The data and values on the HMI device are continuously synchronized with the PLC and updated. You therefore see the current program status with the actual values of the signal states on the HMI device.

If an error occurs in your plant, you have the option of jumping to the program code from the corresponding error message and displaying the error location in the network in the “PLC code view". In the "Criteria analysis view" object, you see the faulty operands for a selected GRAPH alarm or ProDiag alarm at a glance.

The initial value acquisition and criteria analysis functions enable you to record the values at the time of the error and to quickly identify the faulty operands in the program.

The actual value acquisition and criteria analysis functions are available for GRAPH function blocks, ProDiag function blocks and safety programs (F-blocks).

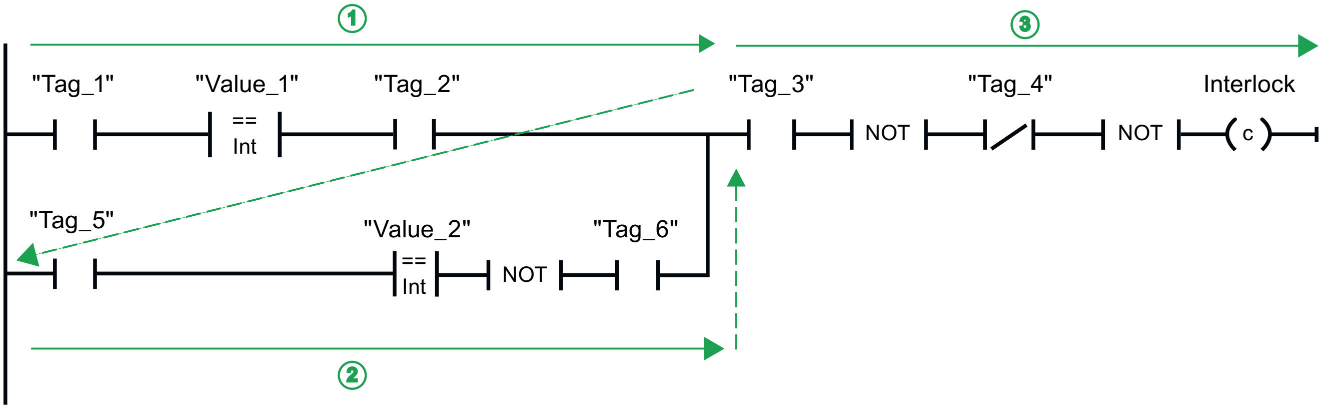
Requirement

- The initial value acquisition is available in WinCC Unified Runtime for the following blocks:
  - For the GRAPH function blocks as of version 6.0.
  - For the ProDiag function blocks as of version 2.0.
- Maximum of 32 statuses can be recorded. The initial values for a network that contains more than 32 elements are not recorded.

Initial value acquisition

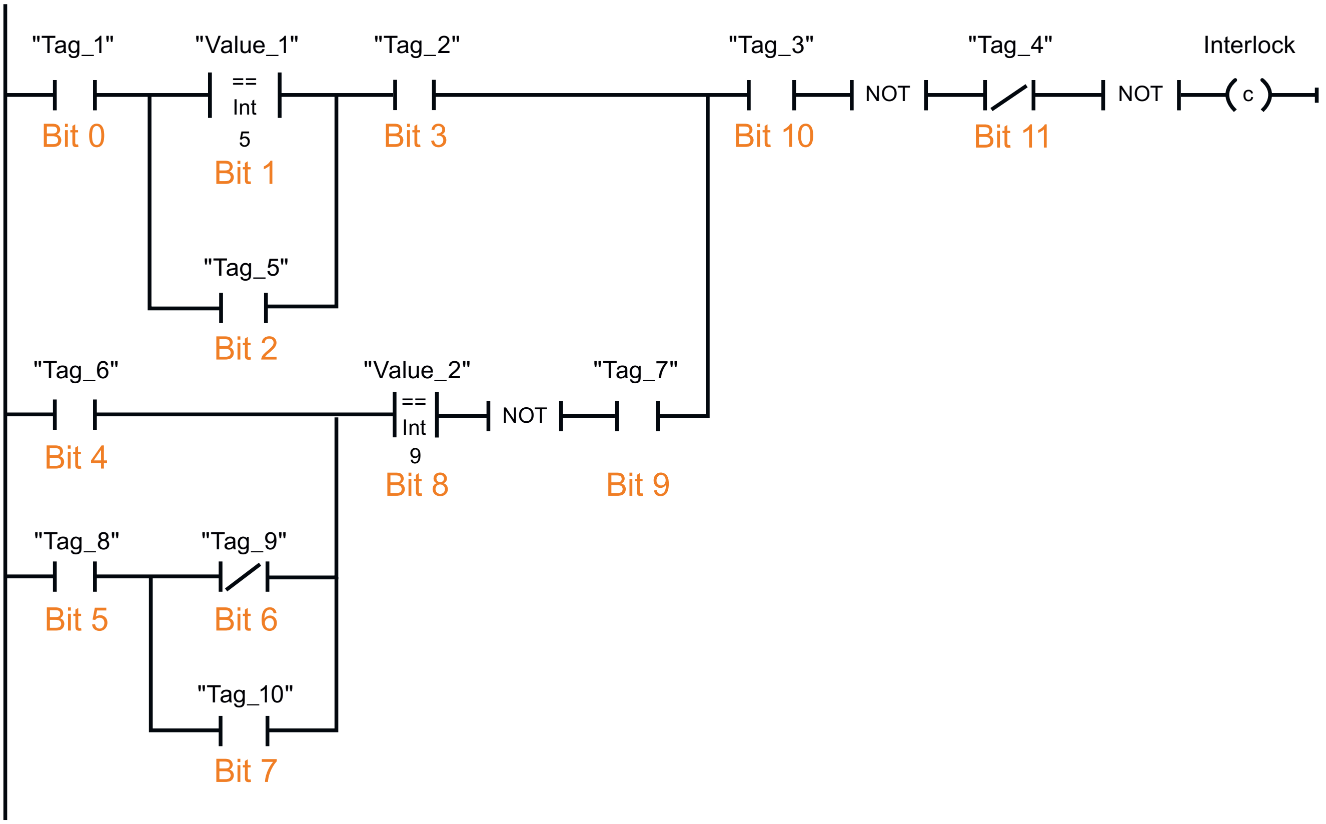
With the help of initial value acquisition you can acquire the values at the time of the error in the PLC, display them in the PLC code view and compare them with the actual values. With initial value acquisition you continuously record the signal states of Boolean operands and results of comparators in transitions and interlocks.

The signal states are recorded in a defined order from top left to bottom right:



You activate initial value acquisition individually for each GRAPH block in the user program. A maximum of 32 signal states of Boolean operands can be recorded per interlock or per transition of a GRAPH step. Each individual signal state occupies one bit. The values are saved in a DWORD.

In the following example you can see the principle and order in which the initial values are recorded in the interlock:



Criteria analysis

Initial value acquisition in the PLC enables the analysis of criteria and operands with error in the program. You see the evaluation of the criteria analysis on your HMI in the PLC code view. In addition, in the "Criteria analysis view" object, you can use the criteria analysis to have the faulty operands displayed for a selected GRAPH alarm or ProDiag alarm.

Note

If the upstream network has been changed, the alarm is not be triggered again. This leads to inconsistencies between the network and faulty operands. As a result, the criteria analysis view cannot correctly display the faulty operands. If the alarm is triggered again, the faulty operands are displayed correctly again in the criteria analysis view.

For the blocks for which you have activated initial value acquisition, after the jump the initial value view is displayed by default in the PLC code view. In addition, the operands with error and criteria are highlighted visually in the initial value view.

All information about the selected operand can be seen in one line of the PLC code view.

In the event of an error in a comparator, both operands are marked as having errors. Only the recorded values are shown in the initial value view. To see the actual values of the tags, change to the actual value view.

Supported instructions

Introduction

You see the initial values and the results of the criteria analysis in the "PLC code view" object.

For global supervisions, the initial values of all Boolean operands in the network are recorded. If the network contains multiple individual power rails that are not connected to each other, only the initial values of the respective power rail are recorded.

For local supervisions, only the initial values that are specified as conditions for the supervised parameter for the block call are recorded.

Supported instructions

The following instructions are supported in LAD and FBD for initial value acquisition:

Instructions	Display on the HMI device
Bit logic operations	
Normally open contact	Initial values and criteria analysis
Normally closed contact	
Invert RLO	The instruction is supported but it is not relevant for initial values or the criteria analysis.
Assignment	
Negate assignment	
Reset output	Initial values
Set output	

Instructions	Display on the HMI device
Set/reset flip-flop	Initial values and criteria analysis up to and including the instruction box
Reset/set flip-flop	
Comparator operations	
Equal	Initial values and criteria analysis
Not equal	
Greater or equal	
Less or equal	
Greater than	
Less than	
Timers	
TP	Initial values and criteria analysis up to and including the instruction box
TON	Initial values and criteria analysis
TOF	Initial values and criteria analysis up to and including the instruction box
TONR	
Counters	
CTU	Initial values and criteria analysis up to and including the instruction box
CTD	
CTUD	

For bit logic operations, the status of the operand is recorded. For comparators, the result of the comparison is recorded.

For flip-flops, both inputs (R and S) are recorded if they are interconnected.

For timers and counters, the status of the operand at the output, and the inputs if they are interconnected, are recorded. (For example, for CTUD: CU, CD, R, LD)

The FBD instructions AND and OR are also supported for initial value acquisition and criteria analysis. The FBD instruction EXCLUSIVE OR is not supported by the initial value acquisition and criteria analysis.

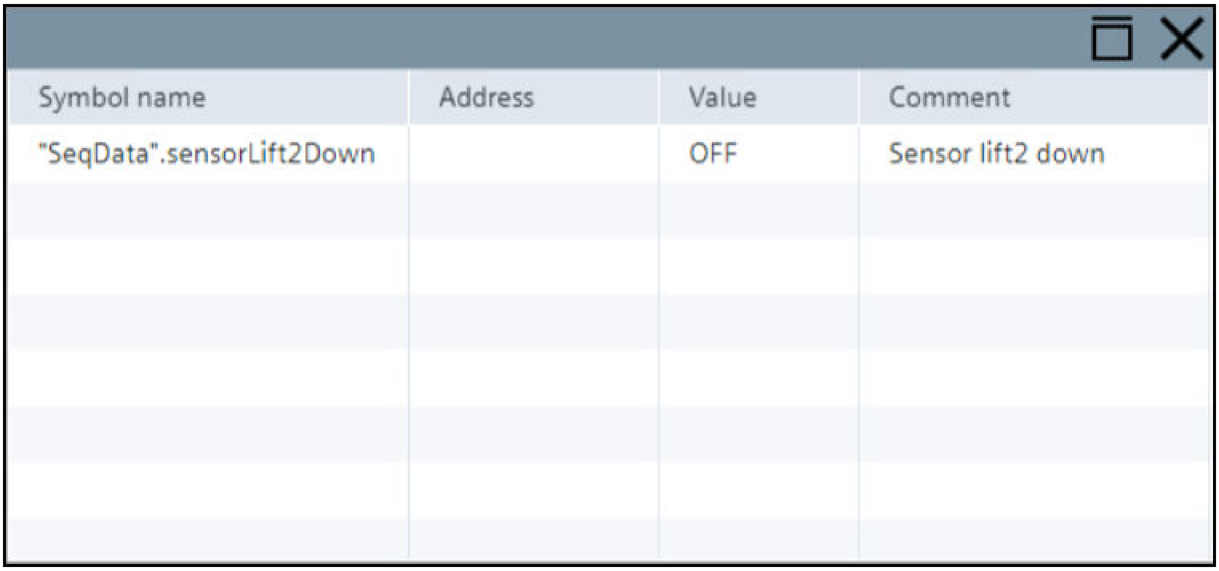
Criteria analysis view

Use

The "Criteria analysis view" object shows you the faulty operands in the user program that have triggered a selected ProDiag alarm or GRAPH alarm. As a result, you have the option of seeing the list of faulty operands in addition to the alarm in the same screen.

To see the evaluation of the criteria analysis in the "Criteria analysis view" object in Runtime, select the initial value acquisition in the settings of the function blocks in the user program. The initial value acquisition is available for GRAPH function blocks as of version 6.0 and ProDiag function blocks as of version 2.0.

To enable the link to the corresponding error message, configure a reference to a previously configured alarm control. If you select a GRAPH alarm or a ProDiag alarm in the alarm control in Runtime, then the name, address, comment and value of the operand that caused this error is displayed in the criteria analysis view.



Symbol name	Address	Value	Comment
"SeqData".sensorLift2Down		OFF	Sensor lift2 down

You see the incoming alarms and the faulty operands at a glance in Runtime if you configure the criteria analysis view and its linked alarm control in the same screen.

Note

Criteria analysis is only available for the user programs for which initial value acquisition has been activated.

Activate initial value acquisition in the properties of the following blocks:

- ProDiag function blocks with version greater than or equal to V2.0
- GRAPH function blocks with version greater than or equal to 6.0

Layout

You change the settings for the position, style, colors, and fonts of the object in the Inspector window.

Columns

The following columns are displayed in the criteria analysis view in Runtime.

Column	Description
Symbol name	Symbolic name of the operand in the user program.
Address	Absolute address of the operand.
Value	The value of the operand at the time of the error.
Comment	Additional comments from the user program in the language that is loaded into the controller.

See also

Configuring the criteria analysis view (Page 306)

Configuring the criteria analysis view

"Criteria analysis view" object

The "Criteria analysis view" object shows you the faulty operands in the user program that have triggered a selected ProDiag alarm or GRAPH alarm. It is used to list the initial values in a separate view in order to obtain an overview of the fault status of the plant.

If you select the incoming ProDiag alarm or GRAPH alarm in the alarm control in Runtime, you see the operands that were determined in the criteria analysis view.

You configure the criteria analysis view and its linked alarm control in the same screen.

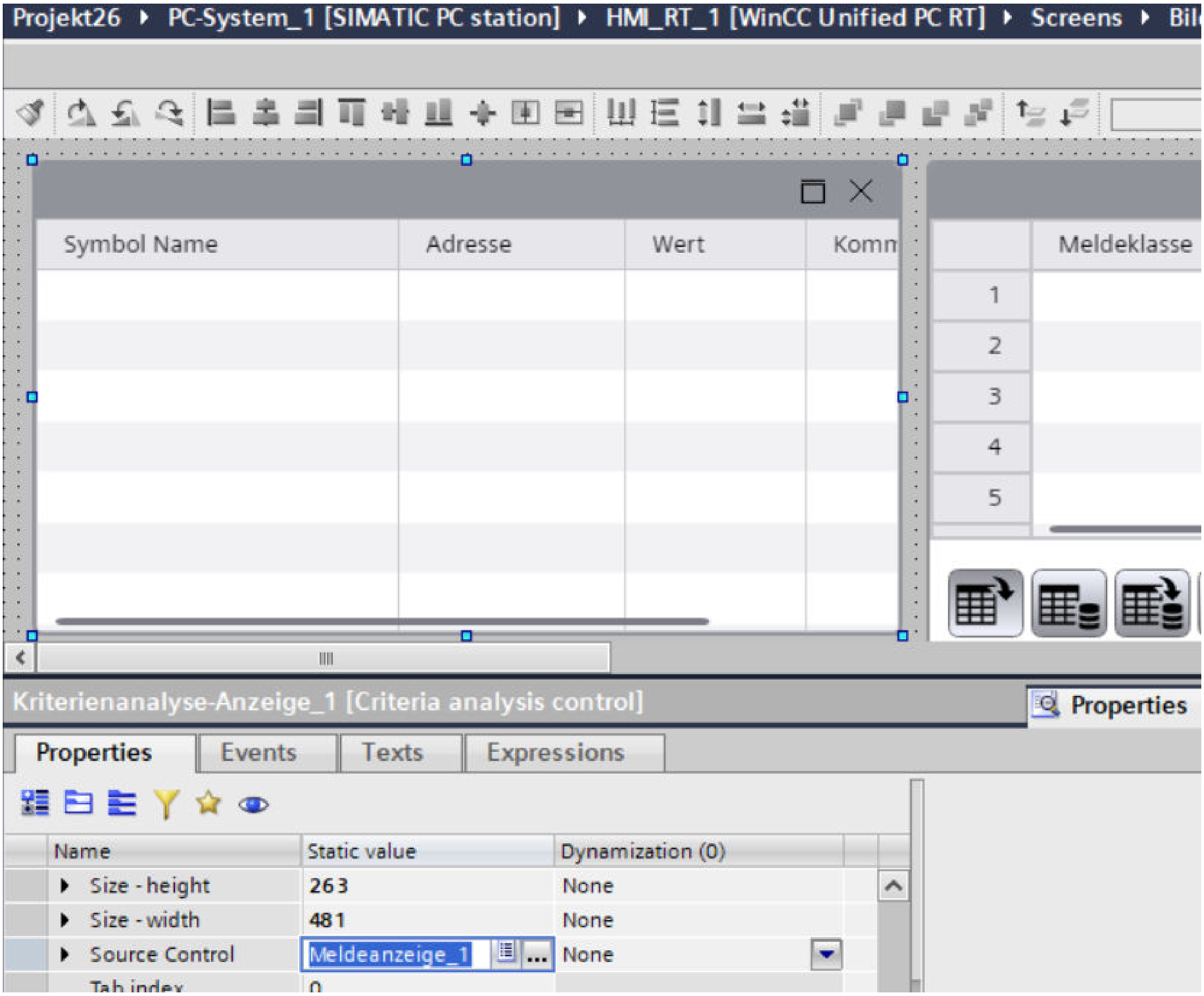
Requirement

- The HMI device is connected to the controller.
- A ProDiag program version 2.0 or a GRAPH program Version 6.0 or higher is installed on the controller.
- Process diagnostics is enabled in the "Runtime settings > Process diagnostics > General" of the Unified Runtime device.
- Initial value acquisition is enabled for the function blocks.
- An alarm control has been configured.

Procedure

1. Move the criteria analysis view from the toolbox window using drag-and-drop.
2. Click on "Properties > Properties" in the Inspector window.

3. Open the selection button under the "Data source" property.
4. Select the configured alarm control.


Projekt26 ▸ PC-System_1 [SIMATIC PC station] ▸ HMI_RT_1 [WinCC Unified PC RT] ▸ Screens ▸ Bil
Symbol Name
Adresse
Wert
Komm
Meldeklasse
1
2
3
4
5
III
Properties
Properties
Events
Texts
Expressions

Kriterienanalyse-Anzeige_1 [Criteria analysis control]

Name	Static value	Dynamization (0)
Size - height	263	None
Size - width	481	None
Source Control	Meldeanzeige_1	None
Tab index	0	

Result

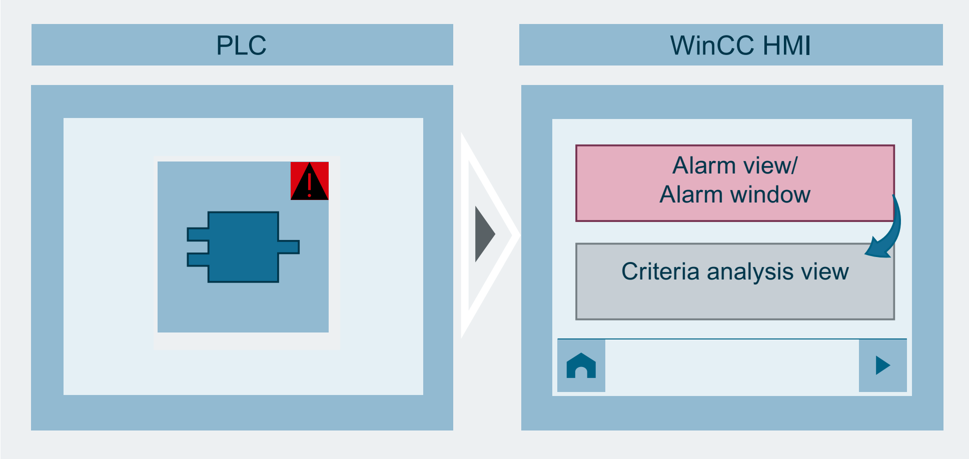
The criteria analysis view is configured in the screen and connected to the alarm control. For a selected alarm you can see detailed information in Runtime about that operands that triggered this alarm.

Outputting alarms with criteria

Introduction

When initial value acquisition is activated, the values of the faulty operands are recorded at the time of the error and missing criteria are analyzed and determined.

You have the option to add additional information about faulty operands to the GRAPH and ProDiag alarms and output them on your HMI device. If an error occurs in the program flow in runtime, the error message also indicates the faulty operands in the faulty network. You see detailed information on all operands with error of the error message in the "Criteria analysis view" object.



In WinCC Unified Runtime, you have the option to add additional information to the alarms. For this, select the appropriate text that you want to extend under "Runtime settings > Process diagnostics > Criteria analysis > Extend text", i.e. alarm text, info text or additional text 1 - 9. You can extend the texts with the first faulty operand or with all faulty operands.

The following information can be added to the operands:

- Symbol: The symbolic name of the first or all faulty operands.
- Absolute address: The address of the first or all faulty operands.
- Value: The value of the first or all faulty operands at the time of the fault.
- Comment: Multilingual comments that were configured in the user program.

The additional information is separated in the alarm by semicolons and spaces.

Note

The order of the additional information that is added to the alarm is predefined and cannot be changed.

Note

To completely display the alarms from the controller on the HMI device, the "Automatic update" option must be selected under "Runtime settings > Alarms > Controller alarms" for the relevant connection. You can find additional information on complete alarms under "Sending a complete alarm from the controller to the HMI device".

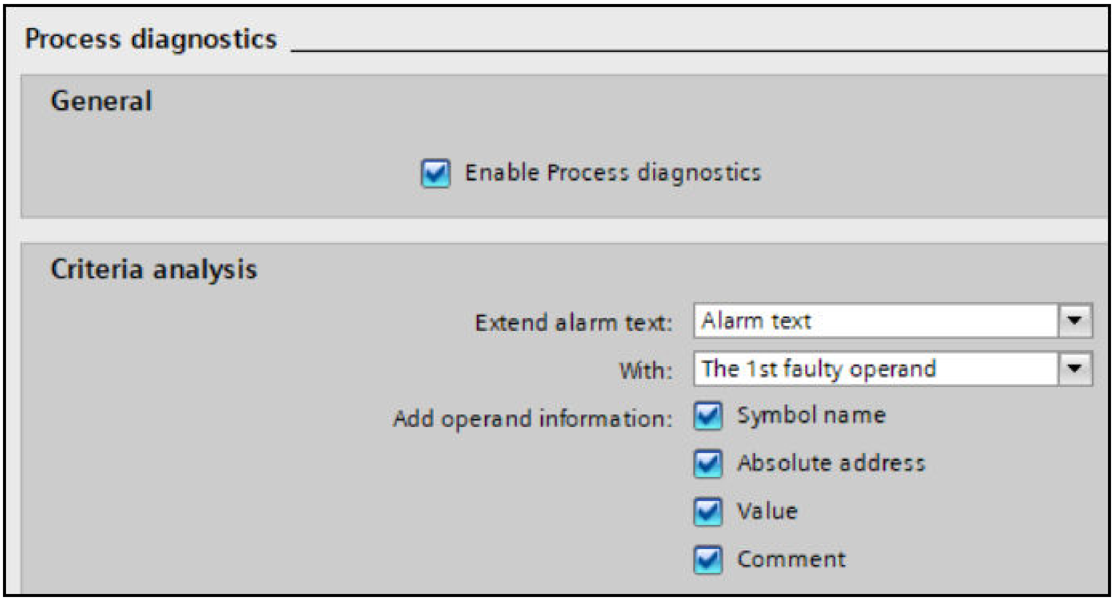
Criteria analysis in the alarm system

You visualize the alarms for the criteria analysis in the following steps:

- You enable the initial value acquisition in the properties of the ProDiag function block or GRAPH function block of the user program
- You enable the options to extend the alarm texts or info texts in the runtime settings of the HMI device

Extend alarms

1. Open the "Runtime settings" editor of the HMI device.
2. Click "Process diagnostics > Criteria analysis".
3. Under "Criteria analysis > Extend text", select which texts you want to extend.
4. Select the additional information to be added to the alarm text in the alarm, such as symbol name, address and value of the first faulty operand and comment.



Process diagnostics

General

☑ Enable Process diagnostics

Criteria analysis

Extend alarm text: Alarm text

With: The 1st faulty operand

Add operand information: ☑ Symbol name
☑ Absolute address
☑ Value
☑ Comment

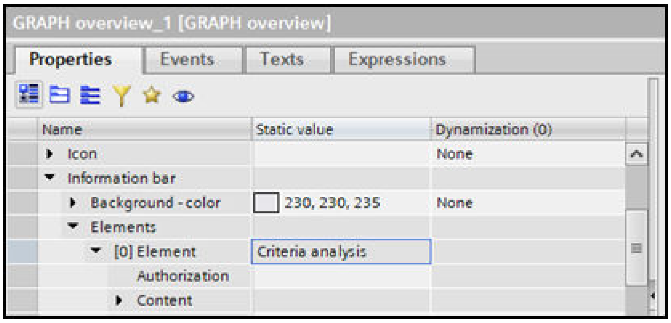
Result

If an error occurs, you see not only the alarm text in the alarm control but also the operands that triggered the error message.

Criteria analysis in the "GRAPH overview" object

Extension of the "GRAPH overview" object with the criteria analysis

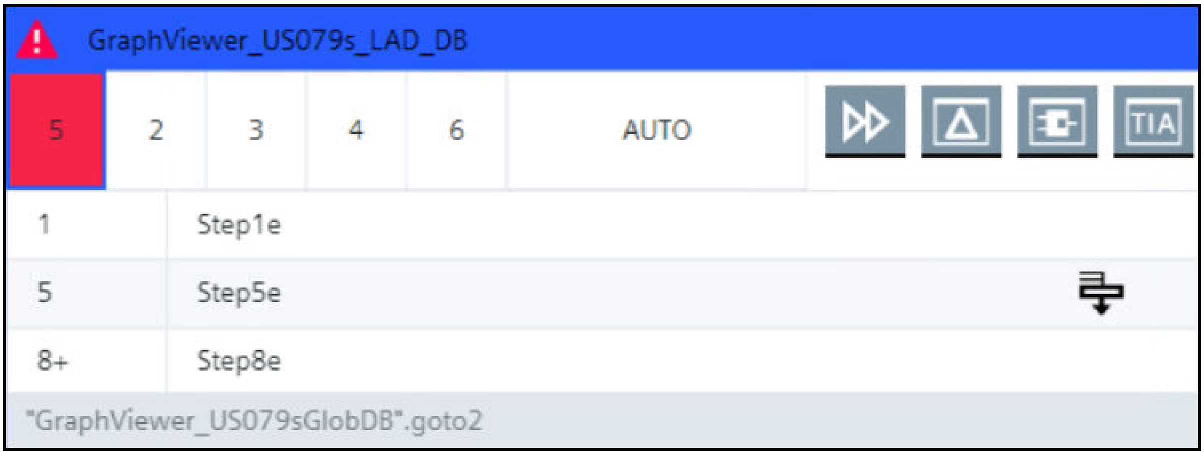
To display the criteria analysis in the "GRAPH overview" object, the criteria analysis must be enabled in the Inspector window under "Properties > Properties > Information bar > Elements".



Name	Static value	Dynamization (0)
Icon		None
Information bar		
Background - color	□ 230, 230, 235	None
Elements		
[0] Element	Criteria analysis	
Authorization		
Content		

Result

In runtime, the information bar of the "GRAPH overview" object displays the symbolic name of the 1st faulty operand.



1	Step1e
5	Step5e
8+	Step8e

"GraphViewer_US079sGlobDB".goto2

3.5 Elements

3.5.1 Overview of elements

Operable elements are available in process pictures in Runtime.

The following elements are available depending on the configured access rights:

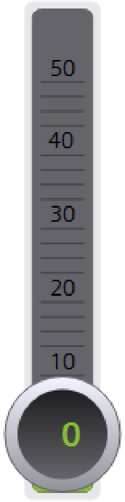
Icon	Element	Brief description
	Bar	Represents tags graphically. The bar graph can be labeled with a value scale.
0.12	I/O field	Used for entry and display of process values.
▾	Symbolic I/O field	A drop-down list with texts or graphics for display and input in runtime.
☑ □	Check box	Used for display and selection of multiple options.
	List box	Used for display and selection of multiple list entries.
◉ ○	Radio button	Used for display and selection of various options of which only one can be selected.
0 I	Switch	Used for toggling between two predefined states.
	Button	Executes a configured function.
	Slider	Used for monitoring and changing process values within a defined range and adjusts them. By adjusting the slider, you intervene in the process and correct the displayed process value.
🕒	Clock	Used for display of date and time.
	Gauge	Represents numerical values in the form of an analog gauge. For example, it can be seen at a glance whether the boiler pressure is in the normal range.

3.5.2 Using elements

3.5.2.1 Bar

Application

The tags are displayed graphically with the "Bar" object. The bar graph can be labeled with a value scale.



Layout

The settings for the position, geometry, style, colors and fonts of the object are made during configuration.

In particular, the following properties are changed:

- Color transition: Specifies the change in color display when limit values are exceeded.
- Limit marking: Displays the configured limit value as an arrow.
- Bar segments: Defines the gradations on the bar scale.
- Scale gradation: Defines the position of the zero point on a bar scale.

If the object falls below a certain size in the light or dark style, it is automatically displayed in compact mode.

Color transition

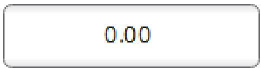
The display of the color change is specified during configuration.

Color transition	Description
"Segmented"	If a particular limit was reached, the bar changes color segment by segment. With segmented display, for example, the limits exceeded by the displayed value are visualized.
"Entire bar"	If a particular limit was reached, the entire bar changes color.

3.5.2.2 IO field

Use

The "I/O field" object is used to enter and display process values.



Layout

The settings for the position, geometry, style, color and fonts of the object are made during configuration.

In particular, the following properties are changed:

- Mode: Specifies the behavior of the object in Runtime.
- Display format: Specifies the display format in the I/O field for input and output of values.
- Hidden input: Specifies whether the input value is displayed normally or encrypted during input.

Note

Reports

In reports, I/O fields only output data. "Output" mode is preset. Properties for configuring input are not available, e.g. "hidden input".

Mode

The behavior of the I/O field is specified during configuration.

Mode	Description
"Input/output"	Values can be input and output in the I/O field.
"Output"	The I/O field is used for the output of values only.

Layout

The "display format" for the input and output of values is specified during configuration.

Layout	
"Binary"	Input and output of values in binary form
"Date"	Input and output of date information. The format depends on the language setting on the HMI device.
"Date/time"	Input and output of date and time information. The format depends on the language setting on the HMI device.
"Decimal"	Input and output of values in decimal form
"Hexadecimal"	Input and output of values in hexadecimal form
"Time"	Input and output of times. The format depends on the language setting on the HMI device.
"Character string"	Input and output of character strings.

Hidden input

In Runtime the input can be displayed normally or encrypted, for example for hidden input of a password. A "*" is displayed for every character during hidden input. The data format of the value entered cannot be recognized.

Avoid overlaps in output fields

If several I/O fields are configured as output fields with a transparent background in a screen, these I/O fields may overlap. The transparent part of the one field covers the digits of the other field. This may cause display problems. In order to avoid such overlaps, the border of the I/O fields must be set to zero during configuration.

Limits

During configuration, colors can be specified for the values that exceed or fall below limits.

When there is a limit violation, the background color of the I/O field changes according to the configuration, even if the I/O field is in input mode.

A limit range can also be defined for the input in the I/O field for the configuration.

If you enter a numeric value outside this limit, it is not applied; for example, 80 with a limit of 78. In this case, a system alarm is generated on the HMI device if an alarm window is configured. The original value is displayed again.

Decimal places for numerical values

The number of decimal places can be specified for a numerical input field during configuration. The number of decimal places is checked when you enter a value in this type of I/O field. Decimal places in excess of the limit are ignored. Empty decimal places are filled with "0".

In the exponential display, the displayed numerical value is represented with a maximum precision of nine decimal places.

Setting an LTime PLC tag via HMI

S7-1500 tags with data type LTime have the unit nanoseconds (ns). IO fields that are linked with such a PLC tag have the unit 100 ns.

HMI user inputs to the I/O field are converted to ns when the value is sent to the PLC.

Note

MAX_SAFE_INTEGER

Depending on the JavaScript engine of the web client, the actual value may lose accuracy during communication between the HMI device and the controller due to rounding if it is outside the value range of MAX_SAFE_INTEGER.

Additional information on MAX_SAFE_INTEGER can be found here (https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/Number/MAX_SAFE_INTEGER).

Behavior when switching between input fields

When you change from one input field to another within a screen due to an operator input and the on-screen keyboard appears, the "Exit field" event is not immediately triggered for the previous field. Rather, it is only triggered after the on-screen keyboard is closed.

No events during the input

While an I/O field is in input mode, no events are transmitted to the server for the I/O field.

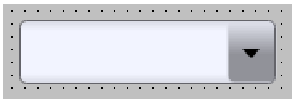
Terminate the input mode with Enter or Esc so that the events configured for the I/O field in engineering take effect again.

3.5.2.3 Symbolic IO field

Use

The "Symbolic I/O field" list is used for displaying texts and graphics in runtime as well as text input, if configured.

The displayed texts or graphics are assigned to the potential tag values.



Note

Selecting the default entry is not possible in runtime.

Layout

The settings for the position, geometry, style, color and fonts of the object are made during configuration.

In particular, the following properties are changed:

- "Mode": Specifies the response of the object in runtime.
- "Resource list": Specifies the text or graphic list that will be associated with the object.

Mode

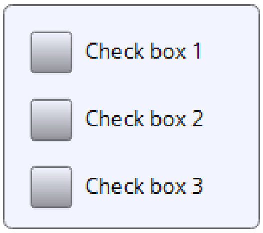
The behavior of the symbolic I/O field is specified during configuration.

Mode	Description
"Output"	The symbolic IO field is used for the output of values.
"Input/output"	The symbolic IO field is used for the input and output of values.

3.5.2.4 Check box

Application

You use the "Checkbox" object to select multiple options. Checkboxes can be activated by default so that the user changes the default values only as required. Multiple options can be selected if the corresponding properties are dynamized.



Layout

The settings for the position, geometry, style, color and fonts of the object are made during configuration.

In particular, the following properties are changed:

- Number of the checkboxes: Defines the number of options.
- Selection of the checkboxes: Defines which options are displayed as activated by default.

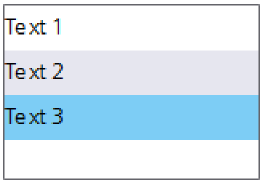
Default setting of the checkboxes

Each option is represented by a bit in a 32-bit word. To activate a field, the corresponding bit must have the value "1". The 32-bit word contains the information for all options of the checkbox list. The value of the "Presetting enabled" property is specified in hexadecimal format.

3.5.2.5 List box

Application

You use the "List box" object to present and select multiple list entries. List entries are selected by default so that the default setting can be changed only when necessary. If the list box is larger than the selection rectangle, WinCC automatically adds a scroll bar to the right margin.



Layout

The settings for the position, geometry, style, color and fonts of the object are made during configuration.

In particular, the following properties are changed:

- Number of entries: Defines the number of list entries.
- Selection of entries: Defines which entry is displayed as activated by default.

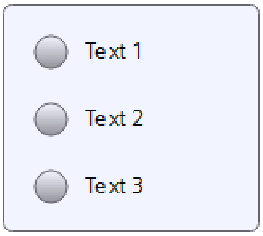
Default setting of the list boxes

Each option is represented by a bit in a 32-bit word. To activate a field, the corresponding bit must have the value "1". The 32-bit word contains the information for all texts of the list of list boxes. The value of the "Selected fields" property is given in hexadecimal notation.

3.5.2.6 Option buttons

Application

You use the "Option button" object for selection of various options. Options are selected by default so that the default setting can be changed only when necessary. Only one option can be selected if the corresponding property is dynamized.



Layout

The settings for the position, geometry, style, color and fonts of the object are made during configuration.

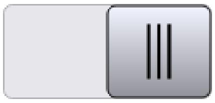
In particular, the following properties are changed:

- Number of fields
- Selection of the fields: Specifies which fields are displayed as activated.

3.5.2.7 Switch

Application

With the "Switch" object you switch between two predefined states. The current state of the "Switch" object is visualized with either a label or a graphic.



Layout

The settings for the position, geometry, style, color and fonts of the object are made during configuration.

In particular, the following property is changed:

- Type: Defines the graphic representation of the object.

Type

The display of the switch is specified during configuration.

Type	Description
"Switch"	The two states of the "Switch" are displayed in the form of a switch. The position of the switch indicates the current state. The switch is switched by moving it.
"Switch with text"	The switch is shown as a button. The current state is visualized with a label. The switch is switched by clicking the button.
"Switch with graphic"	The switch is shown as a button. The current state is visualized with a graphic. The switch is switched by clicking the button.

3.5.2.8 Button

Use

With the "Button" object, you execute a configured function.

Layout

The settings for the position, geometry, style, color and font of the object are made during configuration.

In particular, the following properties are changed:

- Mode: Defines the graphic representation of the object.
- Text / Graphic: Defines whether the Graphic view is static or dynamic.
- Define hotkey: Defines a key, or shortcut that the operator can use to actuate the button.

Note

You can only define a hotkey for HMI devices with keys.

Mode

The display of the button is specified during configuration.

Mode	Description
"Invisible"	The button is not visible.
"Text"	The button is displayed with text. This text explains the function of the button.
"Graphic"	The button is displayed with a graphic. This graphic represents the function of the button.
"Graphic or text"	The button is displayed with text or graphics. If the graphic cannot be displayed, the corresponding text is displayed.
"Graphic and text"	The button is displayed with text and graphic.

Different options are available depending on the device.

Text / Graphic

Depending on the "Mode" property, the display can be specified as a static or dynamic display. The display is specified during configuration.

You can, for example, select the following options for the "Graphic" or "Text" type.

Type	Option	Description
"Graphic"	"Graphic"	With "Graphic when button "not pressed"", a graphic is specified that is displayed in the button for the "OFF" state. When "Graphic when button "pressed"" is selected, a graphic for the "ON" state can be entered.
	"Graphics list"	The graphic in the button depends on the state. The corresponding entry from the graphics list is displayed depending on the state.
"Text"	"Text"	With "Text when button "not pressed"", a text is specified that is displayed in the button for the "OFF" state. When "Text when button "pressed"" is selected, a text for the "ON" state can be entered.
	"Text list"	The text in the button depends on the state. The entry from the text list corresponding to the state is displayed.

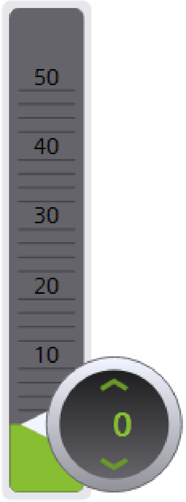
Hotkey

A key or key combination that the operator can use to actuate the button can be defined during configuration.

3.5.2.9 Slider

Use

Process values are monitored and adapted within a defined range with the "Slider" object. The monitored range is visualized in the form of a slider. By adjusting the slider, you intervene in the process and correct the displayed process value.



Layout

The settings for the position, geometry, style, color and fonts of the object are made during configuration.

In particular, the following properties are changed:

- Maximum Value and Minimum Value: Specifies the top and bottom values of the scale.
- Display current value: Specifies whether the current position of the controller appears below the slider.
- Display of bars: The sliders above and below the bar can be hidden.
- You can represent limits and ranges in different colors. The colors are defined during configuration.

If the object falls below a certain size in the light or dark style, it is automatically displayed in compact mode.

Behavior during operation

The displayed value on the slider control may deviate from the actual value of the associated tag in the following circumstances:

- The value range (minimum and maximum value) configured for the slider control does not correspond to the configured limits for the slider control tag.
- An invalid password has been entered for a password-protected slider control.

3.5.2.10 Clock

Use

The "Clock" object displays the date and time.

12
1
2
3
4
5
6
7
8
9
10
11

By default, the "Clock" object displays the date and time of the client.

If the "Process value" property of the clock is connected to a DateTime tag, the clock uses the tag value as a start value and continues counting. When the tag value is changed, the clock is synchronized and continues counting from the new value.

Layout

The display of the clock is configured in the engineering, for example:

- Whether hour markers are displayed as graduation marks or numbers.
- Whether hour hand, minute hand and second hand are displayed.

When the object in the light or dark style is less than 100 pixels high or wide in runtime, the clock is automatically displayed in compact mode.

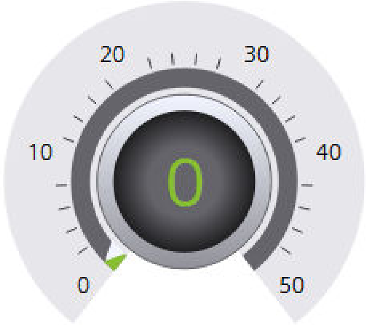
3.5.2.11 Gauge

Use

The "Gauge" object shows numeric values in the form of an analog gauge. For example, it can be seen at a glance whether the boiler pressure is in the normal range.

Note

The gauge is for display only and cannot be controlled by the operator.



Layout

The settings for the position, geometry, style, color and fonts of the object are made during configuration.

In particular, the following properties are changed:

- Display peak value: Specifies whether the actual measuring range is indicated with a peak indicator.
- Maximum Value and Minimum Value: Specifies the top and bottom values of the scale.
- Start value of the danger range and start value of the warning range: Specifies the scale value from which the danger range and the warning range start.

- Display normal range: Specifies whether the normal range is shown in color on the scale.
- Color of individual ranges: Different operating modes, such as normal range, warning range and danger range, are shown in different colors so that the operator can distinguish them easily.

If the object falls below a certain size in the light or dark style, it is automatically displayed in compact mode.

Note

The use of many differently sized "Gauge" objects can reduce the performance in Runtime. With "Gauge", avoid minimally different heights and widths, for example, 48 pixels, 49 pixels, 51 pixels, etc. Use the same sizes instead.

Display peak value

The "Display peak value" property can be used to enable a marker function for the maximum and minimum pointer movement in Runtime. The actual measuring range is shown with a min/max pointer.

Color of individual ranges

The normal range, danger range and warning range can be displayed in different colors. The colors are defined during configuration.

3.6 Basic objects

In addition to controls and elements, HMI screens contain basic objects such as circles, polygons or text boxes. Basic objects are often used for design purposes, but can also provide information about the process.

Dynamically configured basic objects react to changes in the process or to operator actions. Example: In engineering, a text box is linked to a text list that defines text entries for the value range of a tag. In Runtime, the text box always shows the text assigned to the current tag value. When the tag changes its value, the content of the text box changes.

Overview of basic objects

Depending on the configuration, screens can contain the following basic objects:

- Line
- Polyline
- Polygon
- Ellipse
- Ellipse segment
- Circle segment

- Elliptical arc
- Circular arc
- Circle
- Rectangle
- Text box
- Graphic view

Process values in text fields

If a text box has been connected to a tag in engineering, the text box shows the process value of the tag in runtime.

If the text box was connected to a tag and a text list, the text box shows the text list entry that corresponds to the tag value.

Note

If no default value is assigned to the text list and the tag value is outside the defined value range of the text list, the last valid process value displayed by the text box is output.

3.7 Popup window

Popup windows are freely movable windows that open when an event configured in the engineering system occurs. They show, for example, additional information on a partial area of the process image.

You close a popup window using the button in the top right corner of the popup window.

Example

Runtime shows a screen with an overview graphic for a pump and its valves.

Configuration in the engineering system

A faceplate instance was positioned on the screen for each valve, which is displayed by the graphic of the valve. The faceplate instances have a script that opens an additional faceplate instance in a popup window in Runtime. This second instance shows detailed information on the valve as well as input fields.

Behavior in Runtime

When you click on a valve in the overview graphic in the screen, a popup window opens. In the popup window, you can check the state of the valve and edit the valve using the input fields.

3.8 Tests and error analysis

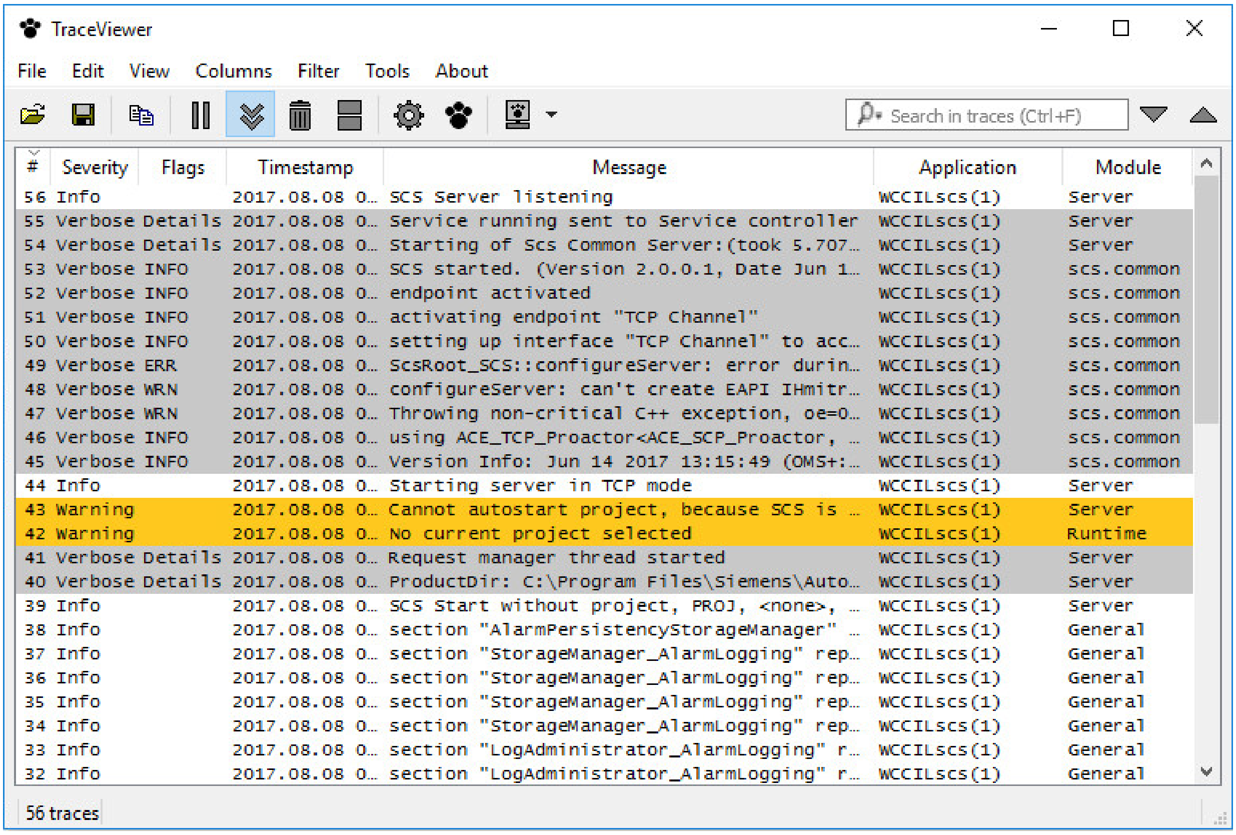
3.8.1 Trace logs for function calls and tag values

WinCC Unified provides trace logging for error analysis. Tag values and function calls can be logged for test purposes and for troubleshooting with the trace.

All trace outputs with "Fatal", "Error" or "Warning" severity are stored in LOG files (.log) in the directory "%ProgramData%\Siemens\Automation\Logfiles\WinCC_Unified_SCADA_Vxx". In case of problems you must send these files to SIEMENS Customer Support.

TraceViewer

The LOG files can be viewed with the TraceViewer. It is located in the installation directory of WinCC Unified under "WinCCUnified\bin". To open the Trace Viewer start the file "RTILtraceViewer.exe".



#	Severity	Flags	Timestamp	Message	Application	Module
56	Info		2017.08.08 0…	SCS Server listening	WCCILscs(1)	Server
55	Verbose	Details	2017.08.08 0…	Service running sent to Service controller	WCCILscs(1)	Server
54	Verbose	Details	2017.08.08 0…	Starting of Scs Common Server:(took 5.707…	WCCILscs(1)	Server
53	Verbose	INFO	2017.08.08 0…	SCS started. (Version 2.0.0.1, Date Jun 1…	WCCILscs(1)	scs.common
52	Verbose	INFO	2017.08.08 0…	endpoint activated	WCCILscs(1)	scs.common
51	Verbose	INFO	2017.08.08 0…	activating endpoint "TCP Channel"	WCCILscs(1)	scs.common
50	Verbose	INFO	2017.08.08 0…	setting up interface "TCP Channel" to acc…	WCCILscs(1)	scs.common
49	Verbose	ERR	2017.08.08 0…	ScsRoot_SCS::configureServer: error durin…	WCCILscs(1)	scs.common
48	Verbose	WRN	2017.08.08 0…	configureServer: can't create EAPI IHmitr…	WCCILscs(1)	scs.common
47	Verbose	WRN	2017.08.08 0…	Throwing non-critical C++ exception, oe=0…	WCCILscs(1)	scs.common
46	Verbose	INFO	2017.08.08 0…	using ACE_TCP_Proactor<ACE_SCP_Proactor, …	WCCILscs(1)	scs.common
45	Verbose	INFO	2017.08.08 0…	Version Info: Jun 14 2017 13:15:49 (OMS+:…	WCCILscs(1)	scs.common
44	Info		2017.08.08 0…	Starting server in TCP mode	WCCILscs(1)	Server
43	Warning		2017.08.08 0…	Cannot autostart project, because SCS is …	WCCILscs(1)	Server
42	Warning		2017.08.08 0…	No current project selected	WCCILscs(1)	Runtime
41	Verbose	Details	2017.08.08 0…	Request manager thread started	WCCILscs(1)	Server
40	Verbose	Details	2017.08.08 0…	ProductDir: C:\Program Files\Siemens\Auto…	WCCILscs(1)	Server
39	Info		2017.08.08 0…	SCS Start without project, PROJ, <none>, …	WCCILscs(1)	Server
38	Info		2017.08.08 0…	section "AlarmPersistencyStorageManager" …	WCCILscs(1)	General
37	Info		2017.08.08 0…	section "StorageManager_AlarmLogging" rep…	WCCILscs(1)	General
36	Info		2017.08.08 0…	section "StorageManager_AlarmLogging" rep…	WCCILscs(1)	General
35	Info		2017.08.08 0…	section "StorageManager_AlarmLogging" rep…	WCCILscs(1)	General
34	Info		2017.08.08 0…	section "StorageManager_AlarmLogging" rep…	WCCILscs(1)	General
33	Info		2017.08.08 0…	section "LogAdministrator_AlarmLogging" r…	WCCILscs(1)	General
32	Info		2017.08.08 0…	section "LogAdministrator_AlarmLogging" r…	WCCILscs(1)	General

3.8.2 Debugging scripts

3.8.2.1 Basics of debugging

Introduction

For example, you can use a debugger to test whether correct values are being transferred to tags and whether abort conditions are being correctly implemented. Check the following in the debugger:

- Source code of functions
- Function sequence
- Values

Note

Your code is displayed in the debugger but is write-protected.

Basic procedure

To find an error, check the script with the debugger.

The following options are available for your support:

- Setting breakpoints
- Step-by-step execution
- Viewing values parallel to execution of the script

You do not edit the code of your scripts directly in the debugger. When you find an error, follow these steps:

1. Correct the error in the engineering system.
2. Compile the changed code.
3. Load the runtime.
4. Update the debugger.

3.8.2.2 Design and function of the debugger

Google Chrome provides the user interface of the debugger. Not all functions of the user interface of the debugger are relevant for debugging WinCC Unified Scripts. Only the functions that are needed to debug scripts in WinCC Unified are explained below.

You can find more information on Chrome DevTools under: https://developers.google.com/web/tools/chrome-devtools/.

The debugger is divided into two areas:

- Debugger for screens
- Debugger for jobs

With the debugger for screens you view scripts at screens and screen objects. With the debugger for jobs, you view scripts that you have configured in the Scheduler.

Start page of the debugger

After the debugger has been started, its start page is displayed.

The available contents differ depending on the selected area.

On the start page of the debugger for screens you can see two different contexts:

- Dynamizations (e.g. "UMCadmin@192.168.116.144 VCS_1 Dynamics")
- Events (e.g. "UMCadmin@192.168.116.144 VCS_1 Events")

The name of the contexts is composed as follows:

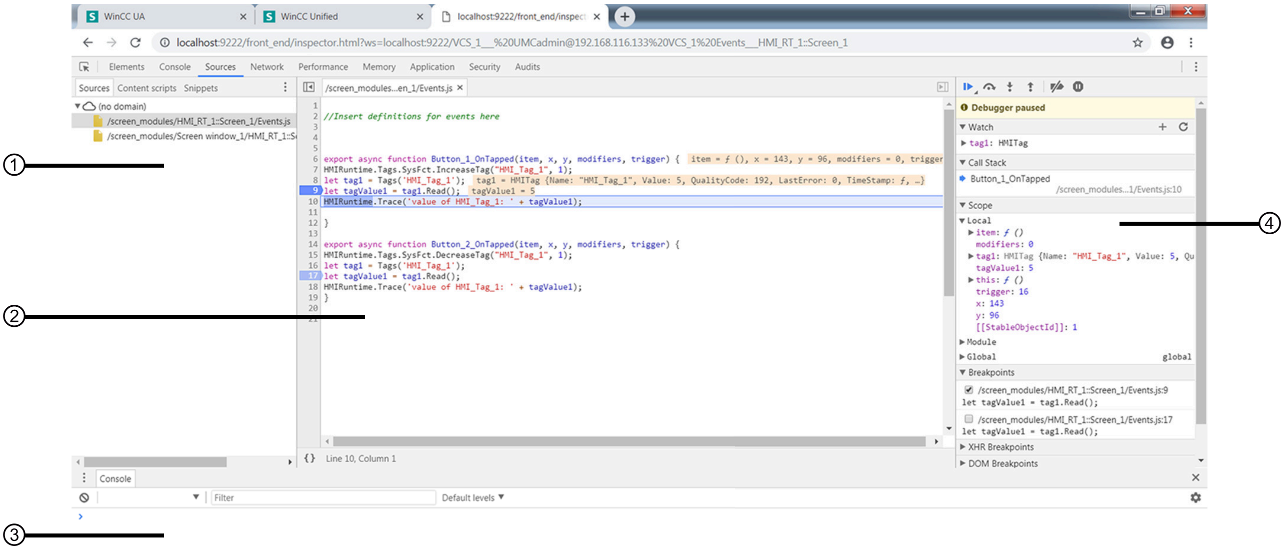
- UMCadmin: User name
- 192.168.116.144: IP address of the computer
- VCS: Name of the graphic component
- _1: Number of the open client
- Events/Dynamics: Scripts at events or dynamizations

Note

A client corresponds to a tab in Google Chrome in which the runtime is open. When you have opened runtime in multiple tabs, multiple clients are used. The client opened first is given the number 1. Numbering is reset when the runtime is restarted.

On the start page of the debugger for jobs you can see the context "JobsExecution".

User interface of the debugger



WinCC UA
WinCC Unified
localhost:9222/front_end/inspect
localhost:9222/front_end/inspector.html?ws=localhost:9222/VCS_1__%20UMCadmin@192.168.116.133%20VCS_1%20Events__HMI_RT_1::Screen_1
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
Sources
Content scripts
Snippets
(no domain)
/screen_modules/HMI_RT_1::Screen_1/Events.js
/screen_modules/Screen window_1/HMI_RT_1::S
/screen_modules...en_1/Events.js
Line 10, Column 1
Console
Filter
Default levels
1
2
3
4

```
//Insert definitions for events here


export async function Button_1_OnTapped(item, x, y, modifiers, trigger) {  item = ƒ (), x = 143, y = 96, modifiers = 0, trigger
HMIRuntime.Tags.SysFct.IncreaseTag("HMI_Tag_1", 1);
let tag1 = Tags('HMI_Tag_1');  tag1 = HMITag {Name: "HMI_Tag_1", Value: 5, QualityCode: 192, LastError: 0, TimeStamp: ƒ, …}
let tagValue1 = tag1.Read();  tagValue1 = 5
HMIRuntime.Trace('value of HMI_Tag_1: ' + tagValue1);

}

export async function Button_2_OnTapped(item, x, y, modifiers, trigger) {
HMIRuntime.Tags.SysFct.DecreaseTag("HMI_Tag_1", 1);
let tag1 = Tags('HMI_Tag_1');
let tagValue1 = tag1.Read();
HMIRuntime.Trace('value of HMI_Tag_1: ' + tagValue1);
}
```

```
Debugger paused
▼ Watch
  ▶ tag1: HMITag
▼ Call Stack
  Button_1_OnTapped
                 /screen_modules...1/Events.js:10
▼ Scope
▼ Local
  ▶ item: ƒ ()
    modifiers: 0
  ▶ tag1: HMITag {Name: "HMI_Tag_1", Value: 5, Qu
    tagValue1: 5
  ▶ this: ƒ ()
    trigger: 16
    x: 143
    y: 96
    [[StableObjectId]]: 1
▶ Module
▶ Global                                   global
▼ Breakpoints
  ☑ /screen_modules/HMI_RT_1::Screen_1/Events.js:9
  let tagValue1 = tag1.Read();
  □ /screen_modules/HMI_RT_1::Screen_1/Events.js:17
  let tagValue1 = tag1.Read();
▶ XHR Breakpoints
▶ DOM Breakpoints
```

① Navigation area

② Code display area

③ Console

④ Debugging area

Navigation area

In the navigation area, the available contents for the screen shown in runtime are displayed in groups. The available groups vary depending on the use of scripts and functions.

Groups in the debugger for screens

The debugger for screens can contain the following groups in the dynamizations context:

- A group for scripts that were configured for dynamizations.
- One group per screen window in which scripts were configured for dynamizations.

The debugger for screens can contain the following groups in the events context:

- A group for scripts that were configured for events.
- One group for functions that were configured for events using the function list.
- One group per screen window in which scripts were configured for events.
- One group per screen window in which functions were configured for events using the function list.

Groups in the debugger for jobs

The debugger for jobs can contain the following groups:

- A group for scripts that were configured for tasks.
- One group for functions that were configured for tasks using the function list.

Code display area

Your code is displayed in the code display area. The rows are numbered.

Debugging area

The debugging area offers the following relevant options for WinCC Unified:

- Toolbar: Control for executing the script
- "Watch": Display of values
- "Callstack": Display of the current call stack
- "Scope": Available local values ("Local"), functions ("Module") and global values ("Global"),
- "Breakpoints": List of set breakpoints

3.8.2.3 Enabling the debugger

Requirement

- SIMATIC Runtime Manager is installed.
- The logged-on user belongs to the Windows user group "SIMATIC HMI".

Note

The debugger is only available locally.

Remote access from the debugger to other devices is not possible.

Procedure

The debugger is disabled by default.

Note

The debugger should be disabled in production operation, as using the debugger can endanger system stability and security. Actions can accumulate if the debugger is, for example, at a breakpoint for a long time or the screen is not refreshed.

To enable the debugger, follow these steps:

1. Start the SIMATIC Runtime Manager application.
2. Click the ⚙ button in the toolbar.
3. Switch to the "Scripts Debugger" tab.
4. To enable the debugger for screens, select the "Enable" check box in the "Screen debugger" area.
5. To enable the debugger for scheduled tasks, select the "Enable" check box in the "Scheduler debugger" area.
6. Assign an available port number to the debugger for screens (default port number: 9222).
7. Assign an available port number to the debugger for jobs (default port number: 9224).
8. Confirm your entries.

Note

Start Runtime after enabling the debugger.

3.8.2.4 Starting the debugger

Requirement

- Google Chrome (as of version 70) is installed.
- A project is opened in runtime.
- The debugger was activated in SIMATIC Runtime Manager.

Note

The debugger is only available locally.

Remote access from the debugger to other devices is not possible.

Procedure

1. In a new tab, call up the URL chrome://inspect in Google Chrome.
2. The home page of the Chrome DevTools is loaded in the tab.
3. Click "Devices".
4. Select the "Discover network targets" check box.
5. Click "Configure".

6. In the "Target discovery settings" dialog box, enter one of the following strings:
   - `127.0.0.1:<Port number>`
   - `localhost:<Port number>`

   Use the port entered for the Script Debugger in SIMATIC Runtime Manager.
7. Press <Enter>.
8. Click "Done".
9. Under "Remote Target", click "inspect" for the desired target.
   The DevTools open in a separate window with the selected target.
10. In the DevTools, select "Sources".
    The debugger is displayed.
11. Click "Toggle screencast".
12. In the navigation area under "Page", select the desired script module.

Updating the debugger

The debugger must be updated:

- After starting a new project
- After restarting a running project, for example, because you have reloaded the project in engineering with "Download to device > Software (all)".
- After a screen change in Runtime

The connection to the debugger is lost in each case. Google Chrome therefore shows an error message and asks whether you want to restore the connection.

To restore the connection, proceed as follows:

1. Close the DevTools window.
2. On the DevTools start page under "Remote Target", click "inspect" again for the desired target.

Stopping the debugger

Exit the debugger by closing the DevTools window and, if necessary, the DevTools homepage.

This does not stop runtime.

3.8.2.5 Working with breakpoints

Set breakpoints to stop the execution of the script at certain points and thus localize errors step-by-step. Previously set breakpoints are still available after updating the debugger.

Requirement

- Runtime has started.
- The debugger has been started.
- The group you want to debug is selected.

Pause script

To pause the execution of a script, you have 2 options:

- To pause the script immediately, click the ⏸ "Pause script execution" button while the script is being executed.
- Set a breakpoint in the desired line.
  The script pauses when a breakpoint is reached.

To pause a script at a breakpoint that is configured to an event, follow these steps:

1. Set a breakpoint in the script.
2. Trip the respective event in runtime.
   The script pauses at the breakpoint.

Setting breakpoints

You have several options to set a breakpoint in a line of the script:

- Click on the line number.
- Right-click the line number and select "Add Breakpoint".

All set breakpoints are displayed in the debugging area under "Breakpoints".

Linking breakpoints to conditions

To link a breakpoint to a condition, proceed as follows:

1. Open the shortcut menu of the relevant line.
2. Select the entry "Add conditional breakpoint".
   Execution of the script is stopped at the breakpoint when the condition is fulfilled.

Edit conditions as follows:

1. Open the shortcut menu of the relevant line.
2. Select the entry "Edit breakpoint...".

To prevent the script from pausing at a selected line, proceed as follows:

1. Open the shortcut menu of the respective line.
2. Select the entry "Never pause here".

Showing and hiding breakpoints

When you hide a breakpoint, its position is retained. The script then ignores the hidden breakpoint. When you need the breakpoint again, it can simply be shown.

In the debugging area, all breakpoints set in the selected group are displayed under "Breakpoints".

You have several options to show a breakpoint:

- Set the check mark in front of the relevant breakpoint in the debugging area under "Breakpoints".
- Alternatively, right-click the number of the respective line in the code display area and then select "Enable breakpoint".

You have several options to hide a breakpoint:

- Remove the check mark in front of the relevant breakpoint in debugging area under "Breakpoints".
- Alternatively, right-click the number of the respective line in the code display area and then select "Disable breakpoint".

To show or hide all breakpoints, follow these steps:

1. Open the shortcut menu in the debugging area under "Breakpoints".
2. Select "Enable all breakpoints" or "Disable all breakpoints"

Enabling and disabling breakpoints

You can enable or disable all breakpoints independent of showing or hiding individual breakpoints.

You have several options to enable or disable all breakpoints:

- Click on the "Deactivate breaktpoints" button in the debugging area.
- Open the shortcut menu of a breakpoint in the debugging area and select "Activate breakpoints" or "Deactivate breakpoints".
- Press <Ctrl + F8>.

Deleting breakpoints

You have several options to delete a breakpoint:

- Click on the breakpoint in the code display area.
- Open the shortcut menu of the breakpoint in the code display area and select "Remove breakpoint".
- Open the shortcut menu in the debugging area under "Breakpoints" and select "Remove breakpoint"..

To delete breakpoints, the shortcut menu offers the following additional options in the debugging area under "Breakpoints":

- Delete all breakpoints ("Remove all breakpoints")
- Delete all breakpoints except the selected breakpoint ("Remove other breakpoints")

3.8.2.6 Step-by-step execution of scripts

Introduction

The following options are available to execute your script step-by-step:

- Execute script to the next breakpoint
- Force execution of a script
- Execute script to the next function call
- Jump into a function
- Jump out of a function
- Execute script up to a selected line
- Pause at Exceptions
- Use call stack

Requirement

- The group you want to debug is selected.
- The script pauses at a breakpoint.

Execute script to the next breakpoint

To pause the continuation of a script, you have several options:

- Click on the ❙▶ "Resume script execution" button in the debugging area.
- Press the <F8> key.
  The script is executed to the next breakpoint. If there is no other breakpoint, the script is executed completely.

Force execution of a script

To ignore the following breakpoints when resuming execution of a paused script, proceed as follows:

1. Click and hold down the ❙▶ "Resume script execution" button.
   The ▶ "Force script execution" button appears.
2. Move the mouse pointer to the ▶ "Force script execution" button while keeping the mouse button pressed.
3. Now release the mouse button.
   The script is executed to the end.

Execute script to the next function call

If a line with a breakpoint contains a function that you are not interested in, you can suppress the debugging of this function:

- Click on the ↷ "Step over next function call" button in the debugging area.
- Press the <F10> key.
  The function is executed without the script pausing within the function.

Jumping into a function

If the script pauses in a line containing a function that interests you, you can pause the script in that function:

- Click on the ↓ "Step into next function call" button in the debugging area.
- Press the <F11> key.
  The script pauses in the first line of the function.

Note

You can only jump into functions that you have defined yourself.

Jump out of a function

If the script pauses within a function that you are not interested in, you can suppress further debugging of this function:

- Click on the ↑ "Step out of current function" button in the debugging area.
- Press the key combination <Shift + F11>.

Note

You can only jump out of a function that you have defined yourself.

Execute script up to a selected line

To pause a paused script again at a selected line, proceeds as follows:

1. Right-click the number of the line in the code display area.
2. Select the entry "Continue to here".
   The script pauses at the selected line.

Pause at Exceptions

- To pause the script at Exceptions, click on the ⏸ "Pause on exceptions" button in the debugging area.

Use call stack

- To jump into a function of the call stack, click on the corresponding entry under "Call Stack".

Note

You can only jump into functions that you have defined yourself.

3.8.2.7 Show values

Introduction

To identify errors in your script efficiently, have current values displayed while the script is being executed. This way you can view properties of objects or parameters of functions, for example. You can find additional information on objects and their properties under "WinCC Unified Object Model".

Requirements

- The group you want to debug is selected.
- The script pauses at a breakpoint.

Procedure

You view values by moving the mouse over the label in the code display area.

You also have the following options to view values:

- In the debugging area under "Scope"
- In the debugging area under "Watch"
- In the console

"Scope" area

All local values ("Local"), functions ("Module") and global values ("Global") that are defined at this time are displayed in the "Scope" area.

The values cannot be edited.

"Watch" area

In the "Watch" area, you view how values change in the course of a script.

The following buttons are available to you:

- + "Add expression": Add a value
- ↻ "Refresh": Refresh the "Watch" area
- ▬ "Delete watch expression": Delete a value from the "Watch" area. Available when the mouse pointer is located above the respective value.

Console

The values available at the current time can be called in the console.

- You show or hide the console with <Esc>.

Call the current values in the console as follows:

1. Enter the name of a local or global value in the console.
2. Press <Enter>.

Options

4

4.1 Plant Intelligence Options

Overview

The Plant Intelligence options offer optional enhancements to the WinCC Unified Basic System. These can be combined freely in line with your requirements.

The options allow you to plan production processes and analyze and optimize the overall effectiveness of your plant. In addition, you can design flexible production processes and coordinate complex and interlinked production processes.

Plant Intelligence options

- WinCC Unified Performance Insight
  Define, calculate and analyze plant-specific key performance indicators (KPIs) for individual aggregates, machines or entire production lines in machine-oriented or line-oriented manufacturing plants.
- WinCC Unified Calendar
  Plan, configure and manage events and actions together in a shared calendar in WinCC and combine these with WinCC tags or scripts.
- WinCC Unified Sequence
  Control step-based and sequence-based processes, define the production steps of the production units and adapt the production processes flexibly in runtime.
- WinCC Unified Line Coordination
  Coordinate and supervise processes in the production line in your plant. Control and manage recipes, processes and jobs for the production of various end products.

Note

The Plant Intelligence options are successively released as add-on packages. To use the Plant Intelligence options, you require the relevant software packages and licenses.

You can find information on the licenses in the TIA Portal installation instructions in the section "Licensing of Plant Intelligence options".

Requirements

Please note the following requirements for using the options:

- SIMATIC WinCC Runtime Unified is installed.
- STEP7 Professional is installed.
- Plant Intelligence option, including license, is installed.
- The plant hierarchy is configured.
- License for the respective option is available.
- The configuration engineer has WinCC experience.

User administration in Runtime 5

5.1 User management scenarios

In the user management, you create new users and manage existing users.

Select one of the following scenarios of local or central user management.

Creating a local user management on a PC

WinCC Unified Runtime and the user management are installed on one PC.

Central user management

TIA Portal and WinCC Unified Runtime can be installed on one PC, UMC Server runs on a different PC.

5.2 User management in Runtime

5.2.1 User logon

Introduction

From a PC, you access local user management via an Internet browser.

To manage the local users on a Unified PC, you require the "User management" function rights. Configure a user with the required rights in the engineering system and load the user into Runtime.

Note

The specific possible operations depend on the function right.

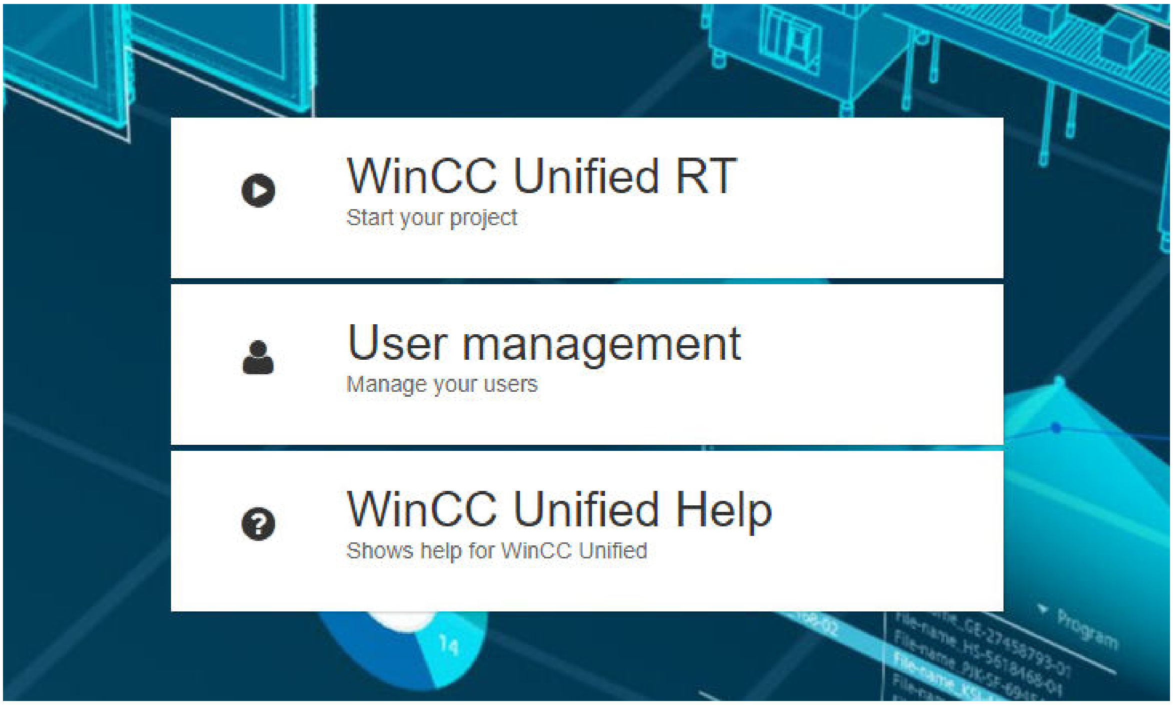
Requirement

- The user has the "User management" function rights.
- Internet browser is open.

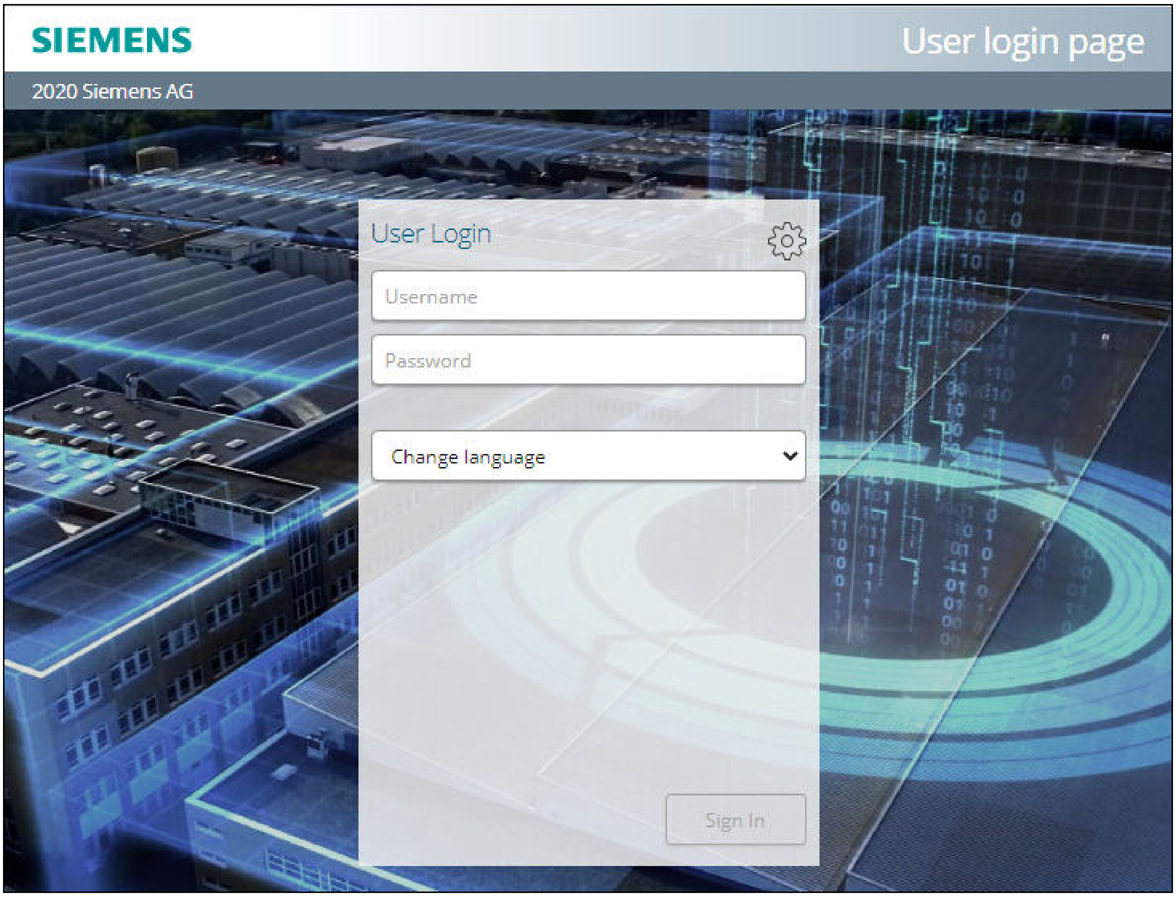
Logging on to the user management

To log on to the user management in Runtime, follow these steps:

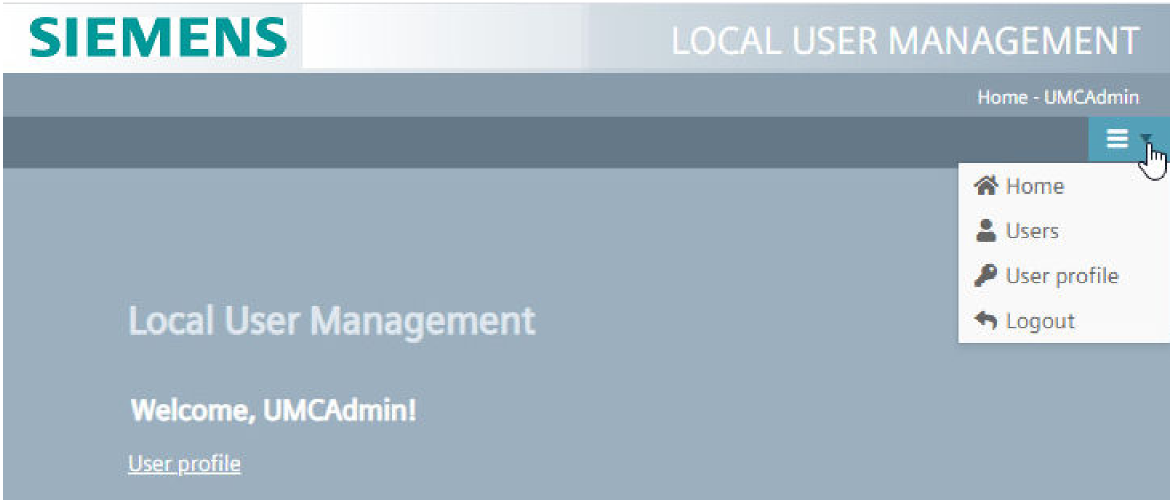
1. In the browser, enter the IP address of the Runtime PC "https://<PC-IP>/umc". If runtime is installed on the same PC as the browser, enter the address "https://localhost/umc".
   The start page of Runtime is displayed.



2. Click the "User management" button. The "User login" dialog is displayed.



3. Type in the user name and password.
4. If required, use the selection list to change the displayed language.
5. Click "Login".
   The user management start page opens in Runtime.



5.2.2 Structure of the start page

Introduction

In menu on the start page, select whether you want to manage the users, change the password or language, or log out. You can find the menu via the drop-down list in the upper right corner.

Note

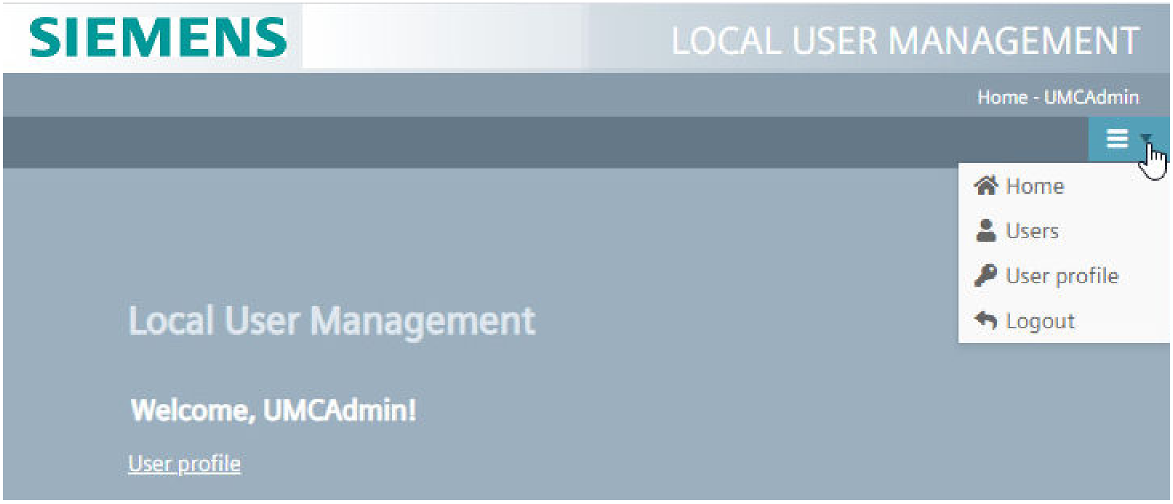
Users with the "User management" function right have access to all functions.

Users without the "User management" function right can change their password under "User profile".

Menu

The following options are available to you under the symbols in the menu:

- "Home"
  This takes you to the start page of the user management.
- "Users"
  You can create new users or manage the existing users.
- "User profile"
  You can change your password and switch the language.
- "Logoff"
  You will be logged out directly and can log in again.



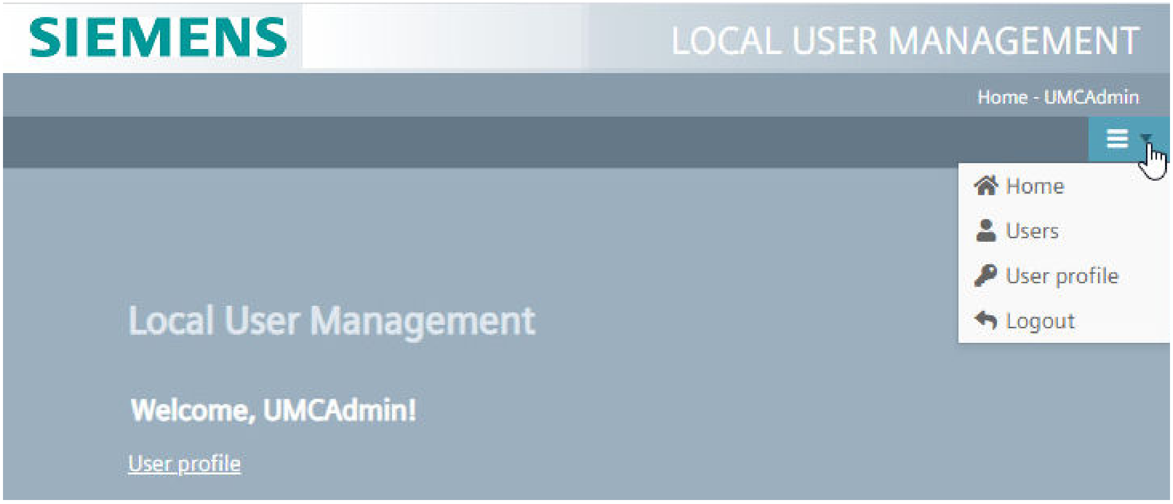
5.2.3 Changing your password

Introduction

You can change your own password in the user management.

Requirement

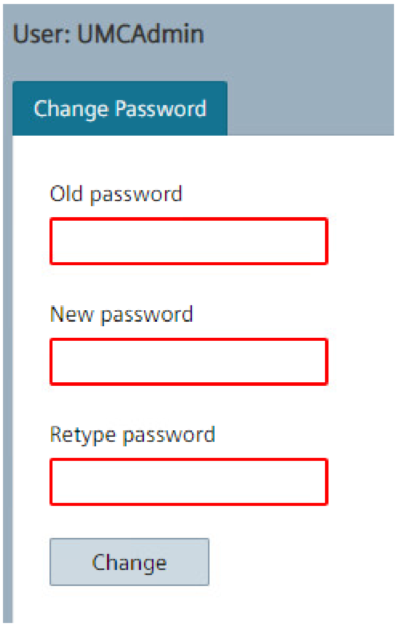
- You have the "User management" function right.
- The home page of the user management is open.



Procedure

To change the password, follow these steps:

1. Select "User profile" directly on the home page or in the menu.
   The "Change Password" dialog is displayed.

2. Change the password and save the change with the "Change" button. The password must meet the password policies.

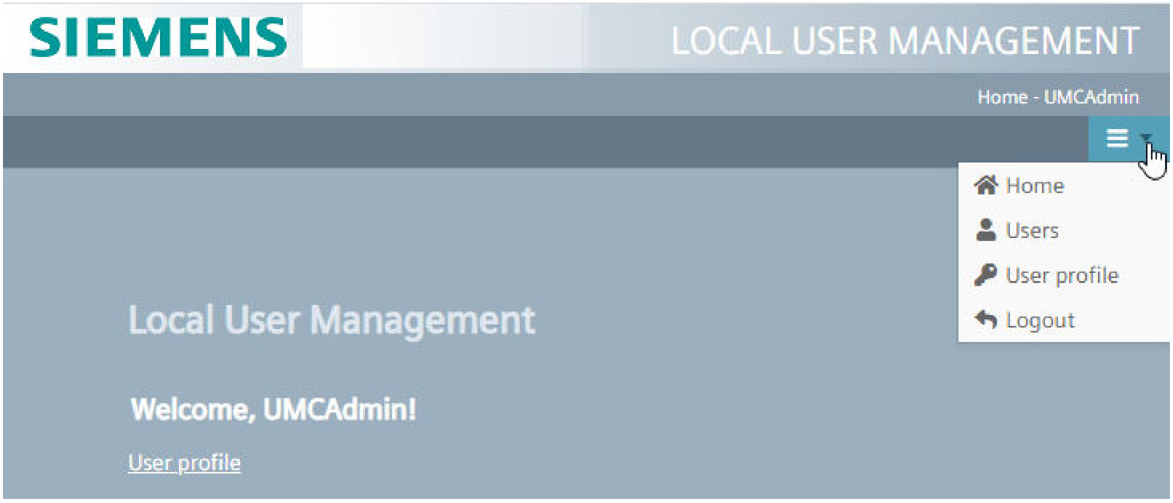
5.2.4 Managing the user list

Introduction

In the user list you can manage the data of the other users.

Requirement

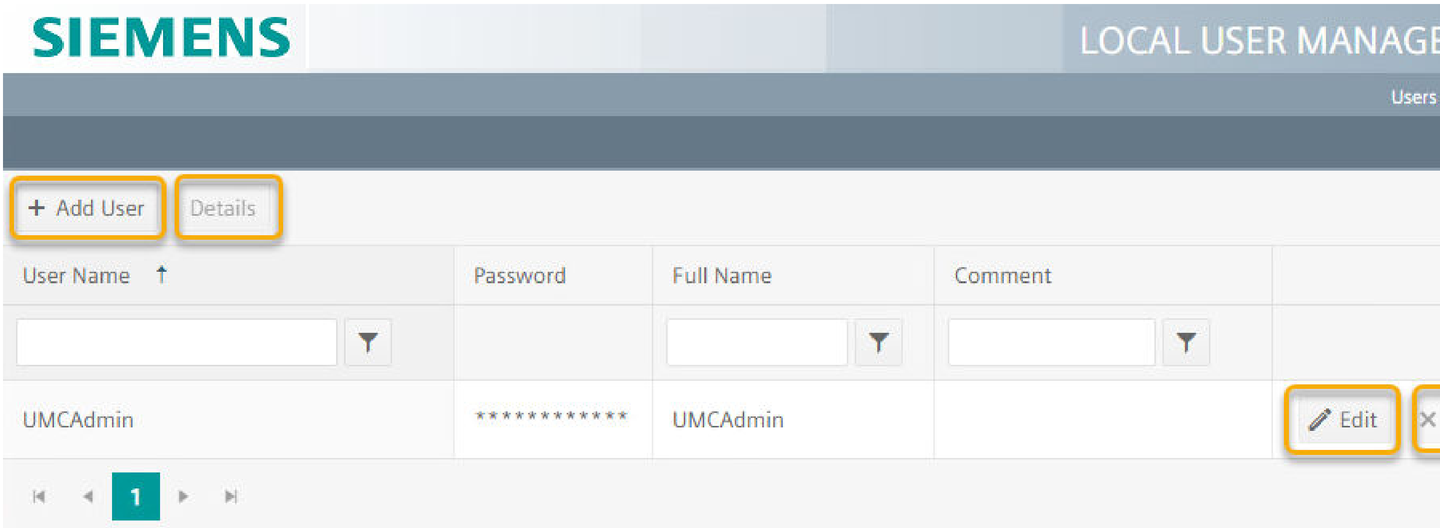
- You have the "User management" function right.
- The home page of the user management is open.



Opening a user list

To display the user list, click "Users" in the menu on the homepage.

The user list is displayed.



Options in the user list

In the user list you can manage the data of the user via the following buttons:

- "Add users"
- "Details"

- "Edit"
- "Clear"

In the user list, you can:

- Sort users by user name or comment.
- Filter users by user name or comment.
- Display 20 users on one page. Additional users are displayed on a new page. You can switch between the pages.

5.2.5 Changing the password of a different user

Introduction

In the user management you can change the password of a different user. You can also edit the comment.

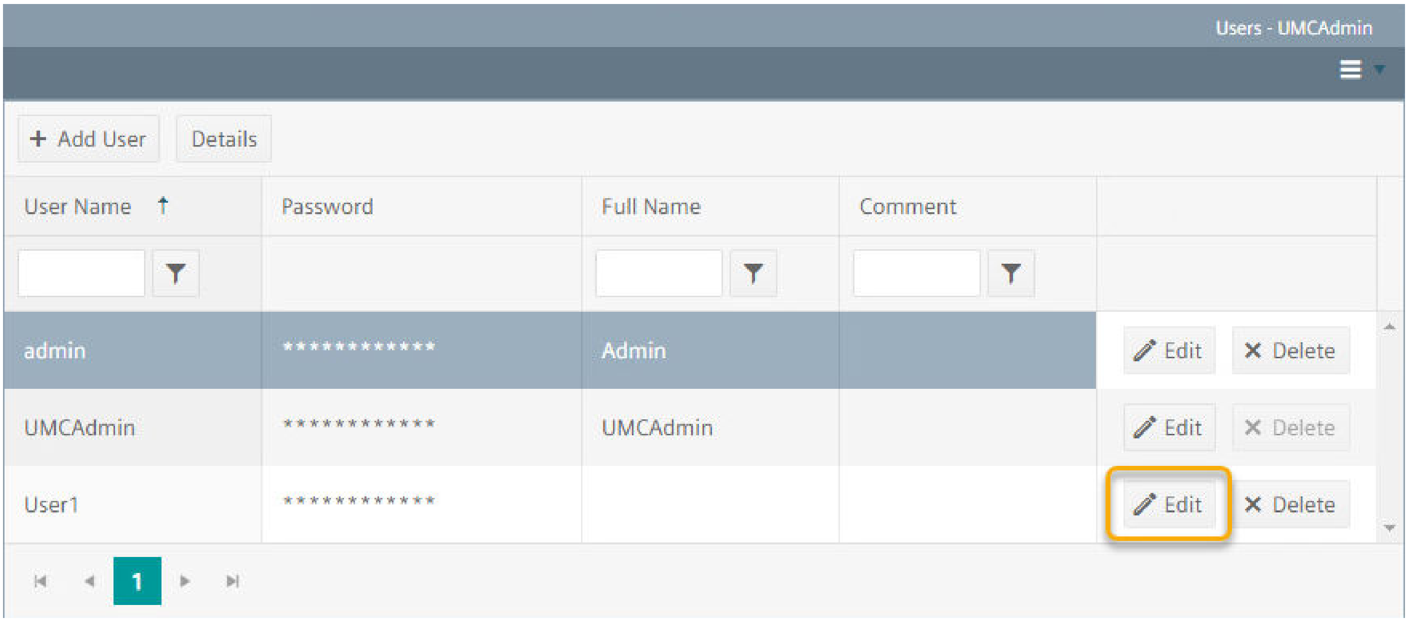
Requirement

- You have the "User management" function right.
- The home page of the user management is open.

Changing the password and comment

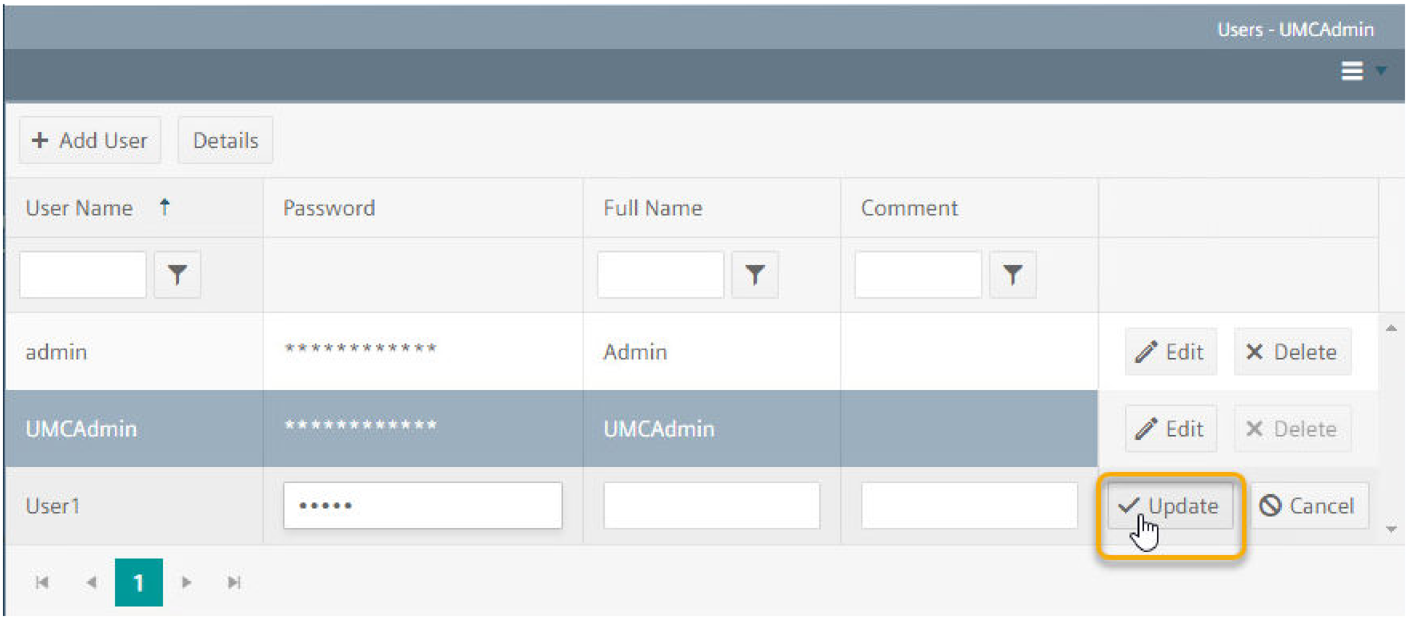
To change the password or comment of a user in the user list, follow these steps:

1. Select "Users" in the menu.
   The user list is displayed.



User Name ↑	Password	Full Name	Comment	
admin	************	Admin		Edit ✕ Delete
UMCAdmin	************	UMCAdmin		Edit ✕ Delete
User1	************			Edit ✕ Delete

2. Select a user and click on "Edit" in the respective row.
3. Change the password or the comment and save the change with the "Update" button.



User Name ↑	Password	Full Name	Comment	
admin	************	Admin		Edit ✕ Delete
UMCAdmin	************	UMCAdmin		Edit ✕ Delete
User1	•••••			✓ Update ⃠ Cancel

5.2.6 Editing password, status or role

Introduction

In the user list you can edit the password, the status or the role of a user.

Requirement

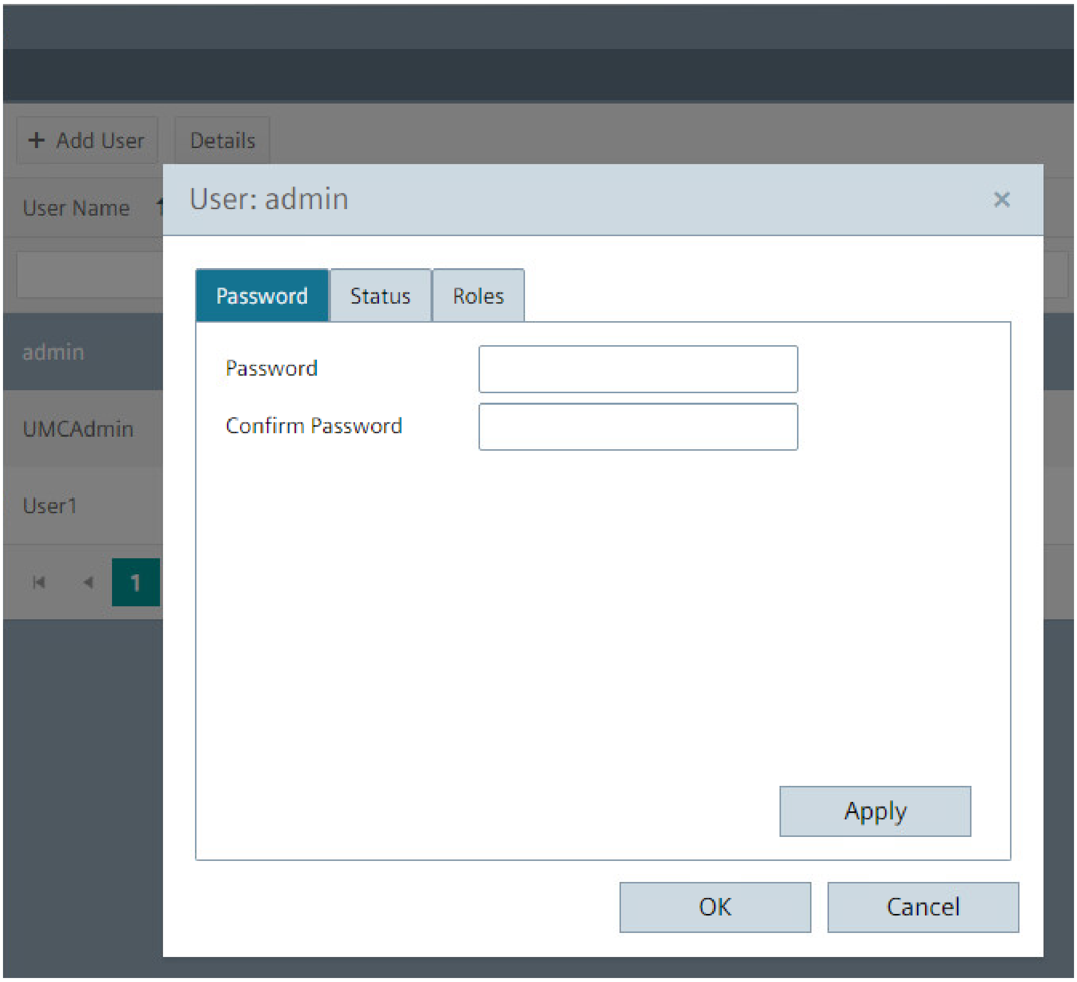
- You have the "User management" function right.
- The home page of the user management is open.

Changing the password

To change the password of a user, follow these steps:

1. Select "Users" in the menu. The user list is displayed.
2. Select a user and click the "Details" button.

3. Enter the new password in the "Password" tab and confirm the password.
4. Confirm your entries with the "Apply" button.
   Save the settings with "OK".

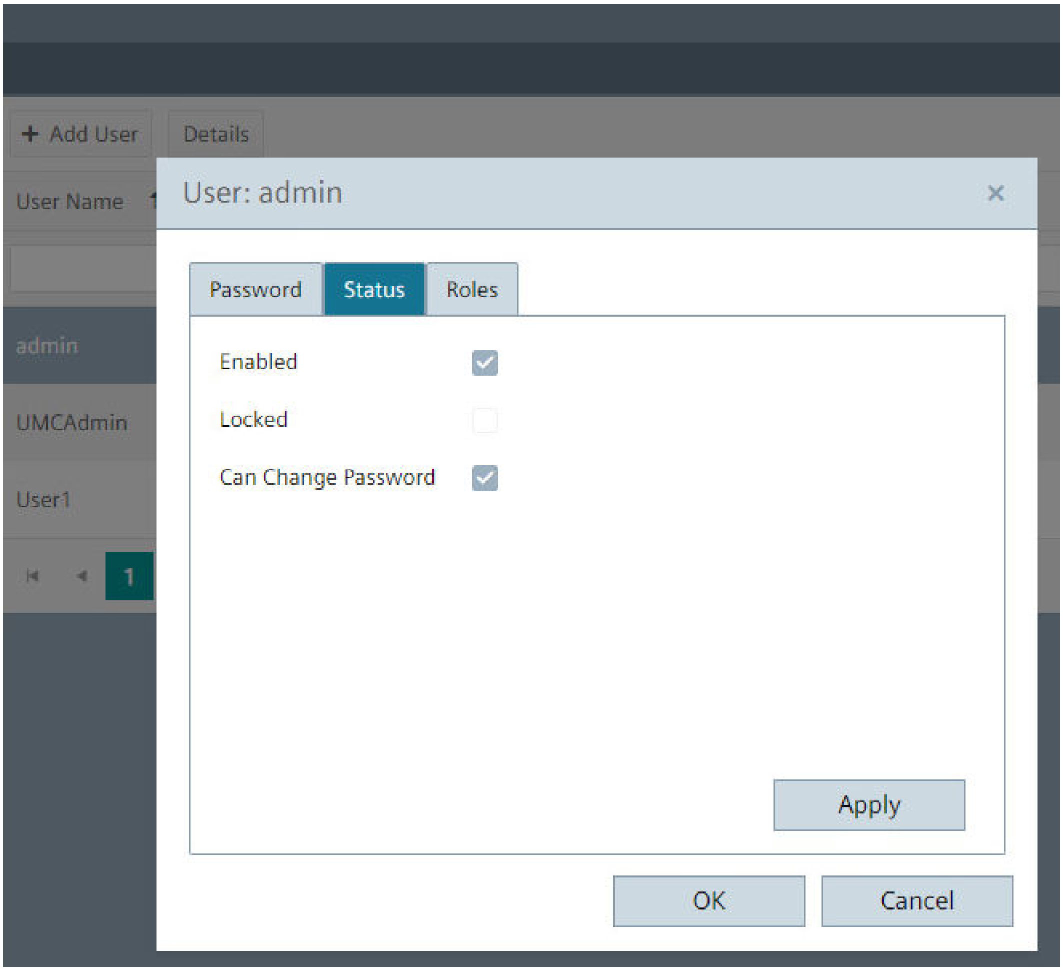


Changing the status

To edit the status of a user, follow these steps:

1. Select "Users" in the menu. The user list is displayed.
2. Select a user and click the "Details" button.

3. In the "Status" tab, you can disable the user or keep this user from changing the password. You cannot change the "Locked" property.
4. Confirm your entries with the "Apply" button.
   Save the settings with "OK".


User: admin

Enabled ☑

Locked □

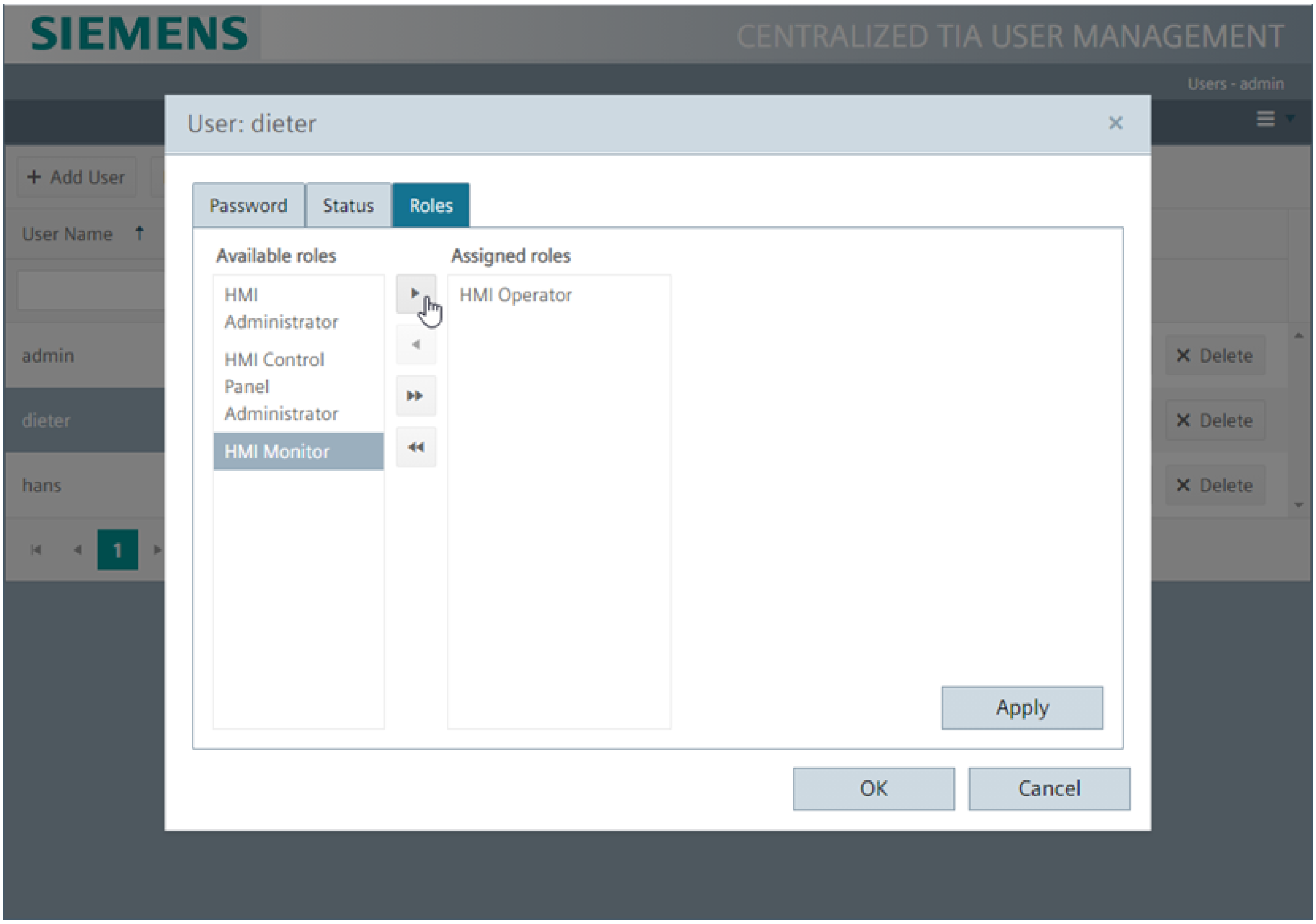
Can Change Password ☑

Changing the role

To edit the role of a user, follow these steps:

1. Select "Users" in the menu. The user list is displayed.
2. Select a user and click the "Details" button.
3. In the "Roles" tab, you can change the roles and thus the associated function rights of the user:
   - Select a role from the "Available roles" or "Assigned roles" list.
   - Change the assignment of this role using the buttons between the two lists.
   - Confirm your entries with the "Apply" button.
     Save the settings with "OK".

   The figure below shows you how to assign the "HMI Monitor" role to a user in addition to the "HMI Operator" role.



Note

Note that at least one user in the project has the "HMI Administrator" role. If access to the user management is not possible, a complete download from the TIA Portal is necessary.

5.2.7 Adding users

Introduction

You can add a new user in the user list.

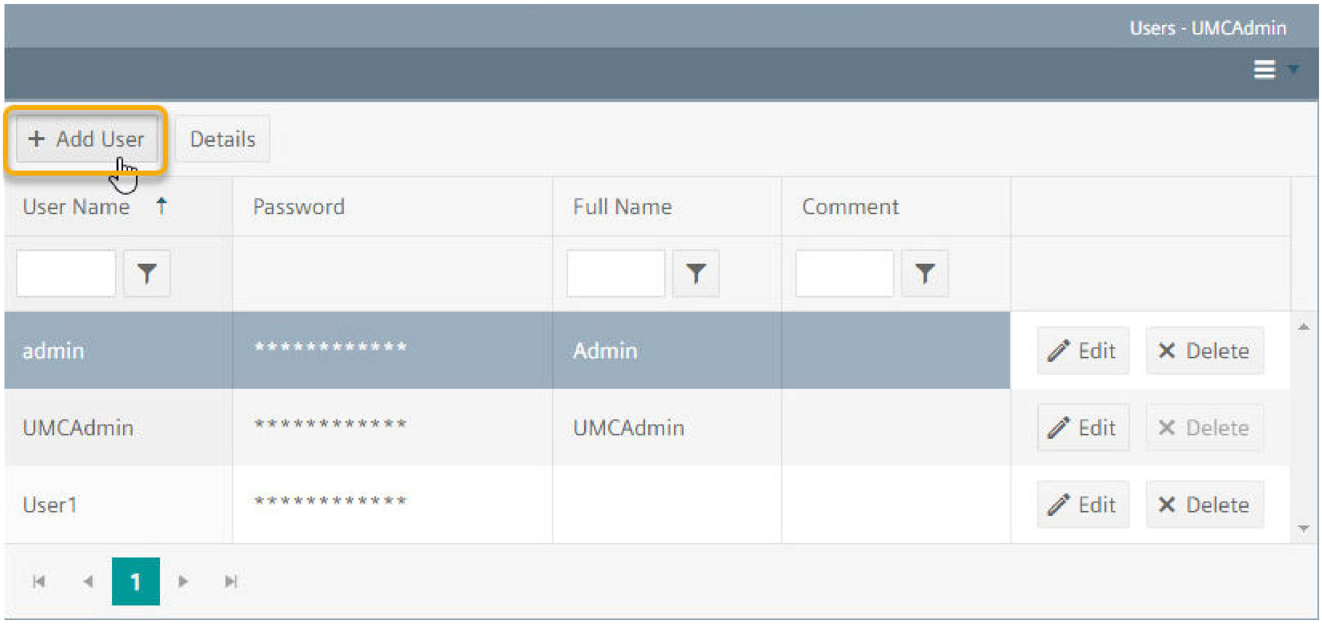
Requirement

- You have the "User management" function right.
- The home page of the user management is open.

Adding a new user

To add a new user, follow these steps:

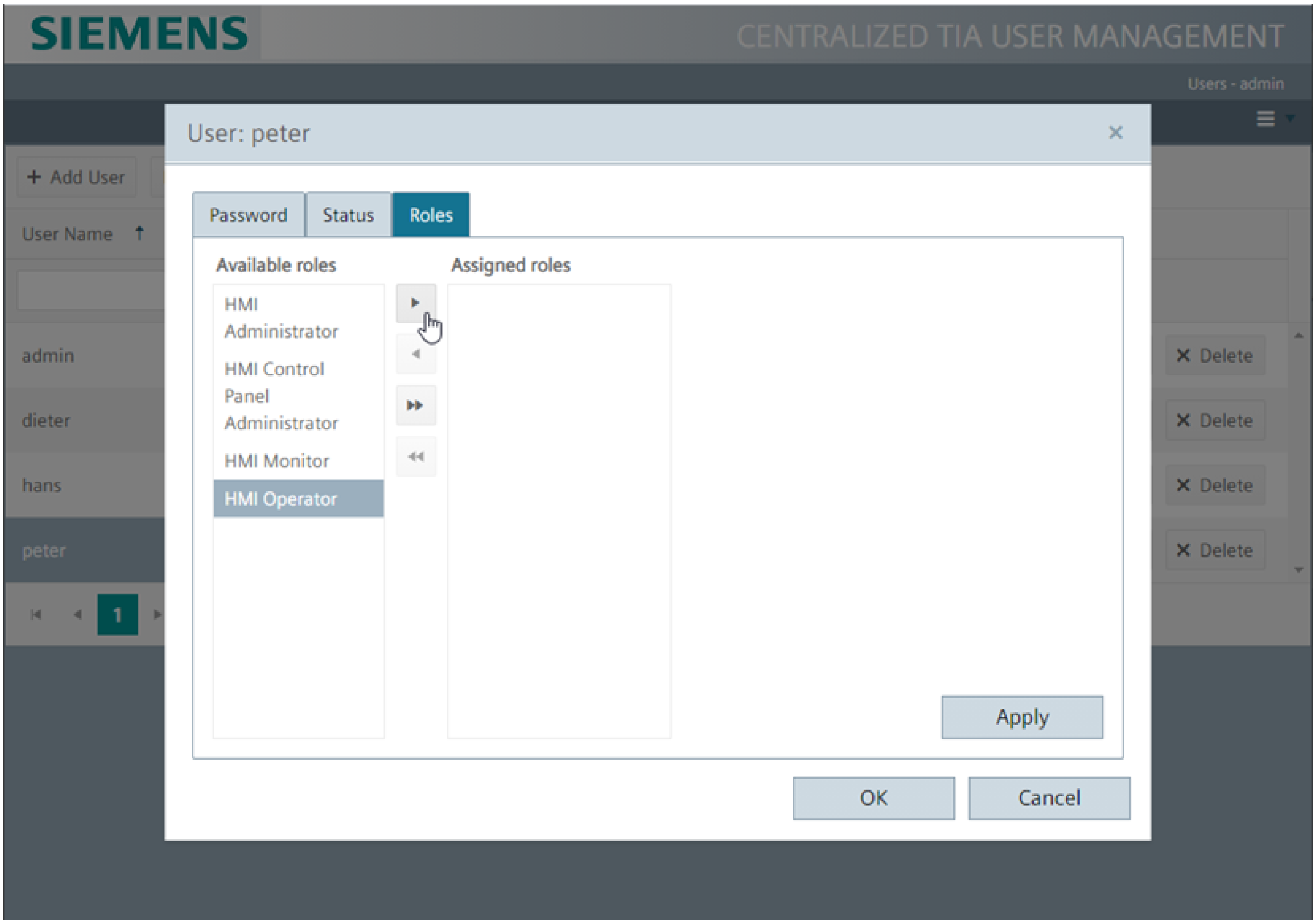
1. Select "Users" in the menu. The user list is displayed.
2. In the user list, click "Add User".



User Name ↑	Password	Full Name	Comment	
admin	************	Admin		Edit ✕ Delete
UMCAdmin	************	UMCAdmin		Edit ✕ Delete
User1	************			Edit ✕ Delete

3. A new row is displayed for the new user in the user list. Enter the information of the new user in the row.

4. Click "Details" in the user list. Assign roles to the new user.



5. Confirm your entries with the "Apply" button.
   Save the settings with "OK".

5.2.8 Deleting users

Introduction

You can delete a user in the user list.

Requirement

- You have the "User management" function right.
- The home page of the user management is open.

Deleting users

To delete a user, follow these steps:

1. Select "Users" in the menu. The user list is displayed.
2. Select the user.
3. Click the "Delete" button in the row. The user is deleted.

Deleting the user from the user list will become effective once the user logs off in Runtime.

5.2.9 Logging a user out

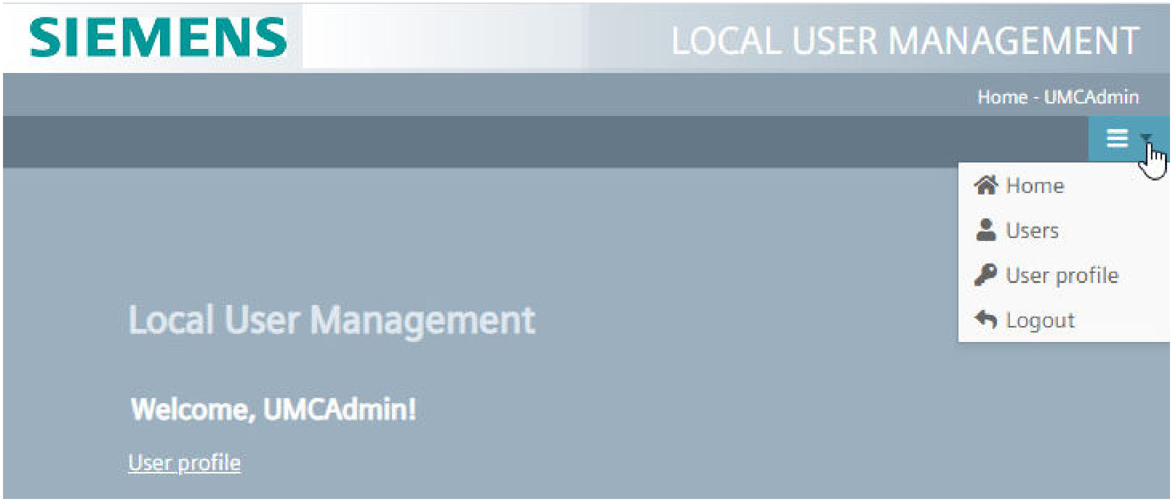
Introduction

You can log out from the user management.

Logging out

To log out, proceed as follows:

1. Close all open pages.
2. Select "Logout" from the menu.

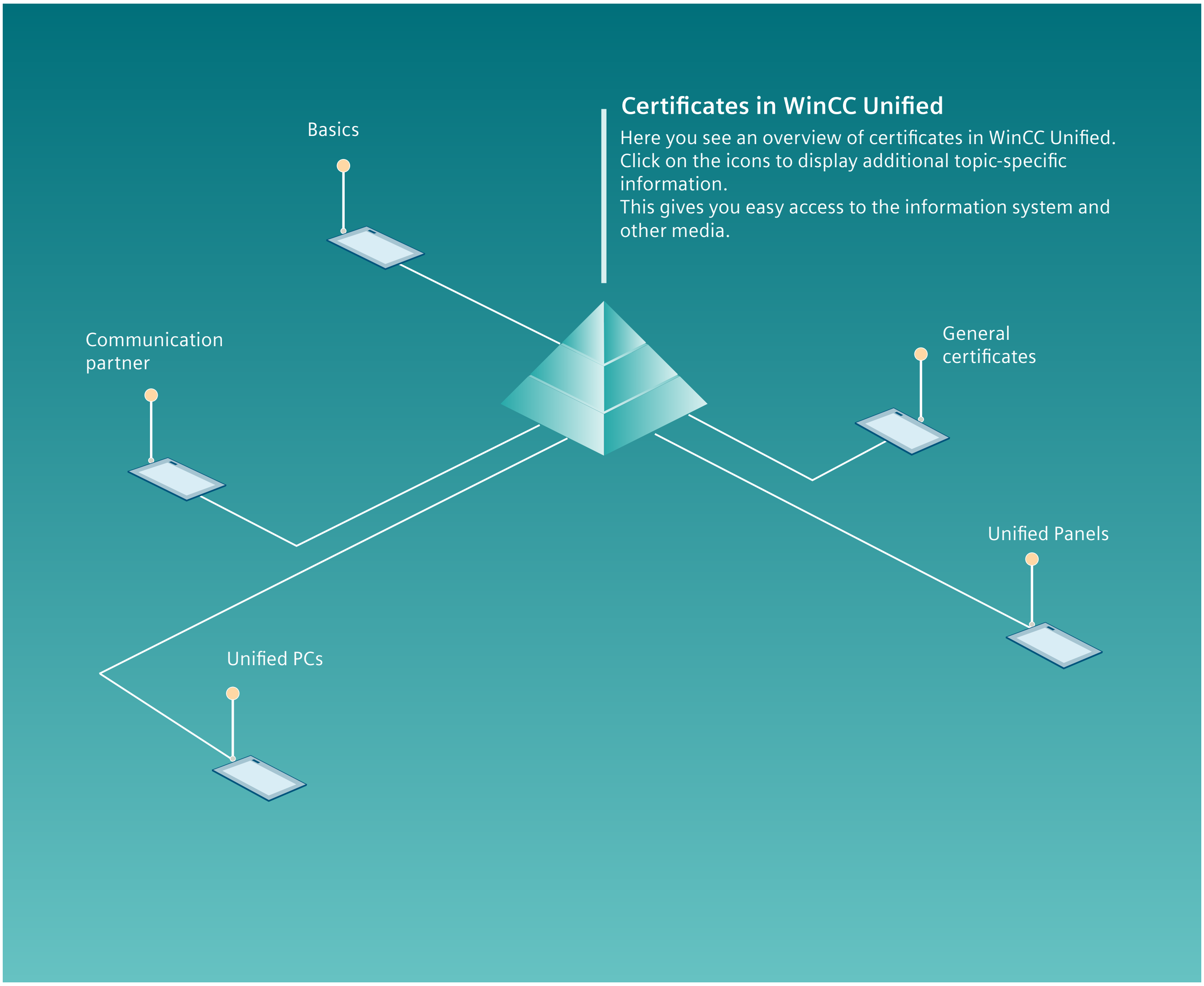


You are logged out from runtime and from the user management.

Newly loaded data from the TIA Portal will not be applied until the next time you log in.

Certificates in WinCC Unified Runtime 6

6.1 Certificates in WinCC Unified

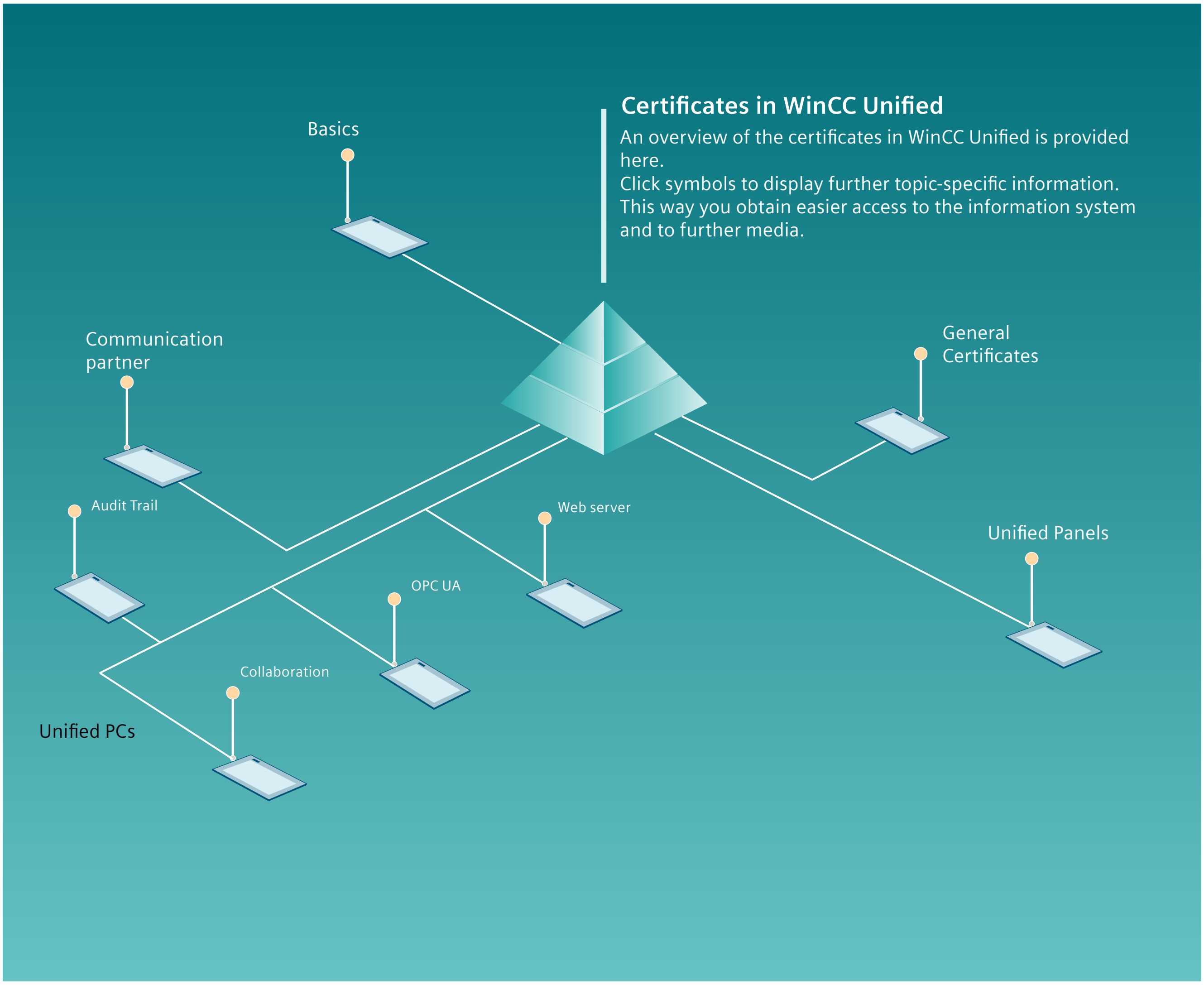


Certificates in WinCC Unified

Here you see an overview of certificates in WinCC Unified. Click on the icons to display additional topic-specific information.
This gives you easy access to the information system and other media.

6.2 Certificates in WinCC Unified

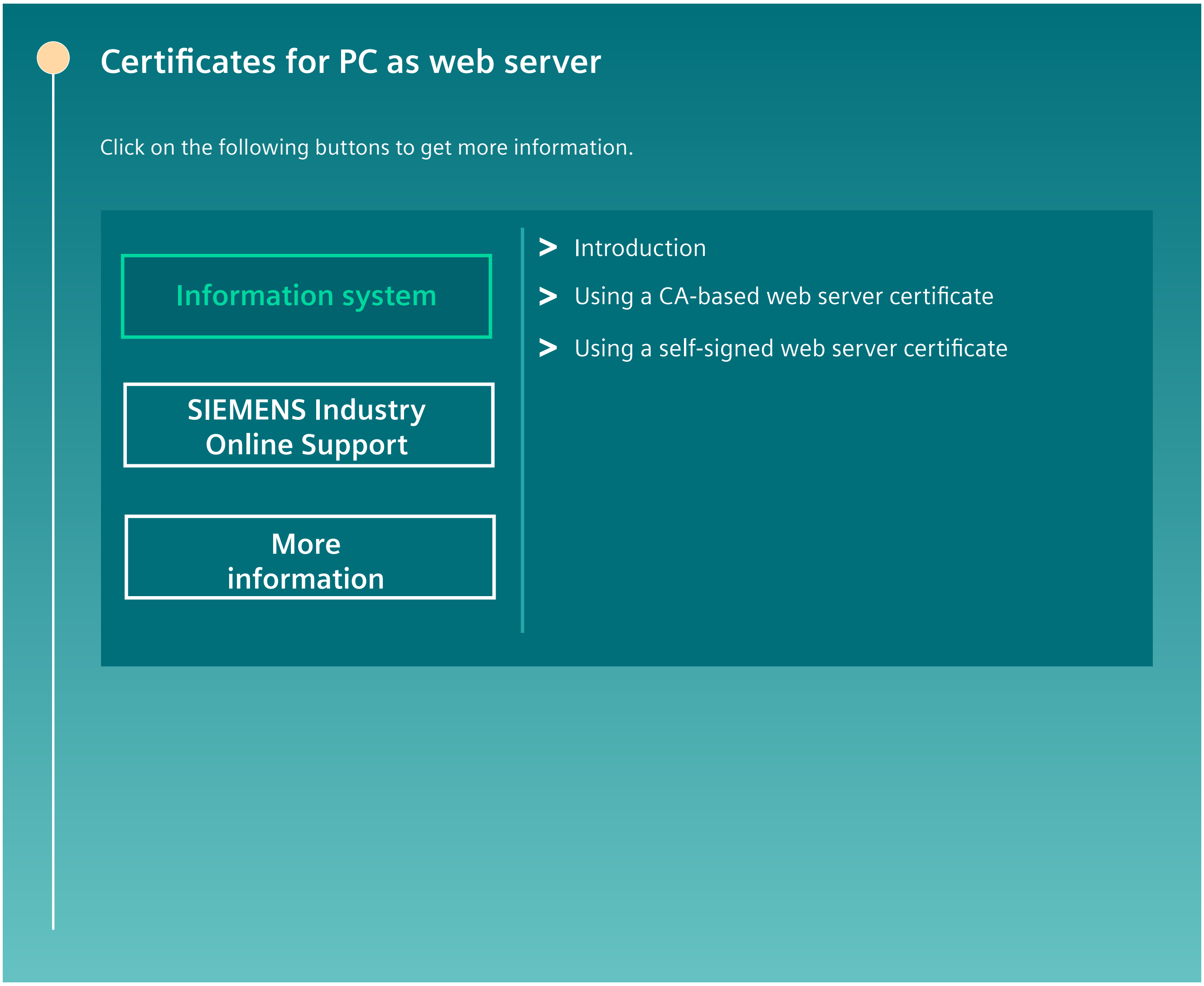
6.2.1 Certificates in WinCC Unified



Certificates in WinCC Unified

An overview of the certificates in WinCC Unified is provided here.
Click symbols to display further topic-specific information.
This way you obtain easier access to the information system and to further media.

6.2.2 Certificates in WinCC Unified

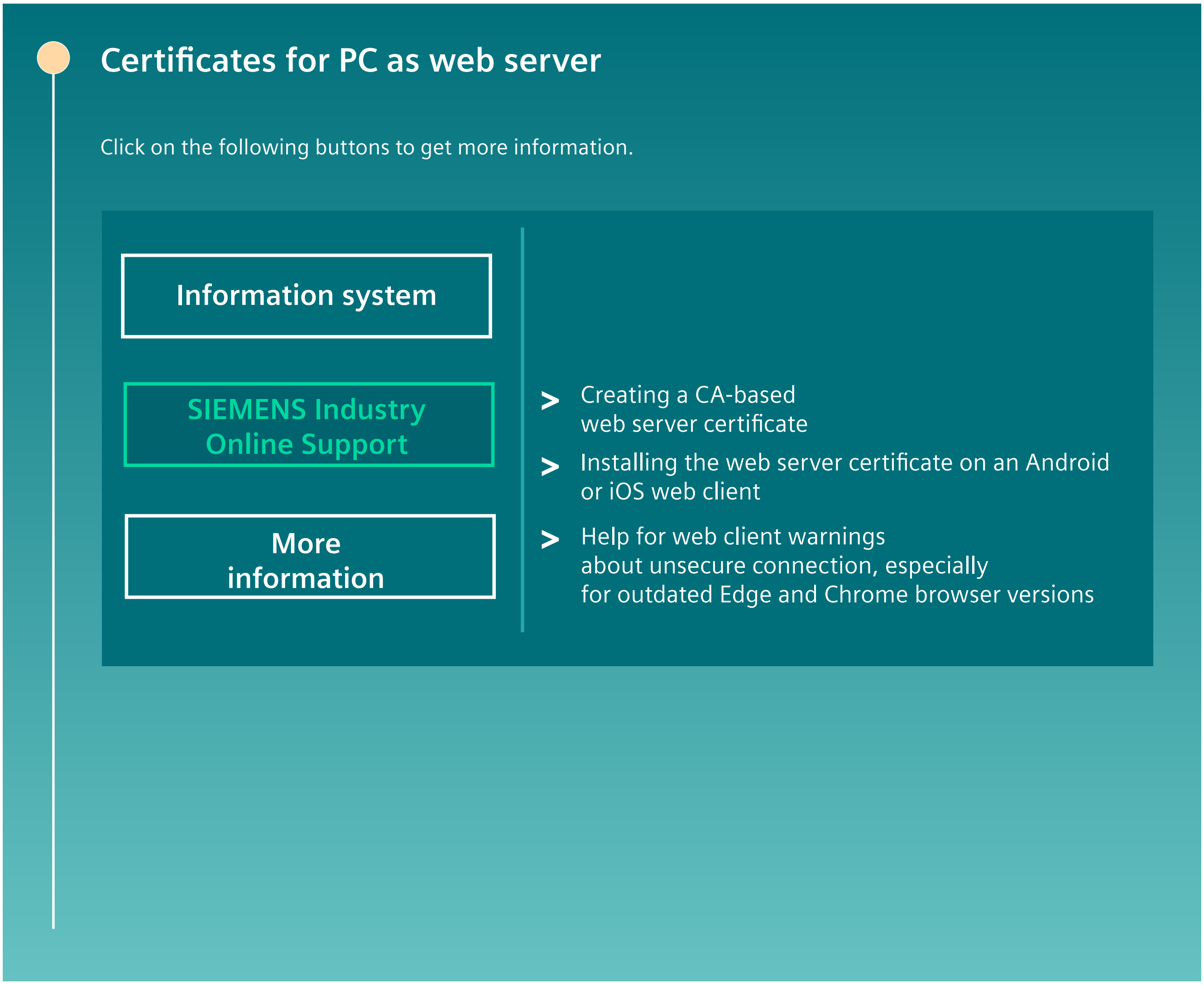


Certificates for PC as web server

Click on the following buttons to get more information.

Information system
SIEMENS Industry Online Support
More information
> Introduction
> Using a CA-based web server certificate
> Using a self-signed web server certificate

6.2.3 Certificates in WinCC Unified

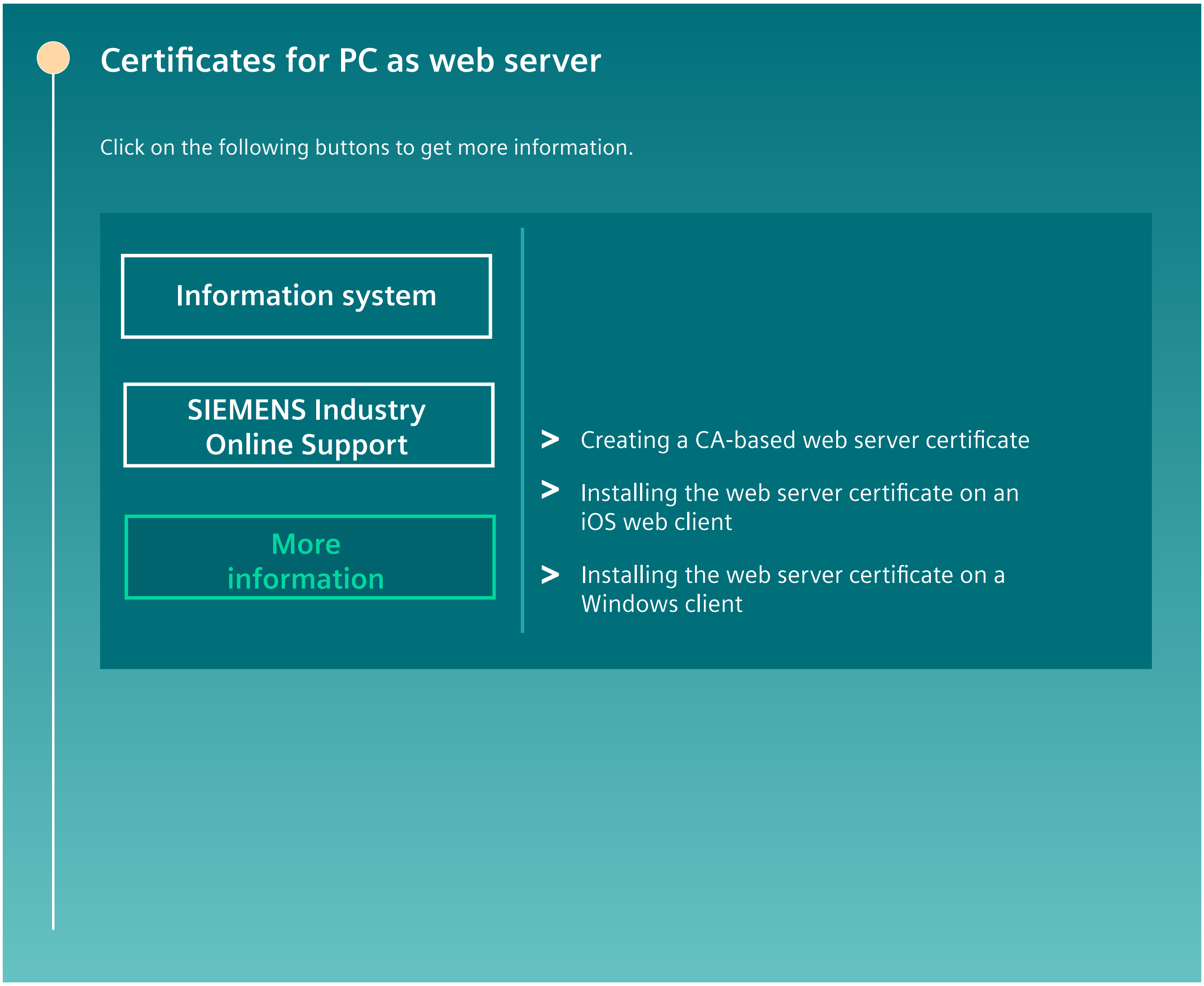


Certificates for PC as web server

Click on the following buttons to get more information.

- > Creating a CA-based web server certificate
- > Installing the web server certificate on an Android or iOS web client
- > Help for web client warnings about unsecure connection, especially for outdated Edge and Chrome browser versions

6.2.4 Certificates in WinCC Unified



Certificates for PC as web server

Click on the following buttons to get more information.

> Creating a CA-based web server certificate

> Installing the web server certificate on an iOS web client

> Installing the web server certificate on a Windows client

See also

Hecht4.0: Web Server Certificate Tutorial Part 3 connect a Windows Client and install the CA (https://www.youtube.com/watch?v=eO3EldpJDlY)

6.2.5 Certificates in WinCC Unified

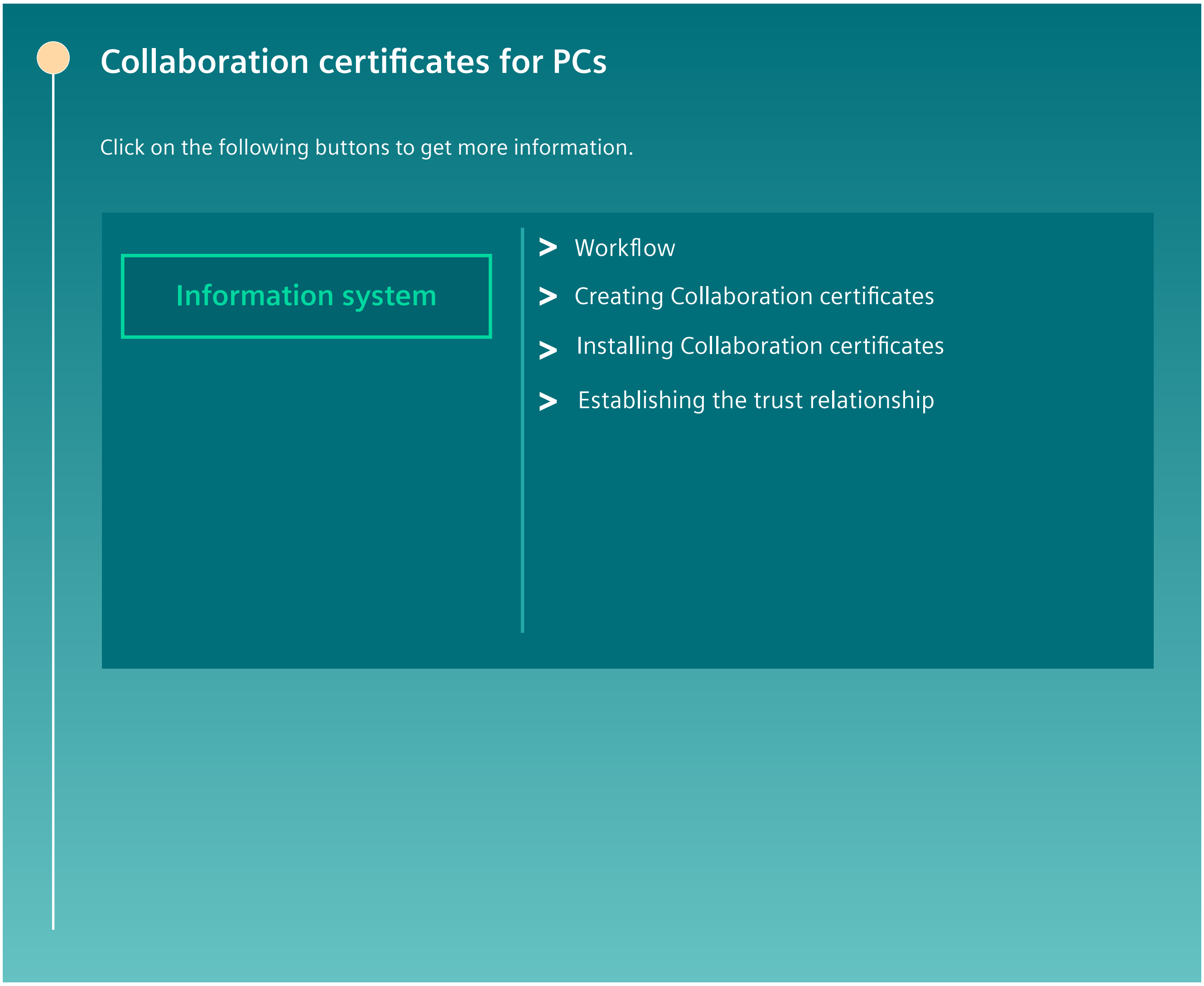
OPC UA certificates for PCs

Click on the following buttons to get more information.

Information system

- > Introduction
- > Using CA-based OPC UA certificates (PC as OPC UA server or client)
- > Using a self-signed default certificate (PC as OPC UA server)
- > Engineering System as OPC UA client

6.2.6 Certificates in WinCC Unified



Collaboration certificates for PCs

Click on the following buttons to get more information.

Information system
> Workflow
> Creating Collaboration certificates
> Installing Collaboration certificates
> Establishing the trust relationship

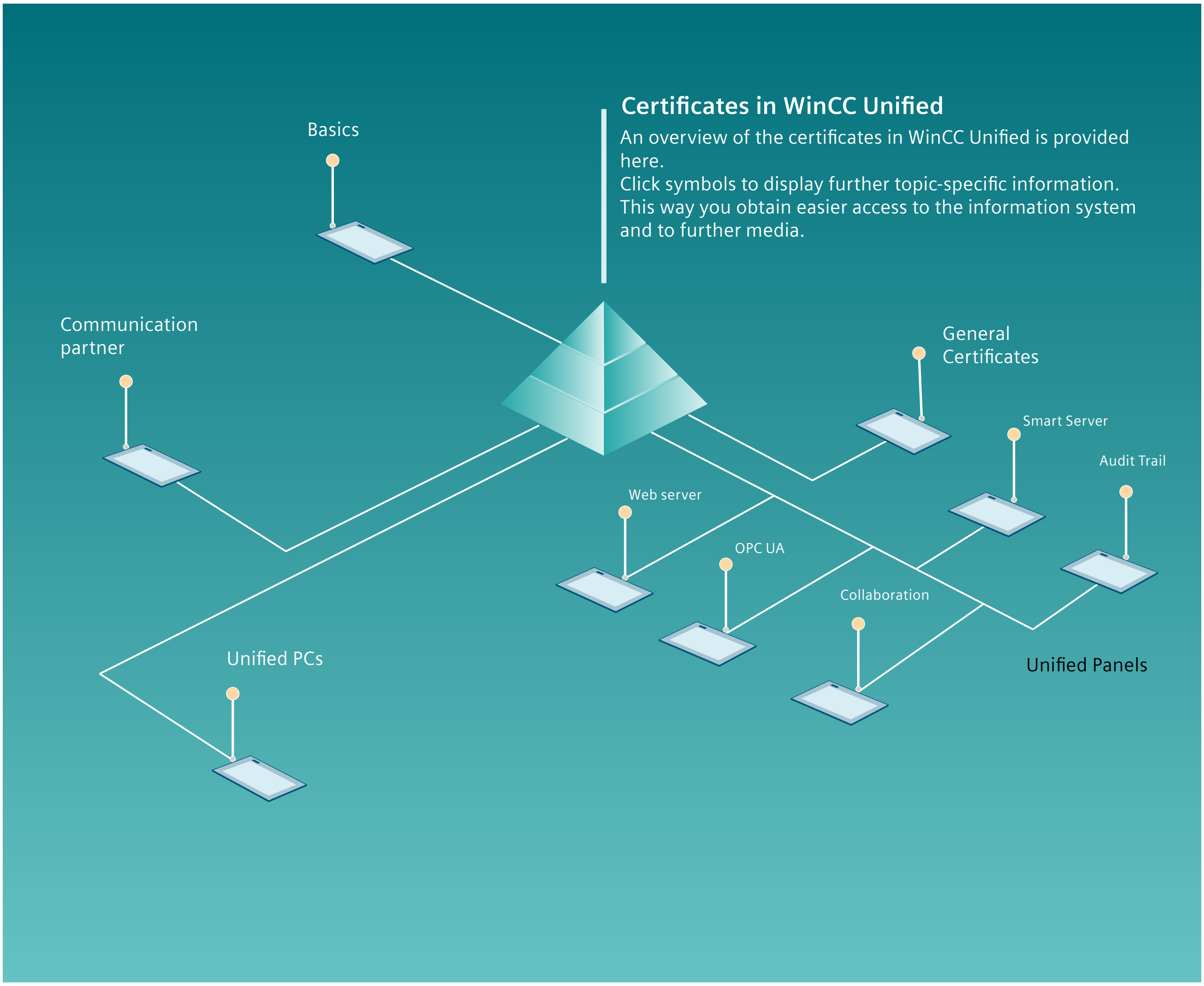
6.2.7 Certificates in WinCC Unified

Audit certificates for PCs

Click on the following buttons to get more information.

Information system
> Workflow
> Creating an Audit certificate
> Installing an Audit certificate

6.2.8 Certificates in WinCC Unified

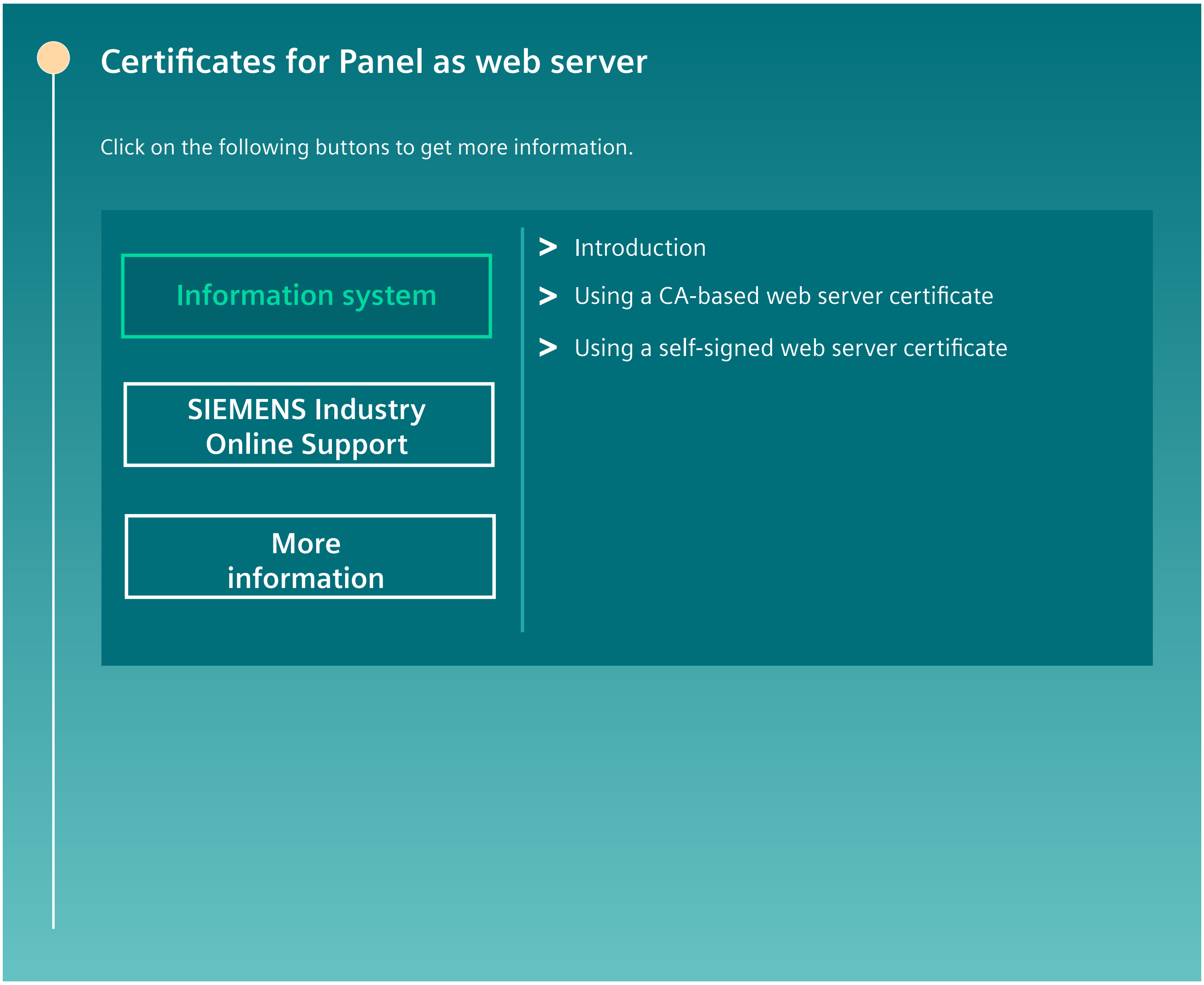


Certificates in WinCC Unified

An overview of the certificates in WinCC Unified is provided here.

Click symbols to display further topic-specific information. This way you obtain easier access to the information system and to further media.

6.2.9 Certificates in WinCC Unified

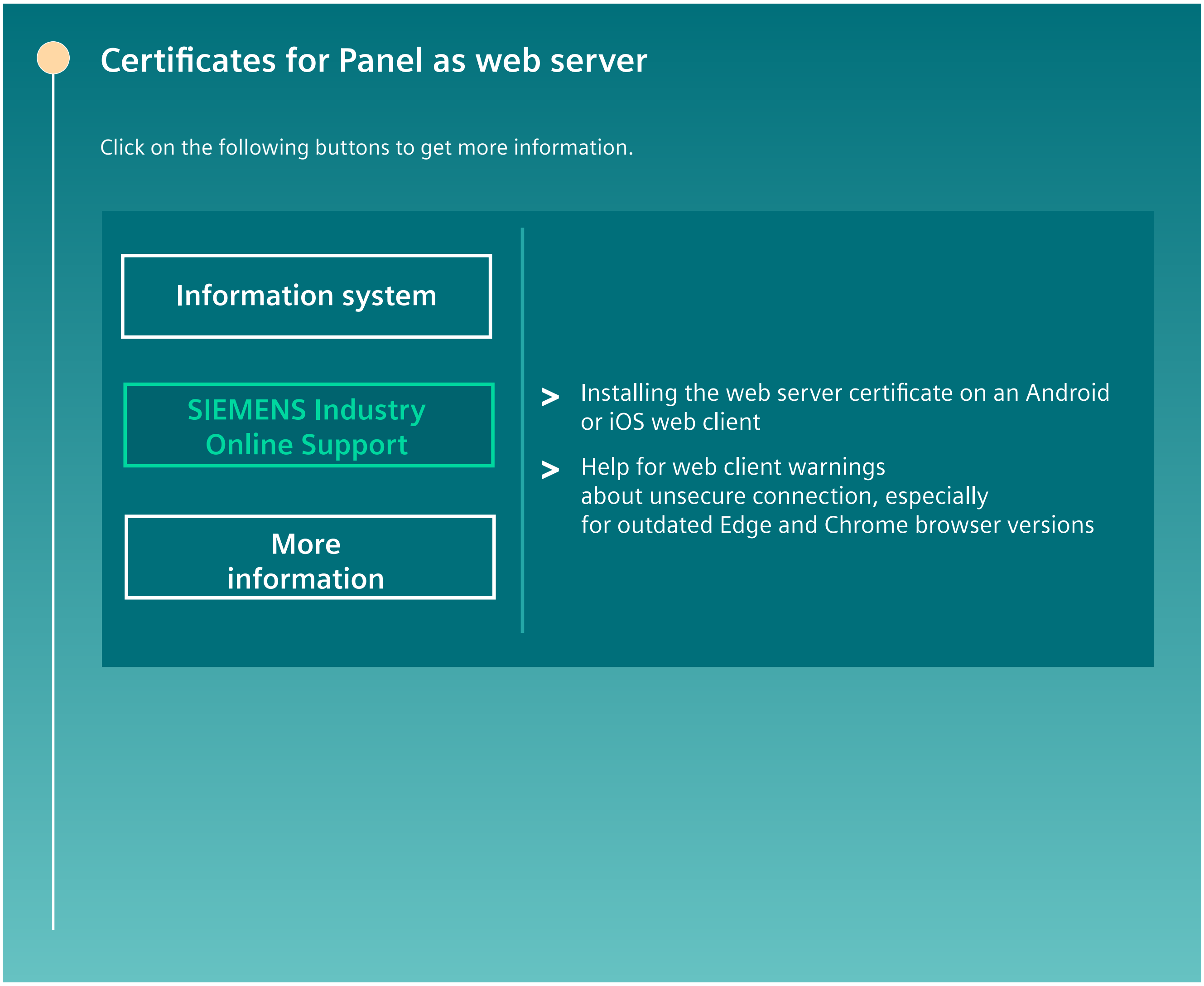


Certificates for Panel as web server

Click on the following buttons to get more information.

- > Introduction
- > Using a CA-based web server certificate
- > Using a self-signed web server certificate

6.2.10 Certificates in WinCC Unified



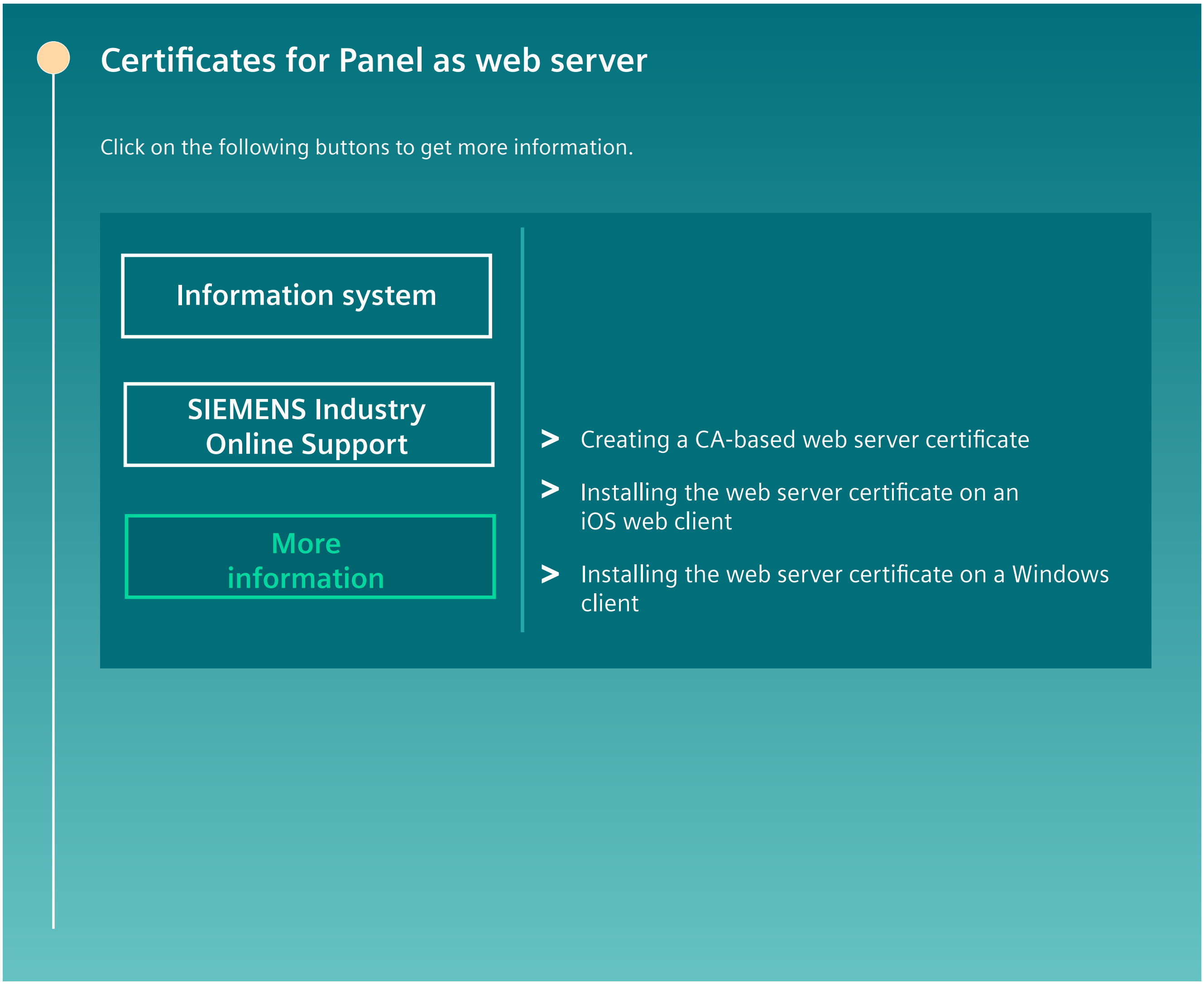
Certificates for Panel as web server

Click on the following buttons to get more information.

> Installing the web server certificate on an Android or iOS web client

> Help for web client warnings about unsecure connection, especially for outdated Edge and Chrome browser versions

6.2.11 Certificates in WinCC Unified



Certificates for Panel as web server

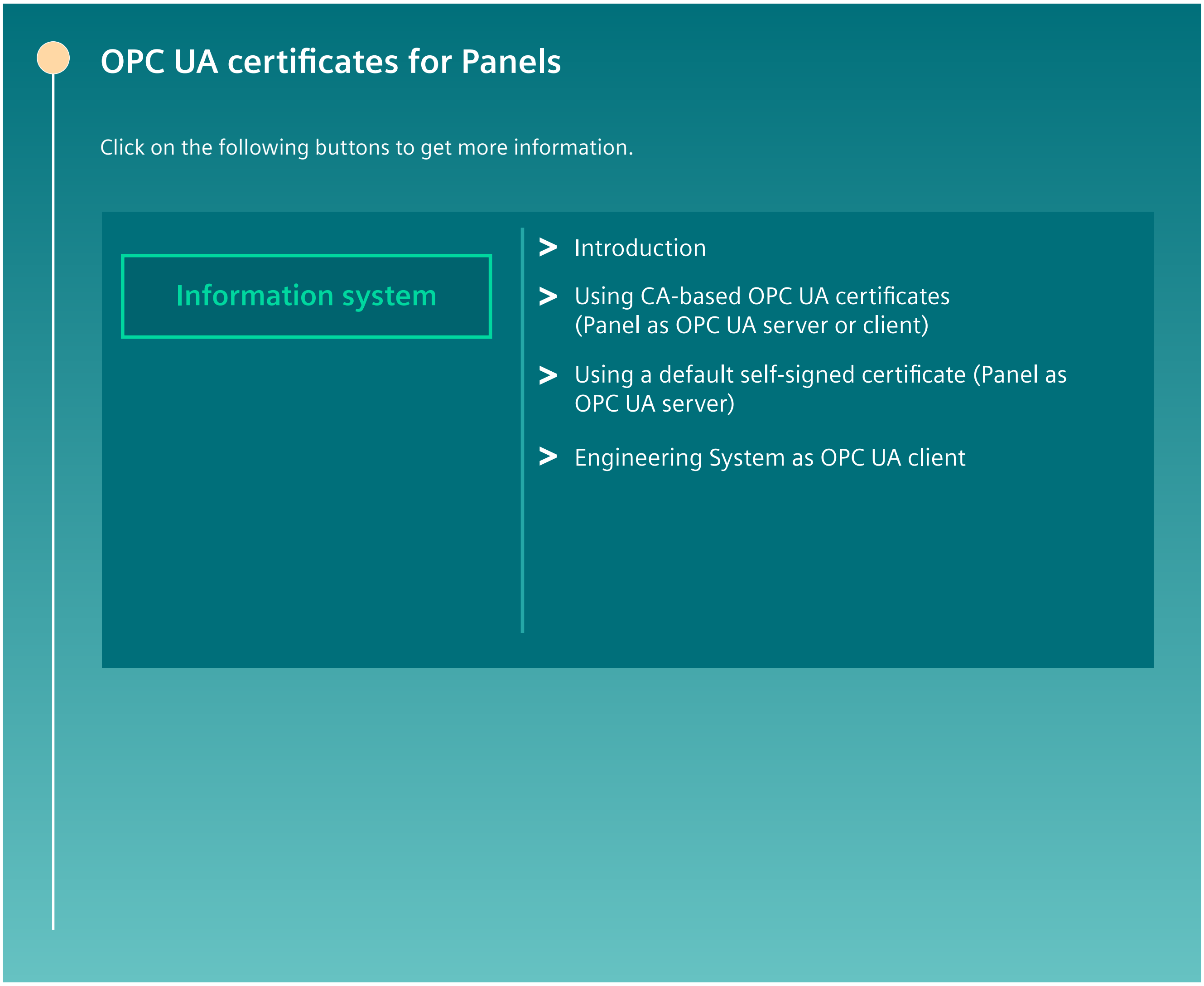
Click on the following buttons to get more information.

> Creating a CA-based web server certificate

> Installing the web server certificate on an iOS web client

> Installing the web server certificate on a Windows client

6.2.12 Certificates in WinCC Unified



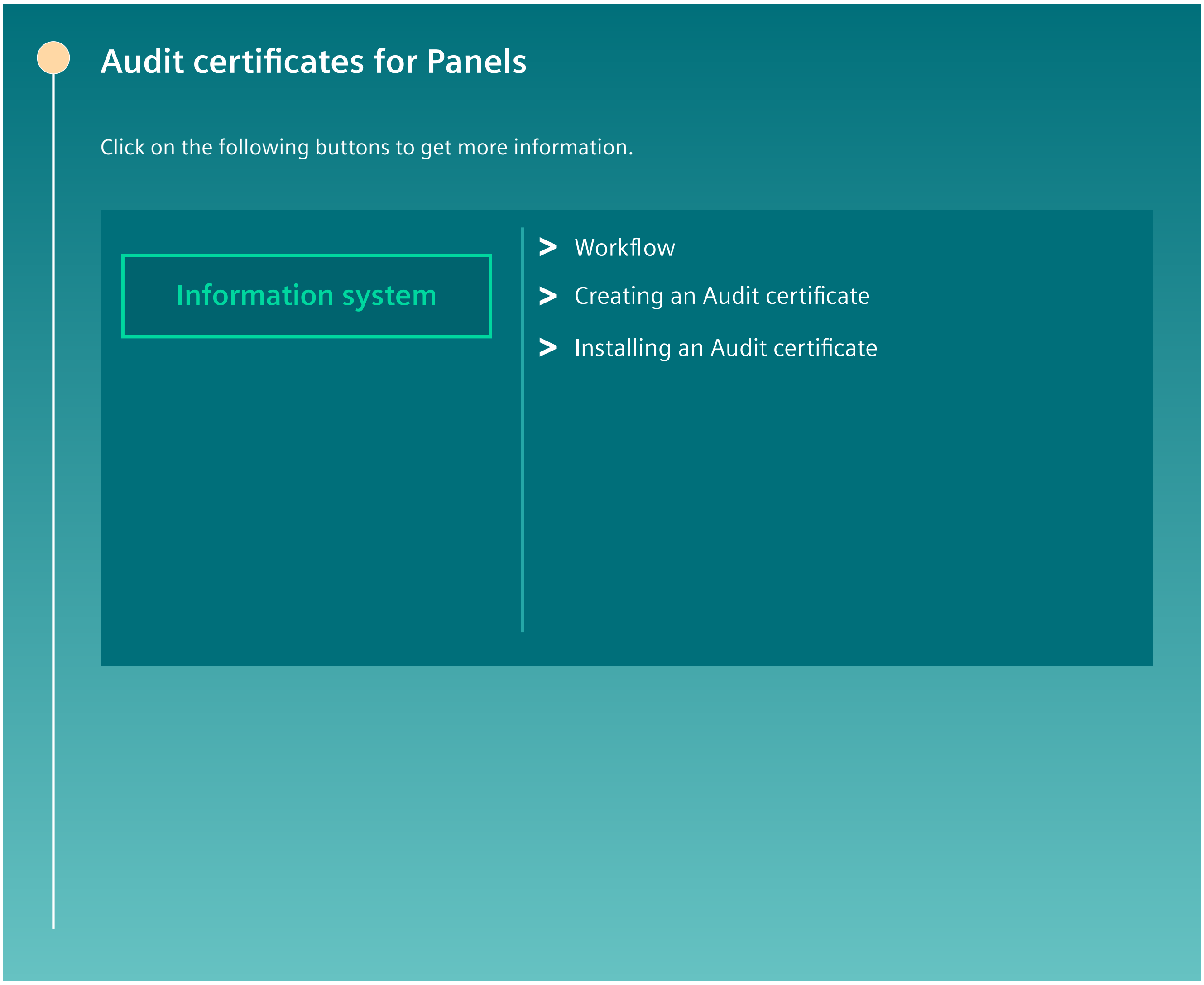
OPC UA certificates for Panels

Click on the following buttons to get more information.

Information system

- > Introduction
- > Using CA-based OPC UA certificates (Panel as OPC UA server or client)
- > Using a default self-signed certificate (Panel as OPC UA server)
- > Engineering System as OPC UA client

6.2.13 Certificates in WinCC Unified

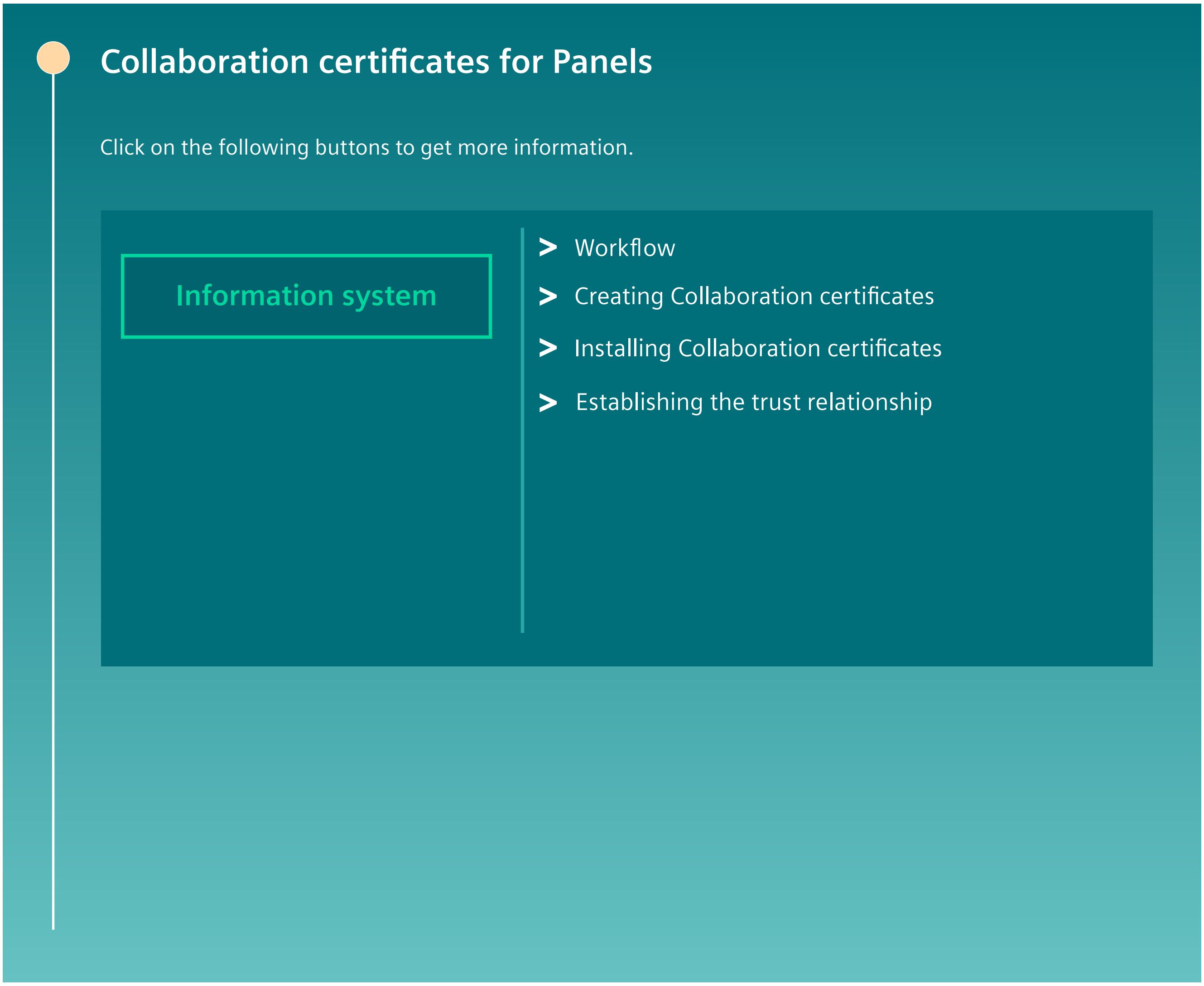


Audit certificates for Panels

Click on the following buttons to get more information.

Information system
> Workflow
> Creating an Audit certificate
> Installing an Audit certificate

6.2.14 Certificates in WinCC Unified



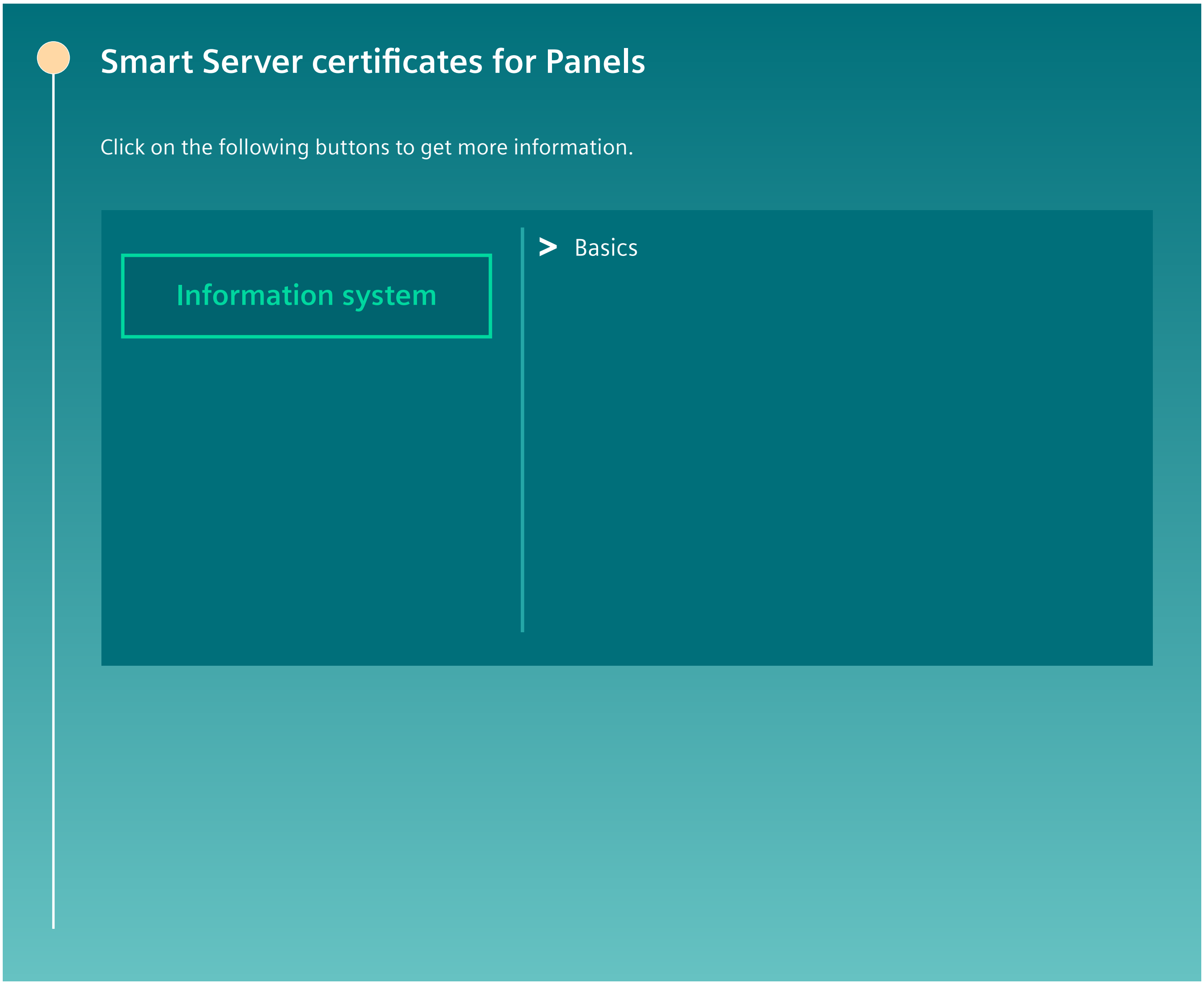
Collaboration certificates for Panels

Click on the following buttons to get more information.

Information system

- > Workflow
- > Creating Collaboration certificates
- > Installing Collaboration certificates
- > Establishing the trust relationship

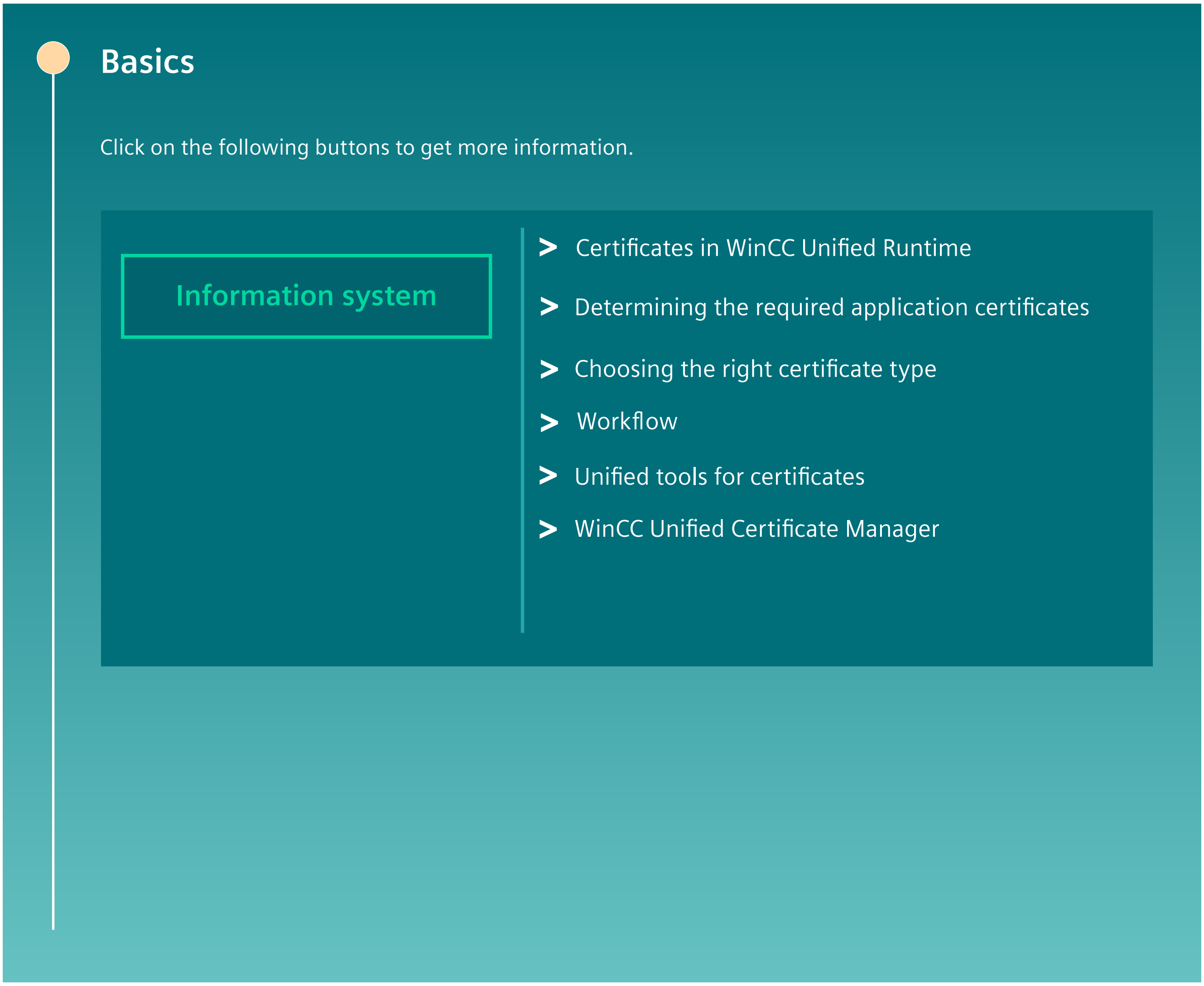
6.2.15 Certificates in WinCC Unified



Smart Server certificates for Panels

Click on the following buttons to get more information.

6.2.16 Certificates in WinCC Unified

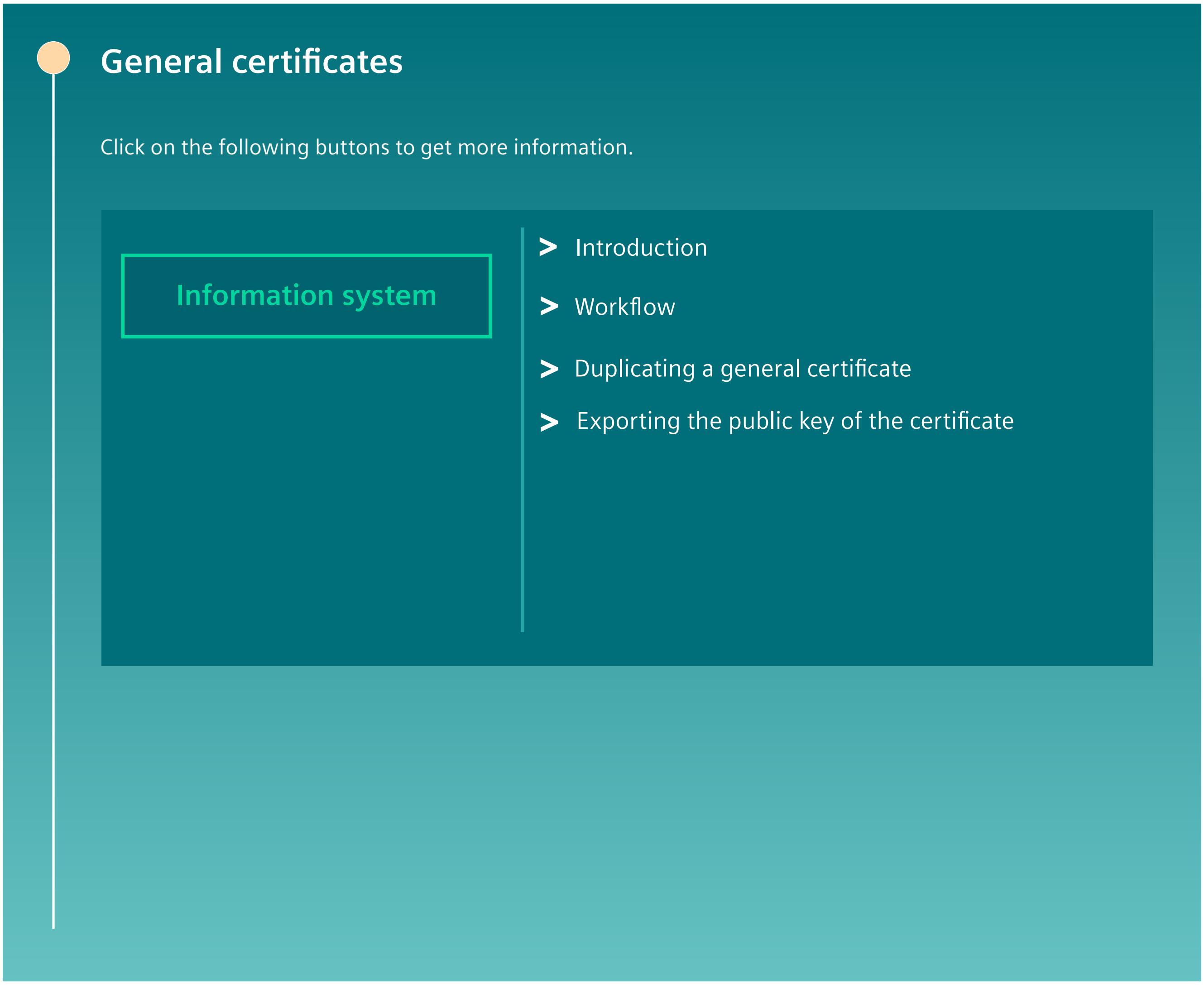


Basics

Click on the following buttons to get more information.

Information system
> Certificates in WinCC Unified Runtime
> Determining the required application certificates
> Choosing the right certificate type
> Workflow
> Unified tools for certificates
> WinCC Unified Certificate Manager

6.2.17 Certificates in WinCC Unified



General certificates

Click on the following buttons to get more information.

Information system
> Introduction
> Workflow
> Duplicating a general certificate
> Exporting the public key of the certificate

6.3 Introduction

6.3.1 Certificates in WinCC Unified Runtime

Certificates protect the communication of plants, systems and networks against cyber threats. Certificates are used for:

- The authentication
- The encryption and decryption of the transferred data

Certificates in WinCC Unified

Protecting communication

Certificates protect the security-relevant communication between the Runtime of a Unified HMI device and the communication partners of the Runtime.

The following communication is always protected through certificates:

- Unified Collaboration communication
- Unified web server communication

With respective configuration the following communication can also be protected with certificates:

- OPC UA communication
- Communication with S7-1500 controller series as of Firmware 2.9 and S7-1200 controllers as of Firmware 4.5
- WinCC Smart Server communication between a Smart Client panel und and a Smart Server

Detecting changes to data records in Audit Trail

The WinCC Unified Audit option uses certificates to generate a checksum for Audit Trail data records. You can determine whether the contents of a data record were changed by means of the checksum. This checksum also ensures that no lines have been added to or removed from the Audit Trail file.

Audit certificates are not used for communication with another device.

Plant protection through certificate authorities

Certificates issued by a certificate authority (abbreviated CA) (CA-based certificates) are unique and provide the highest level of protection for your plant.

WinCC Unified supports you:

- With the generation of the CA-based certificates of your HMI devices (Unified certificates), their installation on the HMI devices and their distribution to the communication partners of the HMI devices
- With the installation of the CA-based certificates of the communication partners (third party certificates) on the HMI devices

Note

Self-signed certificates

Alternatively the use of self-signed certificates is also possible. Self-signed certificates are less secure than CA-based certificates. Their usage is subject to numerous limitations.

Also when using self-signed Unified certificates, WinCC Unified supports you with the creation or installation of the certificates of the HMI device as well as with the installation of the self-signed third party certificates of its communication partners.

Mixed usage is also possible. For example. a Unified OPC UA server can use a CA-based certificate, while one of its clients uses a self-signed certificate.

Note

Recommendation

For security reasons the usage of CA-based certificates is recommended.

General certificates

WinCC Unified furthermore allows you to create general CA-based certificates for your HMI devices or other devices, for example to protection the communication of an own application.

See also

Communication partners (Page 481)

Runtime and simulation (Page 490)

Unified certificate authority (Page 505)

Certificates for Unified Panels (Page 377)

Certificates for Unified PCs (Page 428)

Workflow for using certificates on HMI devices (Page 490)

Using general certificates (Page 548)

About this help (Page 376)

6.3.2 About this help

Contents

This help describes the following:

- The certificate-bound communication between devices from the same network
- How to create certificates of a Unified HMI device and distribute them to and install them on the HMI device and its communication partners
- How to install the third-party certificates of the communication partners of an HMI device on the HMI device

Information on how to create the third-party certificates and how to install the Unified certificates on the devices of the communication partners can be found in the user help of the respective communication partner.

For the mutual SSL authentication, it is assumed that the HMI device and its communication partners use the same certificate type.

See also

Certificates in WinCC Unified Runtime (Page 374)

6.4 Certificates for Unified Panels

6.4.1 Collaboration certificates (Panel)

6.4.1.1 Collaboration certificates and Runtime version

Runtime Collaboration requires that the Collaboration certificates of 2 Collaboration partners be created with a certificate authority device whose installed Runtime version is equal to or higher than the installed Runtime version of the Collaboration partner with the higher Runtime version.

For this reason, the upgrading of Collaboration devices requires the creation, distribution and installation of new Collaboration certificates.

Example:

- A Unified PC and a Unified Panel with Runtime version V17 are Collaboration partners.
- You upgrade the Panel to V18.
- Create new Collaboration certificates for both HMI devices on a certificate authority device with installed Runtime version V18 or higher. Distribute them to and install them on the devices.

See also

Workflow (Collaboration for Panels) (Page 377)

6.4.1.2 Workflow (Collaboration for Panels)

Introduction

WinCC Unified Collaboration protects the communication between the Collaboration devices through the use of certificates.

The certificates must be issued by a Unified certificate authority (CA-based certificates). You use the WinCC Unified Certificate Manager application for this.

Note

Certificate Manager always creates CA-based certificates. The use of CA-based certificates facilitates establishment of the trust relationship and provides the highest protection for your plant.

The use of self-signed certificates is not supported for Collaboration.

Required certificates

For successful communication between two Collaboration devices, you need the following certificates for each Collaboration device:

- Collaboration certificate of the HMI device
- Root certificate of the certificate authority that issued the Collaboration certificate, along with its CRL file.

Workflow

To provide the certificates needed by a Unified Panel Collaboration device, follow these steps:

1. Create the Collaboration certificate of the Panel.
2. Install the Collaboration certificate on the Panel.
3. Restart Runtime on the Panel.
4. Establish the trust relationship between the Panel and its Collaboration partner.

See also

Creating certificates (Collaboration for Panels) (Page 378)

Installing certificates (Collaboration for Panels) (Page 379)

Establishing the trust relationship (Collaboration for Panels) (Page 380)

Collaboration certificates (PC) (Page 428)

Collaboration certificates and Runtime version (Page 377)

6.4.1.3 Creating certificates (Collaboration for Panels)

Introduction

You create the Collaboration certificate of a Unified Panels on the certificate authority device. You use the WinCC Unified Certificate Manager application for this.

The certificate authority device is always a Unified PC.

Procedure

If you do not have a certificate authority yet, follow these steps:

1. Create the certificate authority.
   In so doing, you create the root certificate of the certificate authority and its CRL file automatically.
   See section Creating a certificate authority and root certificate (Page 519).
2. Add the Panel to the certificate authority.
   See section Adding devices (Page 521).
3. Add the Collaboration certificate to the Panel.
   See section Add application certificates (Page 524).

If you already have a certificate authority, follow these steps:

1. If the Panel has not yet been added to the infrastructure of the certificate authority, add the Panel.
   See section Adding devices (Page 521).
2. Add the Collaboration certificate to the Panel.
   See section Add application certificates (Page 524).

See also

Workflow (Collaboration for Panels) (Page 377)

Collaboration certificates and Runtime version (Page 377)

6.4.1.4 Installing certificates (Collaboration for Panels)

Introduction

The Collaboration certificate of a Unified Panel is installed in the following steps:

- Export on the certificate authority device
- Import on the Panel

Note

You always export and import all certificates of the Panel as well as the root certificate of the issuing certificate authority and its CRL file.

These certificates are automatically installed by the import.

Requirement

- The Collaboration certificate has been added for the Panel on the certificate authority device.

Procedure

1. Export the certificates of the Panel on the certificate authority device. Use the WinCC Unified Certificate Manager for this.
   See section Exporting certificates of a Panel (Page 530).
2. Import the certificates to the Panel. Use the Control Panel for this.
   See section Importing and installing certificates of a Panel (Page 541).

See also

Workflow (Collaboration for Panels) (Page 377)

Add application certificates (Page 524)

6.4.1.5 Establishing the trust relationship (Collaboration for Panels)

Introduction

Secure communication between Collaboration devices requires that the devices trust each other's Collaboration certificate.

That is automatically the case when a device trusts the root certificate of the certificate authority that issued the Collaboration certificate of the other device, and vice versa.

Trusting the Collaboration partner of a Panel

To ensure that a Unified Panel trusts its Collaboration partner, follow these steps:

1. Check whether the Panel already trusts the root certificate of its Collaboration partner.
   See sections Checking the status of a root certificate on the HMI device (Page 544) and Automatic trust relationship between Collaboration devices (Page 380).
2. If the Panel does not yet trust the root certificate, install it manually.
   See section Importing and installing root certificates and CRL files on Panels (Page 545).

See also

Workflow (Collaboration for Panels) (Page 377)

6.4.1.6 Automatic trust relationship between Collaboration devices

This section describes cases in which a Collaboration device automatically trusts the certificate of its Collaboration partner. You do not have to establish the trust relationship manually.

Same certificate authority

Requirement:

- The Collaboration certificates of both devices have the same certificate authority. That is, the certificates have the same root certificate.
- The own Collaboration certificate has been installed on each device
  During installation of this certificate, the root certificate is also automatically installed on the device. It is installed in the folder containing the trusted certificate authorities.

Result:

The first time the connection is established for Collaboration, the devices check the Collaboration certificate of their Collaboration partner. Since they already trust the root certificate, the Collaboration certificate is automatically installed in the folder with the trusted certificates.

Trusted certificate authority

Requirement:

- The Collaboration certificates of the Collaboration devices have different certificate authorities. That is, the certificates have different root certificates.
- One Collaboration device has a communication partner whose application certificate was issued by the same certificate authority as the Collaboration certificate of its Collaboration partner. The device already trusts the certificate authority of this communication partner.

Result:

- The first time the connection is established for Collaboration, the device checks the Collaboration certificate of the Collaboration partner.
- Since the device already trusts the root certificate of the other communication partner, it automatically installs the Collaboration certificate in the folder with the trusted certificates.

Note

For successful Collaboration communication, the devices must trust each other. Check on the other Collaboration device to determine if it also already trusts the root certificate. See section Checking the status of a root certificate on the HMI device (Page 544).

Establish the trust relationship there manually, if necessary.

Example**:**

A Panel communicates with a second Panel using Unified Collaboration. The Collaboration application certificates of the Panels have different certificate authorities. Both Panels already trust the root certificates of their Collaboration partner.

For the first Panel, a Unified PC is configured as an additional Collaboration partner. The Collaboration application certificate of the PC has the same certificate authority and, thus, the same root certificate as the second Panel.

Since the first Panel already trusts the root certificate of the second Panel, it automatically also trusts the Collaboration application certificate of the PC.

See also

Establishing the trust relationship (Collaboration for Panels) (Page 380)

6.4.2 Web server certificates (Panel)

6.4.2.1 Introduction

Basics of web server communication

WinCC Unified protects the communication between a Runtime web server and its web clients through the use of a web server certificate. The clients must trust the web server certificate (one-way SSL authentication).

The web server certificate can be issued by a Unified certificate authority (CA-based certificate) or be self-signed.

Note

For security reasons, it is recommended to use a CA-based certificate. You use the "WinCC Unified Certificate Manager" application to create the certificate.

You can find help on choosing a certificate type in section Selecting a suitable certificate type (Page 493).

The procedure for creating the web server certificate, installing it on the web server device and establishing the trust relationship with the web server on the clients depends on the chosen certificate type.

See also

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Workflow with a self-signed certificate (Panel as web server) (Page 406)

Unified certificate authority (Page 505)

6.4.2.2 Using a CA-based certificate (Panel as web server)

Workflow with a CA-based certificate (Panel as web server)

If you are using a Unified Panel as a Runtime web server and want to use a CA-based web server certificate, you need the following certificates:

- Web server certificate of the Panel
- Root certificate of the certificate authority that issued the web server certificate, along with its CRL file.

Requirement

- Web-based client access has been enabled for the Panel.

Procedure

1. Create the web server certificate of the Panel.
   See section Creating certificates (Panel as web server) (Page 383).
2. Install the web server certificate on the Panel.
   See section Installing certificates (Panel as web server) (Page 383).
3. Establish the trust relationship with the web server on the web clients.
   See section Establishing the trust relationship with the web server (Page 384).

See also

Introduction (Page 381)

Managing third party certificates and own certificates of a Unified Panel (Page 496)

Trusting the Panel web server on the web client (Page 407)

Creating certificates (Panel as web server)

Introduction

You create the CA-based web server certificate of a Unified Panels on the certificate authority device. You use the WinCC Unified Certificate Manager application for this.

The certificate authority device is always a Unified PC.

Procedure

If you do not have a certificate authority yet, follow these steps:

1. Create the certificate authority.
   In so doing, you create the root certificate of the certificate authority and its CRL file automatically.
   See section Creating a certificate authority and root certificate (Page 519).
2. Add the Panel to the certificate authority.
   See section Adding devices (Page 521).
3. Add the web server certificate to the Panel.
   See section Add application certificates (Page 524).

If you already have a certificate authority, follow these steps:

1. If the Panel has not yet been added to the infrastructure of the certificate authority, add the web server Panel.
   See section Adding devices (Page 521).
2. Add the web server certificate to the Panel.
   See section Add application certificates (Page 524).

See also

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Installing certificates (Panel as web server)

Introduction

The web server certificate of a Unified Panel is installed in the following steps:

- Export on the certificate authority device
- Import to the Panel

Note

You always export and import all certificates of the Panel as well as the root certificate of the issuing certificate authority and its CRL file.

These certificates are automatically installed by the import.

Requirement

- The web server certificate has been added for the Panel on the certificate authority device.

Procedure

1. Export the certificates of the Panel on the certificate authority device. Use the WinCC Unified Certificate Manager for this.
   See section Exporting certificates of a Panel (Page 530).
2. Import the certificates to the Panel. Use the Control Panel for this.
   See section Importing and installing certificates of a Panel (Page 541).

Note

The import installs the web server certificate and binds it to the Runtime web page of the Panel.

The web page is then restarted to enforce the use of the new certificate. Any connected web clients are thereby disconnected and must log in again.

See also

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Add application certificates (Page 524)

Establishing the trust relationship with the web server

Introduction

Secure communication between a Unified Runtime web server and its web clients requires that the clients trust the web server certificate.

That is automatically the case when a client trusts the root certificate of the certificate authority that issued the web server certificate.

Timing

You can establish the trust relationship on a planned or as needed basis:

- Planned: You install the root certificate before the client attempts to connect to the web server for the first time.
  The client then already trusts the web server certificate the first time a connection is established.
- As needed: You install the root certificate when the client first attempts to connect to the web server.
  If the root certificate of the web server has not yet been installed at that time, you can download it on the Unified home page and then install it in the client.

Installing the root certificate before a connection is established for the first time

1. If applicable, check whether the client already trusts the root certificate of the web server.
   See sections Checking the status of the web server root certificate on the web client. (Page 386) and Automatic trust relationship with a Panel web server (Page 387).
2. If the client already trusts the root certificate, you don't have to do anything.
   If the client does not trust the root certificate, install it manually in the certificate store of the browser.

Utilized browser	Certificate store used by the browser	For procedure, see section
Edge and Chrome on Windows	Windows system certificate store	Installing the root certificate before the first connection (Edge and Chrome) (Page 388)
Firefox on Windows	Certificate store of Firefox	Installing the root certificate before the first connection (for Firefox) (Page 393)
Web browser of a Unified Panel	Certificate store of the Panel	Installing the root certificate before the first connection (Panel web browser) (Page 404)
Browser on iOS devices	System certificate store of the iOS device	Installing the root certificate on iOS devices before the first connection (Page 397)

Installing the root certificate at the first connection attempt

Follow the steps below according to the browser:

Browser	Certificate store used by the browser	For procedure, see section
Edge and Chrome on Windows	Windows system certificate store	Installing the root certificate at the first connection (Edge and Chrome) (Page 390)
Firefox on Windows	Certificate store of Firefox	Installing the root certificate at the first connection (for Firefox) (Page 395)

Browser	Certificate store used by the browser	For procedure, see section
Web browser of a Unified Panel	Certificate store of the Panel	Installing the root certificate at the first connection (Panel web browser) (Page 405)
Browser on iOS devices	System certificate store of the iOS device	Installing the root certificate on iOS devices at the first connection (Page 399)

See also

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Checking the status of the web server root certificate on the web client.

Introduction

This section describes how to check whether a web client already trusts the root certificate of a Runtime web server.

In that case, the root certificate has been installed in the certificate store of the web client in the folder containing the trusted certificate authorities.

Procedure for Microsoft Edge and Chrome as web client

Microsoft Edge and Chrome use the Windows system certificate store.

Use Windows > Search "Manage computer certificates" to check whether the root certificate has been installed under "Certificates - Local Computer" > "Trusted Root Certification Authorities" > "Certificates".

Procedure for Firefox

Firefox uses its own dedicated certificate store.

To check the status of a certificate, follow these steps:

1. Open the "Settings" page of Firefox.
2. Select "Privacy & Security".
3. Click "View Certificates" in the "Certificates" area.
4. Select the "Authorities" tab in the "Certificate Manager" window.
5. Check whether the root certificate is included in the list of trusted authorities.

Procedure for iOS devices

Follow the procedure described in the user help of the manufacturer.

Procedure for "Web browser" of a Unified Panel

"Web browser" of the Unified Panel uses the certificate store of the Panel.

To check whether the Panel already trusts the root certificate, follow the procedure described in section Checking the status of a root certificate on the HMI device (Page 544).

Automatic trust relationship with a Panel web server

This section describes cases in which a web client automatically trusts the CA-based certificate of a Unified Panel web server. You do not have to establish the trust relationship manually.

Edge or Chrome as client and same certificate authority

Requirement

- You use Microsoft Edge or Chrome as web client.
- The clients have been installed on a Unified PC.
- The web server certificate of the Panel and at least one application certificate of the client PC were issued by the same certificate authority. That is, they have the same root certificate.

Result:

- During installation of the certificates of the Unified PC, WinCC Unified Certificate Manager also installs the root certificate in the system certificate store of Windows. Microsoft Edge and Chrome use this certificate store.
- Since the clients already trust the root certificate, the web server certificate is automatically installed in the folder with the trusted certificates when a connection is established for the first time.
- The connection between the client and web server is secure from the outset.

Communicating with multiple web servers of the same certificate authority

Requirement:

- The web server certificates of two Unified Runtime web servers were issued by the same certificate authority. That is, they have the same root certificate.
- The web client already trusts the root certificate of one of the Unified Runtime web servers.
- The client connects to the second web server.

Result:

- The client already trusts the root certificate at the first connection attempt. For this reason, the web server certificate of the second web server is automatically installed in the folder with the trusted certificates when the connection is established.
- The connection between the web client and web server is secure from the outset.

See also

Establishing the trust relationship with the web server (Page 384)

Installing the root certificate for Edge and Chrome

Installing the root certificate before the first connection (Edge and Chrome)

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) on an Edge or Chrome web client before the client connects to the web server for the first time. The description applies to clients installed on Windows devices.

The procedure is explained using Edge as an example. The procedure is the same for Chrome.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager.
  See section Creating a certificate authority and root certificate (Page 519).
- The web server root certificate has been exported on the certificate authority device with Certificate Manager to a storage location the web client can access.
  See section Exporting root certificate and CRL file (Page 531).

  Note

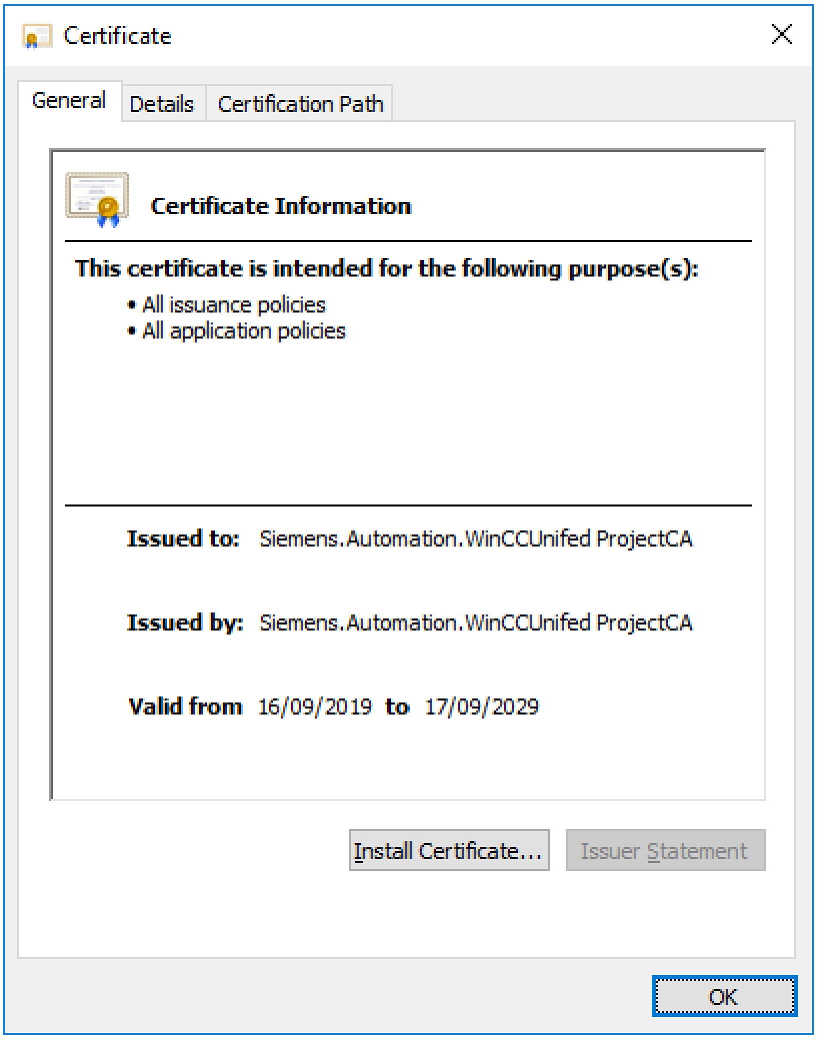
  Alternative

  If a Unified PC belongs to the infrastructure of the certificate authority of the web server whose certificates were already installed with Certificate Manager, you can export the root certificate on the PC with SIMATIC Runtime Manager.

  See section Managing third-party certificates of a Unified PC (Page 499).
- Microsoft Edge or Chrome has been installed on the web client device.

Procedure

1. Double-click the root certificate file on the web client device.
   The root certificate is opened with the Windows standard form.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: Siemens.Automation.WinCCUnifed ProjectCA

Issued by: Siemens.Automation.WinCCUnifed ProjectCA

Valid from 16/09/2019 **to** 17/09/2029

2. Click "Install Certificate".
3. In the certificate import wizard, select "Local Machine" as the storage location and "Trusted Root Certification Authority" as the certificate store.
4. Start the import.
5. (optional) Check whether the root certificate was successfully installed in the Windows system certificate store.
   See section Checking the status of the web server root certificate on the web client. (Page 386).

Result

At the first call of the web server web page, the browser trusts the root certificate of the web server and, thus, it automatically also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Establishing the trust relationship with the web server (Page 384)

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Installing the root certificate at the first connection (Edge and Chrome)

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) at the first connection attempt of an Edge or Chrome web client. The description applies to clients installed on Windows devices.

The procedure is explained using Edge as an example. The procedure is the same for Chrome.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager. It has been installed on the web server.
- A Runtime project is running on the web server.
- Microsoft Edge or Chrome has been installed on the web client device.
- The web server root certificate has not yet been installed in the Windows system certificate store of the client device.
- The client device has access to the web server.

Procedure

1. Start Microsoft Edge on the web client device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

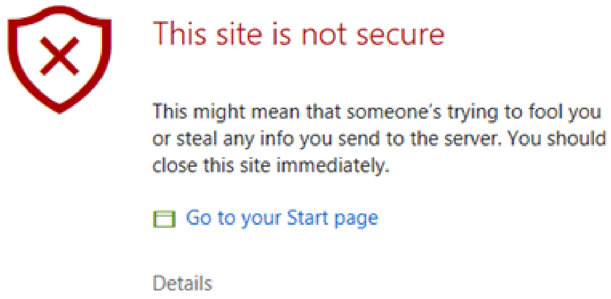
   Note

   URL of a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

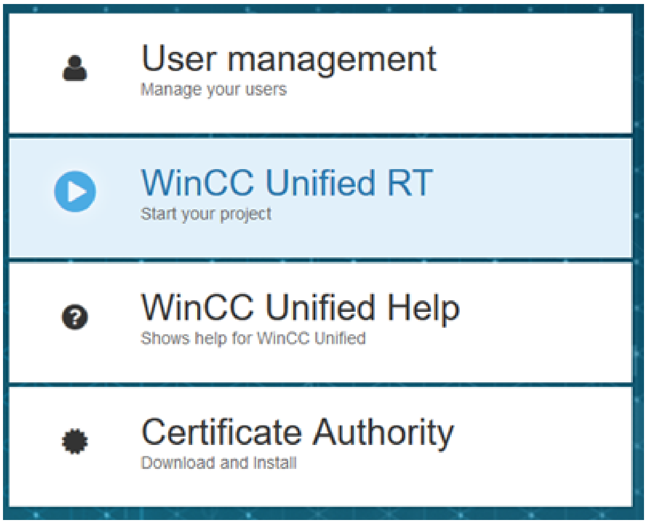
   An error message is displayed:



This site is not secure

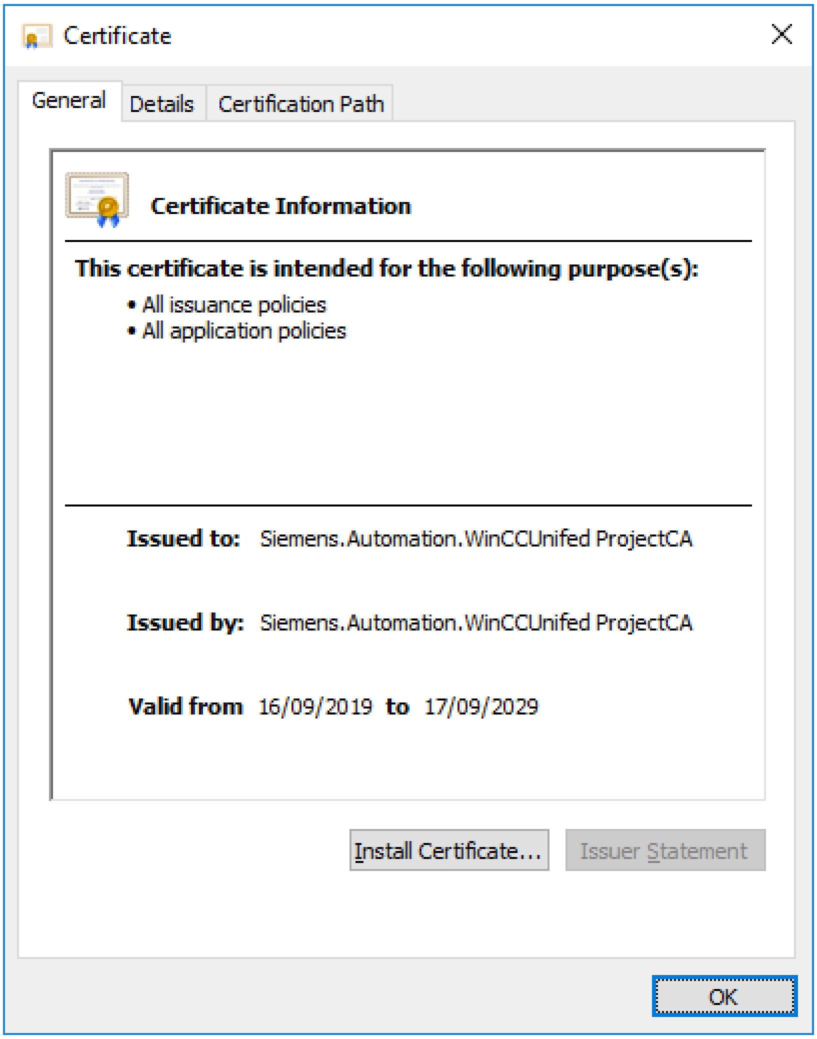
This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

3. Open the field with the error details and confirm that you want to open the web page. The WinCC Unified home page is loaded.
4. On the home page, select the "Certificate Authority" field and confirm "Open file" in the download dialog.



   The root certificate is downloaded to the default download directory.

5. Double-click the downloaded file.
   The root certificate is opened with the Windows standard form.



Certificate Information

This certificate is intended for the following purpose(s):
- All issuance policies
- All application policies

Issued to: Siemens.Automation.WinCCUnifed ProjectCA

Issued by: Siemens.Automation.WinCCUnifed ProjectCA

Valid from 16/09/2019 **to** 17/09/2029

6. Click "Install Certificate".
7. In the certificate import wizard, select "Local Machine" as the storage location and "Trusted Root Certification Authority" as the certificate store.
8. Start the import.
9. (optional) Check whether the root certificate was successfully installed in the Windows system certificate store.
   See section Checking the status of the web server root certificate on the web client. (Page 386).
10. Reload the page.

Result

The browser trusts the root certificate of the web server and, thus, it also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Establishing the trust relationship with the web server (Page 384)

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Creating a certificate authority and root certificate (Page 519)

Installing the root certificate for Firefox

Installing the root certificate before the first connection (for Firefox)

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) on a Firefox web client before the client connects to the web server for the first time. The description applies to clients installed on Windows devices.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager.
  See also section Creating a certificate authority and root certificate (Page 519).
- The web server root certificate has been exported on the certificate authority device with Certificate Manager to a storage location the web client can access.
  See section Exporting root certificate and CRL file (Page 531).

  Note

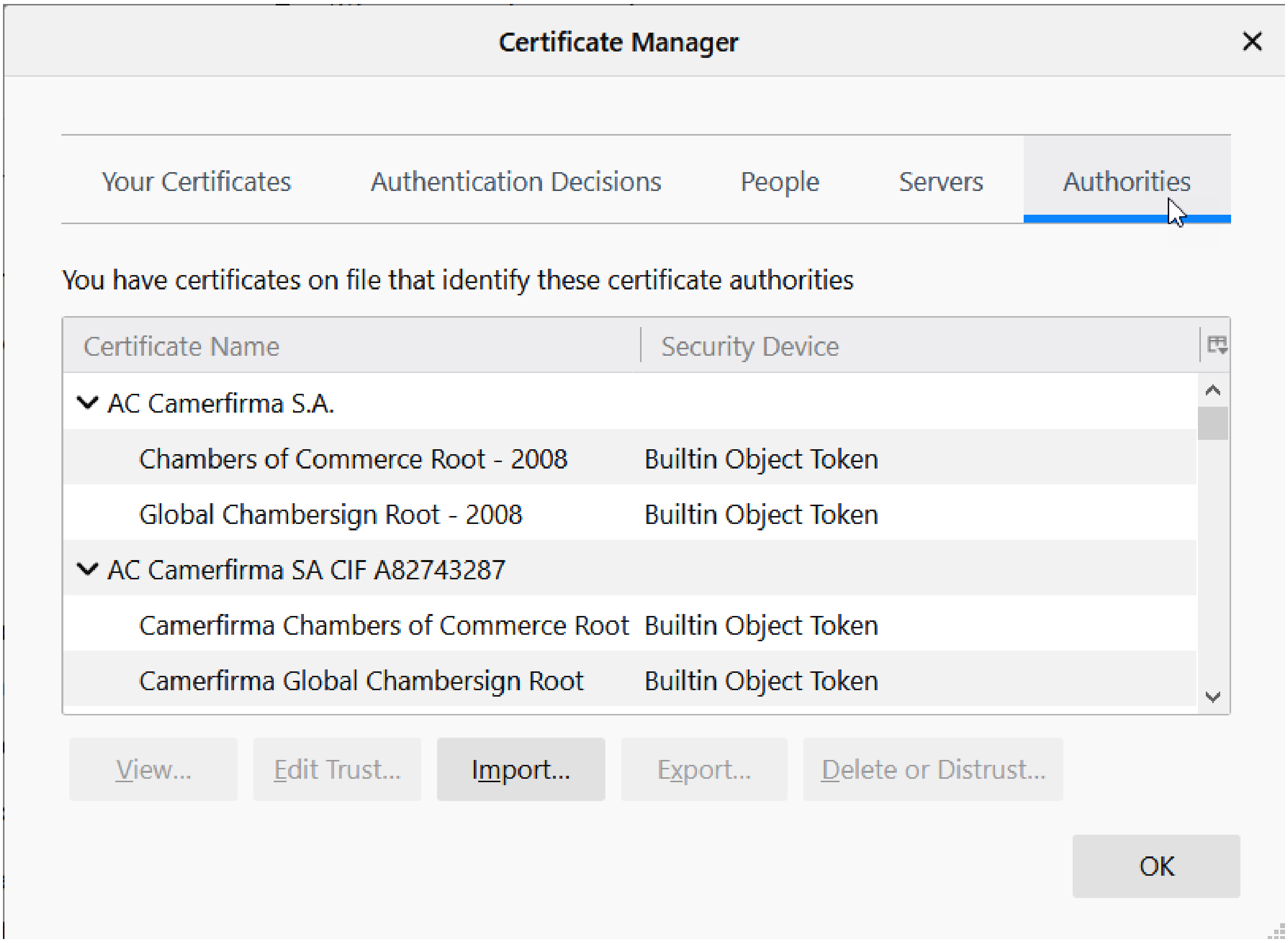
  Alternative

  If a Unified PC belongs to the infrastructure of the certificate authority of the web server whose certificates were already installed with Certificate Manager, you can export the root certificate on the PC with SIMATIC Runtime Manager.

  See section Managing third-party certificates of a Unified PC (Page 499).
- Firefox has been installed on the web client device.

Procedure

1. Start Firefox on the web client device.
2. Install the root certificate in the certificate store of Firefox. To do this, follow these steps:
   - Open the "Settings" page of Firefox.
   - Select "Privacy & Security".
   - Click "View Certificates" in the "Certificates" area.
   - Select the "Authorities" tab in the "Certificate Manager" window:



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

   - Click "Import" and select the root certificate file.
   - In the window that opens, select the option "This certificate can identify websites" and confirm your selection.

Result

At the first call of the web server web page, the browser trusts the root certificate of the web server and, thus, it automatically also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Checking the status of the web server root certificate on the web client. (Page 386)

Establishing the trust relationship with the web server (Page 384)

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Installing the root certificate at the first connection (for Firefox)

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) on a Firefox web client when the client first attempts to connect to the web server. The description applies to clients installed on Windows devices.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager. It has been installed on the web server.
- A Runtime project is running on the web server.
- Firefox has been installed on the web client device.
- The web server root certificate has not yet been installed in the certificate store of the browser.
- The client device has access to the web server.

Procedure

1. Start Firefox on the web client device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

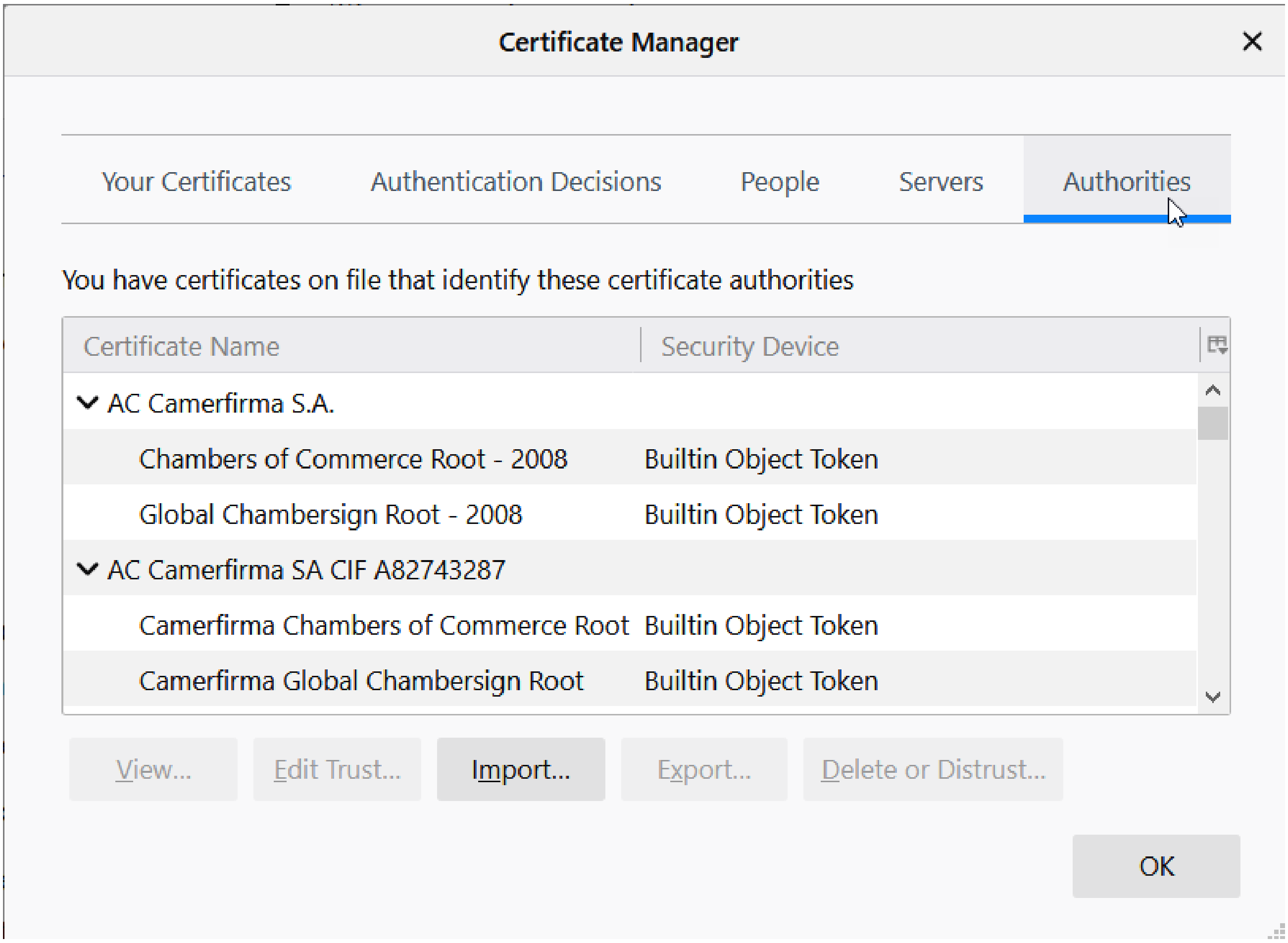
   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   An error message is displayed.
3. Open the "Advanced" field and confirm the "Accept the Risk and Continue" field.
4. An exception is entered for this page in the Firefox Certificate Manager.
5. On the WinCC Unified home page, select the "Certificate Authority" field.
6. Save the root certificate. To do this, click "Save file" in the Firefox dialog that follows.

7. Install the root certificate in the certificate store of Firefox. To do this, follow these steps:
   – Open the "Settings" page of Firefox.
   – Select "Privacy & Security".
   – Click "View Certificates" in the "Certificates" area.
   – Select the "Authorities" tab in the "Certificate Manager" window:



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

   – Click "Import" and select the root certificate file.
   – In the window that opens, select the option "This certificate can identify websites" and confirm your selection.
   – Click "Servers" and remove the exception that was created by step 2.
8. Reload the page.

Result

The browser trusts the root certificate of the web server and, thus, it also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Checking the status of the web server root certificate on the web client. (Page 386)

Creating a certificate authority and root certificate (Page 519)

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Establishing the trust relationship with the web server (Page 384)

Installing the root certificate on iOS devices

Installing the root certificate on iOS devices before the first connection

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) on an iOS web client before the client connects to the web server for the first time.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager.
- The web server root certificate has been exported on the certificate authority device with Certificate Manager to a storage location.
  See section Exporting root certificate and CRL file (Page 531).

Note

Alternative

If a Unified PC belongs to the infrastructure of the certificate authority of the web server whose certificates were already installed with Certificate Manager, you can export the root certificate on the PC with SIMATIC Runtime Manager.

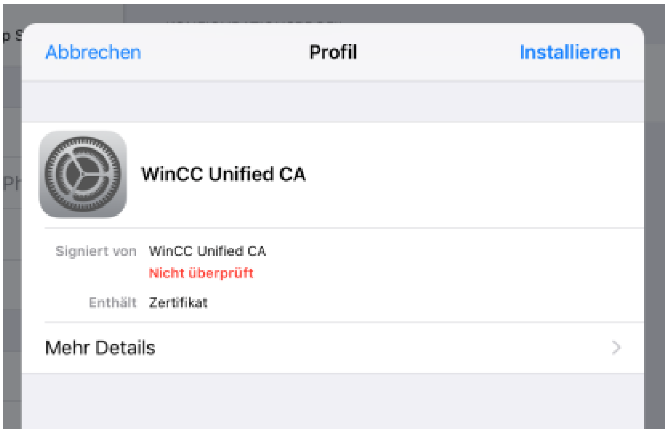
See section Managing third-party certificates of a Unified PC (Page 499).

- The web client device has access to the root certificate file, for example, because the file was sent to the device via email.
- The desired browser has been installed on the web client device.

Procedure

1. Tap the root certificate file on the iOS device.
   You are informed that the website is trying to load a configuration profile.
2. Tap "Allow"
   The configuration profile is loaded.
3. Tap "Close".
4. Select "Settings > General > Profile" on the device.
5. Tap the configuration profile you just loaded.

6. Tap "Install" at the top right.

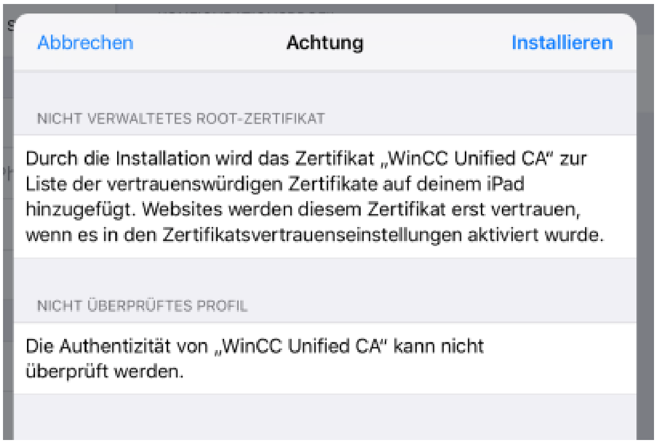


WinCC Unified CA

Signiert von WinCC Unified CA
Nicht überprüft

Enthält Zertifikat

7. Tap "Install" again at the top right.



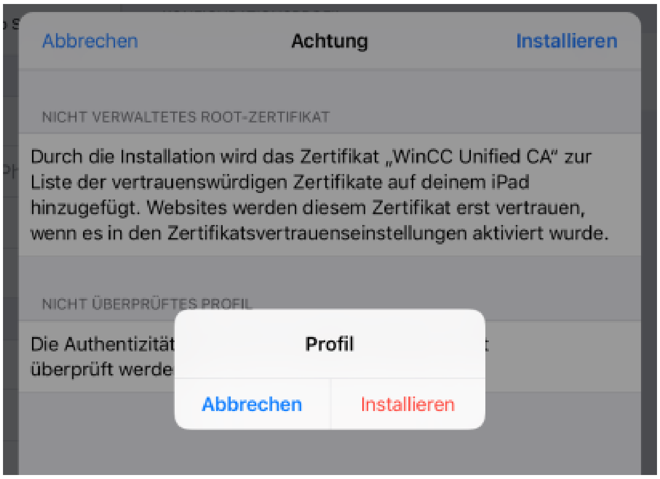
NICHT VERWALTETES ROOT-ZERTIFIKAT

Durch die Installation wird das Zertifikat „WinCC Unified CA“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

NICHT ÜBERPRÜFTES PROFIL

Die Authentizität von „WinCC Unified CA“ kann nicht überprüft werden.

8. Tap "Install" again in the "Profile" confirmation prompt:



NICHT VERWALTETES ROOT-ZERTIFIKAT

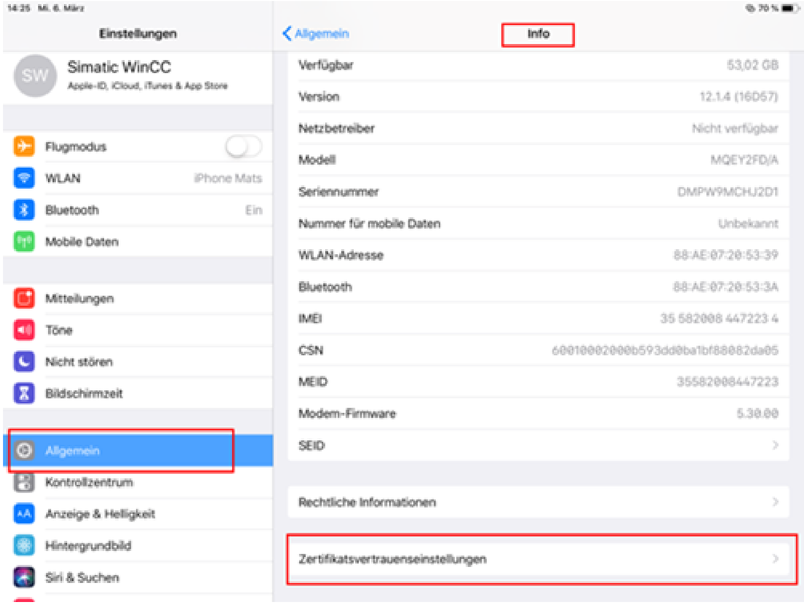
Durch die Installation wird das Zertifikat „WinCC Unified CA“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

NICHT ÜBERPRÜFTES PROFIL

Die Authentizität … überprüft werde…

The certificate is installed.

9. Select "Settings > General > About > Certificate Trust Settings" on the device:



Verfügbar	53,02 GB
Version	12.1.4 (16D57)
Netzbetreiber	Nicht verfügbar
Modell	MQEY2FD/A
Seriennummer	DMPW9MCHJ2D1
Nummer für mobile Daten	Unbekannt
WLAN-Adresse	88:AE:07:20:53:39
Bluetooth	88:AE:07:20:53:3A
IMEI	35 582008 447223 4
CSN	60010002000b593dd0ba1bf88082da05
MEID	35582008447223
Modem-Firmware	5.30.00

10. Select the "Enable full trust for root certificates" option for the web server root certificate.

Result

At the first call of the web server web page, the browser trusts the root certificate of the web server and, thus, it automatically also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Establishing the trust relationship with the web server (Page 384)

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Creating a certificate authority and root certificate (Page 519)

Installing the root certificate on iOS devices at the first connection

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) on an iOS web client when the client first attempts to connect to the web server.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager. It has been installed on the web server.
- A Runtime project is running on the web server.

- The desired browser has been installed on the web client device.
- The web server root certificate has not yet been installed in the certificate store of the browser.
- The client device has access to the web server.

Procedure

1. Start the browser on the web client device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

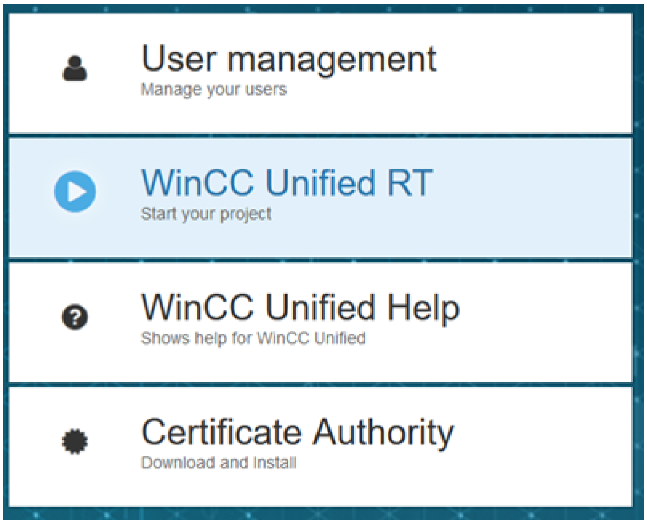
   Note

   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   A warning message is displayed.
3. Open the details for the message and select the button for loading the page.
   The WinCC Unified home page is loaded.
4. Load the root certificate to your device. Follow these steps:
   – On the home page, select the "Certificate Authority" field.

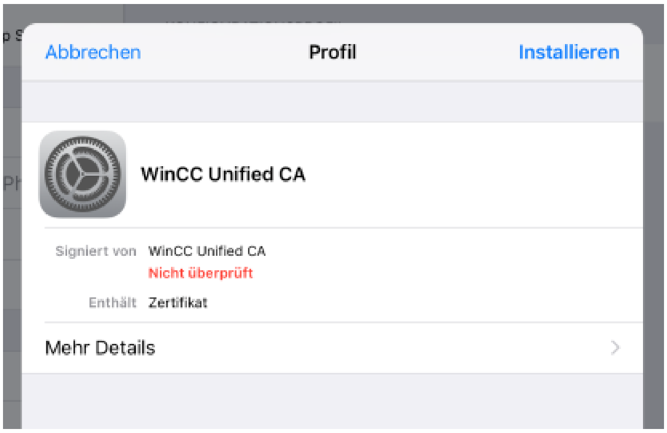


   A pop-up opens. It informs you that the website is trying to load a configuration profile.

   – Tap "Allow"
   The configuration profile is loaded.

   – Tap "Close".

5. Install the configuration profile on your device. Follow these steps:
   - Select "Settings > General > Profile" on the device.
   - Tap the configuration profile you just loaded.
   - Tap "Install" at the top right.



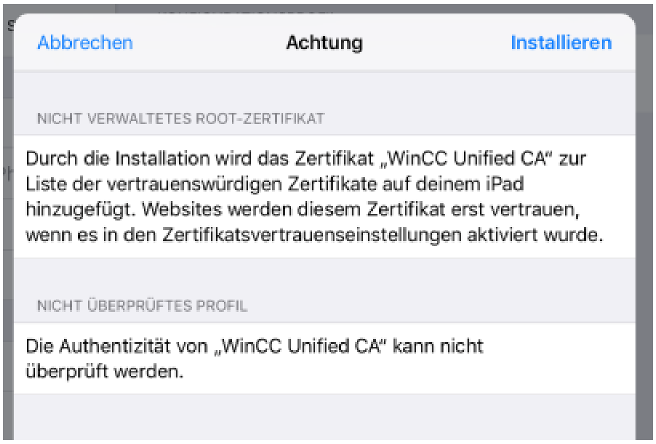
Abbrechen Profil Installieren

WinCC Unified CA

Signiert von WinCC Unified CA
Nicht überprüft
Enthält Zertifikat

Mehr Details

   - Tap "Install" again at the top right.



Abbrechen Achtung Installieren

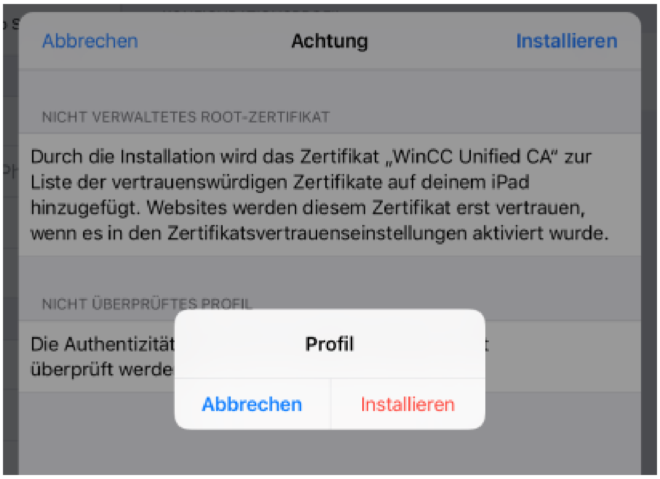
NICHT VERWALTETES ROOT-ZERTIFIKAT

Durch die Installation wird das Zertifikat „WinCC Unified CA" zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

NICHT ÜBERPRÜFTES PROFIL

Die Authentizität von „WinCC Unified CA" kann nicht überprüft werden.

– Tap "Install" again in the "Profile" confirmation prompt:



Abbrechen Achtung Installieren

NICHT VERWALTETES ROOT-ZERTIFIKAT

Durch die Installation wird das Zertifikat „WinCC Unified CA“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

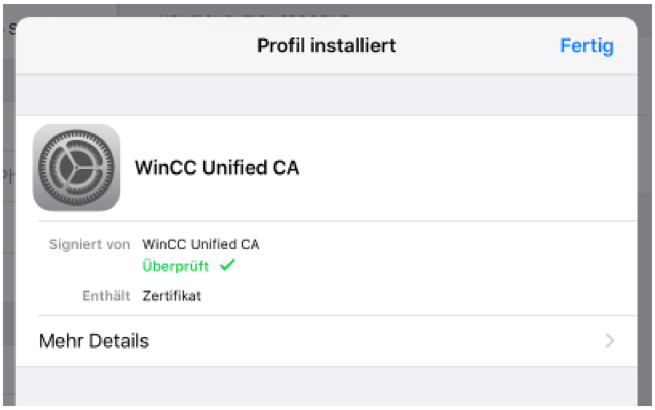
NICHT ÜBERPRÜFTES PROFIL

Die Authentizität
überprüft werde

Profil

Abbrechen Installieren

The root certificate is installed.
You see the entry "Verified".



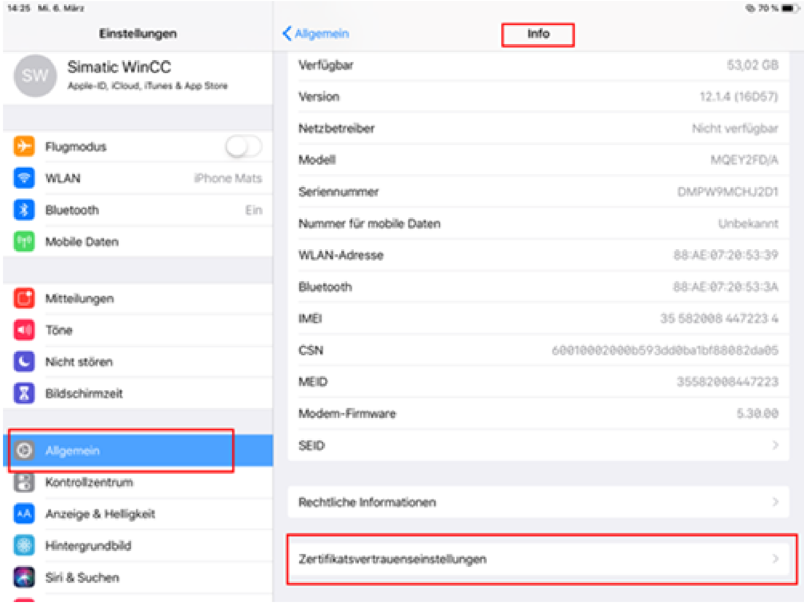
Profil installiert Fertig

WinCC Unified CA

Signiert von WinCC Unified CA
Überprüft ✓
Enthält Zertifikat

Mehr Details

– Select "General > About > Certificate Trust Settings".

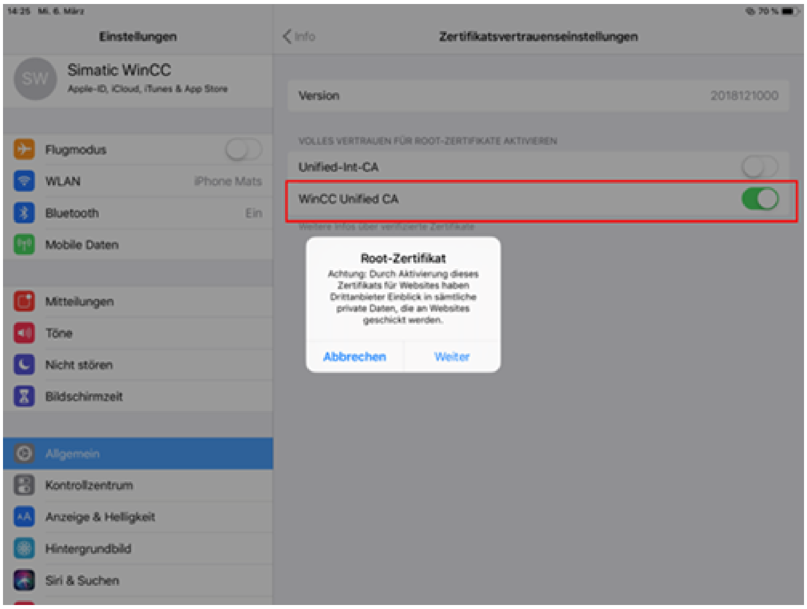


Verfügbar	53,02 GB
Version	12.1.4 (16D57)
Netzbetreiber	Nicht verfügbar
Modell	MQEY2FD/A
Seriennummer	DMPW9MCHJ2D1
Nummer für mobile Daten	Unbekannt
WLAN-Adresse	88:AE:07:20:53:39
Bluetooth	88:AE:07:20:53:3A
IMEI	35 582008 447223 4
CSN	60010002000b593dd0ba1bf88082da05
MEID	35582008447223
Modem-Firmware	5.30.00
SEID	>

Rechtliche Informationen >

Zertifikatsvertrauenseinstellungen >

– Select "WinCC Unified CA" and select "Next".



Version 2018121000

VOLLES VERTRAUEN FÜR ROOT-ZERTIFIKATE AKTIVIEREN

Unified-Int-CA ○

WinCC Unified CA ●

Weitere Infos über verifizierte Zertifikate

Root-Zertifikat

Achtung: Durch Aktivierung dieses Zertifikats für Websites haben Drittanbieter Einblick in sämtliche private Daten, die an Websites geschickt werden.

Abbrechen | Weiter

6. Load the Unified home page again.

Result

The browser trusts the root certificate of the web server and, thus, it also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Establishing the trust relationship with the web server (Page 384)

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Creating a certificate authority and root certificate (Page 519)

Installing the root certificate for the web browser of a Panel

Installing the root certificate before the first connection (Panel web browser)

Introduction

This section describes how to install the root certificate of a Runtime web server in the web browser of a Unified Panel before the browser connects to the web server for the first time.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager.
- The web server root certificate has been exported on the certificate authority device with Certificate Manager to a storage location the web client can access.
  See section Exporting root certificate and CRL file (Page 531).

Note

Alternative

If a Unified PC belongs to the infrastructure of the certificate authority of the web server whose certificates were already installed with Certificate Manager, you can export the root certificate on the PC with SIMATIC Runtime Manager.

See section Managing third-party certificates of a Unified PC (Page 499).

Procedure

Web browser uses the certificate store of the Panel. To install the root certificate there, follow the procedure described in section Importing and installing root certificates and CRL files on Panels (Page 545).

Result

At the first call of the web server web page, the browser trusts the root certificate of the web server and, thus, it automatically also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Creating a certificate authority and root certificate (Page 519)

Checking the status of a root certificate on the HMI device (Page 544)

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Establishing the trust relationship with the web server (Page 384)

Installing the root certificate at the first connection (Panel web browser)

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) in the web browser of a Unified Panel when the web browser first attempts to connect to the web server.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager. It has been installed on the web server.
- A Runtime project is running on the web server.
- The web server root certificate has not yet been installed in the certificate store of the Panel.
- The Panel has access to the web server.

Procedure

1. Start the "Web browser" application on the Panel.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   An error message is displayed.
3. Open the field with the error details and confirm that you want to open the web page.
   The WinCC Unified home page is loaded.

4. On the home page, select the "Certificate Authority" field and confirm "Open file" in the download dialog.
   The root certificate is downloaded.
5. Web browser uses the certificate store of the Panel. Install the root certificate there. Follow the procedure described in section Importing and installing root certificates and CRL files on Panels (Page 545).

Result

Web browser trusts the root certificate of the web server and, thus, it also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Checking the status of a root certificate on the HMI device (Page 544)

Workflow with a CA-based certificate (Panel as web server) (Page 382)

Establishing the trust relationship with the web server (Page 384)

Creating a certificate authority and root certificate (Page 519)

6.4.2.3 Using a self-signed certificate (Panel as web server)

Workflow with a self-signed certificate (Panel as web server)

A Unified Panel that is used as a Runtime web server can use a self-signed web server certificate.

Note

Self-signed certificates provide less protection than CA-based certificates. Use them for testing, for example. It is recommended that they then be replaced with CA-based certificates.

Limitations

- The self-signed web server certificate has a lifetime of 12 months.
- If no CA-based web server certificate has been installed on the Panel, each Runtime restart creates a new self-signed web server certificate. You must install the certificate on the web clients as a trusted certificate.

Requirement

- Web-based client access has been enabled for the Unified Panel.

Procedure

1. Stop Runtime on the Panel.
2. Check whether a CA-based web server certificate has already been installed on the Panel in the own application certificates. If so, uninstall it.
   See section Managing third party certificates and own certificates of a Unified Panel (Page 496).
3. Start Runtime on the Panel.
   A self-signed web server certificate is created, installed on the Panel and bound to the Runtime web page.
   The certificate is bound to the IP address and device name/FQDN of the Panel.
4. Trust the web server certificate on the web clients. See section Trusting the Panel web server on the web client (Page 407).

   Note

   Repeat this step after each Runtime start or Panel restart.

See also

Introduction (Page 381)

Trusting the Panel web server on the web client

Installing the self-signed web server certificate for Edge and Chrome

Introduction

This section describes how to install the self-signed web server certificate of a Runtime web server (Unified PC or Unified Panel) on an Edge or Chrome web client on Windows.

The procedure is explained using Edge as an example. The procedure is the same for Chrome.

Requirement

- The Runtime web server uses a self-signed web server certificate.
- A Runtime project is running on the web server.
- Microsoft Edge or Chrome has been installed on the web client device.
- The client device has access to the web server.

Procedure

1. Start Microsoft Edge on the web client device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

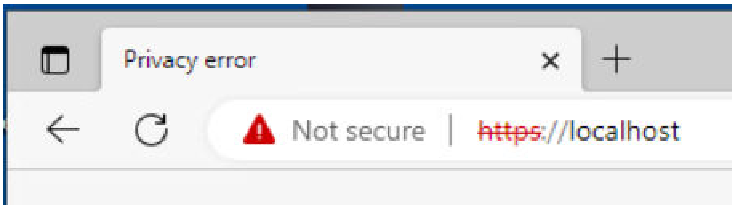
   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

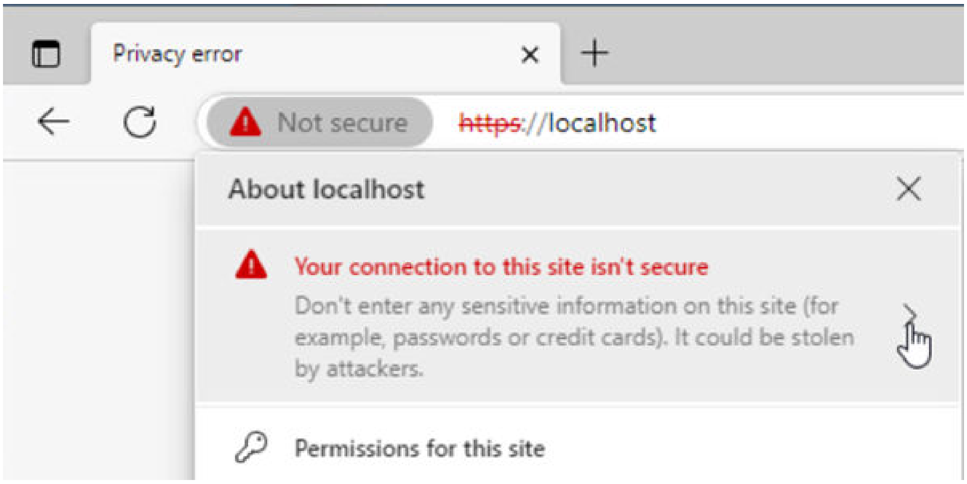
   If needed, ask your administrator.

   Edge warns you that the connection is not secure.

3. Download the certificate. To do this, follow these steps:
   - Click the triangle with the exclamation point in the address bar:



   - Click the notice that the connection to the website is not secure:

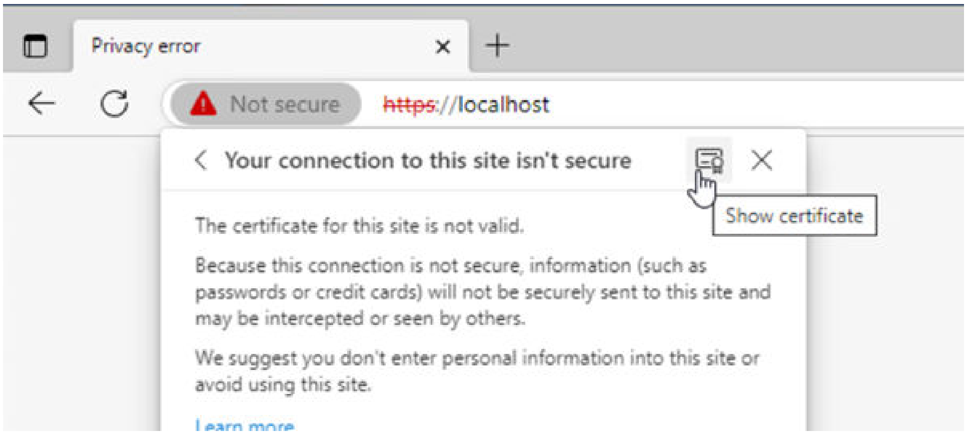


About localhost

Your connection to this site isn't secure

Don't enter any sensitive information on this site (for example, passwords or credit cards). It could be stolen by attackers.

   - Click the "Show certificate" icon:



Your connection to this site isn't secure

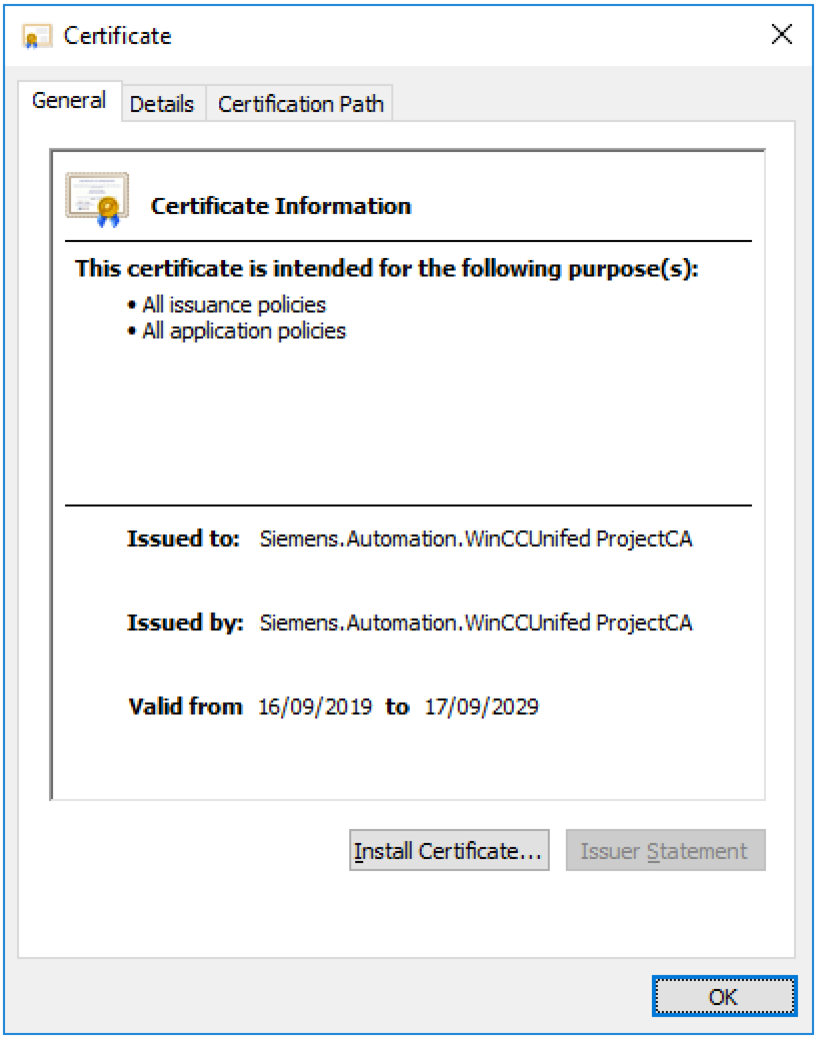
The certificate for this site is not valid.

Because this connection is not secure, information (such as passwords or credit cards) will not be securely sent to this site and may be intercepted or seen by others.

We suggest you don't enter personal information into this site or avoid using this site.

   - Click "Export" in the "Details" tab.
   - Select a storage location and save the certificate.

4. Install the certificate in the certificate store of Windows. To do this, follow these steps:
   - Double-click the downloaded certificate file.
     The certificate is opened with the Windows standard form.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: Siemens.Automation.WinCCUnifed ProjectCA

Issued by: Siemens.Automation.WinCCUnifed ProjectCA

Valid from 16/09/2019 **to** 17/09/2029

   - Click "Install Certificate".
   - In the certificate import wizard, select "Local Machine" as the storage location and "Trusted Root Certification Authority" as the certificate store.
   - Start the import.
5. Reload the page.

Result

The browser trusts the self-signed web server certificate.

You can log in to Runtime with a secure connection.

See also

Checking the status of the web server root certificate on the web client. (Page 386)

Workflow with a self-signed certificate (Panel as web server) (Page 406)

Installing the self-signed web server certificate for Firefox

Introduction

This section describes how to install the self-signed web server certificate of a Runtime web server (Unified PC or Unified Panel) on a Firefox web client on Windows.

Requirement

- The Runtime web server uses a self-signed web server certificate.
- A Runtime project is running on the web server.
- Firefox has been installed on the web client device.
- The client device has access to the web server.

Procedure

1. Start Firefox on the web client device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   An error message is displayed.
3. Download the certificate. To do this, follow these steps:
   - Open the "Advanced" field.
   - Click "More Information".
     A dialog with the page information opens.
   - Click "Security > View Certificate".
     A tab with the certificate information opens.
   - Click "PEM (certificate)" under "Miscellaneous > Save".
   - Select a storage location and save the certificate.

4. Install the certificate in the certificate store of Firefox. To do this, follow these steps:
   - Open the "Settings" page of Firefox.
   - Select "Privacy & Security".
   - Click "View Certificates" in the "Certificates" area.
   - Click "Import" and select the certificate file.
5. Reload the page.

Result

The browser trusts the self-signed web server certificate.

You can log in to Runtime with a secure connection.

See also

Workflow with a self-signed certificate (Panel as web server) (Page 406)

Installing the self-signed web server certificate for an iOS device

Introduction

This section describes how to install the self-signed web server certificate of a Runtime web server (Unified PC or Unified Panel) on the web client of an iOS device.

The procedure is explained using Safari as an example. The procedure is the same for other browsers.

Requirement

- A self-signed web server certificate has been installed on the web server HMI device.
- A Runtime project is running on the web server.
- The client device is an iOS device.
- The device has access to the web server.
- Safari has been installed on the device.

Procedure

1. Start Safari on the HMI device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

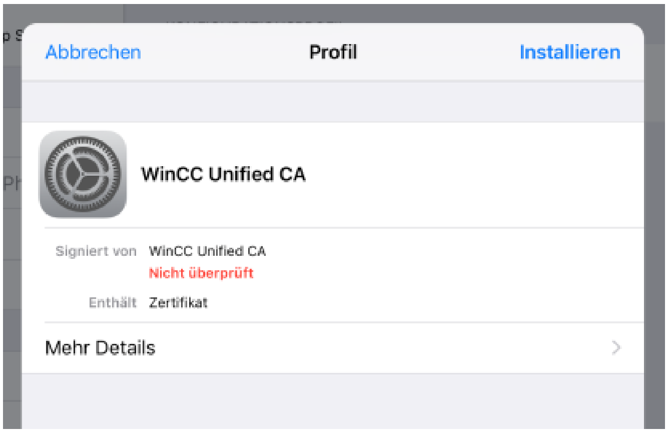
   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   An error message is displayed.
3. Load the self-signed web server certificate to your device. Follow these steps:
   – CHECK: How? / Click where?
   Is the self-signed certificate also considered a configuration profile?
   A pop-up opens. It informs you that the website is trying to load a configuration profile.
   – Tap "Allow".
   The configuration profile is loaded.
   – Tap "Close".

4. Install the configuration profile on your device. Follow these steps:
   - Select "Settings > General > Profile" on the device.
   - Tap the configuration profile you just loaded.
   - Tap "Install" at the top right.

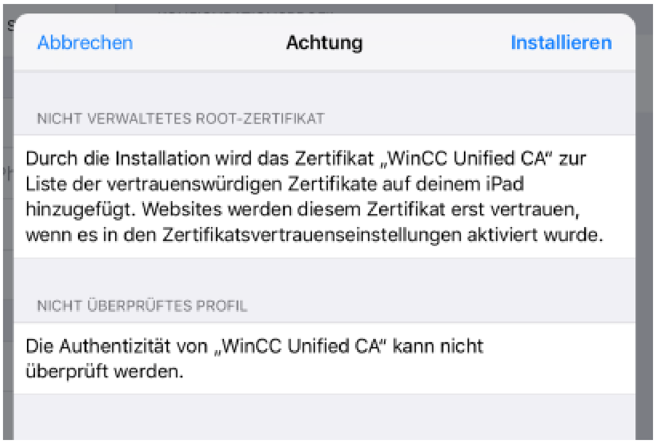


WinCC Unified CA

Signiert von WinCC Unified CA
Nicht überprüft

Enthält Zertifikat

   - Tap "Install" again at the top right.



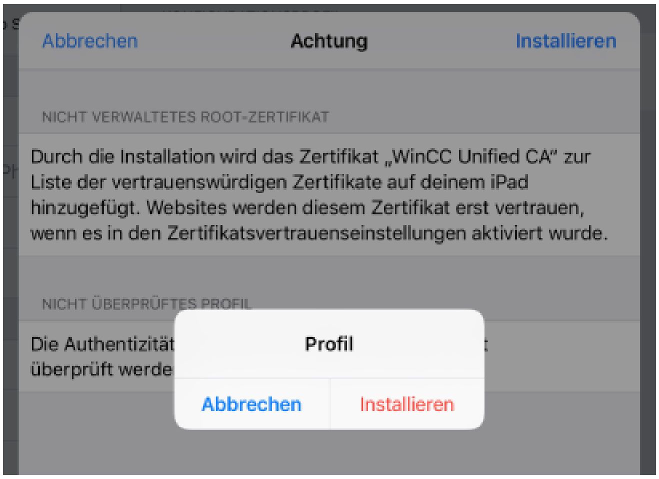
NICHT VERWALTETES ROOT-ZERTIFIKAT

Durch die Installation wird das Zertifikat „WinCC Unified CA“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

NICHT ÜBERPRÜFTES PROFIL

Die Authentizität von „WinCC Unified CA“ kann nicht überprüft werden.

– Tap "Install" again in the "Profile" confirmation prompt:



NICHT VERWALTETES ROOT-ZERTIFIKAT

Durch die Installation wird das Zertifikat „WinCC Unified CA“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

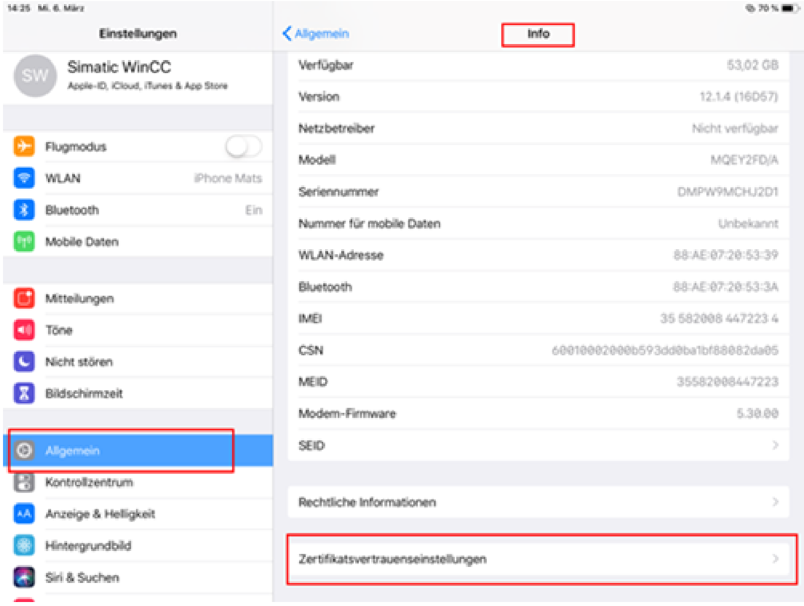
NICHT ÜBERPRÜFTES PROFIL

Die Authentizität ... überprüft werde...

Profil

The certificate is installed.

– Select "Settings > General > About > Certificate Trust Settings" on the device:



Verfügbar	53,02 GB
Version	12.1.4 (16D57)
Netzbetreiber	Nicht verfügbar
Modell	MQEY2FD/A
Seriennummer	DMPW9MCHJ2D1
Nummer für mobile Daten	Unbekannt
WLAN-Adresse	88:AE:07:20:53:39
Bluetooth	88:AE:07:20:53:3A
IMEI	35 582008 447223 4
CSN	60010002000b593dd0ba1bf88082da05
MEID	35582008447223
Modem-Firmware	5.30.00
SEID	

Rechtliche Informationen

Zertifikatsvertrauenseinstellungen

– Select the "Full trust for root certificates" option for the certificate.

5. (optional) Check whether the web server certificate was successfully installed.
   Follow the same procedure as you use to check whether a web server root certificate has been installed on the web client.
6. Load the Unified home page again.

Result

The browser trusts the self-signed web server certificate.

You can log in to Runtime with a secure connection.

Alternative procedure

1. Export the self-signed web server certificate on the device of another web client that communicates with the same web server, e.g. with Edge.
2. Transfer the certificate to the iOS device, for example, by sending it as an email attachment and downloading the attachment to the iOS device.
   A pop-up opens. It informs you that the website is trying to load a configuration profile.
3. Tap "Allow".
   The configuration profile is loaded.
4. Tap "Close".
5. Continue as described above, starting from step 4.

See also

Workflow with a self-signed certificate (Panel as web server) (Page 406)

Checking the status of the web server root certificate on the web client. (Page 386)

Installing the self-signed web server certificate for the web browser of a Panel

Introduction

This section describes how to install the self-signed web server certificate of a Runtime web server (Unified PC or Unified Panel) in the web browser of a Unified Panel.

Requirement

- A self-signed web server certificate has been installed on the web server HMI device.
- A Runtime project is running on the web server.
- The client device has access to the web server.

Procedure

1. Start the "Web browser" application on the Panel.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   The browser warns you that the connection is not secure.

3. Display the details for the connection.
4. Display the certificate.
5. Download the certificate.
   The certificate is loaded into the certificate store of the Panel. The Panel does not yet trust the certificate.
6. Trust the certificate with "Control Panel > Security > Certificates".
7. Reload the page in the web browser.

Result

The web browser trusts the self-signed web server certificate.

You can log in to Runtime with a secure connection.

See also

Workflow with a self-signed certificate (Panel as web server) (Page 406)

Importing and installing root certificates and CRL files on Panels (Page 545)

6.4.3 OPC UA certificates (Panel)

6.4.3.1 Introduction

If the OPC UA server uses a security policy, the OPC UA communication is protected through the use of certificates. The OPC UA server must trust the OPC UA certificates of its clients, and vice versa (mutual SSL authentication).

Panel as OPC UA server

If you are using a Unified Panel as an OPC UA server, its OPC UA server certificate can be issued by a certificate authority (CA-based certificate) or be self-signed.

Note

For security reasons, it is recommended to use a CA-based certificate. You use WinCC Unified Certificate Manager to create the certificate.

Note

For Panels that are used as OPC UA servers, a tag export to an OPC UA NodeSet XML file is not possible.

Panel as OPC UA client

A Unified Panel that is used as an OPC UA client must use a certificate issued by a Unified certificate authority (CA-based certificate). You use WinCC Unified Certificate Manager to create the certificate.

Note

If you are using a Panel as an OPC UA client, the Engineering System also acts as an OPC UA client during configuration of the device. See section Engineering System as OPC UA client (Page 424).

Contents of this help

This help describes the following:

- Creating a CA-based OPC UA server certificate or OPC UA client certificate of the Panel
- Installing the CA-based certificate on the Panel
- Using the default self-signed certificate for Panel as OPC UA server
- Establishing the trust relationship with the OPC UA communication partner on the Panel
- Distributing the OPC UA certificate of the Panel to the OPC UA communication partner
  This step sets up the establishment of the trust relationship with the Panel on the OPC UA communication partner.

Note

Procedure at the OPC UA communication partners

For information on how to create and install the OPC UA certificate of the communication partner and distribute it to the Panel and how to trust the certificate of the Panel on the communication partner, refer to the operating instructions of the respective communication partner.

See also

CA-based certificate workflow (OPC UA for Panel) (Page 419)

Using a default self-signed certificate (Panel as OPC UA server) (Page 423)

Selecting a suitable certificate type (Page 493)

6.4.3.2 Using CA-based certificates (OPC UA for Panel)

CA-based certificate workflow (OPC UA for Panel)

For CA-based OPC UA communication, a Unified Panel needs the following certificates:

- OPC UA application certificate suitable for the role of the Panel during OPC UA communication:
  - OPC UA server certificate
    or
  - OPC UA client certificate
- Root certificate of the certificate authority that issued the OPC UA application certificate of the Panel, along with its CRL file.

Requirement

- The OPC UA server uses a security policy.
- The OPC UA communication partner of the Panel has an OPC UA application certificate that was issued by a certificate authority.
- The certificate has been installed on the communication partner as an own certificate.

Workflow

1. Create an OPC UA server certificate or an OPC UA client certificate for the Panel, depending on the role of the Panel.
   See section Creating certificates (OPC UA for Panel) (Page 419).
2. Install the certificate on the Panel.
   See section Installing certificates (OPC UA for Panel) (Page 420).
3. Restart Runtime on the Panel.
4. Establish the trust relationship between the Panel and its OPC UA communication partner.
   See section Establishing the trust relationship (OPC UA for Panel) (Page 421).

See also

Introduction (Page 417)

Creating certificates (OPC UA for Panel)

Introduction

You create the OPC UA server certificate or OPC UA client certificate of a Unified Panel on the certificate authority device. You use the WinCC Unified Certificate Manager application for this.

The certificate authority device is always a Unified PC.

Procedure

If you do not have a certificate authority yet, follow these steps:

1. Create the certificate authority.
   In so doing, you create the root certificate of the certificate authority and its CRL file automatically.
   See section Creating a certificate authority and root certificate (Page 519).
2. Add the Panel to the certificate authority.
   See section Adding devices (Page 521).
3. Add the OPC UA server certificate or the OPC UA client certificate to the Panel, depending on the role of the Panel.
   See section Add application certificates (Page 524).

If you already have a certificate authority, follow these steps:

1. If the Panel has not yet been added to the infrastructure of the certificate authority, add the Panel.
   See section Adding devices (Page 521).
2. Add the OPC UA server certificate or the OPC UA client certificate to the Panel, depending on the role of the Panel.
   See section Add application certificates (Page 524).

See also

CA-based certificate workflow (OPC UA for Panel) (Page 419)

Installing certificates (OPC UA for Panel)

Introduction

The OPC UA application certificate of a Unified Panel is installed in the following steps:

- Export on the certificate authority device
- Import on the Panel

Note

You always export and import all certificates of the Panel as well as the root certificate of the issuing certificate authority and its CRL file.

These certificates are automatically installed by the import.

Requirement

- The desired OPC UA application certificate has been added for the Panel on the certificate authority device.

Procedure

1. Export the certificates of the Panel on the certificate authority device. Use the WinCC Unified Certificate Manager for this.
   See section Exporting certificates of a Panel (Page 530).
2. Import the certificates to the Panel. Use the Control Panel for this.
   See section Importing and installing certificates of a Unified Panel (Page 541).

See also

CA-based certificate workflow (OPC UA for Panel) (Page 419)

Add application certificates (Page 524)

Establishing the trust relationship (OPC UA for Panel)

Introduction

Secure OPC UA communication requires that the communication partners trust each other's OPC UA application certificates.

That is automatically the case when the OPC UA client trusts the root certificate of the certificate authority that issued the OPC UA server certificate, and vice versa.

Procedure

1. Check the Panel to determine whether it already trusts the root certificate of its OPC UA communication partner.
   See sections Checking the status of a root certificate on the HMI device (Page 544) and Automatic trust relationship in OPC UA communication (Page 422).
   If the Panel already trusts the root certificate, continue with step 3.
2. If the Panel does not trust the root certificate, install it manually.
   Follow these steps:
   - Export the root certificate of the OPC UA communication partner and its CRL file to a storage location the Panel can access.
     Follow the procedure described in the operating instructions of the communication partner.
   - Install the root certificate and the CRL file on the Panel.
     See section Importing and installing root certificates and CRL files on Panels (Page 545).

3. Check the communication partner to determine whether it already trusts the root certificate of the Panel.
   Follow the procedure described in the application help of the communication partner.
   If the communication partner already trusts the root certificate, you don't have to do anything.
4. If the communication partner does not trust the root certificate, install it manually.
   Follow these steps:
   - Export the root certificate on the certificate authority device with Certificate Manager to an external data storage medium.
     See section Exporting root certificate and CRL file (Page 531).

     Note

     Alternative

     If a Unified PC belongs to the infrastructure of the certificate authority of the Panel whose certificates were already installed with Certificate Manager, you can export the root certificate on the PC with SIMATIC Runtime Manager.

     See section Managing third-party certificates of a Unified PC (Page 499).
   - Connect the OPC UA communication partner to the external data storage medium.
   - Install the root certificate and its CRL file on the communication partner.
     Follow the procedure described in the user help of the communication partner. If necessary, manually copy both files to the folder for trusted certificates.

At the next connection attempt, the OPC UA server and OPC UA client trust each other.

See also

CA-based certificate workflow (OPC UA for Panel) (Page 419)

Managing third party certificates and own certificates of a Unified Panel (Page 496)

Automatic trust relationship in OPC UA communication

This section describes cases in which a device automatically trusts the CA-based certificate of its OPC UA communication partner. You do not have to establish the trust relationship manually on this device.

Same certificate authority

If both OPC UA communication partners are HMI devices and their OPC UA certificates have the same certificate authority, they automatically trust their OPC UA certificates.

Trusted certificate authority

If a device already trusts the certificate authority that issued the OPC UA certificate of the other device, it also automatically trusts the other device's OPC UA certificate.

Example

A Unified OPC UA server communicates with an OPC UA client. Server and client have different certificate authorities. The Unified OPC UA server trusts the root certificate of the OPC UA client, and vice versa. As a result, the devices also trust their OPC UA certificates.

A second OPC UA client authenticates itself to the Unified OPC UA server. Its OPC UA client certificate was issued by the same certificate authority that issued the OPC UA client certificate of the first client.

Since the Unified OPC UA server already trusts the root certificate, the server automatically also trusts the OPC UA client certificate of the second client.

Tag export of a Unified OPC UA server

In OPC UA communication, you have the option of exporting the tags of the project of a Unified OPC UA server running in Runtime. The device must be a Unified PC that has an OPC UA server certificate and OPC UA exporter certificate.

In CA-based communication, the root certificate of the certificate authority that issues these certificates is also automatically installed when you generate the certificates of the device with WinCC Unified Certificate Manager. The OPC UA server component and OPC UA exporter component of the device trust each other automatically.

See also

Establishing the trust relationship (OPC UA for Panel) (Page 421)

6.4.3.3 Using a default self-signed certificate (Panel as OPC UA server)

Introduction

A Unified Panel that is used as an OPC UA server can use a self-signed OPC UA server certificate (default certificate).

If there is no CA-based OPC UA server certificate in the own certificates at Runtime start of the Panel, the self-signed OPC UA server certificate is automatically created and installed on the Panel.

Note

Self-signed certificates provide less protection than CA-based certificates. Use them for testing, for example. It is recommended that they then be replaced with CA-based certificates.

Limitations

- The self-signed OPC UA server certificate has a lifetime of 12 months.
- If no CA-based OPC UA server certificate has been installed on the Panel, each Runtime restart creates a new self-signed OPC UA server certificate. You must reestablish the trust relationship with the OPC UA server after each Runtime restart on the client.

Requirement

- The OPC UA server uses a security policy.
- The OPC UA client uses a self-signed OPC UA client certificate.
- Server and client do not yet trust their OPC UA certificates.
- Server and client are running.

Procedure

1. Check whether a CA-based OPC UA server certificate has been installed on the Panel as an own certificate.
   See section Managing third party certificates and own certificates of a Unified Panel (Page 496).
2. If so, uninstall the CA-based OPC UA server certificate and restart Runtime.
   See section Managing third party certificates and own certificates of a Unified Panel (Page 496).
   At the next connection attempt, the OPC UA client and OPC UA server exchange their certificates.
3. After the first connection attempt, the OPC UA client certificate is in the "untrusted" folder of the certificate store on the Panel.
   Trust the certificate on the Panel. See section Managing third party certificates and own certificates of a Unified Panel (Page 496).
4. After the first connection attempt, the OPC UA server certificate is in the rejected certificate store on the client device.
   Trust the certificate on the client. Follow the procedure described in the user help of the client. If necessary, manually copy the certificate to the folder for trusted certificates.

   Note

   Repeat this step after each Runtime start or Panel restart.

See also

Importing and installing root certificates and CRL files on Panels (Page 545)

Establishing the trust relationship (OPC UA for Panel) (Page 421)

Introduction (Page 417)

6.4.3.4 Engineering System as OPC UA client

Introduction

If you are using a Unified PC or a Unified Panel as an OPC UA client, you configure which tags of the OPC UA server the client accesses and which alarm instances it receives in the Engineering System. For this reason, the Engineering System also acts as an OPC UA client during configuration of the device.

Provision and installation of the certificates

The client certificate of the Engineering System is created and transferred to the server automatically the first time a connection is established.

Trust the client certificate on the server. Follow the procedure described in the user help of the server. If necessary, manually copy the certificate to the folder for trusted certificates.

The Engineering System automatically receives the server certificate and trusts it without your having to take any action.

See also

Introduction (Page 417)

6.4.4 Audit certificates (Panel)

6.4.4.1 Workflow

Introduction

The WinCC Unified Audit option uses certificates to generate a checksum for Audit Trail data records. The checksum can be used to determine if the contents of a data record have been altered. The checksum also ensures that no lines have been removed from or added to the Audit Trail.

Audit certificates are not used for communication with another device.

The Audit certificate of a Unified Panel or Unified PC must be issued by a Unified certificate authority (CA-based certificate). You use the "WinCC Unified Certificate Manager" application for this.

Note

Certificate Manager always creates CA-based certificates. The use of CA-based certificates facilitates establishment of the trust relationship and provides the highest protection for your plant.

The use of self-signed certificates is not supported for Audit.

Required certificates

For WinCC Unified Audit, you need the following certificates:

- Audit certificate of the HMI device
- Root certificate of the certificate authority that issued the Audit certificate, along with its CRL file.

Workflow

To provide the certificates needed by an HMI device for Audit, follow these steps:

1. Create the Audit certificate of the HMI device.
2. Install the Audit certificate on the HMI device.
3. Restart Runtime on the HMI device.

See also

Creating certificates (Audit for Panels) (Page 426)

Installing certificates (Audit for Panels) (Page 427)

6.4.4.2 Creating certificates (Audit for Panels)

Introduction

You create the Audit certificate of a Unified Panel on the certificate authority device. You use the "WinCC Unified Certificate Manager" application for this.

The certificate authority device is always a Unified PC.

Procedure

If you do not have a certificate authority yet, follow these steps:

1. Create the certificate authority.
   In so doing, you create the root certificate of the certificate authority and its CRL file automatically.
   See section Creating a certificate authority and root certificate (Page 519).
2. Add the Panel to the certificate authority.
   See section Adding devices (Page 521).
3. Add the Collaboration certificate to the Panel.
   See section Add application certificates (Page 524).

If you already have a certificate authority, follow these steps:

1. If the Panel has not yet been added to the infrastructure of the certificate authority, add the Panel.
   See section Adding devices (Page 521).
2. Add the Audit certificate to the Panel.
   See section Add application certificates (Page 524).

See also

Workflow (Page 425)

6.4.4.3 Installing certificates (Audit for Panels)

Introduction

The Audit certificate of a Unified Panel is installed in the following steps:

- Export on the certificate authority device
- Import on the Panel

Note

You always export and import all certificates of the Panel as well as the root certificate of the issuing certificate authority and its CRL file.

These certificates are automatically installed by the import.

Requirement

- The Audit certificate has been added for the Panel on the certificate authority device.

Procedure

1. Export the certificates of the Panel on the certificate authority device. Use the WinCC Unified Certificate Manager for this.
   See section Exporting certificates of a Panel (Page 530).
2. Import the certificates to the Panel. Use the Control Panel for this.
   See section Importing and installing certificates of a Panel (Page 541).

See also

Workflow (Page 425)

6.4.5 Smart Server certificates for Panels

If you are using a Unified Panel as a Smart Server, you can protect the communication between the Smart Server and Smart Client through the use of a self-signed Smart Server certificate.

With corresponding configuration of the Panel in the Engineering System, the certificate is automatically created and installed on the Panel when the Panel is loaded. When the connection between the server and client is established, the certificate is automatically transferred to the client. The client must trust the certificate.

You can find more information in the TIA Portal help system under "Using distributed systems > WinCC Smart Server".

6.5 Certificates for Unified PCs

6.5.1 Collaboration certificates (PC)

6.5.1.1 Collaboration certificates and Runtime version

Runtime Collaboration requires that the Collaboration certificates of 2 Collaboration partners be created with a certificate authority device whose installed Runtime version is equal to or higher than the installed Runtime version of the Collaboration partner with the higher Runtime version.

For this reason, the upgrading of Collaboration devices requires the creation, distribution and installation of new Collaboration certificates.

Example:

- A Unified PC and a Unified Panel with Runtime version V17 are Collaboration partners.
- You upgrade the Panel to V18.
- Create new Collaboration certificates for both HMI devices on a certificate authority device with installed Runtime version V18 or higher. Distribute them to and install them on the devices.

See also

Workflow (Collaboration for PCs) (Page 428)

6.5.1.2 Workflow (Collaboration for PCs)

Introduction

WinCC Unified Collaboration protects the communication between the Collaboration devices through the use of certificates.

The certificates must be issued by a Unified certificate authority (CA-based certificates). You use the WinCC Unified Certificate Manager application for this.

Note

Certificate Manager always creates CA-based certificates. The use of CA-based certificates facilitates establishment of the trust relationship and provides the highest protection for your plant.

The use of self-signed certificates is not supported for Collaboration.

Required certificates

For successful communication between two Collaboration devices, you need the following certificates for each Collaboration device:

- Collaboration certificate of the device
- Root certificate of the certificate authority that issued the Collaboration certificate, along with its CRL file.

Workflow

To provide the certificates needed by a Unified PC Collaboration device, follow these steps:

1. Create the Collaboration certificate of the PC.
2. Install the Collaboration certificate on the PC.
3. Restart Runtime on the PC.
4. Establish the trust relationship between the PC and its Collaboration partner.

See also

Creating certificates (Collaboration for PCs) (Page 429)

Installing certificates (Collaboration for PCs) (Page 430)

Establishing the trust relationship (Collaboration for PCs) (Page 431)

Collaboration certificates (Panel) (Page 377)

Collaboration certificates and Runtime version (Page 428)

6.5.1.3 Creating certificates (Collaboration for PCs)

Introduction

You create the Collaboration certificate of a Unified PC on the certificate authority device. You use the WinCC Unified Certificate Manager application for this.

The certificate authority device is always a Unified PC.

Procedure

If you do not have a certificate authority yet, follow these steps:

1. Create the certificate authority.
   In so doing, you create the root certificate of the certificate authority and its CRL file automatically.
   See section Creating a certificate authority and root certificate (Page 519).
2. Add the PC to the certificate authority.
   See section Adding devices (Page 521).
3. Add the Collaboration certificate to the PC.
   See section Add application certificates (Page 524).

If you already have a certificate authority, follow these steps:

1. If the PC has not yet been added to the infrastructure of the certificate authority, add the PC.
   See section Adding devices (Page 521).
2. Add the Collaboration certificate to the PC.
   See section Add application certificates (Page 524).

See also

Workflow (Collaboration for PCs) (Page 428)

Collaboration certificates and Runtime version (Page 428)

6.5.1.4 Installing certificates (Collaboration for PCs)

Introduction

The Collaboration certificate of a Unified PC is installed in the following steps:

- Export on the certificate authority device
- Import to the PC
- Installation on the PC

Note

You always export and import all certificates of the PC as well as the root certificate of the issuing certificate authority and its CRL file.

Requirement

- The Collaboration certificate has been added for the PC on the certificate authority device.

Procedure

1. Export the certificates of the PC on the certificate authority device. Use the WinCC Unified Certificate Manager for this.
   See section Exporting certificates of a Unified PC (Page 528).
2. Import the certificates to the PC. Use the Certificate Manager for this.
   See section Importing certificates of a Unified PC (Page 538).
3. Install all certificates together on the PC or only the Collaboration certificate. Use the Certificate Manager for this.
   See section Installing all certificates or single certificates of a PC (Page 539).

See also

Workflow (Collaboration for PCs) (Page 428)

Add application certificates (Page 524)

6.5.1.5 Establishing the trust relationship (Collaboration for PCs)

Introduction

Secure communication between Collaboration devices requires that the devices trust each other's Collaboration certificate.

That is automatically the case when a device trusts the root certificate of the certificate authority that issued the Collaboration certificate of the other device, and vice versa.

Trusting the Collaboration partner of a PC

To ensure that a Unified PC trusts its Collaboration partner, follow these steps:

1. Check whether the PC already trusts the root certificate of its Collaboration partner.
   See sections Checking the status of a root certificate on the HMI device (Page 544) and Automatic trust relationship between Collaboration devices (Page 431).
2. If the PC does not yet trust the root certificate, install it manually.
   See section Managing third-party certificates of a Unified PC (Page 499).

See also

Workflow (Collaboration for PCs) (Page 428)

6.5.1.6 Automatic trust relationship between Collaboration devices

This section describes cases in which a Collaboration device automatically trusts the certificate of its Collaboration partner. You do not have to establish the trust relationship manually.

Same certificate authority

Requirement:

- The Collaboration certificates of both devices have the same certificate authority. That is, the certificates have the same root certificate.
- The own Collaboration certificate has been installed on each device
  During installation of this certificate, the root certificate is also automatically installed on the device. It is installed in the folder containing the trusted certificate authorities.

Result:

The first time the connection is established for Collaboration, the devices check the Collaboration certificate of their Collaboration partner. Since they already trust the root certificate, the Collaboration certificate is automatically installed in the folder with the trusted certificates.

Trusted certificate authority

Requirement:

- The Collaboration certificates of the Collaboration devices have different certificate authorities. That is, the certificates have different root certificates.
- One Collaboration device has a communication partner whose application certificate was issued by the same certificate authority as the Collaboration certificate of its Collaboration partner. The device already trusts the certificate authority of this communication partner.

Result:

- The first time the connection is established for Collaboration, the device checks the Collaboration certificate of the Collaboration partner.
- Since the device already trusts the root certificate of the other communication partner, it automatically installs the Collaboration certificate in the folder with the trusted certificates.

Note

For successful Collaboration communication, the devices must trust each other. Check on the other Collaboration device to determine if it also already trusts the root certificate. See section Checking the status of a root certificate on the HMI device (Page 544).

Establish the trust relationship there manually, if necessary.

Example**:**

A Panel communicates with a second Panel using Unified Collaboration. The Collaboration application certificates of the Panels have different certificate authorities. Both Panels already trust the root certificates of their Collaboration partner.

For the first Panel, a Unified PC is configured as an additional Collaboration partner. The Collaboration application certificate of the PC has the same certificate authority and, thus, the same root certificate as the second Panel.

Since the first Panel already trusts the root certificate of the second Panel, it automatically also trusts the Collaboration application certificate of the PC.

See also

Establishing the trust relationship (Collaboration for PCs) (Page 431)

6.5.2 Web server certificates (PC)

6.5.2.1 Introduction

Basics of web server communication

WinCC Unified protects the communication between a Runtime web server and its web clients through the use of a web server certificate. The clients must trust the web server certificate (one-way SSL authentication).

The web server certificate can be issued by a certificate authority (CA-based certificate) or be self-signed.

Note

For security reasons, it is recommended to use a CA-based certificate. You use the WinCC Unified Certificate Manager application to create the certificate.

You create a self-signed web server certificate during installation of Runtime or later with the "WinCC Unified Configuration Manager" application.

You can find help on choosing a certificate type in section Selecting a suitable certificate type (Page 493).

The procedure for creating the web server certificate, installing it on the web server device and establishing the trust relationship with the web server on the clients depends on whether you are using CA-based or self-signed certificates.

See also

Workflow with a CA-based certificate (PC as web server) (Page 433)

Workflow with a self-signed certificate (PC as web server) (Page 458)

Unified certificate authority (Page 505)

6.5.2.2 Using a CA-based certificate (PC as web server)

Workflow with a CA-based certificate (PC as web server)

Note

Unified PCs always need a web server certificate.

If you are using a Unified PC as a Runtime web server and want to use a CA-based web server certificate, you need the following certificates:

- Web server certificate of the PC
- Root certificate of the certificate authority that issued the web server certificate, along with its CRL file.

Procedure

1. Create the web server certificate of the PC.
   See section Creating certificates (PC as web server) (Page 434).
2. Install the certificate on the PC.
   See section Installing certificates (PC as web server) (Page 435).
   This binds the web server certificate to the Runtime web page of the PC.
3. Establish the trust relationship with the web server on the web clients.
   See section Establishing the trust relationship with the web server (Page 436).

See also

Introduction (Page 432)

Creating certificates (PC as web server)

Introduction

You create the CA-based web server certificate of a Unified PC on the certificate authority device. You use the WinCC Unified Certificate Manager application for this.

The certificate authority device is always a Unified PC.

Procedure

If you do not have a certificate authority yet, follow these steps:

1. Create the certificate authority.
   In so doing, you create the root certificate of the certificate authority and its CRL file automatically.
   See section Creating a certificate authority and root certificate (Page 519).
2. Add the web server PC to the certificate authority.
   See section Adding devices (Page 521).
3. Add the web server certificate to the PC.
   See section Add application certificates (Page 524).

If you already have a certificate authority, follow these steps:

1. If the PC has not yet been added to the infrastructure of the certificate authority, add the web server PC.
   See section Adding devices (Page 521).
2. Add the web server certificate to the PC.
   See section Add application certificates (Page 524).

See also

Workflow with a CA-based certificate (PC as web server) (Page 433)

Installing certificates (PC as web server)

Introduction

The web server certificate of a Unified PC is installed in the following steps:

- Export on the certificate authority device
- Import to the PC
- Installation on the PC

Note

You always export and import all certificates of the PC as well as the root certificate of the issuing certificate authority and its CRL file.

Requirement

- The web server certificate has been added for the PC on the certificate authority device.

Procedure

1. Export the certificates of the PC on the certificate authority device. Use the WinCC Unified Certificate Manager for this.
   See section Exporting certificates of a Unified PC (Page 528).
2. Import the certificates to the PC. Use the Certificate Manager for this.
   See section Importing certificates of a Unified PC (Page 538).
3. Install all certificates together on the PC or only the web server certificate. Use the Certificate Manager for this.
   See section Installing all certificates or single certificates of a PC (Page 539).

Note

The installation binds the web server certificate to the Runtime web page. It replaces the web server certificate selected during Runtime installation or later in the "Website settings" step in the WinCC Unified Configuration tool.

The web page is then restarted to enforce the use of the new certificate. Any connected web clients are thereby disconnected and must log in again.

See also

Workflow with a CA-based certificate (PC as web server) (Page 433)

Add application certificates (Page 524)

Establishing the trust relationship with the web server

Introduction

Secure communication between a Unified Runtime web server and its web clients requires that the clients trust the web server certificate.

That is automatically the case when a client trusts the root certificate of the certificate authority that issued the web server certificate.

Timing

You can establish the trust relationship on a planned or as needed basis:

- Planned: You install the root certificate before the client attempts to connect to the web server for the first time.
  The client then already trusts the web server certificate the first time a connection is established.
- As needed: You install the root certificate when the client first attempts to connect to the web server.
  If the root certificate of the web server has not yet been installed at that time, you can download it on the Unified home page and then install it in the client.

Installing the root certificate before a connection is established for the first time

1. If applicable, check whether the client already trusts the root certificate of the web server.
   See sections Checking the status of the web server root certificate on the web client. (Page 437) and Automatic trust relationship with a PC web server (Page 438).
2. If the client already trusts the root certificate, you don't have to do anything.
   If the client does not trust the root certificate, install it manually in the certificate store of the browser.

Utilized browser	Certificate store used by the browser	For procedure, see section
Edge and Chrome on Windows	Windows system certificate store	Installing the root certificate before the first connection (Edge and Chrome) (Page 439)
Firefox on Windows	Certificate store of Firefox	Installing the root certificate before the first connection (for Firefox) (Page 445)
Web browser of a Unified Panel	Certificate store of the Panel	Installing the root certificate before the first connection (Panel web browser) (Page 456)
Browser on iOS devices	System certificate store of the iOS device	Installing the root certificate on iOS devices before the first connection (Page 449)

Installing the root certificate at the first connection attempt

Follow the steps below according to the browser:

Browser	Certificate store used by the browser	For procedure, see section
Edge and Chrome on Windows	Windows system certificate store	Installing the root certificate at the first connection (Edge and Chrome) (Page 442)
Firefox on Windows	Certificate store of Firefox	Installing the root certificate at the first connection (for Firefox) (Page 447)
Web browser of a Unified Panel	Certificate store of the Panel	Installing the root certificate at the first connection (Panel web browser) (Page 457)
Browser on iOS devices	System certificate store of the iOS device	Installing the root certificate on iOS devices at the first connection (Page 451)

See also

Workflow with a CA-based certificate (PC as web server) (Page 433)

Checking the status of the web server root certificate on the web client.

Introduction

This section describes how to check whether a web client already trusts the root certificate of a Runtime web server.

In that case, the root certificate has been installed in the certificate store of the web client in the folder containing the trusted certificate authorities.

Procedure for Microsoft Edge and Chrome as web client

Microsoft Edge and Chrome use the Windows system certificate store.

Use Windows > Search "Manage computer certificates" to check whether the root certificate has been installed under "Certificates - Local Computer" > "Trusted Root Certification Authorities" > "Certificates".

Procedure for Firefox

Firefox uses its own dedicated certificate store.

To check the status of a certificate, follow these steps:

1. Open the "Settings" page of Firefox.
2. Select "Privacy & Security".
3. Click "View Certificates" in the "Certificates" area.

4. Select the "Authorities" tab in the "Certificate Manager" window.
5. Check whether the root certificate is included in the list of trusted authorities.

Procedure for iOS devices

Follow the procedure described in the user help of the manufacturer.

Procedure for "Web browser" of a Unified Panel

"Web browser" of the Unified Panel uses the certificate store of the Panel.

To check whether the Panel already trusts the root certificate, follow the procedure described in section Checking the status of a root certificate on the HMI device (Page 544).

See also

Establishing the trust relationship with the web server (Page 436)

Automatic trust relationship with a PC web server

This section describes cases in which a web client automatically trusts the CA-based certificate of a Unified PC Runtime web server. You do not have to establish the trust relationship manually.

Edge or Chrome as local web client

Requirement:

- You use Microsoft Edge or Chrome as web client.
- Web server and client are installed on the same Unified PC.

Result:

- During installation of the certificates of the Unified PC, WinCC Unified Certificate Manager also installs the web server root certificate in the system certificate store of Windows. Microsoft Edge and Chrome use this certificate store.
- Since the clients already trust the root certificate, the web server certificate is automatically installed in the folder with the trusted certificates when a connection is established for the first time.
- The connection between the client and web server is secure from the outset.

Edge or Chrome as remote web client and same certificate authority

Requirement

- You use Microsoft Edge or Chrome as web client.
- The clients have been installed on a Unified PC.
- The web server certificate of the web server PC and at least one application certificate of the client PC were issued by the same certificate authority. That is, they have the same root certificate.

Result:

- During installation of the certificates of the Unified PC, Certificate Manager also installs the root certificate in the system certificate store of Windows. Microsoft Edge and Chrome use this certificate store.
- Since the clients already trust the root certificate, the web server certificate is automatically installed in the folder with the trusted certificates when a connection is established for the first time.
- The connection between the client and web server is secure from the outset.

Communicating with multiple web servers of the same certificate authority

Requirement:

- The web server certificates of two Unified Runtime web servers were issued by the same certificate authority. That is, they have the same root certificate.
- The web client already trusts the root certificate of one of the web servers.
  The manner in which the trust relationship was established is irrelevant.
- The client connects to the second web server.

Result:

- The client already trusts the root certificate at the first connection attempt. For this reason, the web server certificate of the second web server is automatically installed in the folder with the trusted certificates when the connection is established.
- The connection between the client and web server is secure from the outset.

See also

Establishing the trust relationship with the web server (Page 436)

Installing the root certificate for Edge and Chrome

Installing the root certificate before the first connection (Edge and Chrome)

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) on an Edge or Chrome web client before the client connects to the web server for the first time. The description applies to clients installed on Windows devices.

The procedure is explained using Edge as an example. The procedure is the same for Chrome.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager.
  See section Creating a certificate authority and root certificate (Page 519).
- The web server root certificate has been exported on the certificate authority device with Certificate Manager to a storage location the web client can access.
  See section Exporting root certificate and CRL file (Page 531).

Note

Alternative

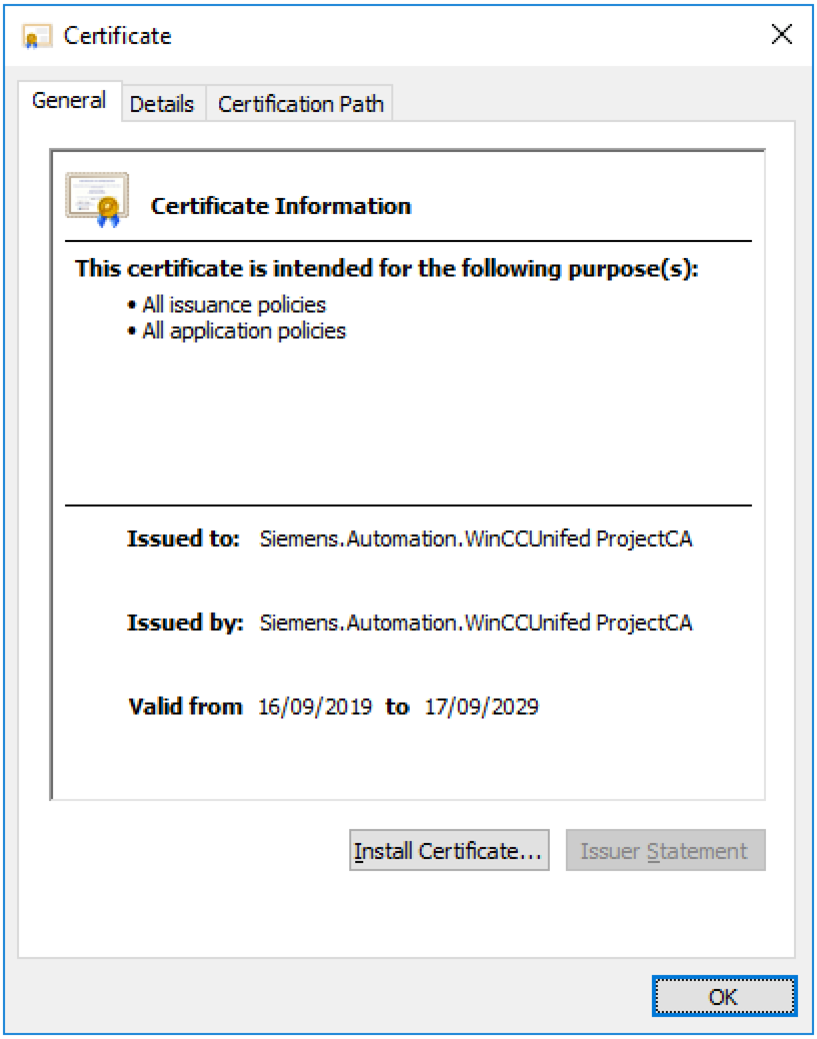
If a Unified PC belongs to the infrastructure of the certificate authority of the web server whose certificates were already installed with Certificate Manager, you can export the root certificate on the PC with SIMATIC Runtime Manager.

See section Managing third-party certificates of a Unified PC (Page 499).

- Microsoft Edge or Chrome has been installed on the web client device.

Procedure

1. Double-click the root certificate file on the web client device.
   The root certificate is opened with the Windows standard form.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: Siemens.Automation.WinCCUnifed ProjectCA

Issued by: Siemens.Automation.WinCCUnifed ProjectCA

Valid from 16/09/2019 **to** 17/09/2029

2. Click "Install Certificate".
3. In the certificate import wizard, select "Local Machine" as the storage location and "Trusted Root Certification Authority" as the certificate store.
4. Start the import.
5. (optional) Check whether the root certificate was successfully installed in the Windows system certificate store.
   See section Checking the status of the web server root certificate on the web client. (Page 437).

Result

At the first call of the web server web page, the browser trusts the root certificate of the web server and, thus, it automatically also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Workflow with a CA-based certificate (PC as web server) (Page 433)

Installing the root certificate at the first connection (Edge and Chrome)

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) at the first connection attempt of an Edge or Chrome web client. The description applies to clients installed on Windows devices.

The procedure is explained using Edge as an example. The procedure is the same for Chrome.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager. It has been installed on the web server.
- A Runtime project is running on the web server.
- Microsoft Edge or Chrome has been installed on the web client device.
- The web server root certificate has not yet been installed in the Windows system certificate store of the client device.
- The client device has access to the web server.

Procedure

1. Start Microsoft Edge on the web client device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

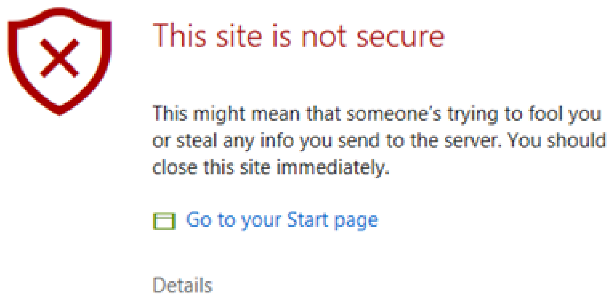
   Note

   URL of a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

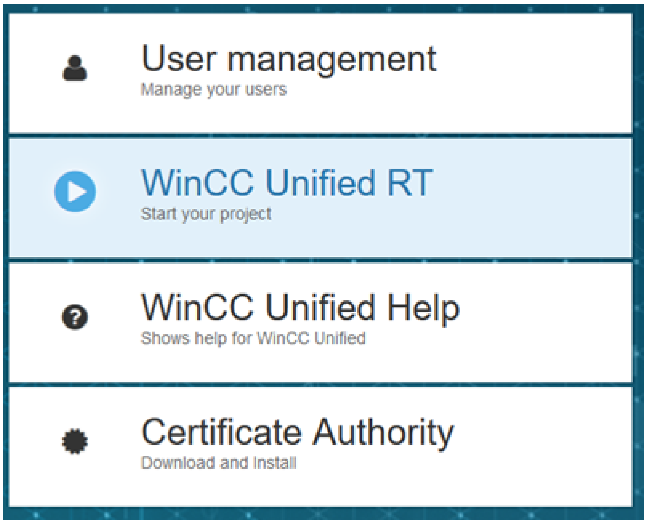
   An error message is displayed:

   This site is not secure

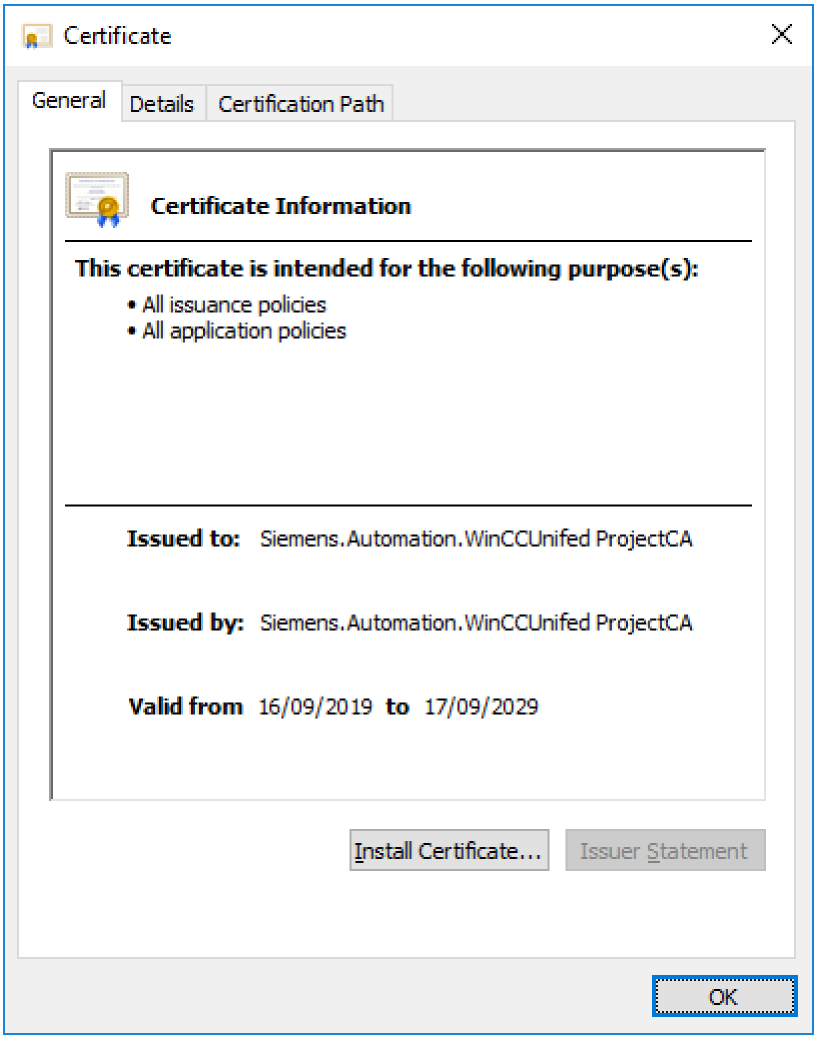
   This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

3. Open the field with the error details and confirm that you want to open the web page. The WinCC Unified home page is loaded.
4. On the home page, select the "Certificate Authority" field and confirm "Open file" in the download dialog.

   The root certificate is downloaded to the default download directory.

5. Double-click the downloaded file.
   The root certificate is opened with the Windows standard form.



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: Siemens.Automation.WinCCUnifed ProjectCA

Issued by: Siemens.Automation.WinCCUnifed ProjectCA

Valid from 16/09/2019 **to** 17/09/2029

6. Click "Install Certificate".
7. In the certificate import wizard, select "Local Machine" as the storage location and "Trusted Root Certification Authority" as the certificate store.
8. Start the import.
9. (optional) Check whether the root certificate was successfully installed in the Windows system certificate store.
   See section Checking the status of the web server root certificate on the web client. (Page 437).
10. Reload the page.

Result

The browser trusts the root certificate of the web server and, thus, it also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Workflow with a CA-based certificate (PC as web server) (Page 433)

Installing the root certificate for Firefox

Installing the root certificate before the first connection (for Firefox)

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) on a Firefox web client before the client connects to the web server for the first time. The description applies to clients installed on Windows devices.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager.
  See also section Creating a certificate authority and root certificate (Page 519).
- The web server root certificate has been exported on the certificate authority device with Certificate Manager to a storage location the web client can access.
  See section Exporting root certificate and CRL file (Page 531).

Note

Alternative

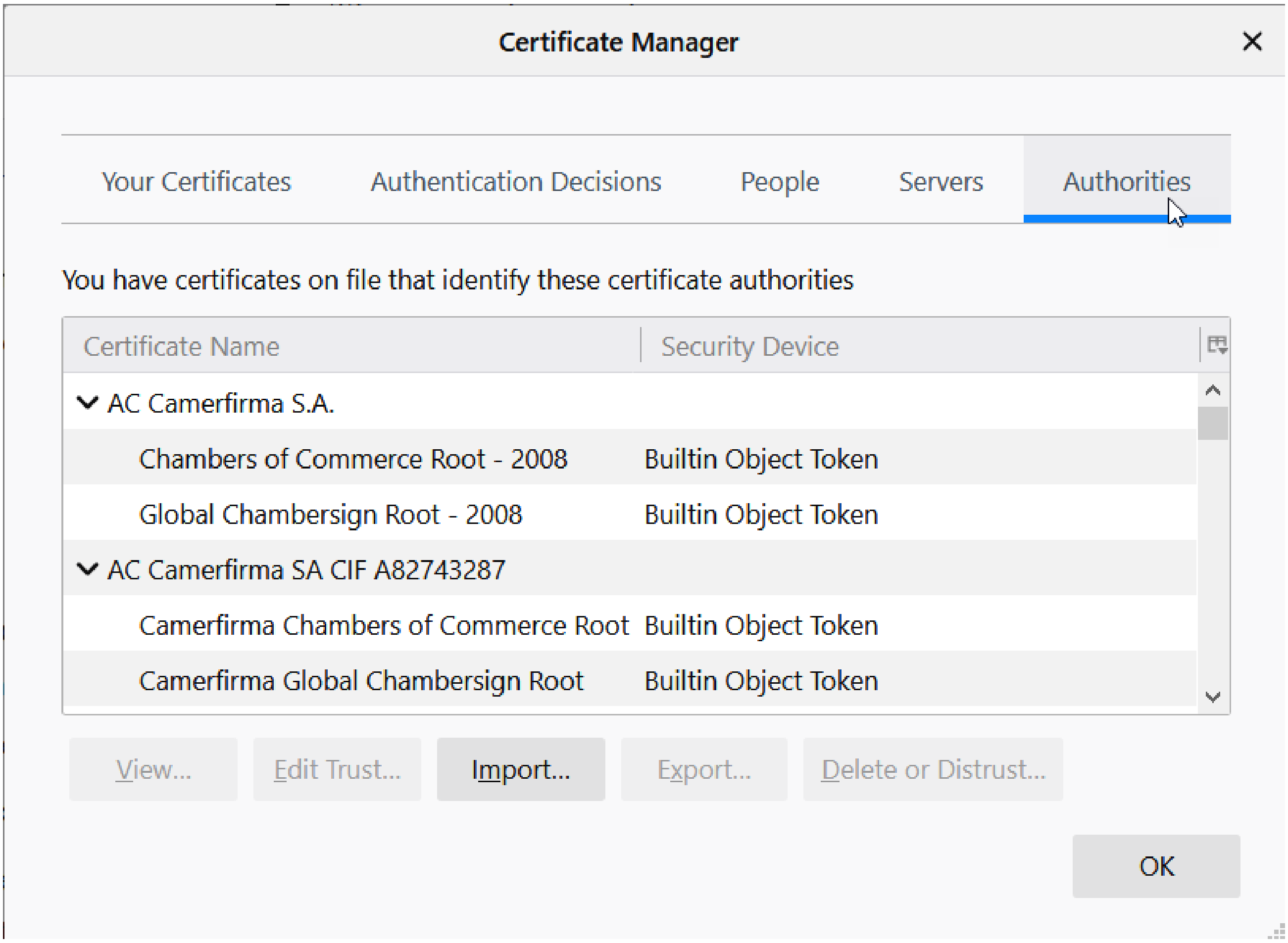
If a Unified PC belongs to the infrastructure of the certificate authority of the web server whose certificates were already installed with Certificate Manager, you can export the root certificate on the PC with SIMATIC Runtime Manager.

See section Managing third-party certificates of a Unified PC (Page 499).

- Firefox has been installed on the web client device.

Procedure

1. Start Firefox on the web client device.
2. Install the root certificate in the certificate store of Firefox. To do this, follow these steps:
   - Open the "Settings" page of Firefox.
   - Select "Privacy & Security".
   - Click "View Certificates" in the "Certificates" area.
   - Select the "Authorities" tab in the "Certificate Manager" window:



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

   - Click "Import" and select the root certificate file.
   - In the window that opens, select the option "This certificate can identify websites" and confirm your selection.

Result

At the first call of the web server web page, the browser trusts the root certificate of the web server and, thus, it automatically also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Checking the status of the web server root certificate on the web client. (Page 437)

Workflow with a CA-based certificate (PC as web server) (Page 433)

Establishing the trust relationship with the web server (Page 436)

Installing the root certificate at the first connection (for Firefox)

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) on a Firefox web client when the client first attempts to connect to the web server. The description applies to clients installed on Windows devices.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager. It has been installed on the web server.
- A Runtime project is running on the web server.
- Firefox has been installed on the web client device.
- The web server root certificate has not yet been installed in the certificate store of the browser.
- The client device has access to the web server.

Procedure

1. Start Firefox on the web client device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

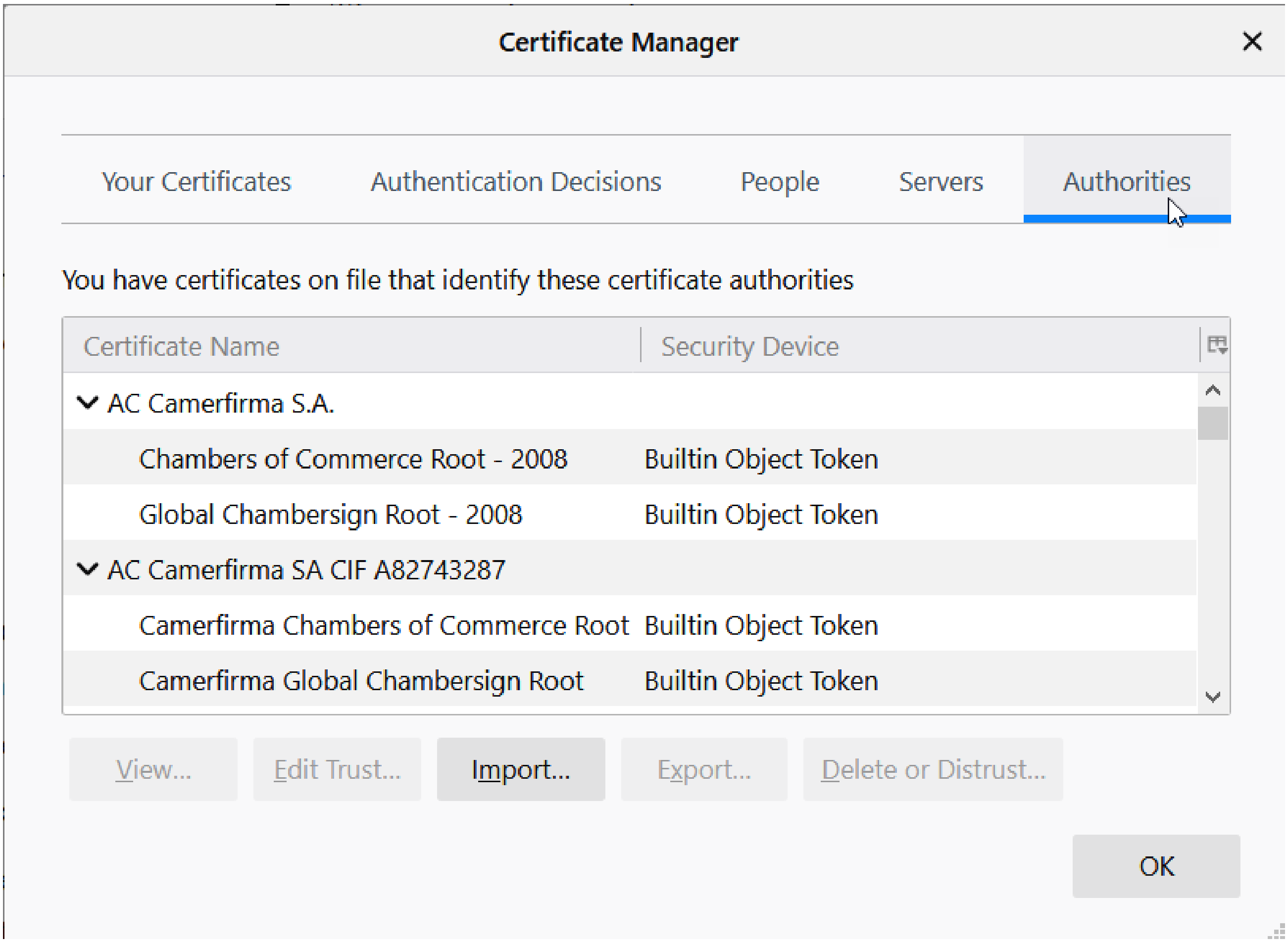
   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   An error message is displayed.
3. Open the "Advanced" field and confirm the "Accept the Risk and Continue" field.
4. An exception is entered for this page in the Firefox Certificate Manager.
5. On the WinCC Unified home page, select the "Certificate Authority" field.
6. Save the root certificate. To do this, click "Save file" in the Firefox dialog that follows.

7. Install the root certificate in the certificate store of Firefox. To do this, follow these steps:
   - Open the "Settings" page of Firefox.
   - Select "Privacy & Security".
   - Click "View Certificates" in the "Certificates" area.
   - Select the "Authorities" tab in the "Certificate Manager" window:



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

   - Click "Import" and select the root certificate file.
   - In the window that opens, select the option "This certificate can identify websites" and confirm your selection.
   - Click "Servers" and remove the exception that was created by step 2.
8. Reload the page.

Result

The browser trusts the root certificate of the web server and, thus, it also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Checking the status of the web server root certificate on the web client. (Page 437)

Workflow with a CA-based certificate (PC as web server) (Page 433)

Establishing the trust relationship with the web server (Page 436)

Creating a certificate authority and root certificate (Page 519)

Installing the root certificate on iOS devices

Installing the root certificate on iOS devices before the first connection

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) on an iOS web client before the client connects to the web server for the first time.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager.
- The web server root certificate has been exported on the certificate authority device with Certificate Manager to a storage location.
  See section Exporting root certificate and CRL file (Page 531).

Note

Alternative

If a Unified PC belongs to the infrastructure of the certificate authority of the web server whose certificates were already installed with Certificate Manager, you can export the root certificate on the PC with SIMATIC Runtime Manager.

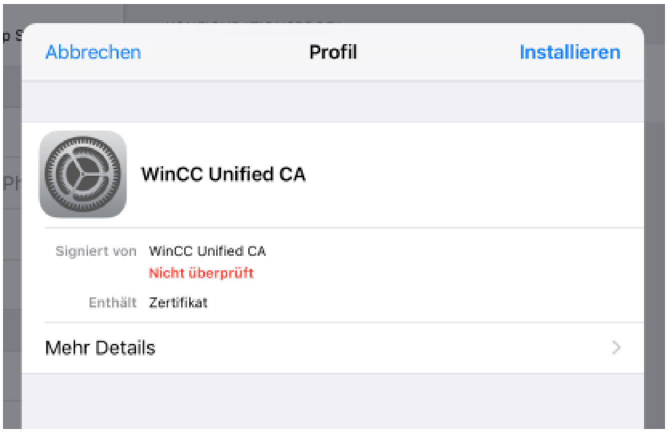
See section Managing third-party certificates of a Unified PC (Page 499).

- The web client device has access to the root certificate file, for example, because the file was sent to the device via email.
- The desired browser has been installed on the web client device.

Procedure

1. Tap the root certificate file on the iOS device.
   You are informed that the website is trying to load a configuration profile.
2. Tap "Allow"
   The configuration profile is loaded.
3. Tap "Close".
4. Select "Settings > General > Profile" on the device.
5. Tap the configuration profile you just loaded.

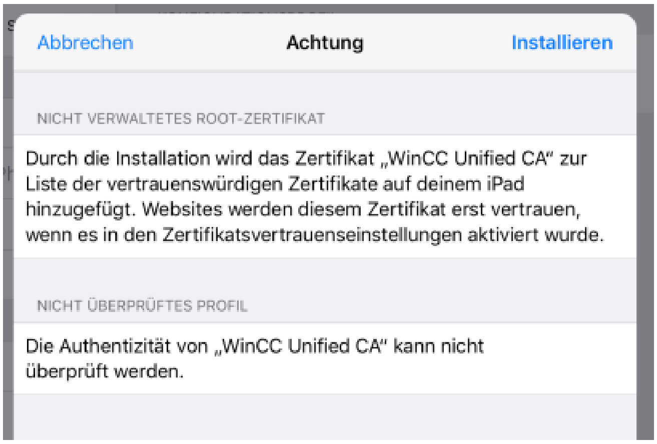
6. Tap "Install" at the top right.



WinCC Unified CA

Signiert von WinCC Unified CA
Nicht überprüft
Enthält Zertifikat

7. Tap "Install" again at the top right.



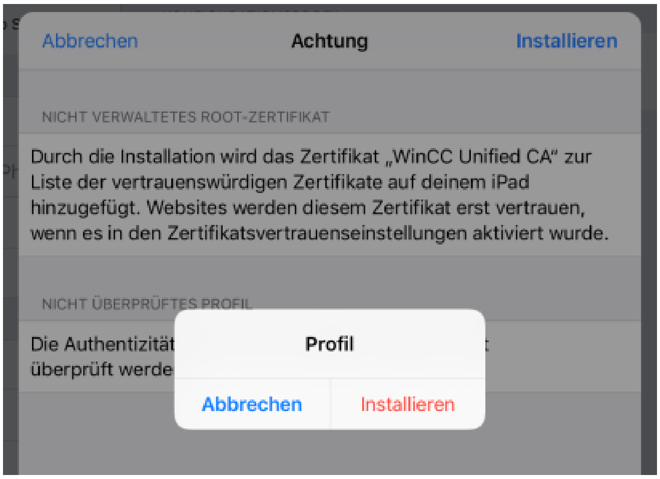
NICHT VERWALTETES ROOT-ZERTIFIKAT

Durch die Installation wird das Zertifikat „WinCC Unified CA“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

NICHT ÜBERPRÜFTES PROFIL

Die Authentizität von „WinCC Unified CA“ kann nicht überprüft werden.

8. Tap "Install" again in the "Profile" confirmation prompt:



NICHT VERWALTETES ROOT-ZERTIFIKAT

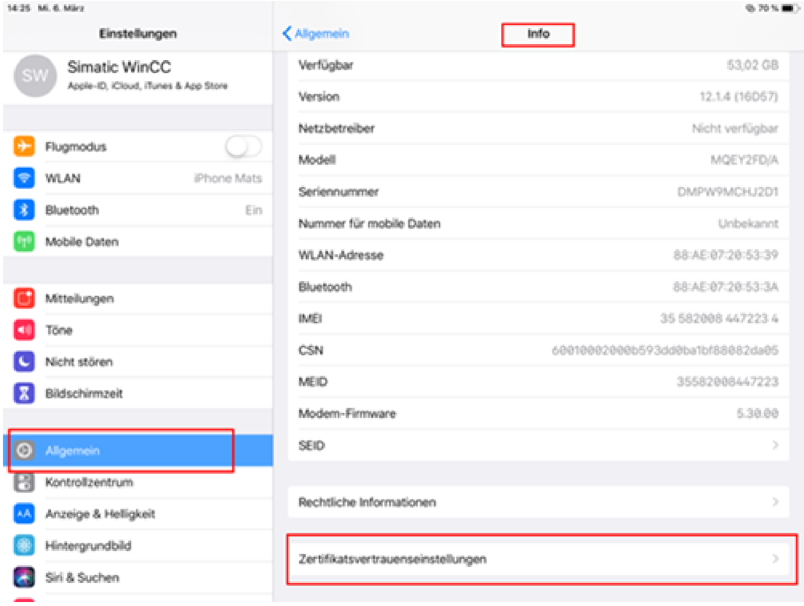
Durch die Installation wird das Zertifikat „WinCC Unified CA“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

NICHT ÜBERPRÜFTES PROFIL

Die Authentizität
überprüft werde

The certificate is installed.

9. Select "Settings > General > About > Certificate Trust Settings" on the device:



Verfügbar	53,02 GB
Version	12.1.4 (16D57)
Netzbetreiber	Nicht verfügbar
Modell	MQEY2FD/A
Seriennummer	DMPW9MCHJ2D1
Nummer für mobile Daten	Unbekannt
WLAN-Adresse	88:AE:07:20:53:39
Bluetooth	88:AE:07:20:53:3A
IMEI	35 582008 447223 4
CSN	60010002000b593dd0ba1bf88082da05
MEID	35582008447223
Modem-Firmware	5.30.00
SEID	>
Rechtliche Informationen	>
Zertifikatsvertrauenseinstellungen	>

10. Select the "Enable full trust for root certificates" option for the web server root certificate.

Result

At the first call of the web server web page, the browser trusts the root certificate of the web server and, thus, it automatically also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Workflow with a CA-based certificate (PC as web server) (Page 433)

Establishing the trust relationship with the web server (Page 436)

Creating a certificate authority and root certificate (Page 519)

Installing the root certificate on iOS devices at the first connection

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) on an iOS web client when the client first attempts to connect to the web server.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager. It has been installed on the web server.
- A Runtime project is running on the web server.

- The desired browser has been installed on the web client device.
- The web server root certificate has not yet been installed in the certificate store of the browser.
- The client device has access to the web server.

Procedure

1. Start the browser on the web client device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

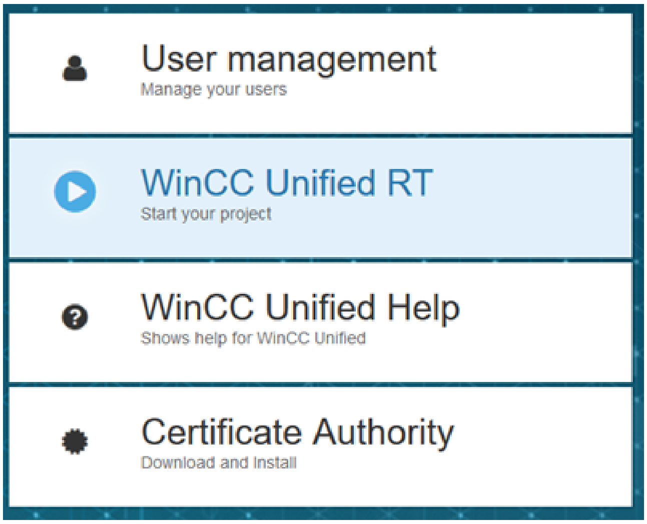
   Note

   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   A warning message is displayed.
3. Open the details for the message and select the button for loading the page.
   The WinCC Unified home page is loaded.
4. Load the root certificate to your device. Follow these steps:
   – On the home page, select the "Certificate Authority" field.



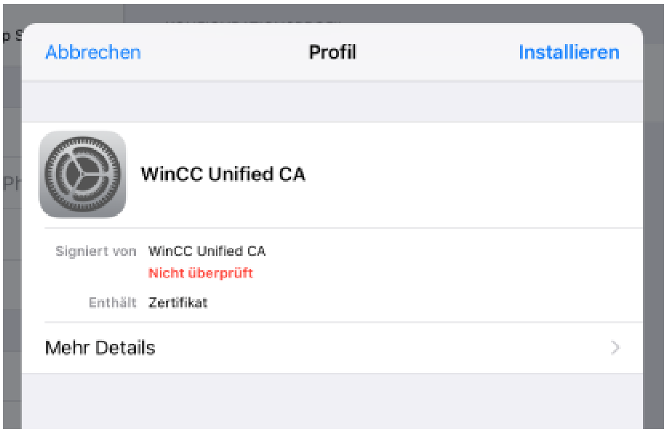
User management
Manage your users
WinCC Unified RT
Start your project
WinCC Unified Help
Shows help for WinCC Unified
Certificate Authority
Download and Install

   A pop-up opens. It informs you that the website is trying to load a configuration profile.

   – Tap "Allow"
   The configuration profile is loaded.

   – Tap "Close".

5. Install the configuration profile on your device. Follow these steps:
   - Select "Settings > General > Profile" on the device.
   - Tap the configuration profile you just loaded.
   - Tap "Install" at the top right.

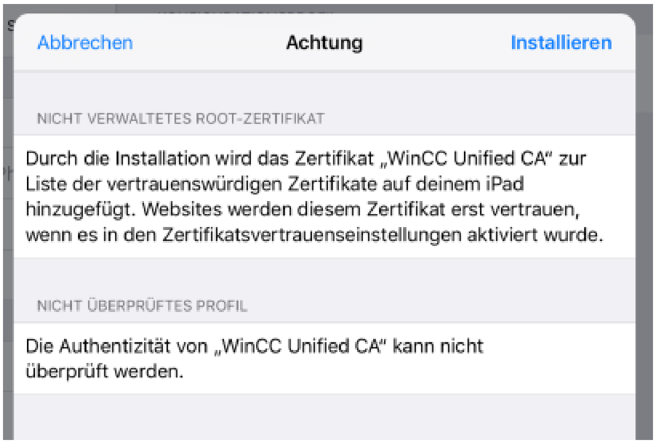


WinCC Unified CA

Signiert von WinCC Unified CA
Nicht überprüft

Enthält Zertifikat

   - Tap "Install" again at the top right.



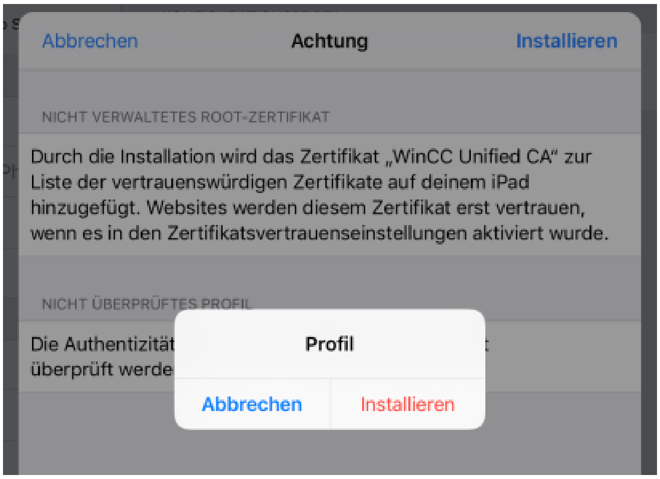
NICHT VERWALTETES ROOT-ZERTIFIKAT

Durch die Installation wird das Zertifikat „WinCC Unified CA“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

NICHT ÜBERPRÜFTES PROFIL

Die Authentizität von „WinCC Unified CA“ kann nicht überprüft werden.

– Tap "Install" again in the "Profile" confirmation prompt:



Abbrechen Achtung Installieren

NICHT VERWALTETES ROOT-ZERTIFIKAT

Durch die Installation wird das Zertifikat „WinCC Unified CA“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

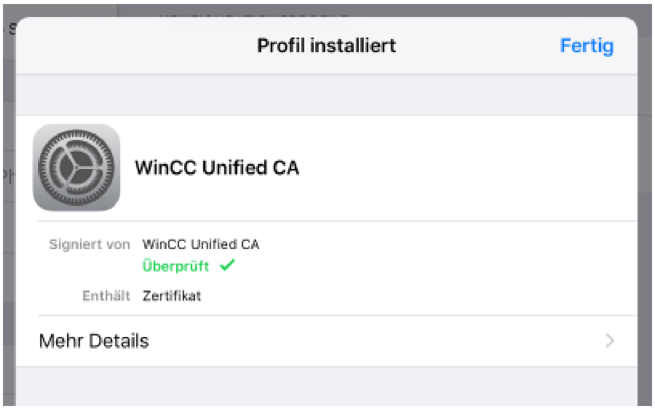
NICHT ÜBERPRÜFTES PROFIL

Die Authentizität
überprüft werde

Profil

Abbrechen Installieren

The root certificate is installed.
You see the entry "Verified".



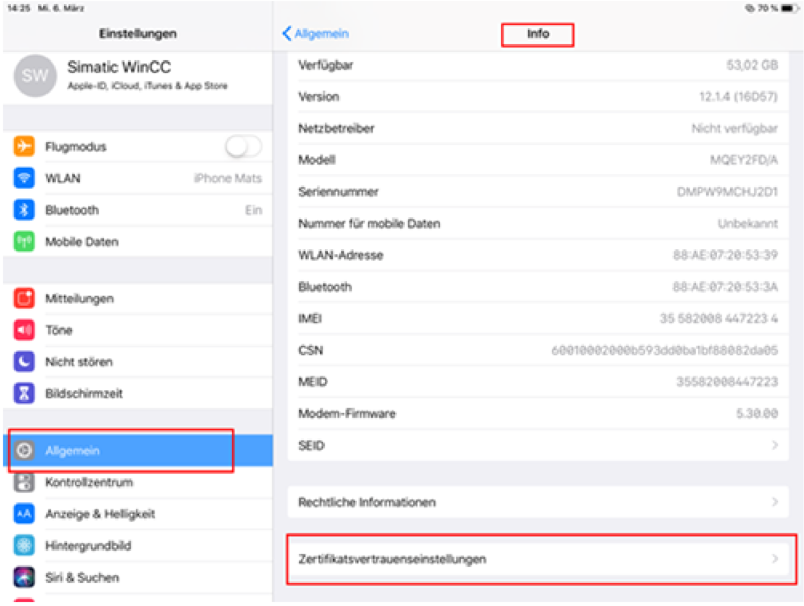
Profil installiert Fertig

WinCC Unified CA

Signiert von WinCC Unified CA
Überprüft ✓
Enthält Zertifikat

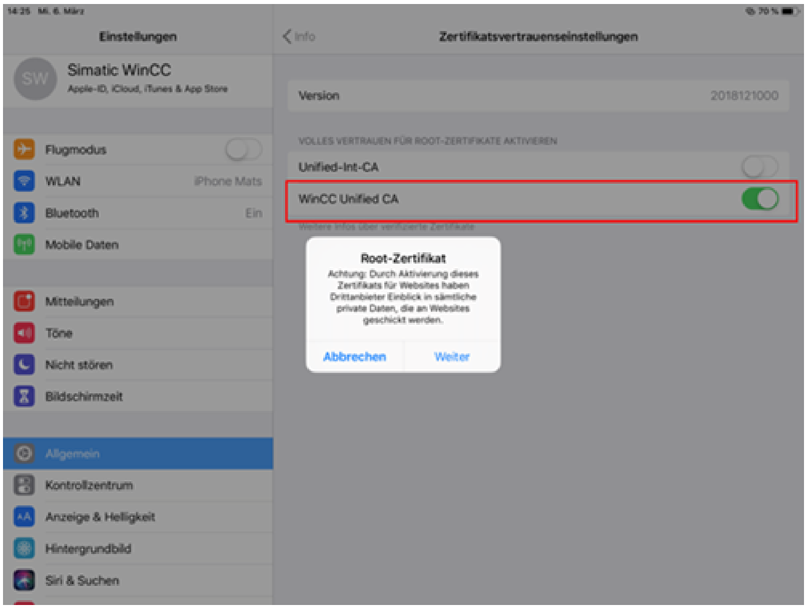
Mehr Details

- Select "General > About > Certificate Trust Settings".



Verfügbar	53,02 GB
Version	12.1.4 (16D57)
Netzbetreiber	Nicht verfügbar
Modell	MQEY2FD/A
Seriennummer	DMPW9MCHJ2D1
Nummer für mobile Daten	Unbekannt
WLAN-Adresse	88:AE:07:20:53:39
Bluetooth	88:AE:07:20:53:3A
IMEI	35 582008 447223 4
CSN	60010002000b593dd0ba1bf88082da05
MEID	35582008447223
Modem-Firmware	5.30.00

- Select "WinCC Unified CA" and select "Next".



Version 2018121000

VOLLES VERTRAUEN FÜR ROOT-ZERTIFIKATE AKTIVIEREN

Unified-Int-CA ○

WinCC Unified CA ●

Root-Zertifikat

Achtung: Durch Aktivierung dieses Zertifikats für Websites haben Drittanbieter Einblick in sämtliche private Daten, die an Websites geschickt werden.

6. Load the Unified home page again.

Result

The browser trusts the root certificate of the web server and, thus, it also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Establishing the trust relationship with the web server (Page 436)

Workflow with a CA-based certificate (PC as web server) (Page 433)

Creating a certificate authority and root certificate (Page 519)

Installing the root certificate for a UCP web browser

Installing the root certificate before the first connection (Panel web browser)

Introduction

This section describes how to install the root certificate of a Runtime web server in the web browser of a Unified Panel before the browser connects to the web server for the first time.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager.
- The web server root certificate has been exported on the certificate authority device with Certificate Manager to a storage location the web client can access.
  See section Exporting root certificate and CRL file (Page 531).

Note

Alternative

If a Unified PC belongs to the infrastructure of the certificate authority of the web server whose certificates were already installed with Certificate Manager, you can export the root certificate on the PC with SIMATIC Runtime Manager.

See section Managing third-party certificates of a Unified PC (Page 499).

Procedure

Web browser uses the certificate store of the Panel. To install the root certificate there, follow the procedure described in section Importing and installing root certificates and CRL files on Panels (Page 545).

Result

At the first call of the web server web page, the browser trusts the root certificate of the web server and, thus, it automatically also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Workflow with a CA-based certificate (PC as web server) (Page 433)

Checking the status of a root certificate on the HMI device (Page 544)

Establishing the trust relationship with the web server (Page 436)

Creating a certificate authority and root certificate (Page 519)

Installing the root certificate at the first connection (Panel web browser)

Introduction

This section describes how to install the root certificate of a Runtime web server (Unified PC or Unified Panel) in the web browser of a Unified Panel when the web browser first attempts to connect to the web server.

Requirement

- The web server certificate has been created with WinCC Unified Certificate Manager. It has been installed on the web server.
- A Runtime project is running on the web server.
- The web server root certificate has not yet been installed in the certificate store of the Panel.
- The Panel has access to the web server.

Procedure

1. Start the "Web browser" application on the Panel.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   An error message is displayed.
3. Open the field with the error details and confirm that you want to open the web page.
   The WinCC Unified home page is loaded.

4. On the home page, select the "Certificate Authority" field and confirm "Open file" in the download dialog.
   The root certificate is downloaded.
5. Web browser uses the certificate store of the Panel. Install the root certificate there. Follow the procedure described in section Importing and installing root certificates and CRL files on Panels (Page 545).

Result

Web browser trusts the root certificate of the web server and, thus, it also trusts the web server certificate.

You can log in to Runtime with a secure connection.

See also

Workflow with a CA-based certificate (PC as web server) (Page 433)

Checking the status of a root certificate on the HMI device (Page 544)

Establishing the trust relationship with the web server (Page 436)

Creating a certificate authority and root certificate (Page 519)

6.5.2.3 Using a self-signed certificate (PC as web server)

Workflow with a self-signed certificate (PC as web server)

A Unified PC that is used as a Runtime web server can use a self-signed web server certificate.

Note

Self-signed certificates provide less protection than CA-based certificates. Use them for testing, for example. It is recommended that they then be replaced with CA-based certificates.

Note

Unified PCs always need a web server certificate.

Limitations

- The self-signed web server certificate has a lifetime of 12 months.

Procedure

1. Create a new self-signed web server certificate and bind it to the Runtime web page. Or, select an existing self-signed certificate and bind it to the web page.
   See section Configuring a self-signed certificate (Page 459).
2. If a Runtime project is not yet running on the PC, start the desired project.
3. Establish the trust relationship with the web server on the web clients.
   See section Trusting the PC web server on the web client (Page 460).

See also

Introduction (Page 432)

Configuring a self-signed certificate

Tips for effective procedure

Typically, you create a self-signed web server certificate during Runtime installation. You use this certificate to test the configuration.

Afterwards, you replace it with a CA-based web server certificate.

Introduction

You create and install the self-signed web server certificate of the Unified PC during installation of Unified Runtime or at a later time.

During installation

1. In the "Website settings" step of the installation, select the "Create a new certificate" option.
2. (optional) Runtime uses the device name/FQDN of the PC by default for addressing the Runtime web page and the identity provider. To use the IP address instead, select the "Use IP address instead of computer name" option under "Addressing the website and the identity provider".
3. Configure the other steps if required.
4. Restart the system.

After installation

1. Start the "WinCC Unified Configuration Manager" application on the PC.
2. Navigate to the "Website settings" step.
3. (optional) Runtime uses the device name/FQDN of the PC by default for addressing the Runtime web page and the identity provider. To use the IP address instead, select the "Use IP address instead of computer name" option under "Addressing the website and the identity provider".

4. To create a new self-signed certificate, follow these steps:
   - Select the "Create a new certificate" option.
   - Enter a certificate name.
5. To use a previously created self-signed certificate, follow these steps:
   - Select the "Select an existing certificate" option.
   - Select the desired self-signed certificate from the list.

Note

Displayed certificates

You see all certificates whose device binding is consistent with the setting you selected for addressing the Runtime web page and identity provider.

Result

- "Create a new certificate" option selected:
  A new self-signed certificate is created, installed and bound to the web page.
- "Select an existing certificate" option selected:
  The selected self-signed certificate is installed and bound to the web page.

The Runtime web page and the identity provider are addressed according to your selection.

See also

Workflow with a self-signed certificate (PC as web server) (Page 458)

Trusting the PC web server on the web client

Installing the self-signed web server certificate for Edge and Chrome

Introduction

This section describes how to install the self-signed web server certificate of a Runtime web server (Unified PC or Unified Panel) on an Edge or Chrome web client on Windows.

The procedure is explained using Edge as an example. The procedure is the same for Chrome.

Requirement

- The Runtime web server uses a self-signed web server certificate.
- A Runtime project is running on the web server.
- Microsoft Edge or Chrome has been installed on the web client device.
- The client device has access to the web server.

Procedure

1. Start Microsoft Edge on the web client device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

   Access to a Unified PC web server

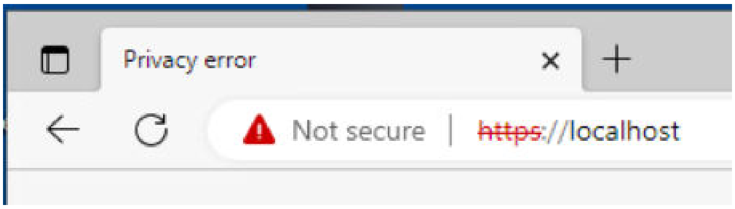
   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

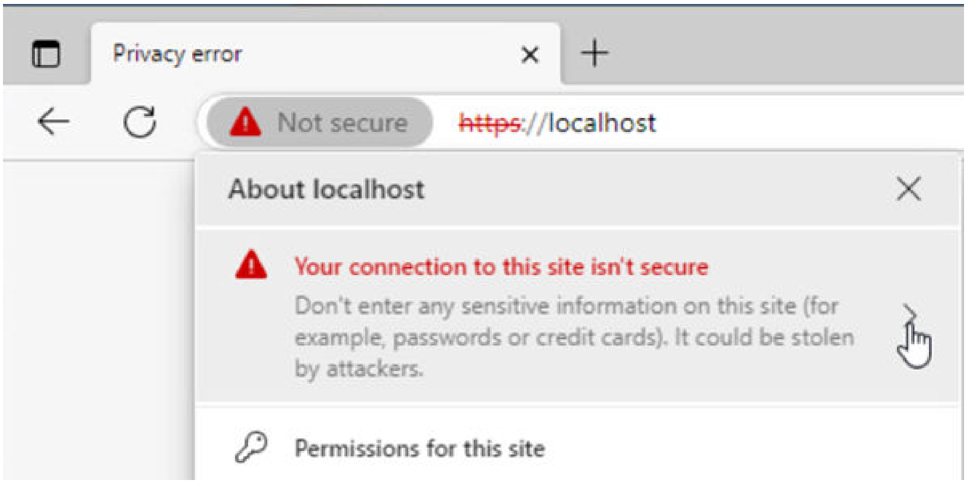
   Edge warns you that the connection is not secure.

3. Download the certificate. To do this, follow these steps:

   – Click the triangle with the exclamation point in the address bar:



   – Click the notice that the connection to the website is not secure:

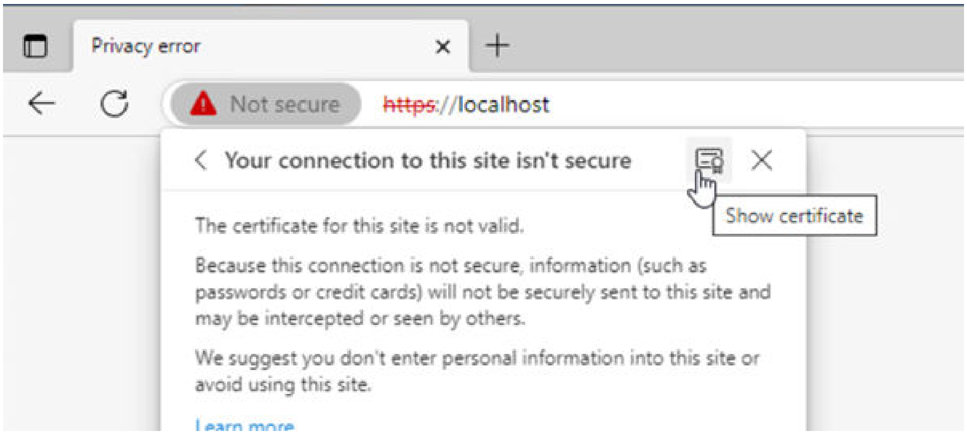


About localhost

Your connection to this site isn't secure

Don't enter any sensitive information on this site (for example, passwords or credit cards). It could be stolen by attackers.

   – Click the "Show certificate" icon:



Your connection to this site isn't secure

The certificate for this site is not valid.

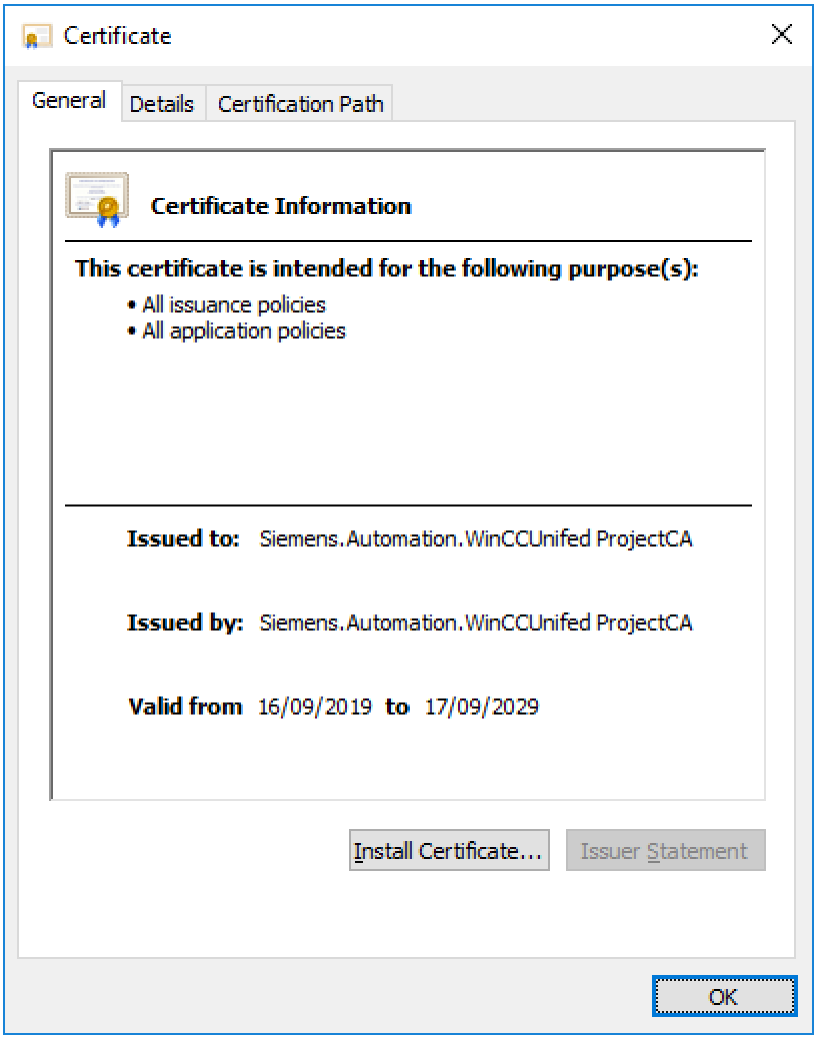
Because this connection is not secure, information (such as passwords or credit cards) will not be securely sent to this site and may be intercepted or seen by others.

We suggest you don't enter personal information into this site or avoid using this site.

   – Click "Export" in the "Details" tab.

   – Select a storage location and save the certificate.

4. Install the certificate in the certificate store of Windows. To do this, follow these steps:
   - Double-click the downloaded certificate file.
     The certificate is opened with the Windows standard form.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):
- All issuance policies
- All application policies

Issued to: Siemens.Automation.WinCCUnifed ProjectCA

Issued by: Siemens.Automation.WinCCUnifed ProjectCA

Valid from 16/09/2019 to 17/09/2029

   - Click "Install Certificate".
   - In the certificate import wizard, select "Local Machine" as the storage location and "Trusted Root Certification Authority" as the certificate store.
   - Start the import.
5. Reload the page.

Result

The browser trusts the self-signed web server certificate.

You can log in to Runtime with a secure connection.

See also

Configuring a self-signed certificate (Page 459)

Workflow with a self-signed certificate (PC as web server) (Page 458)

Checking the status of the web server root certificate on the web client. (Page 437)

Installing the self-signed web server certificate for Firefox

Introduction

This section describes how to install the self-signed web server certificate of a Runtime web server (Unified PC or Unified Panel) on a Firefox web client on Windows.

Requirement

- The Runtime web server uses a self-signed web server certificate.
- A Runtime project is running on the web server.
- Firefox has been installed on the web client device.
- The client device has access to the web server.

Procedure

1. Start Firefox on the web client device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   An error message is displayed.
3. Download the certificate. To do this, follow these steps:
   - Open the "Advanced" field.
   - Click "More Information".
     A dialog with the page information opens.
   - Click "Security > View Certificate".
     A tab with the certificate information opens.
   - Click "PEM (certificate)" under "Miscellaneous > Save".
   - Select a storage location and save the certificate.

4. Install the certificate in the certificate store of Firefox. To do this, follow these steps:
   - Open the "Settings" page of Firefox.
   - Select "Privacy & Security".
   - Click "View Certificates" in the "Certificates" area.
   - Click "Import" and select the certificate file.
5. Reload the page.

Result

The browser trusts the self-signed web server certificate.

You can log in to Runtime with a secure connection.

See also

Workflow with a self-signed certificate (PC as web server) (Page 458)

Checking the status of the web server root certificate on the web client. (Page 437)

Installing the self-signed web server certificate for an iOS device

Introduction

This section describes how to install the self-signed web server certificate of a Runtime web server (Unified PC or Unified Panel) on the web client of an iOS device.

The procedure is explained using Safari as an example. The procedure is the same for other browsers.

Requirement

- A self-signed web server certificate has been installed on the web server HMI device.
- A Runtime project is running on the web server.
- The client device is an iOS device.
- The device has access to the web server.
- Safari has been installed on the device.

Procedure

1. Start Safari on the HMI device.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

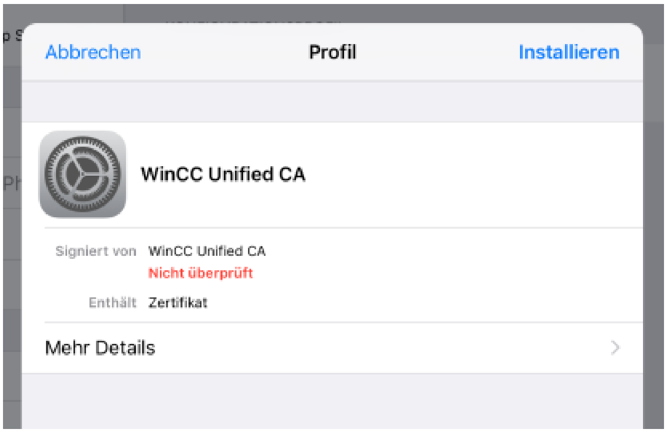
   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   An error message is displayed.
3. Load the self-signed web server certificate to your device. Follow these steps:
   - CHECK: How? / Click where?
     Is the self-signed certificate also considered a configuration profile?
     A pop-up opens. It informs you that the website is trying to load a configuration profile.
   - Tap "Allow".
     The configuration profile is loaded.
   - Tap "Close".

4. Install the configuration profile on your device. Follow these steps:
   - Select "Settings > General > Profile" on the device.
   - Tap the configuration profile you just loaded.
   - Tap "Install" at the top right.



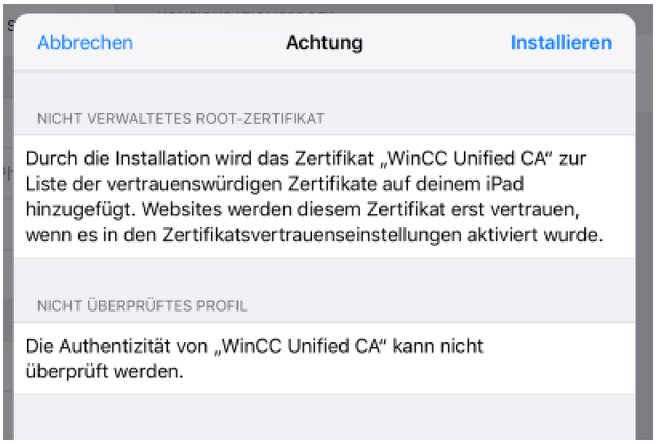
Abbrechen Profil Installieren

WinCC Unified CA

Signiert von WinCC Unified CA
Nicht überprüft
Enthält Zertifikat

Mehr Details

   - Tap "Install" again at the top right.



Abbrechen Achtung Installieren

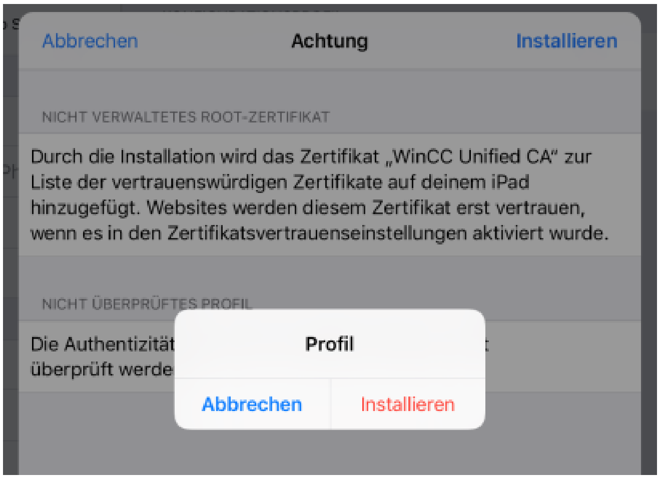
NICHT VERWALTETES ROOT-ZERTIFIKAT

Durch die Installation wird das Zertifikat „WinCC Unified CA" zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

NICHT ÜBERPRÜFTES PROFIL

Die Authentizität von „WinCC Unified CA" kann nicht überprüft werden.

– Tap "Install" again in the "Profile" confirmation prompt:



NICHT VERWALTETES ROOT-ZERTIFIKAT

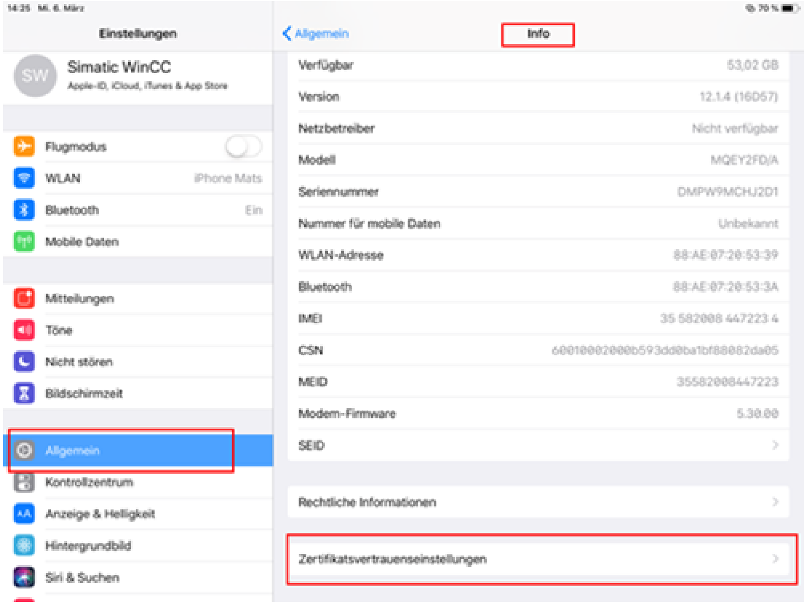
Durch die Installation wird das Zertifikat „WinCC Unified CA“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.

NICHT ÜBERPRÜFTES PROFIL

Die Authentizität … überprüft werde…

The certificate is installed.

– Select "Settings > General > About > Certificate Trust Settings" on the device:



Verfügbar	53,02 GB
Version	12.1.4 (16D57)
Netzbetreiber	Nicht verfügbar
Modell	MQEY2FD/A
Seriennummer	DMPW9MCHJ2D1
Nummer für mobile Daten	Unbekannt
WLAN-Adresse	88:AE:07:20:53:39
Bluetooth	88:AE:07:20:53:3A
IMEI	35 582008 447223 4
CSN	60010002000b593dd0ba1bf88082da05
MEID	35582008447223
Modem-Firmware	5.30.00
SEID	

– Select the "Full trust for root certificates" option for the certificate.

5. (optional) Check whether the web server certificate was successfully installed.
   Follow the same procedure as you use to check whether a web server root certificate has been installed on the web client.
6. Load the Unified home page again.

Result

The browser trusts the self-signed web server certificate.

You can log in to Runtime with a secure connection.

Alternative procedure

1. Export the self-signed web server certificate on the device of another web client that communicates with the same web server, e.g. with Edge.
2. Transfer the certificate to the iOS device, for example, by sending it as an email attachment and downloading the attachment to the iOS device.
   A pop-up opens. It informs you that the website is trying to load a configuration profile.
3. Tap "Allow".
   The configuration profile is loaded.
4. Tap "Close".
5. Continue as described above, starting from step 4.

See also

Workflow with a self-signed certificate (PC as web server) (Page 458)

Checking the status of the web server root certificate on the web client. (Page 437)

Installing the self-signed web server certificate for the web browser of a Panel

Introduction

This section describes how to install the self-signed web server certificate of a Runtime web server (Unified PC or Unified Panel) in the web browser of a Unified Panel.

Requirement

- A self-signed web server certificate has been installed on the web server HMI device.
- A Runtime project is running on the web server.
- The client device has access to the web server.

Procedure

1. Start the "Web browser" application on the Panel.
2. Enter the URL of the Unified web server in the address bar: `https://<IP address of the HMI device or its FQDN/device name>`

   Note

   Access to a Unified PC web server

   Whether you enter the IP address, the FQDN (fully qualified domain name) or the device name as the URL depends on how the web server certificate was bound to the web server PC. This is defined during Runtime installation or later in the "Website settings" step of WinCC Unified Configuration.

   If needed, ask your administrator.

   The browser warns you that the connection is not secure.

3. Display the details for the connection.
4. Display the certificate.
5. Download the certificate.
   The certificate is loaded into the certificate store of the Panel. The Panel does not yet trust the certificate.
6. Trust the certificate with "Control Panel > Security > Certificates".
7. Reload the page in the web browser.

Result

The web browser trusts the self-signed web server certificate.

You can log in to Runtime with a secure connection.

See also

Workflow with a self-signed certificate (PC as web server) (Page 458)

Checking the status of the web server root certificate on the web client. (Page 437)

Importing and installing root certificates and CRL files on Panels (Page 545)

Managing third party certificates and own certificates of a Unified Panel (Page 496)

6.5.3 OPC UA certificates (PC)

6.5.3.1 Introduction

If the OPC UA server uses a security policy, the OPC UA communication is protected through the use of certificates. The OPC UA server must trust the OPC UA certificates of its clients, and vice versa (mutual SSL authentication).

PC as OPC UA server

If you are using a Unified PC as an OPC UA server, its OPC UA server certificate and OPC UA exporter certificate can be issued by a certificate authority (CA-based certificate) or be self-signed.

Note

For security reasons, it is recommended to use a CA-based certificate. You use WinCC Unified Certificate Manager to create the certificate.

PC as OPC UA client

A Unified PC that is used as an OPC UA client must use a certificate issued by a Unified certificate authority (CA-based certificate). You use WinCC Unified Certificate Manager to create the certificate.

Note

If you are using a PC as an OPC UA client, the Engineering System also acts as an OPC UA client during configuration of the device. Its certificate is created, installed and transferred automatically. For details on this and on establishing the trust relationship, see section Engineering System as OPC UA client (Page 478).

Contents of this help

This help describes the following:

- Creating a CA-based OPC UA server certificate or OPC UA client certificate of the PC
- Installing the CA-based certificate on the PC
- Using the default self-signed certificate for PCs as OPC UA server
- Establishing the trust relationship with the OPC UA communication partner on the PC
- Distributing the OPC UA certificate of the PC to the OPC UA communication partner
  This step sets up the establishment of the trust relationship with the PC on the OPC UA communication partner.

Note

Procedure at the OPC UA communication partners

For information on how to create and install the OPC UA certificate of the communication partner and distribute it to the PC and how to trust the certificate of the PC on the communication partner, refer to the operating instructions of the respective communication partner.

See also

CA-based workflow (OPC UA for PC) (Page 472)

Using a default self-signed certificate (PC as OPC UA server and exporter) (Page 476)

6.5.3.2 Using CA-based certificates (OPC UA for PC)

CA-based workflow (OPC UA for PC)

For CA-based OPC UA communication, a Unified PC needs the following certificates:

- OPC UA application certificate suitable for the role of the PC during OPC UA communication:
  - OPC UA server certificate and, if applicable, OPC UA exporter certificate,
    or
  - OPC UA client certificate
- Root certificate of the certificate authority that issued the OPC UA application certificate, along with its CRL file.

Requirement

- The OPC UA server uses a security policy.
- The OPC UA communication partner of the PC has an OPC UA application certificate that was issued by a certificate authority.
- The certificate has been installed on the communication partner as an own certificate.

Workflow

1. Create an OPC UA server certificate and OPC UA exporter certificate or an OPC UA client certificate for the PC, depending on the role of the PC.
   See section Creating certificates (OPC UA for PC) (Page 472).
2. Install the certificate(s) on the PC.
   See section Installing certificates (OPC UA for PC) (Page 473).
3. Restart Runtime on the PC.
4. Establish the trust relationship between the PC and its OPC UA communication partner.
   See section Establishing the trust relationship (OPC UA for PC) (Page 474).

See also

Introduction (Page 470)

Creating certificates (OPC UA for PC)

Introduction

You create the OPC UA server certificate and OPC UA exporter certificate or the OPC UA client certificate of a Unified PC on the certificate authority device. You use the WinCC Unified Certificate Manager application for this.

The certificate authority device is always a Unified PC.

Procedure

If you do not have a certificate authority yet, follow these steps:

1. Create the certificate authority.
   In so doing, you create the root certificate of the certificate authority and its CRL file automatically.
   See section Creating a certificate authority and root certificate (Page 519).
2. Add the PC to the certificate authority.
   See section Adding devices (Page 521).
3. Add the OPC UA server certificate and, if applicable, OPC UA exporter certificate or the OPC UA client certificate to the PC, depending on the role of the PC.
   See section Add application certificates (Page 524).

If you already have a certificate authority, follow these steps:

1. If the PC has not yet been added to the infrastructure of the certificate authority, add the PC.
   See section Adding devices (Page 521).
2. Add the OPC UA server certificate and, if applicable, OPC UA exporter certificate or the OPC UA client certificate to the PC, depending on the role of the PC.
   See section Add application certificates (Page 524).

See also

CA-based workflow (OPC UA for PC) (Page 472)

Installing certificates (OPC UA for PC)

Introduction

The OPC UA application certificate of a Unified PC is installed in the following steps:

- Export on the certificate authority device
- Import on the PC
- Installation on the PC

Note

You always export and import all certificates of the PC as well as the root certificate of the issuing certificate authority and its CRL file.

Requirement

- The desired OPC UA application certificate has been added for the PC on the certificate authority device.

Procedure

1. Export the certificates of the PC on the certificate authority device. Use the WinCC Unified Certificate Manager for this.
   See section Exporting certificates of a Unified PC (Page 528).
2. Import the certificates to the PC. Use the Certificate Manager for this.
   See section Importing certificates of a Unified PC (Page 538).
3. Install all certificates together on the PC or only the OPC UA certificate. Use the Certificate Manager for this.
   See section Installing all certificates or single certificates of a PC (Page 539).

See also

CA-based workflow (OPC UA for PC) (Page 472)

Establishing the trust relationship (OPC UA for PC)

Introduction

Secure OPC UA communication requires that the communication partners trust each other's OPC UA application certificates.

That is automatically the case when the OPC UA client trusts the root certificate of the certificate authority that issued the OPC UA server certificate, and vice versa.

Procedure

1. Check the PC to determine whether it already trusts the root certificate of its OPC UA communication partner.
   See sections Checking the status of a root certificate on the HMI device (Page 544) and Automatic trust relationship in OPC UA communication (Page 475).
   If the PC already trusts the root certificate, continue with step 3.
2. If the PC does not trust the root certificate, install it manually.
   Follow these steps:
   - Export the root certificate of the OPC UA communication partner and its CRL file to a storage location the PC can access.
     Follow the procedure described in the operating instructions of the communication partner.
   - Install the root certificate and the CRL file on the PC.
     See section Managing third-party certificates of a Unified PC (Page 499).

3. Check the communication partner to determine whether it already trusts the root certificate of the PC.
   Follow the procedure described in the application help of the communication partner.
   If the communication partner already trusts the root certificate, you don't have to do anything.
4. If the communication partner does not trust the root certificate, install it manually.
   Follow these steps:
   - Export the root certificate on the certificate authority device with Certificate Manager to an external data storage medium.
     See section Exporting root certificate and CRL file (Page 531).

     Note

     Alternative

     If the certificates of the PC were already installed with Certificate Manager, you can export the root certificate on the PC with SIMATIC Runtime Manager.

     See section Managing third-party certificates of a Unified PC (Page 499).
   - Connect the OPC UA communication partner to the external data storage medium.
   - Install the root certificate and its CRL file on the communication partner.
     Follow the procedure described in the user help of the communication partner. If necessary, manually copy both files to the folder for trusted certificates.

At the next connection attempt, the OPC UA server and OPC UA client trust each other.

See also

CA-based workflow (OPC UA for PC) (Page 472)

Automatic trust relationship in OPC UA communication

This section describes cases in which a device automatically trusts the CA-based certificate of its OPC UA communication partner. You do not have to establish the trust relationship manually on this device.

Same certificate authority

If both OPC UA communication partners are HMI devices and their OPC UA certificates have the same certificate authority, they automatically trust their OPC UA certificates.

Trusted certificate authority

If a device already trusts the certificate authority that issued the OPC UA certificate of the other device, it also automatically trusts the other device's OPC UA certificate.

Example

A Unified OPC UA server communicates with an OPC UA client. Server and client have different certificate authorities. The Unified OPC UA server trusts the root certificate of the OPC UA client, and vice versa. As a result, the devices also trust their OPC UA certificates.

A second OPC UA client authenticates itself to the Unified OPC UA server. Its OPC UA client certificate was issued by the same certificate authority that issued the OPC UA client certificate of the first client.

Since the Unified OPC UA server already trusts the root certificate, the server automatically also trusts the OPC UA client certificate of the second client.

Tag export of a Unified OPC UA server

In OPC UA communication, you have the option of exporting the tags of the project of a Unified OPC UA server running in Runtime. The device must be a Unified PC that has an OPC UA server certificate and OPC UA exporter certificate.

In CA-based communication, the root certificate of the certificate authority that issues these certificates is also automatically installed when you generate the certificates of the device with WinCC Unified Certificate Manager. The OPC UA server component and OPC UA exporter component of the device trust each other automatically.

See also

Establishing the trust relationship (OPC UA for PC) (Page 474)

6.5.3.3 Using a default self-signed certificate (PC as OPC UA server and exporter)

Introduction

A Unified PC that is used as an OPC UA server can use a self-signed OPC UA server certificate. It can use a self-signed OPC UA exporter certificate for tag export. (default certificates)

The certificates are created and installed on the PC automatically.

Note

These self-signed certificates are only used if no corresponding CA-based OPC UA certificate has been installed in the own certificates at Runtime start on the PC.

Note

Self-signed certificates provide less protection than CA-based certificates. Use them for testing, for example. It is recommended that they then be replaced with CA-based certificates.

Establishing the trust relationship

You can establish the trust relationship between the OPC UA server and OPC UA client before or after the first connection attempt.

The OPC UA server certificate and OPC UA exporter certificate trust each other automatically.

Requirement

- The OPC UA server uses a security policy.
- The OPC UA client uses a self-signed OPC UA client certificate.
- Server and client do not yet trust their OPC UA certificates.
- Server and client are running.

Procedure

1. Check whether a CA-based OPC UA server certificate and an OPC UA exporter certificate have been installed on the PC as an own certificate.
   See section Managing own certificates of a Unified PC (Page 498).
2. If so, uninstall these CA-based OPC UA certificates and restart Runtime on the PC.
   At the next connection attempt between the server and client, the PC sends the self-signed OPC UA server certificate. The PC uses the self-signed OPC UA exporter certificate for that tag export.
3. Trust the OPC UA client certificate on the PC.
   Follow the procedure described below.
4. Trust the OPC UA server certificate of the PC on the OPC UA client.
   Follow the procedure described below.

Trusting the OPC UA client certificate on the PC

To trust the client certificate before the first connection attempt, follow these steps:

1. Export the self-signed OPC UA client certificate on the client device to a storage location the PC can access. Follow the procedure described in the user help of the client.
2. Trust the certificate on the PC. See section Managing third-party certificates of a Unified PC (Page 499).

To trust the client certificate after the first connection attempt, follow these steps:

1. After the first connection attempt, the OPC UA client certificate is in the "untrusted" folder of the certificate store on the PC.
   Trust the certificate on the PC. See section Managing third-party certificates of a Unified PC (Page 499).

Trusting the OPC UA server certificate on the OPC UA client

To trust the server certificate before the first connection attempt, follow these steps:

1. Copy the OPC UA server certificate from the certificate store of the PC to a storage location the OPC UA client can access.
   The certificate store is located in `C:\ProgrammData\SCADAProjects\certstore`.
2. Trust the OPC UA server certificate on the OPC UA client. Follow the procedure described in the user help of the client. If necessary, manually copy the certificate to the folder for trusted certificates.

To trust the server certificate after the first connection attempt, follow these steps:

1. After the first connection attempt, the OPC UA server certificate is in the rejected certificate store on the client device.
   Trust the certificate on the client. Follow the procedure described in the user help of the client. If necessary, manually copy the certificate to the folder for trusted certificates.

See also

Introduction (Page 470)

6.5.3.4 Engineering System as OPC UA client

Introduction

If you are using a Unified PC or a Unified Panel as an OPC UA client, you configure which tags of the OPC UA server the client accesses and which alarm instances it receives in the Engineering System. For this reason, the Engineering System also acts as an OPC UA client during configuration of the device.

Provision and installation of the certificates

The client certificate of the Engineering System is created and transferred to the server automatically the first time a connection is established.

Trust the client certificate on the server. Follow the procedure described in the user help of the server. If necessary, manually copy the certificate to the folder for trusted certificates.

The Engineering System automatically receives the server certificate and trusts it without your having to take any action.

See also

Introduction (Page 470)

6.5.4 Audit certificates (PC)

6.5.4.1 Workflow

Introduction

The WinCC Unified Audit option uses certificates to generate a checksum for Audit Trail data records. The checksum can be used to determine if the contents of a data record have been altered. The checksum also ensures that no lines have been removed from or added to the Audit Trail.

Audit certificates are not used for communication with another device.

The Audit certificate of a Unified Panel or Unified PC must be issued by a Unified certificate authority (CA-based certificate). You use the "WinCC Unified Certificate Manager" application for this.

Note

Certificate Manager always creates CA-based certificates. The use of CA-based certificates facilitates establishment of the trust relationship and provides the highest protection for your plant.

The use of self-signed certificates is not supported for Audit.

Required certificates

For WinCC Unified Audit, you need the following certificates:

- Audit certificate of the HMI device
- Root certificate of the certificate authority that issued the Audit certificate, along with its CRL file.

Workflow

To provide the certificates needed by an HMI device for Audit, follow these steps:

1. Create the Audit certificate of the HMI device.
2. Install the Audit certificate on the HMI device.
3. Restart Runtime on the HMI device.

6.5.4.2 Creating certificates (Audit for PCs)

Introduction

You create the Audit certificate of a Unified PC on the certificate authority device. You use the "WinCC Unified Certificate Manager" application for this.

The certificate authority device is always a Unified PC.

Procedure

If you do not have a certificate authority yet, follow these steps:

1. Create the certificate authority.
   In so doing, you create the root certificate of the certificate authority and its CRL file automatically.
   See section Creating a certificate authority and root certificate (Page 519).
2. Add the PC to the certificate authority.
   See section Adding devices (Page 521).
3. Add the Collaboration certificate to the PC.
   See section Add application certificates (Page 524).

If you already have a certificate authority, follow these steps:

1. If the PC has not yet been added to the infrastructure of the certificate authority, add the PC.
   See section Adding devices (Page 521).
2. Add the Audit certificate to the PC.
   See section Add application certificates (Page 524).

6.5.4.3 Installing certificates (Audit for PCs)

Introduction

The audit certificate of a Unified PC is installed in the following steps:

- Export on the certificate authority device
- Import on the PC
- Installation on the PC

Note

You always export and import all certificates of the PC as well as the root certificate of the issuing certificate authority and its CRL file.

Requirement

- The Audit certificate has been added for the PC on the certificate authority device.

Procedure

1. Export the certificates of the PC on the certificate authority device. Use the WinCC Unified Certificate Manager for this.
   See section Exporting certificates of a Unified PC (Page 528).
2. Import the certificates to the PC. Use the Certificate Manager for this.
   See section Importing certificates of a Unified PC (Page 538).
3. Install all certificates together on the PC or only the Audit certificate. Use the Certificate Manager for this.
   See section Installing all certificates or single certificates of a PC (Page 539).

6.6 Working with certificates

6.6.1 Basics

6.6.1.1 Communication partners

The following table shows:

- With which communication partners a Unified HMI device can communicate via certificates.
- Whether the usage of certificates is mandatory for communication.

Communication partners	Using certificates ...	See also
Runtime of a different Unified HMI device	Communication runs via Runtime Collaboration: Is obligatory	Workflow (Collaboration for Panels) (Page 377) Workflow (Collaboration for PCs) (Page 428)
	Communication runs via OPC UA: Depends on the security guideline configured at the OPC UA server.	OPC UA certificates (Panel) (Page 417) OPC UA certificates (PC) (Page 470)
Web client[1]	Is obligatory	Web server certificates (Panel) (Page 381) Web server certificates (PC) (Page 432)
Smart Client[2]	Depends on the configuration of the Panel in the Engineering System.	Smart Server certificates for Panels (Page 427)
S7 PLC of the series S7-1500 and S7-1200	Depends on the configuration of the controller in the Engineering System.	Communication with S7-1500 and S7-1200 (Page 487)
Other Siemens devices Example: S7 PLC of a different series, SINUMERIK device or Comfort Panel	Communication runs via OPC UA: Depends on the security guideline configured at the OPC UA server.	OPC UA certificates (Panel) (Page 417) OPC UA certificates (PC) (Page 470)
Third-party devices		

[1] Only for communication with a Unified Runtime web server

[2] Only for communication with a Unified Panel WinCC Smart Server

Note

Audit

The audit certificate is not used for communication with a communication partner.

See also

Certificates in WinCC Unified Runtime (Page 374)

6.6.1.2 Own certificates and third-party certificates of HMI devices

Own certificates

An HMI device authenticates itself to its communication partners or encrypts the communication with the communication partners with its own certificates.

An HMI device can have the following own certificates:

	Storage location on the HMI device
CA-based application certificates	Unified certificate store, in the folder containing the own certificates
Self-signed application certificates	Internal
General certificates (always CA-based)	Unified PC: Certificate store of the application that uses the general certificate Unified Panel: Unified certificate store, in the folder containing the own certificates

Note

When you install CA-based own certificates on an HMI device, you install the root certificate of the Unified certificate authority and its CRL file automatically.

The root certificate and CRL file do not belong to the own certificates. These files are located in the certificate store, in the folder containing the trusted certificate authorities.

They are installed on the HMI device in order to establish the trust relationship with other HMI devices of the same Unified certificate authority automatically. This help includes the root certificate and CRL file in the group of third-party certificates.

Third-party certificates

The communication partners use the third-party certificates to authenticate themselves to the HMI device or encrypt the communication with the HMI device.

An HMI can have the following third-party certificates:

	Storage location on the HMI device
CA-based application certificates	Unified certificate store, in the third-party certificates folder
Self-signed application certificates	
General certificates (always CA-based)	
When using a third-party CA-based certificate: Root certificate and CRL file of the issuing certificate authority	Unified certificate store, in the folder containing the trusted certificate authorities

See also

Unified tools for certificates (Page 483)

Determining the required application certificates (Page 492)

Using general certificates (Page 548)

6.6.1.3 Unified tools for certificates

Introduction

This section describes the tools you use to perform the following tasks:

- Creating and managing own certificates of the HMI device and distributing them to the communication partners
- Installing and managing own certificates of an HMI device on the device
- Trusting and managing the third-party certificates of the communication partners on the HMI devices

Information on how to create the third-party certificates and how to install the Unified certificates on the devices of the communication partners can be found in the user help of the respective communication partner.

Creating and distributing CA-based own certificates

You create the CA-based certificates of your HMI devices on the certificate authority device with the WinCC Unified Certificate Manager tool.

You use Certificate Manager to perform the following tasks:

- Creating the Unified certificate authority (private key, root certificate and CRL file)
- Issuing or renewing the application certificates and general certificates of your HMI devices
- Exporting the configured certificates as setup for installation on the respective HMI devices
  The procedure is different for application certificates and general certificates.

- Distributing the root certificate and its CRL file to the communication partners

Note

Alternative for Unified PCs

If the certificates of a Unified PC were already installed on the PC, you can also export the root certificate and its CRL file on the PC with SIMATIC Runtime Manager and distribute them to the communication partners.

- Recreating the complete configuration of the certificate authority
- Creating a backup of the complete configuration of the certificate authority

Installing and managing CA-based own certificates

You install and manage CA-based own certificates of an HMI device with the following tools:

- Unified PC:
  - Application certificates: WinCC Unified Certificate Manager
  - General certificates: The installation is performed outside of Certificate Manager. See section Using general certificates (Page 548).
- Unified Panel: Control Panel (application certificates and general certificates)

The tools access the Unified certificate store of the HMI device.

Installing the Unified root certificate

During export, import and installation of CA-based own certificates of an HMI device, the root certificate of the Unified certificate authority and its CRL file are also exported and imported and installed in the folder containing the trusted root certificate authorities.

Alternatively, you can individually install the root certificate and/or its CRL file. On a Unified PC you use SIMATIC Runtime Manager for this. On a Unified Panel you use Control Panel.

Creating, installing and distributing self-signed own certificates

HMI devices that are used as a Runtime web server or an OPC UA server can use self-signed own certificates instead of CA-based certificates.

Unified PCs that are used as an OPC UA server can also use a self-signed OPC UA exporter certificate.

Unified Panels that are Smart Servers can only use a self-signed Smart Server certificate.

You use the following tools to create these certificates and install them in the own certificates:

Certificate	Tool
Self-signed web server certificate of a Unified PC	Creation and installation of the certificate: with WinCC Unified Configuration Transfer to the web clients: automatically
Self-signed web server certificate of a Unified Panel	The certificate is created and installed automatically.
Self-signed OPC UA server certificates of a Unified Panel or Unified PC Self-signed OPC UA exporter certificate of a Unified PC	
Self-signed Smart Server certificate of a Unified Panel	

The certificates are automatically transferred when the connection to the communication partners is established.

Managing third-party certificates

You use the following tools to manage the certificates of the communication partners of an HMI device:

Device type	Tool
Unified PC	SIMATIC Runtime Manager
Unified Panel	Control Panel

This includes the following activities:

- Importing root certificates and their CRL files
  You can also export the root certificate and CRL file with SIMATIC Manager.
- Trusting or rejecting certificates
- Displaying details for a certificate
- Uninstalling certificates by deleting them

The tools access the Unified certificate store of the HMI device.

See also

Managing third party certificates and own certificates of a Unified Panel (Page 496)

Managing third-party certificates of a Unified PC (Page 499)

Managing own certificates of a Unified PC (Page 498)

Using CA-based certificates (Page 502)

6.6.1.4 Device binding of a certificate

Introduction

An application certificate is always bound to the device on which the application is installed. In order for the certificate to be bound to a device, the following information is written to the certificate:

- Device name
  Restricts communication to accesses from the same network
  or
  Fully Qualified Domain Name/FQDN
  If the device belongs to a domain
- Or the IP address
  Only when fixed IP addresses are used
- Or both

The communication partners use this information to verify whether the sender of the transferred certificate is identical to the device for which the certificate was issued.

Device binding for CA-based certificates

When you use CA-based Unified certificates, you configure the information used to bind the application certificates to the HMI device when you add the HMI device in WinCC Unified Certificate Manager. All application certificates of the device use the same setting.

Note

A subsequent change to this setting is only possible if you delete the device from the CA infrastructure and add it again. You must then add, distribute and install the application certificates of the device again.

For this reason, it is recommended that the device name/FQDN and IP address be entered for this setting.

Note

Device binding for Unified PC web server

The web server certificate must always also contain the information that is used to generate the address of the identity provider and the website of WinCC Unified Runtime. You define the method for generating this address during installation of Runtime or later with the WinCC Unified Configuration tool in the "Website settings" step.

Note

Device binding for OPC UA server and OPC UA exporter

The application certificates for OPC UA server and OPC UA exporter must always also contain the device name or FQDN.

Device binding for self-signed certificates

Self-signed Unified certificates are always bound to the certificate using device name/FQDN and IP address.

See also

Adding devices (Page 521)

Website settings (Page 40)

6.6.1.5 Communication with S7-1500 and S7-1200

Runtime Unified supports secure communication with PLCs of the series S7-1200 and S7-1500.

With secure communication, the connection between Runtime and PLC is encrypted by the TLS protocol. A valid PLC certificate must be configured on the PLC.

Requirement

- Firmware installed on the controller:
  - S7-1500: 2.9 and higher
  - S7-1200: 4.5 and higher
- A certificate was provided for the controller in the Certificate Manager in the Engineering System.

Note

It is recommended to enable the "Only allow secure PG/PC and HMI communication" option on the PLC under "Protection & Security > Connection mechanism". If this option is selected, the Engineering System automatically generates a self-signed PLC certificate. The PLC always uses secure communication. Disabling this option increases the security risk.

You can replace this default certificate in the certificate manager of TIA Portal:

- Generate your own self-signed certificate with different certificate settings.
- Upload a self-signed one.
- Upload a CA-based certificate, the root certificate of the issuing certification authority and its CRL file.

More information on the certificate manager of TIA Portal is available in the TIA Portal online help under "Editing devices and networks > Configuring devices and networks > Configuring networks > Secure Communication > Secure PG/HMI Communication".

- Communication between HMI device and PLC:
  - The HMI device has an integrated connection to the PLC.
    Or
  - The HMI device has a non-integrated connection to a device proxy. The device proxy uses the current device proxy data of the PLC.
    Or
  - The HMI device has been connected to the PLC using the "ChangeConnection" system function.

Connection establishment

The PLC sends its certificate to the HMI device (one-way SSL authentication). The HMI device checks the certificate:

- If the HMI device trusts the PLC certificate, the connection is established. The session remains until the connection is interrupted. The process is repeated the next time the connection is established.

  Note

  Stopping or restarting Runtime interrupts the connection.

  The following actions do not interrupt the connection:

  - Stopping or restarting the PLC.
  - Download to device (PLC or HMI device)

- If the HMI device does not trust the certificate, the connection is rejected. A system event is output. After the time needed for reconnection (ReconnectTime) has elapsed, the HMI device starts a new connection attempt.

Integrated connection and non-integrated connection via device proxy.

When loading the HMI device, the PLC certificate is automatically loaded into the HMI device as well. The PLC certificate is part of the current configuration of the device and has the "Trusted" status. It is managed internally in the system and is not visible in SIMATIC Runtime Manager or in the Control Panel.

When establishing a connection, the HMI device already trusts the PLC certificate. The connection is established automatically.

Note

If you change the PLC certificate after loading the HMI device without reloading the HMI device, the HMI device will not trust the new PLC certificate the next time it connects. You must trust the certificate manually.

Connection via "ChangeConnection"

After calling the "ChangeConnection" system function, the HMI device initially does not trust the PLC certificate. The PLC certificate has the status "untrusted". You must trust the certificate manually.

Distributing a PLC certificate manually

Proceed as described here:

- Unified PC: Managing third-party certificates of a Unified PC (Page 499)
- Unified Panel: Managing third party certificates and own certificates of a Unified Panel (Page 496)

Communication with other controllers

The certificated-protected communication between a Unified HMI device and a Siemens controller with different firmware, or from a different series, or with a controller from a third party must run via OPC UA.

See also

Communication partners (Page 481)

6.6.1.6 Runtime and simulation

When the communication of an HMI device is protected through the use of certificates, you need certificates for simulation and system operation of the device.

6.6.2 Workflow for using certificates on HMI devices

Introduction

If you are using security-related Unified components on the HMI devices of your system, you must provide the following certificates:

- Certificates used by the HMI devices to authenticate themselves to their communication partners (Unified certificates)
- Certificates used by the communication partners of the HMI devices to authenticate themselves to the HMI devices (third-party certificates)

Note

Some components require a mutual SSL authentication, meaning that both the HMI device and its communication partner need a certificate. They must trust each other's certificates.

Other components require a one-way SSL authentication, meaning that only the HMI device needs a certificate and its communication partner must trust the certificate, or vice versa.

See also section Determining the required application certificates (Page 492).

Procedure

To provide these certificates, follow these steps:

1. Determine which application certificates are needed by the HMI devices and which are needed by their communication partners.
   See section Determining the required application certificates (Page 492).
2. Decide whether to use CA-based or self-signed certificates for these certificates.
   See section Selecting a suitable certificate type (Page 493).

   Note

   The use of CA-based certificates is recommended.

   CA-based certificates are mandatory for some Unified components.

3. When using CA-based Unified certificates, issue the needed application certificates of the HMI device with a Unified certificate authority, distribute them to the HMI devices and install them there:
   - If you do not have a certificate authority yet, follow the procedure described in section First-time use of CA-based certificates (Page 507).
   - If you already have a certificate authority, follow the procedure described in section Continued use of CA-based certificates (Page 513).

   Note

   Installation at runtime

   When you install the CA-based certificates of an HMI device at runtime, the existing connections are not interrupted. The HMI device does not start using the new certificates until after a Runtime restart.

   A Runtime restart is not required for use of a newly installed web server certificate.

4. The use of self-signed certificates is also possible for the following components:
   - Unified OPC UA server
   - Unified OPC UA exporter
   - Unified web server
   - Smart Server

   You can find information on creating and installing the certificates in section Using self-signed certificates (Page 552).
5. Create the certificates of the communication partners and install them on their devices.
   To do this, follow the procedure described in the user help of the respective communication partner.
6. Establish the trust relationship between the HMI devices and their communication partners:
   - For CA-based certificates, follow the procedure described in section Trusting CA-based certificates (Page 543).
   - For self-signed certificates, follow the procedure described in section Using self-signed certificates (Page 552).

6.6.3 Determining the required application certificates

An application certificate is the certificate which sends an application during the connection establishment to another application to authenticate itself.

Procedure

1. Note for each HMI device which security-relevant Unified components are used on the device.
2. Use the table below to determine which application certificate the HMI devices and their communication partners require.

Note

Some components require reciprocal SSL authentication, meaning that the HMI device and its communication partner both require a certificate. They must trust their certificates reciprocally.

Some components require one-sided SSL authentication, meaning that only the HMI device requires a certificate and its communication partner must trust the certificate or vice versa.

Required certificates

Unified components used on the HMI device	Communication partners of the HMI device	Required application certificates	Trust relationship
Runtime web server[1]	Web clients	The HMI device requires a web server certificate.	One-sided SSL authentication The web clients must trust the web server certificate.
OPC UA Server	OPC UA clients	The HMI device requires an OPC UA Server certificate and the communication partners an OPC UA Client certificate or vice versa.	Reciprocate SSL authentication The OPC UA clients must trust the OPC UA Server certificate and vice versa.
OPC UA Client	OPC UA Server		
OPC UA Exporter[2]	n.a.	The Unified PC requires an OPC UA Server certificate and an OPC UA Exporter certificate.	n.a. OPC UA Server certificate and the OPC UA Exporter certificate trust each other automatically.
Collaboration	A different HMI device	Both HMI devices require a Collaboration certificate.	Reciprocate SSL authentication The devices must trust their Collaboration certificates.
Audit	n.a.	The HMI device requires an Audit certificate.	n.a. The certificate generates checksums. It is not used for communication.

Unified components used on the HMI device	Communication partners of the HMI device	Required application certificates	Trust relationship
Component of the PLC communication	S7-1500 and S7-1200	The S7 controller requires a certificate.	One-sided SSL authentication The HMI device must trust the PLC certificate.
Smart Server[3]	Smart Client	The Smart Server requires a certificate	One-sided SSL authentication The Smart Client must trust the Smart Server certificate.

[1] Unified PCs are always Runtime web servers. They always need a web server certificate.

[2] Only on Unified PCs that are used as OPC UA servers. OPC UA Exporter exports the runtime variables into an OPC UA Nodeset XML file.

[3] Only for Unified Comfort Panels

See also

Trusting CA-based certificates (Page 543)

Workflow for using CA-based certificates (Page 507)

6.6.4 Selecting a suitable certificate type

Introduction

Application certificates are issued by a certification instance. By signing the application certificate the certification instance guarantees the authenticity of the certificate and thus the identity of its owner (subject).

There are two types of certification instances:

- A Certificate Authority (CA)
  Application certificates which were signed by a certificate authority are CA-based certificates.

  Note

  It is not possible to create own CA-based application certificates of an HMI device with an external certificate authority. The certificates must be created by a Unified certificate authority with the application "WinCC Unified Certificate Manager".

- The certificate itself
  Application certificates that confirm the validity of the certificate through their own signature are self-signed certificates.

If a communication partner trusts the certification instance, it trusts all application certificates that were issued by the certificate authority.

Note

This user help assumes that both devices use the same type of certificate authority for reciprocal SSL authentication.

Mixed usage is also technically possible.

Supported types

The following table provides an overview of which certificate types support the security-relevant components:

Component/role of the HMI device	Own certificates		Third-party certificates		
	CA-based	Self-signed	Communication partners	CA-based	Self-signed
Web server	✓	✓	Web client	n.a.	
OPC UA Client	✓	-	OPC UA server	✓	✓
OPC UA Server	✓	✓	OPC UA Client[1]	✓	✓
OPC UA Exporter[2]	✓	✓	n.a.		
Runtime Collaboration	✓	-	Runtime Collaboration partner[3]	✓	-
Audit	✓	-	n. a.		
PLC communication	n.a.		S7-1500, S7-1200	✓	✓
Smart Server	-	✓	Smart Client	n.a.	

[1] If the OPC UA Client is an HMI device, the Client HMI device must use a CA-based certificate.

[2] Variable export is only possible on Unified PCs that are used as OPC UA Servers. The OPC UA Exporter component communicates with the OPC UA Server component of the Unified PC. Communication with a different device does not take place for the variable export.

[3] The communication partner must also be a Unified HMI device. Its certificate must be issued by a Unified certificate authority.

Selection of the suitable type

CA-based certificates are especially suitable in the following cases:

- For a high protection level of the plant communication
- For access to an HMI device from an external network

Self-signed certificates are suitable:

- For testing the system configuration
- For small plants or plant sections that operate in a closed network

Note

- For security reasons the use of CA-based certificates is recommended, both for Unified certificates as well as for third party certificates.
- When making your decision, also consider internal company specifications or project-specific factors such as the security guideline that is relevant for a plant.

Benefits from the usage of CA-based Unified certificates

- Central creation and management of all Unified certificates
- Easy distribution of the certificates TO the HMI devices as well as installation on the HMI devices
- Easy update, distribution and installation of expired certificates during running operation, including update of the entire certificate configuration of the certificate authority in case the root certificate expires.
- Easy establishment of the trust relationship to the HMI devices at the communication partners
- Encrypted, password-protected export and import of certificates
- Very high protection level of the communication
- Simple data backup of the entire configuration of the certificate authority

Benefits for the use of self-signed Unified certificates

- No or low effort for the creation of the certificates and for their installation on the HMI devices

See also

Unified certificate authority (Page 505)

Using self-signed certificates (Page 552)

Requirements and limitations when using CA-based certificates (Page 502)

6.6.5 Managing third party certificates and own certificates of a Unified Panel

Introduction

You manage the CA-based own certificates of the panel and its third-party certificates in the Control Panel of a Unified Panel.

Note

Self-signed own certificates are generated and installed outside the Control Panel. You have the possibility to delete them in the Control Panel.

Certificates of S7 controllers with an integrated connection to the Panel are managed system-internally. They are not visible in the Control Panel.

Own certificates

The Control Panel offers the following possibilities for own certificates:

Import and install	Only for CA-based own certificates Proceed as described: • For application certificates, see the section Importing and installing certificates of a Panel (Page 541). • For general certificates, see the section Workflow for general certificates (Page 548).
Display	For CA-based and self-signed certificates Proceed as described below.
Delete	

Third-party certificates

The Control Panel offers the following possibilities for third party certificates:

	Root certificates and CRL files	Application certificates and general certificates	
Import and install	✓	-	You import and install only root certificates and their CRL file manually. Follow the steps described in the section Importing and installing root certificates and CRL files on Panels (Page 545). A third-party CA-based application certificate or general certificate is automatically trusted by the panel if its root certificate is installed on the panel. Manual import and installation of the certificate are not required. Third-party self-signed certificates are transferred automatically during the first connection attempt at the certificate stores of the Panel and receive the status "untrusted". You can trust or delete them in the Control Panel. Manual import and installation of the certificate are not required.

Display	✓	✓	Proceed as described below.
Trust	-	✓	As a rule you only trust self-signed certificates manually. CA-based certificates are trusted by the Panel automatically after import and installation of the root certificate.
Reject	-	✓	
Delete	✓	✓	

Note

Third-party application-certificates can be CA-based or self-signed. Third-party general certificates must be CA-based.

More information

You can find additional information on the function "Certificates" of the Control Panel in the "SIMATIC HMI devices Unified Comfort Panels" operating instructions.

Display

1. In the Control Panel, select "Security"" > "Certificates".
2. In the "Certificate stores" list select one of the following entries:
   - To display own certificates, select the entry "My Certificates".
     You can see a list with own certificates of the Panel.
   - To display third-party application certificates or third-party general certificates, select the entry "Other Certificates".
     You can see a list of the CA-based or self-signed third party certificates available on the Panel. You see both certificates with the status "Trusted" and "Untrusted".
   - For root certificates and their CRL files select the entry "Certificate Authorities".
     You see a list of the root certificates installed on the panel as trusted and their CRL files.
3. Click the desired certificate.

The certificate details are displayed.

Trusting or rejecting

1. In the Control Panel select "Security" > "Certificates".
2. Select the "Other Certificates" entry from the "Certificate stores" list.
   You see both certificates with the status "Trusted" and "Untrusted".
3. To trust a third-party certificate marked as untrusted, select it and choose "Trust".
   The certificate receives the status "Trusted".
4. To identify a third-party certificate as untrusted without deleting, mark it and select "Revoke".
   The certificate receives the status "Untrusted".
   The certificate is still available in the certificate store. If required, you can trust them again in the future.

Delete

Note

Deleting uninstalls and removes a certificate from the certificate store.

1. In the Control Panel select "Security" > "Certificates".
2. Select the desired entry from the "Certificate stores" list.
   Depending on the selected entry you see a list of the certificates available on this device. After selection of "Other certificates" you see both certificates with the status "Trusted" and "Untrusted".
3. Click the desired certificate or the CRL file and select "Delete".

The selected certificate or the file is deleted immediately without query.

See also

Deleting application certificates (Page 526)

6.6.6 Managing own certificates of a Unified PC

Overview

You manage the CA-based own application certificates of a Unified PC with WinCC Unified Certificate Manager.

Certificate Manager offers the following options:

Import and install	Follow the procedure described in section Importing and installing certificates of a Unified PC (Page 538).
Display	Follow the procedure described below.
Delete	

Note

Self-signed own certificates are created, installed and managed outside of Certificate Manager.

You install and manage general own certificates outside of Certificate Manager. See section Workflow for general certificates (Page 548).

For information on how to manage the third-party certificates of the PC (self-signed certificates and CA-based certificates of the communication partners and their root certificates), see section Managing third-party certificates of a Unified PC (Page 499).

Requirement

- Certificate Manager is open on the Unified PC.
- The certificates of the device have been imported or imported and installed with Certificate Manager.
- The "Installed certificates" tab is visible.

Displaying a certificate

1. Select a certificate.

The "Details" area shows detailed information about the certificate.

Deleting a certificate

1. Select a certificate.
2. Right-click and select "Delete".

The certificate is uninstalled.

See also

Opening Certificate Manager (Page 554)

6.6.7 Managing third-party certificates of a Unified PC

Introduction

Data exchange between WinCC Unified Runtime and its communication partners can be protected by certificates. The communication partners use self-signed certificates or certificates issued by a certificate authority (CA-based certificates).

In the SIMATIC Runtime Manager, you manage the certificates of the communication partners of the Unified PC (third-party certificates) in the "Certificates" tab.

You have the following options:

- Importing certificates, root certificates and CRL files
- Trust, reject, or delete certificates and root certificates already in the certificate store
- Exporting certificates, root certificates and CRL files to distribute them to other devices

Note

Alternative

If the Unified PC has its own CA-based certificates, you can also export the root certificate and CRL file of its Unified Certificate Authority using the WinCC Unified Certificate Manager application.

Note

Import and export of root certificates and CRL files

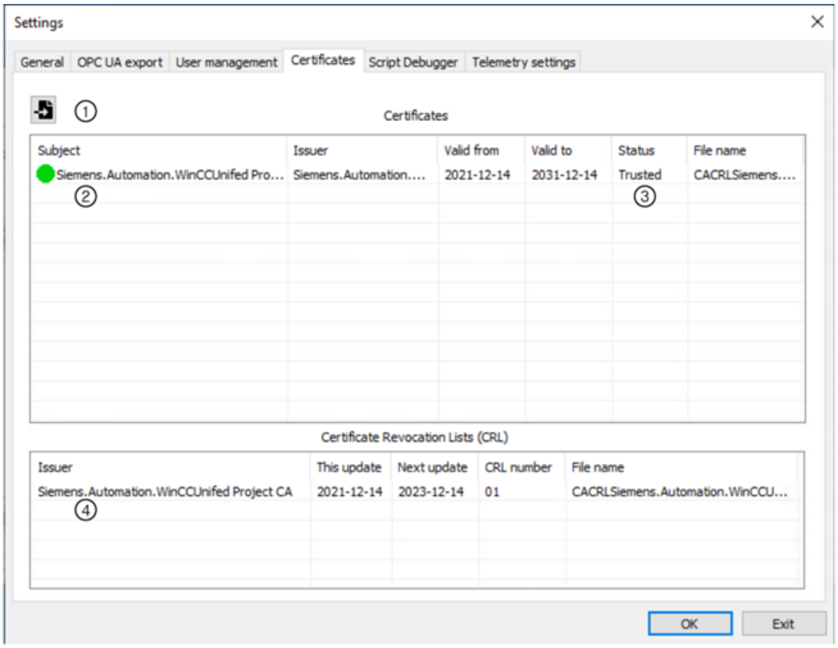
A root certificate and its CRL file must be imported separately.

If you have exported a root certificate, its CRL file is also exported. If required, you can also export the CRL files individually.

Note

Certificates of S7 controllers with an integrated connection to the Unified PC are managed system-internally. They are not visible in the SIMATIC Runtime Manager.

Structure



Certificates

Subject	Issuer	Valid from	Valid to	Status	File name
● Siemens.Automation.WinCCUnifed Pro...	Siemens.Automation....	2021-12-14	2031-12-14	Trusted	CACRLSiemens....

Certificate Revocation Lists (CRL)

Issuer	This update	Next update	CRL number	File name
Siemens.Automation.WinCCUnifed Project CA	2021-12-14	2023-12-14	01	CACRLSiemens.Automation.WinCCU...

① Button for importing a certificate or CRL file

② "Certificates" area

A list of the third-party certificates available in the certificate store (self-signed certificates, CA-based certificates and their root certificate). If the PC has its own CA-based certificates, you can also find the root certificate of the Unified Certificate Authority here.

③ "State" column

Shows whether the Unified PC trusts a certificate.

④ "Certificate Revocation Lists (CRL)" area

A list of the root certificate CRL files from "Certificates"

Requirement

- The Runtime Manager is open.
- The certificates and CRL files to be imported are located in a folder to which the Unified PC has access.

Managing certificates

1. Click the ⚙ button in the toolbar.
2. Select the "Certificates" tab.
3. You can perform the following actions:

Action	Procedure
Import and trust	1. Click "Import new certificate or certificate revocation list (CRL)": 2. Select the location where the certificate is stored, for example, an external data carrier, and select the certificate. 3. Confirm your input. The certificate is imported and copied to the "trusted" folder on the PC. Or the CRL file is imported.
Trust	Right-click on a certificate and select "Trust". The certificate is moved to the "trusted" folder on the PC.
Reject	Right-click the certificate and select "Reject". The certificate is moved to the "untrusted" folder on the PC.
Display	Right-click on a certificate and select "Show". A window with detailed information on the certificate opens.
Delete	Right-click on a certificate and select "Delete". The certificate is deleted from the certificate store on the PC.
Export	1. Right-click the certificate and select "Export". 2. If you have selected a root certificate, select the file format. 3. Select the target folder, for example, an external data storage medium. 4. Confirm your input. The certificate is copied to the target folder. If you have selected a root certificate, its CRL file is also copied. Distribute the files to the desired devices. To do this, proceed as described in the application help of the device.

Managing CRL files

1. Click the ⚙ button in the toolbar.
2. Select the "Certificates" tab.
3. You can perform the following actions:

Action	Procedure
Import	1. Click "Import new certificate or certificate revocation list (CRL)": 2. Select the location of the CRL file, e.g. an external data storage medium, and select the file. 3. Confirm your input. The file is imported and copied in the "trusted" folder on the PC.
Delete	Right-click on a CRL file and select "Delete". The file is deleted from the "trusted" folder on the PC.
Export	1. Right-click on the CRL file and select "Export". 2. Select the file format. 3. Select the target folder, for example, an external data storage medium. 4. Confirm your input. The CRL file is copied to the target folder. Distribute the files to the desired devices. To do this, proceed as described in the application help of the device.

See also

Exporting root certificate and CRL file (Page 531)

Managing own certificates of a Unified PC (Page 498)

6.7 Using CA-based certificates

6.7.1 Requirements and limitations when using CA-based certificates

The following requirements and limitations apply to the use of CA-based Unified certificates.

Requirements

- The certificate authority device must be a Unified PC.
- Users need local Administrator rights to start WinCC Unified Certificate Manager.

Limitations

- Use of an external certificate authority is not possible.
- The certificate authority and certificates must be created with Certificate Manager.
- The CA infrastructure includes the root with the root certificate and the end-entities with the application certificates. Use of intermediate certificates (intermediate CAs) is not possible.
- The root certificate has a maximum lifetime of 150 months.
- Application certificates become invalid when their root certificate expires.
- Runtime Collaboration requires that the Collaboration certificates of 2 Collaboration partners be created with a certificate authority device whose installed Runtime version is equal to or higher than the installed Runtime version of the Collaboration partner with the higher Runtime version.
  For this reason, the upgrading of Collaboration devices requires the creation, distribution and installation of new Collaboration certificates.
  Example:
  - A Unified PC and a Unified Panel with Runtime version V17 are Collaboration partners.
  - You upgrade the Panel to V18.
  - Create new Collaboration certificates for both HMI devices on a certificate authority device with installed Runtime version V18 or higher. Distribute them to and install them on the devices.

6.7.2 Basics of CA-based communication

Note

This user help assumes that, in the case of mutual SSL authentication, both devices use the same type of certificate authority.

A mixed use is technically also possible.

Certificate authorities

CA-based certificates are issued by a certificate authority (CA). The certificate authority can be an independent organization or a recognized service provider. Companies themselves can also act as certificate authority. They themselves then issue certificates, for example, for company-internal communication or for communication with partners or customers.

By signing the application certificate, the certificate authority guarantees the authenticity of the certificate and, thus, the identity of its owner (subject).

For use of CA-based Unified certificates, you need a Unified certificate authority. See section Unified certificate authority (Page 505).

Establishing the trust relationship in CA-based communication

When a device trusts the root certificate of a certificate authority, it automatically trusts all application certificates issued by this certificate authority.

Communication using public and private keys

When CA-based certificates are used, communication takes place using public and private keys

- A certificate authority has a private key and a public key.
  - The certificate authority signs the certificates it issues. It uses the private key for this. The signature guarantees that the certificate was really issued by the certificate authority. The private key remains secret. It is known only to the certificate authority.
  - The public key is the root certificate.
    When a device trusts the root certificate, it trusts all application certificates that were signed with the private key of the certificate authority.
- The certificate authority issues a CA-based application certificate for a device on request.
  - It binds the certificate to the device. See also section Device binding of a certificate (Page 486).
  - It signs the application certificate with its private key.
  - It creates a private key and a public key for the application certificate.
    These keys are used later to encrypt the communication between the device and its communication partners.
- The device must install the application certificate in its certificate store in the folder containing the own certificates.
- In the case of one-way SSL authentication, you establish the trust relationship between the communication partner and the device by exporting the root certificate of the application certificate and installing it on the communication partner in the folder containing the trusted certificate authorities.
- When the device establishes a connection to the communication partner, it transfers the public key of its application certificate. The communication partner checks the following:
  - The signature of the application certificate belongs to one of the certificate authorities it trusts.
  - The sender of the certificate is identical to the device to which the certificate is bound.

  If this is the case, the communication partner automatically installs the application certificate in its certificate store in the folder with trusted certificates.
- The communication partner generates a session key, encrypts it with the public key of the application certificate and sends it to the device.
- The device decrypts the session key with the private key of its application certificate.
- The device and the communication partner then use this session key to encrypt and decrypt their communication.

In the case of mutual SSL authentication, the device must also trust the root certificate of its communication partner.

Use of CA-based Unified certificates

You create and install the CA-based application certificates of an HMI device using WinCC Unified Certificate Manager.

The communication between the HMI device and its communication partners takes place as described above.

The following applies:

- Issuing application certificates, distributing them to the HMI device and installing them there: procedure depends on the communication partners of the device (web clients, OPC UA communication partners, etc.).
- Establishing the trust relationship between an HMI device and its communication partner: procedure depends on the communication partner (web client, OPC UA communication partner, etc.).
- When you use WinCC Unified Certificate Manager to install all certificates of an HMI device together or a single application certificate, the root certificate of the issuing certificate authority is automatically also installed on the HMI device:
  - In the certificate store of WinCC Unified
  - For Unified PCs: In the Windows system certificate store

  If the HMI device has a communication partner whose application certificate has the same certificate authority, the HMI device trusts this certificate automatically.

See also

Requirements and limitations when using CA-based certificates (Page 502)

Managing third-party certificates of a Unified PC (Page 499)

Selecting a suitable certificate type (Page 493)

Workflow for using CA-based certificates (Page 507)

Creating and exporting the CA infrastructure (Page 519)

Importing and installing certificates of a Unified PC (Page 538)

Importing and installing certificates of a Unified Panel (Page 541)

Trusting CA-based certificates (Page 543)

6.7.3 Unified certificate authority

For use of CA-based Unified certificates, you need a Unified certificate authority.

Note

The use of an external certificate authority to create CA-based Unified certificates is not supported.

Creating the Unified certificate authority

You create the certificate authority on a PC with a Unified Runtime installation using the WinCC Unified Certificate Manager tool.

Infrastructure of the Unified certificate authority

The infrastructure of the Unified certificate authority includes the following:

- Root (Root CA)
  The root includes the following:
  - Private key
    The private key is not visible in the user interface of Certificate Manager.
  - Root certificate (public key / CA certificate)
    The root certificate is the highest visible node of the certificate authority in the user interface of Certificate Manager.
  - CRL file (Certificate Revocation List)
    The CRL file contains a list of the certificates that the certificate authority has issued and then revoked.
- Devices for which you issue CA-based certificates
  These are usually HMI devices. When general certificates are used, they can also be other devices.
- Certificates (end-entities/leaf certificates) of the devices
  For HMI devices you create application certificates and, if applicable, general certificates. For devices that are not HMI devices, you create only general certificates.
  The certificates are located under the device nodes in the user interface of Certificate Manager.

Note

Configuration Manager does not support intermediate certificates (intermediate CAs).

CA container of the certificate authority

The CA container (certificate authority container) of a Unified certificate authority includes the following:

- Root certificate
- CRL file
- Application certificates and general certificates of the added devices

Complete configuration of the certificate authority

The complete configuration of a Unified certificate authority includes the following:

- Private key
- Root certificate (public key)

- CRL file
- Application certificates and general certificates of the added devices

See also

Basics of CA-based communication (Page 503)

Creating a certificate authority and root certificate (Page 519)

Selecting a suitable certificate type (Page 493)

WinCC Unified Certificate Manager (Page 554)

6.7.4 Workflow for using CA-based certificates

6.7.4.1 First-time use of CA-based certificates

Follow the procedure described in this section if you do not have a Unified certificate authority yet and want to use CA-based Unified certificates on HMI devices.

You can find information on how to use general CA-based certificates in section Using general certificates (Page 548).

Note

This description assumes that both the HMI devices and their communication partners are using CA-based application certificates.

Requirement

- WinCC Unified Runtime is installed on the PC that is to serve as the certificate authority (certificate authority device).
- The required CA-based application certificates have been issued for the communication partners.
  To create these certificates, follow the procedure described in the user help of the respective communication partner.
- The root certificate and CRL file of the certificate authority that issued the application certificates of the communication partners have been exported as described in the user help of the respective communication partner. You have access to both files.
- For communication with an S7 controller:
  – The controller has the following firmware:
    S7-1500: Firmware 2.9 or higher
    S7-1200: Firmware 4.5 or higher
  – The HMI device has an integrated connection to the controller.
  – Secure communication was enabled for the controller in the Engineering System

Procedure

1. Create the certificate authority and its CA infrastructure (HMI devices and their application certificates) on the certificate authority device.
2. Export the certificates of the HMI devices.
3. Import the certificates of the HMI device to each HMI device and install them there.
4. If you install the certificates of an HMI device at runtime, restart Runtime on the device.

   Note

   Existing connections are not interrupted by the installation of certificates. Runtime uses the old certificates until it is restarted.

   A Runtime restart is not required for use of a newly installed web server certificate.

5. Establish the trust relationship between the HMI device and its communication partners for each HMI device.

Follow the procedure described below.

Note

Certificate authority device as HMI device

If you are using the certificate authority device as a Unified PC and you only want to provide the application certificates of this PC, the export and import steps are omitted. You can install the certificates of the PC without exporting and importing them beforehand.

Creating the certificate authority and CA infrastructure

1. Start the Certificate Manager tool on the certificate authority device.
2. Create the certificate authority.
   See section Creating a certificate authority and root certificate (Page 519).
3. Add the needed HMI devices to the certificate authority.
   See section Adding devices (Page 521).
4. Add the needed application certificates to each HMI device.
   See section Add application certificates (Page 524).
5. (optional) Create a backup of the complete configuration of the certificate authority
   See section Create backup (Page 537).

Note

You can change the infrastructure of your system later, for example, as follows:

- Add or delete application certificates to or from an HMI device.
- Add or delete HMI devices.
- Renew application certificates whose lifetime has expired.
- Renew an expired root certificate or its CRL file.

See section Continued use of CA-based certificates (Page 513).

Exporting certificates of HMI devices

The export of certificates sets up their installation on the HMI devices.

Follow these steps:

- For Unified PCs: Export the CA container once.
  The certificates of all devices of the certificate authority are exported to a common storage file.
  When the file is imported to a Unified PC, you see the certificates of all devices of the certificate authority. However, you can only install the certificates of the local device. The other devices are shown for information purposes only.

  Note

  If a small storage file is needed to save memory space, you can also export the certificates of a single Unified PC. Then, all certificates of the selected PC are exported to the storage files.

  See section Exporting certificates of a Unified PC (Page 528).
- For Unified Panels: Export the certificates of a single Unified Panel. All certificates of the selected Panel are exported to the storage files.
  Repeat this action for all Panels.

  Note

  A joint export of the certificates of all devices of the certificate authority is not possible.

  See section Exporting certificates of a Panel (Page 530).

Importing and installing certificates

Import the certificates to the HMI devices and install them there:

- For Unified PCs: See sections Importing certificates of a Unified PC (Page 538) and Installing all certificates or single certificates of a PC (Page 539).
- For Unified Panels: See sections Importing and installing certificates of a Panel (Page 541) and Manually importing and individual certificates to a Panel and installing them (Page 542).

Establishing the trust relationship

Note

If the following conditions are met, no further steps are needed to establish the trust relationship:

- The HMI devices of the certificate authority communicate only with each other and with S7 controllers to which they have an integrated connection.
- The HMI devices communicate with each other exclusively using CA-based certificates of their common certificate authority.
- The certificates of the HMI devices have been installed on the devices.
- For web server communication, you use only the following web clients:
  - Edge and Chrome on Unified PCs that belong to the infrastructure of the certificate authority
  - Web browser of Unified Panels that belong to the infrastructure of the certificate authority

1. Export the Unified root certificate and the CRL file on the certificate authority device using Certificate Manager.
   See section Exporting root certificate and CRL file (Page 531).

   Note

   Alternative approach for Unified PCs

   If one of the HMI devices is a Unified PC whose certificates were already installed with Certificate Manager, you can also export both files on the Unified PC with SIMATIC Runtime Manager.

   See also section Managing third-party certificates of a Unified PC (Page 499).

2. Install the Unified root certificate on the communication partners of the HMI devices:

Communication partner	Procedure
Web client of a Runtime web server	Follow the procedure described in section Trusting the web server certificate (Page 543) for the respective web client.
OPC UA device	Follow the procedure described in the user help of the respective OPC UA communication partner.
Runtime Collaboration device	If the Collaboration devices have different Unified certificate authorities, install the root certificate and CRL file of one device on the other, and vice versa. For Panels, follow the procedure described in section Importing and installing root certificates and CRL files on Panels (Page 545). For PCs, follow the procedure described in section Managing third-party certificates of a Unified PC (Page 499). If the devices have the same Unified certificate authority, the devices trust each other automatically.
S7 controller	Not applicable

Note

If the same communication partner communicates with multiple HMI devices that have the same certificate authority, install the root certificate on the communication partner once.

It is not necessary to manually install the root certificate in some following cases: You will find information on this in the following sections:

- Automatic trust relationship with a PC web server (Page 438)
- Automatic trust relationship with a Panel web server (Page 387)
- Automatic trust relationship in OPC UA communication (Page 422)
- Automatic trust relationship between Collaboration devices (Page 380)

Where appropriate, check whether the root certificate has already been installed on the communication partner:

- Web client as communication partner: See section Checking the status of the web server root certificate on the web client. (Page 437).
- Runtime Collaboration communication partner: See section Checking the status of a root certificate on the HMI device (Page 544).
- Remaining communication partners: Follow the procedure described in the user help of the respective communication partner.

3. Install the root certificates of the communication partners on each HMI device:

Communication partner	Procedure on the HMI device
Web client	Not applicable
Runtime Collaboration device	If the Collaboration devices have different Unified certificate authorities, install the root certificate and CRL file of one device on the other, and vice versa. For Panels, follow the procedure described in section Importing and installing root certificates and CRL files on Panels (Page 545). For PCs, follow the procedure described in section Managing third-party certificates of a Unified PC (Page 499). If the devices have the same Unified certificate authority, the devices trust each other automatically.
OPC UA device	Follow the procedure described in section Trusting OPC UA certificates (Page 543).
S7 controller	No action is necessary. See section Communication with S7-1500 and S7-1200 (Page 487).

Note

If the HMI device has multiple communication partners of the same certificate authority, install the root certificate on the HMI device once.

Note

Establishment of a trust relationship is not required to use Audit Trail on an HMI device.

See also

Recreation of certificates (Page 534)

Trusting CA-based certificates (Page 543)

6.7.4.2 Continued use of CA-based certificates

Introduction

If you are using security-related Unified components on the HMI devices of your system, you must provide the following certificates:

- Certificates used by the HMI devices to authenticate themselves to their communication partners (Unified certificates)
- Certificates used by the communication partners of the HMI devices to authenticate themselves to the HMI devices (third-party certificates)

Follow the procedure described in this section if you are already using CA-based Unified certificates and the infrastructure of your system changes, for example, because application certificates or HMI device had to be added or deleted or certificates had to be renewed.

You can find information on how to use general CA-based certificates in section Using general certificates (Page 548).

Note

This description assumes that both the HMI devices and their communication partners are using CA-based application certificates.

Note

Some components require a mutual SSL authentication, meaning that both the HMI device and its communication partner need a certificate. They must trust each other's certificates.

Other components require a one-way SSL authentication, meaning that only the HMI device needs a certificate and its communication partner must trust the certificate, or vice versa.

See also section Determining the required application certificates (Page 492).

Requirement

- A certificate authority with the desired infrastructure has been created on the certificate authority device using WinCC Unified Certificate Manager.
- The required CA-based application certificates have been issued for the communication partners.
  To create these certificates, follow the procedure described in the user help of the respective communication partner.
- The root certificate and CRL file of the certificate authority that issued the application certificates of the communication partners have been exported as described in the user help of the respective communication partner. You have access to both files.
- For communication with an S7 controller:
  - The controller has the following firmware:
    S7-1500: Firmware 2.9 or higher
    S7-1200: Firmware 4.5 or higher
  - The HMI device has an integrated connection to the controller.
  - Secure communication was enabled for the controller in the Engineering System

Procedure

1. Start Certificate Manager on the certificate authority device.
2. Change the CA infrastructure as needed, for example, by adding or deleting devices and certificates.
3. Export the certificates of the HMI devices.
4. Import the certificates of the HMI device to each HMI device for which you made changes and install them there.
5. If you install the certificates of an HMI device at runtime, restart Runtime on the device.

   Note

   Existing connections are not interrupted by the installation of certificates. Runtime uses the old certificates until it is restarted.

   A Runtime restart is not required for use of a newly installed web server certificate.

6. Establish the trust relationship between the HMI devices and their communication partners for the newly added or renewed certificates.

Follow the procedure described below.

Note

Certificate authority device as HMI device

If you are using the certificate authority device as a Unified PC and you only want to provide the application certificates of this PC, the export and import steps are omitted. You can install the certificates of the PC without exporting and importing them beforehand.

Changing the CA infrastructure of the certificate authority

1. Change the infrastructure of the certificate authority as needed.
   You have the following options:
   - Add new devices and their application certificates.
     See sections Adding devices (Page 521) and Add application certificates (Page 524).
   - Edit the certificates of an existing device, for example, by adding a new application certificate or renewing or deleting an existing application certificate.
     See sections Add application certificates (Page 524), Deleting application certificates (Page 526) and Recreating a certificate (Page 534).
   - Delete devices.
     See section Deleting devices (Page 524).
   - Renew the CRL file on expiration
     See section Updating a CRL file (Page 536).
   - To renew an expiring root certificate, recreate the complete configuration of the certificate authority (root certificate, CRL file and certificates of all devices).
     See section Recreating the entire configuration (Page 535).
2. Optional: Back up the certificate authority.

Exporting certificates of HMI devices

Export the certificates of newly added or changed HMI devices. The export sets up their installation on the HMI device.

Follow these steps:

- For Unified PCs: Export the CA container once.
  The certificates of all devices of the certificate authority are exported to a common storage file.
  When the certificates are imported to a Unified PC, you see the certificates of all devices of the certificate authority. However, you can only install the certificates of the local device. The other devices are shown for information purposes only.

  Note

  If a small storage file is needed to save memory space, you can also export the certificates of a single Unified PC. Then, all certificates of the selected PC are exported to the storage files.

  See section Exporting certificates of a Unified PC (Page 528).
- For Unified Panels: Export the certificates of a single Unified Panel. All certificates of the selected Panel are exported to the storage files.
  Repeat this action for all Panels whose certificate configuration was changed.

  Note

  A joint export of the certificates of all devices of the certificate authority is not possible.

  See section Exporting certificates of a Panel (Page 530).

Importing and installing certificates

Import the certificates to the HMI devices whose configuration you changed in Certificate Manager and install them there:

- For Unified PCs: See sections Importing certificates of a Unified PC (Page 538) and Installing all certificates or single certificates of a PC (Page 539).
- For Unified Panels: See sections Importing and installing certificates of a Panel (Page 541) and Manually importing and individual certificates to a Panel and installing them (Page 542).

Establishing the trust relationship

You establish the trust relationship for the following:

- HMI devices you have newly added
- HMI devices for which you added a new certificate or renewed or deleted an existing certificate
- If you recreated the configuration of the certificate authority: all HMI devices

Note

If the following conditions are met, no further steps are needed to establish the trust relationship:

- The HMI devices of the certificate authority communicate only with each other and with S7 controllers to which they have an integrated connection.
- The certificates of the HMI devices have been installed on the devices.
- The HMI devices communicate with each other exclusively using CA-based certificates of their common certificate authority.
- For web server communication, you use only the following web clients:
  - Edge and Chrome on Unified PCs that belong to the infrastructure of the certificate authority
  - Web browser of Unified Panels that belong to the infrastructure of the certificate authority

Follow these steps:

1. (optional) Create a list of the communication partners of these HMI devices.
2. Export the Unified root certificate and the CRL file on the certificate authority device using Certificate Manager.
   See section Exporting root certificate and CRL file (Page 531).

   Note

   Alternative approach for Unified PCs

   If one of the HMI devices is a Unified PC whose certificates were already installed with Certificate Manager, you can also export both files on the Unified PC with SIMATIC Runtime Manager.

   See also section Managing third-party certificates of a Unified PC (Page 499).

3. Install the Unified root certificate on the communication partners of the HMI devices:

Communication partner	Procedure on the communication partner
Web client	Follow the procedure described in section Trusting the web server certificate (Page 543) for the respective web client.
OPC UA device	Follow the procedure described in the user help of the respective OPC UA communication partner.
Runtime Collaboration device	If the Collaboration devices have different Unified certificate authorities, install the root certificate and CRL file of one device on the other, and vice versa. For Panels, follow the procedure described in section Importing and installing root certificates and CRL files on Panels (Page 545). For PCs, follow the procedure described in section Managing third-party certificates of a Unified PC (Page 499). If the devices have the same Unified certificate authority, the devices trust each other automatically.
S7 controller	Not applicable

Note

If the same communication partner communicates with multiple HMI devices that have the same certificate authority, install the root certificate on the communication partner once.

It is not necessary to manually install the root certificate in some following cases: You can find more information on this in the following sections:

- Automatic trust relationship with a PC web server (Page 438)
- Automatic trust relationship with a Panel web server (Page 387)
- Automatic trust relationship in OPC UA communication (Page 422)
- Automatic trust relationship between Collaboration devices (Page 380)

Where appropriate, check whether the root certificate has already been installed on the communication partner:

- Web client as communication partner: See section Checking the status of the web server root certificate on the web client. (Page 386).
- Runtime Collaboration communication partner: See section Checking the status of a root certificate on the HMI device (Page 544).
- Remaining communication partners: Follow the procedure described in the user help of the respective communication partner.

4. Install the root certificates of the communication partners on each HMI device:

Communication partner	Procedure on the HMI device
Web client	Not applicable
Runtime Collaboration device	If the Collaboration devices have different Unified certificate authorities, install the root certificate and CRL file of one device on the other, and vice versa. For Panels, follow the procedure described in section Importing and installing root certificates and CRL files on Panels (Page 545). For PCs, follow the procedure described in section Managing third-party certificates of a Unified PC (Page 499). If the devices have the same Unified certificate authority, the devices trust each other automatically.
OPC UA device	Follow the procedure described in section Trusting OPC UA certificates (Page 543).
S7 controller	No action is necessary. See section Communication with S7-1500 and S7-1200 (Page 487).

Note

If the HMI device has multiple communication partners of the same certificate authority, install the root certificate on the HMI device once.

Note

Establishment of a trust relationship is not required to use Audit Trail on an HMI device.

See also

Create backup (Page 537)

Trusting CA-based certificates (Page 543)

Creating a certificate authority and root certificate (Page 519)

6.7.5 Creating and exporting the CA infrastructure

6.7.5.1 Creating a certificate authority and root certificate

Normally, you issue the CA-based certificates of the HMI devices of a system or subsystem with the same Unified certificate authority.

Note

Use of an external certificate authority is not possible. The Unified certificate authority and its certificates must be created with WinCC Unified Certificate Manager.

Requirement

A certificate authority has not yet been created on the certificate authority device with Certificate Manager.

Procedure

1. Decide which Unified PC in your network is to be the certificate authority device.
2. Open WinCC Unified Certificate Manager on this device.
3. Select the "CA configuration" tab.
4. In the work area, double-click "Create new certificate authority".
5. Enter the properties of the root certificate in the "New certificate authority" dialog.
   - "General" tab
     The general properties of the new certificate authority, e.g. name, name of organization
     Mandatory field: "Name"
   - "Security" tab
     Security-related properties of the new certificate authority, such as key size and lifetime.
     If necessary, select a different key size and lifetime for the certificate.
     Mandatory fields: Password fields for the private key
6. Click "Create".

Result

- The private key is generated.
- The root certificate is generated.
- An empty CRL (Certificate Revocation List) file is generated.
- In the "CA configuration" tab, a node for the root certificate is created and below it one for the CRL file.

Note

The private key is only available on the certificate authority device. The certificate authority uses it to sign the application certificates of the Unified devices. It is not visible in the user interface of Certificate Manager.

Next steps

- Create the CA infrastructure. To do this, add the Unified devices to the certificate authority and create their application certificates.

  Note

  If there are changes to the infrastructure of your system later, such as addition of HMI devices, adapt the infrastructure of the certificate authority as needed.

- To distribute the Unified root certificate and its CRL file without distributing the certificates of the devices, for example, to external communication partners, export them individually.

Deleting certificate authority and root certificate

NOTICE

Data loss prevention

Delete the certificate authority and root certificate only in the following cases:

- After you have saved the data of the certificate authority.
- When you no longer need the certificate authority and its data.

Procedure

1. Open Certificate Manager on the certificate authority device.
2. Select the "CA configuration" tab.
3. Click the root certificate on the left and select "Delete".

Result

The certificate authority and all its data are deleted from the certificate authority device.

Note

If the certificates were already installed on the HMI devices, they are still installed there. Delete them from the devices if necessary.

See also

Opening Certificate Manager (Page 554)

Password requirements (Page 563)

Adding devices (Page 521)

Add application certificates (Page 524)

Exporting root certificate and CRL file (Page 531)

6.7.5.2 Adding devices

Requirement

A certificate authority has been created on the certificate authority device in WinCC Unified Certificate Manager.

Procedure

1. On the certificate authority device, open Certificate Manager.
2. Select the "CA configuration" tab.
   You see the root certificate and its CRL file, as well as all the devices that have already been added and their application certificates.

3. Right-click the root certificate and select "Add device ...".
4. In the "New device" dialog, enter the device name, the IP address of the device, or both.
   For devices in a domain, enter the fully qualified domain name (FQDN) or IP address of the device, or both.
   The application certificates of the device are bound to the device using the information.
   You can no longer change your entries afterward.

Note

Recommendation

Enter the device name/FQDN and IP address.

For devices with dynamic IP addresses, use the FQDN.

Note

Allowed device names

The use of the name "localhost" is not allowed and will be automatically replaced by Certificate Manager with the device name of the local device.

Specific characteristics	Mandatory information	Optional additional information (recommended)
The HMI device operates as a web server, and the identity provider and Unified Runtime website are addressed using the IP address.	IP address If the IP address is missing, a validation error occurs when accessing the Runtime web page.	Device name or FQDN
HMI device operates as an OPC UA server (OPC UA server certificate, OPC UA exporter certificate)	Device name or FQDN	IP address

Result

A node for the device is generated in the "CA configuration" tab.

Icons of the device nodes:

🟩	The local machine (if added)
⬛	Other devices

Next step

Create the application certificates of the added device.

Changing the device binding of the certificates

When adding a device, you define how the application certificates are bound to the device. To change your definition, follow these steps:

1. Delete the HMI device from the certificate authority.
2. Add the HMI device again, this time using the desired definition.
3. Add the needed application certificates to the HMI device.
4. Export the certificates of the HMI device.
5. Install the certificates on the HMI device.
6. Uninstall the certificates with the outdated device binding:
   – On a Unified PC: See section Managing own certificates of a Unified PC (Page 498).
   – On a Unified Panel: See section Managing third party certificates and own certificates of a Unified Panel (Page 496).

Handling a device after a change of IP address or computer name

If the IP address or computer name of a device added in Certificate Manager was changed subsequently, follow these steps:

1. Delete the device from the certificate authority.
2. Create it again, this time with the new IP address and/or new computer name.
3. Add the needed application certificates to the HMI device.
4. Export the certificates of the HMI device.
5. Install the certificates on the HMI device.
6. Uninstall the certificates with the outdated device binding:
   – On a Unified PC: See section Managing own certificates of a Unified PC (Page 498).
   – On a Unified Panel: See section Managing third party certificates and own certificates of a Unified Panel (Page 496).

See also

Opening Certificate Manager (Page 554)

Creating a certificate authority and root certificate (Page 519)

Add application certificates (Page 524)

Deleting devices (Page 524)

Device binding of a certificate (Page 486)

6.7.5.3 Deleting devices

Requirement

A device has been added to the certificate authority.

Procedure

1. Right-click on the device.
2. Select "Delete".
3. Confirm your selection.

Result

The device and its application certificates are deleted from the certificate authority.

Note

The certificates installed on the HMI device are not deleted. If necessary, delete the certificates from the device, as well:

- On a Unified PC: See section Managing own certificates of a Unified PC (Page 498).
- On a Unified Panel: See section Managing third party certificates and own certificates of a Unified Panel (Page 496).

See also

Adding devices (Page 521)

Opening Certificate Manager (Page 554)

6.7.5.4 Add application certificates

This section describes how to add application certificates to HMI devices. For information on adding general certificates, see section Using general certificates (Page 548).

Requirement

An HMI device has been added to the certificate authority in Certificate Manager.

Procedure

1. On the certificate authority device, open Certificate Manager.
2. Select the "CA configuration" tab.
3. Right-click on the device and select "Add Certificate > <Certificate type> ... "

4. Enter the properties of the certificate in the "New certificate" dialog.
   - "General" tab
     The general properties of the new certificate, e.g. name of organization
     Mandatory field for the "Web server" certificate: "Name" field

     Note

     Use the "Fully qualified domain name" as name for web server certificates.

   - "Security" tab
     Security-related properties of the new certificate, e.g. key length and lifetime.
     If necessary, select a different key size and lifetime for the certificate.

     Note

     Runtime

     For web server certificates, the runtime is limited to a maximum of 27 months. Longer runtimes are not accepted by some browsers.

   Some fields are write-protected. The properties you can edit on the tabs depend on the certificate type.
5. Click "OK".
6. Repeat steps 3 through 5 until the device has the needed application certificates.

Result

The application certificates of the device have been configured.

Next step

Export the certificates.

Note

If you are using the certificate authority device as a Unified PC and you only want to provide the application certificates of this PC, the export and import steps are omitted. You can install the certificates of the PC without exporting and importing them beforehand.

Other options

You can create a new application certificate, for example, because it has reached the end of its lifetime.

You can export an application certificate as a public certificate.

You can export the root certificate to distribute it to the communication partners.

See also

Deleting application certificates (Page 526)

Recreating a certificate (Page 534)

Exporting an application certificate as a public certificate (Page 546)

Opening Certificate Manager (Page 554)

6.7.5.5 Deleting application certificates

Requirement

The certificate authority has a device with an application certificate.

Procedure

1. On the certificate authority device, open Certificate Manager.
2. Select the "CA configuration" tab.
3. Right-click on the application certificate under the desired device.
4. Select "Delete".
5. Confirm your selection.

Deleting the application certificate

The application certificate is deleted.

Note

The certificates installed on the device are not deleted.

If necessary, delete the certificate from the device. On a Unified PC, you use Certificate Manager to do this. On a Unified Panel, you use the "Security > Certificates" function in the Control Panel.

See also

Add application certificates (Page 524)

Opening Certificate Manager (Page 554)

Managing own certificates of a Unified PC (Page 498)

Managing third party certificates and own certificates of a Unified Panel (Page 496)

6.7.5.6 Export options

Overview

The following table provides an overview of which export options WinCC Unified Certificate Manager offers and how to use them:

Option	**Use**	**Available on the certificate authority device**	**Available on a Unified PC target device**
Export the CA container	To provide the certificates of one or more Unified PCs	✓	-
Export the certificates of a device	To provide the certificates of a single Unified Panel Can also be used to provide the certificates of a single Unified PC.	✓	-
Export a single application certificate	To provide it as a public certificate	✓	✓
Export the root certificate and CRL file	To establish the trust relationship between a Unified device and its communication partners To provide an updated CRL file	✓	-
Export the complete configuration of the certificate authority	To back up data of the certificate authority	✓	-

Exporting a general certificate

The following table provides an overview of the export options offered by WinCC Unified Certificate Manager and how to use them:

Option	**Use**	**Available on the certificate authority device**	**Available on a Unified PC (PC as communication partner)**
Export the public key	To provide it as a public certificate	✓	✓
Export the private key and public key	As preparation for installing the general certificate on the device for which the certificate was issued	✓	-

6.7.5.7 Exporting certificates of a Unified PC

Introduction

This step sets up the import and installation of application certificates of the Unified PC on the PC as well as the root certificate of the issuing certificate authority and its CRL file.

Note

General certificates are exported and imported and installed separately. See section Using general certificates (Page 548).

Use cases

You export certificates in the following cases:

- After adding the device and configuring its application certificates for the first time
- When you change the certificates configured for the PC on the certificate authority device after the certificates were installed on the PC, for example, by adding, deleting or recreating application certificates
- After recreation of the complete configuration of the certificate authority (for example, due to expiration of the root certificate)
- After updating the CRL file

  Note

  If you only want to update the CRL file, an export is not mandatory. You can also export the CRL file individually and import it to the PC using SIMATIC Runtime Manager.

  See section Exporting root certificate and CRL file (Page 531) and section Managing third-party certificates of a Unified PC (Page 499).

Note

If you are using the certificate authority device as a Unified PC and you only want to provide the application certificates of this PC, the export and import steps are omitted. You can install the certificates of the PC without exporting and importing them beforehand.

Export options

You have the following options:

- Export CA container
  The certificates of all devices of the certificate authority are written to a common export file.
- Export device
  The export file contains only the certificates of the selected Unified PC.

In both cases, you can only install the certificates of this PC on the Unified PC.

Tip for an efficient procedure

Recommended procedure:

- If you have changed the certificates of multiple devices, export the CA container.
- If you have changed the certificates of a single Unified PC, export the certificates of this device.

Requirement

The certificates of the Unified PC have been configured on the certificate authority device.

Procedure

1. On the certificate authority device, open Certificate Manager.
2. Select the "CA configuration" tab.
3. Follow these steps:
   To export the certificates of all devices:
   – Right-click on the root certificate.
   – Select "Export > CA Container".

   To export only the certificates of the Unified PC:
   – Right-click on the Unified PC.
   – Select "Export device > To PC".
4. In the dialog that opens, enter and repeat a password to protect the export file.
   See also section Password requirements (Page 563).
5. Click "Export".
6. Click on "Save" and select the storage location and the file name.

Result

The root certificate, CRL file and certificates of the Unified PC or all devices are stored encrypted with the specified password in a secure storage file.

Next step

Import the certificates of the PC to the PC and install them.

See also

Importing certificates of a Unified PC (Page 538)

Opening Certificate Manager (Page 554)

6.7.5.8 Exporting certificates of a Panel

Introduction

This step sets up the import and installation of application certificates of the Unified Panel on the Panel as well as the root certificate of the issuing certificate authority and its CRL file.

Note

General certificates are exported and imported and installed separately. See section Using general certificates (Page 548).

Use cases

You export certificates in the following cases:

- After adding the device and configuring its application certificates for the first time
- When you change the certificates configured for the Panel on the certificate authority device after the certificates were installed on the Panel, for example, by adding, deleting or creating new application certificates
- After recreation of the complete configuration of the certificate authority (for example, due to expiration of the root certificate)
- After updating the CRL file

  Note

  Alternatively, you can also export the CRL file individually. See section Exporting root certificate and CRL file (Page 531). Then import it using the "Security > Certificates" function in the Control Panel of the Unified Panel.

Requirement

The certificates of the Panel have been configured on the certificate authority device.

Procedure

1. Open WinCC Unified Certificate Manager on the certificate authority device.
2. Select the "CA configuration" tab.
3. Right-click on the desired Panel.
4. Select "Export device > To Panel".
5. In the dialog that opens, enter and repeat a password to protect the export file.
   See also section Password requirements (Page 563).
6. (Optional) Adjust the number of iterations for the encryption.
7. Click "Export".

8. Select the file path and file name and click "Save".

   Note

   Do not use spaces or special characters, such as "/", that the Panel might interpret as a command during the import.

   The data is stored in a TAR log and encrypted with the password.
9. Copy the TAR log to an external storage medium.

Next step

Import the certificates to the device and install them.

See also

Opening Certificate Manager (Page 554)

Managing third party certificates and own certificates of a Unified Panel (Page 496)

6.7.5.9 Exporting root certificate and CRL file

Introduction

You can export and distribute the root certificate and CRL file separately from the certificates of devices as a public certificate with Certificate Manager. This is necessary in the following cases, for example:

- To establish the trust relationship between an HMI device and its communication partners
- To update an expired CRL file

You can select between the following options:

- Exporting root certificate and CRL file
- Exporting CRL file only

Note

Alternative approach for Unified PCs

If the HMI device is a PC on which the root certificate and its CRL file are already installed, you can also export both files with SIMATIC Runtime Manager.

See also section Managing third-party certificates of a Unified PC (Page 499).

Requirement

A certificate authority has been created on the certificate authority device in Certificate Manager.

Exporting root certificate and CRL file

1. On the certificate authority device, open Certificate Manager.
2. In the "CA configuration" tab, click the root certificate on the right.
3. Select "Export > CA Certificate ...".
4. Select a file format.
5. Confirm your entries.
6. Select a target folder.
7. Confirm your entries.

The root certificate and its CRL file are exported to the target folder, each to a separate file.

Export CRL file only

1. On the certificate authority device, open Certificate Manager.
2. Select the "CA configuration" tab.
3. Under the root certificate, right-click the Certificate Revocation list.
4. Select "Export".
5. Select a file format.
6. Confirm your entries.
7. Select a target folder.
8. Confirm your entries.

The CRL file is exported to the target folder.

Distribute files

After the export, distribute the files to the target devices:

- For distribution to communication partners, follow the procedure described in the user help of the device.
- On a Unified PC you install the files with SIMATIC Runtime Manager.
- On a Unified Panel you install the files in the Control Panel under "Security > Certificates" using the "Import" function.

See also

Opening Certificate Manager (Page 554)

6.7.5.10 Exporting a single application certificate

With WinCC Unified Certificate Manager, you can export application certificates individually as public certificates.

Requirement

An application certificate has been added to a device in WinCC Unified Certificate Manager.

Exporting certificate to the certificate authority device

1. On the certificate authority device, open Certificate Manager.
2. Select the "CA configuration" tab.
3. Right-click on the application certificate under the device.
4. Select "Export certificate...".
5. Select a file format.
6. Confirm your entries.
7. Select a target folder.
8. Confirm your entries.

Export certificate on the device

Additional requirements

- The device is a unified PC.
- The application certificate has been installed on the device.

Procedure

1. On the Unified PC, open Certificate Manager.
2. Select the "Installed certificates" tab.
3. Right-click on the application certificate.
4. Select "Export certificate...".
5. Select a file format.
6. Confirm your entries.
7. Select a target folder.
8. Confirm your entries.

Result

The public key of the certificate is exported. Distribute it to the external communication partners of the device.

See also

Opening Certificate Manager (Page 554)

6.7.5.11 Recreation of certificates

Certificate Manager offers the option to recreate existing certificates.

You must recreate certificates in the following cases:

Expiration of an application certificate or a general certificate	Recreate the certificate.
Expiry of the root certificate	Recreate the entire configuration of the certificate authority.
Expiry of the CRL file	Update the CRL file.
Change to the IP address or the computer name of a Unified device[1]	Recreate the application certificates and general certificates of the device.

[1] For a Unified PC that is used as an HMI device as well as a certificate authority device: If you have changed the computer name or the IP address, recreate the entire configuration of the certificate authority. Distribute and install it.
When the certificate authority device is not used as an HMI device, there is no need to renew the certificate configuration.

See also

Recreating a certificate (Page 534)

Recreating the entire configuration (Page 535)

Updating a CRL file (Page 536)

6.7.5.12 Recreating a certificate

You recreate application certificates and general certificates in the following cases:

- The lifetime of a certificate has expired.
- Entries for a valid certificate are to be edited, for example to correct entries.
- The IP address or computer name of the device has been changed.

Procedure

1. Open WinCC Unified Certificate Manager on the certificate authority device.
2. Select the "CA configuration" tab.
3. Right-click on the certificate of the desired device and select "Recreate ...".
   The "New <description> certificate" dialog opens. The entries of the old certificate are downloaded into the dialog.
4. Change the desired properties.
5. Click "OK".

Result

A new certificate is created. Export the certificates of the device and install the certificate on the device.

See also

Add application certificates (Page 524)

Recreation of certificates (Page 534)

Opening Certificate Manager (Page 554)

Exporting certificates of a Unified PC (Page 528)

Exporting certificates of a Panel (Page 530)

Using general certificates (Page 548)

6.7.5.13 Recreating the entire configuration

The expiration of the root certificate requires that the entire configuration of the certificate authority is created again.

Requirement

A certificate authority has been created and configured on the certificate authority device in Certificate Manager.

Procedure

1. On the certificate authority device, open Certificate Manager.
2. Select the "CA configuration" tab.
   You will see the configuration of the certificate authority.
3. Right-click the root certificate and select "Recreate all".
4. The "Recreate certificate authority" dialog opens.
   The properties of the previous certificate authority are taken over as default. Change them if necessary.
5. Enter the same password as when you created the certificate authority and confirm it.
6. Click "Create".

Result

The configuration of the certificate authority is recreated:

- Private key
- Root certificate
- CRL file
- All devices and their certificates

Next steps

- Export the certificates of the devices. Import and install them on the devices.
- Distribute the root certificate and CRL file to the communication partners of the devices.

See also

Recreation of certificates (Page 534)

Opening Certificate Manager (Page 554)

6.7.5.14 Updating a CRL file

When the root certificate is created, the CRL file is given a lifetime of 24 months. When the lifetime expires, it is necessary to update the CRL file.

Requirement

A certificate authority has been created on the certificate authority device in Certificate Manager.

Procedure

1. On the certificate authority device, open Certificate Manager.
2. Select the "CA configuration" tab.
3. Under the root certificate, click the "Certificate Revocation List" node on the right.
4. Select "Update".

Result

A new CRL file with a lifetime of 24 months is created.

Next step

Distribute and install the CRL file to the target devices:

- On a Unified PC, you install the file with SIMATIC Runtime Manager. See section Managing third-party certificates of a Unified PC (Page 499).
- On a Unified Panel, you install the file in the Control Panel under "Security > Security" using the "Import" function. See section Managing third party certificates and own certificates of a Unified Panel (Page 496).
- For distribution to the communication partners, follow the procedure described in the user help of the device.

See also

Recreation of certificates (Page 534)

Exporting root certificate and CRL file (Page 531)

Opening Certificate Manager (Page 554)

6.7.5.15 Create backup

Procedure

To create a backup copy of all the data of the certificate authority, follow these steps:

1. Open Certificate Manager on the certificate authority device.
2. Select the "CA configuration" tab.
3. Right-click the root certificate and select "Export > Full backup".
4. To protect the backup file, enter a password and repeat it in the "Export" dialog.
   See also section Password requirements (Page 537).
5. Click "Export".
6. Select a storage location and file name and click "Export".

Result

The entire configuration of the certificate authority is written to a backup file.

Loading the backup

1. Open Certificate Manager.
2. In the "CA configuration" tab, double-click the "Open configuration ..." entry.
3. Select the backup file and confirm with "Open".
4. Enter the password set when creating the backup and confirm with "Open".

See also

Recreation of certificates (Page 534)

Opening Certificate Manager (Page 554)

6.7.5.16 Password requirements

The passwords defined in the Certificate Manager must meet the following requirements:

- Length: At least 8 characters
- In each case at least one uppercase letter, one lowercase letter, one number and one special character

6.7.6 Importing and installing certificates of a Unified PC

6.7.6.1 Importing certificates of a Unified PC

Introduction

The import sets up the installation of CA-based own application certificates on the Unified PC as well as the root certificate of the issuing certificate authority and its CRL file.

Note

General certificates are exported and imported and installed separately. See section Using general certificates (Page 548).

Note

If you are using the certificate authority device as a Unified PC and you only want to provide the application certificates of this PC, no import is necessary. You can install the certificates of the PC without exporting and importing them beforehand.

Requirement

- The CA container or the certificates of the Unified PC have been exported on the certificate authority device.
- The PC has access to the storage location of the export file.

Procedure

1. Open WinCC Unified Certificate Manager on the PC.
2. Select the "CA configuration" tab.
3. Double-click "Open configuration ...".
4. Select the export file.
5. Enter the password selected during export.
6. Confirm your entries.

Result

The configuration file is loaded to the "CA configuration" tab. What you see on the tab after loading depends on the selected export option:

- CA container exported:
  You see the complete infrastructure of the certificate authority, except for the private key. You can only install the application certificates of the local device. The other devices and their certificates and the general certificates are shown for information purposes only.
- Certificates of the device exported:
  You see the root certificate and its CRL file, as well as the certificates of the local device. The general certificates of the device are shown for information purposes only. You cannot install these certificates.

Exiting Certificate Manager closes the loaded configuration.

Next step

Install the certificates on the device.

See also

Opening Certificate Manager (Page 554)

6.7.6.2 Installing all certificates or single certificates of a PC

You can choose between the following:

- Install all certificates of the Unified PC as well as the root certificate and CRL file.

  Note

  General certificates are exported and imported and installed separately. See section Using general certificates (Page 548).

  On Unified PCs, you also see the general certificates in WinCC Unified Certificate Manager after importing a configuration file. This is for information purposes only. You cannot install the general certificates with Certificate Manager.

- Install a single application certificate.
  Root certificate and CRL file are automatically also installed.

Requirement

- Certificate Manager is open on the PC on which you want to install the certificates.
- The certificates of the PC have been imported to the device using Certificate Manager.

Procedure

1. Select the "CA configuration" tab.
2. Select one of the following options:
   To install all certificates of the PC:
   - Right-click the node of the local machine.
     The local machine has the following icon:
   - Select "Install all certificates".

   To install a single application certificate:
   - Under the local machine node, right-click the certificate.
   - Select "Install".

Result

Depending on your choice, either the root certificate and CRL file as well as all application certificates are installed or only the selected application certificate is installed:

- The application certificates are installed in the certificate stores defined for the respective application, in the folder containing own certificates.

  Note

  The web server certificate is automatically bound to the Runtime web page by the installation. It replaces the web server certificate selected during Runtime installation or later in the "Website settings" step in the "WinCC Unified Configuration" tool. The web page will then be restarted to enforce the use of the new certificate. Any connected web browsers will be disconnected as a result and will have to log in again.

  The following certificates only become effective after a restart of the WinCC Unified Runtime:
  - OPC UA server certificate
  - Runtime Collaboration certificate
  - Audit Trail system certificate

- The root certificate and its CRL file are installed in the certificate stores, in the folders containing the trusted certificate authorities.

If the trust relationship between the PC and its communication partners has already been established, the PC can successfully communicate with its communication partners.

See also

Opening Certificate Manager (Page 554)

Managing own certificates of a Unified PC (Page 498)

6.7.7 Importing and installing certificates of a Unified Panel

6.7.7.1 Importing and installing certificates of a Panel

Note

You always import all application certificates of the Unified Panel. These certificates as well as the root certificate of the issuing certificate authority and its CRL file are installed on the Panel by the import.

Note

General certificates are exported and imported and installed separately. See section Using general certificates (Page 548).

Requirement

- The certificates of the Panel have been exported on the certificate authority device with "Export device > To Panel".
  See section Exporting certificates of a Panel (Page 530).
- The export file was copied to an external storage medium.
- The file name contains no spaces or special characters, such as "/", that the Panel might interpret as a command during the import.

Procedure

1. Connect the panel to the external storage medium.
2. In the Control Panel, select "Security > Certificates".
3. Click "Import".
   The "Import certificates" dialog opens.
4. Select the storage medium and the export file containing the certificates.
5. Enter the password that was used to encrypt the file during export.
6. Enter the iteration that was specified when the certificate was created.
7. Click "Import".

Result

The certificates are imported and installed:

- The application certificates are installed in the own certificates of the Panel.
  To display them, select the entry "My Certificates" as the "Certificate store".

  Note

  The web server certificate is automatically bound to the Runtime web page by the installation. The web page is then restarted to enforce the use of the new certificate. Any connected web browsers are thereby disconnected and must log in again.

  The following certificates only become effective after a restart of WinCC Unified Runtime:

  - OPC UA server certificate
  - Runtime Collaboration certificate
  - Audit Trail system certificate

- The root certificate and its CRL file are installed in the trusted certificate authorities of the Panel.
  To display them, select the entry "Certificate Authorities" in "Certificate Store".

Note

Manual importing and installing

Alternatively, you can import the certificates to the Panel manually and install them. See section Manually importing and individual certificates to a Panel and installing them (Page 542).

See also

Managing third party certificates and own certificates of a Unified Panel (Page 496)

6.7.7.2 Manually importing and individual certificates to a Panel and installing them

You can also import and install the application certificates of a Unified Panel manually instead of using the Control Panel of the device.

Requirement

- The certificates of the Unified Panel have been exported with "Export device > To Panel". See section Exporting certificates of a Panel (Page 530).
- The export file was copied to an external storage medium.

Procedure

1. Decrypt the export file using OpenSSL.
   ```
   openssl enc -d -aes256 -salt -iter <25000> -in <exportfilename>
   -out <tarfilename.tar> -k <password>
   ```
   The value for the parameter `-iter` must match the iteration count specified during export. The decrypted TAR log contains the configured certificates in the respective application-specific folder structure.
2. Copy the file to the Panel device.
3. Manually distribute the certificates to the specific repositories of the respective application.

6.7.8 Trusting CA-based certificates

6.7.8.1 Trusting the web server certificate

You can find information on how to trust a CA-based web server certificate on a web client here:

- Unified Panel as web server: See section Establishing the trust relationship with the web server (Page 384).
- Unified PC as web server: See section Establishing the trust relationship with the web server (Page 436).

6.7.8.2 Trusting Collaboration certificates

You can find information on how to trust the Collaboration certificate of a Collaboration partner on a Collaboration Panel in section Establishing the trust relationship (Collaboration for Panels) (Page 380).

You can find information on how to trust the Collaboration certificate of a Collaboration partner on a Collaboration PC in section Establishing the trust relationship (Collaboration for PCs) (Page 431).

6.7.8.3 Trusting OPC UA certificates

You can find information on how to establish the trust relationship between a Unified Panel and its OPC UA communication partner on a Unified Panel that is used as an OPC UA server or OPC UA client in section Establishing the trust relationship (OPC UA for Panel) (Page 421).

You can find information on how to establish the trust relationship between a Unified PC and its OPC UA communication partner on a Unified PC that is used as an OPC UA server or OPC UA client in section Establishing the trust relationship (OPC UA for PC) (Page 474).

6.7.8.4 Checking the status of a root certificate on the HMI device

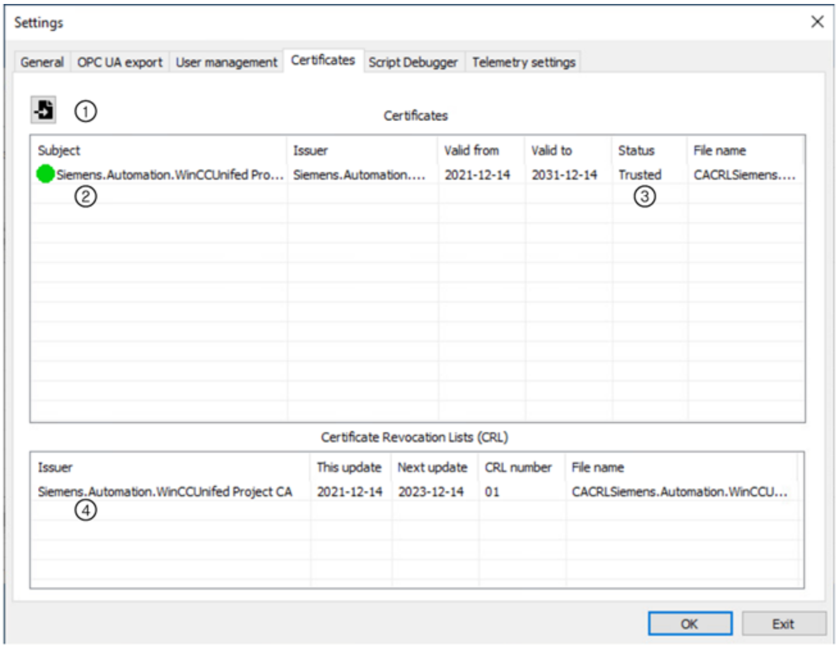
Introduction

This section describes how to check whether an HMI device already trusts the root certificate of a communication partner.

In that case, the root certificate has been installed in the certificate store of the HMI device, in the folder containing the trusted certificate authorities.

Procedure on a Unified PC

1. Start the SIMATIC Runtime Manager application on the PC.
2. Click the ⚙ button in the toolbar.
3. Select the "Certificates" tab.
4. Check under ② and ③ to see if the desired root certificate is included in the list of root certificates and third-party certificates installed on the device and whether the device trusts the certificate:



Certificates

Subject	Issuer	Valid from	Valid to	Status	File name
● Siemens.Automation.WinCCUnifed Pro...	Siemens.Automation....	2021-12-14	2031-12-14	Trusted	CACRLSiemens....

Certificate Revocation Lists (CRL)

Issuer	This update	Next update	CRL number	File name
Siemens.Automation.WinCCUnifed Project CA	2021-12-14	2023-12-14	01	CACRLSiemens.Automation.WinCCU...

① Button for importing a certificate or CRL file
You trust a certificate by importing it. You can later reject the certificate and trust it again.

② List of third-party certificates:
- Root certificates
- Application certificates that are self-signed or issued by a certification authority
- General certificates

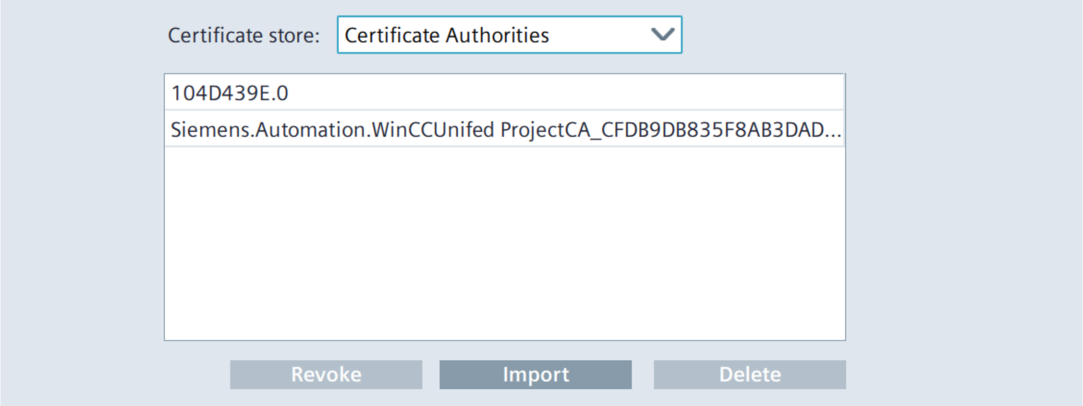
③ Shows whether the HMI device trusts a certificate

④ List of CRL files

You can find information on how to trust a root certificate or how to import and trust one in section Managing third-party certificates of a Unified PC (Page 499).

Procedure on a Unified Panel

1. In the Control Panel, select "Security" > "Certificates".
2. In the "Certificate stores" list, select the entry "Certificate Authorities".



Certificate store: Certificate Authorities

104D439E.0

Siemens.Automation.WinCCUnifed ProjectCA_CFDB9DB835F8AB3DAD...

3. Check whether the desired root certificate is included in the list of trusted root certificates installed on the device.

You can find information on how to trust a root certificate or how to import and trust one in section Importing and installing root certificates and CRL files on Panels (Page 545).

See also

Checking the status of the web server root certificate on the web client. (Page 437)

6.7.8.5 Importing and installing root certificates and CRL files on Panels

This section describes how to import a root certificate and its CRL file to a Unified Panel. The root certificate and CRL file are installed in the folder containing trusted certificate authorities by the import. The Panel trusts the root certificate and automatically trusts all certificates that were issued by the certificate authority of the root certificate.

The import is required in the following cases:

- To establish the trust relationship between the Panel and a communication partner whose application certificate was issued by a certificate authority.
- When the CRL file of an installed root certificate has been updated.

Note

If the Panel has a CA-based own certificate and its root certificate changes, it is not sufficient to import the new root certificate. You must recreate the complete configuration on the certificate authority device and import and install the certificates of the Panel on the Panel. See section Recreating the entire configuration (Page 535).

Requirement

- The root certificate or CRL file of the communication partner was copied to an external storage medium.

Procedure

1. Connect the Panel to the external storage medium.
2. In the Control Panel, select "Security > Certificates".
3. Click "Import".
   The "Import certificates" dialog opens.
4. To install the root certificate, select the storage medium and the export file containing the root certificate.
   To update the CRL file, select the storage medium and the export file containing the CRL file.
5. Enter the password that was used to encrypt the file during export.
6. Enter the iteration that was specified when the certificate was created.
7. Click "Import".

Result

The root certificate or CRL file is installed in the folder containing trusted certificate authorities. The Panel automatically trusts all application certificates that have this root certificate, except for the certificates listed in the CRL file.

To display the root certificate and the CRL file, select the entry "Certificate Authorities" as the "Certificate Store".

See also

Unified tools for certificates (Page 483)

Checking the status of a root certificate on the HMI device (Page 544)

Managing third party certificates and own certificates of a Unified Panel (Page 496)

6.7.9 Exporting an application certificate as a public certificate

You can export application certificates individually as public certificates with Certificate Manager.

Requirement

An application certificate has been added to a device in Certificate Manager.

Exporting certificate to the certificate authority device

1. On the certificate authority device, open Certificate Manager.
2. Select the "CA configuration" tab.
3. Right-click on the application certificate under the device.
4. Select "Export certificate...".
5. Select a file format.
6. Confirm your entries.
7. Select a target folder.
8. Confirm your entries.

Export certificate on the device

Additional requirements

- The device whose application certificate is to be exported is a Unified PC.
- The application certificate has been installed on the device.

Procedure

1. On the Unified PC, open Certificate Manager.
2. Select the "Installed certificates" tab.
3. Right-click on the application certificate.
4. Select "Export certificate...".
5. Select a file format.
6. Confirm your entries.
7. Select a target folder.
8. Confirm your entries.

Result

The public key of the certificate is exported. Distribute it to the external communication partners.

See also

Add application certificates (Page 524)

Opening Certificate Manager (Page 554)

6.8 Using general certificates

6.8.1 Introduction

WinCC Unified Certificate Manager enables you to create general CA-based certificates for both HMI devices and other devices.

Application examples:

- Protecting communication of self-written applications through the use of certificates
  For example, ODK applications for HMI devices or applications for other devices
- When using a local web client that logs in to the Runtime web server with RFID and PM-LOGON: creating the certificate that the PM-LOGON server uses to authenticate itself to its clients.

Advantages

General certificates provide the same overall advantages as CA-based certificates:

- Secure communication
- Easy establishment of the trust relationship through installation of the root certificate
- Automatic trust relationship if the device and its communication partner have the same certificate authority or the communication partner already trusts the root certificate of the certificate authority

Overview

You create a general certificate with Certificate Manager. A device added in Certificate Manager can have multiple general certificates.

You distribute the general certificate with Certificate Manager. This sets up the installation on the device itself and the establishment of the trust relationship on its communication partners.

A general certificate is installed on its device outside of Certificate Manager.

See also

Workflow for general certificates (Page 548)

6.8.2 Workflow for general certificates

Requirement

- WinCC Unified Runtime is installed on a PC.
- The PC serves as the certificate authority device for the CA-based communication of your HMI devices.

- A certificate authority has already been created on the PC in Certificate Manager.
- For an application created for a Unified Panel to use the general certificate of the Panel, it must address the certificate store of the Panel.

Procedure

To use general certificates, follow these steps:

1. Start Certificate Manager on the certificate authority device.
2. If the device for which you want to create the general certificate is not yet part of the CA infrastructure, add it.
3. Right-click the device and select "Add Certificate > General ...".
4. Enter the properties of the certificate in the "New certificate" dialog.
   The following applies:
   – You can use a template. To do this, select the "Use template" option and select the template from the list next to it.

     Note

     Only one template is available in the current version.

     Alternatively, you can duplicate a general certificate that has already been added and change the desired properties on the duplicate.

   – "Security" tab, "Key usage" and "Enhanced key usage" fields: To add, delete or edit a usage, right-click in the field and select the desired command.
5. Set up the installation of the general certificate on the device. Follow these steps:
   – Right-click on the general certificate and select "Export certificate ...".
     The "Export certificate" dialog opens.
   – Select the "Export with private key" option.
   – To protect the usage of the private key, assign a password.

     Note

     To be able to use the private key, the target application must also provide this password.

   – Specify the format for the export. Select one of the following options for this:

"Export public certificate in DER format"	Public key and private key are exported to a common PFX file.
"Export public certificate in PEM format"	Public key and private key are each exported to a separate PEM file.

   – Click "Export".
   – Select the storage location and confirm your entry.
6. Transfer the file or files to the device.

7. Install the private key and public key of the certificate in the own certificates of the device. Follow the procedure described in the user help of the respective device or the application.

   Note

   If the device is a Unified Panel, install them in the certificate store of the Panel. Follow the procedure described below.

   If the device is a Unified PC, the certificate store depends on the implementation of the application. Use of the following certificate stores is possible:

   - Windows certificate store
     Double-click the export file(s). Manually install the file(s) in the appropriate folder of the Windows certificate store.
   - WinCC Unified certificate store, other file-based certificate stores
     Manually copy the file(s) in a file explorer to the appropriate folder of the certificate store.

   Installation with Certificate Manager is not possible.

8. If necessary, establish the trust relationship between the device and its communication partner.

   Note

   In the following cases, the communication partner already trusts the root certificate and, thus, also the general certificate of the device:

   - The communication partner is an HMI device. The HMI device has the same certificate authority as the device. The certificates of the HMI device are installed on the HMI device.
   - The device and its communication partner have different certificate authorities. The communication partner already communicates with another device that has the same Unified certificate authority as the device with the general certificate.

   Follow these steps:

   – Export the root certificate and its CRL file on the certificate authority device in Certificate Manager.

   – Transfer the file containing the root certificate and the CRL file to the device of the communication partner.

   – Install the root certificate on the device of the communication partner in the folder containing the trusted root certificate authorities.
     Follow the procedure described in the user help of the respective device.
     If the communication partner is a Unified PC, use SIMATIC Runtime Manager for this.
     If the communication partner is a Unified Panel, use "Control Panel > Security > Certificates".

Installing the general certificate of a Unified Panel on the Panel

1. Transfer the file(s) with the public key and private key of the general certificate to an external storage medium.
2. Connect the storage medium to the Panel.
3. In the Control Panel, select "Security > Certificates".
4. Click "Import".
   The "Import certificates" dialog opens.

5. Select the storage medium and the export file.
6. Enter the password that was used to encrypt the file during export.
7. Enter the iteration that was specified when the certificate was created.
8. Click "Import".

See also

Opening Certificate Manager (Page 554)

Adding devices (Page 521)

Creating a certificate authority and root certificate (Page 519)

Introduction (Page 548)

6.8.3 Duplicating a general certificate

Requirement

A general certificate has been added to a device in WinCC Unified Certificate Manager.

Procedure

1. In the "CA Configuration" tab, open a device that has a general certificate.
2. Right-click the certificate and select "Duplicate ...".
3. The "Duplicate certificate" dialog opens.
4. Edit the properties of the new general certificate as needed.
5. Click "OK".

6.8.4 Exporting the public key

Requirement

A general certificate has been added to a device in WinCC Unified Certificate Manager.

Procedure

1. In Certificate Manager, right-click the general certificate and select "Export certificate ...".
   The "Export certificate" dialog opens.
   The "Export with private key" option is deselected
2. Specify the file format in which the public key is exported. Select one of the following options for this:
   - "Export public certificate in DER format"
   - "Export public certificate in PEM format"
3. Click "Export".
4. Select the storage location and confirm your entry.

Result

The public key of the certificate is exported. Distribute it to the external communication partners of the device.

6.9 Using self-signed certificates

Note

Recommendation

For security reasons the usage of CA-based certificates is recommended.

Introduction

A self-signed certificate confirms its validity through its own signature. It is less secure than a CA-based certificate. Its usage is subject to numerous limitations.

Limitations

Self-signed certificates offer a lower protection than CA-based certificates:

- They are vulnerable to "man in the middle" attacks.
  In the case of "Man in the middle" attacks, data exchanged between the communication partners is intercepted or changed.
- It is not possible to detect whether a self-signed certificate was compromised.
- Self-signed certificates can not be managed centrally.
- Users must trust self-signed web server certificates in each browser individually and call the certificate individually again if it is no longer trustworthy.

Furthermore, using self-signed certificates is subject to the following limitations:

- Firewall and network settings can prevent the usage of self-signed certificates.
- The web clients of a Unified web server must install the web server certificate in the web browser. The installation of self-signed certificates is not supported by all web browsers.
- Depending on the web browser, it is possible to define exceptions. For more detailed information, refer to the operating instructions of the browser.
- You can not use self-signed certificates for the following Unified components. They always require the usage of CA-based Unified certificates:
  - WinCC Unified Collaboration
  - WinCC Unified Audit
  - Unified OPC UA Clients
- The self-signed web server certificate expires after 12 months.
- The self-signed certificates of Unified Panels are re-created with each runtime start or restart. The communication partners must subsequently trust the new certificate.

Self-signed own certificates of HMI devices

A HMI device can have the following self-signed own certificates:

Certificate	HMI device	More information
Web server certificate	Unified Panels	Section Workflow with a self-signed certificate (Panel as web server) (Page 406)
	Unified PCs	Section Workflow with a self-signed certificate (PC as web server) (Page 458)
OPC UA Server certificate	Unified Panels	Section Using a default self-signed certificate (Panel as OPC UA server) (Page 423)
	Unified PCs	Section Using a default self-signed certificate (PC as OPC UA server and exporter) (Page 476)
OPC UA Exporter certificate	Unified PC that is an OPC UA Server	
Smart Server certificate	Unified Panels	Section Smart Server certificates for Panels (Page 427)

Self-signed third-party certificates

The communication partners of an HMI device can have self-signed certificates. Information on how you create these certificates is available in the user help of the respective communication partner.

For information on how to display the self-signed third-party certificates on an HMI device, how to trust, reject or uninstall them, see section Managing third party certificates and own certificates of a Unified Panel (Page 496) and section Managing third-party certificates of a Unified PC (Page 499).

For information on the protection of the communication between HMI device and S7 controller through a self-signed PLC certificate, see section Communication with S7-1500 and S7-1200 (Page 487).

Self-signed OPC UA Client certificate of the engineering system.

During the configuration of a Unified OPC UA Client the engineering system acts as an OPC UA Client. It uses a self-signed certificate. For information on using this certificate, see section Engineering System as OPC UA client (Page 478).

See also

Using CA-based certificates (Page 502)

6.10 WinCC Unified Certificate Manager

6.10.1 Introduction

You use the WinCC Unified Certificate Manager application to create, manage and distribute the CA-based application certificates of your HMI devices. You also use Certificate Manager to create, manage and distribute the general CA-based certificates of the HMI devices and, if needed, other devices.

On Unified web server PCs, you also use Certificate Manager to install own CA-based application certificates of the PC and to display or uninstall them.

See also

Customize surface (Page 560)

Changing the user interface language (Page 562)

Using CA-based certificates (Page 502)

Workflow for using CA-based certificates (Page 507)

Using general certificates (Page 548)

6.10.2 Opening Certificate Manager

Requirement

The user logged in to the PC has local administrator rights.

Procedure

To open WinCC Unified Certificate Manager, choose one of the following options:

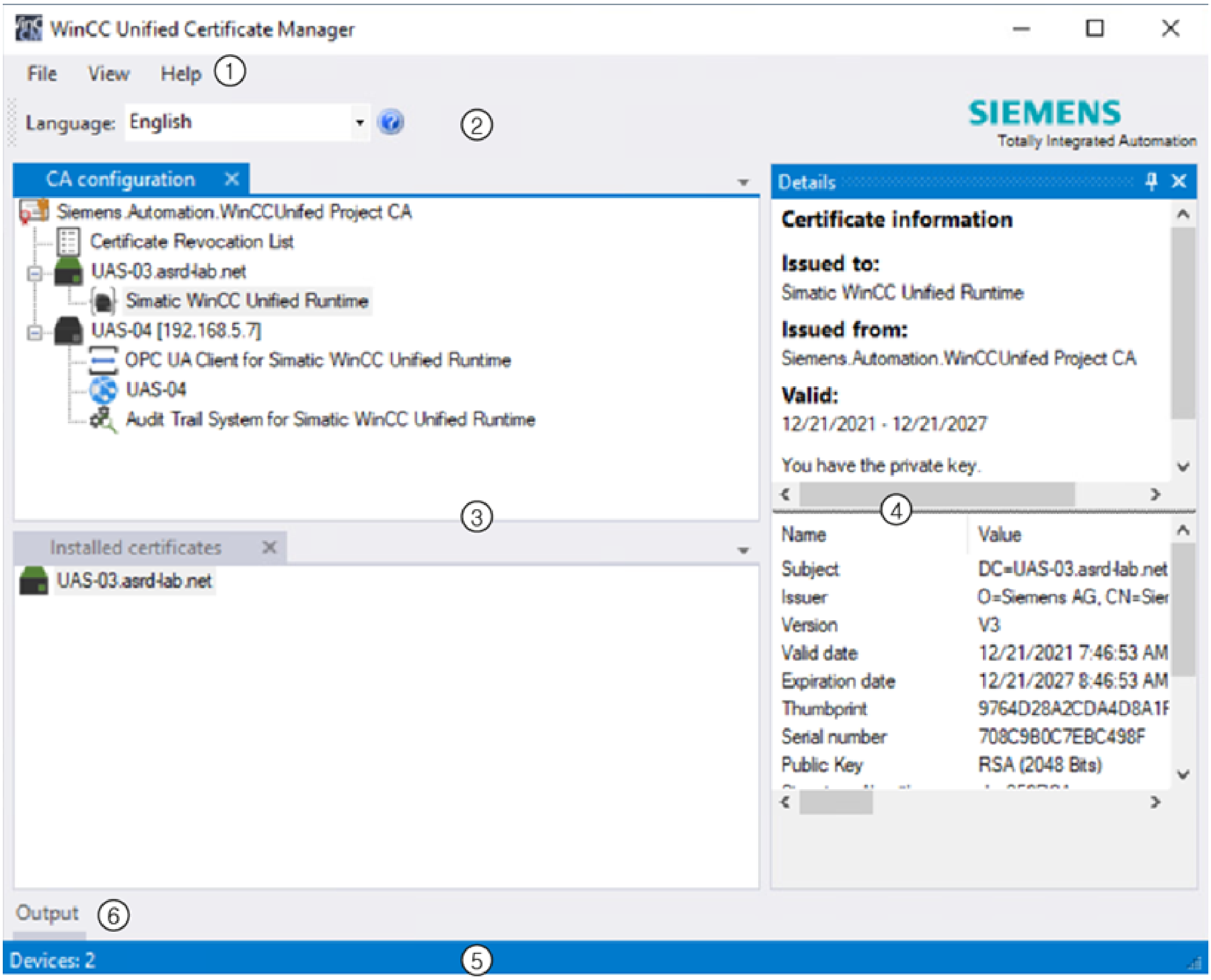
- Double-click the Desktop shortcut that was created during Runtime installation.
- Select the application in the Windows Start bar.
- With standard installation, you will find the application under "C:\Program Files\Siemens\Automation\WinCCUnified\ WebConfigurator\WinCC_CertManager.exe". Double-click the EXE file.

6.10.3 User interface

6.10.3.1 Structure of the user interface

Overview

The interface of WinCC Unified Certificate Manager has the following structure:



Language: English

- Siemens.Automation.WinCCUnifed Project CA
  - Certificate Revocation List
  - UAS-03.asrd-lab.net
    - Simatic WinCC Unified Runtime
  - UAS-04 [192.168.5.7]
    - OPC UA Client for Simatic WinCC Unified Runtime
    - UAS-04
    - Audit Trail System for Simatic WinCC Unified Runtime

UAS-03.asrd-lab.net

Certificate information

Issued to:
Simatic WinCC Unified Runtime

Issued from:
Siemens.Automation.WinCCUnifed Project CA

Valid:
12/21/2021 - 12/21/2027

You have the private key.

Name	Value
Subject	DC=UAS-03.asrd-lab.net
Issuer	O=Siemens AG, CN=Sier
Version	V3
Valid date	12/21/2021 7:46:53 AM
Expiration date	12/21/2027 8:46:53 AM
Thumbprint	9764D28A2CDA4D8A1F
Serial number	708C9B0C7EBC498F
Public Key	RSA (2048 Bits)

Devices: 2

① Menu bar
② Toolbar
③ Work area with the "CA configuration" and "Installed certificates" tabs
④ "Details" area (fixed)
The "Details" area shows you detailed information about the certificate selected in the work area.

⑤ Information bar

⑥ "Output" area (hidden)

The "Output" area logs operator control actions.

You can customize the display of the interface to suit your needs. See also Customize surface (Page 560).

Menu bar

Menu	Description
"File > Exit"	Closes Certificate Manager.
"View"	Configure which Certificate Manager interface elements you see. You can open or close the following interface elements: • "Output" area • "Details" area • "CA configuration" tab • "Installed certificates" tab
"Help"	"Certificate Manager Help" Opens the user help in a browser.
	"Info Certificate Manager" Opens a dialog with information about the installed software version.

Toolbar

Button	
▾	To change the user interface language
?	To call the user help

Tab of the working area

See "Installed certificates" tab (Page 559) and "CA configuration" tab (Page 558).

See also

Creating and exporting the CA infrastructure (Page 519)

Importing and installing certificates of a Unified PC (Page 538)

6.10.3.2 "CA configuration" tab

On a certificate authority device

On a certificate authority device, you can perform the following actions on the "CA configuration" tab:

- Create the certificate authority (root certificate and CRL file)
- Manage devices and certificates (add, delete, recreate)
- Export the device certificates as well as the root certificate and the CRL file
- If the certificate authority device is also used as an HMI device: Install or delete the application certificates issued by the certificate authority
- Renew all certificates of a device, individual certificates, the CRL file or the entire CA infrastructure including the root certificate
- Data backup

Note

Content of the tab

After starting WinCC Unified Certificate Manager, you will see the same data that the certificate authority had when you last closed the Certificate Manager:

- If no data has been generated yet, you will see the nodes "Open configuration ..." and "Create certificate authority ..."
- If data has already been generated, you see the root certificate of the Unified certificate authority and its CRL file as well as the devices added to the CA infrastructure, their application certificates and general certificates.
  You can edit them.

On runtime PCs

On Unified PCs that do not serve as a certificate authority, you can perform the following actions on the "CA configuration" tab:

- Import and install or delete the application certificates issued for the PC by the certificate authority

Note

Content of the tab

After launching the Certificate Manager, you will see the nodes "Open new configuration ..." and "Create certificate authority ...".

After opening a new configuration, you will see the root certificate of the Unified certificate authority and its CRL file, as well as the configured devices, their application certificates, and general certificates.

You can only install the application certificates of the local device. The display of the general certificates of the PC as well as the certificates of the other devices is for information purposes only.

Closing the Certificate Manager also closes the configuration.

General certificates

You can generate and export general certificates on the "CA configuration" tab on the certificate authority device. The export prepares the installation of the general certificate on its device.

On Unified PCs, you also see the general certificates in Certificate Manager after the import. This is for information purposes only. A general certificate is installed on the PC outside of Certificate Manager.

See also

Structure of the user interface (Page 556)

Creating and exporting the CA infrastructure (Page 519)

6.10.3.3 "Installed certificates" tab

In the "Installed certificates" tab, you can see which application certificates are installed on the local device.

You have the option to uninstall certificates by deleting them.

See also

Structure of the user interface (Page 556)

6.10.4 Customize surface

Display and arrangement of the interface elements of WinCC Unified Certificate Manager are configurable:

User interface elements	Close / Open	Move	Undock / dock	Fix / Unfix	Show / Hide
"Details" area	✓	✓	✓	✓	✓
"Output" area	✓	✓	✓	✓	✓
Tab of the working area	✓	✓	-	-	-

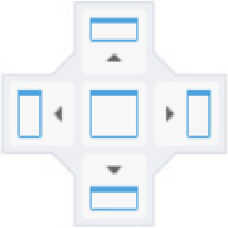
Closing and opening

To close a user interface element, click the "X" button. Alternatively, disable it in the "View" menu.

To open a closed user interface element, enable it in the "View" menu.

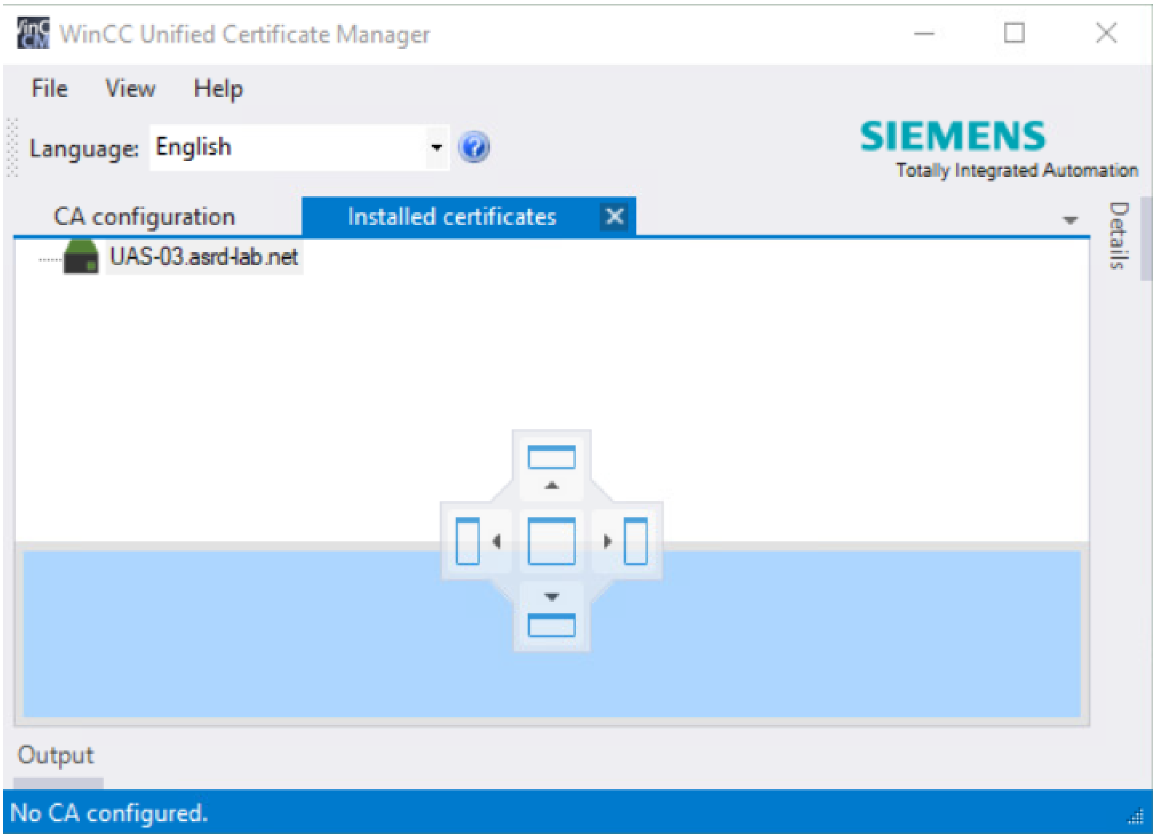
Move

1. Move the title bar of the desired user interface element with the left mouse button pressed. Possible insertion positions are displayed in the interface:



The offered insertion positions depend on which element you move and which elements the application window already displays.

2. To see a preview of the new arrangement, move the mouse cursor to one of the positions and keep the mouse cursor pressed:



3. Release the mouse cursor over the desired insertion position.

The user interface element is moved.

Undocking and docking

When you move the header of the "Details" or "Output" area, the area is undocked from the application window and displayed as a standalone window. You can move the window freely.

To dock the area back to the application window, move it to one of the suggested insertion positions.

Fixing and unfixing

The following button fixes or unfixes the "Details" and "Output" areas:

Representation of the user interface	Status	Changing setting
📌	Fixed The area is displayed even if it does not have the focus.	Click the button to switch the setting.
📌	The area is hidden as soon as it loses focus.	

Showing and hiding

Requirement

The "Details" and "Output" areas are not fixed.

Procedure

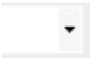
To show an area, click on its text. The area is displayed.

It is automatically hidden when you click the mouse cursor outside the area.

6.10.5 Changing the user interface language

Procedure

1. Click the button with the arrow in the toolbar:



2. Select the desired language.

Result

Changing the user interface language

6.10.6 Password requirements

The passwords defined in the Certificate Manager must meet the following requirements:

- Length: At least 8 characters
- In each case at least one uppercase letter, one lowercase letter, one number and one special character

SIMATIC Runtime Manager

7

7.1 SIMATIC Runtime Manager functions

Introduction

The SIMATIC Runtime Manager offers the following options for WinCC Unified PC:

- Use the project list to get an overview of the projects loaded into the Runtime and their properties.
  See The Runtime Manager user interface (Page 566).
- Manually start and stop a project loaded into the Runtime.
  See Starting the project (Page 568).
- Define a project that is started automatically when the HMI device starts up.
  See Selecting an autostart project (Page 572).
- Restore log segments in Runtime and delete restored segments.
  See Restoring and deleting log segments (Page 572).
- Load a project from an external storage medium into Runtime.
  See Adding a project (Page 570).
- Make the following settings, if required:

Password	Enter the password that is used by the Runtime Manager for secure communication with Runtime.	See Enter password (Page 573).
Autoscaling	Enable automatic adaptation of the HMI screens to the window size of the browser in which the Runtime project is displayed (autoscale).	See Setting general settings (Page 574).
Language	Change the user interface language of the Runtime Manager.	
Automatic login	Enable automatic login for a local web client of a Unified PC.	See Activating automatic login (Page 575).
Start external processes	Enable the start of external processes from runtime.	See Configuring security settings (Page 576).
OPC UA Export	Export the tags of the project running in Runtime into an XML file via the OPC UA server.	See Exporting tags via the OPC UA server (Page 580).
User management	Enable the user administration of the project running in Runtime.	See Activating user management (Page 581).
Certificates	Manage and distribute certificates of external communication partners and manage and distribute the root certificate of the Unified PC.	See Managing certificates (Page 577).
Runtime script debugger	Configure and enable the Runtime script debugger (screen debugger and scheduler debugger).	See Setting the Runtime Script Debugger settings (Page 582).

7.2 Start Runtime Manager

Requirement

WinCC Unified Runtime for PC is installed on the device.

Procedure

Double-click the desktop link of SIMATIC Runtime Manage created during the installation of WinCC Unified Runtime.

Alternatively, start the Runtime Manager from a file explorer by double-clicking the following file: "<Path to the Unified installation directory>\bin\SIMATICRuntimeManager.exe"

For example C:\Program Files\Siemens\Automation\WinCCUnified\bin\SIMATICRuntimeManager.exe

---

Note

Starting the Runtime Manager as administrator

Some settings under "Settings" require the Runtime Manager to be started as administrator. Right-click on the .exe and select "Run as administrator".

7.3 The Runtime Manager user interface

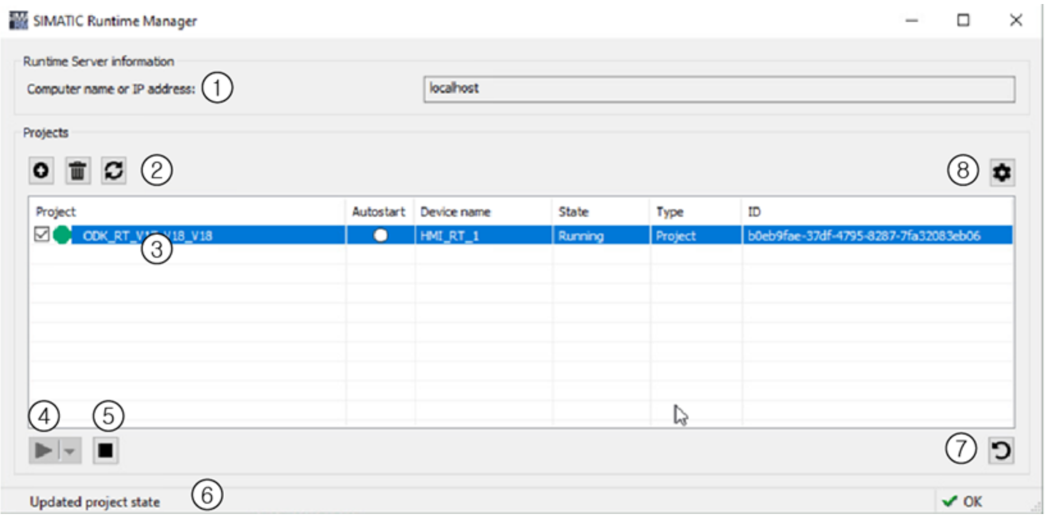
Note

User interface language

The SIMATIC Runtime Manager starts with the language configured in the general settings. You can change the interface language. See also Setting general settings (Page 574).

Structure

The Runtime Manager has the following structure:



SIMATIC Runtime Manager

Runtime Server information

Computer name or IP address: localhost

Projects

Project	Autostart	Device name	State	Type	ID
☑ ● ODK_RT_V1[illegible]18_V18	○	HMI_RT_1	Running	Project	b0eb9fae-37df-4795-8287-7fa32083eb06

Updated project state ✓ OK

① Information about the server on which the Runtime is installed
② Toolbar
③ Project list
④ Button to start the project is selected in the project list
⑤ Button to stop the project is selected in the project list
⑥ Information bar
⑦ "Restore/remove database segments for logs" button
⑧ "SIMATIC Runtime Manager settings" button

Toolbar

The toolbar has the following buttons:

Icon	Function
⊕	Loads a project from an external storage medium into the Runtime.
🗑	Deletes from the Runtime the project selected in the project list. The project folder and the log folders are deleted.
🔄	Updates the project list.

Content of the project list.

The project list shows all projects loaded into the Runtime.

The list provides the following information on the projects:

Project details	Description
Project	Project name
Autostart	Indicates whether the "Autostart" option is enabled.
Device name	Device name
State	State of the associated Runtime service Possible status values: • Running • Partly running • Shutting down • Stopped • Unknown
Type	Type of the Runtime service Project: Runtime mode Simulation: Simulation mode
ID	Project-ID

7.4 Starting the project

Requirement

A project is loaded in runtime that does not have the "Running" state.

Start without reset

Proceed as follows to start the project in a state that existed before the last project stop:

1. Click on the project in the project list.
2. Click the "Start" button ▶|▾.
3. Select "Start".

Start with reset

Proceed as follows to start the project in a state that existed during the first project start:

1. Click on the project in the project list.
2. Click the "Start" button ▶|▾.
3. Select "Start with options".
4. Enable the options "Reset logging data" and/or "Reset Runtime data" in the "Start project options" dialog.
5. Click "Start".

"Partly running" status

If it is not possible to start the simulation or the Unified Runtime and the status of the project is displayed as "partly running", check the following:

- Does the user currently logged on in Runtime have sufficient rights? Is the user registered in the following Windows user groups:
  - PlcSimUsers
  - RTIL Tracing Users
  - Siemens TIA Engineer
  - SIMATIC HMI
  - SIMATIC HMI VIEWER
- Is the computer name no longer than 15 characters?
- Is the "OPC UA" activated in the Runtime settings and is a certificate is available?

Result

- The project is started.

  Note

  Activating user management

  The login to the Runtime project requires that its user management is active in Runtime.

  After starting a project manually, you have to activate its user management manually.

- If the "Reset logging data" option was enabled, the following data is deleted when Runtime is started:
  - Logging tags
  - Logging alarms
  - Logged context values
- If the "Reset Runtime data" option was enabled, the following data originating from the last runtime of the project is deleted when Runtime is started:
  - The last values of internal, persistent tags
  - The last alarm states
  - The persistent attributes of the alarm system
  - The persistent attributes for the last logging cycle of the logging tags.

See also

Activating user management (Page 581)

7.5 Adding a project

You have the option of loading projects from an external storage medium into Runtime with the SIMATIC Runtime Manager.

Requirement

- The external storage medium with the Runtime project is connected to the computer.
- The Runtime Manager is open.
- To download a project for which only the changes to the project have been downloaded to the external storage medium, the following additional requirements must be met:
  - The project that is to receive the changes is running on the HMI device.
  - The Runtime ID of the running project and the project on the external storage medium match.

Procedure

1. In the toolbar, click "Add project from offline transmission": ⊕
   The "Add projects" dialog box opens.
2. Under "Select project log", click "...".
   A selection dialog opens.
3. Select the compressed ZIP folder of the Runtime project on the storage medium.
4. Click "Open".
   Under "Project information" you can see details of the selected project.

5. For a project that has been completely loaded onto the external storage medium, set the following options:
   - To start the project in Runtime after loading, select the "Start Runtime with project" option under "Options".
     Alternatively, you can start the project later in Runtime Manager.
   - Define whether project data is reset on startup.
     To start the project in a state that existed when the project was first started, activate the options "Reset logging data" or "Reset Runtime data".
     Disable these options to start the project in a state that existed before the last project stop.
     For more information on which data is reset with these options, see section Starting the project (Page 568).
   - Under "Check IDs", determine whether or not to check the synchronization of IDs between engineering data and runtime data.
     Check activated: If inconsistent IDs are reported, the download is canceled. The IDs are then not synchronized.
     Check not activated: The project is loaded without checking. The system cannot guarantee that the data loaded from the Engineering System match the data present in Runtime.

   Note

   Restart Runtime

   To prevent data inconsistencies, restart Runtime when you select "Do not Sync".

6. To overwrite the Runtime UMC data with UMC data from the project, select the "Overwrite UMC data with the context of the offline loading" option under "Options".
7. Confirm with "Add project".

Result

- The project is downloaded to Runtime and appears in the project list.
- When "Start Runtime with project" is activated: The running project is stopped and the downloaded project is started. Depending on your settings, the Runtime data and log data of the project is reset and the Runtime UMC data is overwritten by the UMC data from the project.

Note

When you load a project from an external storage medium, the Runtime Manager extracts the repository to a temporary folder on the target system. The transfer to Runtime takes place from this folder, which is then deleted again.

7.6 Selecting an autostart project

Requirements

- At least one project is loaded into Runtime.
- The SIMATIC Runtime Manager is open.

Procedure

In the project list for the desired project, select the option in the "Autostart" column.

Note

Restrictions

- You can only select one project for autostart at a time.
- The project must not have the "Simulation" project type.

Result

The project is started automatically when the device on which the Runtime is installed is started.

7.7 Restoring and deleting log segments

In Runtime you have the option of restoring segments from logs for which a backup was created.

You can visualize the restored data in a trend control, for example.

Note

Database types for backups

- Microsoft SQL
  Must support the "Microsoft ODBC Driver 17 for SQL Server" driver in Version 17.9.
- SQLite
  Must support the "SQLite3" driver.

You can find more information on logs in the help of the TIA Portal.

Requirement

- At least one backup of a tag or alarm log is available.
- A project is loaded into Runtime and is in the "Running" state.
- The SIMATIC Runtime Manager is open.

Restoring log segments

1. Select the project.
2. Click "Restore/delete database segments for logs".
   A dialog opens.
3. Select the log type:
   – "Alarm" for alarm logs
   – "Tag" for data log
4. If required, select the relevant log in the selection menu.
5. If required, define a start time or end time.
   If you define a start time, all entries from this point in time are restored.
   If you define an end time, all entries up to this point in time are restored.
   If you define a start time and an end time, all entries between the defined points in time are restored.
6. If you have moved the backup of the log to be restored, enter the changed storage path of the backup under "Backup path".

   Note

   Only one log can be restored using the "Backup path" option.

7. Click "Restore segments".
   The selected segments are restored.
   If you have selected a time period, data may be restored beyond the selected period, as the restoration is carried out segment by segment.
   Information on the restoration can be found under "Status".

Delete log segments

To delete all previously restored segments of the tag logs or alarm logs, follow these steps:

1. Select the log type:
   – "Alarm" for alarm logs
   – "Tag" for data log
2. Click "Delete segments".

   Note

   All restored segments of the selected log type are deleted regardless of the log or the defined period.

   Information on the deletion process can be found under "Status".

7.8 Enter password

For secure communication with Runtime, the same password must be stored in the SIMATIC Runtime Manager as in Runtime.

Requirement

The Runtime uses secure communication.

Note

Enabling secure communication

Secure communication for Runtime can be enabled as follows:

- During the installation of the Runtime, in the step "Secure Download";
  Or after the installation in the application "WinCC Unified Configuration".
- In the Engineering System, if encrypted transmission is configured in the Runtime settings of a device and the option "Allow initial password transfer via unencrypted download" is enabled when downloading the device to Runtime.
  After the first, unencrypted transmission, the Runtime switches to secure communication.

Enter password for secure communication

1. Click the ⚙ button in the toolbar.
2. Select the "General" tab.
3. Under "Secure connection", enter the same password that is used by Runtime for secure communication.
   For more information, refer to the "SIMATIC Unified PC Installation" user help under "Secure download".

Note

If Runtime does not use secure communication, the password entered here is ignored during communication with Runtime.

See also

Configuring the settings during installation (Page 39)

7.9 Setting general settings

Enable Autoscale

Proceed as follows to automatically adapt the size of HMI screens to the window size of the browser in which a Runtime project is open:

1. Click the ⚙ button in the toolbar.
2. Select the "General" tab.
3. Under "Autoscale", select the "Adapt screen to window" check box.
4. Restart the currently running project or start another project that is loaded into the Runtime.

When users zoom in or out of the browser window, the HMI screens automatically adapt. Users always see the entire screen.

Changing the user interface language

Proceed as follows:

1. Click the ⚙ button in the toolbar.
2. Select the "General" tab.
3. Select a language under "Language > Select language".
4. Click "OK".
   Changing the interface language requires you to restart the SIMATIC Runtime Manager. To restart the Runtime Manager directly, confirm the message that opens with "OK".

7.10 Activating automatic login

Introduction

Automatic login to Runtime can be enabled for local web clients of a Unified PC.

A local web client is a web client located on the same HMI device as Unified Runtime.

Requirement

- The HMI device is a Unified PC.

Procedure

1. On the HMI device, open the SIMATIC Runtime Manager as administrator.
2. Click the button ⚙ in the toolbar.
3. Select the "General" tab.
4. Under "Automatic login", activate the "Enable automatic login" option.
5. Enter the user name and password of the UMC user that automatic login is to use if no UMC user is logged into Runtime via UMC Desktop Single Sign-on yet when the local web client is started or on login to Runtime.
6. Confirm your entries with "OK".
7. Restart Runtime.

Result

- On the start of a local web client or on connection to Runtime, the web client automatically authenticates itself with the following user data:

A UMC user is already logged in on the HMI device via UMC Desktop Single Sign-on (DSSO)	
Yes	The logged-in user is used.
No	The user configured in SIMATIC Runtime Manager is used. If no user has been configured in SIMATIC Runtime Manager, a hard-coded default user without function rights is used.

  All local web clients use the same logged-in user.
- Operators see the start screen of the project running in Runtime.
- If the logged-in user does not have the authorization to operate a screen element, a login dialog opens.
  To operate the screen element, the operator must log in with a user with corresponding function rights. The open process screens remain open.
- After logout of the user used for automatic login, for example, via the "LogOff" system function, or after switchover to another user, automatic login is only possible again after Runtime is restarted.
  Logout takes effect in all applications that use DSSO. The local web client switches to the hard-coded default user without function rights. The open process screens remain open.

7.11 Configuring security settings

Allowing start of external processes

System functions that start an external process in Runtime can be configured in the engineering.

Example: The `OpenTIAPortalProject` system function, which starts the TIA Portal, can be called in Runtime in the process diagnostics.

To allow Runtime to start an external process when such a system function is called, follow these steps:

1. On the HMI device, open the SIMATIC Runtime Manager.
2. Click the ⚙ button in the toolbar.
3. Select the "Security" tab.
4. Enable the "Allow start of external processes via Unified Runtime" option.

Enabling and disabling automatic logout

If the user management is configured accordingly, users who have been inactive in Runtime for too long are automatically logged out of Runtime. The login page is displayed.

You have the option to completely disable or re-enable the automatic logout for the HMI device.

Requirement

The user logged into Windows belongs to the SIMATIC HMI Windows user group.

Procedure

1. On the HMI device, open the SIMATIC Runtime Manager.
2. Click the ⚙ button in the toolbar.
3. Select the "Security" tab.
4. Enable or disable the "Auto logout" option under "Enable automatic logout".

By default, the automatic logout is disabled.

For additional information on the configuration of the automatic logout in the user management, please refer to the help "Configuring users and roles".

7.12 Managing certificates

Introduction

Data exchange between WinCC Unified Runtime and its communication partners can be protected by certificates. The communication partners use self-signed certificates or certificates issued by a certificate authority (CA-based certificates).

In the SIMATIC Runtime Manager, you manage the certificates of the communication partners of the Unified PC (third-party certificates) in the "Certificates" tab.

You have the following options:

- Importing certificates, root certificates and CRL files
- Trust, reject, or delete certificates and root certificates already in the certificate store
- Exporting certificates, root certificates and CRL files to distribute them to other devices

Note

Alternative

If the Unified PC has its own CA-based certificates, you can also export the root certificate and CRL file of its Unified Certificate Authority using the WinCC Unified Certificate Manager application.

Note

Import and export of root certificates and CRL files

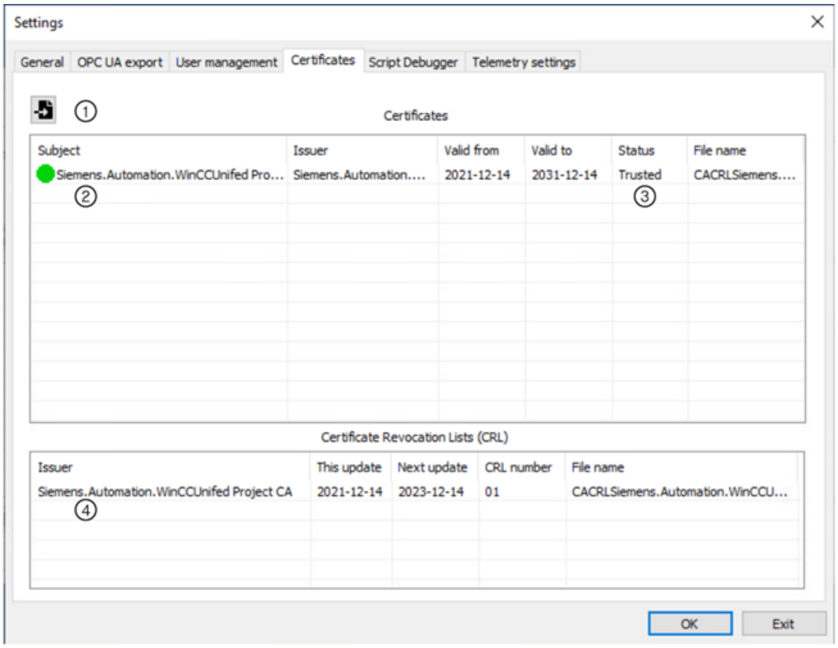
A root certificate and its CRL file must be imported separately.

If you have exported a root certificate, its CRL file is also exported. If required, you can also export the CRL files individually.

Note

Certificates of S7 controllers with an integrated connection to the Unified PC are managed system-internally. They are not visible in the SIMATIC Runtime Manager.

Structure



Certificates

Subject	Issuer	Valid from	Valid to	Status	File name
● Siemens.Automation.WinCCUnifed Pro...	Siemens.Automation....	2021-12-14	2031-12-14	Trusted	CACRLSiemens....

Certificate Revocation Lists (CRL)

Issuer	This update	Next update	CRL number	File name
Siemens.Automation.WinCCUnifed Project CA	2021-12-14	2023-12-14	01	CACRLSiemens.Automation.WinCCU...

① Button for importing a certificate or CRL file

② "Certificates" area

A list of the third-party certificates available in the certificate store (self-signed certificates, CA-based certificates and their root certificate). If the PC has its own CA-based certificates, you can also find the root certificate of the Unified Certificate Authority here.

③ "State" column

Shows whether the Unified PC trusts a certificate.

④ "Certificate Revocation Lists (CRL)" area

A list of the root certificate CRL files from "Certificates"

Requirement

- The Runtime Manager is open.
- The certificates and CRL files to be imported are located in a folder to which the Unified PC has access.

Managing certificates

1. Click the ⚙ button in the toolbar.
2. Select the "Certificates" tab.
3. You can perform the following actions:

Action	Procedure
Import and trust	1. Click "Import new certificate or certificate revocation list (CRL)": 2. Select the location where the certificate is stored, for example, an external data carrier, and select the certificate. 3. Confirm your input. The certificate is imported and copied to the "trusted" folder on the PC. Or the CRL file is imported.
Trust	Right-click on a certificate and select "Trust". The certificate is moved to the "trusted" folder on the PC.
Reject	Right-click the certificate and select "Reject". The certificate is moved to the "untrusted" folder on the PC.
Display	Right-click on a certificate and select "Show". A window with detailed information on the certificate opens.
Delete	Right-click on a certificate and select "Delete". The certificate is deleted from the certificate store on the PC.
Export	1. Right-click the certificate and select "Export". 2. If you have selected a root certificate, select the file format. 3. Select the target folder, for example, an external data storage medium. 4. Confirm your input. The certificate is copied to the target folder. If you have selected a root certificate, its CRL file is also copied. Distribute the files to the desired devices. To do this, proceed as described in the application help of the device.

Managing CRL files

1. Click the ⚙ button in the toolbar.
2. Select the "Certificates" tab.
3. You can perform the following actions:

Action	Procedure
Import	1. Click "Import new certificate or certificate revocation list (CRL)": 2. Select the location of the CRL file, e.g. an external data storage medium, and select the file. 3. Confirm your input. The file is imported and copied in the "trusted" folder on the PC.
Delete	Right-click on a CRL file and select "Delete". The file is deleted from the "trusted" folder on the PC.
Export	1. Right-click on the CRL file and select "Export". 2. Select the file format. 3. Select the target folder, for example, an external data storage medium. 4. Confirm your input. The CRL file is copied to the target folder. Distribute the files to the desired devices. To do this, proceed as described in the application help of the device.

7.13 Exporting tags via the OPC UA server

In the "OPC UA Export" tab, you can export the tags of the project running in Runtime via the OPC UA server into an XML file. The exported data can then be imported into another application, e.g. the TIA Portal, without the need for a connection to the OPC UA server.

The export makes it easier for you to apply an existing configuration to a new Runtime system.

You can find a detailed description in the help "OPC UA - Open Platform Communications".
To do this, open the following file after installing Runtime: "<Path to the Unified installation directory>\Documentation\<Language folder>\OPCWCCU<Language code>.pdf"

For example C:\Program Files\Siemens\Automation\WinCCUnified\Documentation\English\OPCWCCUenUS.pdf

7.14 Activating user management

Introduction

Several projects can be loaded on one Unified PC. The configuration of their user management may differ. For a successful login to a project in Runtime, the project must be running in Runtime and the appropriate user management must be active.

In the "User administration" tab, activate the appropriate user administration. For a project with central user management, you can also adapt the connection settings to the UMC server, e.g. to add missing settings in the TIA Portal or to use different settings.

Configuring the user administration

The user management of a project is configured in the TIA Portal under "Runtime settings > User management". In the SIMATIC Runtime Manager, it is not possible to switch a project from local to central user management.

You can find information on configuring the user management in the TIA Portal in the TIA Portal online help.

You can find information on how to configure the runtime system settings for user management during runtime installation or later with WinCC Unified Configuration here (Page 42).

Requirement

- In the Runtime system settings, it has been specified that Runtime uses the user management configuration downloaded from the TIA Portal.
- At least one user has been configured with an HMI function right for the user management active in Runtime.
- At least one user has been configured with an HMI function right for the user management that you want to activate.
- The Runtime Manager is open.
- A project is running in Runtime, and:
  - The active user management does not match the user management configured for the project.
  - For projects with central user management: The connection settings configured in the TIA Portal for the project are incomplete, or you want to use different settings.

Procedure

1. Click the button ⚙ in the toolbar.
2. Select the "User management" tab.
3. Under "Select configuration", in the "From" list, select the project whose user management configuration you want to activate in Runtime.
   Default setting after starting the Runtime Manager: The project running in Runtime

4. Confirm the confirmation prompt.
   The "Operating mode" area shows the operating mode of the user management of the selected project. The displayed options are read-only.
5. If the project selected under "From" uses local user management, click "Load user management".
   User management is activated in Runtime:
   - The user data pre-configured in the TIA Portal for the project is loaded into the local user management.
   - Runtime uses the local user management.
   - The "Status" field shows the status of the user management.

NOTICE
Possible data loss The user data configured in the TIA Portal overwrites the user data added or changed on the HMI device in the local user management. Data loss can occur.

6. If the project selected under "From" uses central user management, proceed as follows:
   - Add missing or incorrect information about the connection settings.
     By default, the identity provider address is automatically generated based on the UMC server address.
     To enter the address of the identity provider manually, deactivate the option "Generate the address of the identity provider automatically".
     To set all fields to empty, click "Reset configuration".
   - Click "Connect to server".
     The system will notify you if the configured server ID and the server ID reported during the connection attempt are different from each other. To continue with the ID reported online, click "Yes"; to continue with the configured server ID, click "No".

   User management is activated in Runtime:
   - A connection to the UMC server is established using the connection settings from the Runtime Manager.
   - Runtime uses the UMC server for user management.
   - If you later select the project under "From", the connection settings you entered are loaded.

7.15 Setting the Runtime Script Debugger settings

The scripts of the screens and jobs of a Runtime project can be tested using the Google Chrome script debugger.

To this end, the debugger must be configured and enabled in advance in the "Script debugger" tab in the SIMATIC Runtime Manager.

See also

Enabling the debugger (Page 329)

7.16 Enabling telemetry service

Introduction

The telemetry service is used to analyze problems occurring in Runtime projects. It helps the Siemens support team to support you in analyzing and correcting such problems in the best possible way. The service generates an encrypted ECD file that combines the visual recording of the process running in runtime with the recording of detailed internal system information about the process.

The ECD file records the following information from the project running in runtime:

- Screen configuration of the visible screens
- User input with mouse and keyboard
- IO addresses of all connections
- Property values of the underlying CHROM objects

Note

- Enable the telemetry service only after being requested by the Siemens support team.
- The size of the ECD file depends on the length of the recording, the number of connections and the events in the process.
- The ECD file contains machine-specific and user-specific data such as user names, but not passwords.
  This data is visible to the Siemens support team. The data is not processed or stored longer than necessary.

Requirement

SIMATIC Runtime Manager has been started in admin mode.

Enabling telemetry service

1. Click the ⚙ button in the toolbar.
2. Select the "Telemetry settings" tab.
3. Under "Storage directory", specify the path to the directory where the ECD file is to be stored. Use an already existing directory.
4. Enable the "Enable telemetry" option.
5. Restart Runtime.

The telemetry service will be enabled for the currently running project.

Next steps

1. Reproduce the error scenario in Runtime.
2. Stop the telemetry service by disabling the "Enable telemetry" option and restarting Runtime.
3. Submit the ECD file to the Siemens Support team.

7.17 Operation via command line

The SIMATIC Runtime Manager has an interface with which you can start numerous functions of the Runtime Manager via a command line program:

Requirement

- Runtime and command line program are installed on the same device.
- For starting/stopping projects: Projects have been loaded into Runtime.

Procedure

1. Start the command line program.
2. Enter the command line call. Separate the individual elements of the call with spaces.
   – Enter the path to the SIMATIC Runtime Manager.exe:
   "<Runtime installation directory>\bin> start /wait SIMATICRuntimeManager.exe"
   Example: C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait SIMATICRuntimeManager.exe
   – Enter the options with which the command line program calls the Runtime Manager. The last option must be "-c".

Option	Description
`-s`	Option for starting the Runtime Manager in silent mode. Without this option, the UI of the Runtime Manager is started when the command line call is processed.
`-u`	Option to enable help messages that assist you in operating the Runtime Manager via the command line program.
`-sim`	Only use this option if you call the option "-c" with the command `projectstate`, `start`, `stop` or `remove`.
`-quiet`	Option for calling the Runtime Manager without output.
`-o`	Option for diverting the output into an Output.txt file that is stored parallel to SIMATICRuntimeManager.exe. You can redirect the output to another folder. The Unified Administrator must have write access to the folder. Example: `-o “C:\Program Files\Siemens\Automation\WinCCUnified\bin\MyOutput.txt"` If an error occurs during the write and -quiet is not set, the error indication appears on the console.
`-keepUmc`	Optional Only in combination with the `fulldownload` command Set the option to keep the Runtime UMC data.
`-overwriteUmc`	Optional Only in combination with the `fulldownload` command Set this option to replace the UMC data of the Runtime with the UMC data from the project.
`-c`	Option for inputting the commands that are transmitted to the Runtime Manager.

– After the option "-c", enter the command that the Runtime Manager should run and the argument that is transmitted to the command:

Command	Argument	Description
`start`	<Project ID>	Starts the project.
`stop`	<Project ID>	Stops the project.
`projectlist`	[ALL] or [RUNNING] Default: [ALL]	`[ALL]`: Returns a list of projects loaded in the Runtime. `[RUNNING]`: Returns the project running in Runtime.
`projectstate`	<Project ID>	Returns the state of the project running in Runtime.
`remove`	<Project ID>	Removes the project from Runtime. If the autostart option was previously set for the project: Removes the autostart option.
`securemode`	<Password>	Sets the password for secure communication with SCS. Enter the same password that Runtime uses for secure communication.
`setautostart`	<Project ID>	The project is started when the device is booted. The project must have the Project type. The option can only be set for 1 project.
`removeautostart`	<Project ID>	Removes the autostart of the project.
`fulldownload`	<Log path>	Starts the full download of a TIA Portal log. If the project is already running in Runtime, it is stopped first before the full download. To start the project after successful download, use the command `start`.
`deltadownload`	<Log path>	Starts the change loading of a TIA Portal log. Check in advance if the corresponding project is downloaded and running in Runtime.

To run multiple commands, use multiple command line calls.

3. Press Enter.

Result

- The command is executed.
- A return code with description is output in the console.
  List of possible return codes:

Return code	Description
0x00000000	Success
0x0080400b	Project already running
0x0080400c	Project started
0x0080400d	Project already stopped
0x0080400e	Project stopped
0x80000000	General error
0x80000001	Not supported (e. g. wrong command)
0x80000003	Timeout during communication with SCS
0x80000004	Invalid arguments
0x80000005	Access denied – password required for secure connection
0x8000000C	Another project is currently flagged as autostart project, remove autostart from the other project
0x80000016	Unable to connect to SCS
0x80804019	Project not found
0x80B0412E	Write output file error
0x80B0412F	Autostart option cannot be set on simulation project
0x80B04130	Empty command value
0x80B04131	archive target path could not be created
0x80B04132	project archive can not be extracted
0x80B04133	DownloadTask file can not be read
0x80B04134	Could not change UMC Data override option
0x80B04135	Missing config folder in archive
0x80B04136	Missing delta folder in archive

- An output is written to the console or to the output file.
  Requirement: The command was called without the -quiet option.

Examples

- Call a list of all projects loaded into Runtime:
  - Input: `C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait SIMATICRuntimeManager.exe -s -c projectlist [ALL]`
  - Example output:

```
[1]
 Project name:  T1
 Device name:  T1
 Project type:  Project
 Project ID:  0B527D12-6BBD-4F2F-BEB9-23E3C37A8932
 Autostart:  0
[2]
 Project name:  T2
 Device name:  T2
 Project type:  Project
 Project ID:  29DCBA1D-C615-4560-AFB4-94EB9565682C
 Autostart:  0
[3]
 Project name:  T3
 Device name:  T3
 Project type:  Project
 Project ID:  96FE68D0-5337-4072-A96C-F7C1D7525CAF
 Autostart:  0
```

- Call the project running in Runtime:
  Input:

```
C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
SIMATiCRuntimeManager.exe -s -c projectlist RUNNING
```

- Query project state:
  Input:

```
C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
SIMATICRuntimeManager.exe -s -c projectstate 96FE68D0-5337-4072-
A96C-F7C1D7525CAF
```

- Start a project:
  Input:

```
C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
SIMATICRuntimeManager.exe -s -c start 96FE68D0-5337-4072-A96C-
F7C1D7525CAF
```

- Stop a project:
  Input:

```
C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
SIMATICRuntimeManager.exe -s -c stop 96FE68D0-5337-4072-A96C-
F7C1D7525CAF
```

- Remove a project from Runtime:
  Input:

```
C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
SIMATICRuntimeManager.exe -s -c remove 96FE68D0-5337-4072-A96C-
F7C1D7525CAF
```

- Example of a query regarding the state of a simulation project:
  Input:
  ```
  C:\Program
  Files\Siemens\Automation\WinCCUnified\bin>SIMATICRuntimeManager.ex
  e -s -sim -c projectstate 96FE68D0-5337-4072-A96C-F7C1D7525CAF
  ```
- Set password for secure communication with Runtime:
  Input:
  ```
  C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
  SIMATICRuntimeManager.exe -s -c securemode <password>
  ```
- Enable autostart for a project:
  Input:
  ```
  C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
  SIMATICRuntimeManager.exe -s -c setautostart 28AC5BD5-0741-42D1-
  B3C6-503359F32B7E
  ```
- Disable autostart for a project:
  ```
  C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
  SIMATICRuntimeManager.exe -s -c removeautostart
  28AC5BD5-0741-42D1-B3C6-503359F32B7E
  ```
- Perform a full download of a TIA Portal log:
  Input:
  ```
  C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
  SIMATICRuntimeManager.exe -s -c fulldownload
  "C:\Users\admin\Desktop\ HMI_RT_1[Project1] - Full 2019-10-21 -
  08.00.22.zip"
  ```
- Download only the changes of a TIA Portal log (delta download):
  Input:
  ```
  C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
  SIMATICRuntimeManager.exe -s -keepUmc -c fulldownload
  "C:\Users\admin\Desktop\HMI_RT_1[Project1] - Full 2020-03-27 -
  11.39.51.zip"
  ```
- Retain UMC data during full download:
  Input:
  ```
  C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
  SIMATICRuntimeManager.exe -s -c deltadownload
  "C:\Users\admin\Desktop\ HMI_RT_1[Project1] - Delta 2019-10-21 -
  08.03.18.zip"
  ```
- Replace UMC data during full download:
  Input:
  ```
  C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
  SIMATICRuntimeManager.exe -s -overwriteUmc -c fulldownload
  "C:\Users\admin\Desktop\HMI_RT_1[Project1] - Full 2020-03-27 -
  11.39.51.zip"
  ```
- Enable help messages:
  Input:
  ```
  C:\Program Files\Siemens\Automation\WinCCUnified\bin> start /wait
  SIMATICRuntimeManager.exe -s – u
  ```

See also

Enabling the debugger (Page 329)

My WinCC Unified 8

8.1 Introduction

Introduction

With My WinCC Unified, you define during runtime how the Runtime of a Unified PC web server is displayed in its clients.

My WinCC Unified works rule-based. For each rule, you define:

- For which client device the rule applies.
  The rule is applied to all users who log in to the Runtime of the Unified PC runtime on this client device.
- Whether auto-login is active.
  When auto-login is enabled, the client can automatically log in to Runtime without entering a username and password (auto-login).
  A default user who has no function rights is used to log in.
- Whether Runtime is displayed in kiosk mode.
- Which start screen is displayed after logging in to Runtime, and display of the start screen (section, start point, etc.).

My WinCC Unified is available:

- As web application
- On client devices for which kiosk mode is configured: In the Windows tray, via "WinCC Unified Control Center".

Workflow

1. Install the SIMATIC WinCC Unified Control Center application on the client devices on which you want to display Runtime in kiosk mode.
2. Open My WinCC Unified.
   My WinCC Unified connects to the Runtime of the Unified PC in the background.
3. Add rules for the client devices of the Unified PC in My WinCC Unified.
4. Configure the rules.

When a user logs in to Runtime in a web client or starts Runtime in kiosk mode on a kiosk device, Runtime is displayed as defined by the rule.

See also

Restrictions and requirements (Page 592)

Install SIMATIC WinCC Unified Control Center (Page 610)

Opening My WinCC Unified (Page 595)

Add rule (Page 601)

8.2 Restrictions and requirements

My WinCC Unified restrictions

- My WinCC Unified is only available for Unified PC Runtime web server.
- You can create rules only for client devices with static IP addresses.
- If you enable auto-login in a rule for a client device, no operator control of objects or functions that are linked to function rights is possible on this device after automatic login to Runtime.

Restrictions in kiosk mode

- The display of Runtime in kiosk mode is supported only on Windows PCs.
- It is not possible to exit the kiosk mode via touch gestures.

Requirements

The following general requirements apply for opening My WinCC Unified and starting Runtime in kiosk mode:

- WinCC Unified Runtime 19 is installed on the Unified PC.
- A Unified PC with device version V19 was configured in the engineering system and loaded onto the Unified PC.
- The corresponding Runtime project has the status "Running" on the Unified PC.
- The user management configuration of the project is active.
- When using the central user management:
  - At least one user is created in the UMC system.
  - The user created in the UMC system has been imported into the TIA Portal project before the loading.
  - The user has the function rights required to operate My WinCC Unified through his roles.
- When using the local user management:
  - Before the loading, at least one user has been created in TIA Portal.
  - The user has the function rights required to operate My WinCC Unified through his roles.
- A valid web server certificate (self-signed or CA-based) is installed on the Unified PC that is used as the Runtime web server.

- Opening My WinCC Unified:
  - In a web client: The browser you use as a web client trusts the web server certificate.
  - Via the SIMATIC WinCC Unified Control Center application using the Windows tray:
    The SIMATIC WinCC Unified Control Center application is installed on the client device.
    The Windows certificate store of the device trusts the Runtime web server certificate.
- Start kiosk mode:
  - The SIMATIC WinCC Unified Control Center application is installed on the kiosk device.
  - The Windows certificate store of the kiosk device trusts the Runtime web server certificate.
  - In My WinCC Unified, a rule has been added for the kiosk device in which the kiosk mode has been enabled.

Function rights

The following function rights are required to log on to and operate My WinCC Unified:

- Read access: "My WinCC Unified - Read device and user settings"

  Note

  V19 supports only device-specific settings.

- Read access and write access: "My WinCC Unified - Read and write access to device specific settings"

Note

For compatibility reasons, logging on to My WinCC Unified and configuring the start screen settings is also possible via the "Remote access" function right.

Trust web server certificate

Start kiosk mode:

Web server certificate	Establishing the trust relationship	Procedure
CA-based	Establish the trust relationship before connecting to Runtime.	Install the root certificate before connecting for the first time in Edge or Chrome.
Self-signed		On the kiosk device, start Edge or Chrome and open the Unified Runtime start page. Install the self-signed web server certificate in Edge or Chrome.

Starting My WinCC Unified with the Windows tray via "WinCC Unified Control Center":

Web server certificate	Establishing the trust relationship	Procedure
CA-based	Establish the trust relationship before connecting to Runtime.	Install the root certificate in Edge or Chrome before connecting for the first time.
Self-signed		On the kiosk device, start Edge or Chrome and open the Unified Runtime start page. Install the self-signed web server certificate in Edge or Chrome.

Starting My WinCC Unified in a web client:

Web server certificate	Establishing the trust relationship	Procedure
CA-based	Recommendation: Establish the trust relationship before connecting to Runtime.	• Edge and Chrome as web client: Install the root certificate before connecting for the first time in Edge or Chrome. • Firefox as web client: Install the root certificate before connecting to Firefox for the first time.
	Alternative: Establish the trust relationship when you first establish the connection.	• Edge and Chrome as web client: Install the root certificate the first time you connect in Edge or Chrome. • Firefox as web client: Install the root certificate the first time you connect to Firefox.
Self-signed	Establish the trust relationship when you first establish the connection.	• Edge and Chrome as web client: Install the self-signed web server certificate the first time you connect in Edge or Chrome. • Firefox as web client: Install the self-signed web server certificate the first time you connect in Firefox.

See also

Install SIMATIC WinCC Unified Control Center (Page 610)

Installing the root certificate before the first connection (Edge and Chrome) (Page 439)

Installing the root certificate at the first connection (Edge and Chrome) (Page 442)

Installing the root certificate before the first connection (for Firefox) (Page 445)

Installing the root certificate at the first connection (for Firefox) (Page 447)

Installing the self-signed web server certificate for Edge and Chrome (Page 460)

Installing the self-signed web server certificate for Firefox (Page 464)

8.3 Opening My WinCC Unified

Introduction

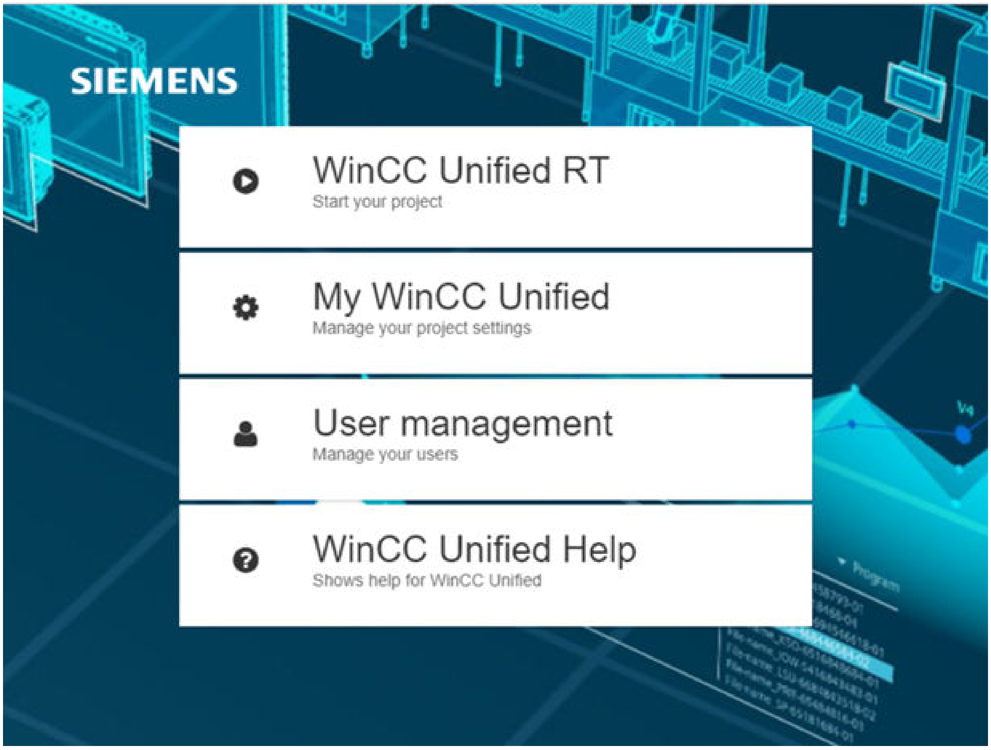
Your procedure depends on whether you open My WinCC Unified in a web client or on a kiosk device with the Windows tray via "WinCC Unified Control Center".

Requirement

See section Restrictions and requirements (Page 592).

Open in a web client

1. Start the Web client.
2. In the address bar of the browser, enter the URL of the Unified Runtime web server: "https://<IP-address of the HMI device or its FQDN or device name> ".
3. Press Enter.
   You see the Unified home page:

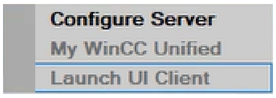


4. Click "My WinCC Unified".
   A new tab opens. You see the logon dialog.
5. Enter the user name and password of a user with the required function rights and select another language if necessary. Confirm your entries.

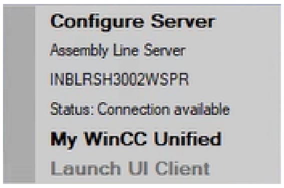
Open on a kiosk device via the Windows tray

1. If the device is in kiosk mode, exit kiosk mode.
2. Select "WinCC Unified Control Center" in the Windows tray:

   If no server is configured yet, you will see the following extended Windows tray.

   Continue with step 3.
   If a Unified Server has already been configured, the extended Windows tray shows details about that server and the connection status:

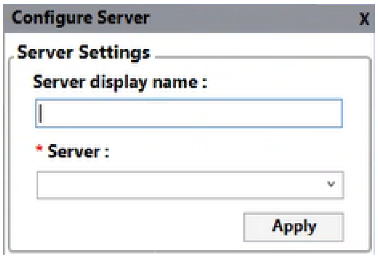
   

   Your procedure depends on whether you want to connect My WinCC Unified to this server, and on the connection status:

   – Connect to other server: Continue with step 4.
   – Connect to the configured server. The connection status is not "Connection available": Start Runtime on the server. Then continue with step 5.
   – Connect to the configured server. The connection status is "Connection available": Continue with step 6.

3. If no server is configured yet, follow these steps:

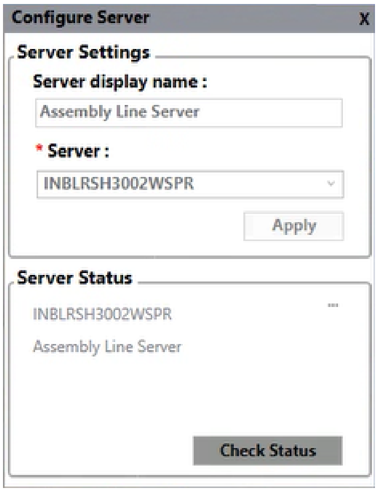
   – In the extended Windows tray, select "Configure Server".
   The "Configure Server" dialog box opens.



   – "Server display name": Enter the display name of the server.

   – "Server": Depending on what information is stored in the web server certificate, enter the IP address or the device name of the server.
   Mandatory information

   – Click "Apply".
   The window is extended:



Server display name : Assembly Line Server

* Server : INBLRSH3002WSPR

INBLRSH3002WSPR
Assembly Line Server

   Continue with step 5.

4. If a different server is configured than the one you want to connect to, change the server.
   Follow these steps:

   – In the "Server Status" area, click "...".

   – Select "Delete".

   – Configure the server in the "Configure Server" area:
   "Server display name": Enter the display name of the server.
   "Server": Depending on what information is stored in the web server certificate, enter the IP address or the device name of the server. Mandatory information

   – Click "Apply".

5. Under "Server Status", click on "Check Status".
   It is checked whether a connection to the configured server is possible.
   - Status is not "Connection available": No connection is possible. Start the Runtime of the server and repeat the check.
   - Status is "Connection available": The connection is possible.
6. If a connection is possible, select "WinCC Unified Control Center > My WinCC Unified" in the Windows tray.
7. Log in to Runtime in the "User login" dialog:
   - Enter the user name and password of a user with the necessary function rights.
   - Select another language if required.
   - Confirm your entries.

Note

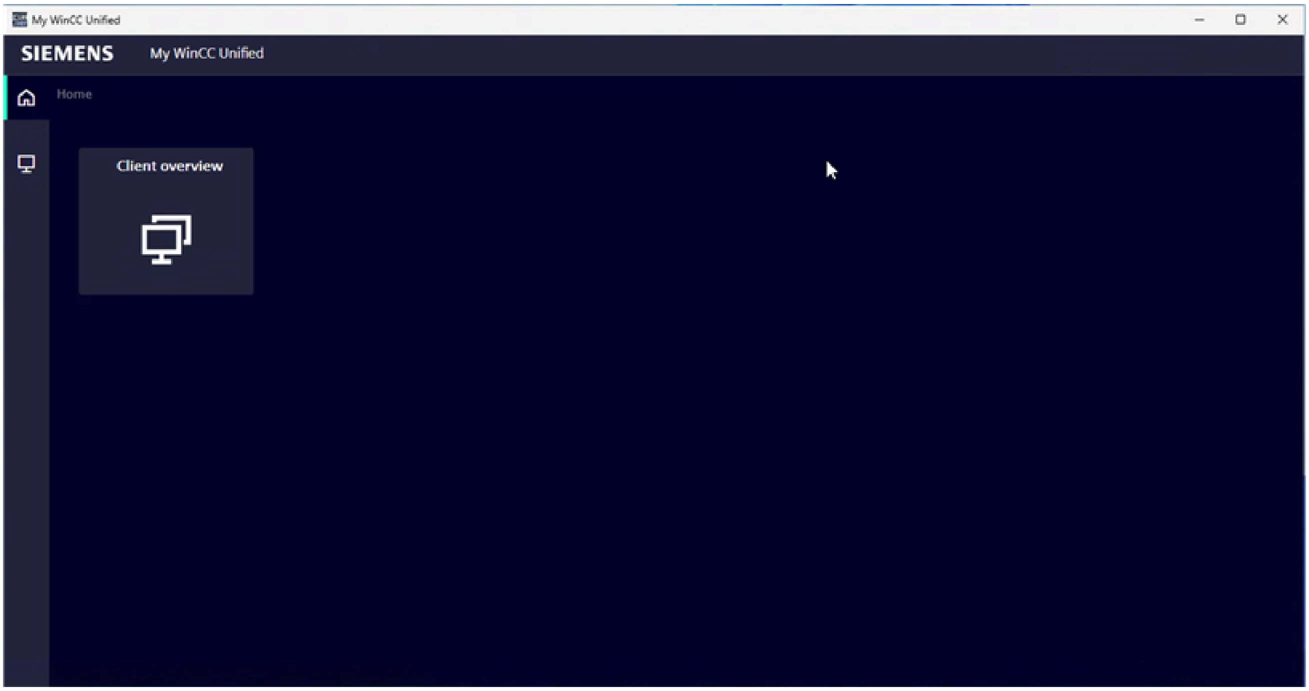
"Configure Server" remembers inputs transferred by "Apply". If you select the IP address provided under "Server", the display name transferred with "Server display name" for this IP address is automatically entered under "Apply".

You can change the display name of the configured server later. In the "Server Status" area, click "... > Edit" and change your entry.

Result

My WinCC Unified connects to the Runtime of the Unified PC in the background.

You see the start view of My WinCC Unified:



Note

When using a central user management, My WinCC Unified is displayed in the language you selected when you logged in in the "User login" dialog.
If this language is not available for the current project or if the language setting has not been set in the central user management, the following language is displayed:

- Engineering with TIA Portal: The language for which the lowest number was configured in the Runtime settings.
- Engineering with Online Engineering: The language set as default language in the "Languages" tab in the "Languages and Resources" editor.

If you do not select a language in the "User login" dialog, My WinCC Unified is displayed in the language that is set for the browser.

See also

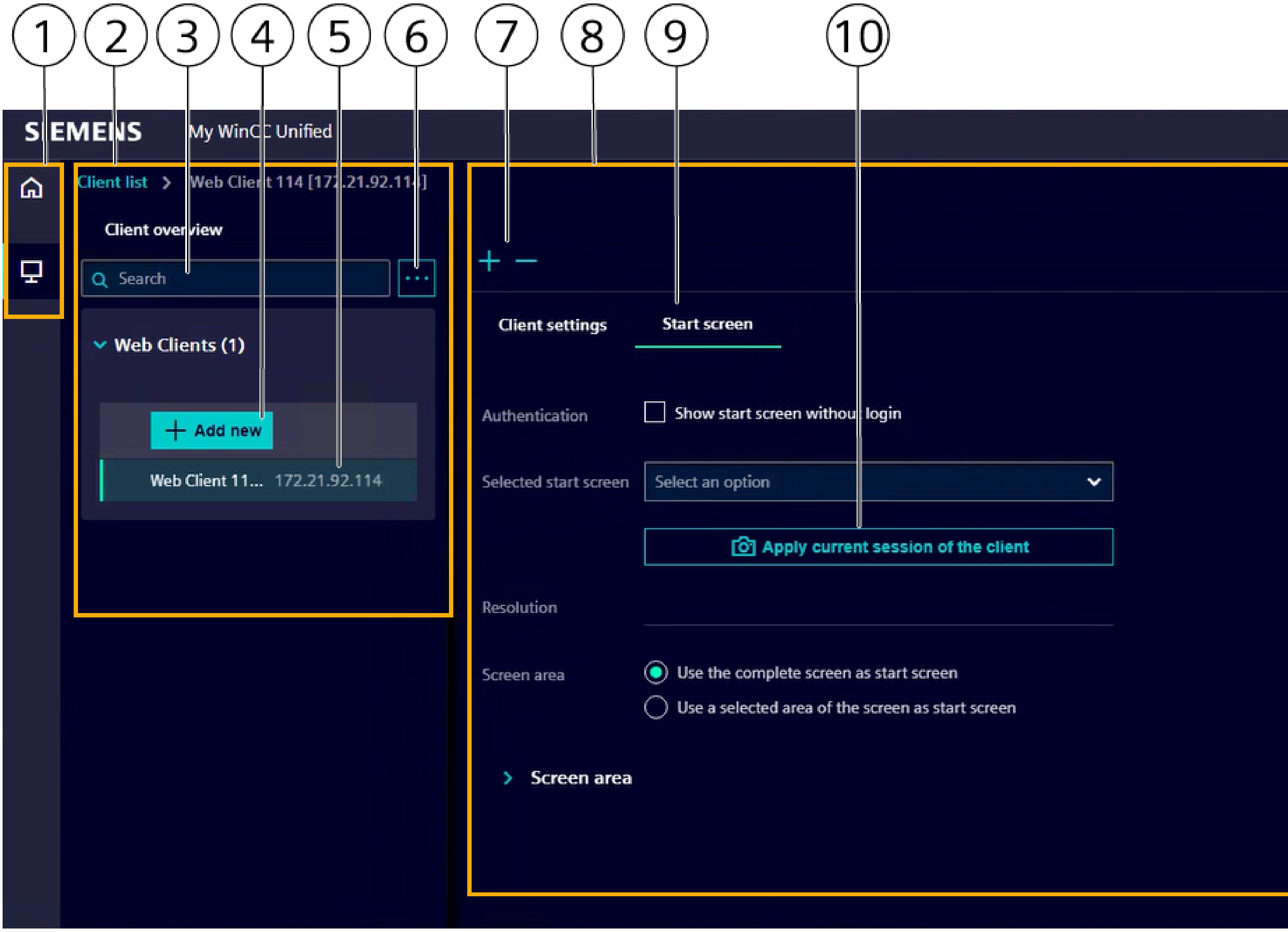
Exit Kiosk mode (Page 614)

User interface (Page 600)

8.4 User interface

Structure

Structure of the My WinCC Unified user interface using the client overview as an example:



Authentication □ Show start screen without login

Selected start screen: Select an option

Resolution

Screen area ● Use the complete screen as start screen

○ Use a selected area of the screen as start screen

① Navigation bar

② Navigator for rules

③ Search field

Filters the rules displayed in the navigator according to the entered search string.

④ "+ Add new" button

To add a new rule.

⑤ A list of available rules. The rules are sorted according to when they are added.

To load a rule into the work area, click on the rule.

⑥ "..." button

Opens a menu for exporting and importing the rules.

⑦ "+" and "-" buttons
Adds or removes a facet from the rule.
The "Client settings" facet is always available. You cannot remove it.

⑧ Work area
Shows the rule selected in the navigator.

⑨ The facets of the rule loaded into the work area
To display a facet, click on the facet.
The facet settings are displayed in the work area. You can edit them.

⑩ To configure the currently selected facet.

⑪ Function bar for saving, cloning or deleting the displayed rule

Navigation bar buttons

Button	Description
⌂	Home
🖥	Client overview To manage and configure the client-specific rules

Buttons of the toolbar

Button	Description
💾	Saves the changes to the rule currently loaded in the work area.
⧉	Clones the rule loaded into the work area. Edit the client settings and, if required, the other facets of the rule.
🗑	Deletes the rule loaded into the work area.

8.5 Add rule

Requirement

My WinCC Unified is open.

Procedure

1. In the "Client overview" navigation bar, click 🖥.
2. Click "+ Add new" in the navigator.
   The new rule is created and loaded into the work area.
   The rule has the facet "Client settings".
3. Configure the client settings.
   See section Client settings (Page 605).

4. Click "+" and select the facets you require.
5. Configure the settings of the added facets.
   See sections Start screen settings (Page 607) and Settings for kiosk (Page 608).
6. To remove a facet, click on the facet and then on "-".
   The "Client settings" facet cannot be removed.
7. Click in the toolbar 💾.

Result

The rule is applied to all clients that log in to Runtime from the device configured in "Client settings".

When you add or edit a rule for an already started client, the following applies:

- Web client: The configuration takes effect after the web page has been updated.
- Kiosk client: The configuration takes effect after kiosk has been restarted on the client.

See also

Opening My WinCC Unified (Page 595)

Exporting and importing rules (Page 602)

8.6 Exporting and importing rules

Introduction

My WinCC Unified supports the export and import of rules via a YAML file. This enables you to:

- Edit rules locally
- Transfer rules between Unified Runtime servers

Information about the structure of the YAML file can be found below.

Note

The YAML files are not protected against manipulation. You are responsible for ensuring the integrity of these files.

PINs configured in My WinCC Unified are hashed during export.

Export

Requirement

- Rules have been added in My WinCC Unified.
- You are logged on to My WinCC Unified.

Procedure

1. In the "Client overview" navigation bar, click 🖥.
2. Click "..." in the navigator.
3. Select "Export".
4. Select the export file name and location.
5. Confirm your entries.

Result

All rules of the Runtime server are exported to a YAML file.

Import

Requirement

- You have access to the YAML file.
- You are logged on to My WinCC Unified.
- The user logged on to My WinCC Unified has the "My WinCC Unified - Read and write access to device-specific settings" function right.

Procedure

1. Select "Client overview" in the navigation bar.
2. Click "..." in the navigator.
3. Select "Import".
4. Select the YAML file.
5. Confirm your entries.

Result

The rules from the file are imported into the navigator.

If the file and the navigator contain a rule for the same client device, the settings from the file are applied.

Note

If you changed or added a PIN when editing the YAML file, the PIN is hashed during import. The import takes longer than importing a file that contains only PINs that have already been hashed.

Structure of the YAML file

The following example shows the required structure of the YAML files:

```
WebClientConfiguration:
  - Unit_1:
      Identity: 192.168.178.20
      IdentityType: IP_ADDRESS
      StartScreen: 1_Main
      ZoomAndPositionOffset:
        Left: 500
        Top: 1000
        ZoomFactor: 2
      AutoLogin: true
      KioskSettings:
        LockDownStatus: true
        BreakOutData:
          IsEnabled: true
          SelectedKey: ALT+F4
          IsPinConfigured: true
          Pin: RYMUwKebeMiP7KIgLv1iwA0R9RhhkEvqv4vjpW/uuosGXabd4gbeQS/
GbRB2Hbpm+lmHLoZgYR1kEQp4wRbXyg==
          Keys:
            - Alt+F4
        FolderData:
          IsExternalDriveAccessible: true
          FolderItems:
            - Path: c:\user1\download\
              IsDefault: true
  - Unit_2:

      Identity: 192.168.178.21

      IdentityType: IP_ADDRESS

      StartScreen: 2_CustomControl
      ...
```

See also

Add rule (Page 601)

Opening My WinCC Unified (Page 595)

8.7 Clone rules

Requirement

- A rule has been added in My WinCC Unified.
- You are logged on to My WinCC Unified.

Procedure

1. In the "Client overview" navigation bar, click 🖥.
2. Click a rule in the navigator.
   The rule is loaded into the work area.
3. Click in the toolbar ⧉.
   A new rule is added. Except for the client settings, it is identical to the previously loaded rule.
4. Click "Client settings" and configure the settings for the device.
5. (Optional) Edit the other facets as required (edit, add, delete).
6. Click in the toolbar 💾.

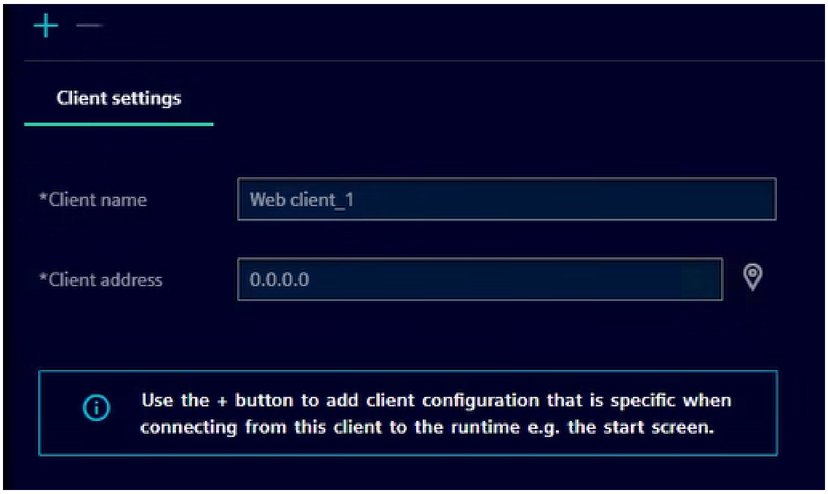
See also

Add rule (Page 601)

Opening My WinCC Unified (Page 595)

8.8 Client settings

In the "Client settings" facet, you specify which device the rule applies to.



*Client name: Web client_1

*Client address: 0.0.0.0

Use the + button to add client configuration that is specific when connecting from this client to the runtime e.g. the start screen.

The rule applies to all clients started on this device.

The facet is mandatory. You cannot add or remove them using the "+" and "-" buttons.

Settings

	Description
"Client name"	Mandatory field The device name or FQDN (Fully Qualified Domain Name) If the rule applies to the local clients of the Unified PC, you can also enter "localhost".
"Client address"	Mandatory field The IP address You have the following options: • Enter an IP address or multiple IP address (e.g. `192.65.168.160` or `192.65.168.160, 192.65.168.165`). The rule applies to this device or these devices. • Enter an IP address range (e.g. `192.65.168.160-192.65.168.190`). The rule applies to all devices in this address range. • Combine these options (e.g. `192.65.168.160, 192.65.168.165-192.65.168.190`).
📍	Reserved for future versions.

Note

Do not enter an IP address in multiple rules.

If you enter an IP address in a rule and the IP address also belongs to the address range configured in another rule, the rule in which you entered the IP address is applied.

Examples of "Client address"

You define the following rules:

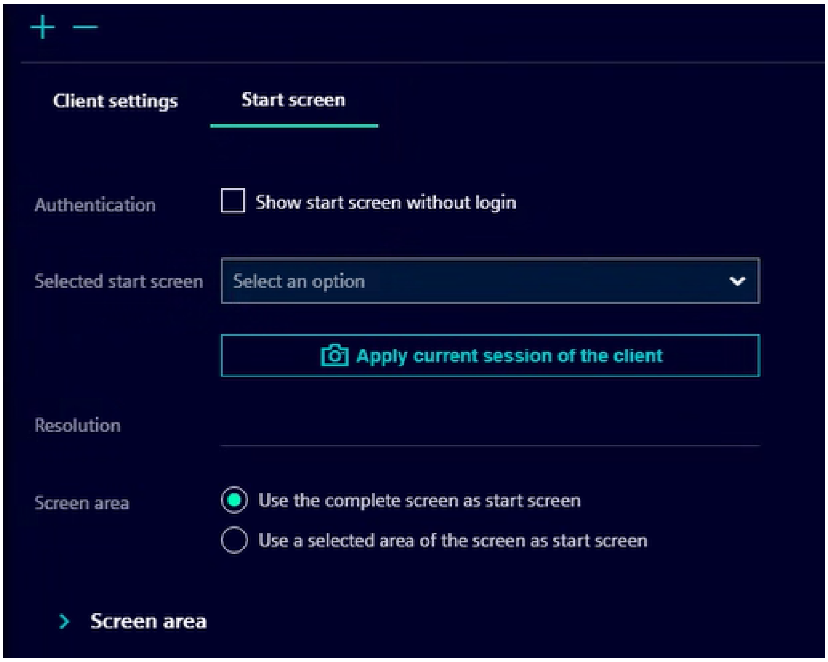
- 1st rule: "Client address": `192.65.168.165`
  Successfully saved.
- 2nd rule: "Client address": `192.65.168.160-192.65.168.190, 192.65.168.199`
  Successfully saved. For the display of Runtime on the client device with the IP address 192.65.168.165, the 1st rule is applied.
- 3rd rule: "Client address": 192.65.168.199
  Saving is not successful because the IP address is already entered in the 2nd rule.

See also

Add rule (Page 601)

8.9 Start screen settings

In the "Start screen" facet, you determine which start screen the clients see in Runtime.



Authentication ☐ Show start screen without login

Selected start screen: Select an option

Resolution

Screen area
● Use the complete screen as start screen
○ Use a selected area of the screen as start screen

You add the facet using the "+" buttons and remove it using the "-" button.

Settings

	Description
"Authentication"	"Show start screen without login" option: • Activated: The Web clients of the device are logged in to Runtime with a default user without user input. You automatically see the start screen that is usually configured. • Disabled: The Web clients of the device must enter their user name and password to log in to Runtime.
"Selected start screen"	Select the start screen: You are offered all the start screens of the project running in Runtime.
"Apply current client session"	If WinCC Unified Runtime is open in the same Web client, click this button to apply the settings of the screen currently displayed in Runtime to the rule. Button is disabled if there is more than 1 address or one address range is entered under "Client address".
"Resolution"	The resolution configured in engineering Read-only
"Screen area"	"Use the complete screen as start screen" option: The complete process screen is displayed as the start screen.
	"Use a selected screen area as start screen" option: Only the area of the process screen selected under "Screen area" is displayed as the start screen.
"Screen area"	

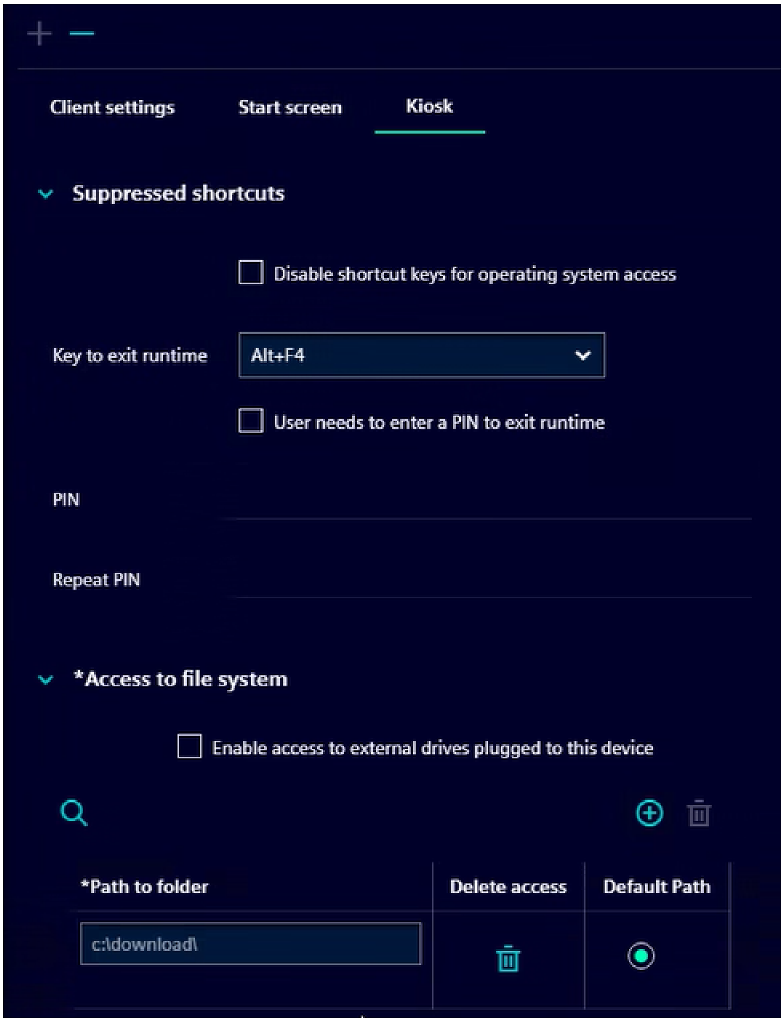
	Description
"Zoom factor":	Enter the zoom factor. Default: 100%
"Start point X", "Start point Y"	Enter the starting point of the upper left corner of the screen area to be displayed. Default: 0

See also

Add rule (Page 601)

8.10 Settings for kiosk

In the "Kiosk" facet, you determine whether Runtime runs in kiosk mode on the device configured in "Client settings".



□ Disable shortcut keys for operating system access

Key to exit runtime: Alt+F4

□ User needs to enter a PIN to exit runtime

PIN

Repeat PIN

□ Enable access to external drives plugged to this device

*Path to folder	Delete access	Default Path
c:\download\	🗑	●

You add the facet using the "+" buttons and remove it using the "-" button.

Settings

	Description
"Suppressed shortcuts"	
"Disable shortcut keyes for operating system"	• Option disabled: Users can use the Windows shortcut keys in kiosk mode. • Option enabled: Users cannot use the Windows shortcut keys in kiosk mode, except for the shortcut configured in "Key to exit runtime".
"Key to exit runtime"	Configure whether users can exit Runtime via a shortcut key when the "Disable shortcut keyes for operating system" option is enabled: • "Disabled" A restart of the kiosk device is required to exit Runtime. • "Alt+F4" Runtime can be exited by pressing "Alt+F4" or by restarting the kiosk device.
"User needs to enter a PIN to exit runtime"	The option is only available if you have selected the entry "Key to exit runtime" in "Alt+F4". • Option enabled: After pressing Alt+F4, the user is prompted to enter a PIN. Runtime is exited only after entering the PIN configured below. • Option disabled: Runtime is exited without entering a PIN.
"PIN"	Enter an 8-digit number as the PIN.
"Repeat PIN"	Repeat the PIN.
"Access to file system"	
"Enable access to external drives plugged to this device"	If this option is enabled, Runtime has access to all external drives connected to the kiosk device.
🔍	Filters which of the added folders you see.
🗑	Removes all added folders
+	Adds a new line to the list of local folders You must add at least the path to a local folder.
Per line:	
"Path to folder"	Enter the path to the local folder to which Runtime will have access.
"Delete access" 🗑	Deletes the line.
"Default path"	Option enabled: Runtime uses entered folder as default for download folder. Can only be enabled for one folder.

See also

Add rule (Page 601)

8.11 Display Runtime in kiosk mode

8.11.1 Install SIMATIC WinCC Unified Control Center

The SIMATIC WinCC Unified Control Center application must be installed on clients that are to run in kiosk mode.

Requirement

- You have administration rights on the PC on which you want to use Runtime in kiosk mode.

Procedure

To install SIMATIC WinCC Unified Control Center, follow these steps:

1. Insert the installation medium in the relevant drive.
2. Copy the installation files to the PC.
3. On the PC, in the folder with the installation files, right-click the "Start" application.
4. Select "Run as administrator".
5. Select the required installation language.
6. Follow the installation instructions.
7. Reboot the PC.

Result

- The application is installed.
- The SIMATIC WinCC Unified Client Service is installed and running.
- The Windows tray is extended by the icon of "WinCC Unified Control Center":

  Commands available via the icon:

  – "Configure Server"
  For configuring the connection to the Runtime web server to which My WinCC Unified and the kiosk mode connect.

  – "My WinCC Unfied"
  At the start of My WinCC Unified.

  – "Launch UI Client"
  To start Runtime in kiosk mode.

See also

Start kiosk mode (Page 611)

8.11.2 Configuring kiosk mode

Requirement

My WinCC Unified is open.

Procedure

1. In the "Client overview" navigation bar, click 🖥.
2. Add a new rule or click on a rule in the navigator.
   See section Add rule (Page 601).
   Or click on an existing rule.
3. If the "Kiosk" facet has not yet been added, click "+" and select "Kiosk".
4. Configure the kiosk settings. See Settings for kiosk (Page 608).
5. Click in the toolbar 💾.

8.11.3 Start kiosk mode

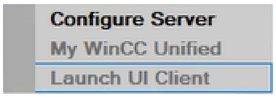
Requirement

See section Restrictions and requirements (Page 592).

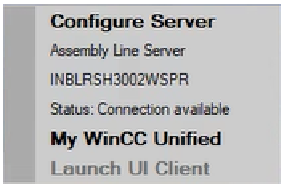
Procedure

1. Select "WinCC Unified Control Center" in the Windows tray:

   If no server is configured yet, you will see the following extended Windows tray.

   Continue with step 2.
   If a server has already been configured, the extended Windows tray shows details about that server and the connection status:

   Assembly Line Server
   INBLRSH3002WSPR
   Status: Connection available

   Your procedure depends on whether you want to connect My WinCC Unified to this server, and on the connection status:

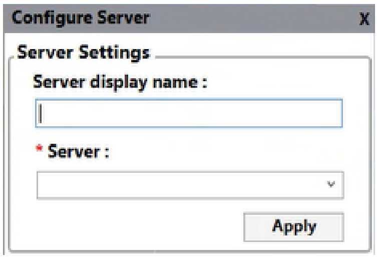
   – Connect to other server: Continue with step 3.

   – Connect to the configured server. The connection status is not "Connection available": Start Runtime on the server. Then continue with step 4.

   – Connect to the configured server. The connection status is "Connection available": Continue with step 5.

2. If no server is configured yet, follow these steps:

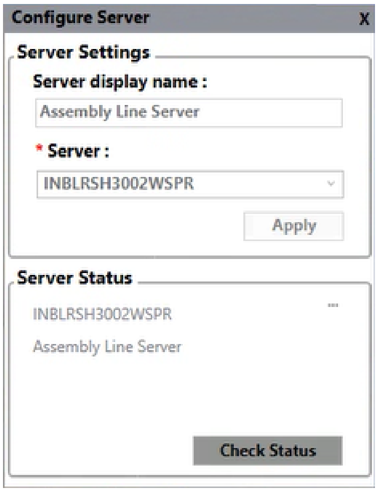
   – In the extended Windows tray, select "Configure Server".
   The "Configure Server" dialog box opens.

   – "Server display name": Enter the display name of the server.

   – "Server": Depending on what information is stored in the web server certificate, enter the IP address or the device name of the server.
   Mandatory information

- Click "Apply".
  The window is extended:



Continue with step 5.

3. If a different server is configured than the one you want to connect to, change the server. Follow these steps:
   - Click "..." in the plant complex "Server Status".
   - Select "Delete".
   - Configure the server in the "Configure Server" area:
     "Server display name": Enter the display name of the server.
     "Server": Depending on what information is stored in the web server certificate, enter the IP address or the device name of the server. Mandatory information
   - Click "Apply".
4. Under "Server Status", click on "Check Status".
   It is checked whether a connection to the configured server is possible.
   - Status is not "Connection available": No connection is possible. Start the Runtime of the server and repeat the check.
   - Status is "Connection available": The connection is possible.
5. If a connection is possible, select "WinCC Unified Control Center > Launch UI Client" in the Windows tray.
6. Log in to Runtime in the "User login" dialog:
   - Enter the user name and password of a user with the necessary function rights.
   - Select another language if required.
   - Confirm your entries.

Result

Runtime is started in kiosk mode.

On the kiosk device, Runtime has access only to the locations configured in the rule.

Note

When using a central user management, My WinCC Unified is displayed in the language you selected when you logged in in the "User login" dialog.
If this language is not available for the current project or if the language setting has not been set in the central user management, the following language is displayed:

- Engineering with TIA Portal: The language for which the lowest number was configured in the Runtime settings.
- Engineering with Online Engineering: The language set as default language in the "Languages" tab in the "Languages and Resources" editor.

If you do not select a language in the "User login" dialog, the application is displayed in the language set for the browser.

See also

Exit Kiosk mode (Page 614)

8.11.4 Exit Kiosk mode

Requirement

Kiosk mode is running.

Procedure

Your procedure depends on how the kiosk mode was configured in the client rule:

Use of Windows shortcut keys disabled, except for Alt+F4 (Default)	1. Press Alt+F4. 2. Depending on the configuration: If you need to enter a PIN to exit, enter the PIN that is configured in the rule.
Use of all Windows shortcut keys disabled	1. Reboot the device.
Use of Windows shortcut keys allowed	1. Press Alt+F4, restart the device or start Windows Task Manager and end the Kiosk process there.

See also

Start kiosk mode (Page 611)

SIMATIC WinCC Unified Station Configurator 9

9.1 Readme SIMATIC WinCC Unified Station Configurator

9.1.1 Security information

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity concept. Siemens' products and solutions only form 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 more information on protective industrial cybersecurity measures for implementation, visit:

https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html)

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends applying product updates as soon as they are available and always using only the latest product versions. 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 at all times, subscribe to the Siemens Industrial Cybersecurity RSS Feed under.

https://new.siemens.com/global/en/products/services/cert.html (https://new.siemens.com/global/en/products/services/cert.html)

See also

www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity)

https://www.siemens.com/cert (https://www.siemens.com/cert)

9.1.2 GDPR - General Data Protection Regulations

Siemens takes data privacy principles, such as the privacy by design and default principle, into account when developing its products and services. For this product WinCC Unified Runtime this means the following:

Personal data processed by the Application

This product collects and processes the following personal data:

- User names, i. e. login data, which might directly contain or establish a reference to the family name and/or first name
- Timestamps: date / time of login, logoff and access
- Location data (time zone)
- Computer name
- IP addresses
- Optional: With UMC, the following additional personal data can be added in the tool:
  - Full name
  - Comment

  This data is not needed for the product functionality and should not be stored on the same medium.

If the user links the above-mentioned data with other data, e. g. shift plans, or stores personal data on the same medium, e. g. hard disk, and thus establishes a personal reference, the user must ensure compliance with data protection regulations.

Purposes

The above data is required for the following purposes:

- Access protection and security measures (e. g. Login, IP address)
- Process synchronization and integrity (e. g. time zone information, IP addresses)
- Archiving system for traceability and verification of processes (e. g. access timestamps)
- Alarm system for traceability and availability (for example, e-mail notification)

The storage of data is appropriate and limited to what is necessary, as it is essential to identify the authorized operators and process events.

Data configuration

The customer can configure the data collected via the product as follows:

- Display data in process pictures
- Data output in form of reports, e. g. for printing or display as electronic file
- Data collection and evaluation in form of graphics, e. g. for KPI analysis

Deletion policy

The product does not provide an automatic deletion of the above data.

If necessary, these can be deleted manually if desired. To do this, refer to the product documentation or contact customer support.

Securing of data

The above data will not be stored anonymously or pseudonymized, because the purpose of access and event identification cannot be achieved otherwise.

For WinCC Unified PC-based, the data specified above should be secured by appropriate technical measures:

- Encryption of log data
- Storing the process data in access-protected SQL databases
  The user must ensure the access protection as part of their process configuration.

You can find information on data backup on the WinCC Unified Comfort Panel in the operating instructions for the Comfort Panel.

9.1.3 Notes on installation

Contents

Information that could not be included in the online help and important information about product features.

Operating system

Installation of SIMATIC WinCC Unified Station Configurator is supported on all client devices with Windows operating system (PCs, notebooks, etc.).

9.1.4 Notes on use

Contents

Information that could not be included in the online help and important information about product features.

Change in name

The application was renamed from "SIMATIC WinCC Unified Control Center" to "SIMATIC WinCC Unified Station Configurator".

No simulation

SIMATIC WinCC Unified Station Configurator does not support Unified Runtime projects of the type "Simulation".

Connection to Unified Runtime web server with Windows server

SIMATIC WinCC Unified Station Configurator does not connect to a Unified PC Runtime web server with a Windows Server operating system.

To enable such a connection, follow these steps on the Runtime web server:

1. In the Group Policy Management Console (GPMC), open "Windows Defender Firewall with Advanced Security".
2. In the navigation area, navigate to "Inbound Rules".
3. Right-click on "Inbound Rules" and select "New Rule".
4. Configure the rules:
   - "Rule type" step: Select the "Port" option.
   - "Protocol and ports" step: Select the "TCP" option and enter "4000" as port under "Specific local ports".
   - "Name" step: Enter the name and description of the rule.
5. Click "Finish".

9.2 SIMATIC WinCC Unified Station Configurator installation

9.2.1 Software and hardware requirements

Operating system

The device has a Windows operating system.

User rights

You have administrator rights on the device.

9.2.2 Starting installation

On a Unified PC with Runtime V19 installed

> **Note**
>
> For the installation of WinCC Unified Runtime V19, the files required for installing WinCC Unified Station Configurator are copied to the PC.

1. Open a File Explorer window.
2. In the installation directory of WinCC Unified Runtime, click the following folder: `StationConfigurator`
3. Double-click the `SIMATIC_WinCC_Unified_Station_Configurator_V19.exe` file.
4. Follow the installation instructions.
5. Reboot the PC.

On devices without Runtime V19 installed

1. Download the download package for SIMATIC WinCC Unified Station Configurator from the Siemens Internet portal to the device and unzip it.
   Alternatively, copy the contents of the folder `<Unified Runtime Installation folder>\StationConfigurator` from a Unified PC with installed Runtime V19 to the client.
2. Double-click the `SIMATIC_WinCC_Unified_Station_Configurator_V19.exe` file.
3. Follow the installation instructions.
4. Reboot the PC.

Result

- The application is installed.
- The SIMATIC WinCC Unified Client Service is installed and running.
- The Windows tray is extended by the icon of the SIMATIC WinCC Unified Station Configurator:

  Commands available via the icon:

  – "Configure Server"
    For configuring the connection to the Runtime web server to which My WinCC Unified and the kiosk mode connect.

  – "My WinCC Unfied"
    At the start of My WinCC Unified.

  – "Launch UI Client"
    To start Runtime in kiosk mode.